# Table of Contents

**Introduction** ........................................................................................................................................................................... 1  
Using the REST API reference......................................................................................................................................................... 1  
Endpoints reference list................................................................................................................................................................. 5  

**Access endpoints** ........................................................................................................................................................................ 24  
Access endpoint descriptions.......................................................................................................................................................... 24  

**Application endpoints** .................................................................................................................................................................. 194  
Application endpoint descriptions.................................................................................................................................................. 194  

**Cluster endpoints** ........................................................................................................................................................................ 222  
Cluster endpoint descriptions.......................................................................................................................................................... 222  

**Configuration endpoints** ............................................................................................................................................................ 356  
Configuration endpoint descriptions.............................................................................................................................................. 356  

**Deployment endpoints** ............................................................................................................................................................... 373  
Deployment endpoint descriptions.................................................................................................................................................. 373  

**Input endpoints** ........................................................................................................................................................................... 432  
Input endpoint descriptions.............................................................................................................................................................. 432  

**Introspection endpoints** ............................................................................................................................................................. 571  
Introspection endpoint descriptions.................................................................................................................................................. 571  

**Knowledge endpoints** ............................................................................................................................................................... 703  
Knowledge endpoint descriptions.................................................................................................................................................... 703  

**KV store endpoints** .................................................................................................................................................................... 838  
KV Store endpoint descriptions........................................................................................................................................................ 838  

**License endpoints** ....................................................................................................................................................................... 860  
License endpoint descriptions.......................................................................................................................................................... 860  

**Metrics Catalog endpoints** ......................................................................................................................................................... 897  
Metrics Catalog endpoint descriptions........................................................................................................................................... 897  

**Output endpoints** ......................................................................................................................................................................... 914  
Output endpoint descriptions........................................................................................................................................................... 914  

**Search endpoints** ......................................................................................................................................................................... 944  
Search endpoint descriptions........................................................................................................................................................... 944  

**System endpoints** ....................................................................................................................................................................... 1129  
System endpoint descriptions........................................................................................................................................................ 1129
Table of Contents

Workload management endpoints.................................................................................................................................1152
Workload management endpoint descriptions..................................................................................................................1152
Introduction

Using the REST API reference

Use the REST API Reference to learn about available endpoints and operations for accessing, creating, updating, or deleting resources. See the REST API User Manual to learn about the Splunk REST API basic concepts.

See the Endpoints reference list for an alphabetical list of endpoints.

Splunk Cloud REST API usage

There are some REST API access and usage differences between Splunk Cloud and Splunk Enterprise. If you are using Splunk Cloud, review details in Access requirements and limitations for the Splunk Cloud REST API.

Splunk REST API admin endpoints

Splunk does not support or document REST API endpoints that contain /admin/ in their URIs. Use the corresponding publicly documented endpoint instead.

Resource groups

Resources are grouped into the following categories.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>Authorize and authenticate users.</td>
</tr>
<tr>
<td>Applications</td>
<td>Install applications and application templates.</td>
</tr>
<tr>
<td>Clusters</td>
<td>Configure and manage indexer clusters and search head clusters.</td>
</tr>
<tr>
<td>Configuration</td>
<td>Manage configuration files and settings.</td>
</tr>
<tr>
<td>Deployment</td>
<td>Manage deployment servers and clients.</td>
</tr>
<tr>
<td>Inputs</td>
<td>Manage data input.</td>
</tr>
<tr>
<td>Introspection</td>
<td>Access system properties.</td>
</tr>
<tr>
<td>Knowledge</td>
<td>Define indexed and searched data configurations.</td>
</tr>
<tr>
<td>KV store</td>
<td>Manage app key-value store.</td>
</tr>
<tr>
<td>Licensing</td>
<td>Manage licensing configurations.</td>
</tr>
<tr>
<td>Outputs</td>
<td>Manage forwarder data configuration.</td>
</tr>
<tr>
<td>Search</td>
<td>Manage searches and search-generated alerts and view objects.</td>
</tr>
<tr>
<td>System</td>
<td>Manage server configuration.</td>
</tr>
<tr>
<td>Workload management</td>
<td>Manage system resources for search workloads.</td>
</tr>
</tbody>
</table>

See the Endpoints reference list for an alphabetical list of endpoints.
Available operations

Depending on the endpoint, GET, POST, and/or DELETE operations are available for accessing, creating, updating, or deleting resources. Some operations have specific capability requirements, as noted.

Using endpoint reference entries

Reference information for each endpoint in the REST API includes the following items.

- URL
- Usage details
- Expandable elements showing available operations (GET, POST, and/or DELETE) for the endpoint.

Expand a GET, POST, or DELETE element to show the following usage information about the operation.

- Request parameter information and requirements.
- Returned values included in the response.
- Example request and response.

Request and response details

Pagination and filtering parameters

In addition to the parameters specific to each endpoint and operation, the following request parameters are valid for some GET methods.

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Number</td>
<td>30</td>
<td>Maximum number of entries to return. Set value to 0 to get all available entries.</td>
</tr>
<tr>
<td>f</td>
<td>String</td>
<td></td>
<td>Filters the response to include only the named values. Specify multiple times to return multiple values. Examples:&lt;br&gt;[ f=\text{qualifiedSearch} ] returns only the value for \text{qualifiedSearch}.&lt;br&gt;[ f=s* ] returns all the values that have names beginning with \text{s}.&lt;br&gt;[ f=\text{qualifiedSearch} &amp; f=\text{is_visible} ] returns the values for \text{qualifiedSearch} as well as \text{is_visible}.</td>
</tr>
<tr>
<td>offset</td>
<td>Number</td>
<td>0</td>
<td>Index of first item to return.</td>
</tr>
<tr>
<td>search</td>
<td>String</td>
<td></td>
<td>Response filter, where the response field values are matched against this search expression. Example:&lt;br&gt;[ search=foo ] matches on any field with the string \text{foo} in the name.&lt;br&gt;[ search=\text{name%3Dfield_value} ] restricts the match to a single field. (Requires URI-encoding.)</td>
</tr>
<tr>
<td>sort_dir</td>
<td>Enum</td>
<td>asc</td>
<td>Response sort order:</td>
</tr>
</tbody>
</table>
### Returned values

The response to GET and other requests typically includes key-value pairs representing details about the resource that you are accessing. Returned values specific to the resource and/or operation are listed along with their descriptions.

### HTTP status codes

Responses can include HTTP status codes. Standard HTTP status codes are not included in endpoint documentation, but status codes with specific meaning for an endpoint and/or operation are noted.

### Error messages

Requests with an error, such as a missing required parameter, can prompt an error response like the following example.

```xml
<response>
  <messages>
    <msg type="ERROR">
      In handler 'datamodelgenerate': The following required arguments are missing: sid.
    </msg>
  </messages>
</response>
```

### EAI response data

EAI response data, the `<eai:acl>` and `<eai:attributes>` elements, typically apply to all endpoints and are configuration-dependent, so redundant explanation is omitted. These elements are also elided from the response examples to make the documentation easier to read.

### Access Control List (ACL) [eai:acl]

The REST implementation enforces ownership and permissions for a resource based on application context namespace. The ACL includes the following parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
|        |          | asc = ascending 
|        |          | desc = descending |
| sort_key | String   | name    | Field name to use for sorting. |
| sort_mode | Enum     | auto    | Collated ordering: |
|          |          | auto = If all field values are numeric, collate numerically. Otherwise, collate alphabetically. |
|          |          | alpha = Collate alphabetically, not case-sensitive. |
|          |          | alpha_case = Collate alphabetically, case-sensitive. |
|          |          | num = Collate numerically. |
| summarize | Bool     | false   | Response type: |
|          |          | true = Summarized response, omitting some index details, providing a faster response. |
|          |          | false = full response. |
---

**app**
The app context for the resource. Allowed values are:
- The name of an app
- system

**can_list**
For internal use only for the Splunk Web manager UI.

**can_share_***
Indicates whether or not the current user can change the sharing state. The sharing state can be one of:
- can_share_app = App-level sharing
- can_share_global = Global sharing
- can_share_user = User-level sharing

**can_write**
Indicates whether or not the current user can edit this item.

**owner**
The user that owns the resource.
A value of nobody indicates that all users have access to the resource, but that write access to the resource might be restricted.

**modifiable**
Indicates whether or not you can change the Access Control List (ACL).
Set to false for items not controlled by ACLs, such as items under /server/logger.

**perms.read**
Properties that indicate read permissions of the resource.

**perms.write**
Properties that indicate write permissions of the resource.

**removable**
Indicates if an admin or user with sufficient permissions can remove the entity.

**sharing**
Indicates how the resource is shared. Allowed values are:
- app = Shared through an app.
- global = Shared to all apps.
- user = Private to a user.

**Note:** You can append /acl to an endpoint to access its ACL properties. For more information, see Access Control List in the REST API User Manual.

---

**EAI attributes [eai:attributes]**

The eai:attributes element shows the mandatory and optional fields.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>optionalFields</td>
<td>Field is optional.</td>
</tr>
<tr>
<td>requiredFields</td>
<td>Field is required.</td>
</tr>
<tr>
<td>wildcardFields</td>
<td>Field can use wildcard.</td>
</tr>
</tbody>
</table>

**References**

See the following resources for more information on working with the Splunk REST API.

- REST API User Manual
- REST API Tutorials

---

4
Endpoints reference list

Navigate to specific endpoints and review available REST operations. Endpoints are listed alphabetically.

The PUT operation is not available for REST API endpoints. Depending on the endpoint, you can use a POST operation to create and/or update resources. Check specific endpoints for details.

Namespace access

Some resources in the REST API are associated with specific namespaced user and app contexts.

To access namespaces associated with all users, all apps, or resources shared by all users for an endpoint (similar to ‘file gloving’ or ‘recursion’ of input directories), make a GET request using servicesNS with wildcard - characters for the app and user. For example, use /servicesNS/~/-/saved/searches.

For more details, see Namespace in the REST API User Manual.

Endpoints

Jump to: A - C - D - I - L - M - P - R - S

<table>
<thead>
<tr>
<th>URI</th>
<th>Summary</th>
<th>GET</th>
<th>PUT</th>
<th>POST</th>
<th>DEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/LDAP-groups</td>
<td>Access Manage LDAP authentication.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/metrics-reload/_metrics</td>
<td>Access Reload the metrics processor after updating a metrics-related configuration.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/ProxySSO-auth</td>
<td>Access Manage ProxySSO mappings and configurations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/replicate-SAML-certs</td>
<td>Access Manage SAML authentication.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/Rsa-MFA</td>
<td>Access Configure RSA Multifactor Authentication.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/SAML-groups</td>
<td>Access Convert external groups in an IdP response to internal Splunk platform roles.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/SAML-idp-metadata</td>
<td>Access Access IdP SAML metadata attributes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/SAML-sp-metadata</td>
<td>Access Access service provider SAML metadata</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>admin/SAML-user-role-map</td>
<td>Access or create SAML user and role information for saved searches if your IdP does not support Attribute Query Requests.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>admin/SAML-user-role-map/{name}</td>
<td>Access or create SAML user and role information for saved searches if your IdP does not support Attribute Query Requests.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>alerts/</td>
<td></td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>alerts/alert_actions</td>
<td>Search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>alerts/fired_alerts</td>
<td>Search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>alerts/fired_alerts/{name}</td>
<td>Search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apps/</td>
<td></td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>apps/appinstall</td>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apps/apptemplates</td>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apps/apptemplates/{name}</td>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apps/local</td>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apps/local/{name}</td>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apps/local/{name}/package</td>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apps/local/{name}/setup</td>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>apps/local/{name}/update</td>
<td>Applications</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication/</td>
<td></td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>auth/login</td>
<td>Access control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication/current-context</td>
<td>Access control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication/current-context/{name}</td>
<td>Access specific user context</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication/httpauth-tokens</td>
<td>Access control</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication/httpauth-tokens/{name}</td>
<td>Manage session tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>authentication/ldap-auth</td>
<td>Access Create and manage LDAP strategies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication/providers/saml</td>
<td>Access control Access and create SAML configurations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication/providers/saml/{stanza_name}</td>
<td>Access control Access and update SAML configurations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication/users</td>
<td>Access control Manage user accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authentication/users/{name}</td>
<td>Access control Manage specific user account</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorization/</td>
<td>GET PUT Post DELETE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorization/capabilities</td>
<td>Access control Access capability authorization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorization/grantable_capabilities</td>
<td>Access control Access capabilities that current user can grant.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorization/roles</td>
<td>Access control Access user roles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorization/roles/{name}</td>
<td>Access control Access specific user role</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorization/tokens</td>
<td>Access control Access authentication tokens</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>authorization/tokens/{user}</td>
<td>Access control Access authentication tokens for a specific user</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>catalog/</td>
<td>GET PUT Post DELETE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>catalog/metricstore/metrics</td>
<td>Metrics List metric names.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>catalog/metricstore/dimensions</td>
<td>Metrics List dimension names.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>catalog/metricstore/dimensions/{dimension-name}/values</td>
<td>Metrics List values for given dimensions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>catalog/metricstore/rollup</td>
<td>Metrics Retrieve lists of metric indexes and their rollup summaries. Create new rollup policies for a given metric index.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>catalog/metricstore/rollup/{index}</td>
<td>Metrics Manage rollup summaries and rollup policies associated with a specific source {index}.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/</td>
<td>GET PUT Post DELETE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/config</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>cluster/config/config</td>
<td>Access cluster configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/buckets</td>
<td>Access master node bucket configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/buckets/{name}</td>
<td>Access specific bucket configuration, master node</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/control/control/rebalance_primaries</td>
<td>Access master controls to rebalance primary buckets across peers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/control/control/remove_peers</td>
<td>Remove disabled peer nodes.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/control/control/roll-hot-buckets</td>
<td>Force a specified bucket in an indexer cluster to roll from hot to warm.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/control/control/rolling_upgrade_finalize</td>
<td>Finalizes indexer cluster rolling upgrade.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/control/control/rolling_upgrade_init</td>
<td>Initializes indexer cluster rolling upgrade.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/generation</td>
<td>Access current generations information, master node</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/generation/{name}</td>
<td>Access specific generation information, cluster master</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/indexes</td>
<td>Access cluster index information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/indexes/{name}</td>
<td>Access specific cluster index information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/info</td>
<td>Access cluster master node information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/health</td>
<td>Performs health checks</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/peers</td>
<td>Access peer information, master node</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/peers/{name}</td>
<td>Access specific master node peer information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/sites</td>
<td>Access cluster site information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/sites/{name}</td>
<td>Access specific cluster site information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/master/status</td>
<td>Status of rolling restart</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>cluster/searchhead/generation</td>
<td>Clusters Access searchhead peer information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/searchhead/generation/{name}</td>
<td>Clusters Access specific searchhead peer information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/searchhead/searchheadconfig</td>
<td>Clusters Access cluster configuration for searchhead</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/searchhead/searchheadconfig/{name}</td>
<td>Clusters Access specific cluster node</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/slave/buckets</td>
<td>Clusters Access peer bucket configuration information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/slave/buckets/{name}</td>
<td>Clusters Access specific peer bucket configuration information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/slave/control/control/decommission</td>
<td>Clusters Decommission indexer cluster peer node</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/slave/control/control/set_manual_detention</td>
<td>Clusters Configure indexer detention.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/slave/info</td>
<td>Clusters Access peer node information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>cluster/slave/info/{name}</td>
<td>Clusters Access information about specific peer</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>configs/</td>
<td>Configuration Raw access to .conf files</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>configs/conf-{file}</td>
<td>Configuration Raw access to specific .conf file</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/</td>
<td>Search Access search commands</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>data/commands</td>
<td>Search Access specific search command</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/commands/{name}</td>
<td>Search Access specific search command</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/index-volumes</td>
<td>Indexes Access logical drive information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/index-volumes/{name}</td>
<td>Indexes Access information for a logical drive</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/indexes</td>
<td>Indexes Manage data indexes</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/indexes/{name}</td>
<td>Indexes Manage specific data index</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/indexes-extended</td>
<td>Indexes Access index bucket level information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/indexes-extended/{name}</td>
<td>Indexes Access specific index bucket level information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>data/inputs/ad</td>
<td>Inputs, Access Active Directory monitoring input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/ad/{name}</td>
<td>Inputs, Access Active Directory monitoring stanza</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/all</td>
<td>Inputs, Access all inputs, including Modular Inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/all/{name}</td>
<td>Inputs, Access specific input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/http</td>
<td>Input, Configure HTTP Event Collection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/http/{name}</td>
<td>Input, Configure HTTP Event Collection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/monitor</td>
<td>Inputs, Access monitor inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/monitor/{name}</td>
<td>Inputs, Manage specific monitor input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/monitor/{name}/members</td>
<td>Inputs, Access files for the specific monitor input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/oneshot</td>
<td>Inputs, Access one-shot inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/oneshot/{name}</td>
<td>Inputs, Access specific one-shot input information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/registry</td>
<td>Inputs, Access Windows registry monitor input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/registry/{name}</td>
<td>Inputs, Manage Windows registry monitor stanza</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/script</td>
<td>Inputs, Manage scripted inputs settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/script/restart</td>
<td>Inputs, Restart scripted input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/script/{name}</td>
<td>Inputs, Manage specific scripted input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/cooked</td>
<td>Inputs, Access forwarder TCP inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/cooked/{name}</td>
<td>Inputs, Manage TCP inputs for specific host:port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/cooked/{name}/connections</td>
<td>Inputs, Access connections for specific port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/raw</td>
<td>Inputs, Manage raw forwarder TCP inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/raw/{name}</td>
<td>Inputs, Access raw TCP input information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/raw/{name}/connections</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>data/inputs/tcp/splunktcpinput</td>
<td>Manage raw TCP input information for specific host:port</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/splunktcpinput/{name}</td>
<td>Manage receiver access using tokens.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/splunktcpinput/{name}</td>
<td>Manage existing receiver tokens.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/ssl</td>
<td>Access SSL configuration information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/tcp/ssl/{name}</td>
<td>Access SSL configuration for specific host</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/token/http</td>
<td>Access http inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/token/http/{name}</td>
<td>Manage specific http input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/token/http/{name}/enable</td>
<td>Enable the {name} HTTP Event Collector token.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/token/http/{name}/disable</td>
<td>Disable the {name} HTTP Event Collector token.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/udp</td>
<td>Access UDP inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/udp/{name}</td>
<td>Manage specific UDP input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/udp/{name}/connections</td>
<td>Manage specific UDP input connection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/win-event-log-collections</td>
<td>Access all configured event log collections</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/win-event-log-collections/{name}</td>
<td>Manage specific event log</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/win-perfmon</td>
<td>Access Windows performance monitor information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/win-perfmon/{name}</td>
<td>Manage specific performance monitor configuration stanza</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/win-wmi-collections</td>
<td>Access configured WMI collections</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/inputs/win-wmi-collections/{name}</td>
<td>Manage specific WMI collection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/lookup-table-files</td>
<td>Access lookup table files</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td><code>data/lookup-table-files/{name}</code></td>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific lookup table file</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/modular-inputs</code></td>
<td>Inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access defined modular inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/modular-inputs/{name}</code></td>
<td>Inputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific modular input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/outputs/tcp/default</code></td>
<td>Outputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access global TCP output properties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/outputs/tcp/default/{name}</code></td>
<td>Outputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific TCP output property setting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/outputs/tcp/group</code></td>
<td>Outputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access data forwarding group configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/outputs/tcp/group/{name}</code></td>
<td>Outputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific data forwarding group</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/outputs/tcp/server</code></td>
<td>Outputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access data forwarding configurations</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/outputs/tcp/server/{name}</code></td>
<td>Outputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific forwarder configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/outputs/tcp/server/{name}/allconnections</code></td>
<td>Outputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access current connections for specific forwarder</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/outputs/tcp/syslog</code></td>
<td>Outputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access forwarded server configured to provide data in standard syslog format</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/outputs/tcp/syslog/{name}</code></td>
<td>Outputs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific forwarder, which sends data in syslog format</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/props/calcfields</code></td>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access props.conf file calculated fields</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/props/calcfields/{name}</code></td>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific props.conf file calculated field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/props/extractions</code></td>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access props.conf file search-time field extractions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/props/extractions/{name}</code></td>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific props.conf file extraction</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/props/fieldaliases</code></td>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access props.conf file field aliases</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/props/fieldaliases/{name}</code></td>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific props.conf file field alias</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/props/lookups</code></td>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access props.conf file automatic lookups</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><code>data/props/lookups/{name}</code></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>data/props/sourcetype-rename</td>
<td>Manage specific props.conf file sourcetype name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/props/sourcetype-rename/(name)</td>
<td>Access renamed sourcetypes configured in props.conf file</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/summaries</td>
<td>Introspection Get disk usage information about all summaries in an indexer.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/summaries/{summary_name}</td>
<td>Introspection Get disk usage information about a particular summary in an indexer.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/transforms/extractions</td>
<td>Knowledge Access field extraction definitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/transforms/extractions/{name}</td>
<td>Knowledge Manage specific field extraction definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/transforms/lookups</td>
<td>Knowledge Access transforms.conf file lookup definitions</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/transforms/lookups/{name}</td>
<td>Knowledge Manage specific transforms.conf file lookup definition</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/transforms/metric-schema</td>
<td>Knowledge Review and manage ingest-time log-to-metrics configurations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/transforms/statsdextractions</td>
<td>Knowledge Configure metrics dimension extraction for StatsD.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/ui/panels</td>
<td>Knowledge Create dashboard panel XML definitions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/ui/views</td>
<td>Knowledge Create dashboard XML definitions.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>data/ui/views/{name}</td>
<td>Knowledge Access, update, or delete dashboard XML.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>datamodel/</td>
<td>Knowledge Access information about data models</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>datamodel/model</td>
<td>Knowledge Access information about data models</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>datamodel/model/{name}</td>
<td>Knowledge Access information about a data model</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>datamodel/pivot</td>
<td>Knowledge Access pivots based on named data models</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>deployment/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/client</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment client information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/client/config</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment client configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/client/config/listsIsDisabled</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment client state information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/client/config/reload</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment client reload information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/client/{name}/reload</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific deployment client reload</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/applications</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment server application and class information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/applications/{name}</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific server client application and class information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/clients</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment server client information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/clients/countClients_by_machineType</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment server client information by machine type</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/clients/countRecentDownloads</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access client download information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/clients/{name}</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific client</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/config</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment server configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/config/attributesUnsupportedInUI</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment server attributes not available using Splunk Web</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/config/listsIsDisabled</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access deployment server state</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/serverclasses</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access server class information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/serverclasses/{name}</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific server class of deployment server</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>deployment/server/serverclasses/rename</td>
<td>Deployment</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage server class name</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>directory/</td>
<td></td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>directory</td>
<td>Knowledge</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access user-configurable entities</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>directory/(name)</td>
<td>Knowledge</td>
<td>GET</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific entity in directory service</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>indexing/</td>
<td>enumeration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>indexing/preview</td>
<td>Deployment Preview events from a file before indexing</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>indexing/preview/{job_id}</td>
<td>Inputs Access <code>props.conf</code> file settings for specific data preview job</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kvstore/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kvstore/backup/create</td>
<td>KV store Create a KV Store backup archive file.</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>kvstore/backup/restore</td>
<td>KV store Extracts the KV Store backup archive file and restores the KV Store.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>kvstore/status</td>
<td>KV store Access KV store status information for standalone or search head clustering (SHC) deployments.</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>licenser/</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>licenser/groups</td>
<td>Licensing Access licenser groups configuration</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>licenser/groups/{name}</td>
<td>Licensing Manage specific licenser group configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>licenser/licenses</td>
<td>Licensing Access licenses</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>licenser/licenses/{name}</td>
<td>Licensing Manage specific license</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>licenser/localslave</td>
<td>Licensing Get information about relevant license state for the splunk instance.</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>licenser/messages</td>
<td>Licensing Access licenser messages</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>licenser/messages/{name}</td>
<td>Licensing Access specific licenser message</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>licenser/pools</td>
<td>Licensing Access licenser pool information</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>licenser/pools/{name}</td>
<td>Licensing Manage specific licenser pool</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>licenser/slaves</td>
<td>Licensing Access license master slaves</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>licenser/slaves/{name}</td>
<td>Licensing Access specific license master slave</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>licenser/stacks</td>
<td>Licensing Access license stack configuration</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>licenser/stacks/{name}</td>
<td>Licensing Access specific license master slave</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>licensing</td>
<td>Access specific license stack configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>messages/</td>
<td>GET PUT POST DELETE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>messages</td>
<td>System Manage system messages</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>messages/(name)</td>
<td>System Manage specific system message</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>properties/</td>
<td>GET PUT POST DELETE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>properties</td>
<td>Configuration Access configuration files</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>properties/(file_name)</td>
<td>Configuration Manage specific configuration file</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>properties/(file_name)/(stanza_name)</td>
<td>Configuration Manage specific configuration file stanzas</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>properties/(file_name)/(stanza_name)/(key_name)</td>
<td>Configuration Manage specific stanza in specific configuration file</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>receivers/</td>
<td>GET PUT POST DELETE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>receivers/simple</td>
<td>Inputs Use HTTP to send events</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>receivers/stream</td>
<td>Inputs Use socket to stream events</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>receivers/token</td>
<td>Input Log events using HTTP Input with application authentication token.</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>receivers/token/event</td>
<td>Input Post JSON formatted data to the data input endpoint.</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>receivers/token/event/1.0</td>
<td>Input Post JSON formatted data to the data input endpoint.</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>receivers/token/mint</td>
<td>Input Post MINT formatted data to the data input endpoint.</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>receivers/token/mint/1.0</td>
<td>Input Post MINT formatted data to the data input endpoint.</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>saved/</td>
<td>GET PUT POST DELETE</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>saved/eventtypes</td>
<td>Knowledge Manage saved event types</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>saved/eventtypes/(name)</td>
<td>Knowledge Manage specific saved event type</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>----------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>saved/searches</td>
<td>Search Manage saved searches configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>saved/searches/(name)</td>
<td>Search Manage specific saved search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>saved/searches/(name)/acknowledge</td>
<td>Search Manage saved search alerting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>saved/searches/(name)/dispatch</td>
<td>Search Dispatch saved search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>saved/searches/(name)/history</td>
<td>Search Access saved search job history</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>saved/searches/(name)/reschedule</td>
<td>Search Manage saved search job scheduling</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>saved/searches/(name)/scheduled_times</td>
<td>Search Access saved search scheduled times</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>saved/searches/(name)/suppress</td>
<td>Search Access saved search alerting state</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduled/</td>
<td>Get</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduled/views</td>
<td>Search Access scheduled views for PDF delivery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduled/views/(name)</td>
<td>Search Manage specific scheduled view</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduled/views/(name)/dispatch</td>
<td>Search Dispatch search for specific scheduled view</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduled/views/(name)/history</td>
<td>Search Access specific scheduled view job history</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduled/views/(name)/reschedule</td>
<td>Search Manage scheduled view scheduling</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>scheduled/views/(name)/scheduled_times</td>
<td>Search Access specific scheduled view times</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/</td>
<td>Get</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/concurrency-settings</td>
<td>Search List search concurrency settings.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/concurrency-settings/scheduler</td>
<td>Search Edit settings for concurrent scheduled search limits.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/concurrency-settings/search</td>
<td>Search Edit settings for the maximum number of concurrent scheduled searches.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/distributed/bundle/replication/config</td>
<td>Deployment Provides information on knowledge bundle replication configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/distributed/bundle/replication/cycles</td>
<td>Deployment Provides information and status for knowledge bundle replication cycles</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>search/distributed/bundle-replication-files</td>
<td>Deployment Access distributed search bundle replication files</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/distributed/bundle-replication-files/(name)</td>
<td>Deployment Access specific search bundle replication file</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/distributed/config</td>
<td>Deployment Access distributed search options</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/distributed/peers</td>
<td>Deployment Manage distributed server peers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/distributed/peers/(name)</td>
<td>Deployment Manage distributed server peers</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/fields</td>
<td>Knowledge Access search field configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/fields/(field_name)</td>
<td>Knowledge Access specific search field configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/fields/(field_name)/tags</td>
<td>Knowledge Manage tags associated with specific search field</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs</td>
<td>Search Manage search jobs</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs/(search_id)</td>
<td>Search Manage specific search job</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs/(search_id)/control</td>
<td>Search Execute job control command for specific search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs/(search_id)/events</td>
<td>Search Access events for specific search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs/(search_id)/results</td>
<td>Search Access results of specific search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs/(search_id)/results_preview</td>
<td>Search Access preview results for specific search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs/(search_id)/search.log</td>
<td>Search Access search.log file for specific search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs/(search_id)/summary</td>
<td>Search Access getFieldsAndStats output of so-far-read events</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs/(search_id)/timeline</td>
<td>Search Access event distribution over time</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/jobs/export</td>
<td>Search Stream search results</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/parser</td>
<td>Search Access search language parsing services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/scheduler</td>
<td>Search Access search scheduler enablement status.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>----------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>search/scheduler/status</td>
<td>Search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disable or enable the search scheduler.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/tags/{tag_name}</td>
<td>Knowledge</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific search time tag</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/timeparser</td>
<td>Search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Parse time argument</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search/typeahead</td>
<td>Search</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Suggest search string auto-completion strings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/</td>
<td>System</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>server/control</td>
<td>Access server controls</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/control/restart</td>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restart Splunk Enterprise splunkd server daemon.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/control/restart_webui</td>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restart Splunk Enterprise splunkweb Web interface process.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/httpsettings/proxysettings</td>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Create an HTTP proxy configuration stanza.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/httpsettings/proxysettings/proxyConfig</td>
<td>Update HTTP proxy settings.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/info</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Splunk instance information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/sysinfo</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access server information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/health/deployment</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access distributed deployment overall health status informa</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/health/deployment/details</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access distributed deployment feature health status informa</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/health/splunkd</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access splunkd health status information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/health/splunkd/details</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access splunkd feature health status information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/health-config</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access splunkd health report configuration information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/health-config/{alert_action}</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configure alert actions for the splunkd health report.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/health-config/{feature_name}</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edit feature and indicator settings for the splunkd health report.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>server/introspection</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>List introspection resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/introspection/indexer</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Get indexer status</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/introspection/kvstore</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>List app kvstore status resources</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/introspection/kvstore/collectionstats</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Get storage statistics for a collection.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/introspection/kvstore/replicasetstats</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Get the status of the replica set from the point of view of the current server.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/introspection/kvstore/serverstatus</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Get an overview of the database process state.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/introspection/search/saved</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check most recent search scheduling details.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/logger</td>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access logging categories</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/logger/{name}</td>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Manage specific logging category</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/pipelinesets</td>
<td>Input</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access information on an indexer's ingestion pipeline sets.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/roles</td>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access server configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/security/rotate-splunk-secret</td>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rotate the splunk.secret key file on a standalone Splunk Enterprise installation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/settings</td>
<td>System</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access server configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/status</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access system status information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/status/dispatch-artifacts</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access search job information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/status/fishbucket</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access information about the private BTree database</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/status/installed-file-integrity</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check for system file irregularities.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/status/limits/search-concurrency</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access search concurrency metrics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/status/partitions-space</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access disk utilization information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/status/resource-usage</td>
<td>Introspection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access current resource utilization information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DEL</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>-----</td>
</tr>
<tr>
<td>server/status/resource-usage/hostwide</td>
<td>Introspection Access host-level resource utilization information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/status/resource-usage/iostats</td>
<td>Introspection Access the most recent disk I/O statistics for each disk. This endpoint is currently available only for Linux.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>server/status/resource-usage/splunk-processes</td>
<td>Introspection Access operating system resource utilization information</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>services/collector</td>
<td>Input Log events using HTTP Event Collector.</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>services/collector/ack</td>
<td>Input Query event indexing status.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>services/collector/event</td>
<td>Input Post JSON formatted data to the data input endpoint.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>services/collector/health</td>
<td>Input Checks if HEC is healthy and able to accept new data from a load balancer.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>services/collector/mint</td>
<td>Input Post MINT formatted data to the data input endpoint.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>services/collector/raw</td>
<td>Input Send raw data directly to the indexer queue.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/</td>
<td>Clusters</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>shcluster/captain/artifacts</td>
<td>Get artifact configuration information for a cluster captain node.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/captain/artifacts/{name}</td>
<td>Clusters Get artifact configuration information for {name} node.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/captain/control/control/upgrade-init</td>
<td>Clusters Initiate rolling upgrade of SHC.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/captain/control/control/upgrade-finalize</td>
<td>Clusters Finish rolling upgrade of SHC.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/captain/control/control/rotate-splunk-secret</td>
<td>System Rotate the splunk.secret key file on all nodes of a Splunk Enterprise search head cluster</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/captain/control/default/restart</td>
<td>Clusters Initiate rolling restart of SHC.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/captain/info</td>
<td>Clusters Access information about searchhead cluster captain node.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>shcluster/captain/jobs</td>
<td>Clusters List running and recently finished jobs for all cluster members.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/captain/jobs/{name}</td>
<td>Clusters Get running and recently finished jobs for {name} cluster.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/captain/members</td>
<td>Clusters List cluster members.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/captain/members/{name}</td>
<td>Clusters Get information about the {name} searchhead cluster member.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/config</td>
<td>Clusters List searchhead cluster node configuration.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/config/config</td>
<td>Clusters Configure search head cluster members.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/member/artifacts</td>
<td>Clusters Get searchhead cluster member artifact configuration.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/member/artifacts/{name}</td>
<td>Clusters Get {name} member artifact configuration.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/member/consensus</td>
<td>Clusters Get latest cluster configuration from the raft consensus protocol.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/member/control/control/set_manual_detention</td>
<td>Clusters Adjust search head manual detention mode.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/member/info</td>
<td>Clusters Get searchhead cluster member node information.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>shcluster/status</td>
<td>Clusters Determine SHC health status.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>replication/configuration/health</td>
<td>Clusters Get configuration replication health statistics for a SHC.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**storage/**

<table>
<thead>
<tr>
<th>URI</th>
<th>Summary</th>
<th>GET</th>
<th>PUT</th>
<th>POST</th>
<th>DELETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage/passwords</td>
<td>Access control Manage authentication credentials</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>storage/passwords/{name}</td>
<td>Access control Manage specific authentication credential</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**storage/collections**

<table>
<thead>
<tr>
<th>URI</th>
<th>Summary</th>
<th>GET</th>
<th>PUT</th>
<th>POST</th>
<th>DELETE</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage/collections/config</td>
<td>KV store Create or list connections.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>storage/collections/config/{collection}</td>
<td>KV store Manage a specific collection.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>storage/collections/data/{collection}</td>
<td>KV store Manage items of a collection.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>URI</td>
<td>Summary</td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>-----</td>
<td>---------</td>
<td>-----</td>
<td>-----</td>
<td>------</td>
<td>--------</td>
</tr>
<tr>
<td>storage/collections/data/{collection}/{id}</td>
<td>KV store Manage a specific item of a collection.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>storage/collections/data/{collection}/batch_save</td>
<td>KV store Perform multiple save operations.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>workloads/</td>
<td></td>
<td>GET</td>
<td>PUT</td>
<td>POST</td>
<td>DELETE</td>
</tr>
<tr>
<td>workloads/categories</td>
<td>Workloads List and edit workload categories.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>workloads/config/enable</td>
<td>Workloads Enable workload management.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>workloads/config/disable</td>
<td>Workloads Disable workload management.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>workloads/config/get-base-dirname</td>
<td>Workloads Get the name of the splunk parent cgroup.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>workloads/config/set-base-dirname</td>
<td>Workloads Set the name of the splunk parent cgroup.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>workloads/status</td>
<td>Workloads Get information on the current status of workload management.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>workloads/pools</td>
<td>Workloads Perform CRUD operations on workload pools.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>workloads/rules</td>
<td>Workloads Perform CRUD operations on workload rules.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Access endpoints

Access endpoint descriptions

Access and manage user credentials.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select Settings > Access controls and click Users. To determine the capabilities assigned to a role, select Settings > Access controls and click Roles.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

Managed Splunk Cloud deployments
Use the following URL for managed deployments. If necessary, submit a support case to open port 8089 on your deployment.

https://<deployment-name>.splunkcloud.com:8089

Self-service Splunk Cloud deployments
Use the following URL for self-service deployments. To get the required non-SAML user credentials, submit a support case.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the Splunk REST API Tutorials for more information.
admin/Duo-MFA

Configure Duo Multifactor authentication.

Authentication and Authorization
Requires the change_authentication capability.

Usage details
Disable any SSO configurations, such as SAML, before enabling Duo authentication for the first time. Duo only works with local auth types.

GET

List Duo Multifactor configuration settings.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Configuration stanza name</td>
</tr>
<tr>
<td>integrationKey</td>
<td>Duo integration key for Splunk. Must be of size = 20.</td>
</tr>
<tr>
<td>secretKey</td>
<td>Shared secret key between Splunk and Duo.</td>
</tr>
<tr>
<td>apiHostname</td>
<td>Duo REST API endpoint used by Splunk for multifactor authentication</td>
</tr>
<tr>
<td>appSecretKey</td>
<td>Splunk application specific secret key. Must be a random generated hex of length 40 or more.</td>
</tr>
<tr>
<td>failOpen</td>
<td>Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to false.</td>
</tr>
<tr>
<td>timeout</td>
<td>Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>SSL version to use for accessing the Duo REST API. Defaults to Splunkd sslVersion.</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd cipherSuite.</td>
</tr>
<tr>
<td>ecdhCurves</td>
<td>ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd ecdhCurves.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Boolean indicating if Duo server certificate verification is required. Defaults to false.</td>
</tr>
<tr>
<td>sslRootCAPath</td>
<td>Full path of the certificate to be used for certificate verification if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>Common name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>Alternate name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>useClientSSLCompression</td>
<td>Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd useClientSSLCompression.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
admin:changeme -X GET https://localhost:8089/services/admin/Duo-MFA

XML Response

<title>Duo-MFA</title>
<id>https://localhost:8089/services/admin/Duo-MFA</id>
<updated>2016-07-26T11:05:14-07:00</updated>
<generator build="321df14f210847b51259ee2d4eeacb4184dc6679" version="20160720"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/Duo-MFA/_new" rel="create"/>
<link href="/services/admin/Duo-MFA/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>duo-mfa</title>
  <id>https://localhost:8089/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa</id>
  <updated>2016-07-26T11:05:14-07:00</updated>
  <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="list"/>
  <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="edit"/>
  <link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="apiHostname">api-cc7a8eab.duosecurity.com</s:key>
      <s:key name="appSecretKey">$1$cQdFd4+XlOrAfqQWwe+VevD/MOOFTIA4vwoaFncX0V0TO8ZsCsKQ</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">system</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s,key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">*
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
POST

Create a Duo Multifactor configuration.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td><strong>Required.</strong> Configuration stanza name</td>
</tr>
<tr>
<td>integrationKey</td>
<td>See description</td>
<td><strong>Required.</strong> Duo integration key for Splunk. Must be of size = 20.</td>
</tr>
<tr>
<td>secretKey</td>
<td>See description</td>
<td><strong>Required.</strong> Shared secret key between Splunk and Duo.</td>
</tr>
<tr>
<td>apiHostname</td>
<td>See description</td>
<td><strong>Required.</strong> Duo REST API endpoint used by Splunk for multifactor authentication</td>
</tr>
<tr>
<td>appSecretKey</td>
<td>See description</td>
<td><strong>Required.</strong> Splunk application specific secret key. Must be a random generated hex of length 40 or more.</td>
</tr>
<tr>
<td>failOpen</td>
<td>Boolean</td>
<td>Optional. Indicates whether Splunk should bypass the Duo service if it is unavailable. Defaults to false.</td>
</tr>
<tr>
<td>timeout</td>
<td>Positive integer</td>
<td>Optional. Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>See description</td>
<td>Optional. SSL version to use for accessing the Duo REST API. Defaults to Splunkd sslVersion.</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>See description</td>
<td>Optional. Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd cipherSuite.</td>
</tr>
<tr>
<td>ecdhCurves</td>
<td>See description</td>
<td>Optional. ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd ecdhCurves.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Boolean</td>
<td>Optional. Indicates if Duo server certificate verification is required. Defaults to false. If set to true, provide a sslRootCAPath to ensure successful certificate validation.</td>
</tr>
<tr>
<td>sslRootCAPath</td>
<td>See description</td>
<td>Optional. Full path of the certificate to be used for certificate verification. If sslVerifyServerCert is true, this path must be provided to ensure successful certificate validation.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>See description</td>
<td>Optional. Common name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>See description</td>
<td>Optional. Alternate name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>useClientSSLCompression</td>
<td>See description</td>
<td>Optional. Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd useClientSSLCompression.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Configuration stanza name</td>
</tr>
<tr>
<td>integrationKey</td>
<td>Duo integration key for Splunk. Must be of size = 20.</td>
</tr>
<tr>
<td>secretKey</td>
<td>Shared secret key between Splunk and Duo.</td>
</tr>
<tr>
<td>apiHostname</td>
<td>Duo REST API endpoint used by Splunk for multifactor authentication</td>
</tr>
<tr>
<td>appSecretKey</td>
<td>Splunk application specific secret key. Must be a random generated hex of length 40 or more.</td>
</tr>
<tr>
<td>failOpen</td>
<td>Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to false.</td>
</tr>
<tr>
<td>timeout</td>
<td>Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>SSL version to use for accessing the Duo REST API. Defaults to Splunkd sslVersion.</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd cipherSuite.</td>
</tr>
<tr>
<td>ecdhCurves</td>
<td>ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd ecdhCurves.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Boolean that indicates if Duo server certificate verification is required. Defaults to false. If set to true, provide a sslRootCAPath to ensure successful certificate validation.</td>
</tr>
<tr>
<td>sslRootCAPath</td>
<td>Full path of the certificate to be used for certificate verification. If sslVerifyServerCert is true, this path must be provided to ensure successful certificate validation.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>Common name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>Alternate name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>useClientSSLCompression</td>
<td>Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd useClientSSLCompression.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:changeme -X POST https://localhost:8089/services/admin/Duo-MFA/duo-mfa -d integrationKey=DIOXYOKGDKJNK4JRRT0KT -d secretKey=DABZXYbRVW2yqvTM6fPMbkgxBna0HTuYa9XuCQ2 -d appSecretKey=56a15e48ec796f3d6ee2763b088f8ca77109692c -d apiHostname=api-cc7a8eab.duosecurity.com -d failOpen=false -d timeout=10 -d sslVersions=tls1.2 -d sslCommonNameToCheck=*.duosecurity.com -d useClientSSLCompression=true -d sslVerifyServerCert=true -d sslRootCAPath=/home/user1/git/example/splunk/etc/auth/DigiCertHighAssuranceEVRootCA.pem

**XML Response**

```xml
title>Duo-MFA</title>
id>https://localhost:8089/services/admin/Duo-MFA</id>
updated>2016-09-21T14:54:43-07:00</updated>
generator build="3fe21d2159a8" version="6.5.0" />

<author>
```
<name>Splunk</name>
</author>
<link href="/services/admin/Duo-MFA/_new" rel="create"/>
<link href="/services/admin/Duo-MFA/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>duo-mfa</title>
<id>https://localhost:8089/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa</id>
<updated>2016-09-21T14:54:43-07:00</updated>
<link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="alternate"/>
<author>
<name>nobody</name>
</author>
<link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="list"/>
<link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="edit"/>
<link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="remove"/>
<content type="text/xml">
<s:dict>
<s:key name="apiHostname">api-cc7a8eab.duosecurity.com</s:key>
<s:key name="appSecretKey">****************************************</s:key>
<s:key name="cipherSuite">TLSv1+HIGH:TLSv1.2+HIGH:@STRENGTH</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app">system</s:key>
<s:key name="can_change_perms">1</s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_share_app">1</s:key>
<s:key name="can_share_global">1</s:key>
<s:key name="can_share_user">0</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">1</s:key>
<s:key name="owner">nobody</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
</s:dict>
<s:key name="removable">1</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
<s:key name="failOpen">0</s:key>
<s:key name="integrationKey">$1$W0/LVm4ziyz2U1HZEP8Xzn8WNRal</s:key>
<s:key name="secretKey">****************************************</s:key>
<s:key name="sslCommonNameToCheck">*.duosecurity.com</s:key>
<s:key name="sslRootCAPath">/home/user1/git/example/splunk/etc/auth/DigiCertHighAssuranceEVRootCA.pem</s:key>
<s:key name="sslVerifyServerCert">true</s:key>
<s:key name="sslVersions">tls1.2</s:key>
<s:key name="timeout">10</s:key>
</s:dict>
</entry>
admin/Duo-MFA/{name}

Access and manage the {name} Duo Multifactor configuration.

Authentication and Authorization
Requires the change_authentication capability.

GET

List the {name} Duo Multifactor configuration settings.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Configuration stanza name</td>
</tr>
<tr>
<td>integrationKey</td>
<td>Duo integration key for Splunk. Must be of size = 20.</td>
</tr>
<tr>
<td>secretKey</td>
<td>Shared secret key between Splunk and Duo.</td>
</tr>
<tr>
<td>apiHostname</td>
<td>Duo REST API endpoint used by Splunk for multifactor authentication</td>
</tr>
<tr>
<td>appSecretKey</td>
<td>Splunk application specific secret key. Must be a random generated hex of length 40 or more.</td>
</tr>
<tr>
<td>failOpen</td>
<td>Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to false.</td>
</tr>
<tr>
<td>timeout</td>
<td>Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>SSL version to use for accessing the Duo REST API. Defaults to Splunkd sslVersion.</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd cipherSuite.</td>
</tr>
<tr>
<td>ecdhCurves</td>
<td>ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd ecdhCurves.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Boolean indicating if Duo server certificate verification is required. Defaults to false.</td>
</tr>
<tr>
<td>sslRootCAPath</td>
<td>Full path of the certificate to be used for certificate verification if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>Common name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>Alternate name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>useClientSSLCompression</td>
<td>Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd useClientSSLCompression.</td>
</tr>
</tbody>
</table>

Example request and response
XML Request

admin:changeme -X GET https://localhost:8089/services/admin/Duo-MFA

XML Response

<title>Duo-MFA</title>
<id>https://localhost:8089/services/admin/Duo-MFA</id>
<updated>2016-07-26T11:05:14-07:00</updated>
<generator build="321df14f2b1047b51259ee2d4eaeac844184dc6679" version="20160720"/>
<author><name>Splunk</name></author>
<link href="/services/admin/Duo-MFA/_new" rel="create"/>
<link href="/services/admin/Duo-MFA/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>duo-mfa</title>
<id>https://localhost:8089/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa</id>
<updated>2016-07-26T11:05:14-07:00</updated>
<author><name>nobody</name></author>
<link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="alternate"/>
<link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="list"/>
<link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="edit"/>
<link href="/servicesNS/nobody/system/admin/Duo-MFA/duo-mfa" rel="remove"/>
<content type="text/xml">
<s:dict>
  <s:key name="apiHostname">api-cc7a8eab.duosecurity.com</s:key>
  <s:key name="appSecretKey">$1$cQdFd4+XlOrAfgBgQgEwe+VevD/MOOGFTIA4vwoaFncX0V0708ZsCsKQ0</s:key>
  <s:key name="app">system</s:key>
  <s:key name="can_change_perms">1</s:key>
  <s:key name="can_list">1</s:key>
  <s:key name="can_share_app">1</s:key>
  <s:key name="can_share_global">1</s:key>
  <s:key name="can_share_user">0</s:key>
  <s:key name="can_write">1</s:key>
  <s:key name="modifiable">1</s:key>
  <s:key name="owner">nobody</s:key>
  <s:key name="perms">
    <s:dict>
      <s:key name="read">
        <s:list>
          <s:item>*</s:item>
        </s:list>
      </s:key>
      <s:key name="write">
        <s:list>
          <s:item>*</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </s:key>
</s:dict>
POST

Update the \{name\} Duo Multifactor configuration.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Configuration stanza name</td>
</tr>
<tr>
<td>integrationKey</td>
<td>See description</td>
<td>Duo integration key for Splunk. Must be of size = 20.</td>
</tr>
<tr>
<td>secretKey</td>
<td>See description</td>
<td>Shared secret key between Splunk and Duo.</td>
</tr>
<tr>
<td>apiHostname</td>
<td>See description</td>
<td>Duo REST API endpoint used by Splunk for multifactor authentication</td>
</tr>
<tr>
<td>appSecretKey</td>
<td>See description</td>
<td>Splunk application specific secret key. Must be a random generated hex of length 40 or more.</td>
</tr>
<tr>
<td>failOpen</td>
<td>Boolean</td>
<td>Indicates whether Splunk should bypass the Duo service if it is unavailable. Defaults to false.</td>
</tr>
<tr>
<td>timeout</td>
<td>Positive integer</td>
<td>Optional. Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>See description</td>
<td>Optional. SSL version to use for accessing the Duo REST API. Defaults to Splunkd sslVersion.</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>See description</td>
<td>Optional. Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd cipherSuite.</td>
</tr>
<tr>
<td>ecdhCurves</td>
<td>See description</td>
<td>Optional. ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd ecdhCurves.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Boolean</td>
<td>Optional. Indicates if Duo server certificate verification is required. Defaults to false. If set to true, provide a sslRootCAPath to ensure successful certificate validation.</td>
</tr>
<tr>
<td>sslRootCAPath</td>
<td>See description</td>
<td>Optional. Full path of the certificate to be used for certificate verification. If sslVerifyServerCert is true, this path must be provided to ensure successful certificate validation.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>See description</td>
<td>Optional. Common name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>See description</td>
<td>Optional. Alternate name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>useClientSSLCompression</td>
<td>See description</td>
<td>Optional. Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd useClientSSLCompression.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Configuration stanza name</td>
</tr>
<tr>
<td>integrationKey</td>
<td>Duo integration key for Splunk. Must be of size = 20.</td>
</tr>
<tr>
<td>secretKey</td>
<td>Shared secret key between Splunk and Duo.</td>
</tr>
<tr>
<td>apiHostname</td>
<td>Duo REST API endpoint used by Splunk for multifactor authentication</td>
</tr>
<tr>
<td>appSecretKey</td>
<td>Splunk application specific secret key. Must be a random generated hex of length 40 or more.</td>
</tr>
<tr>
<td>failOpen</td>
<td>Boolean indicating whether Splunk should bypass the Duo service if it is unavailable. Defaults to false.</td>
</tr>
<tr>
<td>timeout</td>
<td>Positive integer indicating the Duo connection timeout, in seconds, for declaring the Duo service unavailable. Defaults to 15 seconds.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>SSL version to use for accessing the Duo REST API. Defaults to Splunkd sslVersion.</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Cipher suite to use for accessing the Duo REST API. Defaults to Splunkd cipherSuite.</td>
</tr>
<tr>
<td>ecdhCurves</td>
<td>ECDH curve value to use for accessing the Duo REST API. Defaults to Splunkd ecdhCurves.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Boolean that indicates if Duo server certificate verification is required. Defaults to false. If set to true, provide a sslRootCAPath to ensure successful certificate validation.</td>
</tr>
<tr>
<td>sslRootCAPath</td>
<td>Full path of the certificate to be used for certificate verification. If sslVerifyServerCert is true, this path must be provided to ensure successful certificate validation.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>Common name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>Alternate name to verify if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>useClientSSLCompression</td>
<td>Boolean indicating if client side SSL compression is enabled. Defaults to Splunkd useClientSSLCompression.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:changed https://localhost:8089/services/admin/Duo-MFA/duo-mfa -d failOpen=0
```

**XML Response**

```xml
<title>Duo-MFA</title>  
<id>https://localhost:8089/services/admin/Duo-MFA</id>  
<updated>2016-07-26T11:03:58-07:00</updated>  
<generator build="321d123f2b1047b51259ee2d4eeacb4184dc6679" version="20160720"></generator>  
<author>  
  <name>Splunk</name>  
</author>  
```
Delete the Duo Multifactor configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:changeme -X DELETE https://localhost:8089/services/admin/Duo-MFA/duo-mfa

XML Response

...  
<title>Duo-MFA</title>
'id'="https://localhost:8089/services/admin/Duo-MFA"'/id>
<updated>2016-07-26T11:06:00-07:00</updated>
<generator build="321df14f2b1047b51259ee2d4eeacb4184dc6679" version="20160720"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/Duo-MFA/_new" rel="create"/>
<link href="/services/admin/Duo-MFA/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages>
  <s:msg type="WARN">No active Duo MFA configuration to list.</s:msg>
</s:messages>

RSA multifactor authentication REST API usage details

Splunk Enterprise users can configure RSA user authentication using the REST API.

You can use the RSA multifactor authentication REST API to configure RSA authentication and to verify that the authentication is configured correctly.

- To configure multifactor authentication for Splunk Web, you use the /services/admin/Rsa-MFA endpoint. To enable CLI and management port, set the parameter enableMfaAuthRest to true.
- To verify the authentication, you use the /services/admin/Rsa-MFA-config-verify/ endpoint.
Authentication and Authorization

Requires the change_authentication capability.

To learn more about using RSA multifactor authentication, see About multifactor authentication with RSA Authentication Manager in Securing Splunk Enterprise.

admin/Rsa-MFA

Configure RSA multifactor authentication.

GET

List the RSA Authentication Manager configuration settings.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Configuration stanza name</td>
</tr>
<tr>
<td>authManagerUrl</td>
<td>URL of REST endpoint of RSA Authentication Manager.</td>
</tr>
<tr>
<td>accessKey</td>
<td>Access key needed by Splunk to communicate with RSA Authentication Manager. Note that this value is hidden output.</td>
</tr>
<tr>
<td>clientId</td>
<td>Agent name created on RSA Authentication Manager is clientId.</td>
</tr>
<tr>
<td>failOpen</td>
<td>If true, allow login in case authentication server is unavailable.</td>
</tr>
<tr>
<td>timeout</td>
<td>It determines the connection timeout in seconds for the outbound HTTPS connection.</td>
</tr>
<tr>
<td>messageOnError</td>
<td>Message that will be shown to user in case of login failure.</td>
</tr>
<tr>
<td>enableMfaAuthRest</td>
<td>If true, enable authentication of REST calls.</td>
</tr>
<tr>
<td>caCertBundlePayload</td>
<td>SSL certificate chain return by RSA server.</td>
</tr>
<tr>
<td>replicateCertificates</td>
<td>If enabled, RSA certificate files are replicated across search head cluster setup.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request


XML Response

...<title>Rsa-MFA</title>

<![CDATA[<id>https://ronnie.sv.splunk.com:8130/services/admin/Rsa-MFA</id>]]>

<updated>2018-04-03T12:42:27-07:00</updated>
<entry>
  <title>rsa-mfa</title>
  <id>https://ronnie.sv.splunk.com:8130/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="list"/>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="edit"/>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="remove"/>
  <link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="accessKey">****************************************</s:key>
      <s:key name="authManagerCertPath">etc/auth/rsa-2fa/cert.pem</s:key>
      <s:key name="authManagerUrl">https://qa-rsaam-002.sv.splunk.com:5555</s:key>
      <s:key name="clientId">ronnie.splunk.com</s:key>
      <s:key name="eai:acl">system</s:key>
    </s:dict>
  </content>
</entry>
<s:dict>
  <s:dict>
    <s:key name="perm_type">read</s:key>
    <s:list>
      <s:item>*</s:item>
    </s:list>
  </s:dict>
  <s:dict>
    <s:key name="perm_type">write</s:key>
    <s:list>
      <s:item>*</s:item>
    </s:list>
  </s:dict>
  <s:dict>
    <s:key name="perm_type">removable</s:key>
  </s:dict>
  <s:dict>
    <s:key name="perm_type">sharing</s:key>
    <s:value>system</s:value>
  </s:dict>
  <s:dict>
    <s:key name="can_change_perms">1</s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_share_app">1</s:key>
    <s:key name="can_share_global">1</s:key>
    <s:key name="can_share_user">0</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">1</s:key>
    <s:key name="owner">nobody</s:key>
    <s:dict>
      <s:dict>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:dict>
      </s:dict>
      <s:dict>
        <s:key name="removable">1</s:key>
      </s:dict>
      <s:dict>
        <s:key name="sharing">system</s:key>
      </s:dict>
      <s:dict>
        <s:key name="enableMfaAuthRest">false</s:key>
        <s:key name="failOpen">1</s:key>
        <s:key name="messageOnError">Please_contact_admin</s:key>
        <s:key name="timeout">10</s:key>
      </s:dict>
    </s:dict>
  </s:dict>
</s:dict>
POST

Edit the RSA Authentication Manager configuration.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required. Name of RSA configuration stanza</td>
</tr>
<tr>
<td>authManagerUrl</td>
<td>String</td>
<td>Required. URL of REST endpoint of RSA Authentication Manager.</td>
</tr>
<tr>
<td>accessKey</td>
<td>String</td>
<td>Required. Access key needed by Splunk to communicate with RSA Authentication Manager.</td>
</tr>
<tr>
<td>clientId</td>
<td>String</td>
<td>Required. Agent name created on RSA Authentication Manager is clientId.</td>
</tr>
<tr>
<td>failOpen</td>
<td>Boolean</td>
<td>Optional. If true, allow login in case authentication server is unavailable.</td>
</tr>
<tr>
<td>timeout</td>
<td>Integer</td>
<td>Optional. It determines the connection timeout in seconds for the outbound HTTPS connection.</td>
</tr>
<tr>
<td>messageOnError</td>
<td>String</td>
<td>Optional. Message that will be shown to user in case of login failure.</td>
</tr>
<tr>
<td>enableMfaAuthRest</td>
<td>Boolean</td>
<td>Optional. If true, enable authentication of REST calls.</td>
</tr>
<tr>
<td>caCertBundlePayload</td>
<td>String</td>
<td>Required. SSL certificate chain return by RSA server.</td>
</tr>
<tr>
<td>replicateCertificates</td>
<td>Boolean</td>
<td>If enabled, RSA certificate files will be replicated across search head cluster setup.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Configuration stanza name</td>
</tr>
<tr>
<td>authManagerUrl</td>
<td>URL of REST endpoint of RSA Authentication Manager.</td>
</tr>
<tr>
<td>accessKey</td>
<td>Access key needed by Splunk to communicate with RSA Authentication Manager. Note that this value is hidden output.</td>
</tr>
<tr>
<td>clientId</td>
<td>Agent name created on RSA Authentication Manager is clientId.</td>
</tr>
<tr>
<td>failOpen</td>
<td>If true, allow login in case authentication server is unavailable.</td>
</tr>
<tr>
<td>timeout</td>
<td>It determines the connection timeout in seconds for the outbound HTTPS connection.</td>
</tr>
<tr>
<td>messageOnError</td>
<td>Message that will be shown to user in case of login failure.</td>
</tr>
<tr>
<td>enableMfaAuthRest</td>
<td>If true, enable authentication of REST calls.</td>
</tr>
<tr>
<td>caCertBundlePayload</td>
<td>SSL certificate chain return by RSA server.</td>
</tr>
<tr>
<td>replicateCertificates</td>
<td>If enabled, RSA certificate files will be replicated across search head cluster setup.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -k -u admin:Splunk_123 -X POST https://localhost:8092/services/admin/Rsa-MFA -d name=rsa-mfa -d timeout=10 -d failOpen=true -d authManagerUrl=https://rsa-auth-manager.company.com:5555 -d accessKey=aaa -d clientId=linux-vm -d messageOnError=Please_contact_admin

XML Response

...
<updated>1969-12-31T16:00:00-08:00</updated>

<link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa" rel="alternate"/>

<author>
   <name>nobody</name>
</author>

<link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa" rel="list"/>

<link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa" rel="edit"/>

<link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa" rel="remove"/>

<link href="/servicesNS/nobody/search/admin/Rsa-MFA/rsa-mfa/disable" rel="disable"/>

<content type="text/xml">

   <s:dict>
      <s:key name="accessKey">****************************************</s:key>
      <s:key name="authManagerUrl">https://rsa-auth-manager.company.com:5555</s:key>
      <s:key name="clientId">linux-vm</s:key>
      <s:key name="eai:acl">
         <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
               <s:dict>
                  <s:key name="read">
                     <s:list>
                        <s:item>*</s:item>
                     </s:list>
                  </s:key>
               </s:dict>
            </s:key>
         </s:dict>
      </s:key>
   </s:dict>

</content>
DELETE

Delete the RSA Authentication Manager configuration.

Request parameters
None

Returned values
None

Example request and response
XML Request


XML Response

...  
<title>Rsa-MFA</title>  
&id>https://ronnie.sv.splunk.com:8130/services/admin/Rsa-MFA</id>  
<updated>2018-04-03T12:42:27-07:00</updated>  
<generator build="80906e769c378b3c090160fc090717553dd4e8ef" version="20180331"/>

</author>

<link href="/services/admin/Rsa-MFA/_new" rel="create"/>
<link href="/services/admin/Rsa-MFA/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

<entry>
<title>rsa-mfa</title>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="alternate"/>

</author>

<link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="list"/>
<link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="edit"/>
<link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa" rel="remove"/>
<link href="/servicesNS/nobody/system/admin/Rsa-MFA/rsa-mfa/disable" rel="disable"/>
<content type="text/xml">

43
<s:dict>
  <s:key name="accessKey">
  ****************************************
  </s:key>
  <s:key name="authManagerCertPath">etc/auth/rsa-2fa/cert.pem</s:key>
  <s:key name="authManagerUrl">https://qa-rsaam-002.sv.splunk.com:5555</s:key>
  <s:key name="clientId">ronnie.splunk.com</s:key>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app">system</s:key>
      <s:key name="can_change_perms">1</s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_share_app">1</s:key>
      <s:key name="can_share_global">1</s:key>
      <s:key name="can_share_user">0</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">1</s:key>
      <s:key name="owner">nobody</s:key>
      <s:key name="perms">
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:key>
          <s:key name="write">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
    <s:key name="removable">1</s:key>
  </s:dict>
</s:dict>
admin/Rsa-MFA-config-verify/<rsa-stanza-name>

Verify RSA multifactor authentication.

**POST**

Verify the RSA multifactor authentication.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>String</td>
<td>Optional. RSA username.</td>
</tr>
<tr>
<td>passcode</td>
<td>String</td>
<td>Optional. RSA passcode consists of PIN followed by tokencode.</td>
</tr>
</tbody>
</table>

**Returned values**

Information on whether RSA configuration is valid or not.

**Example request and response**

**XML Request**

```bash
```

**XML Response**

```xml
...<title>Rsa-MFA-config-verify</title>

<id>https://localhost:8201/services/admin/Rsa-MFA-config-verify</id>
```
LDAP REST API usage details

Splunk Enterprise users can configure LDAP user authentication using the REST API. If you are using Splunk Cloud, contact Support for assistance with setting up LDAP authentication.

LDAP user authentication lets you specify configurations, user groups, and group to role mappings to manage permissions in your Splunk deployment.

You can use the LDAP REST API for the following LDAP management tasks.

- Configure an LDAP strategy for a server in your deployment.
- Map LDAP groups to user roles in a server to manage group permissions.
- Enable or disable an LDAP strategy.

To learn more about using LDAP authentication, see Set up user authentication with LDAP in Securing Splunk Enterprise.

admin/LDAP-groups

https://<host>:<mPort>/services/admin/LDAP-groups
Access and update LDAP group to role mappings.

Authentication and authorization
Requires the change_authentication capability for access.
If you are passing in a strategy name with an LDAP group name, they must be comma separated.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategy</td>
<td>LDAP strategy name</td>
</tr>
<tr>
<td>LDAPgroup</td>
<td>LDAP group name</td>
</tr>
</tbody>
</table>

Returned values
For each group, the following values are returned in the response.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roles</td>
<td>Roles mapped to this group</td>
</tr>
<tr>
<td>strategy</td>
<td>Strategy name</td>
</tr>
<tr>
<td>type</td>
<td>Group type</td>
</tr>
<tr>
<td>users</td>
<td>List of users in this group</td>
</tr>
</tbody>
</table>

Example request and response

curl -u admin:changeme -X GET -k https://localhost:8089/services/admin/LDAP-groups/

...
Create an LDAP group.

**Request parameters**
Append the group name to the `LDAP-groups/` endpoint. Pass in a strategy name using comma separation. For example, this POST creates the `ActiveDirectory_New` strategy and specifies the `Abc123` group name.

```bash
curl -k -u admin:password -X POST https://localhost:8089/services/admin/LDAP-groups/ActiveDirectory_New,Abc123-Admin -d roles=user
```

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategy</td>
<td>Required. LDAP strategy name</td>
</tr>
<tr>
<td>LDAPgroup</td>
<td>Required. LDAP group name</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roles</td>
<td>Roles mapped to this group.</td>
</tr>
<tr>
<td>strategy</td>
<td>Strategy name</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>type</td>
<td>Group type</td>
</tr>
<tr>
<td>users</td>
<td>List of users in this group.</td>
</tr>
</tbody>
</table>

**Example request and response**

```
curl -k -u admin:password -X POST https://localhost:8089/services/admin/LDAP-groups/ActiveDirectory_New,Abc123-Admin -d roles=user
```

```
<title>Abc123-Admin</title>  
{id>https://localhost:8089/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin</id>  
<updated>2016-11-10T13:07:28-08:00</updated>  
<a>https://localhost:8089/services/admin/LDAP-groups/ActiveDirectory_New%2CAbc123-Admin</a>  

<author>  
    <name>system</name>  
</author>  

<content type="text/xml">  
    <s:dict>  
        <s:dict name="eai:acl">  
            <s:dict name="app">"</s:dict>  
            <s:dict name="can_list">1</s:dict>  
            <s:dict name="can_write">1</s:dict>  
            <s:dict name="modifiable">0</s:dict>  
            <s:dict name="owner">"system"</s:dict>  
            <s:dict name="perms">  
                <s:dict name="read">  
                    <s:list>  
                        <s:item>"admin"</s:item>  
                        <s:item>"splunk-system-role"</s:item>  
                    </s:list>  
                </s:dict>  
                <s:dict name="write">  
                    <s:list>  
                        <s:item>"admin"</s:item>  
                        <s:item>"splunk-system-role"</s:item>  
                    </s:list>  
                </s:dict>  
            </s:dict>  
            <s:dict name="removable">0</s:dict>  
            <s:dict name="sharing">"system"</s:dict>  
        </s:dict>  
        <s:dict name="strategy">"ActiveDirectory_New"</s:dict>  
    </s:dict>
```
authentication/providers/LDAP

https://<host>:<mPort>/services/authentication/providers/LDAP
Access or create LDAP authentication strategies on a server in your deployment.

Authentication and authorization
Requires the change_authentication capability for access.

GET
Access LDAP configurations strategies.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>strategy</td>
<td>Name of LDAP configuration strategy</td>
</tr>
</tbody>
</table>

Returned values
The response lists LDAP strategy settings.

See LDAP settings in authentication.conf for strategy settings information.

Example request and response

curl -k -u admin:password https://localhost:8089/services/authentication/providers/LDAP/

  <title>providers/LDAP</title>
  <id>https://localhost:8089/services/authentication/providers/LDAP</id>
  <updated>2016-11-09T16:14:07-08:00</updated>
  <generator build="2469654e091cb630e237a02094e683ced50f2fe5" version="20161031"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authentication/providers/LDAP/_new" rel="create"/>
  <link href="/services/authentication/providers/LDAP/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
<entry><title>my_strategy</title><id>https://localhost:8089/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy</id><updated>2016-11-09T14:07:08-08:00</updated><link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="alternate"/><author><name>nobody</name></author><link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="list"/><link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="edit"/><link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="remove"/><link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy/disable" rel="disable"/><content type="text/xml"> <s:dict> <s:key name="SSLEnabled">0</s:key> <s:key name="anonymous_referrals">1</s:key> <s:key name="bindDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key> <s:key name="bindDNpassword">********</s:key> <s:key name="charset">utf8</s:key> <s:key name="disabled">0</s:key> <s:key name="eai:acl"> <s:dict> <s:key name="app">system</s:key> <s:key name="can_list">1</s:key> <s:key name="can_write">1</s:key> <s:key name="modifiable">0</s:key> <s:key name="owner">nobody</s:key> <s:key name="perms"> <s:dict> <s:key name="read"> <s:list>*</s:list> </s:key> <s:key name="write"> <s:list>*</s:list> </s:key> </s:dict> </s:dict> <s:key name="removable">1</s:key> <s:key name="sharing">system</s:key> </s:dict> <s:key name="emailAttribute">mail</s:key> <s:key name="groupBaseDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key> <s:key name="groupMappingAttribute">dn</s:key> <s:key name="groupNameAttribute">sn</s:key> <s:key name="host">1.1.1.1</s:key> <s:key name="nestedGroups">0</s:key> <s:key name="network_timeout">20</s:key> <s:key name="order">1</s:key> <s:key name="port">389</s:key> <s:key name="realNameAttribute">sn</s:key> <s:key name="sizelimit">1000</s:key> <s:key name="timelimit">15</s:key> <s:key name="userBaseDN">OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key> </s:dict></content>
Create an LDAP strategy.

Usage details
Use the following endpoints to enable or disable an LDAP strategy after you create it.

- services/authentication/providers/LDAP/{LDAP_strategy_name}/enable
- services/authentication/providers/LDAP/{LDAP_strategy_name}/disable

Request parameters
See LDAP settings in authentication.conf for required and optional settings information.

Returned values
None.

Example request and response

curl ?k u admin:password -X POST https://localhost:8089/services/authentication/providers/LDAP/ -d name=my_strategy -d groupBaseDN="CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com" -d groupMemberAttribute=sn -d groupNameAttribute=sn -d host=1.1.1.1 -d realNameAttribute=sn -d userBaseDN="OU=SAML Test,DC=qa,DC=ab2008e2,DC=com" -d userNameAttribute=sn -d bindDN="CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com" -d bindDNpassword=password

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest">
<title>providers/LDAP</title>
<id>https://localhost:8089/services/authentication/providers/LDAP</id>
<updated>2016-11-09T16:20:14-08:00</updated>
<generator build="2469654e091cb630e237a02094e683ced50f2fe5" version="20161031"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authentication/providers/LDAP/_new" rel="create"/>
<link href="/services/authentication/providers/LDAP/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages>
  <s:msg type="INFO">Successfully performed a bind to the LDAP server</s:msg>
  <s:msg type="WARN">Failed to find the email attribute 'mail' in a returned user entry.</s:msg>
</s:messages>
</feed>
<link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="edit"/>
<link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="remove"/>
<link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy/disable" rel="disable"/>

<content type="text/xml">
<s:dict>
  <s:key name="SSLEnabled">0</s:key>
  <s:key name="anonymous_referrals">1</s:key>
  <s:key name="bindDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
  <s:key name="bindDNpassword">********</s:key>
  <s:key name="charset">utf8</s:key>
  <s:key name="emailAttribute">mail</s:key>
  <s:key name="groupBaseDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
  <s:key name="groupMappingAttribute">dn</s:key>
  <s:key name="groupMemberAttribute">sn</s:key>
  <s:key name="groupNameAttribute">sn</s:key>
  <s:key name="host">1.1.1.1</s:key>
  <s:key name="nestedGroups">0</s:key>
  <s:key name="network_timeout">20</s:key>
  <s:key name="order">1</s:key>
  <s:key name="port">389</s:key>
  <s:key name="realNameAttribute">sn</s:key>
  <s:key name="sizelimit">1000</s:key>
  <s:key name="timelimit">15</s:key>
  <s:key name="userBaseDN">OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
  <s:key name="userNameAttribute">sn</s:key>
</s:dict>
</content>
authentication/providers/LDAP/{LDAP_strategy_name}

https://<host>:<mPort>/services/authentication/providers/LDAP/{LDAP_strategy_name}

Access, update, or delete the {LDAP_strategy_name} strategy.

Authentication and authorization
Requires the change_authentication capability for access.

GET

Access an existing LDAP strategy.

Usage details
Use the following endpoints to enable or disable the {LDAP_strategy_name} strategy.

- services/authentication/providers/LDAP/my_strategy/enable
- services/authentication/providers/LDAP/my_strategy/disable

Request parameters
None.

Returned values
See LDAP settings in authentication.conf for strategy settings information.

Example request and response

curl -k u admin:password https://localhost:8089/services/authentication/providers/LDAP/my_strategy

<entry>
  <title>my_strategy</title>
  <id>https://localhost:8089/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy</id>
  <updated>2016-11-09T16:14:07-08:00</updated>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="list"/>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="edit"/>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="remove"/>
  <link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="SSLEnabled">0</s:key>
      <s:key name="anonymous_referrals">1</s:key>
      <s:key name="bindDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
      <s:key name="bindDNpassword">********</s:key>
      <s:key name="charset">utf8</s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        54
      </s:key>
    </s:dict>
  </content>
</entry>
POST

Update an existing LDAP strategy.

Request parameters and returned values
See LDAP settings in authentication.conf for strategy settings information.

Example request and response

curl ?k u admin:password -X POST https://localhost:8089/services/authentication/providers/LDAP/my_strategy
-d port=390

<entry>
<title>my_strategy</title>
</entry>

https://localhost:8089/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy

2016-11-09T16:07-08:00

<link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="alternate"/>
<author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="list"/>
<link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="edit"/>
<link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy" rel="remove"/>
<link href="/servicesNS/nobody/system/authentication/providers/LDAP/my_strategy/disable" rel="disable"/>
<content type="text/xml">
  <s:dict>
    <s:key name="SSLEnabled">0</s:key>
    <s:key name="anonymous_referrals">1</s:key>
    <s:key name="bindDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
    <s:key name="bindDNpassword">********</s:key>
    <s:key name="charset">utf8</s:key>
    <s:key name="disabled">0</s:key>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app">system</s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">0</s:key>
        <s:key name="owner">nobody</s:key>
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:key>
          <s:key name="write">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:key>
        </s:dict>
        <s:key name="removable">1</s:key>
        <s:key name="sharing">system</s:key>
      </s:dict>
    </s:key>
    <s:key name="emailAttribute">mail</s:key>
    <s:key name="groupBaseDN">CN=Saml user2,OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
    <s:key name="groupMappingAttribute">dn</s:key>
    <s:key name="groupNameAttribute">sn</s:key>
    <s:key name="host">1.1.1.1</s:key>
    <s:key name="nestedGroups">0</s:key>
    <s:key name="network_timeout">20</s:key>
    <s:key name="order">1</s:key>
    <s:key name="port">390</s:key>
    <s:key name="realNameAttribute">sn</s:key>
    <s:key name="sizelimit">1000</s:key>
    <s:key name="timelimit">15</s:key>
    <s:key name="userBaseDN">OU=SAML Test,DC=qa,DC=ad2008r2,DC=com</s:key>
    <s:key name="userNameAttribute">sn</s:key>
  </s:dict>
</content>
DELETE

Delete an existing LDAP strategy.

Request parameters
None

Returned values
None

Example request and response

curl -k -u admin:password -X DELETE https://localhost:8089/services/authentication/providers/LDAP/my_strategy

<title>providers/LDAP</title>
<id>https://ronnie:8132/services/authentication/providers/LDAP</id>
<updated>2016-11-09T16:18:37-08:00</updated>
<generator build="2469654e091cb630e237a02094e683ced50f2fe5" version="20161031"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/authentication/providers/LDAP/_new" rel="create"/>
<link href="/services/authentication/providers/LDAP/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
</feed>

authentication/providers/LDAP/{LDAP_strategy_name}/enable

https://<host>:<mPort>/services/authentication/providers/LDAP/{LDAP_strategy_name}/enable

GET

Enable the {LDAP_strategy_name} LDAP strategy.

Request parameters
None

Returned values
None

Example request

curl -k u admin:password https://localhost:8089/services/authentication/providers/LDAP/my_strategy/enable
**authentication/providers/LDAP/{LDAP_strategy_name}/disable**

https://<host>:<mPort>/services/authentication/providers/LDAP/{LDAP_strategy_name}/disable

**GET**

Disable the `{LDAP_strategy_name}` LDAP strategy.

**Request parameters**
None

**Returned values**
None

**Example request**

curl -k u admin:password https://localhost:8089/services/authentication/providers/LDAP/my_strategy/disable

**admin/metrics-reload/_reload**

https://<host>:<mPort>/services/admin/metrics-reload/_reload

Use this endpoint to reload the metrics processor after updating a metrics-related configuration.

**POST**

Reload the metrics processor.

**Example request and response**

**Request**

curl -k -u admin:changeme https://localhost:8089/services/admin/metrics-reload/_reload

**Response**

```xml
...
<title>metrics-reload</title>
<id>https://<localhost>:<mport>/services/admin/metrics-reload/_reload</id>
<updated>2017-08-08T23:33:13+00:00</updated>
<generator build="eb729684699b" version="7.0.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/metrics-reload/_reload" rel="_reload"/>
<link href="/services/admin/metrics-reload/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
</feed>
```
ProxySSO REST API usage details

SSO mode must be enabled before you can configure ProxySSO. If you are creating a new ProxySSO configuration for the first time, follow these steps.

1. Locate the `web.conf` file in the `etc/system/local` directory.
2. Make the following additions to the `[settings]` stanza of `web.conf` file. If the file does not already exist in this location, create a new file called `web.conf` and add only the `[settings]` stanza name and the following settings to it.

   ```
   [settings]
   SSOMode = strict
   trustedIP = <IP_address>
   remoteUser = <remote user>
   remoteGroups = <remote group>
   tools.proxy.on = False
   allowSsoWithoutChangingServerConf = 1
   ```

3. Restart the Splunk deployment after updating `web.conf`.
4. Use the `admin/ProxySSO-auth/{proxy_name}/enable` endpoint to enable the configuration that you are creating.
5. Use the `admin/ProxySSO-auth` endpoint to add the new configuration.
6. (Optional) Use the `services/admin/auth-services` endpoint to verify that the `active_authmodule` is set to `ProxySSO`.

admin/ProxySSO-auth

https://<host>:<mPort>/services/admin/ProxySSO-auth

Access or create a ProxySSO configuration.

GET

Review existing ProxySSO configurations.

Request parameters
None.

Returned values
For each configuration the following values are returned.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultRoleIfMissing</td>
<td>Name of default role to use if no mapping is found.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list of blacklisted users.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list of blacklisted roles.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean value indicating whether the configuration is disabled. 0 indicates that the configuration is enabled.</td>
</tr>
<tr>
<td>title</td>
<td>Configuration name</td>
</tr>
</tbody>
</table>

Example request and response
XML Request

curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth

XML Response

...
POST
Add a new ProxySSO configuration.

Usage details
Changes are written to the app context.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required. New ProxySSO configuration name</td>
</tr>
<tr>
<td>defaultRoleIfMissing</td>
<td>Role name</td>
<td>Specify a default role to use if no mapping is found.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list</td>
<td>Specify blacklisted users.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list</td>
<td>Specify blacklisted roles.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultRoleIfMissing</td>
<td>Name of default role to use if no mapping is found.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list of blacklisted users.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list of blacklisted roles.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean value indicating whether the configuration is disabled. 0 indicates that the configuration is enabled.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth -d name=my_proxy

XML Response

...<title>ProxySSO-auth</title>
<id>https://localhost:8089/services/admin/ProxySSO-auth/my_proxy</id>
<updated>2016-08-31T14:53:42-07:00</updated>
<generator build="ca6bc6de37c2" version="6.5.0"/>
<author>
    <name>system</name>
</author>
<title>my_proxy</title>
<id>https://localhost:8089/services/admin/ProxySSO-auth/my_proxy</id>
<updated>2016-08-31T14:53:42-07:00</updated>
<author>
    <name>system</name>
</author>
<content type="text/xml">
    <s:dict>
        <s:key name="blacklistedAutoMappedRoles"></s:key>
        <s:key name="blacklistedUsers"></s:key>
        <s:key name="defaultRoleIfMissing"></s:key>
        <s:dict>
            <s:key name="eai:acl">
                <s:dict>
                    <s:key name="can_list">1</s:key>
                    <s:key name="can_write">1</s:key>
                    <s:key name="modifiable">0</s:key>
                    <s:key name="owner">system</s:key>
                    <s:dict>
                        <s:key name="read">
                            <s:list>
                                <s:item>admin</s:item>
                                <s:item>splunk-system-role</s:item>
                            </s:list>
                        </s:key>
                        <s:key name="write">
                            <s:list>
                                <s:item>admin</s:item>
                                <s:item>splunk-system-role</s:item>
                            </s:list>
                        </s:key>
                    </s:dict>
                    <s:key name="removable">0</s:key>
                    <s:key name="sharing">system</s:key>
                </s:dict>
            </s:dict>
        </s:dict>
    </s:dict>
</content>
admin/ProxySSO-auth/{proxy_name}

https://<host>:<mPort>/services/admin/ProxySSO-auth/{proxy_name}
Access, update, or delete the {proxy_name} configuration.

GET
Access configuration details.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultRoleIfMissing</td>
<td>Name of default role to use if no mapping is found.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list of blacklisted users.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list of blacklisted roles.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean value indicating whether the configuration is disabled. If 0 indicates that the configuration is enabled.</td>
</tr>
<tr>
<td>title</td>
<td>Configuration name</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth/my_proxy

XML Response

<title>ProxySSO-auth</title>
    <id>https://localhost:8089/services/admin/ProxySSO-auth</id>
        ...
    <entry>
        <title>my_proxy</title>
        <id>https://localhost:8089/services/admin/ProxySSO-auth/my_proxy</id>
        <updated>2016-08-31T16:09:38-07:00</updated>
        <link href="/services/admin/ProxySSO-auth/my_proxy" rel="alternate"/>
        <author>
            <name>system</name>
        </author>
        <link href="/services/admin/ProxySSO-auth/my_proxy" rel="list"/>
        <link href="/services/admin/ProxySSO-auth/my_proxy" rel="edit"/>
        <link href="/services/admin/ProxySSO-auth/my_proxy" rel="remove"/>
        <link href="/services/admin/ProxySSO-auth/my_proxy/disable" rel="disable"/>
        <content type="text/xml">
            <s:dict>
                <s:key name="blacklistedAutoMappedRoles">role1</s:key>
                <s:key name="blacklistedUsers"></s:key>
            </s:dict>
        </content>
POST

Update a configuration.

Changes are written to the app context.

Request parameters
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required. New ProxySSO configuration name</td>
</tr>
<tr>
<td>defaultRoleIfMissing</td>
<td>Role name</td>
<td>Specify a default role to use if no mapping is found.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list</td>
<td>Specify blacklisted users.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list</td>
<td>Specify blacklisted roles.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultRoleIfMissing</td>
<td>Name of default role to use if no mapping is found.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list of blacklisted users.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list of blacklisted roles.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean value indicating whether the configuration is disabled. 0 indicates that the configuration is enabled.</td>
</tr>
<tr>
<td>title</td>
<td>Configuration name</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth/my_proxy -d blacklistedAutoMappedRoles=role2,role3
```

**XML Response**

```
...<title>ProxySSO-auth</title>
<title>my_proxy</title>
```

### XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth/my_proxy -d blacklistedAutoMappedRoles=role2,role3
```
Delete a configuration.

Changes are written to the app context.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changeme -X DELETE https://localhost:8089/services/admin/ProxySSO-auth/my_proxy
```

XML Response
admin/ProxySSO-auth/{proxy_name}/disable

https://<host>:<mPort>/services/admin/ProxySSO-auth/{proxy_name}/disable
Disable the {proxy_name} configuration.

GET
Disable the {proxy_name} configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth/my_proxy/disable
```

XML Response

```
...
<title>ProxySSO-auth</title>
  <id>https://localhost:8089/services/admin/ProxySSO-auth</id>
  <updated>2016-08-31T16:43:46-07:00</updated>
  <generator build="ca6bc6de37c2" version="6.5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/ProxySSO-auth/_new" rel="create"/>
  <link href="/services/admin/ProxySSO-auth/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
...
```

admin/ProxySSO-auth/{proxy_name}/enable

https://<host>:<mPort>/services/admin/ProxySSO-auth/{proxy_name}/enable
Use a GET request to create and enable the {proxy_name} authentication setting. Changes are made in the default app context.
GET

Enable the `proxy_name` configuration.

Usage details
For new configurations, specify a new `proxy_name`. After enabling the configuration, use the same `proxy_name` in the POST to `admin/ProxySSO-auth` to add the configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-auth/my_proxy/enable

XML Response

```xml
<title>ProxySSO-auth</title>
<id>https://wimpy:7102/services/admin/ProxySSO-auth</id>
<updated>2016-08-31T16:44:05-07:00</updated>
<generator build="ca6bc6de37c2" version="6.5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/ProxySSO-auth/_new" rel="create"/>
<link href="/services/admin/ProxySSO-auth/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```

`admin/ProxySSO-groups`

https://<host>:<mPort>/services/admin/ProxySSO-groups

Access or create role to group ProxySSO mappings.

Authentication and authorization
Requires the `change_authentication` capability.

GET

Access ProxySSO role to group mappings.
Request parameters
None

Returned values
For each group returned, lists the roles assigned to it.

Example request and response

XML Request

curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-groups

XML Response

...<title>ProxySSO-groups</title>
  <id>https://localhost:8089/services/admin/ProxySSO-groups</id>
  ...
  <entry>
    <title>group1</title>
    <id>https://localhost:8089/services/admin/ProxySSO-groups/group1</id>
    <updated>2016-08-31T17:03:46-07:00</updated>
    <link href="/services/admin/ProxySSO-groups/group1" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/admin/ProxySSO-groups/group1" rel="list"/>
    <link href="/services/admin/ProxySSO-groups/group1" rel="edit"/>
    <link href="/services/admin/ProxySSO-groups/group1" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="eai:acl">
          <s:dict>
            <s:dict>
              <s:dict>
                <s:dict>
                  <s:dict>
                    <s:dict>
                      <s:dict>
                        <s:dict>
                          <s:dict>
                            <s:dict>
                              <s:dict>
                                <s:dict>
                                  <s:dict>
                                    <s:dict>
                                      <s:dict>
                                        <s:dict>
                                          <s:dict>
                                            <s:dict>
                                              <s:dict>
                                                <s:dict>
                                                  <s:dict>
                                                    <s:dict>
                                                      <s:dict>
                                                        <s:dict>
                                                          <s:dict>
                                                            <s:dict>
                                                              <s:dict>
                                                                <s:dict>
                                                                  <s:dict>
                                                                      ...
POST

Create a new mapping.

Changes are written to the app context.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roles</td>
<td>User role name</td>
<td>Specify roles to map to the group that you are creating. Use a separate roles parameter for each role added.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changed -X POST https://localhost:8089/services/admin/ProxySSO-groups/group1 -d roles=power
```

XML Response

```
...
<title>ProxySSO-groups</title>
<id>https://localhost:8089/services/admin/ProxySSO-groups</id>
<updated>2016-08-31T17:01:20-07:00</updated>
<generator build="ca6bc6de37c2" version="6.5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/ProxySSO-groups/_new" rel="create"/>
<link href="/services/admin/ProxySSO-groups/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
...
```
admin/ProxySSO-groups/{group_name}

https://<host>:<mPort>/services/admin/ProxySSO-groups/{group_name}
Access, create, and manage role to group mappings.

**Authentication and authorization**
Requires the `change_authentication` capability.

**GET**
Access role mappings for the `{group_name}` group.

**Request parameters**
None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roles</td>
<td>Roles mapped to this group.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-groups/group2
```

**XML Response**

```xml
<title>ProxySSO-groups</title>
/id>https://wimpy:7102/services/admin/ProxySSO-groups</id>
...
<title>group2</title>
/id>https://localhost:8089/services/admin/ProxySSO-groups/group2</id>
/<updated>2016-08-31T17:25:01-07:00</updated>
</link href="/services/admin/ProxySSO-groups/group2" rel="alternate"/>
</author>

<title>system</title>
</author>

<title>/services/admin/ProxySSO-groups/group2" rel="list"/>
<title>/services/admin/ProxySSO-groups/group2" rel="edit"/>
<title>/services/admin/ProxySSO-groups/group2" rel="remove"/>
</content type="text/xml">
<s:dict>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
```
POST

Create a new `{group_name}` mapping or update an existing one.

Changes are written to the app context.

**Request parameters**
If you are creating a new group, specify the new group name in the URL.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roles</td>
<td>User role name</td>
<td>Specify roles to map to the group that you are creating or updating. Use a separate <code>roles</code> parameter for each role added.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Returned values</td>
<td></td>
<td>None</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:changed -X POST https://localhost:8089/services/admin/ProxySSO-groups/group1 -d roles=power
```

**XML Response**

```xml
...<title>ProxySSO-groups</title>
{id>https://localhost:8089/services/admin/ProxySSO-groups</id>
<updated>2016-08-31T17:01:20-07:00</updated>
<generator build="ca6bc6de37c2" version="6.5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/ProxySSO-groups/_new" rel="create"/>
<link href="/services/admin/ProxySSO-groups/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
...```

**DELETE**

Delete the `{group_name}` group mapping.

Changes are written to the app context.

**Request parameters**

None

**Returned values**

None

**Example request and response**

**XML Request**

```
curl -k -u admin:changed -X DELETE https://localhost:8089/services/admin/ProxySSO-groups/group2
```
**admin/ProxySSO-user-role-map**

https://<host>:<mPort>/services/admin/ProxySSO-user-role-map

Access or create a user to role mapping.

**Authentication and authorization**

Requires the edit_user capability.

**GET**

Access user to role mappings

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roles</td>
<td>Roles mapped to the user</td>
</tr>
<tr>
<td>title</td>
<td>User name</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:changed https://localhost:8089/services/admin/ProxySSO-user-role-map
```

**XML Response**

```
...
<title>ProxySSO-user-role-map</title>
{id>https://localhost:8089/services/admin/ProxySSO-user-role-map</id>
...
<entry>
```
POST

Create a user to role mapping.

Changes are written to the etc/system/local directory.

Note: User to role mappings cannot be updated.

Request parameters
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>User name</td>
<td>Specify a user to map to specific roles</td>
</tr>
<tr>
<td>roles</td>
<td>User role name</td>
<td>Specify a role to map to the user. Use a separate roles parameter for each role that you are mapping.</td>
</tr>
</tbody>
</table>

**Returned values**
None

**XML Request**

curl -k -u admin:changed -X POST https://localhost:8089/services/admin/ProxySSO-user-role-map -d name=user1 -d roles=power

**XML Response**

```xml
<title>ProxySSO-user-role-map</title>
{id>https://wimpy:7102/services/admin/ProxySSO-user-role-map/id>
   ...
<entry>
   <title>user1</title>
   <id>https://wimpy:7102/services/admin/ProxySSO-user-role-map/user1</id>
   <updated>2016-08-31T17:57:53-07:00</updated>
   <link href="/services/admin/ProxySSO-user-role-map/user1" rel="alternate"/>
   <author>
      <name>system</name>
   </author>
   <link href="/services/admin/ProxySSO-user-role-map/user1" rel="list"/>
   <link href="/services/admin/ProxySSO-user-role-map/user1" rel="remove"/>
   <content type="text/xml">
      <s:dict>
         <s:key name="eai:acl">
            <s:dict>
               <s:key name="app">1</s:key>
               <s:key name="can_list">1</s:key>
               <s:key name="can_write">1</s:key>
               <s:key name="modifiable">0</s:key>
               <s:key name="owner">system</s:key>
               <s:key name="perms">
                  <s:dict>
                     <s:key name="read">
                        <s:list>
                           <s:item>admin</s:item>
                           <s:item>splunk-system-role</s:item>
                        </s:list>
                     </s:key>
                     <s:key name="write">
                        <s:list>
                           <s:item>admin</s:item>
                           <s:item>splunk-system-role</s:item>
                        </s:list>
                     </s:key>
                     <s:key name="removable">0</s:key>
                     <s:key name="sharing">system</s:key>
                  </s:dict>
               </s:key>
               <s:key name="roles">
                  <s:list>
                     <s:item>76</s:item>
                  </s:list>
               </s:key>
            </s:dict>
         </s:key>
      </s:dict>
   </content>
</entry>
```
admin/ProxySSO-user-role-map/{user_name}

https://<host>:<mPort>/services/admin/ProxySSO-user-role-map/{user_name}
Access or delete a user to role mapping.

Authentication and authorization
Requires the edit_user capability.

GET
Access role mappings for the {user_name} user.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roles</td>
<td>Roles mapped to the {user_name} user.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k u admin:changed https://localhost:8089/services/admin/ProxySSO-user-role-map/user1

XML Response

<entry>
<title>user1</title>
</entry>
DELETE

Delete the `{user_name}` user to role mapping.

Changes are written to the `etc/system/local` directory.

Request parameters
None
Returned values
The response lists remaining user to role mappings.

Example request and response

XML Request

curl -k -u admin:changed -X DELETE https://localhost:8089/services/admin/ProxySSO-user-role-map/user2

XML Response

<title>ProxySSO-user-role-map</title>
<id>https://localhost:8089/services/admin/ProxySSO-user-role-map</id>
...
<entry>
<title>user1</title>
<id>https://localhost:8089/services/admin/ProxySSO-user-role-map/user1</id>
<updated>2016-08-31T18:11:02-07:00</updated>
<author>
<name>system</name>
</author>
<link href="/services/admin/ProxySSO-user-role-map/user1" rel="alternate"/>
<link href="/services/admin/ProxySSO-user-role-map/user1" rel="list"/>
<link href="/services/admin/ProxySSO-user-role-map/user1" rel="remove"/>
<content type="text/xml">
<s:dict>
<s:key name="eai:acl">
<s:dict>
<s:key name="app" />
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
<s:key name="roles">
<s:list>
<s:item>power</s:item>
</s:list>
</s:key>
</s:dict>
</s:dict>
</content>
SAML REST API usage details

Splunk Enterprise users can configure SAML authentication for single sign-on (SSO). If you are using Splunk Cloud, contact Support to request assistance.

You can use the REST API to make the following SAML configurations.

- Manage group and user role mappings.
- Access service and identity provider information.
- Replicate SAML IdP certificates across a search head cluster.

For more information on using SAML for SSO, see Authentication using single sign-on with SAML in Securing Splunk Enterprise. You can also review the SAML settings stanza in authentication.conf in the Admin Manual.

admin/replicate-SAML-certs

https://<host>:<mPort>/services/admin/replicate-SAML-certs
Replicate SAML IdP certificates across a search head cluster.

Note: This endpoint is only available for use on search head clustered deployments with KV Store enabled.

Authentication and authorization
Requires the change_authentication capability for access.

POST

Usage details
After editing SAML IdP certificate files in $SPLUNK_HOME/etc/auth/idpCerts on one node in the cluster, you can POST to /replicate-SAML-certs to replicate the certificates across the cluster. This can be useful if there is an error in the certificate files from /SAML-idp-metadata and you need to edit them manually.

There are no request parameters or returned values.

admin/SAML-groups

https://<host>:<mPort>/services/admin/SAML-groups
Manage external groups in an IdP response to internal Splunk roles.

Authentication and authorization
Requires change_authentication capability for all operations.
GET

Access internal roles for this external group.

Request parameters
None.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>roles</td>
<td>Corresponding internal role for the external group.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:password https://localhost:8089/services/admin/SAML-groups

XML Response

<title>SAML-groups</title>
<ID>https://localhost:8089/services/admin/SAML-groups</ID>
<updated>2015-11-07T18:00:05-08:00</updated>
<generator build="05ee6658a12a17d11f47076b544" version="20151021"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/SAML-groups/_new" rel="create"/>
<link href="/services/admin/SAML-groups/_acl" rel="_acl"/>
<opensearch:totalResults>4</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<smessages/>
<entry>
  <title>admin</title>
  <ID>https://localhost:8089/services/admin/SAML-groups/admin</ID>
  <updated>2015-11-07T18:00:05-08:00</updated>
  <author>
    <name>system</name>
  </author>
  <link href="/services/admin/SAML-groups/admin" rel="alternate"/>
  <link href="/services/admin/SAML-groups/admin" rel="list"/>
  <link href="/services/admin/SAML-groups/admin" rel="edit"/>
  <link href="/services/admin/SAML-groups/admin" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
<s:dict>
  <s:key name="modifiable">0</s:key>
  <s:key name="owner">system</s:key>
  <s:key name="perms">
    <s:dict>
      <s:key name="read">
        <s:list>
          <s:item>_spl_cloud</s:item>
          <s:item>_spl_cloud_user</s:item>
          <s:item>admin</s:item>
          <s:item>spl_cloud_user</s:item>
          <s:item>splunk-system-role</s:item>
        </s:list>
      </s:key>
      <s:key name="write">
        <s:list>
          <s:item>_spl_cloud</s:item>
          <s:item>_spl_cloud_user</s:item>
          <s:item>admin</s:item>
          <s:item>spl_cloud_user</s:item>
          <s:item>splunk-system-role</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </s:key>
  <s:key name="removable">0</s:key>
  <s:key name="sharing">system</s:key>
  <s:dict>
    <s:key name="roles">
      <s:list>
        <s:item>sc_admin</s:item>
      </s:list>
    </s:key>
  </s:dict>
</s:dict>
<entry>
<title>power admin</title>
<id>https://localhost:8089/services/admin/SAML-groups/power%20admin</id>
<updated>2015-11-07T18:00:05-08:00</updated>
<link href="/services/admin/SAML-groups/power%20admin" rel="alternate"/>
<author>
<name>system</name>
</author>
<link href="/services/admin/SAML-groups/power%20admin" rel="list"/>
<link href="/services/admin/SAML-groups/power%20admin" rel="edit"/>
<link href="/services/admin/SAML-groups/power%20admin" rel="remove"/>
<content type="text/xml">
<s:dict>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>_spl_cloud</s:item>
<s:item>_spl_cloud_user</s:item>
<s:item>admin</s:item>
<s:item>spcl_cloud_user</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
</s:dict>
</s:dict>
</s:dict>
</entry>
POST

Convert an external group to internal roles.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>External group name.</td>
</tr>
<tr>
<td>roles</td>
<td>String</td>
<td>Equivalent internal role for the group.</td>
</tr>
</tbody>
</table>

Response keys

None

Example request and response

XML Request

```bash
curl -k -u admin:changeme https://localhost:8089/services/admin/SAML-groups -d name=Splunk -d roles=user
```

XML Response

```xml
<title>SAML-groups</title>
<id>https://localhost:8089/services/admin/SAML-groups</id>
<updated>2015-11-07T18:04:56-08:00</updated>
<generator build="05ee6658a1d11f47076b549133a47050ca24" version="20151021"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/SAML-groups/_new" rel="create"/>
<link href="/services/admin/SAML-groups/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```
admin/SAML-groups/{group_name}

https://<host>:<mPort>/services/admin/SAML-groups/{group_name}
Delete the `{group_name}` group.

**Authentication and authorization**
Requires `change_authentication` capability for all operations.

**DELETE**
Delete the `{group_name}` particular group.

**Request parameters**
None

**Response keys**
None

**Example request and response**

**XML Request**

```bash
curl -k -u admin:password --request DELETE https://localhost:8089/services/admin/SAML-groups/group_to_delete
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>SAML-groups</title>
  <id>https://localhost:8089/services/admin/SAML-groups</id>
  <updated>2015-11-07T18:04:25-08:00</updated>
  <generator build="05ee6658a12a17d11f47133a47050ca24" version="20151021"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/SAML-groups/_new" rel="create"/>
  <link href="/services/admin/SAML-groups/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

admin/SAML-idp-metadata

https://<host>:<mPort>/services/admin/SAML-idp-metadata
Access IdP SAML metadata attributes.
Authentication and authorization
Requires change_authentication capability for all operations.

GET
Access SAML user and role information for saved searches.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>idpMetadataFile</td>
<td>File path. See description.</td>
<td>Full path of the metadata file location. File should be local to splunkd server.</td>
</tr>
</tbody>
</table>

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>idpMetadataPayload</td>
<td>SAML IdP metadata in XML format.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/admin/SAML-idp-metadata

XML Response

<title>SAML-idp-metadata</title>
<id>https://localhost:8089/services/admin/SAML-idp-metadata</id>
<updated>2015-11-07T18:34:07-08:00</updated>
<generator build="05ee6658a12a17d11f47076h3453ffdd50ca24" version="20151021"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/SAML-idp-metadata/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>idpMetadataPayload</title>
  <id>https://localhost:8089/services/admin/SAML-idp-metadata/idpMetadataPayload</id>
  <updated>2015-11-07T18:34:07-08:00</updated>
  <link href="/services/admin/SAML-idp-metadata/idpMetadataPayload" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/admin/SAML-idp-metadata/idpMetadataPayload" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
      </s:dict>
    </s:dict>
  </content>
</entry>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
  <s:dict>
    <s:key name="read">
      <s:list>
        <s:item>_spl_cloud</s:item>
        <s:item>_spl_cloud_user</s:item>
        <s:item>admin</s:item>
        <s:item>spl_cloud_user</s:item>
        <s:item>splunk-system-role</s:item>
      </s:list>
    </s:key>
    <s:key name="write">
      <s:list>
        <s:item>_spl_cloud</s:item>
        <s:item>_spl_cloud_user</s:item>
        <s:item>admin</s:item>
        <s:item>spl_cloud_user</s:item>
        <s:item>splunk-system-role</s:item>
      </s:list>
    </s:key>
  </s:dict>
</s:key>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
<s:key name="idpCertificatePayload"><![CDATA[MIIDpjCCAo6gAwIBAgIGAU7gBZ6oMA0GCSqGS1b3DQEBBQUAMIGTQsawCQYDVQQGEwJVUzETMBEGAIUECAwQFsaWZvcrttery444uIEzyYW5jaXNhbnMAsGAIEgwET2t0YTEUMBIGAIECuwL1NFUH5YvdmlkZXZxMzASZwcS53Nt3RicQxRMRwGgYJKoZIhvcNAQkBDQ1phM5aVQ9rDGEuY29tMB4XDTExMD1zcmMzE3MzEyMVcXDTQ1MzczMDE3MzIyMVowZXMCAwJgNBVAYTA1nJhbnNpc2NvMwQwYXV0aWwu+/s这份证书由系统成功签发。证书的有效期为2023-03-22至2024-03-22，使用算法SHA256。证书包含公钥，公钥用于验证对方的签名是否有效。证书中还包含一个签名算法，用于确认证书的合法性。证书的主体部分包括IDP的名称和标识符。IDP的名称为"test.example.com"。

<s:key name="protocol_endpoints">
  <s:dict>
    <s:key name="idpSLOUrl">https://test.example.com/app/example/exk4nkqqsypk32FMF0h7/slo/saml</s:key>
    <s:key name="idpSSOUrl">https://test.example.com/app/example/exk4nkqqsypk32FMF0h7/sso/saml</s:key>
  </s:dict>
</s:key>
<s:key name="signAuthnRequest">1</s:key>
</s:dict>
</entry>
admin/SAML-sp-metadata

https://<host>:<mPort>/services/admin/SAML-sp-metadata
Access service provider SAML metadata attributes.

Authentication and authorization
Requires change_authentication capability for all operations.

GET
Access SAML metadata attributes.

Request parameters
None.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spMetadataPayload</td>
<td>SAML service provider metadata in XML format.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:changeme https://localhost:8089/services/admin/SAML-sp-metadata

**XML Response**

```xml
<title>SAML-sp-metadata</title>
<id>https://localhost:8089/services/admin/SAML-sp-metadata</id>
<updated>2015-12-16T13:47:39-08:00</updated>
<generator build="d48f9f793521" version="6.4.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/SAML-sp-metadata/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>spMetadata</title>
  <id>https://localhost:8089/services/admin/SAML-sp-metadata/spMetadata</id>
  <updated>2015-12-16T13:47:39-08:00</updated>
  <link href="/services/admin/SAML-sp-metadata/spMetadata" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
</entry>
```
<s:dict>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app"></s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">0</s:key>
      <s:key name="owner">system</s:key>
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>admin</s:item>
            <s:item>splunk-system-role</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>admin</s:item>
            <s:item>splunk-system-role</s:item>
          </s:list>
        </s:key>
      </s:dict>
      <s:key name="removable">0</s:key>
      <s:key name="sharing">system</s:key>
    </s:dict>
  </s:dict>
</s:dict>

<content type="text/xml">
<s:dict>
  <s:key name="spMetadata"><![CDATA[<md:EntityDescriptor entityID="splunkEntityId"
<md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
AuthnRequestsSigned="true" WantAssertionsSigned="true" xmlns:oasis:names:tc:SAML:2.0:metadata>
<md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</md:NameIDFormat>
</md:SPSSODescriptor></md:EntityDescriptor>]]></s:key>
</s:dict>
</content>
admin/SAML-user-role-map

https://<host>:<mPort>/services/admin/SAML-user-role-map

Description

Access or create SAML user and role information for saved searches if your IdP does not support Attribute Query Requests. To delete a username, see admin/SAML-user-role-map/{name}.

Authentication and authorization
Requires edit_user capability for all operations.

GET

Access SAML user and role information for saved searches.

Request parameters

None.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>SAML username for running saved searches.</td>
</tr>
<tr>
<td>roles</td>
<td>Assigned roles for this user.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -k -u admin:password https://localhost:8089/services/admin/SAML-user-role-map
```

XML Response

```xml
<title>SAML-user-role-map</title>
<ID>https://localhost:8089/services/admin/SAML-user-role-map</ID>
<updated>2015-11-07T17:34:12-08:00</updated>
<generator build="05ee6658a12a17d11f47076b549133a47050ca24" version="20151021"/>
<author>
   <name>Splunk</name>
</author>
<link href="/services/admin/SAML-user-role-map/_new" rel="create"/>
<link href="/services/admin/SAML-user-role-map/_acl" rel="_acl"/>
<opensearch:totalResults>3</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
   <title>samluser001@example.com</title>
   <ID>https://localhost:8089/services/admin/SAML-user-role-map/samluser001%40example.com</ID>
   <updated>2015-11-07T17:34:12-08:00</updated>
</entry>
```

91
<link href="/services/admin/SAML-user-role-map/samluser001@example.com" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/admin/SAML-user-role-map/samluser001@example.com" rel="list"/>
<link href="/services/admin/SAML-user-role-map/samluser001@example.com" rel="remove"/>
<content type="text/xml">
  <s:dict>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app"></s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">0</s:key>
        <s:key name="owner">system</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>_spl_cloud</s:item>
                <s:item>_spl_cloud_user</s:item>
                <s:item>admin</s:item>
                <s:item>sc_admin</s:item>
                <s:item>spl_cloud_user</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
                <s:item>_spl_cloud</s:item>
                <s:item>_spl_cloud_user</s:item>
                <s:item>admin</s:item>
                <s:item>sc_admin</s:item>
                <s:item>spl_cloud_user</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="removable">0</s:key>
        <s:key name="sharing">system</s:key>
      </s:dict>
    </s:key>
    <s:key name="email">samluser001@example.com</s:key>
    <s:key name="realname">Firstname Lastname001</s:key>
    <s:key name="roles">
      <s:list>
        <s:item>sc_admin</s:item>
        <s:item>user</s:item>
      </s:list>
    </s:key>
  </s:dict>
</content>
</entry>
<entry>
  <title>samluser002@example.com</title>
  <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser002@example.com</id>
  <updated>2015-11-07T17:34:12-08:00</updated>
  <link href="/services/admin/SAML-user-role-map/samluser002@example.com" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
</entry>
<link href="/services/admin/SAML-user-role-map/samluser002@example.com" rel="list"/>
<link href="/services/admin/SAML-user-role-map/samluser002@example.com" rel="remove"/>
<content type="text/xml">
  <s:dict>
    <s:dict name="eai:acl">
      <s:dict name="app">
        <s:dict name="can_list">1</s:dict>
        <s:dict name="can_write">1</s:dict>
        <s:dict name="modifiable">0</s:dict>
        <s:dict name="owner">system</s:dict>
        <s:dict name="perms">
          <s:dict name="read">
            <s:list>
              <s:item>_spl_cloud</s:item>
              <s:item>_spl_cloud_user</s:item>
              <s:item>admin</s:item>
              <s:item>sc_admin</s:item>
              <s:item>spl_cloud_user</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:dict>
          <s:dict name="write">
            <s:list>
              <s:item>_spl_cloud</s:item>
              <s:item>_spl_cloud_user</s:item>
              <s:item>admin</s:item>
              <s:item>sc_admin</s:item>
              <s:item>spl_cloud_user</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:dict>
        </s:dict>
        <s:dict name="removable">0</s:dict>
        <s:dict name="sharing">system</s:dict>
      </s:dict>
    </s:dict>
    <s:dict name="email">samluser002@example.com</s:dict>
    <s:dict name="realname">Firstname Lastname002</s:dict>
    <s:dict name="roles">
      <s:list>
        <s:item>power</s:item>
      </s:list>
    </s:dict>
  </s:dict>
</content>

93
POST

Update SAML user and role information for saved searches.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>SAML username for running saved searches.</td>
</tr>
<tr>
<td>roles</td>
<td>String</td>
<td>Assigned roles for this user.</td>
</tr>
</tbody>
</table>

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>SAML username for running saved searches.</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>roles</td>
<td>Assigned roles for this user.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```
curl -k -u admin:password https://localhost:8089/services/admin/SAML-user-role-map -d
name=samluser004@example.foo -d roles=user
```

**XML Response**

```
<title>SAML-user-role-map</title>
<id>https://localhost:8089/services/admin/SAML-user-role-map</id>
<updated>2015-11-07T17:45:54-08:00</updated>
<generator build="05ee6658a12a17d11f47076b549133a47050ca24" version="20151021"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/admin/SAML-user-role-map/_new" rel="create"/>
<link href="/services/admin/SAML-user-role-map/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>samluser004@example.foo</title>
  <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser004@example.foo</id>
  <updated>2015-11-07T17:45:54-08:00</updated>
  <link href="/services/admin/SAML-user-role-map/samluser004@example.foo" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/admin/SAML-user-role-map/samluser004@example.foo" rel="list"/>
  <link href="/services/admin/SAML-user-role-map/samluser004@example foo" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>_spl_cloud</s:item>
                <s:item>_spl_cloud_user</s:item>
                <s:item>admin</s:item>
                <s:item>sc_admin</s:item>
                <s:item>spl_cloud_user</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:dict>
          </s:dict>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
```
DELETE

See admin/SAML-user-role-map/{name}

admin/SAML-user-role-map/{name}

https://<host>:<mPort>/services/admin/SAML-user-role-map/{name}
Delete SAML user and role information for saved searches if your IdP does not support Attribute Query Requests.

Authentication and authorization
Requires edit_user capability for all operations.

DELETE

Remove a username from SAML users for saved searches.

Request parameters

None.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>SAML username for running saved searches.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>roles</td>
<td>Assigned roles for this user.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:password --request DELETE https://localhost:8089/services/admin/SAML-user-role-map/samluser004@example.com

**XML Response**

```xml
<title>SAML-user-role-map</title>
<id>https://localhost:8089/services/admin/SAML-user-role-map</id>
<updated>2015-11-07T17:46:26-08:00</updated>
<generator build="05ee6658a12a177d11f47076b549133a47050ca24" version="20151021"/>
<author>
    <name>Splunk</name>
</author>
<link href="/services/admin/SAML-user-role-map/_new" rel="create"/>
<link href="/services/admin/SAML-user-role-map/_acl" rel="_acl"/>
<opensearch:totalResults>3</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
    <title>samluser001@example.com</title>
    <id>https://localhost:8089/services/admin/SAML-user-role-map/samluser001%40example.com</id>
    <updated>2015-11-07T17:46:26-08:00</updated>
    <link href="/services/admin/SAML-user-role-map/samluser001%40example.com" rel="alternate"/>
    <author>
        <name>system</name>
    </author>
    <link href="/services/admin/SAML-user-role-map/samluser001%40example.com" rel="list"/>
    <link href="/services/admin/SAML-user-role-map/samluser001%40example.com" rel="remove"/>
    <content type="text/xml">
        <s:dict>
            <s:key name="eai:acl">
                <s:dict>
                    <s:key name="app"></s:key>
                    <s:key name="can_list">1</s:key>
                    <s:key name="can_write">1</s:key>
                    <s:key name="modifiable">0</s:key>
                    <s:key name="owner">system</s:key>
                    <s:key name="perms">
                        <s:dict>
                            <s:key name="read">
                                <s:list>
                                    <s:item>_spl_cloud</s:item>
                                    <s:item>_spl_cloud_user</s:item>
                                    <s:item>admin</s:item>
                                    <s:item>sc_admin</s:item>
                                    <s:item>_spl_cloud_user</s:item>
                                    <s:item>splunk-system-role</s:item>
                                </s:list>
                            </s:key>
                        </s:dict>
                    </s:key>
                    <s:key name="write">
                        <s:list>
                            <s:item>97</s:item>
                        </s:list>
                    </s:key>
                    <s:key name="read"></s:key>
                    <s:key name="write"></s:key>
                </s:dict>
            </s:key>
        </s:dict>
    </content>
</entry>
```
<entry>
<title>samluser002@example.com</title>
<id>https://localhost:8089/services/admin/SAML-user-role-map/samluser002%40example.com</id>
<updated>2015-11-07T17:46:26-08:00</updated>
<author>
  <name>system</name>
</author>
<link href="/services/admin/SAML-user-role-map/samluser002%40example.com" rel="alternate"/>
<content type="text/xml">
<s:dict>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app">0</s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">0</s:key>
      <s:key name="owner">system</s:key>
      <s:key name="perms">
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>_spl_cloud</s:item>
              <s:item>_spl_cloud_user</s:item>
              <s:item>admin</s:item>
              <s:item>sc_admin</s:item>
              <s:item>spl_cloud_user</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:key>
          <s:key name="write">
            <s:list>
              <s:item>_spl_cloud</s:item>
              <s:item>_spl_cloud_user</s:item>
              <s:item>admin</s:item>
              <s:item>sc_admin</s:item>
              <s:item>spl_cloud_user</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
</content>
</entry>
authentication/providers/SAML

https://<host>:<mPort>/services/authentication/providers/SAML

Access and create SAML configurations.

Authentication and authorization
Requires change_authentication capability for all operations.

GET
Access SAML configurations.

Request parameters
None.

Response keys
None.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowSslCompression</td>
<td>Indicates whether ssl data compression is enabled.</td>
</tr>
<tr>
<td>assertionConsumerServiceUrl</td>
<td>Endpoint where SAML assertions are posted by the IdP.</td>
</tr>
<tr>
<td>attributeAliasMail</td>
<td>Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.</td>
</tr>
<tr>
<td>attributeAliasRealName</td>
<td>Specifies which SAML attribute maps to 'realName'. Defaults to realName.</td>
</tr>
<tr>
<td>attributeAliasRole</td>
<td>Specifies which SAML attribute maps to role. Defaults to role.</td>
</tr>
<tr>
<td>attributeQueryRequestSigned</td>
<td>Indicates whether Attribute Queries should be signed.</td>
</tr>
<tr>
<td>attributeQueryResponseSigned</td>
<td>Indicates whether Attribute Query responses should be signed.</td>
</tr>
<tr>
<td>attributeQuerySoapPassword</td>
<td>Credentials for making Attribute Query using SOAP over HTTP.</td>
</tr>
<tr>
<td>attributeQuerySoapUsername</td>
<td>Credentials for making Attribute Query using SOAP over HTTP.</td>
</tr>
<tr>
<td>attributeQueryTTL</td>
<td>ttl (time to live) for the Attribute Query credentials cache.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list of user names from the IDP response to be blacklisted by Splunk software.</td>
</tr>
<tr>
<td>caCertFile</td>
<td>File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Ciphersuite for making Attribute Queries using ssl. For example, TLSv1+HIGH:+STRENGTH.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>defaultRoleIFMissing</td>
<td>Default role to use if no role is returned in a SAML response.</td>
</tr>
<tr>
<td>ecdhCurves</td>
<td>EC curves for ECDH/ECDHE key exchange - ssl setting.</td>
</tr>
<tr>
<td>entityId</td>
<td>Unique id preconfigured by the IdP.</td>
</tr>
<tr>
<td>errorUrl</td>
<td>URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or Splunk deployment.</td>
</tr>
<tr>
<td>errorUrlLabel</td>
<td>Label or title of the content to which errorUrl points. Defaults to Click here to resolve SAML error.</td>
</tr>
<tr>
<td>fqdn</td>
<td>Load balancer url.</td>
</tr>
<tr>
<td>idpAttributeQueryUrl</td>
<td>IdP attribute query url where SAML attribute queries are sent.</td>
</tr>
<tr>
<td>idpCertPath</td>
<td>Path for IdP certificate.</td>
</tr>
<tr>
<td>idpSLOUrl</td>
<td>IdP sso url where SAML SSO requests are sent.</td>
</tr>
<tr>
<td>idpSSOUrl</td>
<td>IdP SSO url where SAML SLO requests are sent.</td>
</tr>
<tr>
<td>maxAttributeQueryQueueSize</td>
<td>Maximum number of Attribute jobs to queue.</td>
</tr>
<tr>
<td>maxAttributeQueryThreads</td>
<td>Maximum number of threads for asynchronous Attribute Queries.</td>
</tr>
<tr>
<td>name</td>
<td>Configuration stanza name.</td>
</tr>
<tr>
<td>redirectAfterLogoutToUrl</td>
<td>Redirect URL after user logout If no SLO URL is configured.</td>
</tr>
<tr>
<td>redirectPort</td>
<td>Port where SAML responses are sent. Typically, this is the web port. Set this port if internal port redirection is needed. The assertionconsumerServiceUrl in the AuthNRequest uses the set port instead of the splunkweb port. To prevent any port information being appended to the assertionConsumerServiceUrl, set to 0.</td>
</tr>
<tr>
<td>signAuthnRequest</td>
<td>Indicates whether to sign authentication requests.</td>
</tr>
<tr>
<td>signatureAlgorithm</td>
<td>Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when signedAuthnRequest is set to true. Possible values are:</td>
</tr>
</tbody>
</table>
|                             | • RSA-SHA1 (default)  
|                             |   • corresponds to http://www.w3.org/2000/09/xmldsig#rsa-sha1  
|                             | • RSA-SHA256  
|                             |   • corresponds to http://www.w3.org/2001/04/xmldsig-more#rsa-sha256                                                                      |
| signedAssertion             | Indicates whether to sign SAML assertions.                                                                                                   |
| singleLogoutServiceUrl      | URL where the IdP posts SAML Single Logout responses.                                                                                       |
| skipAttributeQueryForUsers  | Used in conjunction with defaultRoleIFMissing. Indicates whether to skip Attribute Queries for some users.                                  |
| sloBinding                  | Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are HTTPPost (default) and HTTPRedirect. This binding must match the binding configured on the IDP. |

101
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spCertPath</td>
<td>Service provider certificate path.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>Alternate name to check in the peer certificate.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>Common name to check in the peer certificate.</td>
</tr>
<tr>
<td>sslKeysfile</td>
<td>Location of service provider private key.</td>
</tr>
<tr>
<td>sslKeysfilePassword</td>
<td>SSL password.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Indicates whether to verify peer certificate.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>SSL versions.</td>
</tr>
<tr>
<td>ssoBinding</td>
<td>Binding used when making a SP-initiated SAML request. Possible values are HTTPPost (default) and HTTPRedirect. This binding must match the binding configured on the IDP.</td>
</tr>
<tr>
<td>uiStatusPage</td>
<td>Splunk Web page for redirecting users in case of errors.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```bash
curl -u admin:pass -k -X GET https://localhost:8089/services/authentication/providers/SAML
```

**XML Response**

```xml
<title>SAML-auth</title>
<id>https://localhost:8089/services/authentication/providers/SAML</id>
<updated>2017-04-10T23:27:22+00:00</updated>
<generator build="a8914247a786" version="6.5.1612"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authentication/providers/SAML/_new" rel="create"/>
<link href="/services/authentication/providers/SAML/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>saml-test</title>
<id>https://localhost:8089/services/authentication/providers/SAML/saml-test</id>
<updated>2017-04-10T23:27:22+00:00</updated>
<author>
  <name>system</name>
</author>
<link href="/services/authentication/providers/SAML/saml-test" rel="alternate"/>
<link href="/services/authentication/providers/SAML/saml-test" rel="list"/>
<link href="/services/authentication/providers/SAML/saml-test" rel="edit"/>
<link href="/services/authentication/providers/SAML/saml-test" rel="remove"/>
<link href="/services/authentication/providers/SAML/saml-test/disable" rel="disable"/>
<content type="text/xml">
  <s:dict>
    <s:dict name="allowSslCompression">true</s:dict>
    <s:dict name="assertionConsumerServiceUrl">http://so1:12800/saml/acs</s:dict>
    <s:dict name="attributeQueryRequestSigned">1</s:dict>
    <s:dict name="attributeQueryResponseSigned">1</s:dict>
  </s:dict>
</content>
```

102
POST

Create a new SAML configuration.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowSslCompression</td>
<td>Indicates whether ssl data compression is enabled.</td>
</tr>
<tr>
<td>attributeAliasMail</td>
<td>Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.</td>
</tr>
<tr>
<td>attributeAliasRealName</td>
<td>Specifies which SAML attribute maps to 'realName'. Defaults to realName.</td>
</tr>
<tr>
<td>attributeAliasRole</td>
<td>Specifies which SAML attribute maps to role. Defaults to role.</td>
</tr>
<tr>
<td>attributeQueryRequestSigned</td>
<td>Indicates whether Attribute Queries should be signed.</td>
</tr>
<tr>
<td>attributeQueryResponseSigned</td>
<td>Indicates whether Attribute Query responses should be signed.</td>
</tr>
<tr>
<td>attributeQuerySoapPassword</td>
<td>Credentials for making Attribute Query using SOAP over HTTP.</td>
</tr>
<tr>
<td>attributeQuerySoapUsername</td>
<td>Credentials for making Attribute Query using SOAP over HTTP.</td>
</tr>
<tr>
<td>attributeQueryTTL</td>
<td>ttl (time to live) for the Attribute Query credentials cache.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list of user names from the IDP response to be blacklisted by Splunk software.</td>
</tr>
<tr>
<td>caCertFile</td>
<td>File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Ciphersuite for making Attribute Queries using ssl. For example, TLSv1+HIGH:@STRENGTH.</td>
</tr>
<tr>
<td>defaultRoleIfMissing</td>
<td>Default role to use if no role is returned in a SAML response.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ecdhCurves</td>
<td>EC curves for ECDH/ECDHE key exchange - ssl setting.</td>
</tr>
<tr>
<td>entityId</td>
<td>Required. Unique id preconfigured by the IdP.</td>
</tr>
<tr>
<td>errorUrl</td>
<td>URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or the Splunk deployment.</td>
</tr>
<tr>
<td>errorUrlLabel</td>
<td>Label or title of the content to which errorUrl points. Defaults to Click here to resolve SAML error.</td>
</tr>
<tr>
<td>fqdn</td>
<td>Load balancer url.</td>
</tr>
<tr>
<td>idpAttributeQueryUrl</td>
<td>IdP attribute query url where SAML attribute queries are sent.</td>
</tr>
<tr>
<td>idpCertPath</td>
<td>Path for IdP certificate.</td>
</tr>
<tr>
<td>idpMetadataFile</td>
<td>Full path to idpMetadata on disk. Used to retrieve IdP information such as idpSLOUrl, idpSSOUrl, and signing certificate.</td>
</tr>
<tr>
<td>idpSLOUrl</td>
<td>IdP sso url where SAML SSO requests are sent.</td>
</tr>
<tr>
<td>idpSSOUrl</td>
<td>Required. IdP SSO url where SAML SLO requests are sent.</td>
</tr>
<tr>
<td>name</td>
<td>Required. Configuration stanza name.</td>
</tr>
<tr>
<td>nameIdFormat</td>
<td>Specifies how subject is identified in SAML Assertion. Defaults to urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified Override it when using Azure AD as an IDP and set it to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</td>
</tr>
<tr>
<td>redirectAfterLogoutToUrl</td>
<td>Redirect URL after user logout If no SLO URL is configured.</td>
</tr>
<tr>
<td>redirectPort</td>
<td>Port where SAML responses are sent. Typically, this is the web port. Set this port if internal port redirection is needed. The assertionconsumerServiceUrl in the AuthNRequest uses the set port instead of the splunkweb port. To prevent any port information being appended to the assertionConsumerServiceUrl, set to 0.</td>
</tr>
<tr>
<td>signAuthnRequest</td>
<td>Indicates whether to sign authentication requests.</td>
</tr>
<tr>
<td>signatureAlgorithm</td>
<td>Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when signedAuthnRequest is set to true. Possible values are:RSA-SHA1 (default) corresponds to <a href="http://www.w3.org/2000/09/xmldsig#rsa-sha1">http://www.w3.org/2000/09/xmldsig#rsa-sha1</a> RSA-SHA256 corresponds to <a href="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256">http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</a></td>
</tr>
<tr>
<td>signedAssertion</td>
<td>Indicates whether to sign SAML assertions.</td>
</tr>
<tr>
<td>skipAttributeQueryRequestForUsers</td>
<td>Used in conjunction with defaultRoleIFMissing. Indicates whether to skip Attribute Queries for some users.</td>
</tr>
<tr>
<td>sloBinding</td>
<td>Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are HTTPPost (default) and HTTPRedirect. This binding must match the binding configured on the IDP.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>Alternate name to check in the peer certificate.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>Common name to check in the peer certificate.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>sslKeysfile</td>
<td>Location of service provider private key.</td>
</tr>
<tr>
<td>sslKeysfilePassword</td>
<td>SSL password.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Indicates whether to verify peer certificate.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>SSL versions.</td>
</tr>
<tr>
<td>ssoBinding</td>
<td>Binding used when making a SP-initiated SAML request. Possible values are HTTPPost (default) and HTTPRedirect. This binding must match the binding configured on the IDP.</td>
</tr>
</tbody>
</table>

Response keys
None.

Example request and response

**XML Request**


**XML Response**

```xml
<title>SAML-auth</title>  
<id>https://localhost:8089/services/authentication/providers/SAML</id>  
<updated>2017-04-10T23:26:35+00:00</updated>  
<generator build="a8914247a786" version="6.5.1612"/>

<title>saml-test</title>  
<id>https://localhost:8089/services/authentication/providers/SAML/saml-test</id>  
<updated>2017-04-10T23:26:35+00:00</updated>  
<content type="text/xml">  
<s:dict>  
<s:key name="allowSslCompression">true</s:key>  
<s:key name="assertionConsumerServiceUrl">http://so1:12800/saml/acs</s:key>
```
authentication/providers/SAML/{stanza_name}

https://<host>:<mPort>/services/authentication/providers/SAML/{stanza_name}

GET

Access a SAML configuration.

Request parameters
None.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowSslCompression</td>
<td>Indicates whether ssl data compression is enabled.</td>
</tr>
<tr>
<td>assertionConsumerServiceUrl</td>
<td>Endpoint where SAML assertions are posted by the IdP.</td>
</tr>
<tr>
<td>attributeAliasMail</td>
<td>Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.</td>
</tr>
<tr>
<td>attributeAliasRealName</td>
<td>Specifies which SAML attribute maps to 'realName'. Defaults to realName.</td>
</tr>
<tr>
<td>attributeAliasRole</td>
<td>Specifies which SAML attribute maps to role. Defaults to role.</td>
</tr>
<tr>
<td>attributeQueryRequestSigned</td>
<td>Indicates whether Attribute Queries should be signed.</td>
</tr>
<tr>
<td>attributeQueryResponseSigned</td>
<td>Indicates whether Attribute Query responses should be signed.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>attributeQuerySoapUsername</td>
<td>Credentials for making Attribute Query using SOAP over HTTP.</td>
</tr>
<tr>
<td>attributeQuerySoapPassword</td>
<td>Credentials for making Attribute Query using SOAP over HTTP.</td>
</tr>
<tr>
<td>attributeQueryTTL</td>
<td>TTL (time to live) for the Attribute Query credentials cache.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP response.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list of user names from the IDP response to be blacklisted by Splunk software.</td>
</tr>
<tr>
<td>caCertFile</td>
<td>File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Ciphersuite for making Attribute Queries using ssl. For example, TLSv1+HIGH:@STRENGTH.</td>
</tr>
<tr>
<td>defaultRoleIfMissing</td>
<td>Default role to use if no role is returned in a SAML response.</td>
</tr>
<tr>
<td>ecdfCurves</td>
<td>EC curves for ECDH/ECDHE key exchange - ssl setting.</td>
</tr>
<tr>
<td>entityId</td>
<td>Unique id preconfigured by the IdP.</td>
</tr>
<tr>
<td>errorUrl</td>
<td>URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or Splunk deployment.</td>
</tr>
<tr>
<td>errorUrlLabel</td>
<td>Label or title of the content to which errorUrl points. Defaults to Click here to resolve SAML error..</td>
</tr>
<tr>
<td>fqdn</td>
<td>Load balancer url.</td>
</tr>
<tr>
<td>idpAttributeQueryUrl</td>
<td>IdP attribute query url where SAML attribute queries are sent.</td>
</tr>
<tr>
<td>idpCertPath</td>
<td>Path for IdP certificate.</td>
</tr>
<tr>
<td>idpSLOUrl</td>
<td>IdP sso url where SAML SSO requests are sent.</td>
</tr>
<tr>
<td>idpSSOUrl</td>
<td>IdP SSO url where SAML SLO requests are sent.</td>
</tr>
<tr>
<td>maxAttributeQueryQueueSize</td>
<td>Maximum number of Attribute jobs to queue.</td>
</tr>
<tr>
<td>maxAttributeQueryThreads</td>
<td>Maximum number of threads for asynchronous Attribute Queries.</td>
</tr>
<tr>
<td>name</td>
<td>Configuration stanza name.</td>
</tr>
<tr>
<td>nameIdFormat</td>
<td>Specifies how subject is identified in SAML Assertion. Defaults to urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified Override it when using Azure AD as an IDP and set it to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</td>
</tr>
<tr>
<td>redirectAfterLogoutToUrl</td>
<td>Redirect URL after user logout If no SLO URL is configured.</td>
</tr>
<tr>
<td>redirectPort</td>
<td>Port where SAML responses are sent. Typically, this is the web port. Set this port if internal port redirection is needed. The assertionconsumerServiceUrl in the AuthNRequest uses the set port instead of the splunkweb port. To prevent any port information being appended to the assertionConsumerServiceUrl, set to 0.</td>
</tr>
<tr>
<td>signAuthnRequest</td>
<td>Indicates whether to sign authentication requests.</td>
</tr>
<tr>
<td>signatureAlgorithm</td>
<td>Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when signedAuthnRequest is set to true. Possible values are:</td>
</tr>
</tbody>
</table>

109
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>signedAssertion</td>
<td>Indicates whether to sign SAML assertions.</td>
</tr>
<tr>
<td>singleLogoutServiceUrl</td>
<td>URL where the IdP posts SAML Single Logout responses.</td>
</tr>
<tr>
<td>skipAttributeQueryRequestForUsers</td>
<td>Used in conjunction with <code>defaultRoleIFMissing</code>. Indicates whether to skip Attribute Queries for some users.</td>
</tr>
<tr>
<td>sloBinding</td>
<td>Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are <code>HTTPPost</code> (default) and <code>HTTPRedirect</code>. This binding must match the binding configured on the IDP.</td>
</tr>
<tr>
<td>spCertPath</td>
<td>Service provider certificate path.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>Alternate name to check in the peer certificate.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>Common name to check in the peer certificate.</td>
</tr>
<tr>
<td>sslKeysfile</td>
<td>Location of service provider private key.</td>
</tr>
<tr>
<td>sslKeysfilePassword</td>
<td>SSL password.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Indicates whether to verify peer certificate.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>SSL versions.</td>
</tr>
<tr>
<td>ssoBinding</td>
<td>Binding used when making a SP-initiated SAML request. Possible values are <code>HTTPPost</code> (default) and <code>HTTPRedirect</code>. This binding must match the binding configured on the IDP.</td>
</tr>
<tr>
<td>uiStatusPage</td>
<td>Splunk Web page for redirecting users in case of errors.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:password https://localhost:8089/services/authentication/providers/SAML/saml_settings
```

**XML Response**

```xml
<title>SAML-auth</title>
<id>https://localhost:8089/services/authentication/providers/SAML</id>
<updated>2017-04-10T23:29:58+00:00</updated>
<generator build="a8914247a786" version="6.5.1612"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authentication/providers/SAML/_new" rel="create"/>
<link href="/services/authentication/providers/SAML/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>saml-test</title>
  <id>https://localhost:8089/services/authentication/providers/SAML/saml-test</id>
  <updated>2017-04-10T23:29:58+00:00</updated>
```

110
<content type="text/xml">
<s:dict>
  <s:key name="allowSslCompression">true</s:key>
  <s:key name="assertionConsumerServiceUrl">http://so1:12800/saml/acs</s:key>
  <s:key name="attributeQueryRequestSigned">1</s:key>
  <s:key name="attributeQueryResponseSigned">1</s:key>
  <s:key name="attributeQuerySoapPassword">******</s:key>
  <s:key name="attributeQuerySoapUsername">test_ping</s:key>
  <s:key name="attributeQueryTTL">3600</s:key>
  <s:key name="attribute_aliases"/>
  <s:key name="blacklistedAutoMappedRoles">
    <s:list/>
  </s:key>
  <s:key name="blacklistedUsers">
    <s:list/>
  </s:key>
  <s:key name="caCertFile">/opt/splunk/etc/auth/cacert.pem</s:key>
  <s:key name="cipherSuite"></s:key>
  <s:key name="defaultRoleIfMissing">
    <s:list/>
  </s:key>
  <s:key name="disabled">0</s:key>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app"></s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">0</s:key>
      <s:key name="owner">system</s:key>
      <s:key name="perms">
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>admin</s:item>
              <s:item>download</s:item>
              <s:item>report</s:item>
            </s:list>
          </s:key>
          <s:key name="write">
            <s:list>
              <s:item>admin</s:item>
              <s:item>download</s:item>
            </s:list>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
  <s:key name="eai:attributes">
    <s:dict>
      <s:key name="optionalFields">
        <s:list>
          <s:item>allowSslCompression</s:item>
          <s:item>attributeAliasMail</s:item>
          <s:item>attributeAliasRealName</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </s:key>
</s:dict>
</content>
<s:item>attributeAliasRole</s:item>
<s:item>attributeQueryRequestSigned</s:item>
<s:item>attributeQueryResponseSigned</s:item>
<s:item>attributeQuerySoapPassword</s:item>
<s:item>attributeQuerySoapUsername</s:item>
<s:item>attributeQueryTTL</s:item>
<s:item>blacklistedAutoMappedRoles</s:item>
<s:item>blacklistedUsers</s:item>
<s:item>caCertFile</s:item>
<s:item>cipherSuite</s:item>
<s:item>defaultRoleIfMissing</s:item>
<s:item>ecdhCurveName</s:item>
<s:item>ecdhCurves</s:item>
<s:item>entityId</s:item>
<s:item>errorUrl</s:item>
<s:item>errorUrlLabel</s:item>
<s:item>fqdn</s:item>
<s:item>idpAttributeQueryUrl</s:item>
<s:item>idpCertChains</s:item>
<s:item>idpCertPath</s:item>
<s:item>idpCertificatePayload</s:item>
<s:item>idpMetadataFile</s:item>
<s:item>idpMetadataPayload</s-item>
<s:item>idpSLOUrl</s-item>
<s:item>idpSSOUrl</s-item>
<s:item>issuerId</s-item>
<s:item>nameIdFormat</s-item>
<s:item>redirectAfterLogoutToUrl</s-item>
<s:item>redirectPort</s-item>
<s:item>replicateCertificates</s-item>
<s:item>signAuthnRequest</s-item>
<s:item>signatureAlgorithm</s-item>
<s:item>signedAssertion</s-item>
<s:item>skipAttributeQueryRequestForUsers</s-item>
<s:item>sloBinding</s-item>
<s:item>sslAltNameToCheck</s-item>
<s:item>sslCommonNameToCheck</s-item>
<s:item>sslKeysfile</s-item>
<s-item>sslKeysfilePassword</s-item>
<s-item>sslVerifyServerCert</s-item>
<s-item>sslVersions</s-item>
<s-item>ssoBinding</s-item>

<s:dict>

</s:dict>
POST

Update a SAML configuration.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>allowSslCompression</td>
<td>Indicates whether ssl data compression is enabled.</td>
</tr>
<tr>
<td>attributeAliasMail</td>
<td>Specifies which SAML attribute is mapped to 'email'. Defaults to 'email'.</td>
</tr>
<tr>
<td>attributeAliasRealName</td>
<td>Specifies which SAML attribute maps to 'realName'. Defaults to realName.</td>
</tr>
<tr>
<td>attributeAliasRole</td>
<td>Specifies which SAML attribute maps to role. Defaults to role.</td>
</tr>
<tr>
<td>attributeQueryRequestSigned</td>
<td>Indicates whether Attribute Queries should be signed.</td>
</tr>
<tr>
<td>attributeQueryResponseSigned</td>
<td>Indicates whether Attribute Query responses should be signed.</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attributeQuerySoapPassword</td>
<td>Credentials for making Attribute Query using SOAP over HTTP.</td>
</tr>
<tr>
<td>attributeQuerySoapUsername</td>
<td>Credentials for making Attribute Query using SOAP over HTTP.</td>
</tr>
<tr>
<td>attributeQueryTTL</td>
<td>ttl (time to live) for the Attribute Query credentials cache.</td>
</tr>
<tr>
<td>blacklistedAutoMappedRoles</td>
<td>Comma separated list of Splunk roles that should be blacklisted from being auto-mapped from the IDP Response.</td>
</tr>
<tr>
<td>blacklistedUsers</td>
<td>Comma separated list of user names from the IDP response to be blacklisted by Splunk software.</td>
</tr>
<tr>
<td>caCertFile</td>
<td>File path for CA certificate. For example, /home/user123/saml-install/etc/auth/server.pem</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Ciphersuite for making Attribute Queries using ssl. For example, TLSv1+HIGH:%STRENGTH.</td>
</tr>
<tr>
<td>defaultRoleIfMissing</td>
<td>Default role to use if no role is returned in a SAML response.</td>
</tr>
<tr>
<td>ecdhCurves</td>
<td>EC curves for ECDH/ECDHE key exchange - ssl setting.</td>
</tr>
<tr>
<td>entityId</td>
<td>Required. Unique id preconfigured by the IdP.</td>
</tr>
<tr>
<td>errorUrl</td>
<td>URL to display for a SAML error. Errors may be due to incorrect or incomplete configuration in either the IDP or the Splunk deployment.</td>
</tr>
<tr>
<td>errorUrlLabel</td>
<td>Label or title of the content to which errorUrl points. Defaults to Click here to resolve SAML error..</td>
</tr>
<tr>
<td>fqdn</td>
<td>Load balancer url.</td>
</tr>
<tr>
<td>idpAttributeQueryUrl</td>
<td>IdP attribute query url where SAML attribute queries are sent.</td>
</tr>
<tr>
<td>idpCertPath</td>
<td>Path for IdP certificate.</td>
</tr>
<tr>
<td>idpSLOUrl</td>
<td>IdP sso url where SAML SSO requests are sent.</td>
</tr>
<tr>
<td>idpSSOUrl</td>
<td>Required. IdP SSO url where SAML SLO requests are sent.</td>
</tr>
<tr>
<td>name</td>
<td>Required. Configuration stanza name.</td>
</tr>
<tr>
<td>nameIdFormat</td>
<td>Specifies how subject is identified in SAML Assertion. Defaults to urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified Override it when using Azure AD as an IDP and set it to urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</td>
</tr>
<tr>
<td>redirectAfterLogoutToUrl</td>
<td>Redirect URL after user logout If no SLO URL is configured.</td>
</tr>
<tr>
<td>redirectPort</td>
<td>Port where SAML responses are sent. Typically, this is the web port. Set this port if internal port redirection is needed. The assertionconsumerServiceUrl in the AuthNRequest uses the set port instead of the splunkweb port. To prevent any port information being appended to the assertionConsumerServiceUrl, set to 0.</td>
</tr>
<tr>
<td>signAuthnRequest</td>
<td>Indicates whether to sign authentication requests.</td>
</tr>
<tr>
<td>signatureAlgorithm</td>
<td>Applicable only for redirect binding. Indicates the signature algorithm used for a SP-initiated SAML request when signedAuthnRequest is set to true. Possible values are:</td>
</tr>
</tbody>
</table>
|                                          | • RSA-SHA1 (default)  
|                                          |  ♦ corresponds to http://www.w3.org/2000/09/xmldsig#rsa-sha1  
|                                          | • RSA-SHA256  
<p>|                                          |  ♦ corresponds to <a href="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256">http://www.w3.org/2001/04/xmldsig-more#rsa-sha256</a> |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>signedAssertion</td>
<td>Indicates whether to sign SAML assertions.</td>
</tr>
<tr>
<td>skipAttributeQueryRequestForUsers</td>
<td>Used in conjunction with defaultRoleIFMissing. Indicates whether to skip Attribute Queries for some users.</td>
</tr>
<tr>
<td>sloBinding</td>
<td>Binding used when making a logout request or sending a logout response to complete the logout workflow. Possible values are HTTPPost (default) and HTTPRedirect. This binding must match the binding configured on the IDP.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>Alternate name to check in the peer certificate.</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>Common name to check in the peer certificate.</td>
</tr>
<tr>
<td>sslKeysfile</td>
<td>Location of service provider private key.</td>
</tr>
<tr>
<td>sslKeysfilePassword</td>
<td>SSL password.</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Indicates whether to verify peer certificate.</td>
</tr>
<tr>
<td>sslVersions</td>
<td>SSL versions.</td>
</tr>
<tr>
<td>ssoBinding</td>
<td>Binding used when making a SP-initiated SAML request. Possible values are HTTPPost (default) and HTTPRedirect. This binding must match the binding configured on the IDP.</td>
</tr>
</tbody>
</table>

Response keys
None

Example request and response

XML Request

curl -k -u admin:changed https://localhost:8089/services/authentication/providers/SAML/saml-test -d "entityId=someOtherEntityId"

XML Response

```xml
<title>SAML-auth</title>
<id>https://localhost:8089/services/authentication/providers/SAML</id>
<updated>2017-04-10T23:30:41+00:00</updated>
<generator build="a8914247a786" version="6.5.1612"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authentication/providers/SAML/_new" rel="create"/>
<link href="/services/authentication/providers/SAML/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>saml-test</title>
  <id>https://localhost:8089/services/authentication/providers/SAML/saml-test</id>
  <updated>2017-04-10T23:30:41+00:00</updated>
  <link href="/services/authentication/providers/SAML/saml-test" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/providers/SAML/saml-test" rel="list"/>
```

115
authentication/providers/SAML/{stanza_name}/enable

https://<host>:<mPort>/services/authentication/providers/SAML/{stanza_name}/enable

POST

Enable a SAML strategy.

Request parameters
None

Returned values
None

Example request

curl -k -u admin:password -X POST
https://localhost:8089/services/authentication/providers/SAML/my_strategy/disable
authentication/providers/SAML/{stanza_name}/disable

https://<host>:<mPort>/services/authentication/providers/SAML/{stanza_name}/disable

POST

Disable a SAML strategy.

Request parameters
None

Returned values
None

Example request

curl -k -u admin:password -X POST
https://localhost:8089/services/authentication/providers/SAML/my_strategy/disable

auth/login

https://<host>:<mPort>/services/auth/login

Get a session ID for use in subsequent API calls that require authentication. Set up cookie-based authorization.

The splunkd server supports token-based authentication using the standard HTTP authorization header. Before you can access Splunk Enterprise resources, you must authenticate with the splunkd server using your username and password.

Use cookie-based authorization

To use cookie-based authorization, first ensure that the allowCookieAuth setting is enabled in server.conf. By default, this setting is enabled in Splunk software versions 6.2 and later.

If allowCookieAuth is enabled, you can pass a cookie=1 parameter to the POST request on auth/login. As noted in the Response data keys section below, a Set-Cookie header is returned. This header must be used in subsequent requests.

Any request authenticated using a cookie may include a new Set-Cookie header in its response. Use this new cookie value in any subsequent requests.

If you do not receive a Set-Cookie header in response to the auth/login POST request but login succeeded, you can use the standard Authorization:Splunk... header with the session key for authorization.

See also

- Authentication
- authentication/current-context
POST

Get a session ID for use in subsequent API calls that require authentication. Optionally, use cookie-based authentication or multifactor authentication.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cookie</td>
<td>Boolean</td>
<td>To use cookie-based REST auth, pass in cookie=1. Cookies will only be returned if the cookie parameter is passed in with the value of 1.</td>
</tr>
<tr>
<td>password</td>
<td>String</td>
<td>Required. Current username password.</td>
</tr>
<tr>
<td>passcode</td>
<td>String</td>
<td>Required for users with RSA multifactor authentication. The passcode associated with RSA multifactor authentication. This is a combination of the user's RSA token and PIN.</td>
</tr>
<tr>
<td>username</td>
<td>String</td>
<td>Required. Authenticated session owner name.</td>
</tr>
</tbody>
</table>

Response data keys

Note: Only a <response> element is returned instead of a full <atom> feed.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sessionKey</td>
<td>Session ID.</td>
</tr>
</tbody>
</table>

A Set-Cookie HTTP header is returned if cookie-based authentication is requested.

Failure to authenticate returns the following response.

```xml
<response>
  <messages>
    <msg type="WARN">Login failed</msg>
  </messages>
</response>
```

Example request and response

**XML Request**

```bash
curl -k -u admin:changeme https://localhost:8089/services/auth/login -d username=admin -d password=changeme
```

**XML Response**

```xml
<response>
  <sessionKey>192fd3e46a31246da7ea7f109e7f95fd</sessionKey>
</response>
```

Example request and response using RSA passcode

**XML Request**

```bash
curl -k https://tsen-centos62x64-7:8089/services/auth/login -d username= john@test-splunk.com -d
```
password=changed123 -d passcode='gq!k##9b'

XML Response

<response>
  <sessionKey>8Q1QczpArNgKqfUmkmhwgiZVER4^phZzEbX9NGon0^EdW8DKXHR9iXNStzAEpVteSkShTxS^8QcyZ8zYj4P812lRBskRurK_RZ2dEy7FZjYoalGw0wx2rkSS0sIC</sessionKey>
</response>

Example failed login with missing RSA passcode

XML Request

curl -k https://tsen-centos62x64-7:8089/services/auth/login -d username=john@test-splunk.com -d password='changed123:gq!k##9b'

XML Response

<response>
  <messages>
    <msg type="WARN" code="incorrect_username_or_password">Login failed</msg>
  </messages>
</response>

authentication/current-context

https://<host>:<mPort>/services/authentication/current-context

Get the authenticated session owner username.

For additional information, see the following resources.

• auth/login
• List of available capabilities in Securing Splunk Enterprise.

GET

Get user information for the current context.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>List of capabilities assigned to role.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>defaultApp</td>
<td>Default app for the user, which is invoked at login.</td>
</tr>
<tr>
<td>defaultAppIsUserOverride</td>
<td>Default app override indicates: true = Default app overrides the user role default app. false = Default app does not override the user role default app.</td>
</tr>
<tr>
<td>defaultAppSourceRole</td>
<td>The role that determines the default app for the user, if the user has multiple roles.</td>
</tr>
<tr>
<td>email</td>
<td>User email address.</td>
</tr>
<tr>
<td>password</td>
<td>User password.</td>
</tr>
<tr>
<td>realname</td>
<td>User full name.</td>
</tr>
<tr>
<td>restart_background_jobs</td>
<td>Restart background search job that has not completed when Splunk restarts indication: true = Restart job. false = Do not restart job.</td>
</tr>
<tr>
<td>roles</td>
<td>Roles assigned to the user.</td>
</tr>
<tr>
<td>type</td>
<td>User authentication system type:</td>
</tr>
<tr>
<td></td>
<td>• LDAP</td>
</tr>
<tr>
<td></td>
<td>• Scripted</td>
</tr>
<tr>
<td></td>
<td>• Splunk</td>
</tr>
<tr>
<td></td>
<td>• System (reserved for system user)</td>
</tr>
<tr>
<td>tz</td>
<td>User timezone.</td>
</tr>
<tr>
<td>username</td>
<td>Authenticated session owner name.</td>
</tr>
</tbody>
</table>

Usage in search
Here is an example of calling this endpoint in a search command to get the current user.

```plaintext
... rest /services/authentication/current-context/context | fields + username ...
```

Example request and response

XML Request

```bash
curl -k -u admin:changeme https://localhost:8089/services/authentication/current-context
```

XML Response

```xml
<result>
<title>current-context</title>
<id>https://localhost:8089/services/authentication/current-context</id>
<updated>2014-06-30T11:26:19-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
```

121
<s:dict>
  <s:key name="capabilities">
    <s:list>
      <s:item>accelerate_datamodel</s:item>
      <s:item>accelerate_search</s:item>
      <s:item>admin_all_objects</s:item>
      <s:item>change_authentication</s:item>
      <s:item>change_own_password</s:item>
      <s:item>edit_deployment_client</s:item>
      <s:item>edit_deployment_server</s:item>
      <s:item>edit_dist_peer</s:item>
      <s:item>edit_forwarders</s:item>
      <s:item>edit_httpauths</s:item>
      <s:item>edit_input_defaults</s:item>
      <s:item>edit_monitor</s:item>
      <s:item>edit_roles</s:item>
      <s:item>edit_scripted</s:item>
      <s:item>edit_search_server</s:item>
      <s:item>edit_server</s:item>
      <s:item>edit_splunktcp</s:item>
      <s:item>edit_splunktcp_ssl</s:item>
      <s:item>edit_tcp</s:item>
      <s:item>edit_udp</s:item>
      <s:item>edit_user</s:item>
      <s:item>edit_view_html</s:item>
      <s:item>edit_web_settings</s:item>
      <s:item>edit_win_admon</s:item>
      <s:item>edit_win_eventlogs</s:item>
      <s:item>edit_win_perfmon</s:item>
      <s:item>edit_win_regmon</s:item>
      <s:item>edit_win_wmiconf</s:item>
      <s:item>embed_report</s:item>
      <s:item>get_diag</s:item>
      <s:item>get_metadata</s:item>
      <s:item>get_typeahead</s:item>
      <s:item>indexes_edit</s:item>
      <s:item>input_file</s:item>
      <s:item>license_edit</s:item>
      <s:item>license_tab</s:item>
      <s:item>list_deployment_client</s:item>
      <s:item>list_deployment_server</s:item>
      <s:item>list_forwarders</s:item>
      <s:item>list_httpauths</s:item>
      <s:item>list_inputs</s:item>
      <s:item>list_pdfserver</s:item>
      <s:item>list_win_localavailablelogs</s:item>
      <s:item>output_file</s:item>
      <s:item>request_remote_tok</s:item>
      <s:item>rest_apps_management</s:item>
      <s:item>rest_apps_view</s:item>
    </s:list>
  </s:key>
</s:dict>
authentication/httpauth-tokens

https://<host>:<mPort>/services/authentication/httpauth-tokens

List currently active session IDs and users.
For additional information, see the following resources.

- auth/login
- authentication/current-context

**GET**

List currently active session IDs/users.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Response keys**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authString</td>
<td>Unique identifier for this session.</td>
</tr>
<tr>
<td>searchId</td>
<td>Search ID associated with the session. If it was created for a search job. If it is a login-type session, the value is empty. The session ID token is valid for the duration of the web session.</td>
</tr>
<tr>
<td>timeAccessed</td>
<td>Last time the session was touched.</td>
</tr>
<tr>
<td>userName</td>
<td>Username associated with the session.</td>
</tr>
</tbody>
</table>

**Usage in searches**

Here is an example of calling this endpoint in a search.

```
| rest /services/authentication/httpauth-tokens | search (NOT userName="splunk-system-user") searchId="" | table userName splunk_server timeAccessed
```

**Example request and response**

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/httpauth-tokens
```

**XML Response**

```
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
```
authentication/httpauth-tokens/{name}

https://<host>:<mPort>/services/authentication/httpauth-tokens/<name>

Access or delete the {name} session, where {name} is the session ID returned by auth/login.

For additional information, see the following resources.

- auth/login
- authentication/current-context

DELETE

Delete the session associated with this session ID.

Request parameters
None

Response keys
None
Example request and response

XML Request

curl -k -u admin:changeme --request DELETE https://localhost:8089/services/authentication/httpauth-tokens/vdZv2e8F0842dyJhrEI8GNTcBMPeGwGPyxtGLKAEESQkzjSjG7dymQW58y"oI3kxXYWfK_Fd3cRGqwPQGp58RvEkwzCaC6PmQgCsK

XML Response

<title>httpauth-tokens</title>

<id>https://localhost:8089/services/authentication/httpauth-tokens</id>

<updated>2014-06-30T12:02:12-07:00</updated>

<generator build="200839" version="6.1"/>

<author>
  <name>Splunk</name>
</author>

<opensearch:totalResults>1</opensearch:totalResults>

<opensearch:itemsPerPage>30</opensearch:itemsPerPage>

<opensearch:startIndex>0</opensearch:startIndex>

<s:messages/>

<entry>
  <title>694ef5bda40ae8c4f59626671b5f0c9a</title>
  <id>https://localhost:8089/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a</id>
  <updated>2014-06-30T12:02:12-07:00</updated>
  <link href="/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a" rel="list"/>
  <link href="/services/authentication/httpauth-tokens/694ef5bda40ae8c4f59626671b5f0c9a" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="authString">1RU5vGFm2OPq29plLtvqlEB9xzPDLZ3AeUhe1bwPjIrKtvyLE4fODHs"Tg14_NamvVtqusj8emuNfx5Sw81W"q8Xn1DoV7LoCvErpyTzOv1Sr"2TnKUC</s:key>
      <s:dict>
        <s:key name="app"></s:key>
        <s:dict>
          <s:key name="can_list">1</s:key>
          <s:dict>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
                <s:dict>
                  <s:dict>
                    <s:dict>
                      <s:dict>
                        <s:dict>
                          <s:dict>
                            <s:dict>
                              <s:dict>
                                <s:dict>
                                  <s:dict>
                                    <s:dict>
                                      <s:dict>
                                        <s:dict>
                                          <s:dict>
                                            <s:dict>
                                              <s:dict>
                                                <s:dict>
                                                  <s:dict>
                                                    <s:dict>
                                                      <s:dict>
                                                        <s:dict>
                                                          <s:dict>
                                                            <s:dict>
                                                              <s:dict>
                                                                <s:dict>
                                                                  <s:dict>
                                                                    <s:dict>
                                                                      <s:dict>
                                                                        <s:dict>
                                                                          <s:dict>
                                                                            <s:dict>
                                                                              <s:dict>
                                                                                <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <s:dict>
                                                                                                  <s:dict>
                                                                                                 <s:dict>
                                                                                               <s:dict>
                                                                                             <s:dict>
                                                                                           <s:dict>
                                                                                         <s:dict>
                                                                                       <s:dict>
                                                                                     <s:dict>
                                                                                   <s:dict>
                                                                                  <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                   <a:dict>
GET

Get session information.

Request parameters
None

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>authString</td>
<td>Unique session identifier.</td>
</tr>
<tr>
<td>searchId</td>
<td>Session search ID, if it is a search job session. The value is blank for a login-type session.</td>
</tr>
<tr>
<td>timeAccessed</td>
<td>Last time the session was touched.</td>
</tr>
<tr>
<td>userName</td>
<td>Username associated with the session.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authentication/httpauth-tokens
```

XML Response

```
<title>httpauth-tokens</title>
<id>https://localhost:8089/services/authentication/httpauth-tokens</id>
<updated>2014-06-30T11:39:52-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>15a773187d3e4437cbe9809f41f23d8f</title>
  <id>https://localhost:8089/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f</id>
```
<updated>2014-06-30T11:39:52-07:00</updated>
<link href="/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f" rel="list"/>
<link href="/services/authentication/httpauth-tokens/15a773187d3e4437cbe9809f41f23d8f" rel="remove"/>
<content type="text/xml">
  <s:dict>
    <s:key name="authString">vdZv2eB9F0842dyJhrIEiGNtCBMBeGuwGPYxtGLKAESQkzjSjG7dbymQW58y"oI3kkYXWfK
_Fd3cRGqwPQspS8RvEKzwCaC6PqqCsK</s:key>
    <s:dict>
      <s:key name="app"></s:key>
      <s:dict>
        <s:key name="can_list">1</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">0</s:key>
        <s:key name="owner">system</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="removable">0</s:key>
        <s:key name="sharing">system</s:key>
      </s:dict>
    </s:dict>
    <s:dict>
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields"></s:key>
          <s:dict>
            <s:key name="requiredFields"></s:dict>
          </s:dict>
          <s:key name="wildcardFields"></s:dict>
        </s:dict>
      </s:key>
    </s:dict>
    <s:dict>
      <s:key name="searchId"></s:dict>
      <s:dict>
        <s:dict>
          <s:key name="userName">admin</s:dict>
        </s:dict>
      </s:dict>
    </s:dict>
  </s:dict>
</content>
authentication/users

https://<host>:<mPort>/services/authentication/users

List current users and create new users.

For additional information about configuring users and roles, see the following resources in Securing Splunk Enterprise.

- About configuring role-based user access
- Securing Splunk Enterprise
- List of available capabilities

Authentication and authorization
Requires the edit_user capability.

GET

List current users.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>List of capabilities assigned to role.</td>
</tr>
<tr>
<td>defaultApp</td>
<td>Default app for the user, which is invoked at login.</td>
</tr>
</tbody>
</table>
| defaultAppIsUserOverride | Default app override indicates:  
|                       | true = Default app overrides the user role default app.  
|                       | false = Default app does not override the user role default app.             |
| defaultAppSourceRole  | The role that determines the default app for the user, if the user has multiple roles. |
| email                 | User email address.                                                         |
| password              | User password.                                                              |
| realName              | User full name.                                                             |
| restart_background_jobs | Restart background search job that has not completed when Splunk restarts indication:  
|                       | true = Restart job.                                                        |
|                       | false = Do not restart job.                                                 |
| roles                 | Roles assigned to the user.                                                 |
| type                  | One of the following user authentication system types.                       |
|                       | • LDAP                                                                       |
|                       | • Scripted                                                                  |
|                       | • Splunk                                                                    |
|                       | • System (reserved for system user)                                         |
| tz                    | User timezone.                                                              |
Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/authentication/users

XML Response

<title>users</title>
{id>https://localhost:8089/services/authentication/users</id>
<updated>2014-06-30T12:27:48-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authentication/users/_new" rel="create"/>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>admin</title>
  <id>https://localhost:8089/services/authentication/users/admin</id>
  <updated>2014-06-30T12:27:48-07:00</updated>
  <link href="/services/authentication/users/admin" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/users/admin" rel="list"/>
  <link href="/services/authentication/users/admin" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list>
          <s:item>accelerate_datamodel</s:item>
          <s:item>accelerate_search</s:item>
          <s:item>admin_all_objects</s:item>
          <s:item>change_authentication</s:item>
          <s:item>change_own_password</s:item>
          <s:item>edit_deployment_client</s:item>
          <s:item>edit_deployment_server</s:item>
          <s:item>edit_dist_peer</s:item>
          <s:item>edit_forwarders</s:item>
          <s:item>edit_httpauths</s:item>
          <s:item>edit_input_defaults</s:item>
          <s:item>edit_monitor</s:item>
          <s:item>edit_roles</s:item>
          <s:item>edit_scripted</s:item>
          <s:item>edit_search_server</s:item>
          <s:item>edit_server</s:item>
          <s:item>edit_splunktcp</s:item>
          <s:item>edit_splunktcp_ssl</s:item>
          <s:item>edit_ssl</s:item>
          <s:item>edit_tcp</s:item>
          <s:item>edit_udp</s:item>
          <s:item>edit_user</s:item>
          <s:item>edit_view_html</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
<s:dict>
  <s:key name="email">changeme@example.com</s:key>
  <s:key name="password">********</s:key>
  <s:key name="realname">Administrator</s:key>
  <s:key name="restart_background_jobs">1</s:key>
  <s:key name="roles">
    <s:list>
      <s:item>admin</s:item>
    </s:list>
  </s:key>
  <s:key name="type">Splunk</s:key>
  <s:key name="tz"></s:key>
</s:dict>

<entry>
  <title>user1</title>
  <id>https://localhost:8089/services/authentication/users/user1</id>
  <updated>2014-06-30T12:27:48-07:00</updated>
  <link href="/services/authentication/users/user1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/users/user1" rel="list"/>
  <link href="/services/authentication/users/user1" rel="edit"/>
  <link href="/services/authentication/users/user1" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list>
          <s:item>accelerate_datamodel</s:item>
          <s:item>accelerate_search</s:item>
          <s:item>admin_all_objects</s:item>
          <s:item>change_authentication</s:item>
          <s:item>change_own_password</s:item>
          <s:item>edit_deployment_client</s:item>
          <s:item>edit_deployment_server</s:item>
          <s:item>edit_dist_peer</s:item>
          <s:item>edit_forwarders</s:item>
          <s:item>edit_httpauths</s:item>
          <s:item>edit_input_defaults</s:item>
          <s:item>edit_monitor</s:item>
          <s:item>edit_roles</s:item>
          <s:item>edit_search_server</s:item>
          <s:item>edit_server</s:item>
          <s:item>edit_splunktcp</s:item>
          <s:item>edit_splunktcp_ssl</s:item>
          <s:item>edit_tcp</s:item>
          <s:item>edit_udp</s:item>
          <s:item>edit_user</s:item>
          <s:item>edit_view_html</s:item>
          <s:item>edit_web_settings</s:item>
          <s:item>edit_win_admon</s:item>
          <s:item>edit_win_eventlogs</s:item>
          <s:item>edit_win_perfmon</s:item>
          <s:item>edit_win_regmon</s:item>
          <s:item>edit_win_wmiconf</s:item>
          <s:item>embed_report</s:item>
          <s:item>get_diag</s:item>
          <s:item>get_metadata</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
<s:item>get_typeahead</s:item>
<s:item>indexes_edit</s:item>
<s:item>input_file</s:item>
<s:item>license_edit</s:item>
<s:item>license_tab</s:item>
<s:item>list_deployment_client</s:item>
<s:item>list_deployment_server</s:item>
<s:item>list_forwarders</s:item>
<s:item>list_httpauths</s:item>
<s:item>list_inputs</s:item>
<s:item>list_pdfserver</s:item>
<s:item>list_win_localavailablelogs</s:item>
<s:item>output_file</s:item>
<s:item>request_remote_tok</s:item>
<s:item>rest_apps_management</s:item>
<s:item>rest_apps_view</s:item>
<s:item>rest_properties_get</s:item>
<s:item>rest_properties_set</s:item>
<s:item>restart_splunkd</s:item>
<s:item>rtsearch</s:item>
<s:item>run_debug_commands</s:item>
<s:item>schedule_rtsearch</s:item>
<s:item>schedule_search</s:item>
<s:item>search</s:item>
<s:item>write_pdfserver</s:item>
</s:list>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">0</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:dict name="perms">
<s:dict name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:dict name="write">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
</s:dict>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
<s:key name="email"></s:key>
<s:key name="password">********</s:key>
<s:key name="realname"></s:key>
<s:key name="restart_background_jobs">1</s:key>
<s:key name="roles">
<s:list>
<s:item>admin</s:item>
</s:list>
</s:key>
POST
Create a user.

Usage details
When creating a user you must specify at least one role.

Specify one or more roles for the user. You can create a new role for the user by setting the `createrole` parameter to "true" and specify the new role name as a `roles` parameter value.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>createrole</code></td>
<td>Boolean</td>
<td>Flag to indicate that a new role should be created for the user. If set to &quot;true&quot;, the new role &lt;name&gt; is created and assigned to the user. The &lt;name&gt; portion of the new role matches the name parameter value passed in with this POST request. If set to &quot;false&quot;, at least one existing role must be specified using the <code>roles</code> parameter for the POST request. Defaults to &quot;false&quot;.</td>
</tr>
<tr>
<td><code>defaultApp</code></td>
<td>String</td>
<td>User default app.Overrides the default app inherited from the user roles.</td>
</tr>
<tr>
<td><code>email</code></td>
<td>String</td>
<td>User email address.</td>
</tr>
<tr>
<td><code>force-change-pass</code></td>
<td>Boolean</td>
<td>Force user to change password indication: true = Force password change. false = Do not force password change.</td>
</tr>
<tr>
<td><code>name</code></td>
<td>String</td>
<td>Required. Unique user login name.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>String</td>
<td>User login password.</td>
</tr>
<tr>
<td><code>realname</code></td>
<td>String</td>
<td>Full user name.</td>
</tr>
<tr>
<td><code>restart_background_jobs</code></td>
<td>Boolean</td>
<td>Restart background search job that has not completed when Splunk restarts indication: true = Restart job. false = Do not restart job.</td>
</tr>
<tr>
<td><code>roles</code></td>
<td>String</td>
<td>Role to assign to this user. To assign multiple roles, pass in each role using a separate roles parameter value. For example, <code>-d roles=&quot;role1&quot;, -d roles=&quot;role2&quot;</code>. At least one existing role is required if you are not using the <code>createrole</code> parameter to create a new role for the user. If you are using <code>createrole</code> to create a new role, you can optionally use this parameter to specify additional roles to assign to the user.</td>
</tr>
<tr>
<td><code>tz</code></td>
<td>String</td>
<td>User timezone.</td>
</tr>
</tbody>
</table>

Response keys
None
Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/authentication/users -d name=User1 -d password=changeme -d roles=admin

XML Response

<title>users</title>
{id>https://localhost:8089/services/authentication/users</id>
<updated>2014-06-30T12:18:19-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authentication/users/_new" rel="create"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>user1</title>
  <id>https://localhost:8089/services/authentication/users/user1</id>
  <updated>2014-06-30T12:18:19-07:00</updated>
  <link href="/services/authentication/users/user1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/users/user1" rel="list"/>
  <link href="/services/authentication/users/user1" rel="edit"/>
  <link href="/services/authentication/users/user1" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list>
          <s:item>accelerate_datamodel</s:item>
          <s:item>accelerate_search</s:item>
          <s:item>admin_all_objects</s:item>
          <s:item>change_authentication</s:item>
          <s:item>change_own_password</s:item>
          <s:item>edit_deployment_client</s:item>
          <s:item>edit_deployment_server</s:item>
          <s:item>edit_dist_peer</s:item>
          <s:item>edit_forwarders</s:item>
          <s:item>edit_httpauths</s:item>
          <s:item>edit_input_defaults</s:item>
          <s:item>edit_monitor</s:item>
          <s:item>edit_roles</s:item>
          <s:item>edit_scripted</s:item>
          <s:item>edit_search_server</s:item>
          <s:item>edit_server</s:item>
          <s:item>editSplunkTCP</s:item>
          <s:item>editSplunkTCP_ssl</s:item>
          <s:item>edit_tcp</s:item>
          <s:item>edit_udp</s:item>
          <s:item>edit_user</s:item>
          <s:item>edit_view_html</s:item>
          <s:item>edit_web_settings</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
<s:item>edit_win_admon</s:item>
<s:item>edit_win_eventlogs</s:item>
<s:item>edit_win_perfmon</s:item>
<s:item>edit_win_regmon</s:item>
<s:item>edit_win_wmiconf</s:item>
<s:item>embed_report</s:item>
<s:item>get_diag</s:item>
<s:item>get_metadata</s:item>
<s:item>get_typeahead</s:item>
<s:item>indexes_edit</s:item>
<s:item>input_file</s:item>
<s:item>license_edit</s:item>
<s:item>license_tab</s:item>
<s:item>list_deployment_client</s:item>
<s:item>list_deployment_server</s:item>
<s:item>list_forwarders</s:item>
<s:item>list_httpauths</s:item>
<s:item>list_inputs</s:item>
<s:item>list_pdfserver</s:item>
<s:item>list_win_localavailablelogs</s:item>
<s:item>output_file</s:item>
<s:item>request_remote_tok</s:item>
<s:item>rest_apps_management</s:item>
<s:item>rest_apps_view</s:item>
<s:item>rest_properties_get</s:item>
<s:item>rest_properties_set</s:item>
<s:item>restart_splunkd</s:item>
<s:item>rtsearch</s:item>
<s:item>run_debug_commands</s:item>
<s:item>schedule_rtsearch</s:item>
<s:item>schedule_search</s:item>
<s:item>search</s:item>
<s:item>write_pdfserver</s:item>
</s:list>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">0</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:dict>
<s:key name="read">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
</s:dict>
</s:key>
<s:dict>
<s:key name="removable">0</s:key>

authentication/users/{name}

https://<host>:<mPort>/services/authentication/users/{name}
Access and update user information or delete the {name} user.

**Usage details**
The `{name}` username portion of the URL is not case sensitive.

For additional information about user capabilities, see the following resource in *Securing Splunk Enterprise*.

- List of available capabilities

**Authentication and authorization**
Requires the `edit_user` capability.

**DELETE**
Remove the specified user from the system.

**Request parameters**
None

**Response keys**
None

**Example request and response**

**XML Request**

curl -k -u admin:changeme --request DELETE https://localhost:8089/services/authentication/users/user1

**XML Response**
<title>users</title>

/id>https://localhost:8089/services/authentication/users</id>
<updated>2014-06-30T12:51:09-07:00</updated>
<generator build="200839" version="6.1"/>

<author>
  <name>Splunk</name>
</author>

<link href="/services/authentication/users/_new" rel="create"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

<entry>
  <title>admin</title>
  <id>https://localhost:8089/services/authentication/users/admin</id>
  <updated>2014-06-30T12:51:09-07:00</updated>
  <link href="/services/authentication/users/admin" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/users/admin" rel="list"/>
  <link href="/services/authentication/users/admin" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list>
          <s:item>accelerate_datamodel</s:item>
          <s:item>accelerate_search</s:item>
          <s:item>admin_all_objects</s:item>
          <s:item>change_authentication</s:item>
          <s:item>change_own_password</s:item>
          <s:item>edit_deployment_client</s:item>
          <s:item>edit_deployment_server</s:item>
          <s:item>edit_dist_peer</s:item>
          <s:item>edit_forwarders</s:item>
          <s:item>edit_httpauths</s:item>
          <s:item>edit_input_defaults</s:item>
          <s:item>edit_monitor</s:item>
          <s:item>edit_roles</s:item>
          <s:item>edit_scripted</s:item>
          <s:item>edit_search_server</s:item>
          <s:item>edit_server</s:item>
          <s:item>editSplunkTcp</s:item>
          <s:item>editSplunkTcp_ssl</s:item>
          <s:item>edit_tcp</s:item>
          <s:item>edit_udp</s:item>
          <s:item>edit_user</s:item>
          <s:item>edit_view_html</s:item>
          <s:item>edit_web_settings</s:item>
          <s:item>edit_win_admon</s:item>
          <s:item>edit_win_eventlogs</s:item>
          <s:item>edit_win_perfmon</s:item>
          <s:item>edit_win_regmon</s:item>
          <s:item>edit_win_wmiconf</s:item>
          <s:item>embed_report</s:item>
          <s:item>get_diag</s:item>
          <s:item>get_metadata</s:item>
          <s:item>get_typeahead</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>
GET

Return information for the specified user.

Request parameters
None

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>List of capabilities assigned to role.</td>
</tr>
<tr>
<td>defaultApp</td>
<td>Default app for the user, which is invoked at login.</td>
</tr>
<tr>
<td>defaultAppIsUserOverride</td>
<td>Default app override indicator.</td>
</tr>
<tr>
<td></td>
<td>true = Default app overrides the user role default app.</td>
</tr>
<tr>
<td></td>
<td>false = Default app does not override the user role default app.</td>
</tr>
<tr>
<td>defaultAppSourceRole</td>
<td>Role that determines the default app for the user, if the user has multiple roles.</td>
</tr>
<tr>
<td>email</td>
<td>User email address</td>
</tr>
<tr>
<td>password</td>
<td>User password</td>
</tr>
<tr>
<td>realname</td>
<td>User full name</td>
</tr>
<tr>
<td>restart_background_jobs</td>
<td>Indicates whether incomplete background search jobs restart when the Splunk deployment restarts.</td>
</tr>
<tr>
<td></td>
<td>true = Restart jobs.</td>
</tr>
<tr>
<td></td>
<td>false = Do not restart jobs.</td>
</tr>
<tr>
<td>roles</td>
<td>Roles assigned to the user.</td>
</tr>
<tr>
<td>type</td>
<td>One of the following user authentication system types.</td>
</tr>
<tr>
<td></td>
<td>• LDAP</td>
</tr>
<tr>
<td></td>
<td>• Scripted</td>
</tr>
<tr>
<td></td>
<td>• Splunk</td>
</tr>
<tr>
<td></td>
<td>• System (reserved for system user)</td>
</tr>
<tr>
<td>tz</td>
<td>User timezone</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/authentication/users/user1

XML Response
<title>users</title>

:id=https://localhost:8089/services/authentication/users</id>

<updated>2014-06-30T12:39:18-07:00</updated>

<generator build="200839" version="6.1"/>

<author>
  <name>Splunk</name>
</author>

<link href="/services/authentication/users/_new" rel="create"/>

<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>

<s:messages/>

<entry>
  <title>user1</title>
  <id>https://localhost:8089/services/authentication/users/user1</id>
  <updated>2014-06-30T12:39:18-07:00</updated>
  <link href="/services/authentication/users/user1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/users/user1" rel="list"/>
  <link href="/services/authentication/users/user1" rel="edit"/>
  <link href="/services/authentication/users/user1" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list>
          <s:item>accelerate_datamodel</s:item>
          <s:item>accelerate_search</s:item>
          <s:item>admin_all_objects</s:item>
          <s:item>change_authentication</s:item>
          <s:item>change_own_password</s:item>
          <s:item>edit_deployment_client</s:item>
          <s:item>edit_deployment_server</s:item>
          <s:item>edit_dist_peer</s:item>
          <s:item>edit_forwarders</s:item>
          <s:item>edit_httpauths</s:item>
          <s:item>edit_input_defaults</s:item>
          <s:item>edit_monitor</s:item>
          <s:item>edit_roles</s:item>
          <s:item>edit_scripted</s:item>
          <s:item>edit_search_server</s:item>
          <s:item>edit_search_server</s:item>
          <s:item>edit_server</s:item>
          <s:item>edit_splunktcp</s:item>
          <s:item>edit_splunktcp_ssl</s:item>
          <s:item>edit Tcp</s:item>
          <s:item>edit_udp</s:item>
          <s:item>edit_user</s:item>
          <s:item>edit_view_html</s:item>
          <s:item>edit_web_settings</s:item>
          <s:item>edit_win_admon</s:item>
          <s:item>edit_win_eventlogs</s:item>
          <s:item>edit_win_perfmon</s:item>
          <s:item>edit_win_regmon</s:item>
          <s:item>edit_win_wmiconf</s:item>
          <s:item>embed_report</s:item>
          <s:item>get_diag</s:item>
          <s:item>get_metadata</s:item>
        </s:list>
      </s:dict>
    </s:dict>
  </content>
</entry>
<s:item>get_typeahead</s:item>
<s:item>indexes_edit</s:item>
<s:item>input_file</s:item>
<s:item>license_edit</s:item>
<s:item>license_tab</s:item>
<s:item>list_deployment_client</s:item>
<s:item>list_deployment_server</s:item>
<s:item>list_forwarders</s:item>
<s:item>list_httpauths</s:item>
<s:item>list_inputs</s:item>
<s:item>list_pdfserver</s:item>
<s:item>list_win_localavailablelogs</s:item>
<s:item>output_file</s:item>
<s:item>request_remote_tok</s:item>
<s:item>rest_apps_management</s:item>
<s:item>rest_apps_view</s:item>
<s:item>rest_properties_get</s:item>
<s:item>rest_properties_set</s:item>
<s:item>restart_splunkd</s:item>
<s:item>rtsearch</s:item>
<s:item>run_debug_commands</s:item>
<s:item>schedule_rtsearch</s:item>
<s:item>schedule_search</s:item>
<s:item>search</s:item>
<s:item>write_pdfserver</s:item>

</s:list>
</s:key>
</s:key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppsUserOverride">0</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app">system</s:key>
    <s:dict>
      <s:dict name="can_list">1</s:dict>
      <s:dict name="can_write">1</s:dict>
      <s:dict name="modifiable">0</s:dict>
      <s:dict name="owner">system</s:dict>
      <s:dict name="perms">
        <s:dict name="read">
          <s:list＠＊</s:list>
        </s:dict>
        <s:dict name="write">
          <s:list＠＊</s:list>
        </s:dict>
      </s:dict>
      <s:dict name="removable">0</s:dict>
      <s:dict name="sharing">system</s:dict>
    </s:dict>
  </s:dict>
  <s:dict name="eai:attributes">
    <s:dict name="optionalFields">
      <s:list>
        <s:item>defaultApp</s:item>
        <s:item>email</s:item>
        <s:item>force-change-pass</s:item>
      </s:list>
    </s:dict>
  </s:dict>
</s:key>
POST

Update the specified user.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>defaultApp</td>
<td>String</td>
<td>User default app. This overrides the default app inherited from the user roles.</td>
</tr>
<tr>
<td>email</td>
<td>String</td>
<td>User email address.</td>
</tr>
<tr>
<td>force-change-pass</td>
<td>Boolean</td>
<td>Indicates whether to force user password change.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true = Force password change.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false = Do not force password change.</td>
</tr>
<tr>
<td>oldpassword</td>
<td>String</td>
<td>Old user login password. Only <strong>required</strong> if using the <strong>password</strong> parameter to change the current user's password.</td>
</tr>
<tr>
<td>password</td>
<td>String</td>
<td><strong>Required.</strong> User login password. To change the user password, enter the new user login password here. To change the current user's password, also supply the old password in the <strong>oldpassword</strong> parameter.</td>
</tr>
<tr>
<td>realname</td>
<td>String</td>
<td>Full user name.</td>
</tr>
<tr>
<td>restart_background_jobs</td>
<td>Boolean</td>
<td>Indicates whether to restart background search job that has not completed when the Splunk deployment restarts.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true = Restart job.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false = Do not restart job.</td>
</tr>
<tr>
<td>roles</td>
<td>String</td>
<td>Role to assign to this user. To assign multiple roles, pass in each role using a separate <strong>roles</strong> parameter value.</td>
</tr>
</tbody>
</table>
For example, `-d roles="role1", -d roles="role2"`. At least one existing role is required if you are not using the `createrole` parameter to create a new role for the user. If you are using `createrole` to create a new role, you can optionally use this parameter to specify additional roles to assign to the user.

**Response keys**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>List of capabilities assigned to role.</td>
</tr>
<tr>
<td>defaultApp</td>
<td>Default app for the user, which is invoked at login.</td>
</tr>
<tr>
<td>defaultAppIsUserOverride</td>
<td>Default app override indicator.</td>
</tr>
<tr>
<td>true</td>
<td>Default app overrides the user role default app.</td>
</tr>
<tr>
<td>false</td>
<td>Default app does not override the user role default app.</td>
</tr>
<tr>
<td>defaultAppSourceRole</td>
<td>Role that determines the default app for the user, if the user has multiple roles.</td>
</tr>
<tr>
<td>email</td>
<td>User email address.</td>
</tr>
<tr>
<td>password</td>
<td>User password.</td>
</tr>
<tr>
<td>realtime</td>
<td>User full name.</td>
</tr>
<tr>
<td>restart_background_jobs</td>
<td>Indicates whether to restart background search job that has not completed when the Splunk deployment restarts.</td>
</tr>
<tr>
<td>true</td>
<td>Restart job.</td>
</tr>
<tr>
<td>false</td>
<td>Do not restart job.</td>
</tr>
<tr>
<td>roles</td>
<td>Roles assigned to the user.</td>
</tr>
<tr>
<td>type</td>
<td>One of the following user authentication system types.</td>
</tr>
<tr>
<td>LDAP</td>
<td></td>
</tr>
<tr>
<td>Scripted</td>
<td></td>
</tr>
<tr>
<td>Splunk</td>
<td></td>
</tr>
<tr>
<td>System (reserved for system user)</td>
<td></td>
</tr>
<tr>
<td>tz</td>
<td>User timezone.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:changeme https://localhost:8089/services/authentication/users/user1 -d defaultApp=launcher
```

**XML Response**

```xml
<title>users</title>

<id>https://localhost:8089/services/authentication/users</id>
<updated>2014-06-30T12:45:23-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
```
<name>Splunk</name>
</author>
<link href="/services/authentication/users/_new" rel="create"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>user1</title>
  <id>https://localhost:8089/services/authentication/users/user1</id>
  <updated>2014-06-30T12:45:23-07:00</updated>
  <link href="/services/authentication/users/user1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authentication/users/user1" rel="list"/>
  <link href="/services/authentication/users/user1" rel="edit"/>
  <link href="/services/authentication/users/user1" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:dict>
        <s:list>
          <s:item>accelerate_datamodel</s:item>
          <s:item>accelerate_search</s:item>
          <s:item>admin_all_objects</s:item>
          <s:item>change_authentication</s:item>
          <s:item>change_own_password</s:item>
          <s:item>edit_deployment_client</s:item>
          <s:item>edit_deployment_server</s:item>
          <s:item>edit_dist_peer</s:item>
          <s:item>edit_forwarders</s:item>
          <s:item>edit_httpauths</s:item>
          <s:item>edit_input_defaults</s:item>
          <s:item>edit_monitor</s:item>
          <s:item>edit_roles</s:item>
          <s:item>edit_scripted</s:item>
          <s:item>edit_search_server</s:item>
          <s:item>edit_server</s:item>
          <s:item>edit_splunktcp</s:item>
          <s:item>edit_splunktcp_ssl</s:item>
          <s:item>edit_tcp</s:item>
          <s:item>edit_udp</s:item>
          <s:item>edit_user</s:item>
          <s:item>edit_view_html</s:item>
          <s:item>edit_web_settings</s:item>
          <s:item>edit_win_admon</s:item>
          <s:item>edit_win_eventlogs</s:item>
          <s:item>edit_win_perfmon</s:item>
          <s:item>edit_win_regmon</s:item>
          <s:item>edit_win_wmiconf</s:item>
          <s:item>embed_report</s:item>
          <s:item>get_diag</s:item>
          <s:item>get_metadata</s:item>
          <s:item>get_typeahead</s:item>
          <s:item>indexes_edit</s:item>
          <s:item>input_file</s:item>
          <s:item>license_edit</s:item>
          <s:item>license_tab</s:item>
          <s:item>list_deployment_client</s:item>
          <s:item>list_deployment_server</s:item>
          <s:item>list_forwarders</s:item>
          <s:item>list_httpauths</s:item>
        </s:list>
      </s:dict>
    </s:dict>
  </content>
</entry>
<s:item>list_inputs</s:item>
<s:item>list_pdfserver</s:item>
<s:item>list_win_localavailablelogs</s:item>
<s:item>output_file</s:item>
<s:item>request_remote_tok</s:item>
<s:item>rest_apps_management</s:item>
<s:item>rest_appsview</s:item>
<s:item>rest_properties_get</s:item>
<s:item>rest_properties_set</s:item>
<s:item>restart_splunkd</s:item>
<s:item>rtsearch</s:item>
<s:item>run_debug_commands</s:item>
<s:item>schedule_rtsearch</s:item>
<s:item>schedule_search</s:item>
<s:item>search</s:item>
<s:item>write_pdfserver</s:item>
</list>
</key>
<s:key name="defaultApp">launcher</s:key>
<s:key name="defaultAppIsUserOverride">1</s:key>
<s:key name="defaultAppSourceRole">system</s:key>
<s:key name="ema:acl">
  <s:dict>
    <s:key name="app">system</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>*</s:list>
        </s:key>
        <s:key name="write">
          <s:list>*</s:list>
        </s:key>
      </s:dict>
      <s:key name="removable">0</s:key>
      <s:key name="sharing">system</s:key>
    </s:dict>
    <s:key name="email"></s:key>
    <s:key name="password">********</s:key>
    <s:key name="realname"></s:key>
    <s:key name="restart_background_jobs">1</s:key>
    <s:key name="roles">
      <s:list>
        <s:item>admin</s:item>
      </s:list>
    </s:key>
    <s:key name="type">Splunk</s:key>
    <s:key name="tz"></s:key>
  </s:dict>
</entry>
authorization/capabilities

https://<host>:{mPort}/services/authorization/capabilities
Access system capabilities.

GET
List system capabilities.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>List of capabilities assigned to role.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/authorization/capabilities

XML Response

```xml
<entry>
  <title>capabilities</title>
  <id>https://localhost:8089/services/authorization/capabilities</id>
  <updated>2014-06-30T12:56:35-07:00</updated>
  <generator build="200839" version="6.1"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>capabilities</title>
    <id>https://localhost:8089/services/authorization/capabilities/capabilities</id>
    <updated>2014-06-30T12:56:35-07:00</updated>
    <link href="/services/authorization/capabilities/capabilities" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authorization/capabilities/capabilities" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="capabilities">
          <s:list>
            <s:item>accelerate_datamodel</s:item>
          </s:list>
        </s:dict>
      </content>
```
<s:item>accelerate_search</s:item>
<s:item>admin_all_objects</s:item>
<s:item>change_authentication</s:item>
<s:item>change_own_password</s:item>
<s:item>delete_by_keyword</s:item>
<s:item>edit_deployment_client</s:item>
<s:item>edit_deployment_server</s:item>
<s:item>edit_dist_peer</s:item>
<s:item>edit_forwarders</s:item>
<s:item>edit_httpauths</s:item>
<s:item>edit_input_defaults</s:item>
<s:item>edit_monitor</s:item>
<s:item>edit_roles</s:item>
<s:item>edit_scripted</s:item>
<s:item>edit_search_server</s:item>
<s:item>edit_server</s:item>
<s:item>editSplunktcp</s:item>
<s:item>editSplunktcp_ssl</s:item>
<s:item>edit_tcp</s:item>
<s:item>edit_udp</s:item>
<s:item>edit_user</s:item>
<s:item>edit_web_html</s:item>
<s:item>edit_web_settings</s:item>
<s:item>edit_win_admon</s:item>
<s:item>edit_win_eventlogs</s:item>
<s:item>edit_win_perfmon</s:item>
<s:item>edit_win_regmon</s:item>
<s:item>edit_win_wmiconf</s:item>
<s:item>embed_report</s:item>
<s:item>get_diag</s:item>
<s:item>get_metadata</s:item>
<s:item>get_typeahead</s:item>
<s:item>input_file</s:item>
<s:item>license_edit</s:item>
<s:item>license_tab</s:item>
<s:item>list_deployment_client</s:item>
<s:item>list_deployment_server</s:item>
<s:item>list_forwarders</s:item>
<s:item>list_httpauths</s:item>
<s:item>list_inputs</s:item>
<s:item>list_pdfserver</s:item>
<s:item>list_win_localavailablelogs</s:item>
<s:item>output_file</s:item>
<s:item>request_remote_tok</s:item>
<s:item>rest_apps_management</s:item>
<s:item>rest_apps_view</s:item>
<s:item>rest_properties_get</s:item>
<s:item>rest_properties_set</s:item>
<s:item>restart_splunkd</s:item>
<s:item>rtsearch</s:item>
<s:item>run_debug_commands</s:item>
<s:item>schedule_rtsearch</s:item>
<s:item>schedule_search</s:item>
<s:item>search</s:item>
<s:item>use_file_operator</s:item>
<s:item>write_pdfserver</s:item>
</s:list>
</s:key>
</s:dict>
</s:key name="eai:acl"/>
<s:dict>
<s:key name="app"/>
</s:key name="app"/>
authorization/grantable_capabilities

https://<host>:<mPort>/services/authorization/grantable_capabilities

Get a list of all capabilities that the current user can grant.

**Authorization**
Capabilities listed depend on the current user authorization. If the current user has the `edit_roles` capability, the response lists all capabilities. Otherwise, depending on the current user’s `edit_user` permissions and configured `grantableRoles` in authorize.conf, the response lists only the capabilities that the current user can grant.

**GET**
List capabilities that the current user can grant.

**Request parameters**
Pagination and filtering parameters can be used with this method.

**Response keys**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>For users with the <code>edit_roles</code> capability, lists all capabilities. For users with <code>edit_roles_grantable</code>, <code>edit_user</code>, and <code>grantableRoles</code>, lists only grantable capabilities.</td>
</tr>
</tbody>
</table>

**Example request and response**

```xml
<entry>
  <dict>
    <key name="can_list">1</key>
    <key name="can_write">1</key>
    <key name="modifiable">0</key>
    <key name="owner">system</key>
    <dict name="perms">
      <dict>
        <key name="read">
          <list>*</list>
        </key>
        <key name="write">
          <list>*</list>
        </key>
      </dict>
    </dict>
    <key name="removable">0</key>
    <key name="sharing">system</key>
  </dict>
</entry>
```
XML Request

curl -k -u admin:changeme https://localhost:8089/services/authorization/grantable_capabilities

XML Response

<title>grantable_capabilities</title>
  <id>https://localhost:8089/services/authorization/grantable_capabilities</id>
  ...
  ...
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/grantable_capabilities/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>capabilities</title>
    <id>https://localhost:8089/services/authorization/grantable_capabilities/capabilities</id>
    <updated>2015-10-06T17:44:09-07:00</updated>
    <link href="/services/authorization/grantable_capabilities/capabilities" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/authorization/grantable_capabilities/capabilities" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="capabilities">
          <s:list>
            <s:item>accelerate_datamodel</s:item>
            <s:item>accelerate_search</s:item>
            <s:item>admin_all_objects</s:item>
            <s:item>change_authentication</s:item>
            <s:item>change_own_password</s:item>
            <s:item>delete_by_keyword</s:item>
            <s:item>edit_deployment_client</s:item>
            <s:item>edit_deployment_server</s:item>
            <s:item>edit_dist_peer</s:item>
            <s:item>edit_forwarders</s:item>
            <s:item>edit_httpauths</s:item>
            <s:item>edit_input_defaults</s:item>
            <s:item>edit_monitor</s:item>
            <s:item>edit_roles</s:item>
            <s:item>edit_roles_grantable</s:item>
            <s:item>edit_scripted</s:item>
            <s:item>edit_search_head_clustering</s:item>
            <s:item>edit_search_scheduler</s:item>
            <s:item>edit_search_server</s:item>
            <s:item>edit_server</s:item>
            <s:item>edit_sourcetypes</s:item>
            <s:item>edit_splunktcp</s:item>
            <s:item>edit_splunktcp_ssl</s:item>
            <s:item>edit_tcp</s:item>
            <s:item>edit_token_http</s:item>
            <s:item>edit_udp</s:item>
            <s:item>edit_user</s:item>
            <s:item>edit_view_html</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
authorization/roles

https://<host>:<mPort>/services/authorization/roles

Create a role or get a list of defined roles with role permissions.

For additional information, see the following resources in *Securing Splunk Enterprise*.

- About role-based user access
- List of available capabilities

**GET**

List all roles and the permissions for each role.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Response keys**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>List of capabilities assigned to role.</td>
</tr>
<tr>
<td>cumulativeRTSrchJobsQuota</td>
<td>Maximum number of concurrently running real-time searches for all role members. Warning message logged when limit is reached.</td>
</tr>
<tr>
<td>cumulativeSrchJobsQuota</td>
<td>Maximum number of concurrently running searches for all role members. Warning message logged when limit is reached.</td>
</tr>
<tr>
<td>defaultApp</td>
<td>The name of the app to use as the default app for this role.</td>
</tr>
<tr>
<td></td>
<td>A user-specific default app overrides this.</td>
</tr>
<tr>
<td>imported_capabilities</td>
<td>List of capabilities assigned to role made available from imported roles.</td>
</tr>
<tr>
<td>imported_roles</td>
<td>List of imported roles for this role.</td>
</tr>
<tr>
<td>imported_rtSrchJobsQuota</td>
<td>The maximum number of concurrent real time search jobs for this role. This count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td></td>
<td>imported_rtSrchJobsQuota specifies the quota imported from other roles.</td>
</tr>
<tr>
<td>imported_srchDiskQuota</td>
<td>The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>imported_srchFilter</td>
<td>Search string, imported from other roles, that restricts the scope of searches run by this role. Search results for this role only show events that also match this search string. When a user has multiple roles with different search filters, they are combined with an OR.</td>
</tr>
<tr>
<td>imported_srchIndexesAllowed</td>
<td>A list of indexes, imported from other roles, this role has permissions to search.</td>
</tr>
<tr>
<td>imported_srchIndexesDefault</td>
<td>A list of indexes, imported from other roles, that this role defaults to when no index is specified in a search.</td>
</tr>
<tr>
<td>imported_srchJobsQuota</td>
<td>The maximum number of historical searches for this role that are imported from other roles.</td>
</tr>
<tr>
<td>imported_srchTimeWin</td>
<td>Maximum time span of a search, in seconds.</td>
</tr>
<tr>
<td></td>
<td>0 indicates searches are not limited to any specific time window.</td>
</tr>
<tr>
<td>rtSrchJobsQuota</td>
<td>The maximum number of concurrent real time search jobs for this role. This count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td>srchDiskQuota</td>
<td>The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total.</td>
</tr>
<tr>
<td>srchFilter</td>
<td>Search string that restricts the scope of searches run by this role. Search results for this role only show events that also match this search string. When a user has multiple roles with different search filters, they are combined with an OR.</td>
</tr>
<tr>
<td>srchIndexesAllowed</td>
<td>A list of indexes this role has permissions to search.</td>
</tr>
<tr>
<td>srchIndexesDefault</td>
<td>List of search indexes that default to this role when no index is specified.</td>
</tr>
<tr>
<td>srchJobsQuota</td>
<td>The maximum number of concurrent real time search jobs for this role. This count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td>srchTimeWin</td>
<td>Maximum time span of a search, in seconds.</td>
</tr>
<tr>
<td></td>
<td>0 indicates searches are not limited to any specific time window.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/roles
```

**XML Response**

```
<title>roles</title>
?id=https://localhost:8089/services/authorization/roles?id
<updated>2014-06-30T13:17:07:00</updated>
<generator build="200839" version="6.1"/>
<author>
```
<name>Splunk</name>

<title>admin</title>
<id>https://localhost:8089/services/authorization/roles/admin</id>
<updated>2014-06-30T13:17:07-07:00</updated>
<author>

<name>system</name>
</author>

<content type="text/xml">
<s:dict>
<s:key name="capabilities">
<s:list>
<s:item>accelerate_datamodel</s:item>
<s:item>admin_all_objects</s:item>
<s:item>change_authentication</s:item>
<s:item>edit_deployment_client</s:item>
<s:item>edit_deployment_server</s:item>
<s:item>edit_dist_peer</s:item>
<s:item>edit_forwarders</s:item>
<s:item>edit_httpauths</s:item>
<s:item>edit_input_defaults</s:item>
<s:item>edit_monitor</s:item>
<s:item>edit_roles</s:item>
<s:item>edit_scripted</s:item>
<s:item>edit_search_server</s:item>
<s:item>edit_server</s:item>
<s:item>edit_splunktcp</s:item>
<s:item>edit_splunktcp_ssl</s:item>
<s:item>edit_tcp</s:item>
<s:item>edit_udp</s:item>
<s:item>edit_user</s:item>
<s:item>edit_view_html</s:item>
<s:item>edit_web_settings</s:item>
<s:item>edit_win_admon</s:item>
<s:item>edit_win_eventlogs</s:item>
<s:item>edit_win_perfmon</s:item>
<s:item>edit_win_regmon</s:item>
<s:item>edit_win_wmiconf</s:item>
<s:item>get_diag</s:item>
<s:item>indexes_edit</s:item>
<s:item>license_edit</s:item>
<s:item>license_tab</s:item>
<s:item>list_deployment_client</s:item>
<s:item>list_deployment_server</s:item>
<s:item>list_forwarders</s:item>
<s:item>list_httpauths</s:item>
<s:item>list_pdfserver</s:item>
<s:item>list_win_localavailablelogs</s:item>
<s:item>rest_apps_management</s:item>
<s:item>restartSplunkd</s:item>
<s:item>run_debug_commands</s:item>
<s:item>write_pdfserver</s:item>
</s:list>
</s:dict>
</content>
<s:list>
<s:key name="cumulativeRTSrchJobsQuota">400</s:key>
<s:key name="cumulativeSrchJobsQuota">200</s:key>
<s:key name="defaultApp"></s:key>
<s:dict name="eai:acl">
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
</s:dict>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
<s:key name="imported_capabilities">
<s:list>
<s:item>accelerate_search</s:item>
<s:item>change_own_password</s:item>
<s:item>embed_report</s:item>
<s:item>get_metadata</s:item>
<s:item>get_typeahead</s:item>
<s:item>input_file</s:item>
<s:item>list_inputs</s:item>
<s:item>output_file</s:item>
<s:item>request_remote_tok</s:item>
<s:item>rest_apps_view</s:item>
<s:item>rest_properties_get</s:item>
<s:item>rest_properties_set</s:item>
<s:item>rtsearch</s:item>
<s:item>schedule_rtsearch</s:item>
<s:item>schedule_search</s:item>
<s:item>search</s:item>
</s:list>
</s:key>
<s:key name="imported_roles">
<s:list>
<s:item>power</s:item>
<s:item>user</s:item>
</s:list>
</s:key>
<s:key name="imported_rtSrchJobsQuota">20</s:key>
<s:key name="imported_srchDiskQuota">500</s:key>
<s:key name="imported_srchFilter"></s:key>
<s:key name="imported_srchIndexesAllowed">
<s:list>
<s:item>*</s:item>
</s:list>
156
<s:list>
  <s:item>main</s:item>
</s:list>

<s:key name="imported_srchIndexesDefault">
  <s:list>
  <s:item>main</s:item>
  </s:list>
</s:key>

<s:key name="imported_srchJobsQuota">10</s:key>
<s:key name="imported_srchTimeWin">-1</s:key>
<s:key name="rtsrchJobsQuota">100</s:key>
<s:key name="srchDiskQuota">10000</s:key>
<s:key name="srchFilter"></s:key>
<s:key name="srchIndexesAllowed">
  <s:list>
  <s:item>*</s:item>
  <s:item>_*</s:item>
  </s:list>
</s:key>
<s:key name="srchIndexesDefault">
  <s:list>
  <s:item>main</s:item>
  <s:item>os</s:item>
  </s:list>
</s:key>
<s:key name="srchJobsQuota">50</s:key>
<s:key name="srchTimeWin">0</s:key>
<s:key name="rtSrchJobsQuota">100</s:key>
<s:key name="srchFilter"></s:key>
<s:key name="srchIndexesAllowed">
  <s:list>
  <s:item>*</s:item>
  <s:item>_*</s:item>
  </s:list>
</s:key>
<s:key name="imported_srchIndexesDefault">
  <s:list>
  <s:item>main</s:item>
  <s:item>os</s:item>
  </s:list>
</s:key>
<s:key name="srchFilter"></s:key>
<s:key name="srchIndexesDefault">
  <s:list>
  <s:item>main</s:item>
  <s:item>os</s:item>
  </s:list>
</s:key>

<entry>
<title>can_delete</title>
<id>https://localhost:8089/services/authorization/roles/can_delete</id>
<updated>2014-06-30T13:12:17-07:00</updated>
<link href="/services/authorization/roles/can_delete" rel="alternate"/>
<author>
  <name>system</name>
</author>
<content type="text/xml">
  <s:dict>
  <s:key name="capabilities">
    <s:list>
    <s:item>delete_by_keyword</s:item>
    <s:item>schedule_rtsearch</s:item>
    </s:list>
  </s:key>
  <s:key name="cumulativeRTSrchJobsQuota">0</s:key>
  <s:key name="cumulativeSrchJobsQuota">0</s:key>
  <s:key name="defaultApp"></s:key>
  <s:key name="eai:acl">
    <s:dict>
    <s:key name="app"></s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">0</s:key>
    <s:key name="owner">system</s:key>
    <s:key name="perms"/>
    </s:dict>
  </s:key>
</content>
</entry>
<s:dict>
  <s:key name="capabilities">
    <s:list>
      <s:item>embed_report</s:item>
      <s:item>rtsearch</s:item>
    </s:list>
  </s:key>
  <s:key name="imported_capabilities">
    <s:list/>
  </s:key>
  <s:key name="imported_roles">
    <s:list/>
  </s:key>
  <s:key name="imported_rtSrchJobsQuota">0</s:key>
  <s:key name="imported_srchDiskQuota">0</s:key>
  <s:key name="imported_srchFilter"></s:key>
  <s:key name="imported_srchIndexesAllowed">
    <s:list/>
  </s:key>
  <s:key name="imported_srchIndexesDefault">
    <s:list/>
  </s:key>
  <s:key name="imported_srchJobsQuota">0</s:key>
  <s:key name="imported_srchTimeWin">-1</s:key>
  <s:key name="rtSrchJobsQuota">6</s:key>
  <s:key name="srchDiskQuota">100</s:key>
  <s:key name="srchFilter"></s:key>
  <s:key name="srchIndexesAllowed">
    <s:list/>
  </s:key>
  <s:key name="srchIndexesDefault">
    <s:list/>
  </s:key>
  <s:key name="srchJobsQuota">3</s:key>
  <s:key name="srchTimeWin">-1</s:key>
</s:dict>
<s:item>schedule_search</s:item>
</s:list>
</s:key>
<s:key name="cumulativeRTSearchJobsQuota">200</s:key>
<s:key name="cumulativeSearchJobsQuota">100</s:key>
<s:key name="defaultApp"></s:key>
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
</s:dict>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
<s:key name="imported_capabilities">
<s:list>
<s:item>accelerate_search</s:item>
<s:item>change_own_password</s:item>
<s:item>get_metadata</s:item>
<s:item>get_typeahead</s:item>
<s:item>input_file</s:item>
<s:item>list_inputs</s:item>
<s:item>output_file</s:item>
<s:item>request_remote_tok</s:item>
<s:item>rest_apps_view</s:item>
<s:item>rest_properties_get</s:item>
<s:item>rest_properties_set</s:item>
<s:item>schedule_rtsearch</s:item>
<s:item>search</s:item>
</s:list>
</s:key>
</s:list>
</s:item>
</s:dict>
</s:key>
<s:key name="imported_roles">
<s:list>
<s:item>user</s:item>
</s:list>
</s:key>
<s:key name="imported RtSearchJobsQuota">6</s:key>
<s:key name="imported SearchDiskQuota">100</s:key>
<s:key name="imported SearchFilter"></s:key>
<s:key name="imported SearchIndexesAllowed">
<s:list>
<s:item>**</s:item>
</s:list>
</s:key>
<s:key name="imported SearchIndexesDefault">

<s:list>
    <s:item>main</s:item>
</s:list>

<s:dict>
    <s:key name="imported_srchJobsQuota">3</s:key>
    <s:key name="imported_srchTimeWin">-1</s:key>
    <s:key name="rtSrchJobsQuota">20</s:key>
    <s:key name="srchDiskQuota">500</s:key>
    <s:key name="srchFilter"></s:key>
    <s:key name="srchIndexesAllowed">
        <s:list>
            <s:item>*</s:item>
        </s:list>
    </s:key>
    <s:key name="srchIndexesDefault">
        <s:list>
            <s:item>main</s:item>
        </s:list>
    </s:key>
    <s:key name="srchJobsQuota">10</s:key>
    <s:key name="srchTimeWin">-1</s:key>
</s:dict>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<title>splunk-system-role</title>
</entry>

<entry>
<s:dict>
<s:key name="removeable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
<s:dict>
<s:key name="imported_capabilities">
<s:list>
<s:item>accelerate_datamodel</s:item>
<s:item>accelerate_search</s:item>
<s:item>admin_all_objects</s:item>
<s:item>change_authentication</s:item>
<s:item>change_own_password</s:item>
<s:item>edit_deployment_client</s:item>
<s:item>edit_deployment_server</s:item>
<s:item>edit_dist_peer</s:item>
<s:item>edit_forwarders</s:item>
<s:item>edit_httpauths</s:item>
<s:item>edit_input_defaults</s:item>
<s:item>edit_monitor</s:item>
<s:item>edit_roles</s:item>
<s:item>edit_scripted</s:item>
<s:item>edit_search_server</s:item>
<s:item>edit_server</s:item>
<s:item>edit_splunktcp</s:item>
<s:item>edit_splunktcp_ssl</s:item>
<s:item>edit_tcp</s:item>
<s:item>edit_udp</s:item>
<s:item>edit_user</s:item>
<s:item>edit_view_html</s:item>
<s:item>edit_web_settings</s:item>
<s:item>edit_win_admon</s:item>
<s:item>edit_win_eventlogs</s:item>
<s:item>edit_win_perfmon</s:item>
<s:item>edit_win_regmon</s:item>
<s:item>edit_win_wmiconf</s:item>
<s:item>embed_report</s:item>
<s:item>get_diag</s:item>
<s:item>get_metadata</s:item>
<s:item>get_typeahead</s:item>
<s:item>indexes_edit</s:item>
<s:item>input_file</s:item>
<s:item>license_edit</s:item>
<s:item>license_tab</s:item>
<s:item>list_deployment_client</s:item>
<s:item>list_deployment_server</s:item>
<s:item>list_forwarders</s:item>
<s:item>list_httpauths</s:item>
<s:item>list_inputs</s:item>
<s:item>list_pdfservlet</s:item>
<s:item>list_win_localavailablelogs</s:item>
<s:item>output_file</s:item>
<s:item>request_remote_tok</s:item>
<s:item>rest_apps_management</s:item>
<s:item>rest_apps_view</s:item>
<s:item>rest_properties_get</s:item>
<s:item>rest_properties_set</s:item>
<s:item>restart_splunkd</s:item>
<s:item>rtsearch</s:item>
<s:item>run_debug_commands</s:item>
<s:item>schedule_rtsearch</s:item>
<s:item>schedule_search</s:item>
</s:list>
</s:dict>
<s:item>search</s:item>
<s:item>write_pdfserver</s:item>
</s:list>
</s:key>
<s:key name="imported_roles">
<s:list>
<s:item>admin</s:item>
</s:list>
</s:key>
<s:key name="imported_rtSrchJobsQuota">100</s:key>
<s:key name="imported_srchDiskQuota">10000</s:key>
<s:key name="imported_srchFilter">*</s:key>
<s:key name="imported_srchIndexesAllowed">
<s:list>
<s:item>*</s:item>
<s:item>_*</s:item>
</s:list>
</s:key>
<s:key name="imported_srchIndexesDefault">
<s:list>
<s:item>main</s:item>
<s:item>os</s:item>
</s:list>
</s:key>
<s:key name="imported_srchJobsQuota">50</s:key>
<s:key name="imported_srchTimeWin">-1</s:key>
<s:key name="rtSrchJobsQuota">6</s:key>
<s:key name="srchDiskQuota">100</s:key>
<s:key name="srchFilter"></s:key>
<s:key name="srchIndexesAllowed">
<s:list/>
</s:key>
<s:key name="srchIndexesDefault">
<s:list/>
</s:key>
<s:key name="srchJobsQuota">3</s:key>
<s:key name="srchTimeWin">-1</s:key>
</s:dict>
</entry>
<entry>
<title>user</title>
{id>https://localhost:8089/services/authorization/roles/user</id>
<updated>2014-06-30T13:12:17-07:00</updated>
<link href="/services/authorization/roles/user" rel="alternate"/>
<author>
<name>system</name>
</author>
<link href="/services/authorization/roles/user" rel="list"/>
<link href="/services/authorization/roles/user" rel="edit"/>
<link href="/services/authorization/roles/user" rel="remove"/>
<content type="text/xml">
<s:dict>
<s:key name="capabilities">
<s:list>
<s:item>accelerate_search</s:item>
<s:item>change_own_password</s:item>
<s:item>get_metadata</s:item>
<s:item>get_typeahead</s:item>
<s:item>input_file</s:item>
<s:item>list_inputs</s:item>
<s:item>output_file</s:item>
</s:list>
</s:key>
</content>
</entry>
POST

Create a user role.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>String</td>
<td>List of capabilities assigned to role. To send multiple capabilities, send this argument multiple times. Roles inherit all capabilities from imported roles.</td>
</tr>
<tr>
<td>cumulativeRTSrchJobsQuota</td>
<td>Number</td>
<td>Maximum number of concurrently running real-time searches that all members of this role can have. Note: If a user belongs to multiple roles then the user first consumes searches from the roles with the largest cumulative search quota. When the quota of a role is completely used up then roles with lower quotas are examined.</td>
</tr>
<tr>
<td>cumulativeSrchJobsQuota</td>
<td>Number</td>
<td>Maximum number of concurrently running searches for all role members. Warning message logged when limit is reached. Note: If a user belongs to multiple roles then the user first consumes searches from the roles with the largest cumulative search quota. When the quota of a role is completely used up then roles with lower quotas are examined.</td>
</tr>
<tr>
<td>defaultApp</td>
<td>String</td>
<td>Specify the folder name of the default app to use for this role. A user-specific default app overrides this.</td>
</tr>
<tr>
<td>imported_roles</td>
<td>String</td>
<td>Specify a role to import attributes from. To import multiple roles, specify them separately. By default a role imports no other roles. Importing other roles imports all aspects of that role, such as capabilities and allowed indexes to search. In combining multiple roles, the effective value for each attribute is the value with the broadest permissions. Default roles are admin, can_delete, power, and user. You can specify additional roles created.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Required. The name of the user role to create.</td>
</tr>
</tbody>
</table>

164
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtSrchJobsQuota</td>
<td>Number</td>
<td>Specify the maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td>srchDiskQuota</td>
<td>Number</td>
<td>Specifies the maximum disk space in MB that can be used by a user's search jobs. For example, a value of 100 limits this role to 100 MB total.</td>
</tr>
</tbody>
</table>
| srchFilter         | String   | Specify a search string that restricts the scope of searches run by this role. Search results for this role only show events that also match the search string you specify. In the case that a user has multiple roles with different search filters, they are combined with an OR. The search string can include search fields and the following terms.  
  - source
  - host
  - index
  - eventtype
  - sourcetype
  - *
  - OR
  - AND

  Example: "host=web* OR source=/var/log/*"

  Note: You can also use the srchIndexesAllowed and srchIndexesDefault parameters to limit the search on indexes. |
| srchIndexesAllowed | String   | Index that this role has permissions to search. Pass this argument once for each index that you want to specify. These may be wildcarded, but the index name must begin with an underscore to match internal indexes.

  Search indexes available by default include the following.
  - All internal indexes
  - All non-internal indexes
  - _audit
  - _blocks
  - _internal
  - _thefishbucket
  - history
  - main

  You can also specify other search indexes added to the server. |
| srchIndexesDefault | String   | For this role, indexes to search when no index is specified.

  These indexes can be wildcarded, with the exception that '*' does not match internal indexes. To match internal indexes, start with '_'. All internal indexes are represented by '_*'.

  A user with this role can search other indexes using "index= "

  For example, "index=special_index".

  Search indexes available by default include the following. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>srchJobsQuota</td>
<td>Number</td>
<td>The maximum number of concurrent searches a user with this role is allowed to run. For users with multiple roles, the maximum quota value among all of the roles applies.</td>
</tr>
<tr>
<td>srchTimeWin</td>
<td>Number</td>
<td>Maximum time span of a search, in seconds. By default, searches are not limited to any specific time window. To override any search time windows from imported roles, set srchTimeWin to '0', as the 'admin' role does.</td>
</tr>
</tbody>
</table>

**Response keys**
None

**Example request and response**

**XML Request**

curl -k -u admin:changeme https://localhost:8089/services/authorization/roles -d name=newrole1 -d imported_roles=user

**XML Response**

```
<entry>
<title>newrole1</title>
<id>https://localhost:8089/services/authorization/roles/newrole1</id>
<updated>2014-06-30T13:21:50-07:00</updated>
<author>
  <name>system</name>
</author>
<link href="/services/authorization/roles/newrole1" rel="list"/>
<link href="/services/authorization/roles/newrole1" rel="edit"/>
<link href="/services/authorization/roles/newrole1" rel="remove"/>
```
<s:dict>
  <s:dict>
    <s:key name="capabilities">
      <s:list/>
    </s:key>
    <s:key name="cumulativeRTSrchJobsQuota">0</s:key>
    <s:key name="cumulativeSrchJobsQuota">0</s:key>
    <s:key name="defaultApp"></s:key>
  </s:dict>
  <s:dict>
    <s:dict>
      <s:key name="app"></s:key>
      <s:list>
        <s:item>accelerate_search</s:item>
        <s:item>change_own_password</s:item>
        <s:item>get_metadata</s:item>
        <s:item>get_typeahead</s:item>
        <s:item>input_file</s:item>
        <s:item>list_inputs</s:item>
        <s:item>output_file</s:item>
        <s:item>request_remote_tok</s:item>
        <s:item>rest_apps_view</s:item>
        <s:item>rest_properties_get</s:item>
        <s:item>rest_properties_set</s:item>
        <s:item>schedule_rtsearch</s:item>
        <s:item>search</s:item>
      </s:list>
    </s:dict>
    <s:dict>
      <s:list>
        <s:item>admin</s:item>
        <s:item>splunk-system-role</s:item>
      </s:list>
    </s:dict>
    <s:dict>
      <s:list>
        <s:item>admin</s:item>
        <s:item>splunk-system-role</s:item>
      </s:list>
    </s:dict>
    <s:dict>
      <s:list/>
    </s:dict>
  </s:dict>
  <s:dict>
    <s:dict>
      <s:key name="imported_capabilities">
        <s:list>
          <s:item>accelerate_search</s:item>
          <s:item>change_own_password</s:item>
          <s:item>get_metadata</s:item>
          <s:item>get_typeahead</s:item>
          <s:item>input_file</s:item>
          <s:item>list_inputs</s:item>
          <s:item>output_file</s:item>
          <s:item>request_remote_tok</s:item>
          <s:item>rest_apps_view</s:item>
          <s:item>rest_properties_get</s:item>
          <s:item>rest_properties_set</s:item>
          <s:item>schedule_rtsearch</s:item>
          <s:item>search</s:item>
        </s:list>
      </s:key>
      <s:key name="imported_roles">
        <s:list>
          <s:item>user</s:item>
        </s:list>
      </s:key>
      <s:key name="imported_rtSrchJobsQuota">6</s:key>
      <s:key name="imported_srchDiskQuota">100</s:key>
      <s:key name="imported_srchFilter"></s:key>
      <s:key name="imported_srchIndexesAllowed">
        <s:list>
          167
        </s:list>
      </s:key>
    </s:dict>
  </s:dict>
</s:dict>
authorization/roles/{name}

https://<host>:<mPort>/services/authorization/roles/{name}

Access, create, or delete properties for the {name} role.

For additional information, see the following resource in Securing Splunk Enterprise. List of available capabilities

DELETE

Delete the specified role.

Request parameters
None

Response keys
None

Example request and response

XML Request

curl -k -u admin:changeme --request DELETE https://localhost:8089/services/authorization/roles/newrole1

XML Response
<title>roles</title>
?id=https://localhost:8089/services/authorization/roles/id
<updated>2014-06-30T13:21:50-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authorization/roles/_new" rel="create"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>newrole1</title>
?id=https://localhost:8089/services/authorization/roles/newrole1/id
<updated>2014-06-30T13:21:50-07:00</updated>
<link href="/services/authorization/roles/newrole1" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/authorization/roles/newrole1" rel="list"/>
<link href="/services/authorization/roles/newrole1" rel="edit"/>
<link href="/services/authorization/roles/newrole1" rel="remove"/>
<content type="text/xml">
<s:dict>
  <s:dict name="capabilities">
  </s:dict>
  <s:dict name="cumulativeRTSrchJobsQuota">0</s:dict>
  <s:dict name="cumulativeSrchJobsQuota">0</s:dict>
  <s:dict name="defaultApp"></s:dict>
  <s:dict name="eai:acl">
    <s:dict name="app"></s:dict>
    <s:dict name="can_list">1</s:dict>
    <s:dict name="can_write">1</s:dict>
    <s:dict name="modifiable">0</s:dict>
    <s:dict name="owner">system</s:dict>
    <s:dict name="perms">
      <s:dict name="read">
        <s:list>
          <s:item>admin</s:item>
          <s:item>splunk-system-role</s:item>
        </s:list>
      </s:dict>
      <s:dict name="write">
        <s:list>
          <s:item>admin</s:item>
          <s:item>splunk-system-role</s:item>
        </s:list>
      </s:dict>
      <s:dict name="removable">0</s:dict>
      <s:dict name="sharing">system</s:dict>
    </s:dict>
    <s:dict name="imported_capabilities">
      <s:list>
        <s:item>accelerate_search</s:item>
      </s:list>
    </s:dict>
  </s:dict>
</s:dict>
</entry>
GET

Access the specified role.

Request parameters
None

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rtSrchJobsQuota</td>
<td></td>
</tr>
<tr>
<td>srchJobsQuota</td>
<td></td>
</tr>
<tr>
<td>srchTimeWin</td>
<td></td>
</tr>
<tr>
<td>srchFilter</td>
<td></td>
</tr>
<tr>
<td>srchIndexesAllowed</td>
<td></td>
</tr>
<tr>
<td>srchIndexesDefault</td>
<td></td>
</tr>
<tr>
<td>srchDiskQuota</td>
<td></td>
</tr>
<tr>
<td>imported_roles</td>
<td></td>
</tr>
<tr>
<td>imported_srchJobsQuota</td>
<td></td>
</tr>
<tr>
<td>imported_srchDiskQuota</td>
<td></td>
</tr>
<tr>
<td>imported_srchIndexesAllowed</td>
<td></td>
</tr>
<tr>
<td>imported_srchIndexesDefault</td>
<td></td>
</tr>
</tbody>
</table>

170
<table>
<thead>
<tr>
<th>capabilities</th>
<th>List of capabilities assigned to this role.</th>
</tr>
</thead>
<tbody>
<tr>
<td>cumulativeRTSrchJobsQuota</td>
<td>Maximum number of concurrently running real-time searches for all role members. A warning message is logged when this limit is reached.</td>
</tr>
<tr>
<td>cumulativeSrchJobsQuota</td>
<td>Maximum number of concurrently running searches for all role members. A warning message is logged when this limit is reached.</td>
</tr>
<tr>
<td>defaultApp</td>
<td>The name of the app to use as the default app for this role. A user-specific default app overrides this.</td>
</tr>
<tr>
<td>imported_capabilities</td>
<td>List of capabilities assigned to role that were made available from imported roles.</td>
</tr>
<tr>
<td>imported_roles</td>
<td>List of imported roles for this role.</td>
</tr>
<tr>
<td>imported_rtSrchJobsQuota</td>
<td>The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td>imported_rtSrchJObsQuota</td>
<td>specifies the quota imported from other roles.</td>
</tr>
<tr>
<td>imported_srchDiskQuota</td>
<td>The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total.</td>
</tr>
<tr>
<td>imported_srchDiskQuota</td>
<td>specifies the quota imported from other roles.</td>
</tr>
<tr>
<td>imported_srchFilter</td>
<td>Search string, imported from other roles, that restricts the scope of searches run by this role. Search results for this role only show events that also match this search string. When a user has multiple roles with different search filters, they are combined with an OR.</td>
</tr>
<tr>
<td>imported_srchIndexesAllowed</td>
<td>A list of indexes, imported from other roles, this role has permissions to search.</td>
</tr>
<tr>
<td>imported_srchIndexesDefault</td>
<td>A list of indexes, imported from other roles, that this role defaults to when no index is specified in a search.</td>
</tr>
<tr>
<td>imported_srchJobsQuota</td>
<td>The maximum number of historical searches for this role that are imported from other roles.</td>
</tr>
<tr>
<td>imported_srchTimeWin</td>
<td>Maximum time span of a search, in seconds. 0 indicates searches are not limited to any specific time window.</td>
</tr>
<tr>
<td>imported_srchTimeWin</td>
<td>specifies the limit from imported roles.</td>
</tr>
<tr>
<td>rtSrchJobsQuota</td>
<td>The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td>srchDiskQuota</td>
<td>The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total.</td>
</tr>
<tr>
<td>srchFilter</td>
<td>Search string that restricts the scope of searches run by this role. Search results for this role only show events that also match this search string. When a user has multiple roles with different search filters, they are combined with an OR.</td>
</tr>
<tr>
<td>srchIndexesAllowed</td>
<td>A list of indexes this role has permissions to search.</td>
</tr>
<tr>
<td>srchIndexesDefault</td>
<td>List of search indexes that default to this role when no index is specified.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>srchJobsQuota</td>
<td>The maximum number of concurrent real time search jobs for this role. This</td>
</tr>
<tr>
<td></td>
<td>count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td>srchTimeWin</td>
<td>Maximum time span of a search, in seconds. 0 indicates searches are not</td>
</tr>
<tr>
<td></td>
<td>limited to any specific time window.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -k -u admin:changeme https://localhost:8089/services/authorization/roles/newrole1
```

XML Response

```xml
<title>roles</title>
<id>https://localhost:8089/services/authorization/roles</id>
<updated>2014-06-30T13:30:34-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authorization/roles/_new" rel="create"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>newrole1</title>
  <id>https://localhost:8089/services/authorization/roles/newrole1</id>
  <updated>2014-06-30T13:30:34-07:00</updated>
  <link href="/services/authorization/roles/newrole1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authorization/roles/newrole1" rel="list"/>
  <link href="/services/authorization/roles/newrole1" rel="edit"/>
  <link href="/services/authorization/roles/newrole1" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list/>
      </s:key>
      <s:key name="cumulativeRTSrchJobsQuota">0</s:key>
      <s:key name="cumulativeSrchJobsQuota">0</s:key>
      <s:key name="defaultApp"></s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
            <s:dict>
              <s:key name="wildcardFields">
                <s:list/>
              </s:key>
            </s:dict>
            <s:dict>
              <s:key name="imported_capabilities">
                <s:list>
                  <s:item>accelerate_search</s:item>
                  <s:item>change_own_password</s:item>
                  <s:item>get_metadata</s:item>
                  <s:item>get_typeahead</s:item>
                  <s:item>input_file</s:item>
                  <s:item>list_inputs</s:item>
                  <s:item>output_file</s:item>
                  <s:item>request_remote_tok</s:item>
                  <s:item>rest_apps_view</s:item>
                  <s:item>rest_properties_get</s:item>
                  <s:item>rest_properties_set</s:item>
                  <s:item>schedule_rtsearch</s:item>
                  <s:item>search</s:item>
                </s:list>
              </s:key>
              <s:dict>
                <s:key name="imported_roles">
                  <s:list>
                    <s:item>user</s:item>
                  </s:list>
                </s:dict>
                <s:dict>
                  <s:key name="imported_rtSrchJobsQuota">6</s:key>
                  <s:key name="imported_srchDiskQuota">100</s:key>
                </s:dict>
              </s:dict>
            </s:dict>
            <s:dict>
              <s:key name="imported_capabilities">
                <s:list>
                  <s:item>accelerate_search</s:item>
                  <s:item>change_own_password</s:item>
                  <s:item>get_metadata</s:item>
                  <s:item>get_typeahead</s:item>
                  <s:item>input_file</s:item>
                  <s:item>list_inputs</s:item>
                  <s:item>output_file</s:item>
                  <s:item>request_remote_tok</s:item>
                  <s:item>rest_apps_view</s:item>
                  <s:item>rest_properties_get</s:item>
                  <s:item>rest_properties_set</s:item>
                  <s:item>schedule_rtsearch</s:item>
                  <s:item>search</s:item>
                </s:list>
              </s?key>
              <s:dict>
                <s:key name="imported_roles">
                  <s:list>
                    <s:item>user</s:item>
                  </s:list>
                </s:dict>
                <s:dict>
                  <s:key name="imported_rtSrchJobsQuota">6</s:key>
                  <s:key name="imported_srchDiskQuota">100</s:key>
                </s:dict>
              </s:dict>
            </s:dict>
          </s:dict>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
```
POST

Update the specified role.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capabilities</td>
<td>String</td>
<td>List of capabilities assigned to this role.</td>
</tr>
<tr>
<td>cumulativeRTSrchJobsQuota</td>
<td>Number</td>
<td>Maximum number of concurrently running real-time searches for all role members. A warning message is logged when this limit is reached.</td>
</tr>
<tr>
<td>cumulativeSrchJobsQuota</td>
<td>Number</td>
<td>Maximum number of concurrently running searches for all role members. A warning message is logged when this limit is reached.</td>
</tr>
<tr>
<td>defaultApp</td>
<td>String</td>
<td>The folder name for the app to use as the default app for this role. A user-specific default app overrides this.</td>
</tr>
<tr>
<td>imported_capabilities</td>
<td>String</td>
<td>List of capabilities assigned to role that were made available from imported roles.</td>
</tr>
<tr>
<td>imported_roles</td>
<td>String</td>
<td>List of imported roles for this role. Importing other roles imports all aspects of that role, such as capabilities and allowed indexes to search. In combining multiple roles, the effective value for each attribute is value with the broadest permissions.</td>
</tr>
<tr>
<td>imported_rtSrchJobsQuota</td>
<td>String</td>
<td>The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>imported_rtSrchJObsQuota</td>
<td>String</td>
<td>specifies the quota imported from other roles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>imported_rtSrchJObsQuota specifies the quota imported from other roles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>imported_srchDiskQuota</td>
<td>String</td>
<td>The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>imported_srchDiskQuota specifies the quota imported from other roles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>imported_srchFilter</td>
<td>String</td>
<td>Search string, imported from other roles, that restricts the scope of searches run by this role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Search results for this role only show events that also match this search string. When a user has multiple roles with different search filters, they are combined with an OR.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>imported_srchIndexesAllowed</td>
<td>String</td>
<td>A list of indexes, imported from other roles, this role has permissions to search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>imported_srchIndexesDefault</td>
<td>String</td>
<td>A list of indexes, imported from other roles, that this role defaults to when no index is specified in a search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>imported_srchJobsQuota</td>
<td>String</td>
<td>The maximum number of historical searches for this role that are imported from other roles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>imported_srchTimeWin</td>
<td>String</td>
<td>Maximum time span of a search, in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>specifies the limit from imported roles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>rtSrchJobsQuota</td>
<td>Number</td>
<td>The maximum number of concurrent real-time search jobs for this role. This count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>srchDiskQuota</td>
<td>Number</td>
<td>The maximum disk space in MB that can be used by a user's search jobs. For example, 100 limits this role to 100 MB total.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>srchFilter</td>
<td>String</td>
<td>Search string that restricts the scope of searches run by this role.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Search results for this role only show events that also match this search string. When a user has multiple roles with different search filters, they are combined with an OR.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>srchIndexesAllowed</td>
<td>String</td>
<td>A list of indexes this role has permissions to search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>srchIndexesDefault</td>
<td>String</td>
<td>List of search indexes that default to this role when no index is specified.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>srchJobsQuota</td>
<td>Number</td>
<td>The maximum number of concurrent real time search jobs for this role. This count is independent from the normal search jobs limit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>srchTimeWin</td>
<td>Number</td>
<td>Maximum time span of a search, in seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>specifies searches are not limited to any specific time window.</td>
</tr>
</tbody>
</table>

Response keys
None

Example request and response

XML Request
curl -k -u admin:changeme https://localhost:8089/services/authorization/roles/newrole1 -d
defaultApp=launcher

XML Response

<title>roles</title>
<id>https://localhost:8089/services/authorization/roles</id>
<updated>2014-06-30T13:33:38-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authorization/roles/_new" rel="create"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>newrole1</title>
  <id>https://localhost:8089/services/authorization/roles/newrole1</id>
  <updated>2014-06-30T13:33:38-07:00</updated>
  <link href="/services/authorization/roles/newrole1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authorization/roles/newrole1" rel="list"/>
  <link href="/services/authorization/roles/newrole1" rel="edit"/>
  <link href="/services/authorization/roles/newrole1" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="capabilities">
        <s:list/>
      </s:key>
      <s:key name="cumulativeRTSrchJobsQuota">0</s:key>
      <s:key name="cumulativeSrchJobsQuota">0</s:key>
      <s:key name="defaultApp">launcher</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="removable">0</s:key>
    </s:dict>
  </content>
authorization/tokens

https://<host>:<mPort>/services/authorization/tokens

Create, get information on, or modify tokens for authentication.
For additional information, see the following resources in *Securing Splunk Enterprise*.

- Set up authentication with tokens
- Create authentication tokens
- Manage or delete authentication tokens

**GET**

List information on tokens.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Response keys**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>The username whose tokens you want to see. Optional. If not provided, all tokens are displayed.</td>
</tr>
<tr>
<td>id</td>
<td>The ID of the token whose information you want to see. Optional.</td>
</tr>
<tr>
<td>status</td>
<td>Show only tokens of a specific status. Optional. Valid values are enabled or disabled.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:changeme https://localhost:8089/services/authorization/tokens
```

**XML Response**

```xml
<title>tokens</title>
{id>https://splunkaday-linux-current:8089/services/authorization/tokens</id>
<updated>2019-04-28T15:04:30-07:00</updated>
<generator build="6c6f0a26991" version="7.3.0"/>

<title>60ccc93ef090ca6746cc56d5dd5c6c38359bcae2d0e8ddecc9dc3b21a93ad7f9</title>
<id>https://splunkaday-linux-current:8089/services/authorization/tokens/60ccc93ef090ca6746cc56d5dd5c6c38359bcae2d0e8ddecc9dc3b21a93ad7f9</id>
<updated>2019-04-28T15:04:30-07:00</updated>
```
<author>
  <name>system</name>
</author>

<content type="text/xml">
  <s:dict>
    <s:key name="claims">
      <s:dict>
        <s:key name="aud">Tokentown</s:key>
        <s:key name="exp">0</s:key>
        <s:key name="iat">1556488991</s:key>
        <s:key name="idp">splunk</s:key>
        <s:key name="iss">admin from docs-unix-4</s:key>
        <s:key name="nbr">1556488991</s:key>
        <s:key name="roles">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="sub">admin</s:key>
      </s:dict>
    </s:key>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app"></s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">0</s:key>
        <s:key name="owner">system</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
  </s:dict>
</content>
POST

Change the status of one or more tokens.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>The user of the token. Can be up to 1024 characters.</td>
</tr>
<tr>
<td>audience</td>
<td>String</td>
<td>The purpose for the token. Can be up to 256 characters.</td>
</tr>
<tr>
<td>expires_on</td>
<td>String</td>
<td>The time that the token expires. Can be either of an absolute time (ex.: 2019-02-09T07:35:00+07:00) or a relative time (ex.: +90d). This time cannot be in the past.</td>
</tr>
<tr>
<td>not_before</td>
<td>String</td>
<td>The time that the token becomes valid. Can be an absolute time or a relative time. This time cannot be in the past.</td>
</tr>
</tbody>
</table>

Note: If you specify not_before in addition to expires_on, not_before cannot be after expires_on.

Response keys

None

Example request and response

XML Request

```bash
curl -k -u admin:changeme https://localhost:8089/services/authorization/tokens -d name=user12 -d audience=Users
```

XML Response

```xml
     xmlns:tokens="http://localhost:8089/services/authorization/tokens"
     xmlns:atom="http://www.w3.org/2005/Atom"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <title>tokens</title>
  <id>https://splunkaday-linux-current:8089/services/authorization/tokens</id>
  <updated>2019-04-28T15:26:52-07:00</updated>
  <generator build="6c6f0a269b91" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/tokens/_new" rel="create"/>
</feed>
```
authorization/tokens/{name}

https://<host>:<mPort>/services/authorization/tokens/name

Get information on, modify, or delete authentication tokens for the {name} user.

For additional information, see the following resources in *Securing Splunk Enterprise*.

- Set up authentication with tokens
- Manage or delete authentication tokens

**DELETE**

Delete a token for the specified user.

**Request parameters**

Pagination and filtering parameters can be used with this method.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>The ID of the token you want to delete. Optional. If not specified, then all tokens that belong to {username} are deleted.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:changeme -X DELETE https://localhost:8089/services/authorization/tokens/user12

**XML Response**

```xml
  <title>tokens</title>
  <id>https://splunkaday-linux-current:8089/services/authorization/tokens</id>
  <updated>2019-04-28T16:13:45-07:00</updated>
  <generator build="6c6f0a269b91" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/authorization/tokens/_new" rel="create"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages>
    <s:msg type="INFO">Token(s), removed.</s:msg>
  </s:messages>
  <entry>
    <title>cdc2f1dddc0e240695fe97c5474d27d6224eb49e4bb70d6a7dad1b7041b66bf</title>
    <id>https://splunkaday-linux-current:8089/services/authorization/tokens</id>
  </entry>
</feed>
```
<s:dict name="claims">
  <s:dict name="aud">Tokentown</s:dict>
  <s:dict name="exp">0</s:dict>
  <s:dict name="iat">1556490311</s:dict>
  <s:dict name="idp">splunk</s:dict>
  <s:dict name="iss">admin from docs-unix-4</s:dict>
  <s:dict name="nbr">1556490311</s:dict>
  <s:dict name="roles">
    <s:list>*</s:list>
  </s:dict>
  <s:dict name="sub">admin</s:dict>
</s:dict>

<s:dict name="eai:acl">
  <s:dict name="app"></s:dict>
  <s:dict name="can_list">1</s:dict>
  <s:dict name="can_write">1</s:dict>
  <s:dict name="modifiable">0</s:dict>
  <s:dict name="owner">system</s:dict>
  <s:dict name="perms">
    <s:dict name="read">
      <s:list>
        <s:item>admin</s:item>
        <s:item>splunk-system-role</s:item>
      </s:list>
    </s:dict>
    <s:dict name="write">
      <s:list>
        <s:item>admin</s:item>
        <s:item>splunk-system-role</s:item>
      </s:list>
    </s:dict>
    <s:dict name="removable">0</s:dict>
    <s:dict name="sharing">system</s:dict>
  </s:dict>
</s:dict>
POST

Create a token for the specified username.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>The user of the token. Can be up to 1024 characters.</td>
</tr>
<tr>
<td>audience</td>
<td>String</td>
<td>The purpose for the token. Can be up to 256 characters.</td>
</tr>
<tr>
<td>expires_on</td>
<td>String</td>
<td>The time that the token expires. Can be either of an absolute time (ex.: 2019-02-09T07:35:00+07:00) or a relative time (ex.: +90d). This time cannot be in the past. Note: If you specify not_before in addition to expires_on, not_before cannot be after expires_on.</td>
</tr>
<tr>
<td>not_before</td>
<td>String</td>
<td>The time that the token becomes valid. Can be an absolute time or a relative time. This time cannot be in the past. Note: If you specify not_before in addition to expires_on, not_before cannot be after expires_on.</td>
</tr>
</tbody>
</table>

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/authorization/tokens/user12 -d audience=Users -d expires_on=+90d@d
```

XML Response

```
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xsi:schemaLocation="http://dev.splunk.com/ns/rest http://dev.splunk.com/ns/rest.xsd">
  <title>tokens</title>
  <id>https://splunkaday-linux-current:8089/services/authorization/tokens</id>
  <updated>2019-04-28T15:26:52-07:00</updated>
</feed>
```
<generator build="6c6f0a269b91" version="7.3.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/authorization/tokens/_new" rel="create"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>tokens</title>
  <id>https://splunkaday-linux-current:8089/services/authorization/tokens/tokens</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/authorization/tokens/tokens" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/authorization/tokens/tokens" rel="list"/>
  <link href="/services/authorization/tokens/tokens" rel="edit"/>
  <link href="/services/authorization/tokens/tokens" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">
            <s:list>
              <s:item>admin</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
        </s:dict>
        <s:dict>
          <s:key name="id">a1afa1a74528731191ab3e597889b2013c57cc301e06a9cf4e86f8282144ba09</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</feed>
storage/passwords

https://<host>:<mPort>/services/storage/passwords
Create or update user credentials, or list credentials for all users.

Authorization
The list_storage_passwords capability is required for the GET operation. The admin_all_objects capability is required for the POST operation.

Usage details
The password credential is the only part of the user credentials that is stored securely. It is encrypted with a secure key resident on the same server.

GET
List available credentials.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear_password</td>
<td>Clear text password.</td>
</tr>
<tr>
<td>encr_password</td>
<td>Encrypted, stored password.</td>
</tr>
<tr>
<td>password</td>
<td>Password mask, always *********.</td>
</tr>
<tr>
<td>realm</td>
<td>Realm in which credentials are valid.</td>
</tr>
<tr>
<td>username</td>
<td>User name associated with credentials.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/storage/passwords

XML Response

```xml
.".
<id>https://localhost:8089/services/storage/passwords</id>
<updated>2014-06-30T13:43:06-07:00</updated>
<generator build="200839" version="6.1"/>
```
<author>
  <name>Splunk</name>
</author>

<link href="/services/storage/passwords/_new" rel="create"/>
<link href="/services/storage/passwords/_reload" rel="_reload"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>:testuser:</title>
  <id>https://localhost:8089/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A</id>
  <updated>2014-06-30T13:43:06-07:00</updated>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A" rel="list"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A" rel="edit"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Atestuser%3A" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="clear_password">newpwd</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">admin</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>power</s:item>
                </s:list>
              </s:key>
              <s:key name="removable">1</s:key>
              <s:key name="sharing">app</s:key>
            </s:dict>
            <s:key name="encr_password">$1$prTUy3vRWg==</s:key>
            <s:key name="password">********</s:key>
            <s:key name="realm"></s:key>
            <s:key name="username">testuser</s:key>
          </s:dict>
        </s:dict>
        <s:dict>
          <s:key name="password">S18prTuY3vRMg==</s:key>
          <s:key name="password">********</s:key>
          <s:key name="realm"></s:key>
          <s:key name="username">testuser</s:key>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
POST

Create/update new credentials.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td><strong>Required</strong>. Credentials username.</td>
</tr>
<tr>
<td>password</td>
<td>String</td>
<td><strong>Required</strong>. Credentials user password.</td>
</tr>
<tr>
<td>realm</td>
<td>String</td>
<td>Credentials realm.</td>
</tr>
</tbody>
</table>

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear_password</td>
<td>Clear text password.</td>
</tr>
<tr>
<td>encr_password</td>
<td>Encrypted, stored password.</td>
</tr>
<tr>
<td>password</td>
<td>Password mask, always ********.</td>
</tr>
<tr>
<td>realm</td>
<td>Realm in which credentials are valid.</td>
</tr>
<tr>
<td>username</td>
<td>Username associated with credentials.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/passwords -d name=user1 -d password=changeme2

**XML Response**

```
<title>passwords</title>

<id>https://localhost:8089/services/storage/passwords</id>
<generator build="200839" version="6.1"/>

<title>user1</title>

<id>https://localhost:8089/servicesNS/nobody/search/storage/passwords/%7Buser1%7D</id>
```
storage/passwords/{name}

https://<host>:<mPort>/services/storage/passwords/{name}

Update, delete, or list credentials for the {name} user.

Authorization

The admin_all_objects capability is required for the DELETE and POST operations. The list_storage_passwords capability is required for the GET operation.
DELETE

Delete the specified user credentials.

Usage details
The `{name}` portion of the URL must be bounded by the colon (:) symbol as in this example.

/services/storage/passwords/:uname:

Request parameters
None

Response keys
Returns a list of the remaining credentials in the `{name}` namespace.

Example request and response

XML Request

curl -k -u admin:changeme --request DELETE
https://localhost:8089/servicesNS/nobody/search/storage/passwords/:user1:

XML Response

<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

GET

Access the specified user credentials.

Request parameters
None

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>

189
<table>
<thead>
<tr>
<th>clear_password</th>
<th>Clear text password.</th>
</tr>
</thead>
<tbody>
<tr>
<td>encr_password</td>
<td>Encrypted, stored password.</td>
</tr>
<tr>
<td>password</td>
<td>Password mask, always ********.</td>
</tr>
<tr>
<td>realm</td>
<td>Realm in which credentials are valid.</td>
</tr>
<tr>
<td>username</td>
<td>User name associated with credentials.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/passwords/user1

**XML Response**

```xml
<title>passwords</title>
<id>https://localhost:8089/servicesNS/nobody/search/storage/passwords</id>
<updated>2014-06-30T14:06:04-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/storage/passwords/_new" rel="create"/>
<link href="/services/storage/passwords/_reload" rel="_reload"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>:user1:</title>
  <id>https://localhost:8089/servicesNS/nobody/search/storage/passwords/%3Auser1%3A</id>
  <updated>2014-06-30T14:06:04-07:00</updated>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="list"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="edit"/>
  <link href="/servicesNS/nobody/search/storage/passwords/%3Auser1%3A" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="clear_password">changeme2</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">admin</s:key>
          <s:key name="perms"/>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```
POST

Update the specified user credentials.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
<td>String</td>
<td>User password credential.</td>
</tr>
</tbody>
</table>

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear_password</td>
<td>Clear text password.</td>
</tr>
<tr>
<td>encr_password</td>
<td>Encrypted, stored password.</td>
</tr>
<tr>
<td>password</td>
<td>Password mask, always *******</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>realm</td>
<td>Realm in which credentials are valid.</td>
</tr>
<tr>
<td>username</td>
<td>User name associated with credentials.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/passwords/splunker -d password=changemeAgain
```

**XML Response**

```
<title>passwords</title>
{id>https://localhost:8089/services/storage/passwords</id>
<updated>2014-06-30T14:35:57-07:00</updated>
<author>
  <name>Splunk</name>
</author>
<title>:user1:</title>
{id>https://localhost:8089/servicesNS/nobody/search/storage/passwords/%3Auser1%3A</id>
<updated>2014-06-30T14:35:57-07:00</updated>
<author>
  <name>admin</name>
</author>
<s:dict>
  <s:key name="clear_password">changemeAgain</s:key>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app">search</s:key>
      <s:key name="can_change_perms">1</s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_share_app">1</s:key>
      <s:key name="can_share_global">1</s:key>
      <s:key name="can_share_user">1</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">1</s:key>
      <s:key name="owner">admin</s:key>
      <s:key name="perms">
        <s:dict>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
</s:dict>
```

192
"<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>admin</s:item>
<s:item>power</s:item>
</s:list>
</s:key>
</s:dict>
<s:dict>
<s:key name="removable">1</s:key>
<s:key name="sharing">app</s:key>
</s:dict>
<s:dict>
<s:key name="encr_password">$1$q7nCiWvQY/p0UtMdIYM=</s:key>
<s:key name="password">********</s:key>
<s:key name="realm"></s:key>
<s:key name="username">user1</s:key>
</s:dict>
"
Application endpoints

Application endpoint descriptions

Manage applications.

Usage details

*Review ACL information for an endpoint*

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the *REST API User Manual*.

**Authentication and Authorization**

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select *Settings > Access controls* and click *Users*. To determine the capabilities assigned to a role, select *Settings > Access controls* and click *Roles*.

**App and user context**

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

**Splunk Cloud URL for REST API access**

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

**Managed Splunk Cloud deployments**

Use the following URL for managed deployments. If necessary, submit a support case to open port 8089 on your deployment.

https://<deployment-name>.splunkcloud.com:8089

**Self-service Splunk Cloud deployments**

Use the following URL for self-service deployments. To get the required non-SAML user credentials, submit a support case.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the the *Splunk REST API Tutorials* for more information.
apps/appinstall (deprecated)

https://<host>:<port>/services/apps/appinstall

Install or update an application.

This endpoint is deprecated as of software version 6.6.0. To create an app or see a list of apps, see apps/local in this topic.

POST

Install or update an application from a local file or URL.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required. Full Unix or Windows path of the .tgz or .spl app source file. The path can be on the local disk or a URL.</td>
</tr>
<tr>
<td>update</td>
<td>Boolean</td>
<td>Indicates whether to update installed app.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true = update existing app, overwriting the existing app folder.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false = [Default] install new app.</td>
</tr>
</tbody>
</table>

Response keys

Response might be delayed while app installs.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>location</td>
<td>Installed location $SPLUNK_HOME/etc/apps/&lt;app_name&gt;.</td>
</tr>
<tr>
<td>name</td>
<td>App name.</td>
</tr>
<tr>
<td>source_location</td>
<td>App source file location, the path name request parameter.</td>
</tr>
<tr>
<td>status</td>
<td>Install status.</td>
</tr>
<tr>
<td></td>
<td>installed = Successfully installed.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/apps/appinstall/ -d name=c:/tmp/splunk-dashboard-examples_50.tgz
```

**XML Response**

```
<result></result>
<title></title>
{id>https://localhost:8089/services/apps/appinstall/id
<updated>2014-07-01T09:44:41-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
    <name>Splunk</name>
```
apps/apptemplates

https://<host>:<port>/services/apps/apptemplates

List installed app templates. You can use an app template as the template parameter in a POST to /services/apps/local.
For additional information, see apps/local.

GET

List installed app templates.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

None

Each <entry> element includes a <link> reference to an app template. The barebones and sample_app templates are installed by default.

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/apps/apptemplates

XML Response

<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

<entry>
<title>barebones</title>
</entry>
<s:dict>
<s:key name="eai:acl">
197
</s:key>
</s:dict>
apps/apptemplates/{name}

https://<host>:<port>/services/apps/apptemplates/{name}

Get the {name} app template descriptor.

For additional information, see apps/apptemplates.

GET

Get the {name} app template descriptor.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys
None

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/apps/apptemplates/sample_app

XML Response

```xml
<entry>
   <id>https://localhost:8089/services/apps/apptemplates</id>
   <updated>2014-07-01T09:54:23-07:00</updated>
   <generator build="200839" version="6.1"/>
   <author>
      <name>Splunk</name>
   </author>
   <opensearch:totalResults>1</opensearch:totalResults>
   <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
   <opensearch:startIndex>0</opensearch:startIndex>
</entry>
```
<entry>
<title>sample_app</title>
<id>https://localhost:8089/services/apps/apptemplates/sample_app</id>
<updated>2014-07-01T09:54:23-07:00</updated>
<author>
  <name>system</name>
</author>
<link href="/services/apps/apptemplates/sample_app" rel="alternate"/>
<link href="/services/apps/apptemplates/sample_app" rel="list"/>
<content type="text/xml">
  <s:dict>
    <s:dict name="eai:acl">
      <s:dict>
        <s:dict name="app">
          <s:dict name="can_list">1</s:dict>
          <s:dict name="can_write">1</s:dict>
          <s:dict name="modifiable">0</s:dict>
          <s:dict name="owner">system</s:dict>
          <s:dict name="perms">
            <s:dict name="read">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:dict>
            <s:dict name="write">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:dict>
          </s:dict>
        </s:dict>
        <s:dict name="removable">0</s:dict>
        <s:dict name="sharing">system</s:dict>
      </s:dict>
    </s:dict>
    <s:dict name="eai:attributes">
      <s:dict name="optionalFields">
        <s:list/>
      </s:dict>
      <s:dict name="requiredFields">
        <s:list/>
      </s:dict>
      <s:dict name="wildcardFields">
        <s:list/>
      </s:dict>
    </s:dict>
    <s:dict name="lol">wut</s:dict>
  </s:dict>
</content>
</entry>

apps/local

https://<host>:<port>/services/apps/local
Create an app or list installed apps and properties.

The capabilities that this endpoint requires change based on the enable_install_apps setting in limits.conf. If this setting is true, the install_apps and edit_local_apps settings are required. If this setting is false, the admin_all_objects capability is required. By default, this setting value is false but you can change it on your system to improve security.

GET

List installed apps and properties.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Response keys**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>author</strong></td>
<td>App author and optional contact information. For apps deployed on Splunkbase, the Splunkbase account username.</td>
</tr>
<tr>
<td><strong>check_for_updates</strong></td>
<td>Indicates whether to check for updates. true = Check Splunkbase for app updates. false = Do not check Splunkbase for app updates.</td>
</tr>
<tr>
<td><strong>configured</strong></td>
<td>Custom setup complete indication: true = Custom app setup complete. false = Custom app setup not complete.</td>
</tr>
<tr>
<td><strong>description</strong></td>
<td>App description.</td>
</tr>
<tr>
<td><strong>details</strong></td>
<td>URL to use for detailed information about the app.</td>
</tr>
<tr>
<td><strong>disabled</strong></td>
<td>App state indication. true = App is disabled. false = App is enabled.</td>
</tr>
<tr>
<td><strong>label</strong></td>
<td>App name.</td>
</tr>
<tr>
<td><strong>state_change_requires_restart</strong></td>
<td>Indicates whether to require restart on state change. true = App state change requires restart. false = App state change might not require restart depending on other restart requirements.</td>
</tr>
<tr>
<td><strong>version</strong></td>
<td>App version.</td>
</tr>
<tr>
<td><strong>visible</strong></td>
<td>Indicates whether app is visible and navigable from Splunk Web. true = App is visible and navigable. false = App is not visible and navigable.</td>
</tr>
</tbody>
</table>

**Application usage**

Splunkbase can correlate locally-installed apps with the same app on Splunkbase for update notifications.

**Example request and response**

**XML Request**

```xml
201```
curl -k -u admin:changeme https://localhost:8089/services/apps/local

XML Response

<title>localapps</title>
<id>https://localhost:17001/services/apps/local</id>
<updated>2015-10-13T17:53:03-07:00</updated>
<generator build="a1c9b1f0dcf9" version="6.3.0"/>
<author>
 <name>Splunk</name>
</author>

<title>alert_logevent</title>
<id>https://localhost:17001/servicesNS/nobody/system/apps/local/alert_logevent</id>
<updated>2015-10-13T17:53:03-07:00</updated>
<author>
 <name>nobody</name>
</author>

<s:dict>
 <s:key name="author">Splunk</s:key>
 <s:key name="check_for_updates">1</s:key>
 <s:key name="configured">1</s:key>
 <s:key name="core">1</s:key>
 <s:key name="description">Log Event Alert Action</s:key>
 <s:key name="disabled">0</s:key>
 <s:key name="eai:acl"/>
 <s:dict>
  <s:key name="app">system</s:key>
  <s:key name="can_change_perms">1</s:key>
  <s:key name="can_list">1</s:key>
  <s:key name="can_share_app">1</s:key>
  <s:key name="can_share_global">1</s:key>
  <s:key name="can_share_user">0</s:key>
  <s:key name="can_write">1</s:key>
  <s:key name="modifiable">1</s:key>
  <s:key name="owner">nobody</s:key>
  <s:key name="perms">
   <s:dict>
    <s:key name="read">
     <s:list>
      <s:item>*</s:item>
     </s:list>
    </s:key>
    <s:key name="write">
     <s:list>
      <s:item>202</s:item>
     </s:list>
    </s:key>
   </s:dict>
  </s:dict>
 </s:dict>
</s:dict>
<s:dict>
  <s:key name="author">Splunk</s:key>
  <s:key name="check_for_updates">1</s:key>
  <s:key name="configured">1</s:key>
  <s:key name="core">1</s:key>
  <s:key name="description">Webhook Alert Action</s:key>
  <s:key name="disabled">0</s:key>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app">system</s:key>
      <s:key name="can_change_perms">1</s:key>
      <s:key name="can_change_perms">1</s:key>
      <s:key name="can_share_app">1</s:key>
      <s:key name="can_share_global">1</s:key>
      <s:key name="can_share_user">0</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">1</s:key>
      <s:key name="owner">nobody</s:key>
      <s:key name="perms">
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:key>
          <s:key name="write">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
</s:dict>
<s:dict>
    <s:key name="check_for_updates">1</s:key>
    <s:key name="configured">0</s:key>
    <s:key name="core">1</s:key>
    <s:key name="disabled">0</s:key>
    <s:key name="eai:acl">
        <s:dict>
            <s:key name="app">system</s:key>
            <s:key name="can_change_perms">1</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_share_app">1</s:key>
            <s:key name="can_share_global">1</s:key>
            <s:key name="can_share_user">0</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">1</s:key>
            <s:key name="owner">nobody</s:key>
            <s:key name="perms">
                <s:dict>
                    <s:key name="read">
                        <s:list>
                            <s:item>*</s:item>
                        </s:list>
                    </s:key>
                    <s:key name="write">
                        <s:list>
                            <s:item>*</s:item>
                        </s:list>
                    </s:key>
                </s:dict>
            </s:key>
        </s:dict>
    </s:key>
    <s:key name="removable">0</s:key>
    <s:key name="sharing">app</s:key>
</s:dict>
<s:dict>
  <s:key name="label">Getting started</s:key>
  <s:dict name="eai:acl">
    <s:dict name="author">system</s:dict>
    <s:dict name="can_change_perms">1</s:dict>
    <s:dict name="can_share_app">1</s:dict>
    <s:dict name="can_share_global">1</s:dict>
    <s:dict name="can_share_user">0</s:dict>
    <s:dict name="can_write">1</s:dict>
    <s:dict name="modifiable">1</s:dict>
    <s:dict name="owner">nobody</s:dict>
    <s:dict name="perms">
      <s:dict name="read">
        <s:list>
          <s:item>*</s:item>
        </s:list>
      </s:dict>
      <s:dict name="write">
        <s:list>
          <s:item>power</s:item>
        </s:list>
      </s:dict>
    </s:dict>
  </s:dict>
  <s:dict name="sharing">
    <s:dict name="app">nobody</s:dict>
  </s:dict>
  <s:key name="author">Splunk</s:key>
  <s:key name="check_for_updates">1</s:key>
  <s:key name="configured">1</s:key>
  <s:key name="core">1</s:key>
  <s:key name="description">Get started with Splunk. This app introduces you to many of Splunk's features. You'll learn how to use Splunk to index data, search and investigate, add knowledge, monitor and alert, report and analyze.</s:key>
  <s:key name="disabled">1</s:key>
  <s:dict name="framework">
    <s:dict name="managed_by_deployment_client">0</s:dict>
    <s:dict name="show_in_nav">1</s:dict>
    <s:dict name="state_change_requires_restart">0</s:dict>
    <s:dict name="visible">0</s:dict>
  </s:dict>
  <s:dict name="state_change_requires_restart">0</s:dict>
  <s:key name="visible">0</s:key>
</s:dict>
POST

Create an app.

Usage details

- Splunkbase can correlate locally installed apps with the same app on Splunkbase for update notifications.
- The app folder name cannot include spaces or special characters.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth</td>
<td>String</td>
<td>Splunkbase session token for operations like install and update that require login. Use <code>auth</code> or <code>session</code> when installing or updating an app through Splunkbase.</td>
</tr>
<tr>
<td>author</td>
<td>String</td>
<td>For apps posted to Splunkbase, use your Splunk account username. For internal apps, include your name and contact information.</td>
</tr>
<tr>
<td>configured</td>
<td>Boolean</td>
<td>Custom setup complete indication:</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>true</code> = Custom app setup complete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>false</code> = Custom app setup not complete.</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td>Short app description also displayed below the app title in Splunk Web Launcher.</td>
</tr>
<tr>
<td>explicit_appname</td>
<td>String</td>
<td>Custom app name. Overrides <code>name</code> when installing an app from a file where <code>filename</code> is set to <code>true</code>. See also <code>filename</code>.</td>
</tr>
<tr>
<td>filename</td>
<td>Boolean</td>
<td>Indicates whether to use the <code>name</code> value as the app source location. <code>true</code> indicates that <code>name</code> is a path to a file to install. <code>false</code> indicates that <code>name</code> is the literal app name and that the app is created from Splunkbase using a template.</td>
</tr>
<tr>
<td>label</td>
<td>String</td>
<td>App name displayed in Splunk Web, from five to eighty characters excluding the prefix “Splunk for”.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td><strong>Required.</strong> Literal app name or path for the file to install, depending on the value of <code>filename</code>.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>filename = false</code> indicates that <code>name</code> is the literal app name and that the app is created from Splunkbase using a template.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>filename = true</code> indicates that <code>name</code> is the URL or path to the local <code>.tar</code>, <code>.tgz</code> or <code>.spl</code> file. If <code>name</code> is the Splunkbase URL, set <code>auth</code> or <code>session</code> to authenticate the request.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The app folder name cannot include spaces or special characters.</td>
</tr>
<tr>
<td>session</td>
<td>String</td>
<td>Login session token for installing or updating an app on Splunkbase. Alternatively, use <code>auth</code>.</td>
</tr>
<tr>
<td>template</td>
<td>Enum</td>
<td>App template to use when creating the app.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><code>barebones</code> - [Default] Basic app framework.</td>
</tr>
</tbody>
</table>
### Name | Type | Description
--- | --- | ---
| **sample_app** | Example views and searches. Any custom app template. | 

| **update** | Boolean | File-based update indication: 
true specifies that filename should be used to update an existing app. If not specified, update defaults to false, which indicates that filename should not be used to update an existing app. |

| **version** | String | App version. |

| **visible** | Boolean | Indicates whether the app is visible and navigable from Splunk Web. 
true = App is visible and navigable. 
false = App is not visible or navigable. |

### Response keys

| Name | Description |
--- | --- |
| **author** | For apps posted to Splunkbase, your Splunk account username. For internal apps, your full name and contact information. |

| **check_for_updates** | true = Check Splunkbase for app updates. 
false = Do not check Splunkbase for app updates. |

| **configured** | Custom setup completeness indication. 
true = Custom app setup complete. 
false = Custom app setup not complete. |

| **description** | Brief app description, displayed below the app title in Splunk Web. |

| **disabled** | App state indication. 
true = App is disabled. 
false = App is enabled. |

| **label** | App name displayed in Splunk Web. |

| **name** | Installed app name, which might differ from the POST name parameter. |

| **state_change_requires_restart** | Indicates whether restart required on state change. 
true = App state change requires restart. 
false = App state change might not require restart, depending on other restart requirements. |

| **version** | App version. |

| **visible** | Indicates whether app is visible and navigable from Splunk Web. 
true = App is visible and navigable. 
false = App is not visible or navigable. |

### Example request and response

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local -d name=restDemo
```

**XML Response**

```
<title></title>
/id>https://localhost:8089/services/apps/local/id>
/updated>2014-07-01T10:09:37-07:00</updated>
<generator build="200839" version="6.1"/>
```
<author>
  <name>Splunk</name>
</author>
<link href="/services/apps/local/_new" rel="create"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>restDemo</title>
  <id>https://localhost:8089/servicesNS/nobody/system/apps/local/restDemo</id>
  <updated>2014-07-01T10:09:37-07:00</updated>
  <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="list"/>
  <link href="/servicesNS/nobody/system/apps/local/restDemo" rel="edit"/>
  <link href="/servicesNS/nobody/system/apps/local/restDemo/package" rel="package"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="author"></s:key>
      <s:key name="check_for_updates">1</s:key>
      <s:key name="configured">0</s:key>
      <s:key name="description"></s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">system</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>power</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="label">restDemo</s:key>
      <s:key name="name">restDemo</s:key>
      <s:key name="state_changeRequiresRestart">0</s:key>
      <s:key name="version">1.0</s:key>
      <s:key name="visible">1</s:key>
    </s:dict>
  </content>
</entry>
apps/local/{name}

https://<host>:<port>/services/apps/local/{name}

Manage {name} app. For additional information, see "Uninstall an app" in the Admin Manual.

DELETE
Delete the {name} app.

Usage details
- Use the /apps/local GET method to confirm that the app is no longer installed.
- See "Uninstall an app" for additional manual cleanup that might be needed after deleting an app.

Request parameters
None

Response keys
A message is displayed that might indicate a restart is required.

Specifying the name of a non-existent app returns an error message, as shown below.

In handler 'localapps': Could not find object id=<app_name>.

Example request and response

XML Request

curl -k -u admin:changeme --request DELETE https://localhost:8089/services/apps/local/sample_app

XML Response

210
GET

List information about the {name} app.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>refresh</td>
<td>Boolean</td>
<td>Indicates whether to reload any objects associated with the {name} app indication: true = Reload objects. false = Do not reload objects.</td>
</tr>
</tbody>
</table>

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>author</td>
<td>For apps posted to Splunkbase, your Splunk account username. For internal apps, your full name and contact information.</td>
</tr>
<tr>
<td>check_for_updates</td>
<td>Indicates whether to check for updates. true = Check Splunkbase for app updates. false = Do not check Splunkbase for app updates.</td>
</tr>
<tr>
<td>configured</td>
<td>Custom setup completeness indication. true = Custom app setup complete. false = Custom app setup not complete.</td>
</tr>
<tr>
<td>description</td>
<td>Brief app description also displayed below the app title in Splunk Web.</td>
</tr>
<tr>
<td>disabled</td>
<td>App state indication: true = App is disabled. false = App is enabled.</td>
</tr>
<tr>
<td>label</td>
<td>App name displayed in Splunk Web, from five to 80 characters and excluding the prefix “Splunk For”.</td>
</tr>
<tr>
<td>state_change_requires_restart</td>
<td>Indicates whether restart is required on state change indication: true = App state change requires restart. false = App state change might not require restart, depending on other restart requirements.</td>
</tr>
<tr>
<td>version</td>
<td>App version.</td>
</tr>
<tr>
<td>visible</td>
<td>App is visible and navigable from Splunk Web indication: true = App is visible and navigable. false = App is not visible or navigable.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/apps/local/dashboard_examples

XML Response

211
<title>dashboard_examples</title>

{id>https://localhost:8089/servicesNS/nobody/system/apps/local/dashboard_examples</id>

<updated>2014-07-01T10:23:46-07:00</updated>

<generator build="200839" version="6.1"/>

<author>
  <name>nobody</name>
</author>

<link href="/servicesNS/nobody/system/apps/local/dashboard_examples" rel="create"/>
<link href="/servicesNS/nobody/system/apps/local/dashboard_examples/_new" rel="_new"/>
<link href="/servicesNS/nobody/system/apps/local/dashboard_examples/_reload" rel="_reload"/>

<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>

<entry>
  <title>dashboard_examples</title>
  <id>https://localhost:8089/servicesNS/nobody/system/apps/local/dashboard_examples</id>
  <updated>2014-07-01T10:23:46-07:00</updated>
  <link href="/servicesNS/nobody/system/apps/local/dashboard_examples" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/apps/local.dashboard_examples/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/apps/local.dashboard_examples" rel="edit"/>
  <link href="/servicesNS/nobody/system/apps/local/dashboard_examples/remove" rel="remove"/>
  <link href="/servicesNS/nobody/system/apps/local/dashboard_examples/disable" rel="disable"/>
  <link href="/servicesNS/nobody/system/apps/local/dashboard_examples/package" rel="package"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="author">Splunk, Inc.</s:key>
      <s:key name="check_for_updates">1</s:key>
      <s:key name="configured">0</s:key>
      <s:key name="description">Example dashboards, forms, and views for Splunk 5+. This is the successor app to UI Examples 4.1+. Splunk Dashboard Examples contains over 50 examples updated for Splunk 5. Each example contains inline documentation to help get you started building Splunk dashboards.</s:description>
      <s:key name="details">https://splunkbase.splunk.com/apps/id/dashboard_examples</s:details>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl"/>
      <s:dict>
        <s:key name="app">system</s:key>
        <s:key name="can_change_perms">1</s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_share_app">1</s:key>
        <s:key name="can_share_global">1</s:key>
        <s:key name="can_share_user">0</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">1</s:key>
        <s:key name="owner">nobody</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">*</s:read>
          </s:dict>
        </s:key>
        <s:dict>
          <s:key name="write">*</s:write>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
POST

Update the {name} app properties. Append /enable or /disable to enable or disable the app. See Enable and disable endpoint for more information.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>author</td>
<td>String</td>
<td>For apps posted to Splunkbase, use your Splunk account username. For internal apps, use your full name and contact information.</td>
</tr>
<tr>
<td>check_for_updates</td>
<td>Boolean</td>
<td>Check for updates indicator. true = Check Splunkbase for app updates. false = Do not check Splunkbase for app updates.</td>
</tr>
<tr>
<td>configured</td>
<td>Boolean</td>
<td>Custom setup completion indicator. true = Custom app setup complete. false = Custom app setup not complete.</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td>Short app description also displayed below the app title in Splunk Web.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>label</td>
<td>String</td>
<td>App name displayed in Splunk Web, from five to 80 characters and excluding the prefix “Splunk For”.</td>
</tr>
<tr>
<td>version</td>
<td>String</td>
<td>App version.</td>
</tr>
<tr>
<td>visible</td>
<td>Boolean</td>
<td>Indicates whether app is visible and navigable from Splunk Web.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true = App is visible and navigable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false = App is not visible and navigable.</td>
</tr>
</tbody>
</table>

### Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>author</td>
<td>For apps posted to Splunkbase, your Splunk account username. For internal apps, your full name and contact information.</td>
</tr>
<tr>
<td>check_for_updates</td>
<td>Check for updates indication:</td>
</tr>
<tr>
<td></td>
<td>true = Check Splunkbase for app updates.</td>
</tr>
<tr>
<td></td>
<td>false = Do not check Splunkbase for app updates.</td>
</tr>
<tr>
<td>configured</td>
<td>Custom setup completion indicator.</td>
</tr>
<tr>
<td></td>
<td>true = Custom app setup complete.</td>
</tr>
<tr>
<td></td>
<td>false = Custom app setup not complete.</td>
</tr>
<tr>
<td>description</td>
<td>App description also displayed below the app title in Splunk Web.</td>
</tr>
<tr>
<td>disabled</td>
<td>App state indication.</td>
</tr>
<tr>
<td></td>
<td>true = App is disabled.</td>
</tr>
<tr>
<td></td>
<td>false = App is enabled.</td>
</tr>
<tr>
<td>label</td>
<td>App name displayed in Splunk Web, from five to 80 characters and excluding the prefix “Splunk For”.</td>
</tr>
<tr>
<td>state_change_requires_restart</td>
<td>Restart required on state change indication:</td>
</tr>
<tr>
<td></td>
<td>true = App state change requires restart.</td>
</tr>
<tr>
<td></td>
<td>false = App state change might not require restart, depending on other restart requirements.</td>
</tr>
<tr>
<td>version</td>
<td>App version.</td>
</tr>
<tr>
<td>visible</td>
<td>Indicator of whether app is visible and navigable from Splunk Web.</td>
</tr>
<tr>
<td></td>
<td>true = App is visible and navigable.</td>
</tr>
<tr>
<td></td>
<td>false = App is not visible or navigable.</td>
</tr>
</tbody>
</table>

### Example request and response

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local/restDemo -d version=1.1
```

**XML Response**

```
```
<link href="/services/apps/local/_new" rel="create"/>
<link href="/services/apps/local/_reload" rel="_reload"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>restDemo</title>
<id>https://localhost:8089/servicesNS/nobody/system/apps/local/restDemo/id</id>
<updated>2014-07-01T10:28:35-07:00</updated>
<link href="/servicesNS/nobody/system/apps/local/restDemo" rel="alternate"/>
<author>
 <name>nobody</name>
</author>
<link href="/servicesNS/nobody/system/apps/local/restDemo" rel="list"/>
<link href="/servicesNS/nobody/system/apps/local/restDemo/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/system/apps/local/restDemo" rel="edit"/>
<link href="/servicesNS/nobody/system/apps/local/restDemo" rel="remove"/>
<link href="/servicesNS/nobody/system/apps/local/restDemo/package" rel="package"/>
<content type="text/xml">
<s:dict>
 <s:key name="author"></s:key>
 <s:key name="check_for_updates">1</s:key>
 <s:key name="configured">0</s:key>
 <s:key name="description"></s:key>
 <s:key name="disabled">0</s:key>
 <s:key name="eai:acl">
   <s:dict>
     <s:key name="app">system</s:key>
     <s:key name="can_change_perms">1</s:key>
     <s:key name="can_list">1</s:key>
     <s:key name="can_share_app">1</s:key>
     <s:key name="can_share_global">1</s:key>
     <s:key name="can_share_user">0</s:key>
     <s:key name="can_write">1</s:key>
     <s:key name="modifiable">1</s:key>
     <s:key name="owner">nobody</s:key>
     <s:key name="perms">
       <s:dict>
         <s:dict>
           <s:key name="read">
             <s:list>
               <s:item>*</s:item>
             </s:list>
           </s:key>
           <s:dict>
             <s:key name="write">
               <s:list>
                 <s:item>admin</s:item>
                 <s:item>power</s:item>
               </s:list>
             </s:key>
           </s:dict>
         </s:dict>
         <s:dict>
           <s:key name="removable">0</s:key>
           <s:key name="sharing">app</s:key>
         </s:dict>
       </s:dict>
       <s:key name="label">restDemo</s:key>
       <s:key name="state_change_requires_restart">0</s:key>
       <s:key name="version">1.1</s:key>
       <s:key name="visible">1</s:key>
     </s:dict>
   </s:dict>
 </s:key>
</s:dict>
</content>
apps/local/{name}/package

https://<host>:<port>/services/apps/local/{name}/package
Archive the {name} app as a .spl file in the $SPLUNK_HOME/etc/system/static/app-packages directory.

GET
Archive the {name}.spl app.

Usage details
Download the archived app using the following URL:

https://host:<port>/static/app-packages/{name}.spl

Request parameters
None

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>App name and name of the folder containing the app.</td>
</tr>
<tr>
<td>path</td>
<td>Local path to an archive of the app.</td>
</tr>
<tr>
<td>url</td>
<td>App download URL.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/apps/local/restDemo/package
```

XML Response

```
<title></title>

```
216
<entry>
<title>Package</title>
<id>https://localhost:8089/services/apps/local/Package</id>
<updated>2014-07-01T10:46:43-07:00</updated>
<link href="/services/apps/local/Package" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/apps/local/Package/setup" rel="edit"/>
<content type="text/xml">
  <s:dict>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app"></s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">0</s:key>
        <s:key name="owner">system</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="removable">0</s:key>
        <s:key name="sharing">system</s:key>
      </s:dict>
    </s:key>
    <s:key name="name">restDemo</s:key>
    <s:key name="path">C:\Program Files\Splunk\etc\system\static\app-packages\restDemo.spl</s:key>
    <s:key name="url">https://localhost:8089/static/app-packages/restDemo.spl</s:key>
  </s:dict>
</content>
</entry>

Get the {name} app setup information.

https://<host>:<port>/services/apps/local/{name}/setup
GET
Get setup information for the \{name\} app.

Usage details
Some apps contain setup scripts that must be run before the app is enabled. For those apps, the setup.xml file must exist in the $SPLUNK_BASE\etc\apps\<appname>\default directory.

Request parameters
None

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;script location&gt;</td>
<td>TBD</td>
</tr>
<tr>
<td>eai:setup</td>
<td>CDATA setup script location.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/apps/local/unix/setup

XML Response

```xml
... elided ...
```
<s:key name="/admin/script/.%252Fbin%252Fwho.sh/interval">150</s:key>
... eai:acl element elided ...
... eai:attributes element elided ...
<s:key name="eai:setup">
<![CDATA[<?xml version="1.0" encoding="UTF-8"?> <SetupInfo> <block title="Welcome to the Splunk for nix App"> <text>The Splunk for nix app provides some sample searches and reports to boot-strap your use of Splunk for Unix host management. To work, it needs certain inputs enabled. These system metrics drive the sample dashboards. Please review and confirm the inputs below before proceeding. </text> </block> <block title="CPU Stats (sar / mpstat / etc.)" endpoint="admin/script" entity=".%252Fbin%252Fcpu.sh"> <input field="interval" id="/admin/script/.%252Fbin%252Fcpu.sh/interval"> <label>Polling Interval (sec)</label> <type>text</type> </input> <input field="enabled" id="/admin/script/.%252Fbin%252Fcpu.sh/enabled"> <label>Enable</label> <type>bool</type> </input> </block> ...

<block title="Time Query (date, ntpdate -q)" endpoint="admin/script" entity=".%252Fbin%252Ftime.sh"> <input field="interval" id="/admin/script/.%252Fbin%252Ftime.sh/interval"> <label>Polling Interval (sec)</label> <type>text</type> </input> <input field="enabled" id="/admin/script/.%252Fbin%252Ftime.sh/enabled"> <label>Enable</label> <type>bool</type> </input> </block> <block title="Linux Audit Log (/var/log/audit/audit.log | ausearch)" endpoint="admin/script" entity=".%252Fbin%252Frlog.sh"> <input field="interval" id="/admin/script/.%252Fbin%252Frlog.sh/interval"> <label>Polling Interval (sec)</label> <type>text</type> </input> <input field="enabled" id="/admin/script/.%252Fbin%252Frlog.sh/enabled"> <label>Enable</label> <type>bool</type> </input> </block> <block title="Warning"> <text>Submitting this form can take a long time. Please be patient and wait for it to complete before navigating away from this page. </text> </block> </SetupInfo> ]]> </s:dict>
</content>
</entry>

**apps/local/{name}/update**

https://<host>:<port>/services/apps/local/{name}/update

Get eai:acl information for the {name} app.

**GET**

Get {name} app eai:acl information.

**Request parameters**

None

**Response keys**

The eai:acl key of the {name} app.

**Example request and response**

**XML Request**

curl -k -u admin:changeme https://localhost:8089/services/apps/local/gettingstarted/update
<title>localapps</title>

$id$https://localhost:8089/services/apps/local</id>


<generator build="200839" version="6.1"/>

<author>

<name>Splunk</name>

</author>

<link href="/services/apps/local/_new" rel="create"/>

<link href="/services/apps/local/_reload" rel="_reload"/>

<opensearch:totalResults>1</opensearch:totalResults>

<opensearch:itemsPerPage>30</opensearch:itemsPerPage>

<opensearch:startIndex>0</opensearch:startIndex>

<entry>

<title>gettingstarted</title>

$id$https://localhost:8089/services/apps/local/gettingstarted</id>


<link href="/services/apps/local/gettingstarted" rel="alternate"/>

<author>

<name>system</name>

</author>

<link href="/services/apps/local/gettingstarted/_new" rel="create"/>

<link href="/services/apps/local/gettingstarted/_reload" rel="_reload"/>

<link href="/services/apps/local/gettingstarted/_edit" rel="edit"/>

<link href="/services/apps/local/gettingstarted" rel="remove"/>

<content type="text/xml">

<s:dict>

<s:key name="eai:acl">

<s:dict>

<s:key name="app"></s:key>

<s:key name="can_list">1</s:key>

<s:key name="can_write">1</s:key>

<s:key name="modifiable">0</s:key>

<s:key name="owner">system</s:key>

<s:key name="perms">

<s:dict>

<s:key name="read">

<s:list>*</s:list>

</s:dict>

<s:dict>

<s:key name="write">

<s:list>

<s:item>admin</s:item>

<s:item>splunk-system-role</s:item>

</s:list>

</s:dict>

<s:dict>

<s:key name="removable">0</s:key>

<s:key name="sharing">system</s:key>

</s:dict>

</s:dict>

</s:dict>

</s:dict>

</content>

</entry>
Cluster endpoints

Cluster endpoint descriptions

Manage indexer clusters and search head clusters in Splunk Enterprise.

To distinguish indexer cluster endpoints from search cluster endpoints, note:

- **Indexer cluster endpoints**: Endpoints that contain `cluster` in their URIs pertain to indexer clusters.
- **Search head cluster endpoints**: Endpoints that contain `shcluster` in their URIs pertain to search head clusters.

Usage details

**Review ACL information for an endpoint**

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the REST API User Manual.

**Authentication and Authorization**

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings > Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings > Access controls** and click **Roles**.

**App and user context**

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

**Splunk Cloud limitations**

If you have a managed Splunk Cloud deployment with search head clustering and index clustering, the REST API supports access to the search head only. You can use the REST API to interact with the search head in your deployment. Using the REST API to access any other indexer cluster nodes is not supported. For example, index cluster management endpoints are not applicable to Splunk Cloud deployments.

Authorized users can access and configure other indexer cluster nodes, including indexer or cluster master, or license master nodes, in the Splunk Cloud manager user interface.

**Indexer cluster endpoints**

The endpoints in this section pertain to **indexer clusters**.

All endpoints that contain `cluster` in their URIs pertain to indexer clusters. In this section, if a URI contains the term `search head`, it refers to search head nodes in the indexer cluster. The term `peer node` refers to peer nodes in the indexer cluster. For more information about indexer cluster architecture, see The basics of indexer cluster architecture.
and Search head configuration overview in the *Managing Indexers and Clusters of Indexers* manual.

### cluster/config

https://<host>:<mPort>/services/cluster/config

Access cluster node configuration details.

**GET**

List cluster node configuration.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cxn_timeout</td>
<td>Low-level timeout, in seconds, for establishing connection between cluster nodes. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this node is disabled.</td>
</tr>
<tr>
<td>forwarderdata_rcv_port</td>
<td>The port from which to receive data from a forwarder.</td>
</tr>
<tr>
<td>forwarderdata_use_ssl</td>
<td>Indicates whether to use SSL when receiving data from a forwarder.</td>
</tr>
<tr>
<td>heartbeat_period</td>
<td>Only valid for peer nodes in a cluster. The time, in seconds, that a peer attempts to send a heartbeat to the master</td>
</tr>
<tr>
<td>heartbeat_timeout</td>
<td>Only valid for the master node in a cluster configuration. The time, in seconds, before a master considers a peer down. Once a peer is down, the master initiates steps to replicate buckets from the dead peer to its live peers. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>master_uri</td>
<td>Valid only for nodes configured as a peer or searchhead. URI of the cluster master to which this node connects.</td>
</tr>
<tr>
<td>max_peer_build_load</td>
<td>The number of jobs that a peer can have in progress at any time that make the bucket searchable.</td>
</tr>
<tr>
<td>max_peer_rep_load</td>
<td>Maximum number of replications that can be ongoing as a target.</td>
</tr>
<tr>
<td>mode</td>
<td>Valid values: (master</td>
</tr>
<tr>
<td>ping_flag</td>
<td>For internal use to facilitate communication between the master and peers.</td>
</tr>
<tr>
<td>quiet_period</td>
<td>The time, in seconds, that a master waits for peers to add themselves to the cluster.</td>
</tr>
<tr>
<td>rcv_timeout</td>
<td>Low-level timeout, in seconds, for receiving data between cluster nodes. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>register_forwarder_address</td>
<td>Not used.</td>
</tr>
<tr>
<td>register_replication_address</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>register_search_address</td>
<td>IP address that advertises this indexer to search heads.</td>
</tr>
<tr>
<td>rep_cxn_timeout</td>
<td>Low-level timeout, in seconds, for establishing a connection for replicating data.</td>
</tr>
<tr>
<td>rep_max_rcv_timeout</td>
<td>Maximum cumulative time, in seconds, for receiving acknowledgement data from peers. Defaults to 600s.</td>
</tr>
<tr>
<td>rep_max_send_timeout</td>
<td>Maximum time, in seconds, for sending replication slice data between cluster nodes. Defaults to 600s.</td>
</tr>
<tr>
<td>rep_rcv_timeout</td>
<td>Low-level timeout, in seconds, for receiving data between cluster nodes.</td>
</tr>
<tr>
<td>rep_send_timeout</td>
<td>Low-level timeout, in seconds, for sending replication data between cluster nodes. Defaults to 5 seconds.</td>
</tr>
<tr>
<td>replication_factor</td>
<td>Only valid for nodes configured as a master. Determines how many copies of raw data are created in the cluster. This could be less than the number of cluster peers. Must be greater than 0 and greater than or equal to the search factor. Defaults to 3.</td>
</tr>
<tr>
<td>replication_port</td>
<td>TCP port to listen for replicated data from another cluster member.</td>
</tr>
<tr>
<td>replication_use_ssl</td>
<td>Indicates whether to use SSL when sending replication data.</td>
</tr>
<tr>
<td>restart_timeout</td>
<td>Only valid for nodes configured as a master. The amount of time, in seconds, the master waits for a peer to come back when the peer is restarted (to avoid the overhead of trying to fix the buckets that were on the peer). Defaults to 600 seconds.</td>
</tr>
<tr>
<td>search_factor</td>
<td>Only valid for nodes configured as a master. Determines how many searchable copies of each bucket to maintain. Must be less than or equal to replication_factor and greater than 0. Defaults to 2.</td>
</tr>
<tr>
<td>secret</td>
<td>Secret shared among the nodes in the cluster to prevent any arbitrary node from connecting to the cluster. If a peer or searchhead is not configured with the same secret as the master, it is not able to communicate with the master. Corresponds to pass4SymmKey setting in server.conf.</td>
</tr>
<tr>
<td>send_timeout</td>
<td>Low-level timeout, in seconds, for sending data between cluster nodes. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>summary_replication</td>
<td>Boolean indicator of whether summary replication is on or off. A true value means that it is turned on.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/cluster/config

**XML Response**

```xml
<title>clusterconfig</title>
<id>https://localhost:8089/services/cluster/config</id>
<updated>2012-09-05T10:19:49-07:00</updated>
<generator build="136169" version="5.0"/>
<author>
```
cluster/config/config

https://<host>:<mPort>/services/cluster/config/config
Manage cluster node configuration details.
GET

List cluster node configuration.

This operation works identically to the GET on `cluster/config`.

POST

Manage configuration details.

See Indexer cluster configuration overview in *Managing Indexers and Clusters of Indexers* and the `[clustering]` stanza options in the server.conf spec file for more details on indexer cluster configuration.

### Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>available_sites</td>
<td>N/A</td>
<td>Sets the various sites that are recognized for this master. Valid values include site1 to site64.</td>
</tr>
<tr>
<td>cluster_label</td>
<td>String</td>
<td>Label for this cluster.</td>
</tr>
<tr>
<td>cxn_timeout</td>
<td>Number</td>
<td>Low-level timeout, in seconds, for establishing connection between cluster nodes. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>heartbeat_period</td>
<td>Number</td>
<td>Only valid for peer nodes in a cluster. Time, in seconds, that a peer attempts to send a heartbeat to the master</td>
</tr>
<tr>
<td>heartbeat_timeout</td>
<td>Number</td>
<td>Only valid for the master node in a cluster configuration. Time, in seconds, before a master considers a peer down. Once a peer is down, the master initiates steps to replicate buckets from the dead peer to its live peers. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>master_uri</td>
<td>URI</td>
<td>Valid only for nodes configured as a peer or searchhead. URI of the cluster master to which this node connects.</td>
</tr>
<tr>
<td>max_peer_build_load</td>
<td>Number</td>
<td>The number of jobs that a peer can have in progress at any time that make the bucket searchable.</td>
</tr>
<tr>
<td>max_peer_rep_load</td>
<td>Number</td>
<td>Maximum number of replications that can be ongoing as a target.</td>
</tr>
<tr>
<td>mode</td>
<td>See description.</td>
<td>Required. Valid values: (master</td>
</tr>
<tr>
<td>multisite</td>
<td>Boolean</td>
<td>Enable or disable the multisite feature for this cluster.</td>
</tr>
<tr>
<td>notify_scan_period</td>
<td>Non-zero number</td>
<td>Controls the frequency that the indexer scans summary folders for summary updates. Only used when <code>summary_replication</code> is enabled on the Master. Defaults to 10 seconds.</td>
</tr>
<tr>
<td>ping_flag</td>
<td>N/A</td>
<td>For internal use to facilitate communication between the master and peers.</td>
</tr>
<tr>
<td>quiet_period</td>
<td>Number</td>
<td>The time, in seconds, that a master waits for peers to add themselves to the cluster.</td>
</tr>
<tr>
<td>rcv_timeout</td>
<td>Number</td>
<td>Low-level timeout, in seconds, for receiving data between cluster nodes. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>register_forwarder_address</td>
<td>N/A</td>
<td>Reserved for future use.</td>
</tr>
<tr>
<td>register_replication_address</td>
<td>See description.</td>
<td>Valid only for nodes configured as peers. The address on which a peer is available for accepting replication data. This is useful in the cases where a peer host machine has multiple interfaces and only one of them can be reached by another splunkd instance.</td>
</tr>
<tr>
<td>Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>register_search_address</td>
<td>N/A</td>
<td>IP address that advertises this indexer to search heads.</td>
</tr>
<tr>
<td>rep_cxn_timeout</td>
<td>Number</td>
<td>Low-level timeout, in seconds, for establishing a connection for replicating data.</td>
</tr>
<tr>
<td>rep_max_rcv_timeout</td>
<td>Number</td>
<td>Maximum cumulative time, in seconds, for receiving acknowledgement data from peers. Defaults to 600s.</td>
</tr>
<tr>
<td>rep_max_send_timeout</td>
<td>Number</td>
<td>Maximum time, in seconds, for sending replication slice data between cluster nodes. Defaults to 600s.</td>
</tr>
<tr>
<td>rep_rcv_timeout</td>
<td>Number</td>
<td>Low-level timeout, in seconds, for receiving data between cluster nodes.</td>
</tr>
<tr>
<td>rep_send_timeout</td>
<td>Number</td>
<td>Low-level timeout, in seconds, for sending replication data between cluster nodes. Defaults to 5 seconds.</td>
</tr>
<tr>
<td>replication_factor</td>
<td>Number</td>
<td>Only valid for nodes configured as a master. Determines how many copies of raw data are created in the cluster. This could be less than the number of cluster peers. Must be greater than 0 and greater than or equal to the search factor. Defaults to 3.</td>
</tr>
<tr>
<td>replication_port</td>
<td>Number</td>
<td>TCP port to listen for replicated data from another cluster member.</td>
</tr>
<tr>
<td>replication_use_ssl</td>
<td>Number</td>
<td>Indicates whether to use SSL when sending replication data.</td>
</tr>
<tr>
<td>restart_timeout</td>
<td>Number</td>
<td>Only valid for nodes configured as a master. The amount of time, in seconds, the master waits for a peer to come back when the peer is restarted (to avoid the overhead of trying to fix the buckets that were on the peer). Defaults to 600 seconds.</td>
</tr>
<tr>
<td>search_factor</td>
<td>Number</td>
<td>Only valid for nodes configured as a master. Determines how many searchable copies of each bucket to maintain. Must be less than or equal to replication_factor and greater than 0. Defaults to 2.</td>
</tr>
<tr>
<td>secret</td>
<td>N/A</td>
<td>Secret shared among the nodes in the cluster to prevent any arbitrary node from connecting to the cluster. If a peer or searchhead is not configured with the same secret as the master, it is not able to communicate with the master. Corresponds to pass4SymmKey setting in server.conf.</td>
</tr>
<tr>
<td>send_timeout</td>
<td>Number</td>
<td>Low-level timeout, in seconds, for sending data between cluster nodes. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>site</td>
<td>N/A</td>
<td>Site ID for slave/searchhead indexer. Valid values include site1 to site64.</td>
</tr>
<tr>
<td>site_replication_factor</td>
<td>Number</td>
<td>Replication factor for a multisite configuration.</td>
</tr>
<tr>
<td>site_search_factor</td>
<td>Number</td>
<td>Search factor for a multisite configuration.</td>
</tr>
<tr>
<td>summary_replication</td>
<td>Boolean</td>
<td>Enable or disable summary replication.</td>
</tr>
<tr>
<td>use_batch_mask_changes</td>
<td>Boolean</td>
<td>Only valid for mode-master. Specifies if the master should process bucket mask changes in batch or individually one by one. Defaults to true. Set to false when there are 6.1 peers in the cluster for backwards compatibility.</td>
</tr>
</tbody>
</table>

Response data keys

None.

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8089/services/cluster/config/config -d cxn_timeout=59

XML Response

<title>clusterconfig</title>
{id>https://localhost:8089/services/cluster/config</id>
<updated>2015-12-07T17:09:48-08:00</updated>
<generator build="917abedc8bb44ec1c225a6eb730808a606174cf0" version="20151123"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/config/_reload" rel="_reload"/>
<link href="/services/cluster/config/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

cluster/master/buckets

https://<host>:<mPort>/services/cluster/master/buckets

Provides bucket configuration information for a cluster master node.

GET

List cluster master node bucket configuration.

Request parameters

Use an &summaries=true field in the query string to show summaries.

Use one or more filters in the query string to select buckets or bucket states. For example, use this URL to filter buckets returned for both the main index and StreamingSource status.

https://localhost:8089/services/cluster/master /buckets?filter=index=main&filter=status=StreamingSource

See the following table for available filters.

<table>
<thead>
<tr>
<th>Filter name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>String</td>
<td>Index name.</td>
</tr>
</tbody>
</table>
| status      | String   | Bucket state. Available options are
|             |          | • StreamingSource
|             |          | • StreamingTarget
|             |          | • Complete
|             |          | • StreamingError
|             |          | • PendingTruncate Bucket is scheduled to truncate.
|             |          | • PendingDiscard Bucket is scheduled to discard.
|             |          | • NonStreamingTarget
| search_state| String   | Bucket search state. Available options are

228
### Filter name  
<table>
<thead>
<tr>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>replication_count</td>
<td>Number Use &lt;, &gt;, != or = with numbers to indicate filtering values.</td>
</tr>
<tr>
<td>search_count</td>
<td>Number Use &lt;, &gt;, != or = with numbers to indicate filtering values.</td>
</tr>
<tr>
<td>bucket_size</td>
<td>Number Use &lt;, &gt;, != or = with numbers to indicate filtering values.</td>
</tr>
<tr>
<td>frozen</td>
<td>Boolean Return frozen buckets or non-frozen buckets.</td>
</tr>
<tr>
<td>has_primary</td>
<td>Boolean Return buckets with primaries or without primaries.</td>
</tr>
<tr>
<td>meets_multisite_replication_count</td>
<td>Boolean Return buckets that meet cluster replication policy or buckets that do not meet cluster replication policy.</td>
</tr>
<tr>
<td>meets_multisite_search_count</td>
<td>Boolean Return buckets that meet cluster search policy or buckets that do not meet cluster search policy.</td>
</tr>
<tr>
<td>multisite_bucket</td>
<td>Boolean Return buckets created in multisite mode or buckets not created in multisite mode.</td>
</tr>
<tr>
<td>origin_site</td>
<td>String Site of the indexer where buckets were created.</td>
</tr>
<tr>
<td>standalone</td>
<td>Boolean Use true or 1 to return standalone buckets. Use false or 0 to return clustered buckets.</td>
</tr>
</tbody>
</table>

### Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket_size</td>
<td>Indicates the size, in bytes, of the bucket.</td>
</tr>
<tr>
<td>constrain_to_origin_site</td>
<td>Flag indicating this particular bucket is a clustered pre-multisite bucket. Such buckets are replicated only within their origin site.</td>
</tr>
<tr>
<td>frozen</td>
<td>Indicates if the bucket is frozen.</td>
</tr>
<tr>
<td>index</td>
<td>Name of the index to which the bucket belongs.</td>
</tr>
<tr>
<td>origin_site</td>
<td>Where the bucket originated.</td>
</tr>
<tr>
<td>peers</td>
<td>Lists information about buckets on peers to this master.</td>
</tr>
<tr>
<td>primaries_by_site</td>
<td>Primary peer (GIUD).</td>
</tr>
<tr>
<td>rep_count_by_site</td>
<td>Number of buckets.</td>
</tr>
<tr>
<td>search_count_by_site</td>
<td>Number of searchable buckets.</td>
</tr>
<tr>
<td>service_after_time</td>
<td>Bucket service is deferred until after this time.</td>
</tr>
<tr>
<td>standalone</td>
<td>Indicates if the bucket was created on the peer before the peer entered into a cluster configuration with this master.</td>
</tr>
</tbody>
</table>

Pagination and filtering parameters can be used with this method.

### Example request and response

229
XML Request

curl -k -u admin:pass https://localhost:8089/services/cluster/master/buckets

XML Response

<title>clustermasterbuckets</title>
<id>https://localhost:8089/services/cluster/master/buckets</id>
<updated>2014-04-17T19:13:57+00:00</updated>
<generator build="204899" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/master/buckets/_new" rel="create"/>
<link href="/services/cluster/master/buckets/_audit~0~238C3311-F0A4-4A9B-97F0-53667CFFEAB" rel="create"/>
<link href="/services/cluster/master/buckets/_audit~0~238C3311-F0A4-4A9B-97F0-53667CFFEAB" rel="list"/>
<link href="/services/cluster/master/buckets/_audit~0~238C3311-F0A4-4A9B-97F0-53667CFFEAB" rel="remove"/>

<content type="text/xml">
  <s:dict>
    <s:key name="bucket_size">47187</s:key>
    <s:key name="constrain_to_origin_site">1</s:key>
    <s:key name="eai:acl">
      ... elided ...
    </s:key>
    <s:key name="frozen">0</s:key>
    <s:key name="index">_audit</s:key>
    <s:key name="origin_site">site2</s:key>
    <s:key name="peers">
      <s:dict>
        <s:key name="238C3311-F0A4-4A9B-97F0-53667CFFEAB">
          <s:dict>
            <s:key name="bucket_flags">0x6</s:key>
            <s:key name="checksum"></s:key>
            <s:key name="checksum_state">StableCksum</s:key>
            <s:key name="search_state">Searchable</s:key>
            <s:key name="status">Complete</s:key>
          </s:dict>
        </s:key>
        <s:key name="C878FADC-513D-4BDD-BA48-F25BB82FE565">
          <s:dict>
            <s:key name="bucket_flags">0x0</s:key>
            <s:key name="checksum"></s:key>
            <s:key name="checksum_state">StableCksum</s:key>
            <s:key name="search_state">Searchable</s:key>
            <s:key name="status">Complete</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
  </s:dict>
</content>
<s:dict>
<s:key name="E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C">
<s:key name="bucket_flags">0x0</s:key>
<s:key name="checksum"></s:key>
<s:key name="checksum_state">StableCksum</s:key>
<s:key name="search_state">Unsearchable</s:key>
<s:key name="status">Complete</s:key>
</s:dict>

<s:dict>
<s:dict>
<s:key name="primaries_by_site">
<s:dict>
<s:key name="site1">238C3311-F0A4-4A9B-97F0-53667CFEEAB</s:key>
<s:key name="site2">238C3311-F0A4-4A9B-97F0-53667CFEEAB</s:key>
</s:dict>
</s:dict>

<s:dict>
<s:key name="rep_count_by_site">
<s:dict>
<s:key name="site2">3</s:key>
</s:dict>
</s:dict>

<s:dict>
<s:key name="search_count_by_site">
<s:dict>
<s:key name="site2">2</s:key>
</s:dict>
</s:dict>

<s:key name="service_after_time">0</s:key>
<s:key name="standalone">0</s:key>
</s:dict>

</content>
</entry>

<entry>
...
...
.... elided ...
...

</entry>

<entry>
<title>_internal~1~E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C</title>
<id>https://localhost:8089/services/cluster/master/buckets/_internal~1~E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C</id>
<updated>2014-04-17T19:13:57+00:00</updated>
<link href="/services/cluster/master/buckets/_internal~1~E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C" rel="alternate"/>
<author>
<name>system</name>
</author>
<link href="/services/cluster/master/buckets/_internal~1~E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C" rel="list"/>
<link href="/services/cluster/master/buckets/_internal~1~E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C" rel="remove"/>
<content type="text/xml">
<s:dict>
<s:key name="bucket_size"></s:key>
<s:key name="constrain_to_origin_site">0</s:key>
<s:key name="eai:acl">
... elided ...
</s:dict>
<s:dict>
  <s:key name="frozen">0</s:key>
  <s:key name="index">_internal</s:key>
  <s:key name="origin_site">site2</s:key>
  <s:key name="peers">
    <s:dict>
      <s:key name="61666763-43E9-411B-9464-D80A5119EF0E">
        <s:dict>
          <s:key name="bucket_flags">0x2</s:key>
          <s:key name="checksum"></s:key>
          <s:key name="checksum_state">StableCksum</s:key>
          <s:key name="search_state">Searchable</s:key>
          <s:key name="status">StreamingTarget</s:key>
        </s:dict>
      </s:key>
      <s:key name="C878FADC-513D-4BDD-BA48-F25BB82FE565">
        <s:dict>
          <s:key name="bucket_flags">0x0</s:key>
          <s:key name="checksum"></s:key>
          <s:key name="checksum_state">StableCksum</s:key>
          <s:key name="search_state">Unsearchable</s:key>
          <s:key name="status">StreamingTarget</s:key>
        </s:dict>
      </s:key>
      <s:key name="E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C">
        <s:dict>
          <s:key name="bucket_flags">0x4</s:key>
          <s:key name="checksum"></s:key>
          <s:key name="checksum_state">StableCksum</s:key>
          <s:key name="search_state">Searchable</s:key>
          <s:key name="status">StreamingSource</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
  <s:key name="primaries_by_site">
    <s:dict>
      <s:key name="site1">61666763-43E9-411B-9464-D80A5119EF0E</s:key>
      <s:key name="site2">E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C</s:key>
    </s:dict>
  </s:key>
  <s:key name="rep_count_by_site">
    <s:dict>
      <s:key name="site1">1</s:key>
      <s:key name="site2">2</s:key>
    </s:dict>
  </s:key>
  <s:key name="search_count_by_site">
    <s:dict>
      <s:key name="site1">1</s:key>
      <s:key name="site2">1</s:key>
    </s:dict>
  </s:key>
  <s:key name="service_after_time">0</s:key>
  <s:key name="standalone">0</s:key>
</s:dict>
cluster/master/buckets/{name}

https://{host}:{mPort}/services/cluster/master/buckets/{name}
Access bucket configuration information.

GET
List bucket configuration information.

**Request parameters**
The `filter` parameter of the Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket_size</td>
<td>Indicates the size, in bytes, of the bucket.</td>
</tr>
<tr>
<td>constrain_to_origin_site</td>
<td>Flag indicating this particular bucket is a clustered pre-multisite bucket. Such buckets are replicated only within their origin site.</td>
</tr>
<tr>
<td>frozen</td>
<td>Indicates if the bucket is frozen.</td>
</tr>
<tr>
<td>index</td>
<td>Name of the index to which the bucket belongs.</td>
</tr>
<tr>
<td>origin_site</td>
<td>Where the bucket originated.</td>
</tr>
<tr>
<td>peers</td>
<td>Lists information about buckets on peers to this master.</td>
</tr>
<tr>
<td>primaries_by_site</td>
<td>Primary peer (GIUD).</td>
</tr>
<tr>
<td>rep_count_by_site</td>
<td>Number of buckets.</td>
</tr>
<tr>
<td>search_count_by_site</td>
<td>Number of searchable buckets.</td>
</tr>
<tr>
<td>service_after_time</td>
<td>Bucket service is deferred until after this time.</td>
</tr>
<tr>
<td>standalone</td>
<td>Indicates if the bucket was created on the peer before the peer entered into a cluster configuration with this master.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/cluster/master/buckets/internal~1~238C3311-F0A4-4A9B-97F0-53667CFFEEAB
```

**XML Response**

```xml
<title>clustermasterbuckets</title> <id>https://localhost:8089/services/cluster/master/buckets</id> <updated>2014-04-17T19:16:03+00:00</updated> <generator build="204899" version="6.1"/>
```
cluster/master/buckets/{bucket_id}/fix

https://<host>:<mPort>/services/cluster/master/buckets/{bucket_id}/fix
Add the specified bucket to the fix list.

For more information, see Bucket-fixing scenarios in Managing Indexers and Clusters of Indexers.

Authentication and Authorization
Requires the admin role or indexes_edit capability.

POST
Add this bucket to the fix list.

Request parameters
None

Returned values
None

Example request and response
XML Request

curl -k -u admin:changeme
https://localhost:8089/services/cluster/master/buckets/_internal~0~111175BA-00DF-4CFE-9AEC-48A87B97EC71/fix
-X POST

XML Response

<title>clustermasterbuckets</title>
/id&gt;
<updated>2015-11-04T12:23:57-08:00</updated>
<generator build="8effae892620f7b651853d141b7a6b61b929c0" version="20151102"/>
<author>
 &lt;name&gt;Splunk&lt;/name&gt;
&lt;/author&gt;
&lt;link href="/services/cluster/master/buckets/_new" rel="create"/&gt;
&lt;link href="/services/cluster/master/buckets/_acl" rel="_acl"/&gt;
&lt;opensearch:totalResults&gt;0&lt;/opensearch:totalResults&gt;
&lt;opensearch:itemsPerPage&gt;30&lt;/opensearch:itemsPerPage&gt;
&lt;opensearch:startIndex&gt;0&lt;/opensearch:startIndex&gt;
&lt;s:messages/&gt;

cluster/master/buckets/{bucket_id}/freeze

https://&lt;host&gt;:&lt;mPort&gt;/services/cluster/master/buckets/{bucket_id}/freeze
Set the bucket's state to frozen. The frozen state may not persist after a cluster master restart unless one of the peers has
set the frozen state. A POST to this endpoint does not set the bucket's state to frozen on peers.

Note: Use this endpoint with caution. It is recommended to test the endpoint in a test cluster prior to use on an
actual bucket.

For more information, see How the cluster handles frozen buckets in Managing Indexers and Clusters of Indexers.

Authentication and Authorization

Requires the admin role or indexes_edit capability.

POST

Set this bucket's state to frozen.

Request parameters
None

Returned values
None
Example request and response

XML Request

curl -k -u admin:pass
https://localhost:8089/services/cluster/master/buckets/_internal~0~111175BA-00DF-4CFE-9AEC-48A87B97EC71/freeze
-X POST

XML Response

<title>clustermasterbuckets</title>
<ID>https://locahost:8089/services/cluster/master/buckets</id>
<updated>2015-11-04T12:21:27-08:00</updated>
<generator build="8effae892620f7b651853d141b7a6b61b929c0" version="20151102"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/master/buckets/_new" rel="create"/>
<link href="/services/cluster/master/buckets/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

cluster/master/buckets/{bucket_id}/remove_all

https://<host>:<mPort>/services/cluster/master/buckets/{bucket_id}/remove_all
Delete all copies of the specified bucket.

Caution: Using this endpoint will cause irreversible data loss. It is recommended to test the endpoint on a test cluster prior to use on an actual bucket.

Authentication and Authorization
Requires the admin role or indexes_edit capability.

POST

Delete all copies of the specified bucket.

Request parameters

None

Returned values

None. If an invalid bucket id is used, an error message is returned.
If the request is made on a hot bucket, an error message is returned.

```
<response>
  <messages>
    <msg type="ERROR">
      In handler 'clustermasterbuckets': bucket not found
    </msg>
  </messages>
</response>
```

Example request and response

**XML Request**

```
curl -k -u admin:password
https://localhost:8089/services/cluster/master/buckets/_internal~0~111175BA-00DF-4CFE-9AEC-48A87B97EC71/remove_all
-X POST
```

**XML Response**

```
<title>clustermasterbuckets</title>
<id>https://localhost:8089/services/cluster/master/buckets</id>
<updated>2015-11-04T12:24:12-08:00</updated>
<generator build="8e1fae892620f7b653d141b7b7a6b61b929c0" version="20151102"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/master/buckets/_new" rel="create"/>
<link href="/services/cluster/master/buckets/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```

**cluster/master/buckets/{bucket_id}/remove_from_peer**

```
https://<host>:<mPort>/services/cluster/master/buckets/{bucket_id}/remove_from_peer
```

Deletes the copy of this bucket from specified peer.

If the request causes the cluster to lose its complete state, the cluster will engage in fixup activities. This may result in another copy of the same bucket appearing on this peer. If, however, the specified bucket is frozen, the cluster does not attempt any fixup activities.

**Caution:** Using this endpoint will cause irreversible data loss. It is recommended to test the endpoint on a test-cluster prior to use on an actual bucket.

**Authentication and Authorization**

Requires the `admin` role or `indexes_edit` capability.
POST

Delete this bucket from specified peer. Set bucket state to frozen

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer</td>
<td>GUID</td>
<td>Peer GUID</td>
</tr>
</tbody>
</table>

Returned values

None. If the peer parameter is missing from the request, an error message is returned.

Example request and response

XML Request

curl -k -u admin:pass
https://localhost:8089/services/cluster/master/buckets/_internal~0~111175BA-00DF-4CFE-9AEC-48A87B97EC71/remove_from_peer -X POST -d peer=222275BA-00DF-4CFE-9AEC-48A87B97EC71

XML Response

```
<title>clustermasterbuckets</title>
<id>https://localhost:8089/services/cluster/master/buckets</id>
<updated>2015-11-04T12:23:18-08:00</updated>
<generator build="8effae892620f7b651853d141b7a6b61b929c0" version="20151102"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/master/buckets/_new" rel="create"/>
<link href="/services/cluster/master/buckets/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```

cluster/master/control/control/prune_index

https://<host>:<mPort>/services/cluster/master/control/control/prune_index

Clean up excess bucket copies across an index.

For more information, see Remove extra bucket copies in *Managing Indexers and Clusters of Indexers.*
POST

Clean up excess bucket copies across an index.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>Optional. The index from which to remove excess bucket copies. If not specified, the POST operation clears excess bucket copies across all indexes.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request

XML Request

curl -k -u admin:pass https://localhost:8089/services/cluster/master/control/control/prune_index -d index="my_index"

curl -k -u admin:pass https://localhost:8089/services/cluster/master/control/control/prune_index -d index="my_index"

Rebalance primary bucket copies across peers. For more information, see Rebalance the indexer cluster primary buckets in Managing Indexers and Clusters of Indexers.

POST

Rebalance primary buckets across all peers of this master.

Request parameters

None

Returned values

None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/cluster/master/control/control/rebalance_primaries --request POST
### XML Response

```xml
<title>clustermastercontrol</title>
<id>https://localhost:8089/services/cluster/master/control</id>
<updated>2013-08-21T13:08:52-07:00</updated>
<generator build="176231" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```

### `cluster/master/control/control/remove_peers`

**https://<host>:<mPort>/services/cluster/master/control/control/remove_peers**

Remove one or more peers.

**See also**

`cluster/master/peers`

**POST**

Remove one or more peers.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peers</td>
<td>String</td>
<td>One or more comma-separated peer GUIDs.</td>
</tr>
</tbody>
</table>

**Required**

**Returned values**

None

**Application usage**

If peer status is not Down or GracefulShutdown, the interface returns the following error message:

```xml
<response>
  <messages>
    <msg type="ERROR">
      In handler 'clustermastercontrol': Remove aborted, Reason: Peer=<hostname> with guid=<peerID> cannot be removed. Peer has status=Up. Only peers with status=Down (or) GracefulShutdown can be removed.</msg>
  </messages>
</response>
```
Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/cluster/master/control/control/remove_peers --request POST -d "peers=F2AA19BD-622F-4F8C-A8E0-1233"

XML Response

<title>clustermastercontrol</title>
{id>https://localhost:8089/services/cluster/master/control</id>
<updated>2014-09-10T13:12:54-07:00</updated>
<generator build="230688" version="6.2"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...

cluster/master/control/control/resync_bucket_from_peer

https://<host>:<mPort>/services/cluster/master/control/control/resync_bucket_from_peer

This endpoint resets the state of a specified bucket based on the current state of the bucket at a peer.

POST

Reset bucket state based on the current state of the bucket at a peer.

Request Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket_id</td>
<td>String</td>
<td>N/A</td>
<td>Required. ID of bucket to update.</td>
</tr>
<tr>
<td>peer</td>
<td>GUID</td>
<td>N/A</td>
<td>Required. GUID of peer from which to update the bucket.</td>
</tr>
</tbody>
</table>

Returned Values

None.

Example request and response

XML Request

curl -k -u admin:pass
https://hostname:mPort:/services/cluster/master/control/control/resync_bucket_from_peer -X POST -d bucket_id=_audit~2~8F6747E9-88C9-4488-8806-4EA3CA433CF5 -d peer=8F6747E9-88C9-4488-8806-4EA3CA433CF5

XML Response

242
cluster/master/control/control/roll-hot-buckets

https://<host>:<mPort>/services/cluster/master/control/control/roll-hot-buckets

This endpoint forces a specified bucket in an indexer cluster to roll from hot to warm. Pass the bucket id (bid) to the master node. The master instructs the origin peer for that bucket to roll its copy. In turn, the origin peer tells all the replicating peers to roll their copies.

You might discover a bucket that is stuck in fixup and needs to be rolled using logs, Splunk Web, or either of the following two endpoints.

- cluster/master/fixup
- cluster/master/buckets

Authorization and authentication
This endpoint requires the admin role for use.

POST

Force a bucket to roll from hot to warm.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket_id</td>
<td>String</td>
<td>N/A</td>
<td>Required. ID for bucket to roll.</td>
</tr>
</tbody>
</table>

Returned values
None.

Example request and response

XML Request
curl -k -u username:password https://localhost:8089/services/cluster/master/control/control/roll-hot-buckets
-X POST -d "bucket_id=_audit~2~1A3889D7-954B-4CE6-B071-01B438DE9865"

XML Response

<title>clustermastercontrol</title>
  <id>https://localhost:8089/services/cluster/master/control</id>
  <updated>2015-10-30T07:34:56+08:00</updated>
  <generator build="0d9d63e4338" version="6.4.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/master/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <n:message/>

(cluster/master/control/control/rolling_upgrade_finalize

https://<host>:<mPort>/services/cluster/master/control/control/rolling_upgrade_finalize
Finalizes an indexer cluster rolling upgrade.

POST

Finalizes an indexer cluster rolling upgrade.

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass
https://localhost:8089/services/cluster/master/control/control/rolling_upgrade_finalize
-X POST

XML Response

<title>clustermastercontrol</title>
  <id>https://10.141.65.179:52000/services/cluster/master/control</id>
  <updated>2018-04-01T22:04:46+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/master/control/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <n:message/>

244
cluster/master/control/control/rolling_upgrade_init

https://<host>:<mPort>/services/cluster/master/control/control/rolling_upgrade_init
Initializes an indexer cluster rolling upgrade.

**POST**
Initializes an indexer cluster rolling upgrade.

**Returned values**
None

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/cluster/master/control/control/rolling_upgrade_init -X POST

**XML Response**

```xml
<title>clustermastercontrol</title>
<id>https://10.141.65.179:52000/services/cluster/master/control</id>
<updated>2018-04-01T21:06:21+00:00</updated>
<generator build="b233a6c1ade2" version="7.2.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/master/control/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages>
  <s:msg type="INFO">Cluster is now in searchable rolling upgrade mode.</s:msg>
</s:messages>
```

cluster/master/control/default/apply

https://<host>:<mPort>/services/cluster/master/control/default/apply
Pushes a bundle.
POST

Push a bundle.

Request Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>skip-validation</td>
<td>Boolean</td>
<td>False</td>
<td>Set as true to skip the validation step for this bundle.</td>
</tr>
<tr>
<td>ignore_identical_bundle</td>
<td>Boolean</td>
<td>True</td>
<td>Set as false to push this bundle even if current active bundle is identical to this bundle.</td>
</tr>
</tbody>
</table>

Returned Values

None.

Example request and response

XML Request

```bash
curl -k -u admin:pass https://host:mPort/services/cluster/master/control/default/apply -X POST
```

XML Response

```xml
<title>clustermastercontrol</title>
<id>https://wimpy:7420/services/cluster/master/control</id>
<updated>2019-01-02T13:46:04-08:00</updated>
<generator build="c5340c4d9387ab182815dc279bcd14979b747dc9" version="20181119"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/master/control/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>clusterbundles</title>
  <id>https://wimpy:7420/services/cluster/master/control/clusterbundles</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/cluster/master/control/clusterbundles" rel="alternate"/>
  <link href="/services/cluster/master/control/clusterbundles" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="checksum">288845778D5B1952F534AB16DD82881E</s:key>
      <s:key name="eai:acl"></s:key>
      <s:dict>
        <s:key name="app"></s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">0</s:key>
        <s:key name="owner">system</s:key>
    </s:dict>
  </content>
</entry>
```

246
cluster/master/control/default/cancel_bundle_push

https://<host>:<mPort>/services/cluster/master/control/default/cancel_bundle_push

Cancels and resets the bundle push operation. Use this endpoint when the cluster master does not receive a validation response from the cluster peer due to an error. For more information, see Configuration bundle issues.

POST

Cancel and reset the bundle push operation.

Request Parameters
None.

Returned Values
None.

Example request and response

XML Request

curl -k -u admin:pass https://host:mPort/services/cluster/master/control/default/cancel_bundle_push -X POST

XML Response

<title>clustermastercontrol</title>
<id>https://<hostname>:<mgt-port>/services/cluster/master/control</id>
cluster/master/control/default/rollback

https://<host>:<mPort>/services/cluster/master/control/default/rollback

Roll a bundle back to the previously active bundle.

**POST**

Roll back a bundle.

**Request Parameters**

None.

**Returned Values**

None.

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://host:mPort/services/cluster/master/control/default/rollback -X POST
```

**XML Response**

```xml
<title>clustermastercontrol</title>
</id>https://wimpy:7420/services/cluster/master/control</id>
<updated>2019-01-02T13:46:26-08:00</updated>
<generator build="c5340c4d9387ab182815d279b679747dc9" version="20181119"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/master/control/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>clusterbundles</title>
</id>https://wimpy:7420/services/cluster/master/control/clusterbundles</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/services/cluster/master/control/clusterbundles" rel="alternate"/>
<author>
```
cluster/master/control/default/validate_bundle

https://<host>:<mPort>/services/cluster/master/control/default/validate_bundle
Tests if the bundle in etc/master-apps passes validation. Optionally, tests if the bundle will trigger an indexer restart.

POST

Validate a bundle.

Request Parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>check-restart</td>
<td>Boolean</td>
<td>False</td>
<td>By default, checks if the bundle passes validation on the cluster master and indexers. Set to true to check if the bundle will trigger a restart on the indexers.</td>
</tr>
</tbody>
</table>
Returned Values
None.

Example request and response

XML Request

curl -k -u admin:pass https://host:mPort/services/cluster/master/control/default/validate_bundle -d check-restart=true -X POST

XML Response

<title>clustermastercontrol</title>
&lt;id&gt;https://wimpy:7420/services/cluster/master/control</id&gt;
&lt;updated&gt;2019-01-02T13:56:48-08:00&lt;/updated&gt;
&lt;generator build="c5340c4d9387ab182815dc279bcd14979b747dc9" version="20181119"/&gt;
&lt;author&gt;
&lt;name&gt;Splunk&lt;/name&gt;
&lt;/author&gt;
&lt;link href="/services/cluster/master/control/_acl" rel="_acl"/&gt;
&lt;opensearch:totalResults&gt;1&lt;/opensearch:totalResults&gt;
&lt;opensearch:itemsPerPage&gt;30&lt;/opensearch:itemsPerPage&gt;
&lt;opensearch:startIndex&gt;0&lt;/opensearch:startIndex&gt;
&lt;s:messages/&gt;
&lt;entry&gt;
&lt;title&gt;clusterbundles&lt;/title&gt;
&lt;id&gt;https://wimpy:7420/services/cluster/master/control/clusterbundles&lt;/id&gt;
&lt;updated&gt;1969-12-31T16:00:00-08:00&lt;/updated&gt;
&lt;link href="/services/cluster/master/control/clusterbundles" rel="alternate"/&gt;
&lt;author&gt;
&lt;name&gt;system&lt;/name&gt;
&lt;/author&gt;
&lt;link href="/services/cluster/master/control/clusterbundles" rel="list"/&gt;
&lt;link href="/services/cluster/master/control/clusterbundles" rel="edit"/&gt;
&lt;content type="text/xml"&gt;
&lt;s:dict&gt;
&lt;s:key name="checksum">288845778D5B1952F534AB16D82881E&lt;/s:key&gt;
&lt;s:key name="eai:acl"&gt;
&lt;s:dict&gt;
&lt;s:key name="app"&gt;&lt;/s:key&gt;
&lt;s:key name="can_list">1&lt;/s:key&gt;
&lt;s:key name="can_write">1&lt;/s:key&gt;
&lt;s:key name="modifiable">0&lt;/s:key&gt;
&lt;s:key name="owner">system&lt;/s:key&gt;
&lt;s:key name="perms"&gt;
&lt;s:dict&gt;
&lt;s:key name="read"&gt;
&lt;s:list&gt;
&lt;s:item&gt;admin&lt;/s:item&gt;
&lt;s:item&gt;splunk-system-role&lt;/s:item&gt;
&lt;/s:list&gt;
&lt;/s:key&gt;
&lt;s:key name="write"&gt;
&lt;s:list&gt;
&lt;s:item&gt;admin&lt;/s:item&gt;
&lt;s:item&gt;splunk-system-role&lt;/s:item&gt;
&lt;/s:list&gt;
&lt;/s:key&gt;

250
cluster/master/fixup

https://<host>:<mPort>/services/cluster/master/fixup

Access a list of buckets on a specific fixup priority level. Bucket fixups are processed in order of priority level. See Request parameters below for priority level details.

When you access a particular fixup level, buckets may appear in it even though they do not need fixup at this level. Initially, each bucket requiring fixup is added to all levels, even though it might only require processing in a subset of all levels. As the bucket is processed through a level, it is deleted from that level.

GET

List buckets on the specified fixup level.

Request parameters

Pagination and filtering parameters can be used with this method.

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>String</td>
<td>Required. Fixup priority level. Use one of the following level values, listed in order of priority.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• streaming: Hot buckets that need to be rolled or have their size committed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• data_safety: Buckets without at least two rawdata copies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• generation: Buckets without a primary copy.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• replication_factor: Buckets without replication factor number of copies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• search_factor: Buckets without search factor number of copies.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• checksum_sync: Level for syncing a bucket's delete files across all peers that have this bucket. Syncing is determined based on the checksum of all of the delete files.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>Optional. Index name.</td>
</tr>
</tbody>
</table>

Returned values

For each bucket in the specified fixup level, the response includes the following details for the initial time when the bucket went into the fixup level and the latest time that the bucket was checked.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Bucket id.</td>
</tr>
<tr>
<td>reason</td>
<td>Initial or latest reason for the bucket being on this fixup level.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>timestamp</td>
<td>Timestamp for initial bucket addition to fixup list or latest bucket check.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**


**XML Response**

```xml
<title>clustermasterfixup</title>
<ID>https://localhost:8089/services/cluster/master/fixup</ID>
<updated>2015-11-09T17:05:48-08:00</updated>
<generator build="802b4a159bb584c629dcdb8ba57c409b1d5b7ab" version="20151030"/>
<br name="Splunk"/>
<link href="/services/cluster/master/fixup/_acl" rel="_acl"/>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>_audit~212~22220097-5E3F-4D26-B301-ECE3C4CD2222</title>
<ID>https://localhost:8089/services/cluster/master/fixup/_audit~212~22220097-5E3F-4D26-B301-ECE3C4CD2222</ID>
<updated>2015-11-09T17:05:48-08:00</updated>
<link href="/services/cluster/master/fixup/_audit~212~22220097-5E3F-4D26-B301-ECE3C4CD2222" rel="alternate"/>
<br name="system"/>
<link href="/services/cluster/master/fixup/_audit~212~22220097-5E3F-4D26-B301-ECE3C4CD2222" rel="list"/>
<content type="text/xml">
  <s:dict>
    <s:dict name="eai:acl">
      <s:dict name="app">
        <s:dict name="can_list">1</s:dict>
        <s:dict name="can_write">1</s:dict>
        <s:dict name="modifiable">0</s:dict>
        <s:dict name="owner">system</s:dict>
        <s:dict name="perms">
          <s:dict name="read">
            <s:list>
              <s:item>admin</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:dict>
          <s:dict name="write">
            <s:list>
              <s:item>admin</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:dict>
        </s:dict>
      </s:dict>
    </s:dict>
  </s:dict>
</content>
```

252
<s:dict>
  <s:key name="removable">0</s:key>
  <s:key name="sharing">system</s:key>
  <s:dict>
  <s:key name="index">_audit</s:key>
  <s:dict>
  <s:key name="reason">add peer=22220097-5E3F-4D26-B301-ECE3C4CD2222 new bucket</s:key>
  <s:key name="timestamp">1447099323</s:key>
  </s:dict>
  </s:dict>
  <s:dict>
  <s:key name="reason">Missing enough suitable candidates to create replicated copy in order to
  meet replication policy. Missing={ site2:1 } </s:key>
  <s:key name="timestamp">1447117547</s:key>
  </s:dict>
  <s:dict>
  <s:key name="level">replication_factor</s:key>
  </s:dict>
</content>
</entry>
<entry>
<title>_internal~12628~111163F8-61F4-4AB3-A1A7-2EDCB10C1111</title>
{id>https://localhost:8089/services/cluster/master/fixup/_internal~12628~111163F8-61F4-4AB3-A1A7-2EDCB10C1111</id>
<updated>2015-11-09T17:05:48-08:00</updated>
</entry>
<content type="text/xml">
<s:dict>
  <s:dict>
  <s:key name="eai:acl">
  <s:dict>
  <s:key name="app"></s:key>
  <s:key name="can_list">1</s:key>
  <s:key name="can_write">1</s:key>
  <s:key name="modifiable">0</s:key>
  <s:key name="owner">system</s:key>
  </s:dict>
  <s:dict>
  <s:key name="read">
  <s:list>
  <s:item>admin</s:item>
  <s:item>splunk-system-role</s:item>
  </s:list>
  </s:dict>
  <s:dict>
  <s:key name="write">
  <s:list>
  <s:item>admin</s:item>
  <s:item>splunk-system-role</s:item>
  </s:list>
  </s:dict>
  <s:dict>
  <s:key name="removable">0</s:key>
  </s:dict>
</s:dict>
</content>
clustermaster/generation

https://<host>:<mPort>/services/cluster/master/generation

Access current generation cluster master information and create a cluster generation.

GET

List peer nodes participating in the current generation for this master.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation_id</td>
<td>The ID for the current generation for this master.</td>
</tr>
<tr>
<td>generation_peers</td>
<td>Lists the peers for this generation of the cluster.</td>
</tr>
<tr>
<td>pending_generation_id</td>
<td>The next generation ID used by the master when committing a new generation. This value is useful for debugging.</td>
</tr>
<tr>
<td>pending_last_attempt</td>
<td>The timestamp of the last attempt to commit to the pending generation ID (if ever).</td>
</tr>
<tr>
<td>pending_last_reason</td>
<td>The reason why this peer failed to commit to the pending generation. This parameter is EMPTY if no such attempt was made.</td>
</tr>
</tbody>
</table>
Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/cluster/master/generation

XML Response

<title>clustermastergeneration</title>
/id>https://localhost:8089/services/cluster/master/generation</id>
<updated>2012-09-05T10:39:54-07:00</updated>
<generator build="136169" version="5.0"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>master</title>
  <id>https://localhost:8089/services/cluster/master/generation/master</id>
  <updated>2012-09-05T10:39:54-07:00</updated>
  <link href="/services/cluster/master/generation/master" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/master/generation/master" rel="list"/>
  <content type="text/xml">
    <s:dict>
      ... eai:acl node elided ...
      <s:key name="generation_id">2</s:key>
      <s:key name="generation_peers">
        <s:dict>
          <s:key name="2AF11DD4-1424-4A14-A522-FB9D055E9516">
            <s:dict>
              <s:key name="host_port_pair">splunks-ombra.sv.splunk.com:8389</s:key>
              <s:key name="peer">splunks-ombra.sv.splunk.com</s:key>
            </s:dict>
          </s:key>
          <s:key name="50FCDB42-E167-458D-A6A9-E4587E8F16D9">
            <s:dict>
              <s:key name="host_port_pair">splunks-ombra.sv.splunk.com:8189</s:key>
              <s:key name="peer">splunks-ombra.sv.splunk.com</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="pending_generation_id">3</s:key>
      <s:key name="pending_last_attempt">0</s:key>
      <s:key name="pending_last_reason"></s:key>
    </s:dict>
  </content>
</entry>

POST

Create a cluster generation.
Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>required</td>
<td>The URI of the searchhead node of a cluster upon which to create a new generation.</td>
</tr>
<tr>
<td>generation_poll_interval</td>
<td>Number</td>
<td></td>
<td>How often, in seconds, the searchhead polls the master for generation information. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>label</td>
<td>String</td>
<td></td>
<td>Server name for the Splunk platform instance specified by the name attribute.</td>
</tr>
<tr>
<td>mgmt_port</td>
<td>String</td>
<td></td>
<td>The management port of searchhead node in a cluster upon which you are creating a new generation.</td>
</tr>
<tr>
<td>register_search_address</td>
<td>String</td>
<td></td>
<td>The address on which a peer node is available as search head. This is useful in the cases where a host machine has multiple interfaces and only one of them can be reached by another splunkd instance.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation_id</td>
<td>The ID for the current generation for this master.</td>
</tr>
<tr>
<td>generation_peers</td>
<td>Lists the peers for this generation of the cluster.</td>
</tr>
<tr>
<td>pending_generation_id</td>
<td>The next generation ID used by the master when committing a new generation. This value is useful for debugging.</td>
</tr>
<tr>
<td>pending_last_attempt</td>
<td>The timestamp of the last attempt to commit to the pending generation ID (if ever).</td>
</tr>
<tr>
<td>pending_last_reason</td>
<td>The reason why this peer failed to commit to the pending generation. This parameter is EMPTY if no such attempt was made.</td>
</tr>
<tr>
<td>replication_factor_met</td>
<td>Indicates if the replication factor was met for the cluster.</td>
</tr>
<tr>
<td>search_factor_met</td>
<td>Indicates if the search factor was met for the cluster.</td>
</tr>
<tr>
<td>was_forced</td>
<td>Indicates next generation was forcibly committed.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://myserver:8089/services/cluster/master/generation -d name=foo

**XML Response**

```
<title>clustermastergeneration</title>
<id>https://myserver:8089/services/cluster/master/generation</id>
<updated>2013-10-31T13:58:51-07:00</updated>
<generator build="184661" version="20131030"/>
<author>
  <name>Splunk</name>
</author>
```
cluster/master/generation/{name}

https://<host>:<mPort>/services/cluster/master/generation/{name}

Access information about a peer node participating in the current generation for the specified search head GUID.
GET

List peer node information of the specified search head GUID.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation_id</td>
<td>The ID of the current generation for this master.</td>
</tr>
<tr>
<td>generation_peers</td>
<td>Lists the peers for this generation of the cluster.</td>
</tr>
<tr>
<td>pending_generation_id</td>
<td>The next generation ID used by the master when committing a new generation.</td>
</tr>
<tr>
<td></td>
<td>This value is useful for debugging.</td>
</tr>
<tr>
<td>pending_last_attempt</td>
<td>The timestamp of the last attempt to commit to the pending generation ID (if ever).</td>
</tr>
<tr>
<td></td>
<td>This parameter is EMPTY if no such attempt was made.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/cluster/master/generation/master

XML Response

<title>clustermastergeneration</title>
?id=https://localhost:8089/services/cluster/master/generation/id
<updated>2012-09-05T10:45:27-07:00</updated>
<generator build="136169" version="5.0"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>master</title>
  <id>https://localhost:8089/services/cluster/master/generation/master/id</id>
  <updated>2012-09-05T10:45:27-07:00</updated>
  <link href="/services/cluster/master/generation/master" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/master/generation/master" rel="list"/>
<content type="text/xml">

258
POST

Create a new generation for the specified search head GUID.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation_poll_interval</td>
<td>Number</td>
<td>How often, in seconds, the search head polls the master for generation information. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>label</td>
<td>String</td>
<td>Server name for the search head specified by {name}.</td>
</tr>
<tr>
<td>mgmt_port</td>
<td>String</td>
<td>The management port of the search head node in a cluster upon which you are creating a new generation.</td>
</tr>
<tr>
<td>register_search_address</td>
<td>String</td>
<td>The address on which a peer node is available as search head. This is useful when a host machine has multiple interfaces and only one of them can be reached by another splunkd instance.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation_id</td>
<td>The ID for the current generation for this master.</td>
</tr>
<tr>
<td>generation_peers</td>
<td>Lists the peers for this generation of the cluster.</td>
</tr>
<tr>
<td>pending_generation_id</td>
<td>The next generation ID used by the master when committing a new generation.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>pending_last_attempt</td>
<td>The timestamp of the last attempt to commit to the pending generation ID (if ever).</td>
</tr>
<tr>
<td>pending_last_reason</td>
<td>The reason why this peer failed to commit to the pending generation.</td>
</tr>
<tr>
<td>replication_factor_met</td>
<td>Indicates if the replication factor was met for the cluster.</td>
</tr>
<tr>
<td>search_factor_met</td>
<td>Indicates if the search factor was met for the cluster.</td>
</tr>
<tr>
<td>was_forced</td>
<td>Indicates next generation was forcibly committed.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```bash
curl -k -u admin:pass https://myserver:8089/services/cluster/master/generation/foo -X POST -d
generation_poll_interval=62 -d label=PEER2
```

**XML Response**

```xml
<title>clustermastergeneration</title>
<id>https://myserver:8089/services/cluster/master/generation</id>
<updated>2013-10-31T14:37:20-07:00</updated>
<generator build="184661" version="20131030"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/master/generation/_new" rel="create"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>master</title>
  <id>https://myserver:8089/services/cluster/master/generation/master</id>
  <updated>2013-10-31T14:37:20-07:00</updated>
  <link href="/services/cluster/master/generation/master" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/master/generation/master" rel="list"/>
  <link href="/services/cluster/master/generation/master" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      ... eai:acl node elided ... 
      <s:dict>
        <s:key name="generation_id">5</s:key>
        <s:dict>
          <s:key name="host_port_pair">myserver.splunk.com:6431</s:key>
          <s:dict>
            <s:key name="peer">PEER1</s:key>
          </s:dict>
          <s:dict>
            <s:key name="host_port_pair">myserver.splunk.com:6432</s:key>
          </s:dict>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
```
cluster/master/health

https://<host>:<mPort>/services/cluster/master/health
Performs health checks to determine the cluster health and search impact, prior to a rolling upgrade of the indexer cluster.

Authentication and Authorization

Requires the admin role or list_indexer_cluster capability.

GET

Get indexer cluster health check results.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all_data_is_searchable</td>
<td>Boolean</td>
<td>Indicates if all data in the cluster is searchable.</td>
</tr>
<tr>
<td>all_peers_are_up</td>
<td>Boolean</td>
<td>Indicate if all peers are strictly in the Up status.</td>
</tr>
<tr>
<td>Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cm_version_is_compatible</td>
<td>Boolean</td>
<td>Indicates if any cluster peers are running a Splunk Enterprise version greater than or equal to the cluster master's version.</td>
</tr>
<tr>
<td>multisite</td>
<td>Boolean</td>
<td>Indicates if multisite is enabled.</td>
</tr>
<tr>
<td>no_fixups_in_progress</td>
<td>Boolean</td>
<td>Indicates if there does not exist buckets with bucket state NonStreamingTarget, or bucket search states PendingSearchable or SearchablePendingMask.</td>
</tr>
<tr>
<td>pre_flight_check</td>
<td>Boolean</td>
<td>Indicates if the health check prior to a rolling upgrade was successful. This value is true only if the cluster passed all health checks.</td>
</tr>
<tr>
<td>replication_factor_met</td>
<td>Boolean</td>
<td>Only valid for mode=master and multisite=false. Indicates whether the replication factor is met. If true, the cluster has at least replication_factor number of raw data copies in the cluster.</td>
</tr>
<tr>
<td>search_factor_met</td>
<td>Boolean</td>
<td>Only valid for mode=master and multisite=false. Indicates whether the search factor is met. If true, the cluster has at least search_factor number of raw data copies in the cluster.</td>
</tr>
<tr>
<td>site_replication_factor_met</td>
<td>Boolean</td>
<td>Only valid for mode=master and multisite=true. Indicates whether the site replication factor is met. If true, the cluster has at least replication_factor number of raw data copies in the cluster.</td>
</tr>
<tr>
<td>site_search_factor_met</td>
<td>Boolean</td>
<td>Only valid for mode=master and multisite=true. Indicates whether the site search factor is met. If true, the cluster has at least site_search_factor number of raw data copies in the cluster.</td>
</tr>
<tr>
<td>splunk_version_peer_count</td>
<td>String</td>
<td>Lists the number of cluster peers running each Splunk Enterprise version.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/cluster/master/health

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
><title>clustermasterhealth</title>
  <id>https://10.141.65.179:52000/services/cluster/master/health</id>
  <updated>2018-04-01T19:53:47+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/master/health/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>master</title>
    <id>https://10.141.65.179:52000/services/cluster/master/health/master</id>
    <updated>2018-04-01T19:53:47+00:00</updated>
    <link href="/services/cluster/master/health/master" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <content type="text/xml">
      <s:dict>
```
<s:dict>
  <s:key name="cluster/master/indexes">
  </s:dict>

https://<host>:<mPort>/services/cluster/master/indexes

Access cluster index information.

GET

List cluster indices.

Request parameters

None
Returned values

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buckets_with_excess_copies</td>
<td>Number of distinct buckets that have one or more excess replication copies.</td>
</tr>
<tr>
<td>buckets_with_excess_searchable_copies</td>
<td>Number of distinct buckets that have one or more excess searchable copies.</td>
</tr>
<tr>
<td>index_size</td>
<td>Size of the index</td>
</tr>
<tr>
<td>is_searchable</td>
<td>When every bucket in the index has a primary, the index is considered &quot;searchable&quot;.</td>
</tr>
<tr>
<td>non_site_aware_buckets_in_site_aware_cluster</td>
<td>Number of buckets created when the cluster was not in a multisite config. (Included only when the cluster is in multisite config.)</td>
</tr>
<tr>
<td>num_buckets</td>
<td>Total number of distinct buckets.</td>
</tr>
<tr>
<td>replicatedcopies_tracker</td>
<td>Displays how many distinct buckets have X number of copies. One of the following options.</td>
</tr>
<tr>
<td>actual_copies_per_slot</td>
<td>Number of buckets with X copies.</td>
</tr>
<tr>
<td>expected_total_per_slot</td>
<td>Expected number of buckets with X copies.</td>
</tr>
<tr>
<td>searchablecopies_tracker</td>
<td>Displays how many distinct buckets have X number of searchable copies. One of the following options.</td>
</tr>
<tr>
<td>actual_copies_per_slot</td>
<td>Number of buckets with X searchable copies.</td>
</tr>
<tr>
<td>expected_total_per_slot</td>
<td>Expected number of buckets with X searchable copies.</td>
</tr>
<tr>
<td>sort_order</td>
<td>Used by UI.</td>
</tr>
<tr>
<td>total_excess_bucket_copies</td>
<td>Total number of excess copies for all buckets.</td>
</tr>
<tr>
<td>total_excess_searchable_copies</td>
<td>Total number of excess searchable copies for all buckets.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/cluster/master/indexes
```

XML Response

```
<title>clustermasterpeerindexes</title>
<id>https://localhost:8089/services/cluster/master/indexes</id>
<updated>2014-04-17T19:11:14+00:00</updated>
<generator build="204899" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```
<entry>
<title>_audit</title>
<id>https://localhost:8089/services/cluster/master/indexes/_audit</id>
<updated>2014-04-17T19:11:14+00:00</updated>
<link href="/services/cluster/master/indexes/_audit" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/cluster/master/indexes/_audit" rel="list"/>
<content type="text/xml">
  <s:dict>
    <s:key name="buckets_with_excess_copies">0</s:key>
    <s:key name="buckets_with_excess_searchable_copies">0</s:key>
    <s:key name="eai:acl">... elided ...
    </s:key>
    <s:key name="index_size">284975</s:key>
    <s:key name="is_searchable">1</s:key>
    <s:key name="non_site_aware_buckets_in_site_aware_cluster">6</s:key>
    <s:key name="num_buckets">12</s:key>
    <s:key name="replicated_copies_tracker">
      <s:dict>
        <s:key name="0">
          <s:dict>
            <s:key name="actual_copies_per_slot">12</s:key>
            <s:key name="expected_total_per_slot">12</s:key>
          </s:dict>
        </s:key>
        <s:key name="1">
          <s:dict>
            <s:key name="actual_copies_per_slot">12</s:key>
            <s:key name="expected_total_per_slot">12</s:key>
          </s:dict>
        </s:key>
        <s:key name="2">
          <s:dict>
            <s:key name="actual_copies_per_slot">12</s:key>
            <s:key name="expected_total_per_slot">12</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="searchable_copies_tracker">
      <s:dict>
        <s:key name="0">
          <s:dict>
            <s:key name="actual_copies_per_slot">12</s:key>
            <s:key name="expected_total_per_slot">12</s:key>
          </s:dict>
        </s:key>
        <s:key name="1">
          <s:dict>
            <s:key name="actual_copies_per_slot">12</s:key>
            <s:key name="expected_total_per_slot">12</s:key>
          </s:dict>
        </s:key>
        <s:key name="2">
          <s:dict>
            <s:key name="actual_copies_per_slot">12</s:key>
            <s:key name="expected_total_per_slot">12</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="sort_order">4294967295</s:key>
    <s:key name="total_excess_bucket_copies">0</s:key>
    <s:key name="total_excess_searchable_copies">0</s:key>
  </s:dict>
</content>
265
<content type="text/xml">
<s:dict>
  <s:key name="buckets_with_excess_copies">0</s:key>
  <s:key name="buckets_with_excess_searchable_copies">0</s:key>
  ... elided ...
  <s:key name="index_size">1190869</s:key>
  <s:key name="is_searchable">1</s:key>
  <s:key name="non_site_aware_buckets_in_site_aware_cluster">6</s:key>
  <s:key name="num_buckets">12</s:key>
  <s:key name="replicated_copies_tracker">
    <s:dict>
      <s:key name="0">
        <s:dict>
          <s:key name="actual_copies_per_slot">12</s:key>
          <s:key name="expected_total_per_slot">12</s:key>
        </s:dict>
      </s:key>
      <s:key name="1">
        <s:dict>
          <s:key name="actual_copies_per_slot">12</s:key>
          <s:key name="expected_total_per_slot">12</s:key>
        </s:dict>
      </s:key>
      <s:key name="2">
        <s:dict>
          <s:key name="actual_copies_per_slot">12</s:key>
          <s:key name="expected_total_per_slot">12</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
  <s:key name="searchable_copies_tracker">
    <s:dict>
      <s:key name="0">
        <s:dict>
          <s:key name="actual_copies_per_slot">12</s:key>
          <s:key name="expected_total_per_slot">12</s:key>
        </s:dict>
      </s:key>
      <s:key name="1">
        <s:dict>
          <s:key name="actual_copies_per_slot">12</s:key>
          <s:key name="expected_total_per_slot">12</s:key>
        </s:dict>
      </s:key>
      <s:key name="2">
        <s:dict>
          <s:key name="actual_copies_per_slot">12</s:key>
          <s:key name="expected_total_per_slot">12</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
  <s:key name="sort_order">4294967295</s:key>
  <s:key name="total_excess_bucket_copies">0</s:key>
</s:dict>
</content>
cluster/master/indexes/{name}

https://<host>:<mPort>/services/cluster/master/indexes/{name}
Access specific cluster index information.

GET
List {name} index information.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>buckets_with_excess_copies</td>
<td>Number of distinct buckets that have one or more excess replication copies.</td>
</tr>
<tr>
<td>buckets_with_excess_searchable_copies</td>
<td>Number of distinct buckets that have one or more excess searchable copies.</td>
</tr>
<tr>
<td>index_size</td>
<td>Size of the index</td>
</tr>
<tr>
<td>is_searchable</td>
<td>When every bucket in the index has a primary, the index is considered &quot;searchable&quot;.</td>
</tr>
<tr>
<td>non_site_aware_buckets_in_site_aware_cluster</td>
<td>Number of buckets created when the cluster was not in a multisite config. (Included only when the cluster is in multisite config.)</td>
</tr>
<tr>
<td>num_buckets</td>
<td>Total number of distinct buckets. Displays how many distinct buckets have X number of copies. One of the following options.</td>
</tr>
<tr>
<td>actual_copies_per_slot</td>
<td>Number of buckets with X copies.</td>
</tr>
<tr>
<td>expected_total_per_slot</td>
<td>Expected number of buckets with X copies.</td>
</tr>
<tr>
<td>searchable_copies_tracker</td>
<td>Displays how many distinct buckets have X number of searchable copies. One of the following options.</td>
</tr>
<tr>
<td>actual_copies_per_slot</td>
<td>Number of buckets with X searchable copies.</td>
</tr>
<tr>
<td>expected_total_per_slot</td>
<td>Expected number of buckets with X searchable copies.</td>
</tr>
<tr>
<td>sort_order</td>
<td>Used by UI.</td>
</tr>
</tbody>
</table>

267
<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>total_excess_bucket_copies</td>
<td>Total number of excess copies for all buckets.</td>
</tr>
<tr>
<td>total_excess_searchable_copies</td>
<td>Total number of excess searchable copies for all buckets.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/cluster/master/indexes/_audit
```

**XML Response**

```xml
<title>clustermasterpeerindexes</title>
<id>https://localhost:8089/services/cluster/master/indexes/_audit</id>
<updated>2014-04-17T19:11:14+00:00</updated>
<generator build="204899" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>_audit</title>
  <id>https://localhost:8089/services/cluster/master/indexes/_audit</id>
  <updated>2014-04-17T19:11:14+00:00</updated>
  <link href="/services/cluster/master/indexes/_audit" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/master/indexes/_audit" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="buckets_with_excess_copies">0</s:key>
      <s:key name="buckets_with_excess_searchable_copies">0</s:key>
      ... elided ...
      <s:key name="index_size">284975</s:key>
      <s:key name="is_searchable">1</s:key>
      <s:key name="non_site_aware_buckets_in_site_aware_cluster">6</s:key>
      <s:key name="num_buckets">12</s:key>
      <s:key name="replicated_copies_tracker">
        <s:dict>
          <s:dict>
            <s:key name="actual_copies_per_slot">12</s:key>
            <s:key name="expected_total_per_slot">12</s:key>
          </s:dict>
          <s:dict>
            <s:key name="actual_copies_per_slot">12</s:key>
            <s:key name="expected_total_per_slot">12</s:key>
          </s:dict>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```

268
Access information about cluster master node.

GET

List cluster master node details.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active_bundle</td>
<td>Provides information about the active bundle for this master.</td>
</tr>
<tr>
<td>bundle_creation_time_on_master</td>
<td>The time, in epoch seconds, when the bundle was created on the master.</td>
</tr>
<tr>
<td>bundle_validation_errors_on_master</td>
<td>A list of bundle validation errors.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>bundle_validation_in_progress</td>
<td>Indicates if bundle validation is in progress.</td>
</tr>
<tr>
<td>bundle_validation_on_master_succeeded</td>
<td>Indicates whether the master succeeded validating bundles.</td>
</tr>
<tr>
<td>data_safety_buckets_to_fix</td>
<td>Lists the buckets to fix for the completion of data safety.</td>
</tr>
<tr>
<td>gen_commit_buckets_to_fix</td>
<td>The buckets to be fixed before the next generation can be committed.</td>
</tr>
<tr>
<td>indexing_ready_flag</td>
<td>Indicates if the cluster is ready for indexing.</td>
</tr>
<tr>
<td>initialized_flag</td>
<td>Indicates if the cluster is initialized.</td>
</tr>
<tr>
<td>label</td>
<td>The name for the master. Displayed in the Splunk Web manager page.</td>
</tr>
<tr>
<td>latest_bundle</td>
<td>The most recent information reflecting any changes made to the master-apps configuration bundle.</td>
</tr>
<tr>
<td>In steady state, this is equal to active_bundle. If it is not equal, then pushing the latest bundle to all peers is in process (or needs to be started).</td>
<td></td>
</tr>
<tr>
<td>maintenance_mode</td>
<td>Indicates if the cluster is in maintenance mode.</td>
</tr>
<tr>
<td>reload_bundle Issued</td>
<td>Indicates if the bundle issued is being reloaded.</td>
</tr>
<tr>
<td>rep_count_buckets_to_fix</td>
<td>Number of buckets to fix on peers.</td>
</tr>
<tr>
<td>rolling_restart_flag</td>
<td>Indicates whether the master is restarting the peers in a cluster.</td>
</tr>
<tr>
<td>search_count_buckets_to_fix</td>
<td>Number of buckets to fix to satisfy the search count.</td>
</tr>
<tr>
<td>service_ready_flag</td>
<td>Indicates whether the master is ready to begin servicing, based on whether it is initialized.</td>
</tr>
<tr>
<td>start_time</td>
<td>Timestamp corresponding to the creation of the master.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/services/cluster/master/info
```

**XML Response**

```xml
<title>clustermasterinfo</title>
<id>http://greentea.sv.splunk.com:8089/services/cluster/master/info</id>
<updated>2013-07-23T10:36:35-07:00</updated>
<generator build="172635" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
<title>master</title>
<id>http://greentea.sv.splunk.com:8089/services/cluster/master/info/master</id>
<updated>2013-07-23T10:36:35-07:00</updated>
<link href="/services/cluster/master/info/master" rel="alternate"/>
<author>
  <name>system</name>
</author>
</entry>
```
<s:dict>
    <s:key name="active_bundle">
        <s:dict>
            <s:key name="bundle_path">
                /home/eserv/schoi/apple_master/splunk/var/run/splunk/cluster/remote-bundle/66e383ca8fff0f33e2341e35fc2e09-1374594357.bundle
            </s:key>
            <s:key name="checksum">
                a98f211c7bc6b4d4fe5775c7cd193
            </s:key>
            <s:key name="timestamp">
                1374594357
            </s:key>
        </s:dict>
    </s:key>
    <s:key name="bundle_creation_time_on_master">
        1374594357
    </s:key>
    <s:key name="bundle_validation_errors_on_master">
        <s:list />
    </s:key>
    <s:key name="bundle_validation_in_progress">
        0
    </s:key>
    <s:key name="bundle_validation_on_master_succeeded">
        1
    </s:key>
    <s:key name="data_safety_buckets_to_fix">
        <s:dict>
            <s:key name="_internal~1~05BB0AAC-61A5-491B-9153-3B02E6DA6130">
                <s:dict>
                    <s:key name="initial">
                        <s:dict>
                            <s:key name="reason">
                                resolved initial state
                            </s:key>
                            <s:key name="timestamp">
                                1374594631
                            </s:key>
                        </s:dict>
                    </s:key>
                    <s:key name="latest">
                        <s:dict>
                            <s:key name="reason"></s:key>
                            <s:key name="timestamp">
                                1374600995
                            </s:key>
                        </s:dict>
                    </s:key>
                </s:dict>
            </s:key>
            <s:key name="_internal~1~76AFDA4D-DAA7-48A8-A738-DD669A0853CD">
                <s:dict>
                    <s:key name="initial">
                        <s:dict>
                            <s:key name="reason">
                                resolved initial state
                            </s:key>
                            <s:key name="timestamp">
                                1374594631
                            </s:key>
                        </s:dict>
                    </s:key>
                    <s:key name="latest">
                        <s:dict>
                            <s:key name="reason"></s:key>
                            <s:key name="timestamp">
                                1374600995
                            </s:key>
                        </s:dict>
                    </s:key>
                </s:dict>
            </s:key>
            ...
            ...
            elided ...
            ...
            ...
            ...
            ...
        </s:dict>
    </s:key>
    
</s:dict>
<s:dict>
  <s:key name="reason">streaming success</s:key>
  <s:key name="timestamp">1374600995</s:key>
</s:dict>
<s:dict>
  <s:key name="latest">
    <s:dict>
      <s:key name="reason">streaming success</s:key>
      <s:key name="timestamp">1374600995</s:key>
    </s:dict>
  </s:key>
</s:dict>

... eai:acl node elided ...
<s:dict>
  <s:key name="gen_commit_buckets_to_fix">
    <s:dict>
      <s:key name="_internal~1~05BB0AAC-61A5-491B-9153-3B02E6DA6130">
        <s:dict>
          <s:key name="initial">
            <s:dict>
              <s:key name="reason">resolved initial state</s:key>
              <s:key name="timestamp">1374594631</s:key>
            </s:dict>
          </s:key>
        </s:dict>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason"></s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
      </s:dict>
      <s:key name="_internal~1~76AFDA4D-DAA7-48A8-A738-DD669A0853CD">
        <s:dict>
          <s:key name="initial">
            <s:dict>
              <s:key name="reason">resolved initial state</s:key>
              <s:key name="timestamp">1374594631</s:key>
            </s:dict>
          </s:key>
        </s:dict>
        <s:key name="latest">
          <s:dict>
            <s:key name="reason"></s:key>
            <s:key name="timestamp">1374600995</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:dict>
  </s:dict>
</s:dict>

272
<s:dict>
  <s:dict>
    <s:key name="latest">streaming success</s:key>
    <s:key name="timestamp">1374600995</s:key>
  </s:dict>
  <s:key name="indexing_ready_flag">1</s:key>
  <s:key name="initialized_flag">1</s:key>
  <s:key name="label">master_nc</s:key>
  <s:dict>
    <s:key name="bundle_path">/home/eserv/schoi/apple_master/splunk/var/run/splunk/cluster/remote-bundle/66e383c5f033e23a1e25fde09-1374594357.bundle</s:key>
    <s:key name="checksum">a98f211c7d6b141d4f5775c7cd193</s:key>
    <s:key name="timestamp">1374594357</s:key>
  </s:dict>
  <s:key name="maintenance_mode">0</s:key>
  <s:key name="reload_bundle_issued">0</s:key>
  <s:dict>
    <s:key name="_internal~1~05BB0AAC-61A5-491B-9153-3B02E6DA6130">
      <s:dict>
        <s:key name="initial">resolved initial state</s:key>
        <s:key name="timestamp">1374594631</s:key>
      </s:dict>
    </s:key>
    <s:dict>
      <s:key name="latest">
        <s:dict>
          <s:key name="reason"></s:key>
          <s:key name="timestamp">1374600995</s:key>
        </s:dict>
      </s:key>
    </s:dict>
    <s:dict>
      <s:key name="_internal~1~76AFDA4D-DA47-48A8-A738-DD669A0853CD">
        <s:dict>
          <s:key name="initial">resolved initial state</s:key>
          <s:key name="timestamp">1374594631</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:dict>
  <s:dict>
    <s:key name="_internal~1~6B338005-381B-4C1F-9B23-6E295EC10B62">.
  </s:dict>
  <s:dict>
    <s:key name="_internal~1~6B338005-381B-4C1F-9B23-6E295EC10B62">
      <s:dict>
        <s:key name="initial">resolved initial state</s:key>
        <s:key name="timestamp">1374594631</s:key>
      </s:dict>
    </s:key>
  </s:dict>
  <s:dict>
    <s:key name="_internal~1~6B338005-381B-4C1F-9B23-6E295EC10B62">.
  </s:dict>
  <s:dict>
    <s:key name="_internal~1~6B338005-381B-4C1F-9B23-6E295EC10B62">
      <s:dict>
        <s:key name="initial">resolved initial state</s:key>
        <s:key name="timestamp">1374594631</s:key>
      </s:dict>
    </s:key>
  </s:dict>
  <s:dict>
    <s:key name="_internal~1~6B338005-381B-4C1F-9B23-6E295EC10B62">
      <s:dict>
        <s:key name="initial">resolved initial state</s:key>
        <s:key name="timestamp">1374594631</s:key>
      </s:dict>
    </s:key>
  </s:dict>
  <s:dict>
    <s:key name="_internal~1~6B338005-381B-4C1F-9B23-6E295EC10B62">
      <s:dict>
        <s:key name="initial">resolved initial state</s:key>
        <s:key name="timestamp">1374594631</s:key>
      </s:dict>
    </s:key>
  </s:dict>
</s:dict>
elided

<s:dict>
  <s:key name="initial">
    <s:dict>
      <s:key name="reason">streaming success</s:key>
      <s:key name="timestamp">1374600995</s:key>
    </s:dict>
  </s:key>
  <s:key name="latest">
    <s:dict>
      <s:key name="reason">streaming success</s:key>
      <s:key name="timestamp">1374600995</s:key>
    </s:dict>
  </s:key>
</s:dict>

<s:key name="rolling_restart_flag">0</s:key>

<s:dict>
  <s:key name="_internal~1~05BB0AAC-61A5-491B-9153-3B02E6DA6130">
    <s:dict>
      <s:key name="initial">
        <s:dict>
          <s:key name="reason">resolved initial state</s:key>
          <s:key name="timestamp">1374594631</s:key>
        </s:dict>
      </s:key>
      <s:key name="latest">
        <s:dict>
          <s:key name="timestamp">1374600995</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
</s:dict>

<s:dict>
  <s:key name="_internal~1~76AFDA4D-DAA7-48A8-A738-DD669A0853CD">
    <s:dict>
      <s:key name="initial">
        <s:dict>
          <s:key name="reason">resolved initial state</s:key>
          <s:key name="timestamp">1374594631</s:key>
        </s:dict>
      </s:key>
      <s:key name="latest">
        <s:dict>
          <s:key name="timestamp">1374600995</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
</s:dict>

<s:dict>
  <s:key name="search_count_buckets_to_fix">
    <s:dict>
      <s:key name="_internal~1~05BB0AAC-61A5-491B-9153-3B02E6DA6130">
        <s:dict>
          <s:key name="initial">
            <s:dict>
              <s:key name="reason">resolved initial state</s:key>
              <s:key name="timestamp">1374594631</s:key>
            </s:dict>
          </s:key>
          <s:key name="latest">
            <s:dict>
              <s:key name="timestamp">1374600995</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
</s:dict>

274
cluster/master/peers

https://<host>:<mPort>/services/cluster/master/peers
Access cluster master peers.

See also
cluster/master/control/control/remove_peers

GET
List cluster master peers.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active_bundle_id</td>
<td>The ID of the configuration bundle currently being used by the master.</td>
</tr>
<tr>
<td>apply_bundle_status</td>
<td>Bundle status enumeration.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>base_generation_id</td>
<td>The initial bundle generation ID recognized by this peer. Any searches from previous generations fail. The initial bundle generation ID is created when a peer first comes online, restarts, or recontacts the master.</td>
</tr>
<tr>
<td>bucket_count</td>
<td>Count of the number of buckets on this peer, across all indexes.</td>
</tr>
<tr>
<td>bucket_count_by_index</td>
<td>Count of the number of buckets by index on this peer.</td>
</tr>
<tr>
<td>delayed_buckets_to_discard</td>
<td>List of bucket IDs waiting to be discarded on this peer.</td>
</tr>
<tr>
<td>fixup_set</td>
<td>The set of buckets that need repair once you take the peer offline.</td>
</tr>
<tr>
<td>heartbeat_started</td>
<td>Flag indicating if this peer has started heartbeating.</td>
</tr>
<tr>
<td>host_port_pair</td>
<td>The host and port advertised to peers for the data replication channel.</td>
</tr>
<tr>
<td></td>
<td>Can be either of the form IP:port or hostname:port.</td>
</tr>
<tr>
<td>is_searchable</td>
<td>Flag indicating if this peer belongs to the current committed generation and is searchable.</td>
</tr>
<tr>
<td>label</td>
<td>The name for the peer. Displayed on the manager page.</td>
</tr>
<tr>
<td>last_heartbeat</td>
<td>Timestamp for last heartbeat received from the peer.</td>
</tr>
<tr>
<td>latest_bundle_id</td>
<td>The ID of the configuration bundle this peer is using.</td>
</tr>
<tr>
<td>pending_job_count</td>
<td>Used by the master to keep track of pending jobs requested by the master to this peer.</td>
</tr>
<tr>
<td>primary_count</td>
<td>Number of buckets for which the peer is primary in its local site, or the number of buckets that return search results from same site as the peer.</td>
</tr>
<tr>
<td>primary_count_remote</td>
<td>Number of buckets for which the peer is primary that are not in its local site.</td>
</tr>
<tr>
<td>replication_count</td>
<td>Number of replications this peer is part of, as either source or target.</td>
</tr>
<tr>
<td>replication_port</td>
<td>TCP port to listen for replicated data from another cluster member.</td>
</tr>
<tr>
<td>replication_use_ssl</td>
<td>Indicates whether to use SSL when sending replication data.</td>
</tr>
<tr>
<td>search_state_counter</td>
<td>Lists the number of buckets on the peer for each search state for the bucket. Possible values for search state include:</td>
</tr>
<tr>
<td></td>
<td>Searchable</td>
</tr>
<tr>
<td></td>
<td>Unsearchable</td>
</tr>
<tr>
<td>site</td>
<td>To which site the peer belongs.</td>
</tr>
<tr>
<td>status</td>
<td>Indicates the status of the peer.</td>
</tr>
<tr>
<td></td>
<td>Valid values are:</td>
</tr>
<tr>
<td></td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>Pending</td>
</tr>
<tr>
<td></td>
<td>AutomaticDetention</td>
</tr>
<tr>
<td></td>
<td>ManualDetention-PortsEnabled</td>
</tr>
<tr>
<td></td>
<td>ManualDetention</td>
</tr>
<tr>
<td></td>
<td>Restarting</td>
</tr>
<tr>
<td></td>
<td>ShuttingDown</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>status_counter</td>
<td>Lists the number of buckets on the peer for each bucket status.</td>
</tr>
</tbody>
</table>

Possible values for bucket status:

- Complete: complete (warm/cold) bucket
- NonStreamingTarget: target of replication for already completed (warm/cold) bucket
- PendingTruncate: bucket pending truncation
- PendingDiscard: bucket pending discard
- Standalone: bucket that is not replicated
- StreamingError: copy of streaming bucket where some error was encountered
- StreamingSource: streaming hot bucket on source side
- StreamingTarget: streaming hot bucket copy on target side
- Unset: uninitialized

Example request and response

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/cluster/master/peers
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>clustermasterpeers</title>
  <id>https://localhost:8089/services/cluster/master/peers</id>
  <updated>2014-04-17T19:17:08+00:00</updated>
  <generator build="204899" version="6.1"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/master/peers/_new" rel="create"/>
  <opensearch:totalResults>6</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>238C3311-F0A4-4A9B-97F0-53667CFEEAB</title>
    <id>https://localhost:8089/services/cluster/master/peers/238C3311-F0A4-4A9B-97F0-53667CFEEAB</id>
    <updated>2014-04-17T19:17:08+00:00</updated>
    <link href="/services/cluster/master/peers/238C3311-F0A4-4A9B-97F0-53667CFEEAB" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/cluster/master/peers/238C3311-F0A4-4A9B-97F0-53667CFEEAB" rel="list"/>
    <link href="/services/cluster/master/peers/238C3311-F0A4-4A9B-97F0-53667CFEEAB" rel="edit"/>
    <content type="text/xml">
```

277
<entry>
  <title>E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C</title>
  <id>https://localhost:8089/services/cluster/master/peers/E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C</id>
  <updated>2014-04-17T19:17:08+00:00</updated>
  <link href="/services/cluster/master/peers/E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/master/peers/E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C" rel="list"/>
  <link href="/services/cluster/master/peers/E4B2C5E4-0961-4F3A-A5F7-C3A4BB6B518C" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="active_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
      <s:key name="apply_bundle_status">
        <s:dict>
          <s:key name="invalid_bundle">
            <s:dict>
              <s:key name="bundle_validation_errors">
                <s:list/>
              </s:key>
              <s:key name="invalid_bundle_id"></s:key>
            </s:dict>
            <s:key name="reload_error"></s:key>
            <s:key name="restart_required_for_apply_bundle">0</s:key>
          </s:dict>
        </s:dict>
      </s:key>
      <s:key name="base_generation_id">4</s:key>
      <s:key name="bucket_count">13</s:key>
      <s:dict>
        <s:key name="_audit">6</s:key>
        <s:key name="_internal">7</s:key>
      </s:dict>
      <s:key name="delayed_buckets_to_discard">
        <s:list/>
      </s:key>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="fixup_set">
        <s:list/>
      </s:key>
      <s:key name="heartbeat_started">1</s:key>
      <s:key name="host_port_pair">127.0.1.1:8094</s:key>
      <s:key name="is_searchable">1</s:key>
      <s:key name="label">s2p1</s:key>
      <s:key name="last_heartbeat">1397762227</s:key>
      <s:key name="latest_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
      <s:key name="pending_job_count">0</s:key>
      <s:key name="primary_count">7</s:key>
    </s:dict>
  </content>
</entry>
**cluster/master/peers/{name}**

https://<host>:<mPort>/services/cluster/master/peers/{name}

Access specified peer.

**GET**

Get {name} peer information.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>list_buckets</td>
<td>Boolean</td>
<td>Indicates whether to list the buckets for the peers to this master.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active_bundle_id</td>
<td>The ID of the configuration bundle currently being used by the master.</td>
</tr>
<tr>
<td>apply_bundle_status</td>
<td>Bundle status enumeration.</td>
</tr>
<tr>
<td>base_generation_id</td>
<td>The initial bundle generation ID recognized by this peer. Any searches from previous generations fail.</td>
</tr>
<tr>
<td></td>
<td>The initial bundle generation ID is created when a peer first comes online, restarts, or recontacts the master.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><code>bucket_count</code></td>
<td>Count of the number of buckets on this peer, across all indexes.</td>
</tr>
<tr>
<td><code>bucket_count_by_index</code></td>
<td>Count of the number of buckets by index on this peer.</td>
</tr>
<tr>
<td><code>delayed_buckets_to_discard</code></td>
<td>List of bucket IDs waiting to be discarded on this peer.</td>
</tr>
<tr>
<td><code>fixup_set</code></td>
<td>The set of buckets that need repair once you take the peer offline.</td>
</tr>
<tr>
<td><code>heartbeat_started</code></td>
<td>Flag indicating if this peer has started heartbeating.</td>
</tr>
<tr>
<td><code>host_port_pair</code></td>
<td>The host and port advertised to peers for the data replication channel. Can be either of the form IP:port or hostname:port.</td>
</tr>
<tr>
<td><code>is_searchable</code></td>
<td>Flag indicating if this peer belongs to the current committed generation and is searchable.</td>
</tr>
<tr>
<td><code>label</code></td>
<td>The name for the peer. Displayed on the Splunk Web manager page.</td>
</tr>
<tr>
<td><code>last_heartbeat</code></td>
<td>Timestamp for last heartbeat recieved from the peer.</td>
</tr>
<tr>
<td><code>latest_bundle_id</code></td>
<td>The ID of the configuration bundle this peer is using.</td>
</tr>
<tr>
<td><code>pending_job_count</code></td>
<td>Used by the master to keep track of pending jobs requested by the master to this peer.</td>
</tr>
<tr>
<td><code>primary_count</code></td>
<td>Number of buckets for which the peer is primary in its local site, or the number of buckets that return search results from same site as the peer.</td>
</tr>
<tr>
<td><code>primary_count_remote</code></td>
<td>Number of buckets for which the peer is primary that are not in its local site.</td>
</tr>
<tr>
<td><code>replication_count</code></td>
<td>Number of replications this peer is part of, as either source or target.</td>
</tr>
<tr>
<td><code>replication_port</code></td>
<td>TCP port to listen for replicated data from another cluster member.</td>
</tr>
<tr>
<td><code>replication_use_ssl</code></td>
<td>Indicates whether to use SSL when sending replication data.</td>
</tr>
</tbody>
</table>
| `search_state_counter`       | Lists the number of buckets on the peer for each search state for the bucket. Possible values for search state include: 
  - Searchable 
  - Unsearchable |
| `site`                       | To which site the peer belongs. |
| `splunk_version`             | The version of Splunk that the peer is running. This will be of the form X.Y.Z where X is the major version, Y is the minor version, and Z is the maintenance version. |
| `status`                     | Indicates the status of the peer. Valid values are: 
  - Up 
  - Pending 
  - AutomaticDetention 
  - ManualDetention-PortsEnabled 
  - ManualDetention 
  - Restarting 
  - ShuttingDown 
  - ReassigningPrimaries 
  - Decommissioning 
  - GracefulShutdown 
  - Stopped |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status_counter</td>
<td>Lists the number of buckets on the peer for each bucket status.</td>
</tr>
<tr>
<td></td>
<td>Possible values for bucket status:</td>
</tr>
<tr>
<td></td>
<td>Complete: complete (warm/cold) bucket</td>
</tr>
<tr>
<td></td>
<td>NonStreamingTarget: target of replication for already completed (warm/cold) bucket</td>
</tr>
<tr>
<td></td>
<td>PendingTruncate: bucket pending truncation</td>
</tr>
<tr>
<td></td>
<td>PendingDiscard: bucket pending discard</td>
</tr>
<tr>
<td></td>
<td>Standalone: bucket that is not replicated</td>
</tr>
<tr>
<td></td>
<td>StreamingError: copy of streaming bucket where some error was encountered</td>
</tr>
<tr>
<td></td>
<td>StreamingSource: streaming hot bucket on source side</td>
</tr>
<tr>
<td></td>
<td>StreamingTarget: streaming hot bucket copy on target side</td>
</tr>
<tr>
<td></td>
<td>Unset: uninitialized</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k-u admin:pass
https://localhost:8089/services/cluster/master/peers/29F9560E-A44A-425C-8753-1C6158B46C84

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>clustermasterpeers</title>
  <id>https://localhost:8089/services/cluster/master/peers</id>
  <updated>2014-04-17T19:18:19+00:00</updated>
  <generator build="204899" version="6.1"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/cluster/master/peers/_new" rel="create"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <opensearch:items/>
  <s:messages/>
  <s:messages/>
  <entry>
    <title>29F9560E-A44A-425C-8753-1C6158B46C84</title>
    <id>https://localhost:8089/services/cluster/master/peers/29F9560E-A44A-425C-8753-1C6158B46C84</id>
    <updated>2014-04-17T19:18:19+00:00</updated>
    <link href="/services/cluster/master/peers/29F9560E-A44A-425C-8753-1C6158B46C84" rel="alternate"/>
    <link href="/services/cluster/master/peers/29F9560E-A44A-425C-8753-1C6158B46C84" rel="list"/>
    <link href="/services/cluster/master/peers/29F9560E-A44A-425C-8753-1C6158B46C84" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="active_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
        <s:key name="apply_bundle_status">
          <s:dict>
            <s:key name="invalid_bundle">
          </s:dict>
        </s:dict>
      </s:dict>
    </content>
  </entry>
</feed>
```
<s:dict>
  <s:key name="bundle_validation_errors">
    </s:list/>
  </s:key>
  <s:key name="invalid_bundle_id"></s:key>
  </s:dict>
  <s:key name="reload_error"></s:key>
  <s:key name="restart_required_for_apply_bundle">0</s:key>
  </s:dict>
  <s:key name="base_generation_id">3</s:key>
  <s:key name="bucket_count">11</s:key>
  <s:key name="bucket_count_by_index">
    <s:dict>
      <s:key name="_audit">6</s:key>
      <s:key name="_internal">5</s:key>
    </s:dict>
    <s:key name="delayed_buckets_to_discard">
      </s:list/>
    </s:key>
    <s:key name="eai:acl">
      ... elided ...
    </s:key>
    <s:key name="eai:attributes">
      ... elided ...
    </s:key>
    <s:key name="fixup_set">
      </s:list/>
    </s:key>
    <s:key name="heartbeat_started">1</s:key>
    <s:key name="host_port_pair">127.0.0.1:8092</s:key>
    <s:key name="is_searchable">1</s:key>
    <s:key name="label">s1p3</s:key>
    <s:key name="last_heartbeat">1397762298</s:key>
    <s:key name="latest_bundle_id">4708B74780A1E5101449548B1E103616</s:key>
    <s:key name="pending_job_count">0</s:key>
    <s:key name="primary_count">6</s:key>
    <s:key name="primary_count_remote">2</s:key>
    <s:key name="replication_count">0</s:key>
    <s:key name="replication_port">9902</s:key>
    <s:key name="replication_use_ssl">0</s:key>
    <s:key name="search_state_counter">
      <s:dict>
        <s:key name="PendingSearchable">0</s:key>
        <s:key name="Searchable">8</s:key>
        <s:key name="SearchablePendingMask">0</s:key>
        <s:key name="Unsearchable">3</s:key>
      </s:dict>
    </s:key>
    <s:key name="site">site1</s:key>
    <s:key name="splunk_version">7.2.0</s:key>
    <s:key name="status">Up</s:key>
    <s:key name="status_counter">
      <s:dict>
        <s:key name="Complete">6</s:key>
        <s:key name="NonStreamingTarget">0</s:key>
        <s:key name="StreamingSource">2</s:key>
        <s:key name="StreamingTarget">3</s:key>
      </s:dict>
    </s:key>
  </s:key>
cluster/master/sites

https://<host>:<mPort>/services/cluster/master/sites
Access cluster site information.

GET

List available cluster sites.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peers</td>
<td>Peers list of host:port and server name.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/cluster/master/sites

XML Response

  <title>clustermastersites</title>
  <id>https://localhost:8089/services/cluster/master/sites</id>
  <updated>2014-04-17T19:12:15+00:00</updated>
  <generator build="204899" version="6.1"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>2</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>site1</title>
  </entry>
</feed>


<id>https://localhost:8089/services/cluster/master/sites/site1</id>
<updated>2014-04-17T19:12:15+00:00</updated>
<link href="/services/cluster/master/sites/site1" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/cluster/master/sites/site1" rel="list"/>

<content type="text/xml">
  
  <s:dict>
    <s:key name="eai:acl">
      ... elided ...
    </s:key>
    <s:key name="peers">
      
      <s:dict>
        <s:key name="29F956D0E-A44A-425C-8753-1C6158B46C84">
          
          <s:dict>
            <s:key name="host_port_pair">127.0.1.1:8092</s:key>
            <s:key name="server_name">s1p3</s:key>
          </s:dict>
        </s:key>
        
        <s:key name="61666763-43E9-411B-9464-D80A5119E0E">
          
          <s:dict>
            <s:key name="host_port_pair">127.0.1.1:8091</s:key>
            <s:key name="server_name">s1p2</s:key>
          </s:dict>
        </s:key>
        
        <s:key name="76C88808-2727-42B4-8C05-72DC44630F4">
          
          <s:dict>
            <s:key name="host_port_pair">127.0.1.1:8090</s:key>
            <s:key name="server_name">s1p1</s:key>
          </s:dict>
        </s:key>
        
        <s:dict>
        </s:dict>
        
        <s:dict>
        </s:dict>
        
      </s:dict>
    </s:key>
    
  </s:dict>
  
</content>

</entry>

<entry>
  
  <id>https://localhost:8089/services/cluster/master/sites/site2</id>
  <updated>2014-04-17T19:12:15+00:00</updated>
  <link href="/services/cluster/master/sites/site2" rel="alternate"/>
  
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/master/sites/site2" rel="list"/>
  
  <content type="text/xml">
    
    <s:dict>
      <s:key name="eai:acl">
        ... elided ...
      </s:key>
      <s:key name="peers">
        
        <s:dict>
          <s:key name="238C3311-F0A4-4A9B-97F0-53667CFFFEA8">
            
            <s:dict>
              <s:key name="host_port_pair">127.0.1.1:8096</s:key>
              <s:key name="server_name">s2p3</s:key>
            </s:dict>
          </s:key>
          
          <s:dict>
            <s:key name="host_port_pair">127.0.1.1:8095</s:key>
          </s:dict>
        </s:dict>
      </s:key>
      
    </s:dict>
    
  </content>

</entry>
cluster/master/sites/{name}

https://<host>:<mPort>/services/cluster/master/sites/{name}

Access specific cluster site information.

GET

List the {name} cluster site information.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peers</td>
<td>Site peer reference, for each peer. Possible values include the following.</td>
</tr>
<tr>
<td>host_port_pair</td>
<td>Peer port number.</td>
</tr>
<tr>
<td>server_name</td>
<td>Peer server name.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/cluster/master/sites/site1

XML Response

<title>clustermastersites</title>
<id>https://localhost:8089/services/cluster/master/sites</id>
<updated>2014-04-17T19:13:07+00:00</updated>
<generator build="204899" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>site1</title>
  <id>https://localhost:8089/services/cluster/master/sites/site1</id>
  <updated>2014-04-17T19:13:07+00:00</updated>
  <link href="/services/cluster/master/sites/site1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/master/sites/site1" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        ...
      </s:key>
      <s:key name="eai:attributes">
        ...
      </s:key>
      <s:key name="peers">
        <s:dict>
          <s:key name="29F9560E-A44A-425C-8753-1C6158B46C84">
            <s:dict>
              <s:key name="host_port_pair">127.0.1.1:8092</s:key>
              <s:key name="server_name">s1p3</s:key>
            </s:dict>
          </s:key>
          <s:key name="61666763-43E9-411B-9464-D80A5119EF0E">
            <s:dict>
              <s:key name="host_port_pair">127.0.1.1:8091</s:key>
              <s:key name="server_name">s1p2</s:key>
            </s:dict>
          </s:key>
          <s:key name="76C88808-2727-42B4-8C05-72DC44630FE4">
            <s:dict>
              <s:key name="host_port_pair">127.0.1.1:8090</s:key>
              <s:key name="server_name">s1p1</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
# cluster/master/status

**https://<host>:{mPort}/services/cluster/master/status**

Endpoint to get the status of a rolling restart.

## GET

Get the status of a rolling restart.

### Request parameters

Pagination and filtering parameters can be used with this method.

### Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>decommission_force_timeout</td>
<td>The amount of time, in seconds, the cluster master will wait for a peer in primary decommission status to finish primary reassignment and restart, during a searchable rolling restart with timeouts. Only valid for rolling_restart-searchable_force. Default value is 180. Max accepted value is 1800.</td>
</tr>
<tr>
<td>maintenance_mode</td>
<td>Indicates if the cluster is in maintenance mode. Happens during rolling restart, bundle push, and other maintenance activities.</td>
</tr>
<tr>
<td>messages</td>
<td>Array of messages from server.</td>
</tr>
<tr>
<td>multisite</td>
<td>Indicates if multisite is enabled for this master. Make sure you set site parameters on the peers if you set this to true. Defaults to false.</td>
</tr>
<tr>
<td>peers</td>
<td>Object containing all the peers in the cluster. For each peer, the label, site and status are provided.</td>
</tr>
<tr>
<td>restart_inactivity_timeout</td>
<td>The amount of time, in seconds, that the master waits for a peer to restart and rejoin the cluster before it considers the restart a failure and proceeds to restart other peers. A value of zero (0) means that the master waits indefinitely for a peer to restart. Only valid for rolling_restart-searchable_force. Default is 600secs.</td>
</tr>
<tr>
<td>restart_progress</td>
<td>Object containing lists of peers in &quot;done&quot;, &quot;failed&quot;, &quot;in_progress&quot; and &quot;to_be_restarted&quot; state.</td>
</tr>
<tr>
<td>rolling_restart_flag</td>
<td>Boolean that indicates if there is a rolling restart in progress.</td>
</tr>
<tr>
<td>rolling_restart_or_upgrade</td>
<td>Boolean that indicates if there is a rolling restart or rolling upgrade in progress.</td>
</tr>
<tr>
<td>searchable_rolling</td>
<td>Boolean that indicates if a searchable rolling restart/upgrade in progress.</td>
</tr>
<tr>
<td>service_ready_flag</td>
<td>Boolean that indicates if the cluster is ready.</td>
</tr>
</tbody>
</table>

### Example request and response

**XML Request**

```xml
<Request>
    ...<response>
```

288
curl -k -u admin:pass https://localhost:8089/services/cluster/master/status

XML Response

<title>clustermasterstatus</title>
<id>https://10.141.65.179:52000/services/cluster/master/status</id>
<updated>2018-04-01T23:00:53+00:00</updated>
<generator build="b233a6c1ade2" version="7.2.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/master/status/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>master</title>
  <id>https://10.141.65.179:52000/services/cluster/master/status/master</id>
  <updated>1970-01-01T00:00:00+00:00</updated>
  <link href="/services/cluster/master/status/master" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/cluster/master/status/master" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="decommission_force_timeout">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:dict>
      </s:key>
      <s:key name="maintenance_mode">0</s:key>
      <s:key name="messages"></s:key>
      <s:key name="multisite">0</s:key>
      <s:key name="peers">
        <s:dict>
          <s:key name="08696C19-548F-4563-BA53-2A18769091DB">
            289
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
cluster/searchhead/generation

https://<host>:<mPort>/services/cluster/searchhead/generation
Access peer information in a cluster searchhead.

GET

List peers available to a cluster searchhead.
Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation_id</td>
<td>The current generation ID for this searchhead, which is part of a cluster configuration. The search head uses this information to determine which buckets to search across.</td>
</tr>
<tr>
<td>generation_peers</td>
<td>List of peer nodes for the current generation in the cluster configuration for this searchhead.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

`curl -k -u admin:pass https://localhost:8089/services/cluster/searchhead/generation`

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
 xmlns:s="http://dev.splunk.com/ns/rest"
 xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
 <title>clustersearchheadgeneration</title>
 <id>https://localhost:8089/services/cluster/searchhead/generation</id>
 <updated>2012-09-05T11:13:45-07:00</updated>
 <generator build="136169" version="5.0"/>
 <author>
   <name>Splunk</name>
 </author>
 ... opensearch nodes elided ...
 <s:messages/>
 <entry>
   <title>master</title>
   <id>https://localhost:8089/services/cluster/searchhead/generation/master</id>
   <updated>2012-09-05T11:13:45-07:00</updated>
   <link href="/services/cluster/searchhead/generation/master" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/cluster/searchhead/generation/master" rel="list"/>
   <content type="text/xml">
     <s:dict>
       ... eai:acl node elided ...
     <s:key name="generation_id">2</s:key>
     <s:key name="generation_peers">
       <s:dict>
         <s:key name="2AF11DD4-1424-4A14-A522-FB9D055E9516">splunks-ombra.sv.splunk.com:8389</s:key>
         <s:key name="peer">splunks-ombra.sv.splunk.com</s:key>
       </s:dict>
     </s:dict>

   </content>
 </entry>
</feed>
```
cluster/searchhead/generation/{name}

https://<host>:<mPort>/services/cluster/searchhead/generation/{name}
Access peer of the master URI.

GET

Get {name} searchhead generation ID and generation peers.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation_id</td>
<td>The current generation ID for this searchhead, which is part of a cluster configuration. The search head uses this information to determine which buckets to search across.</td>
</tr>
<tr>
<td>generation_peers</td>
<td>List of peer nodes for the current generation in the cluster configuration for this searchhead.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass
https://localhost:8089/services/cluster/searchhead/generation/https%3A%252F%252Fmyserver-mbp15.sv.splunk.com%3A8989

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <entry>
    ...
  </entry>
</feed>
**cluster/searchhead/searchheadconfig**

https://<host>:<mPort>/services/cluster/searchhead/searchheadconfig

Access cluster searchhead node configuration.
GET

List this cluster search head node configuration.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/cluster/searchhead/searchheadconfig

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
    <title>clustersearchheadconfig</title>
    <id>https://localhost:8089/services/cluster/searchhead/searchheadconfig</id>
    <updated>2013-10-31T14:04:45-07:00</updated>
    <generator build="184661" version="20131030"/>
    <author>
        <name>Splunk</name>
    </author>
    <link href="/services/cluster/searchhead/searchheadconfig/_new" rel="create"/>
    <link href="/services/cluster/searchhead/searchheadconfig/_reload" rel="_reload"/>
    ... opensearch nodes elided ... 
    <s:messages/>
    <entry>
        <title>https://localhost:4567</title>
        <updated>2013-10-31T14:04:45-07:00</updated>
        <link href="/services/cluster/searchhead/searchheadconfig/https%3A%2F%2Flocalhost%3A4567" rel="alternate"/>
        <author>
            <name>system</name>
        </author>
        <link href="/services/cluster/searchhead/searchheadconfig/https%3A%2F%2Flocalhost%3A4567" rel="list"/>
        <link href="/services/cluster/searchhead/searchheadconfig/https%3A%2F%2Flocalhost%3A4567/_reload" rel="_reload"/>
        <link href="/services/cluster/searchhead/searchheadconfig/https%3A%2F%2Flocalhost%3A4567/edit" rel="edit"/>
        <link href="/services/cluster/searchhead/searchheadconfig/https%3A%2F%2Flocalhost%3A4567/remove" rel="remove"/>
        <content type="text/xml">
            <s:dict>
                ... eai:acl node elided ...
                <s:key name="master_uri">https://localhost:4567</s:key>
            </s:dict>
        </content>
    </entry>
</feed>
POST

Configure this server as a cluster searchhead node.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required. The URI of the master node in the cluster.</td>
</tr>
<tr>
<td>secret</td>
<td>String</td>
<td>Required. Secret shared among the nodes in the cluster to prevent any arbitrary node from connecting to the cluster. If a peer or searchhead is not configured with the same secret as the master, it is not able to communicate with the master. Corresponds to pass4SymmKey setting in server.conf.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request


XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:s="http://dev.splunk.com/ns/rest"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
><title>clustersearchheadconfig</title>
/id>https://localhost:8089/services/cluster/searchhead/searchheadconfig</id>
<updated>2013-10-31T14:04:45-07:00</updated>
<generator build="184661" version="20131030"/>
<author>
  <name>Splunk</name>
</author>
<s:messages/>
<entry>
  <title>https://localhost:4567</title>
  <id>https://myserver:8089/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567</id>
  <updated>2013-10-31T14:04:45-07:00</updated>
  <link href="https://myserver:8089/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567" rel="alternate"/>
</entry></feed>
cluster/searchhead/searchheadconfig/{name}

Manage node in a cluster.

DELETE

Remove node from cluster.

Request parameters

None

Returned values

None

Example request and response

XML Request

curl -k -u admin:changeme --request DELETE
https://myserver.splunk.com:8089/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Fmyserver%3A8211

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest"
GET

List cluster search head node configuration.

Request parameters

None

Returned values

None

Example request and response

XML Request

curl -k -u admin:pass
https://myserver.splunk.com:7588/services/cluster/searchhead/searchheadconfig/https%3A%252F%252Flocalhost%3A4567

XML Response

<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:s="http://dev.splunk.com/ns/rest"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
  xmlns:clustersearchheadconfig=""
  xmlns:searchheadconfig="/services/cluster/searchhead/searchheadconfig"</feed>
POST

Update cluster search head node configuration.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>master_uri</td>
<td>String</td>
<td>The URI of the master node in the cluster for which this searchhead is configured.</td>
</tr>
<tr>
<td>secret</td>
<td>String</td>
<td>Secret shared among the nodes in the cluster to prevent any arbitrary node from connecting to the cluster. If a peer or searchhead is not configured with the same secret as the master, it is not able to communicate with the master. Corresponds to pass4SymmKey setting in server.conf.</td>
</tr>
</tbody>
</table>

Returned values

None

cluster/slave/buckets

https://<host>::<mPort>/services/cluster/slave/buckets

Access cluster peers bucket configuration.

GET

List cluster peers bucket configuration.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation_id</td>
<td>String</td>
<td>The generation ID for this peer. For each generation, the master server in a cluster configuration assigns generation IDs. A generation identifies which copies of a cluster's buckets are primary and therefore can participate in a search.</td>
</tr>
</tbody>
</table>

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>checksum</td>
<td>Used internally to identify this bucket.</td>
</tr>
<tr>
<td>earliest_time</td>
<td>Indicates the time of the earliest event in this bucket.</td>
</tr>
<tr>
<td>generation_id</td>
<td>The generation ID for this peer.</td>
</tr>
<tr>
<td>generations</td>
<td>A sparse list of generation id to bucket primacy for the given peer.</td>
</tr>
<tr>
<td>latest_time</td>
<td>Indicates the time for the latest event in this bucket.</td>
</tr>
<tr>
<td>search_state</td>
<td>Indicates if the bucket is searchable or unsearchable.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Status</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>The copy of this bucket contains the full complement of information.</td>
</tr>
<tr>
<td>StreamingSource</td>
<td>The copy of this bucket is sending data to peer nodes for replication.</td>
</tr>
<tr>
<td>StreamingTarget</td>
<td>The copy of this bucket is receiving replicated data.</td>
</tr>
<tr>
<td>NonStreamingTarget</td>
<td>This copy of a warm bucket replication is in progress. Once replication is complete, the status changes to Complete.</td>
</tr>
<tr>
<td>StreamingError</td>
<td>The copy of this bucket encountered errors while streaming data.</td>
</tr>
<tr>
<td>PendingTruncate</td>
<td>The master asked the peer to truncate this copy of the bucket to a certain size and is waiting for confirmation.</td>
</tr>
<tr>
<td>PendingDiscard</td>
<td>The master asked the peer to discard this copy of the bucket (for whatever reason, and is waiting for confirmation.</td>
</tr>
<tr>
<td>Standalone</td>
<td>A bucket in the cluster that is not replicated.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8189/services/cluster/slave/buckets
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>clusterslavebuckets</title>
  <id>https://localhost:8189/services/cluster/slave/buckets</id>
  <updated>2012-09-05T12:29:42-07:00</updated>
  <generator build="136169" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>_audit~0~2AF11DD4-1424-4A14-A522-FB9D055E9516</title>
    <id>https://localhost:8189/services/cluster/slave/buckets/_audit~0~2AF11DD4-1424-4A14-A522-FB9D055E9516</id>
  </entry>
</feed>
```
cluster/slave/buckets/{name}

https://<host>:<mPort>/services/cluster/slave/buckets/{name}
Manage peer buckets.

DELETE
Remove specified bucket from peer node.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket_id</td>
<td>String</td>
<td>Required. The identifier for the bucket to remove.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
```

301
GET

List peer specified bucket information.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>generation_id</td>
<td>String</td>
<td>The generation ID for this peer. For each generation, the master server in a cluster configuration assigns generation IDs. A generation identifies which copies of a cluster's buckets are primary and therefore can participate in a search.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>checksum</td>
<td>Used internally to identify this bucket.</td>
</tr>
<tr>
<td>earliest_time</td>
<td>Indicates the time of the earliest event in this bucket.</td>
</tr>
<tr>
<td>generation_id</td>
<td>The generation ID for this peer.</td>
</tr>
<tr>
<td>generations</td>
<td>A sparse list of generation id to bucket primacy for the given peer.</td>
</tr>
<tr>
<td>latest_time</td>
<td>Indicates the time for the latest event in this bucket.</td>
</tr>
<tr>
<td>search_state</td>
<td>Indicates if the bucket is Searchable or Unsearchable.</td>
</tr>
<tr>
<td>status</td>
<td>Indicates the status of this bucket. One of the following values. Complete The copy of this bucket contains the full complement of information. StreamingSource The copy of this bucket is sending data to peer nodes for replication.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
StreamingTarget | The copy of this bucket is receiving replicated data.
NonStreamingTarget | This copy of a warm bucket replication is in progress. Once replication is complete, the status changes to Complete.
StreamingError | The copy of this bucket encountered errors while streaming data.
PendingTruncate | The master asked the peer to truncate this copy of the bucket to a certain size and is waiting for confirmation.
PendingDiscard | The master asked the peer to discard this copy of the bucket (for whatever reason, and is waiting for confirmation.
Standalone | A bucket in the cluster that is not replicated.

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass
https://localhost:8189/services/cluster/slave/buckets/_audit~0~B8B5E5C6-DB26-4952-AFB1-C5EFEFFF0EA31
```

**XML Response**

```xml
curl -k -u admin:pass
https://localhost:8189/services/cluster/slave/buckets/_audit~0~B8B5E5C6-DB26-4952-AFB1-C5EFEFFF0EA31
```

```xml
<xml>
  <title>clusterslavebuckets</title>
  <id>https://localhost:8189/services/cluster/slave/buckets</id>
  <updated>2012-09-05T12:40:43-07:00</updated>
  <generator build="136169" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>_internal~1~50FCDB42-E167-458D-A6A9-E4587E8F16D9</title>
    <id>https://localhost:8189/services/cluster/slave/buckets/_internal~1~50FCDB42-E167-458D-A6A9-E4587E8F16D9</id>
    <updated>2012-09-05T12:40:43-07:00</updated>
    <link href="/services/cluster/slave/buckets/_internal~1~50FCDB42-E167-458D-A6A9-E4587E8F16D9" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/cluster/slave/buckets/_internal~1~50FCDB42-E167-458D-A6A9-E4587E8F16D9" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:dict>
          <s:dict>
            <s:key name="checksum""></s:key>
            ... eai:acl node elided ...
            <s:dict>
              <s:dict>
                <s:key name="optionalFields""></s:key>
                <s:list/>
              </s:dict>
            </s:dict>
          </s:dict>
        </s:dict>
      </s:dict>
    </content>
</entry>
</xml>
```
cluster/slave/control/control/decommission

https://<host>:<mPort>/services/cluster/slave/control/control/decommission

Endpoint to decommission an indexer cluster peer node.

POST

Decommission a peer node.

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass https://indexer:8089/services/cluster/slave/control/control/decommission -X POST

XML Response

<title>clusterslavecontrol</title>
<id>https://10.141.66.19:46772/services/cluster/slave/control</id>
<updated>2018-04-01T21:23:46+00:00</updated>
<generator build="b233a6c1ade2" version="7.2.0"/>
<author>
  <name>Splunk</name>
</author>
304
cluster/slave/control/control/re-add-peer

https://<host>:<mPort>/services/cluster/slave/control/control/re-add-peer

Set the peer to re-add itself to the master. This syncs the peer's state, including its in-memory bucket state, to the master. By default, this resets the peer's primary bucket copies and the master reassigns them across the cluster. To keep the peer's existing primary bucket copies, use the optional clearMasks=false parameter.

This endpoint can be useful when the master and the peer have a state mismatch, for example when bucket information is not in sync between them.

POST

Re-add the cluster indexer to the cluster master.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clearMasks</td>
<td>Boolean. Use</td>
<td>true</td>
<td>Optional. Indicates whether the master should reassign all primary bucket</td>
</tr>
<tr>
<td></td>
<td>true or false</td>
<td></td>
<td>copies across all peers. The default true value prompts the master to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>reassign all primary bucket copies across all peers. Use false to re-add</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>the peer but keep the existing primary bucket copies.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -k -u admin:changeme https://localhost:8089/services/cluster/slave/control/control/re-add-peer -d clearMasks=false -X POST
```

XML Response

```xml
<title>clusterslavecontrol</title>
{id}https://localhost:8089/services/cluster/slave/control</id>
<updated>2015-11-06T18:08:54-08:00</updated>
<generator build="802b4e159bb584c629dcd8ba57c409b15d7ab" version="20151030"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/cluster/slave/control/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```
cluster/slave/control/control/set_detention_override

https://<host>:<mPort>/services/cluster/slave/control/control/set_manual_detention

Deprecated. Use /set_manual_detention to manage peer node manual detention mode.

cluster/slave/control/control/set_manual_detention

https://<host>:<mPort>/services/cluster/slave/control/control/set_manual_detention
If you have Splunk Enterprise, you can use this endpoint to put the peer node in manual detention mode or take the peer out of this mode. In manual detention, the peer does not serve as a replication target. Detention helps slow the growth of disk usage on the peer.

Note:

- This endpoint replaces the /set_detention_override endpoint.
- Starting with Splunk Enterprise software version 6.5, manual detention persists through restarts.
- For more information, see Put a peer in detention in Managing Indexers and Clusters of Indexers.

**POST**

Adjust cluster peer detention mode.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>manual_detention</td>
<td>Use one of the following values.</td>
<td>Enable or disable manual detention. Opt to close data ports or leave them open when manual detention is enabled.</td>
</tr>
<tr>
<td></td>
<td>• off: <strong>Default</strong>: Remove the indexer from the detention state.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• on: Put the indexer in manual detention mode. Close the TCP, UDP, and HTTP Event Collector data ports. Closing the ports causes most external data indexing to stop during detention.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• on_ports_enabled: Put the indexer in manual detention mode. Do not close the TCP, UDP, or HTTP Event Collector data ports. The peer continues to index data during detention.</td>
<td></td>
</tr>
</tbody>
</table>

** Returned values**

None

**Example request and response**

**XML Request**

```
curl -k -u admin:password https://localhost:8089/services/cluster/slave/control/control/set_manual_detention
```

306
-d manual_detention-on

**XML Response**

```xml
<xml response>

<title>clusterslavecontrol</title>
<id>https://localhost:8089/services/cluster/slave/control</id>
<updated>2016-11-15T20:33:01-08:00</updated>
<generator build="f3ca72fbbf1234a88e7a5af9d073ae698f264de6" version="20161115"/>
<author>
    <name>Splunk</name>
</author>
<link href="/services/cluster/slave/control/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
</xml response>
```

---

### cluster/slave/info

**https://<host>:<mPort>/services/cluster/slave/info**

Access cluster peer node information.

**GET**

List peer information.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active_bundle</td>
<td>Current bundle being used by this peer.</td>
</tr>
<tr>
<td>base_generation_id</td>
<td>The initial bundle generation ID recognized by this peer. Any searches from previous generations fail.</td>
</tr>
<tr>
<td></td>
<td>The initial bundle generation ID is created when a peer first comes online, restarts, or recontacts the master.</td>
</tr>
<tr>
<td>invalid_bundle_ids</td>
<td>List of bundle ids with validation errors in the peer.</td>
</tr>
<tr>
<td>is_registered</td>
<td>Indicates if this peer is registered with the master in the cluster.</td>
</tr>
<tr>
<td>last_heartbeat_attempt</td>
<td>Timestamp for the last attempt to contact the master.</td>
</tr>
</tbody>
</table>

307
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>latest_bundle</td>
<td>Lists information about the most recent bundle downloaded from the master.</td>
</tr>
<tr>
<td>restart_state</td>
<td>Indicates whether the peer needs to be restarted to enable its cluster configuration.</td>
</tr>
</tbody>
</table>

**status**

Indicates the status of the peer. One of the following values.

- Up
- Down
- Pending
- Detention
- Restarting
- Decommissioning
- Decommissioned

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8189/services/cluster/slave/info

**XML Response**

```
<entry>
<title>slave</title>
<id>https://localhost:8189/services/cluster/slave/info/slave</id>
<updated>2012-09-05T12:45:59-07:00</updated>
<link href="/services/cluster/slave/info/slave" rel="alternate"/>
<author>
  <name>system</name>
</author>
<content type="text/xml">
  <s:dict>
    <s:dict>
      <s:key name="active_bundle">
        <s:dict>
          <s:key name="bundle_path">/Applications/splunk-peer/var/run/splunk/cluster/remote-bundle/0f607895127ab1f715ee78a6e1ff8a1-1346858928.bundle</s:key>
          <s:key name="checksum">36a883f4d47af66f78531ef474349b59</s:key>
          <s:key name="timestamp">1346858928</s:key>
        </s:dict>
      </s:dict>
      <s:key name="base_generation_id">2</s:key>
    </s:dict>
  </s:dict>
</entry>
```

308
Search head cluster endpoints

The endpoints in this section pertain to search head clusters.

All endpoints contain `shcluster` in their URIs pertain to search head clusters. For more information about search head clustering architecture, see Search head clustering architecture in the Distributed Search manual.

**replication/configuration/health**

```plaintext
https://<host>:<mPort>/services/replication/configuration/health
```

Access configuration replication health statistics for a search head cluster.

**GET**

Access the configuration replication health statistics for a search head cluster.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bookmark</td>
<td>Boolean</td>
<td>Use this parameter with a GET request on the captain. Set to 1 to list the most recent changesets that members pulled from the captain. A timestamp is also returned for each changeset.</td>
</tr>
<tr>
<td>check_share_baseline</td>
<td>Boolean</td>
<td>Set to 1 to check for a shared baseline among members. This parameter can be used with a request on any member, including the captain.</td>
</tr>
<tr>
<td>unpublished</td>
<td>Boolean</td>
<td>Set to 1 to check for unpublished changes on members. Use this parameter with a request on a member to check if the member has any changes that have not been pushed to the captain.</td>
</tr>
</tbody>
</table>

**Returned values**

Values returned depend on the request parameters used.

| bookmark |
For each [server_name] member, a changeset and timestamp are shown, indicating when the [server_name] member last pulled this set of configuration changes from the captain.

Example request and response

curl -k -u admin:pass https://localhost:8089/services/replication/configuration/health?bookmark=1


check_share_baseline

Application usage
This parameter compares the baseline between the current instance, on which the GET request is made, with the baseline of other members. From each of the other members, the system retrieves the oldest changeset that is not more than 23 hours old and therefore safe from purging. The system then tries to find that changeset in the current instance’s local changeset repository. If the changeset is found in the local repository, then the current instance and the member share a baseline.

Establishing a shared baseline between a captain and members is a prerequisite for successful configuration replication.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>check_share_baseline</td>
<td>One of the following values is returned for each of the other members.</td>
</tr>
<tr>
<td>Yes:</td>
<td>The current instance shares a baseline with this node.</td>
</tr>
<tr>
<td>No:</td>
<td>The current instance node does not share a baseline with this node.</td>
</tr>
<tr>
<td>Connection error:</td>
<td>The current instance cannot contact this node. A warning is logged with</td>
</tr>
<tr>
<td></td>
<td>additional details.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>server_name</td>
<td>Name for the member whose baseline is being compared to the current instance.</td>
</tr>
</tbody>
</table>

Example request and response

curl -k -u admin:pass
https://localhost:11089/services/replication/configuration/health?check_share_baseline=1

...<title>health</title>
$id>https://localhost:11089/services/replication/configuration/health</id>
$updated>2016-08-09T15:51:06-07:00</updated>
$generator build="99005df760a86096252bb6b287ad7a6f3149a218" version="20160805"/>
$author>
$name>Splunk</name>
$author>
$entry>
$title>https://localhost:8089</title>
$id>https://localhost:11089/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A8089</id>
$updated>2016-08-09T15:51:06-07:00</updated>
$link href="/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A8089" rel="alternate"/>
$content type="text/xml">
<s:dict>
 <s:key name="check_share_baseline">Yes</s:key>
 <s:key name="server_name">yxu-mbp15-node2</s:key>
</s:dict>
</content>
</entry>
$entry>
$title>https://localhost:9089</title>
$id>https://localhost:11089/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A9089</id>
$updated>2016-08-09T15:51:06-07:00</updated>
$link href="/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A9089" rel="alternate"/>
$content type="text/xml">
<s:dict>
 <s:key name="check_share_baseline">Yes</s:key>
 <s:key name="server_name">localhost-node3</s:key>
</s:dict>
</content>
</entry>
$entry>
$title>https://localhost:11089</title>
$id>https://localhost:11089/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A11089</id>
$updated>2016-08-09T15:51:06-07:00</updated>
$link href="/services/replication/configuration/health/https%3A%2F%2Flocalhost%3A11089" rel="alternate"/>
$content type="text/xml">
<s:dict>
 <s:key name="check_share_baseline">Yes</s:key>
 <s:key name="server_name">localhost-node1</s:key>
</s:dict>
</content>
</entry>
...unpublished

A Number of unpublished changes key is returned with one of the following values.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
All changes on this cluster member have been pushed to the captain. There are no unpublished changes on this member.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 (This instance is the captain)</td>
<td>This message is returned when requesting unpublished status on the captain. The captain is always in sync with itself, so there are no unpublished changes.</td>
</tr>
<tr>
<td>[Number greater than 0]</td>
<td>The number unpublished local changes on this member. Changes are held until the next replication occurs. The node is still healthy in this case.</td>
</tr>
<tr>
<td>No captain is available</td>
<td>The search head cluster does not currently have a captain.</td>
</tr>
<tr>
<td>Missing common baseline with the captain</td>
<td>This member might be out of sync with the captain if this message persists after several replication periods. This message can also appear during a transition period, for example, when a captain is switched or a member is manually resynced. On a healthy search head cluster, the unpublished value should return to a numeric value after one replication period.</td>
</tr>
</tbody>
</table>

Example request and response

curl -k -u admin:pass https://localhost:11089/services/replication/configuration/health?unpublished=1

```
<title>health</title>
<id>https://localhost:8089/services/replication/configuration/health</id>
<updated>2016-08-09T13:14:16-07:00</updated>
<generator build="99005df760a86096252bb6b287ad7a6f3149a218" version="20160805"/>
<author>
  <name>Splunk</name>
</author>
<entry>
  <title>unpublished</title>
  <id>https://localhost:8089/services/replication/configuration/health/unpublished</id>
  <updated>2016-08-09T13:14:16-07:00</updated>
  <link href="/services/replication/configuration/health/unpublished" rel="alternate"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="Number of unpublished changes">0</s:key>
    </s:dict>
  </content>
</entry>
```

shcluster/captain/artifacts

https://<host>:<mPort>/services/shcluster/captain/artifacts

Provides list of artifacts and replicas currently managed by the captain across a search head cluster.

This endpoint can only be accessed on the captain. The response lists all artifacts that are currently resident on the set of search head cluster members.

An artifact in search head clustering is a managed search directory. Currently, only scheduled search results directories are managed and replicated according to replication policy.
Note: Ad hoc searches are not considered artifacts and are not listed.

GET

Lists search head cluster artifacts and replicas.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>remote_sids</td>
<td>Bool</td>
<td>Required. Set this to true to return the searches that the captain is seeing. Will include adhoc searches on remote members.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>artifact_size</td>
<td>Artifact size, in bytes.</td>
</tr>
<tr>
<td>origin_guid</td>
<td>Guid of the origin peer where this artifact was created/search was run.</td>
</tr>
<tr>
<td>peers</td>
<td>Lists information about replicas of this artifact on members of this search head cluster.</td>
</tr>
<tr>
<td>service_after_time</td>
<td>Artifact service/fixup is deferred until after this time.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -k -u admin:pass https://localhost:8189/services/shcluster/captain/artifacts
```

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
 xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustercaptainartifacts</title>
  <id>https://localhost:8089/services/shcluster/captain/artifacts</id>
  <updated>2014-10-15T08:44:41-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/artifacts/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888-888888888888</title>
    <id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413381600_268_88888888-8888-8888-8888-888888888888</id>
    <updated>2014-10-15T08:44:41-07:00</updated>
    <link
```
<entry>
<title>scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</title>
<id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</id>
<updated>2014-10-15T08:44:40-07:00</updated>
<author>
<name>system</name>
</author>
</entry>
<s:dict>
  <s:key name="origin_guid">88888888-8888-8888-8888-888888888888</s:key>
  <s:key name="peers">
    <s:dict>
      <s:key name="directory_path">/home/svasan/splunk/searchhead/var/run/splunk/dispatch/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</s:key>
      <s:key name="status">Complete</s:key>
    </s:dict>
    <s:key name="99999999-9999-9999-9999-999999999999">
      <s:dict>
        <s:key name="directory_path">/home/svasan/splunk/dash/var/run/splunk/dispatch/rsa_scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</s:key>
        <s:key name="status">Complete</s:key>
      </s:dict>
    </s:key>
  </s:dict>
  <s:key name="service_after_time">0</s:key>
</s:dict>
</entry>

<title>scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413387300_288_88888888-8888-8888-8888-888888888888</title>
<id>https://localhost:8089/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413387300_288_88888888-8888-8888-8888-888888888888</id>
<updated>2014-10-15T08:44:41-07:00</updated>
<link href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413387300_288_88888888-8888-8888-8888-888888888888" rel="alternate"/>
<author>
  <name>system</name>
</author>
</link>
</link>
<href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413387300_288_88888888-8888-8888-8888-888888888888" rel="list"/>
<link href="/services/shcluster/captain/artifacts/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413387300_288_88888888-8888-8888-8888-888888888888" rel="remove"/>
</link>
</content type="text/xml">
<s:dict>
  <s:key name="artifact_size">253952</s:key>
  <s:key name="origin_guid">88888888-8888-8888-8888-888888888888</s/key>
  <s:dict name="peers">
    <s:dict>
      <s:key name="directory_path">/home/svasan/splunk/searchhead/var/run/splunk/dispatch/scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</s:key>
      <s:key name="status">Complete</s:key>
    </s:dict>
    <s:dict>
      <s:key name="99999999-9999-9999-9999-999999999999">
        <s:dict>
          <s:key name="directory_path">/home/svasan/splunk/dash/var/run/splunk/dispatch/rsa_scheduler__admin_U0Etbm14__RMD592d31e53ed62579e_at_1413385200_281_88888888-8888-8888-8888-888888888888</s:key>
          <s:key name="status">Complete</s:key>
        </s:dict>
      </s:dict>
    </s:dict>
  </s:dict>
  <s:key name="service_after_time">0</s/key>
</s:dict>
shcluster/captain/artifacts/{name}

https://<host>:<mPort>/services/shcluster/captain/artifacts/{name}

Get artifact information for a specific artifact.

GET

Get artifact information, size, replicas and earliest service time.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>artifact_size</td>
<td>Artifact size, in bytes.</td>
</tr>
<tr>
<td>origin_guid</td>
<td>Guid of the origin peer where this artifact was created.</td>
</tr>
<tr>
<td>peers</td>
<td>Lists information about artifacts on members of this captain.</td>
</tr>
<tr>
<td>service_after_time</td>
<td>Artifact service is deferred until after this time.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass
https://localhost:8089/services/shcluster/captain/artifacts/scheduler__nobody__simplexml__RMD5dc07327042a35a17_at_1469214000_37__11111111-1111-1111-1111-111111111111

XML Response

<title>shclustercaptainartifacts</title>
{id}https://localhost:8089/services/shcluster/captain/artifacts</id>
<updated>2016-07-22T13:39:03-07:00</updated>
<generator build="d6d01722fcee508a9e2f032d36d8d6a445b7d6292" version="20160721"/>
<author>
    <name>Splunk</name>
</author>
<link href="/services/shcluster/captain/artifacts/_new" rel="create"/>
<link href="/services/shcluster/captain/artifacts/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>

317
shcluster/captain/control/default/restart

https://<host>:<mPort>/services/shcluster/captain/control/default/restart

Endpoint to initiate rolling restart of a search head cluster.

POST

Initiates rolling restart of a search head cluster

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>searchable</td>
<td>Boolean</td>
<td>Maintain high search availability during a rolling restart.</td>
</tr>
<tr>
<td>force</td>
<td>Boolean</td>
<td>Override health check failures to continue searchable rolling restart.</td>
</tr>
<tr>
<td>decommission_search_jobs_wait_secs</td>
<td>Integer</td>
<td>Maximum time in secs that searchable rolling restart waits for existing searches to finish. Default: 180 secs.</td>
</tr>
</tbody>
</table>

Returned values

None
Example request and response

XML Request

curl -k -u admin:password  https://localhost:8089/services/shcluster/captain/control/default/restart -d searchable=1 -d force=1 -d decommission_search_jobs_wait_secs=30 -X POST

XML Response

<title>shclustercaptaincontrol</title>

<id>https://10.222.21.58:8089/services/shcluster/captain/control</id>

<updated>2018-03-29T12:08:09-07:00</updated>

<generator build="d75793dbca24" version="7.1.0"/>

<author>
  <name>Splunk</name>
</author>

<link href="/services/shcluster/captain/control/_acl" rel="_acl"/>

<opensearch:totalResults>1</opensearch:totalResults>

<opensearch:itemsPerPage>30</opensearch:itemsPerPage>

<opensearch:startIndex>0</opensearch:startIndex>

<s:messages>
  <s:msg type="INFO">Restart of search head cluster members initiated.</s:msg>
</s:messages>

<entry>
  <title>restart</title>
  <id>https://10.222.21.58:8089/services/shcluster/captain/control/restart</id>
  <updated>1969-12-31T16:00:00-08:00</updated>

  <link href="/services/shcluster/captain/control/restart" rel="alternate"/>

  <author>
    <name>system</name>
  </author>

  <link href="/services/shcluster/captain/control/restart" rel="list"/>
  <link href="/services/shcluster/captain/control/restart" rel="edit"/>

  <content type="text/xml">
    <s:dict>
      <s:dict name="eai:acl">
        <s:dict name="app">
          1
        </s:dict>
        <s:dict name="can_list">
          1
        </s:dict>
        <s:dict name="can_write">
          1
        </s:dict>
        <s:dict name="modifiable">0</s:dict>
        <s:dict name="owner">
          system
        </s:dict>
        <s:dict name="perms">
          <s:dict name="read">
            <s:list>
              admin
              splunk-system-role
            </s:list>
          </s:dict>
          <s:dict name="write">
            <s:list>
              admin
              splunk-system-role
            </s:list>
          </s:dict>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
shcluster/captain/control/control/rotate-splunk-secret

https://<host>:<mPort>/services/shcluster/captain/control/control/rotate-splunk-secret
Rotates the splunk.secret file on all nodes of a search head cluster.

POST
Rotates the splunk.secret file on all nodes of a search head cluster.

Returned values
None

Example request and response

XML Request

curl -k -u admin:changeme
https://localhost:8089/services/shcluster/captain/control/control/rotate-splunk-secret -X POST

XML Response

shcluster/captain/control/control/upgrade-init

https://<host>:<mPort>/services/shcluster/captain/control/control/upgrade-init
Initializes a search head cluster rolling upgrade.

POST
Initializes a search head cluster rolling upgrade.

Returned values

321
Example request and response

XML Request

curl -k -u admin:changeme  https://localhost:8089/services/shcluster/captain/control/control/upgrade-init -X POST

XML Response

<title>shclustercaptaincontrol</title>
<ID>https://10.222.21.58:8089/services/shcluster/captain/control</ID>
<updated>2018-03-29T12:02:54-07:00</updated>
<generator build="d75793dbca24" version="7.1.0"/>

<author>
  <name>Splunk</name>
</author>

<link href="/services/shcluster/captain/control/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>

<s:messages>
  <s:msg type="INFO">Upgrade of search head cluster members initiated.</s:msg>
</s:messages>

<entry>
  <title>upgrade-init</title>
  <ID>https://10.222.21.58:8089/services/shcluster/captain/control/upgrade-init</ID>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/shcluster/captain/control/upgrade-init" rel="alternate"/>
  <author>
    <name>system</name>
  </author>

  <link href="/services/shcluster/captain/control/upgrade-init" rel="list"/>
  <link href="/services/shcluster/captain/control/upgrade-init" rel="edit"/>

  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write"></s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>

322
shcluster/captain/control/control/upgrade-finalize

https://<host>:<mPort>/services/shcluster/captain/control/control/upgrade-finalize
Finishes a search head cluster rolling upgrade.

POST
Finishes a search head cluster rolling upgrade.

Returned values
None

Example request and response

XML Request
curl -k -u admin:changeme
https://localhost:8089/services/shcluster/captain/control/control/upgrade-finalize -X POST

XML Response

<title>shclustercaptaincontrol</title>
<id>https://10.222.21.58:8089/services/shcluster/captain/control/control</id>
<updated>2018-03-29T12:06:47-07:00</updated>
<generator build="d75793dbca24" version="7.1.0"/>
<author>
 <name>Splunk</name>
</author>
<link href="/services/shcluster/captain/control/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages>
<s:msg type="INFO">Upgrade of search head cluster members finalized.</s:msg>
</s:messages>
shcluster/captain/info

https://<host>:<mPort>/services/shcluster/captain/info
Access information about searchhead cluster captain node.

GET

List searchhead cluster captain node details.
### Request parameters

Pagination and filtering parameters can be used with this method.

### Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>elected_captain</td>
<td>Time when the current captain was elected</td>
</tr>
<tr>
<td>id</td>
<td>Id of this SH cluster. This is used as the unique identifier for the Search Head Cluster in bundle replication and acceleration summary management.</td>
</tr>
<tr>
<td>initialized_flag</td>
<td>Indicates if the searchhead cluster is initialized.</td>
</tr>
<tr>
<td>label</td>
<td>The name for the captain. Displayed on the Splunk Web manager page.</td>
</tr>
<tr>
<td>maintenance_mode</td>
<td>Indicates if the cluster is in maintenance mode.</td>
</tr>
<tr>
<td>min_peers_joined_flag</td>
<td>Flag to indicate if more then replication_factor peers have joined the cluster.</td>
</tr>
<tr>
<td>peer_scheme_host_port</td>
<td>URI of the current captain.</td>
</tr>
<tr>
<td>rolling_restart_flag</td>
<td>Indicates whether the captain is restarting the members in a searchhead cluster.</td>
</tr>
<tr>
<td>service_ready_flag</td>
<td>Indicates whether the captain is ready to begin servicing, based on whether it is initialized.</td>
</tr>
<tr>
<td>start_time</td>
<td>Timestamp corresponding to the creation of the captain.</td>
</tr>
</tbody>
</table>

### Example request and response

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/shcluster/captain/info
```

**XML Response**

```xml
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>shclustercaptaininfo</title>
  <id>https://localhost:8089/services/shcluster/captain/info</id>
  <updated>2014-10-15T08:45:25-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>captain</title>
    <id>https://localhost:8089/services/shcluster/captain/info/captain</id>
    <updated>2014-10-15T08:45:25-07:00</updated>
    <link href="/services/shcluster/captain/info/captain" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
  </entry>
</feed>
```
shcluster/captain/jobs

https://<host>:/<mPort>/services/shcluster/captain/jobs
List running and recently finished jobs for all cluster members.

GET
List running and recently finished jobs for this cluster.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
For each job:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATTEMPT_[n]</td>
<td>dispatch_time - The UTC time of dispatch for the job</td>
</tr>
<tr>
<td></td>
<td>errormsg - If the job failed, capturing the reason for failure</td>
</tr>
<tr>
<td></td>
<td>peer - GUID of the member that the job was sent to</td>
</tr>
<tr>
<td></td>
<td>sid - the search id of this attempt</td>
</tr>
<tr>
<td></td>
<td>success - a boolean for success/failure of the job</td>
</tr>
<tr>
<td>job_state</td>
<td>Job State can be SCHEDULED/DISPATCHED/COMPLETED. A SCHEDULED job has been received by the captain from the scheduler to schedule. A DISPATCHED job has started to run on a remote member. A COMPLETED job has finished running on the remote member.</td>
</tr>
<tr>
<td>saved_search</td>
<td>The name of the saved-search from the associated savedsearches.conf file.</td>
</tr>
<tr>
<td>savedsearchtype</td>
<td>The scheduler manages three kinds of scheduled jobs, regular savedsearch for both realtime and historical reports, and tsidx tsidx build searches.</td>
</tr>
<tr>
<td>search_app</td>
<td>The application in which the savedsearch was created.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>search_owner</td>
<td>The owner of the saved search.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/services/shcluster/captain/jobs
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>shclustercaptainjobs</title>
  <id>https://localhost:8089/services/shcluster/captain/jobs</id>
  <updated>2014-10-15T08:47:50-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/jobs/_new" rel="create"/>
  ... opensearch nodes elided ...
  <entry>
    <title>savedsearch_Alert - syslog errors last hour_1087026166</title>
    <id>https://localhost:8089/services/shcluster/captain/jobs/savedsearch_Alert-%20syslog%20errors%20last%20hour_1087026166</id>
    <updated>2014-10-15T08:47:50-07:00</updated>
    <link href="/services/shcluster/captain/jobs/savedsearch_Alert-%20syslog%20errors%20last%20hour_1087026166" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/captain/jobs/savedsearch_Alert-%20syslog%20errors%20last%20hour_1087026166" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="ATTEMPT_1">
          <s:dict>
            <s:key name="dispatch_time">1413363600</s:key>
            <s:key name="errormsg">error response peer=https://wimpy.splunk.com:55560 rc=404 reason='"<xml version="1.0" encoding="UTF-8"/>'
            <s:key name="peer">99999999-9999-9999-9999-999999999999</s:key>
            <s:key name="NO_SID_RECEIVED_YET"/>
            <s:key name="success">0</s:key>
          </s:dict>
        </s:key>
        <s:key name="ATTEMPT_2">
          <s:dict>
            <s:key name="dispatch_time">1413363600</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
<s:dict>
  <s:key name="pe..." name="sid">scheduler__admin_U0Et...a_1413363600_203_88888888-8888-8888-8888-888888888888</s:key>
  <s:key name="success">1</s:key>
</s:dict>

... eai:acl node elided ...
<s:key name="job_state">COMPLETED</s:key>
<s:key name="saved_search">Alert - syslog errors last hour</s:key>
<s:key name="savedsearchtype">savedsearch</s:key>
<s:key name="search_app">SA-nix</s:key>
<s:key name="search_owner">admin</s:key>
</s:dict>
</entry>
<entry>
  <title>savedsearch_Alert - syslog errors last hour_11648853</title>
  <id>https://localhost:8089/services/shcluster/captain/jobs/savedsearch_Alert%20-%20syslog%20errors%20last%20hour_11648853</id>
  <updated>2014-10-15T08:47:50-07:00</updated>
  <link href="/services/shcluster/captain/jobs/savedsearch_Alert%20-%20syslog%20errors%20last%20hour_11648853" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/shcluster/captain/jobs/savedsearch_Alert%20-%20syslog%20errors%20last%20hour_11648853" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="ATTEMPT_1">
        <s:dict>
          <s:key name="errormsg">error response peer=https://wimpy.splunk.com:55560 rc=404 reason='&lt;?xml version="1.0" encoding="UTF-8"?&gt;<response>
            &lt;messages&gt;
              &lt;msg type="ERROR">Application does not exist: SA-nix&lt;/msg&gt;
            &lt;/messages&gt;
          &lt;/response&gt;
          <s:key name="dispatch_time">1413316800</s:key>
          <s:key name="peer">88888888-8888-8888-8888-888888888888</s:key>
          <s:key name="sid">scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413316800_34_88888888-8888-8888-8888-888888888888</s:key>
          <s:key name="success">1</s:key>
        </s:dict>
      </s:key>
      ... eai:acl node elided ...
      <s:key name="job_state">COMPLETED</s:key>
      <s:key name="saved_search">Alert - syslog errors last hour</s:key>
      <s:key name="savedsearchtype">savedsearch</s:key>
    </s:dict>
  </content>
</entry>
<s:dict>
  <s:key name="search_app">SA-nix</s:key>
  <s:key name="search_owner">admin</s:key>
</s:dict>

<entry>
  <title>savedsearch_fired_alerts_1050236433</title>
  <id>https://localhost:8089/services/shcluster/captain/jobs/savedsearch_fired_alerts_1050236433</id>
  <updated>2014-10-15T08:47:50-07:00</updated>
  <link href="/services/shcluster/captain/jobs/savedsearch_fired_alerts_1050236433" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/shcluster/captain/jobs/savedsearch_fired_alerts_1050236433" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="ATTEMPT_1">
        <s:dict>
          <s:key name="dispatch_time">1413308100</s:key>
          <s:key name="errormsg">error response peer=https://wimpy.splunk.com:55560 rc=404 reason='<?xml version="1.0" encoding="UTF-8"?>
<response>
  <messages>
    <msg type="ERROR">Application does not exist: SA-nix</msg>
  </messages>
</response>
'</s:key>
          <s:key name="peer">99999999-9999-9999-9999-999999999999</s:key>
          <s:key name="sid">NO_SID_RECEIVED_YET</s:key>
          <s:key name="success">0</s:key>
        </s:dict>
      </s:key>
      <s:key name="ATTEMPT_2">
        <s:dict>
          <s:key name="dispatch_time">1413308100</s:key>
          <s:key name="peer">88888888-8888-8888-8888-888888888888</s:key>
          <s:key name="sid">scheduler__admin_U0Etbml4__RMD5b9b800e209365567_at_1413308100_2_88888888-8888-8888-8888-888888888888</s:key>
          <s:key name="success">1</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</feed>

shcluster/captain/jobs/{name}

https://<host>:<mPort>/services/shcluster/captain/jobs/{name}
GET

Get running and recently finished jobs for \( \text{name} \) cluster.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| ATTEMPT\_[\(n\)] | dispatch\_time - The UTC time of dispatch for the job  
|                 | errmsg - If the job failed, capturing the reason for failure  
|                 | peer - GUID of the member that the job was sent to  
|                 | sid - the search id of this attempt  
|                 | success - a boolean for success/failure of the job                                                  |
| job\_state      | Job State can be SCHEDULED/DISPATCHED/COMPLETED. A SCHEDULED job has been received by the captain from the scheduler to schedule. A DISPATCHED job has started to run on a remote member. A COMPLETED job has finished running on the remote member. |
| saved\_search   | The name of the saved-search from the associated savedsearches.conf file.                             |
| savedsearchtype | The scheduler manages three kinds of scheduled jobs, regular savedsearch for both realtime and historical, autosummary report acceleration build searches, and tsidx tsidx build searches. |
| search\_app     | The application in which the savedsearch was created.                                                |
| search\_owner   | The owner of the saved search.                                                                          |

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/shcluster/captain/jobs/scheduled
```

**XML Response**

```xml
<title>shclustercaptainjobs</title>
<id>https://localhost:8089/services/shcluster/captain/jobs</id>
<updated>2016-07-22T13:56:18-07:00</updated>
<generator build="d6d01722f00e2f0032d236d85d6a445b7d6292" version="20160721"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/shcluster/captain/jobs/_new" rel="create"/>
<link href="/services/shcluster/captain/jobs/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
    <title>scheduled_sample scheduled search for dashboards (existing job case) timechart_1290934515</title>
    <id>https://localhost:8089/services/shcluster/captain/jobs/scheduled\_sample%20scheduled%20search%20for%20dashboards%20%28existing%20job%20case%29%20timechart_1290934515</id>
    <updated>2016-07-22T13:56:18-07:00</updated>
</entry>
```

330
<link href="/services/shcluster/captain/jobs/scheduled_sample%20scheduled%20search%20for%20dashboards%20%28existing%20job%20case%29%20timechart_1294444515" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/shcluster/captain/jobs/scheduled_sample%20scheduled%20search%20for%20dashboards%20%28existing%20job%20case%29%20timechart_12904444515" rel="list"/>
<link href="/services/shcluster/captain/jobs/scheduled_sample%20scheduled%20search%20for%20dashboards%20%28existing%20job%20case%29%20timechart_12909444515" rel="edit"/>
<content type="text/xml">
<s:dict>
  <s:key name="dispatch_time">1469214120</s:key>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app"></s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">0</s:key>
      <s:key name="owner">system</s:key>
      <s:key name="perms">
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>admin</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:key>
          <s:key name="write">
            <s:list>
              <s:item>admin</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="removable">0</s:key>
      <s:key name="sharing">system</s:key>
    </s:dict>
  </s:key>
  <s:key name="eai:attributes">
    <s:dict>
      <s:key name="optionalFields"></s:dict>
      <s:key name="requiredFields"></s:dict>
      <s:key name="wildcardFields"></s:dict>
    </s:dict>
  </s:key>
  <s:key name="job_state">COMPLETED</s:key>
  <s:key name="peer">11111111-1111-1111-1111-111111111111</s:key>
  <s:key name="peer_scheme_host_port">https://wimpy:13221</s:key>
  <s:key name="peer_servername">home-1</s:key>
  <s:key name="saved_search">sample scheduled search for dashboards (existing job case) timechart</s:key>
  <s:key name="savedsearchtype">scheduled</s:dict>
</s:dict>
shcluster/captain/members

https://<host>:<mPort>/services/shcluster/captain/members

Lists the search head cluster members.

GET

List cluster members.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adhoc_searchhead</td>
<td>Flag to indicate if this member does not run scheduled searches.</td>
</tr>
<tr>
<td>advertise_restart_required</td>
<td>Flag to indicate if this peer advertised that it needed a restart.</td>
</tr>
<tr>
<td>artifact_count</td>
<td>Number of artifacts on this peer</td>
</tr>
<tr>
<td>delayed_artifacts_to_discard</td>
<td>List of artifacts waiting to be deleted from this peer.</td>
</tr>
<tr>
<td>fixup_set</td>
<td>N/A</td>
</tr>
<tr>
<td>host_port_pair</td>
<td>The host and management port advertised by this peer.</td>
</tr>
<tr>
<td>kv_store_host_port</td>
<td>Host and port of the kv store instance of this member.</td>
</tr>
<tr>
<td>label</td>
<td>The name for this member. Displayed on the Splunk Web manager page.</td>
</tr>
<tr>
<td>last_heartbeat</td>
<td>Timestamp for last heartbeat received from the peer</td>
</tr>
<tr>
<td>peer_scheme_host_port</td>
<td>URI of the current captain.</td>
</tr>
<tr>
<td>pending_job_count</td>
<td>Used by the captain to keep track of pending jobs requested by the captain to this member.</td>
</tr>
<tr>
<td>replication_count</td>
<td>Number of replications this peer is part of, as either source or target.</td>
</tr>
<tr>
<td>replication_port</td>
<td>TCP port to listen for replicated data from another cluster member.</td>
</tr>
<tr>
<td>replication_use_ssl</td>
<td>Indicates whether to use SSL when sending replication data.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>site</td>
<td>N/A</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>status</th>
<th>Indicates the status of the member. Possible values are the following.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Up</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
<tr>
<td></td>
<td>• AutomaticDetention</td>
</tr>
<tr>
<td></td>
<td>• ManualDetention-PortsEnabled</td>
</tr>
<tr>
<td></td>
<td>• ManualDetention</td>
</tr>
<tr>
<td></td>
<td>• Restarting</td>
</tr>
<tr>
<td></td>
<td>• ShuttingDown</td>
</tr>
<tr>
<td></td>
<td>• ReassigningPrimaries</td>
</tr>
<tr>
<td></td>
<td>• Decommissioning</td>
</tr>
<tr>
<td></td>
<td>• GracefulShutdown</td>
</tr>
<tr>
<td></td>
<td>• Stopped</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
<tr>
<td></td>
<td>• BatchAdding</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>status_counter</th>
<th>Lists the number of buckets on the peer for each bucket status. Possible values are the following.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete</td>
<td>Complete (warm/cold) bucket</td>
</tr>
<tr>
<td>NonStreamingTarget</td>
<td>Target of replication for already completed (warm/cold) bucket</td>
</tr>
<tr>
<td>PendingTruncate</td>
<td>Bucket pending truncation</td>
</tr>
<tr>
<td>PendingDiscard</td>
<td>Bucket pending discard</td>
</tr>
<tr>
<td>Standalone</td>
<td>Bucket that is not replicated</td>
</tr>
<tr>
<td>StreamingError</td>
<td>Copy of streaming bucket where some error was encountered</td>
</tr>
<tr>
<td>StreamingSource</td>
<td>Streaming hot bucket on source side</td>
</tr>
<tr>
<td>StreamingTarget</td>
<td>Streaming hot bucket copy on target side</td>
</tr>
<tr>
<td>Unset</td>
<td>Uninitialized</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/services/shcluster/captain/members
```

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
<title>shclustercaptainmembers</title>
<id>https://localhost:8089/services/shcluster/captain/members</id>
<updated>2014-10-15T08:49:34-07:00</updated>
<generator build="235980" version="20141014"/>
<author>
  <name>Splunk</name>
</author>
```
88888888-8888-8888-8888-888888888888

99999999-9999-9999-9999-999999999999

99999999-9999-9999-9999-999999999999

99999999-9999-9999-9999-999999999999

ad hoc searchhead
advertise_restart_required
artifact_count
delayed_artifacts_to_discard
host_port_pair
kv_store_host_port
label
last_heartbeat
peer_scheme_host_port
pending_job_count
replication_count
replication_port
replication_use_ssl
site
status
status_counter
shcluster/captain/members/{name}

https://<host>:<mPort>/services/shcluster/captain/members/{name}
Get information about the {name} searchhead cluster member.

GET

Get information about the {name} searchhead cluster member.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adhoc_searchhead</td>
<td>Flag to indicate if this member does not run scheduled searches.</td>
</tr>
<tr>
<td>advertise_restart_required</td>
<td>Flag to indicate if this peer advertised that it needed a restart.</td>
</tr>
<tr>
<td>artifact_count</td>
<td>Number of artifacts on this peer.</td>
</tr>
<tr>
<td>delayed_artifacts_to_discard</td>
<td>List of artifacts waiting to be deleted from this peer.</td>
</tr>
</tbody>
</table>

335
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fixup_set</td>
<td>N/A</td>
</tr>
<tr>
<td>host_port_pair</td>
<td>The host and management port advertised by this peer.</td>
</tr>
<tr>
<td>kv_store_host_port</td>
<td>Host and port of the kv store instance of this member.</td>
</tr>
<tr>
<td>label</td>
<td>The name for this member. Displayed on the Splunk Web manager page.</td>
</tr>
<tr>
<td>last_heartbeat</td>
<td>Timestamp for last heartbeat received from the peer</td>
</tr>
<tr>
<td>peer_scheme_host_port</td>
<td>URI of the current captain.</td>
</tr>
<tr>
<td>pending_job_count</td>
<td>Used by the master to keep track of pending jobs requested by the master to this peer.</td>
</tr>
<tr>
<td>replication_count</td>
<td>Number of replications this peer is part of, as either source or target.</td>
</tr>
<tr>
<td>replication_port</td>
<td>TCP port to listen for replicated data from another cluster member.</td>
</tr>
<tr>
<td>replication_use_ssl</td>
<td>Indicates whether to use SSL when sending replication data.</td>
</tr>
<tr>
<td>site</td>
<td>N/A</td>
</tr>
<tr>
<td>status</td>
<td>Indicates the status of the member.</td>
</tr>
<tr>
<td></td>
<td>Possible values are the following.</td>
</tr>
<tr>
<td></td>
<td>• Up</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
<tr>
<td></td>
<td>• AutomaticDetention</td>
</tr>
<tr>
<td></td>
<td>• ManualDetention-PortsEnabled</td>
</tr>
<tr>
<td></td>
<td>• ManualDetention</td>
</tr>
<tr>
<td></td>
<td>• Restart</td>
</tr>
<tr>
<td></td>
<td>• ShuttingDown</td>
</tr>
<tr>
<td></td>
<td>• ReassigningPrimaries</td>
</tr>
<tr>
<td></td>
<td>• Decommissioning</td>
</tr>
<tr>
<td></td>
<td>• GracefulShutdown</td>
</tr>
<tr>
<td></td>
<td>• Stopped</td>
</tr>
<tr>
<td></td>
<td>• Down</td>
</tr>
<tr>
<td></td>
<td>• BatchAdding</td>
</tr>
<tr>
<td>status_counter</td>
<td>Lists the number of buckets on the peer for each bucket status. Possible values are the following.</td>
</tr>
<tr>
<td></td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td>• Complete (warm/cold) bucket</td>
</tr>
<tr>
<td></td>
<td>NonStreamingTarget</td>
</tr>
<tr>
<td></td>
<td>• Target of replication for already completed (warm/cold) bucket</td>
</tr>
<tr>
<td></td>
<td>PendingTruncate</td>
</tr>
<tr>
<td></td>
<td>• Bucket pending truncation</td>
</tr>
<tr>
<td></td>
<td>PendingDiscard</td>
</tr>
<tr>
<td></td>
<td>• Bucket pending discard</td>
</tr>
<tr>
<td></td>
<td>Standalone</td>
</tr>
<tr>
<td></td>
<td>• Bucket that is not replicated</td>
</tr>
<tr>
<td></td>
<td>StreamingError</td>
</tr>
<tr>
<td></td>
<td>• Copy of streaming bucket where some error was encountered</td>
</tr>
<tr>
<td></td>
<td>StreamingSource</td>
</tr>
<tr>
<td></td>
<td>• Streaming hot bucket on source side</td>
</tr>
<tr>
<td></td>
<td>StreamingTarget</td>
</tr>
<tr>
<td></td>
<td>• Streaming hot bucket copy on target side</td>
</tr>
<tr>
<td></td>
<td>Unset</td>
</tr>
<tr>
<td></td>
<td>• Uninitialized</td>
</tr>
</tbody>
</table>

336
Example request and response

XML Request

curl -k -u admin:pass
https://localhost:8089/services/shcluster/captain/members/33333333-3333-3333-3333-333333333333

XML Response

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>shclustercaptainmembers</title>
  <id>https://wimpy:13221/services/shcluster/captain/members</id>
  <updated>2016-07-22T14:12:50-07:00</updated>
  <generator build="d6d01722fcej508a9e2f032d36d8d6a445b7d6292" version="20160721"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/captain/members/_new" rel="create"/>
  <link href="/services/shcluster/captain/members/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>33333333-3333-3333-3333-333333333333</title>
    <id>https://localhost:8089/services/shcluster/captain/members/33333333-3333-3333-3333-333333333333</id>
    <updated>2016-07-22T14:12:50-07:00</updated>
    <link href="/services/shcluster/captain/members/33333333-3333-3333-3333-333333333333" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
  </entry>
</feed>
<s:item>admin</s:item>
<s:item>splunk-system-role</s:item>
</s:list>
</s:key>
</s:dict>
</s:key>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
<s:key name="eai:attributes">
<s:dict>
<s:key name="optionalFields">
<s:list>
<s:item>advertise_restart_required</s:item>
<s:item>advertise_restart_required_reason</s:item>
<s:item>alert_csv</s:item>
<s:item>alert_csv_epoch</s:item>
<s:item>artifacts_location_csv</s:item>
<s:item>completed_summaries</s:item>
<s:item>last_oaep</s:item>
<s:item>last_osep</s:item>
<s:item>partial_alert_delta</s:item>
<s:item>partial_suppression_delta</s:item>
<s:item>peer_load_stats_gla_15m</s:item>
<s:item>peer_load_stats_gla_1m</s:item>
<s:item>peer_load_stats_gla_5m</s:item>
<s:item>peer_load_stats_max_runtime</s:item>
<s:item>peer_load_stats_num_autosummary</s:item>
<s:item>peer_load_stats_num_historical</s:item>
<s:item>peer_load_stats_num_realtime</s:item>
<s:item>peer_load_stats_num_running</s:item>
<s:item>peer_load_stats_total_runtime</s:item>
<s:item>peer_pid</s:item>
<s:item>scheduler_disabled</s:item>
<s:item>suppression_csv</s:item>
<s:item>suppression_csv_epoch</s:item>
</s:list>
</s:key>
<s:key name="requiredFields">
<s:list>
<s:item>last_artifact_log_entry_processed</s:item>
<s:item>last_si_entry_processed</s:item>
<s:item>mgmt_port</s:item>
<s:item>peer_load_stats</s:item>
<s:item>queue_blocked_count</s:item>
</s:list>
</s:key>
<s:key name="wildcardFields">
</s:list>
</s:dict>
</s:key>
<s:key name="fixup_set">
</s:list>
</s:key>
<s:key name="host_port_pair">wimpy:13223</s:key>
<s:key name="is_captain">0</s:key>
<s:key name="kv_store_host_port">wimpy:18323</s:key>
<s:key name="label">wimpy-3</s:key>
<s:key name="last_heartbeat">1469221966</s:key>
<s:key name="mgmt_uri">https://wimpy:13223</s:key>
shcluster/config

https://<host>:<mPort>/services/shcluster/config
List searchhead cluster node configuration.

GET
List searchhead cluster node configuration.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cxn_timeout</td>
<td>Low-level timeout, in seconds, for establishing connection between searchhead cluster nodes. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this node is disabled.</td>
</tr>
<tr>
<td>heartbeat_period</td>
<td>Only valid for member nodes in a searchhead cluster. The time, in seconds, that a member attempts to send a heartbeat to the captain</td>
</tr>
<tr>
<td>heartbeat_timeout</td>
<td>Only valid for the captain node in a searchhead cluster configuration. The time, in seconds, before a captain considers a member down. Once a member is down, the captain initiates steps to replicate artifacts from the dead member to its live members. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>id</td>
<td>Id of the SH cluster this member is a part of.</td>
</tr>
<tr>
<td>max_peer_rep_load</td>
<td>Maximum number of replications that can be ongoing as a target.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>mode</td>
<td>Valid values: (disabled, member, captain, dynamic_captain) Defaults to disabled. Multiple values are permitted. Sets operational mode for this searchhead cluster node. Only one captain may exist per searchhead cluster.</td>
</tr>
<tr>
<td>percent_peers_to_restart</td>
<td>Percentage of peers to restart at the same time when doing a rolling restart.</td>
</tr>
<tr>
<td>ping_flag</td>
<td>For internal use to facilitate communication between the captain and members.</td>
</tr>
<tr>
<td>quiet_period</td>
<td>The time, in seconds, that a captain waits for members to add themselves to the searchhead cluster.</td>
</tr>
<tr>
<td>rcv_timeout</td>
<td>Low-level timeout, in seconds, for receiving data between searchhead cluster nodes. Defaults to 60 seconds.</td>
</tr>
<tr>
<td>register_replication_address</td>
<td>Valid only for nodes configured as members. The address on which a member is available for accepting replication data. This is useful in the cases where a member host machine has multiple interfaces and only one of them can be reached by another splunkd instance.</td>
</tr>
<tr>
<td>rep_cxn_timeout</td>
<td>Low-level timeout, in seconds, for establishing a connection for replicating data.</td>
</tr>
<tr>
<td>rep_max_rcv_timeout</td>
<td>Maximum cumulative time, in seconds, for receiving acknowledgement data from members. Defaults to 600s.</td>
</tr>
<tr>
<td>rep_max_send_timeout</td>
<td>Maximum time, in seconds, for sending replication slice data between searchhead cluster nodes. Defaults to 600s.</td>
</tr>
<tr>
<td>rep_rcv_timeout</td>
<td>Low-level timeout, in seconds, for receiving data between searchhead cluster nodes.</td>
</tr>
<tr>
<td>rep_send_timeout</td>
<td>Low-level timeout, in seconds, for sending replication data between searchhead cluster nodes. Defaults to 5 seconds.</td>
</tr>
<tr>
<td>replication_factor</td>
<td>Only valid for nodes configured as a captain. Determines how many copies of raw data are created in the searchhead cluster. This could be less than the number of searchhead cluster members. Must be greater than 0 and greater than or equal to the search factor. Defaults to 3.</td>
</tr>
<tr>
<td>replication_port</td>
<td>TCP port to listen for replicated data from another searchhead cluster member.</td>
</tr>
<tr>
<td>replication_use_ssl</td>
<td>Indicates whether to use SSL when sending replication data.</td>
</tr>
<tr>
<td>restart_timeout</td>
<td>Only valid for nodes configured as a captain. The amount of time, in seconds, the captain waits for a member to come back when the member is restarted (to avoid the overhead of trying to fix the artifacts that were on the member). Defaults to 600 seconds.</td>
</tr>
<tr>
<td>secret</td>
<td>Secret shared among the nodes in the searchhead cluster to prevent any arbitrary node from connecting to the searchhead cluster. If a member or searchhead is not configured with the same secret as the captain, it is not able to communicate with the captain.</td>
</tr>
<tr>
<td></td>
<td>Corresponds to pass4SymmKey setting in server.conf.</td>
</tr>
<tr>
<td>send_timeout</td>
<td>Low-level timeout, in seconds, for sending data between searchhead cluster nodes. Defaults to 60 seconds.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8189/services/shcluster/config

XML Response

  <title>shclusterconfig</title>
  <id>https://localhost:8089/services/shcluster/config</id>
  <updated>2014-10-15T08:50:47-07:00</updated>
  <generator build="235980" version="20141014"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/config/_reload" rel="_reload"/>
  ... opensearch nodes elided ... 
  <s:messages/>
  <entry>
    <title>config</title>
    <id>https://localhost:8089/services/shcluster/config/config</id>
    <updated>2014-10-15T08:50:47-07:00</updated>
    <link href="/services/shcluster/config/config" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/config/config/_reload" rel="_reload"/>
    <link href="/services/shcluster/config/config/edit" rel="edit"/>
    <link href="/services/shcluster/config/config/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="cxn_timeout">60</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="heartbeat_period">5</s:key>
        <s:key name="heartbeat_timeout">60</s:key>
        <s:key name="id">BB3116C0-73B9-459A-B473-254A18A69776</s:key>
        <s:key name="max_peer_rep_load">5</s:key>
        <s:key name="mode">dynamic_captain</s:key>
        <s:key name="percent_peers_to_restart">10</s:key>
        <s:key name="ping_flag">1</s:key>
        <s:key name="quiet_period">60</s:key>
        <s:key name="rcv_timeout">60</s:key>
        <s:key name="register_replication_address"></s:key>
        <s:key name="rep_cxn_timeout">60</s:key>
        <s:key name="rep_max_rcv_timeout">600</s:key>
        <s:key name="rep_max_send_timeout">600</s:key>
        <s:key name="rep_rcv_timeout">60</s:key>
        <s:key name="rep_send_timeout">60</s:key>
        <s:key name="replication_factor">2</s:key>
        <s:key name="replication_port">3456</s:key>
        <s:key name="replication_use_ssl">0</s:key>
        <s:key name="restart_timeout">60</s:key>
        <s:key name="secret">********</s:key>
        <s:key name="send_timeout">60</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
Configure search head cluster members.

POST

Configure search head cluster members.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rolling_restart</td>
<td>String</td>
<td>Sets the mode for search head cluster rolling restart. Options include:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• restart: Initiates a rolling restart in classic mode (no guarantee of search continuity).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• searchable: Initiates a rolling restart with minimum search interruption.</td>
</tr>
<tr>
<td>decommission_search_jobs_wait_secs</td>
<td>Integer</td>
<td>Specifies the amount of time, in seconds, that a search head cluster member waits for existing searches to complete before restarting. Default: 180 secs.</td>
</tr>
<tr>
<td>manual_detention</td>
<td></td>
<td>Use one of the following values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• off: Default. Remove the target search head from the detention state.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• on: Put the target search head in manual detention mode.</td>
</tr>
<tr>
<td>target_uri</td>
<td>String</td>
<td>Specifies the target node you want to put in manual detention.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

```bash
curl -k -u admin:changed https://10.140.127.233:8089/services/shcluster/config/config -d rolling_restart=searchable -d decommission_search_jobs_wait secs=120
```

XML Response

http://docs.splunk.com/Documentation/Splunk/7.2.0/RESTREF/RESTcluster

Example request and response for manual detention of a cluster member

XML Request

```bash
```

XML Response

<title>shclusterconfig</title>
&id>https://10.140.127.233:8089/services/shcluster/config</id>
<updated>2018-04-02T16:08:07-07:00</updated>
<generator build="6a9fda63434" version="7.1.0"/>
<author>
   <name>Splunk</name>
</author>
<link href="/services/shcluster/config/_reload" rel="_reload"/>
<link href="/services/shcluster/config/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

shcluster/member/artifacts

https://<host>:<mPort>/services/shcluster/member/artifacts
Manage searchhead cluster member artifact configuration.

GET
List searchhead cluster members artifact configuration.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
For each member:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Indicates the status of this artifact. Possible values are as follows.</td>
</tr>
<tr>
<td></td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td>The copy of this artifact contains the full complement of information.</td>
</tr>
<tr>
<td></td>
<td>StreamingSource</td>
</tr>
<tr>
<td></td>
<td>The copy of this artifact is sending data to member nodes for replication.</td>
</tr>
<tr>
<td></td>
<td>StreamingTarget</td>
</tr>
<tr>
<td></td>
<td>The copy of this artifact is receiving replicated data.</td>
</tr>
<tr>
<td></td>
<td>NonStreamingTarget</td>
</tr>
<tr>
<td></td>
<td>This copy of a warm artifact replication is in progress. Once replication is complete, the status changes to Complete.</td>
</tr>
<tr>
<td></td>
<td>StreamingError</td>
</tr>
<tr>
<td></td>
<td>The copy of this artifact encountered errors while streaming data.</td>
</tr>
<tr>
<td></td>
<td>PendingTruncate</td>
</tr>
</tbody>
</table>
The captain asked the member to truncate this copy of the artifact to a certain size and is waiting for confirmation.

PendingDiscard
The captain asked the member to discard this copy of the artifact and is waiting for confirmation.

Standalone
An artifact in the searchhead cluster that is not replicated.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>Example request and response</td>
<td></td>
</tr>
<tr>
<td>XML Request</td>
<td>curl -k -u admin:pass <a href="https://localhost:8189/services/shcluster/member/artifacts">https://localhost:8189/services/shcluster/member/artifacts</a></td>
</tr>
</tbody>
</table>
<s:key name="status">Complete</s:key></content></s:dict></entry><entry><title>scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_281_88888888-8888-8888-8888-888888888888</title><id>https://localhost:8089/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_281_88888888-8888-8888-8888-888888888888</id><updated>2014-10-15T08:51:46-07:00</updated><link href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413381600_281_88888888-8888-8888-8888-888888888888" rel="alternate"/><s:dict><content type="text/xml">... eai:acl node elided ...
<s:key name="status">Complete</s:key></content></s:dict></entry>
shcluster/member/artifacts/{name}

https://<host>:<mPort>/services/shcluster/member/artifacts/{name}

Get {name} member artifact configuration.

GET

List {name} member artifact information.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Indicates the status of this artifact. Possible values are as follows.</td>
</tr>
<tr>
<td></td>
<td>Complete</td>
</tr>
<tr>
<td></td>
<td>The copy of this artifact contains the full complement of information.</td>
</tr>
<tr>
<td></td>
<td>StreamingSource</td>
</tr>
<tr>
<td></td>
<td>The copy of this artifact is sending data to member nodes for replication.</td>
</tr>
<tr>
<td></td>
<td>StreamingTarget</td>
</tr>
<tr>
<td></td>
<td>The copy of this artifact is receiving replicated data.</td>
</tr>
<tr>
<td></td>
<td>NonStreamingTarget</td>
</tr>
<tr>
<td></td>
<td>This copy of a warm artifact replication is in progress. Once replication is complete, the status changes to Complete.</td>
</tr>
<tr>
<td></td>
<td>StreamingError</td>
</tr>
<tr>
<td></td>
<td>The copy of this artifact encountered errors while streaming data.</td>
</tr>
<tr>
<td></td>
<td>PendingTruncate</td>
</tr>
<tr>
<td></td>
<td>The captain asked the member to truncate this copy of the artifact to a certain size and is waiting for confirmation.</td>
</tr>
<tr>
<td></td>
<td>PendingDiscard</td>
</tr>
<tr>
<td></td>
<td>The captain asked the member to discard this copy of the artifact and is waiting for confirmation.</td>
</tr>
<tr>
<td></td>
<td>Standalone</td>
</tr>
<tr>
<td></td>
<td>An artifact in the searchhead cluster that is not replicated.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -k -u admin:pass
https://localhost:8189/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888

XML Response

<title>shclustermemberartifacts</title>
<id>https://localhost:8089/services/shcluster/member/artifacts</id>
<updated>2014-10-16T23:37:07-07:00</updated>
<generator build="235980" version="20141014"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888</title>
  <id>https://wimpy.splunk.com:55569/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888</id>
  <updated>2014-10-16T23:37:07-07:00</updated>
  <link href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888" rel="list"/>
  <link href="/services/shcluster/member/artifacts/scheduler__admin_U0Etbml4__RMD592d31e53ed62579e_at_1413518400_762_88888888-8888-8888-8888-888888888888" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      ... eai:acl node elided ...
      ... eai:attributes node elided ...
      <s:key name="status">Complete</s:key>
    </s:dict>
  </content>
</entry>
</feed>

shcluster/member/control/control/set_manual_detention

https://<host>:<mPort>//services/shcluster/member/control/control/set_manual_detention

Put the search head cluster member in manual detention mode or take the search head cluster member out of this mode. When a search head cluster member is in manual detention, it does not accept new search jobs, including both scheduled and ad-hoc searches. Existing search jobs run to completion. It also participates in cluster administration operations with the exception of artifact replication.
POST

Adjust search head manual detention mode.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| manual_detention| Use one of the following values. | • off: Default. Remove the search head from the detention state.  
• on: Put the search head in manual detention mode. | Enable or disable manual detention. |

Returned values

None

Example request and response

XML Request

```bash
curl -u admin:password -k  
https://localhost:8089/servicesNS/admin/search/shcluster/member/control/control/set_manual_detention -d  
manual_detention=on
```

XML Response

```xml
<title>shclustermembercontrol</title> 
<id>https://localhost:8089/servicesNS/admin/search/shcluser/member/control</id>  
<updated>2018-03-28T08:04:28-07:00</updated>  
<generator build="5fbc8cfc742f" version="7.2.0"/>  
<author>  
<name>Splunk</name>  
</author>  
<link href="/servicesNS/admin/search/shcluser/member/control/_acl" rel="_acl"/>  
<opensearch:totalResults>0</opensearch:totalResults>  
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>  
<opensearch:startIndex>0</opensearch:startIndex>  
<s:messages/>
```

shcluster/member/consensus

https://<host>:<mPort>/services/shcluser/member/consensus

Get latest cluster configuration from the raft consensus protocol.
GET

Get latest cluster configuration from the raft consensus protocol.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

These values are returned for each member.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration_id</td>
<td>Unique id for this configuration.</td>
</tr>
<tr>
<td>servers_list</td>
<td>Comma-separated list of members that are part of the cluster. Each member is listed as scheme://host:port</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

`curl -k -u admin:pass https://localhost:8189/services/shcluster/member/consensus`

XML Response

  <title>shclustermemberconsensus</title> 
  <id>https://localhost:8089/services/shcluster/member/consensus</id> 
  <updated>2014-10-15T08:52:28-07:00</updated> 
  <generator build="235980" version="20141014"/> 
  <author> 
    <name>Splunk</name> 
  </author> 
  ... opensearch nodes elided ... 
  <s:messages/> 
  <entry> 
    <title>shc_cluster_configuration</title> 
    <id>https://localhost:8089/services/shcluster/member/consensus/shc_cluster_configuration</id> 
    <updated>2014-10-15T08:52:28-07:00</updated> 
    <link href="/services/shcluster/member/consensus/shc_cluster_configuration" rel="alternate"/> 
    <author> 
      <name>system</name> 
    </author> 
    <link href="/services/shcluster/member/consensus/shc_cluster_configuration" rel="list"/> 
    <link href="/services/shcluster/member/consensus/shc_cluster_configuration" rel="edit"/> 
    <content type="text/xml"> 
      <s:dict> 
        <s:key name="configuration_id">4</s:key> 
        ... eai:acl node elided ... 
      </s:dict> 
    </content> 
  </entry> 
</feed>`
shclustermember/info

https://<host>:<mPort>/services/shclustermember/info
Access searchhead cluster member node information.

GET
List member information.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
These values are returned for each member.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active_historical_search_count</td>
<td>Number of currently running historical searches.</td>
</tr>
<tr>
<td>active_realtime_search_count</td>
<td>Number of currently running realtime searches.</td>
</tr>
<tr>
<td>adhoc_searchhead</td>
<td>Flag that indicates if this member can run scheduled searches.</td>
</tr>
<tr>
<td>is_registered</td>
<td>Indicates if this member is registered with the searchhead cluster captain.</td>
</tr>
<tr>
<td>last_heartbeat_attempt</td>
<td>Timestamp for the last attempt to contact the captain.</td>
</tr>
<tr>
<td>maintenance_mode</td>
<td>N/A</td>
</tr>
<tr>
<td>peer_load_stats_gla_15m</td>
<td>Number of scheduled searches run in the last 15 minutes.</td>
</tr>
<tr>
<td>peer_load_stats_gla_1m</td>
<td>Number of scheduled searches run in the last one minute.</td>
</tr>
<tr>
<td>peer_load_stats_gla_5m</td>
<td>Number of scheduled searches run in the last five minutes.</td>
</tr>
<tr>
<td>peer_load_stats_max_runtime</td>
<td>N/A</td>
</tr>
<tr>
<td>peer_load_stats_num_autosummary</td>
<td>N/A</td>
</tr>
<tr>
<td>peer_load_stats_num_historical</td>
<td>N/A</td>
</tr>
<tr>
<td>peer_load_stats_num_realtime</td>
<td>N/A</td>
</tr>
<tr>
<td>peer_load_stats_num_running</td>
<td>N/A</td>
</tr>
<tr>
<td>peer_load_stats_total_runtime</td>
<td>N/A</td>
</tr>
<tr>
<td>restart_state</td>
<td>Indicates whether the member needs to be restarted to enable its searchhead cluster configuration.</td>
</tr>
<tr>
<td>status</td>
<td>Indicates the status of the member. Possible values are as follows.</td>
</tr>
<tr>
<td></td>
<td>• Up</td>
</tr>
<tr>
<td></td>
<td>• Pending</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AutomaticDetention</td>
<td></td>
</tr>
<tr>
<td>ManualDetention</td>
<td></td>
</tr>
<tr>
<td>Restarting</td>
<td></td>
</tr>
<tr>
<td>ShuttingDown</td>
<td></td>
</tr>
<tr>
<td>ReassigningPrimarys</td>
<td></td>
</tr>
<tr>
<td>Decommissioning</td>
<td></td>
</tr>
<tr>
<td>GracefulShutdown</td>
<td></td>
</tr>
<tr>
<td>Down</td>
<td></td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8189/services/shcluster/member/info

**XML Response**

```xml
  <title>shclustermemberinfo</title>
  <id>https://10.222.21.58:8089/services/shcluster/member/info/id</id>
  <updated>2018-03-29T12:05:35-07:00</updated>
  <generator build="d75793dbca24" version="7.1.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/shcluster/member/info/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>member</title>
    <id>https://10.222.21.58:8089/services/shcluster/member/info/member</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/shcluster/member/info/member" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/shcluster/member/info/member" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="active_historical_search_count">0</s:key>
        <s:key name="active_realtime_search_count">0</s:key>
        <s:key name="adhoc_searchhead">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">351</s:key>
                <s:list>
                  <s:integer>351</s:integer>
                </s:list>
              </s:dict>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
shcluster/status

https://<host>:<mPort>/services/shcluster/status
Performs health checks to determine search head cluster health status, prior to a rolling upgrade or rolling restart.

Authentication and Authorization

Requires the admin role or list_search_head_clustering capability.

GET

Get search head cluster health status information.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>

352
### Name | Type | Description
--- | --- | ---
advanced | Boolean | Lists search head cluster status information in a verbose manner.

#### Returned values
These values are returned for each member.

<table>
<thead>
<tr>
<th>Node</th>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Captain</strong></td>
<td>decommission_search_jobs_wait_secs</td>
<td>Integer</td>
<td>Determines the maximum time, in seconds, that a member waits for search jobs to complete before it transitions to the down or GracefulShutdown state.</td>
</tr>
<tr>
<td></td>
<td>dynamic_captain</td>
<td>Boolean</td>
<td>If true (1), then the captain is selected by elections. If false (0), then a static captain (no elections) is assigned.</td>
</tr>
<tr>
<td></td>
<td>elected_captain</td>
<td>String</td>
<td>The time when new captain is elected.</td>
</tr>
<tr>
<td></td>
<td>id</td>
<td>String</td>
<td>Specifies the search head cluster GUID.</td>
</tr>
<tr>
<td></td>
<td>initialized_flag</td>
<td>Boolean</td>
<td>Indicates if the captain is initialized.</td>
</tr>
<tr>
<td></td>
<td>label</td>
<td>String</td>
<td>Specifies the search head cluster label.</td>
</tr>
<tr>
<td></td>
<td>max_failures_to_keep_majority</td>
<td>Boolean</td>
<td>Indicates how many more nodes can be down to keep majority.</td>
</tr>
<tr>
<td></td>
<td>mgmt_uri</td>
<td>String</td>
<td>Specifies the URI and management port for the captain.</td>
</tr>
<tr>
<td></td>
<td>min_peersJoinedFlag</td>
<td>Boolean</td>
<td>min_peersJoinedFlag is true when there are at least as many search head peers as the replicationFactor.</td>
</tr>
<tr>
<td></td>
<td>rollingRestart</td>
<td>String</td>
<td>Shows the restart mode, either restart or searchable.</td>
</tr>
<tr>
<td></td>
<td>rollingRestartFlag</td>
<td>Boolean</td>
<td>rollingRestartFlag is true when a rolling restart is in progress.</td>
</tr>
<tr>
<td></td>
<td>rollingUpgradeFlag</td>
<td>Boolean</td>
<td>rollingUpgradeFlag is true when a rolling upgrade is in progress.</td>
</tr>
<tr>
<td></td>
<td>serviceReadyFlag</td>
<td>Boolean</td>
<td>serviceReadyFlag is true when everything is up and running as expected and &quot;ready to go!&quot;</td>
</tr>
<tr>
<td></td>
<td>stable_captain</td>
<td>Boolean</td>
<td>Indicates stable captain based on heartbeat.</td>
</tr>
<tr>
<td><strong>Member</strong></td>
<td>label</td>
<td>String</td>
<td>Specifies the search head label.</td>
</tr>
<tr>
<td></td>
<td>last_conf_replication</td>
<td>String</td>
<td>Specifies when the member last pulled a set of configurations from the captain.</td>
</tr>
<tr>
<td></td>
<td>manualDetention</td>
<td>Boolean</td>
<td>Indicates if the member is in manual detention.</td>
</tr>
<tr>
<td></td>
<td>mgmt_uri</td>
<td>String</td>
<td>Specifies the URI and management port for the member.</td>
</tr>
<tr>
<td></td>
<td>mgmt_uri_alias</td>
<td>String</td>
<td>Specifies the URI and management port for the member.</td>
</tr>
<tr>
<td></td>
<td>out_of_sync_node</td>
<td>Boolean</td>
<td>out_of_sync_node is true when the member is out of sync.</td>
</tr>
<tr>
<td></td>
<td>preferred_captain</td>
<td>Boolean</td>
<td>Indicates the member’s preference for captaincy.</td>
</tr>
<tr>
<td></td>
<td>restart_required</td>
<td>Boolean</td>
<td>restart_required is true when member requests a restart</td>
</tr>
<tr>
<td></td>
<td>splunk_version</td>
<td>String</td>
<td>Splunk version running on the search head.</td>
</tr>
<tr>
<td></td>
<td>status</td>
<td>String</td>
<td>Indicates the current status of the member.</td>
</tr>
</tbody>
</table>

#### Example request and response
XML Request

curl -k -u admin:changed123 https://localhost:8089/services/shcluster/status?advanced=1?

XML Response

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
<title>shclusterstatus</title>
<id>https://10.222.21.58:8089/services/shcluster/status</id>
<updated>2018-03-29T12:00:50-07:00</updated>
<generator build="d75793dbca24" version="7.1.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/shcluster/status/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<opensearch:messages/>
<entry>
  <title>status</title>
  <id>https://10.222.21.58:8089/services/shcluster/status/status</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/shcluster/status/status" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/shcluster/status/status" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="captain">
        <s:dict>
          <s:key name="dynamic_captain">1</s:key>
          <s:key name="elected_captain">Thu Mar 29 11:58:04 2018</s:key>
          <s:key name="id">93E0DBE8-A435-462F-BF7D-6297C9D9F939</s:key>
          <s:key name="initialized_flag">1</s:key>
          <s:key name="label">ip-10-222-21-58</s:key>
          <s:key name="mgmt_uri">https://10.222.21.58:8089</s:key>
          <s:key name="min_peers_joined_flag">1</s:key>
          <s:key name="rolling_restart_flag">0</s:key>
          <s:key name="service_ready_flag">1</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
Configuration endpoints

Configuration endpoint descriptions

Manage configuration files and settings.

Usage details

*Review ACL information for an endpoint*

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the *REST API User Manual*.

*Authentication and Authorization*

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as *admin*, can access authorization information in Splunk Web. To view the roles assigned to a user, select *Settings > Access controls* and click *Users*. To determine the capabilities assigned to a role, select *Settings > Access controls* and click *Roles*.

*App and user context*

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

*Additional configuration file information*

For details about working with configuration files, see the following topics in the *Admin Manual*.

- About configuration files
- Configuration file precedence

*Splunk Cloud URL for REST API access*

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

*Managed Splunk Cloud deployments*

https://<deployment-name>.splunkcloud.com:8089

*Self-service Splunk Cloud deployments*

To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089
configs/conf-{file}

https://<host>:<mPort>/services/configs/conf-{file}
Access and update a .conf configuration file.

For additional information, see the following resources.

- properties/{file}

GET

List {file} configuration file stanzas.

Namespace determines which instance of the file is retrieved.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys
None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/configs/conf-props

XML Response

```xml
...
<title>conf-props</title>
{id>https://localhost:8089/services/configs/conf-props</id>
<updated>2011-07-08T01:26-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/configs/conf-props/_new" rel="create"/>
<link href="/services/configs/conf-props/_reload" rel="_reload"/>
<!-- opensearch nodes elided for brevity. -->
<s:messages/>
<entry>
  <title>(?i)source::....zip(\d+)?</title>
  <id>https://localhost:8089/servicesNS/nobody/system/configs/conf-props/%28%3Fi%29source%3A%3A....zip%28.%5Cd%2B%29%3F</id>
  <updated>2011-07-08T01:26-07:00</updated>
  <link href="/servicesNS/nobody/system/configs/conf-props/%28%3F%29source%3A%3A....zip%28.%5Cd%2B%29%3F"/>
</entry>
```
POST

Add stanza to {file} configuration file.

Namespace determines which instance of the file is updated.
Authorization
Requires `admin_all_objects` capability.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required. Stanza name in <code>{file}</code> configuration file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&lt;variable&gt; Arbitrary number of key/value pairs.</td>
</tr>
</tbody>
</table>

Response keys
None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/configs/conf-props -d name=myblog

XML Response

```xml
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>conf-props</title>
  <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props</id>
  <updated>2015-07-17T10:50:13+08:00</updated>
  <generator build="ab1a3707c875" version="6.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/configs/conf-props/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/configs/conf-props/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/configs/conf-props/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>myblog</title>
    <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props/myblog</id>
    <updated>2015-07-17T10:50:13+08:00</updated>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog" rel="list"/>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog/_new" rel="create"/>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/configs/conf-props/myblog/_acl" rel="_acl"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="ANNOTATE_PUNCT">1</s:key>
        <s:key name="AUTO_KV_JSON">1</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
configs/conf-{file}/{stanza}

https://<host>:<mPort>/services/configs/conf-{file}/{stanza}

Manage configuration file stanzas.

**DELETE**

Delete `{stanza}` in `{file}` configuration file.

**Request parameters**
None

**Response keys**
None

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/configs/conf-props/myweblogs
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>conf-props</title>
  <id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props</id>
  <updated>2011-07-08T01:01:27-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/configs/conf-props/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/configs/conf-props/_reload" rel="_reload"/>
<!-- opensearch nodes elided for brevity. -->
<s:messages/>
</feed>
```
GET

Get \{stanza\} in \{file\} configuration file.

Request parameters
None

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message
```

XML Response

```
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```

```
<entry>
<title>splunkd_message</title>
<id>https://localhost:8089/servicesNS/nobody/search/configs/conf-eventtypes/splunkd_message</id>
<updated>2014-07-01T13:08:45-07:00</updated>
<author>
  <name>admin</name>
</author>
<content type="text/xml">
  <s:dict>
    <s:key name="CHARSET">UTF-8</s:key>
    <s:key name="description"></s:key>
    <s:key name="disabled">0</s:key>
    <s:key name="eai:acl">362</s:key>
    <s:key name="app">search</s:key>
  </s:dict>
```

362
POST

Update or add property to `{stanza}` in `{file}` configuration file.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>{stanza}</td>
<td>string</td>
<td></td>
</tr>
<tr>
<td>{file}</td>
<td>string</td>
<td></td>
</tr>
</tbody>
</table>

The XML content represents a configuration file property with the following permissions and sharing settings:

- **can_change_perms**: 1
- **can_list**: 1
- **can_share_app**: 1
- **can_share_global**: 1
- **can_share_user**: 1
- **can_write**: 1
- **modifiable**: 1
- **owner**: admin
- **perms**: 
  - **read**: *
  - **write**: admin, power
- **removable**: 1
- **sharing**: global
- **eai:appName**: search
- **eai:attributes**: 
  - **optionalFields**: 
  - **requiredFields**: 
  - **wildcardFields**: `.*`
- **eai:userName**: nobody
- **priority**: 1
- **search**: 
- **tags**: 

363
<table>
<thead>
<tr>
<th><strong>variable</strong></th>
<th>String</th>
<th>Arbitrary number of key/value pairs to update.</th>
</tr>
</thead>
</table>

**Response keys**
None

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/configs/conf-props/myweblogs -d SHOULD_LINEMERGE=true

**XML Response**

```xml
<title>conf-props</title>

/id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props</id>

<updated>2011-07-08T01:26-07:00</updated>

<generator version="102807"/>

<author>

<title>myweblogs</title>

/id>https://localhost:8089/servicesNS/nobody/search/configs/conf-props/myweblogs</id>

<updated>2011-07-08T01:26-07:00</updated>

<author>

<s:messages/>

<entry>

<s:dict>

<s:key name="ANNOTATE_PUNCT">1</s:key>
<s:key name="BREAK_ONLY_BEFORE">1</s:key>
<s:key name="CHARSET">UTF-8</s:key>
<s:key name="DATETIME_CONFIG">/etc/datetime.xml</s:key>
<s:key name="HEADER_MODE"/>2</s:key>
<s:key name="LEARN_SOURCETYPE">1</s:key>
<s:key name="LINE_BREAKER_LOOKBEHIND">100</s:key>
<s:key name="MAX_DAYS_AGO">2000</s:key>
<s:key name="MAX_DAYS_HENCE">2</s:key>
<s:key name="MAX_DIFF_SECS_AGO">3600</s:key>
<s:key name="MAX_DIFF_SECS_HENCE">604800</s:key>
<s:key name="MAX_EVENTS">256</s:key>
<s:key name="MAX_TIMESTAMP_LOOKAHEAD">128</s:key>
<s:key name="MUST_BREAK_AFTER"/>
```
properties

https://<host>:<mPort>/services/properties

Manage .conf configuration files.

GET

List all system and app configuration files.

Request parameters
None

Response keys
None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/properties

XML Response

<author>
POST

Create a configuration file.

Usage details

The namespace specified in the URL determines where the configuration file is created. For example, /services/properties creates the file in the $SPLUNK_BASE/etc/system/local directory and servicesNS/nobody/search creates the file in the $SPLUNK_BASE/etc/apps/search/local directory.

Authentication and Authorization

Requires the admin_all_objects capability.
Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>__conf</td>
<td>String</td>
<td><strong>Required.</strong> Name of the configuration file to create. (Note double underscore prefix.)</td>
</tr>
</tbody>
</table>

Response keys
None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/properties -d __conf=myAppConfigFile

XML Response

No response body.

Returns: **HTTP status = 201 (created)**

properties/{file}

https://<host>:<mPort>/services/properties/{file}
Access stanzas in specified configuration file.

Usage details
The URL namespace determines the scope of visible stanzas. The endpoint returns all stanzas of the specified configuration file, for all configuration files and stanzas visible in the namespace.

GET

List stanzas in {file} configuration file.

Request parameters
None

Response keys
This endpoint returns an `<entry>` for each stanza in addition to `<default>` stanzas.

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/properties/eventtypes

XML Response

<title>eventtypes</title>

<title>default</title>

<title>internal_search_terms</title>

<title>proxylogs</title>

<title>splunkd-access</title>

<title>splunkd-log</title>

<title>splunkd_message</title>

POST

Add stanza to {file} configuration file.
Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>__stanza</td>
<td>String</td>
<td>Required. The key/value pair of the stanza to add. Note double underscore prefix.</td>
</tr>
</tbody>
</table>

Response keys
None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/properties/eventtypes -d __stanza=proxylogs

XML Response
No data returned in body.

Returns: HTTP status 201 (created)

`properties/{file}/{stanza}`

https://<host>:<mPort>/services/properties/{file}/{stanza}

Access and update key/value pair(s) of the specified configuration file and stanza.

GET

List {stanza} key/value pair(s) of {file} configuration file.

Usage details
The URL namespace determines the scope of visible stanzas. This endpoint returns all stanzas of the specified configuration file for all configuration files and stanzas visible in the namespace.

Request parameters
None

Response keys
Each <entry> is a <stanza> key with a <content> value.

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8089/services/properties/props/proxylogs

XML Response

<title>proxylogs</title>
<id>https://localhost:8089/services/properties/props/proxylogs</id>
<updated>2011-07-08T12:08:52-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<entry>
  <title>ANNOTATE_PUNCT</title>
  <id>https://localhost:8089/services/properties/props/proxylogs/ANNOTATE_PUNCT</id>
  <updated>2011-07-08T12:08:52-07:00</updated>
  <link href="/services/properties/props/proxylogs/ANNOTATE_PUNCT" rel="alternate"/>
  <content type="text">True</content>
</entry>
<entry>
  <title>BREAK_ONLY_BEFORE</title>
  <id>https://localhost:8089/services/properties/props/proxylogs/BREAK_ONLY_BEFORE</id>
  <updated>2011-07-08T12:08:52-07:00</updated>
  <link href="/services/properties/props/proxylogs/BREAK_ONLY_BEFORE" rel="alternate"/>
  <content type="text"></content>
</entry>
<entry>
  <title>BREAK_ONLY_BEFORE_DATE</title>
  <id>https://localhost:8089/services/properties/props/proxylogs/BREAK_ONLY_BEFORE_DATE</id>
  <updated>2011-07-08T12:08:52-07:00</updated>
  <link href="/services/properties/props/proxylogs/BREAK_ONLY_BEFORE_DATE" rel="alternate"/>
  <content type="text">True</content>
</entry>
... elided ...
<entry>
  <title>TRANSFORMS</title>
  <id>https://localhost:8089/services/properties/props/proxylogs/TRANSFORMS</id>
  <updated>2011-07-08T12:08:52-07:00</updated>
  <link href="/services/properties/props/proxylogs/TRANSFORMS" rel="alternate"/>
  <content type="text"></content>
</entry>
<entry>
  <title>TRUNCATE</title>
  <id>https://localhost:8089/services/properties/props/proxylogs/TRUNCATE</id>
  <updated>2011-07-08T12:08:52-07:00</updated>
  <link href="/services/properties/props/proxylogs/TRUNCATE" rel="alternate"/>
  <content type="text">10000</content>
</entry>
<entry>
  <title>maxDist</title>
  <id>https://localhost:8089/services/properties/props/proxylogs/maxDist</id>
  <updated>2011-07-08T12:08:52-07:00</updated>
  <link href="/services/properties/props/proxylogs/maxDist" rel="alternate"/>
  <content type="text">370</content>
</entry>
POST

Add or update one or more key/value pair(s) in `{stanza}` of `{file}` configuration file.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;variable&gt;</code></td>
<td>String</td>
<td>Required. One or more key/value pair(s).</td>
</tr>
</tbody>
</table>

Response keys

A response `<message>` indicates update success or failure.

Example request and response

XML Request

```xml
curl -k -u admin:pass https://localhost:8089/services/properties/props/proxylogs -d NO_BINARY_CHECK=true -d CHARSET=UTF-8
```

XML Response

```xml
<response>
  <messages>
    <msg type="INFO">Successfully modified 2 key(s)</msg>
  </messages>
</response>
```

`properties/{file}/{stanza}/{key}`

https://<host>:<mPort>/services/properties/{file}/{stanza}/{key}

Access and update values for the specified configuration file, stanza, and key.

GET

Get a plaintext `{key}` value for a configuration file stanza and key.

Request parameters

None

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>

371
Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/properties/props/proxylogs/SHOULD_LINEMERGE
```

XML Response

```
True
```

POST

Update a plaintext `{key}` value for a configuration file stanza and key.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;variable&gt;</code></td>
<td>String</td>
<td>Required. Plaintext value.</td>
</tr>
</tbody>
</table>

Response keys

Message indicates update success or failure.

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/properties/props/proxylogs/SHOULD_LINEMERGE -d value=false
```

XML Response

```
<response>
  <messages>
    <msg type="INFO">Successfully modified 1 key(s)</msg>
  </messages>
</response>
```

372
Deployment endpoints

Deployment endpoint descriptions

Manage deployment servers and clients.

A deployment server configures a deployment client. Deployment clients and servers can reside on separate, distributed, Splunk instances or can reside on the same instance.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select Settings > Access controls and click Users. To determine the capabilities assigned to a role, select Settings > Access controls and click Roles.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

Managed Splunk Cloud deployments

https://<deployment-name>.splunkcloud.com:8089

Self-service Splunk Cloud deployments

To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the the Splunk REST API Tutorials for more information.
**deployment/client**

https://<host>:<mPort>/services/deployment/client

List deployment client configuration and status.

**GET**

Get deployment client list with enabled status, server class, and host and port number of each.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

For each deployment client, the following values are returned.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Disabled status: 0 = Enabled 1 = Disabled</td>
</tr>
<tr>
<td>serverClasses</td>
<td>List of member server classes for app download authorization.</td>
</tr>
<tr>
<td>targetUri</td>
<td>Host and port number (&lt;host&gt;:&lt;port&gt;).</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/deployment/client
```

**XML Response**

```xml
...
<title>deploymentclient</title>
$id HTTPS://localhost:8089/services/deployment/client$id
<updated>2011-07-11T00:35:37-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <id>https://localhost:8089/services/deployment/client/deployment-client$id>
  <updated>2011-07-11T00:35:37-07:00</updated>
  <link href="/services/deployment/client/deployment-client" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  ... more entries ...
</entry>
...
deployment/client/config

https://<host>:<mPort>/services/deployment/client/config

Get deployment client configuration and status.

GET

Get deployment client enabled status, server class for app distribution, and host and port number.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Disabled status: 0 = Enabled 1 = Disabled</td>
</tr>
<tr>
<td>serverClasses</td>
<td>List of member server classes for app download authorization.</td>
</tr>
<tr>
<td>targetUri</td>
<td>Host and port number (host:port).</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8089/services/deployment/client/config

XML Response

<title>deployment/client</title>
/id>https://localhost:8089/services/deployment/client</id>
/updated>2013-07-31T20:49:58-07:00</updated>
<generator build="172889" version="6.0"/>
<author>

</author>
<link href="/services/deployment/client/listIsDisabled" rel="listIsDisabled"/>
... opensearch nodes elided ...
<s:messages/>

<entry>
<title>config</title>
/id>https://localhost:8089/services/deployment/client/config</id>
/updated>2013-07-31T20:49:58-07:00</updated>
<link href="/services/deployment/client/config" rel="alternate"/>
<author>

</author>
<link href="/services/deployment/client/config" rel="list"/>
<link href="/services/deployment/client/config" rel="edit"/>
<link href="/services/deployment/client/config/reload" rel="reload"/>

<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict>
<s:dict> deployment/client/config/listIsDisabled

https://<host>:<mPort>/services/deployment/client/config/listIsDisabled

Get deployment client status.

GET

Get deployment client disabled status.
Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Disabled status: 0 = Enabled 1 = Disabled</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/deployment/client/config/listIsDisabled

XML Response

...<title>deploymentclient</title>
<id>https://localhost:8089/services/deployment/client/id</id>
<updated>2013-08-04T18:49:25-07:00</updated>
<generator build="172889" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/client/listIsDisabled" rel="listIsDisabled"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>default</title>
  <id>https://localhost:8089/services/deployment/client/default/id</id>
  <updated>2013-08-04T18:49:25-07:00</updated>
  <link href="/services/deployment/client/default" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/deployment/client/default" rel="list"/>
  <link href="/services/deployment/client/default" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:dict>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
      </s:dict>
    </s:dict>
  </content>
</entry>
deployment/client/config/reload

Access information on reloading the named client.

POST

Access client reload information.

Request parameters
No parameters for this request.

Returned values

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>Endpoint returned successfully.</td>
</tr>
<tr>
<td>400</td>
<td>Request error. See response body for details.</td>
</tr>
<tr>
<td>401</td>
<td>Authentication failure: must pass valid credentials with request.</td>
</tr>
<tr>
<td>403</td>
<td>Insufficient permissions to access resource.</td>
</tr>
<tr>
<td>404</td>
<td>Specified resource does not exist.</td>
</tr>
<tr>
<td>409</td>
<td>Request error: this operation is invalid for this item. See response body for details.</td>
</tr>
<tr>
<td>500</td>
<td>Internal server error. See response body for details.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass -X POST https://localhost:8089/services/deployment/client/config/reload

XML Response

...
deployment/client/{name}/reload

```
https://<host>:<mPort>/services/deployment/client/{name}/reload
```

Restart and reload the `{name}` deployment client.

**POST**

Restart and reload `{name}` deployment client.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>disabled</strong></td>
<td>Disabled status: 0 = Enabled 1 = Disabled</td>
</tr>
<tr>
<td><strong>serverClasses</strong></td>
<td>List of member server classes for app download authorization.</td>
</tr>
<tr>
<td><strong>targetUri</strong></td>
<td>Host and port number (&lt;host&gt;:&lt;port&gt;).</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/services/deployment/client/deployment-client/reload
```

**XML Response**

379
deployment/server/applications

https://<host>:<mPort>/services/deployment/server/applications
List distributed apps.

GET
List distributed apps, including distributed state information.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clientId</td>
<td>String</td>
<td></td>
<td>Select apps that match clientId.</td>
</tr>
<tr>
<td>hasDeploymentError</td>
<td>Boolean</td>
<td></td>
<td>Select apps according to deployment fault status: 0 = Do not include apps with a deployment fault indication.</td>
</tr>
</tbody>
</table>
Include apps with a deployment fault indication.

Pagination and filtering parameters can be used with this method.

Returned values
The response includes these values for each app listed.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Disk location of the archived version of the app.</td>
</tr>
<tr>
<td>clientId</td>
<td>Deployment client ID associated with the app, an MD5 hash value of serialized (catenated) client attributes.</td>
</tr>
<tr>
<td>hasDeploymentError</td>
<td>Indicates deployment fault status on at least one deployment client: 0 = Do not include apps with a deployment fault indication. 1 = Include apps with a deployment fault indication.</td>
</tr>
<tr>
<td>loadtime</td>
<td>Last deployment server app loaded or reloaded date and time. An application not mapped to serverclasses is not loaded so loadtime is 0.</td>
</tr>
<tr>
<td>restartSplunkWeb</td>
<td>Restart Splunk Web indication: 0 = Do not restart Splunk Web. 1 = Restart Splunk Web.</td>
</tr>
<tr>
<td>restartSplunkd</td>
<td>Restart splunkd indication: 0 = Do not restart splunkd. 1 = Restart splunkd.</td>
</tr>
<tr>
<td>serverclasses</td>
<td>List of server classes associated with the application.</td>
</tr>
<tr>
<td>size</td>
<td>Size on disk of the compressed app (bundle), in bytes.</td>
</tr>
<tr>
<td>stateOnClient</td>
<td>App enablement status: 0 = Not enabled. 1 = Enabled.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/deployment/server/applications

XML Response

...<title>applications</title>
<id>https://localhost:8089/services/deployment/server/applications</id>
<updated>2013-08-01T09:35:22-07:00</updated>
<generator build="172889" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/server/applications/_new" rel="create"/>
... opensearch nodes elided ...
<s:messages/>

381
Get or update distribution information for `{name}` app.
GET

Get (name) app distribution information.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Disk location of archived version of the app.</td>
</tr>
<tr>
<td>clientId</td>
<td>Deployment client ID associated with the app, an MD5 hash value of serialized (catenated) client attributes.</td>
</tr>
</tbody>
</table>
| hasDeploymentError | Indicates deployment fault status on at least one deployment client:  
|               | 0 = Do not include apps with a deployment fault indication.  
|               | 1 = Include apps with a deployment fault indication.                  |
| loadtime    | Last deployment server app loaded or reloaded date and time. An application not mapped to serverclasses is not loaded so loadtime is 0. |
| restartSplunkWeb | Restart Splunk Web indication:  
|               | 0 = Do not restart Splunk Web.  
|               | 1 = Restart Splunk Web.                                                   |
| restartSplunkd | Restart splunkd indication:  
|               | 0 = Do not restart splunkd.  
|               | 1 = Restart splunkd.                                                     |
| serverclasses | List of server classes associated with the application.                |
| size        | Size on disk of the compressed app (bundle), in bytes.                   |
| stateOnClient | App enablement status:  
|               | 0 = Not enabled.  
|               | 1 = Enabled.                                                            |

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/deployment/server/applications/wma-app1

XML Response

...
POST

Update \{name\} app distribution information.

Usage details
When continueMatching is true, matching is in the order in which server classes are defined.

The whitelist setting indicates a filtering strategy that includes a subset.

- Items are not considered to match the server class by default.
- Items that match any whitelist entry, and do not match any blacklist entry, are considered to match the server class.
- Items that match any blacklist entry are not considered to match the server class, regardless of whitelist.

The blacklist setting indicates a filtering strategy that excludes a subset.

- Items are considered to match the server class by default.
- Items that match any blacklist entry, and do not match any whitelist entry, are considered to not match the server class.
- Items that match any whitelist entry are considered to match the server class.

That is,
**whitelist**: default no-match -> whitelists enable -> blacklists disable

**blacklist**: default match -> blacklists disable -> whitelists enable

If you specify whitelist at the global level, and then specify blacklist for an individual server class, the setting becomes blacklist for that server class, and you have to provide another filter in that server class definition to replace the one you overrode.

### Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blacklist.*</td>
<td>String</td>
<td></td>
<td>List of hosts to exclude when mapping application to a server class. For each blacklist, replace the wildcard (*) with an ordinal number to specify additional blacklists. Filter ordinals must start at 0 and be consecutive.</td>
</tr>
<tr>
<td>continueMatching</td>
<td>Boolean</td>
<td></td>
<td>Configuration layering indication, across classes and server-specific settings: true = [Default] Configuration lookups continue matching server classes after the first match. false = Use the first match, only.</td>
</tr>
<tr>
<td>deinstall</td>
<td>Boolean</td>
<td></td>
<td>Remove mapping indication: true = Remove mapping of {name} from all server classes and delete it from client target repositories. false = Do not remove mapping of {name}.</td>
</tr>
<tr>
<td>filterType</td>
<td>Enum</td>
<td></td>
<td>Filter execution order: whitelist = Whitelist filters are applied before blacklist filters. blacklist = Blacklist filters are applied before whitelist filters.</td>
</tr>
<tr>
<td>machineTypesFilter</td>
<td>String</td>
<td></td>
<td>Comma-separated list of filters to be used in Boolean and logic with whitelist and blacklist filters. Only clients that match the white/blacklist filters AND that match this machineTypesFilter are included. Thus the match is an intersection of the matches for the white/blacklist and the matches for MachineTypesFilter. The patterns are PCRE regular expressions, with the following aids for easier entry: • You can specify '.' to mean '.' • You can specify '<em>' to mean '.</em>' • Matches are always case-insensitive; you do not need to specify the '(?i)' prefix.</td>
</tr>
<tr>
<td>repositoryLocation</td>
<td>String</td>
<td></td>
<td>The location on the deployment server to store the content that is to be deployed for this server class. For example: $SPLUNK_HOME/etc/deployment-apps</td>
</tr>
<tr>
<td>restartSplunkWeb</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to restart SplunkWeb on the client when a member app or a directly configured app is updated. Defaults to false</td>
</tr>
<tr>
<td>restartSplunkd</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to restart splunkd on the client when a member app or a directly configured app is updated.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>serverclass</td>
<td>String</td>
<td>Defaults to false</td>
<td>The name of the server class to which the application is mapped. Do not specify this parameter if <code>deinstall</code> is true.</td>
</tr>
<tr>
<td>stateOnClient</td>
<td>Enum</td>
<td>Valid values are (enabled</td>
<td>disabled</td>
</tr>
<tr>
<td>targetRepositoryLocation</td>
<td>String</td>
<td>The location on the deployment client to install the apps defined for this Deployment Server. If unset, or set to empty, the repositoryLocation path is used. That is, defaults to: <code>$SPLUNK_HOME/etc/apps</code> (the live configuration directory for a Splunk deployment) Useful only with complex (for example, tiered) deployment strategies.</td>
<td></td>
</tr>
<tr>
<td>tmpFolder</td>
<td>String</td>
<td>Working folder used by deployment server. Defaults to <code>$SPLUNK_HOME/var/run/tmp</code></td>
<td></td>
</tr>
<tr>
<td>unmapped</td>
<td>Boolean</td>
<td>Indicates whether to remove the mapping of the application to the specified server class.</td>
<td></td>
</tr>
<tr>
<td>whitelist.*</td>
<td>String</td>
<td>List of hosts to accept for this server class. For each whitelist, replace * with an ordinal number to specify additional whitelists. Filter ordinals must start at 0 and be consecutive.</td>
<td></td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive</td>
<td>Specifies the location of the compressed version (<code>bundle</code>) of the app.</td>
</tr>
<tr>
<td>blacklist.*</td>
<td>Regular expressions used to exclude, when mapping this application to a client. If a client matches any of the blacklist regular expressions, it does not receive the application. The * is replaced by an integral ordinal number.</td>
</tr>
<tr>
<td>continueMatching</td>
<td>If true, configuration lookups continue matching server classes, beyond the first match. If false, only the first match is used.</td>
</tr>
<tr>
<td>filterType</td>
<td>blacklist) Determines the order of execution of filters. If filterType is whitelist, all whitelist filters are applied first, followed by blacklist filters. If filterType is blacklist, all blacklist filters are applied first, followed by whitelist filters. See description for the filterType POST parameter for more information.</td>
</tr>
</tbody>
</table>
### Name and Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>loadtime</td>
<td>Specifies the date and time the application was last loaded (or reloaded) by the deployment server. An application not mapped to any serverclasses does not get loaded, thus its loadtime attribute is 0; in epoch terms, which is 01 Jan 1970 at midnight GMT.</td>
</tr>
<tr>
<td>machineTypesFilter</td>
<td>List of filters to be used in Boolean and logic with whitelist and blacklist filters.</td>
</tr>
<tr>
<td>repositoryLocation</td>
<td>The location on the deployment server to store the content that is to be deployed for this server class.</td>
</tr>
<tr>
<td>restartSplunkWeb</td>
<td>Indicates whether to restart Splunk Web.</td>
</tr>
<tr>
<td>restartSplunkd</td>
<td>Indicates whether to restart splunkd.</td>
</tr>
<tr>
<td>serverclass</td>
<td>The name of the server class to which the application is mapped.</td>
</tr>
<tr>
<td>serverclasses</td>
<td>List of server classes associated with the application.</td>
</tr>
<tr>
<td>size</td>
<td>Indicates in bytes the size on disk of the compressed version (bundle) of the application.</td>
</tr>
<tr>
<td>stateOnClient</td>
<td>Specifies whether the deployment client is enabled or disabled.</td>
</tr>
<tr>
<td>targetRepositoryLocation</td>
<td>The location on the deployment client to install the apps defined for this Deployment Server. If unset, or set to empty, the repositoryLocation path is used.</td>
</tr>
<tr>
<td>tmpFolder</td>
<td>Working folder used by deployment server.</td>
</tr>
<tr>
<td>whitelist.*</td>
<td>Regular expressions used to accept, when mapping this application to a client. The * is replaced by an integral ordinal number.</td>
</tr>
</tbody>
</table>

### Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/deployment/server/applications/wma-app3 -d serverclass=sc_apps_wma

**XML Response**

```xml
...<id>https://localhost:8089/services/deployment/server/applications</id>
<updated>2013-08-10T12:50:59-07:00</updated>
<generator build="176231" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/server/applications/_new" rel="create"/>...
<s:messages/>
<entry>
  <title>wma-app3</title>
```

387
deployment/server/clients

https://<host>:<mPort>/services/deployment/server/clients

Provides access to information about clients to a deployment server.

GET

Access information about clients to a deployment server.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action</td>
<td>String</td>
<td></td>
<td>Use one of the following values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• phonehome: deployment client is verifying app status (typical state)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• unknown: app state on deployment client restart</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• download: deployment client is downloading the app or app update</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• install: deployment client is installing or updating the app</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• uninstall: app removed from deployment server, marked for uninstall on the deployment client</td>
</tr>
</tbody>
</table>

The GET response includes all clients with an app that has the specified action.
| Name                  | Type      | Default | Description                                                                 
|-----------------------|-----------|---------|-----------------------------------------------------------------------------
| application           | String    |         | Lists clients to the deployment server that have attempted to download the named application. |
| hasDeploymentError    | Boolean   | False   | Indicates whether to list only clients that have a deployment error.          |
| maxPhonehome_latency_to_avgInterval_ratio | Number |         | List clients to the deployment server when the ratio of the phone home latency to the average phone home interval is less than the value supplied to this parameter. |
| minLatestPhonehomeTime| Number    |         | Lists clients for which there is a phone home message at the specified time or later, in epoch seconds. That is, list the client for the following condition: client latency > (now - minLatestPhonehomeTime) |
| minPhonehome_latency_to_avgInterval_ratio | Number |         | List clients to the deployment server when the ratio of the phone home latency to the average phone home interval is greater than the value supplied with this parameter. |
| serverclasses         | String    |         | Comma-separated list of serverclasses. List clients that are configured to receive an application to a listed serverclass. The match is a logical OR of, for each Si, include C if C is sent an app A that maps to Si in serverclass.conf, if such an app existed. The "would have" is per blacklist.n or whitelist.n/machineTypesFilter in serverclass.conf |

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applications</td>
<td>List of applications deployed to the deployment client.</td>
</tr>
<tr>
<td>averagePhoneHomeInterval</td>
<td>The average phone home interval, in seconds.</td>
</tr>
<tr>
<td>build</td>
<td>The build number for the Splunk instance on the deployment client.</td>
</tr>
<tr>
<td>dns</td>
<td>The DNS lookup name of the deployment client server.</td>
</tr>
<tr>
<td>guid</td>
<td>Identifier for the deployment server client.</td>
</tr>
<tr>
<td>hasDeploymentError</td>
<td>Specifies whether to check for clients with a deployment error.</td>
</tr>
<tr>
<td>hostname</td>
<td>The host name of the deployment client server.</td>
</tr>
<tr>
<td>id</td>
<td>ID for the client based on client name and IP address.</td>
</tr>
<tr>
<td>ip</td>
<td>The IP address of the client to the deployment server.</td>
</tr>
<tr>
<td>lastPhonehomeTime</td>
<td>The last time the deployment client phones home to the deployment server, in epoch time.</td>
</tr>
<tr>
<td>mgmt</td>
<td>The managament port for the deployment client.</td>
</tr>
<tr>
<td>minLatestPhonehomeTime</td>
<td>Specifies in epoch seconds the minimum latency for a client to contact the deployment server.</td>
</tr>
</tbody>
</table>
### Example request and response

#### XML Request

```bash
curl -k -u admin:pass https://localhost:8089/services/deployment/server/clients
```

#### XML Response

```xml
<entry>
<title>dc95537d0e8fdadc44d00c50fc431e25</title>
<id>https://localhost:8089/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25</id>
<updated>2013-08-01T09:41:42-07:00</updated>
<author>
  <name>system</name>
</author>
<link href="/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25" rel="alternate"/>
<link href="/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25" rel="list"/>
<link href="/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25" rel="remove"/>
<content type="text/xml">
  
  <s:dict>
    <s:key name="applications">
      <s:dict>
        <s:key name="wma-app-test2">
          <s:dict>
            <s:key name="action">Install</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:dict>
  </s:dict>
  
  <s:dict>
    <s:key name="archive"/>
    <s:dict>
      <s:key name="wma-app-test2">
        <s:dict>
          <s:key name="action">Install</s:key>
        </s:dict>
      </s:dict>
    </s:dict>
  </s:dict>

  <s:key name="archive"/>
  <s:dict>
    <s:dict>
      <s:key name="wma-app-test2">
        <s:dict>
          <s:key name="action">Install</s:key>
        </s:dict>
      </s:dict>
    </s:dict>
  </s:dict>
```

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minPhonehome_latency_to_avgInterval_ratio</td>
<td>The minimum value specified for the ratio of the phone home latency to the average phone home interval.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the deployment client server.</td>
</tr>
<tr>
<td>serverclasses</td>
<td>List of server classes for the deployment client.</td>
</tr>
<tr>
<td>utname</td>
<td>Machine type for the deployment server client.</td>
</tr>
</tbody>
</table>
**deployment/server/clients/countClients_by_machineType**

https://<host>:<mPort>/services/deployment/server/clients/countClients_by_machineType

Access information about deployment clients to this server according to the machine type of the client.

**GET**

List the count of deployment clients for this server by machine type.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counts</td>
<td>The list of machine types for this deployment client, showing the count of each machine type.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/deployment/server/clients/countClients_by_machineType

**XML Response**

```xml
<title>serverclients</title>
<id>https://localhost:8089/services/deployment/server/clients</id>
<updated>2013-07-30T15:07:38-07:00</updated>
<generator build="172889" version="6.0"/>
<author>
```
**deployment/server/clients/countRecentDownloads**

https://<host>:<mPort>/services/deployment/server/clients/countRecentDownloads

Access the count of the number of downloads from this client to the deployment server during the last specified time period.

**GET**

Return the count of the number of downloads from this client to the deployment server during the last specified time period.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
<td>String</td>
<td></td>
<td>Count the number of downloads for clients that have attempted to download the named application.</td>
</tr>
<tr>
<td>hasDeploymentError</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to count downloads for clients that have a deployment error.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>maxAgeSecs</td>
<td>Number</td>
<td></td>
<td>Age of the downloads to count, in seconds.</td>
</tr>
<tr>
<td>maxPhonehome_latency_to_avgInterval_ratio</td>
<td>Number</td>
<td></td>
<td>List the count of recent download by this client to the deployment server when the ratio of the phone home latency to the average phone home interval is less than the value supplied to this parameter.</td>
</tr>
<tr>
<td>minLatestPhonehomeTime</td>
<td>Number</td>
<td></td>
<td>Specifies in epoch seconds the minimum latency for a client to contact the deployment server. This endpoint lists the number of downloads for clients to the deployment server with a latency equal to or greater than specified by this parameter.</td>
</tr>
<tr>
<td>minPhonehome_latency_to_avgInterval_ratio</td>
<td>Number</td>
<td></td>
<td>List the number of recent downloads by clients to the deployment server when the ratio of the phone home latency to the average phone home interval is greater than the value supplied with this parameter.</td>
</tr>
<tr>
<td>serverclasses</td>
<td>String</td>
<td></td>
<td>Comma-separated list of server classes. Lists the number of recent downloads by clients to the deployment server that are configured to send an application to a listed serverclass.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>The number of recent downloads.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass -d maxAgeSecs=1 -G https://localhost:8089/services/deployment/server/clients/countRecentDownloads

**XML Response**

```xml
...<title>serverclients</title>
<id>https://localhost:8089/services/deployment/server/clients</id>
<updated>2013-07-30T20:00:43-07:00</updated>
<generator build="172889" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/server/clients/countClients_by_machineType" rel="countClients_by_machineType"/>
<link href="/services/deployment/server/clients/countRecentDownloads" rel="countRecentDownloads"/>
<link href="/services/deployment/server/clients/getMatchingAppsForClient_dryRun" rel="getMatchingAppsForClient_dryRun"/>
<link href="/services/deployment/server/clients/preview" rel="preview"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>default</title>
  <id>https://localhost:8089/services/deployment/server/clients/default</id>
  <updated>2013-07-30T20:00:43-07:00</updated>
</entry>
```
deployment/server/clients/{name}

https://{host}:{mPort}/services/deployment/server/clients/{name}

Get client information or remove a client.

DELETE

Remove the specified client from the deployment server registry. The next time the client "phones home" the record is re-created.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/services/deployment/server/clients/1d3de43af2aae61139c367044127f44a
```

XML Response

```
...
<title>serverclients</title>
{id>https://qa-sv-rh61x64-7:8103/services/deployment/server/clients</id>
<updated>2013-10-21T16:03:49-07:00</updated>
<generator build="182785" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
```
GET

Lists information about the named client to the deployment server.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
<td>String</td>
<td></td>
<td>Lists information about this client with respect to the named application.</td>
</tr>
<tr>
<td>hasDeploymentError</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to list this client if it has a deployment error.</td>
</tr>
<tr>
<td>maxPhonehome_latency_to_avgInterval_ratio</td>
<td>Number</td>
<td></td>
<td>List clients to the deployment server when the ratio of the phone home latency to the average phone home interval is less than the value supplied to this parameter.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>minLatestPhonehomeTime</td>
<td>Number</td>
<td></td>
<td>Specifies in epoch seconds the minimum latency for a client to contact the deployment server. This endpoint lists information about the named client if it has a latency equal to or greater than specified by this parameter.</td>
</tr>
<tr>
<td>minPhonehome_latency_to_avgInterval_ratio</td>
<td>Number</td>
<td></td>
<td>List information about the named client to the deployment server when the ratio of the phone home latency to the average phone home interval is greater than the value supplied with this parameter.</td>
</tr>
<tr>
<td>serverclasses</td>
<td>String</td>
<td></td>
<td>Comma-separated list of serverclasses. Lists information about this client if it is configured to send an application to a listed serverclass.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application</td>
<td>The name of the application specified to filter the results of this call.</td>
</tr>
<tr>
<td>applications</td>
<td>List of applications deployed to the deployment client.</td>
</tr>
<tr>
<td>averagePhoneHomeInterval</td>
<td>The average phone home interval, in seconds.</td>
</tr>
<tr>
<td>build</td>
<td>The build number for the Splunk instance on the deployment client.</td>
</tr>
<tr>
<td>dns</td>
<td>The DNS lookup name of the deployment client server.</td>
</tr>
<tr>
<td>guid</td>
<td>Identifier for the deployment server client.</td>
</tr>
<tr>
<td>hasDeploymentError</td>
<td>Specifies whether to check for clients with a deployment error.</td>
</tr>
<tr>
<td>hostname</td>
<td>The host name of the deployment client server.</td>
</tr>
<tr>
<td>id</td>
<td>ID for the client based on client name and IP address.</td>
</tr>
<tr>
<td>ip</td>
<td>The IP address of the client to the deployment server.</td>
</tr>
<tr>
<td>lastPhoneHomeTime</td>
<td>The last time the deployment client phones home to the deployment server, in epoch time.</td>
</tr>
<tr>
<td>maxPhonehome_latency_to_avgInterval_ratio</td>
<td>The maximum value specified for the ratio of the phone home latency to the average phone home interval.</td>
</tr>
<tr>
<td>mgmt</td>
<td>The management port for the deployment client.</td>
</tr>
<tr>
<td>minLatestPhonehomeTime</td>
<td>Specifies in epoch seconds the minimum latency for a client to contact the deployment server.</td>
</tr>
<tr>
<td>minPhonehome_latency_to_avgInterval_ratio</td>
<td>The minimum value specified for the ratio of the phone home latency to the average phone home interval.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the deployment client server.</td>
</tr>
<tr>
<td>serverClasses</td>
<td>The list of server classes to which the client belongs.</td>
</tr>
<tr>
<td>serverclasses</td>
<td>List of server classes for the deployment client.</td>
</tr>
<tr>
<td>utsname</td>
<td>Machine type for the deployment server client.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -k -u admin:pass
https://localhost:8089/services/deployment/server/clients/dc95537d0e8fdadc44d00c50fc431e25

XML Response

...
<s:dict>
  <s:key name="restartSplunkd">0</s:key>
  <s:key name="result">Ok</s:key>
  <s:key name="serverclasses">
    <s:list>
      <s:item>sc_new</s:item>
      <s:item>sc_apps_wma</s:item>
    </s:list>
  </s:key>
  <s:key name="size">112640</s:key>
  <s:key name="stateOnClient">enabled</s:key>
  <s:key name="averagePhoneHomeInterval">60</s:key>
  <s:key name="build">172889</s:key>
  <s:key name="dns">localhost.sv.splunk.com</s:key>
  <s:key name="guid">dc95537d0e8fdadc44d00c50fc431e25</s:key>
  <s:key name="hostname">localhost.sv.splunk.com</s:key>
  <s:key name="id">connection_10.160.24.187_8089_localhost.sv.splunk.com_localhost.sv.splunk.com_Ombra</s:key>
  <s:key name="ip">10.160.24.187</s:key>
  <s:key name="lastPhoneHomeTime">1375667964</s:key>
  <s:key name="mgmt">8089</s:key>
  <s:key name="name">Ombra</s:key>
  <s:key name="serverClasses">
    <s:dict>
      <s:key name="sc_apps_wma">
        <s:dict>
          <s:key name="loadTime">1375467593</s:key>
          <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
          <s:key name="restartSplunkWeb">0</s:key>
          <s:key name="restartSplunkd">0</s:key>
          <s:key name="stateOnClient">enabled</s:key>
        </s:dict>
      </s:key>
      <s:key name="sc_mach_type">
        <s:dict>
          <s:key name="loadTime">1375467593</s:key>
          <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
          <s:key name="restartSplunkWeb">0</s:key>
          <s:key name="restartSplunkd">0</s:key>
          <s:key name="stateOnClient">enabled</s:key>
        </s:dict>
      </s:key>
      <s:key name="sc_new">
        <s:dict>
          <s:key name="loadTime">1375467593</s:key>
          <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
          <s:key name="restartSplunkWeb">0</s:key>
          <s:key name="restartSplunkd">0</s:key>
          <s:key name="stateOnClient">enabled</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
  <s:key name="utsname">linux-x86_64</s:key>
</s:dict>
deployment/server/config

https://<host>:<mPort>/services/deployment/server/config

Access server configuration information for deployment servers.

POST

List configuration information for all deployment servers.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>currentDownloads</td>
<td>The number of current downloads for this deployment server.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates whether the deployment server is disabled.</td>
</tr>
<tr>
<td>loadTime</td>
<td>The time, in epoch seconds, the serverclass for this server was loaded.</td>
</tr>
<tr>
<td>repositoryLocation</td>
<td>The location on the deployment server to store the content that is to be deployed.</td>
</tr>
<tr>
<td>whitelist.0</td>
<td>Lists the contents of whitelist.0.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/deployment/server/config

XML Response

...<title>deploymentserver</title>
<id>https://localhost:8089/services/deployment/server/config</id>
<updated>2013-08-01T08:17:38-07:00</updated>
<generator build="172889" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/server/config/_reload" rel="_reload"/>
<link href="/services/deployment/server/config/attributesUnsupportedInUI" rel="attributesUnsupportedInUI"/>
<link href="/services/deployment/server/config/listIsDisabled" rel="listIsDisabled"/>
... opensearch nodes elided ...
<s:messages/>

400
deployment/server/config/attributesUnsupportedInUI

https://<host>:<mPort>/services/deployment/server/config/attributesUnsupportedInUI

Access deployment server attributes that cannot be configured from Splunk Web.

GET

Lists deployment server attributes that cannot be configured from Splunk Web.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>property</td>
<td>The attribute that cannot be configured from Splunk Web.</td>
</tr>
<tr>
<td>reason</td>
<td>The reason an attribute cannot be configured from Splunk Web.</td>
</tr>
<tr>
<td>stanza</td>
<td>In Splunk Enterprise, the stanza in serverclass.conf that lists deployment server attributes that cannot be configured from Splunk Web.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

401
curl -k -u admin:pass https://localhost:8089/services/deployment/server/config/attributesUnsupportedInUI

**XML Response**

...  
<title>deploymentserver</title>  
$id>https://localhost:8089/services/deployment/server/config</id>  
<updated>2013-08-04T19:14:20-07:00</updated>  
<generator build="172889" version="6.0"/>  
<author>  
 <name>Splunk</name>  
</author>  
<link href="/services/deployment/server/config/_reload" rel="_reload"/>  
<link href="/services/deployment/server/config/attributesUnsupportedInUI" rel="attributesUnsupportedInUI"/>  
<link href="/services/deployment/server/config/listIsDisabled" rel="listIsDisabled"/>  
... eai:acl node elided ...  
<s:messages/>  
<entry>  
 <title>item_0</title>  
$id>https://localhost:8089/services/deployment/server/config/item_0</id>  
<updated>2013-08-04T19:14:20-07:00</updated>  
<author>  
 <name>system</name>  
</author>  
<link href="/services/deployment/server/config/item_0" rel="alternate"/>  
<link href="/services/deployment/server/config/item_0" rel="list"/>  
<link href="/services/deployment/server/config/item_0/_reload" rel="_reload"/>  
<link href="/services/deployment/server/config/item_0" rel="edit"/>  
<content type="text/xml">  
<s:dict>  
 ... opensearch nodes elided ...  
<s:key name="property">whitelist.0</s:key>  
<s:key name="reason">unsupported at this level</s:key>  
<s:key name="stanza">global</s:key>  
</s:dict>  
</content>  
</entry>  

**deployment/server/config/listIsDisabled**

https://<host>:<mPort>/services/deployment/server/config/listIsDisabled

Access deployment server enablement status.

**GET**

Access deployment server enablement status.

**Request parameters**
None
Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Indicates if the deployment server is disabled.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/deployment/server/config/listIsDisabled

**XML Response**

```
...<title>deploymentserver</title>
{id>https://localhost:8089/services/deployment/server/config</id>
<updated>2013-08-10T14:08:11-07:00</updated>
<generator build="176231" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/server/config/_reload" rel="_reload"/>
<link href="/services/deployment/server/config/attributesUnsupportedInUI" rel="attributesUnsupportedInUI"/>
<link href="/services/deployment/server/config/listIsDisabled" rel="listIsDisabled"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>default</title>
  <id>https://localhost:8089/services/deployment/server/config/default</id>
  <updated>2013-08-10T14:08:11-07:00</updated>
  <link href="/services/deployment/server/config/default" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/deployment/server/config/default" rel="list"/>
  <link href="/services/deployment/server/config/default/_reload" rel="_reload"/>
  <link href="/services/deployment/server/config/default/edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      ... eai:acl node elided ...
    </s:dict>
  </content>
</entry>
```

deployment/server/serverclasses

https://host>:<mPort>/services/deployment/server/serverclasses
Access information about server classes.
GET

List server classes for this deployment server.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blacklist-size</td>
<td>The number of entries in the blacklist for this server class.</td>
</tr>
<tr>
<td>clientId</td>
<td>ID of deployment client for this server class.</td>
</tr>
<tr>
<td>currentDownloads</td>
<td>Number of applications currently downloaded.</td>
</tr>
<tr>
<td>hasDeploymentError</td>
<td>Indicates whether the server class has at least one deployment error.</td>
</tr>
<tr>
<td>loadTime</td>
<td>The time, in epoch seconds, this server class was loaded.</td>
</tr>
<tr>
<td>machineTypesFilter</td>
<td>List of filters to be used in Boolean and logic with whitelist and blacklist filters.</td>
</tr>
<tr>
<td>repositoryList</td>
<td>List of applications stored at the location specified by repositoryLocation.</td>
</tr>
<tr>
<td>repositoryLocation</td>
<td>The location on the deployment server to store the content that is to be deployed for this server class.</td>
</tr>
<tr>
<td>restartSplunkWeb</td>
<td>Indicates whether to restart Splunk Web.</td>
</tr>
<tr>
<td>restartSplunkd</td>
<td>Indicates whether to restart splunkd.</td>
</tr>
<tr>
<td>stateOnClient</td>
<td>Indicates whether this server class is enabled or disabled.</td>
</tr>
<tr>
<td>whitelist-size</td>
<td>Specifies the number of entries in the whitelist for this server class.</td>
</tr>
<tr>
<td>whitelist.0</td>
<td>List of servers for whitelist.0 for this server class.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses
```

**XML Response**

```xml
...<title>serverclasses</title>
<id>https://localhost:8089/services/deployment/server/serverclasses</id>
<updated>2013-08-01T09:50:16-07:00</updated>
<generator build="172889" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/server/serverclasses/_new" rel="create"/>
<link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
... opensearch nodes elided ...
<s:messages/>
```

404
POST

Create a server class.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
<td>String</td>
<td>required</td>
<td>The name of the server class.</td>
</tr>
<tr>
<td>blacklist.*</td>
<td>String</td>
<td></td>
<td>List of hosts to exclude for this server class.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For each blacklist, replace * with an ordinal number to specify additional blacklists. Filter ordinals must start at 0 and be consecutive.</td>
</tr>
<tr>
<td><strong>continueMatching</strong></td>
<td>Boolean</td>
<td></td>
<td>Controls how configuration is layered across classes and server-specific settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If true, configuration lookups continue matching server classes, beyond the first match. If false, only the first match is used. Matching is done in the order that server classes are defined. Defaults to true.</td>
</tr>
<tr>
<td><strong>filterType</strong></td>
<td>Enum</td>
<td></td>
<td>Valid values: (whitelist</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Determines the order of execution of filters. If filterType is whitelist, all whitelist filters are applied first, followed by blacklist filters. If filterType is blacklist, all blacklist filters are applied first, followed by whitelist filters.</td>
</tr>
</tbody>
</table>

The whitelist setting indicates a filtering strategy that pulls in a subset:

- Items are not considered to match the server class by default.
- Items that match any whitelist entry, and do not match any blacklist entry, are considered to match the server class.
- Items that match any blacklist entry are not considered to match the server class, regardless of whitelist.

The blacklist setting indicates a filtering strategy that rules out a subset:
Items are considered to match the server class by default.
• Items that match any blacklist entry, and do not match any whitelist entry, are considered to not match the server class.
• Items that match any whitelist entry are considered to match the server class.

More briefly:

whitelist: default no-match -> whitelists enable -> blacklists disable
blacklist: default match -> blacklists disable-> whitelists enable

If you specify whitelist at the global level, and then specify blacklist for an individual server class, the setting becomes blacklist for that server class, and you have to provide another filter in that server class definition to replace the one you overrode.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| machineTypesFilter  | String  |         | Comma-separated list of filters to be used in Boolean and logic with whitelist and blacklist filters. Only clients that match the white/blacklist filters AND that match this machineTypesFilter are included. Thus the match is an intersection of the matches for the white/blacklist and the matches for MachineTypesFilter. The patterns are PCRE regular expressions, with the following aids for easier entry:  
• You can specify `\.` to mean `.\.`  
• You can specify `\*` to mean `.\*`  
• Matches are always case-insensitive; you do not need to specify the `(?!)` prefix. |
| repositoryLocation  | String  |         | The location on the deployment server to store the content that is to be deployed for this server class.  
For example: `$SPLUNK_HOME/etc/deployment-apps` |
| restartSplunkWeb    | Boolean |         | Indicates whether to restart SplunkWeb on the client when a member app or a directly configured app is updated.  
Defaults to false |
| restartSplunkd      | Boolean |         | Indicates whether to restart splunkd on the client when a member app or a directly configured app is updated.  
Defaults to false |
| stateOnClient       | Enum    |         | Valid values are (enabled | disabled | noop).  
• enabled: Default value. Sets the application state to enabled on the client, regardless of state on the deployment server.  
• disabled: Sets the application state to disabled on the client, regardless of state on the deployment server.  
• noop: The state on the client is the same as on the deployment server. |
| targetRepositoryLocation | String |         | The location on the deployment client to install the apps defined for this Deployment Server. |
If unset, or set to empty, the repositoryLocation path is used. That is, defaults to:

$SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk instance)

Useful only with complex (for example, tiered) deployment strategies.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tmpFolder</td>
<td>String</td>
<td>Working folder used by deployment server.</td>
<td>Defaults to $SPLUNK_HOME/var/run/tmp</td>
</tr>
<tr>
<td>whitelist.*</td>
<td>String</td>
<td>List of hosts to accept for this server class.</td>
<td>For each whitelist, replace * with an ordinal number to specify additional</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>whitelists. Filter ordinals must start at 0 and be consecutive.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blacklist-size</td>
<td>The number of entries in the blacklist for this serverclass.</td>
</tr>
<tr>
<td>blacklist.*</td>
<td>Regular expressions used to exclude for this server class.</td>
</tr>
<tr>
<td>continueMatching</td>
<td>If true, configuration lookups continue matching server classes, beyond the first match. If false, only the first match is used.</td>
</tr>
<tr>
<td>currentDownloads</td>
<td>Number of applications currently downloaded.</td>
</tr>
<tr>
<td>filterType</td>
<td>Determines the order of execution of filters. If filterType is whitelist, all whitelist filters are applied first, followed by blacklist filters. If filterType is blacklist, all blacklist filters are applied first, followed by whitelist filters.</td>
</tr>
<tr>
<td>loadTime</td>
<td>The time, in epoch seconds, this serverclass was loaded.</td>
</tr>
<tr>
<td>machineTypesFilter</td>
<td>List of filters to be used in Boolean and logic with whitelist and blacklist filters.</td>
</tr>
<tr>
<td>repositoryList</td>
<td>List of applications stored at the location specified by repositoryLocation.</td>
</tr>
<tr>
<td>repositoryLocation</td>
<td>The location on the deployment server to store the content that is to be deployed for this server class.</td>
</tr>
<tr>
<td>restartSplunkWeb</td>
<td>Indicates whether to restart Splunk Web.</td>
</tr>
<tr>
<td>restartSplunkd</td>
<td>Indicates whether to restart splunkd.</td>
</tr>
<tr>
<td>stateOnClient</td>
<td>Specifies whether the deployment client is enabled or disabled.</td>
</tr>
<tr>
<td>targetRepositoryLocation</td>
<td>The location on the deployment client to install the apps defined for this Deployment Server.</td>
</tr>
</tbody>
</table>
If unset, or set to empty, the repositoryLocation path is used.

That is, defaults to: $SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk deployment.

Useful only with complex (for example, tiered) deployment strategies.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tmpFolder</td>
<td>Working folder used by deployment server. Defaults to $SPLUNK_HOME/var/run/tmp</td>
</tr>
<tr>
<td>whitelist-size</td>
<td>Specifies the number of entries in the whitelist for this server class.</td>
</tr>
<tr>
<td>whitelist.*</td>
<td>Regular expressions used to accept for this server class. If a client matches any of the whitelist regular expressions, it is included in the server class. The * is replaced by an integral ordinal number.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses -d name=sc_apps_ombra
```

**XML Response**

```xml
...<title>serverclasses</title>
<id>https://localhost:8089/services/deployment/server/serverclasses</id>
<updated>2013-08-10T13:18:28-07:00</updated>
<generator build="176231" version="6.0"/>
<author>
     <name>Splunk</name>
</author>
<link href="/services/deployment/server/serverclasses/_new" rel="create"/>
<link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
     <title>sc_apps_ombra</title>
     <id>https://localhost:8089/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra</id>
     <updated>2013-08-10T13:18:28-07:00</updated>
     <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra" rel="alternate"/>
     <author>
          <name>nobody</name>
     </author>
     <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra/applications" rel="applications"/>
     <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra/clients" rel="clients"/>
     <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_ombra/reload" rel="reload"/>
     <content type="text/xml">
          <s:dict>
```

409
deployment/server/serverclasses/rename

https://<host>:<mPort>/services/deployment/server/serverclasses/rename

Rename a server class.

POST

Specify a new name for a server class.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>newName</td>
<td>String</td>
<td></td>
<td>The new name of the server class.</td>
</tr>
<tr>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>oldName</td>
<td>String</td>
<td></td>
<td>The current name of the server class.</td>
</tr>
<tr>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

```bash
curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses/rename -d
```
oldName=sc_apps_ombra -d newName=sc_apps_shadow

**XML Response**

... 
<title>serverclasses</title>
{id>https://localhost:8089/services/deployment/server/serverclasses</id>
<updated>2013-10-09T08:54:09-07:00</updated>
<generator build="176231" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/server/serverclasses/_new" rel="create"/>
<link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>sc_apps_shadow</title>
  <id>https://localhost:8089/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow</id>
  <updated>2013-10-09T08:54:09-07:00</updated>
  <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow" rel="list"/>
  <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow" rel="edit"/>
  <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow" rel="remove"/>
  <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow/applications" rel="applications"/>
  <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow/clients" rel="clients"/>
  <link href="/servicesNS/nobody/search/deployment/server/serverclasses/sc_apps_shadow/reload" rel="reload"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="blacklist-size">0</s:key>
      <s:key name="currentDownloads">0</s:key>
      ... eai:acl node elided ...
      <s:key name="loadTime">1381334049</s:key>
      <s:key name="machineTypesFilter"></s:key>
      <s:key name="repositoryList">
        <s:dict>
          <s:key name="tmp"/>
          <s:key name="wma-app-test2"/>
          <s:key name="wma-app3"/>
          <s:key name="wma-app_test1"/>
        </s:dict>
      </s:key>
      <s:key name="repositoryLocation">/opt/cluster/peer1/splunk/etc/deployment-apps</s:key>
      <s:key name="restartSplunkWeb"></s:key>
      <s:key name="restartSplunkd"></s:key>
      <s:key name="stateOnClient">enabled</s:key>
      <s:key name="whitelist-size">0</s:key>
    </s:dict>
  </content>
</entry>
deployment/server/serverclasses/{name}

https://<host>:<mPort>/services/deployment/server/serverclasses/{name}

Manage the {name} serverclass.

DELETE

Remove the specified server class from this deployment server.

Request parameters
None

 Returned values
None

Example request and response

XML Request

curl -k -u admin:pass --request DELETE
https://localhost:8089/services/deployment/server/serverclasses/sc_apps_shadow

XML Response

...  
<title>serverclasses</title>
{id>https://localhost:8089/services/deployment/server/serverclasses</id>
<updated>2013-10-09T09:13:27-07:00</updated>
<generator build="176231" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/server/serverclasses/_new" rel="create"/>
<link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>sc_apps_wma</title>
  <id>https://localhost:8089/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma</id>
  <updated>2013-10-09T09:13:27-07:00</updated>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="list"/>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="edit"/>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma" rel="remove"/>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_apps_wma/applications" rel="applications"/>

412
GET

List information about the named server class.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clientId</td>
<td>String</td>
<td>GUID</td>
<td>GUID of a deployment client that is a member of the named server class. Lists information about the named server class with respect to this client.</td>
</tr>
<tr>
<td>hasDeploymentError</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to only list server classes that have a deployment error.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blacklist-size</td>
<td>Specifies the size of the blacklist for the named server class.</td>
</tr>
<tr>
<td>clientId</td>
<td>ID of deployment client for this server class.</td>
</tr>
<tr>
<td>currentDownloads</td>
<td>The number of entries in the blacklist for this server class.</td>
</tr>
<tr>
<td>hasDeploymentError</td>
<td>Indicates whether the serverclass has at least one deployment error.</td>
</tr>
<tr>
<td>loadTime</td>
<td>The time, in epoch seconds, this serverclass was loaded.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>machineTypesFilter</td>
<td>List of filters to be used in Boolean and logic with whitelist and blacklist filters.</td>
</tr>
<tr>
<td>repositoryList</td>
<td>List of applications stored at the location specified by repositoryLocation.</td>
</tr>
<tr>
<td>repositoryLocation</td>
<td>The location on the deployment server to store the content that is to be deployed for this server class.</td>
</tr>
<tr>
<td>restartSplunkWeb</td>
<td>Indicates whether to restart Splunk Web.</td>
</tr>
<tr>
<td>restartSplunkd</td>
<td>Indicates whether to restart splunkd.</td>
</tr>
<tr>
<td>stateOnClient</td>
<td>Indicates whether this server class is enabled or disabled.</td>
</tr>
<tr>
<td>whitelist-size</td>
<td>Specifies the number of entries in the whitelist for this server class.</td>
</tr>
<tr>
<td>whitelist.0</td>
<td>List of servers for whitelist.0 for this server class.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses/sc_mach_type
```

**XML Response**

```xml
...<title>serverclasses</title>
<id>https://localhost:8089/services/deployment/server/serverclasses</id>
<updated>2013-08-04T19:34-07:00</updated>
<generator build="172889" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/deployment/server/serverclasses/_new" rel="create"/>
<link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>sc_mach_type</title>
  <id>https://localhost:8089/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type</id>
  <updated>2013-08-04T19:34-07:00</updated>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="list"/>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="edit"/>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type" rel="remove"/>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type/applications" rel="applications"/>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type/clients" rel="clients"/>
  <link href="/servicesNS/nobody/system/deployment/server/serverclasses/sc_mach_type/reload" rel="reload"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="blacklist-size">0</s:key>
      <s:key name="currentDownloads">0</s:key>
      ... eai:acl node elided ...
      <s:key name="eai:attributes">... elided ...</s:key>
    </s:dict>
  </content>
</entry>
```
POST

Update the named server class.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blacklist.*</td>
<td>String</td>
<td></td>
<td>List of hosts to exclude for this server class.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For each blacklist, replace * with an ordinal number to specify additional</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>blacklists. Filter ordinals must start at 0 and be consecutive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For each blacklist, replace * with an ordinal number to specify additional</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>blacklists. Filter ordinals must start at 0 and be consecutive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Controls how configuration is layered across classes and server-specific</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If true, configuration lookups continue matching server classes, beyond the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>first match. If false, only the first match is used. Matching is done in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>order that server classes are defined. Defaults to true.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A serverClass can override this property and stop the matching.</td>
</tr>
<tr>
<td>filterType</td>
<td>Enum</td>
<td></td>
<td>Valid values: (whitelist</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Determines the order of execution of filters. If filterType is whitelist,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>all whitelist filters are applied first, followed by blacklist filters. If</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>filterType is blacklist, all blacklist filters are applied first, followed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>by whitelist filters.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The whitelist setting indicates a filtering strategy that pulls in a subset:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Items are not considered to match the server class by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Items that match any whitelist entry, and do not match any blacklist</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>entry, are considered to match the server class.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Items that match any blacklist entry are not considered to match the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>server class, regardless of whitelist.</td>
</tr>
</tbody>
</table>
The blacklist setting indicates a filtering strategy that rules out a subset:

- Items are considered to match the server class by default.
- Items that match any blacklist entry, and do not match any whitelist entry, are considered to not match the server class.
- Items that match any whitelist entry are considered to match the server class.

More briefly:

whitelist: default no-match -> whitelists enable -> blacklists disable
blacklist: default match -> blacklists disable-> whitelists enable

If you specify whitelist at the global level, and then specify blacklist for an individual server class, the setting becomes blacklist for that server class, and you have to provide another filter in that server class definition to replace the one you overrode.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| machineTypesFilter | String |         | Comma-separated list of filters to be used in Boolean and logic with whitelist and blacklist filters. Only clients that match the white/blacklist filters AND that match this machineTypesFilter are included. Thus the match is an intersection of the matches for the white/blacklist and the matches for MachineTypesFilter. The patterns are PCRE regular expressions, with the following aids for easier entry:
  - You can specify `\.` to mean `\.\`
  - You can specify `\*` to mean `\.*`
  - Matches are always case-insensitive; you do not need to specify the `(?!)` prefix. |
| repositoryLocation | String |         | The location on the deployment server to store the content that is to be deployed for this server class. For example: `$SPLUNK_HOME/etc/deployment-apps` |
| restartSplunkWeb  | Boolean |         | Indicates whether to restart SplunkWeb on the client when a member app or a directly configured app is updated. Defaults to false |
| restartSplunkd    | Boolean |         | Indicates whether to restart splunkd on the client when a member app or a directly configured app is updated. Defaults to false |
| stateOnClient     | Enum   |         | Valid values are (enabled | disabled | noop).
  - enabled: Default value. Sets the application state to enabled on the client, regardless of state on the deployment server.
  - disabled: Sets the application state to disabled on the client, regardless of state on the deployment server.
  - noop: The state on the client is the same as on the deployment server. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>targetRepositoryLocation</td>
<td>String</td>
<td></td>
<td>The location on the deployment client to install the apps defined for this Deployment Server. If unset, or set to empty, the repositoryLocation path is used. That is, defaults to: $SPLUNK_HOME/etc/apps (the live configuration directory for a Splunk instance Useful only with complex (for example, tiered) deployment strategies.</td>
</tr>
<tr>
<td>tmpFolder</td>
<td>String</td>
<td></td>
<td>Working folder used by deployment server. Defaults to $SPLUNK_HOME/var/run/tmp</td>
</tr>
<tr>
<td>whitelist.*</td>
<td>String</td>
<td></td>
<td>List of hosts to accept for this server class. For each whitelist, replace * with an ordinal number to specify additional whitelists. Filter ordinals must start at 0 and be consecutive.</td>
</tr>
</tbody>
</table>

**Returned values**
None

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/deployment/server/serverclasses/sc_apps_ombra -d stateOnClient=noop

**XML Response**

```xml
<title>serverclasses</title>
<id>https://localhost:8089/services/deployment/server/serverclasses</id>
<updated>2013-08-10T13:24:16-07:00</updated>
<generator build="176231" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
(link href="/services/deployment/server/serverclasses/_new" rel="create"/>
<link href="/services/deployment/server/serverclasses/rename" rel="rename"/>
... opensearch nodes elided ...
<s:messages/>
</entry>
<title>sc_apps_ombra</title>
<id>https://localhost:8089/services/deployment/server/serverclasses/sc_apps_ombra</id>
<updated>2013-08-10T13:24:16-07:00</updated>
<link href="/services/deployment/server/serverclasses/sc_apps_ombre" rel="alternate"/>
<author>
  <name>system</name>
</author>
```
search/distributed/bundle/replication/config

https://<host>:<mPort>/services/search/distributed/bundle/replication/config
Provides information on knowledge bundle replication configuration on a search head.

Authentication and Authorization
Requires the search capability.

Usage details
See Troubleshoot knowledge bundle replication in Distributed Search.

GET
List knowledge bundle replication configuration settings.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>concerningReplicatedFileSize</td>
<td>A warning will be logged if the bundle lookup size exceeds this value</td>
</tr>
<tr>
<td>connectionTimeout</td>
<td>Timeout value for establishing connection between search head and indexer</td>
</tr>
<tr>
<td>maxBundleSize</td>
<td>Maximum allowable bundle size</td>
</tr>
<tr>
<td>receiveTimeout</td>
<td>Timeout value for receiving data between search head and indexer</td>
</tr>
<tr>
<td>replicationPeriod</td>
<td>Period during which the replicationThread checks whether bundle replication is required</td>
</tr>
<tr>
<td>replicationPolicy</td>
<td>Bundle replication policy in use</td>
</tr>
<tr>
<td>sendTimeout</td>
<td>Timeout value for sending data between search head and indexer</td>
</tr>
<tr>
<td>statusQueueSize</td>
<td>Size of the cycles maintained in memory and available through the cycles endpoint</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://ronnie:8089/services/search/distributed/bundle/replication/config

XML Response
<title>bundle-replication-config</title>
<id>https://qa-centos7x64-056:8089/services/search/distributed/bundle/replication/config</id>
<updated>2019-08-23T16:26:22-07:00</updated>
<generator build="9f02da632403" version="8.0.0"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>bundleReplicationConfig</title>
  <id>https://qa-centos7x64-056:8089/services/search/distributed/bundle/replication/config/bundleReplicationConfig</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/search/distributed/bundle/replication/config/bundleReplicationConfig" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/search/distributed/bundle/replication/config/bundleReplicationConfig" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="concerningReplicatedFileSize">52428800</s:key>
      <s:key name="connectionTimeout">60</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>power</s:item>
                  <s:item>splunk-system-role</s:item>
                  <s:item>user</s:item>
                </s:list>
              </s:key>
              <s:key name="write"></s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="maxBundleSize">2147483648</s:key>
      <s:key name="receiveTimeout">60</s:key>
      <s:key name="replicationPeriod">60</s:key>
      <s:key name="replicationPolicy">classic</s:key>
      <s:key name="replicationThreads">9</s:key>
      <s:key name="sendTimeout">60</s:key>
    </s:dict>
  </content>
</entry>
search/distributed/bundle/replication/cycles

https://<host>:<mPort>/services/search/distributed/bundle/replication/cycles
Provides information and status for knowledge bundle replication cycles on a search head.

Authentication and Authorization
Requires the search capability.

Usage details
See Troubleshoot knowledge bundle replication in Distributed Search.

GET
List information and status for knowledge bundle replication cycles.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>latest</td>
<td>Boolean</td>
<td>Optional. If set to true, information about only the latest cycle is returned.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle_id</td>
<td>Knowledge bundle unique identifier composed of hostname-creation_time</td>
</tr>
<tr>
<td>current_bundle</td>
<td>Path to active knowledge bundle on disk</td>
</tr>
<tr>
<td>current_repl_start_time</td>
<td>Start time of current replication cycle</td>
</tr>
<tr>
<td>cycle_id</td>
<td>Bundle replication cycle unique identifier</td>
</tr>
<tr>
<td>delta_path</td>
<td>Path to the delta knowledge bundle on disk, if a delta was created</td>
</tr>
<tr>
<td>is_repl_in_progress</td>
<td>Boolean to indicate whether the replication cycle is in progress or completed</td>
</tr>
<tr>
<td>peers_status</td>
<td>Entry for each peer with peer_name and replication state for each peer</td>
</tr>
<tr>
<td>replicationPolicy</td>
<td>Bundle replication policy in use</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:changeme

**XML Response**
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:replication-cycles="http://dev.splunk.com/ns/rest">
  <title>bundle-replication-cycles</title>
  <id>https://qa-centos7x64-056:8089/services/search/distributed/bundle/replication/cycles</id>
  <updated>2019-08-23T16:32:20-07:00</updated>
  <generator build="9f02da632403" version="8.0.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>80CC124B-2D46-44A7-95C2-A92ECC32C050</title>
    <id>https://qa-centos7x64-056:8089/services/search/distributed/bundle/replication/cycles/80CC124B-2D46-44A7-95C2-A92ECC32C050</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/search/distributed/bundle/replication/cycles/80CC124B-2D46-44A7-95C2-A92ECC32C050" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/search/distributed/bundle/replication/cycles/80CC124B-2D46-44A7-95C2-A92ECC32C050" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="bundle_id">qa-centos7x64-056-1566601784</s:key>
        <s:key name="current_bundle">/root/splunk_install/var/run/qa-centos7x64-056-1566601784.bundle</s:key>
        <s:key name="current_repl_start_time">1566602286</s:key>
        <s:key name="cycle_id">80CC124B-2D46-44A7-95C2-A92ECC32C050</s:key>
        <s:key name="delta_path">/root/splunk_install/var/run/qa-centos7x64-056-1566601708-1566601784.delta</s:key>
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner" s:dict>system</s:key>
          <s:dict>
            <s:key name="read">
              <s:list>admin</s:list>
              <s:list>power</s:list>
              <s:list>splunk-system-role</s:list>
              <s:list>user</s:list>
            </s:list>
            <s:key name="write"></s:key>
          </s:dict>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:dict>
    </content>
  </entry>
</feed>
search/distributed/bundle-replication-files

https://<host>:<mPort>/services/search/distributed/bundle-replication-files
Access information for the most recent distributed search bundle.

GET
List distributed search bundle replication files.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>checksum</td>
<td>Common checksum for entities in the bundle.</td>
</tr>
<tr>
<td>filename</td>
<td>Bundle file name</td>
</tr>
<tr>
<td>location</td>
<td>Bundle file path</td>
</tr>
<tr>
<td>size</td>
<td>Bundle size, in bytes</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>timestamp</td>
<td>Bundle creation timestamp.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/search/distributed/bundle-replication-files

**XML Response**

```xml
<author><name>Splunk</name></author>... opensearch nodes elided ...
<s:messages/>
<entry>
<title>13134207368020721783</title>
<id>https://localhost:8089/services/search/distributed/bundle-replication-files/13134207368020721783</id>
<updated>2013-10-09T09:42:51-07:00</updated>
<link href="/services/search/distributed/bundle-replication-files/13134207368020721783" rel="alternate"/>
<author><name>system</name></author>
<link href="/services/search/distributed/bundle-replication-files/13134207368020721783" rel="list"/>
<content type="text/xml">
<s:dict>
<s:key name="checksum">13134207368020721783</s:key>
... eai:acl node elided ...
<s:key name="filename">localhost-1381336958.bundle</s:key>
<s:key name="location">/opt/cluster/peer1/splunk/var/run/localhost-1381336958.bundle</s:key>
<s:key name="timestamp">1381336958</s:key>
</s:dict>
</content>
</entry>
```

**search/distributed/bundle-replication-files/{name}**

https://<host>:<mPort>/services/search/distributed/bundle-replication-files/{name}

Get (name) bundle replication file information.
GET

List information about the specified bundle replication file. For \(\text{name}\), specify the checksum for the file.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\text{force_list_all})</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to force a listing of the file.</td>
</tr>
</tbody>
</table>

**Returned values**

None

**Example request and response**

**XML Request**

```
curl -k -u admin:pass
```

**XML Response**

```xml
...<title>search-head-bundles</title>
<updated>2013-10-09T10:07:17-07:00</updated>
<generator build="176231" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>13134207368020721783</title>
  <id>https://localhost:8089/services/search/distributed/bundle-replication-files/13134207368020721783</id>
  <updated>2013-10-09T10:07:17-07:00</updated>
  <link href="/services/search/distributed/bundle-replication-files/13134207368020721783" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/search/distributed/bundle-replication-files/13134207368020721783" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:dict>
        <s:dict>
          <s:dict>
      <s:dict>
        <s:dict>
          <s:dict>
            <s:dict>
          <s:dict>
        <s:dict>
      <s:dict>
    </s:dict>
  </content>
</entry>
```
**search/distributed/config**

https://<host>:<mPort>/services/search/distributed/config

Provides access to the Splunk Enterprise distributed search options. This option is not for adding search peers.

**GET**

Lists the configuration options for the distributed search system.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoAddServers</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>blacklistNames</td>
<td>List of filenames that match the blacklist pattern, and are not replicated.</td>
</tr>
<tr>
<td>blacklistURLs</td>
<td>List of URLs that are blacklisted, and thus is not replicated.</td>
</tr>
<tr>
<td>checkTimedOutServersFrequency</td>
<td>Rechecks servers at the specified frequency (in seconds). If this is set to 0, then no recheck occurs. Defaults to 60.</td>
</tr>
<tr>
<td></td>
<td>This attribute is ONLY relevant if <code>removeTimedOutServers</code> is set to <code>true</code>. If <code>removeTimedOutServers</code> is <code>false</code>, this attribute is ignored.</td>
</tr>
<tr>
<td>connectionTimeout</td>
<td>Connection timeout.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the distributed search is disabled.</td>
</tr>
<tr>
<td>dist_search_enabled</td>
<td>Indicates if the distributed search is enabled.</td>
</tr>
<tr>
<td>heartbeatFrequency</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>heartbeatMcastAddr</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>heartbeatPort</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>receiveTimeout</td>
<td>Amount of time in seconds to use as a timeout while trying to read/receive data from a search peer.</td>
</tr>
<tr>
<td>removedTimedOutServers</td>
<td>If true, removes a server connection that cannot be made within <code>serverTimeout</code>. If false, every call to that server attempts to connect. This may result in a slow user interface.</td>
</tr>
<tr>
<td>sendTimeout</td>
<td>Send timeout.</td>
</tr>
<tr>
<td>serverTimeout</td>
<td>[Deprecated] Refer to <code>connectionTimeout</code>, <code>sendTimeout</code>, and <code>receiveTimeout</code>.</td>
</tr>
<tr>
<td>servers</td>
<td>The initial list of servers.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>shareBundles</td>
<td>Indicates whether this server uses bundle replication to share search time configuration with search peers. If set to false, the search head assumes that the search peers can access the correct bundles using an NFS share and have correctly configured the options listed under: &quot;SEARCH HEAD BUNDLE MOUNTING OPTIONS.&quot;</td>
</tr>
<tr>
<td>skipOurselves</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>statusTimeout</td>
<td>Set connection timeout when gathering a search peer's basic info (/services/server/info). Read/write timeouts are automatically set to twice this value.</td>
</tr>
<tr>
<td>ttl</td>
<td>[Deprecated]</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/search/distributed/config
```

**XML Response**

```xml
...<title>distsearch-setup</title>
<id>https://localhost:8089/services/search/distributed/config</id>
<updated>2011-07-10T23:51:07-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>distributedSearch</title>
  <id>https://localhost:8089/services/search/distributed/config/distributedSearch</id>
  <updated>2011-07-10T23:51:07-07:00</updated>
  <link href="/services/search/distributed/config/distributedSearch" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/search/distributed/config/distributedSearch" rel="list"/>
  <link href="/services/search/distributed/config/distributedSearch" rel="edit"/>
  <link href="/services/search/distributed/config/distributedSearch" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="autoAddServers">0</s:key>
      <s:key name="blacklistNames"/>
      <s:key name="blacklistURLs"/>
      <s:key name="checkTimedOutServersFrequency">60</s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="dist_search_enabled">1</s:key>
      ... eai:acl node elided ...
      <s:key name="heartbeatFrequency">0</s:key>
      <s:key name="heartbeatMcastAddr">224.0.0.37</s:key>
```
search/distributed/peers

https://<host>:<mPort>/services/search/distributed/peers

Provides distributed peer server management. A search peer is defined as a Splunk server to which another Splunk server distributes searches. The Splunk server where the search request originates is referred to as the search head.

GET

Get configured search peers to which this search head is configured to distribute searches. This includes configured but disabled search peers.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>build</td>
<td>The Splunk build number for this peer.</td>
</tr>
<tr>
<td>bundle_versions</td>
<td>The IDs of the bundles (of this search head) that the peer has.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the peer is disabled.</td>
</tr>
<tr>
<td>guid</td>
<td>GUID of the peer.</td>
</tr>
<tr>
<td>is_https</td>
<td>Indicates if the management port is using SSL.</td>
</tr>
<tr>
<td>licenseSignature</td>
<td>The license signature.</td>
</tr>
<tr>
<td>peerName</td>
<td>The Splunk server name of the peer.</td>
</tr>
<tr>
<td>peerType</td>
<td>Specifies whether the peer is configured or discovered.</td>
</tr>
<tr>
<td>replicationStatus</td>
<td>The status of bundle replication to this peer. Can be any of the following values:</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>status</td>
<td>The status of the peer.</td>
</tr>
<tr>
<td></td>
<td>Can be one of the following values:</td>
</tr>
<tr>
<td></td>
<td>Up</td>
</tr>
<tr>
<td></td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>Blacklisted</td>
</tr>
<tr>
<td></td>
<td>Not a Splunk server</td>
</tr>
<tr>
<td></td>
<td>Free Splunk server</td>
</tr>
<tr>
<td></td>
<td>Authentication Failed</td>
</tr>
<tr>
<td></td>
<td>Duplicate License</td>
</tr>
<tr>
<td></td>
<td>Duplicate Servername</td>
</tr>
<tr>
<td></td>
<td>Inconsistent bundles</td>
</tr>
<tr>
<td>status_details</td>
<td>Details of any errors encountered in the last heartbeat period.</td>
</tr>
<tr>
<td>version</td>
<td>The Splunk software version string this peer is running.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/search/distributed/peers
```

**XML Response**

```xml
...
<title>distsearch-peer</title>
{id>https://localhost:8089/services/search/distributed/peers</id>
<updated>2011-07-11T18:21:48-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/search/distributed/peers/_new" rel="create"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>tiny:8090</title>
  <id>https://localhost:8089/services/search/distributed/peers/tiny%3A8090</id>
  <updated>2011-07-11T18:21:48-07:00</updated>
  <link href="/services/search/distributed/peers/tiny%3A8090" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/search/distributed/peers/tiny%3A8090" rel="list"/>
  <link href="/services/search/distributed/peers/tiny%3A8090" rel="edit"/>
  <link href="/services/search/distributed/peers/tiny%3A8090" rel="remove"/>
  <link href="/services/search/distributed/peers/tiny%3A8090/disable" rel="disable"/>
  <content type="text/xml">
```
POST

Add a new distributed search peer.

Usage details
The distributed search must first be enabled using the search/distributed/config endpoint.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Required</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required</td>
<td></td>
<td>The name of the search peer. Defined as hostname:port, where port is the management port.</td>
</tr>
<tr>
<td>remotePassword</td>
<td>String</td>
<td>Required</td>
<td></td>
<td>The password of the remote user.</td>
</tr>
<tr>
<td>remoteUsername</td>
<td>String</td>
<td>Required</td>
<td></td>
<td>The username of a user with admin privileges in the search peer server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This is used to exchange certificates.</td>
</tr>
</tbody>
</table>

HTTP response codes

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Created successfully.</td>
</tr>
<tr>
<td>400</td>
<td>Request error. See response body for details.</td>
</tr>
<tr>
<td>401</td>
<td>Authentication failure: must pass valid credentials with request.</td>
</tr>
<tr>
<td>402</td>
<td>The Splunk license in use has disabled this feature.</td>
</tr>
<tr>
<td>403</td>
<td>Insufficient permissions to create specified resource.</td>
</tr>
<tr>
<td>409</td>
<td>Request error: this operation is invalid for this item. See response body for details.</td>
</tr>
<tr>
<td>500</td>
<td>Internal server error. See response body for details.</td>
</tr>
<tr>
<td>Status Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>503</td>
<td>This feature has been disabled in Splunk configuration files.</td>
</tr>
</tbody>
</table>

Returned values
No values returned for this request.

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/search/distributed/peers -d name=MrT:8092 -d remoteUsername=admin -d remotePassword=mypass

XML Response

```xml

<title>distsearch-peer</title>
<id>https://localhost:8089/services/search/distributed/peers</id>
<updated>2011-07-11T18:22:00-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/search/distributed/peers/_new" rel="create"/>
... opensearch nodes elided ...
<s:messages/>
```

**search/distributed/peers/{name}**

https://<host>:<mPort>/services/search/distributed/peers
Manage distributed peer servers. A search peer is defined as a Splunk server to which another Splunk server distributes searches. The Splunk server where the search request originates is referred to as the search head.

**POST**

Update a peer server.

**Usage details**
The distributed search must first be enabled using the search/distributed/config endpoint.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Required</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

430
<table>
<thead>
<tr>
<th>remotePassword</th>
<th>String</th>
<th>The password of the remote user.</th>
</tr>
</thead>
<tbody>
<tr>
<td>remoteUsername</td>
<td>String</td>
<td>The username of a user with admin privileges in the search peer server. This is used to exchange certificates.</td>
</tr>
</tbody>
</table>

Returned values
See example.

Example request and response

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/search/distributed/peers/MrT:8092  -d remoteUsername=admin -d remotePassword=mypass
```

**XML Response**

```xml
<title>distsearch-peer</title>
?id>https://localhost:8089/services/search/distributed/peers</id>
<updated>2011-07-11T18:22:00-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/search/distributed/peers/_new" rel="create"/>
... opensearch nodes elided ...
<s:messages/>
```
Input endpoints

Input endpoint descriptions

Manage and preview streaming and non-streaming and other input data.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select Settings > Access controls and click Users. To determine the capabilities assigned to a role, select Settings > Access controls and click Roles.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

Managed Splunk Cloud deployments

https://<deployment-name>.splunkcloud.com:8089

Self-service Splunk Cloud deployments

To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the the Splunk REST API Tutorials for more information.
Access and configure the active directory monitoring input.

GET

Get the current active directory monitoring configuration.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Indicates whether this input is disabled.</td>
</tr>
<tr>
<td>index</td>
<td>The index in which to store the gathered data. If no value is present, sends data to the default index.</td>
</tr>
<tr>
<td>monitorSubtree</td>
<td>Indicates whether or not to monitor the subtrees of a given Active Directory tree path.</td>
</tr>
<tr>
<td>startingNode</td>
<td>Tells Splunk software where in the Active Directory directory tree to start monitoring. If not specified, Splunk software attempts to start at the root of the directory tree. The user as which you configure Splunk to run at installation determines where Splunk software starts monitoring.</td>
</tr>
<tr>
<td>targetDc</td>
<td>Fully qualified domain name of a valid, network-accessible Active Directory domain controller. If not specified, Splunk software obtains the local computer DC by default, and binds to its root Distinguished Name (DN).</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -u admin:pass https://localhost:8089/services/data/inputs/ad
```

XML Response

```xml
...<title>win-admon</title>
{id}https://10.1.157:8089/services/data/inputs/ad</id>
<updated>2011-07-29T19:13:28-07:00</updated>
<generator version=104976”/>
<author>
  <name>Splunk</name>
```

433
POST

Create or modify performance monitoring settings.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>baseline</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to query baseline objects. Defaults to true.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>Docs-W8R2-Std7</td>
<td>Host name for the Active Directory Monitor.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>monitorSubtree</td>
<td>Number</td>
<td>Required</td>
<td>Whether or not to monitor the subtree(s) of a given directory tree path. 1 means yes, 0 means no.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Required</td>
<td>A unique name that represents a configuration or set of configurations for a specific domain controller.</td>
</tr>
<tr>
<td>printSchema</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to print the Active Directory schema. Defaults to true.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Source for data inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>Source type of data inputs.</td>
</tr>
<tr>
<td>Name</td>
<td>Datatype</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>startingNode</td>
<td>String</td>
<td></td>
<td>Where in the Active Directory directory tree to start monitoring. If not specified, attempts to start at the root of the directory tree.</td>
</tr>
<tr>
<td>targetDc</td>
<td>String</td>
<td></td>
<td>Specifies a fully qualified domain name of a valid, network-accessible domain controller. If not specified, Splunk software gets the local domain controller.</td>
</tr>
</tbody>
</table>

**Returned values**
None

**Example request and response**

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/admin/search/data/inputs/ad -d monitorSubtree=0 -d name=newdc

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-admon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad/id</id>
  <updated>2011-07-29T19:14:57-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

**data/inputs/ad/{name}**

https://<host>:<mPort>/services/data/inputs/ad/{name}

Manage **{name}** active directory monitoring.

**DELETE**

Delete the **{name}** Active Directory monitoring stanza.

**Request parameters**
None

**Returned values**
None
Example request and response

XML Request

curl -u admin:pass --request DELETE https://localhost:8089/servicesNS/nobody/search/data/inputs/ad/newdc

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-admon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad</id>
  <updated>2011-07-29T19:22:50-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>

GET

Gets the current configuration for the `{name}` Active Directory monitoring stanza.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates whether this input is disabled.</td>
</tr>
<tr>
<td>index</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td></td>
<td>If no value is present, send data to the default index.</td>
</tr>
<tr>
<td>monitorSubtree</td>
<td>Indicates whether or not to monitor the subtrees of a given Active Directory tree path.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
POST

Update the `{name}` Active Directory monitoring stanza.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>baseline</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to query baseline objects. Defaults to true.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Baseline objects are objects which currently reside in Active Directory and</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>include previously deleted objects.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>Docs-W8R2-Std7</td>
<td>Host name for the Active Directory Monitor.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If not specified defaults to the default index.</td>
</tr>
<tr>
<td>monitorSubtree</td>
<td>Number</td>
<td></td>
<td>Whether or not to monitor the subtree(s) of a given directory tree path.</td>
</tr>
<tr>
<td>required</td>
<td></td>
<td></td>
<td>1 means yes, 0 means no.</td>
</tr>
<tr>
<td>printSchema</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to print the Active Directory schema. Defaults to true.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Source for data inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>Source type of data inputs.</td>
</tr>
<tr>
<td>startingNode</td>
<td>String</td>
<td></td>
<td>Where in the Active Directory directory tree to start monitoring. If not</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>specified, attempts to start at the root of the directory tree.</td>
</tr>
<tr>
<td>targetDc</td>
<td>String</td>
<td></td>
<td>Specifies a fully qualified domain name of a valid, network-accessible DC.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If not specified, Splunk software gets the local computer's DC.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/ad/newdc -d monitorSubtree=1

**XML Response**

```
...<title>win-admon</title>
:id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad</id>
<updated>2011-07-29T19:20:16-07:00</updated>
<generator version="104976"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/data/inputs/ad/_new" rel="create"/>
<link href="/servicesNS/nobody/search/data/inputs/ad/_reload" rel="_reload"/>
```
**data/inputs/all**

https://<host>:<mPort>/services/data/inputs/all

Access all inputs to the Splunk deployment. This includes any modular inputs that may be defined on the system.

**GET**

List all inputs, including modular inputs.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>common</td>
<td>Boolean</td>
<td>Indicates whether to return only attributes common to all inputs. The common attributes are as follows.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• app</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• index</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• owner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• source</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sourcetype</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• title</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• updated</td>
</tr>
</tbody>
</table>

Pagination and filtering parameters can be used with this method.

**Returned values**

Returns an `<entry>` element for each input, listing attributes specific to the input. See the following example for more details.

**Example request and response**

**XML Request**

```bash
curl -u admin:pass https://localhost:8089/services/data/inputs/all
```

**XML Response**

```xml
...<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:s="http://dev.splunk.com/ns/rest"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
```
**data/inputs/all/{name}**

https://<host>:<mPort>/services/data/inputs/all/{name}

Get information about the `{name}` input source.

**GET**

List details for the `{name}` input.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>common</td>
<td>Boolean</td>
<td>Indicates whether to return only attributes common to all inputs. These common attributes are as follows.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• app</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• disabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• index</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• owner</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• source</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• sourcetype</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• title</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• updated</td>
</tr>
</tbody>
</table>

**Returned values**

The response lists attributes for the `{name}` input. See the following example for details.

**Example request and response**

**XML Request**

curl -u admin:pass https://localhost:8089/services/data/inputs/all/twitter

**XML Response**

...
<entry>
  <title>twitter</title>
  <id>https://localhost:8089/services/data/inputs/all/twitter</id>
  <updated>2012-07-11T08:03:17-07:00</updated>
  <link href="/services/data/inputs/all/twitter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/inputs/all/twitter" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="description">Get data from Twitter.</s:key>
      ... eai:acl nodes and eai:attribute nodes elided ...
      <s:key name="endpoint">
        <s:dict>
          <s:key name="args">
            <s:dict>
              <s:key name="data_type">string</s:key>
              <s:key name="description">Name of the current feed using the user credentials supplied.</s:key>
              <s:key name="order">0</s:key>
              <s:key name="title">Twitter feed name</s:key>
            </s:dict>
          </s:key>
          <s:key name="password">
            <s:dict>
              <s:key name="data_type">string</s:key>
              <s:key name="description">Your twitter password</s:key>
              <s:key name="order">2</s:key>
              <s:key name="required_on_create">1</s:key>
              <s:key name="required_on_edit">0</s:key>
              <s:key name="title">Password</s:key>
            </s:dict>
          </s:key>
          <s:key name="username">
            <s:dict>
              <s:key name="data_type">string</s:key>
              <s:key name="description">Your Twitter ID.</s:key>
              <s:key name="order">1</s:key>
              <s:key name="required_on_create">1</s:key>
              <s:key name="required_on_edit">0</s:key>
              <s:key name="title">Twitter ID/Handle</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="streaming_mode">simple</s:key>
      <s:key name="title">Twitter</s:key>
    </s:dict>
  </content>
</entry>
data/inputs/http

https://<host>:<mPort>/services/data/inputs/http

Access or update HTTP Event Collector global configuration tokens and application tokens.

See also

For more information, see details for the following associated endpoints.

- data/inputs/http/{name}
- data/inputs/http/{name}/enable
- data/inputs/http/{name}/disable
- collector/event

GET

Access global configuration information and a list of tokens

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

See data/inputs/http/{name} for app-level response data keys.

Example request and response

XML Request

`curl -u admin:pass https://localhost:8089/services/data/inputs/http`

XML Response

```
<title>http</title>
{id>https://localhost:8089/services/data/inputs/http</id>
<updated>2015-01-26T22:43:26-08:00</updated>
<generator build="250128" version="20150120"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/inputs/http/_new" rel="create"/>
<link href="/services/data/inputs/http/_reload" rel="_reload"/>
... opensearch elided ...
<s:messages/>
<entry>
  <title>http</title>
  <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http</id>
  <updated>2015-01-26T22:43:26-08:00</updated>
```
POST

Modify global configuration. Add and modify tokens.

Global request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>444</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Datatype</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>dedicatedIoThreads</td>
<td>Number</td>
<td>2</td>
<td>Number of threads used by HTTP Input server.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>1</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>enableSSL</td>
<td>Boolean</td>
<td>1</td>
<td>Enable SSL protocol for HTTP data input. 1 = SSL enabled, 0 = SSL disabled.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td></td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>indexes</td>
<td>String</td>
<td></td>
<td>Set of indexes allowed for events with this token.</td>
</tr>
<tr>
<td>maxSockets</td>
<td>Number</td>
<td>0</td>
<td>Maximum number of simultaneous HTTP connections accepted. Adjusting this value may cause server performance issues and is not generally recommended. Possible values for this setting vary by OS.</td>
</tr>
<tr>
<td>maxThreads</td>
<td>Number</td>
<td>0</td>
<td>Maximum number of threads that can be used by active HTTP transactions. Adjusting this value may cause server performance issues and is not generally recommended. Possible values for this setting vary by OS.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Token name (inputs.conf key)</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td>8088</td>
<td>HTTP data input IP port.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>Default sourcetype for events with this token.</td>
</tr>
<tr>
<td>useDeploymentServer</td>
<td>Boolean</td>
<td>0 (disabled)</td>
<td>Indicates whether the event collector input writes its configuration to a deployment server repository. When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as repositoryLocation in serverclass.conf. Copy the full contents of the splunk_httpinput app directory to this directory for the configuration to work. When enabled, only the tokens defined in the splunk_httpinput app in this repository are viewable and editable on the API and the Data Inputs page in Splunk Web. When disabled, the input writes its configuration to $SPLUNK_HOME/etc/apps by default. Defaults to 0 (disabled).</td>
</tr>
</tbody>
</table>

**Application-level request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>1</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td></td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>indexes</td>
<td>String</td>
<td></td>
<td>Set of indexes allowed for events with this token.</td>
</tr>
<tr>
<td>name required</td>
<td>String</td>
<td></td>
<td>Token name (inputs.conf key)</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Default source for events with this token.</td>
</tr>
<tr>
<td>Name</td>
<td>Datatype</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>sourcetype</code></td>
<td>String</td>
<td>Default</td>
<td>Default sourcetype for events with this token.</td>
</tr>
</tbody>
</table>

**Global returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>dedicatedIoThreads</code></td>
<td>Number of threads used by HTTP Input server.</td>
</tr>
<tr>
<td><code>disabled</code></td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td><code>enableSSL</code></td>
<td>Enable SSL protocol for HTTP data input. 1 = SSL enabled, 0 = SSL disabled.</td>
</tr>
<tr>
<td><code>host</code></td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td><code>index</code></td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td><code>indexes</code></td>
<td>Set of indexes allowed for events with this token.</td>
</tr>
<tr>
<td><code>port</code></td>
<td>HTTP data input IP port.</td>
</tr>
<tr>
<td><code>_rcvbuf</code></td>
<td>Socket receive buffer size (bytes).</td>
</tr>
<tr>
<td><code>source</code></td>
<td>Default source for events with this token.</td>
</tr>
<tr>
<td><code>sourcetype</code></td>
<td>Default sourcetype for events with this token.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>useDeploymentServer</code></td>
<td>Indicates whether the event collector input writes its configuration to a deployment server repository.</td>
</tr>
</tbody>
</table>

When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as `repositoryLocation` in `serverclass.conf`. Copy the full contents of the `splunk_httpinput` app directory to this directory for the configuration to work.

When enabled, only the tokens defined in the `splunk_httpinput` app in this repository are viewable and editable on the **API and the Data Inputs** page in Splunk Web.

When disabled, the input writes its configuration to `$SPLUNK_HOME/etc/apps` by default.

Defaults to 0 (disabled).
Application-level returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>_rcvbuf</td>
<td>Socket receive buffer size (bytes).</td>
</tr>
<tr>
<td>source</td>
<td>Source for events with this token.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Sourcetype for events with this token.</td>
</tr>
<tr>
<td>token</td>
<td>Token value for sending data to collector/event endpoint.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/http -d name=myapp
```

XML Response

```
...<title>http</title><id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id><updated>2015-01-30T12:45:28-08:00</updated><generator build="250128" version="20150120"/><author><name>Splunk</name></author><link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/><link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>... opensearch ...
<s:messages/>
<entry><title>http://myapp</title><id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp</id><updated>2015-01-30T12:45:28-08:00</updated><link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp" rel="alternate"/><author><name>nobody</name></author><link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp/_new" rel="create"/><link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp/_edit" rel="_edit"/><link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp/_reload" rel="_reload"/><link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp/disable" rel="disable"/>... eai:acl ...
<s:dict><s:key name="_rcvbuf">1572864</s:key><s:key name="disabled">0</s:key>... eai:acl ...
<s:key name="eai:appName">system</s:key><s:key name="eai:userName">nobody</s:key>
```
Manage the `{name}` HTTP Event Collector token. HTTP, as in `data/inputs/http/http`, indicates global configuration.

See also

For more information, see details for the following associated endpoints.

- `data/inputs/http`
- `data/inputs/http/{name}/enable`
- `data/inputs/http/{name}/disable`
- `collector/event`

DELETE

Delete a token.

Request parameters

None

Returned values

None

Example request and response

XML Request

```
curl -u admin:pass --request DELETE https://localhost:8089/servicesNS/nobody/search/data/inputs/http/http%3A%252F%252Fmyapp
```

XML Response

```
<title>http</title>
<id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
<updated>2015-01-30T13:03:18-08:00</updated>
<generator build="250128" version="20150120"/>
<author>
```
GET

Get token configuration details.

Request parameters
None

Global response data keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>Socket receive buffer size (bytes).</td>
</tr>
<tr>
<td>dedicatedIoThreads</td>
<td>Number of threads for HTTP event collector server.</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>enableSSL</td>
<td>SSL enablement status.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>port</td>
<td>HTTP data event collector IP port.</td>
</tr>
<tr>
<td>source</td>
<td>Source for events with this token.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Sourcetype for events with this token.</td>
</tr>
<tr>
<td>token</td>
<td>Token value for sending data to collector/event endpoint.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>useDeploymentServer</th>
<th>Indicates whether the event collector input writes its configuration to a deployment server repository.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as repositoryLocation in serverclass.conf.</td>
</tr>
<tr>
<td></td>
<td>Copy the full contents of the splunk_httpinput app directory to this directory for the configuration to work.</td>
</tr>
<tr>
<td></td>
<td>When enabled, only the tokens defined in the splunk_httpinput app in this repository are viewable and editable on the API and the Data Inputs page in Splunk Web.</td>
</tr>
<tr>
<td></td>
<td>When disabled, the input writes its configuration to $SPLUNK_HOME/etc/apps by default.</td>
</tr>
<tr>
<td></td>
<td>Defaults to 0 (disabled).</td>
</tr>
</tbody>
</table>

Application-level response data keys

449
**Name** | **Description**  
---|---  
_rcvbuf | Socket receive buffer size (bytes).  
disabled | Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.  
host | Host from which the indexer gets data.  
desc | Index to store generated events.  
source | Source for events with this token.  
sourcetype | Sourcetype for events with this token.  
token | Token value for sending data to collector/event endpoint.  

**Example request and response**

**XML Request**

```bash
curl -u admin:pass https://localhost:8089//servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/http/%252Fvar%252Flog
```

**XML Response**

```xml
...  
<id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/http/%252Fvar%252Flog</id>  
<updated>2015-01-26T23:01:34-08:00</updated>  
<generator build="250128" version="20150120"/>  
<author>  
  <name>Splunk</name>  
</author>  
<link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/>  
<link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>  
... opensearch elided ...  
<s:messages/>  
<entry>  
<title>http%22myapp"</title>  
<id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/http/%252Fvar%252Flog</id>  
<updated>2015-01-26T23:01:34-08:00</updated>  
<author>  
  <name>admin</name>  
</author>  
<link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="list"/>  
<link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/_reload" rel="_reload"/>  
<link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/_edit" rel="remove"/>  
<link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22/disable" rel="disable"/>  
<content type="text/xml">  
  <s:dict>  
    <s:key name="_rcvbuf">1572864</s:key>  
    <s:key name="disabled">0</s:key>  
    ... eai:acl elided ...  
  </s:dict>  
```

450
POST

Update token configuration information.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>1</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td></td>
<td>Default host.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td></td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>indexes</td>
<td>String</td>
<td></td>
<td>Set of indexes allowed for events with this token.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Required</td>
<td>Required. Token name (inputs.conf key)</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Default source for events with this token.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>Default sourcetype for events with this token.</td>
</tr>
<tr>
<td>useDeploymentServer</td>
<td>Boolean</td>
<td>0</td>
<td>Indicates whether the event collector input writes its configuration to a deployment server repository.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(disabled)</td>
<td>When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as repositoryLocation in serverclass.conf.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Copy the full contents of the splunk_httpinput app directory to this directory for the configuration to work.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>When enabled, only the tokens defined in the splunk_httpinput app in this repository are viewable and editable on the API and the Data Inputs page in Splunk Web.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>When disabled, the input writes its configuration to $SPLUNK_HOME/etc/apps by default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Defaults to 0 (disabled).</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>Socket receive buffer size (bytes).</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>source</td>
<td>Source for events with this token.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Sourcetype for events with this token.</td>
</tr>
<tr>
<td>token</td>
<td>Token value for sending data to collector/event endpoint.</td>
</tr>
<tr>
<td>useDeploymentServer</td>
<td>Indicates whether the event collector input writes its configuration to a deployment server repository. When this setting is set to 1 (enabled), the input writes its configuration to the directory specified as repositoryLocation in serverclass.conf. Copy the full contents of the splunk_httpinput app directory to this directory for the configuration to work. When enabled, only the tokens defined in the splunk_httpinput app in this repository are viewable and editable on the API and the Data Inputs page in Splunk Web. When disabled, the input writes its configuration to $SPLUNK_HOME/etc/apps by default. Defaults to 0 (disabled).</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/http%3A%252F%252Fmyapp -d recursive=false

**XML Response**

...<title>http</title>
<id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
<updated>2015-01-30T12:51:17-08:00</updated>
<generator build="250128" version="20150120"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/>
<link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>
... opensearch elided ...
<s:messages/>
<entry>
  <title>http://myapp</title>
  <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp</id>
  <updated>2015-01-30T12:51:17-08:00</updated>
  <link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp" rel="alternate"/>
data/inputs/http/{name}/disable

https://{host}:{mPort}/services/data/inputs/http/{name}/disable

Disable the `{name}` HTTP Event Collector token.

See also

- data/inputs/http
- data/inputs/http/{name}
- data/inputs/http/{name}/enable
- collector/event

POST

Disable the `{name}` HTTP Event Collector token.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>Socket receive buffer size (bytes).</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>source</td>
<td>Default source for events with this token.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Default sourcetype for events with this token.</td>
</tr>
<tr>
<td>token</td>
<td>Token value for sending data to collector/event endpoint.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/http/http%3A%252F%252Fmyapp/disable

**XML Response**

```
<title>http</title>
{id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
<updated>2015-01-30T12:59:44-08:00</updated>
<generator build="250128" version="20150120"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/system/data/inputs/http/_new" rel="create"/>
<link href="/servicesNS/nobody/system/data/inputs/http/_reload" rel="_reload"/>
... opensearch elided ...
<s:messages/>
<entry>
  <title>http://myapp</title>
  <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp</id>
  <updated>2015-01-30T12:59:44-08:00</updated>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_enable" rel="_enable"/>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_disable" rel="_disable"/>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_remove" rel="_remove"/>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_edit" rel="_edit"/>
  <link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252Fmyapp/_list" rel="_list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="_rcvbuf">1572864</s:key>
      <s:key name="disabled">1</s:key>
      ... eai:acl elided ...
      <s:key name="eai:appName">system</s:key>
      <s:key name="eai:userName">nobody</s:key>
      <s:key name="host">$decideOnStartup</s:key>
      <s:key name="index">default</s:key>
      <s:key name="recursive">false</s:key>
      <s:key name="token">AABD8B82-2810-4BE8-823F-FE6C15ECB46E</s:key>
    </s:dict>
  </content>
</entry>
```
data/inputs/http/{name}/enable

https://<host>:<mPort>/services/data/inputs/http/{name}/enable
Enable the {name} HTTP Event Collector token.

The POST request to this endpoint reloads the HTTP Event Collector server, including when the server is already enabled and running.

See also

- data/inputs/http
- data/inputs/http/{name}
- data/inputs/http/{name}/disable
- collector/event

POST

Enable the {name} HTTP Event Collector token.

The POST request reloads the HTTP Event Collector server, including when the server is already enabled and running.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>Socket receive buffer size (bytes).</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>source</td>
<td>Default source for events with this token.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Default sourcetype for events with this token.</td>
</tr>
<tr>
<td>token</td>
<td>Token value for sending data to collector/event endpoint.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/http/http%252F%252Fmyapp/enable

XML Response
data/inputs/http/{name}/rotate

https://<host>:<mPort>/services/data/inputs/http/{name}/rotate

Regenerate the {name} token value.

**POST**

Regenerate the {name} token value.

**Request parameters**

None

**Returned values**

456
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>token</td>
<td>Regenerated token value.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/splunk_httpinput/data(inputs/http/my_app_name/rotate )
-X post

**XML Response**

```xml
<?xml version="1.0" encoding="UTF-8"?>
<s:key name="token">64D47EC6-C510-4519-A520-EC4CAA157B97</s:key>
</feed>
```

**data/inputs/monitor**

https://<host>:<mPort>/services/data/inputs/monitor

Access monitor inputs.

**GET**

List enabled and disabled monitor inputs.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_TCP_ROUTING</td>
<td>List of TCP forwarding groups, as specified in outputs.conf.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if inputs monitoring is disabled.</td>
</tr>
<tr>
<td>filecount</td>
<td>Number of files monitored.</td>
</tr>
<tr>
<td>host</td>
<td>Name of the Splunk host for which inputs are monitored.</td>
</tr>
<tr>
<td>index</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Source type being monitored.</td>
</tr>
<tr>
<td></td>
<td>The source type of an event is the format of the data input from which it originates, such as access_combined or cisco_syslog. The source type determines how Splunk software formats your data.</td>
</tr>
</tbody>
</table>

**Example request and response**

457
XML Request

curl -u admin:pass https://localhost:8089/services/data/inputs/monitor

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>monitor</title>
  <id>https://localhost:8089/services/data/inputs/monitor</id>
  <updated>2011-07-10T14:25:53-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/monitor/_new" rel="create"/>
  <link href="/services/data/inputs/monitor/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>$SPLUNK_HOME/etc/splunk.version</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version</id>
    <updated>2011-07-10T14:25:53-07:00</updated>
    <link href="/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version" rel="list"/>
    <link href="/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/inputs/monitor/%24SPLUNK_HOME%252Fetc%252Fsplunk.version/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_TCP_ROUTING">*</s:key>
        <s:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="filecount">1</s:key>
        <s:key name="host">MrT</s:key>
        <s:key name="index">_internal</s:key>
        <s:key name="sourcetype">splunk_version</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
POST

Create a new file or directory monitor input.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blacklist</td>
<td>String</td>
<td>Specify a regular expression for a file path. The file path that matches this regular expression is not indexed.</td>
</tr>
<tr>
<td>check-index</td>
<td>Boolean</td>
<td>If set to true, the index value is checked to ensure that it is the name of a valid index.</td>
</tr>
<tr>
<td>check-path</td>
<td>Boolean</td>
<td>If set to true, the name value is checked to ensure that it exists.</td>
</tr>
<tr>
<td>crc-salt</td>
<td>String</td>
<td>A string that modifies the file tracking identity for files in this input. The magic value &lt;SOURCE&gt; invokes special behavior (see admin documentation).</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>Indicates if input monitoring is disabled.</td>
</tr>
<tr>
<td>followTail</td>
<td>Boolean</td>
<td>If set to true, files that are seen for the first time is read from the end.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>The value to populate in the host field for events from this data input.</td>
</tr>
<tr>
<td>host_regex</td>
<td>String</td>
<td>Specify a regular expression for a file path. If the path for a file matches this regular expression, the captured value is used to populate the host field for events from this data input. The regular expression must have one capture group.</td>
</tr>
<tr>
<td>host_segment</td>
<td>Number</td>
<td>Use the specified slash-separate segment of the filepath as the host field value.</td>
</tr>
<tr>
<td>ignore-older-than</td>
<td>String</td>
<td>Specify a time value. If the modification time of a file being monitored falls outside of this rolling time window, the file is no longer being monitored.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>Which index events from this input should be stored in. Defaults to default.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Required. The file or directory path to monitor on the system.</td>
</tr>
<tr>
<td>recursive</td>
<td>Boolean</td>
<td>Setting this to false prevents monitoring of any subdirectories encountered within this data input.</td>
</tr>
<tr>
<td>rename-source</td>
<td>String</td>
<td>The value to populate in the source field for events from this data input. The same source should not be used for multiple data inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td>The value to populate in the sourcetype field for incoming events.</td>
</tr>
<tr>
<td>time-before-close</td>
<td>Number</td>
<td>When Splunk software reaches the end of a file that is being read, the file is kept open for a minimum of the number of seconds specified in this value. After this period has elapsed, the file is checked again for more data.</td>
</tr>
<tr>
<td>whitelist</td>
<td>String</td>
<td>Specify a regular expression for a file path. Only file paths that match this regular expression are indexed.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor -d name=/var/log

**XML Response**

459
data/inputs/monitor/{name}

https://<host>:<mPort>/services/data/inputs/monitor/{name}

Manage the {name} monitor input.

DELETE

Disable the named monitor data input and remove it from the configuration.

Request parameters

None

Returned values

None

Example request and response

XML Request

curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
  xmlns:s="http://dev.splunk.com/ns/rest">
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
  <updated>2011-07-10T14:27:57-07:00</updated>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
GET

List the properties of a single monitor data input.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Indicates if inputs monitoring is disabled.</td>
</tr>
<tr>
<td>filecount</td>
<td>Number of files being monitored.</td>
</tr>
<tr>
<td>host</td>
<td>Name of the Splunk host for which inputs are monitored.</td>
</tr>
<tr>
<td>index</td>
<td>The index events from this input should be stored in.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>monitor</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
  <updated>2011-07-10T14:33:54-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/monitor/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>/var/log/title</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog</id>
POST

Update properties of the named monitor input.

Request parameters

462
<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blacklist</td>
<td>String</td>
<td>Specify a regular expression for a file path. The file path that matches this regular expression is not indexed.</td>
</tr>
<tr>
<td>check-index</td>
<td>Boolean</td>
<td>If set to true, the &quot;index&quot; value is checked to ensure that it is the name of a valid index.</td>
</tr>
<tr>
<td>check-path</td>
<td>Boolean</td>
<td>If set to true, the &quot;name&quot; value is checked to ensure that it exists.</td>
</tr>
<tr>
<td>crc-salt</td>
<td>String</td>
<td>A string that modifies the file tracking identity for files in this input. The magic value &quot;&lt;SOURCE&gt;&quot; invokes special behavior (see admin documentation).</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>Indicates if input monitoring is disabled.</td>
</tr>
<tr>
<td>followTail</td>
<td>Boolean</td>
<td>If set to true, files that are seen for the first time is read from the end.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>The value to populate in the host field for events from this data input.</td>
</tr>
<tr>
<td>host_regex</td>
<td>String</td>
<td>Specify a regular expression for a file path. If the path for a file matches this regular expression, the captured value is used to populate the host field for events from this data input. The regular expression must have one capture group.</td>
</tr>
<tr>
<td>host_segment</td>
<td>Number</td>
<td>Use the specified slash-separate segment of the filepath as the host field value.</td>
</tr>
<tr>
<td>ignore-older-than</td>
<td>String</td>
<td>Specify a time value. If the modification time of a file being monitored falls outside of this rolling time window, the file is no longer being monitored.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>Which index events from this input should be stored in. Defaults to default.</td>
</tr>
<tr>
<td>recursive</td>
<td>Boolean</td>
<td>Setting this to &quot;false&quot; prevents monitoring of any subdirectories encountered within this data input.</td>
</tr>
<tr>
<td>rename-source</td>
<td>String</td>
<td>The value to populate in the source field for events from this data input. The same source should not be used for multiple data inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td>The value to populate in the sourcetype field for incoming events.</td>
</tr>
<tr>
<td>time-before-close</td>
<td>Number</td>
<td>When Splunk software reaches the end of a file that is being read, the file is kept open for a minimum of the number of seconds specified in this value. After this period has elapsed, the file is checked again for more data.</td>
</tr>
<tr>
<td>whitelist</td>
<td>String</td>
<td>Specify a regular expression for a file path. Only file paths that match this regular expression are indexed.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog -d recursive=false

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">  
  <title>monitor</title>  
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>  
  <updated>2011-07-10T14:35:28-07:00</updated>  
</feed>
data/inputs/monitor/{name}/members

https://<host>:<mPort>/services/data/inputs/monitor/{name}/members

List {name} monitor input files.

GET

List all files monitored under the named monitor input.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
The response includes a list of monitored files. See the following example for more details.

Example request and response

XML Request

curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog/members

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
     <title>monitor</title>
     <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
     <updated>2011-07-10T14:34:28-07:00</updated>
     <generator version="102807"/>
     <author>
         <name>Splunk</name>
     </author>
     <link href="/servicesNS/nobody/search/data/inputs/monitor/_new" rel="create"/>
     <link href="/servicesNS/nobody/search/data/inputs/monitor/_reload" rel="_reload"/>
     ... opensearch nodes elided ...
     <s:messages/>
     <entry>
     
<entry>
data/inputs/oneshot

https://<host>:<mPort>/services/data/inputs/oneshot

Access oneshot inputs in progress or queue a file for immediate indexing.

GET

Access oneshot inputs in progress.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes Indexed</td>
<td>Total number of bytes read and sent to the pipeline for indexing during a oneshot input. This total includes the uncompressed byte count from a source file that is compressed on disk.</td>
</tr>
<tr>
<td>Offset</td>
<td>Current position in the source file, indicating how much of the file is read. For compressed source files, this offset represents the position in the compressed format. You can obtain the percentage of a source file read by calculating offset/size.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the source file, in bytes. You can obtain the percentage of a source file read by calculating offset/size.</td>
</tr>
<tr>
<td>Sources Indexed</td>
<td>Indicates the number of sources read from a file in a compressed format such as tar or zip. A value of 0 indicates the source file was not compressed.</td>
</tr>
<tr>
<td>Spool Time</td>
<td>Time that the request was made to read the source file.</td>
</tr>
</tbody>
</table>
Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/services/data/inputs/oneshot

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>oneshotinput</title>
  <id>https://localhost:8089/services/data/inputs/oneshot</id>
  <updated>2011-07-08T01:48:04-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/oneshot/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>/var/log/distccd.log</title>
    <id>https://localhost:8089/services/data/inputs/oneshot/%252Fvar%252Flog%252Fdistccd.log</id>
    <updated>2011-07-08T01:48:04-07:00</updated>
    <link href="/services/data/inputs/oneshot/%252Fvar%252Flog%252Fdistccd.log" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/data/inputs/oneshot/%252Fvar%252Flog%252Fdistccd.log" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Bytes Indexed">7200768</s:key>
        <s:key name="Offset">7200768</s:key>
        <s:key name="Size">449630160</s:key>
        <s:key name="Sources Indexed">0</s:key>
        <s:key name="Spool Time">Fri Jul  8 01:47:53 PDT 2011</s:key>
        ... eai:acl node elided ...
      </s:dict>
    </content>
  </entry>
</feed>
```

**POST**

Queue a file for immediate indexing.

**Usage details**
The file being queued must be locally accessible from the server. This endpoint can handle any single file: plain, compressed or archive. The file is indexed in full, regardless of whether it is already indexed.

**Request parameters**
<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>String</td>
<td></td>
<td>The value of the <code>host</code> field to be applied to data from this file.</td>
</tr>
<tr>
<td>host_regex</td>
<td>String</td>
<td></td>
<td>A regex to be used to extract a <code>host</code> field from the path. If the path matches this regular expression, the captured value is used to populate the <code>host</code> field for events from this data input. The regular expression must have one capture group.</td>
</tr>
<tr>
<td>host_segment</td>
<td>Number</td>
<td></td>
<td>Use the specified slash-separate segment of the path as the <code>host</code> field value.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td></td>
<td>The destination index for data processed from this file.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Required</td>
<td>The path to the file to be indexed. The file must be locally accessible by the server.</td>
</tr>
<tr>
<td>rename-source</td>
<td>String</td>
<td></td>
<td>The value of the <code>source</code> field to be applied to data from this file.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>The value of the <code>sourcetype</code> field to be applied to data from this file.</td>
</tr>
</tbody>
</table>

**Returned values**
None

**Example request and response**

**XML Request**

curl -u admin:pass https://localhost:8089/services/data/inputs/oneshot -d name=/var/log/messages

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
  xmlns:s="http://dev.splunk.com/ns/rest">
  <title>oneshotinput</title>
  <id>https://localhost:8089/services/data/inputs/oneshot</id>
  <updated>2011-07-08T01:48:04-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/oneshot/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/oneshot/{name}

https://<host>:<mPort>/services/data/inputs/oneshot/{name}

Get information about the `{name}` one-shot input.
GET

Access information about the \(\text{name}\) in-progress oneshot input.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bytes Indexed</td>
<td>Total number of bytes read and sent to the pipeline for indexing during a oneshot input. This total includes the uncompressed byte count from a source file that is compressed on disk.</td>
</tr>
<tr>
<td>Offset</td>
<td>Current position in the source file, indicating how much of the file is read. For compressed source files, this offset represents the position in the compressed format. You can obtain the percentage of a source file read by calculating offset/size.</td>
</tr>
<tr>
<td>Size</td>
<td>Size of the source file, in bytes. You can obtain the percentage of a source file read by calculating offset/size.</td>
</tr>
<tr>
<td>Sources Indexed</td>
<td>Indicates the number of sources read from a file in a compressed format such as tar or zip. A value of 0 indicates the source file was not compressed.</td>
</tr>
<tr>
<td>Spool Time</td>
<td>Time that the request was made to read the source file.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -u admin:pass https://localhost:8089/services/data/inputs/oneshot/%252Fvar%252Flog%252Fmessages
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>oneshotinput</title>
  <id>https://localhost:8089/services/data/inputs/oneshot</id>
  <updated>2011-07-08T01:49:20-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```
data/inputs/registry

https://<host>:<mPort>/services/data/inputs/registry
Access the Windows registry monitoring input.

GET
Get current registry monitoring configuration details.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>baseline</td>
<td>Indicates whether or not Splunk software should get a baseline of Registry events when it starts. Defaults to false.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates whether this input is disabled.</td>
</tr>
<tr>
<td>hive</td>
<td>Regular expression for Registry hives that this input should monitor for Registry access.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>index</td>
<td>Specifies the index that this input should send the data to. If no value is present, defaults to the default index.</td>
</tr>
<tr>
<td>monitorSubnodes</td>
<td>Indicates whether to monitor all Registry hives beneath the specified hive.</td>
</tr>
<tr>
<td>proc</td>
<td>Regular expression for processes this input should monitor for Registry access. It matches against the process name which performed the Registry access. Events generated by processes that do not match the regular expression get filtered out. Events generated by processes that match the regular expression pass through.</td>
</tr>
<tr>
<td>type</td>
<td>A regular expression that specifies the types of Registry events to monitor.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -u admin:pass https://localhost:8089/services/data/inputs/registry
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-regmon</title>
  <id>https://10.1.5.157:8089/services/data/inputs/registry</id>
  <updated>2011-07-29T19:31:32-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/registry/_new" rel="create"/>
  <link href="/services/data/inputs/registry/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>Machine keys</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry/Machine%20keys</id>
    <updated>2011-07-29T19:31:32-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/registry/Machine%20keys" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/registry/Machine%20keys/_new" rel="create"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/Machine%20keys/_reload" rel="_reload"/>
    ... opensearch nodes elided ...
    <content type="text/xml">
```

470
POST

Creates new or modify existing registry monitoring settings.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>baseline</td>
<td>Boolean</td>
<td>Required</td>
<td>Indicate whether to establish a baseline value for the registry keys. Use 1 to establish the baseline, 0 for no baseline.</td>
</tr>
<tr>
<td>hive</td>
<td>String</td>
<td>Required</td>
<td>Specify the registry hive for monitoring changes.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Required</td>
<td>Name of the configuration stanza.</td>
</tr>
<tr>
<td>proc</td>
<td>String</td>
<td>Required</td>
<td>Specify a regex for collecting changes if a process name matches the regex.</td>
</tr>
<tr>
<td>type</td>
<td>String</td>
<td>Required</td>
<td>List registry event types that you want to monitor. Separate each type with a pipe ('</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether the monitoring is disabled.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>monitorSubnodes</td>
<td>Boolean</td>
<td>True</td>
<td>Indicates whether to monitor all registry hives beneath the specified hive.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/registry -d baseline=1 -d
hive="HKU\.*" -d name=mykeys -d proc="c:\.*" -d type="set|create|delete|rename"

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-regmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry</id>
  <updated>2011-07-29T19:29:18-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

**data/inputs/registry/{name}**

https://<host>:<mPort>/services/data/inputs/registry/{name}

Manage registry monitoring {name} stanza.

**DELETE**

Delete a registry monitoring configuration stanza.

**Request parameters**

None

**Returned values**

None

**Example request and response**

**XML Request**

```bash
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/registry/mykeys
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  ... XML content elided ...
</feed>
```
GET

Gets current registry monitoring configuration stanza

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>baseline</td>
<td>Indicates whether to get a baseline of Registry events when Splunk software starts.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td>hive</td>
<td>Regular expression for Registry hives that this input should monitor for Registry access. Matches against the Registry key which was accessed. Events that contain hives that do not match the regular expression get filtered out. Events that contain hives that match the regular expression pass through.</td>
</tr>
<tr>
<td>index</td>
<td>Specifies the index that this input should send the data to. If no value is present, defaults to the default index.</td>
</tr>
<tr>
<td>monitorSubnodes</td>
<td>Indicates whether to monitor all Registry hives beneath the specified hive.</td>
</tr>
<tr>
<td>proc</td>
<td>Regular expression for processes this input should monitor for Registry access. It matches against the process name which performed the Registry access. Events generated by processes that do not match the regular expression get filtered out. Events generated by processes that match the regular expression pass through.</td>
</tr>
<tr>
<td>type</td>
<td>Regular expression that specifies the types of Registry events to monitor.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/registry/mykeys
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-regmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry</id>
  <updated>2011-07-29T19:33:21-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/registry/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>mykeys</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry/mykeys</id>
    <updated>2011-07-29T19:33:21-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="baseline">1</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>disabled</s:item>
                <s:item>index</s:item>
                <s:item>monitorSubnodes</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>baseline</s:item>
                <s:item>hive</s:item>
                <s:item>proc</s:item>
                <s:item>type</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="hive">HKU</s:key>
        <s:key name="index">default</s:key>
        <s:key name="monitorSubnodes">1</s:key>
        <s:key name="proc">c:\.*</s:key>
        <s:key name="type">474
      </s:dict>
    </content>
  </entry>
</feed>
POST

Modify the named registry monitoring stanza.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>baseline</td>
<td>Number</td>
<td></td>
<td>Required. Specifies whether or not to establish a baseline value for the registry keys. 1 means yes, 0 no.</td>
</tr>
<tr>
<td>hive</td>
<td>String</td>
<td></td>
<td>Required. Specifies the registry hive under which to monitor for changes.</td>
</tr>
<tr>
<td>proc</td>
<td>String</td>
<td></td>
<td>Required. Specifies a regex. If specified, collect changes if a process name matches that regex.</td>
</tr>
<tr>
<td>type</td>
<td>String</td>
<td></td>
<td>Required. A list of registry events types that you want to monitor. Separate each type with a pipe ('</td>
</tr>
<tr>
<td>disabled</td>
<td>Number</td>
<td></td>
<td>Indicates whether the monitoring is disabled.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>monitorSubnodes</td>
<td>Boolean</td>
<td>True</td>
<td>Indicates whether to monitor all Registry hives beneath the specified hive.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/registry/mykeys -d baseline=1 -d hive="HKU\.*" -d proc="c:\.*" -d type="set|create"

XML Response
data/inputs/script

https://<host>:<mPort>/services/data/inputs/script

Access scripted inputs.

GET

Get the configuration settings for scripted inputs.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Specifies whether the input script is disabled.</td>
</tr>
<tr>
<td>endtime</td>
<td>If available, the time when the script stopped executing.</td>
</tr>
<tr>
<td>group</td>
<td>The name of the inputstatus group, which is always &quot;exec commands.&quot;</td>
</tr>
<tr>
<td>host</td>
<td>Host with which these data are identified.</td>
</tr>
<tr>
<td>index</td>
<td>Sets the index for events from this input. Defaults to the main index.</td>
</tr>
<tr>
<td>interval</td>
<td>An integer or cron schedule.</td>
</tr>
<tr>
<td></td>
<td>Specifies how often to execute the specified script, in seconds or a valid cron schedule. For a cron schedule, the script is not executed on start-up.</td>
</tr>
<tr>
<td>source</td>
<td>The source key/field for events from this input. Defaults to the input file path.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Sets the source key initial value. The key is used during parsing/indexing, in particular to set the source field during indexing. It is also the source field used at search time. As a convenience, the chosen string is prepended with 'source::'.</td>
</tr>
</tbody>
</table>
Sets the sourcetype key/field for events from this input. If unset, Splunk software picks a source type based on various aspects of the data. There is no hard-coded default.

For more information, see the documentation for the sourcetype parameter for the POST operation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>starttime</td>
<td>If available, the time when the script was executed.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/services/data/inputs/script

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>script</title>
  <id>https://localhost:8089/services/data/inputs/script</id>
  <updated>2011-07-09T20:16:11-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/script/_new" rel="create"/>
  <link href="/services/data/inputs/script/_reload" rel="_reload"/>
  <link href="/services/data/inputs/script/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>/Applications/splunk4.3/etc/apps/unix/bin/cpu.sh</title>
    <id>https://localhost:8089/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh</id>
    <updated>2011-07-09T20:16:11-07:00</updated>
    <link href="/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh/_edit" rel="edit"/>
    <link href="/servicesNS/nobody/unix/data/inputs/script/.%252Fbin%252Fcpu.sh/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:dict>
          <s:key name="_rcvbuf">1572864</s:key>
          <s:key name="disabled">0</s:key>
          ... eai:acl node elided ...
          <s:key name="endtime">Sat Jul  9 20:15:54 2011</s:key>
          <s:key name="group">exec commands</s:key>
          <s:key name="host">myhost.splunk.com</s:key>
          <s:key name="interval">30</s:key>
          <s:key name="source">cpu</s:key>
          <s:key name="sourcetype">cpu</s:key>
          <s:key name="starttime">Sat Jul  9 20:15:52 2011</s:key>
        </s:dict>
      </s:dict>
    </content>
  </entry>
</feed>
POST

Configure scripted input settings.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Specifies whether the input script is disabled.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td></td>
<td>Sets the host for events from this input. Defaults to whatever host sent the event.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>Sets the index for events from this input. Defaults to the main index.</td>
</tr>
<tr>
<td>interval</td>
<td>Number</td>
<td>60.0</td>
<td><strong>Required.</strong> Specify an integer or cron schedule. This parameter specifies how often to execute the specified script, in seconds or a valid cron schedule. If you specify a cron schedule, the script is not executed on start-up.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td><strong>Required.</strong> Specify the name of the scripted input.</td>
</tr>
<tr>
<td>passAuth</td>
<td>String</td>
<td></td>
<td>User to run the script as.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If you provide a username, Splunk software generates an auth token for that user and passes it to the script.</td>
</tr>
<tr>
<td>rename-source</td>
<td>String</td>
<td></td>
<td>Specify a new name for the source field for the script.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Sets the source key/field for events from this input. Defaults to the input file path.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sets the source key initial value. The key is used during parsing/indexing, in particular to set the source field during indexing. It is also the source field used at search time. As a convenience, the chosen string is prepended with 'source::'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> Overriding the source key is generally not recommended. Typically, the input layer provides a more accurate string to aid in problem analysis and investigation, accurately recording the file from which the data was retrieved. Consider use of source types, tagging, and search wildcards before overriding this value.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>Sets the sourcetype key/field for events from this input. If unset, Splunk software picks a source type based on various aspects of the data. As a convenience, the chosen string is prepended with 'sourcetype::'. There is no hard-coded default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sets the sourcetype key initial value. The key is used during parsing/indexing, in particular to set the source type field during indexing. It is also the source type field used at search time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Primarily used to explicitly declare the source type for this data, as opposed to allowing it to be determined using automated methods. This is typically important both for searchability and for applying the relevant configuration for this type of data during parsing and indexing.</td>
</tr>
</tbody>
</table>
Name | Datatype | Default | Description
--- | --- | --- | ---

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Returned values</td>
<td>None</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/script -d
name=/Applications/splunk4.3/etc/apps/myApp/bin/myScript.sh -d disabled=true -d interval=3600
```

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom"
 xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
 xmlns:s="http://dev.splunk.com/ns/rest">
 <title>script</title>
 <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script</id>
 <updated>2011-07-09T20:25:17-07:00</updated>
 <generator version="102824"/>
 <author>
  <name>Splunk</name>
 </author>
 <link href="/servicesNS/nobody/search/data/inputs/script/_new" rel="create"/>
 <link href="/servicesNS/nobody/search/data/inputs/script/_reload" rel="_reload"/>
 <link href="/servicesNS/nobody/search/data/inputs/script/restart" rel="restart"/>
 ... opensearch nodes elided ... 
 <s:messages/>
 </feed>
```

**data/inputs/script/restart**

https://<host>:<mPort>/services/data/inputs/script/restart

Allows for restarting scripted inputs.

**POST**

Causes a restart on a given scripted input.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>script</code></td>
<td>String</td>
<td></td>
<td><strong>Required.</strong> Path to the script to be restarted. This path must match an already-configured existing scripted input.</td>
</tr>
</tbody>
</table>

**Returned values**

None
Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/script/restart -d script=/Applications/splunk/bin/scripts/myScript.sh

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>script</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script</id>
  <updated>2011-07-09T20:38:38-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/script/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/inputs/script/restart" rel="restart"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

**data/inputs/script/\{name\}**

https://<host>:<mPort>/services/data/inputs/script/{name}

Manage the {name} scripted input.

**DELETE**

Removes the {name} scripted input.

**Request parameters**

None

**Returned values**

None

**Example request and response**

**XML Request**

curl -u admin:pass --request DELETE https://localhost:8089/servicesNS/nobody/search/data/inputs/script
GET

Returns the configuration settings for the {name} scripted input.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Specifies whether the input script is disabled.</td>
</tr>
<tr>
<td>group</td>
<td>The name of the inputstatus group, which is always &quot;exec commands.&quot;</td>
</tr>
<tr>
<td>host</td>
<td>Host these data are identified with.</td>
</tr>
<tr>
<td>index</td>
<td>Sets the index for events from this input. Defaults to the main index.</td>
</tr>
<tr>
<td>interval</td>
<td>An integer or cron schedule. Specifies how often to execute the specified script, in seconds or a valid cron schedule. For a cron schedule, the script is not executed on start-up.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/script/%252FApplications%252Fsplunk4.3%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh

XML Response

481
POST

Configures settings for the `{name}` scripted input.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Specifies whether the input script is disabled.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td></td>
<td>Sets the host for events from this input. Defaults to whatever host sent the event.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>Sets the index for events from this input. Defaults to the main index.</td>
</tr>
<tr>
<td>interval</td>
<td>Number</td>
<td>60.0</td>
<td>Specify an integer or cron schedule. This parameter specifies how often to execute the specified script, in seconds or a valid cron schedule. If you specify a cron schedule, the script is not executed on start-up.</td>
</tr>
<tr>
<td>passAuth</td>
<td>String</td>
<td></td>
<td>User to run the script as.</td>
</tr>
</tbody>
</table>

If you provide a username, Splunk software generates an auth token for that user and passes it to the script.

<table>
<thead>
<tr>
<th>rename-source</th>
<th>String</th>
<th></th>
<th>Specify a new name for the source field for the script.</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Sets the source key/field for events from this input. Defaults to the input file path.</td>
</tr>
</tbody>
</table>

Sets the source key initial value. The key is used during parsing/indexing, in particular to set the source field during indexing. It is also the source field used at search time. As a convenience, the chosen string is prepended with 'source::'.

Note: Overriding the source key is generally not recommended. Typically, the input layer provides a more accurate string to aid in problem analysis and investigation, accurately recording the file from which the data was retrieved. Consider use of source types, tagging, and search wildcards before overriding this value.

| sourcetype    | String   |         | Sets the sourcetype key/field for events from this input. If unset, Splunk software picks a source type based on various aspects of the data. As a convenience, the chosen string is prepended with 'sourcetype::'. There is no hard-coded default. |

Sets the sourcetype key initial value. The key is used during parsing/indexing, in particular to set the source type field during indexing. It is also the source type field used at search time.
Primarily used to explicitly declare the source type for this data, as opposed to allowing it to be determined using automated methods. This is typically important both for searchability and for applying the relevant configuration for this type of data during parsing and indexing.

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Primarily used to explicitly declare the source type for this data, as opposed to allowing it to be determined using automated methods. This is typically important both for searchability and for applying the relevant configuration for this type of data during parsing and indexing.</td>
</tr>
</tbody>
</table>

**Returned values**
None

**Example request and response**

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/script/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh -d interval=86400

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
   xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
   <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script</id>
   <updated>2011-07-09T20:27:59-07:00</updated>
   <generator version="102824"/>
   <author>
     <name>Splunk</name>
   </author>
   <link href="/servicesNS/nobody/search/data/inputs/script/_new" rel="create"/>
   <link href="/servicesNS/nobody/search/data/inputs/script/_reload" rel="_reload"/>
   <link href="/servicesNS/nobody/search/data/inputs/script/restart" rel="restart"/>
   ... opensearch nodes elided ...
   <s:messages/>
</feed>
```

data/inputs/tcp/cooked

https://<host>:<mPort>/services/data/inputs/tcp/cooked

Access cooked TCP input information and create new containers for managing cooked data.

**Usage details**
Forwarders can transmit three types of data: raw, unparsed, or parsed. "Cooked" data refers to parsed and unparsed formats.
GET

Access information about all cooked TCP inputs.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>group</td>
<td>Set to <code>listenerports</code> for listening ports.</td>
</tr>
<tr>
<td>host</td>
<td>The default value to fill in for events lacking a host value.</td>
</tr>
<tr>
<td>index</td>
<td>The index in which to store generated events.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/cooked

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>cooked</title>
  <id>https://localhost:8089/services/data/inputs/tcp/cooked</id>
  <updated>2011-07-10T14:50:50-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/services/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>9993</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9993</id>
    <updated>2011-07-10T14:50:50-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9993" rel="edit"/>
</entry>
</feed>
```
POST

Create a new container for managing cooked data.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>Boolean</td>
<td></td>
<td>If SSL is not already configured, error is returned</td>
</tr>
</tbody>
</table>
| connection_host | Enum    | dns     | Valid values: (ip | dns | none)  
|               |          |         | Set the host for the remote server that is sending data.                  |
|               |          |         | ip sets the host to the IP address of the remote server sending data.     |
|               |          |         | dns sets the host to the reverse DNS entry for the IP address of the      |
|               |          |         | remote server sending data.                                              |
|               |          |         | none leaves the host as specified in inputs.conf, which is typically      |
|               |          |         | the Splunk system hostname.                                              |
| disabled      | Boolean  |         | Indicates whether the input is disabled.                                  |
| host          | String   |         | The default value to fill in for events lacking a host value.             |
| name          | Number   |         | Required. The port number of this input.                                 |
| queue         | "parsingQueue" | "parsingQueue" | Specifies where the input processor should deposit the events it reads. |
| restrictToHost | String   |         | Restrict incoming connections on this port to the host specified here.   |

Returned values
None
Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/datainputs/tcp/cooked -d name=9998

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>cooked</title>
  <id>https://localhost:8089/servicesNS/nobody/search/datainputs/tcp/cooked</id>
  <updated>2011-07-10T14:52:33-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/datainputs/tcp/cooked/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/datainputs/tcp/cooked/_reload" rel="_reload"/>
  ...
  <s:messages/>
</feed>

**data/inputs/tcp/cooked/{name}**

https://<host>:<mPort>/services/datainputs/tcp/cooked/{name}

Manage cooked TCP inputs for the {name} host or port.

**DELETE**

Remove the cooked TCP inputs for port or host:port specified by {name}.

**Request parameters**

None

**Returned values**

None

**Example request and response**

XML Request

curl -u admin:pass --request DELETE
GET

Access information for the \{name\} cooked TCP input.

Usage details
If port is restricted to a host, \{name\} should be a URI-encoded host:port.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>group</td>
<td>Set to listenerports for listening ports.</td>
</tr>
<tr>
<td>host</td>
<td>The default value to fill in for events lacking a host value.</td>
</tr>
<tr>
<td>index</td>
<td>The index in which to store generated events.</td>
</tr>
<tr>
<td>restrictToHost</td>
<td>Restrict incoming connections on this port to the specified host.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9998

488
POST

Update the container for managing cooked data.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>Boolean</td>
<td></td>
<td>If SSL is not already configured, error is returned</td>
</tr>
<tr>
<td>connection_host</td>
<td>Enum</td>
<td>ip</td>
<td>Valid values: (ip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Set the host for the remote server that is sending data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ip sets the host to the IP address of the remote server sending data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>dns sets the host to the reverse DNS entry for the IP address of the remote server sending data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>none leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether the input is disabled.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td></td>
<td>The default value to fill in for events lacking a host value.</td>
</tr>
<tr>
<td>restrictToHost</td>
<td>String</td>
<td></td>
<td>Restrict incoming connections on this port to the host specified here.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9998 -d restrictToHost=tiny
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      ...>
  ...</feed>
```
data/inputs/tcp/cooked/{name}/connections

https://<host>:<mPort>/services/data/inputs/tcp/cooked/{name}/connections

Get active connections to the {name} port.

GET

List active connections to the {name} port.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection</td>
<td>Identifies the connection to port.</td>
</tr>
<tr>
<td>servername</td>
<td>Server name of forwarder connecting to this port.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9998/connections
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest">
  ...
</feed>
```
data/inputs/tcp/raw

https://<host>:<mPort>/services/data/inputs/tcp/raw

Container for managing raw tcp inputs from forwarders.

Forwarders can transmit three types of data: raw, unparsed, or parsed. Cooked data refers to parsed and unparsed formats.

Authentication and authorization
The edit_tcp capability is required for this endpoint.

GET

Get information about all raw TCP inputs.
Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>group</td>
<td>Set to listenerports for listening ports.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>The index in which to store generated events.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/raw

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>raw</title>
  <id>https://localhost:8089/services/data/inputs/tcp/raw</id>
  <updated>2011-07-08T02:30:30-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/services/data/inputs/tcp/raw/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>44000</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44000</id>
    <updated>2011-07-08T02:30:30-07:00</updated>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000" rel="alternate"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/_edit" rel="_edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/_remove" rel="_remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/connections" rel="connections"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="_rcvbuf">1572864</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

493
POST

Create a new data input for accepting raw TCP data.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| connection_host| Enum     | dns     | Valid values: (ip | dns | none)  
Set the host for the remote server that is sending data.  
ip sets the host to the IP address of the remote server sending data.  
dns sets the host to the reverse DNS entry for the IP address of the remote server sending data.  
none leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.  
Default value is ip. |
| disabled      | Boolean  |         | Indicates whether the inputs are disabled.                                  |
| host          | String   |         | Host from which the indexer gets data.                                     |
| index         | String   | default | Index to store generated events.                                            |
| name required | String   |         | The input port which receives raw data.                                    |
| queue         | Enum     |         | Valid values: (parsingQueue | indexQueue)  
Specifies where the input processor should deposit the events it reads. Defaults to parsingQueue.  
Set queue to parsingQueue to apply props.conf and other parsing rules to your data. For more information about props.conf and rules for timestamping and linebreaking, refer to props.conf and the online documentation at "Monitor files and directories with inputs.conf"  
Set queue to indexQueue to send your data directly into the index. |

494
<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rawTcpDoneTimeout</td>
<td>Number</td>
<td></td>
<td>Specifies in seconds the timeout value for adding a Done-key. Default value is 10 seconds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If a connection over the port specified by <code>name</code> remains idle after receiving data for specified number of seconds, it adds a Done-key. This implies the last event is completely received.</td>
</tr>
<tr>
<td>restrictToHost</td>
<td>String</td>
<td></td>
<td>Allows for restricting this input to only accept data from the host specified here.</td>
</tr>
<tr>
<td>SSL</td>
<td>Boolean</td>
<td></td>
<td>Sets the source key/field for events from this input. Defaults to the input file path.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Sets the source key initial value. The key is used during parsing/indexing, in particular to set the source field during indexing. It is also the source field used at search time. As a convenience, the chosen string is prepended with 'source::'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: Overriding the source key is generally not recommended. Typically, the input layer provides a more accurate string to aid in problem analysis and investigation, accurately recording the file from which the data was retrieved. Consider use of source types, tagging, and search wildcards before overriding this value.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>Set the source type for events from this input.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;sourcetype=&quot; is automatically prepended to &lt;string&gt;. Defaults to audittrail (if signedaudit=true) or fschange (if signedaudit=false).</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw -d name=44343

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>raw</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw</id>
  <updated>2011-07-08T02:30:30-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_reload" rel="_reload"/>
</feed>
```
data/inputs/tcp/raw/{name}

https://<host>:<mPort>/services/data/inputs/tcp/raw/{name}
Manage raw inputs for the {name} host or port.

Authentication and authorization
The edit_tcp capability is additionally required for this endpoint.

DELETE

Remove the raw inputs for port or host:port specified by {name}

Request parameters
None

Returned values
None

Example request and response

XML Request
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44343

XML Response
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>raw</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw</id>
  <updated>2011-07-08T02:30:31-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
GET

Returns information about raw TCP input port (name).

If port is restricted to a host, name should be URI-encoded host:port.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>group</td>
<td>Set to listenerports for listening ports.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>restrictToHost</td>
<td>Restrict incoming connections on this port to the specified host.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44343

XML Response

<!-- XML content -->
POST

Updates the container for managing raw data.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>Boolean</td>
<td></td>
<td></td>
</tr>
<tr>
<td>connection_host</td>
<td>Enum</td>
<td>dns</td>
<td>Valid values: (ip</td>
</tr>
</tbody>
</table>
Set the host for the remote server that is sending data.

- ip sets the host to the IP address of the remote server sending data.
- dns sets the host to the reverse DNS entry for the IP address of the remote server sending data.
- none leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.

Default value is ip.

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether the inputs are disabled.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>default</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td></td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>queue</td>
<td>Enum</td>
<td></td>
<td>Specifies where the input processor should deposit the events it reads.</td>
</tr>
<tr>
<td>rawTcpDoneTimeout</td>
<td>Number</td>
<td></td>
<td>Specifies in seconds the timeout value for adding a Done-key.</td>
</tr>
<tr>
<td>restrictToHost</td>
<td>String</td>
<td></td>
<td>Allows for restricting this input to only accept data from the host specified here.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Sets the source key/field for events from this input. Defaults to the input file path.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>Set the source type for events from this input. &quot;sourcetype=&quot; is automatically prepended to &lt;string&gt;.</td>
</tr>
</tbody>
</table>

Note: Overriding the source key is generally not recommended. Typically, the input layer provides a more accurate string to aid in problem analysis and investigation, accurately recording the file from which the data was retrieved. Consider use of source types, tagging, and search wildcards before overriding this value.
Defaults to audittrail (if signedaudit=true) or fschange (if signedaudit=false).

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Defaults to audittrail (if signedaudit=true) or fschange (if signedaudit=false).</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44343 -d sourcetype=syslog

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>raw</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw</id>
  <updated>2011-07-08T02:30:30-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/_reload" rel="_reload"/>
  ... opensearch nodes elided ... 
  <s:messages/>
</feed>
```

**data/inputs/tcp/raw/{name}/connections**

https://<host>:{mPort}/services/data/inputs/tcp/raw/{name}/connections

Get active connections the `{name}` host or port.

**Authentication and authorization**

The `edit_tcp` capability is additionally required for this endpoint.

**GET**

View all connections to the named data input.

**Request parameters**

None
Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection</td>
<td>IP address and port of the source connecting to this TCP input port.</td>
</tr>
<tr>
<td>servername</td>
<td>DNS name of the source connecting to this TCP input port.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/raw/9998/connections

XML Response

...<title>raw</title>
:id>https://localhost:8089/services/data/inputs/tcp/raw</id>
:<updater>2011-07-13T16:33-07:00</updater>
:generator version="103477"/>
:author>
  :name>Splunk</name>
</author>
:link href="/services/data/inputs/tcp/raw/_new" rel="create"/>
:link href="/services/data/inputs/tcp/raw/_reload" rel="_reload"/>
... opensearch nodes elided ...  
:s:messages/>
</entry>
<title>Raw:9998:127.0.0.1</title>
:id>https://localhost:8089/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1</id>
:<updater>2011-07-13T14:33-07:00</updater>
:link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1" rel="alternate"/>
:author>
  :name>system</name>
</author>
:link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1" rel="list"/>
:link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1/_reload" rel="_reload"/>
:link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1/_edit"/>
:link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1" rel="remove"/>
<s:dict type="text/xml">
  :<s:key name="connection">9998:127.0.0.1</s:key>
  ... eai:acl node elided ...
  :<s:key name="servername"></s:key>
</s:dict>
</content>
</entry>
data/inputs/tcp/splunktcptoken

https://<host>:<mPort>/services/data/inputs/tcp/splunktcptoken
Manage receiver access using tokens.

Usage details
Get information on all receiver tokens or create a new token. To edit or delete an existing token, see data/inputs/tcp/splunktcptoken/{name}.

Note: Configure the forwarder with the same token as the receiver to ensure that the forwarder receives data.

Authentication and Authorization:
The edit_splunktcp_token capability is required for this endpoint.

GET
Return all configured tokens.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
Response data keys are returned for each receiver token.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>token</td>
<td>Token value.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -k -u admin:changeme https://localhost:8089/services/data/inputs/tcp/splunktcptoken
```

XML Response

```xml
<title>splunktcptoken</title>
<id>https://localhost:8089/services/data/inputs/tcp/splunktcptoken</id>
<updated>2015-09-16T09:31:52-07:00</updated>
<generator build="71e3b8d1908254f21434f97320ac5ad7e6bb1c16" version="20150910"/>
<author>
  <name>Splunk</name>
</author>
```

502
<entry>
<title>splunktcptoken://tok1</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1</id>
<updated>2015-09-16T09:31:52-07:00</updated>
</entry>
POST

Create a new token.

Request parameters

Pagination and filtering parameters can be used with this method.

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>None</td>
<td>Required. Name for the token to create.</td>
</tr>
<tr>
<td>token</td>
<td>String</td>
<td>None</td>
<td>Optional. Token value to use. If unspecified, a token is generated automatically.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>token</td>
<td>Token value.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:changeme https://localhost:8089/services/data/inputs/tcp/splunktcptoken -d "name=tok1" -d "token=99C91C9E-F92E-40AF-BCDC-1A6AD2DC7AEF"

**XML Response**

```xml
<title>splunktcptoken</title>
<id>https://localhost:8089/services/data/inputs/tcp/splunktcptoken</id>
<updated>2015-09-16T09:27:03-07:00</updated>
<generator build="71e3b8d1908254f21434f97320ac5ad7e6bb1c16" version="20150910"/>  
<author>  
  <name>Splunk</name>  
</author>  
<link href="/services/data/inputs/tcp/splunktcptoken/_new" rel="create"/>  
<link href="/services/data/inputs/tcp/splunktcptoken/_reload" rel="_reload"/>  
<link href="/services/data/inputs/tcp/splunktcptoken/_acl" rel="_acl"/>
```
data/inputs/tcp/splunktctoken/{name}

https://<host>:<mPort>/services/data/inputs/tcp/splunktctoken/{name}
Manage existing receiver tokens.

**Authentication and Authorization**
The `edit_splunktcp_token` capability is required for this endpoint.

**GET**
Access token information.

**Request parameters**
Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>token</td>
<td>Token value.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/splunktctoken
```

**XML Response**

```
...
<title>splunktctoken</title>
<id>https://localhost:8089/services/data/inputs/tcp/splunktctoken</id>
<updated>2015-09-16T09:28:22-07:00</updated>
<generator build="71e3b8d1908254f21434f97320ac5ad7e6bb1c16" version="20150910"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/inputs/tcp/splunktctoken/_new" rel="create"/>
```
POST

Update the \{name\} token.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>token</td>
<td>String</td>
<td>None</td>
<td>New token value.</td>
</tr>
</tbody>
</table>

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>token</td>
<td>Token value.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/data/inputs/tcp/splunktcptoken/tok1
XML Response

...  
<title>splunktcp:token://tok1</title>  
<id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/splunktcp:token/splunktcp:token%3A%252F%252Ftok1</id>  
<updated>2015-09-16T09:28:22-07:00</updated>  
<author>  
  <name>nobody</name>  
</author>  
<link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcp:token/splunktcp:token%3A%252F%252Ftok1" rel="alternate"/>  
<link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcp:token/splunktcp:token%3A%252F%252Ftok1" rel="list"/>  
<link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcp:token/splunktcp:token%3A%252F%252Ftok1/_reload" rel="_reload"/>  
<link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcp:token/splunktcp:token%3A%252F%252Ftok1/edit" rel="edit"/>  
<link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcp:token/splunktcp:token%3A%252F%252Ftok1/" rel="remove"/>  
<link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcp:token/splunktcp:token%3A%252F%252Ftok1/disable" rel="disable"/>  
<content type="text/xml">  
  <s:dict>  
    <s:key name="rcvbuf">1572864</s:key>  
    <s:key name="disabled">0</s:key>  
    <s:key name="eai:acl">  
      <s:dict>  
        <s:key name="app">search</s:key>  
        <s:key name="can_change_perms">1</s:key>  
        <s:key name="can_list">1</s:key>  
        <s:key name="can_share_app">1</s:key>  
        <s:key name="can_share_global">1</s:key>  
        <s:key name="can_share_user">0</s:key>  
        <s:key name="can_write">1</s:key>  
        <s:key name="modifiable">1</s:key>  
        <s:key name="owner">nobody</s:key>  
        <s:key name="perms">  
          <s:dict>  
            <s:key name="read">  
              <s:list>  
                <s:item>*</s:item>  
              </s:list>  
            </s:key>  
            <s:key name="write">  
              <s:list>  
                <s:item>*</s:item>  
              </s:list>  
            </s:key>  
            <s:key name="removable">1</s:key>  
            <s:key name="sharing">app</s:key>  
          </s:dict>  
        </s:key>  
      </s:dict>  
    </s:key>  
    <s:key name="eai:attributes">510</s:key>  
  </s:dict>  
</content>
DELETE

Delete the \{name\} token.

Request parameters
None.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>token</td>
<td>Token value.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -X "DELETE" -u admin:changeme https://localhost:8089/services/data/inputs/tcp/splunktcptoken/tok1

XML Response

<title>splunktcptoken</title>
<id>https://localhost:8089/services/data/inputs/tcp/splunktcptoken</id>
<updated>2015-09-16T09:34:51-07:00</updated>
<generator build="71e3b8d1908254f21434f97320ac5ad7e6bb1c16" version="20150910"/>
<author>
data/inputs/tcp/ssl

https://<host>:<mPort>/services/data/inputs/tcp/ssl
Provides access to the SSL configuration of a Splunk server.

GET
Get SSL configuration details. There is only one SSL configuration for all input ports.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Specifies list of acceptable ciphers to use in ssl.</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/ssl

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
xmlns:s="http://dev.splunk.com/ns/rest">
data/inputs/tcp/ssl/{name}

https://<host>:<mPort>/services/data/inputs/tcp/ssl/{name}

Access or update the SSL configuration for the {name} host.

GET

Returns the SSL configuration for the host {name}.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>513</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>_rcvbuf</td>
<td>[Deprecated]</td>
</tr>
<tr>
<td>cipherSuite</td>
<td>Specifies list of acceptable ciphers to use in ssl.</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/ssl/ssl

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>ssl</title>
  <id>https://localhost:8089/services/data/inputs/tcp/ssl</id>
  <updated>2011-07-12T15:04:41-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/ssl/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <link href="/servicesNS/nobody/system/data/inputs/tcp/ssl/_reload" rel="_reload"/>
    ... eai:acl node elided ...
    <s:dict>
      <s:key name="_rcvbuf">1572864</s:key>
      <s:key name="cipherSuite">ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM</s:key>
      <s:key name="disabled">1</s:key>
      ... eai:acl node elided ...
      <s:key name="host">ombroso-mbp15.splunk.com</s:key>
      <s:key name="index">default</s:key>
    </s:dict>
  </entry>
</feed>
```
POST

Configure SSL for the `{name}` host.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether the inputs are disabled.</td>
</tr>
<tr>
<td>password</td>
<td>String</td>
<td></td>
<td>Server certificate password, if any.</td>
</tr>
<tr>
<td>requireClientCert</td>
<td>Boolean</td>
<td></td>
<td>Determines whether a client must authenticate.</td>
</tr>
<tr>
<td>rootCA</td>
<td>String</td>
<td></td>
<td>Certificate authority list (root file)</td>
</tr>
<tr>
<td>serverCert</td>
<td>String</td>
<td></td>
<td>Full path to the server certificate.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

**XML Request**

```
curl -u admin:pass https://localhost:8089/services/data/inputs/tcp/ssl/ssl -d disabled=true
```

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>ssl</title>
  <id>https://localhost:8089/services/data/inputs/tcp/ssl</id>
  <updated>2011-07-12T15:05:42-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/tcp/ssl/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

data/inputs/udp

https://<host>:<mPort>/services/data/inputs/udp
Access or create UDP data inputs.

**GET**

List enabled and disabled UDP data inputs.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>Socket receive buffer size (bytes).</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td>group</td>
<td>Set to listenerports for listening ports.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -u admin:pass https://localhost:8089/services/data/inputs/udp
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/services/data/inputs/udp</id>
  <updated>2011-07-08T14:11:57-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/udp/_new" rel="create="/>
  <link href="/services/data/inputs/udp/_reload" rel="_reload">...
  <s:messages/>
  <entry>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44000</id>
    <updated>2011-07-08T14:11:57-07:00</updated>
```

516
POST

Create a new UDP data input.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| connection_host | Enum     | ip      | Valid values: (ip | dns | none)  
|               |          |         | Set the host for the remote server that is sending data.  
|               |          |         | ip sets the host to the IP address of the remote server sending data.  
|               |          |         | dns sets the host to the reverse DNS entry for the IP address of the remote server sending data.  
|               |          |         | none leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.  
|               |          |         | Default value is ip.  |
| disabled      | Boolean  |         | Indicates if the input is disabled. |
| host          | String   |         | The value to populate in the host field for incoming events.  
<p>|               |          |         | This is used during parsing/indexing, in particular to set the host field. It is also the host field used at search time. |
| index         | String   | default | Which index events from this input should be stored in. |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required</td>
<td>The UDP port that this input should listen on.</td>
</tr>
<tr>
<td>no_appending_timestamp</td>
<td>Boolean</td>
<td></td>
<td>If set to true, prevents Splunk software from prepending a timestamp and hostname to incoming events.</td>
</tr>
<tr>
<td>no_priority_stripping</td>
<td>Boolean</td>
<td></td>
<td>If set to true, Splunk software does not remove the priority field from incoming syslog events.</td>
</tr>
<tr>
<td>queue</td>
<td>String</td>
<td></td>
<td>Which queue events from this input should be sent to. Generally this does not need to be changed.</td>
</tr>
<tr>
<td>restrictToHost</td>
<td>String</td>
<td></td>
<td>Restrict incoming connections on this port to the host specified here. If this is not set, the value specified in inputs.conf is used.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>The value to populate in the source field for incoming events. The same source should not be used for multiple data inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>The value to populate in the sourcetype field for incoming events.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/udp -d name=44321

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
  <updated>2011-07-08T14:12:13-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

**data/inputs/udp/{name}**

https://<host>:<mPort>/services/data/inputs/udp/{name}
Manage the `{name}` UDP host or port.

**DELETE**

Disable the named UDP data input and remove it from the configuration.

**Request parameters**

None

**Returned values**

None

**Example request and response**

**XML Request**

```
curl -u admin:pass --request DELETE https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44321
```

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom"
   xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
   xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
  <updated>2011-07-08T14:12:53-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

**GET**

List the properties of a single UDP data input port or `host:port {name}`.

**Usage details**

If port is restricted to a host, `{name}` should be URI-encoded `host:port`.

**Request parameters**

None
Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>_rcvbuf</td>
<td>Socket receive buffer size (bytes).</td>
</tr>
<tr>
<td>disabled</td>
<td>Input disabled indicator: $0 = Input Not disabled, $1 = Input disabled.</td>
</tr>
<tr>
<td>group</td>
<td>Set to listenerports for listening ports.</td>
</tr>
<tr>
<td>host</td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store generated events.</td>
</tr>
</tbody>
</table>

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44321

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
  <updated>2011-07-08T14:12:27-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>44321</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44321</id>
    <updated>2011-07-08T14:12:27-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/_new" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/connections" rel="connections"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:dict name="_rcvbuf">1572864</s:dict>
        <s:dict name="disabled">0</s:dict>
        ... eai:acl node elided ...
        <s:dict name="eai:attributes">
          <s:dict name="optionalFields">
            <s:list>
              <s:item>connection_host</s:item>
              <s:item>host</s:item>
            </s:list>
          </s:dict>
        </s:dict>
      </s:dict>
    </content>
  </entry>
</feed>
```
POST

Edit properties of the named UDP data input.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connection_host</td>
<td>Enum</td>
<td>ip</td>
<td>Valid values: ( \text{ip} \mid \text{dns} \mid \text{none} )</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Set the host for the remote server that is sending data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>\text{ip} sets the host to the IP address of the remote server sending data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>\text{dns} sets the host to the reverse DNS entry for the IP address of the remote server sending data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>none leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value is ip.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td></td>
<td>The value to populate in the host field for incoming events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This is used during parsing/indexing, in particular to set the host field. It is also the host field used at search time.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>Which index events from this input should be stored in.</td>
</tr>
<tr>
<td>Name</td>
<td>Datatype</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>no_appending_timestamp</td>
<td>Boolean</td>
<td></td>
<td>If set to true, prevents Splunk software from prepending a timestamp and hostname to incoming events.</td>
</tr>
<tr>
<td>no_priority_stripping</td>
<td>Boolean</td>
<td></td>
<td>If set to true, Splunk software does not remove the priority field from incoming syslog events.</td>
</tr>
<tr>
<td>queue</td>
<td>String</td>
<td></td>
<td>Which queue events from this input should be sent to. Generally this does not need to be changed.</td>
</tr>
<tr>
<td>restrictToHost</td>
<td>String</td>
<td></td>
<td>Restrict incoming connections on this port to the host specified here. If this is not set, the value specified in [udp://&lt;remote server&gt;]:&lt;port&gt; in inputs.conf is used.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>The value to populate in the source field for incoming events. The same source should not be used for multiple data inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>The value to populate in the sourcetype field for incoming events.</td>
</tr>
</tbody>
</table>

**Returned values**
None

**Example request and response**

**XML Request**

```bash
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/44321 -d sourcetype=syslog
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>udp</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
  <updated>2011-07-08T14:12:47-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```
**data/inputs/udp/{name}/connections**

https://<host>:<mPort>/services/data/inputs/udp/{name}/connections

List connections to the `{name}` host or port.

**GET**

List connections to the `{name}` host or port.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Indicates whether the inputs are disabled.</td>
</tr>
<tr>
<td>group</td>
<td>Set to 'listenerports' for listening ports.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```sh
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/9998/connections
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:s="http://dev.splunk.com/ns/rest"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
    <title>udp</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp</id>
    <updated>2011-07-13T17:08:18-07:00</updated>
    <generator version="103477"/>
    <author>
        <name>Splunk</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/udp/_new" rel="create"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/_reload" rel="_reload"/>
    <opensearch:totalResults>1</opensearch:totalResults>
    <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
    <opensearch:startIndex>0</opensearch:startIndex>
    <s:messages/>
    <entry>
        <title>127.0.0.1</title>
        <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/udp/127.0.0.1</id>
        <updated>2011-07-13T17:08:18-07:00</updated>
        <link href="/servicesNS/nobody/search/data/inputs/udp/127.0.0.1" rel="alternate"/>
        <author>
            <name>system</name>
        </author>
        <link href="/servicesNS/nobody/search/data/inputs/udp/127.0.0.1" rel="list"/>
    </entry>
</feed>
```
data/inputs/win-event-log-collections

https://<host>:<mPort>/services/data/inputs/win-event-log-collections

Provides access to all configured event log collections.

GET

Retrieve a list of configured event log collections.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lookup_host</td>
<td>String</td>
<td></td>
<td>For internal use. Used by the UI when editing the initial host from which we gather event log data.</td>
</tr>
</tbody>
</table>

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td>hosts</td>
<td>Hosts you are monitoring.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store data. If not specified defaults to the default index.</td>
</tr>
<tr>
<td>logs</td>
<td>List of event log channels to monitor.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -u admin:pass https://localhost:8089/services/data/inputs/win-event-log-collections

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-event-log-collections</title>
  <id>https://10.1.5.157:8089/services/data/inputs/win-event-log-collections</id>
  <updated>2011-07-27T11:26:47-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/win-event-log-collections/_new" rel="create"/>
  <link href="/services/data/inputs/win-event-log-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>localhost</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost</id>
    <updated>2011-07-27T11:26:47-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="edit"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost/enable" rel="enable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="hosts">localhost</s:key>
        <s:key name="index">default</s:key>
        <s:key name="logs">
          <s:list>
            <s:item>Application</s:item>
            <s:item>ForwardedEvents</s:item>
            <s:item>HardwareEvents</s:item>
            <s:item>Internet Explorer</s:item>
            <s:item>Security</s:item>
            <s:item>Setup</s:item>
            <s:item>System</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
POST

Create or modify existing event log collection settings.

Usage details
You can configure both native and WMI collections with this endpoint.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>String</td>
<td></td>
<td>A comma-separated list of additional hosts to be used for monitoring. The first host should be specified with &quot;lookup_host&quot;, and the additional ones using this parameter.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>logs</td>
<td>String</td>
<td></td>
<td>List of event log names from which to gather data:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- WMI collection format (CSV) example: logs=Application%2CSystem%2CSetup%2CSecurity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- Native event log collection format example: logs=Application&amp;logs=System&amp;logs=Setup</td>
</tr>
<tr>
<td>lookup_host</td>
<td>String</td>
<td></td>
<td>Required. Host from which to monitor log events. To specify additional hosts to be monitored using WMI, use the &quot;hosts&quot; parameter.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Required. Collection name. This name appears in configuration file, as well as the source and the sourcetype of the indexed data. If the value is &quot;localhost&quot;, it uses native event log collection; otherwise, it uses WMI.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td>hosts</td>
<td>Monitored hosts.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store data.</td>
</tr>
<tr>
<td>logs</td>
<td>List of event log channels to monitor.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>Host from which to monitor log events.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the collection. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is &quot;localhost&quot;, it uses native event log collection; otherwise, it uses WMI</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections -d lookup_host=localhost -d name=mylogs -d logs=Application,System

XML Response

526
data/inputs/win-event-log-collections/{name}

https://<host>:<mPort>/services/data/inputs/win-event-log-collections/{name}

Manage the {name} Windows event log.
DELETE

Deletes an event log collection.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-event-log-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections</id>
  <updated>2011-07-27T13:45:24-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_reload" rel="_reload"/>
... opensearch nodes elided ...
  <s:messages/>
</feed>

GET

Gets event log collection configurations.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lookup_host</td>
<td>String</td>
<td></td>
<td>For internal use. Used by the UI when editing the initial host from which we gather event log data.</td>
</tr>
</tbody>
</table>
Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td>hosts</td>
<td>Monitored hosts.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store data. If not specified defaults to the default index.</td>
</tr>
<tr>
<td>logs</td>
<td>List of event log channels to monitor.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>Host from which to monitor log events.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the collection. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is localhost, it uses native event log collection; otherwise, it uses WMI.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -u admin:pass  
https://localhost:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom"  
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"  
xmlns:s="http://dev.splunk.com/ns/rest">  
<title>win-event-log-collections</title>  
<id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections</id>  
<updated>2011-07-27T12:00:38-07:00</updated>  
<generator version="103620"/>  
<author>  
  <name>Splunk</name>  
</author>  
<link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_new" rel="create"/>  
<link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_reload" rel="_reload"/>  
... opensearch nodes elided ...  
<opensearch:totalResults>1</opensearch:totalResults>  
<opensearch:startIndex>1</opensearch:startIndex>  
<opensearch:itemsPerPage>1</opensearch:itemsPerPage>  
<opensearch:resultsPerPage>1</opensearch:resultsPerPage>  
<opensearch:updatedGmt>2011-07-27T12:00:38-07:00</opensearch:updatedGmt>  
<opensearch:query></opensearch:query>  
<opensearch:searchUrl>/services/search/jsp/search ?q=win-event-log-collections</opensearch:searchUrl>  
<opensearch:facets></opensearch:facets>  
<opensearch:version>1.1</opensearch:version>  
<entry>  
<title>mylogs</title>  
<id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs</id>  
<updated>2011-07-27T12:00:38-07:00</updated>  
<link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs/_new" rel="create"/>  
<link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs/_edit" rel="edit"/>  
<link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs/_remove" rel="remove"/>  
<link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs/_reload" rel="_reload"/>  
<link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs/disable" rel="disable"/>  
</entry>  
</feed>
```
POST

Modify an existing event log collection.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hosts</td>
<td>String</td>
<td></td>
<td>A comma-separated list of additional hosts to be used for monitoring. The first host should be specified with &quot;lookup_host&quot;, and the additional ones using this parameter.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>logs</td>
<td>String</td>
<td></td>
<td>A comma-separated list of event log names to gather data from.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>String</td>
<td>Required</td>
<td>This is a host from which we monitor log events. To specify additional hosts to be monitored using WMI, use the &quot;hosts&quot; parameter.</td>
</tr>
</tbody>
</table>
## Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td>hosts</td>
<td>Monitored hosts.</td>
</tr>
<tr>
<td>index</td>
<td>Index to store data.</td>
</tr>
<tr>
<td>logs</td>
<td>List of event log channels to monitor.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>Host from which to monitor log events.</td>
</tr>
<tr>
<td>name</td>
<td>The name of the collection. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is localhost, it uses native event log collection; otherwise, it uses WMI.</td>
</tr>
</tbody>
</table>

## Example request and response

### XML Request

```bash
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs -d lookup_host=localhost -d logs=Application
```

### XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-event-log-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-event-log-collections</id>
  <updated>2011-07-27T13:43:46-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>localhost</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost</id>
    <updated>2011-07-27T13:43:46-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="list"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost" rel="edit"/>
    <content type="text/xml">
    </content>
  </entry>
</feed>
```
data/inputs/win-wmi-collections

https://<host>:<mPort>/services/data/inputs/win-wmi-collections

Access configured WMI collections.

GET

Access configured WMI collections.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>class</td>
<td>The WMI performance object class being monitored.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates whether the input is disabled.</td>
</tr>
<tr>
<td>fields</td>
<td>The WMI performance counters being monitored.</td>
</tr>
<tr>
<td>index</td>
<td>The index to which you are sending input data.</td>
</tr>
<tr>
<td>instances</td>
<td>Instances of the WMI performance counter.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>interval</td>
<td>The interval, in seconds, at which the WMI provider(s) are queried.</td>
</tr>
<tr>
<td>name</td>
<td>the name of the input.</td>
</tr>
<tr>
<td>server</td>
<td>The server you are monitoring.</td>
</tr>
<tr>
<td>wql</td>
<td>The actual WQL query for monitoring the performance object.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -u admin:pass https://localhost:8089/services/data/inputs/win-wmi-collections
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
    <title>win-wmi-collections</title>
    <id>https://10.1.5.157:8089/services/data/inputs/win-wmi-collections</id>
    <updated>2011-07-27T14:00:24-07:00</updated>
    <generator version="103620"/>
    <author>
        <name>Splunk</name>
    </author>
    <link href="/services/data/inputs/win-wmi-collections/_new" rel="create"/>
    <link href="/services/data/inputs/win-wmi-collections/_reload" rel="_reload"/>
    ... opensearch nodes elided ...  
    <s:messages/>
    <entry>
        <title>CPUTime</title>
        <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime</id>
        <updated>2011-07-27T14:00:24-07:00</updated>
        <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime" rel="alternate"/>
        <author>
            <name>nobody</name>
        </author>
        <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime/_reload" rel="_reload"/>
        <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime/edit" rel="edit"/>
        <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime/enable" rel="enable"/>
        <content type="text/xml">
        <s:dict>
            <s:key name="class">Win32_PerfFormattedData_PerfOS_Processor</s:key>
            <s:key name="disabled">1</s:key>
            ... eai:acl node elided ...  
            <s:keys name="fields">
                <s:list>
                    <s:item>PercentProcessorTime</s:item>
                    <s:item>PercentUserTime</s:item>
                </s:list>
            </s:keys>
            <s:key name="index">default</s:key>
            <s:keys name="instances">
                <s:list>
                    <s:item>_Total</s:item>
                    533
                </s:list>
            </s:keys>
        </s:dict>
    </entry>
</feed>
```
POST

Create or modify existing WMI collection settings.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>classes</td>
<td>String</td>
<td></td>
<td>Required. A valid WMI class name.</td>
</tr>
<tr>
<td>disabled</td>
<td>Number</td>
<td>0</td>
<td>Disables the given collection.</td>
</tr>
<tr>
<td>fields</td>
<td>String</td>
<td>1.*</td>
<td>Properties (fields) that you want to gather from the given class. Specify each property as a separate argument to the POST operation.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>instances</td>
<td>String</td>
<td>empty</td>
<td>Instances of a given class for which data is gathered. Specify each instance as a separate argument to the POST operation.</td>
</tr>
<tr>
<td>interval</td>
<td>Number</td>
<td></td>
<td>Required. The interval, in seconds, at which the WMI provider(s) is queried.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>String</td>
<td></td>
<td>Required. This is the server from which we is gathering WMI data. If you need to gather data from more than one machine, additional servers can be specified in the 'server' parameter.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Required. This is the name of the collection. This name appears in configuration file, as well as the source and the sourcetype of the indexed data.</td>
</tr>
<tr>
<td>server</td>
<td>String</td>
<td>localhost</td>
<td>A comma-separated list of additional servers that you want to gather data from. Use this if you need to gather from more than a single machine. See also lookup_host.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>classes</td>
<td>A valid WMI class name.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td>fields</td>
<td>Properties (fields) that you want to gather from the given class.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>index</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>instances</td>
<td>Instances of a given class for which data is gathered.</td>
</tr>
<tr>
<td>interval</td>
<td>The interval, in seconds, at which the WMI provider(s) is queried.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>Host from which to monitor log events.</td>
</tr>
<tr>
<td>server</td>
<td>Servers from which to gather data. Used if you need to gather from more than a single machine. See also lookup_host.</td>
</tr>
<tr>
<td>wql</td>
<td>The actual WQL query for monitoring the performance object.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections -d classes=Win32_PerfFormattedData_PerfOS_Processor -d interval=5 -d lookup_host=localhost -d name=cpu

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-wmi-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections</id>
  <updated>2011-07-27T14:05:43-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>CPUTime</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime</id>
    <updated>2011-07-27T14:05:43-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime" rel="alternate"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime/_edit" rel="edit"/>
    <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime/_reload" rel="_reload"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">1</s:key>
        ... eai:acl node elided ...
        <s:key name="index">default</s:key>
        <s:key name="interval">3</s:key>
        <s:key name="wql">SELECT PercentProcessorTime,PercentUserTime FROM Win32_PerfFormattedData_PerfOS_Processor WHERE Name="_Total"</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
data/inputs/win-wmi-collections/{name}

https://<host>:<mPort>/services/data/inputs/win-wmi-collections/{name}

Manage the {name} WMI collection.

Method summary

<table>
<thead>
<tr>
<th>Method</th>
<th>Description</th>
<th>Formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>DELETE</td>
<td>Deletes a given collection.</td>
<td>XML, JSON</td>
</tr>
<tr>
<td>GET</td>
<td>Gets information about a single collection.</td>
<td>XML, JSON</td>
</tr>
<tr>
<td>POST</td>
<td>Modifies a given WMI collection.</td>
<td>XML, JSON</td>
</tr>
</tbody>
</table>

DELETE

Delete a given collection.

Usage details
The method returns HTTP status code = 400, if {name} does not exist.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -u admin:pass --request DELETE https://localhost:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-wmi-collections</title>
</feed>
GET

Get information about a single collection.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>classes</td>
<td>A valid WMI class name.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td>fields</td>
<td>Properties (fields) that you want to gather from the given class.</td>
</tr>
<tr>
<td>index</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>instances</td>
<td>Instances of a given class for which data is gathered.</td>
</tr>
<tr>
<td>interval</td>
<td>The interval, in seconds, at which the WMI provider(s) is queried.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>Host from which to monitor log events.</td>
</tr>
<tr>
<td>name</td>
<td>Collection name. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is localhost, it uses native event log collection; otherwise, it uses WMI.</td>
</tr>
<tr>
<td>server</td>
<td>Servers from which to gather data from. Used if you need to gather from more than a single machine. See also lookup_host.</td>
</tr>
<tr>
<td>wql</td>
<td>The actual WQL query for monitoring the performance object.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu

XML Response

<?xml version="1.0" encoding="UTF-8"?>
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"/>
<s:dict>
<s:key name="classes">Win32_PerfFormattedData_PerfOS_Processor</s:key>
<s:key name="disabled">0</s:key>
<s:dict name="eai:attributes">
<s:list name="optionalFields">
<s:item>disabled</s:item>
<s:item>fields</s:item>
<s:item>index</s:item>
<s:item>instances</s:item>
<s:item>server</s:item>
</s:list>
<s:list name="requiredFields">
<s:item>classes</s:item>
<s:item>interval</s:item>
<s:item>lookup_host</s:item>
</s:list>
</s:dict>
<s:dict name="wildcardFields">
</s:dict>
<s:dict name="fields">
<s:list>
<s:item>*</s:item>
</s:list>
</s:dict>
<s:key name="index">default</s:key>
<s:dict name="instances">
</s:dict>
</entry>
POST

Modify a collection.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>classes</td>
<td>String</td>
<td></td>
<td>Required. A valid WMI class name.</td>
</tr>
<tr>
<td>disabled</td>
<td>Number</td>
<td></td>
<td>Disables the given collection.</td>
</tr>
<tr>
<td>fields</td>
<td>String</td>
<td></td>
<td>Properties (fields) that you want to gather from the given class.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specify each property as a separate argument to the POST operation.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td></td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>instances</td>
<td>String</td>
<td></td>
<td>Instances of a given class for which data is gathered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specify each instance as a separate argument to the POST operation.</td>
</tr>
<tr>
<td>interval</td>
<td>Number</td>
<td></td>
<td>Required. The interval, in seconds, at which the WMI provider(s) is queried.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>String</td>
<td></td>
<td>Required. This is the server from which we is gathering WMI data. If you need to gather data from more than one machine, additional servers can be specified in the 'server' parameter.</td>
</tr>
<tr>
<td>server</td>
<td>String</td>
<td></td>
<td>A comma-separated list of additional servers that you want to gather data from. Use this if you need to gather from more than a single machine. See also lookup_host parameter.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>classes</td>
<td>A valid WMI class name.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td>fields</td>
<td>Properties (fields) that you want to gather from the given class.</td>
</tr>
<tr>
<td>index</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>instances</td>
<td>Instances of a given class for which data is gathered.</td>
</tr>
<tr>
<td>interval</td>
<td>The interval, in seconds, at which the WMI provider(s) are queried.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>Host from which to monitor log events.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>name</td>
<td>Collection name. This name appears in a configuration file, as well as the source and the sourcetype of the indexed data. If the value is localhost, it uses native event log collection; otherwise, it uses WMI.</td>
</tr>
<tr>
<td>server</td>
<td>Servers from which to gather data. Used if you need to gather from more than a single machine. See also lookup_host.</td>
</tr>
<tr>
<td>wql</td>
<td>The actual WQL query for monitoring the performance object.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu -d classes=Win32_PerfFormattedData_PerfOS_Processor -d interval=5 -d lookup_host=localhost -d server=xx.1.5.157,10.1.5.158

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
  xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-wmi-collections</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections</id>
  <updated>2011-07-27T14:15:33-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>cpu</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu</id>
    <updated>2011-07-27T14:15:33-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="classes">Win32_PerfFormattedData_PerfOS_Processor</s:key>
        <s:dict>
          <s:key name="disabled">0</s:key>
          ... eai:acl node elided ...
          <s:key name="fields">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:key>
        </s:dict>
        <s:key name="index">default</s:key>
        <s:key name="instances">540
```
data/inputs/win-perfmon

https://<host>:<mPort>/services/data/inputs/win-perfmon

Access and manage performance monitoring configurations. This input allows you to poll Windows performance monitor counters.

GET

Get current performance monitoring configuration details.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>List of valid Performance Monitor counters.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates whether the input is disabled.</td>
</tr>
<tr>
<td>index</td>
<td>The index that this input should send data to.</td>
</tr>
<tr>
<td>instances</td>
<td>List of valid instances for a Performance Monitor counter.</td>
</tr>
<tr>
<td>interval</td>
<td>How often, in seconds, to poll for new data.</td>
</tr>
<tr>
<td>object</td>
<td>A valid Performance Monitor object as defined within Performance Monitor.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -u admin:pass https://localhost:8089/services/data/inputs/win-perfmon
```
Update performance monitoring collection settings.

Request parameters
### Table

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>String</td>
<td></td>
<td>A set of counters to monitor. A '*' is equivalent to all counters. Specify each counter as a separate argument to the POST operation.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>Docs-W8R2-Std7</td>
<td>Name of the host for the Windows Performance Monitor.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>instances</td>
<td>String</td>
<td></td>
<td>A set of counter instances to monitor. A '*' is equivalent to all instances. Specify each instance as a separate argument to the POST operation.</td>
</tr>
<tr>
<td>interval</td>
<td>Number</td>
<td></td>
<td>How frequently, in seconds, to poll for new data.</td>
</tr>
<tr>
<td>name required</td>
<td>String</td>
<td></td>
<td>This is the name of the collection. This name appears in configuration file, as well as the source and the sourcetype of the indexed data.</td>
</tr>
<tr>
<td>object</td>
<td>String</td>
<td></td>
<td>A valid performance monitor object (for example, 'Process,' 'Server,' 'PhysicalDisk.')</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Source for inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>Source type of input.</td>
</tr>
</tbody>
</table>

### Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>List of valid Performance Monitor counters.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates whether the input is disabled.</td>
</tr>
<tr>
<td>host</td>
<td>Name of the host for the Windows Performance Monitor.</td>
</tr>
<tr>
<td>index</td>
<td>The index that this input should send data to.</td>
</tr>
<tr>
<td>If no value is present, send data to the default index.</td>
<td></td>
</tr>
<tr>
<td>instances</td>
<td>List of valid instances for a Performance Monitor counter.</td>
</tr>
<tr>
<td>interval</td>
<td>How frequently, in seconds, to poll for new data.</td>
</tr>
<tr>
<td>object</td>
<td>A valid Performance Monitor object as defined within Performance Monitor.</td>
</tr>
<tr>
<td>source</td>
<td>Source for inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Source type of the input.</td>
</tr>
</tbody>
</table>

### Example request and response

**XML Request**

```bash
curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-perfmon -d interval=4 -d name=mymemory -d object=Memory
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
```

543
Manage the `{name}` performance monitoring stanza.

**DELETE**

Delete a given monitoring stanza.

**Request parameters**

None

**Returned values**

None
Example request and response

XML Request

curl -u admin:pass --request DELETE  
https://localhost:8089/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"  
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"  
      xmlns:s="http://dev.splunk.com/ns/rest">  
  <title>win-perfmon</title>  
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-perfmon/id</id>  
  <updated>2011-07-29T19:47:06-07:00</updated>  
  <generator version="104976"/>  
  <author>  
    <name>Splunk</name>  
  </author>  
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_new" rel="create"/>  
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_reload" rel="_reload"/>  
  ... opensearch nodes elided ...  
  <s:messages/>  
</feed>

GET

Get settings for a given performance stanza.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>List of valid Performance Monitor counters.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates whether the input is disabled.</td>
</tr>
<tr>
<td>index</td>
<td>The index that this input should send data to.</td>
</tr>
<tr>
<td></td>
<td>If no value is present, send data to the default index.</td>
</tr>
<tr>
<td>instances</td>
<td>List of valid instances for a Performance Monitor counter.</td>
</tr>
<tr>
<td>interval</td>
<td>How often, in seconds, to poll for new data.</td>
</tr>
<tr>
<td>object</td>
<td>A valid Performance Monitor object as defined within Performance Monitor.</td>
</tr>
</tbody>
</table>
Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>win-perfmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-perfmon</id>
  <updated>2011-07-29T19:44:21-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>mymemory</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory</id>
    <updated>2011-07-29T19:44:21-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory/_new" rel="create"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory/edit" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory/remove" rel="remove"/>
    <link href="/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="counters">
          <s:list/>
        </s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:list>
                <s:item>counters</s:item>
                <s:item disabled</s:item>
                <s:item>index</s:item>
                <s:item>instances</s:item>
                <s:item>interval</s:item>
                <s:item>object</s:item>
              </s:list>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                ... eai:acl node elided ...
              </s:list>
            </s:key>
          </s:dict>
        </s:key>
        <s:key name="requiredFields">
          <s:list>
            <s:item>counters</s:item>
            <s:item disabled</s:item>
            <s:item>index</s:item>
            <s:item>instances</s:item>
            <s:item>interval</s:item>
            <s:item>object</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
POST

Modify an existing monitoring stanza.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>String</td>
<td></td>
<td>A set of counters to monitor. A '*' is equivalent to all counters. Specify each counter as a separate argument to the POST operation.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>Docs-W8R2-Std7</td>
<td>Name of the host for the Windows Performance Monitor.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The index in which to store the gathered data.</td>
</tr>
<tr>
<td>instances</td>
<td>String</td>
<td></td>
<td>A set of counter instances to monitor. A '*' is equivalent to all instances. Specify each instance as a separate argument to the POST operation.</td>
</tr>
<tr>
<td>interval</td>
<td>Number</td>
<td></td>
<td>How frequently, in seconds, to poll for new data.</td>
</tr>
<tr>
<td>object</td>
<td>String</td>
<td></td>
<td>A valid performance monitor object (for example, 'Process,' 'Server,' 'PhysicalDisk.')</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>Source for inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>Source type of input.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>counters</td>
<td>List of valid Performance Monitor counters.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates whether the input is disabled.</td>
</tr>
<tr>
<td>host</td>
<td>Name of the host for the Windows Performance Monitor.</td>
</tr>
</tbody>
</table>

547
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>The index that this input should send data to. If no value is present, send</td>
</tr>
<tr>
<td></td>
<td>data to the default index.</td>
</tr>
<tr>
<td>instances</td>
<td>List of valid instances for a Performance Monitor counter.</td>
</tr>
<tr>
<td>interval</td>
<td>How frequently, in seconds, to poll for new data.</td>
</tr>
<tr>
<td>object</td>
<td>A valid Performance Monitor object as defined within Performance Monitor,</td>
</tr>
<tr>
<td>source</td>
<td>Source for inputs.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>Source type of the input.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/inputs/win-perfmon/mymemory -d
interval=10

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/
      xmlns:s="http://dev.splunk.com/ns/rest">
<title>win-perfmon</title>
</feed>
```
data/modular-inputs

https://<host>:<mPort>/services/data/modular-inputs
Access currently defined modular inputs on the system.

For more information, refer to Modular inputs: Introspection scheme details in Developing Views and Apps for Splunk Web.

GET
Get information about configured modular inputs.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Provides descriptive text for title shown on the Data inputs manager page.</td>
</tr>
<tr>
<td></td>
<td>The description also appears on the Add new data inputs page.</td>
</tr>
<tr>
<td>endpoint</td>
<td>Contains one or more &lt;arg&gt; elements, which define the parameters to an endpoint.</td>
</tr>
<tr>
<td>streaming_mode</td>
<td>Indicates the streaming mode for the modular input. Valid values are xml and simple.</td>
</tr>
<tr>
<td>title</td>
<td>The label for a modular input script. The title appears on the Data inputs manager page.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/services/data/modular-inputs

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
<title>modular-inputs</title>
<iid>https://localhost:8089/services/data/modular-inputs</iid>
<updated>2012-07-09T12:41-07:00</updated>
<generator build="129290" version="5.0"/>
<author>
  <name>Splunk</name>
</author>

... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>s3</title>
  <id>https://localhost:8089/services/data/modular-inputs/s3</id>
  <updated>2012-07-09T12:41-07:00</updated>
  <link href="/services/data/modular-inputs/s3" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/modular-inputs/s3" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="description">Get data from Amazon S3.  
      ... eai:acl node elided ...
      </s:key>
      <s:key name="endpoint">
        <s:dict>
          <s:key name="args">
            <s:dict>
              <s:key name="key_id">
                <s:dict>
                  <s:key name="data_type">string</s:key>
                  <s:key name="description">Your Amazon key ID.</s:key>
                  <s:key name="order">1</s:key>
                  <s:key name="required_on_create">1</s:key>
                  <s:key name="required_on_edit">0</s:key>
                  <s:key name="title">Key ID</s:key>
                </s:dict>
              </s:key>
              <s:key name="name">
                <s:dict>
                  <s:key name="data_type">string</s:key>
                  <s:key name="description">An S3 resource name without the leading s3://.  For example, for s3://bucket/file.txt specify bucket/file.txt.  You can also monitor a whole bucket (for example by specifying 'bucket'), or files within a sub-directory of a bucket (for example 'bucket/some/directory/'; note the trailing slash).]]</s:key>
                  <s:key name="order">0</s:key>
                  <s:key name="title">Resource name</s:key>
                </s:dict>
              </s:key>
              <s:key name="secret_key">
                <s:dict>
                  <s:key name="data_type">string</s:key>
                  <s:key name="description">Your Amazon secret key.</s:key>
                  <s:key name="order">2</s:key>
                  <s:key name="required_on_create">1</s:key>
                  <s:key name="required_on_edit">0</s:key>
                  <s:key name="title">Secret key</s:key>
                </s:dict>
              </s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
data/modular-inputs/{name}

https://<host>:<mPort>/services/data/modular-inputs/{name}

Get information about the `{name}` modular input.

GET

Get information about a modular input.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>The label for a modular input script. The label appears in the <strong>Data inputs</strong> manager page.</td>
</tr>
<tr>
<td>endpoint</td>
<td>Contains one or more <code>&lt;arg&gt;</code> elements, which define the parameters to an endpoint.</td>
</tr>
<tr>
<td>streaming_mode</td>
<td>Indicates the streaming mode for the modular input. Valid values are <code>xml</code> or <code>simple</code> (plain text). Contains one or more <code>&lt;arg&gt;</code> elements, which define the parameters to an endpoint.</td>
</tr>
<tr>
<td>title</td>
<td>The label for a modular input script. The label appears in the <strong>Data inputs</strong> manager page.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -u admin:pass https://localhost:8089/services/data/modular-inputs/twitter
```

XML Response

```
551
```
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:a="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
  <title>modular-inputs</title>
  <id>https://localhost:8089/services/data/modular-inputs</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <generator build="129290" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
</feed>

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:a="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
  <title>twitter</title>
  <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <link href="/services/data/modular-inputs/twitter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/modular-inputs/twitter" rel="list"/>
</feed>

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:a="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
  <title>twitter</title>
  <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <link href="/services/data/modular-inputs/twitter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/modular-inputs/twitter" rel="list"/>
</feed>

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:a="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
  <title>twitter</title>
  <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <link href="/services/data/modular-inputs/twitter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/modular-inputs/twitter" rel="list"/>
</feed>

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:a="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
  <title>twitter</title>
  <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <link href="/services/data/modular-inputs/twitter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/modular-inputs/twitter" rel="list"/>
</feed>

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:a="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
  <title>twitter</title>
  <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <link href="/services/data/modular-inputs/twitter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/modular-inputs/twitter" rel="list"/>
</feed>

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:a="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
  <title>twitter</title>
  <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <link href="/services/data/modular-inputs/twitter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/modular-inputs/twitter" rel="list"/>
</feed>

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:a="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
  <title>twitter</title>
  <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <link href="/services/data/modular-inputs/twitter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/modular-inputs/twitter" rel="list"/>
</feed>

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:a="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/*">
  <title>twitter</title>
  <id>https://localhost:8089/services/data/modular-inputs/twitter</id>
  <updated>2012-07-09T11:07:29-07:00</updated>
  <link href="/services/data/modular-inputs/twitter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/modular-inputs/twitter" rel="list"/>
</feed>
indexing/preview

https://<host>:<mPort>/services/indexing/preview

Preview events from a source file before you index the file.

The `edit_monitor` or `edit_upload_and_index` capabilities are required for this endpoint.

**GET**

Return a list of all data preview jobs.

**Usage details**

Data returned includes the Splunk management URI to access each preview job.

You can check the status of a data preview job with GET request to `/search/jobs/{search_id}` to obtain information such as the `dispatchState`, `doneProgress`, and `eventCount`. You can also use the data preview job ID as the `search_id` parameter in a GET request to `/search/jobs/{search_id}/results_preview` to preview events from the source file.

**Request parameters**

None

**Returned values**

None

**Example request and response**

**XML Request**

curl -u admin:pass https://localhost:8089/services/indexing/preview

**XML Response**

<title>preview</title>
:id>https://localhost:8089/services/indexing/preview</id>
<updated>2011-11-28T14:35:35-08:00</updated>
POST

Create a preview data job for the specified source file, returning the preview data job ID.

Usage details
Typically, you first examine preview data events returned from GET /search/jobs/{job_id}/events. Then you define new sourcetypes as needed with this endpoint.

Use the POST operation to create a data preview job and return the corresponding data preview job ID. Use the preview job ID as the search_id parameter in GET /search/jobs/{search_id}/results_preview to obtain a data preview.

You can optionally define sourcetypes for a preview data job in props.conf.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>input.path</td>
<td>String</td>
<td></td>
<td>Required. The absolute file path to a local file that you want to preview data returned from indexing.</td>
</tr>
<tr>
<td>props.&lt;props_attr&gt;</td>
<td>String</td>
<td></td>
<td>Define a new sourcetype in props.conf for preview data that you are indexing.</td>
</tr>
</tbody>
</table>

Returned values
None
Example request and response

XML Request

curl -u admin:pass https://localhost:8089/services/indexing/preview -d
input.path=/Applications/splunk/var/log/splunk/metrics.log

XML Response

<response>
  <messages>
    <msg type='INFO'>1319496093.11</msg>
  </messages>
</response>

indexing/preview/{job_id}

https://<host>:<mPort>/services/indexing/preview/{job_id}

Get props.conf file settings for the {job_id} job.

GET

Get props.conf file settings for a job.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -u admin:pass https://localhost:8089/services/indexing/preview/1319496093.11

XML Response

<entry xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest">
  <title>1319496093.11</title>
  <id>https://localhost:8089/services/indexing/preview/1319496093.11</id>
</entry>
receivers/simple

https://<host>:<mPort>/services/receivers/simple
Allows for sending events to Splunk in an HTTP request.

Authentication and authorization
The edit_tcp capability is additionally required for this endpoint.

POST
Create events from the contents contained in the HTTP body.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>

556
<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;arbitrary_data&gt;</td>
<td>String</td>
<td>Required</td>
<td>Raw event text. This is the entirety of the HTTP request body.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td></td>
<td>The value to populate in the host field for events from this data input.</td>
</tr>
<tr>
<td>host_regex</td>
<td>String</td>
<td></td>
<td>A regular expression used to extract the host value from each event.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>The destination index where events are sent.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>The source value to fill in the metadata for this input's events.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>The sourcetype to apply to events from this input.</td>
</tr>
</tbody>
</table>

**Returned values**

None

**Example request and response**

**XML Request**


**XML Response**

```xml
<response>
  <results>
    <result>
      <field k="_index">
        <value>
          <text>default</text>
        </value>
      </field>
      <field k="bytes">
        <value>
          <text>67</text>
        </value>
      </field>
      <field k="host">
        <value>
          <text>127.0.0.1</text>
        </value>
      </field>
      <field k="source">
        <value>
          <text>www</text>
        </value>
      </field>
      <field k="sourcetype">
        <value>
          <text>web_event</text>
        </value>
      </field>
    </result>
  </results>
</response>
```
receivers/stream

https://<host>:<mPort>/services/receivers/stream

Open a socket to receive streaming data.

Authentication and authorization
The edit_tcp or edit_tcp_stream capabilities are required for this endpoint.

POST

Create events from the stream of data following HTTP headers.

Usage details

Data transfer continues until you enter <CTRL-C>.

For streaming connections, set streaming and x-splunk-input-mode arguments in the header.

For HTTP uploads, if the caller passes a content-type of "multipart/form data", the HTTP file upload protocol is used and files are indexed.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;data_stream&gt;</td>
<td>String</td>
<td></td>
<td><strong>Required.</strong> Raw event text. This does not need to be presented as a complete HTTP request, but can be streamed in as data is available.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td></td>
<td>The value to populate in the host field for events from this data input.</td>
</tr>
<tr>
<td>host_regex</td>
<td>String</td>
<td></td>
<td>A regular expression used to extract the host value from each event.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td></td>
<td>The index to send events from this input to.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td></td>
<td>The source value to fill in the metadata for this input's events.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</td>
<td></td>
<td>The sourcetype to apply to events from this input.</td>
</tr>
</tbody>
</table>

Returned values
None

Example

Python Request
import httpplib, time

conn = httpplib.HTTPSConnection("localhost", 8089)
conn.connect()
conn.putrequest("POST", "/services/receivers/stream?source=www\source=web_data")
conn.putheader("Authorization", "Splunk 67bed982ce1af9ba2e393b15ed63c916")
conn.putheader("x-splunk-input-mode", "streaming")
conn.endheaders()

i = 0
while i < 100:
    conn.send("%s A sample event (idx: %s).\n" % (time.asctime(), i))
    time.sleep(1)
    i += 1

conn.close()

server/pipelinesets

https://<host>:<mPort>/services/server/pipelinesets
Provides information on the ingestion pipeline sets on an indexer.

Authentication and authorization
The list_pipeline_sets capability is required for this endpoint.

Usage details
See Manage pipeline sets for index parallelization in Managing Indexers and Clusters of Indexers.

GET

Query the status of pipeline sets.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>busiest_thread_name</td>
<td>The name of the busiest pipeline thread within the pipeline set for past calculation period.</td>
</tr>
<tr>
<td>dutycycle_ratio</td>
<td>The dutycycle ratio of the busiest pipeline thread within the pipeline set for past calculation period.</td>
</tr>
<tr>
<td>requests_last_period</td>
<td>The number of ingestion requests processed by the pipeline set in the past calculation period.</td>
</tr>
<tr>
<td>share</td>
<td>The relative probability of selection of the pipeline set for the past calculation period.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://ronnie:8178/services/server/pipelinesets

XML Response
services/collector

<protocol>://<host>:<mPort>/services/collector
Send events to HTTP Event Collector using the Splunk platform JSON event protocol.

By default, this endpoint works on port 8088 and uses HTTPS for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Note: When using an ACK-enabled token, an ackID is returned within a JSON object in the response. For example, {"ackID": "0"} indicates an ackID of 0. Use the ackID to query the services/collector/ack endpoint to verify event indexing. For more information, see services/collector/ack.

Authorization
Requires an HTTP Event Collector token or basic auth, as defined in RFC 1945. See request examples for more details.

See also
• data/inputs/http
• data/inputs/http/{name}
• data/inputs/http/{name}/disable
• data/inputs/http/{name}/enable

POST
Send events to the HTTP Event Collector.

Usage details
HTTP Event Collector functionality must be enabled to send events.

To send events to the HTTP Event Collector, you must provide an HTTP Event Collector token in the authorization header. The token is created using the data/inputs/http endpoint. You can then retrieve the token with a GET request on the data/inputs/http/{name} endpoint, where {name} is the name of your token. Include the authentication token in the request header using the following format: Authorization: Splunk <token>. The format is case-sensitive.

Use the Splunk search application to view the logged events. For example, use index=main | search sourcetype=access to view all logged events with a sourcetype of access.

For performance reasons, the data input endpoint follows a simple error handling model. It assumes that in most cases it receives a well-formed event data payload. If there is malformed event data in the payload, events continue to be extracted until an error is encountered. Processing stops immediately on an error and the error and number of payload events processed successfully are reported. Events processed before the error are sent to indexers and all events after the first error are dropped.

Request parameters
<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel</td>
<td>See description</td>
<td>Required if useAck is enabled. Pass in the channel GUID as a string parameter or using the &quot;x-splunk-request-channel&quot; header.</td>
</tr>
<tr>
<td>event</td>
<td>string</td>
<td>Required. Event payload key-value. Value can be a string or a JSON object.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>JSON example: {&quot;event&quot;: &quot;message&quot;: &quot;Access log test message&quot;}</td>
</tr>
<tr>
<td></td>
<td></td>
<td>String example: &quot;event&quot;: &quot;Access log test message.&quot;</td>
</tr>
<tr>
<td>fields</td>
<td>JSON object</td>
<td>Fields for indexing that do not occur in the event payload itself. You can use this parameter when you do not want particular fields to be included in the event data, but you need additional metadata for indexing and searching. Specify one or more additional fields to include for indexing with the event payload. For each field, use a key to specify the name and include one or more values. Specify multiple values in an array. In the following example, the &quot;severity&quot; field gets the value &quot;INFO&quot; and the &quot;category&quot; key gets both &quot;foo&quot; and &quot;bar&quot; values. -d {&quot;event&quot;: &quot;something happened&quot;, &quot;fields&quot;: {&quot;severity&quot;: &quot;INFO&quot;, &quot;category&quot;: [&quot;foo&quot;, &quot;bar&quot;]}}</td>
</tr>
<tr>
<td>host</td>
<td>string</td>
<td>Host name. Specify with the host query string parameter. Sets a default for all events in the request. The default host name can be overridden.</td>
</tr>
<tr>
<td>index</td>
<td>string</td>
<td>Index name. Specify with the index query string parameter. Sets a default for all events in the request. The default index name can be overridden.</td>
</tr>
<tr>
<td>source</td>
<td>string</td>
<td>User-defined event source. Specify with the source query string parameter. Sets a default for all events in the request. The default source can be overridden.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>string</td>
<td>User-defined event sourcetype. Specify with the sourcetype query string parameter. Sets a default for all events in the request. The default sourcetype can be overridden.</td>
</tr>
<tr>
<td>time</td>
<td>string or unsigned integer</td>
<td>Epoch-formatted time. Specify with the time query string parameter. Sets a default for all events in the request. The default time can be overridden.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>text</td>
<td>Human readable status, same value as code.</td>
</tr>
<tr>
<td>code</td>
<td>Machine format status, same value as text.</td>
</tr>
<tr>
<td>invalid-event-number</td>
<td>When errors occur, indicates the zero-based index of first invalid event in an event sequence.</td>
</tr>
<tr>
<td>ackId</td>
<td>If useACK is enabled for the token, indicates the ackId to use for checking an indexer acknowledgement.</td>
</tr>
</tbody>
</table>

**Response status codes**

The following status codes have particular meaning for all HTTP Event Collector endpoints:

<table>
<thead>
<tr>
<th>Status Code</th>
<th>HTTP status code ID</th>
<th>HTTP status code</th>
<th>Status message</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>200</td>
<td>OK</td>
<td>Success</td>
</tr>
<tr>
<td>1</td>
<td>403</td>
<td>Forbidden</td>
<td>Token disabled</td>
</tr>
<tr>
<td>2</td>
<td>401</td>
<td>Unauthorized</td>
<td>Token is required</td>
</tr>
<tr>
<td>Status Code</td>
<td>HTTP status code ID</td>
<td>HTTP status code</td>
<td>Status message</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------</td>
<td>--------------------------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>401</td>
<td>Unauthorized</td>
<td>Invalid authorization</td>
</tr>
<tr>
<td>4</td>
<td>403</td>
<td>Forbidden</td>
<td>Invalid token</td>
</tr>
<tr>
<td>5</td>
<td>400</td>
<td>Bad Request</td>
<td>No data</td>
</tr>
<tr>
<td>6</td>
<td>400</td>
<td>Bad Request</td>
<td>Invalid data format</td>
</tr>
<tr>
<td>7</td>
<td>400</td>
<td>Bad Request</td>
<td>Incorrect index</td>
</tr>
<tr>
<td>8</td>
<td>500</td>
<td>Internal Error</td>
<td>Internal server error</td>
</tr>
<tr>
<td>9</td>
<td>503</td>
<td>Service Unavailable</td>
<td>Server is busy</td>
</tr>
<tr>
<td>10</td>
<td>400</td>
<td>Bad Request</td>
<td>Data channel is missing</td>
</tr>
<tr>
<td>11</td>
<td>400</td>
<td>Bad Request</td>
<td>Invalid data channel</td>
</tr>
<tr>
<td>12</td>
<td>400</td>
<td>Bad Request</td>
<td>Event field is required</td>
</tr>
<tr>
<td>13</td>
<td>400</td>
<td>Bad Request</td>
<td>Event field cannot be blank</td>
</tr>
<tr>
<td>14</td>
<td>400</td>
<td>Bad Request</td>
<td>ACK is disabled</td>
</tr>
<tr>
<td>15</td>
<td>400</td>
<td>Bad Request</td>
<td>Error in handling indexed fields</td>
</tr>
<tr>
<td>16</td>
<td>400</td>
<td>Bad Request</td>
<td>Query string authorization is not enabled</td>
</tr>
</tbody>
</table>

Example response messages

Success:

```
{"text":"Success","code":0}
```

Failure:

```
{"text":"Incorrect data format","code":5,"invalid-event-number":0}
```

Example request and response

**JSON Request**

```
```

**JSON Response**

```
{"text":"Success","code":0}
```

**JSON Response**

563
For `index=main | search sourcetype=access`

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/26/15 10:07:09.000 PM</td>
<td>{ [-] message: Access log test message 2 }</td>
</tr>
<tr>
<td>1/26/15 10:07:09.000 PM</td>
<td>{ [-] message: Access log test message }</td>
</tr>
</tbody>
</table>

**Request including the fields parameter**

```bash
```

**Basic auth request**

```bash
curl -u x:46931F1C-352C-4DF6-820C-F2689CF88494 -k https://localhost:8088/services/collector/JSON -d 'Hello World'
```

**services/collector/ack**

Use `services/collector/ack` to query event indexing status.

For events sent using HTTP Event Collector, check event indexing status. Requests must use a valid channel ID and authorization token with `useACK` enabled. An event ACK ID, returned in response to a POST to `services/collector`, is also required.

By default, this endpoint works on port 8088 and uses HTTPS for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

**Authentication and authorization**

Requires an HTTP Event Collector `<Token>`.

**GET**

Get HTTP Event Collector event indexing status.
Request parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel</td>
<td>See description</td>
<td>Required. Pass in the channel GUID as the channel string parameter or using the x-splunk-request-channel header.</td>
</tr>
<tr>
<td>&quot;acks&quot;</td>
<td>JSON object</td>
<td>Required. JSON object with an array of ack ID values. Include in the request payload.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acks</td>
<td>Contains the key/value pairs for each ACK ID requested. For each key in the &quot;acks&quot; object, a true value means the ACK ID's events were indexed. A false value means that indexing status is unknown. For example, an event may have an indexing delay long enough that it is no longer tracked.</td>
</tr>
</tbody>
</table>

Here is an example response.

{"acks": {"0": true, "1": false, "2": true, "3": false}}

Response status codes

Several HTTP status codes have particular meaning for all HTTP Event Collector endpoints. See HTTP Status Codes in services/collector.

Example requests and responses

For application token = B48F6736-479F-486B-96F9-3EF8C6378E70.

**Note:** useACK must be enabled on the token for use with this endpoint.

**JSON request**

```
```

**JSON response body**

{"acks":{"0":true,"1":true}}

**services/collector/event**

Sends timestamped events to HTTP Event Collector using the Splunk platform JSON event protocol when auto_extract_timestamp is set to "true" in the /event URL.

- An example of a timestamp is: 2017-01-02 00:00:00.
- If there is a timestamp in the event's JSON envelope, Splunk honors that timestamp first.
- If there is no timestamp in the event's JSON envelope, the merging pipeline extracts the timestamp from the event.
- If "time=xxx" is used in the /event URL then auto_extract_timestamp is disabled.
services/collector/event/1.0

This endpoint works identically to services/collector/event but introduces a protocol version for future scalability. For more information, see services/collector.

services/collector/health

<protocol>://<host>:8088/services/collector/health
This endpoint checks if HEC is healthy and able to accept new data from a load balancer. HEC health is determined if there is space available in the queue.

This endpoint works identically to services/health/1.0 but introduces a format version for future scalability. For more information, see services/collector/health/1.0.

Usage details

Port and protocol
By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Response codes

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>HEC is available and accepting input</td>
</tr>
<tr>
<td>400</td>
<td>Invalid HEC token</td>
</tr>
<tr>
<td>503</td>
<td>HEC is unhealthy, queues are full</td>
</tr>
</tbody>
</table>

services/collector/health/1.0

<protocol>://<host>:8088/services/collector/health/1.0
This endpoint checks if HEC is healthy and able to accept new data from a load balancer. HEC health is determined if there is space available in the queue.

This endpoint works identically to services/health but introduces a protocol version for future scalability. For more information, see services/collector/health.

Usage details

Port and protocol
By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Response codes

<table>
<thead>
<tr>
<th>Status Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>200</td>
<td>HEC is available and accepting input</td>
</tr>
<tr>
<td>Status Code</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>400</td>
<td>Invalid HEC token</td>
</tr>
<tr>
<td>503</td>
<td>HEC is unhealthy, queues are full</td>
</tr>
</tbody>
</table>

**services/collector/mint**

```<protocol>://<host>:<mPort>/services/collector/mint```

Post MINT formatted data to the HTTP Event Collector. The authorization header contains the authorization scheme and application token. The HTTP POST body contains event data in the MINT payload format.

**Authentication and authorization**

Requires an HTTP Event Collector `<token>`.

**Note:** By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

**POST**

Post MINT formatted data.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>String</td>
<td>Host name. Specify with the <code>host</code> query string parameter. Sets a default for all events in the request. Can be overridden.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>Index name. Specify with the <code>index</code> query string parameter. Sets a default for all events in the request. Can be overridden.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td>User-defined event source. Specify with the <code>source</code> query string parameter. Sets a default for all events in the request. The default source can be overridden.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>string</td>
<td>User-defined event sourcetype. Specify with the <code>sourcetype</code> query string parameter. Sets a default for all events in the request. The default sourcetype can be overridden.</td>
</tr>
<tr>
<td>time</td>
<td><code>string</code> or unsigned <code>integer</code></td>
<td>Epoch-formatted time. Specify with the <code>time</code> query string parameter. Sets a default for all events in the request. The default time can be overridden.</td>
</tr>
</tbody>
</table>

**Returned values**

None

**Response status codes**

Several HTTP status codes have particular meaning for all HTTP Event Collector endpoints. See HTTP Status Codes in services/collector.

**Example request and response**

567
Observe that the POST request is made to port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

MINT

For application token = B5A79AAD-D822-46CC-80D1-819F80D7BFB0

MINT Request

curl -k http://localhost:8088/services/collector/mint -H 'Authorization: Splunk B5A79AAD-D822-46CC-80D1-819F80D7BFB0' -d '{"data":"hello"}{^1^log^1433256}'

services/collector/mint/1.0

This endpoint works identically to receivers/token/mint but introduces a protocol version for future scalability.

[ Top ]

services/collector/raw

<protocol>://<host>:<mPort>/services/collector/raw

Send raw data directly to the HTTP Event Collector. This endpoint allows one or more raw events to be sent in a single request. Events are parsed using regex or JSON extraction. JSON field extraction works at index time.

Usage details

Channel
This endpoint requires a data channel GUID to differentiate data from different clients. Generate a GUID and provide it in a POST request as a custom HTTP header or as a parameter.

If a channel is not provided in the POST request, an error response is sent. Only valid GUIDs can be used. An error message is returned if GUID validation fails.

Port and protocol
By default, this endpoint works on port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Authentication and authorization
Requires an HTTP Event Collector token or basic auth, as defined in RFC 1945. See request examples for more details.

POST

Send raw data to the to the indexer queue. Requires a data channel GUID, provided as a custom HTTP header or request parameter.
Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>channel</td>
<td>See description.</td>
<td>Required. Pass in the channel GUID as the channel string parameter or using the x-splunk-request-channel header.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>Host name. Specify with the host query string parameter. Sets a default for all events in the request. Can be overridden.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>Index name. Specify with the index query string parameter. Sets a default for all events in the request. Can be overridden.</td>
</tr>
<tr>
<td>source</td>
<td>String</td>
<td>User-defined event source. Specify with the source query string parameter. Sets a default for all events in the request. The default source can be overridden.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>string</td>
<td>User-defined event sourcetype. Specify with the sourcetype query string parameter. Sets a default for all events in the request. The default sourcetype can be overridden.</td>
</tr>
<tr>
<td>time</td>
<td>string or unsigned integer</td>
<td>Epoch-formatted time. Specify with the time query string parameter. Sets a default for all events in the request. The default time can be overridden.</td>
</tr>
</tbody>
</table>

Returned values

None

Response status codes
Several HTTP status codes have particular meaning for all HTTP Event Collector endpoints. See HTTP Status Codes in services/collector.

Example request and response

Note that the following POST request examples are made to port 8088 and uses HTTPs for transport. The port and HTTP protocol settings can be configured independently of settings for any other servers in your deployment.

Simple request

This example passes the channel ID as part of the header.


Request including a timestamp


JSON request with timestamp


Basic auth request
curl -u x:46931F1C-352C-4DF6-820C-F2689CF88494
-k https://localhost:8088/services/collector/raw?channel=934793C0-FC91-467E-965A-7EAACEFBC4AB
-d 'Hello World'

Example JSON Response

{"text":"Success","code":0}

services/collector/raw/1.0

This endpoint works identically to services/collector/raw but introduces a protocol version for future scalability. See services/collector/raw.
Introspection endpoints

Introspection endpoint descriptions
Access server and instance information.

Usage details

*Review ACL information for an endpoint*

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

*Authentication and Authorization*

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings > Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings > Access controls** and click **Roles**.

*App and user context*

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

*Splunk Cloud URL for REST API access*

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

**Managed Splunk Cloud deployments**

https://<deployment-name>.splunkcloud.com:8089

**Self-service Splunk Cloud deployments**
To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the the Splunk REST API Tutorials for more information.
**data/index-volumes**

https://<host>:<mPort>/services/data/index-volumes

Get information about the volume (logical drives) in use by the Splunk deployment.

**GET**

List the Splunk deployment volumes.

**Usage details**

The default update period is 10 minutes, as defined by the `collectionPeriodInSecs` attribute in the following file.

`$SPLUNK_HOME/etc/apps/introspection_generator_addon/default/server.conf`

At least one observation period must pass after Splunk software startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```bash
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>max_size</code></td>
<td>Maximum <code>name</code> volume size limit (MB): infinite = No maximum specified.</td>
</tr>
<tr>
<td><code>name</code></td>
<td>Volume name</td>
</tr>
<tr>
<td><code>total_size</code></td>
<td>Total <code>name</code> volume capacity (MB). If <code>max_size</code> is infinite, this field is not listed.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:passwd https://localhost:8089/services/data/index-volumes
```

**XML Response**

```
...<title>introspection--disk-objects--volumes</title>
  <id>https://localhost:8089/services/data/index-volumes</id>
  <updated>2014-03-25T14:41:09-07:00</updated>
  <generator build="200839" version="6.1"/>
  <author>
    <name>Splunk</name>
```

572
data/index-volumes/{name}

https://<host>:<mPort>/services/data/index-volumes/{name}

Get information about the {name} volume (logical drive).

GET

List {name} volume properties.

Usage details
The default update period is 10 minutes, as defined by the collectionPeriodInSecs attribute in the following file.

$SPLUNK_HOME/etc/apps/introspection_generator_addon/default/server.conf

At least one observation period must pass after Splunk software startup for valid endpoint data to be available. The observation period is defined in the following $SPLUNK_HOME/etc/system/default/server.conf stanza.

[introspection:generator:disk_objects]
collectionPeriodInSecs = 600

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_size</td>
<td>Maximum name volume size limit (MB).</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>infinite</td>
<td>No maximum specified (i.e., 0, the default)</td>
</tr>
<tr>
<td>name</td>
<td>Volume name.</td>
</tr>
<tr>
<td>total_size</td>
<td>Total name volume capacity (MB). If max_size is infinite, this field is not listed.</td>
</tr>
</tbody>
</table>

### Example request and response

**XML Request**

```bash
curl -k -u admin:passwd https://localhost:8089/services/data/index-volumes/_splunk_summaries
```

**XML Response**

```xml
...<title>introspection--disk-objects--volumes</title>
{id>https://localhost:8089/services/data/index-volumes</id>
<updated>2014-03-27T14:35:26-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
... opensearch elements elided ...
<s:messages/>

<entry>
  <title>_splunk_summaries</title>
  <id>https://localhost:8089/services/data/index-volumes/_splunk_summaries</id>
  <updated>2014-03-27T14:35:26-07:00</updated>
  <link href="/services/data/index-volumes/_splunk_summaries" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/index-volumes/_splunk_summaries" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">... elided ...
      </s:key>
      <s:key name="eai:attributes">... elided ...
      </s:key>
      <s:key name="max_size">infinite</s:key>
      <s:key name="name">_splunk_summaries</s:key>
    </s:dict>
  </content>
</entry>
```

**data/indexes**

https://<host>:<mPort>/services/data/indexes

Create and manage data indexes.

**Authorization and authentication**

By default, all users can list all indexes. However, if the `indexes_list_all` capability is enabled in `authorize.conf`, access...
to all indexes is limited to only those roles with this capability.

To enable `indexes_list_all` capability restrictions on the `data/indexes` endpoint, create a `[capability::indexes_list_all]` stanza in `authorize.conf`. Specify `indexes_list_all-enabled` for any role permitted to list all indexes from this endpoint.

For more information, see the `authorize.conf` spec file in the *Admin Manual*.

**GET**

List the recognized indexes on the server.

**Request parameters**

Pagination and filtering parameters can be used with this method.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>datatype</code></td>
<td>String</td>
<td>event</td>
<td>Valid values: (all</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>assureUTF8</code></td>
<td>Indicates whether all data retrieved from the index is proper UTF8. If enabled (set to True), degrades indexing performance.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td><code>blockSignSize</code></td>
<td>Controls how many events make up a block for block signatures.</td>
</tr>
<tr>
<td></td>
<td>If this is set to 0, block signing is disabled for this index.</td>
</tr>
<tr>
<td></td>
<td>A recommended value is 100.</td>
</tr>
<tr>
<td><code>blockSignatureDatabase</code></td>
<td>The index that stores block signatures of events.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td><code>coldPath</code></td>
<td>Filepath to the cold databases for the index.</td>
</tr>
<tr>
<td><code>coldPath_expanded</code></td>
<td>Absolute filepath to the cold databases.</td>
</tr>
<tr>
<td><code>coldToFrozenDir</code></td>
<td>Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory.</td>
</tr>
</tbody>
</table>

Bucket freezing policy is as follows:

- New style buckets (4.2 and on): removes all files but the rawdata
  
  To thaw, run `splunk rebuild <bucket dir> on the bucket, then move to the thawed directory

- Old style buckets (Pre-4.2): gzip all the .data and .tsidx files
  
  To thaw, unzip the zipped files and move the bucket into the thawed directory
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coldToFrozenDir</td>
<td>If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence.</td>
</tr>
<tr>
<td>coldToFrozenScript</td>
<td>Path to the archiving script.</td>
</tr>
<tr>
<td></td>
<td>See the POST parameter description for details.</td>
</tr>
<tr>
<td>compressRawdata</td>
<td>This value is ignored. splunkd process always compresses raw data.</td>
</tr>
<tr>
<td>currentDBSizeMB</td>
<td>Total size, in MB, of data stored in the index. The total includes data in the home, cold and thawed paths.</td>
</tr>
<tr>
<td>datatype</td>
<td>The type of index (event</td>
</tr>
<tr>
<td>defaultDatabase</td>
<td>If no index destination information is available in the input data, the index shown here is the destination of such data.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the index is disabled.</td>
</tr>
<tr>
<td>enableRealtimeSearch</td>
<td>Indicates if this is a real-time search.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>frozenTimePeriodInSecs</td>
<td>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).</td>
</tr>
<tr>
<td></td>
<td>Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.</td>
</tr>
<tr>
<td>homePath</td>
<td>An absolute path that contains the hot and warm buckets for the index.</td>
</tr>
<tr>
<td>homePath_expanded</td>
<td>An absolute filepath to the hot and warm buckets for the index.</td>
</tr>
<tr>
<td>indexThreads</td>
<td>Number of threads used for indexing.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>isInternal</td>
<td>Indicates if this is an internal index (for example, _internal, _audit).</td>
</tr>
<tr>
<td>isReady</td>
<td>Indicates if the index is properly initialized.</td>
</tr>
<tr>
<td>lastInitTime</td>
<td>Last time the index processor was successfully initialized.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>maxConcurrentOptimizes</td>
<td>The number of concurrent optimize processes that can run against a hot bucket.</td>
</tr>
<tr>
<td></td>
<td>This number should be increased if instructed by Splunk Support. Typically the default value should suffice.</td>
</tr>
<tr>
<td>maxDataSize</td>
<td>The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying &quot;auto&quot; or &quot;auto_high_volume&quot; causes Splunk software to autotune this parameter (recommended). Use &quot;auto_high_volume&quot; for high volume indexes (such as the main index); otherwise, use &quot;auto&quot;. A &quot;high volume index&quot; is typically one that gets over 10GB of data per day.</td>
</tr>
<tr>
<td></td>
<td>* &quot;auto&quot; sets the size to 750MB.</td>
</tr>
<tr>
<td></td>
<td>* &quot;auto_high_volume&quot; sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.</td>
</tr>
<tr>
<td></td>
<td>Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>maxHotBuckets</td>
<td>If you specify an invalid number or string, maxDataSize is auto-tuned. Note: The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.</td>
</tr>
<tr>
<td>maxHotIdleSecs</td>
<td>Maximum life, in seconds, of a hot bucket. Defaults to 0. A value of 0 turns off the idle check (equivalent to INFINITE idle time). If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll.</td>
</tr>
<tr>
<td>maxHotSpanSecs</td>
<td>Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days). Note: If set too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.</td>
</tr>
<tr>
<td>maxMemMB</td>
<td>The amount of memory, in MB, allocated for indexing. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>maxMetaEntries</td>
<td>Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite). If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the punct field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README). There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.</td>
</tr>
<tr>
<td>maxRunningProcessGroups</td>
<td>Maximum number of processes that the indexer fires off at a time. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>maxTime</td>
<td>ISO8601 timestamp of the newest event time in the index.</td>
</tr>
<tr>
<td>maxTotalDataSizeMB</td>
<td>The maximum size of an index, in MB.</td>
</tr>
<tr>
<td>maxWarmDBCount</td>
<td>The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times are moved to cold.</td>
</tr>
<tr>
<td>memPoolMB</td>
<td>Determines how much memory is given to the indexer memory pool. This is a global setting, not a per-index setting.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>minRawFileSyncSecs</td>
<td>Can be either an integer (or &quot;disable&quot;). Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed. The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files. If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying &quot;disable&quot; disables syncing entirely: uncompressed slices are removed as soon as compression is complete.</td>
</tr>
<tr>
<td>minTime</td>
<td>ISO8601 timestamp of the oldest event time in the index.</td>
</tr>
<tr>
<td>partialServiceMetaPeriod</td>
<td>Related to serviceMetaPeriod. By default it is turned off (zero). If set, it enables metadata sync every &lt;integer&gt; seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync'ed at serviceMetaPeriod. partialServiceMetaPeriod specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.</td>
</tr>
<tr>
<td>quarantineFutureSecs</td>
<td>Events with timestamp of quarantineFutureSecs newer than &quot;now&quot; that are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>quarantinePastSecs</td>
<td>Events with timestamp of quarantinePastSecs older than &quot;now&quot; are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>rawChunkSizeBytes</td>
<td>Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, rawChunkSizeBytes is set to the default value. <strong>Note:</strong> rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. <strong>Warning:</strong> This is an advanced parameter. Only change it if instructed to do so by Splunk Support.</td>
</tr>
<tr>
<td>rotatePeriodInSecs</td>
<td>Rotation period, in seconds, that specifies how frequently to check: * If a new hot bucket needs to be created. * If there are any cold buckets that should be frozen. * If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.</td>
</tr>
<tr>
<td>serviceMetaPeriod</td>
<td>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds).</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>summarize</td>
<td>If true, leaves out certain index details, which provides a faster response.</td>
</tr>
<tr>
<td>suppressBannerList</td>
<td>List of indexes for which we suppress “index missing” warning banner messages. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>sync</td>
<td>Specifies the number of events that trigger the indexer to sync events. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>syncMeta</td>
<td>When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. Note: Do not change this parameter without the input of Splunk Support.</td>
</tr>
<tr>
<td>thawedPath</td>
<td>An absolute path that contains the thawed (resurrected) databases for the index.</td>
</tr>
<tr>
<td>thawedPath_expanded</td>
<td>Absolute filepath to the thawed (resurrected) databases.</td>
</tr>
<tr>
<td>throttleCheckPeriod</td>
<td>Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds). Note: Do not change this parameter without the input of Splunk Support.</td>
</tr>
<tr>
<td>totalEventCount</td>
<td>Total number of events in the index.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/data/indexes
```

**XML Response**

```xml
<entry>
  <title>indexes</title>
  <id>https://localhost:8089/services/data/indexes</id>
  <updated>2011-07-11T18:09:22-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/indexes/_new" rel="create"/>
  <link href="/services/data/indexes/_reload" rel="reload"/>
    ... opensearch elements elided ...
  <s:messages/>
  <entry>
    <title>_audit</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/indexes/_audit</id>
    <updated>2011-07-11T18:09:22-07:00</updated>
    <link href="/servicesNS/nobody/system/data/indexes/_audit" rel="alternate"/>
```

579
<content type="text/xml">
<s:dict>
  <s:key name="assureUTF8">0</s:key>
  <s:key name="blockSignSize">0</s:key>
  <s:key name="blockSignatureDatabase">_blocksignature</s:key>
  <s:key name="coldPath">$SPLUNK_DB/audit/colddb</s:key>
  <s:key name="coldPath_expanded">/home/amrit/temp/curl/splunk/var/lib/splunk/audit/colddb</s:key>
  <s:key name="coldToFrozenDir"/>
  <s:key name="coldToFrozenScript"/>
  <s:key name="compressRawdata">1</s:key>
  <s:key name="currentDBSizeMB">1</s:key>
  <s:key name="datatype">event</s:key>
  <s:key name="defaultDatabase">main</s:key>
  <s:key name="disabled">0</s:key>
  <s:key name="enableRealtimeSearch">1</s:key>
  <s:key name="frozenTimePeriodInSecs">188697600</s:key>
  <s:key name="homePath">$SPLUNK_DB/audit/db</s:key>
  <s:key name="homePath_expanded">/home/amrit/temp/curl/splunk/var/lib/splunk/audit/db</s:key>
  <s:key name="indexThreads">auto</s:key>
  <s:key name="isInternal">1</s:key>
  <s:key name="lastInitTime">1310432962.424512</s:key>
  <s:key name="maxConcurrentOptimizes">3</s:key>
  <s:key name="maxDataSize">auto</s:key>
  <s:key name="maxHotBuckets">3</s:key>
  <s:key name="maxHotIdleSecs">0</s:key>
  <s:key name="maxHotSpanSecs">7776000</s:key>
  <s:key name="maxMemMB">5</s:key>
  <s:key name="maxMetaEntries">1000000</s:key>
  <s:key name="maxRunningProcessGroups">20</s:key>
  <s:key name="maxTime">2011-07-10T22:20:53-0700</s:key>
  <s:key name="maxTotalDataSizeMB">500000</s:key>
  <s:key name="maxWarmDBCount">300</s:key>
  <s:key name="memPoolMB">auto</s:key>
  <s:key name="minRawFileSyncSecs">disable</s:key>
  <s:key name="minTime">2011-07-10T14:33:00-0700</s:key>
  <s:key name="partialServiceMetaPeriod">0</s:key>
  <s:key name="quarantineFutureSecs">2592000</s:key>
  <s:key name="quarantinePastSecs">77760000</s:key>
  <s:key name="rawChunkSizeBytes">131072</s:key>
  <s:key name="rotatePeriodInSecs">60</s:key>
  <s:key name="serviceMetaPeriod">25</s:key>
  <s:key name="suppressBannerList"/>
  <s:key name="sync">0</s:key>
  <s:key name="syncMeta"/>
  <s:key name="thawedPath">$SPLUNK_DB/audit/thaweddb</s:key>
  <s:key name="thawedPath_expanded">/home/amrit/temp/curl/splunk/var/lib/splunk/audit/thaweddb</s:key>
  <s:key name="throttleCheckPeriod">15</s:key>
  <s:key name="totalEventCount">230</s:key>
</s:dict>
</content>
POST

Create a new index.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blockSignSize</td>
<td>Number</td>
<td>0</td>
<td>Controls how many events make up a block for block signatures. If this is set to 0, block signing is disabled for this index. A recommended value is 100.</td>
</tr>
</tbody>
</table>
| bucketRebuildMemoryHint | String  | auto    | Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make. **Caution:** This is an advanced parameter. Inappropriate use of this parameter causes splunkd to not start if rebuild is required. **Do not set this parameter unless instructed by Splunk Support.** Default value, `auto`, varies by the amount of physical RAM on the host:
- less than 2GB RAM = 67108864 (64MB) tsidx
- 2GB to 8GB RAM = 134217728 (128MB) tsidx
- more than 8GB RAM = 268435456 (256MB) tsidx
Values other than "auto" must be 16MB-1GB. Highest legal value (of the numerical part) is 4294967295
You can specify the value using a size suffix: "16777216" or "16MB" are equivalent. |
| coldPath              | String  |         | An absolute path that contains the colddbs for the index. The path must be readable and writable. Cold databases are opened as needed when searching. May be defined in terms of a volume definition (see volume section below). Required. Splunk software does not start if an index lacks a valid colddPath. |
| coldToFrozenDir       | String  |         | Destination path for the frozen archive. Use as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory. Bucket freezing policy is as follows:
- New style buckets (4.2 and on): removes all files but the rawdata
  To thaw, run `splunk rebuild <bucket dir>` on the bucket, then move to the thawed directory
- Old style buckets (Pre-4.2): gzip all the .data and .tsidx files
  To thaw, gunzip the zipped files and move the bucket into the thawed directory |
If both `coldToFrozenDir` and `coldToFrozenScript` are specified, `coldToFrozenDir` takes precedence.

**coldToFrozenScript**
- **Type**: String
- **Default**: Path to the archiving script.
- **Description**: If your script requires a program to run it (for example, python), specify the program followed by the path. The script must be in `$SPLUNK_HOME/bin` or one of its subdirectories.

Splunk software ships with an example archiving script in `$SPLUNK_HOME/bin` called `coldToFrozenExample.py`. DO NOT use this example script directly. It uses a default path, and if modified in place any changes are overwritten on upgrade.

It is best to copy the example script to a new file in `bin` and modify it for your system. Most importantly, change the default archive path to an existing directory that fits your needs.

If your new script in `bin/` is named `myColdToFrozen.py`, set this key to the following:
```
coldToFrozenScript = "${SPLUNK_HOME}/bin/python" "${SPLUNK_HOME}/bin/myColdToFrozen.py"
```

By default, the example script has two possible behaviors when archiving:

- For buckets created from version 4.2 and on, it removes all files except for `rawdata`. To thaw: cd to the frozen bucket and type `splunk rebuild .`, then copy the bucket to thawed for that index. We recommend using the `coldToFrozenDir` parameter unless you need to perform a more advanced operation upon freezing buckets.
- For older-style buckets, we simply gzip all the `.tsidx` files. To thaw: cd to the frozen bucket and unzip the tsidx files, then copy the bucket to thawed for that index.

**compressRawdata**
- **Type**: Boolean
- **Default**: true
- **Description**: This parameter is ignored. The `splunkd` process always compresses raw data.

**datatype**
- **Type**: String
- **Default**: event
- **Description**: Valid values: (event | metric). Specifies the type of index.

**enableOnlineBucketRepair**
- **Type**: Boolean
- **Default**: true
- **Description**: Enables asynchronous "online fsck" bucket repair, which runs concurrently with Splunk software.

When enabled, you do not have to wait until buckets are repaired to start the Splunk platform. However, you might observe a slight performance degradation.

**frozenTimePeriodInSecs**
- **Type**: Number
- **Default**: 188697600
- **Description**: Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).

Freezing data means it is removed from the index. If you need to archive your data, refer to `coldToFrozenDir` and `coldToFrozenScript` parameter documentation.

**homePath**
- **Type**: String
- **Default**: An absolute path that contains the hot and warm buckets for the index.
Required. Splunk software does not start if an index lacks a valid `homePath`.

**Caution:** The path must be readable and writable.

Valid values are: `Integer[m|s|h|d]`

If a warm or cold bucket is older than the specified age, do not create or rebuild its Bloom filter. Specify 0 to never rebuild Bloom filters.

For example, if a bucket is older than specified with `maxBloomBackfillBucketAge`, and the rebuilding of its Bloom filter started but did not finish, do not rebuild it.

The number of concurrent optimize processes that can run against a hot bucket.

This number should be increased if instructed by Splunk Support. Typically the default value should suffice.

The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying "auto" or "auto_high_volume" causes Splunk software to autotune this parameter (recommended). Use "auto_high_volume" for high volume indexes (such as the main index); otherwise, use "auto". A "high volume index" would typically be considered one that gets over 10GB of data per day.

- "auto" sets the size to 750MB.
- "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.

Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding.

If you specify an invalid number or string, `maxDataSize` is auto-tuned.

*Note:* The precise size of your warm buckets may vary from `maxDataSize`, due to post-processing and timing issues with the rolling policy.

Maximum hot buckets that can exist per index. Defaults to 3.

When `maxHotBuckets` is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of `maxHotIdleSecs`, which can also cause hot buckets to roll.

Maximum life, in seconds, of a hot bucket. Defaults to 0.

If a hot bucket exceeds `maxHotIdleSecs`, Splunk software rolls it to warm. This setting operates independently of `maxHotBuckets`, which can also cause hot buckets to roll. A value of 0 turns off the idle check (equivalent to INFINITE idle time).
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| maxHotSpanSecs                | Number   | 7776000 | Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).  
                                 |          |         | *Note:* If you set this too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data. |
| maxMemMB                      | Number   | 5       | The amount of memory, expressed in MB, to allocate for buffering a single tsidx file into memory before flushing to disk. Defaults to 5. The default is recommended for all environments.  
                                 |          |         | IMPORTANT: Calculate this number carefully. Setting this number incorrectly may have adverse effects on your systems memory and/or splunkd stability/performance. |
| maxMetaEntries                | Number   | 1000000 | Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite).  
                                 |          |         | If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the punct field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README).  
                                 |          |         | There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant. |
| maxTimeUnreplicatedNoAcks     | Number   | 300     | Upper limit, in seconds, on how long an event can sit in raw slice. Applies only if replication is enabled for this index. Otherwise ignored.  
                                 |          |         | If there are any acknowledged events sharing this raw slice, this parameter does not apply. In this case, maxTimeUnreplicatedWithAcks applies.  
                                 |          |         | Highest legal value is 2147483647. To disable this parameter, set to 0.  
                                 |          |         | *Note:* this is an advanced parameter. Understand the consequences before changing. |
| maxTimeUnreplicatedWithAcks   | Number   | 60      | Upper limit, in seconds, on how long events can sit unacknowledged in a raw slice. Applies only if you have enabled acks on forwarders and have replication enabled (with clustering).  
<pre><code>                             |          |         | *Note:* This is an advanced parameter. Make sure you understand the settings on all forwarders before changing this. This number should not exceed ack timeout configured on any forwarder, and should actually be set to at most half of the minimum value of that timeout. You can find this setting in outputs.conf readTimeout setting under the tcpout stanza. |
</code></pre>
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.</td>
</tr>
<tr>
<td>maxTotalDataSizeMB</td>
<td>Number</td>
<td>500000</td>
<td>The maximum size of an index (in MB). If an index grows larger than the maximum size, the oldest data is frozen.</td>
</tr>
<tr>
<td>maxWarmDBCount</td>
<td>Number</td>
<td>300</td>
<td>The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times is moved to cold.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>minRawFileSyncSecs</td>
<td>Number</td>
<td>disable</td>
<td>Specify an integer (or &quot;disable&quot;) for this parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This parameter sets how frequently splunkd forces a filesystem sync while compressing journal slices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying &quot;disable&quot; disables syncing entirely: uncompressed slices are removed as soon as compression is complete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Note: Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed</td>
</tr>
<tr>
<td>minStreamGroupQueueSize</td>
<td>Number</td>
<td>2000</td>
<td>Minimum size of the queue that stores events in memory before committing them to a tsidx file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Caution: Do not set this value, except under advice from Splunk Support.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>The name of the index to create.</td>
</tr>
<tr>
<td>processTrackerServiceInterval</td>
<td>Number</td>
<td>1</td>
<td>Specifies, in seconds, how often the indexer checks the status of the child OS processes it launched to see if it can launch new processes for queued requests. Defaults to 15.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If set to 0, the indexer checks child process status every second.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Highest legal value is 4294967295.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>quarantineFutureSecs</td>
<td>Number</td>
<td>2592000</td>
<td>Events with timestamp of <code>quarantineFutureSecs</code> newer than &quot;now&quot; are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>quarantinePastSecs</td>
<td>Number</td>
<td>77760000</td>
<td>Events with timestamp of <code>quarantinePastSecs</code> older than &quot;now&quot; are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>rawChunkSizeBytes</td>
<td>Number</td>
<td>131072</td>
<td>Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, <code>rawChunkSizeBytes</code> is set to the default value. Note: <code>rawChunkSizeBytes</code> only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. WARNING: This is an advanced parameter. Only change it if you are instructed to do so by Splunk Support.</td>
</tr>
<tr>
<td>repFactor</td>
<td>String</td>
<td>0</td>
<td>Index replication control. This parameter applies to only clustering slaves. <code>auto</code> = Use the master index replication configuration value. <code>0</code> = Turn off replication for this index.</td>
</tr>
<tr>
<td>rotatePeriodInSecs</td>
<td>Number</td>
<td>60</td>
<td>How frequently (in seconds) to check if a new hot bucket needs to be created. Also, how frequently to check if there are any warm/cold buckets that should be rolled/frozen.</td>
</tr>
<tr>
<td>serviceMetaPeriod</td>
<td>Number</td>
<td>25</td>
<td>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.</td>
</tr>
<tr>
<td>syncMeta</td>
<td>Boolean</td>
<td>true</td>
<td>When <code>true</code>, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. Note: Do not change this parameter without the input of a Splunk Support.</td>
</tr>
<tr>
<td>thawedPath</td>
<td>String</td>
<td></td>
<td>An absolute path that contains the thawed (resurrected) databases for the index. Cannot be defined in terms of a volume definition. Required. Splunk software does not start if an index lacks a valid <code>thawedPath</code>.</td>
</tr>
</tbody>
</table>

586
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>throttleCheckPeriod</td>
<td>Number</td>
<td>15</td>
<td>Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).  Note: Do not change this parameter without the input of Splunk Support.</td>
</tr>
<tr>
<td>tstatsHomePath</td>
<td>String</td>
<td></td>
<td>Location to store datamodel acceleration TSIDX data for this index. Restart splunkd after changing this parameter. If specified, it must be defined in terms of a volume definition.  Caution: Path must be writable.  Default value: volume:_splunk_summaries/$_index_name/tstats</td>
</tr>
<tr>
<td>warmToColdScript</td>
<td>String</td>
<td></td>
<td>Path to a script to run when moving data from warm to cold.  This attribute is supported for backwards compatibility with Splunk software versions older than 4.0. Contact Splunk support if you need help configuring this setting.  Caution: Migrating data across filesystems is now handled natively by splunkd. If you specify a script here, the script becomes responsible for moving the event data, and Splunk-native data migration is not used.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assureUTF8</td>
<td>Boolean value indicating whether all data retrieved from the index is proper UTF8.  If enabled (set to True), degrades indexing performance  Can only be set globally.</td>
</tr>
<tr>
<td>blockSignSize</td>
<td>Controls how many events make up a block for block signatures.  If this is set to 0, block signing is disabled for this index.  A recommended value is 100.</td>
</tr>
<tr>
<td>blockSignatureDatabase</td>
<td>The index that stores block signatures of events.  This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>bucketRebuildMemoryHint</td>
<td>Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make.</td>
</tr>
<tr>
<td>coldPath</td>
<td>Filepath to the cold databases for the index.</td>
</tr>
<tr>
<td>coldPath_expanded</td>
<td>Absolute filepath to the cold databases.</td>
</tr>
<tr>
<td>coldToFrozenDir</td>
<td>Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory.</td>
</tr>
</tbody>
</table>
Bucket freezing policy is as follows:

- New style buckets (4.2 and on): removes all files but the rawdata
  
  To thaw, run `splunk rebuild <bucket dir>` on the bucket, then move to the thawed directory

- Old style buckets (Pre-4.2): gzip all the .data and .tsidx files
  
  To thaw, unzip the zipped files and move the bucket into the thawed directory

If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>coldToFrozenScript</td>
<td>Path to the archiving script.</td>
</tr>
<tr>
<td>compressRawdata</td>
<td>This value is ignored. splunkd process always compresses raw data.</td>
</tr>
<tr>
<td>currentDBSizeMB</td>
<td>Total size, in MB, of data stored in the index. The total incudes data in the home, cold and thawed paths.</td>
</tr>
<tr>
<td>datatype</td>
<td>The type of index (event</td>
</tr>
<tr>
<td>defaultDatabase</td>
<td>If no index destination information is available in the input data, the index shown here is the destination of such data.</td>
</tr>
<tr>
<td>enableOnlineBucketRepair</td>
<td>Indicates whether to run asynchronous &quot;online fsck&quot; bucket repair, which runs in a process concurrently with Splunk software.</td>
</tr>
<tr>
<td>enableRealtimeSearch</td>
<td>Indicates if this is a real-time search.</td>
</tr>
<tr>
<td>frozenTimePeriodInSecs</td>
<td>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).</td>
</tr>
<tr>
<td>homePath</td>
<td>An absolute path that contains the hot and warm buckets for the index.</td>
</tr>
<tr>
<td>homePath_expanded</td>
<td>An absolute filepath to the hot and warm buckets for the index.</td>
</tr>
<tr>
<td>indexThreads</td>
<td>Number of threads used for indexing.</td>
</tr>
<tr>
<td>isInternal</td>
<td>Indicates if this is an internal index (for example, _internal, _audit).</td>
</tr>
<tr>
<td>isReady</td>
<td>Indicates if an index is properly initialized.</td>
</tr>
<tr>
<td>lastInitTime</td>
<td>Last time the index processor was successfully initialized.</td>
</tr>
<tr>
<td>maxBloomBackfillBucketAge</td>
<td>If a bucket (warm or cold) is older than this, Splunk software does not create (or re-create) its Bloom filter.</td>
</tr>
<tr>
<td>maxConcurrentOptimizes</td>
<td>The number of concurrent optimize processes that can run against a hot bucket.</td>
</tr>
</tbody>
</table>

This number should be increased if instructed by Splunk Support. Typically the default value should suffice.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| maxDataSize         | The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying "auto" or "auto_high_volume" causes Splunk software to autotune this parameter (recommended). Use "auto_high_volume" for high volume indexes (such as the main index); otherwise, use "auto". A "high volume index" is typically one that gets over 10GB of data per day.  
  - "auto" sets the size to 750MB.  
  - "auto_high_volume" sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.  
  Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding.  
  If you specify an invalid number or string, maxDataSize is auto-tuned.  
  Note: The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.                                                                                                                                       |
| maxHotBuckets       | Maximum hot buckets that can exist per index. Defaults to 3.  
  When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs, which can also cause hot buckets to roll.                                                                                     |
| maxHotIdleSecs      | Maximum life, in seconds, of a hot bucket. Defaults to 0. A value of 0 turns off the idle check (equivalent to INFINITE idle time).  
  If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll.                                                                                                                                       |
| maxHotSpanSecs      | Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).  
  Note: If set too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.                                                                 |
| maxMemMB            | The amount of memory, in MB, allocated for indexing.  
  This is a global setting, not a per index setting.                                                                                                                                                                                                                                                                                                                                                                                                                        |
| maxMetaEntries      | Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite).  
  If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the punct field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README).  
  There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.                                                                 |

589
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxTimeUnreplicatedNoAcks</td>
<td>Upper limit, in seconds, on how long an event can sit in raw slice. Applies only if replication is enabled for this index. Otherwise ignored. If there are any acknowledged events sharing this raw slice, this parameter does not apply. In this case, maxTimeUnreplicatedWithAcks applies. Highest legal value is 2147483647. To disable this parameter, set to 0. Note: this is an advanced parameter. Understand the consequences before changing.</td>
</tr>
<tr>
<td>maxTimeUnreplicatedWithAcks</td>
<td>Upper limit, in seconds, on how long events can sit unacknowledged in a raw slice. Applies only if you have enabled acks on forwarders and have replication enabled (with clustering). Note: This is an advanced parameter. Make sure you understand the settings on all forwarders before changing this. This number should not exceed ack timeout configured on any forwarder, and should actually be set to at most half of the minimum value of that timeout. You can find this setting in outputs.conf readTimeout setting under the tcpout stanza. To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.</td>
</tr>
<tr>
<td>maxTotalDataSizeMB</td>
<td>The maximum size of an index, in MB.</td>
</tr>
<tr>
<td>maxWarmDBCount</td>
<td>The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times are moved to cold.</td>
</tr>
<tr>
<td>memPoolMB</td>
<td>Determines how much memory is given to the indexer memory pool. This is a global setting, not a per-index setting.</td>
</tr>
<tr>
<td>minRawFileSyncSecs</td>
<td>Can be either an integer (or &quot;disable&quot;). Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed. The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files. If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying &quot;disable&quot; disables syncing entirely: uncompressed slices are removed as soon as compression is complete.</td>
</tr>
<tr>
<td>minStreamGroupQueueSize</td>
<td>Minimum size of the queue that stores events in memory before committing them to a tsidx file.</td>
</tr>
<tr>
<td>minTime</td>
<td>ISO8601 timestamp of the oldest event time in the index.</td>
</tr>
<tr>
<td>partialServiceMetaPeriod</td>
<td>Related to serviceMetaPeriod. By default it is turned off (zero). If set, it enables metadata sync every &lt;integer&gt; seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync’ed at serviceMetaPeriod.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>partialServiceMetaPeriod</td>
<td>Specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.</td>
</tr>
<tr>
<td>processTrackerServiceInterval</td>
<td>How often, in seconds, the indexer checks the status of the child OS processes it launched to see if it can launch new processes for queued requests.</td>
</tr>
<tr>
<td>quarantineFutureSecs</td>
<td>Events with timestamp of quarantineFutureSecs newer than &quot;now&quot; are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>quarantinePastSecs</td>
<td>Events with timestamp of quarantinePastSecs older than &quot;now&quot; are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>rawChunkSizeBytes</td>
<td>Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, rawChunkSizeBytes is set to the default value. <strong>Note:</strong> rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. <strong>Warning:</strong> This is an advanced parameter. Only change it if instructed to do so by Splunk Support.</td>
</tr>
<tr>
<td>repFactor</td>
<td>Index replication control. This parameter applies to only clustering slaves. <strong>auto</strong> = Use the master index replication configuration value. <strong>0</strong> = Turn off replication for this index.</td>
</tr>
<tr>
<td>rotatePeriodInSecs</td>
<td>Rotation period, in seconds, that specifies how frequently to check: • If a new hot bucket needs to be created. • If there are any cold buckets that should be frozen. • If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.</td>
</tr>
<tr>
<td>serviceMetaPeriod</td>
<td>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.</td>
</tr>
<tr>
<td>suppressBannerList</td>
<td>List of indexes for which we suppress &quot;index missing&quot; warning banner messages. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>sync</td>
<td>Specifies the number of events that trigger the indexer to sync events. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>syncMeta</td>
<td>When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>thawedPath</td>
<td>Filepath to the thawed (resurrected) databases for the index.</td>
</tr>
<tr>
<td>thawedPath_expanded</td>
<td>Absolute filepath to the thawed (resurrected) databases.</td>
</tr>
<tr>
<td>throttleCheckPeriod</td>
<td>Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).</td>
</tr>
<tr>
<td>Note: Do not change this parameter without the input of Splunk Support.</td>
<td></td>
</tr>
<tr>
<td>totalEventCount</td>
<td>Total number of events in the index.</td>
</tr>
<tr>
<td>tsstatsHomePath</td>
<td>Location where datamodel acceleration TSIDX data for this index is stored.</td>
</tr>
<tr>
<td>warmToColdScript</td>
<td>Script to run when moving data from warm to cold. See input parameter description for details.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/indexes -d name=Shadow
```

**XML Response**

```xml
d...<entry><id>https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow</id><updated>2011-05-13T13:09:27-07:00</updated><link href="/servicesNS/nobody/search/data/indexes/shadow" rel="alternate"/>
```

<s:dict>
<s:key name="assureUTF8">0</s:key>
<s:key name="blockSignatureDatabase">_blocksignature</s:key>
<s:key name="coldPath">$SPLUNK_DB/shadow/colddb</s:key>
<s:key name="coldPath_expanded">/Applications/splunk/var/lib/splunk/shadow/colddb</s:key>
<s:key name="coldToFrozenDir"></s:dict>
```
data/indexes/{name}

https://<host>:<mPort>/services/data/indexes/{name}

Access, update, or delete the {name} index.

DELETE

Removes the {name} index and the data contained in it.

Usage details
Before executing this operation, look through all inputs.conf files (on the indexer and on any forwarders sending data to the indexer) and make sure that none of the stanzas are directing data to the index that you plan to delete.
For example, if you want to delete an index called nogood, make sure the attribute/value pair index=nogood does not appear in any input stanzas. Once the index is deleted, Splunk software discards any data sent to that index.

The method returns HTTP status code 409 if the \{name\} index was disabled but Splunk Enterprise was not restarted. Restart Splunk Enterprise and try again.

For information on deleting indexes and deleting data from indexes, refer to Remove indexes and indexed data in Managing Indexers and Clusters of Indexers.

**Request parameters**
None

**Returned values**
None

**Example request and response**

**XML Request**

curl -k -u admin:pass --request DELETE https://localhost:8089/services/data/indexes/shadow

**XML Response**

..
..
..  
<title>indexes</title>
<id>https://localhost:8089/services/data/indexes</id>
<updated>2012-08-02T11:10:16-07:00</updated>
<generator build="131547" version="5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/indexes/_new" rel="create"/>
<link href="/services/data/indexes/_reload" rel="_reload"/>
  ... opensearch elements elided ...
<s:messages/>

**GET**

Access information about the \{name\} index.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summarize</td>
<td>Boolean</td>
<td>false</td>
<td>[Optional] Response type: true = Summarized response, omitting some index details, providing a faster response. false = full response.</td>
</tr>
</tbody>
</table>

**Returned values**
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>assureUTF8</strong></td>
<td>Indicates whether all data retrieved from the index is proper UTF8. If enabled (set to True), degrades indexing performance.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td><strong>blockSignSize</strong></td>
<td>Controls how many events make up a block for block signatures.</td>
</tr>
<tr>
<td></td>
<td>If this is set to 0, block signing is disabled for this index. Adam recommended value is 100.</td>
</tr>
<tr>
<td><strong>blockSignatureDatabase</strong></td>
<td>The index that stores block signatures of events.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td><strong>bloomfilterTotalSizeKB</strong></td>
<td>Total size of all Bloom filter files, in KB.</td>
</tr>
<tr>
<td><strong>coldPath</strong></td>
<td>Filepath to the cold databases for the index.</td>
</tr>
<tr>
<td><strong>coldPath_expanded</strong></td>
<td>Absolute filepath to the cold databases.</td>
</tr>
<tr>
<td><strong>coldToFrozenDir</strong></td>
<td>Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory.</td>
</tr>
<tr>
<td></td>
<td>Bucket freezing policy is as follows:</td>
</tr>
<tr>
<td></td>
<td>• New style buckets (4.2 and on): removes all files but the rawdata</td>
</tr>
<tr>
<td></td>
<td>To thaw, run <code>splunk rebuild &lt;bucket dir&gt;</code> on the bucket, then move to the thawed directory</td>
</tr>
<tr>
<td></td>
<td>• Old style buckets (Pre-4.2): gzip all the .data and .tsidx files</td>
</tr>
<tr>
<td></td>
<td>To thaw, unzip the zipped files and move the bucket into the thawed directory</td>
</tr>
<tr>
<td></td>
<td>If both coldToFrozenDir and coldToFrozenScript are specified, coldToFrozenDir takes precedence.</td>
</tr>
<tr>
<td><strong>coldToFrozenScript</strong></td>
<td>Path to the archiving script.</td>
</tr>
<tr>
<td></td>
<td>See the POST parameter description for details.</td>
</tr>
<tr>
<td><strong>compressRawdata</strong></td>
<td>This value is ignored. splunkd process always compresses raw data.</td>
</tr>
<tr>
<td><strong>currentDBSizeMB</strong></td>
<td>Total size, in MB, of data stored in the index. The total includes data in the home, cold and thawed paths.</td>
</tr>
<tr>
<td><strong>defaultDatabase</strong></td>
<td>If no index destination information is available in the input data, the index shown here is the destination of such data.</td>
</tr>
<tr>
<td><strong>disabled</strong></td>
<td>Indicates if the index is disabled.</td>
</tr>
<tr>
<td><strong>enableRealtimeSearch</strong></td>
<td>Indicates if this is a real-time search.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td><strong>frozenTimePeriodInSecs</strong></td>
<td>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).</td>
</tr>
<tr>
<td></td>
<td>Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>homePath</td>
<td>An absolute path that contains the hot and warm buckets for the index.</td>
</tr>
<tr>
<td>homePath_expanded</td>
<td>An absolute filepath to the hot and warm buckets for the index.</td>
</tr>
<tr>
<td>indexThreads</td>
<td>Number of threads used for indexing.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>isInternal</td>
<td>Indicates if this is an internal index (for example, _internal, _audit).</td>
</tr>
<tr>
<td>lastInitTime</td>
<td>Last time the index processor was successfully initialized.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>maxConcurrentOptimizes</td>
<td>The number of concurrent optimize processes that can run against a hot bucket.</td>
</tr>
<tr>
<td></td>
<td>This number should be increased if instructed by Splunk Support. Typically the default value should suffice.</td>
</tr>
<tr>
<td>maxDataSize</td>
<td>The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying &quot;auto&quot; or &quot;auto_high_volume&quot; causes Splunk software to autotune this parameter (recommended). Use &quot;auto_high_volume&quot; for high volume indexes (such as the main index); otherwise, use &quot;auto&quot;. A &quot;high volume index&quot; is typically one that gets over 10GB of data per day.</td>
</tr>
<tr>
<td></td>
<td>• “auto” sets the size to 750MB.</td>
</tr>
<tr>
<td></td>
<td>• “auto_high_volume” sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.</td>
</tr>
<tr>
<td></td>
<td>Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding.</td>
</tr>
<tr>
<td></td>
<td>If you specify an invalid number or string, maxDataSize is auto-tuned.</td>
</tr>
<tr>
<td></td>
<td>Note: The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.</td>
</tr>
<tr>
<td>maxHotBuckets</td>
<td>Maximum hot buckets that can exist per index. Defaults to 3.</td>
</tr>
<tr>
<td></td>
<td>When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs, which can also cause hot buckets to roll.</td>
</tr>
<tr>
<td>maxHotIdleSecs</td>
<td>Maximum life, in seconds, of a hot bucket. Defaults to 0. A value of 0 turns off the idle check (equivalent to INFINITE idle time).</td>
</tr>
<tr>
<td></td>
<td>If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll.</td>
</tr>
<tr>
<td>maxHotSpanSecs</td>
<td>Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).</td>
</tr>
<tr>
<td></td>
<td>Note: If set too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>maxMemMB</strong></td>
<td>The amount of memory, in MB, allocated for indexing. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td><strong>maxMetaEntries</strong></td>
<td>Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite).</td>
</tr>
<tr>
<td></td>
<td>If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the punct field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README).</td>
</tr>
<tr>
<td></td>
<td>There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.</td>
</tr>
<tr>
<td><strong>maxRunningProcessGroups</strong></td>
<td>Maximum number of processes that the indexer fires off at a time. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td><strong>maxTime</strong></td>
<td>UNIX timestamp of the newest event time in the index.</td>
</tr>
<tr>
<td><strong>maxTotalDataSizeMB</strong></td>
<td>The maximum size of an index, in MB.</td>
</tr>
<tr>
<td><strong>maxWarmDBCount</strong></td>
<td>Maximum number of warm buckets.</td>
</tr>
<tr>
<td><strong>memPoolMB</strong></td>
<td>Determines how much memory is given to the indexer memory pool. This is a global setting, not a per-index setting.</td>
</tr>
<tr>
<td></td>
<td>Can be either an integer (or &quot;disable&quot;). Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed</td>
</tr>
<tr>
<td></td>
<td>The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices.</td>
</tr>
<tr>
<td></td>
<td>During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files.</td>
</tr>
<tr>
<td></td>
<td>If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying &quot;disable&quot; disables syncing entirely: uncompressed slices are removed as soon as compression is complete.</td>
</tr>
<tr>
<td><strong>minRawFileSyncSecs</strong></td>
<td>UNIX timestamp of the oldest event time in the index.</td>
</tr>
<tr>
<td><strong>numBloomfilters</strong></td>
<td>The number of Bloom filters created for this index.</td>
</tr>
<tr>
<td><strong>numHotBuckets</strong></td>
<td>The number of hot buckets created for this index.</td>
</tr>
<tr>
<td><strong>numWarmBuckets</strong></td>
<td>The number of warm buckets created for this index.</td>
</tr>
<tr>
<td><strong>partialServiceMetaPeriod</strong></td>
<td>Related to serviceMetaPeriod. By default it is turned off (zero). If set, it enables metadata sync every &lt;integer&gt; seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records</td>
</tr>
</tbody>
</table>

597
that require full re-write are be sync'ed at serviceMetaPeriod.

partialServiceMetaPeriod specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>quarantineFutureSecs</td>
<td>Events with timestamp of quarantineFutureSecs newer than “now” that are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>quarantinePastSecs</td>
<td>Events with timestamp of quarantinePastSecs older than “now” are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>rawChunkSizeBytes</td>
<td>Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, rawChunkSizeBytes is set to the default value. Note: rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. Warning: This is an advanced parameter. Only change it if instructed to do so by Splunk Support.</td>
</tr>
</tbody>
</table>
| rotatePeriodInSecs | Rotation period, in seconds, that specifies how frequently to check:  
  • If a new hot bucket needs to be created.  
  • If there are any cold buckets that should be frozen.  
  • If there are any buckets that need to be moved out hot and cold DBs, due to size constraints. |
| serviceMetaPeriod | Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path. |
| summarize         | If true, leaves out certain index details, which provides a faster response.                                                                                                                                 |
| suppressBannerList | List of indexes for which we suppress “index missing” warning banner messages. This is a global setting, not a per index setting.                                                                                 |
| sync              | Specifies the number of events that trigger the indexer to sync events. This is a global setting, not a per index setting.                                                                                     |
| syncMeta          | When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. Note: Do not change this parameter without the input of Splunk Support. |
| thawedPath        | An absolute path that contains the thawed (resurrected) databases for the index.                                                                                                                            |
| thawedPath_expanded | Absolute filepath to the thawed (resurrected) databases.                                                                                                                                                      |
### throttleCheckPeriod

Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).

**Note:** Do not change this parameter without the input of Splunk Support.

### totalEventCount

Total number of events in the index.

---

#### Example request and response

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow
```

**XML Response**

```
...<title>indexes</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/indexes</id>
<updated>2011-08-01T12:25:34-07:00</updated>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/data/indexes/_new" rel="create"/>
<link href="/servicesNS/nobody/search/data/indexes/_reload" rel="_reload"/>
  ... opensearch elements elided ...
<s:messages/>
<entry>
  <title>shadow</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow</id>
  <updated>2011-08-01T11:47:55-07:00</updated>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/data/indexes/shadow" rel="alternate"/>
  <link href="/servicesNS/nobody/search/data/indexes/shadow/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/indexes/shadow/_edit" rel="edit"/>
  <link href="/servicesNS/nobody/search/data/indexes/shadow/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="assureUTF8">0</s:key>
      <s:key name="blockSignatureDatabase">_blocksignature</s:key>
      <s:key name="bloomFilterTotalSizeKB">0</s:key>
      <s:key name="coldPath">$SPLUNK_DB/shadow/colddb</s:key>
      <s:key name="coldPath_expanded">/home/amrit/bin/splunk-current/var/lib/splunk/shadow/colddb</s:key>
      <s:key name="coldToFrozenDir"/>
      <s:key name="compressRawdata">1</s:key>
      <s:key name="defaultDatabase">main</s:key>
      <s:key name="disabled">0</s:key>
      ...eai:acl element elided ...
    </s:dict>
```
<s:dict>
  <s:key name="optionalFields">
    <s:list>
      <s:item>assureUTF8</s:item>
      <s:item>blockSignSize</s:item>
      <s:item>coldToFrozenDir</s:item>
      <s:item>coldToFrozenScript</s:item>
      <s:item>compressRawdata</s:item>
      <s:item>frozenTimePeriodInSecs</s:item>
      <s:item>maxConcurrentOptimizes</s:item>
      <s:item>maxDataSize</s:item>
      <s:item>maxHotBuckets</s:item>
      <s:item>maxHotIdleSecs</s:item>
      <s:item>maxHotSpanSecs</s:item>
      <s:item>maxMemMB</s:item>
      <s:item>maxMetaEntries</s:item>
      <s:item>maxRunningProcessGroups</s:item>
      <s:item>maxTotalDataSizeMB</s:item>
      <s:item>minRawFileSyncSecs</s:item>
      <s:item>partialServiceMetaPeriod</s:item>
      <s:item>quarantineFutureSecs</s:item>
      <s:item>quarantinePastSecs</s:item>
      <s:item>rawChunkSizeBytes</s:item>
      <s:item>rotatePeriodInSecs</s:item>
      <s:item>serviceMetaPeriod</s:item>
      <s:item>suppressBannerList</s:item>
      <s:item>syncMeta</s:item>
      <s:item>throttleCheckPeriod</s:item>
    </s:list>
  </s:key>
  <s:key name="requiredFields">
    <s:list/>
  </s:key>
  <s:key name="wildcardFields">
    <s:list/>
  </s:key>
  <s:dict>
    <s:key name="enableRealtimeSearch">1</s:key>
    <s:key name="frozenTimePeriodInSecs">188697600</s:key>
    <s:key name="homePath">$SPLUNK_DB/shadow/db</s:key>
    <s:key name="homePath_expanded">/home/amrit/bin/splunk-current/var/lib/splunk/shadow/db</s:key>
    <s:key name="indexThreads">auto</s:key>
    <s:key name="isInternal">0</s:key>
    <s:key name="lastInitTime">1312226552.102920</s/key>
    <s:key name="maxConcurrentOptimizes">3</s:key>
    <s:key name="maxDataSize">auto</s:key>
    <s:key name="maxHotBuckets">3</s:key>
    <s:key name="maxHotIdleSecs">0</s:key>
    <s:key name="maxHotSpanSecs">7776000</s:key>
    <s:key name="maxMemMB">5</s:key>
    <s:key name="maxMetaEntries">1000000</s:key>
    <s:key name="maxRunningProcessGroups">20</s:key>
    <s:key name="maxTime"/>
    <s:key name="maxTotalDataSizeMB">500000</s/key>
    <s:key name="maxWarmDBCount">300</s:key>
    <s:key name="memPoolMB">auto</s:key>
    <s:key name="minRawFileSyncSecs">disable</s:key>
    <s:key name="minTime"/>
    <s:key name="numBloomfilters">0</s:key>
    <s:key name="numHotBuckets">0</s:key>
    <s:key name="numWarmBuckets">0</s:key>
  </s:dict>
</s:dict>
POST

Updates the \{name\} index.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blockSignSize</td>
<td>Number</td>
<td>0</td>
<td>Controls how many events make up a block for block signatures.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If this is set to 0, block signing is disabled for this index.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A recommended value is 100.</td>
</tr>
<tr>
<td>bucketRebuildMemoryHint</td>
<td>String</td>
<td>auto</td>
<td>Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Caution</strong>: This is an advanced parameter. Inappropriate use of this parameter causes splunkd to not start if rebuild is required. <em>Do not set this parameter unless instructed by Splunk Support.</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value, auto, varies by the amount of physical RAM on the host</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• less than 2GB RAM = 67108864 (64MB) tsidx</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 2GB to 8GB RAM = 134217728 (128MB) tsidx</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• more than 8GB RAM = 268435456 (256MB) tsidx</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Values other than &quot;auto&quot; must be 16MB-1GB. Highest legal value (of the numerical part) is 4294967295</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>You can specify the value using a size suffix: &quot;16777216&quot; or &quot;16MB&quot; are equivalent.</td>
</tr>
<tr>
<td>coldToFrozenDir</td>
<td>String</td>
<td></td>
<td>Destination path for the frozen archive. Use as an alternative to a coldToFrozenScript. Splunk software automatically puts frozen buckets in this directory.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Bucket freezing policy is as follows:</td>
</tr>
</tbody>
</table>
New style buckets (4.2 and on): removes all files but the rawdata

To thaw, run `splunk rebuild <bucket dir>` on the bucket, then move to the thawed directory

Old style buckets (Pre-4.2): gzip all the .data and .tsidx files

To thaw, gunzip the zipped files and move the bucket into the thawed directory

If both `coldToFrozenDir` and `coldToFrozenScript` are specified, `coldToFrozenDir` takes precedence

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| `coldToFrozenScript` | String    |         | Path to the archiving script. If your script requires a program to run it (for example, python), specify the program followed by the path. The script must be in `$SPLUNK_HOME/bin` or one of its subdirectories. Splunk software ships with an example archiving script in `$SPLUNK_HOME/bin` called `coldToFrozenExample.py`. DO NOT use this example script directly. It uses a default path, and if modified in place any changes are overwritten on upgrade. It is best to copy the example script to a new file in bin and modify it for your system. Most importantly, change the default archive path to an existing directory that fits your needs. If your new script in bin/ is named `myColdToFrozen.py`, set this key to the following:

```
coldToFrozenScript = "`${SPLUNK_HOME}/bin/python` ""`$SPLUNK_HOME/bin/myColdToFrozen.py`"
```

By default, the example script has two possible behaviors when archiving:

- For buckets created from version 4.2 and on, it removes all files except for rawdata. To thaw: cd to the frozen bucket and type `splunk rebuild .`, then copy the bucket to thawed for that index. We recommend using the `coldToFrozenDir` parameter unless you need to perform a more advanced operation upon freezing buckets.
- For older-style buckets, we simply gzip all the .tsidx files. To thaw: cd to the frozen bucket and unzip the tsidx files, then copy the bucket to thawed for that index.

<table>
<thead>
<tr>
<th>compressRawdata</th>
<th>Boolean</th>
<th>true</th>
<th>This parameter is ignored. The splunkd process always compresses raw data.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>enableOnlineBucketRepair</code></td>
<td>Boolean</td>
<td>true</td>
<td>Enables asynchronous &quot;online fsck&quot; bucket repair, which runs concurrently with Splunk software. When enabled, you do not have to wait until buckets are repaired to start Splunk Enterprise. However, you might observe a slight performance degratation.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>frozenTimePeriodInSecs</td>
<td>Number</td>
<td>188697600</td>
<td>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years). Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.</td>
</tr>
<tr>
<td>maxBloomBackfillBucketAge</td>
<td>Number</td>
<td>30d</td>
<td>Valid values are: Integer[m</td>
</tr>
<tr>
<td>maxConcurrentOptimizes</td>
<td>Number</td>
<td>6</td>
<td>The number of concurrent optimize processes that can run against a hot bucket. This number should be increased if instructed by Splunk Support. Typically the default value should suffice.</td>
</tr>
<tr>
<td>maxDataSize</td>
<td>Number</td>
<td>auto</td>
<td>The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying &quot;auto&quot; or &quot;auto_high_volume&quot; causes Splunk software to autotune this parameter (recommended). Use &quot;auto_high_volume&quot; for high volume indexes (such as the main index); otherwise, use &quot;auto&quot;. A &quot;high volume index&quot; would typically be considered one that gets over 10GB of data per day. Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range should be approved by Splunk Support before proceeding. If you specify an invalid number or string, maxDataSize is auto-tuned. <strong>Note:</strong> The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.</td>
</tr>
<tr>
<td>maxHotBuckets</td>
<td>Number</td>
<td>3</td>
<td>Maximum hot buckets that can exist per index. Defaults to 3. When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs, which can also cause hot buckets to roll.</td>
</tr>
<tr>
<td>maxHotIdleSecs</td>
<td>Number</td>
<td>0</td>
<td>Maximum life, in seconds, of a hot bucket. Defaults to 0.</td>
</tr>
</tbody>
</table>
If a hot bucket exceeds `maxHotIdleSecs`, Splunk software rolls it to warm. This setting operates independently of `maxHotBuckets`, which can also cause hot buckets to roll. A value of 0 turns off the idle check (equivalent to INFINITE idle time).

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| `maxHotSpanSecs`  | Number  | 7776000 | Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days).  
*Note:* If you set this too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data. |
| `maxMemMB`        | Number  | 5       | The amount of memory, expressed in MB, to allocate for buffering a single tsidx file into memory before flushing to disk. Defaults to 5. The default is recommended for all environments. |
|                   |         |         | **IMPORTANT:** Calculate this number carefully. Setting this number incorrectly may have adverse effects on your systems memory and/or splunkd stability/performance. |
| `maxMetaEntries`  | Number  | 1000000 | Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite).  
If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the `punct` field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README). |
|                   |         |         | There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant. |
| `maxTimeUnreplicatedNoAcks` | Number | 300     | Upper limit, in seconds, on how long an event can sit in raw slice. Applies only if replication is enabled for this index. Otherwise ignored.  
If there are any acknowledged events sharing this raw slice, this parameter does not apply. In this case, `maxTimeUnreplicatedWithAcks` applies. |
| `maxTimeUnreplicatedWithAcks` | Number | 60      | Upper limit, in seconds, on how long events can sit unacknowledged in a raw slice. Applies only if you have enabled acks on forwarders and have replication enabled (with clustering).  
*Note:* This is an advanced parameter. Make sure you understand the settings on all forwarders before changing this. This number should not... |
exceed ack timeout configured on any forwarder, and should actually be set to at most half of the minimum value of that timeout. You can find this setting in outputs.conf readTimeout setting under the tcpout stanza.

To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxTotalDataSizeMB</td>
<td>Number</td>
<td>500000</td>
<td>The maximum size of an index (in MB). If an index grows larger than the maximum size, the oldest data is frozen.</td>
</tr>
<tr>
<td>maxWarmDBCount</td>
<td>Number</td>
<td>300</td>
<td>The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times are moved to cold.</td>
</tr>
<tr>
<td>minRawFileSyncSecs</td>
<td>Number</td>
<td>disable</td>
<td>Specify an integer (or &quot;disable&quot;) for this parameter. This parameter sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files. If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying &quot;disable&quot; disables syncing entirely: uncompressed slices are removed as soon as compression is complete. Note: Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed.</td>
</tr>
<tr>
<td>minStreamGroupQueueSize</td>
<td>Number</td>
<td>2000</td>
<td>Minimum size of the queue that stores events in memory before committing them to a tsidx file. Caution: Do not set this value, except under advice from Splunk Support.</td>
</tr>
<tr>
<td>partialServiceMetaPeriod</td>
<td>Number</td>
<td>0</td>
<td>Related to serviceMetaPeriod. If set, it enables metadata sync every &lt;integer&gt; seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync'ed at serviceMetaPeriod. partialServiceMetaPeriod specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect. By default it is turned off (zero).</td>
</tr>
<tr>
<td>processTrackerServiceInterval</td>
<td>Number</td>
<td>1</td>
<td>Specifies, in seconds, how often the indexer checks the status of the child OS processes it launched to see if it can launch new processes for queued requests. Defaults to 15. If set to 0, the indexer checks child process status every second.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Highest legal value is 4294967295.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>quarantineFutureSecs</strong></td>
<td>Number</td>
<td>2592000</td>
<td>Events with timestamp of <code>quarantineFutureSecs</code> newer than &quot;now&quot; are dropped into quarantine bucket. Defaults to 2592000 (30 days).</td>
</tr>
<tr>
<td>Events with timestamp of <code>quarantineFutureSecs</code> newer than &quot;now&quot; are dropped into quarantine bucket. Defaults to 2592000 (30 days).</td>
<td></td>
<td></td>
<td>This is a mechanism to prevent main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td><strong>quarantinePastSecs</strong></td>
<td>Number</td>
<td>7776000</td>
<td>Events with timestamp of <code>quarantinePastSecs</code> older than &quot;now&quot; are dropped into quarantine bucket. Defaults to 7776000 (900 days).</td>
</tr>
<tr>
<td>Events with timestamp of <code>quarantinePastSecs</code> older than &quot;now&quot; are dropped into quarantine bucket. Defaults to 7776000 (900 days).</td>
<td></td>
<td></td>
<td>This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td><strong>rawChunkSizeBytes</strong></td>
<td>Number</td>
<td>131072</td>
<td>Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value.</td>
</tr>
<tr>
<td>Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, <code>rawChunkSizeBytes</code> is set to the default value.</td>
<td></td>
<td></td>
<td>Note: <code>rawChunkSizeBytes</code> only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size.</td>
</tr>
<tr>
<td><strong>repFactor</strong></td>
<td>String</td>
<td>0</td>
<td>Index replication control. This parameter applies to only clustering slaves.</td>
</tr>
<tr>
<td>Index replication control. This parameter applies to only clustering slaves.</td>
<td></td>
<td></td>
<td><strong>auto</strong> = Use the master index replication configuration value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>0</strong> = Turn off replication for this index.</td>
</tr>
<tr>
<td><strong>rotatePeriodInSecs</strong></td>
<td>Number</td>
<td>60</td>
<td>How frequently (in seconds) to check if a new hot bucket needs to be created. Also, how frequently to check if there are any warm/cold buckets that should be rolled/frozen.</td>
</tr>
<tr>
<td>How frequently (in seconds) to check if a new hot bucket needs to be created. Also, how frequently to check if there are any warm/cold buckets that should be rolled/frozen.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>serviceMetaPeriod</strong></td>
<td>Number</td>
<td>25</td>
<td>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds).</td>
</tr>
<tr>
<td>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds).</td>
<td></td>
<td></td>
<td>You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.</td>
</tr>
<tr>
<td><strong>syncMeta</strong></td>
<td>Boolean</td>
<td>true</td>
<td>When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures.</td>
</tr>
<tr>
<td>When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures.</td>
<td></td>
<td></td>
<td><strong>Note</strong>: Do not change this parameter without the input of a Splunk Support.</td>
</tr>
<tr>
<td><strong>throttleCheckPeriod</strong></td>
<td>Number</td>
<td>15</td>
<td>Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).</td>
</tr>
<tr>
<td>Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).</td>
<td></td>
<td></td>
<td><strong>Note</strong>: Do not change this parameter without the input of Splunk Support.</td>
</tr>
<tr>
<td><strong>tstatsHomePath</strong></td>
<td>String</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Location to store datamodel acceleration TSIDX data for this index. Restart splunkd after changing this parameter.</td>
<td>If specified, it must be defined in terms of a volume definition.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Caution: Path must be writable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value: volume:_splunk_summaries/$_index_name/tstats</td>
</tr>
<tr>
<td>warmToColdScript</td>
<td>String</td>
<td>Path to a script to run when moving data from warm to cold.</td>
<td>This attribute is supported for backwards compatibility with Splunk software versions older than 4.0. Contact Splunk support if you need help configuring this setting. Caution: Migrating data across filesystems is now handled natively by splunkd. If you specify a script here, the script becomes responsible for moving the event data, and Splunk-native data migration are not used.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>assureUTF8</td>
<td>Boolean value indicating whether all data retrieved from the index is proper UTF8. If enabled (set to True), degrades indexing performance Can only be set globally.</td>
</tr>
<tr>
<td>blockSignSize</td>
<td>Controls how many events make up a block for block signatures. If this is set to 0, block signing is disabled for this index. A recommended value is 100.</td>
</tr>
<tr>
<td>blockSignatureDatabase</td>
<td>The index that stores block signatures of events. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>bucketRebuildMemoryHint</td>
<td>Suggestion for the bucket rebuild process for the size of the time-series (tsidx) file to make.</td>
</tr>
<tr>
<td>coldPath</td>
<td>Filepath to the cold databases for the index.</td>
</tr>
<tr>
<td>coldPath_expanded</td>
<td>Absolute filepath to the cold databases.</td>
</tr>
<tr>
<td>coldToFrozenDir</td>
<td>Destination path for the frozen archive. Used as an alternative to a coldToFrozenScript. Splunk Enterprise automatically puts frozen buckets in this directory. Bucket freezing policy is as follows: New style buckets (4.2 and on): removes all files but the rawdata To thaw, run <code>splunk rebuild &lt;bucket dir&gt;</code> on the bucket, then move to the thawed directory Old style buckets (Pre-4.2): gzip all the .data and .tsidx files</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>coldToFrozenScript</td>
<td>Path to the archiving script.</td>
</tr>
<tr>
<td></td>
<td>See the POST parameter description for details.</td>
</tr>
<tr>
<td>compressRawdata</td>
<td>This value is ignored. splunkd process always compresses raw data.</td>
</tr>
<tr>
<td>currentDBSizeMB</td>
<td>Total size, in MB, of data stored in the index. The total includes data in the home, cold and thawed paths.</td>
</tr>
<tr>
<td>defaultDatabase</td>
<td>If no index destination information is available in the input data, the index shown here is the destination of such data.</td>
</tr>
<tr>
<td>enableOnlineBucketRepair</td>
<td>Indicates whether to run asynchronous &quot;online fsck&quot; bucket repair, which runs in a process concurrently with Splunk software.</td>
</tr>
<tr>
<td>enableRealtimeSearch</td>
<td>Indicates if this is a real-time search.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>frozenTimePeriodInSecs</td>
<td>Number of seconds after which indexed data rolls to frozen. Defaults to 188697600 (6 years).</td>
</tr>
<tr>
<td></td>
<td>Freezing data means it is removed from the index. If you need to archive your data, refer to coldToFrozenDir and coldToFrozenScript parameter documentation.</td>
</tr>
<tr>
<td>homePath</td>
<td>An absolute path that contains the hot and warm buckets for the index.</td>
</tr>
<tr>
<td>homePath_expanded</td>
<td>An absolute filepath to the hot and warm buckets for the index.</td>
</tr>
<tr>
<td>indexThreads</td>
<td>Number of threads used for indexing.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>isInternal</td>
<td>Indicates if this is an internal index (for example, _internal, _audit).</td>
</tr>
<tr>
<td>lastInitTime</td>
<td>Last time the index processor was successfully initialized.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>maxBloomBackfillBucketAge</td>
<td>If a bucket (warm or cold) is older than this, Splunk Enterprise does not create (or re-create) its Bloom filter.</td>
</tr>
<tr>
<td>maxConcurrentOptimizes</td>
<td>The number of concurrent optimize processes that can run against a hot bucket.</td>
</tr>
<tr>
<td></td>
<td>This number should be increased if instructed by Splunk Support. Typically the default value should suffice.</td>
</tr>
<tr>
<td>maxDataSize</td>
<td>The maximum size in MB for a hot DB to reach before a roll to warm is triggered. Specifying &quot;auto&quot; or &quot;auto_high_volume&quot; causes Splunk software to autotune this parameter (recommended). Use &quot;auto_high_volume&quot; for high volume indexes (such as the main index); otherwise, use &quot;auto&quot;. A &quot;high volume index&quot; is typically one that gets over 10GB of data per day.</td>
</tr>
<tr>
<td></td>
<td>- &quot;auto&quot; sets the size to 750MB.</td>
</tr>
<tr>
<td></td>
<td>- &quot;auto_high_volume&quot; sets the size to 10GB on 64-bit, and 1GB on 32-bit systems.</td>
</tr>
<tr>
<td></td>
<td>Although the maximum value you can set this is 1048576 MB, which corresponds to 1 TB, a reasonable number ranges anywhere from 100 - 50000. Any number outside this range</td>
</tr>
</tbody>
</table>
should be approved by Splunk Support before proceeding.

If you specify an invalid number or string, maxDataSize is auto-tuned.

Note: The precise size of your warm buckets may vary from maxDataSize, due to post-processing and timing issues with the rolling policy.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maxHotBuckets</td>
<td>Maximum hot buckets that can exist per index. Defaults to 3. When maxHotBuckets is exceeded, Splunk software rolls the least recently used (LRU) hot bucket to warm. Both normal hot buckets and quarantined hot buckets count towards this total. This setting operates independently of maxHotIdleSecs, which can also cause hot buckets to roll.</td>
</tr>
<tr>
<td>maxHotIdleSecs</td>
<td>Maximum life, in seconds, of a hot bucket. Defaults to 0. A value of 0 turns off the idle check (equivalent to INFINITE idle time). If a hot bucket exceeds maxHotIdleSecs, Splunk software rolls it to warm. This setting operates independently of maxHotBuckets, which can also cause hot buckets to roll.</td>
</tr>
<tr>
<td>maxHotSpanSecs</td>
<td>Upper bound of target maximum timespan of hot/warm buckets in seconds. Defaults to 7776000 seconds (90 days). Note: If set too small, you can get an explosion of hot/warm buckets in the filesystem. The system sets a lower bound implicitly for this parameter at 3600, but this is an advanced parameter that should be set with care and understanding of the characteristics of your data.</td>
</tr>
<tr>
<td>maxMemMB</td>
<td>The amount of memory, in MB, allocated for indexing. This is a global setting, not a per index setting. Sets the maximum number of unique lines in .data files in a bucket, which may help to reduce memory consumption. If set to 0, this setting is ignored (it is treated as infinite). If exceeded, a hot bucket is rolled to prevent further increase. If your buckets are rolling due to Strings.data hitting this limit, the culprit may be the punct field in your data. If you do not use punct, it may be best to simply disable this (see props.conf.spec in $SPLUNK_HOME/etc/system/README). There is a small time delta between when maximum is exceeded and bucket is rolled. This means a bucket may end up with epsilon more lines than specified, but this is not a major concern unless excess is significant.</td>
</tr>
<tr>
<td>maxMetaEntries</td>
<td>UNIX timestamp of the newest event time in the index. maxTimeUnreplicatedNoAcks Upper limit, in seconds, on how long an event can sit in raw slice. Applies only if replication is enabled for this index. Otherwise ignored. If there are any acknowledged events sharing this raw slice, this parameter does not apply. In this case, maxTimeUnreplicatedWithAcks applies. The highest legal value is 2147483647. To disable this parameter, set to 0.</td>
</tr>
</tbody>
</table>

609
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>maxTimeUnreplicatedWithAcks</strong></td>
<td>Upper limit, in seconds, on how long events can sit unacknowledged in a raw slice. Applies only if you have enabled acks on forwarders and have replication enabled (with clustering). Note: This is an advanced parameter. Make sure you understand the settings on all forwarders before changing this. This number should not exceed ack timeout configured on any forwarder, and should actually be set to at most half of the minimum value of that timeout. You can find this setting in outputs.conf readTimeout setting under the tcpout stanza. To disable, set to 0, but this is NOT recommended. Highest legal value is 2147483647.</td>
</tr>
<tr>
<td><strong>maxTotalDataSizeMB</strong></td>
<td>The maximum size of an index, in MB.</td>
</tr>
<tr>
<td><strong>maxWarmDBCount</strong></td>
<td>The maximum number of warm buckets. If this number is exceeded, the warm bucket/s with the lowest value for their latest times are moved to cold.</td>
</tr>
<tr>
<td><strong>memPoolMB</strong></td>
<td>Determines how much memory is given to the indexer memory pool.</td>
</tr>
<tr>
<td></td>
<td>This is a global setting, not a per-index setting.</td>
</tr>
<tr>
<td><strong>minRawFileSyncSecs</strong></td>
<td>Can be either an integer (or &quot;disable&quot;). Some filesystems are very inefficient at performing sync operations, so only enable this if you are sure it is needed. The integer sets how frequently splunkd forces a filesystem sync while compressing journal slices. During this period, uncompressed slices are left on disk even after they are compressed. Then splunkd forces a filesystem sync of the compressed journal and removes the accumulated uncompressed files. If 0 is specified, splunkd forces a filesystem sync after every slice completes compressing. Specifying &quot;disable&quot; disables syncing entirely: uncompressed slices are removed as soon as compression is complete.</td>
</tr>
<tr>
<td><strong>minStreamGroupQueueSize</strong></td>
<td>Minimum size of the queue that stores events in memory before committing them to a tsidx file.</td>
</tr>
<tr>
<td><strong>minTime</strong></td>
<td>UNIX timestamp of the oldest event time in the index.</td>
</tr>
<tr>
<td><strong>partialServiceMetaPeriod</strong></td>
<td>Related to serviceMetaPeriod. By default it is turned off (zero). If set, it enables metadata sync every &lt;integer&gt; seconds, but only for records where the sync can be done efficiently in-place, without requiring a full re-write of the metadata file. Records that require full re-write are be sync’ed at serviceMetaPeriod. partialServiceMetaPeriod specifies, in seconds, how frequently it should sync. Zero means that this feature is turned off and serviceMetaPeriod is the only time when metadata sync happens. If the value of partialServiceMetaPeriod is greater than serviceMetaPeriod, this setting has no effect.</td>
</tr>
<tr>
<td><strong>processTrackerServiceInterval</strong></td>
<td>How often, in seconds, the indexer checks the status of the child OS processes it launched to see if it can launch new processes for queued requests.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>quarantineFutureSecs</td>
<td>Events with timestamp of quarantineFutureSecs newer than &quot;now&quot; are dropped into quarantine bucket. Defaults to 2592000 (30 days). This is a mechanism to prevent main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>quarantinePastSecs</td>
<td>Events with timestamp of quarantinePastSecs older than &quot;now&quot; are dropped into quarantine bucket. Defaults to 77760000 (900 days). This is a mechanism to prevent the main hot buckets from being polluted with fringe events.</td>
</tr>
<tr>
<td>rawChunkSizeBytes</td>
<td>Target uncompressed size in bytes for individual raw slice in the rawdata journal of the index. Defaults to 131072 (128KB). 0 is not a valid value. If 0 is specified, rawChunkSizeBytes is set to the default value. Note: rawChunkSizeBytes only specifies a target chunk size. The actual chunk size may be slightly larger by an amount proportional to an individual event size. Warning: This is an advanced parameter. Only change it if instructed to do so by Splunk Support.</td>
</tr>
<tr>
<td>repFactor</td>
<td>Index replication control. This parameter applies to only clustering slaves. auto = Use the master index replication configuration value. 0 = Turn off replication for this index.</td>
</tr>
<tr>
<td>rotatePeriodInSecs</td>
<td>Rotation period, in seconds, that specifies how frequently to check: If a new hot bucket needs to be created. If there are any cold buckets that should be frozen. If there are any buckets that need to be moved out hot and cold DBs, due to size constraints.</td>
</tr>
<tr>
<td>serviceMetaPeriod</td>
<td>Defines how frequently metadata is synced to disk, in seconds. Defaults to 25 (seconds). You may want to set this to a higher value if the sum of your metadata file sizes is larger than many tens of megabytes, to avoid the hit on I/O in the indexing fast path.</td>
</tr>
<tr>
<td>suppressBannerList</td>
<td>List of indexes for which we suppress &quot;index missing&quot; warning banner messages. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>sync</td>
<td>Specifies the number of events that trigger the indexer to sync events. This is a global setting, not a per index setting.</td>
</tr>
<tr>
<td>syncMeta</td>
<td>When true, a sync operation is called before file descriptor is closed on metadata file updates. This functionality improves integrity of metadata files, especially in regards to operating system crashes/machine failures. Note: Do not change this parameter without the input of Splunk Support.</td>
</tr>
<tr>
<td>thawedPath</td>
<td>Filepath to the thawed (resurrected) databases for the index.</td>
</tr>
<tr>
<td>thawedPath_expanded</td>
<td>Absolute filepath to the thawed (resurrected) databases.</td>
</tr>
<tr>
<td>throttleCheckPeriod</td>
<td>Defines how frequently Splunk software checks for index throttling condition, in seconds. Defaults to 15 (seconds).</td>
</tr>
</tbody>
</table>

611
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>totalEventCount</td>
<td>Total number of events in the index.</td>
</tr>
<tr>
<td>tstatsHomePath</td>
<td>Location where datamodel acceleration TSIDX data for this index is stored.</td>
</tr>
<tr>
<td>warmToColdScript</td>
<td>Script to run when moving data from warm to cold. See input parameter description for details.</td>
</tr>
</tbody>
</table>

Note: Do not change this parameter without the input of Splunk Support.

Example request and response

**XML Request**

curl -k -u admin:pass -d maxTotalDataSizeMB=400000
https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow

**XML Response**

```xml
...<title>indexes</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/indexes</id>
<updated>2011-05-16T12:06-07:00</updated>
<generator version="98392"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/data/indexes/_new" rel="create"/>
<link href="/servicesNS/nobody/search/data/indexes/_reload" rel="_reload"/>
... opensearch elements elided ...
<s:messages/>
<entry>
<title>shadow</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/indexes/shadow</id>
<updated>2011-05-16T12:18:56-07:00</updated>
<author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/data/indexes/shadow" rel="alternate"/>
<link href="/servicesNS/nobody/search/data/indexes/shadow/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/data/indexes/shadow/_edit" rel="edit"/>
<content type="text/xml">
<s:dict>
  <s:key name="assureUTF8">0</s:key>
  <s:key name="blockSignSize">0</s:key>
  <s:key name="blockSignatureDatabase">_blocksignature</s:key>
  <s:key name="coldPath">$SPLUNK_DB/shadow/colddb</s:key>
  <s:key name="coldPath_expanded">/Applications/splunk4.3/var/lib/splunk/shadow/colddb</s:key>
  <s:key name="coldToFrozenDir"></s:key>
  <s:key name="coldToFrozenScript"></s:key>
  <s:key name="compressRawdata">1</s:key>
  <s:key name="currentDBSizeMB">1</s:key>
  <s:key name="defaultDatabase">main</s:key>
  <s:key name="eai:acl"/>...
  <s:key name="enableRealtimeSearch">1</s:key>
  <s:key name="frozenTimePeriodInSecs">188697600</s:key>
</s:dict>
```
data/indexes-extended

https://<host>:<mPort>/services/data/indexes-extended

Access index bucket-level information. There are three bucket super-directories per index.

- home
- cold
- thawed

GET

List bucket attributes for all indexes.

Usage details
The default update period is 10 minutes, as defined by the collectionPeriodInSecs attribute in the
Note: At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

**Request parameters**

**Pagination and filtering parameters** can be used with this method.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>datatype</code></td>
<td>String</td>
<td>all</td>
<td>Valid values: (all</td>
</tr>
</tbody>
</table>

**Returned values**

- **bucket_dirs**
  - (If `total_size > 0`) Lists the following attributes for each index bucket super-directory (home, cold, thawed).
    - **bucket_count**: Number of buckets.
    - **event_count**: (If `size > 0`) Number of events in this bucket super-directory.
    - **event_max_time**: (If `size > 0`) Highest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called `latest time`.
    - **event_min_time**: (If `size > 0`) Lowest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called `earliest time`.
    - **hot_bucket_count**: (If `size > 0`) Number of hot buckets.
    - **size**: Size (fractional MB) on disk of this bucket super-directory.
    - **warm_bucket_count**: (If `size > 0`) Number of warm buckets.

- **name**: Index name.
- **total_bucket_count**: (If `total_size > 0`) Number of index buckets.
- **total_event_count**: (If `total_size > 0`) Number of events for index, excluding frozen events. Approximately equal to the `event_count` sum of all buckets.
- **total_raw_size**: (If `total_size > 0`) Cumulative size (fractional MB) on disk of the `<bucket>/rawdata/` directories of all buckets in this index, excluding frozen.
- **total_size**: Size (fractional MB) on disk of this index.

**Example request and response**

**XML Request**

```bash
curl -k -u admin:passwd https://localhost:8089/services/data/indexes-extended
```
Access bucket-level information for the `{name}` index. There are three bucket super-directories per index.

- home
- cold
- thawed

**GET**

Get `{name}` bucket information.

**Usage details**
The default update period is 10 minutes, as defined by the `collectionPeriodInSecs` attribute in the `$SPLUNK_HOME/etc/apps/introspection_generator_addon/default/server.conf` file.

*Note:* At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```
Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket_dirs</td>
<td>(If total_size &gt; 0) List the following attributes for each index bucket super-directory (home, cold, thawed) as indicated:</td>
</tr>
<tr>
<td>bucket_count</td>
<td>Number of buckets.</td>
</tr>
<tr>
<td>event_count</td>
<td>(If size &gt; 0) Number of events in this bucket super-directory.</td>
</tr>
<tr>
<td>event_max_time</td>
<td>(If size &gt; 0) Highest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called latest time.</td>
</tr>
<tr>
<td>event_min_time</td>
<td>(If size &gt; 0) Lowest time value (Unix epoch seconds) of all events in this bucket super-directory, commonly called earliest time.</td>
</tr>
<tr>
<td>hot_bucket_count</td>
<td>(If size &gt; 0) Number of hot buckets.</td>
</tr>
<tr>
<td>size</td>
<td>Size (fractional MB) on disk of this bucket super-directory.</td>
</tr>
<tr>
<td>warm_bucket_count</td>
<td>(If size &gt; 0) Number of warm buckets.</td>
</tr>
<tr>
<td>name</td>
<td>Index name.</td>
</tr>
<tr>
<td>total_bucket_count</td>
<td>(If total_size &gt; 0) Number of index buckets.</td>
</tr>
<tr>
<td>total_event_count</td>
<td>(If total_size &gt; 0) Number of events for index, excluding frozen events. Approximately equal to the event_count sum of all buckets.</td>
</tr>
<tr>
<td>total_raw_size</td>
<td>(If total_size &gt; 0) Cumulative size (fractional MB) on disk of the &lt;bucket&gt;/rawdata/ directories of all buckets in this index, excluding frozen.</td>
</tr>
<tr>
<td>total_size</td>
<td>Size (fractional MB) on disk of this index.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:passwd https://localhost:8089/services/data/indexes-extended/history

**XML Response**

```xml
...<title>introspection--disk-objects--indexes</title>
<id>https://localhost:8089/services/data/indexes-extended</id>
<updated>2014-03-31T12:42:29-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
  <name>Splunk</name>
</author>
... opensearch elements elided ...<s:messages/>
<entry>

617```
data/summaries

https://<host>:<mPort>/services/data/summaries
Get disk usage information about all summaries in an indexer.
GET

Gets current summary disk usage information.

Usage details
By default, this information is available five minutes after starting the Splunk deployment. Adjust this availability timing in server.conf.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>report_acceleration</td>
<td>Optional. Use &quot;report_acceleration=1&quot; to access disk usage by report acceleration summary.</td>
</tr>
<tr>
<td>data_model_acceleration</td>
<td>Optional. Use &quot;data_model_acceleration=1&quot; to access disk usage by data model acceleration summary.</td>
</tr>
</tbody>
</table>

Pagination and filtering parameters can be used with this method.

Returned values
For each summary, the following values are returned.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Summary name.</td>
</tr>
<tr>
<td>related_indexes</td>
<td>Lists up to 10 indexes that contribute to this summary.</td>
</tr>
<tr>
<td>related_indexes_count</td>
<td>Provides total count of related indexes for this summary.</td>
</tr>
<tr>
<td>search_head_guid</td>
<td>GUID for the search head that created the summary data.</td>
</tr>
<tr>
<td>total_bucket_count</td>
<td>Number of buckets for this summary.</td>
</tr>
<tr>
<td>total_size</td>
<td>Total disk size for this summary, in MB.</td>
</tr>
<tr>
<td>type</td>
<td>Summary type, either &quot;report_acceleration&quot; or &quot;data_model_acceleration&quot;.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u username:password https://localhost:8089/services/data/summaries

XML Response

...
<s:dict>
  <s:key name="can_write">1</s:key>
  <s:key name="modifiable">0</s:key>
  <s:key name="owner">system</s:key>
  <s:key name="perms"/>
  <s:dict>
    <s:key name="read">
      <s:list>
        <s:item>*</s:item>
      </s:list>
    </s:key>
    <s:key name="write"/>
    </s:dict>
    <s:key name="removable">0</s:key>
    <s:key name="sharing">system</s:key>
  </s:dict>
  <s:key name="name">search_admin_NS13c34e21cf577d62</s:key>
  <s:key name="related_indexes">_internal</s:key>
  <s:key name="related_indexes_count">1</s:key>
  <s:key name="search_head_guid">A6FF485E-7AA5-412D-8E03-BE3ED42BA327</s:key>
  <s:key name="total_bucket_count">9</s:key>
  <s:key name="total_size">2.000</s:key>
  <s:key name="type">report_acceleration</s:key>
</s:dict>

<entry>
<title>search_admin_NS6f37597da0cade4c</title>
{id>https://localhost:8089/services/data/summaries/search_admin_NS6f37597da0cade4c</id>
<updated>2015-09-16T16:05:35-07:00</updated>
<link href="/services/data/summaries/search_admin_NS6f37597da0cade4c" rel="alternate"/>
<author>
  <name>system</name>
</author>
<content type="text/xml">}
<s:dict>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app">
        <s:dict>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
        </s:dict>
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:key>
          <s:key name="write"/>
          </s:dict>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:dict>
    </s:dict>
</content>
data/summaries/{summary_name}

https://<host>:<mPort>/services/data/summaries/{summary_name}

Get disk usage information about the {name} indexer summary.

GET

Get disk usage information for the {name} summary.

Request parameters
None.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Summary name.</td>
</tr>
<tr>
<td>related_indexes</td>
<td>Lists up to 10 indexes that contribute to this summary.</td>
</tr>
<tr>
<td>related_indexes_count</td>
<td>Provides total count of related indexes for this summary.</td>
</tr>
<tr>
<td>search_head_guid</td>
<td>GUID for search head creating the summary data.</td>
</tr>
<tr>
<td>total_bucket_count</td>
<td>Number of buckets for this summary.</td>
</tr>
<tr>
<td>total_size</td>
<td>Total summary disk size in MB.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u username:password https://localhost:8089/services/data/summaries/my_summary
```

XML Response

```
```
server/health/deployment

https://<host>:<mPort>/services/server/health/deployment

Shows the overall health of a distributed deployment. The health of the deployment can be red, yellow, or green. The overall health of the deployment is based on the health of all features reporting to it.

Authentication and Authorization

Requires the admin role or list_health capability.

GET

Get the health status of a distributed deployment.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>health</td>
<td>String</td>
<td>Indicates the overall health of the deployment. Health status can be red, yellow, or green.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/server/health/deployment

XML Response

<title>deployment</title>

<id>https://localhost:8089/services/server/health/deployment</id>

<updated>1969-12-31T16:00:00-08:00</updated>

<author>
  <name>system</name>
</author>

<link href="/services/server/health/deployment" rel="alternate"/>

<link href="/services/server/health/deployment/details" rel="details"/>

<content type="text/xml">
  <s:dict>
    <s:key name="disabled">0</s:key>
    <s:key name="eai:acl"></s:dict>
    <s:dict>
      <s:key name="app"></s:keys>
      <s:key name="can_list">1</s:keys>
      <s:key name="can_write">1</s:keys>
      <s:key name="modifiable">0</s:keys>
      <s:key name="owner">system</s:keys>
  </content>
server/health/deployment/details

https://<host>:<mPort>/services/server/health/deployment/details
Shows the overall health of the distributed deployment, as well as each feature node and its respective color.

Authentication and Authorization

Requires the admin role or list_health capability.

GET

Get health status of distributed deployment features.

Request parameters
None

Returned values
<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>display_name</td>
<td>String</td>
<td>The name of the feature in the distributed health tree.</td>
</tr>
<tr>
<td>health</td>
<td>String</td>
<td>Indicates the color of the feature: red, yellow or green. The color of mid-level features defaults to the worst health status color of all features reporting to it.</td>
</tr>
<tr>
<td>reason</td>
<td>String</td>
<td>Descriptive string explaining the reason the indicator is non-green.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/services/server/health/deployment/details
```

**XML Response**

```
<title>health-report</title>
<id>https://mrt:9808/services/server/health</id>
<updated>2020-02-05T09:07:09-08:00</updated>
<generator build="e7558703e5bae4dc0cf8d06fa773eble75e23552" version="20200205"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>deployment</title>
  <id>https://mrt:9808/services/server/health/deployment</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/server/health/deployment" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/health/deployment" rel="list"/>
  <link href="/services/server/health/deployment/details" rel="details"/>
  <content type="text/xml">
    <s:dict>
      <s:dict name="disabled">0</s:dict>
      <s:dict name="eai:acl">
        <s:dict>
          <s:dict name="app">
            <s:dict name="can_list">1</s:dict>
            <s:dict name="can_write">1</s:dict>
            <s:dict name="modifiable">0</s:dict>
            <s:dict name="owner">system</s:dict>
            <s:dict name="perms">
              <s:dict name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:dict>
            </s:dict>
          </s:dict>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
```
<s:dict>
  <s:key name="features">
    <s:dict>
      <s:key name="health">green</s:key>
      <s:key name="num_red">0</s:key>
      <s:key name="num_yellow">0</s:key>
      <s:dict>
        <s:key name="file_monitor_input">
          <s:dict>
            <s:key name="batchreader-0">
              <s:dict>
                <s:key name="data_out_rate">
                  <s:dict>
                    <s:key name="description">"This indicator reflects the number of consecutive times the Batch File Reader was unable to insert data into Splunk's processing queues for a period of 5 seconds. By default, this indicator becomes Yellow when this input stalls for 5 seconds, and Red after 10 seconds.""</s:key>
                    <s:key name="name">data_out_rate</s:key>
                    <s:key name="path">splunkd.file_monitor_input.batchreader-0.data_out_rate</s:key>
                  </s:dict>
                </s:key>
                <s:key name="display_name">Batch Reader</s:key>
                <s:key name="health">green</s:key>
                <s:key name="num_red">0</s:key>
                <s:key name="num_yellow">0</s:key>
              </s:dict>
            </s:key>
            <s:key name="display_name">Batch Reader</s:key>
            <s:key name="health">green</s:key>
            <s:key name="num_red">0</s:key>
            <s:key name="num_yellow">0</s:key>
          </s:dict>
        </s:key>
        <s:key name="health">green</s:key>
        <s:key name="num_red">0</s:key>
        <s:key name="num_yellow">0</s:key>
      </s:dict>
      <s:key name="display_name">Tail Reader</s:key>
      <s:key name="health">green</s:key>
      <s:key name="num_red">0</s:key>
      <s:key name="num_yellow">0</s:key>
    </s:dict>
    <s:key name="tailreader-0">
      <s:dict>
        <s:key name="data_out_rate">
          <s:dict>
            <s:key name="description">"This indicator reflects the number of consecutive times the Tail File Reader was unable to insert data into Splunk's processing queues for a period of 5 seconds. By default, this indicator becomes Yellow when this input stalls for 5 seconds, and Red after 10 seconds.""</s:key>
            <s:key name="name">data_out_rate</s:key>
            <s:key name="path">splunkd.file_monitor_input.tailreader-0.data_out_rate</s:key>
          </s:dict>
        </s:key>
        <s:key name="display_name">Tail Reader</s:key>
        <s:key name="health">green</s:key>
        <s:key name="num_red">0</s:key>
        <s:key name="num_yellow">0</s:key>
      </s:dict>
    </s:key>
    <s:key name="health">green</s:key>
    <s:key name="index_processor">
      <s:dict>
        <s:key name="buckets">
          <s:dict>
            <s:key name="buckets_created_last_60m">
              627
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:key>
  </s:dict>
</s:dict>
This indicator gauges whether incoming data is being appropriately bucketed within the Splunk index. By default, Red occurs when any index has created more than 60 buckets within the last hour. A high rate of bucket creation can cause severe search performance degradation, and might indicate poorly configured data processing (for example, timestamping).

This indicator tracks the percentage of small buckets created over the last 24 hours. A small bucket is defined as less than 10% of the 'maxDataSize' setting in indexes.conf.

This indicator tracks whether all Splunk index filesystems contain sufficient free space to continue indexing. This calculation is based upon the 'minFreeSpace' setting in server.conf. By default, Yellow occurs when a filesystem's free space falls below (2* 'minFreeSpace'), and Red when it falls below 'minFreeSpace'.

This indicator tracks whether index optimization is falling behind. By default, this indicator becomes Yellow when 100% of the maximum allowed "splunk-optimize" processes are running.

628
This indicator checks whether there are any extremely lagged searches in the last hour. These are scheduled searches which have been unable to run within their configured interval. By default, this indicator is never Yellow, and is Red if there is at least 1 extremely lagged scheduled search. This is a numeric threshold rather than a percentage. Setting both thresholds to 0 will disable this indicator.

This indicator tracks the lag rate of high priority scheduled searches. Search lag is a delay that occurs before a search starts. High priority scheduled searches are scheduled searches whose priority is set to "higher" or "highest". By default, this indicator is yellow if the search lag rate exceeds 10%.

This indicator tracks the lag rate for scheduled searches whose priority is set to "default". Search lag is a delay that occurs before a search starts. By default, this indicator is yellow if the search lag rate over the last 24 hours exceeds 40%.
<s:dict>
  <s:key name="description">![CDATA[This indicator tracks the delayed search rate for high priority scheduled searches. These are scheduled searches where the priority field is set to "higher" or "highest". By default, this indicator is yellow if the delayed search ratio over the last 24 hours is 5%, and red if it is 10%.]]></s:key>
  <s:key name="name">percent_searches_delayed_high_priority_last_24h</s:key>
  <s:key name="path">splunkd.search_scheduler.searches_delayed.percent_searches_delayed_high_priority_last_24h</s:key>
</s:dict>

<s:dict>
  <s:key name="description">This indicator tracks the delayed search rate for scheduled searches whose priority field is set to "default". By default, this indicator is yellow if the delayed search ratio over the last 24 hours is 10%, and red if it is 20%.</s:key>
  <s:key name="name">percent_searches_delayed_non_high_priority_last_24h</s:key>
  <s:key name="path">splunkd.search_scheduler.searches_delayed.percent_searches_delayed_non_high_priority_last_24h</s:key>
</s:dict>

<s:dict>
  <s:key name="description">![CDATA[This indicator tracks the skip rate for high priority scheduled searches. These are scheduled searches where the priority field is set to "higher" or "highest". By default, this indicator is yellow if the skipped search ratio over the last 24 hours is 5%, and red if it is 10%.]]></s:key>
  <s:key name="name">percent_searches_skipped_high_priority_last_24h</s:key>
  <s:key name="path">splunkd.search_scheduler.searches_skipped.percent_searches_skipped_high_priority_last_24h</s:key>
</s:dict>

<s:dict>
  <s:key name="description">This indicator tracks the skip rate for scheduled searches whose priority field is set to "default". By default, this indicator is yellow if the skipped search ratio over the last 24 hours is 10%, and red if it is 20%.</s:key>
  <s:key name="name">percent_searches_skipped_non_high_priority_last_24h</s:key>
  <s:key name="path">splunkd.search_scheduler.searches_skipped.percent_searches_skipped_non_high_priority_last_24h</s:key>
</s:dict>
server/health/splunkd

https://<host>:<mPort>/services/server/health/splunkd
Shows the overall health of splunkd. The health of splunkd can be red, yellow, or green. The health of splunkd is based on the health of all features reporting to it.

Authentication and Authorization

Requires the admin role or list_health capability.

GET

Get the health status of splunkd.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>health</td>
<td>String</td>
<td>Indicates the overall health of splunkd. Health status can be red, yellow, or green.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/server/health/splunkd

XML Response

<title>health-report</title>
  <id>https://10.141.65.195:41405/services/server/health</id>
  <updated>2018-04-04T21:32:40+00:00</updated>
  <generator build="b233a6c1ade2" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/health/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <id>https://10.141.65.195:41405/services/server/health/splunkd</id>

631
server/health/splunkd/details

https://<host>:<mPort>/services/server/health/splunkd/details

Shows the overall health of the splunkd health status tree, as well as each feature node and its respective color. For unhealthy nodes (non-green), the output includes reasons, indicators, thresholds, messages, and so on.

Authentication and Authorization
Requires the **admin** role or **list_health** capability.

**GET**

Get health status of splunkd features.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>health</td>
<td>String</td>
<td>Indicate the color of the feature: red, yellow or green. The color of midlevel features is the worst color of all the features reporting to it.</td>
</tr>
<tr>
<td>messages</td>
<td>String</td>
<td>The last 50 messages from splunkd.log that might relate to the feature status change. Returned only if a feature color is not green.</td>
</tr>
<tr>
<td>reasons</td>
<td>String</td>
<td>Describes the indicator(s) that caused the feature's status to change to a non-green state. Returned only if a feature color is not green.</td>
</tr>
<tr>
<td>due_to_stanza</td>
<td>String</td>
<td>Indicates the stanza name in health.conf where the configuration for the non-green indicator exists.</td>
</tr>
<tr>
<td>due_to_threshold</td>
<td>String</td>
<td>Indicates the threshold because of which the color of the indicator is non-green.</td>
</tr>
<tr>
<td>due_to_threshold_value</td>
<td>Numeric</td>
<td>Indicates the value of the above threshold.</td>
</tr>
<tr>
<td>indicator</td>
<td>String</td>
<td>Name of the indicator because of which the feature is non-green.</td>
</tr>
<tr>
<td>reason</td>
<td>String</td>
<td>Descriptive string that explains the reason the indicator is non-green.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/server/health/splunkd/details
```

**XML Response**

```xml
<title>health-report</title>
<id>https://10.141.65.213:42270/services/server/health</id>
<updated>2018-04-03T20:05:34+00:00</updated>
<generator build="b233a6c1ade2" version="7.2.0"/>
<author>
  <name>Splunk</name>
</author>
<link rel="_acl" href="/services/server/health/_acl"/>
<s:messages/>
<entry>
  <title>splunkd</title>
```

633
<s:dict>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app"></s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">0</s:key>
      <s:key name="owner">system</s:key>
      <s:dict name="perms">
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>admin</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:key>
          <s:key name="write"></s:key>
        </s:dict>
      </s:dict>
      <s:key name="removable">0</s:key>
      <s:key name="sharing">system</s:key>
    </s:dict>
  </s:key>
  <s:key name="features">
    <s:dict>
      <s:key name="Data Forwarding">
        <s:dict>
          <s:dict name="Splunk-2-Splunk Forwarding">
            <s:dict name="features">
              <s:dict name="TCPOutAutoLB-0">
                <s:dict name="health">green</s:dict>
              </s:dict>
              <s:key name="health">green</s:key>
            </s:dict>
          </s:dict>
          <s:key name="File Monitor Input">
            <s:dict>
              <s:dict name="features">
                <s:dict name="Splunk-2-Splunk Forwarding">
                  <s:dict name="features">
                    <s:dict name="TCPOutAutoLB-0">
                      <s:dict name="health">green</s:dict>
                    </s:dict>
                    <s:key name="health">green</s:key>
                  </s:dict>
                </s:dict>
              </s:dict>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
</s:dict>
server/health-config

https://<host>..<mPort>/services/server/health-config

Endpoint to configure the splunkd health report.
Authentication and Authorization

Requires the admin role or list_health capability.

GET

List configuration information for the splunkd health report.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:password https://localhost:8089/services/server/health-config

XML Response

<entry>
  <title>alert_action:email</title>
  <id>https://localhost:8089/services/server/health-config/alert_action%3Aemail</id>
  <link href="/services/server/health-config/alert_action%3Aemail" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/health-config/alert_action%3Aemail" rel="list"/>
  <link href="/services/server/health-config/alert_action%3Aemail" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="action.cc">a@company.com, b@company.com</s:key>
      <s:key name="action.to">c@company.com</s:key>
    </s:dict>
  </content>
</entry>

<entry>
  <title>health_reporter</title>
  <id>https://localhost:8089/services/server/health-config/health_reporter</id>
  <link href="/services/server/health-config/health_reporter" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/health-config/health_reporter" rel="list"/>
  <link href="/services/server/health-config/health_reporter" rel="edit"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="alert.disabled">0</s:key>
    </s:dict>
  </content>
</entry>
server/health-config/{alert_action}

https://<host>:<mPort>/services/server/health-config/alert_action:<action_name>
Configure alert actions for the splunkd health report.

Authentication and Authorization

Requires the admin role or edit_health capability.

**POST**

Configure alert actions for the splunkd health report.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert_action:&lt;action_name&gt;</td>
<td>String</td>
<td>Specify the alert action name. &lt;action_name&gt; can be one of the following: [email</td>
</tr>
<tr>
<td>action.to</td>
<td>String</td>
<td>Primary email address to use with the email alert action.</td>
</tr>
<tr>
<td>action.cc</td>
<td>String</td>
<td>CC email address to use with the email alert action.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>action.bcc</td>
<td>String</td>
<td>BCC email address to use with the email alert action.</td>
</tr>
<tr>
<td>action.integration_url_override</td>
<td>String</td>
<td>Sets the <code>&lt;integration_key&gt;</code> value for PagerDuty alert action. For example <code>action.integration_url_override=78c3b6cf0a884a538410fe2812273b0b</code></td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>Enables/disables the alert action. Possible values are 0 and 1. A value of 1 disables the alert action.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/server/health-config/alert_action:email
-d action.to=admin@example.com -d action.cc=admin2@example.com -d disabled=0
```

XML Response

```
<title>health-report-config</title>
-id>https://10.141.65.179:52000/services/server/health-config</id>
<updated>2018-04-02T18:36:31+00:00</updated>
<generator build="b233a6c1ade2" version="7.2.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/health-config/_new" rel="create"/>
<link href="/services/server/health-config/_reload" rel="_reload"/>
<link href="/services/server/health-config/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```

server/health-config/{feature_name}

https://<host>:<mPort>/services/server/health-config/feature:<feature_name>
Edit feature- and indicator-level settings for the splunkd health report.

Authentication and Authorization

Requires the admin role or edit_health capability.

POST

Edit feature- and indicator-level settings for the splunkd health report.

Request parameters
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert.disabled</td>
<td>Boolean</td>
<td>Possible values are 0 or 1. A value of 1 disables alerting for this feature. If alerting is disabled in the [health_reporter] stanza, alerting for this feature is disabled, regardless of the value set here. If the value is set to 1, alerting or all indicators is disabled. Default: 0 (enabled).</td>
</tr>
<tr>
<td>alert.min_duration_sec</td>
<td>Number</td>
<td>The minimum amount of time, in seconds, that the health status color must persist before an alert triggers.</td>
</tr>
<tr>
<td>alert.threshold_color</td>
<td>String</td>
<td>The health status color that triggers an alert. Possible values are yellow and red. Default: red.</td>
</tr>
<tr>
<td>alert:&lt;indicator_name&gt;.disabled</td>
<td>Number</td>
<td>Possible values are 0 or 1. A value of 1 disables alerting for this indicator. Default: 0 (enabled).</td>
</tr>
<tr>
<td>alert:&lt;indicator_name&gt;.min_duration_sec</td>
<td>Number</td>
<td>The minimum amount of time, in seconds, that the health status color must persist before an alert triggers for this indicator.</td>
</tr>
<tr>
<td>alert:&lt;indicator_name&gt;.threshold_color</td>
<td>String</td>
<td>The health status color that triggers an alert for this indicator. Possible values are yellow and red. Default: red.</td>
</tr>
<tr>
<td>disable</td>
<td>Boolean</td>
<td>Disables/enables reporting the health of the feature. Use disabled=1 to disable the feature. Use disabled=0 to enable the feature.</td>
</tr>
<tr>
<td>feature:&lt;feature_name&gt;</td>
<td>String</td>
<td>Specify the feature name. feature_name can be any supported feature listed in $SPLUNK_HOME/etc/system/default/health.conf.</td>
</tr>
<tr>
<td>indicator:&lt;indicator name&gt;:&lt;color&gt;</td>
<td>Number</td>
<td>The indicator threshold value that triggers a health status change to the specified color for the indicator.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

**XML Request**

curl -k -u admin:password https://localhost:8089/services/server/health-config/feature:batchreader -d disabled=1 -d alert.disabled=0 -d alert.min_duration_sec=100 -d alert:data_out_rate.disabled=1 -d alert:data_out_rate.threshold_color=yellow

**XML Response**

```
<title>health-report-config</title>
<id>https://10.141.65.179:52000/services/server/health-config</id>
<updated>2018-04-02T18:36:31+00:00</updated>
<generator build="b233a6c1ade2" version="7.2.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/health-config/_new" rel="create"/>
<link href="/services/server/health-config/_reload" rel="_reload"/>
<link href="/services/server/health-config/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
```
server/info

https://<host>:<mPort>/services/server/info

Access information about the currently running Splunk instance.

**Note:** This endpoint provides information on the currently running Splunk instance. Some values returned in the GET response reflect server status information. However, this endpoint is meant to provide information on the currently running instance, not the machine where the instance is running. Server status values returned by this endpoint should be considered deprecated and might not continue to be accessible from this endpoint. Use `server/sysinfo` to access server status instead. For more information, see `server/sysinfo`.

**GET**

Get Splunk instance information.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activeLicenseGroup</td>
<td>Type of Splunk software license.</td>
</tr>
<tr>
<td></td>
<td>Enterprise</td>
</tr>
<tr>
<td></td>
<td>Forwarder</td>
</tr>
<tr>
<td></td>
<td>Free</td>
</tr>
<tr>
<td></td>
<td>Invalid</td>
</tr>
<tr>
<td></td>
<td>Trial</td>
</tr>
<tr>
<td>addOns</td>
<td>Names of active add-ons.</td>
</tr>
<tr>
<td>build</td>
<td>The build number for this Splunk instance version.</td>
</tr>
<tr>
<td>cpu_arch</td>
<td>The architecture type for the CPU hosting splunkd. The value returned in the server/info response should be considered deprecated. Use server/sysinfo to access this response key and value instead.</td>
</tr>
<tr>
<td>guid</td>
<td>Globally unique identifier for this server.</td>
</tr>
<tr>
<td>host</td>
<td>Server name.</td>
</tr>
<tr>
<td>host_fqdn</td>
<td>host fully-qualified domain name.</td>
</tr>
<tr>
<td>isFree</td>
<td>Indicates if this server is running the Splunk instance under a free license.</td>
</tr>
<tr>
<td>isTrial</td>
<td>Indicates if this server is using a trial license.</td>
</tr>
<tr>
<td>kv_store_status</td>
<td>App KV store availability.</td>
</tr>
<tr>
<td>license_labels</td>
<td>Labels associated with the license used on this server.</td>
</tr>
<tr>
<td>licenseKeys</td>
<td>License key unique for each license.</td>
</tr>
<tr>
<td>licenseSignature</td>
<td>Hash signature for the license used on this server.</td>
</tr>
<tr>
<td>licenseState</td>
<td>Specifies the status of the license, which can be either OK or Expired.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>master_guid</td>
<td>Globally unique identifier for this server.</td>
</tr>
<tr>
<td>max_users</td>
<td>Maximum number of users on the instance.</td>
</tr>
<tr>
<td>mode</td>
<td>Indicates whether the server is a dedicated forwarder. Possible values are: normal, dedicated FORWARDER</td>
</tr>
<tr>
<td>numberOfCores</td>
<td>Server number of processor cores. The value returned in the server/info response should be considered deprecated. Use server/sysinfo to access this response key and value instead.</td>
</tr>
<tr>
<td>os_build</td>
<td>Software build for the server os_version. The value returned in the server/info response should be considered deprecated. Use server/sysinfo to access this response key and value instead.</td>
</tr>
<tr>
<td>os_name</td>
<td>Server operating system. The value returned in the server/info response should be considered deprecated. Use server/sysinfo to access this response key and value instead.</td>
</tr>
<tr>
<td>os_version</td>
<td>Server operating system version. The value returned in the server/info response should be considered deprecated. Use server/sysinfo to access this response key and value instead.</td>
</tr>
<tr>
<td>physicalMemoryMB</td>
<td>Server physical memory (MB). The value returned in the server/info response should be considered deprecated. Use server/sysinfo to access this response key and value instead.</td>
</tr>
<tr>
<td>product_type</td>
<td>Splunk software product type. One of the following values. enterprise, hunk, lite, lite_free, splunk</td>
</tr>
<tr>
<td>rtsearch_enabled</td>
<td>Indicates if real-time search is enabled for the instance on this server.</td>
</tr>
<tr>
<td>server_roles</td>
<td>Zero or more of the following possible server roles. indexer, universal_forwarder, heavyweight_forwarder, lightweight_forwarder, license_master, license_slave, cluster_master, cluster_slave, cluster_search_head, deployment_server, deployment_client, search_head, search_peer, shc_captain, shc_deployer, shc_member</td>
</tr>
<tr>
<td>serverName</td>
<td>Server DNS domain name.</td>
</tr>
<tr>
<td>startup_time</td>
<td>Server platform start time, in seconds since January 1, 1970 (UNIX epoch).</td>
</tr>
<tr>
<td>version</td>
<td>os_build software version number. The value returned in the server/info response should be considered deprecated. Use server/sysinfo to access this response key and value instead.</td>
</tr>
</tbody>
</table>

Example request and response
XML Request

curl -k -u admin:changed https://10.140.53.114:8089/services/server/info

XML Response

<title>server-info</title>
<id>https://localhost:8089/services/server/info</id>
<updated>2016-09-08T17:49:52-07:00</updated>
<generator build="19e4b5854495" version="6.5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/info/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>server-info</title>
  <id>https://localhost:8089/services/server/info/server-info</id>
  <updated>2016-09-08T17:49:52-07:00</updated>
  <link href="/services/server/info/server-info" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/info/server-info" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="activeLicenseGroup">Trial</s:key>
      <s:key name="activeLicenseSubgroup">Production</s:key>
      <s:key name="addOns">
        <s:dict>
          <s:key name="hadoop">
            <s:dict>
              <s:key name="parameters">
                <s:dict>
                  <s:key name="erp_type">report</s:key>
                  <s:key name="guid">C6AAF586-93E0-451B-914B-F63A8BBBC7282</s:key>
                  <s:key name="maxNodes">200</s:key>
                </s:dict>
              </s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
      <s:key name="build">19e4b5854495</s:key>
      <s:key name="cpu_arch">x86_64</s:key>
      <eai:acl>
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">0</s:key>
          <s:key name="can_write">0</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
        </s:dict>
      </eai:acl>
      <s:dict>
        <s:key name="eai:acl"></s:key>
      </s:dict>
    </s:dict>
  </content>
server/introspection

https://<host>:<mPort>/services/server/introspection
Access system introspection artifacts.

See also the following associated endpoints.

• server/introspection/indexer
• server/introspection/kvstore

GET
List introspection resources.

Request parameters
None

Returned values
The endpoint returns a list of introspection artifacts.

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/introspection

XML Response

...  
<title></title>
</id>https://localhost:8089/services/server/introspection</id>
<updated>2014-08-04T11:40:23-07:00</updated>
<generator build="221120" version="6.2"/>
<author>
   <name>Splunk</name>
</author>
<s:messages/>
<entry>
   <title>indexer</title>
   <id>https://localhost:8089/services/server/introspection/indexer</id>
   <updated>2014-08-04T11:40:23-07:00</updated>
   <link href="/services/server/introspection/indexer" rel="alternate"/>
   <author>
      <name>system</name>
   </author>
   <link href="/services/server/introspection/indexer" rel="list"/>
   <content type="text/xml">
      <s:dict/>
   </content>
</entry>
<entry>
<title>kvstore</title>
<id>https://localhost:8089/services/server/introspection/kvstore</id>
<updated>2014-08-04T11:40:23-07:00</updated>
<link href="/services/server/introspection/kvstore" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/server/introspection/kvstore" rel="list"/>
<link href="/services/server/introspection/kvstore/_reload" rel="_reload"/>
<content type="text/xml">
  <s:dict/>
</content>
</entry>

<entry>
<title>pipelines</title>
<id>https://localhost:8089/services/server/introspection/pipelines</id>
<updated>2014-08-04T11:40:23-07:00</updated>
<link href="/services/server/introspection/pipelines" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/server/introspection/pipelines" rel="list"/>
<content type="text/xml">
  <s:dict/>
</content>
</entry>

<entry>
<title>processors</title>
<id>https://localhost:8089/services/server/introspection/processors</id>
<updated>2014-08-04T11:40:23-07:00</updated>
<link href="/services/server/introspection/processors" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/server/introspection/processors" rel="list"/>
<content type="text/xml">
  <s:dict/>
</content>
</entry>

<entry>
<title>queues</title>
<id>https://localhost:8089/services/server/introspection/queues</id>
<updated>2014-08-04T11:40:23-07:00</updated>
<link href="/services/server/introspection/queues" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/server/introspection/queues" rel="list"/>
<content type="text/xml">
  <s:dict/>
</content>
</entry>
**server/introspection/indexer**

https://<host>:<mPort>/services/server/introspection/indexer

Access the current indexer status.

See also server/introspection.

**GET**

Get indexer status information.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>average_KBps</td>
<td>Average indexer throughput (kbps).</td>
</tr>
</tbody>
</table>
| reason     | Status explanation. For a normal status, returns normal. The following examples show possible abnormal status reasons. 

"idx=<indexerName> Throttling indexer, too many tsidx files in bucket=<bucketName>. Is splunk-optimize working? If not, low disk space may be the cause." 

"You are low in disk space on partition <partitionName>. Indexing is paused. Will resume when free disk space rises above <minFreeMB>." |
| status     | Current indexer status. One of the following values.                       |

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>normal</td>
<td></td>
</tr>
<tr>
<td>throttled</td>
<td></td>
</tr>
<tr>
<td>stopped</td>
<td></td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```shell
curl -k -u admin:changeme https://localhost:8089/services/server/introspection/indexer
```

**XML Response**

```xml
...<title>introspection-indexer</title>
<id>https://localhost:8089/services/server/introspection/indexer</id>
<updated>2014-08-04T11:43:04-07:00</updated>
<generator build="221120" version="6.2"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
```
server/introspection/kvstore

https://<host>:<mPort>/services/server/introspection/kvstore

Access app KV store resources.

See also server/introspection.

GET

List app KV store resources.

Request parameters
None

Returned values
Lists the following app /server/introspection/kvstore resources.

- /collectionstats
- /replicasetstats
- /serverstatus

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/introspection/kvstore
server/introspection/kvstore/collectionstats

https://<host>:<mPort>/services/server/introspection/kvstore/collectionstats

Get storage statistics for a collection.
See also the following associated endpoints.

- server/introspection
- /replicasetstats
- /serverstatus

**GET**

Get collection storage statistics.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data</td>
<td>Returns the following JSON document.</td>
</tr>
<tr>
<td></td>
<td>- count - Number of collection documents or objects.</td>
</tr>
<tr>
<td></td>
<td>- indexes - Key and size of every index on the collection.</td>
</tr>
<tr>
<td></td>
<td>- lastExtentSize - Size of last allocated extent.</td>
</tr>
<tr>
<td></td>
<td>- nindexes - Number of indexes on the collection.</td>
</tr>
<tr>
<td></td>
<td>- ns - Current collection namespace.</td>
</tr>
<tr>
<td></td>
<td>- numExtents - Number of contiguously allocated data file regions.</td>
</tr>
<tr>
<td></td>
<td>- paddingFactor - Amount of space added to each document.</td>
</tr>
<tr>
<td></td>
<td>- size - Collection records total size.</td>
</tr>
<tr>
<td></td>
<td>- storageSize - Collection document storage allocation.</td>
</tr>
<tr>
<td></td>
<td>- systemFlags - Collection flags that reflect internal server options.</td>
</tr>
<tr>
<td></td>
<td>- totalIndexSize - Size of all indexes.</td>
</tr>
<tr>
<td></td>
<td>- userFlags - Collection flags set by user.</td>
</tr>
</tbody>
</table>

**Note:** Sizes are returned in MBs. For more information, see Performance Metrics.

**Example request and response**

**XML Request**

```bash
curl -k -u admin:changeme https://localhost:8089/services/server/introspection/kvstore/collectionstats
```

**XML Response**

```xml
<title>kvstore-collectionstats</title>
<id>https://localhost:8089/services/server/introspection/kvstore/collectionstats/id</id>
<updated>2014-08-20T14:31:42-07:00</updated> <generator build="226873" version="6.2"/> <author> <name>Splunk</name> </author> ...
```

649
server/introspection/kvstore/replicasetstats

https://<host>:<mPort>/services/server/introspection/kvstore/replicasetstats

Get the status of the replica set from the point of view of the current server.

See also the following associated endpoints.

- server/introspection
- /collectionstats
- /serverstatus

GET

Get the status of the replica set from the point of view of the current server.

Request parameters

None

Returned values

650
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>set</td>
<td>Replicate Set Name set in the server.conf file.</td>
</tr>
<tr>
<td>date</td>
<td>Current time in ISO format.</td>
</tr>
<tr>
<td>myState</td>
<td>Startup process, basic operations, and potential error states:</td>
</tr>
<tr>
<td>0 STARTUP</td>
<td>Initial member state. Cannot vote.</td>
</tr>
<tr>
<td>1 PRIMARY</td>
<td>Only member that can accept write operations. Can vote.</td>
</tr>
<tr>
<td>2 SECONDARY</td>
<td>Data store replication member. Can vote.</td>
</tr>
<tr>
<td>3 RECOVERING</td>
<td>Members perform startup self-checks, or transition from completing a rollback or resync. Can vote.</td>
</tr>
<tr>
<td>4 FATAL</td>
<td>Unrecoverable error encountered. Cannot vote.</td>
</tr>
<tr>
<td>5 STARTUP2</td>
<td>Forks replication and election threads before becoming a secondary. Cannot vote.</td>
</tr>
<tr>
<td>6 UNKNOWN</td>
<td>Never connected to replica set. Cannot vote.</td>
</tr>
<tr>
<td>7 ARBITER</td>
<td>Participate in elections, do not replicate data. Can vote.</td>
</tr>
<tr>
<td>8 DOWN</td>
<td>Cannot be accessed by the set. Cannot vote.</td>
</tr>
<tr>
<td>9 ROLLOBACK</td>
<td>Performs rollback. Can vote.</td>
</tr>
<tr>
<td>10 REMOVED</td>
<td>Removed from the replica set. Cannot vote.</td>
</tr>
<tr>
<td>members</td>
<td>Descriptions of members of replica set:</td>
</tr>
<tr>
<td>_id</td>
<td>Member ID.</td>
</tr>
<tr>
<td>name</td>
<td>Server name.</td>
</tr>
<tr>
<td>health</td>
<td>Status: 1 = up, 0 = down.</td>
</tr>
<tr>
<td>state</td>
<td>Replica state (See myState).</td>
</tr>
<tr>
<td>stateStr</td>
<td>String representation of state.</td>
</tr>
<tr>
<td>uptime</td>
<td>Online interval (seconds).</td>
</tr>
<tr>
<td>optime</td>
<td>Information about last operations log operation.</td>
</tr>
<tr>
<td>optimeDate</td>
<td>Time of last operations log operation in ISO format.</td>
</tr>
<tr>
<td>lastHeartbeat</td>
<td>Transmission time of last heartbeat in ISO format.</td>
</tr>
<tr>
<td>lastHeartbeatRecv</td>
<td>Time last heartbeat received in ISO format.</td>
</tr>
<tr>
<td>pingMs</td>
<td>Round-trip packet time (msec).</td>
</tr>
<tr>
<td>syncingTo</td>
<td>On secondary and recovering members, hostname of member from which this instance is syncing.</td>
</tr>
<tr>
<td>ok</td>
<td>Command return status: 1 = Success, 0 = Failure.</td>
</tr>
<tr>
<td>oplogInfo</td>
<td>Operations log information:</td>
</tr>
<tr>
<td>start</td>
<td>Start time.</td>
</tr>
<tr>
<td>end</td>
<td>End time.</td>
</tr>
<tr>
<td>collectionStats</td>
<td>Collection storage statistics:</td>
</tr>
<tr>
<td>ns</td>
<td>Current collection namespace.</td>
</tr>
<tr>
<td>count</td>
<td>Number of collection documents or objects.</td>
</tr>
<tr>
<td>size</td>
<td>Collection records total size.</td>
</tr>
<tr>
<td>avgObjSize</td>
<td>Average object size in collection (bytes).</td>
</tr>
<tr>
<td>storageSize</td>
<td>Collection document storage allocation.</td>
</tr>
<tr>
<td>numExtents</td>
<td>Number of contiguously allocated data file regions.</td>
</tr>
<tr>
<td>indexes</td>
<td>Number of indexes on the collection.</td>
</tr>
<tr>
<td>lastExtentSize</td>
<td>Size of last allocated extent.</td>
</tr>
<tr>
<td>paddingFactor</td>
<td>Amount of space added to each document.</td>
</tr>
<tr>
<td>systemFlags</td>
<td>Collection flags that reflect internal server options.</td>
</tr>
<tr>
<td>userFlags</td>
<td>Collection flags set by user.</td>
</tr>
<tr>
<td>totalIndexSize</td>
<td>Size of all indexes.</td>
</tr>
<tr>
<td>indexSizes</td>
<td>Key and size of every index on the collection.</td>
</tr>
</tbody>
</table>
◊ capped - Capped setting: true = capped, false = not capped.
◊ max - Max collection size.
◊ ok - Command return status: 1 = Success, 0 = Failure.
♦ sources - Operations log sources.

Example request and response

**XML Request**

curl -k -u admin:changeme https://localhost:8089/services/server/introspection/kvstore/replicasetstats

**XML Response**

```xml
...<title>replicasetstats</title>
<id>https://localhost:8089/services/server/introspection/kvstore/replicasetstats/replicasetstats</id>
<updated>2014-08-20T14:31:42-07:00</updated>
<author>
  <name>system</name>
</author>
<content type="text/xml">
  <s:dict>
    <s:key name="data">
      <s:list>
        <s:item>
          {
            "replSetStats": {
              "set": "splunkrs",
              "date": 1412203576000,
              "myState": 2,
              "syncingTo": "54.xxx.xxx.xxx:8191",
              "members": [
                {
                  "_id": 2,
                  "name": "54.xxx.xxx.xxx:8191",
                  "health": 1,
                  "state": 2,
                  "stateStr": "SECONDARY",
                  "uptime": 102409,
                  "optime": {
                    "t": 1412101153,
                    "i": 1
                  },
                  "optimeDate": 1412101153000,
                  "lastHeartbeat": 1412203575000,
                  "lastHeartbeatRecv": 1412203575000,
                  "pingMs": 1,
                  "syncingTo": "54.xxx.xxx.xxx:8191"
                },
                {
                  "_id": 3,
                  "name": "54.xxx.xxx.yyy:8191",
                  "health": 1,
                  "state": 2,
                  "syncingTo": "54.xxx.xxx.xxx:8191"
                }
              ]
            }
          }
```

652
"stateStr": "SECONDARY",
"uptime": 102409,
"optime": {
  "t": 1412101153,
  "i": 1
},
"optimeDate": 1412101153000,
"lastHeartbeat": 1412203576000,
"lastHeartbeatRecv": 1412203575000,
"pingMs": 1,
"syncingTo": "54.xxx.xxx.yyy:8191"
},

elided

{
  "_id": 17,
  "name": "54.xxx.xxx.zzz:8191",
  "health": 1,
  "state": 2,
  "stateStr": "SECONDARY",
  "uptime": 102409,
  "optime": {
    "t": 1412101153,
    "i": 1
  },
  "optimeDate": 1412101153000,
  "lastHeartbeat": 1412203574000,
  "lastHeartbeatRecv": 1412203575000,
  "pingMs": 1,
  "syncingTo": "54.xxx.xxx.zzz:8191"
}

"ok": 1

"oplogInfo": {
  "start": 1412022009000,
  "end": 1412101153000,
  "collectionStats": {
    "ns": "local.oplog.rs",
    "count": 631,
    "size": 166964,
    "avgObjSize": 264,
    "storageSize": 1048580080,
    "numExtents": 3,
    "nindexes": 0,
    "lastExtentSize": 4096,
    "paddingFactor": 1,
    "systemFlags": 0,
    "userFlags": 0,
    "totalIndexSize": 0,
    "indexesizes": [],
    "capped": true,
    "max": 9223372036854775808.000000,
    "ok": 1
  },
  "sources": {}
server/introspection(kvstore/serverstatus

https://<host>:<mPort>/services/server/introspection/kvstore/serverstatus

Get an overview of the database process state.

Monitoring applications periodically run this command to get statistical information about the database instance.

See also the following associated endpoints.

- server/introspection
- /collectionstats
- /replicasetstats

GET

Get an overview of the database process state.

Request parameters
None

Returned values
The response data is platform-dependent.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>data</td>
<td>Returns the following CDATA items.</td>
</tr>
<tr>
<td></td>
<td>- asserts - Number of database assertions since the server process started, for each of the following levels/types:</td>
</tr>
<tr>
<td></td>
<td>♦ regular</td>
</tr>
<tr>
<td></td>
<td>♦ warning</td>
</tr>
<tr>
<td></td>
<td>♦ msg</td>
</tr>
<tr>
<td></td>
<td>♦ user</td>
</tr>
<tr>
<td></td>
<td>♦ rollovers</td>
</tr>
<tr>
<td></td>
<td>- backgroundFlushing - Write to disk flush metrics:</td>
</tr>
<tr>
<td></td>
<td>♦ flushes - Number of times writes flushed.</td>
</tr>
<tr>
<td></td>
<td>♦ total_ms - Number of msec processes used to flush writes.</td>
</tr>
<tr>
<td></td>
<td>♦ average_ms - Relationship between flushes and total_ms, in msec.</td>
</tr>
<tr>
<td></td>
<td>♦ last_ms - Number of msec the last flush took.</td>
</tr>
<tr>
<td></td>
<td>♦ last_finished (date) - ISO time of last completed write flush operation.</td>
</tr>
<tr>
<td></td>
<td>- connections - Current incoming connections status and database availability:</td>
</tr>
<tr>
<td></td>
<td>♦ current - Number of active client connections.</td>
</tr>
<tr>
<td></td>
<td>♦ available - Number of unused connections available.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>totalCreated</td>
<td>Total number of connections created, including closed connections.</td>
</tr>
<tr>
<td>cursors</td>
<td>[DEPRECATED] Current cursor and state. Use metrics, instead.</td>
</tr>
<tr>
<td>dur</td>
<td>(Durability) Journaling-related operations and performance. Journaling must be enabled.</td>
</tr>
<tr>
<td>commits</td>
<td>Number of transactions written to the journal during the last group commit interval.</td>
</tr>
<tr>
<td>journaledMB</td>
<td>Amount of data (MB) written to the journal during the last group commit interval.</td>
</tr>
<tr>
<td>writeToDataFilesMB</td>
<td>Amount of data (MB) written from journal to data files during the last group commit interval.</td>
</tr>
<tr>
<td>compression</td>
<td>Compression ratio of data written to journal: ( \frac{\text{jouarnaed size of data}}{\text{uncompressed size of data}} )</td>
</tr>
<tr>
<td>commitsInWriteLock</td>
<td>Number of commits that occurred during a write lock.</td>
</tr>
<tr>
<td>earlyCommits</td>
<td>Number of commits requested before scheduled group commit time.</td>
</tr>
<tr>
<td>timeMs</td>
<td>Performance during various journaling phases.</td>
</tr>
<tr>
<td>dt</td>
<td>Data collection interval (msec).</td>
</tr>
<tr>
<td>prepLogBuffer</td>
<td>Time spend preparing to write to journal (msec).</td>
</tr>
<tr>
<td>writeToJournal</td>
<td>Time spent writing to journal (msec).</td>
</tr>
<tr>
<td>writeToDataFiles</td>
<td>Time spent writing to data files after journaling (msec).</td>
</tr>
<tr>
<td>remapPrivateView</td>
<td>Time spent remapping copy-on-write memory mapped views (msec).</td>
</tr>
<tr>
<td>note</td>
<td>Platform-specific information.</td>
</tr>
<tr>
<td>heap_usage_bytes</td>
<td>Total heap space size used by database (bytes). Applicable to *nix systems, only.</td>
</tr>
<tr>
<td>page_faults</td>
<td>Total number of page faults that require disk operations.</td>
</tr>
<tr>
<td>globalLock</td>
<td>Information about the current database lock state, historical lock status, and active clients:</td>
</tr>
<tr>
<td>totalTime</td>
<td>Time since database started and globalLock creation (usec).</td>
</tr>
<tr>
<td>lockTime</td>
<td>Time since database started that globalLock has been held (usec).</td>
</tr>
<tr>
<td>currentQueue</td>
<td>Information about operations queued because of a lock.</td>
</tr>
<tr>
<td>total</td>
<td>Total number of operations queued waiting on readers and writers locks.</td>
</tr>
<tr>
<td>readers</td>
<td>Number of operations queued waiting for read lock.</td>
</tr>
<tr>
<td>writers</td>
<td>Number of operations queued waiting for write lock.</td>
</tr>
<tr>
<td>activeClients</td>
<td>Information about number and operation types of connected clients.</td>
</tr>
<tr>
<td>total</td>
<td>Total number of readers and writers connections.</td>
</tr>
<tr>
<td>readers</td>
<td>Number of connected clients performing read operations.</td>
</tr>
<tr>
<td>writers</td>
<td>Number of connected clients performing write operations.</td>
</tr>
<tr>
<td>host</td>
<td>Hostname and port number.</td>
</tr>
<tr>
<td>indexCounters</td>
<td>Index usage counters:</td>
</tr>
<tr>
<td>accesses</td>
<td>Number of times operations accessed indexes.</td>
</tr>
<tr>
<td>hits</td>
<td>Number of times index accessed and returned from memory.</td>
</tr>
<tr>
<td>misses</td>
<td>Number of attempts to access index not in memory.</td>
</tr>
<tr>
<td>resets</td>
<td>Number of times index counters reset since database last started.</td>
</tr>
<tr>
<td>missRatio</td>
<td>Ratio of hits to misses.</td>
</tr>
<tr>
<td>localTime</td>
<td>ISO-formatted local time.</td>
</tr>
<tr>
<td>locks</td>
<td>State and read/write use of global and database-specific locks:</td>
</tr>
<tr>
<td>timeLockedMicros</td>
<td>Amount of time a lock existed, for all databases of this server instance (usec).</td>
</tr>
<tr>
<td>timeAcquiringMicros</td>
<td>Amount of time operations spend waiting, for lock for all databases of this server instance (usec).</td>
</tr>
<tr>
<td>admin</td>
<td>Lock use in the admin database.</td>
</tr>
<tr>
<td>timeLockedMicros</td>
<td>Amount of time locks existed in the admin database context (usec).</td>
</tr>
<tr>
<td>timeAcquiringMicros</td>
<td>Amount of time spent waiting to acquire a lock in the admin database context (usec).</td>
</tr>
<tr>
<td>local</td>
<td>Lock use in the local database.</td>
</tr>
<tr>
<td>timeLockedMicros</td>
<td>Amount of time locks existed in the local database context (usec).</td>
</tr>
<tr>
<td>timeAcquiringMicros</td>
<td>Amount of time spent waiting to acquire a lock in the local database context (usec).</td>
</tr>
<tr>
<td>search.collection</td>
<td>Locks used in each collection.</td>
</tr>
<tr>
<td>timeLockedMicros</td>
<td>Amount of time locks exist in the collection context (usec).</td>
</tr>
<tr>
<td>timeAcquiringMicros</td>
<td>Amount of time spent waiting to acquire a lock in the collection context (usec).</td>
</tr>
<tr>
<td>mem</td>
<td>Memory usage: System architecture and memory usage metrics.</td>
</tr>
<tr>
<td>bits</td>
<td>System address architecture: 32 or 64 bit architecture.</td>
</tr>
<tr>
<td>resident</td>
<td>Amount of RAM currently used by the database process (MB).</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>virtual</td>
<td>Amount of virtual memory used (MB).</td>
</tr>
<tr>
<td>supported true/false</td>
<td>true = supports extended memory information, false = does not support extended memory information.</td>
</tr>
<tr>
<td>mapped</td>
<td>Amount of mapped memory for database (MB).</td>
</tr>
<tr>
<td>mappedWithJournal</td>
<td>Amount of mapped memory, including journaling memory (MB). Always twice the size of mapped.</td>
</tr>
<tr>
<td>metrics</td>
<td>Current instance use and state:</td>
</tr>
<tr>
<td>cursor</td>
<td>- timeout: Total number of cursors that have timed out since the server process started.</td>
</tr>
<tr>
<td></td>
<td>- open:</td>
</tr>
<tr>
<td></td>
<td>- noTimeout: Number of open cursors with option set to prevent timeout after a period of inactivity.</td>
</tr>
<tr>
<td></td>
<td>- pinned: Number of pinned open cursors.</td>
</tr>
<tr>
<td></td>
<td>- total: Number of cursors maintained for clients, typically less than zero.</td>
</tr>
<tr>
<td>document</td>
<td>Information about document access and modification patterns and data use. Compare these values to opcounters data, which track total number of operations.</td>
</tr>
<tr>
<td></td>
<td>- deleted: Total number of deleted documents.</td>
</tr>
<tr>
<td></td>
<td>- inserted: Total number of inserted documents.</td>
</tr>
<tr>
<td></td>
<td>- returned: Total number of documents returned by queries.</td>
</tr>
<tr>
<td></td>
<td>- updated: Total number of updated documents.</td>
</tr>
<tr>
<td>getLastError</td>
<td>Information about getLastError use.</td>
</tr>
<tr>
<td></td>
<td>- wtime: getLastError operation counts with a specified write concern that wait for one or more members of a replica set to acknowledge the write operation.</td>
</tr>
<tr>
<td></td>
<td>- num: getLastError operation counts with a specified write concern that wait for one or more members of a replica set to acknowledge the write operation.</td>
</tr>
<tr>
<td></td>
<td>- totalMillis: Amount of time spent performing getLastError operations with write concern that wait for one or more members of a replica set to acknowledge the write operation (msec).</td>
</tr>
<tr>
<td></td>
<td>- wtimeouts: Number of times write concern operations timed out as a result of the wtimeout threshold to getLastError.</td>
</tr>
<tr>
<td>operation</td>
<td>Counters for several types of update and query operations handled using special operation types.</td>
</tr>
<tr>
<td></td>
<td>- fastmod: Number of update operations that neither cause documents to grow nor require updates to the index.</td>
</tr>
<tr>
<td></td>
<td>- idhack: Number of queries that contain the _key field.</td>
</tr>
<tr>
<td></td>
<td>- scanAndOrder: Number of queries that return sorted numbers that cannot perform the sort operation using an index.</td>
</tr>
<tr>
<td>queryExecutor</td>
<td>Data from the query execution system.</td>
</tr>
<tr>
<td></td>
<td>- scanned: Number of index items scanned during queries and query-plan evaluation.</td>
</tr>
<tr>
<td></td>
<td>- scannedObjects: Total number of documents scanned during the query.</td>
</tr>
<tr>
<td>record</td>
<td>Data related to record allocation in the on-disk memory files.</td>
</tr>
<tr>
<td></td>
<td>- moves: Number of times documents move within the on-disk representation of the data set. Documents move as a result of operations that increase the size of the document beyond their allocated record size.</td>
</tr>
<tr>
<td>repl</td>
<td>Metrics related to the ordered history of logical writes.</td>
</tr>
<tr>
<td></td>
<td>- apply: Information about the application of ordered history of logical writes.</td>
</tr>
<tr>
<td></td>
<td>- batches: Information on the ordered history of logical writes application process on secondaries members of replica sets.</td>
</tr>
<tr>
<td></td>
<td>- num: Number of batches applied across all databases.</td>
</tr>
<tr>
<td></td>
<td>- totalMillis: Amount of time spent applying ordered history of logical write operations (msec).</td>
</tr>
<tr>
<td></td>
<td>- buffer: Information to track the ordered history of logical write operations buffer.</td>
</tr>
<tr>
<td></td>
<td>- count: Number of operations on the ordered history of logical writes buffer.</td>
</tr>
<tr>
<td></td>
<td>- maxSizeBytes/: Maximum size of the ordered history of logical writes buffer.</td>
</tr>
<tr>
<td></td>
<td>- sizeBytes: Current size of the contents of the ordered history of logical writes buffer.</td>
</tr>
<tr>
<td></td>
<td>- network: Network use information for the replication process.</td>
</tr>
<tr>
<td></td>
<td>- bytes: Amount of data read from the replication sync source (bytes).</td>
</tr>
<tr>
<td></td>
<td>- getmores: Information about queries for additional results from the ordered history of logical write operations cursor as part of the replication process.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>num</td>
<td>Number of queries for additional results from the ordered history of logical write operations, which are operations that request an additional set of operations from the replication sync source.</td>
</tr>
<tr>
<td>totalMillis</td>
<td>Amount of time to collect data from queries for additional results from the ordered history of logical write operations processes created.</td>
</tr>
<tr>
<td>ops</td>
<td>Number of operations read from the replication source.</td>
</tr>
<tr>
<td>readersCreated</td>
<td>Number of queries for additional results from the ordered history of logical write operations processes created.</td>
</tr>
<tr>
<td>preload</td>
<td>Information about replication pre-fetch.</td>
</tr>
<tr>
<td>docs</td>
<td>Information about documents loaded into memory during replication pre-fetch.</td>
</tr>
<tr>
<td>totalMillis</td>
<td>Amount of time spent loading documents as part of replication pre-fetch (msec).</td>
</tr>
<tr>
<td>indexes</td>
<td>Information about index items loaded into memory during replication pre-fetch.</td>
</tr>
<tr>
<td>num</td>
<td>Number of index entries loaded by members before updating documents as part of replication pre-fetch.</td>
</tr>
<tr>
<td>totalMillis</td>
<td>Amount of time spent loading index entries as part of replication pre-fetch (msec).</td>
</tr>
<tr>
<td>storage</td>
<td>Freelist behavior monitoring statistics.</td>
</tr>
<tr>
<td>freelist</td>
<td>Freelist bucket behavior monitoring statistics.</td>
</tr>
<tr>
<td>search</td>
<td>Freelist bucket behavior monitoring search statistics.</td>
</tr>
<tr>
<td>bucketExhausted</td>
<td>Number of times bucket fully searched, requiring advance to next bucket.</td>
</tr>
<tr>
<td>requests</td>
<td>Number of times the allocation function was called.</td>
</tr>
<tr>
<td>scanned</td>
<td>Number of freelist bucket entries examined.</td>
</tr>
<tr>
<td>deletedDocuments</td>
<td>Number of documents deleted from collections with a ttl index.</td>
</tr>
<tr>
<td>passes</td>
<td>Number of times background process removes documents from collections with a ttl index.</td>
</tr>
<tr>
<td>network</td>
<td>Network use and state:</td>
</tr>
<tr>
<td>bytesRead</td>
<td>Amount of network traffic received by this database (bytes).</td>
</tr>
<tr>
<td>bytesOut</td>
<td>Amount of network traffic sent from this database (bytes).</td>
</tr>
<tr>
<td>numRequests</td>
<td>Number of distinct requests received by the server.</td>
</tr>
<tr>
<td>ok</td>
<td>Command return status: 1 = Success, 0 = Failure.</td>
</tr>
<tr>
<td>opcounters</td>
<td>Overview of database operations by type, similar to opcountersRepl:</td>
</tr>
<tr>
<td>insert</td>
<td>Number of insert operations since instance started.</td>
</tr>
<tr>
<td>query</td>
<td>Number of queries since instance started.</td>
</tr>
<tr>
<td>update</td>
<td>Number of update operations since instance started.</td>
</tr>
<tr>
<td>delete</td>
<td>Number of delete operations since instance started.</td>
</tr>
<tr>
<td>getmore</td>
<td>Number of getmore operations since instance started.</td>
</tr>
<tr>
<td>command</td>
<td>Number of commands issued since instance started.</td>
</tr>
<tr>
<td>opcountersRepl</td>
<td>Overview of replication operations by type, similar to opcounters:</td>
</tr>
<tr>
<td>insert</td>
<td>Number of replicated insert operations since instance started.</td>
</tr>
<tr>
<td>query</td>
<td>Number of replicated queries since instance started.</td>
</tr>
<tr>
<td>update</td>
<td>Number of replicated update operations since instance started.</td>
</tr>
<tr>
<td>delete</td>
<td>Number of replicated delete operations since instance started.</td>
</tr>
<tr>
<td>getmore</td>
<td>Number of replicated getmore operations since instance started.</td>
</tr>
<tr>
<td>command</td>
<td>Number of replicated commands issued since instance started.</td>
</tr>
<tr>
<td>pid</td>
<td>Process ID.</td>
</tr>
<tr>
<td>recordStats</td>
<td>Page fault statistics:</td>
</tr>
<tr>
<td>accessesNotInMemory</td>
<td>Number of times memory page accessed that was not resident in memory, for all databases.</td>
</tr>
<tr>
<td>pageFaultExceptionsThrown</td>
<td>Number of page fault exceptions thrown when accessing data for all databases.</td>
</tr>
<tr>
<td>admin</td>
<td>Admin database page fault statistics.</td>
</tr>
<tr>
<td>accessesNotInMemory</td>
<td>Number of times memory page accessed that was not resident in memory, for the admin database.</td>
</tr>
<tr>
<td>pageFaultExceptionsThrown</td>
<td>Number of page fault exceptions thrown when accessing data for the admin database.</td>
</tr>
<tr>
<td>local</td>
<td>Local database page fault statistics.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>accessesNotInMemory</td>
<td>Number of times memory page accessed that was not resident in memory, for the local database.</td>
</tr>
<tr>
<td>pageFaultExceptionsThrown</td>
<td>Number of page fault exceptions thrown when accessing data for the local database.</td>
</tr>
<tr>
<td>search.collection</td>
<td>Search database page fault statistics.</td>
</tr>
<tr>
<td>accessesNotInMemory</td>
<td>Number of times memory page accessed that was not resident in memory, for the search database.</td>
</tr>
<tr>
<td>pageFaultExceptionsThrown</td>
<td>Number of page fault exceptions thrown when accessing data for the search database.</td>
</tr>
</tbody>
</table>

- **uptime** - Amount of time database process has been active (seconds).
- **uptimeEstimate** - Amount of time database process has been active as calculated from the internal, course-grained time keeping system (seconds).
- **uptimeMillis** - Amount of time database process has been active (msec).
- **version** - Version number (not used).
- **writeBacksQueued** - Write-backs queued status: `true` = write-backs queued, `false` = write-backs not queued.

### Example request and response

#### XML Request

```bash
curl -k -u admin:changeme https://localhost:8089/services/server/introspection/kvstore/serverstatus
```

#### XML Response

```xml
...
<title>serverStatus</title>
/id>https://localhost:8089/services/server/introspection/kvstore/serverstatus/serverStatus</id>
/updatetime>2014-08-20T14:26:42-07:00</updatetime>
</link href="/services/server/introspection/kvstore/serverstatus/serverStatus" rel="alternate"/>
</author>
</link href="/services/server/introspection/kvstore/serverstatus/serverStatus" rel="list"/>

<s:dict>
    <s:key name="data">
        <![CDATA[
            "host":"localhost:8089", "version":"2.6.3", "pid":23009, "uptime":19049, "uptimeMillis":19049447,
            "uptimeEstimate":18295, "localTime":{"$date":1408570002615}, "asserts":{" regular":0, " warning":0, " msg":0,
            " user":0, " rollovers":0, " backgroundFlushing":0, " flushes":317, " total_ms":11523, " average_ms":36.350158,
            " last_ms":0, " last_finished":{"$date":1408569973325}), " connections":{" current":7, " available":3269,
            " totalCreated":7}, " cursors":{ " note":"deprecated, use server status metrics", " clientCursors_size":0,
            " totalOpen":0, " pinned":0, " totalNoTimeout":0, " timedOut":0}, " dur":{ " commits":30, " journaledMB":0,
            " writeToDataFilesMB":0, " compression":0, " commitsInWriteLock":0, " earlyCommits":0, " timeMs":{ " dt":3072,
            " prepLogBuffer":0, " writeToJournal":0, " writeToDataFiles":0, " remapPrivateView":0}), " extra_info":{ " note":"fields vary by platform", " heap_usage_bytes":67624592, " page_faults":3}, " globalLock":{ " totalTime":19049447000, " lockTime":1491098, " currentQueue":{ " total":0, " readers":0, " writers":0, " activeClients":{ " total":0, " readers":0, " writers":0}), " indexCounters":{ " accesses":2, " hits":2,
            " misses":0, " resets":0, " missRatio":0, " locks":{ " "}, " timeLockedMicros":{ " n":2926340, " w":1419098},
            " timeAcquiringMicros":{ " p":1458997, " w":342703}), " admin":{ " timeLockedMicros":{ " r":103638, " w":0},
            " timeAcquiringMicros":{ " r":13202, " w":0}), " local":{ " timeLockedMicros":{ " r":426518, " w":237},
            " timeAcquiringMicros":{ " r":185505, " w":12}), " search.kvstoredemo":{ " timeLockedMicros":{ " r":2832888,
            " w":292}, " timeAcquiringMicros":{ " r":1310820, " w":17}), " network":{ " bytesIn":1133611,
            " bytesOut":11628162, " numRequests":12070), " opcounters":{ " insert":1, " query":4760, " update":0, " delete":0,
            " getmore":0, " command":8264), " opcountersRepl":{ " insert":0, " query":0, " update":0, " delete":0, " getmore":0,

```

658
server/introspection/search/dispatch

https://<host>:<mPort>/services/server/introspection/search/dispatch

Provides vital statistics for distributed search framework, including details on search peer performance.

**GET**

Enumerate scheduled search details.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle_Directory_Reaper_Average_Time(ms)</td>
<td>Average time for dispatch reaper to walk search peer directory and reap obsolete bundles.</td>
</tr>
<tr>
<td>Bundle_Directory_Reaper_Max_Time(ms)</td>
<td>Maximum time for dispatch reaper to walk search peer directory and reap obsolete bundles.</td>
</tr>
<tr>
<td>Compute_User_Search_Quota_Average_Time(ms)</td>
<td>Average time for computing user search quota.</td>
</tr>
<tr>
<td>Compute_User_Search_Quota_Max_Time(ms)</td>
<td>Maximum time for computing user search quota.</td>
</tr>
<tr>
<td>Dispatch_Directory_Reaper_Average_Time(ms)</td>
<td>Average time for dispatch reaper to walk dispatch directory and reap stale artifacts.</td>
</tr>
<tr>
<td>Dispatch_Directory_Reaper_Max_Time(ms)</td>
<td>Maximum time for dispatch reaper to walk dispatch directory and reap stale artifacts.</td>
</tr>
<tr>
<td>Search_StartUp_Time_Average_Time(ms)</td>
<td>Average time for preprocessing before search startup. Counted from time search state is set to RUNNING.</td>
</tr>
</tbody>
</table>
Startup time indicates that parsing is complete and the distributed search infrastructure is set up. At startup, the Splunk platform is ready to wait for responses from indexers.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search_StartUp_Time_Max_Time(ms)</td>
<td>Maximum time for preprocessing before search startup. Counted from time search state is set to <strong>RUNNING</strong>. Startup time indicates that parsing is complete and the distributed search infrastructure is set up. At startup, the Splunk platform is ready to wait for responses from indexers.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u username:password https://localhost:8089/services/server/introspection/search/dispatch

**XML Response**

```xml
<?xml-stylesheet type="text/xml" href="/static/atom.xsl"?>
  <title>introspection-dispatchreaper</title>
  <id>https://localhost:8089/services/server/introspection/search/dispatch</id>
  <updated>2015-08-27T13:49:04-07:00</updated>
  <generator build="ced4d408678cc212328ba3550d23c8a87c24339d4" version="20150826"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/server/introspection/search/dispatch/_acl" rel="_acl"/>
  <opensearch:totalResults>4</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Bundle_Directory_Reaper</title>
    <id>https://localhost:8089/services/server/introspection/search/dispatch/Bundle_Directory_Reaper</id>
    <updated>2015-08-27T13:49:04-07:00</updated>
    <link href="/services/server/introspection/search/dispatch/Bundle_Directory_Reaper" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/server/introspection/search/dispatch/Bundle_Directory_Reaper" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="Bundle_Directory_Reaper_Average_Time(ms)">1.000000</s:key>
        <s:key name="Bundle_Directory_Reaper_Max_Time(ms)">1</s:key>
        <s:key name="eai:acl">1</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
<entry>
<title>Dispatch_Directory_Reaper</title>
<updated>2015-08-27T13:49:04-07:00</updated>
<link href="/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper" rel="alternate"/>
<author>
<name>system</name>
</author>
<content type="text/xml">
<s:dict>
<s:key name="Dispatch_Directory_Reaper_Average_Time(ms)">5.400000</s:key>
<s:key name="Dispatch_Directory_Reaper_Max_Time(ms)">16</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
</s:dict>
</s:key>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
</s:dict>
</content>
</entry>

<entry>
<title>Search_StartUp_Time</title>
/id>https://localhost:8089/services/server/introspection/search/dispatch/Search_StartUp_Time</id>
<updated>2015-08-27T13:49:04-07:00</updated>
<link href="/services/server/introspection/search/dispatch/Search_StartUp_Time" rel="alternate"/>
<author>
<name>system</name>
</author>
<content type="text/xml">
<s:dict>
<s:key name="Search_StartUp_Time_Average_Time(ms)">136.750000</s:key>
<s:key name="Search_StartUp_Time_Max_Time(ms)">185</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
</s:dict>
</s:key>
</s:dict>
</content>
</entry>
server/introspection/search/dispatch/Bundle_Directory_Reaper

https://<host>:<mPort>/services/server/introspection/search/dispatch/Bundle_Directory_Reaper
Get average and maximum time for the dispatch reaper to walk the search peer directory and reap obsolete bundles.

GET

Enumerate routine distributed search method execution times for each peer.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle_Directory_Reaper_Average_Time(ms)</td>
<td>Average time for dispatch reaper to walk search peer directory and reap obsolete bundles.</td>
</tr>
<tr>
<td>Bundle_Directory_Reaper_Max_Time(ms)</td>
<td>Maximum time for dispatch reaper to walk search peer directory and reap obsolete bundles.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u username:password
https://localhost:8089/services/server/introspection/search/dispatch/Bundle_Directory_Reaper

XML Response

663
...<title>introspection-dispatchreaper</title>
(id=https://localhost:8089/services/server/introspection/search//dispatch/id>
<updated>2015-08-26T14:24:43-07:00</updated>
<generator build="ced4408678cc212320ba3550d23c8a7c24339d4" version="20150826"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/introspection/search//dispatch/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>Bundle_Directory_Reaper</title>
  <id>https://localhost:8089/services/server/introspection/search//dispatch/Bundle_Directory_Reaper</id>
  <updated>2015-08-26T14:24:43-07:00</updated>
  <link href="/services/server/introspection/search//dispatch/Bundle_Directory_Reaper" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/introspection/search//dispatch/Bundle_Directory_Reaper" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="Bundle_Directory_Reaper_Average_Time(ms)">1.000000</s:key>
      <s:key name="Bundle_Directory_Reaper_Max_Time(ms)">1</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">
          </s:key>
          <s:key name="can_list">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      </s:dict>
    </s:dict>
  </content>
</entry>

664
server/introspection/search/dispatch/Compute_User_Search_Quota

https://<host>:<mPort>/services/server/introspection/search/dispatch/Compute_User_Search_Quota

Provides average and maximum time for computing user search quotas.

GET

Enumerate average and maximum time for user search quota computation.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compute_User_Search_Quota_Average_Time</td>
<td>Average time for computing user search quota.</td>
</tr>
<tr>
<td>Compute_User_Search_Quota_Max_Time</td>
<td>Maximum time for computing user search quota.</td>
</tr>
</tbody>
</table>

XML Request

```
curl -k -u username:password
https://localhost:8089/services/server/introspection/search/dispatch/Compute_User_Search_Quota
```

XML Response

```
...<title>introspection-dispatchreaper</title>
<id>https://localhost:8089/services/server/introspection/search/dispatch</id>
<updated>2015-08-26T14:33:46-07:00</updated>
<generator build="ced4408678cc212320ba3550d23c8a87c24339d4" version="20150826"/>
<author>
   <name>Splunk</name>
</author>
<link href="/services/server/introspection/search/dispatch/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
   <title>Compute_User_Search_Quota</title>
   <id>https://localhost:8089/services/server/introspection/search/dispatch/Compute_User_Search_Quota</id>
   <updated>2015-08-26T14:33:46-07:00</updated>
   <link href="/services/server/introspection/search/dispatch/Compute_User_Search_Quota" rel="alternate"/>
```
server/introspection/search/dispatch/Dispatch_Directory_Reaper

https://<host>:<mPort>/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper

Get average and maximum time for the dispatch reaper to walk the dispatch directory and reap stale artifacts.
GET

Show dispatch directory reaper times for reaping stale artifacts.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dispatch_Directory_Reaper_Average_Time(ms)</td>
<td>Average time for dispatch reaper to walk dispatch directory and reap stale artifacts.</td>
</tr>
<tr>
<td>Dispatch_Directory_Reaper_Max_Time(ms)</td>
<td>Maximum time for dispatch reaper to walk dispatch directory and reap stale artifacts.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u username:password

XML Response

...<title>introspection-dispatchreaper</title>
<id>https://localhost:8089/services/server/introspection/search/dispatch/</id>
<updated>2015-08-26T14:34:41-07:00</updated>
<generator build="ced4408678cc212328ba3550d23cba87c24339d4" version="20150826"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/introspection/search/dispatch/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>Dispatch_Directory_Reaper</title>
<updated>2015-08-26T14:34:41-07:00</updated>
<link href="/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/server/introspection/search/dispatch/Dispatch_Directory_Reaper" rel="list"/>
<content type="text/xml">
  <s:dict>
    <s:dict name="Dispatch_Directory_Reaper_Average_Time(ms)"">4.500000</s:dict>
    <s:dict name="Dispatch_Directory_Reaper_Max_Time(ms)"">10</s:dict>
    <s:dict name="eai:acl">
      <s:dict name="app">0</s:dict>
      <s:dict name="can_list">0</s:dict>
      <s:dict name="can_write">1</s:dict>
  </s:dict>
</content>
server/introspection/search/dispatch/Search_StartUp_Time

https://<host>:<mPort>/services/server/introspection/search/dispatch/Search_StartUp_Time

Get average and maximum time for search preprocessing before startup.

Startup time indicates that parsing is complete and the distributed search infrastructure is set up. At startup, Splunk software is ready to wait for responses from indexers.

**GET**

Enumerate average and maximum time for search preprocessing before startup.

**Request parameters**

None

**Returned values**

668
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search_StartUp_Time_Average_Time(ms)</td>
<td>Average time for preprocessing before search startup. Counted from time search state is set to RUNNING.</td>
</tr>
<tr>
<td>Search_StartUp_Time_Max_Time(ms)</td>
<td>Maximum time for preprocessing before search startup. Counted from time search state is set to RUNNING.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u username:password
https://localhost:8089/services/server/introspection/search/dispatch/Search_StartUp_Time

**XML Response**

```xml
...<title>introspection-dispatchreaper</title>
    <id>https://localhost:8089/services/server/introspection/search//dispatch</id>
    <updated>2015-08-26T14:25:14-07:00</updated>
    <generator build="ced4408678cc212328ba3550d23c0c87c24339d4" version="20150826"/>
    <author>
        <name>Splunk</name>
    </author>
    <link href="/services/server/introspection/search//dispatch/_acl" rel="_acl"/>
    <opensearch:totalResults>1</opensearch:totalResults>
    <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
    <opensearch:startIndex>0</opensearch:startIndex>
    <s:messages/>
    <entry>
        <title>Search_StartUp_Time</title>
        <id>https://localhost:8089/services/server/introspection/search//dispatch/Search_StartUp_Time</id>
        <updated>2015-08-26T14:25:14-07:00</updated>
        <link href="/services/server/introspection/search//dispatch/Search_StartUp_Time" rel="alternate"/>
        <author>
            <name>system</name>
        </author>
        <link href="/services/server/introspection/search//dispatch/Search_StartUp_Time" rel="list"/>
        <content type="text/xml">
            <s:dict>
                <s:key name="Search_StartUp_Time_Average_Time(ms)">128.619048</s:key>
                <s:key name="Search_StartUp_Time_Max_Time(ms)">171</s:key>
                <s:key name="eai:acl">
                    <s:dict>
                        <s:key name="app"></s:key>
                        <s:key name="can_list">0</s:key>
                        <s:key name="can_write">1</s:key>
                        <s:key name="modifiable">0</s:key>
                        <s:key name="owner">system</s:key>
                        <s:key name="perms">
                            <s:dict>
                                <s:key name="read">8</s:list>
                                <s:item>*</s:item>
                            </s:list>
                        </s:key>
                    </s:dict>
                </s:key>
            </s:dict>
        </content>
    </entry>
```
server/introspection/search/distributed

https://<host>:<mPort>/services/server/introspection/search/distributed
Get information about the search knowledge bundle replication, if the current instance is the search head. Provides details about maximum and average time to execute routine distributed search methods, including peer info, peer bundles list, and authentication token requests from search heads.

GET
Enumerate routine distributed search method execution times for each peer.

Usage details
The default update period is ten minutes, as defined by the collectionPeriodInSecs attribute in the $SPLUNK_HOME/etc/apps/introspection_generator_addon/default/server.conf file. If startup occurs within the last ten minutes, counts are shown from startup to the current time.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
The following values are listed for each peer.

670
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Get_Authentication_Max_Time(ms)</td>
<td>Maximum time for search head to get authentication from this peer.</td>
</tr>
<tr>
<td>Get_Authentication_Mean_Time(ms)</td>
<td>Average time for search head to get authentication from this peer.</td>
</tr>
<tr>
<td>Get_BundleList_Max_Time(ms)</td>
<td>Maximum time for search head to get bundle list from this peer.</td>
</tr>
<tr>
<td>Get_ServerInfo_Max_Time(ms)</td>
<td>Maximum time for search head to get server information back from this peer.</td>
</tr>
<tr>
<td>Get_ServerInfo_Mean_Time(ms)</td>
<td>Average time for search head to get server information back from this peer.</td>
</tr>
</tbody>
</table>

### Example request and response

**XML Request**

```
curl -k -u username:password https://localhost:8089/services/server/introspection/search/distributed
```

**XML Response**

```
<entry>
  <title>per_searchhead_metrics</title>
  <id>https://localhost:8089/services/server/introspection/search/distributed/per_searchhead_metrics</id>
  <updated>2015-08-26T14:35:48-07:00</updated>
  <link href="/services/server/introspection/search/distributed/per_searchhead_metrics" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/server/introspection/search/distributed/per_searchhead_metrics" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:dict>
        <s:dict>
          <s:dict>
          </s:dict>
          <s:dict>
          </s:dict>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
```
<entry>
<title>window_metrics</title>
{id>https://localhost:8089/services/server/introspection/search/distributed/window_metrics</id>
<updated>2015-08-26T14:35:48-07:00</updated>
<link href="/services/server/introspection/search/distributed/window_metrics" rel="alternate"/>
<author>
<name>system</name>
</author>
<content type="text/xml">
<s:dict>
<s:key name="Get_Authentication_Max_Time(ms)">4</s:key>
<s:key name="Get_Authentication_Mean_Time(ms)">3.400000</s:key>
<s:key name="Get_BundleList_Max_Time(ms)">5</s:key>
<s:key name="Get_BundleList_Mean_Time(ms)">3.800000</s:key>
<s:key name="Get_ServerInfo_Max_Time(ms)">14</s:key>
<s:key name="Get_ServerInfo_Mean_Time(ms)">9.300000</s:key>
</s:dict>
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">0</s:key>
<s:key name="can_write">0</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list/>
</s:key>
</s:dict>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:dict>
</content>
</entry>

<entry>
<title>localhost:8089</title>
{id>https://localhost:8089/services/server/introspection/search/distributed/peer.sv.splunk.com%3A10017</id>
<updated>2015-08-26T14:35:48-07:00</updated>
<link href="/services/server/introspection/search/distributed/peer.sv.splunk.com%3A10017" rel="alternate"/>
<author>
<name>system</name>
</author>
<content type="text/xml">
<s:dict>
<s:key name="Get_Authentication_Max_Time(ms)">4</s:key>
<s:key name="Get_Authentication_Mean_Time(ms)">3.400000</s:key>
<s:key name="Get_BundleList_Max_Time(ms)">5</s:key>
<s:key name="Get_BundleList_Mean_Time(ms)">3.800000</s:key>
<s:key name="Get_ServerInfo_Max_Time(ms)">14</s:key>
<s:key name="Get_ServerInfo_Mean_Time(ms)">9.300000</s:key>
</s:dict>
<s:dict>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">0</s:key>
<s:key name="can_write">0</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list/>
</s:key>
</s:dict>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:dict>
</content>
</entry>
server/introspection/search/saved

https://<host>:<mPort>/services/server/introspection/search/saved
Access most recent scheduled search priority scores and score calculation adjustments.

GET
Enumerate scheduled search details.

Request parameters
None

Returned values
'Note:' These response data keys are for informational purposes only. They are subject to change or removal at any time.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>final_score</td>
<td>Most recent calculated priority score, based on adjustments and original score.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>name</td>
<td>Scheduled search name.</td>
</tr>
<tr>
<td>orig_score</td>
<td>A score based on a search's originally scheduled run time.</td>
</tr>
<tr>
<td>owner</td>
<td>Search scope or context owner. This could be a specific user or &quot;nobody&quot; for a search defined in an app or system-level scope.</td>
</tr>
<tr>
<td>priority_no</td>
<td>Most recent calculated priority number for this search.</td>
</tr>
<tr>
<td>real_time_adj</td>
<td>Real-time search priority adjustment. Real-time searches default to -80000 and continuous scheduled searches default to 0. This particular value is for internal purposes only and is subject to change.</td>
</tr>
<tr>
<td>runtime_adj</td>
<td>Calculated value based on average search runtime.</td>
</tr>
<tr>
<td>skipped_adj</td>
<td>Adjustment for number of times search has been skipped and search period. 0 means the search has not been skipped.</td>
</tr>
<tr>
<td>window_adj</td>
<td>Adjustment for remaining time in search run window.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/server/introspection/search/saved

**XML Response**

```
<title>introspection-savedsearches</title>
{id>https://localhost:8089/services/server/introspection/search/saved</id>
<updated>2015-06-03T16:41:21-07:00</updated>
<generator build="6cfc0237739f" version="6.3.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/introspection/search/saved/_acl" rel="_acl"/>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>admin;search;search_1</title>
  <id>https://localhost:8089/services/server/introspection/search/saved/admin%3Bsearch%3Bsearch_1</id>
  <updated>2015-06-03T16:41:21-07:00</updated>
  <link href="/services/server/introspection/search/saved/admin%3Bsearch%3Bsearch_1" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:...></s:dict>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```
<xml>
  <dict>
    <key name="read">
      <list>
        <item>admin</item>
        <item>splunk-system-role</item>
      </list>
    </key>
    <key name="write">
      <list/>
    </key>
    <key name="removable">0</key>
    <key name="sharing">system</key>
  </dict>
  <key name="final_score">1433294868</key>
  <key name="name">search_1</key>
  <key name="orig_score">1433374860</key>
  <key name="owner">admin</key>
  <key name="priority_no">1</key>
  <key name="real_time_adj">-80000</key>
  <key name="runtime_adj">8</key>
  <key name="skipped_adj">0</key>
  <key name="window_adj">0</key>
</xml>
server/status

https://<host>:<mPort>/services/server/status
List server/status child resources.

GET

Enumerate server/status endpoints.

Request parameters
None

Returned values
Returns /server/status/ child endpoints.

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/status

XML Response

...
server/status/dispatch-artifacts

https://<host>:<mPort>/services/server/status/dispatch-artifacts
Access search job information.

GET
Get information about dispatched search jobs.

Usage details
At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following $SPLUNK_HOME/etc/system/default/server.conf stanza.
collectionPeriodInSecs = 600

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count_realtime</td>
<td>Jobs active in the immediate past observation period, not including historical jobs.</td>
</tr>
<tr>
<td>count_scheduled</td>
<td>Jobs active in the immediate past observation period, not including real-time jobs.</td>
</tr>
<tr>
<td>count_summary</td>
<td>Jobs active in the immediate past observation period, not including non-summary jobs.</td>
</tr>
<tr>
<td>top_apps</td>
<td>Top 15 apps in the past observation period, in <code>app:count</code> key-value pair format.</td>
</tr>
<tr>
<td>top_named_searches</td>
<td>Top 15 named searches in the past observation period, in <code>savedSearchName:count</code> key-value pair format.</td>
</tr>
<tr>
<td>top_users</td>
<td>Top 15 users in the past observation period, in <code>username:count</code> key-value pair format, with <code>count</code> as the number of app contexts for the user.</td>
</tr>
<tr>
<td>total_count</td>
<td>Number of dispatched search jobs since start-up.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/status/dispatch-artifacts

XML Response

...<title>introspection--disk-objects--search-dispatch-artifacts</title>
$id>https://localhost:8089/services/server/status/dispatch-artifacts</id>
$updated>2014-03-25T11:10:33-07:00</updated>
$generator build="200839" version="6.1"/>
$author>
$&lt;name>Splunk</name>
$&lt;/author>
... opensearch elements elided ...
&lt;s:messages/>
&lt;entry&gt;
$&lt;title>result</title>
$id>https://localhost:8089/services/server/status/dispatch-artifacts/result</id>
$updated>2014-03-25T11:10:33-07:00</updated>
$&lt;link href="/services/server/status/dispatch-artifacts/result" rel="alternate"/>
$author>
$&lt;name>system</name>
$&lt;/author>
$&lt;link href="/services/server/status/dispatch-artifacts/result" rel="list"/>
$&lt;content type="text/xml">
server/status/fishbucket

https://<host>:<mPort>/services/server/status/fishbucket

Access information about the private BTree database.

GET

Access private BTree database information.

Usage details
At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following $SPLUNK_HOME/etc/system/default/server.conf stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key_count</td>
<td>Number of file input records (keys) seen since start-up.</td>
</tr>
<tr>
<td>total_size</td>
<td>Total number of file input records (keys).</td>
</tr>
</tbody>
</table>

Example request and response
curl -k -u admin:changeme https://localhost:8089/services/server/status/fishbucket

XML Response

...  
<title>introspection--disk-objects--fishbucket</title>  
<id>https://localhost:8089/services/server/status/fishbucket</id>  
<updated>2014-03-25T11:31:10-07:00</updated>  
<generator build="200839" version="6.1"/>  
<author>  
  <name>Splunk</name>  
</author>  
... opensearch elements elided ...  
<s:messages/>  
<entry>  
  <title>result</title>  
  <id>https://localhost:8089/services/server/status/fishbucket/result</id>  
  <updated>2014-03-25T11:31:10-07:00</updated>  
  <link href="/services/server/status/fishbucket/result" rel="alternate"/>  
  <author>  
    <name>system</name>  
  </author>  
  <link href="/services/server/status/fishbucket/result" rel="list"/>  
  <content type="text/xml">  
    <s:dict>  
      <s:key name="eai:acl">  
        ... elided ...  
      </s:key>  
      <s:key name="key_count">0</s:key>  
      <s:key name="total_size">0.000</s:key>  
    </s:dict>  
  </content>  
</entry>

server/status/installed-file-integrity

Check for system file irregularities.

https://<host>:<mPort>/services/server/status/installed-file-integrity

GET

Check file integrity status.

Usage details

The GET request returns cached results for an automatic check of all files installed with the currently running Splunk software version. The check compares currently installed files against the manifest file located in the $SPLUNK_HOME directory. Based on this comparison, the GET response shows an integrity status indicator for each installed file.

By default, this check runs at startup and results are cached when the check completes. The check takes a few minutes to run and results are available after it completes. The response indicates if initial results are not yet ready when the GET request is performed or if the check is disabled.
You can prompt a new check to run by passing in \?refresh=true with the GET request.

To disable the file integrity check, edit the **installed_files_integrity** setting in the **limits.conf** file.

**Note:** Changing or removing the manifest file prevents the check from working.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>refresh</td>
<td>Boolean</td>
<td>Set to <strong>true</strong> to perform a new file integrity check. Only one such check can be performed at a time.</td>
</tr>
<tr>
<td>regex_filter</td>
<td>PCRE regular expression</td>
<td>Specify a regular expression to filter results of the check. For example, use <code>regex_filter=\.conf$</code> to filter results for configuration files.</td>
</tr>
</tbody>
</table>

**Returned values**

For each installed file, one of the following integrity status indicators is returned.

<table>
<thead>
<tr>
<th>Indicator</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;empty&gt;</td>
<td>Indicates complete file integrity. No irregularities were found.</td>
</tr>
<tr>
<td>access_failed</td>
<td>The <strong>splunkd</strong> process does not have permissions to read the file.</td>
</tr>
<tr>
<td>differs</td>
<td>The installed file differs from the manifest file.</td>
</tr>
<tr>
<td>missing</td>
<td>The installed file was not found.</td>
</tr>
<tr>
<td>read_failed</td>
<td>The installed file comparison failed.</td>
</tr>
<tr>
<td>other_open_failed</td>
<td>A failure other than failure to access or read was encountered when trying to open the file.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:changed https://localhost:8089/services/server/status/installed-file-integrity?refresh=true
```

**XML Response**

The following example is a portion of the response data. The full response lists all installed files and their integrity status.

```
...<s:key name="/opt/splunktest/etc/system/README/inputs.conf.example">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/inputs.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/limits.conf.example">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/limits.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/messages.conf.example">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/props.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/savedsearches.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/server.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/user-prefs.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/README/web.conf.spec">differs</s:key>
<s:key name="/opt/splunktest/etc/system/bin/field_extractor.py">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/app.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/authorize.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/indexes.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/inputs.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/limits.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/messages.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/props.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfserver.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfserver.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfserver.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfserver.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfserver.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:key>
<s:key name="/opt/splunktest/etc/system/default/remoteconfsource.conf">differs</s:ke...
server/status/limits/search-concurrency

https://<host>:<mPort>/services/server/status/limits/search-concurrency
Access search concurrency metrics for a standalone Splunk Enterprise instance.

GET

Get search concurrency limits for a standalone Splunk Enterprise instance.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_auto_summary_searches</td>
<td>Maximum number of auto summary searches.</td>
</tr>
<tr>
<td>max_hist_scheduled_searches</td>
<td>Maximum number of historical scheduled searches.</td>
</tr>
<tr>
<td>max_hist_searches</td>
<td>Maximum number of historical searches.</td>
</tr>
<tr>
<td>max_rt_scheduled_searches</td>
<td>Maximum number of scheduled searches.</td>
</tr>
<tr>
<td>max_rt_searches</td>
<td>Maximum number of real-time searches.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/status/limits/search-concurrency

XML Response

...<title>server-status-limits-concurrency</title>
  <id>https://localhost:8089/services/server/status/limits/search-concurrency</id>
  <updated>2014-03-25T11:40:16-07:00</updated>
  <generator build="200839" version="6.1"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch elements elided ...
</entry>
Access disk utilization information for filesystems that have Splunk objects, such as indexes, volumes, and logs. A filesystem can span multiple physical disk partitions.

**GET**

Get disk utilization information.

**Usage details**

At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following `$SPLUNK_HOME/etc/system/default/server.conf` stanza.

```
[introspection:generator:disk_objects]
collectionPeriodInSecs = 600
```

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>capacity</td>
<td>Disk capacity (MB).</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>free</td>
<td>Disk free space (MB).</td>
</tr>
<tr>
<td>fs_type</td>
<td>File system type. Example values:</td>
</tr>
<tr>
<td></td>
<td>• Linux: ext2, ext3, ext4, qnx4</td>
</tr>
<tr>
<td></td>
<td>• Solaris: ufs, zfs</td>
</tr>
<tr>
<td></td>
<td>• Windows: ntfs, fat32</td>
</tr>
<tr>
<td></td>
<td>• AIX: jfs</td>
</tr>
<tr>
<td></td>
<td>• (not OS-specific) WORM: ISO9660, UDF13346</td>
</tr>
<tr>
<td></td>
<td>• (not OS-specific); network-shared: SMB, CIFS, NFS</td>
</tr>
<tr>
<td></td>
<td>• (not OS-specific) Veritas: VxFS.</td>
</tr>
<tr>
<td>mount_point</td>
<td>Absolute path of the directory where this partition is mounted.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/server/status/partitions-space
```

**XML Response**

```
...<title>introspection--disk-objects--partitions-space</title>
{id}https://localhost:8089/services/server/status/partitions-space</id>
<updated>2014-03-25T11:43:39-07:00</updated>
<generator build="200839" version="6.1"/>
<author>
    <name>Splunk</name>
</author>
... opensearch elements elided ...
<s:messages/>
<entry>
    <title>0</title>
    <id>https://localhost:8089/services/server/status/partitions-space/0</id>
    <updated>2014-03-25T11:43:39-07:00</updated>
    <link href="/services/server/status/partitions-space/0" rel="alternate"/>
    <author>
        <name>system</name>
    </author>
    <link href="/services/server/status/partitions-space/0" rel="list"/>
    <content type="text/xml">
        <s:dict>
            <s:key name="capacity">104901.000</s:key>
            <s:key name="eai:acl">
                ... elided ...
            </s:key>
            <s:key name="free">7774.000</s:key>
            <s:key name="fs_type">ntfs</s:key>
            <s:key name="mount_point">C:\</s:key>
        </s:dict>
    </content>
</entry>
```
server/status/resource-usage

https://<host>:<mPort>/services/server/status/resource-usage
Get current resource (CPU, RAM, VM, I/O, file handle) utilization for entire host, and per Splunk-related processes.

GET
Get resource utilization information.

Usage details
At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following $SPLUNK_HOME/etc/system/default/server.conf stanza.

[introspection:generator:disk_objects]
collectionPeriodInSecs = 600

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
Returns a list of server/status/resource-usage/ endpoints.

Example request and response

XML Request
curl -k -u admin:changeme https://localhost:8089/services/server/status/resource-usage

XML Response

...
server/status/resource-usage/hostwide

https://<host>:<mPort>/services/server/status/resource-usage/hostwide
Access host-level dynamic CPU utilization and paging information.

GET
Get host-level, dynamic CPU utilization and paging information.

Usage details
At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following $SPLUNK_HOME/etc/system/default/server.conf stanza.

[introspection:generator:disk_objects]
collectionPeriodInSecs = 600

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_arch</td>
<td>CPU architecture</td>
</tr>
<tr>
<td>cpu_count</td>
<td>CPU count</td>
</tr>
<tr>
<td>cpu_idle_pct</td>
<td>Percentage of time CPU is idle. Value reported as 100.0 on Windows except for Vista+ and XP/Win2003 English-only operating systems.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>cpu_system_pct</td>
<td>Percentage of time CPU is running in system mode. Missing from Windows except for Vista+ and XP/Win2003 English-only operating systems.</td>
</tr>
<tr>
<td>cpu_user_pct</td>
<td>Percentage of time CPU is running in user mode. Missing from Windows except for Vista+ and XP/Win2003 English-only operating systems.</td>
</tr>
<tr>
<td>forks</td>
<td>Cumulative number of forked processes since OS startup. Not available on Windows.</td>
</tr>
<tr>
<td>mem</td>
<td>Total physical memory available (MB)</td>
</tr>
<tr>
<td>mem_used</td>
<td>Total physical memory used (MB). This value represents the amount of actual physical memory minus the amount of physical memory currently available. This is the amount of physical memory that can be immediately reused without having to first write its contents to disk.</td>
</tr>
<tr>
<td>normalized_load_avg_1min</td>
<td>Normalized load average of runnable_process_count across all cores (cumulative_load_avg / number_of_cores). This value is not reliable for a VM guest.</td>
</tr>
<tr>
<td>os_build</td>
<td>Software build for the os_version</td>
</tr>
<tr>
<td>os_name</td>
<td>Operating system name</td>
</tr>
<tr>
<td>os_name_ext</td>
<td>Extended operating system name</td>
</tr>
<tr>
<td>os_version</td>
<td>Operating system version</td>
</tr>
<tr>
<td>pg_paged_out</td>
<td>Cumulative VM page count paged since OS startup. Not available on Windows.</td>
</tr>
<tr>
<td>pg_swapped_out</td>
<td>Cumulative pages swapped out since OS startup. Not available on Windows.</td>
</tr>
<tr>
<td>runnable_process_count</td>
<td>Number of process running or in the runnable queue. Value reported as 1 on Windows except for Vista+ and XP/Win2003 English-only operating systems.</td>
</tr>
<tr>
<td>splunk_version</td>
<td>Currently installed Splunk software version</td>
</tr>
<tr>
<td>swap</td>
<td>Amount of disk allocated to swap (fractional MB)</td>
</tr>
<tr>
<td>swap_used</td>
<td>Swap space currently in use (fractional MB)</td>
</tr>
<tr>
<td>virtual_cpu_count</td>
<td>Virtual CPU count</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:changeme https://localhost:8089/services/server/status/resource-usage/hostwide
```

**XML Response**

```xml
<title>introspection--resource-usage--hostwide</title>
<id>https://localhost:8089/services/server/status/resource-usage/hostwide</id>
<updated>2016-09-19T12:56:56-07:00</updated>
<generator build="bf83e168dd2e" version="6.5.0"/>
<author>
```
<name>Splunk</name>
</author>
<link href="/services/server/status/resource-usage/hostwide/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>result</title>
<id>https://localhost:8089/services/server/status/resource-usage/hostwide/result</id>
<updated>2016-09-19T12:56:56-07:00</updated>
<link href="/services/server/status/resource-usage/hostwide/result" rel="alternate"/>
<author>
<name>system</name>
</author>
<link href="/services/server/status/resource-usage/hostwide/result" rel="list"/>
<content type="text/xml">
<s:dict>
<s:key name="cpu_arch">x86_64</s:key>
<s:key name="cpu_count">4</s:key>
<s:key name="cpu_idle_pct">99.37</s:key>
<s:key name="cpu_system_pct">0.25</s:key>
<s:key name="cpu_user_pct">0.38</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list/>
</s:key>
</s:dict>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
<s:key name="forks">16462040</s:key>
<s:key name="instance_guid">88F85972-368E-45F8-A123-FDB14AE9701E</s:key>
<s:key name="mem">7872.781</s:key>
<s:key name="mem_used">929.883</s:key>
<s:key name="normalized_load_avg_1min">0.00</s:key>
<s:key name="os_build">#1 SMP Fri Aug 24 01:07:11 UTC 2012</s:key>
<s:key name="os_name">Linux</s:key>
<s:key name="os_name_ext">Linux</s:key>
<s:key name="os_version">2.6.32-279.5.2.el6.x86_64</s:key>
<s:key name="pg_paged_out">732923572</s:key>
<s:key name="pg_swapped_out">0</s:key>
<s:key name="runnable_process_count">1</s:key>
<s:key name="splunk_version">6.5.0</s:key>
<s:key name="swap">4031.992</s:key>
<s:key name="swap_used">0.000</s:key>
<s:key name="virtual_cpu_count">4</s:key>
</s:dict>
</content>
server/status/resource-usage/iostats

https://<host>:<mPort>/services/server/status/resource-usage/iostats

Access the most recent disk I/O statistics for each disk. This endpoint is currently supported for Linux, Windows, and Solaris. By default this endpoint is updated every 60s seconds.

GET

Get disk I/O statistics.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>avg_service_ms</td>
<td>Average time requests caused the CPU to be in use, in milliseconds.</td>
</tr>
<tr>
<td>avg_total_ms</td>
<td>Average queue + execution time for requests to be completed, in milliseconds.</td>
</tr>
<tr>
<td>cpu_pct</td>
<td>Percentage of time the CPU was servicing requests.</td>
</tr>
<tr>
<td>device</td>
<td>Device name (e.g., as listed under /dev on UNIX).</td>
</tr>
<tr>
<td>fs_type</td>
<td>Mounted device file system type.</td>
</tr>
<tr>
<td>interval</td>
<td>Interval over which sampling occurred, in seconds.</td>
</tr>
<tr>
<td>mount_point</td>
<td>Mount point(s) of the underlying device.</td>
</tr>
<tr>
<td>reads_kb_ps</td>
<td>Total number of kb read per second.</td>
</tr>
<tr>
<td>reads_ps</td>
<td>Number of read requests per second.</td>
</tr>
<tr>
<td>writes_kb_ps</td>
<td>Total number of kb written per second.</td>
</tr>
<tr>
<td>writes_ps</td>
<td>Number of write requests per second.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -k -u username:password https://localhost:8089/services/server/status/resource-usage/iostats
```

XML Response

689
...<title>introspection--resource-usage--iostats</title>
<id>https://localhost:8089/services/server/status/resource-usage/iostats/id</id>
<updated>2015-09-11T14:45:04:00+00:00</updated>
<generator build="78167cb4239c44472aa42425ebc83481b2d83433" version="20150910"/>

<author>
<title>Splunk</title>
</author>
<link href="/services/server/status/resource-usage/iostats/_acl" rel="_acl"/>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<entry>
<title>0</title>
<id>https://localhost:8089/services/server/status/resource-usage/iostats/0/id</id>
<updated>2015-09-11T14:45:04:00+00:00</updated>
<link href="/services/server/status/resource-usage/iostats/0" rel="alternate"/>
<author>
<title>system</title>
</author>
<link href="/services/server/status/resource-usage/iostats/0" rel="list"/>
<content type="text/xml">
<s:dict>
<s:key name="avg_service_ms">0.142</s:key>
<s:key name="avg_total_ms">4.110</s:key>
<s:key name="cpu_pct">0.05</s:key>
<s:key name="device">/dev/sda1</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write"></s:key>
</s:dict>
</s:key>
<s:key name="fs_type">xfs</s:key>
<s:key name="interval">60</s:key>
<s:key name="mount_point">/</s:key>
<s:key name="reads_kb_ps">0.000</s:key>
<s:key name="reads_ps">0.000</s:key>
<s:key name="writes_kb_ps">43.050</s:key>
<s:key name="writes_ps">3.633</s:key>
</s:dict>
</entry>
server/status/resource-usage/splunk-processes

https://<host>:<mPort>/services/server/status/resource-usage/splunk-processes
Access operating system resource utilization information.

GET
Get process operating system resource utilization information.

Usage details
At least one observation period must pass after startup for valid endpoint data to be available. The observation period is defined in the following $SPLUNK_HOME/etc/system/default/server.conf stanza:

[introspection:generator:disk_objects]
collectionPeriodInSecs = 600

The default period is 10 seconds, but 10 minutes (600 seconds) on a Universal Forwarder.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>args</td>
<td>Non-search process arguments.</td>
</tr>
<tr>
<td>cpu_system_time</td>
<td>Cumulative time this process has spent executing in kernel (incl. system calls). Extra field.</td>
</tr>
<tr>
<td>cpu_user_time</td>
<td>Cumulative time this process has spent executing in user space (incl. library functions). Extra field.</td>
</tr>
<tr>
<td>elapsed</td>
<td>Elapsed wall time, accurate to within the collection period.</td>
</tr>
<tr>
<td>fd_used</td>
<td>Number of currently open files used by this process.</td>
</tr>
<tr>
<td>label</td>
<td>Human-readable label for the saved search.</td>
</tr>
<tr>
<td>mem_unshared_data_used</td>
<td>Amount of heap and stack used. Not available on Windows. Extra field.</td>
</tr>
<tr>
<td>mem_used</td>
<td>Current amount of resident physical memory used (KB). (Usually far less deceiving than virtual memory because operating systems can be liberal with virtual memory size but never with resident memory size.) On Windows, mem_used is obtained by reading the WorkingSetSize property returned by the GetProcessMemoryInfo() function (see GetProcessMemoryInfo function and PROCESS_MEMORY_COUNTERS structure).</td>
</tr>
<tr>
<td>normalized_pct_cpu</td>
<td>Percentage of CPU usage across all cores. 100% is equivalent to all CPU resources on the machine.</td>
</tr>
<tr>
<td>page_faults</td>
<td>Number of major page faults. Extra field.</td>
</tr>
<tr>
<td>pct_cpu</td>
<td>Percentage of CPU usage, relative to one core. 100% is equivalent to 1 core.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>pct_memory</td>
<td>Percentage of physical memory used hostwide ( \left( \frac{\text{mem_used}}{\text{available_host_memory}} \right) \times 100 ).</td>
</tr>
<tr>
<td>pid</td>
<td>Process ID.</td>
</tr>
<tr>
<td>ppid</td>
<td>Parent process ID. Not available for all processes.</td>
</tr>
<tr>
<td>process</td>
<td>Process name. The .exe suffix is stripped on Windows operating systems.</td>
</tr>
<tr>
<td>read_mb</td>
<td>Amount of data read (MB), excluding cache reads.</td>
</tr>
<tr>
<td>search_head</td>
<td>Dispatching search head for processes running saved searches.</td>
</tr>
<tr>
<td>search_props</td>
<td>Search properties map of the following key value pairs.</td>
</tr>
<tr>
<td>status</td>
<td>Status from the OS scheduler. Can be R (runnable or running), W (waiting), stopped, Z (zombie), or O (other). W includes voluntary sleep or blocking on I/O. O means status is knowable but does not fit into one of those categories. Not available on Windows.</td>
</tr>
<tr>
<td>t_count</td>
<td>Current number of threads.</td>
</tr>
<tr>
<td>written_mb</td>
<td>Amount of data written (MB), excluding canceled writes.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/server/status/resource-usage/splunk-processes/0
```
server/sysinfo

https://<host>:<mPort>/services/server/sysinfo

Exposes relevant information about the resources and OS settings of the machine where Splunk Enterprise is running.

Usage details

693
This endpoint provides status information for the server where the current Splunk instance is running. The GET request response includes Kernel Transparent Huge Pages (THP) and ulimit status.

**Note:** Some properties returned by this endpoint are also returned by `server/info`. However, the `server/info` endpoint is meant to provide information on the currently running Splunk instance and not the machine where the instance is running. Server status values returned by `server/info` should be considered deprecated and might not continue to be accessible from this endpoint. Use the `server/sysinfo` endpoint for server information instead.

**GET**

Access server details.

**Request parameters**

None.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_arch</td>
<td>Server CPU architecture.</td>
</tr>
<tr>
<td>numberOfCores</td>
<td>Number of server processor cores. Not applicable if host is a VM guest. A value of 0 is returned if the number cannot be accessed and the access failure reason is logged to splunkd.log.</td>
</tr>
<tr>
<td>numberOfVirtualCores</td>
<td>Number of server virtual cores.</td>
</tr>
<tr>
<td>os_build</td>
<td>Software build for the server os_version.</td>
</tr>
<tr>
<td>os_name</td>
<td>Server operating system name.</td>
</tr>
<tr>
<td>os_name_extended</td>
<td>Server operating system name.</td>
</tr>
<tr>
<td>os_version</td>
<td>Server operating system version.</td>
</tr>
<tr>
<td>physicalMemoryMB</td>
<td>Server physical memory (MB). The same value is returned as the mem field from server/status/resource-usage/hostwide. A value of 0 is returned if the number cannot be accessed and the access failure reason is logged to splunkd.log.</td>
</tr>
<tr>
<td>transparent_hugepages</td>
<td>For Linux systems, includes the following THP status indicators. • defrag • effective_state • enabled</td>
</tr>
<tr>
<td></td>
<td>For non-Linux systems, effective_state is set to ok</td>
</tr>
<tr>
<td>ulimits</td>
<td>On all UNIX systems, lists settings for the following ulimits in place on splunkd at runtime. • core_file_size • cpu_time • data_file_size • data_segment_size • nice • open_files • resident_memory_size • stack_size • user_processes</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>virtual_address_space_size</td>
<td></td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:changed https://localhost:8089/services/server/sysinfo

**XML Response**

```xml
...
<title>system-info</title>
{id>https://localhost:8089/services/server/sysinfo</id>
<updated>2016-09-08T15:28:11-07:00</updated>
<generator build="19e4b5854495" version="6.5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/sysinfo/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>system-info</title>
{id>https://localhost:8089/services/server/sysinfo/system-info</id>
<updated>2016-09-08T15:28:11-07:00</updated>
<link href="/services/server/sysinfo/system-info" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/server/sysinfo/system-info" rel="list"/>
<content type="text/xml">
<s:dict>
  <s:key name="cpu_arch">x86_64</s:key>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app"></s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">0</s:key>
      <s:key name="owner">system</s:key>
      <s:key name="perms">
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>admin</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:key>
          <s:key name="write"></s:list/>
        </s:dict>
      </s:key>
      <s:key name="removable">0</s:key>
      <s:key name="sharing">system</s:key>
```
services/saved/bookmarks/monitoring_console

https://<host>:<mPort>/services/saved/bookmarks/monitoring_console
Add URLs that link to monitoring consoles of your other deployments. For example, if you're admin overseeing multiple separate Splunk deployments for different teams.

GET
List deployment bookmarks.

Request parameters

Optional request parameters:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Number</td>
<td>Number of bookmark URLs to list.</td>
</tr>
<tr>
<td>offset</td>
<td>Number</td>
<td>Lists bookmark URLs, offset from the first bookmark.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>search</td>
<td>String</td>
<td>Items to search for, must be valid as SPL.</td>
</tr>
<tr>
<td>sort_dir</td>
<td>Enum</td>
<td>asc or desc; ascending or descending</td>
</tr>
<tr>
<td>sort_key</td>
<td>String</td>
<td>Key to sort on, must be existing key in the stanza</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/saved/bookmarks/monitoring_console

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
<title>bookmarks-mc</title>
<id>https://qa-ubuntu-022:8089/services/saved/bookmarks/monitoring_console</id>
<updated>2019-10-13T16:47:42-07:00</updated>
<generator build="324da9f5a506" version="8.0.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/saved/bookmarks/monitoring_console/_new" rel="create"/>
<link href="/services/saved/bookmarks/monitoring_console/_reload" rel="_reload"/>
<link href="/services/saved/bookmarks/monitoring_console/_acl" rel="_acl"/>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>deployment-2</title>
<id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="alternate"/>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_edit" rel="edit"/>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/remove" rel="remove"/>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/disable" rel="disable"/>
<content type="text/xml">
  <s:d:dict>
    <s:key name="eai:acl">
      <s:d:dict>
        <s:key name="app">search</s:key>
        <s:key name="can_change_perms">1</s:key>
      </s:d:dict>
    </s:key>
  </s:d:dict>
</content>
</entry>
</feed>
```
POST

Add deployment bookmark URLs.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Name of the deployment bookmark.</td>
</tr>
<tr>
<td>url</td>
<td>string</td>
<td>Full URL to the monitoring console of a different Splunk deployment.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/saved/bookmarks/monitoring_console -d
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"/>
<title>bookmarks-mc</title>
<id>https://localhost:8089/services/saved/bookmarks/monitoring_console</id>
<updated>2019-10-13T16:16:38-07:00</updated>
<generator build="324da9f5a506" version="8.0.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/saved/bookmarks/monitoring_console/_new" rel="create"/>
<link href="/services/saved/bookmarks/monitoring_console/_reload" rel="_reload"/>
```
<link href="/services(saved/bookmarks/monitoringconsole/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>deployment-2</title>
<id>https://localhost:8089/servicesNS/nobody/search/saved/bookmarks/monitoringconsole/deployment-2</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoringconsole/deployment-2" rel="alternate"/>
<author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoringconsole/deployment-2" rel="list"/>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoringconsole/deployment-2/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoringconsole/deployment-2" rel="edit"/>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoringconsole/deployment-2" rel="remove"/>
<link href="/servicesNS/nobody/search/saved/bookmarks/monitoringconsole/deployment-2/disable" rel="disable"/>
<content type="text/xml">
<s:dict>
  <s:field name="eai:acl">
    <s:dict>
      <s:field name="app">search</s:field>
      <s:field name="can_change_perms">1</s:field>
      <s:field name="can_list">1</s:field>
      <s:field name="can_share_app">1</s:field>
      <s:field name="can_share_global">1</s:field>
      <s:field name="can_share_user">0</s:field>
      <s:field name="can_write">1</s:field>
      <s:field name="modifiable">1</s:field>
      <s:field name="owner">nobody</s:field>
      <s:field name="perms">
        <s:dict>
          <s:field name="read">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:field>
          <s:field name="write">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:field>
          <s:field name="removable">1</s:field>
          <s:field name="sharing">app</s:field>
        </s:dict>
      </s:field>
    </s:dict>
  </s:field>
</s:dict>
</content>
</entry>
</feed>
DELETE

Remove deployment bookmark URLs.

Request parameters

None

Returned values

None

Example request and response

XML Request

curl -k -u admin:pass --request DELETE https://localhost:8089/services/saved/bookmarks/monitoring_console/{name}

XML Response

<title>bookmarks-mc</title>
<id>https://localhost:8089/services/saved/bookmarks/monitoring_console</id>
<updated>2019-10-13T16:25:38-07:00</updated>
<generator build="334da9f5a506" version="8.0.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/saved/bookmarks/monitoring_console/_new" rel="create"/>
<link href="/services/saved/bookmarks/monitoring_console/_reload" rel="_reload"/>
<link href="/services/saved/bookmarks/monitoring_console/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>deployment-2</title>
  <id>https://localhost:8089/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2" rel="alternate"/>
  <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/_edit" rel="edit"/>
  <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/remove" rel="remove"/>
  <link href="/servicesNS/nobody/search/saved/bookmarks/monitoring_console/deployment-2/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
    </s:dict>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="app">search</s:key>
    <s:key name="can_change_perms">1</s:key>
    <s:key name="can_list">1</s:key>
    <s:key name="can_share_app">1</s:key>
    <s:key name="can_share_global">1</s:key>
    <s:key name="can_share_user">0</s:key>
    <s:key name="can_write">1</s:key>
    <s:key name="modifiable">1</s:key>
    <s:key name="owner">nobody</s:key>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>*</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="removable">1</s:key>
    <s:key name="sharing">app</s:key>
  </s:dict>
  <s:key name="url">https://deployment-2-host:8000/en-US/app/splunk_monitoring_console</s:key>
</s:dict>
</content>
</entry>
</feed>
Knowledge endpoints

Knowledge endpoint descriptions

Work with searches and other knowledge objects.

- Define data configurations indexed and searched by the Splunk platform.
- Manage how data is handled, using look-ups, field extractions, field aliases, sourcetypes, and transforms.
- Manage saved event types.
- Manage search field configurations and search time tags.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select Settings > Access controls and click Users. To determine the capabilities assigned to a role, select Settings > Access controls and click Roles.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

Managed Splunk Cloud deployments

https://<deployment-name>.splunkcloud.com:8089

Self-service Splunk Cloud deployments

To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the the Splunk REST API Tutorials for more information.
admin/summarization

https://<host>:<mPort>/services/admin/summarization/?by_tstats=1

Get aggregated details about all global accelerated data model summaries.

Authentication and authorization
Authorization to access data model acceleration information is role-based.

GET

Get a list of field:value pairs that provide details about accelerated data models and their summaries.

Request parameters
None.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>search</td>
<td>The data models, represented as search strings.</td>
</tr>
<tr>
<td>summary.access_count</td>
<td>The total number of times that the summary for each data model has been accessed.</td>
</tr>
<tr>
<td>summary.access_time</td>
<td>The last time that the summary of each data model was accessed.</td>
</tr>
<tr>
<td>summary.average_time</td>
<td>The average runtime of the past 48 summarization search jobs for this data model.</td>
</tr>
<tr>
<td>summary.buckets</td>
<td>The total number of buckets in the summaries of each data model.</td>
</tr>
<tr>
<td>summary.buckets_size</td>
<td>The total size of the buckets in the summaries of each data model. The size is reported in terms of megabytes (MB).</td>
</tr>
<tr>
<td>summary.complete</td>
<td>Reports whether or not the summaries for each data model are complete.</td>
</tr>
<tr>
<td>summary.earliest_time</td>
<td>The timestamp of the earliest event in the summaries for each data model.</td>
</tr>
<tr>
<td>summary.id</td>
<td>The ID of the data models being summarized. The format is DM_&lt;app_name&gt;_&lt;data_model_ID&gt;.</td>
</tr>
<tr>
<td>summary.is_inprogress</td>
<td>Indicates whether or not the summary build is currently in progress for each data model.</td>
</tr>
<tr>
<td>summary.last_error</td>
<td>Lists errors that were logged in the latest run (from last_sid) of the summary creation search.</td>
</tr>
<tr>
<td>summary.last_sid</td>
<td>The SID of the latest creation search job for each data model summary.</td>
</tr>
<tr>
<td>summary.latest_time</td>
<td>The timestamp of the latest events in each data model summary.</td>
</tr>
<tr>
<td>summary.latest_dispatch_time</td>
<td>The timestamp of the latest summary creation search for each data model.</td>
</tr>
<tr>
<td>summary.latest_run_duration</td>
<td>The runtime of the latest summary creation search for each data model.</td>
</tr>
<tr>
<td>summary.mod_time</td>
<td>The last time each data model summary was modified.</td>
</tr>
<tr>
<td>summary.p50</td>
<td>The 50th percentile of summarization search runtimes for each data model. 50 percent of the summarization searches for a given data model had runtimes that were less than this value.</td>
</tr>
<tr>
<td>summary.p90</td>
<td>The 90th percentile of summarization search runtimes for each data model. 90 percent of the summarization searches for a given data model had runtimes that were less than this value.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>summary.run_stats</td>
<td>The start and duration of all saved previous summarization search jobs, up to 100 jobs.</td>
</tr>
<tr>
<td>summary.size</td>
<td>The total size of each summary, in bytes.</td>
</tr>
<tr>
<td>summary.time_range</td>
<td>The range of time covered by each summary.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/admin/summarization/?by_tstats=1
```

**XML Response**

```xml
  <title>summarization</title>
  <id>https://localhost:8089/services/admin/summarization</id>
  <updated>2015-06-01T15:21:20-07:00</updated>
  <generator build="e343948e242181aa7b94257ede83830605c853d9" version="20150526"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/admin/summarization/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>tstats:DM_search_mydatamodel</title>
    <id>https://localhost:8089/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel</id>
    <updated>2015-06-01T15:21:20-07:00</updated>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel" rel="list"/>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel" rel="remove"/>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel/details" rel="details"/>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel/reschedule" rel="reschedule"/>
    <link href="/servicesNS/nobody/search/admin/summarization/tstats%3ADM_search_mydatamodel/touch" rel="touch"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="disabled">0</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app">search</s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
admin/summarization/tstats:DM_{app}_{data_model_ID}

https://<host>:<mPort>/services/admin/summarization/tstats:DM_{app}_{data_model_ID}

Review information about the summaries of a specific data model. Identify specific data models by providing their app short name and their data model ID.

Authentication and authorization
Authorization to access data model acceleration information is role-based.

GET

Get detailed information about the acceleration summaries of a specific datamodel. See statistics about data model usage and information about the latest summary creation run.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
**app**
required string The short name of the app to which this data set belongs.

**data model ID**
required string The ID of the data model.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>search</td>
<td>The data model, represented as a search string.</td>
</tr>
<tr>
<td>summary.access_count</td>
<td>The total number of times that the summary for this data model has been accessed.</td>
</tr>
<tr>
<td>summary.access_time</td>
<td>The last time that the summary of this data model was accessed.</td>
</tr>
<tr>
<td>summary.average_time</td>
<td>The average runtime of the past 48 summarization search jobs for this data model.</td>
</tr>
<tr>
<td>summary.buckets</td>
<td>The total number of buckets in the summary of this data model.</td>
</tr>
<tr>
<td>summary.buckets_size</td>
<td>The total size of the buckets in the summary of this data model. The size is reported in terms of megabytes (MB).</td>
</tr>
<tr>
<td>summary.complete</td>
<td>Reports whether or not the summary for the data model are complete.</td>
</tr>
<tr>
<td>summary.earliest_time</td>
<td>The timestamp of the earliest event in the summary for this data model.</td>
</tr>
<tr>
<td>summary.id</td>
<td>The ID of the data model being summarized. The format is DM_&lt;app_name&gt;_data_model_ID.</td>
</tr>
<tr>
<td>summary.is_inprogress</td>
<td>Indicates whether or not the data model summary build is currently in progress.</td>
</tr>
<tr>
<td>summary.last_error</td>
<td>Lists errors that were logged in the latest run (from last_sid) of the summary creation search.</td>
</tr>
<tr>
<td>summary.last_sid</td>
<td>The SID of the latest data model summary creation search job.</td>
</tr>
<tr>
<td>summary.latest_time</td>
<td>The timestamp of the latest event in the data model summary.</td>
</tr>
<tr>
<td>summary.latest_dispatch_time</td>
<td>The timestamp of the latest summary creation search for the data model.</td>
</tr>
<tr>
<td>summary.latest_run_duration</td>
<td>The runtime of the latest summary creation search for the data model.</td>
</tr>
<tr>
<td>summary.mod_time</td>
<td>The last time the data model summary was modified.</td>
</tr>
<tr>
<td>summary.p50</td>
<td>The 50th percentile of summarization search runtimes for the data model. 50 percent of the summarization searches for this data model had runtimes that were less than this value.</td>
</tr>
<tr>
<td>summary.p90</td>
<td>The 90th percentile of summarization search runtimes for the data model. 90 percent of the summarization searches for this data model had runtimes that were less than this value.</td>
</tr>
<tr>
<td>summary.run_stats</td>
<td>The start and duration of all saved previous summarization search jobs, up to 100 jobs.</td>
</tr>
<tr>
<td>summary.size</td>
<td>The total size of the summary, in bytes.</td>
</tr>
<tr>
<td>summary.time_range</td>
<td>The range of time covered by the summary.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
```

**XML Response**

707
...
"test" | fields nodename, _time, host, source, sourcetype
<s:key name="summary.access_count">0</s:key>
<s:key name="summary.access_time">0</s:key>
<s:key name="summary.average_time">3.028</s:key>
<s:key name="summary.buckets">11</s:key>
<s:key name="summary.buckets_size">461</s:key>
<s:key name="summary.complete">1</s:key>
<s:key name="summary.earliest_time">1565398764</s:key>
<s:key name="summary.id">DM_search_test_new_accel</s:key>
<s:key name="summary.is_inprogress">0</s:key>
<s:key name="summary.last_error">[ronnie.sv.splunk.com] A second test error message just because.
[ronnie.sv.splunk.com] Test error message in remote server.</s:key>
<s:key name="summary.last_sid">scheduler__nobody__search__RMD5837da1d4b8a764d1_at_1565733480_379</s:key>
<s:key name="summary.latest_dispatch_time">1565733481</s:key>
<s:key name="summary.latest_run_duration">5.691</s:key>
<s:key name="summary.latest_time">1565730106</s:key>
<s:key name="summary.mod_time">1565733421</s:key>
<s:key name="summary.p50">1.287</s:key>
<s:key name="summary.p90">5.859</s:key>
<s:key name="summary.run_stats">
  <s:dict>
    <s:key name="1565730661">
      <s:dict>
        <s:key name="dispatch_time">1565730661</s:key>
        <s:key name="run_duration">0.357</s:key>
      </s:dict>
    </s:key>
    <s:key name="1565730721">
      <s:dict>
        <s:key name="dispatch_time">1565730721</s:key>
        <s:key name="run_duration">0.240</s:key>
      </s:dict>
    </s:key>
    <s:key name="1565730780">
      <s:dict>
        <s:key name="dispatch_time">1565730780</s:key>
        <s:key name="run_duration">0.253</s:key>
      </s:dict>
    </s:key>
    <s:key name="1565730840">
      <s:dict>
        <s:key name="dispatch_time">1565730840</s:key>
        <s:key name="run_duration">0.247</s:key>
      </s:dict>
    </s:key>
    <s:key name="1565730900">
      <s:dict>
        <s:key name="dispatch_time">1565730900</s:key>
        <s:key name="run_duration">0.233</s:key>
      </s:dict>
    </s:key>
    <s:key name="1565730960">
      <s:dict>
        <s:key name="dispatch_time">1565730960</s:key>
        <s:key name="run_duration">0.266</s:key>
      </s:dict>
    </s:key>
  </s:dict>
</s:key>
<s:key name="summary.run_duration">0.268</s:key>
Access lookup table files.

**GET**

List lookup table files.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:appName</td>
<td>The app for which the lookup table applies.</td>
</tr>
<tr>
<td>eai:data</td>
<td>The source path for the lookup staging area. The lookup table file is moved from here into $SPLUNK_HOME.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The Splunk user who created the lookup table.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/lookup-table-files
```

**XML Response**

```
...<title>lookup-table-files</title>
<id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files</id>
<updated>2011-07-21T19:26:11-07:00</updated>
<generator version="104309"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>
```
POST

Create a lookup table file by moving a file from the upload staging area into $SPLUNK_HOME.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:data</td>
<td>String</td>
<td></td>
<td>Move a lookup table file from the given path into $SPLUNK_HOME. This path must have the lookup staging area as an ancestor.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>The lookup table filename.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:appName</td>
<td>The app for which the lookup table applies.</td>
</tr>
<tr>
<td>eai:data</td>
<td>The source path for the lookup staging area. The lookup table file is moved from here into $SPLUNK_HOME.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The Splunk user who created the lookup table.</td>
</tr>
</tbody>
</table>

Example request and response
**XML Request**

```bash
```

**XML Response**

```xml
... <title>lookup-table-files</title>  
<id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files</id>  
<updated>2011-07-21T18:26:35-07:00</updated>  
<generator version="104309"/>  
<author>  
 <name>Splunk</name>  
</author>  
<link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>  
<link href="/servicesNS/admin/search/data/lookup-table-files/_reload" rel="_reload"/>  
... opensearch nodes elided ...  
<s:messages/>  
<entry>  
<title>lookup.csv</title>  
<id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv</id>  
<updated>2011-07-21T18:26:35-07:00</updated>  
<link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="alternate"/>  
<author>  
 <name>admin</name>  
</author>  
<link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="list"/>  
<link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/_reload" rel="_reload"/>  
<link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="edit"/>  
<link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="remove"/>  
<link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/move" rel="move"/>  
<content type="text/xml">  
<s:dict>  
... eai:acl node elided ...  
<s:key name="eai:appName">search</s:key>  
<s:key name="eai:data"><![[/opt/splunk/etc/users/admin/search/lookups/lookup.csv]]>  
<s:key name="eai:userName">admin</s:key>  
</s:dict>  
</content>  
</entry>  
</feed>  
```

**data/lookup-table-files/**{name}**

https://<host>:<mPort>/services/data/lookup-table-files/{name}

Manage the {name} lookup table file.
DELETE

Delete the named lookup table file.

Request parameters

None

Returned values

None

Example request and response

XML Request

curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>lookup-table-files</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files</id>
  <updated>2011-07-21T18:43:11-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/lookup-table-files/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>

GET

List a single lookup table file.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

713
### eai:appName
The app for which the lookup table applies.

### eai:attributes
Field control information.

### eai:data
The source path for the lookup staging area. The lookup table file is moved from here into $SPLUNK_HOME.

### eai:userName
The Splunk user who created the lookup table.

---

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv
```

**XML Response**

```xml
...<title>lookup-table-files</title>
   <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv</id>
   <updated>2011-07-21T18:37:25-07:00</updated>
   <generator version="104309"/>
   <author>
      <name>Splunk</name>
   </author>
   <link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>
   <link href="/servicesNS/admin/search/data/lookup-table-files/_reload" rel="_reload"/>
   ... opensearch nodes elided ...
   <s:messages/>
   <entry>
      <title>lookup.csv</title>
      <id>https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/lookup.csv</id>
      <updated>2011-07-21T18:37:25-07:00</updated>
      <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="alternate"/>
      <author>
         <name>admin</name>
      </author>
      <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="list"/>
      <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/_reload" rel="_reload"/>
      <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="edit"/>
      <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv" rel="remove"/>
      <link href="/servicesNS/admin/search/data/lookup-table-files/lookup.csv/move" rel="move"/>
      <content type="text/xml">
         <s:dict>
            ... eai:acl node elided ...
            <s:dict><s:dict name="eai:appName">search</s:dict>
            <s:dict><s:dict name="eai:attributes">
            <s:dict name="optionalFields">
            <s:list/>
            </s:dict>
            <s:dict name="requiredFields">
            <s:list>
            <s:item>eai:data</s:item>
            </s:list>
            </s:dict>
            <s:dict name="wildcardFields">
            <s:list/>
            </s:dict>
            </s:dict>
            </s:dict>
```
POST
Modify a lookup table file by replacing it with a file from the upload staging area.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:data</td>
<td>String</td>
<td>required</td>
<td>Move a lookup table file from the given path into $SPLUNK_HOME. This path must have the lookup staging area as an ancestor.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:appName</td>
<td>The app for which the lookup table applies.</td>
</tr>
<tr>
<td>eai:data</td>
<td>The source path for the lookup staging area. The lookup table file is moved from here into $SPLUNK_HOME.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The Splunk user who created the lookup table.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
```

XML Response

```xml
...<title>lookup-table-files</title>
?id=https://localhost:8089/servicesNS/admin/search/data/lookup-table-files/id
<updated>2011-07-21T18:41:52-07:00</updated>
<generator version="104309"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/data/lookup-table-files/_new" rel="create"/>
<link href="/servicesNS/admin/search/data/lookup-table-files/_reload" rel="_reload"/>
```
data/props/calcfields

https://<host>:<mPort>/services/data/props/calcfields

Provides access to calculated fields, which are eval expressions in props.conf.

GET

Returns information on calculated fields for this instance of your Splunk deployment.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>The name of the calculated field, which includes the &quot;EVAL-&quot; prefix.</td>
</tr>
<tr>
<td>field.name</td>
<td>The name of the field which is being calculated with an EVAL expression.</td>
</tr>
<tr>
<td>stanza</td>
<td>The name of the stanza in props.conf that defines the calculated field.</td>
</tr>
<tr>
<td>type</td>
<td>The type of the calculated field.</td>
</tr>
</tbody>
</table>
This is always EVAL.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>The EVAL statement for the calculated field.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/data/props/calcfields

**XML Response**

```xml
<title>props-eval</title>
<id>https://localhost:8089/services/data/props/calcfields</id>
<updated>2012-10-01T15:01:50-07:00</updated>
<generator build="138753" version="5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/props/calcfields/_new" rel="create"/>
... opensearch nodes elided ... 
<s:messages/>
<entry>
<title><access_common> : EVAL-response_time</title>
<id>https://localhost:8089/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time</id>
<updated>2012-10-01T15:01:50-07:00</updated>
<link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="alternate"/>
<author>
  <name>admin</name>
</author>
<link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="list"/>
<link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="edit"/>
<link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="remove"/>
<link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time/move" rel="move"/>
<content type="text/xml">
<s:dict>
  <s:dict>
    <s:key name="attribute">EVAL-response_time</s:key>
    ... eai:acl node elided ... 
    <s:key name="field.name">response_time</s:key>
    <s:key name="stanza"><access_common></s:key>
    <s:key name="type">EVAL</s:key>
    <s:key name="value">response_time/1000</s:key>
  </s:dict>
</s:dict>
```

717
POST

Create an eval expression defining a calculated field in props.conf.

See Create a calculated field by editing props.conf in the Knowledge Manager Manual for more details.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>required</td>
<td>String</td>
<td>The name of the calculated field. Do not specify the “EVAL-” prefix for the field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>When Splunk software writes the calculated field to props.conf, it adds the “EVAL-” prefix.</td>
</tr>
<tr>
<td>stanza</td>
<td>required</td>
<td>String</td>
<td>The name of the stanza in props.conf for the calculated field.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The name can be any of the following:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Sourcetype of an event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• host::&lt;host&gt;, where &lt;host&gt; is the host for an event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• source::&lt;source&gt;, where &lt;source&gt; is the source for an event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> Use URL-encoding to ensure that Splunk software interprets the name of the stanza correctly.</td>
</tr>
<tr>
<td>value</td>
<td>required</td>
<td>String</td>
<td>The eval statement, which can be evaluated to any value type, including multivals, boolean, or null.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> Use URL-encoding to ensure that Splunk software interprets the name of the stanza correctly.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>The name of the calculated field, which includes the “EVAL-” prefix.</td>
</tr>
<tr>
<td>field.name</td>
<td>The name of the field which is being calculated with an EVAL expression.</td>
</tr>
<tr>
<td>stanza</td>
<td>The name of the stanza in props.conf that defines the calculated field.</td>
</tr>
<tr>
<td>type</td>
<td>The type of the calculated field.</td>
</tr>
<tr>
<td></td>
<td>This is always EVAL.</td>
</tr>
<tr>
<td>value</td>
<td>The EVAL statement for the calculated field.</td>
</tr>
</tbody>
</table>

Example request and response

718
XML Request

```
curl -k -u admin:pass https://localhost:8089/services/data/props/calcfields -d name=response_time -d stanza=%3Caccess_common%3E -d value=response_time/1000
```

XML Response

```
...<feed xmlns="http://www.w3.org/2005/Atom"
   xmlns:s="http://dev.splunk.com/ns/rest"
   xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
   <title>props-eval</title>
   <id>https://localhost:8089/services/data/props/calcfields</id>
   <updated>2012-10-01T14:58:45-07:00</updated>
   <generator build="138753" version="5.0"/>
   <author>
     <name>Splunk</name>
   </author>
   <link href="/services/data/props/calcfields/_new" rel="create"/>
   ... opensearch nodes elided ...
   <s:messages/>
   <entry>
     <title><access_common> : EVAL-response_time</title>
     <id>https://localhost:8089/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time</id>
     <updated>2012-10-01T14:58:45-07:00</updated>
     <link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="alternate"/>
     <author>
       <name>admin</name>
     </author>
     <link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="list"/>
     <link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="edit"/>
     <link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="remove"/>
     <link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time/move" rel="move"/>
     <content type="text/xml">
       <s:dict>
         <s:key name="attribute">EVAL-response_time</s:key>
         ... eai:acl node elided ...
         <s:key name="field.name">response_time</s:key>
         <s:key name="stanza"><access_common></s:key>
         <s:key name="type">EVAL</s:key>
         <s:key name="value">response_time/1000</s:key>
       </s:dict>
     </content>
   </entry>
</feed>
...`
data/props/calcfields/{name}

https://<host>:<mPort>/services/data/props/calcfields/{name}
Manage the {name} calculated field.

DELETE

Deletes the named calculated field.

Usage details
Use URL-encoding to ensure that Splunk software interprets the name of the calculated field correctly.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE
https://localhost:8089/services/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>props-eval</title>
  <id>https://localhost:8089/services/data/props/calcfields</id>
  <updated>2012-10-01T15:33:06-07:00</updated>
  <generator build="138753" version="5.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/props/calcfields/_new" rel="create"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```
GET

Access the named calculated field.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>The name of the calculated field, which includes the “EVAL-“ prefix.</td>
</tr>
<tr>
<td>field.name</td>
<td>The name of the field which is being calculated with an EVAL expression.</td>
</tr>
<tr>
<td>stanza</td>
<td>The name of the stanza in props.conf that defines the calculated field.</td>
</tr>
<tr>
<td>type</td>
<td>The type of the calculated field.</td>
</tr>
<tr>
<td></td>
<td>This is always EVAL.</td>
</tr>
<tr>
<td>value</td>
<td>The EVAL statement for the calculated field.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -k -u admin:pass
https://localhost:8089/services/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time
```

XML Response

```xml
<title>props-eval</title>

<id>https://localhost:8089/services/data/props/calcfields</id>

(updated)2012-10-01T15:05:09-07:00</updated>

<generator build="138753" version="5.0"/>

<author>

<name>Splunk</name>

</author>

<link href="/services/data/props/calcfields/_new" rel="create"/>

... opensearch nodes elided ...

<opensearch:totalResults>1</opensearch:totalResults>

<opensearch:itemsPerPage>30</opensearch:itemsPerPage>

<opensearch:startIndex>0</opensearch:startIndex>

<s:messages/>

<entry>

<title><access_common> : EVAL-response_time</title>

<id>https://localhost:8089/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time</id>

(updated)2012-10-01T15:05:09-07:00</updated>

<link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="alternate"/>
```

721
POST

Update the named calculated field.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| value | String | | The eval statement, which can be evaluated to any value type, including multivals, boolean, or null.  
Note: Use URL-encoding to ensure that Splunk software interprets the name of the stanza correctly.  
See Create a calculated field by editing props.conf in the Knowledge Manager Manual for details. |

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>The name of the calculated field, which includes the &quot;EVAL-&quot; prefix.</td>
</tr>
<tr>
<td>field.name</td>
<td>The name of the field which is being calculated with an EVAL expression.</td>
</tr>
<tr>
<td>stanza</td>
<td>The name of the stanza in props.conf that defines the calculated field.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>type</td>
<td>The type of the calculated field. This is always EVAL.</td>
</tr>
<tr>
<td>value</td>
<td>The EVAL statement for the calculated field.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass
https://localhost:8089/services/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time -d
value=response_time/100
```

**XML Response**

```xml
<title>props-eval</title>

<id>https://localhost:8089/services/data/props/calcfields</id>

<updated>2012-10-01T15:14:19-07:00</updated>

<generator build="138753" version="5.0"/>

<author>
  <name>Splunk</name>
</author>

... opensearch nodes elided ...

<s:messages/>

<entry>
  <title><access_common> : EVAL-response_time</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time</id>
  <updated>2012-10-01T15:14:19-07:00</updated>
  <link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <!-- ... elided... -->
  <link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time" rel="create"/>
  <link href="/servicesNS/admin/search/data/props/calcfields/%3Caccess_common%3E%20%3A%20EVAL-response_time/move" rel="move"/>
  ... eai:acl node elided ...  
  <s:dict>
    <s:key name="attribute">EVAL-response_time</s:key>
    ... elided ...
    <s:key name="field.name">response_time</s:key>
    <s:key name="stanza"><access_common></s:key>
    <s:dict>
      ... eai:acl node elided ...
      <s:key name="attribute">response_time</s:key>
      ... elided ...
      <s:key name="field.name">response_time</s:key>
      <s:key name="stanza"><access_common></s:key>
  </s:dict>
</entry>
```

723
data/props/extractions

https://<host>:<mPort>/services/data/props/extractions

GET
List field extractions.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>attribute</strong></td>
<td>Specifies the field extraction configuration. For example, REPORT-&lt;name&gt; or EXTRACT-&lt;name&gt;.</td>
</tr>
<tr>
<td><strong>stanza</strong></td>
<td>The props.conf stanza to which this field extraction applies. For example, the sourcetype or source that triggers this field extraction. The full name of the field extraction includes this stanza name as a prefix.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>Specifies the field extraction type, which can be either inline or uses transform.</td>
</tr>
<tr>
<td><strong>value</strong></td>
<td>If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/extractions

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-extract</title>
</feed>
POST

Create a new field extraction.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>The user-specified part of the field extraction name. The full name of the field extraction includes this identifier as a suffix.</td>
</tr>
<tr>
<td>stanza</td>
<td>String</td>
<td></td>
<td>The props.conf stanza to which this field extraction applies, e.g. the sourcetype or source that triggers this field extraction. The full name of the field extraction includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>type</td>
<td>Enum</td>
<td></td>
<td>Valid values: (REPORT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>An EXTRACT-type field extraction is defined with an “inline” regular expression. A REPORT-type field extraction refers to a transforms.conf stanza.</td>
</tr>
<tr>
<td>value</td>
<td>String</td>
<td></td>
<td>If this is an EXTRACT-type field extraction, specify a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, specify a comma- or space-delimited list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>attribute</td>
<td></td>
<td></td>
<td>Specifies the field extraction configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example, REPORT-&lt;name&gt; or EXTRACT-&lt;name&gt;.</td>
</tr>
<tr>
<td>stanza</td>
<td></td>
<td></td>
<td>Specifies the name of the stanza for the field extraction.</td>
</tr>
<tr>
<td>type</td>
<td></td>
<td>inline</td>
<td>Specifies the field extraction type, which can be either inline or uses transform.</td>
</tr>
<tr>
<td>value</td>
<td></td>
<td></td>
<td>If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/extractions -d name=port -d stanza=ftp_log -d type=EXTRACT -d "value=port (?<port_number>\d+)"

**XML Response**

```xml
...<title>props-extract</title>
<i>https://localhost:8089/servicesNS/admin/search/data/props/extractions</i>
<updated>2011-07-10T22:56:17-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/data/props/extractions/_new" rel="create"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>ftp_log : EXTRACT-port</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port</id>
  <updated>2011-07-10T22:56:17-07:00</updated>
  <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="list"/>
  <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="edit"/>
  <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="remove"/>
  <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port/move" rel="move"/>
  <content type="text/xml">
    <s:dict>
      <i>726</i>
    </s:dict>
  </content>
</entry>
...```
Manage the `{name}` field extraction.

**DELETE**

Delete the named field extraction.

**Request parameters**

None

**Returned values**

None

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass --request DELETE https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions</id>
  <updated>2011-07-10T23:05:42-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/extractions/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```
GET

List a single field extraction.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration. For example, REPORT-&lt;name&gt; or EXTRACT-&lt;name&gt;.</td>
</tr>
<tr>
<td>stanza</td>
<td>The props.conf stanza to which this field extraction applies. For example, the sourcetype or source that triggers this field extraction. The full name of the field extraction includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type, which can be either inline or uses transform.</td>
</tr>
<tr>
<td>value</td>
<td>If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions/_new</id>
  <updated>2011-07-10T23:02:31-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/extractions/_new" rel="create"/>
  ... opensearch nodes elided ...
```
POST

Modify the named field extraction.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>String</td>
<td></td>
<td>If this is an EXTRACT-type field extraction, specify a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, specify a comma- or space-delimited list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
</tbody>
</table>
Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration. For example, REPORT-&lt;name&gt; or EXTRACT-&lt;name&gt;.</td>
</tr>
<tr>
<td>stanza</td>
<td>Specifies the name of the stanza for the field extraction.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type, which can be either inline or uses transform.</td>
</tr>
<tr>
<td>value</td>
<td>If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port -d "value=connection on port (?<port_number>\d+)"

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
    xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions</id>
  <updated>2011-07-10T23:05:05-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/extractions/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>ftp_log : EXTRACT-port</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port</id>
    <updated>2011-07-10T23:05:05-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/extractions/ftp_log%20%3A%20EXTRACT-port/move" rel="move"/>
    <content type="text/xml">
```

---

730
data/props/fieldaliases

https://<host>:<mPort>/services/data/props/fieldaliases

Access or create field aliases.

GET

List field aliases.

Example

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias.*</td>
<td>The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.</td>
</tr>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration. For example, REPORT-&lt;name&gt; or EXTRACT-&lt;name&gt;.</td>
</tr>
<tr>
<td>stanza</td>
<td>The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type, which can be either inline or uses transform.</td>
</tr>
<tr>
<td>value</td>
<td>If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
  xmlns:s="http://dev.splunk.com/ns/rest">
  <title>fieldaliases</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
  <updated>2011-07-21T19:31:41-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/fieldaliases/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : FIELDALIAS-alias_name</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name</id>
    <updated>2011-07-21T19:31:41-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="alias.foo">bar</s:key>
        <s:key name="attribute">FIELDALIAS-alias_name</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">my_sourcetype</s:key>
        <s:key name="type">FIELDALIAS</s:key>
        <s:key name="value">foo AS bar</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
POST

Create a new field alias.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| alias.* | String  |         | The alias for a given field. For example, supply a value of "bar" for an argument "alias.foo" to alias "foo" to "bar".

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name required</td>
<td>String</td>
<td></td>
<td>The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.</td>
</tr>
<tr>
<td>stanza required</td>
<td>String</td>
<td></td>
<td>The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias.*</td>
<td>The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.</td>
</tr>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration. For example, REPORT-&lt;name&gt; or EXTRACT-&lt;name&gt;.</td>
</tr>
<tr>
<td>stanza</td>
<td>The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type, which can be either inline or uses transform.</td>
</tr>
<tr>
<td>value</td>
<td>If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields.</td>
</tr>
<tr>
<td></td>
<td>If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases -d name=alias_name -d stanza=my_sourcetype -d alias.foo=bar

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
    xmlns:s="http://dev.splunk.com/ns/rest">
    <title>fieldaliases</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
    <updated>2011-07-21T19:30:17-07:00</updated>
    <generator version="104309"/>
    <author>
        <name>Splunk</name>
    </author>
</feed>
```
data/props/fieldaliases/{name}

https://<host>:<mPort>/services/data/props/fieldaliases/{name}

Manage the {name} field alias.

**DELETE**

Delete the named field alias.

**Request parameters**

None

**Returned values**

734
Example request and response

XML Request

curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/
  xmlns:s="http://dev.splunk.com/ns/rest">
  <title>fieldaliases</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
  <updated>2011-07-21T19:37:45-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/fieldaliases/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>

GET

Access a field alias.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias.*</td>
<td>The user-specified part of the field alias name. The full name of the field alias includes this identifier as a suffix.</td>
</tr>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration. For example, REPORT-&lt;name&gt; or EXTRACT-&lt;name&gt;.</td>
</tr>
<tr>
<td>stanza</td>
<td>The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type, which can be either inline or uses transform.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>value</td>
<td>If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields. If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
    xmlns:s="http://dev.splunk.com/ns/rest">
  <title>fieldaliases</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
  <updated>2011-07-21T19:33:00-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/fieldaliases/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_sourcetype : FIELDALIAS-alias_name</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name</id>
    <updated>2011-07-21T19:33:00-07:00</updated>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name/move" rel="move"/>
    <content type="text/xml">  
      <s:dict>
        <s:key name="alias.foo">bar</s:key>
        <s:key name="attribute">FIELDALIAS-alias_name</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
POST

Update a field alias.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias.*</td>
<td>String</td>
<td></td>
<td>The alias for a given field. For example, supply a value of “bar” for an argument “alias.foo” to alias “foo” to “bar”.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias.*</td>
<td>The alias for a given field. For example, supply a value of “bar” for an argument “alias.foo” to alias “foo” to “bar”.</td>
</tr>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration. For example, REPORT-&lt;name&gt; or EXTRACT-&lt;name&gt;.</td>
</tr>
<tr>
<td>stanza</td>
<td>The props.conf stanza to which this field alias applies, e.g. the sourcetype or source that causes this field alias to be applied. The full name of the field alias includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type, which can be either inline or uses transform.</td>
</tr>
<tr>
<td>value</td>
<td>If this is an EXTRACT-type field extraction, a regular expression with named capture groups that define the desired fields.</td>
</tr>
<tr>
<td></td>
<td>If this is a REPORT-type field extraction, a list of transforms.conf stanza names that define the field transformations to apply.</td>
</tr>
</tbody>
</table>

Example request and response
XML Request

curl -k -u admin:pass 
https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name 
-d alias.hi=hello  
-d alias.bye=goodbye

XML Response

<feed xmlns="http://www.w3.org/2005/Atom" 
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/" 
    xmlns:s="http://dev.splunk.com/ns/rest">
    <title>fieldaliases</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases</id>
    <updated>2011-07-21T19:34:36-07:00</updated>
    <generator version="104309"/>
    <author>
        <name>Splunk</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/fieldaliases/_new" rel="create"/>
    ... opensearch nodes elided ...
    <s:messages/>
    <entry>
        <title>my_sourcetype : FIELDALIAS-alias_name</title>
        <id>https://localhost:8089/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name</id>
        <updated>2011-07-21T19:34:36-07:00</updated>
        <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name" rel="alternate"/>
        <author>
            <name>admin</name>
        </author>
        <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name" rel="list"/>
        <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name" rel="edit"/>
        <link href="/servicesNS/admin/search/data/props/fieldaliases/my_sourcetype%20%3A%20FIELDALIAS-alias_name/move" rel="move"/>
        <content type="text/xml">
            <s:dict>
                <s:key name="alias.byee">goodbye</s:key>
                <s:key name="alias.hi">hello</s:key>
                ... eai:acl node elided ...
                <s:key name="stanza">my_sourcetype</s:key>
                <s:key name="type">FIELDALIAS</s:key>
                <s:key name="value">bye AS goodbye hi AS hello</s:key>
            </s:dict>
        </content>
    </entry>
</feed>
data/props/lookups

https://<host>:<mPort>/services/data/props/lookups
Access or create automatic lookups.

GET
List automatic lookups.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration. For example, LOOKUP-my_lookup.</td>
</tr>
<tr>
<td>overwrite</td>
<td>If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.</td>
</tr>
<tr>
<td>stanza</td>
<td>The props.conf stanza to which this automatic lookup applies. For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>transform</td>
<td>The transforms.conf stanza that defines the lookup to apply.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type. For this endpoint, this is always LOOKUP</td>
</tr>
<tr>
<td>value</td>
<td>The transform stanza with the value for the lookup.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/lookups

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups</id>
</feed>
POST

Create an automatic lookup.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lookup.field.input.*</td>
<td>String</td>
<td>Default</td>
<td>A column in the lookup table to match against. Supply a non-empty value if the corresponding field has a different name in your actual events.</td>
</tr>
<tr>
<td>lookup.field.output.*</td>
<td>String</td>
<td>Default</td>
<td>A column in the lookup table to output. Supply a non-empty value if the field should have a different name in your actual events.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>name</td>
<td>required</td>
<td>String</td>
<td>The user-specified part of the automatic lookup name. The full name of the automatic lookup includes this identifier as a suffix.</td>
</tr>
<tr>
<td>overwrite</td>
<td>required</td>
<td>Boolean</td>
<td>If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.</td>
</tr>
<tr>
<td>stanza</td>
<td>required</td>
<td>String</td>
<td>The props.conf stanza to which this automatic lookup applies, e.g. the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>transform</td>
<td>required</td>
<td>String</td>
<td>The transforms.conf stanza that defines the lookup to apply.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration.</td>
</tr>
<tr>
<td></td>
<td>For example, LOOKUP-my_lookup.</td>
</tr>
<tr>
<td>lookup.field.input.*</td>
<td>A column in the lookup table to match against. Supply a non-empty value if the corresponding field has a different name in your actual events.</td>
</tr>
<tr>
<td>lookup.field.output.*</td>
<td>A column in the lookup table to output. Supply a non-empty value if the field should have a different name in your actual events.</td>
</tr>
<tr>
<td>overwrite</td>
<td>If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.</td>
</tr>
<tr>
<td>stanza</td>
<td>The props.conf stanza to which this automatic lookup applies.</td>
</tr>
<tr>
<td></td>
<td>For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>transform</td>
<td>The transforms.conf stanza that defines the lookup to apply.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type.</td>
</tr>
<tr>
<td></td>
<td>For this endpoint, this is always LOOKUP.</td>
</tr>
<tr>
<td>value</td>
<td>The props.conf stanza to which this automatic lookup applies.</td>
</tr>
<tr>
<td></td>
<td>For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```sh
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/lookups -d name=my_lookup -d overwrite=1 -d stanza=my_sourcetype -d transform=my_transform -d lookup.field.input.foo= -d lookup.field.output.fuzz=
```

**XML Response**
data/props/lookups/{name}

https://<host>:<mPort>/services/data/props/lookups/{name}

Manage the {name} automatic lookup.
DELETE

Delete an automatic lookup.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups</id>
  <updated>2011-08-01T20:44:32-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/lookups/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>

GET

Access an automatic lookup.

Request parameters
None

Returned values
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration. For example, LOOKUP-my_lookup.</td>
</tr>
<tr>
<td>overwrite</td>
<td>If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.</td>
</tr>
<tr>
<td>stanza</td>
<td>The props.conf stanza to which this automatic lookup applies. For example, the sourcetype or source that automatically triggers this lookup. The full name of the automatic lookup includes this stanza name as a prefix.</td>
</tr>
<tr>
<td>transform</td>
<td>The transforms.conf stanza that defines the lookup to apply.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type. For this endpoint, this is always LOOKUP.</td>
</tr>
<tr>
<td>value</td>
<td>The transform stanza with the value for the lookup.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups</id>
  <updated>2011-08-01T20:44:06-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/lookups/_new" rel="create"/>
  ... opensearch nodes elided ... 
  <s:messages/>
  <entry>
    <title>my_sourcetype : LOOKUP-my_lookup</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup</id>
    <updated>2011-08-01T20:44:06-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup" rel="edit"/>
  </entry>
</feed>
```

744
POST

Update an automatic lookup.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lookup.field.input.*</td>
<td>String</td>
<td></td>
<td>A column in the lookup table to match against. Supply a non-empty value if the corresponding field has a different name in your actual events.</td>
</tr>
<tr>
<td>lookup.field.output.*</td>
<td>String</td>
<td></td>
<td>A column in the lookup table to output. Supply a non-empty value if the field should have a different name in your actual events.</td>
</tr>
<tr>
<td>overwrite</td>
<td>Boolean</td>
<td></td>
<td>If set to true, output fields are always overridden. If set to false, output fields are only written out if they do not already exist.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>transform</td>
<td>String</td>
<td></td>
<td>The transforms.conf stanza that defines the lookup to apply.</td>
</tr>
</tbody>
</table>

### Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>Specifies the field extraction configuration.</td>
</tr>
<tr>
<td></td>
<td>For example, LOOKUP-my_lookup.</td>
</tr>
<tr>
<td>lookup.field.input.*</td>
<td>A column in the lookup table to match against. Supply a non-empty value if</td>
</tr>
<tr>
<td></td>
<td>the corresponding field has a different name in your actual events.</td>
</tr>
<tr>
<td>lookup.field.output.*</td>
<td>A column in the lookup table to output. Supply a non-empty value if the</td>
</tr>
<tr>
<td></td>
<td>field should have a different name in your actual events.</td>
</tr>
<tr>
<td>overwrite</td>
<td>If set to true, output fields are always overridden. If set to false,</td>
</tr>
<tr>
<td></td>
<td>output fields are only written out if they do not already exist.</td>
</tr>
<tr>
<td>stanza</td>
<td>The props.conf stanza to which this automatic lookup applies.</td>
</tr>
<tr>
<td></td>
<td>For example, the sourcetype or source that automatically triggers this</td>
</tr>
<tr>
<td></td>
<td>lookup. The full name of the automatic lookup includes this stanza name as</td>
</tr>
<tr>
<td></td>
<td>a prefix.</td>
</tr>
<tr>
<td>transform</td>
<td>The transforms.conf stanza that defines the lookup to apply.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type.</td>
</tr>
<tr>
<td></td>
<td>For this endpoint, this is always LOOKUP.</td>
</tr>
<tr>
<td>value</td>
<td>The props.conf stanza to which this automatic lookup applies.</td>
</tr>
<tr>
<td></td>
<td>For example, the sourcetype or source that automatically triggers this</td>
</tr>
<tr>
<td></td>
<td>lookup. The full name of the automatic lookup includes this stanza name as</td>
</tr>
<tr>
<td></td>
<td>a prefix.</td>
</tr>
</tbody>
</table>

### Example request and response

#### XML Request

```bash
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/lookups/my_sourcetype%20%3A%20LOOKUP-my_lookup -d overwrite=1 -d transform=other_transform -d lookup.field.input.bar=- -d lookup.field.output.buzz=
```

#### XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>props-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/lookups</id>
  <updated>2011-08-01T20:44:21-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
</feed>
```
data/props/sourcetype-rename

https://<host>:{<mPort>}/services/data/props/sourcetype-rename

Access or rename props.conf sourcetypes.

GET

List renamed sourcetypes.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>The configuration key.</td>
</tr>
<tr>
<td>stanza</td>
<td>The sourcetype to rename, which is the name of a stanza in props.conf.</td>
</tr>
<tr>
<td>type</td>
<td>The value of the configuration key.</td>
</tr>
<tr>
<td>value</td>
<td>The new name for the sourcetype.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype-rename</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename</id>
  <updated>2011-07-12T15:40:53-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/_new" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>hardware</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware</id>
    <updated>2011-07-12T15:40:53-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="list"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="edit"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="remove"/>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware/move" rel="move"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="attribute">rename</s:key>
        ... eai:acl node elided ...
        <s:key name="stanza">hardware</s:key>
        <s:key name="type">rename</s:key>
        <s:key name="value">hw</s:key>
      </s:dict>
    </content>
  </entry>
</feed>

748
POST

Rename a sourcetype.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>required</td>
<td>String</td>
<td>The original sourcetype name.</td>
</tr>
<tr>
<td>value</td>
<td>required</td>
<td>String</td>
<td>The new sourcetype name.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>The configuration key.</td>
</tr>
<tr>
<td>stanza</td>
<td>The sourcetype to rename, which is the name of a stanza in props.conf.</td>
</tr>
<tr>
<td>type</td>
<td>The value of the configuration key.</td>
</tr>
<tr>
<td>value</td>
<td>The new name for the sourcetype.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename -d name=hardware -d value=hw

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype-rename</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename</id>
  <updated>2011-07-12T15:39:57-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/_create" rel="create"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>hardware</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware</id>
    <updated>2011-07-12T15:39:57-07:00</updated>
    <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="alternate"/>
    <author>
```
data/props/sourcetype-rename/{name}

https://<host>:<mPort>/services/data/props/sourcetype-rename/{name}
Access, delete, or update a sourcetype name.

DELETE

Restore the original sourcetype name for {name}.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass --request DELETE https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype-rename</title>
  <content type="text/xml">
    <s:dict>
      <s:key name="attribute">rename</s:key>
      ... eai:acl node elided ...
      <s:key name="stanza">hardware</s:key>
      <s:key name="type">rename</s:key>
      <s:key name="value">hw</s:key>
    </s:dict>
  </content>
</feed>
GET

Access a specific renamed sourcetype.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attribute</td>
<td>The configuration key.</td>
</tr>
<tr>
<td>stanza</td>
<td>The sourcetype to rename, which is the name of a stanza in props.conf.</td>
</tr>
<tr>
<td>type</td>
<td>The value of the configuration key.</td>
</tr>
<tr>
<td>value</td>
<td>The new name for the sourcetype.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware
```

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>sourcetype-rename</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename</id>
  <updated>2011-07-12T15:44:47-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/_new" rel="create"/>
  ... opensearch nodes elided ... 
  <s:messages/>
</feed>
```
POST

Update a renamed sourcetype name.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>String</td>
<td></td>
<td>The new sourcetype name.</td>
</tr>
</tbody>
</table>

Returned values
### Name | Description
---|---
attribute | The configuration key.
stanza | The sourcetype to rename, which is the name of a stanza in props.conf.
type | The value of the configuration key.
value | The new name for the sourcetype.

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware
-d value=hrdwr
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
 xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/
 xmlns:s="http://dev.splunk.com/ns/rest">
 <title>sourcetype-rename</title>
 <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename</id>
 <updated>2011-07-12T15:46:58-07:00</updated>
 <generator version="102824"/>
 <author>
  <name>Splunk</name>
 </author>
 <link href="/servicesNS/admin/search/data/props/sourcetype-rename/_new" rel="create"/>
 ... opensearch nodes elided ... 
 <s:messages/>
 <entry>
  <title>hardware</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/props/sourcetype-rename/hardware</id>
  <updated>2011-07-12T15:46:58-07:00</updated>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="alternate"/>
  <author>
   <name>admin</name>
  </author>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="list"/>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="edit"/>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware" rel="remove"/>
  <link href="/servicesNS/admin/search/data/props/sourcetype-rename/hardware/move" rel="move"/>
  <content type="text/xml">
   <s:dict>
    <s:key name="attribute">rename</s:key>
    ... eai:acl node elided ... 
    <s:key name="stanza">hardware</s:key>
    <s:key name="type">rename</s:key>
    <s:key name="value">hrdwr</s:key>
   </s:dict>
  </content>
 </entry>
</feed>
```
data/transforms/extractions

https://<host>:<mPort>/services/data/transforms/extractions

Access field extraction definitions.

GET

List field extractions.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are always discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td>If set to true, Splunk software “cleans” the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.</td>
</tr>
<tr>
<td>DEFAULT_VALUE</td>
<td>Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.</td>
</tr>
<tr>
<td>DEST_KEY</td>
<td>Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation.</td>
</tr>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>If set to true, Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>LOOKAHEAD</td>
<td>Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.</td>
</tr>
<tr>
<td>REGEX</td>
<td>The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms.</td>
</tr>
</tbody>
</table>
For details, see the documentation for this parameter in the POST operation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE_KEY</td>
<td>The KEY to which Splunk software applies REGEX.</td>
</tr>
<tr>
<td>WRITE_META</td>
<td>Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the field transformation is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which the field extractions are defined. For example, the search app.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The name of the Splunk user who created the field extraction definitions. For example, the admin user.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/extractions

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/id</id>
  <updated>2011-07-21T20:28:03-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_reload" rel="_reload"/>
  ...
  <s:dict>
```

755
POST

Create a new field transformation.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Bool</td>
<td>True</td>
<td>Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off—it ensures that certain fields are <em>always</em> discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is needed for the successful evaluation of a search. NOTE: This option should rarely be set to false.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td>Boolean</td>
<td>True</td>
<td>If set to true, Splunk software “cleans” the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Specifies whether the field transformation is disabled.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>String</td>
<td></td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. FORMAT for index-time extractions: Use $n (for example $1, $2, etc) to specify the output of each REGEX match. If REGEX does not have n groups, the matching fails.</td>
</tr>
</tbody>
</table>
The special identifier $0 represents what was in the DEST_KEY before the REGEX was performed.

At index-time only, you can use FORMAT to create concatenated fields:
FORMAT = ipaddress::$1.$2.$3.$4

When you create concatenated fields with FORMAT, "$" is the only special character. It is treated as a prefix for regex-capturing groups only if it is followed by a number and only if the number applies to an existing capturing group. So if REGEX has only one capturing group and its value is "bar", then: 
- "FORMAT = foo$1" yields "foobar"
- "FORMAT = foo$bar" yields "foo$bar"
- "FORMAT = foo$1234" yields "foo$1234"
- "FORMAT = foo$1\$2" yields "fooobar\$2"

At index-time, FORMAT defaults to <stanza-name>::$1

FORMAT for search-time extractions:

The format of this field as used during search time extractions is as follows:

```
FORMAT = <field-name>::<field-value>( <field-name>::<field-value>)*
```

```
<field-name> = [<string>|$<extracting-group-number>]
<field-value> = [<string>$<extracting-group-number>]
```

Search-time extraction examples:

- "FORMAT = first::$1 second::$2 third::other-value" yields:
  - first: "first::other-value"
  - second: "second::other-value"
  - third: "third::other-value"

You cannot create concatenated fields with FORMAT at search time. That functionality is only available at index time.

At search-time, FORMAT defaults to an empty string.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>Boolean</td>
<td>False</td>
<td>If set to true, Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>Boolean</td>
<td>False</td>
<td>If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>False</td>
<td>The name of the field transformation.</td>
</tr>
<tr>
<td>REGEX</td>
<td>String</td>
<td>False</td>
<td>Specify a regular expression to operate on your data.</td>
</tr>
</tbody>
</table>

This attribute is valid for both index-time and search-time field extractions:

```
\tREGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). \tREGEX is required for all index-time transforms.
```

REGEX and the FORMAT attribute:

Name-capturing groups in the REGEX are extracted directly to fields. This means that you do not need to specify the FORMAT attribute for simple field extraction cases.
If the REGEX extracts both the field name and its corresponding field value, you can use the following special capturing groups if you want to skip specifying the mapping in FORMAT: _KEY_<string>, _VAL_<string>.

For example, the following are equivalent:

```plaintext
Using FORMAT:
REGEX = ([a-z]+)=(^[a-z]+)  
FORMAT = $1:$2
Without using FORMAT
REGEX = (?<__KEY_1>[a-z]+)=(?<__VAL_1>[a-z]+)
```

REGEX defaults to an empty string.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE_KEY</td>
<td>String</td>
<td>_raw</td>
<td>Specify the KEY to which Splunk software applies REGEX.</td>
</tr>
</tbody>
</table>

### Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off—it ensures that certain fields are always discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td>If set to true, Splunk software &quot;cleans&quot; the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.</td>
</tr>
<tr>
<td>DEFAULT_VALUE</td>
<td>Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.</td>
</tr>
<tr>
<td>DEST_KEY</td>
<td>Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation.</td>
</tr>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>If set to true, Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>LOOKAHEAD</td>
<td>Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.</td>
</tr>
<tr>
<td>REGEX</td>
<td>The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms.</td>
</tr>
</tbody>
</table>
For details, see the documentation for this parameter in the POST operation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SOURCE_KEY</strong></td>
<td>The KEY to which Splunk software applies REGEX.</td>
</tr>
<tr>
<td><strong>WRITE_META</strong></td>
<td>Indicates whether to automatically write REGEX to metadata.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the field transformation is disabled.</td>
</tr>
<tr>
<td><strong>eai:appName</strong></td>
<td>The Splunk app for which the field extractions are defined. For example, the search app.</td>
</tr>
<tr>
<td><strong>eai:userName</strong></td>
<td>The name of the Splunk user who created the field extraction definitions. For example, the admin user.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/extractions -d REGEX="(?<_KEY_1>[a-z]*),(?<_VAL_1>[a-z]*)" -d SOURCE_KEY=_raw -d name=my_transform

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/id</id>
  <updated>2011-07-21T20:25:20-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_reload" rel="_reload"/>
  ...
  <opensearch:totalResults>759</opensearch:totalResults>
  ...
  <s:messages/>
  <entry>
    <title>my_transform</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform/id</id>
    <updated>2011-07-21T20:25:20-07:00</updated>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="list"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/edit"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/remove"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/move" rel="move"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/disable" rel="disable"/>
```
data/transforms/extractions/{name}

https://<host>:<mPort>/services/data/transforms/extractions/{name}
Access, delete, or update the {name} field extraction.

DELETE
Delete a field extraction.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform

XML Response
760
GET

Access a specific field extraction.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are always discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td>If set to true, Splunk software &quot;cleans&quot; the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.</td>
</tr>
<tr>
<td>DEFAULT_VALUE</td>
<td>Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.</td>
</tr>
<tr>
<td>DEST_KEY</td>
<td>Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation.</td>
</tr>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>If set to true, Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>LOOKAHEAD</td>
<td>Optional attribute for index-time field extractions. specifies how many characters to search into an event.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.</td>
</tr>
<tr>
<td>REGEX</td>
<td>The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.</td>
</tr>
<tr>
<td>SOURCE_KEY</td>
<td>The KEY to which Splunk software applies REGEX.</td>
</tr>
<tr>
<td>WRITE_META</td>
<td>Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the field transformation is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which the field extractions are defined. For example, the search app.</td>
</tr>
<tr>
<td>eai:attributes</td>
<td>Field control information.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The name of the Splunk user who created the field extraction definitions. For example, the admin user.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**
```bash
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform
```

**XML Response**
```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions</id>
  <updated>2011-07-21T20:29:00-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
</feed>
```
<entry>
  <title>my_transform</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform</id>
  <updated>2011-07-21T20:29:00-07:00</updated>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="alternate"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="list"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/edit" rel="edit"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/remove" rel="remove"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/move" rel="move"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="CAN_OPTIMIZE">1</s:key>
      <s:key name="CLEAN_KEYS">1</s:key>
      <s:key name="DEFAULT_VALUE"/>
      <s:key name="DEST_KEY"/>
      <s:key name="FORMAT"/>
      <s:key name="KEEP_EMPTY_VALS">0</s:key>
      <s:key name="LOOKAHEAD">4096</s:key>
      <s:key name="MV_ADD">0</s:key>
      <s:key name="REGEX">(?<KEY_1>[a-z]*),(?<VAL_1>[a-z]*)</s:key>
      <s:key name="SOURCE_KEY">_raw</s:key>
      <s:key name="WRITE_META">0</s:key>
      <s:key name="disabled">0</s:key>
    </s:dict>
    <s:dict>
      <s:key name="optionalFields">
        <s:list>
          <s:item>CAN_OPTIMIZE</s:item>
          <s:item>CLEAN_KEYS</s:item>
          <s:item>FORMAT</s:item>
          <s:item>KEEP_EMPTY_VALS</s:item>
          <s:item>MV_ADD</s:item>
          <s:item>disabled</s:item>
        </s:list>
      </s:key>
      <s:key name="requiredFields">
        <s:list>
          <s:item>REGEX</s:item>
          <s:item>SOURCE_KEY</s:item>
        </s:list>
      </s:key>
      <s:dict name="eai:attributes">
        <s:dict name="optionalFields">
          <s:list>
            <s:item>CAN_OPTIMIZE</s:item>
            <s:item>CLEAN_KEYS</s:item>
            <s:item>FORMAT</s:item>
            <s:item>KEEP_EMPTY_VALS</s:item>
            <s:item>MV_ADD</s:item>
            <s:item>disabled</s:item>
          </s:list>
        </s:dict>
        <s:dict name="requiredFields">
          <s:list>
            <s:item>REGEX</s:item>
            <s:item>SOURCE_KEY</s:item>
          </s:list>
        </s:dict>
        <s:dict name="eai:appName">search</s:dict>
        <s:dict name="eai:attributes">
          <s:dict name="optionalFields">
            <s:list>
              <s:item>CAN_OPTIMIZE</s:item>
              <s:item>CLEAN_KEYS</s:item>
              <s:item>FORMAT</s:item>
              <s:item>KEEP_EMPTY_VALS</s:item>
              <s:item>MV_ADD</s:item>
              <s:item>disabled</s:item>
            </s:list>
          </s:dict>
          <s:dict name="requiredFields">
            <s:list>
              <s:item>REGEX</s:item>
              <s:item>SOURCE_KEY</s:item>
            </s:list>
          </s:dict>
          <s:dict name="eai:appName">search</s:dict>
        </s:dict>
      </s:dict>
    </s:dict>
    <s:dict name="eai:userName">admin</s:dict>
  </content>
</entry>
</feed>
POST

Update a field extraction.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>REGEX</td>
<td>String</td>
<td></td>
<td>Specify a regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms. REGEX and the FORMAT attribute: Name-capturing groups in the REGEX are extracted directly to fields. This means that you do not need to specify the FORMAT attribute for simple field extraction cases. If the REGEX extracts both the field name and its corresponding field value, you can use the following special capturing groups if you want to skip specifying the mapping in FORMAT: <em>KEY</em>&lt;string&gt;, <em>VAL</em>&lt;string&gt;. For example, the following are equivalent: Using FORMAT: REGEX = ([a-z]+)=(^[a-z]+) FORMAT = $1:$2 Without using FORMAT REGEX = (?&lt;KEY_1&gt;[a-z]+)=(?&lt;VAL_1&gt;[a-z]+) REGEX defaults to an empty string.</td>
</tr>
<tr>
<td>SOURCE_KEY</td>
<td>String</td>
<td>_raw</td>
<td>Specify the KEY to which Splunk software applies REGEX.</td>
</tr>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Bool</td>
<td>True</td>
<td>Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off—it ensures that certain fields are “always” discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is needed for the successful evaluation of a search. NOTE: This option should rarely be set to false.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td>Boolean</td>
<td>True</td>
<td>If set to true, Splunk software “cleans” the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>String</td>
<td></td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time.</td>
</tr>
</tbody>
</table>

764
This attribute specifies the format of the event, including any field names or values you want to add.

FORMAT for index-time extractions:

Use $n (for example $1, $2, etc) to specify the output of each REGEX match.

If REGEX does not have n groups, the matching fails.

The special identifier $0 represents what was in the DEST_KEY before the REGEX was performed.

At index-time only, you can use FORMAT to create concatenated fields: FORMAT = ipaddress::$1.$2.$3.$4

When you create concatenated fields with FORMAT, "$" is the only special character. It is treated as a prefix for regex-capturing groups only if it is followed by a number and only if the number applies to an existing capturing group. So if REGEX has only one capturing group and its value is "bar", then: \t"FORMAT = foo$1" yields "foobar"
\t"FORMAT = foo$bar" yields "foo$bar" \t"FORMAT = foo$1234" yields "foo$1234" \t"FORMAT = foo$1$2" yields "foo$1$2"

At index-time, FORMAT defaults to <stanza-name>::$1

FORMAT for search-time extractions:

The format of this field as used during search time extractions is as follows: \tFORMAT = <field-name>::<field-value>( <field-name>::<field-value>)*
\tfield-name = [<string>$<extracting-group-number>]
\tfield-value = [<string>$<extracting-group-number>]

Search-time extraction examples: \tFORMAT = first::$1 second::$2 third::other-value \tFORMAT = $1::$2

You cannot create concatenated fields with FORMAT at search time. That functionality is only available at index time.

At search-time, FORMAT defaults to an empty string.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>Boolean</td>
<td>False</td>
<td>This is set to true by default. Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>Boolean</td>
<td>False</td>
<td>This is set to true by default. Splunk software preserves extracted fields with empty values.</td>
</tr>
</tbody>
</table>
If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Specifies whether the field transformation is disabled.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off—-it ensures that certain fields are always discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td>If set to true, Splunk software &quot;cleans&quot; the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.</td>
</tr>
<tr>
<td>DEFAULT_VALUE</td>
<td>Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.</td>
</tr>
<tr>
<td>DEST_KEY</td>
<td>Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation.</td>
</tr>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>If set to true, Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>LOOKAHEAD</td>
<td>Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.</td>
</tr>
<tr>
<td>REGEX</td>
<td>The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions. \t\tREGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). \t\tREGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.</td>
</tr>
</tbody>
</table>

766
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE_KEY</td>
<td>The KEY to which Splunk software applies REGEX.</td>
</tr>
<tr>
<td>WRITE_META</td>
<td>Indicates whether to automatically write REGEX to metadata.</td>
</tr>
<tr>
<td></td>
<td>This attribute is required for all index-time field extractions except for</td>
</tr>
<tr>
<td></td>
<td>those where DEST_KEY = meta (see the description of the DEST_KEY attribute).</td>
</tr>
<tr>
<td></td>
<td>Use instead of DEST_KEY = meta.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the field transformation is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which the field extractions are defined. For example, the</td>
</tr>
<tr>
<td></td>
<td>search app.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The name of the Splunk user who created the field extraction definitions. For</td>
</tr>
<tr>
<td></td>
<td>example, the admin user.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass
https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform -d
REGEX="(?<_KEY_1>[a-z]*)((?<_VAL_1>[a-z]*)"," -d SOURCE_KEY=_raw -d CLEAN_KEYS=false

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>transforms-extract</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions</id>
  <updated>2011-07-21T20:33:13-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/extractions/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_transform</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/transforms/extractions/my_transform</id>
    <updated>2011-07-21T20:33:13-07:00</updated>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="alternate"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform" rel="list"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/edit" rel="edit"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/remove" rel="remove"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/move" rel="move"/>
    <link href="/servicesNS/admin/search/data/transforms/extractions/my_transform/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        ... transformed data elided ...
      </s:dict>
    </content>
  </entry>
</feed>
```
data/transforms/lookups

https://<host>://<mPort>/services/data/transforms/lookups
Access or create lookup definitions.

GET
List lookup definitions.

Request parameters
Pagination and filtering parameters can be used with this method.

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>getsize</td>
<td>Boolean</td>
<td>false</td>
<td>Enable to return the file size.</td>
</tr>
<tr>
<td>replicate_delta</td>
<td>Boolean</td>
<td>false</td>
<td>Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are always discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>DEFAULT_VALUE</td>
<td>Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.</td>
</tr>
<tr>
<td>DEST_KEY</td>
<td>Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation for data/transforms/extractions.</td>
</tr>
<tr>
<td>GETSIZE</td>
<td>If enabled, returns the file size.</td>
</tr>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>If set to true, Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>LOOKAHEAD</td>
<td>Optional attribute for index-time filed extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.</td>
</tr>
<tr>
<td>REGEX</td>
<td>The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.</td>
</tr>
<tr>
<td>SOURCE_KEY</td>
<td>The KEY to which Splunk software applies REGEX.</td>
</tr>
<tr>
<td>WRITE_META</td>
<td>Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this lookup is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which the lookups are defined. For example, the search app.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The Splunk user for which the lookups are defined.</td>
</tr>
<tr>
<td>external_cmd</td>
<td>Provides the command and arguments to invoke to perform a lookup. Use this for external (or &quot;scripted&quot;) lookups, where you interface with with an external script rather than a lookup table. This string is parsed like a shell command. The first argument is expected to be a python script located in:</td>
</tr>
</tbody>
</table>

769
### Name Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fields_list</td>
<td>List of all fields that are supported by the external command.</td>
</tr>
<tr>
<td>replicate_delta</td>
<td>Indicates that only the changes to a CSV lookup table are replicated, rather than the entire lookup table.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type. Can be either external or file.</td>
</tr>
</tbody>
</table>

### Example request and response

#### XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/lookups
```

#### XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">  
  <title>transforms-lookup</title>  
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups</id>  
  <updated>2011-08-01T21:10:44-07:00</updated>  
  <generator version="105049"/>  
  <author>  
    <name>Splunk</name>  
  </author>  
  <link href="/servicesNS/admin/search/data/transforms/lookups/_new" rel="create"/>  
  <link href="/servicesNS/admin/search/data/transforms/lookups/_reload" rel="_reload"/>  
  ... opensearch nodes elided ...  
  <s:messages/>  
  <entry>  
    <title>dnslookup</title>  
    <id>https://localhost:8089/servicesNS/nobody/system/data/transforms/lookups/dnslookup</id>  
    <updated>2011-08-01T21:10:44-07:00</updated>  
    <author>  
      <name>nobody</name>  
    </author>  
    <link href="/servicesNS/nobody/system/data/transforms/lookups/dnslookup" rel="alternate"/>  
    <link href="/servicesNS/nobody/system/data/transforms/lookups/dnslookup/_reload" rel="_reload"/>  
    <link href="/servicesNS/nobody/system/data/transforms/lookups/dnslookup/disable" rel="disable"/>  
    <content type="text/xml">  
      <s:dict>  
        <s:key name="CAN_OPTIMIZE">1</s:key>  
        <s:key name="CLEAN_KEYS">1</s:key>  
        <s:key name="DEFAULT_VALUE"/>  
        <s:key name="DEST_KEY"/>  
        <s:key name="FORMAT"/>  
        <s:key name="KEEP_EMPTY_VALS">0</s:key>  
        <s:key name="LOOKAHEAD">4096</s:key>  
        <s:key name="MV_ADD">0</s:key>  
      </s:dict>  
    </content>  
  </entry>  
</feed>
```
POST

Update a lookup definition.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>collection</td>
<td>String</td>
<td>&lt;empty&gt;</td>
<td>Name of the collection to use for this lookup. The collection should be defined in $SPLUNK_HOME/etc/&lt;app_name&gt;/collections.conf for the current app. To create a KV Store lookup, use <code>collection</code> to pass in the KV Store collection name and include the <code>external_type</code> parameter with a value of <code>kvstore</code> in your POST request.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>The name of the lookup definition.</td>
</tr>
<tr>
<td>default_match</td>
<td>String</td>
<td></td>
<td>If min_matches is greater than zero and Splunk software has less than min_matches for any given input, it provides this default_match value one or more times until the min_matches threshold is reached.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Specifies whether the lookup definition is disabled.</td>
</tr>
<tr>
<td>external_cmd</td>
<td>String</td>
<td></td>
<td>Provides the command and arguments to invoke to perform a lookup. Use this for external (or &quot;scripted&quot;) lookups, where you interface with with an external script rather than a lookup table. This string is parsed like a shell command. The first argument is expected to be a python script located in: $SPLUNK_HOME/etc/&lt;app_name&gt;/bin (or ../etc/searchscripts) Presence of this field indicates that the lookup is external and command based.</td>
</tr>
<tr>
<td>external_type</td>
<td>One of the following values: python, executable, geo, kvstore</td>
<td></td>
<td>Type of external command for performing a lookup. To define a KV Store lookup, use <code>external_type = kvstore</code>. Include the KV Store collection name in your POST request.</td>
</tr>
<tr>
<td>fields_list</td>
<td>String</td>
<td></td>
<td>A comma- and space-delimited list of all fields that are supported by the external command. Use this for external (or &quot;scripted&quot;) lookups.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>filename</td>
<td>String</td>
<td></td>
<td>The name of the static lookup table file.</td>
</tr>
<tr>
<td>max_matches</td>
<td>Number</td>
<td></td>
<td>The maximum number of possible matches for each input lookup value.</td>
</tr>
<tr>
<td>max_offset_secs</td>
<td>Number</td>
<td></td>
<td>For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.</td>
</tr>
<tr>
<td>min_matches</td>
<td>Number</td>
<td></td>
<td>The minimum number of possible matches for each input lookup value.</td>
</tr>
<tr>
<td>min_offset_secs</td>
<td>Number</td>
<td></td>
<td>For temporal lookups, this is the minimum time (in seconds) that the event timestamp can be later than the lookup entry timestamp for a match to occur.</td>
</tr>
<tr>
<td>replicate_delta</td>
<td>Boolean</td>
<td>false</td>
<td>Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.</td>
</tr>
<tr>
<td>time_field</td>
<td>String</td>
<td></td>
<td>For temporal lookups, this is the field in the lookup table that represents the timestamp.</td>
</tr>
<tr>
<td>time_format</td>
<td>String</td>
<td></td>
<td>For temporal lookups, this specifies the &quot;strftime&quot; format of the timestamp field.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off--it ensures that certain fields are always discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td>If set to true, Splunk software &quot;cleans&quot; the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.</td>
</tr>
<tr>
<td>DEFAULT_VALUE</td>
<td>Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.</td>
</tr>
<tr>
<td>DEST_KEY</td>
<td>Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation for data/transforms/extractions.</td>
</tr>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>If set to true, Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>LOOKAHEAD</td>
<td>Optional attribute for index-time field extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.</td>
</tr>
<tr>
<td>REGEX</td>
<td>The regular expression to operate on your data.</td>
</tr>
</tbody>
</table>
This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms.

For details, see the documentation for this parameter in the POST operation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE_KEY</td>
<td>The KEY to which Splunk software applies REGEX.</td>
</tr>
<tr>
<td>WRITE_META</td>
<td>Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.</td>
</tr>
<tr>
<td>default_match</td>
<td>If min_matches is greater than zero and Splunk software has less than min_matches for any given input, it provides this default_match value one or more times until the min_matches threshold is reached.</td>
</tr>
<tr>
<td>disabled</td>
<td>Specifies whether the lookup definition is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which the lookups are defined. For example, the search app.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The Splunk user for which the lookups are defined.</td>
</tr>
<tr>
<td>external_cmd</td>
<td>Provides the command and arguments to invoke to perform a lookup. Use this for external (or &quot;scripted&quot;) lookups, where you interface with with an external script rather than a lookup table. This string is parsed like a shell command. The first argument is expected to be a python script located in: $SPLUNK_HOME/etc/&lt;app_name&gt;/bin (or ../etc/searchscripts) Presence of this field indicates that the lookup is external and command based.</td>
</tr>
<tr>
<td>fields_list</td>
<td>List of all fields that are supported by the external command. Use this for external (or &quot;scripted&quot;) lookups.</td>
</tr>
<tr>
<td>filename</td>
<td>The name of the static lookup table file.</td>
</tr>
<tr>
<td>max_matches</td>
<td>The maximum number of possible matches for each input lookup value. If the lookup is non-temporal (not time-bounded, meaning the time_field attribute is not specified), Splunk software uses the first &lt;integer&gt; entries, in file order. If the lookup is temporal, Splunk software uses the first &lt;integer&gt; entries in descending time order. Default = 100 if the lookup is not temporal, default = 1 if it is temporal.</td>
</tr>
<tr>
<td>max_offset_secs</td>
<td>For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.</td>
</tr>
<tr>
<td>min_matches</td>
<td>The minimum number of possible matches for each input lookup value.</td>
</tr>
<tr>
<td>min_offset_secs</td>
<td>For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.</td>
</tr>
<tr>
<td>time_field</td>
<td>For temporal lookups, this is the field in the lookup table that represents the timestamp.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>time_format</td>
<td>For temporal lookups, this specifies the <code>\&quot;strptime\&quot;</code> format of the timestamp field.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type. Can be either external or file.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/lookups -d name=my_lookup -d filename=lookup.csv

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups</id>
  <updated>2011-08-01T21:10:33-07:00</updated>
  <generator version="105049"/>
  <author><name>Splunk</name></author>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>my_lookup</title>
    <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup</id>
    <updated>2011-08-01T21:10:33-07:00</updated>
    <author><name>admin</name></author>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="alternate"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/edit" rel="edit"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/remove" rel="remove"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/move" rel="move"/>
    <link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:dict name="CAN_OPTIMIZE">1</s:dict>
        <s:dict name="CLEAN_KEYS">1</s:dict>
        <s:dict name="DEFAULT_VALUE"/>
        <s:dict name="DEST_KEY"/>
        <s:dict name="FORMAT"/>
        <s:dict name="KEEP_EMPTY_VALS">0</s:dict>
        <s:dict name="LOOKAHEAD">4096</s:dict>
        <s:dict name="MV_ADD">0</s:dict>
        <s:dict name="REGEX"/>
        <s:dict name="SOURCE_KEY">_raw</s:dict>
        <s:dict name="WRITE_META">0</s:dict>
      </s:dict>
    </content>
  </entry>
</feed>
```
data/transforms/lookups/{name}

https://<host>:<mPort>/services/data/transforms/lookups/{name}

Manage the {name} lookup definition.

DELETE

Delete a specific lookup definition.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
    xmlns:s="http://dev.splunk.com/ns/rest">
  <title>transforms-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups</id>
  <updated>2011-07-21T20:03:24-07:00</updated>
  <generator version="104309"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_new" rel="create"/>
GET

Access a specific lookup definition.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>replicate_delta</td>
<td>Boolean</td>
<td>false</td>
<td>Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Indicates whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off—it ensures that certain fields are always discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td>Indicates whether Splunk software &quot;cleans&quot; the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.</td>
</tr>
<tr>
<td>DEFAULT_VALUE</td>
<td>Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.</td>
</tr>
<tr>
<td>DEST_KEY</td>
<td>Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation for data/transforms/extractions.</td>
</tr>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>Indicates whether Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>LOOKAHEAD</td>
<td>For index-time filed extractions. Specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>&quot;If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.</td>
</tr>
<tr>
<td>REGEX</td>
<td>The regular expression to operate on your data.</td>
</tr>
</tbody>
</table>
This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms.

For details, see the documentation for this parameter in the POST operation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE_KEY</td>
<td>The KEY to which Splunk software applies REGEX.</td>
</tr>
<tr>
<td>WRITE_META</td>
<td>Indicates whether to automatically write REGEX to metadata. This attribute is required for all index-time field extractions except for those where DEST_KEY = meta (see the description of the DEST_KEY attribute). Use instead of DEST_KEY = meta.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this lookup is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk software app for which the lookups are defined. For example, the search app.</td>
</tr>
<tr>
<td>eai:attributes</td>
<td>Field control information.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The Splunk user for which the lookups are defined.</td>
</tr>
<tr>
<td>filename</td>
<td>The name of the static lookup table file.</td>
</tr>
<tr>
<td>replicate_delta</td>
<td>Indicates that only the changes to a CSV lookup table are replicated, rather than the entire lookup table.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the field extraction type. Can be either external or file.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup
```

**XML Response**

```xml
  <title>transforms-lookup</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups</id>
  <updated>2011-08-01T21:11:01-07:00</updated>
  <generator version="105049"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_new" rel="create"/>
  <link href="/servicesNS/admin/search/data/transforms/lookups/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
```

777
<title>my_lookup</title>
<id>https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup</id>
<updated>2011-08-01T21:11:01-07:00</updated>
<author>
  <name>admin</name>
</author>
<link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="alternate"/>
<link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="list"/>
<link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/_reload" rel="_reload"/>
<link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="edit"/>
<link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup" rel="remove"/>
<link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/move" rel="move"/>
<link href="/servicesNS/admin/search/data/transforms/lookups/my_lookup/disable" rel="disable"/>
<content type="text/xml">
  <s:dict>
    <s:key name="CAN_OPTIMIZE">1</s:key>
    <s:key name="CLEAN_KEYS">1</s:key>
    <s:key name="DEFAULT_VALUE"/>
    <s:key name="DEST_KEY"/>
    <s:key name="FORMAT"/>
    <s:key name="KEEP_EMPTY_VALS">0</s:key>
    <s:key name="LOOKAHEAD">4096</s:key>
    <s:key name="MV_ADD">0</s:key>
    <s:key name="REGEX"/>
    <s:key name="SOURCE_KEY">_raw</s:key>
    <s:key name="WRITE_META">0</s:key>
    ... eai:acl node elided ...
    <s:key name="eai:appName">search</s:key>
    <s:key name="eai:attributes">
      <s:dict>
        <s:key name="optionalFields">
          <s:list>
            <s:item>default_match</s:item>
            <s:item>disabled</s:item>
            <s:item>external_cmd</s:item>
            <s:item>fields_list</s:item>
            <s:item>filename</s:item>
            <s:item>max_matches</s:item>
            <s:item>max_offset_secs</s:item>
            <s:item>min_matches</s:item>
            <s:item>min_offset_secs</s:item>
            <s:item>replicate_delta</s:item>
            <s:item>time_field</s:item>
            <s:item>time_format</s:item>
          </s:list>
        </s:key>
        <s:key name="requiredFields">
          <s:list/>
        </s:key>
        <s:key name="wildcardFields">
          <s:list/>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="eai:userName">admin</s:key>
    <s:key name="filename">lookup.csv</s:key>
    <s:key name="replicate_delta">1</s:key>
    <s:key name="type">file</s:key>
  </s:dict>
</content>
POST

Update a lookup definition.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>collection</td>
<td>String</td>
<td>&lt;empty&gt;</td>
<td>Name of the collection to use for this lookup. The collection should be defined in $SPLUNK_HOME/etc/&lt;app_name&gt;/collections.conf for the current app. To create a KV Store lookup, use collection to pass in the KV Store collection name and include the external_type parameter with a value of kvstore in your POST request.</td>
</tr>
<tr>
<td>default_match</td>
<td>String</td>
<td></td>
<td>If min_matches is greater than zero and Splunk software has less than min_matches for any given input, it provides this default_match value one or more times until the min_matches threshold is reached.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Specifies whether the lookup definition is disabled.</td>
</tr>
<tr>
<td>external_cmd</td>
<td>String</td>
<td></td>
<td>Provides the command and arguments to invoke to perform a lookup. Use this for external (or &quot;scripted&quot;) lookups, where you interface with with an external script rather than a lookup table. This string is parsed like a shell command. The first argument is expected to be a python script located in: $SPLUNK_HOME/etc/&lt;app_name&gt;/bin (or ../etc/searchscripts) Presence of this field indicates that the lookup is external and command based.</td>
</tr>
<tr>
<td>external_type</td>
<td>String</td>
<td></td>
<td>Type of external command for performing a lookup. Type of external command for performing a lookup. To define a KV Store lookup, use external_type = kvstore. Include the KV Store collection name in your POST request.</td>
</tr>
<tr>
<td>fields_list</td>
<td>String</td>
<td></td>
<td>A comma- and space-delimited list of all fields that are supported by the external command. Use this for external (or &quot;scripted&quot;) lookups.</td>
</tr>
<tr>
<td>filename</td>
<td>String</td>
<td></td>
<td>The name of the static lookup table file.</td>
</tr>
<tr>
<td>max_matches</td>
<td>Number</td>
<td></td>
<td>The maximum number of possible matches for each input lookup value.</td>
</tr>
<tr>
<td>max_offset_secs</td>
<td>Number</td>
<td></td>
<td>For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.</td>
</tr>
<tr>
<td>min_matches</td>
<td>Number</td>
<td></td>
<td>The minimum number of possible matches for each input lookup value.</td>
</tr>
<tr>
<td>min_offset_secs</td>
<td>Number</td>
<td></td>
<td>For temporal lookups, this is the minimum time (in seconds) that the event timestamp can be later than the lookup entry timestamp for a match to occur.</td>
</tr>
<tr>
<td>replicate_delta</td>
<td>Boolean</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>
Enable to replicate only the changes to a CSV lookup table rather than replicating the entire lookup table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time_field</td>
<td>String</td>
<td></td>
<td>For temporal lookups, this is the field in the lookup table that represents the timestamp.</td>
</tr>
<tr>
<td>time_format</td>
<td>String</td>
<td></td>
<td>For temporal lookups, this specifies the &quot;strftime&quot; format of the timestamp field.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAN_OPTIMIZE</td>
<td>Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled). You might use this when you have field discovery turned off—-it ensures that certain fields are always discovered. Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction is ever needed for the successful evaluation of a search.</td>
</tr>
<tr>
<td>CLEAN_KEYS</td>
<td>If set to true, Splunk software “cleans” the field names extracted at search time by replacing non-alphanumeric characters with underscores and stripping leading underscores.</td>
</tr>
<tr>
<td>DEFAULT_VALUE</td>
<td>Optional attribute for index-time field extractions. Splunk software writes the specified value to DEST_KEY if the specified REGEX fails.</td>
</tr>
<tr>
<td>DEST_KEY</td>
<td>Valid for index-time field extractions, specifies where Splunk software stores the REGEX results.</td>
</tr>
<tr>
<td>FORMAT</td>
<td>This option is valid for both index-time and search-time field extractions. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time. This attribute specifies the format of the event, including any field names or values you want to add. For details, refer to the documentation for this parameter in the POST operation for data/transforms/transformations.</td>
</tr>
<tr>
<td>KEEP_EMPTY_VALS</td>
<td>If set to true, Splunk software preserves extracted fields with empty values.</td>
</tr>
<tr>
<td>LOOKAHEAD</td>
<td>Optional attribute for index-time field extractions. specifies how many characters to search into an event. Defaults to 4096. You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).</td>
</tr>
<tr>
<td>MV_ADD</td>
<td>If Splunk software extracts a field that already exists and MV_ADD is set to true, the field becomes multivalued, and the newly-extracted value is appended. If MV_ADD is set to false, the newly-extracted value is discarded.</td>
</tr>
<tr>
<td>REGEX</td>
<td>The regular expression to operate on your data. This attribute is valid for both index-time and search-time field extractions: REGEX is required for all search-time transforms unless you are setting up a delimiter-based field extraction, in which case you use DELIMS (see the DELIMS attribute description, below). REGEX is required for all index-time transforms. For details, see the documentation for this parameter in the POST operation.</td>
</tr>
<tr>
<td>SOURCE_KEY</td>
<td>The KEY to which Splunk software applies REGEX.</td>
</tr>
<tr>
<td>WRITE_META</td>
<td>Indicates whether to automatically write REGEX to metadata.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>default_match</strong></td>
<td>If min_matches is greater than zero and Splunk software has less than min_matches for any given input, it provides this default_match value one or more times until the min_matches threshold is reached.</td>
</tr>
<tr>
<td><strong>disabled</strong></td>
<td>Specifies whether the lookup definition is disabled.</td>
</tr>
<tr>
<td><strong>eai:appName</strong></td>
<td>The Splunk app for which the lookups are defined. For example, the search app.</td>
</tr>
<tr>
<td><strong>eai:userName</strong></td>
<td>The Splunk user for which the lookups are defined.</td>
</tr>
<tr>
<td><strong>external_cmd</strong></td>
<td>Provides the command and arguments to invoke to perform a lookup. Use this for external (or &quot;scripted&quot;) lookups, where you interface with an external script rather than a lookup table.</td>
</tr>
<tr>
<td></td>
<td>This string is parsed like a shell command. The first argument is expected to be a python script located in:</td>
</tr>
<tr>
<td></td>
<td>$SPLUNK_HOME/etc/&lt;app_name&gt;/bin (or ../etc/searchscripts)</td>
</tr>
<tr>
<td></td>
<td>Presence of this field indicates that the lookup is external and command based.</td>
</tr>
<tr>
<td><strong>fields_list</strong></td>
<td>List of all fields that are supported by the external command. Use this for external (or &quot;scripted&quot;) lookups.</td>
</tr>
<tr>
<td><strong>filename</strong></td>
<td>The name of the static lookup table file.</td>
</tr>
<tr>
<td><strong>max_matches</strong></td>
<td>The maximum number of possible matches for each input lookup value.</td>
</tr>
<tr>
<td><strong>max_offset_secs</strong></td>
<td>For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.</td>
</tr>
<tr>
<td><strong>min_matches</strong></td>
<td>The minimum number of possible matches for each input lookup value.</td>
</tr>
<tr>
<td><strong>min_offset_secs</strong></td>
<td>For temporal lookups, this is the maximum time (in seconds) that the event timestamp can be later than the lookup entry time for a match to occur.</td>
</tr>
<tr>
<td><strong>time_field</strong></td>
<td>For temporal lookups, this is the field in the lookup table that represents the timestamp.</td>
</tr>
<tr>
<td><strong>time_format</strong></td>
<td>For temporal lookups, this specifies the &quot;strptime&quot; format of the timestamp field.</td>
</tr>
<tr>
<td><strong>type</strong></td>
<td>Specifies the field extraction type. Can be either external or file.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/transforms/lookups/my_lookup -d external_cmd=myscript.py -d fields_list=a,b,c

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"/>
```

781
data/transforms/metric-schema

https://<host>:<mPort>/services/data/transforms/metric-schema

Use this endpoint to configure ingest-time log-to-metrics transformations. Identify measurements and blacklist dimensions. Design transformations that target specific event schemas within a log.
Authentication and Authorization
Use of this endpoint is restricted to roles that have the edit_metric_schema capability.

Usage Details
For more information about carrying out ingest-time log-to-metrics transformations using this endpoint, see Convert event logs to metric data points in Metrics.

GET
List existing log-to-metrics configurations.

Request parameters
None.

Returned parameters
None

Example request and response

XML Request
curl -k -u admin:ch@ngeme -X GET https://localhost:8089/services/data/transforms/metric-schema/splunk_metrics

XML Response

<title>metric-schema</title>
<id>https://localhost:8089/services/data/transforms/metric-schema</id>
<updated>2018-07-31T17:00:21-07:00</updated>
<generator build="06d0f1f682cc" version="7.1.0"/>
<author>
 <name>Splunk</name>
</author>
<link href="/services/data/transforms/metric-schema/_new" rel="create"/>
<link href="/services/data/transforms/metric-schema/_reload" rel="_reload"/>
<link href="/services/data/transforms/metric-schema/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>metric-schema:splunk_metrics</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics" rel="alternate"/>
<auteur>
 <name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/_acl" rel="_acl"/>
</entry>
POST

Configures ingest-time conversion of log events to metric data points.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required. Name of the <code>metric-schema stanza</code> in <code>transforms.conf</code>.</td>
</tr>
<tr>
<td>field_name</td>
<td>String</td>
<td>Comma-separated list of measure fields to be extracted from a log line.</td>
</tr>
<tr>
<td>blacklist_dimension</td>
<td>String</td>
<td>Comma-separated list of dimension fields to be omitted when log events are converted to metric data points.</td>
</tr>
<tr>
<td>metric_name_prefix</td>
<td>String</td>
<td>Used when the events in a log have more than one schema, meaning that they have differing sets of measure fields and blacklist dimension fields. Takes the value of a field that is shared by all events in the log, and whose values correspond to the different event schemas.</td>
</tr>
</tbody>
</table>

Returned parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>METRIC-SCHEMA-MEASURES-&lt;metric_name_prefix&gt;</code></td>
<td>String</td>
<td>Comma-separated list of measure fields to be extracted from a log line.</td>
</tr>
<tr>
<td><code>METRIC-SCHEMA-BLACKLIST-DIMS-&lt;metric_name_prefix&gt;</code></td>
<td>String</td>
<td>Comma-separated list of dimension fields to be omitted when log events are converted to metric data points.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```bash
curl -k -u admin:ch@ngeme -X POST https://localhost:8089/services/data/transforms/metric-schema -d "name=splunk_metrics" -d "metric_name_prefix=queue" -d "field_names=max_size_kb,current_size_kb,current_size,largest_size,smallest_size" -d "blacklist_dimensions=location,corp"
```

**XML Response**

```xml
...<entry><id>https://localhost:8089/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics</id>
</entry>
```

785
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics" rel="alternate"/>
<author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics" rel="list"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics" rel="edit"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics" rel="remove"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/move" rel="move"/>
<link href="/servicesNS/nobody/search/data/transforms/metric-schema/metric-schema%3Asplunk_metrics/disable" rel="disable"/>
<content type="text/xml">
  <s:dict>
    <s:key name="METRIC-SCHEMA-BLACKLIST-DIMS-queue">location,corp</s:key>
    <s:key name="METRIC-SCHEMA-MEASURES-queue">max_size_kb,current_size_kb,current_size,largest_size,smallest_size</s:key>
    <s:key name="disabled">0</s:key>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app">search</s:key>
        <s:key name="can_change_perms">1</s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_share_app">1</s:key>
        <s:key name="can_share_global">1</s:key>
        <s:key name="can_share_user">0</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">1</s:key>
        <s:key name="owner">nobody</s:key>
      </s:dict>
    </s:key>
    <s:key name="removable">1</s:key>
    <s:key name="sharing">app</s:key>
  </s:dict>
</content>
</entry>
</feed>
DELETE

Delete existing log-to-metrics configurations.

Request parameters
None.

Returned parameters
None

Example request and response

XML Request

curl -k -u admin:changeme -X DELETE
https://localhost:8089/services/data/transforms/metric-schema/splunk_metrics

XML Response

<title>metric-schema</title>
<id>https://localhost:8089/services/data/transforms/metric-schema</id>
<updated>2018-07-31T16:56:36-07:00</updated>
<generator build="06d0f1f682cc" version="7.1.0"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/data/transforms/metric-schema/_new" rel="create"/>
<link href="/services/data/transforms/metric-schema/_reload" rel="_reload"/>
<link href="/services/data/transforms/metric-schema/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
</feed>

data/transforms/statsdextractions

https://<host>:<mPort>/services/data/transforms/statsdextractions
Use this endpoint to configure dimension extraction from StatsD metrics.

Authentication and Authorization
Use of this endpoint is restricted to roles that have the edit_statsd_transforms capability.

Usage Details
For more information about StatsD dimension extraction using this endpoint, see Get metrics in with StatsD in Metrics.

POST

Configures dimension extraction from StatsD metrics.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>787</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>unique_transforms_stanza_name</td>
<td>String</td>
<td>A unique name for this stanza.</td>
</tr>
<tr>
<td>REGEX = &lt;regular expression&gt;</td>
<td>String</td>
<td>A regular expression that defines how to match and extract dimensions from StatsD metrics data. Splunk supports a named capturing-group extraction format ((\text{dim1})(\text{group}))((\text{dim2})(\text{group})) ... to provide dimension names for the corresponding values that are extracted.</td>
</tr>
<tr>
<td>REMOVE_DIMS_FROM_METRIC_NAME= &lt;Boolean&gt;</td>
<td>Boolean</td>
<td>Specifies whether unmatched segments of the StatsD dotted name segment are used as the metric_name. When true, dimension values are be removed from the measurement and the unmatched portion becomes the metric_name. The default value is true. When false, extracted dimension values are included in the metric_name. For example, a metric measurement name is &quot;x.y.z&quot;. The regular expression matches &quot;y&quot; and &quot;z&quot;. When REMOVE_DIMS_FROM_METRIC_NAME is true, metric_name is &quot;x&quot;. When false, metric_name is &quot;x.y.z&quot;.</td>
</tr>
</tbody>
</table>

Example request and response

Request

curl -k -u admin:pass https://localhost:8089/services/data/transforms/statsdextractions \-d "name=statsd-ex&REGEX=.(?<hostname>\S%2B?)\.(?<ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})&REMOVE_DIMS_FROM_METRIC_NAME=true"

Response

...
data/ui/panels

https://<host>:<mPort>/servicesNS/{user}/{app_name}/data/ui/panels

View, add, or edit dashboard panels.
GET

Access all the XML definitions for existing panels.

Request parameters
None.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:appName</td>
<td>App context for the panel.</td>
</tr>
<tr>
<td>eai:data</td>
<td>XML definition for the panel.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>User who created the panel.</td>
</tr>
<tr>
<td>label</td>
<td>Panel label.</td>
</tr>
<tr>
<td>panel.title</td>
<td>Panel title.</td>
</tr>
<tr>
<td>rootNode</td>
<td>XML root node.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl --get -k -u username:password
https://localhost:8089/servicesNS/admin/search/data/ui/panels

XML Response

```xml
<title>panels</title>
<id>https://localhost:8089/servicesNS/admin/search/data/ui/panels</id>
<updated>2018-12-17T12:03:14-08:00</updated>
<generator build="8f0ead9ec3db" version="7.1.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/data/ui/panels/_new" rel="create"/>
<link href="/servicesNS/admin/search/data/ui/panels/_reload" rel="_reload"/>
<link href="/servicesNS/admin/search/data/ui/panels/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/panels/new_panel</id>
  <updated>2018-12-17T12:02:57-08:00</updated>
  <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
</entry>
```
POST

Create a new dashboard panel source XML definition.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Panel name.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:appName</td>
<td>App context for the panel.</td>
</tr>
<tr>
<td>eai:data</td>
<td>XML definition for the panel.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>User who created the panel.</td>
</tr>
</tbody>
</table>
**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/ui/panels -d "name=new_panel&eai:data=<panel><label>the_new_label</label></panel>"

**XML Response**

```xml
<title>panels</title>
<id>https://localhost:8089/servicesNS/admin/search/data/ui/panels</id>
<updated>2018-12-17T12:02:57-08:00</updated>
<generator build="8f0ead9ec3db" version="7.1.1"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/data/ui/panels/_new" rel="create"/>
<link href="/servicesNS/admin/search/data/ui/panels/_reload" rel="_reload"/>
<link href="/servicesNS/admin/search/data/ui/panels/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>new_panel</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/panels/new_panel</id>
  <updated>2018-12-17T12:02:57-08:00</updated>
  <link href="/servicesNS/admin/search/data/ui/panels/new_panel" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/admin/search/data/ui/panels/new_panel/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/ui/panels/new_panel/_edit" rel="edit"/>
  <link href="/servicesNS/admin/search/data/ui/panels/new_panel/_remove" rel="remove"/>
  <link href="/servicesNS/admin/search/data/ui/panels/new_panel/move" rel="move"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```
data/ui/views

https://<host>:<mPort>/servicesNS/{user}/{app_name}/data/ui/views

View or create a dashboard source XML definition.

GET

Access all the XML definitions for existing dashboards.

Request parameters

None.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:appName</td>
<td>App context for the dashboard.</td>
</tr>
<tr>
<td>eai:data</td>
<td>XML definition for the dashboard.</td>
</tr>
<tr>
<td>eai:type</td>
<td>User interface type. For dashboards, this type is view.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>User who created the dashboard.</td>
</tr>
<tr>
<td>isDashboard</td>
<td>Boolean value indicating whether the knowledge object is a dashboard.</td>
</tr>
<tr>
<td>isVisible</td>
<td>Boolean value indicating whether the dashboard is visible.</td>
</tr>
<tr>
<td>label</td>
<td>Dashboard label.</td>
</tr>
<tr>
<td>rootNode</td>
<td>XML root node.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl --get -k -u username:password
https://localhost:8089/servicesNS/admin/search/data/ui/views

XML Response

<title>views</title>
<id>https://localhost:8089/servicesNS/admin/search/data/ui/views</id>
<updated>2015-10-08T16:17:03-07:00</updated>
<generator build="a1c9b18fddcf" version="6.3.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/data/ui/views/_new" rel="create"/>
<link href="/servicesNS/admin/search/data/ui/views/_acl" rel="_acl"/>
<link href="/servicesNS/admin/search/data/ui/views/_reload" rel="_reload"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>my_dashboard</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard</id>
  <updated>2015-10-08T16:17:03-07:00</updated>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="list"/>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="edit"/>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard" rel="remove"/>
  <link href="/servicesNS/admin/search/data/ui/views/my_dashboard/move" rel="move"/>
  <content type="text/xml">
    <s:dict>
      <s:dict name="disabled">0</s:dict>
      <s:dict name="eai:acl">
        <s:dict name="app">search</s:dict>
        <s:dict name="can_change_perms">1</s:dict>
        <s:dict name="can_list">1</s:dict>
        <s:dict name="can_change_app">1</s:dict>
        <s:dict name="can_share_app">1</s:dict>
        <s:dict name="can_share_user">1</s:dict>
        <s:dict name="can_write">1</s:dict>
        <s:dict name="modifiable">1</s:dict>
        <s:dict name="owner">admin</s:dict>
        <s:dict name="perms"/>
        <s:dict name="removable">1</s:dict>
        <s:dict name="sharing">user</s:dict>
      </s:dict>
      <s:dict name="eai:appName">search</s:dict>
      <s:dict name="eai:attributes">
        <s:dict name="optionalFields">
          <s:list>
            <s:dict name="eai:type">s:item</s:dict>
          </s:list>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
POST

Create a new dashboard source XML definition.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Dashboard name.</td>
</tr>
<tr>
<td>eai:data</td>
<td>XML document</td>
<td></td>
<td>Dashboard XML definition.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:appName</td>
<td>App context for the dashboard.</td>
</tr>
<tr>
<td>eai:data</td>
<td>XML definition for the dashboard.</td>
</tr>
<tr>
<td>eai:type</td>
<td>User interface type. For dashboards, this type is view.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>User who created the dashboard.</td>
</tr>
<tr>
<td>isDashboard</td>
<td>Boolean value indicating whether the knowledge object is a dashboard.</td>
</tr>
<tr>
<td>isVisible</td>
<td>Boolean value indicating whether the dashboard is visible.</td>
</tr>
<tr>
<td>label</td>
<td>Dashboard label.</td>
</tr>
<tr>
<td>rootNode</td>
<td>XML root node.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/data/ui/views -d "name=new_dashboard&eai:data=<dashboard><label>the_new_label</label></dashboard>"

XML Response

<title>views</title>
<id>https://localhost:8089/servicesNS/admin/search/data/ui/views</id>
<updated>2015-10-08T15:50:01-07:00</updated>
<generator build="a1c9b18f6d4f" version="6.3.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/data/ui/views/_new" rel="create"/>
<link href="/servicesNS/admin/search/data/ui/views/_reload" rel="_reload"/>
<link href="/servicesNS/admin/search/data/ui/views/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>new_dashboard</title>
  <id>https://localhost:8089/servicesNS/admin/search/data/ui/views/new_dashboard</id>
  <updated>2015-10-08T15:50:01-07:00</updated>
  <link href="/servicesNS/admin/search/data/ui/views/new_dashboard" rel="alternate"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/servicesNS/admin/search/data/ui/views/new_dashboard" rel="list"/>
  <link href="/servicesNS/admin/search/data/ui/views/new_dashboard/_reload" rel="_reload"/>
  <link href="/servicesNS/admin/search/data/ui/views/new_dashboard" rel="edit"/>
  <link href="/servicesNS/admin/search/data/ui/views/new_dashboard" rel="remove"/>
  <link href="/servicesNS/admin/search/data/ui/views/new_dashboard/move" rel="move"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">admin</s:key>
          <s:key name="perms"/>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">user</s:key>
        </s:dict>
      </s:key>
      <s:key name="eai:appName">search</s:key>
      <s:key name="eai:data">"<![](<dashboard><label> the_new_label </label></dashboard>"
      <s:key name="eai:digest">533c60e648b7c4733321ae205d2627d8</s:key>
      <s:key name="eai:type">views</s:key>
      <s:key name="eai:userName">admin</s:key>
      <s:key name="isDashboard">1</s:key>
      <s:key name="isVisible">1</s:key>
      <s:key name="label">the_new_label</s:key>
      <s:key name="rootNode">dashboard</s:key>
    </s:dict>
  </content>
</entry>
data/ui/views/{name}

https://<host>:<mPort>/servicesNS/{user}/{app_name}/data/ui/views/{name}
Access or update source XML for an existing dashboard.

GET
Access an existing dashboard XML definition.

Request parameters
None.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:appName</td>
<td>App context for the dashboard.</td>
</tr>
<tr>
<td>eai:data</td>
<td>XML definition for the dashboard.</td>
</tr>
<tr>
<td>eai:type</td>
<td>User interface type. For dashboards, this type is view.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>User who created the dashboard.</td>
</tr>
<tr>
<td>isDashboard</td>
<td>Boolean value indicating whether the knowledge object is a dashboard.</td>
</tr>
<tr>
<td>isVisible</td>
<td>Boolean value indicating whether the dashboard is visible.</td>
</tr>
<tr>
<td>label</td>
<td>Dashboard label.</td>
</tr>
<tr>
<td>rootNode</td>
<td>XML root node.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u username:password
https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard
```

XML Response

```
<title>views</title>
<id>https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard</id>
<updated>2015-10-08T16:17:03-07:00</updated>
<generator build="alc9b18fdcf" version="6.3.0"/>
```
POST

Update a specific dashboard XML definition.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:data</td>
<td>XML document</td>
<td></td>
<td>Dashboard XML definition.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:appName</td>
<td>App context for the dashboard.</td>
</tr>
<tr>
<td>eai:data</td>
<td>XML definition for the dashboard.</td>
</tr>
<tr>
<td>eai:type</td>
<td>User interface type. For dashboards, this type is view.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>User who created the dashboard.</td>
</tr>
<tr>
<td>isDashboard</td>
<td>Boolean value indicating whether the knowledge object is a dashboard.</td>
</tr>
<tr>
<td>isVisible</td>
<td>Boolean value indicating whether the dashboard is visible.</td>
</tr>
<tr>
<td>label</td>
<td>Dashboard label.</td>
</tr>
<tr>
<td>rootNode</td>
<td>XML root node.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u username:password https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard -d "eai:data=<dashboard><label>new_label</label></dashboard>"

XML Response

<entry>
<title>views</title>
<id>https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard</id>
<updated>2015-10-08T16:38:23-07:00</updated>
<generator build="a9c9b18fddfc" version="6.4.0"/>
</entry>
<author><name>Splunk</name></author>

<entry>
<title> my_dashboard </title>
<id>https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard </id>
<updated>2015-10-08T16:38:23-07:00</updated>
<author><name>admin</name></author>
<content type="text/xml">
<s:dict>
<s:key name="disabled">0</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app">search</s:key>
<s:key name="can_change_perms">1</s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_share_app">1</s:key>
<s:key name="can_share_global">1</s:key>
<s:key name="can_share_user">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">1</s:key>
<s:key name="owner">admin</s:key>
<s:key name="perms"/>
<s:key name="removable">1</s:key>
<s:key name="sharing">user</s:key>
</s:dict>
<s:key name="eai:appName">search</s:key>
<s:key name="eai:data"><![CDATA[<dashboard><label>new_label</label></dashboard>]]></s:key>
<s:key name="eai:digest">31513ad66ce14b5c792f175cc1691e5e</s:key>
<s:key name="eai:type">views</s:key>
<s:key name="eai:userName">admin</s:key>
<s:key name="isDashboard">1</s:key>
<s:key name="isVisible">1</s:key>
<s:key name="label">new_label</s:key>
<s:key name="rootNode">dashboard</s:key>
</s:dict>
</content>
DELETE

Delete a specific dashboard XML definition.

Request parameters
None.

Returned values
None.

Example request and response

XML Request

curl -k -u username:password --request DELETE
https://localhost:8089/servicesNS/admin/search/data/ui/views/my_dashboard

XML Response

<title>views</title>
&id>https://localhost:8089/servicesNS/admin/search/data/ui/views</id>
<updated>2015-10-08T17:07:12-07:00</updated>
<generator build="a1c9b8f9dcfe" version="6.3.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/data/ui/views/_new" rel="create"/>
<link href="/servicesNS/admin/search/data/ui/views/_reload" rel="_reload"/>
<link href="/servicesNS/admin/search/data/ui/views/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

datamodel/acceleration (DEPRECATED)

https://<host>:<mPort>/services/datamodel/acceleration
Access information about data models that have acceleration enabled.

datamodel/acceleration/{name} (DEPRECATED)

https://<host>:<mPort>/services/datamodel/acceleration/{name}
Get information about the {name} datamodel.
Note: This endpoint is deprecated.

GET

Get information about a specific data model.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acceleration</td>
<td>Indicates if acceleration is enabled for this data model.</td>
</tr>
<tr>
<td>acceleration.earliest_time</td>
<td>The earliest time to dispatch the search.</td>
</tr>
<tr>
<td>search</td>
<td>Specifies the search to accelerate this data model.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/datamodel/acceleration/simpleMyAppModel

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"/>
<title></title>
<id>https://myserver-centos62x64-4:8789/services/datamodel/acceleration</id>
<updated>2013-08-24T12:55:07-07:00</updated>
<generator build="178272" version="6.0"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>simpleMyAppModel</title>
  <id>https://myserver-centos62x64-4:8789/servicesNS/nobody/search/datamodel/acceleration/simpleMyAppModel</id>
  <updated>2013-08-24T12:55:07-07:00</updated>
  <link href="/servicesNS/nobody/search/datamodel/acceleration/simpleMyAppModel" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/datamodel/acceleration/simpleMyAppModel" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:int>802</s:int>
    </s:dict>
  </content>
</entry>
```
<s:key name="acceleration">1</s:key>
<s:key name="acceleration.earliest_time">-1mon</s:key>
... eai:acl node elided ...
<s:key name="eai:appName">search</s:key>
<s:key name="eai:attributes">
    <s:dict>
        <s:key name="optionalFields">
            <s:list/>
        </s:key>
        <s:key name="requiredFields">
            <s:list/>
        </s:key>
        <s:key name="wildcardFields">
            <s:list/>
        </s:key>
    </s:dict>
</s:dict>
<s:key name="eai:digest">9a9dba7c96b3f81554e3773b8d8fe45e</s:key>
<s:key name="eai:type">datamodels</s:key>
<s:key name="eai:userName">admin</s:key>
<s:key name="search">![CDATA[uri=* status=* clientip=* referer=* useragent=* (sourcetype=access_*) (status < 600) | elided..."HTTP_Request.HTTP_Success.is_not_Pageview", "HTTP_Request.HTTP_Success.Pageview.myevalfield2"]]></s:key>
</s:dict>
</content>
</entry>
</feed>

datamodel/model

https://<host>:<mPort>/services/datamodel/model
Access or create data models.

GET
List data models on the server.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>concise</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to list a concise JSON description of the data model. The concise description is a summary for human readability. It is not used to create the data model.</td>
</tr>
</tbody>
</table>

Request parameters
Pagination and filtering parameters can be used with this method.
Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acceleration</td>
<td>Indicates whether acceleration is enabled for the data model.</td>
</tr>
<tr>
<td>concise</td>
<td>Indicates whether to list a concise JSON description of the data model.</td>
</tr>
<tr>
<td>description</td>
<td>The JSON describing the data model.</td>
</tr>
<tr>
<td>displayName</td>
<td>The name displayed for the data model in Splunk Web.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app in which the data model was created.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The name of the user who created the data model.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/services/datamodel/model
```

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
... opensearch nodes elided ...
</feed>
```
POST

Create a new data model.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>String</td>
<td>JSON</td>
<td>description of the data model.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Name of the data model.</td>
</tr>
<tr>
<td>acceleration</td>
<td>String</td>
<td></td>
<td>Specify the acceleration settings for the data model. Supply JSON to specify any or all of the following settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enabled</td>
<td>• enabled (true or false)</td>
</tr>
</tbody>
</table>

POST

Create a new data model.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>String</td>
<td>JSON</td>
<td>description of the data model.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Name of the data model.</td>
</tr>
<tr>
<td>acceleration</td>
<td>String</td>
<td></td>
<td>Specify the acceleration settings for the data model. Supply JSON to specify any or all of the following settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>enabled</td>
<td>• enabled (true or false)</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>acceleration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• earliest_time (time modifier)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• cron_schedule (cron string)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Example</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>acceleration= ' {</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;enabled&quot;: true,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;earliest_time&quot;: -1mon,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>&quot;cron_schedule&quot;: 0 */12 * * *</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>} '</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Use these settings to configure acceleration for Hunk data models.

- **hunk.compression_codec**
  
  String, case-sensitive.
  Specifies the compression codec to be used for the accelerated orc or parquet format files.
  For parquet file format, use snappy or gzip.
  For orc file format, use snappy or zlib.

- **hunk.dfs_block_size**
  
  Unsigned integer
  Specifies the block size in bytes for the compression files.

- **hunk.file_format**
  
  String, case sensitive.
  Valid options are orc and parquet

Example

```json
acceleration= ' {
   "hunk.file_format": "orc",
   "hunk.compression_codec": "snappy"
} ' 
```

Returned values
None

Example request and response

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/services/datamodel/model -d name=Debugger --data-urlencode description='{"modelName":"Debugger","displayName":"Debugger", "description": "A data model for debugging purposes". . . elided . . . }'
```

**XML Response**

806
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://qa-sv-rh61x64-10:8089/services/datamodel/model</id>
  <updated>2013-10-16T11:24:07-07:00</updated>
  <generator build="183095" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/datamodel/model/_new" rel="create"/>
  <link href="/services/datamodel/model/desc" rel="desc"/>
  <link href="/services/datamodel/model/report" rel="report"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>Debugger</title>
    <id>https://qa-sv-rh61x64-10:8089/servicesNS/admin/search/datamodel/model/Debugger</id>
    <updated>2013-10-16T11:24:07-07:00</updated>
    <link href="/servicesNS/admin/search/datamodel/model/Debugger" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/datamodel/model/Debugger" rel="list"/>
    <link href="/servicesNS/admin/search/datamodel/model/Debugger" rel="edit"/>
    <link href="/servicesNS/admin/search/datamodel/model/Debugger" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="acceleration">{"enabled": false}</s:key>
        <s:key name="description">
          <![CDATA["displayName": "Debugger", "modelName": "Debugger", "objectSummary": "
... "autoextractSearch": " (index = _internal) "]]]>
        </s:key>
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          {'optionalFields': ['acceleration', 'acceleration.cron_schedule',
            'acceleration.earliest_time', 'eai:data'], 'requiredFields': [], 'wildcardFields': []}
        </s:key>
        <s:key name="eai:digest">05ca1a193365a3b613b919c6401591e3</s:key>
        <s:key name="eai:type">models</s:key>
        <s:key name="eai:userName">admin</s:key>
      </s:dict>
    </content>
  </entry>
</feed>

datamodel/model/{name}

https://{host}:{mPort}/services/datamodel/model/{name}
Access, delete, or update the {name} data model.
DELETE

Delete a specific data model.

Request parameters
None

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE https://localhost:8089/services/datamodel/model/MyApp
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://myserver-centos62x64-4:8789/services/datamodel/model</id>
  <updated>2013-08-24T15:00:54-07:00</updated>
  <generator build="178272" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/datamodel/model/_new" rel="create"/>
  <link href="/services/datamodel/model/desc" rel="desc"/>
  <link href="/services/datamodel/model/report" rel="report"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

GET

Access a specific data model.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

808
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>concise</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to list a concise JSON description of the data model.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The concise description is a summary for human readability. It is not used to create the data model.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acceleration</td>
<td>Indicates whether acceleration is enabled for the data model.</td>
</tr>
<tr>
<td>concise</td>
<td>Indicates whether to list a concise JSON description of the data model.</td>
</tr>
<tr>
<td>description</td>
<td>The JSON describing the data model.</td>
</tr>
<tr>
<td>displayName</td>
<td>The name displayed for the data model in Splunk Web.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app in which the data model was created.</td>
</tr>
<tr>
<td>eai:attributes</td>
<td>Field control information.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The name of the Splunk user who created the data model.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/datamodel/model/MyApp
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:s="http://dev.splunk.com/ns/rest"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://myserver-centos62x64-4:8789/services/datamodel/model</id>
  <updated>2013-08-24T13:07:36-07:00</updated>
  <generator build="178272" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/datamodel/model/_new" rel="create"/>
  <link href="/services/datamodel/model/desc" rel="desc"/>
  <link href="/services/datamodel/model/report" rel="report"/>
  ... opensearch nodes elided ... 
  <s:messages/>
  <entry>
    <title>MyApp</title>
    <id>https://myserver-centos62x64-4:8789/servicesNS/nobody/search/datamodel/model/MyApp</id>
    <updated>2013-08-24T13:07:36-07:00</updated>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="list"/>
</feed>
```
### POST

Update a specific data model.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acceleration</td>
<td>String</td>
<td></td>
<td>Specify the acceleration settings for the data model. Supply JSON to specify any or all of the following settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• enabled (true or false)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• earliest_time (time modifier)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• cron_schedule (cron string)</td>
</tr>
</tbody>
</table>

810
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acceleration</td>
<td></td>
<td></td>
<td>Use these settings to configure acceleration for Hunk data models.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>hunk.compression_codec</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>String, case-sensitive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the compression codec to be used for the accelerated orc or</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>parquet format files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For parquet file format, use snappy or gzip.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For orc file format, use snappy or zlib.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>hunk.dfs_block_size</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Unsigned integer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the block size in bytes for the compression files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- <strong>hunk.file_format</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>String, case sensitive.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Valid options are orc and parquet</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td></td>
<td>JSON description of the data model.</td>
</tr>
<tr>
<td>provisional</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether the data model is provisional. Provisional data models</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>are not saved.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specify true to validate a data model before saving it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If the endpoint returns with no errors, then specify this endpoint again,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>with provisional set to false, to save the data model.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>acceleration</td>
<td>Indicates whether acceleration is enabled for the data model.</td>
</tr>
<tr>
<td>concise</td>
<td>Indicates whether to list a concise JSON description of the data model.</td>
</tr>
<tr>
<td>description</td>
<td>The JSON describing the data model.</td>
</tr>
<tr>
<td>displayName</td>
<td>The name displayed for the data model in Splunk Web.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app in which the data model was created.</td>
</tr>
<tr>
<td>eai:attributes</td>
<td>Field control information.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>The name of the Splunk user who created the data model.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/datamodel/model/MyApp -d concise=true

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title></title>
  <id>https://myserver-centos62x64-4:8789/services/datamodel/model</id>
  <updated>2013-08-24T13:35:54-07:00</updated>
  <generator build="178272" version="6.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/datamodel/model/_new" rel="create"/>
  <link href="/services/datamodel/model/desc" rel="desc"/>
  <link href="/services/datamodel/model/report" rel="report"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>MyApp</title>
    <id>https://myserver-centos62x64-4:8789/servicesNS/nobody/search/datamodel/model/MyApp</id>
    <updated>2013-08-24T13:35:54-07:00</updated>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="list"/>
    <link href="/servicesNS/nobody/search/datamodel/model/MyApp" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="acceleration">{"enabled": false, "earliest_time": ":-1mon"}</s:key>
        <s:key name="description"><![CDATA["modelName": "MyApp", "objects": [{"constraints": [{"search": "sourcetype=access_" OR PodcastDownload", "WebSession", "User"}, "description": "Data model for web analytics."}]}]]></s:key>
        <s:key name="displayName">Web Intelligence</s:key>
        ... eai:acl node elided ...
      </s:dict>
    </content>
  </entry>
</feed>
```
datamodel/pivot

https://<host>:<mPort>/services/datamodel/pivot/{name}
Access pivots that are based on named data models.

GET

Get information about a specific pivot.

Usage details
{name} refers to a data model on the system.

Specify a pivot using either the pivot_search or pivot_json parameter.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pivot_json</td>
<td>String</td>
<td></td>
<td>JSON specifying a pivot based on the named data model.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Typically, you URL encode this parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This endpoint requires either this pivot_json parameter or a pivot_search parameter.</td>
</tr>
<tr>
<td>pivot_search</td>
<td>String</td>
<td></td>
<td>A pivot search command based on the named data model.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Typically, you URL encode this parameter.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This endpoint requires either a pivot_json or this pivot_search parameter.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drilldown_search</td>
<td>The search for running this pivot report using drilldown</td>
</tr>
<tr>
<td>open_in_search</td>
<td>Equivalent to search parameter, but listed more simply.</td>
</tr>
<tr>
<td>pivot_json</td>
<td>JSON specifying a pivot based on the named data model.</td>
</tr>
<tr>
<td>pivot_search</td>
<td>A pivot search command based on the named data model.</td>
</tr>
<tr>
<td>search</td>
<td>The search string for running the pivot report</td>
</tr>
<tr>
<td>tstats_search</td>
<td>The search for running this pivot report using tstats</td>
</tr>
</tbody>
</table>
Example request and response

XML Request


XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:s="http://dev.splunk.com/ns/rest"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
    <title></title>
    <id>https://localhost:8089/services/datamodel/pivot</id>
    <updated>2013-08-26T15:07:57-07:00</updated>
    <generator build="178683" version="20130826"/>
    <author>
        <name>Splunk</name>
    </author>
    ... opensearch nodes elided ...
    <s:messages/>
    <entry>
        <title>Authentication</title>
        <id>https://localhost:8089/servicesNS/nobody/search/datamodel/pivot/Authentication</id>
        <updated>2013-08-26T15:07:57-07:00</updated>
        <link href="/servicesNS/nobody/search/datamodel/pivot/Authentication" rel="alternate"/>
        <author>
            <name>nobody</name>
        </author>
        <link href="/servicesNS/nobody/search/datamodel/pivot/Authentication" rel="list"/>
        <content type="text/xml">
            <s:dict>
                <s:key name="drilldown_search">| search (login OR "log in" OR authenticated) sourcetype!=stash NOT tag=authentication | stats count AS "Count of Untagged Authentication (S.o.S)" | fields , "Count of Untagged Authentication (S.o.S)"| fillnull "Count of Untagged Authentication (S.o.S)"</s:key>
                ... eai:acl node elided ...
                <s:key name="eai:appName">search</s:key>
                <s:dict>
                    <s:dict>
                        <s:dict>
                            <s:dict>
                                <s:dict>
                                    <s:dict>
                                        <s:dict>
                                            <s:dict>
                                                <s:dict>
                                                    <s:dict>
                                                        <s:dict>
                                                            <s:dict>
                                                                <s:dict>
                                                                    <s:dict>
                                                                        <s:dict>
                                                                            <s:dict>
                                                                                <s:dict>
                                                                                    <s:dict>
                                                                                        <s:dict>
                                                                                            <s:dict>
                                                                                                <s:dict>
                                                                                                    <s:dict>
                                                                                                        <s:dict>
                                                                                                            <s:dict>
                                                                                                                <s:dict>
                                                                                                                    <s:dict>
                                                                                                                        <s:dict>
                                                                                                                            <s:dict>
                                                                                                                                <s:dict>
                                                                                                                                    <s:dict>
                                                                                                                                        <s:dict>
                                                                                                                                                <s:dict>
                                                                                                                                                    <s:dict>
                                                                                                                                                        <s:dict>
                                                                                                                                                            <s:dict>
                                                                                                                                                                <s:dict>
                                                                                                                                                                    <s:dict>
                                                                                                                                                                        <s:dict>
                                                                                                                                                                            <s:dict>
                                                                                                                                                                                <s:dict>
                                                                                                                                                                                    <s:dict>
                                                                                                                                                                                        <s:dict>
                                                                                                                                                                                            <s:dict>
                                                                                                                                                                                                <s:dict>
                                                                                                                                                                                                    <s:dict>
                                                                                                                                                                                                        <s:dict>
                                                                                                                                                                                                                <s:dict>
                                                                                                                                                                                                                    <s:dict>
                                                                                                                                                                                                                        <s:dict>
                                                                                                                                                                                                                            <s:dict>
                                                                                                                                                                                                                           <s:dict>
                                                                                                                                                                                                                                   <s:dict>
                                                                                                                                                                                                                                       <s:dict>
                                                                                                                                                                                                                                          <s:dict>
                                                                                                                                                                                                                                                     <s:dict>
                                                                                                                                                                                                                                                    <s:dict>
                                                                                                                                                                                                                                                        <s:dict>
                                                                                                                                                                                                                                                            <s:dict>
                                                                                                                                                                                                                                                                <s:dict>
                                                                                                                                                                                                                                                                    <s:dict>
                                                                                                                                                                                                                                                                        <s:dict>
                                                                                                                                                                                                                                                                                <s:dict>
                                                                                                                                                                                                                                                                                    <s:dict>
                                                                                                                                             ... eai:acl node elided ...
                                                                            <s:dict>
                                                                        <s:dict>
                                                        <s:dict>
                                                    <s:dict>
                                                                                                      ... eai:acl node elided ...
                                            <s:dict>
                                        <s:dict>
                                <s:dict>
                            <s:dict>
                        <s:dict>
                    <s:dict>
                <s:dict>
            <s:dict>
        </entry>
    </feed>
directory

https://<host>:<mPort>/services/directory

Access user configurable objects.

These objects includes search commands, UI views, UI navigation, saved searches and event types. This is useful to see which objects are provided by all apps, or a specific app when the call is namespaced.

GET

List app-scoped objects.

Usage details
Returns an enumeration of the following app scoped objects.

* event types
* saved searches
* time configurations
* views
* navs
* manager XML
* quickstart XML
* search commands
* tags
* field extractions
* lookups
* workflow actions
* field aliases
* sourcetype renames
This is useful to see which apps provide which objects, or all the objects provided by a specific app. To change the visibility of an object type in this listing, use the `showInDirSvc` setting in `restmap.conf`.

**Request parameters**

Pagination and filtering parameters can be used with this method.

**Returned values**

None

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/directory
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      >
  <title>directory</title>
  <id>https://localhost:8089/services/directory</id>
  <updated>2011-05-16T19:03:40-0700</updated>
  <generator version="98144"/>
  <author>
    <name>Splunk</name>
  </author>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>_admin</title>
    <id>https://localhost:8089/servicesNS/nobody/system/data/ui/views/_admin</id>
    <updated>2011-05-16T19:03:40-0700</updated>
    <link href="/servicesNS/nobody/system/data/ui/views/_admin" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/data/ui/views/_admin/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/data/ui/views/_admin" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
      </s:dict>
    </content>
  </entry>
  <entry>
    <title>abc</title>
```
directory/{name}

https://{host}:{mPort}/services/directory/{name}
Get information about the {name} directory entity.

Usage details
This is rarely used. Typically after using the directory service enumeration, a client follows the specific link for an object in an enumeration.

GET
Get information about a specific directory entity.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>eai:type</td>
<td>Entity type.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/directory/dashboard_live

XML Response

817
saved/bookmarks/monitoring_console

https://<host>:<mPort>/services/saved/bookmarks/monitoring_console

Access or create an event type.

GET

Retrieve saved event types.
Example

Request parameters

Pagination and filtering parameters can be used with this method.

Response data keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of this event type.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the event type is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which this event type applies. For example, the Splunk search app.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>Splunk user name of the creator of this event type. For example, the Splunk admin user.</td>
</tr>
<tr>
<td>priority</td>
<td>The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.</td>
</tr>
<tr>
<td>search</td>
<td>Search terms for this event type.</td>
</tr>
<tr>
<td>tags</td>
<td>[Deprecated] Tags associated with this event type.</td>
</tr>
</tbody>
</table>

Use the tags.conf.spec file to assign tags to groups of events with related field values.

Returned values

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
    xmlns:s="http://dev.splunk.com/ns/rest">
    <title>eventtypes</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
    <updated>2011-07-10T23:46:52-07:00</updated>
    <generator version="102807"/>
    <author>
        <name>Splunk</name>
    </author>
    <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
    ... opensearch nodes elided ...
    <s:messages/>
    <entry>
        <title>internal_search_terms</title>
        <id>https://localhost:8089/servicesNS/nobody/system/saved/eventtypes/internal_search_terms</id>
        <updated>2011-07-10T23:46:52-07:00</updated>
        <link href="/servicesNS/nobody/system/saved/eventtypes/internal_search_terms" rel="alternate"/>
        <author>
            <name>nobody</name>
        </author>
    </entry>
</feed>
POST

Create an event type.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>The name for the event type.</td>
</tr>
<tr>
<td>search</td>
<td>String</td>
<td></td>
<td>Search terms for this event type.</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td></td>
<td>Human-readable description of this event type.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>0</td>
<td>If True, disables the event type.</td>
</tr>
<tr>
<td>priority</td>
<td>Number</td>
<td>1</td>
<td>Specify an integer from 1 to 10 for the value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.</td>
</tr>
<tr>
<td>tags</td>
<td>String</td>
<td></td>
<td>[Deprecated] Use tags.conf.spec file to assign tags to groups of events with related field values.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of this event type.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this event type is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which this event type applies. For example, the Splunk search app.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>eai:userName</td>
<td>Splunk user name of the creator of this event type. For example, the Splunk admin user.</td>
</tr>
<tr>
<td>priority</td>
<td>The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.</td>
</tr>
<tr>
<td>search</td>
<td>Search terms for this event type.</td>
</tr>
<tr>
<td>tags</td>
<td>[Deprecated] Tags associated with this event type. Use tags.conf.spec file to assign tags to groups of events with related field values.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes -d name="client-errors" --data-urlencode search=search="http client error NOT (403 OR 404)"

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:47:10-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ...
  <s:messages/>
  <entry>
    <title>client-errors</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors</id>
    <updated>2011-07-10T23:47:10-07:00</updated>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="list"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/edit" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/remove" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="description"/>
        <s:key name="disabled">0</s:key>
        ...
        eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="priority">1</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
saved/eventtypes

https://<host>:<mPort>/services/saved/eventtypes
Access or create an event type.

GET
Retrieve saved event types.

Example

Request parameters

Pagination and filtering parameters can be used with this method.

Response data keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of this event type.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the event type is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which this event type applies. For example, the Splunk search app.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>Splunk user name of the creator of this event type. For example, the Splunk admin user.</td>
</tr>
<tr>
<td>priority</td>
<td>The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.</td>
</tr>
<tr>
<td>search</td>
<td>Search terms for this event type.</td>
</tr>
<tr>
<td>tags</td>
<td>[Deprecated] Tags associated with this event type. Use the tags.conf.spec file to assign tags to groups of events with related field values.</td>
</tr>
</tbody>
</table>

Returned values

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes
XML Response

<Post Create an event type.>

<Request parameters>

823
### Name  
**name** 
*String*  
The name for the event type.

**search** 
*String*  
Search terms for this event type.

**description** 
*String*  
Human-readable description of this event type.

**disabled** 
*Boolean*  
0  
If True, disables the event type.

**priority** 
*Number*  
1  
Specify an integer from 1 to 10 for the value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.

**tags** 
*String*  
[Deprecated] Use tags.conf.spec file to assign tags to groups of events with related field values.

### Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of this event type.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this event type is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which this event type applies. For example, the Splunk search app.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>Splunk user name of the creator of this event type. For example, the Splunk admin user.</td>
</tr>
<tr>
<td>priority</td>
<td>The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.</td>
</tr>
<tr>
<td>search</td>
<td>Search terms for this event type.</td>
</tr>
<tr>
<td>tags</td>
<td>[Deprecated] Tags associated with this event type. Use tags.conf.spec file to assign tags to groups of events with related field values.</td>
</tr>
</tbody>
</table>

### Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes -d name="client-errors" --data-urlencode search=search="http client error NOT (403 OR 404)"

**XML Response**

```xml
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:47:10-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```
saved/eventtypes/{name}

https://{host}:{<mPort>}/services/saved/eventtypes/{name}

Manage the {name} event type.

**DELETE**

Delete an event type.

**Request parameters**

None

**Returned values**

None

**Example request and response**
XML Request

curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:48:29-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
```

GET

Access the {name} event type.

Requests parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of this event type.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the event type is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which this event type applies. For example, the Splunk search app.</td>
</tr>
<tr>
<td>eai:attributes</td>
<td>Field control information.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>Splunk user name of the creator of this event type. For example, the Splunk admin user.</td>
</tr>
<tr>
<td>priority</td>
<td>The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.</td>
</tr>
<tr>
<td>search</td>
<td>Search terms for this event type.</td>
</tr>
<tr>
<td>tags</td>
<td>[Deprecated] Tags associated with this event type. Use the tags.conf.spec file to assign tags to groups of events with related field values.</td>
</tr>
</tbody>
</table>

Example request and response
XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:47:17-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>client-errors</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors</id>
    <updated>2011-07-10T23:47:17-07:00</updated>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/_list" rel="list"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/_edit" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/_remove" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="description"/>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:attributes">
          <s:dict>
            <s:key name="optionalFields">
              <s:dict>
                <s:item>description</s:item>
                <s:item>disabled</s:item>
                <s:item>priority</s:item>
                <s:item>tags</s:item>
              </s:dict>
            </s:key>
            <s:key name="requiredFields">
              <s:list>
                <s:item>search</s:item>
              </s:list>
            </s:key>
            <s:key name="wildcardFields">
              <s:list/>
            </s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
POST

Update an event type.

Usage details
The search must be re-specified for this edit.

URI-encode the search string if it contains any of the following characters: =, &, ?, %

If the search string is not URI-encoded, these characters can be interpreted as part of the HTTP request.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>search</td>
<td>String</td>
<td></td>
<td>Search terms for this event type.</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td></td>
<td>Human-readable description of this event type.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>0</td>
<td>If True, disables the event type.</td>
</tr>
<tr>
<td>priority</td>
<td>Number</td>
<td>1</td>
<td>Specify an integer from 1 to 10 for the value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.</td>
</tr>
<tr>
<td>tags</td>
<td>String</td>
<td>[Deprecated] Use tags.conf.spec file to assign tags to groups of events with related field values.</td>
<td></td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of this event type.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this event type is disabled.</td>
</tr>
<tr>
<td>eai:appName</td>
<td>The Splunk app for which this event type applies. For example, the Splunk search app.</td>
</tr>
<tr>
<td>eai:userName</td>
<td>Splunk user name of the creator of this event type. For example, the Splunk admin user.</td>
</tr>
<tr>
<td>priority</td>
<td>The value used to determine the order in which the matching event types of an event are displayed. 1 is the highest priority.</td>
</tr>
<tr>
<td>search</td>
<td>Search terms for this event type.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>tags</td>
<td>[Deprecated] Tags associated with this event type. Use tags.conf.spec file to assign tags to groups of events with related field values.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors -d description="HTTP Client Errors" --data-urlencode search=search="http client error NOT (403 OR 404)"

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>eventtypes</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes</id>
  <updated>2011-07-10T23:48:22-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/eventtypes/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/eventtypes/_reload" rel="_reload"/>
  ... opensearch nodes elided ... 
  <s:messages/>
  <entry>
    <title>client-errors</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/eventtypes/client-errors</id>
    <updated>2011-07-10T23:48:22-07:00</updated>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="list"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/eventtypes/client-errors/disable" rel="disable"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="description">HTTP Client Errors</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:appName">search</s:key>
        <s:key name="eai:userName">admin</s:key>
        <s:key name="priority">1</s:key>
        <s:key name="search">search</s:key>
        <s:keys name="tags">
          <s:list/>
        </s:keys>
      </s:dict>
    </content>
  </entry>
</feed>
```
search/fields

https://<host>:<mPort>/services/search/fields
Access search field configurations.

Usage details
Field configuration is specified in $SPLUNK_HOME/etc/system/default/fields.conf, with overridden values in $SPLUNK_HOME/etc/system/local/fields.conf.

GET
Get a list of fields registered for field configuration.

Request parameters
None

Returned values
None

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/fields

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>Fields</title>
  <id>/servicesNS/admin/search/search/fields</id>
  <updated>2011-07-11T10:04:51-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>_indextime</title>
    <id>/servicesNS/admin/search/search/fields/_indextime</id>
    <updated>2011-07-11T10:04:51-07:00</updated>
    <link href="/servicesNS/admin/search/search/fields/_indextime" rel="alternate"/>
  </entry>
</feed>
search/fields/{field_name}

https://<host>:<mPort>/services/search/fields/{field_name}
Access the {field_name} field.

GET
Get information about the {field_name} field.

Request parameters
None

Returned values
None
Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/fields/sourcetype

XML Response

<entry xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest">
    <title>sourcetype</title>
    <id>/servicesNS/admin/search/search/fields/sourcetype</id>
    <updated>2011-07-11T10:08:54-07:00</updated>
    <link href="/servicesNS/admin/search/search/fields/sourcetype" rel="alternate"/>
    <content type="text">
        Attr:INDEXED        True
        Attr:INDEXED_VALUE        False
        Attr:TOKENIZER
    </content>
</entry>

search/fields/{field_name}/tags

https://<host>:<mPort>/services/search/fields/{field_name}/tags
Access or update the tags associated with the {field_name} field.

GET

Get tags associated with the {field_name} field.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/fields/host/tags

XML Response

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest">
    <title>Tags for the host field"</title>
</feed>
POST

Update tags associated with the \{field_name\} field.

Usage details
The value parameter specifies the specific value on which to bind tag actions. Multiple tags can be attached by passing multiple add or delete form parameters. The server processes all of the adds first, and then processes the deletes.

You must specify at least one add or delete parameter.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>String</td>
<td></td>
<td>The specific field value on which to bind the tags.</td>
</tr>
<tr>
<td>add</td>
<td>String</td>
<td></td>
<td>The tag to attach to this field_name:value combination.</td>
</tr>
<tr>
<td>delete</td>
<td>String</td>
<td></td>
<td>The tag to remove to this field_name::value combination.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/fields/host/tags -d add=sfo -d delete=nyc -d value=location

XML Response

<response>
  <messages>

833
<msg type='INFO'>Successfully processed adds/deletes for field host</msg>
</response>

search/tags

https://<host>:<mPort>/services/search/tags
Access search time tags.

GET

List all search time tags.

Request parameters

None

Returned values

None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/tags

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>Tags</title>
  <id>/servicesNS/admin/search/search/tags</id>
  <updated>2011-07-08T01:35:09-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>machine</title>
    <id>/servicesNS/admin/search/search/tags/machine</id>
    <updated>2011-07-08T01:35:09-07:00</updated>
    <link href="/servicesNS/admin/search/search/tags/machine" rel="alternate"/>
  </entry>
  <entry>
    <title>user</title>
    <id>/servicesNS/admin/search/search/tags/user</id>
    <updated>2011-07-08T01:35:09-07:00</updated>
    <link href="/servicesNS/admin/search/search/tags/user" rel="alternate"/>
</feed>
search/tags/{tag_name}

https://<host>:<mPort>/services/search/tags/{tag_name}
Access, update, or delete {tag_name} values.

DELETE
Delete the tag and its associated field:value pair assignments.

Usage details
When a tag is deleted, field:value pairs are set to disabled in tags.conf.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass --request DELETE https://localhost:8089/servicesNS/admin/search/search/tags/user

XML Response

<response>
  <messages>
    <msg type="INFO">Tag successfully deleted</msg>
  </messages>
</response>

GET

Returns a list of field:value pairs associated with the {tag_name} tag.

Request parameters
None
Returned values
None

Example request and response

XML Request

```bash
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/tags/user
```

XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>Field::Value pairs with tag user</title>
  <id>/servicesNS/admin/search/search/tags/user</id>
  <updated>2011-07-08T01:35:28-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <entry>
    <title>eventtype::userupdate</title>
    <id>/servicesNS/admin/search/search/tags/user#eventtype::userupdate</id>
    <updated>2011-07-08T01:35:28-07:00</updated>
    <link href="/servicesNS/admin/search/search/tags/user#eventtype::userupdate" rel="alternate"/>
  </entry>
</feed>
```

POST

Update the field:value pairs associated with the `{tag_name}` tag.

Usage details
Multiple field:value pairs can be attached by passing multiple add or delete form parameters. The server processes all of the adds first, and then deletes.

If `{tag_name}` does not exist, then the tag is created inline. Notification is sent to the client using the HTTP 201 status.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>String</td>
<td></td>
<td>A field:value pair to tag with <code>{tag_name}</code>.</td>
</tr>
<tr>
<td>delete</td>
<td>String</td>
<td></td>
<td>A field:value pair to remove from <code>{tag_name}</code>.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response
XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/tags/user -d add=eventtype::userupdate -d delete=eventtype::useradd-suse

XML Response

<response>
    <messages>
        <msg type="INFO">Processed adds/deletes for tag</msg>
    </messages>
</response>
KV store endpoints

KV Store endpoint descriptions

This introduction describes syntax common to all app KV Store REST endpoints. For more information about the KV Store, see App Key Value Store on the Splunk developer portal.

REST API usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select Settings > Access controls and click Users. To determine the capabilities assigned to a role, select Settings > Access controls and click Roles.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

Managed Splunk Cloud deployments

https://<deployment-name>.splunkcloud.com:8089

Self-service Splunk Cloud deployments

To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the the Splunk REST API Tutorials for more information.
App KV Store REST API features

The app KV Store provides the following functions.

- Create, read, list and delete EAI operations on a collection.
- Create, read, list and delete indexes for a given collection. All collection methods are EAI-compatible. These are not regular EAI operations because the indexes are stored as attributes on the EAI entity. Users must have collection permission to use these operations for a particular collection.
- The ability to insert, read, update and delete a single key and key value, for a given collection, provided that you have permission to modify the collection.
  - Duplicate keys are not allowed.
  - All updates are wholesale updates.
  - Partial value updates are not available.
- The ability to query key-value pairs, for a given collection. For example, to find all the documents that have a host field with a value, use the query \{"host": "bar.com"\}.

Only the following operations are permitted.

- $gt
- $gte
- $lt
- $lte
- $ne
- $and
- $or,
- $not.

The API also supports mechanisms for projection, sorting and pagination.

- Batch reads, inserts, and/or updates for a given collection. This supports high-volume operations and limits network traffic. These operations have the same semantics as their individual counterparts.

**Limits**

- 16MB per record
- 1KB per accelerated field

**Collections**

A Collection is a container of "documents" or "values". Most documents have a similar structure, although structure is not enforced. For example, a Collection might have Notable Events or entities.

Collections are declared in a collections.conf configuration file, where a stanza is a single collection.

**Collection permissioning**

Collections are Splunk entities, which means they are permissioned using the Splunk RBAC/ACL system. Only app-level permissions are available for collections. This means that collections can be defined only in the etc/apps/<app>/[default|local]> directory, not in etc/users/... Attempts to create a user-specific Collection using the API fail and Collections created manually in the .conf files are ignored.
Data

A collection stores key-value pairs consisting of a user-specified or autogenerated key and a JSON document-formatted value. A JSON document/object of values is enforced for simplicity instead of using integer or string raw values. For example, {
  "key": "10.0.0.1",
  "host": "bar.com"
} defines the key ("10.0.0.1") and the full JSON document value.

A key is fetched, updated, and deleted. Partial updates, including array append, are not available. You must set the whole document. Keys are unique within a collection and support only the basic JSON data types: boolean, string, number, object, array, and null.

A value is specified in the _key attribute of the document and, if one is not specified, a random value with a desirable sort order is automatically generated.

A collection is defined in the following directory location.

/servicesNS/nobody/search/storage/collections/mycollection

You can use the following URLs to access the collection.

- /servicesNS/nobody/search/storage/collections/mycollection
- /servicesNS/itay/search/storage/collections/mycollection
- /servicesNS/mark/search/storage/collections/mycollection

Namespaces are separate and data are not interleaved. Wildcard operations on the <user> or <app> parts of the namespace are not available.

User-specific collections are not supported. All users, including nobody, share a single namespace and _key is unique across all namespaces.

Types

You can define a set of types for some fields in a collection. If a field has no type defined, it uses the type submitted over the API. If a type conversion fails, the insert/update operation is aborted.

Here is an example collection in collections.conf.

[mycollection]
field.enabled = bool
field.data.range = cidr

The data inserted or updated in this collection have the fields enabled and range-converted to the applicable type.
Items need to specified using the field prefix only if type needs to be enforced for the field. The array type is not enforceable so does not need to be specified.

**Arrays**

Arrays do not change a nested key name. For example, the key "a.b.c" can refer to{"a": {"b": {"c": 1}}} or{"a": [{"b": [{"c": 1}]}].

**Numbers**

All strings/numbers/booleans are converted to doubles. If a number fails to convert, it inserts the string instead.

**Booleans**

All numbers/strings/booleans are converted to booleans. If a boolean fails to convert, it inserts the string instead. Epoch time can be a string or a number. If it fails to convert, the string version is inserted.

**Strings**

Everything is converted to a string.

**CIDR**

All provided strings are converted to canonical CIDR strings. Here is an example.

```
127.0.0.1       -> 127.000.000.001/32
127.0.0.0/24    -> 127.000.000.000/24
127.0.0/24      -> 127.000.000.000/24
```

Here is an example of similar canonicalization for IPv6.

```
2001:db8::/96               -> 2001:0db8:0000:0000:0000:0000:0000:0000/096
2001:db8:0:0:0:0:ffff     -> 2001:0db8:0000:0000:0000:0000:0000:ffff/128
```

**Queries**

Combining the Data and Index patterns gives the ability to do basic querying. Queries are limited to the basic operators available in most databases, and at the moment do not expose in-array and not-in-array containers. A query can have the following operators.

- `gt`
- `gte`
- `lt`
- `lte`
- `eq`
- `neq`
- `or`
- `and`
- `not`
Queries are permitted regardless of whether an index covers the query. If the index does not cover the query, the query takes longer to complete. For example, here is a query to find all Notable Events authored by userA or userB.

```
{ "$or": [ { "author": "userA" }, { "author": "userB" } ] }
```

Use \$and to search for a range of values. For example, use the following query to find all events with a time field value between 12 and 13.

```
{ "$and": [ { "time": { "$gt": "12" } }, { "time": { "$lt": "13" } } ] }
```

**REST methods**

The REST API for App KV Store implements the GET, POST, and DELETE methods described in this reference.

**Defining KV Store lookups**

For information on using the REST API to define or update a KV Store lookup, see `data/transforms/lookups/` and `data/transforms/lookups/{name}`.

---

**kvstore/backup/create**

https://<host>:<mPort>/services/kvstore/backup/create

**POST**

Create a KV Store backup archive file.

**Usage details**

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive_name</td>
<td>String</td>
<td>Optional. Specify a file name for the backup.</td>
</tr>
<tr>
<td>appname_name</td>
<td>String</td>
<td>Optional. Specify a target collection for backup, rather than all of the KV Store.</td>
</tr>
<tr>
<td>collection_name</td>
<td>String</td>
<td>Optional. Specify a target app for backup, rather than all of the KV Store.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Code 200 for success, and code 404 for failure.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML request**

```
curl -k -u admin:changed -X POST https://localhost:8089/services/kvstore/backup/create -d
```
kvstore/backup/restore

https://<host>:<mPort>/services/kvstore/backup/restore

POST

Extracts the KV Store backup archive file and restores the KV Store.

Usage details

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive_name</td>
<td>String</td>
<td>Required. Specifies the name of the backup file.</td>
</tr>
<tr>
<td>appname_name</td>
<td>String</td>
<td>Optional. Specify a target collection to restore, rather than the entire contents of the archive file.</td>
</tr>
<tr>
<td>collection_name</td>
<td>String</td>
<td>Optional. Specify a target app to restore, rather than the entire contents of the archive file.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Code 200 for success, and code 404 for failure.</td>
</tr>
</tbody>
</table>

Example request and response

XML request

curl -k -u admin:changed -X POST https://localhost:8089/services/kvstore/backup/restore -d 'archiveName=kvdump.tar.gz&appName=search&collectionName=testcollection'

XML response

<title>kvstorebackup</title>
<id>https://localhost:8089/services/kvstore/backup</id>
<updated>2018-04-05T14:18:14-07:00</updated>
<generator build="dbd2996dbabd8f6751392c845684e0ff9d1c2a3" version="20180302"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/kvstore/backup/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

kvstore/backup/restore

https://<host>:<mPort>/services/kvstore/backup/restore

POST

Extracts the KV Store backup archive file and restores the KV Store.

Usage details

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>archive_name</td>
<td>String</td>
<td>Required. Specifies the name of the backup file.</td>
</tr>
<tr>
<td>appname_name</td>
<td>String</td>
<td>Optional. Specify a target collection to restore, rather than the entire contents of the archive file.</td>
</tr>
<tr>
<td>collection_name</td>
<td>String</td>
<td>Optional. Specify a target app to restore, rather than the entire contents of the archive file.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>status</td>
<td>Code 200 for success, and code 404 for failure.</td>
</tr>
</tbody>
</table>

Example request and response

XML request

curl -k -u admin:changed -X POST https://localhost:8089/services/kvstore/backup/restore -d 'archiveName=kvdump.tar.gz&appName=search&collectionName=testcollection'

XML response

<title>kvstorebackup</title>
<id>https://localhost:8089/services/kvstore/backup</id>
<updated>2018-04-05T14:18:14-07:00</updated>
<generator build="dbd2996dbabd8f6751392c845684e0ff9d1c2a3" version="20180302"/>
<author>
kvstore/status

https://<host>:<mPort>/services/kvstore/status

Access KV store status information for standalone or search head clustering (SHC) deployments. For SHC deployments, provides information on SHC members where KV Store is enabled and used for replication.

See also the following KV Store introspection endpoints.

- server/introspection/kvstore
- server/introspection/kvstore/collectionstats
- server/introspection/kvstore/replicasetstats
- server/introspection/kvstore/serverstatus

GET

Access KV store status information.

Usage details

Request parameters

None.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>current</td>
<td>Includes the following indicators for the machine making the GET request.</td>
</tr>
<tr>
<td></td>
<td>• backupRestoreStatus: Status for a KV Store backup in progress. One of the following values:</td>
</tr>
<tr>
<td></td>
<td>• Busy: Backup or restore in progress.</td>
</tr>
<tr>
<td></td>
<td>• Failed: Restore failed to extract an archive file.</td>
</tr>
<tr>
<td></td>
<td>• Ready: Ready to run a backup or restore.</td>
</tr>
<tr>
<td></td>
<td>• Shutdown: KV Store is in the process of shutting down.</td>
</tr>
<tr>
<td></td>
<td>• date: DateTime when this status was retrieved.</td>
</tr>
<tr>
<td></td>
<td>• datesec: Unix timestamp, equivalent to date</td>
</tr>
<tr>
<td></td>
<td>• disabled: If KV Store is disabled on the current member. 0 means enabled, 1 means disabled.</td>
</tr>
<tr>
<td></td>
<td>• guid: Instance ID of the current member.</td>
</tr>
<tr>
<td></td>
<td>• oplogEndTimestamp: Last recorded timestamp in the operations log. Last update in all KV Store collections.</td>
</tr>
<tr>
<td></td>
<td>• oplogEndTimestampSec: Unix timestamp equivalent to oplogEndTimestamp</td>
</tr>
<tr>
<td></td>
<td>• oplogStartTimestamp: First recorded timestamp in the operations log.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>• oplogStartTimestampSec:</td>
<td>Unix timestamp equivalent to oplogStartTimestamp</td>
</tr>
<tr>
<td>• port:</td>
<td>KV Store port</td>
</tr>
<tr>
<td>• replicaSet:</td>
<td>Replica set name. Instance ID by default for standalone mode. Configured in server.conf for SHC.</td>
</tr>
<tr>
<td>• replicationStatus:</td>
<td>In standalone mode, this is KV Store captain. Otherwise, one of the following values.</td>
</tr>
<tr>
<td>• Startup</td>
<td></td>
</tr>
<tr>
<td>• KV Store captain</td>
<td></td>
</tr>
<tr>
<td>• Non-captain KV Store member</td>
<td></td>
</tr>
<tr>
<td>• Recovering</td>
<td></td>
</tr>
<tr>
<td>• Initial Sync</td>
<td></td>
</tr>
<tr>
<td>• Unknown status</td>
<td></td>
</tr>
<tr>
<td>• Down</td>
<td></td>
</tr>
<tr>
<td>• Rollback</td>
<td></td>
</tr>
<tr>
<td>• Removed</td>
<td></td>
</tr>
<tr>
<td>• standalone:</td>
<td>Indicates whether the machine making the request is a standalone member or SHC member. 1 indicates a standalone member.</td>
</tr>
<tr>
<td>• status:</td>
<td>KV Store status. One of the following values.</td>
</tr>
<tr>
<td>• unknown</td>
<td></td>
</tr>
<tr>
<td>• disabled</td>
<td></td>
</tr>
<tr>
<td>• starting</td>
<td></td>
</tr>
<tr>
<td>• ready</td>
<td></td>
</tr>
<tr>
<td>• failed</td>
<td></td>
</tr>
<tr>
<td>• shuttingdown</td>
<td></td>
</tr>
</tbody>
</table>

**Enabled KV Store members**

- Returned for SHC deployments. Lists the following values for SHC members where KV Store is enabled and used for replication.
  - • guid: Instance ID of the current member.
  - • hostAndPort: Address used for replication between KV Store members and for accessing members from splunkd. Can be configured in server.conf.

**KV Store members**

- For KV Store members, lists the following indicators.
  - • configVersion: Version number that increases each time the KV Store cluster is updated.
  - • electionDate: Date/Time for election.
  - • electionDateSec: Unix equivalent of electionDate
  - • hostAndPort: Address used for replication between KV Store members and for accessing members from splunkd. Can be configured in server.conf.
  - • lastHeartbeat: Last time the requesting member sent a heartbeat to this member.
  - • lastHeartbeatRecv: Last time this member replied on heartbeat.
  - • lastHeartbeatRecvSec: Unix equivalent of lastHeartbeatRecv
  - • lastHeartbeatSec: Unix equivalent of lastHeartbeat
  - • optimeDate: Last recorded timestamp for this member in the operations log.
  - • optimeDateSec: Unix equivalent of optimeDate
  - • pingMs: Latency (milliseconds for round trip).
  - • replicationStatus: In standalone mode, this is KV Store captain. Otherwise, one of the following values.
    - • Startup
    - • KV Store captain
    - • Non-captain KV Store member
    - • Recovering
    - • Initial Sync
    - • Unknown status
    - • Down
    - • Rollback
    - • Removed
  - • uptime: Number of seconds this member has been online.

Example request and response
XML request

curl -k -u admin:changed https://localhost:8089/services/kvstore/status

XML response

<title>kvstorestatus</title>
<id>https://localhost:8089/services/kvstore/status</id>
<updated>2016-09-09T15:04:35-07:00</updated>
<generator build="c9af8322d148" version="6.5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/kvstore/status/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>status</title>
  <id>https://localhost:8089/services/kvstore/status/status</id>
  <updated>2016-09-09T15:04:35-07:00</updated>
  <link href="/services/kvstore/status/status" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/kvstore/status/status" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="current">Ready</s:key>
      <s:dict name="backupRestoreStatus">Ready</s:dict>
      <s:key name="date">Fri Sep 9 15:04:35 2016</s:key>
      <s:dict name="dateSec">1473458675.554000</s:dict>
      <s:key name="disabled">0</s:key>
      <s:key name="guid">B4E173F1-02AA-4D46-9DDC-ECF0016F165E</s:key>
      <s:key name="oplogEndTimestamp">Fri Sep 9 14:17:01 2016</s:key>
      <s:dict name="oplogEndTimestampSec">1473455821.000000</s:dict>
      <s:key name="oplogStartTimestamp">Fri Sep 9 07:16:53 2016</s:key>
      <s:dict name="oplogStartTimestampSec">1473430613.000000</s:dict>
      <s:dict name="port">8191</s:dict>
      <s:dict name="replicaSet">B4E173F1-02AA-4D46-9DDC-ECF0016F165E</s:dict>
      <s:dict name="replicationStatus">KV store captain</s:dict>
      <s:dict name="standalone">1</s:dict>
      <s:dict name="status">ready</s:dict>
    </s:dict>
    <s:dict name="eai:acl">
      <s:dict name="app"></s:dict>
      <s:dict name="can_list">1</s:dict>
      <s:dict name="can_write">1</s:dict>
      <s:dict name="modifiable">0</s:dict>
      <s:dict name="owner">system</s:dict>
      <s:dict name="perms">
        <s:dict name="read">
          <s:list>
            <s:item>admin</s:item>
            <s:item>splunk-system-role</s:item>
          </s:list>
        </s:dict>
      </s:dict>
    </s:dict>
  </content>
</entry>
storage/collections/config

https://<host>:<mPort>/servicesNS/{owner}/{app}/storage/collections/config

Access and create collections.

GET

List all collections.

Request parameters
None.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean indicating collection state. By default, the value is false, indicating that the collection is enabled.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>profilingEnabled</td>
<td>Boolean indicating profiling status of slow-running operations. By default, this value is <code>false</code>, meaning that profiling is disabled.</td>
</tr>
<tr>
<td>profilingThresholdMs</td>
<td>Threshold for logging slow-running operations, in milliseconds. Applies only if <code>profilingEnabled</code> is <code>true</code>.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/collections/config

**XML Response**

```xml
...<title>collections-conf</title>
<id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config</id>
<updated>2014-09-02T11:28:27-07:00</updated> <generator build="229629" version="6.2"/>

<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/storage/collections/config/_new" rel="create"/>
<link href="/servicesNS/nobody/search/storage/collections/config/_reload" rel="_reload"/>
... opensearch nodes elided ...</s:messages/>
<entry>
<title>kvstoredemo</title>
<id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config/kvstoredemo</id>
<updated>2014-09-02T11:28:27-07:00</updated>
<author>
  <name>admin</name>
</author>
<link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo" rel="alternate"/>
<link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo" rel="edit"/>
<link href="/servicesNS/nobody/search/storage/collections/config/kvstoredemo/remove" rel="remove"/>
<content type="text/xml">
  <s:dict>
    <s:key name="disabled">0</s:key>
    <s:key name="eai:acl"> ... elided ... </s:key>
    <s:key name="eai:appName">search</s:key>
    <s:key name="eai:userName">nobody</s:key>
    <s:key name="profilingEnabled">false</s:key>
    <s:key name="profilingThresholdMs">100</s:key>
  </s:dict>
</content>
</entry>
<entry>
<title>test</title>
<id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test</id>
<updated>2014-09-02T11:28:27-07:00</updated>
<author>
  <name>admin</name>
</author>
```
POST

Create a collection.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required. Collection name</td>
</tr>
<tr>
<td>profilingEnabled</td>
<td>Boolean</td>
<td>A collections.conf file property that affects profilingThresholdMs. Defaults to false. Enable profiling of slow-running operations by setting profilingEnabled to true.</td>
</tr>
<tr>
<td>profilingThresholdMs</td>
<td>Number</td>
<td>Threshold for logging slow-running operations, in milliseconds. Applies only if profilingEnabled is true. Defaults to 100. Set to 0 to log all slow-running operations.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean indicating collection state. By default, the value is false, indicating that the collection is enabled.</td>
</tr>
<tr>
<td>profilingEnabled</td>
<td>Profiling status of slow-running operations, profilingThresholdMs. Defaults to false.</td>
</tr>
<tr>
<td>profilingThresholdMs</td>
<td>Threshold for logging slow-running operations, in milliseconds. Applies only if profilingEnabled is true.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme -d name=test1
https://localhost:8089/servicesNS/nobody/search/storage/collections/config

XML Response

...
storage/collections/config/{collection}

https://<host>:<mPort>/servicesNS/{owner}/{app}/storage/collections/config/{collection}
Access, delete, or update a specific {collection}.

DELETE
Delete a specific {collection}.

Request parameters
None

Returned values
None

Example request and response

XML Request
curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test -X DELETE

XML Response

...<title>collections-conf</title>
?id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config</id>
<updated>2014-06-02T20:08:11-07:00</updated>
<generator build="210538" version="20140530"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/storage/collections/config/_new" rel="create"/>
<link href="/servicesNS/nobody/search/storage/collections/config/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>

GET

Access a specific {collection}.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean indicating collection state. By default, the value is 0, meaning that the collection is enabled.</td>
</tr>
<tr>
<td>field.&lt;fieldType&gt;</td>
<td>Field type. One of the following values.</td>
</tr>
<tr>
<td></td>
<td>• array</td>
</tr>
<tr>
<td></td>
<td>• number</td>
</tr>
<tr>
<td></td>
<td>• bool</td>
</tr>
<tr>
<td></td>
<td>• string</td>
</tr>
<tr>
<td></td>
<td>• cidr</td>
</tr>
<tr>
<td></td>
<td>• time</td>
</tr>
<tr>
<td>accelerated_fields.&lt;field_name&gt;</td>
<td>Field acceleration name and JSON definition.</td>
</tr>
<tr>
<td>enforceTypes</td>
<td>Boolean indicating if data types are enforced when inserting data into the collection. Defaults to false.</td>
</tr>
<tr>
<td>profilingEnabled</td>
<td>Profiling status of slow-running operations, affecting profilingThresholdMs. By default, the value is false, meaning that profiling is disabled. If true, profiling is enabled.</td>
</tr>
<tr>
<td>profilingThresholdMs</td>
<td>Threshold for logging slow-running operations, in milliseconds. Applies only if profilingEnabled is true.</td>
</tr>
<tr>
<td>replicate</td>
<td>Boolean indicating whether the collection is replicated on indexers. Defaults to false, meaning that this collection is not replicated, and lookups that depend on the collection will not be available. However, if you run a lookup command with local=true, local lookups will still be available.</td>
</tr>
</tbody>
</table>

When true, this collection is replicated on indexers.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>replication_dump_maximum_file_size</td>
<td>Indicates the maximum file size (in KB) for each dump file when <code>replication_dump_strategy</code>=auto. Defaults to 10240KB. If this value is larger than concerningReplicatedFileSize, which is set in the distsearch.conf file, the value of concerningReplicatedFileSize is used instead. KV Store does not pre-calculate the size of the records that will be written to disk, so the size of the resulting files can be affected by the max_rows_in_memory_per_dump setting in the limits.conf file.</td>
</tr>
<tr>
<td>replication_dump_strategy</td>
<td>One of the following two values.</td>
</tr>
<tr>
<td></td>
<td>• auto: Default. Dumps are stored in multiple files when the size of the collection exceeds the value of <code>replication_dump_maximum_file_size</code>.</td>
</tr>
<tr>
<td></td>
<td>• one_file: Dump files are stored in a single file.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/collections/config/test

**XML Response**

```xml
...<title>collections-conf</title>
<id>https://localhost:8089/servicesNS/nobody/search/storage/collections/config</id>
<updated>2014-09-02T11:42:54-07:00</updated> <generator build="229629" version="6.2"/>

<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/nobody/search/storage/collections/config/_new" rel="create"/> <link href="/servicesNS/nobody/search/storage/collections/config/_reload" rel="_reload"/> ...
</xml>
```
Update a specific `{collection}`.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>field.&lt;fieldType&gt;</td>
<td>String</td>
<td>Field type. One of the following values.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• array</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• bool</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• cidr</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• time</td>
</tr>
<tr>
<td>accelerated_fields.&lt;field_name&gt;</td>
<td>String, JSON (see description)</td>
<td>The name of a field acceleration (string) and its definition, in JSON key value format. For example, <code>accelerated_fields.my_accel = {&quot;id&quot;: 1}</code></td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Collection state:</td>
</tr>
<tr>
<td></td>
<td>true = disabled.</td>
</tr>
<tr>
<td></td>
<td>false = [Default] enabled.</td>
</tr>
<tr>
<td>field.&lt;fieldType&gt;</td>
<td>Field type. One of the following values.</td>
</tr>
<tr>
<td></td>
<td>• array</td>
</tr>
<tr>
<td></td>
<td>• number</td>
</tr>
<tr>
<td></td>
<td>• bool</td>
</tr>
<tr>
<td></td>
<td>• string</td>
</tr>
<tr>
<td></td>
<td>• cidr</td>
</tr>
<tr>
<td></td>
<td>• time</td>
</tr>
<tr>
<td>accelerated_fields.&lt;field_name&gt;</td>
<td>The name of a field acceleration (string) and its definition, in JSON key value format. For example, <code>accelerated_fields.my_accel = {&quot;id&quot;: 1}</code></td>
</tr>
<tr>
<td>profilingEnabled</td>
<td>Profiling status of slow-running operations, affecting <code>profilingThresholdMs</code>. By default, the value is false, meaning that profiling is disabled. If <code>true</code>, profiling is enabled.</td>
</tr>
<tr>
<td>profilingThresholdMs</td>
<td>Threshold for logging slow-running operations, in milliseconds. Applies only if <code>profilingEnabled</code> is <code>true</code>.</td>
</tr>
<tr>
<td>replicate</td>
<td>Boolean indicating whether the collection is replicated on indexers. Defaults to false, meaning that this collection is not replicated, and lookups that depend on the collection will not be available. However, if you run a lookup command with <code>local=true</code>, local lookups will still be available. When <code>true</code>, this collection is replicated on indexers.</td>
</tr>
<tr>
<td>replication_dump_maximum_file_size</td>
<td>Indicates the maximum file size (in KB) for each dump file when <code>replication_dump_strategy=auto</code>. Defaults to 10240KB. If this value is larger than <code>concerningReplicatedFileSize</code>, which is set in the <code>distsearch.conf</code> file, the value of <code>concerningReplicatedFileSize</code> is used instead.</td>
</tr>
</tbody>
</table>
KV Store does not pre-calculate the size of the records that will be written to disk, so the size of the resulting files can be affected by the `max_rows_in_memory_per_dump` setting in the `limits.conf` file.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>replication_dump_strategy</td>
<td>One of the following two values.</td>
</tr>
<tr>
<td></td>
<td>• auto: Default. Dumps are stored in multiple files when the size of the collection exceeds the value of <code>replication_dump_maximum_file_size</code>.</td>
</tr>
<tr>
<td></td>
<td>• one_file: Dump files are stored in a single file.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:changeme https://localhost:8089/servicesNS/nobody/search/storage/collections/config/test -d 'accelerated_fields.foo={"a": 1}' -d 'accelerated_fields.bar={"b": -1}' -d "field.a=number" -d "field.b=cidr"

**XML Response**

```xml
...
<title>collections-conf</title>
/id=https://localhost:8089/servicesNS/nobody/search/storage/collections/config</id> <updated>2014-09-02T11:50:57-07:00</updated> <generator build="229629" version="6.2"/>

<author>
  <name>Splunk</name>
</author> <link href="/servicesNS/nobody/search/storage/collections/config/_new" rel="create"/> <link href="/servicesNS/nobody/search/storage/collections/config/_reload" rel="_reload"/> ...

title=test</title> <id=https://localhost:8089/servicesNS/nobod...>2014-09-02T11:50:57-07:00</updated> <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="alternate"/> <author>
  <name>admin</name>
</author> <link href="/servicesNS/nobody/search/storage/collections/config/test" rel="list"/> <link href="/servicesNS/nobody/search/storage/collections/config/test/_reload" rel="_reload"/> <link href="/servicesNS/nobody/search/storage/collections/config/test/edit"/> <link href="/servicesNS/nobody/search/storage/collections/config/test/remove"/> <link href="/servicesNS/nobody/search/storage/collections/config/test/disable" rel="disable"/>

<content type="text/xml">
  <s:dict>
    <s:key name="disabled">0</s:key>
    <s:key name="eai:acl">... elided ...</s:key>
    <s:key name="eai:appName">search</s:key>
    <s:key name="eai:userName">nobody</s:key>
    <s:key name="accelerated_fields.foo">{"a": 1}</s:key>
    <s:key name="accelerated_fields.bar">{"b": -1}</s:key>
    <s:key name="field.a=number">field.b=cidr</s:key>
  <s:dict>
```
storage/collections/data/{collection}

https://<host>:<mPort>/servicesNS/{owner}/{app}/storage/collections/data/{collection}

Access and manage items of a collection.

DELETE

Delete items in the {collection} or delete an entire collection.

Usage details
Use the query parameter to specify which entries to delete. If no query is provided, all entries in the collection are deleted.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>query</td>
<td>JSON object</td>
<td>Query JSON object. Conditional operators: $gt, $gte, $lt, $lte, and $ne Logical operators: $and, $or, and $not (invert conditional operators) Examples: query={&quot;title&quot;:&quot;Item&quot;} (Select all documents with property title that has value Item) query={&quot;price&quot;:{&quot;$gt&quot;:5}} (Select all documents with price greater than 5)</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA -X DELETE

XML Response
No values returned.

GET

Access a specific {collection}.

Request parameters
Parameter order in the request does not matter. Parameters are always applied in the order of sort, skip, and limit.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fields</td>
<td>String</td>
<td>Comma-separated list of fields to include (1) or exclude (0). A fields value cannot contain both include and exclude specifications except for exclusion of the _key field. Examples: fields=firstname,surname (include only firstname, surname, and _key fields) fields=firstname,surname,_key:0 (include only the firstname and surname fields). fields-address:0 (include all fields except the address field)</td>
</tr>
<tr>
<td>limit</td>
<td>Number</td>
<td>Maximum number of items to return. For example, to return five items, use limit=5.</td>
</tr>
<tr>
<td>skip</td>
<td>Number</td>
<td>Number of items to skip from the start. For example, to skip the first ten items, use skip=10.</td>
</tr>
<tr>
<td>sort</td>
<td>String</td>
<td>Sort order. Examples: sort=surname (Sort by surname, ascending) sort=surname,firstname (Sort by surname, ascending, after firstname, ascending) sort=surname:-1,firstname:1 (Sort by surname, descending, after firstname, ascending) sort=surname:1,firstname (Sort by surname, ascending, after firstname, ascending)</td>
</tr>
<tr>
<td>query</td>
<td>JSON object</td>
<td>Query JSON object. Conditional operators: $gt, $gte, $lt, $lte, and $ne Logical operators: $and, $or, and $not (invert conditional operators) Examples: query={&quot;title&quot;:&quot;Item&quot;} (Select all documents with property title that has value Item) query={&quot;price&quot;:{&quot;$gt&quot;:5}} (Select all documents with price greater than 5)</td>
</tr>
</tbody>
</table>

Returned values
The response includes a JSON document.

Example

```json
[{ "myKey" : "abc", "_user" : "nobody", "_key" : "5410be5441ba15298e4624d1" }]
```

POST

Insert an item into the {collection}.

Usage details
The Content-Type header must be application/json.

The _key is autogenerated, if not manually specified.

Request parameters
Make sure that the item to add is a JSON-formatted document, such as the following example.

```json
{ "name": "A" }
```

Returned values
The response includes a JSON-formatted document key, such as the following example.

856
Example request and response

XML Request

curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA -H "Content-Type: application/json" -d '{ "myKey": "abc", "myOtherKey": "abcdef"}"

XML Response

{"_key": "5410be5441ba15298e4624d1"}

storage/collections/data/{collection}/{key}

https://<host>:<mPort>/servicesNS/{owner}/{app}/storage/collections/data/{collection}/{key}
Access and manage a specific {key} item in a {collection}.

DELETE

Delete a collection item.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/collections/data/testCollectionA/5410caf041ba15298e4624d6 -X DELETE

XML Response
No values returned.
GET

Access a collection item.

Request parameters
None

Returned values
The response includes a JSON-formatted \{key\} document, such as the following example.

```
{"myKey" : "abc", "myOtherKey" : "uvwxyz", "_user" : "nobody", "_key" : "5410c8dc41ba15298e4624d5"}
```

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/collections/data/testCollectionA/5410c8dc41ba15298e4624d5
```

XML Response

```
{ "myKey" : "abc", "myOtherKey" : "uvwxyz", "_user" : "nobody", "_key" : "5410c8dc41ba15298e4624d5" }
```

POST

Update a collection item.

Usage details
The header \texttt{Content-Type must be} \texttt{application/json}.

Request parameters
Pass in a JSON-formatted document for the \{key\} that you are updating. For example, use \{ "myKey": "fizz" \}.

Returned values
The response includes a JSON-formatted \{key\} such as the following example.

```
{"_key":"5410c8dc41ba15298e4624d5"}
```

Example request and response

XML Request

```
curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA/5410c8dc41ba15298e4624d5
-H "Content-Type: application/json" -d '{ "myKey": "fizz"}''
```

XML Response

```
858
```
storage/collections/data/{collection}/batch_save

https://<host>:<mPort>/servicesNS/storage/collections/data/{collection}/batch_save
Perform multiple save operations in a batch.

POST
Perform multiple save operations in a batch.

Usage details
The request header 

Content-Type must be application/json.

If a document does not have a 

_key field or store does not have a matching document ID, a _key new document is created.

If an operation fails, the server stops batch processing and returns an HTTP status code other than 200.

Request parameters
Pass in the JSON array of documents to save.

Returned values
The response includes a JSON-formatted list of keys added, such as the following example.

```json
[ "5410c43241ba15298e4624d3", "5418c54e41ba1522677763c01" ]
```

Example request and response

XML Request

curl -k -u admin:changeme
https://localhost:8089/servicesNS/nobody/search/storage/collections/data/testCollectionA/batch_save -H "Content-Type: application/json" -d '{ "_key": "5410c43241ba15298e4624d3", "name": "AAAAAAAA" }, { "name": "A" }'

XML Response

```xml
[ "5410c43241ba15298e4624d3", "5418c54e41ba1522677763c01" ]
```
License endpoints

License endpoint descriptions

Manage licensing configurations.

Usage details

*Review ACL information for an endpoint*

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the REST API User Manual.

*Authentication and Authorization*

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select **Settings > Access controls** and click **Users**. To determine the capabilities assigned to a role, select **Settings > Access controls** and click **Roles**.

*App and user context*

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

*Splunk Cloud URL for REST API access*

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

**Managed Splunk Cloud deployments**

https://<deployment-name>.splunkcloud.com:8089

**Self-service Splunk Cloud deployments**

To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the the Splunk REST API Tutorials for more information.
licenser/groups

https://<host>:<mPort>/services/licenser/groups
Provides access to the configuration of licenser groups.

A licenser group contains one or more licenser stacks that can operate concurrently. Only one licenser group is active at any given time.

GET

Lists all licenser groups.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is_active</td>
<td>Indicates if the license group is active.</td>
</tr>
<tr>
<td>stack_ids</td>
<td>The license stacks in the license group.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

`curl -k -u admin:pass https://localhost:8089/services/licenser/groups`

XML Response

```xml
...<title>groups</title>
<id>https://localhost:8089/services/licenser/groups</id>
<updated>2011-07-11T09:45:35-07:00</updated>
<generator version="102824"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>Enterprise</title>
  <id>https://localhost:8089/services/licenser/groups/Enterprise</id>
  <updated>2011-07-11T09:45:35-07:00</updated>
  <link href="/services/licenser/groups/Enterprise" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/licenser/groups/Enterprise" rel="list"/>
```
licenser/groups/{name}

https://<host>:<mPort>/services/licenser/groups/{name}

Manage the {name} licenser group.

GET

List a specific licenser group.

Usage details
A licenser group contains one or more licenser stacks that can operate concurrently. Only one licenser group is active at any given time.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is_active</td>
<td>Indicates if the license group is active.</td>
</tr>
<tr>
<td>stack_ids</td>
<td>The license stacks in the license group.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```bash
curl -k -u admin:pass https://localhost:8089/services/licenser/groups/Forwarder
```
POST

Activate a specific licenser group and deactivate the previously active one.

Usage details
There can only be a single active licenser group for a given Splunk instance. Use this to switch between, for example, free to enterprise, or download-trial to free.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>is_active</td>
<td>Boolean</td>
<td></td>
<td>Required. Active specific licenser group</td>
</tr>
</tbody>
</table>

**Returned values**

None

**Example request and response**

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/services/licenser/groups/Enterprise -d is_active=1
```

**XML Response**

```
<title>groups</title>
<id>https://localhost:8089/services/licenser/groups</id>
<updated>2011-07-11T09:55:02-07:00</updated>
<generator version="102824"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
```

**licenser/licenses**

https://<host>:<mPort>/services/licenser/licenses

Provides access to the licenses for this Splunk Enterprise instance.

A license enables various features for a Splunk instance, including but not limited to indexing quota, auth, search, forwarding.
GET

List all licenses added.

Usage details

Only a subset of these licenses may be active however, this is simply listing all licenses in every stack/group, regardless of which group is active.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>creation_time</td>
<td>The creation time of this license, in Coordinated Universal Time (UTC).</td>
</tr>
<tr>
<td>expiration_time</td>
<td>The time this license expires, in Coordinated Universal Time (UTC).</td>
</tr>
<tr>
<td>features</td>
<td>The list of features and components enabled by this license.</td>
</tr>
<tr>
<td>group_id</td>
<td>The ID of the group to which this license belongs.</td>
</tr>
<tr>
<td>label</td>
<td>Plain text description of this license.</td>
</tr>
<tr>
<td>license_hash</td>
<td>Unique identifier for the license.</td>
</tr>
<tr>
<td>max_violations</td>
<td>The maximum number of violations allowed during the specified window period.</td>
</tr>
<tr>
<td>quota</td>
<td>Daily indexing quota, in bytes, for this license.</td>
</tr>
<tr>
<td>sourcetypes</td>
<td>The list of allowed sourcetypes for this license. You cannot use this license to index sourcetypes that are not present in this list. An empty list indicates all sourcetypes are allowed.</td>
</tr>
<tr>
<td>stack_id</td>
<td>The ID of the license stack to which this license belongs.</td>
</tr>
<tr>
<td>status</td>
<td>The status of a license can be either VALID or EXPIRED.</td>
</tr>
<tr>
<td>type</td>
<td>Provides any additional information about the type of this license.</td>
</tr>
<tr>
<td>window_period</td>
<td>The rolling period, in days, in which violations are aggregated.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/licenser/licenses

XML Response
<title>licenses</title>

<id>https://localhost:8089/services/licenser/licenses</id>

<updated>2011-07-11T09:30:33-07:00</updated>

<generator version="102824"/>

<author>
   <name>Splunk</name>
</author>

<link href="/services/licenser/licenses/_new" rel="create"/>

... opensearch nodes elided ...

<s:messages/>

<entry>
   <title>E08B ... elided ...FA75BF</title>
   <id>https://localhost:8089/services/licenser/licenses/E08B ... elided ...FA75BF</id>
   <updated>2011-07-11T09:30:33-07:00</updated>
   <link href="/services/licenser/licenses/E08B ... elided ...FA75BF" rel="alternate"/>
   <author>
      <name>system</name>
   </author>
   <link href="/services/licenser/licenses/E08B ... elided ...FA75BF" rel="list"/>
   <link href="/services/licenser/licenses/E08B ... elided ...FA75BF" rel="remove"/>
   <content type="text/xml">
      <s:dict>
         <s:key name="creation_time">1309852804</s:key>
         ... eai:acl node elided ...
         <s:key name="expiration_time">1315641604</s:key>
         <s:key name="features">
            <s:list>
               <s:item>Auth</s:item>
               <s:item>FwdData</s:item>
               <s:item>RcvData</s:item>
               <s:item>LocalSearch</s:item>
               <s:item>DistSearch</s:item>
               <s:item>RcvSearch</s:item>
               <s:item>ScheduledSearch</s:item>
               <s:item>Alerting</s:item>
               <s:item>DeployClient</s:item>
               <s:item>DeployServer</s:item>
               <s:item>SplunkWeb</s:item>
               <s:item>SigningProcessor</s:item>
               <s:item>SyslogOutputProcessor</s:item>
               <s:item>AllowDuplicateKeys</s:item>
            </s:list>
         </s:key>
         <s:key name="group_id">Trial</s:key>
         <s:key name="label">Splunk Enterprise Download Trial</s:key>
         <s:key name="license_hash">E08B ... elided ...FA75BF</s:key>
         <s:key name="max_violations">5</s:key>
         <s:key name="quota">524288000</s:key>
         <s:key name="sourcetypes"></s:list>
         <s:key name="stack_id">download-trial</s:key>
         <s:key name="status">VALID</s:key>
         <s:key name="type">download-trial</s:key>
         <s:key name="window_period">30</s:key>
      </s:dict>
   </content>
</entry>
POST

Add a license entitlement to the current instance.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>string</td>
<td>Required</td>
<td>Path to license file on server. If the payload parameter is specified, the name parameter is ignored.</td>
</tr>
<tr>
<td>payload</td>
<td>string</td>
<td>String representation of license, encoded in xml</td>
<td></td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>creation_time</td>
<td>The creation time of this license, in Coordinated Universal Time (UTC).</td>
</tr>
<tr>
<td>expiration_time</td>
<td>The time this license expires, in Coordinated Universal Time (UTC).</td>
</tr>
<tr>
<td>features</td>
<td>The list of features and components enabled by this license.</td>
</tr>
<tr>
<td>group_id</td>
<td>The ID of the group to which this license belongs.</td>
</tr>
<tr>
<td>label</td>
<td>Plain text description of this license.</td>
</tr>
<tr>
<td>license_hash</td>
<td>Unique identifier for the license. The REST API uses this identifier to access this license.</td>
</tr>
<tr>
<td>max_violations</td>
<td>The maximum number of violations allowed during the specified window period ( window_period ).</td>
</tr>
<tr>
<td>payload</td>
<td>String representation of license, encoded in xml.</td>
</tr>
<tr>
<td>quota</td>
<td>Daily indexing quota, in bytes, for this license.</td>
</tr>
<tr>
<td>sourcetypes</td>
<td>The list of allowed sourcetypes for this list. You cannot use this license to index sourcetypes that are not present in this list. An empty list indicates all sourcetypes are allowed.</td>
</tr>
<tr>
<td>stack_id</td>
<td>The ID of the license stack to which this license belongs.</td>
</tr>
<tr>
<td>status</td>
<td>The status of a license can be either VALID or EXPIRED.</td>
</tr>
<tr>
<td>type</td>
<td>Provides any additional information about the type of this license.</td>
</tr>
<tr>
<td>window_period</td>
<td>The rolling period, in days, in which violations are aggregated.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/licenser/licenses -d
name=/Users/myusername/downloads/Splunk_enterprise.lic
```
<title>licenses</title>
{id>https://localhost:8089/services/licenser/licenses</id>
<updated>2011-07-11T09:41:32-07:00</updated>
<generator version="102824"/>
<author>
    <name>Splunk</name>
</author>
<link href="/services/licenser/licenses/_new" rel="create"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
    <title>CF6C50 ... elided ...72CE6C</title>
    <id>https://localhost:8089/services/licenser/licenses/CF6C50 ... elided ...72CE6C</id>
    <updated>2011-07-11T09:41:32-07:00</updated>
    <link href="/services/licenser/licenses/CF6C50 ... elided ...72CE6C" rel="alternate"/>
    <author>
        <name>system</name>
    </author>
    <link href="/services/licenser/licenses/CF6C50 ... elided ...72CE6C" rel="list"/>
    <link href="/services/licenser/licenses/CF6C50 ... elided ...72CE6C" rel="remove"/>
    <content type="text/xml">
        <s:dict>
            <s:key name="creation_time">1306168427</s:key>
            ... eai:acl node elided ...
            <s:key name="expiration_time">2147483647</s:key>
            <s:key name="features">
                <s:list>
                    <s:item>Auth</s:item>
                    <s:item>FwdData</s:item>
                    <s:item>RcvData</s:item>
                    <s:item>LocalSearch</s:item>
                    <s:item>DistSearch</s:item>
                    <s:item>RcvSearch</s:item>
                    <s:item>ScheduledSearch</s:item>
                    <s:item>Alerting</s:item>
                    <s:item>DeployClient</s:item>
                    <s:item>DeployServer</s:item>
                    <s:item>SplunkWeb</s:item>
                    <s:item>SigningProcessor</s:item>
                    <s:item>SyslogOutputProcessor</s:item>
                    <s:item>CanBeRemoteMaster</s:item>
                </s:list>
            </s:key>
            <s:key name="group_id">Enterprise</s:key>
            <s:key name="license_hash">CF6C50 ... elided ...72CE6C</s:key>
            <s:key name="max_violations">5</s:key>
            <s:key name="quota">10737418240</s:key>
            <s:key name="sourcetypes">
                <s:list/>
            </s:key>
            <s:key name="stack_id">enterprise</s:key>
            <s:key name="status">VALID</s:key>
            <s:key name="type">enterprise</s:key>
            <s:key name="window_period">30</s:key>
        </s:dict>
    </content>
licenser/licenses/{name}

https://<host>:<mPort>/services/licenser/licenses/{name}
Access or delete the {name} license.

DELETE

Delete the license with a hash corresponding to {name}

Usage details
You cannot delete the last license out of an active group. First, deactivate the group (by switching to another group) and then perform the delete.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass --request DELETE https://localhost:8089/services/licenser/licenses/E4BF ... elided ...FC639D

XML Response

...<title>licenses</title>
<!--elided-->
  <s:messages/>
</html>
GET

List license details.

Usage details
The {name} portion of URL is the hash of the license payload.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>creation_time</td>
<td>The creation time of this license, in Coordinated Universal Time (UTC).</td>
</tr>
<tr>
<td>expiration_time</td>
<td>The time this license expires, in Coordinated Universal Time (UTC).</td>
</tr>
<tr>
<td>features</td>
<td>The list of features and components enabled by this license.</td>
</tr>
<tr>
<td>group_id</td>
<td>The ID of the group to which this license belongs.</td>
</tr>
<tr>
<td>label</td>
<td>Plain text description of this license.</td>
</tr>
<tr>
<td>license_hash</td>
<td>Unique identifier for the license. The REST API uses this identifier to access this license.</td>
</tr>
<tr>
<td>max_violations</td>
<td>The maximum number of violations allowed during the specified window period (window_period). Searching is disabled when max_violations is exceeded.</td>
</tr>
<tr>
<td>quota</td>
<td>Daily indexing quota, in bytes, for this license.</td>
</tr>
<tr>
<td>sourcetypes</td>
<td>The list of allowed sourcetypes for this list. You cannot use this license to index sourcetypes that are not present in this list. An empty list indicates all sourcetypes are allowed.</td>
</tr>
<tr>
<td>stack_id</td>
<td>The ID of the license stack to which this license belongs.</td>
</tr>
<tr>
<td>status</td>
<td>The status of a license can be either VALID or EXPIRED.</td>
</tr>
<tr>
<td>type</td>
<td>Provides any additional information about the type of this license.</td>
</tr>
<tr>
<td>window_period</td>
<td>The rolling period, in days, in which violations are aggregated.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://127.0.0.1:3339/services/licenser/licenses/E4BF ... elided ...FC639D

XML Response

870
...<title>licenses</title>
 <id>https://localhost:8089/services/licenser/licenses</id>
 <updated>2011-07-05T15:57:08-07:00</updated>
 <generator version="102824"/>
 <author>
   <name>Splunk</name>
 </author>
 <link href="/services/licenser/licenses/_new" rel="create"/>
 <opensearch:totalResults>1</opensearch:totalResults>
 <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
 <opensearch:startIndex>0</opensearch:startIndex>
 <s:messages/>
 <entry>
   <title>E4BF ... elided ... FC639D</title>
   <id>https://localhost:8089/services/licenser/licenses/E4BF ... elided ... FC639D</id>
   <updated>2011-07-05T15:57:08-07:00</updated>
   <link href="/services/licenser/licenses/E4BF ... elided ... FC639D" rel="alternate"/>
   <author>
     <name>system</name>
   </author>
   <link href="/services/licenser/licenses/E4BF ... elided ... FC639D" rel="list"/>
   <content type="text/xml">
     <s:dict>
       <s:key name="creation_time">1300901512</s:key>
       <s:key name="eai:acl"> ... elided ...</s:key>
       <s:key name="eai:attributes">
         <s:dict>
           <s:key name="optionalFields">
             <s:list/>
           </s:key>
           <s:key name="requiredFields">
             <s:list/>
           </s:key>
           <s:key name="wildcardFields">
             <s:list/>
           </s:key>
         </s:dict>
       </s:key>
       <s:key name="expiration_time">1314811912</s:key>
       <s:key name="features">
         <s:list>
           <s:item>Auth</s:item>
           <s:item>FwdData</s:item>
           <s:item>RcvData</s:item>
           <s:item>LocalSearch</s:item>
           <s:item>DistSearch</s:item>
           <s:item>RcvSearch</s:item>
           <s:item>ScheduledSearch</s:item>
           <s:item>Alerting</s:item>
           <s:item>DeployClient</s:item>
           <s:item>DeployServer</s:item>
           <s:item>SplunkWeb</s:item>
           <s:item>SigningProcessor</s:item>
           <s:item>SyslogOutputProcessor</s:item>
           <s:item>AllowDuplicateKeys</s:item>
           <s:item>CanBeRemoteMaster</s:item>
         </s:list>
       </s:key>
       <s:key name="group_id">Enterprise</s:key>
       <s:key name="label">Splunk Internal License</s:key>
     </s:dict>
   </content>
 </entry>
licenser/localslave

https://<host>:<mPort>/services/licenser/localslave

Get license state information for the Splunk instance.

GET

Get license state information for the Splunk instance.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add_ons</td>
<td>List of add-ons resident on this instance, and add-on parameters.</td>
</tr>
<tr>
<td>connection_timeout</td>
<td>Instance connection timeout (seconds).</td>
</tr>
<tr>
<td>features</td>
<td>List of key-value pairs of the following features and their ENABLED/DISABLED status:</td>
</tr>
<tr>
<td></td>
<td>• Acceleration</td>
</tr>
<tr>
<td></td>
<td>• AdvancedSearchCommands</td>
</tr>
<tr>
<td></td>
<td>• AdvancedXML</td>
</tr>
<tr>
<td></td>
<td>• Alerting</td>
</tr>
<tr>
<td></td>
<td>• AllowDuplicateKeys</td>
</tr>
<tr>
<td></td>
<td>• Auth</td>
</tr>
<tr>
<td></td>
<td>• CanBeRemoteMaster</td>
</tr>
<tr>
<td></td>
<td>• CustomRoles</td>
</tr>
<tr>
<td></td>
<td>• DeployClient</td>
</tr>
<tr>
<td></td>
<td>• DeployServer</td>
</tr>
<tr>
<td></td>
<td>• DistSearch</td>
</tr>
<tr>
<td></td>
<td>• FwdData</td>
</tr>
<tr>
<td></td>
<td>• GuestPass</td>
</tr>
<tr>
<td></td>
<td>• KVStore</td>
</tr>
<tr>
<td></td>
<td>• LDAPAuth</td>
</tr>
<tr>
<td></td>
<td>• LocalSearch</td>
</tr>
<tr>
<td></td>
<td>• MultisiteClustering</td>
</tr>
<tr>
<td></td>
<td>• NontableLookups</td>
</tr>
<tr>
<td></td>
<td>• RcvData</td>
</tr>
</tbody>
</table>

872
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>last_master_contact_attempt_time</td>
<td>Time of last attempt to contact master.</td>
</tr>
<tr>
<td>last_master_contact_success_time</td>
<td>Time of last successful attempt to contact master.</td>
</tr>
<tr>
<td>last_trackerdb_service_time</td>
<td>Time of last license servicing, tracking persistent store.</td>
</tr>
<tr>
<td>license_keys</td>
<td>List of license keys this instance is using.</td>
</tr>
<tr>
<td>master_guid</td>
<td>Master license GUID.</td>
</tr>
<tr>
<td>master_uri</td>
<td>Master license URI.</td>
</tr>
<tr>
<td>receive_timeout</td>
<td>Network layer receive timeout for communication to master (seconds).</td>
</tr>
<tr>
<td>send_timeout</td>
<td>Network layer send timeout for communication to master (seconds).</td>
</tr>
<tr>
<td>slave_id</td>
<td>This instance GUID.</td>
</tr>
<tr>
<td>slave_label</td>
<td>This instance server name.</td>
</tr>
<tr>
<td>squash_threshold</td>
<td>Threshold that enables source/host squashing of rows of usage data sent to master periodically.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/licenser/localslave
```

**XML Response**

```xml
...
<title>localslave</title>
{id}https://localhost:8089/services/licenser/localslave</id>
<updated>2014-09-08T11:30:21-07:00</updated>
<generator build="221120" version="6.2"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messages/>
<entry>
<title>license</title>
{id}https://localhost:8089/services/licenser/localslave/license</id>
<updated>2014-09-08T11:30:21-07:00</updated>
<link href="/services/licenser/localslave/license" rel="alternate"/>
<author>
```
<s:dict>
  <s:key name="add_ons">
    <s:dict>
      <s:key name="hadoop">
        <s:dict>
          <s:key name="parameters">
            <s:dict>
              <s:key name="erp_type">report</s:key>
              <s:key name="maxNodes">10</s:key>
            </s:dict>
          </s:key>
          <s:key name="type">external_results_provider</s:key>
        </s:dict>
      </s:key>
    </s:dict>
    <s:key name="connection_timeout">30</s:key>
    <s:key name="eai:acl">... elided ...</s:key>
  </s:dict>
  <s:key name="features">
    <s:dict>
      <s:key name="Acceleration">ENABLED</s:key>
      <s:key name="AdvancedSearchCommands">ENABLED</s:key>
      <s:key name="AdvancedXML">ENABLED</s:key>
      <s:key name="Alerting">ENABLED</s:key>
      <s:key name="AllowDuplicateKeys">ENABLED</s:key>
      <s:key name="Auth">ENABLED</s:key>
      <s:key name="CanBeRemoteMaster">ENABLED</s:key>
      <s:key name="CustomRoles">ENABLED</s:key>
      <s:key name="DeployClient">ENABLED</s:key>
      <s:key name="DeployServer">ENABLED</s:key>
      <s:key name="DistSearch">ENABLED</s:key>
      <s:key name="FwdData">ENABLED</s:key>
      <s:key name="GuestPass">ENABLED</s:key>
      <s:key name="KVStore">ENABLED</s:key>
      <s:key name="LDAPAuth">ENABLED</s:key>
      <s:key name="LocalSearch">ENABLED</s:key>
      <s:key name="MultisiteClustering">ENABLED</s:key>
      <s:key name="NontableLookups">ENABLED</s:key>
      <s:key name="RcvData">ENABLED</s:key>
      <s:key name="RcvSearch">ENABLED</s:key>
      <s:key name="ResetWarnings">DISABLED_DUE_TO_LICENSE</s:key>
      <s:key name="RollingWindowAlerts">ENABLED</s:key>
      <s:key name="ScheduledAlerts">ENABLED</s:key>
      <s:key name="ScheduledReports">ENABLED</s:key>
      <s:key name="ScheduledSearch">ENABLED</s:key>
      <s:key name="SearchheadPooling">ENABLED</s:key>
      <s:key name="SigningProcessor">ENABLED</s:key>
      <s:key name="SplunkWeb">ENABLED</s:key>
      <s:key name="SyslogOutputProcessor">ENABLED</s:key>
      <s:key name="UnisiteClustering">ENABLED</s:key>
    </s:dict>
  </s:dict>
  <s:key name="last_master_contact_attempt_time">1410201013</s:key>
  <s:key name="last_master_contact_success_time">1410201013</s:key>
  <s:key name="last_trackerdb_service_time">0</s:key>
  <s:key name="license_keys">
    <s:list>
      <s:item>874</s:item>
    </s:list>
  </s:dict>
</s:dict>
licenser/messages

Access licenser messages.

Messages may range from helpful warnings about being close to violations, licenses expiring or more severe alerts regarding overages and exceeding license warning window.

GET

List all messages/alerts/persisted warnings for this node.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>category</td>
<td>Indicates the category for the licenser message. The category can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>license_window</td>
</tr>
<tr>
<td></td>
<td>pool_over_quota</td>
</tr>
<tr>
<td></td>
<td>stack_over_quota</td>
</tr>
<tr>
<td></td>
<td>orphan_slave</td>
</tr>
<tr>
<td></td>
<td>pool_warning_count</td>
</tr>
<tr>
<td></td>
<td>pool_violated_slave_count</td>
</tr>
<tr>
<td>create_time</td>
<td>The time the message was created in the system, expressed in Coordinated Universal time (UTC).</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>description</td>
<td>The actual licenser message that is displayed.</td>
</tr>
<tr>
<td>pool_id</td>
<td>The ID of the license pool to which the message applies. If a pool ID is not present, then the message in not applicable to a specific license pool.</td>
</tr>
</tbody>
</table>
| severity | Indicates the severity of the message. The severity can be any of the following:  
  INFO  
  WARN  
  ERROR |
| slave_id | The ID of the license slave to which the message applies.                   |
| stack_id | The ID of the license stack to which the message applies. If a stack ID is not present, then the message is not applicable to a specific license stack. |

Example request and response

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/services/licenser/messages
```

**XML Response**

```
...<title>licensermessages</title>
<id>https://localhost:8089/services/licenser/messages</id>
<updated>2011-08-02T03:50:46-07:00</updated>
<generator version="105103"/>
<author>
  <name>Splunk</name>
</author>
... opensearch nodes elided ...
<s:messions/>
<entry>
  <title>70a19a5cfe6d7c2a678089638dee7bea</title>
  <id>https://localhost:8089/services/licenser/messages/70a19a5cfe6d7c2a678089638dee7bea</id>
  <updated>2011-08-02T03:50:46-07:00</updated>
  <link href="/services/licenser/messages/70a19a5cfe6d7c2a678089638dee7bea" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/licenser/messages/70a19a5cfe6d7c2a678089638dee7bea" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:dict name="category">pool_warning_count</s:dict>
      <s:dict name="create_time">1312282230</s:dict>
      <s:dict name="description">This pool contains slave(s) with 3 warnings</s:dict>
      ... eai:acl node elided ...
      <s:dict name="pool_id"/>
      <s:dict name="severity">WARN</s:dict>
```
licenser/messages/{name}

https://<host>:<mPort>/services/licenser/messages/{name}

Get the message with message ID `{name}`.

GET

List specific message whose msgId corresponds to `{name}` component.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>create_time</td>
<td>The time the message was created in the system, expressed in Coordinated Universal time (UTC).</td>
</tr>
<tr>
<td>description</td>
<td>The actual licenser message that is displayed.</td>
</tr>
<tr>
<td>pool_id</td>
<td>The ID of the license pool to which the message applies.</td>
</tr>
<tr>
<td></td>
<td>If a pool ID is not present, then the message is not applicable to a specific license pool.</td>
</tr>
<tr>
<td>severity</td>
<td>Indicates the severity of the message. The severity can be any of the following:</td>
</tr>
<tr>
<td></td>
<td>INFO</td>
</tr>
<tr>
<td></td>
<td>WARN</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>slave_id</td>
<td>The ID of the license slave to which the message applies.</td>
</tr>
<tr>
<td>stack_id</td>
<td>The ID of the license stack to which the message applies.</td>
</tr>
<tr>
<td></td>
<td>If a stack ID is not present, then the message is not applicable to a specific license stack.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://127.0.0.1:3339/services/licenser/messages/2702b33a1bd369ae9209a9ecf4cb39db

**XML Response**

...
licenser/pools

https://<host>:<mPort>/services/licenser/pools

Access the licenser pools configuration.

A pool logically partitions the daily volume entitlements of a stack. You can use a license pool to divide license privileges amongst multiple slaves.

GET

Enumerate all pools.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of the license pool.</td>
</tr>
<tr>
<td>quota</td>
<td>The byte quota of this license pool.</td>
</tr>
<tr>
<td></td>
<td>MAX: maximum amount allowed by the license. You can only have one pool with</td>
</tr>
<tr>
<td></td>
<td>MAX size in a stack.</td>
</tr>
<tr>
<td></td>
<td>Number: the number of bytes allowed by this license.</td>
</tr>
<tr>
<td>slaves</td>
<td>slaveids that are members of this pool.</td>
</tr>
<tr>
<td></td>
<td>Returned as a list in Atom format. See example below.</td>
</tr>
<tr>
<td>slaves_usage_bytes</td>
<td>Usage, in bytes, of slaves to this license.</td>
</tr>
<tr>
<td>stack_id</td>
<td>Stack ID of the stack corresponding to this pool.</td>
</tr>
<tr>
<td>used_bytes</td>
<td>Usage, in bytes, for this license pool.</td>
</tr>
</tbody>
</table>

Example request and response
XML Request

curl -k -u admin:pass https://localhost:8089/services/licenser/pools

XML Response

<title>pools</title>
{id>https://localhost:8089/services/licenser/pools</id>
<updated>2011-07-08T10:55:18-07:00</updated>
<generator version="102824"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/licenser/pools/_new" rel="create"/>
<link href="/services/licenser/pools/_reload" rel="_reload"/>
<opensearch:totalResults>4</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
... elided ...
<entry>
  <title>auto_generated_pool_enterprise</title>
  <id>https://localhost:8089/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise</id>
  <updated>2011-07-08T10:55:18-07:00</updated>
  <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise" rel="list"/>
  <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_enterprise" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="description">auto_generated_pool_enterprise</s:key>
      <s:key name="eai:acl"> ... elided ...</s:key>
      <s:key name="quota">MAX</s:key>
      <s:key name="slaves"><s:list><s:item>*</s:item></s:list></s:key>
      <s:key name="slaves_usage_bytes">
        <s:dict><s:key name="1F3A34AE-75DA-4680-B184-5BF309843919">26445659</s:key></s:dict>
      </s:key>
      <s:key name="stack_id">enterprise</s:key>
      <s:key name="used_bytes">26445659</s:key>
    </s:dict>
  </content>
</entry>
<entry>
  <title>auto_generated_pool_forwarder</title>
  <id>https://localhost:8089/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder</id>
  <updated>2011-07-08T10:55:18-07:00</updated>
  <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="list"/>
  <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="description">auto_generated_pool_forwarder</s:key>
    </s:dict>
  </content>
</entry>
POST

Create a license pool.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>name</strong></td>
<td>String</td>
<td>Required</td>
<td>The name of the license pool you are creating.</td>
</tr>
</tbody>
</table>
| **quota** | String |           | **Required.** Defines the byte quota of this pool.  
Valid values:  
MAX: maximum amount allowed by the license. You can only have one pool with MAX size in a stack.  
Number[MB|GB]: Specify a specific size. For example, 552428800, or simply specify 50MB. |
| **slaves** | String |           | Comma-separated list of slaveids that are members of this pool, or "*" to accept all slaves.  
You can also specify a comma-separated list of guids to specify slaves that can connect to this pool. |
| **stack_id** | Enum | Required | Valid values: (download-trial | Enterprise | Forwarder | Free | Lite | Lite_Free)  
Stack ID of the stack corresponding to this pool |

Returned values

None

Example request and response

881
**XML Request**

curl -k -u admin:pass https://localhost:8089/services/licenser/pools -d name=myLicensePool -d quota=MAX -d slaves=* -d stack_id=enterprise

**XML Response**

...<title>pools</title>
{id>https://localhost:8089/services/licenser/pools</id>
<updated>2011-07-08T11:31:47-07:00</updated>
<generator version="102824"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/licenser/pools/_new" rel="create"/>
<link href="/services/licenser/pools/_reload" rel="_reload"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

**licenser/pools/{name}**

https://<host>:<mPort>/services/licenser/pools/{name}

Manage the {name} license pool.

**DELETE**

Delete the specified pool.

**Usage details**
Deleting pools is not supported for every pool. Certain stacks have fixed pools which cannot be deleted.

**Request parameters**
None

**Returned values**
None

**Example request and response**
XML Request

curl -k -u admin:pass --request DELETE
https://localhost:8089/services/licenser/pools/auto_generated_pool_enterprise

XML Response

...<title>pools</title>
{id>https://localhost:8089/services/licenser/pools</id>
<updated>2011-07-08T11:29:26-07:00</updated>
<generator version="102824"/>
<author>
   <name>Splunk</name>
</author>
</s:messages/>

GET

Lists details of the pool specified by (name).

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of the license pool.</td>
</tr>
<tr>
<td>quota</td>
<td>The byte quota of this license pool.</td>
</tr>
<tr>
<td></td>
<td>MAX: maximum amount allowed by the license. You can only have one pool with</td>
</tr>
<tr>
<td></td>
<td>MAX size in a stack.</td>
</tr>
<tr>
<td></td>
<td>Number: the number of bytes allowed by this license.</td>
</tr>
<tr>
<td>slaves</td>
<td>slaveids that are members of this pool.</td>
</tr>
<tr>
<td></td>
<td>Returned as a list in Atom format. See example below.</td>
</tr>
<tr>
<td>slaves_usage_bytes</td>
<td>Usage, in bytes, of slaves to this license.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
*stack_id* | Stack ID of the stack corresponding to this pool.
*used_bytes* | Usage, in bytes, for this license pool.

**Example request and response**

**XML Request**

```shell
curl -k -u admin:pass https://localhost:8089/services/licenser/pools/auto_generated_pool_forwarder
```

**XML Response**

```xml
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

<entry>
<title>auto_generated_pool_forwarder</title>
<id>https://localhost:8089/servicesNS/nobody/system/licenser/pools/auto_generated_pool_forwarder</id>
<updated>2011-07-08T11:03:37-07:00</updated>
<author>
  <name>nobody</name>
</author>
<opensearch:permissions>
  <eai:acl> ... elided ...</eai:acl>
</opensearch:permissions>
<content type="text/xml">
<s:dict>
  <s:key name="description">auto_generated_pool_forwarder</s:key>
  <s:dict name="eai:attributes">
    <s:list>
      <s:dict name="optionalFields">
        <s:list>
          <s:dict name="appendslaves">
            <s:list>
              <s:dict name="description">
                <s:dict name="quota">
                  <s:dict name="slaves">
                    <s:list/>
                  </s:dict>
                </s:dict>
              </s:dict>
            </s:list>
          </s:dict>
        </s:list>
      </s:dict>
    </s:list>
  </s:dict>
</s:dict>
```
POST

Edit properties of the pool specified by {name}.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>append_slaves</td>
<td>Boolean</td>
<td></td>
<td>Flag which controls whether newly specified slaves is appended to existing slaves list or overwritten</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td></td>
<td>Description of this pool</td>
</tr>
<tr>
<td>quota</td>
<td>String</td>
<td></td>
<td>Defines the byte quota of this pool.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>MAX: maximum amount allowed by the license. You can only have one pool with MAX size in a stack.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Number[MB</td>
</tr>
<tr>
<td>slaves</td>
<td>String</td>
<td></td>
<td>Comma-separated list of slaveids that are members of this pool, or '*' to accept all slaves.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>You can also specify a comma-separated list of guids to specify slaves that can connect to this pool.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/licenser/pools/myLicensePool -d quota=50MB

885
**XML Response**

```xml
... elided ...
<entry>
  <title>myLicensePool</title>
  <id>https://localhost:8085/servicesNS/nobody/system/licenser/pools/myLicensePool</id>
  <updated>2011-07-24T08:46:49-07:00</updated>
  <link href="/servicesNS/nobody/system/licenser/pools/myLicensePool" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/licenser/pools/myLicensePool" rel="list"/>
  <link href="/servicesNS/nobody/system/licenser/pools/myLicensePool/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/licenser/pools/myLicensePool" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="description"></s:key>
      ... eai:acl node elided ...
      <s:key name="eai:attributes">
        <s:dict>
          <s:key name="optionalFields">
            <s:list>
              <s:item>append_slaves</s:item>
              <s:item>description</s:item>
              <s:item>quota</s:item>
              <s:item>slaves</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list/>
          </s:key>
          <s:key name="wildcardFields">
            <s:list/>
          </s:key>
        </s:dict>
        <s:key name="quota">552428800</s:key>
        <s:key name="slaves"><s:list><s:item>*</s:item></s:list></s:key>
        <s:key name="slaves_usage_bytes">
          <s:dict>
            <s:key name="1F3A34AE-75DA-4680-B184-5BF309843919">39846322</s:key>
          </s:dict>
        </s:key>
        <s:key name="stack_id">enterprise</s:key>
        <s:key name="used_bytes">39846322</s:key>
      </s:dict>
    </s:dict>
  </content>
</entry>
```

---

**licenser/slaves**

https://<host>:<mPort>/services/licenser/slaves

Access license slave instances.
GET

List all slaves registered to this license master.

**Request parameters**

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label</td>
<td>Plain text name for the license slave.</td>
</tr>
<tr>
<td>pool_ids</td>
<td>License pools for which this license slave is a member.</td>
</tr>
<tr>
<td>stack_ids</td>
<td>License stacks for which this license slave is a member.</td>
</tr>
<tr>
<td>warning_count</td>
<td>Number of license warnings issued for this license slave.</td>
</tr>
</tbody>
</table>

**Usage details**

Any license slave master connection attempt is reported regardless of whether it is allocated to a master licenser pool.

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/licenser/slaves

**XML Response**

```xml
<title>slaves</title>
<id>https://localhost:8089/services/licenser/slaves</id>
<updated>2011-05-17T09:37:54-07:00</updated>
<generator version="99849"/>
<author>
 <name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
 <title>74A43C7E-C33C-41F6-B027-E603D2C3FE68</title>
 <id>https://localhost:8089/servicesNS/nobody/system/licenser/slaves/74A43C7E-C33C-41F6-B027-E603D2C3FE68</id>
 <updated>2011-05-17T09:37:54-07:00</updated>
 <link href="/servicesNS/nobody/system/licenser/slaves/74A43C7E-C33C-41F6-B027-E603D2C3FE68" rel="alternate"/>
 <author>
  <name>nobody</name>
 </author>
 <link href="/servicesNS/nobody/system/licenser/slaves/74A43C7E-C33C-41F6-B027-E603D2C3FE68" rel="list"/>
 <content type="text/xml">
  <s:dict>
```
licenser/slaves/{name}

https://<host>:<mPort>/services/licenser/slaves/{name}

Get {name} licenser slave license information.

GET

List attributes of the slave instance specified by {name}.

Request parameters

888
Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label</td>
<td>Plain text name for the license slave.</td>
</tr>
<tr>
<td>pool_ids</td>
<td>License pools for which this license slave is a member.</td>
</tr>
<tr>
<td>stack_ids</td>
<td>License stacks for which this license slave is a member.</td>
</tr>
<tr>
<td>warning_count</td>
<td>Number of license warnings issued for this license slave.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/licenser/slaves/74A43C7E-C33C-41F6-B027-E603D2C3FE68

XML Response

...
licenser/stacks

https://<host>:<mPort>/services/licenser/stacks

Provides access to the license stack configuration.

A license stack is comprised of one or more licenses of the same "type". The daily indexing quota of a license stack is additive, so a stack represents the aggregate entitlement for a collection of licenses.
GET

Enumerate all license stacks.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label</td>
<td>The name of this license stack.</td>
</tr>
<tr>
<td>quota</td>
<td>The byte quota of this license stack. This value is the sum of the byte quota for all the licenses in the license stack.</td>
</tr>
<tr>
<td>type</td>
<td>Any additional information about the type of this license stack.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/licenser/stacks

XML Response

<title>stacks</title>
{id>https://localhost:8089/services/licenser/stacks/id>
<updated>2011-07-08T10:37:33-07:00</updated>
<generator version="102824"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>4</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>download-trial</title>
<id>https://localhost:8089/services/licenser/stacks/download-trial</id>
<updated>2011-07-08T10:37:33-07:00</updated>
<link href="/services/licenser/stacks/download-trial" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/licenser/stacks/download-trial" rel="list"/>
<content type="text/xml">
  <s:dict>
    <s:dict name="eai:acl">... elided ...
    <s:key name="label">Splunk Enterprise Download Trial</s:key>
    <s:key name="quota">524288000</s:key>
    <s:key name="type">download-trial</s:key>
  </s:dict>
</content>
</entry>

<entry>
<entry>
license/stacks/{name}

https://<host>:{mPort}/services/licenser/stacks/{name}
Get \{name\} license stack information.

**GET**

Retrieve details of a specific license stack.

**Usage details**

A license stack is comprised of one or more licenses of the same "type". The daily indexing quota of a license stack is additive, so a stack represents the aggregate entitlement for a collection of licenses.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>label</td>
<td>The name of this license stack.</td>
</tr>
<tr>
<td>quota</td>
<td>The byte quota of this license stack. This value is the sum of the byte quota for all the licenses in the license stack.</td>
</tr>
<tr>
<td>type</td>
<td>Any additional information about the type of this license stack.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/enterprise
```

**XML Response**

```
<entry>
<title>enterprise</title>
<id>https://localhost:8089/services/licenser/stacks/enterprise</id>
<updated>2011-07-08T10:44:07:00Z</updated>
<author>
  <name>system</name>
</author>
<content type="text/xml">893</content>
</entry>
```
licenser/usage

https://<host>:<mPort>/services/licenser/usage

Get current license usage stats from the last minute.

GET

Enumerate license usage information from the last minute.

Request parameters
Pagination and filtering parameters can be used with this method.

 Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>quota</td>
<td>The byte quota of this license stack. This value is the sum of the byte quota for all the licenses in the active license group.</td>
</tr>
<tr>
<td>slaves_usage_bytes</td>
<td>Slave usage bytes across all pools that are within the active license group.</td>
</tr>
</tbody>
</table>

Example request and response
**XML Request**

curl -k -u admin:pass https://localhost:8089/services/licenser/usage

**XML Response**

```xml
<title>licenseusage</title>
<id>https://localhost:8089/services/licenser/usage</id>
<updated>2015-06-03T11:46:10-07:00</updated>
<generator build="6cfc0237739f" version="6.3.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/licenser/usage/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>license_usage</title>
  <id>https://localhost:8089/services/licenser/usage/license_usage</id>
  <updated>2015-06-03T11:46:10-07:00</updated>
  <link href="/services/licenser/usage/license_usage" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/licenser/usage/license_usage" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
              <s:key name="write"></s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="quota">21474836480</s:key>
      <s:key name="slaves_usage_bytes">0</s:key>
    </s:dict>
  </content>
</entry>
```

895
</feed>
Metrics Catalog endpoints

Metrics Catalog endpoint descriptions

Use the Metrics Catalog REST API to enumerate metrics and the dimensions and dimension values associated with metrics.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

Authentication and Authorization

Username and password authentication are required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints, and must have the list_metrics_catalog capability to use the Metrics Catalog endpoint. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select Settings > Access controls > Users. To determine the capabilities assigned to a role, select Settings > Access controls > Roles.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

Default indexes for Metrics Catalog endpoints

If no metric indexes are defined with the filter parameter, Metrics Catalog endpoints use the default indexes specified for the role of the user. To review or update the default indexes for specific roles, select Settings > Access controls > Roles, select a role, and review or update the Indexes searched by default field.

If the set of default indexes for a role includes a mix of metrics indexes and event indexes, the Metrics Catalog endpoints only use the metrics indexes.

If there are no metrics indexes, the Metrics Catalog endpoints display an empty list.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

Managed Splunk Cloud deployments

https://<deployment-name>.splunkcloud.com:8089

Self-service Splunk Cloud deployments
To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the Splunk REST API Tutorials for more information.

catalog/metricstore/metrics

https://<host>:<mPort>/services/catalog/metricstore/metrics

Use this endpoint to list metric names.

GET

Returns metric names.

Request parameters

Pagination and filtering parameters can be used with this method.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest</td>
<td>String</td>
<td>Optional. A time string that specifies the earliest time for this search. Can be a relative or absolute time. The default value is -1d.</td>
</tr>
<tr>
<td>filter</td>
<td>String</td>
<td>Optional. A URL-encoded set of one or more key-value pairs, where keys correspond to metric fields such as index or dimension. For example, to specify a dimension named app, use filter=app. To specify two index names and values such as index-index1 and index-index2, use index%3dindex1%26index%3dindex2.</td>
</tr>
<tr>
<td>latest</td>
<td>String</td>
<td>Optional. A time string that specifies the latest time for this search. Can be a relative or absolute time. The default value is now.</td>
</tr>
<tr>
<td>list_indexes</td>
<td>Boolean</td>
<td>Optional. When set to true, the endpoint returns the index or indexes associated with each metric. The default value is false.</td>
</tr>
</tbody>
</table>

Returned values

There are no returned values other than the metric names.

Example request and response

XML Request

List all metric names:

curl -k -u admin:passwd https://localhost:8089/services/catalog/metricstore/metrics

XML Response

...

<title>metricstore-metrics</title>
<id>https://epic-metriks-splk.sv.splunk.com:8089/services/catalog/metricstore/metrics</id>
<updated>2017-12-19T19:49:00+00:00</updated>
<generator build="31fcdba9ddc1" version="7.0.0"/>
<author>
    <name>Splunk</name>
</author>
<link href="/services/catalog/metricstore/metrics/_acl" rel="_acl"/>
<opensearch:totalResults>16</opensearch:totalResults>
Example requests

- **List all metric names that include the dimension field** `dc`:

  ```bash
  ```

- **List all metric names that include either** `dc-east` **or** `dc-west** dimension fields**:

  ```bash
curl -k -u admin:passwd https://localhost:8089/services/catalog/metricstore/metrics?filter=dc%3deast&filter=dc%3dwest
  ```
• List all metric names that are in `index1` or `index2` by their index:

curl -k -u admin:passwd
https://localhost:8089/services/catalog/metricstore/metrics?filter-index=index1%26index=index2&list_indexes=t

catalog/metricstore/dimensions

https://<host>:<mPort>/services/catalog/metricstore/dimensions

Use this endpoint to list dimension names.

GET

Returns dimension names for a given metric.

Request parameters

Pagination and filtering parameters can be used with this method.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest</td>
<td>String</td>
<td>Optional. A time string that specifies the earliest time for this search. Can be a relative or absolute time. The default value is -1d.</td>
</tr>
<tr>
<td>filter</td>
<td>String</td>
<td>Optional. A URL-encoded set of one or more key-value pairs, where keys correspond to metric fields such as index or dimension. For example, to specify a dimension named <code>os</code>, use <code>filter=os</code>. To specify two index names and values such as <code>index=index1</code> and <code>index=index2</code>, use <code>index%3dindex1%26index%3dindex2</code>.</td>
</tr>
<tr>
<td>latest</td>
<td>String</td>
<td>Optional. A time string that specifies the latest time for this search. Can be a relative or absolute time. The default value is now.</td>
</tr>
<tr>
<td>metric_name</td>
<td>String</td>
<td>Required. The name of a metric.</td>
</tr>
</tbody>
</table>

Returned values

There are no returned values other than the dimension names.

Example request and response

XML Request

curl -k -u admin:passwd https://localhost:8089/services/catalog/metricstore/dimensions?metric_name=*  

XML Response

```xml
...  
<title>metricstore-dimensions</title>  
<id>https://epic-metriks-spik.sv.splunk.com:8089/services/catalog/metricstore/dimensions</id>  
<updated>2017-12-19T00:27:00+00:00</updated>  
<generator build="31fcd8a9ddc1" version="7.0.0"/>  
<author>  
  <name>Splunk</name>  
</author>  
<link href="/services/catalog/metricstore/dimensions/_acl" rel="_acl"/>  
<opensearch:totalResults>7</opensearch:totalResults>  
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>  
<opensearch:startIndex>0</opensearch:startIndex>  
```
Another example request:

List all the dimension fields for the `os.mem.free` metric when the `dc` dimension field is limited to a value of `east`:

```
curl -k -u admin:passwd https://localhost:8089/services/catalog/metricstore/dimensions?metric_name=os.mem.free&filter=dc%3deast
catalog/metricstore/dimensions/{dimension-name}/values
```

Use this endpoint to list values for a given `{dimension-name}`.
GET

Returns values of a (dimension-name) for a given metric.

Request parameters
Pagination and filtering parameters can be used with this method.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest</td>
<td>String</td>
<td>Optional. A time string that specifies the earliest time for this search. Can be a relative or absolute time. The default value is -1d.</td>
</tr>
<tr>
<td>filter</td>
<td>String</td>
<td>Optional. A URL-encoded set of one or more key-value pairs, where keys correspond to metric fields such as index or dimension. For example, to specify a dimension named os, use filter=os. To specify two index names and values such as index=index1 and index-index2, use index%3dindex1%26index%3dindex2.</td>
</tr>
<tr>
<td>latest</td>
<td>String</td>
<td>Optional. A time string that specifies the latest time for this search. Can be a relative or absolute time. The default value is now.</td>
</tr>
<tr>
<td>metric_name</td>
<td>String</td>
<td>Required. The name of a metric.</td>
</tr>
</tbody>
</table>

Returned values
There are no returned values other than those of the selected (dimension-name).

Example request and response

XML Request
List all values for the app dimension of the os.mem.free metric:

curl -k -u statsd:statsd
https://localhost:8089/services/catalog/metricstore/dimensions/app/values?metric_name=os.mem.free

XML Response

```xml
...<title>metricstore-dimensions</title>
    <id>https://epic-metriks-splk.sv.splunk.com:8089/services/catalog/metricstore/dimensions</id>
    <updated>2017-12-19T02:05:19+00:00</updated>
    <generator build="31fcdba9ddc1" version="7.0.0"/>
    <author>
        <name>Splunk</name>
```
More example requests

- List all values for the `dc` dimension of the `os.mem.free` metric, where `dc` is limited to a value of `east`:

  ```bash
  ```

- List all values for the `dc` dimension of the `mem.free` metric, where the recorded measurements also have an `os` dimension field:

  ```bash
  curl -k -u admin:changeme  https://localhost:8089/services/catalog/metricstore/rollup
  ```

### catalog/metricstore/rollup

https://<host>:<mPort>/services/catalog/metricstore/rollup

Use this endpoint to retrieve lists of metric indexes and their rollup summaries and to create new rollup policies for a given metric index.

**Authentication and authorization**

Use of the GET operation for this endpoint is restricted to roles that have the `list_metrics_catalog` capability. Use of the POST operation for this endpoint is restricted to roles that have the `edit_metrics_rollup` capability.
GET

Returns rollup summaries and the metric indexes with which they are associated.

Request parameters
None specific to this method. This method can use pagination and filtering parameters.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The source index name. Rollup summaries are made up of aggregated metric data points that are derived from the metric data points in a source index.</td>
</tr>
<tr>
<td>summaries</td>
<td>A comma-separated list of the rollup summaries associated with the source metric index. Each summary configuration consists of a span and a rollup_index. The span is the interval by which the search head generates the aggregated rollup metric data points that make up the summary. The rollup_index is the target index for the rollup summary. The endpoint uses the following format when it lists summaries:</td>
</tr>
<tr>
<td>&lt;span_i&gt;</td>
<td>&lt;rollup_index_i&gt;,&lt;span_2&gt;</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/catalog/metricstore/rollup
```

XML response

```
...
<entry>
  <title>index_s</title>
  <id>https://127.0.0.1:8101/servicesNS/nobody/search/catalog/metricstore/rollup/index_s</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="list"/>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="edit"/>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="remove"/>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="aggregation.foo1">min#avg</s:key>
      <s:key name="aggregation.foo2">count#avg</s:key>
      <s:key name="defaultAggregation">avg#max</s:key>
      <s:key name="dimensionList">app,region</s:key>
      <s:key name="dimensionListType">included</s:key>
      <s:key name="disabled">0</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```
POST

Creates rollup policies for a specified metric index.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td><strong>Required.</strong> Specify the name of the source metric index. This is the index from which the aggregated metric data points in the rollup summaries will be derived.</td>
</tr>
<tr>
<td>summaries</td>
<td>String</td>
<td><strong>Required.</strong> Specify one or more rollup summaries, separated by commas. A rollup summary is a combination of a rollup metric index and a rollup period. The rollup period is the span. This time range string is the interval on which the search head generates the aggregated rollup metric data points that make up the summary. The rollup index is the target index for the rollup summary. The endpoint uses the following format when it lists summaries: (&lt;span_1&gt;</td>
</tr>
<tr>
<td>default_agg</td>
<td>String</td>
<td><strong>Optional.</strong> A list of aggregation functions, separated by # characters. Provides the set of aggregation functions that the rollup search uses when it aggregates the metric data points in the source metric index for a rollup summary. The defaultAggregation can be overruled for specific metrics by the aggregation.&lt;metric_name&gt; setting. This setting supports the following functions: avg, count, max, median, min, perc&lt;int&gt;, and sum. Defaults to avg.</td>
</tr>
<tr>
<td>metric_list</td>
<td>String</td>
<td><strong>Optional.</strong> A comma-separated list of metric names. All of the listed metrics must appear in the source metric index identified by the name parameter. This list works in conjunction with the metric_list_type parameter to create a filter at the search head that allows certain metrics to be rolled up but not others. Defaults to empty string.</td>
</tr>
<tr>
<td>metric_list_type</td>
<td>[included</td>
<td><strong>Optional.</strong> Works in conjunction with the metric_list parameter to create a filter at the search head that allows certain metrics to be rolled up to the rollup summaries but not others. Defaults to excluded.</td>
</tr>
</tbody>
</table>
Use **included** to indicate that the search head should filter out all available metrics from the set of metrics being rolled up to the rollup summaries, except for the metrics listed in **metric_list** parameter.

Use **excluded** to indicate that the search head should roll up all available metrics to the rollup summaries except the metrics listed in **metric_list** parameter.

---

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>dimension_list</strong></td>
<td>String</td>
<td>Optional. A comma-separated list of dimensions that appear in the source metric index identified by the <strong>name</strong> parameter. This list corresponds to the <strong>dimension_list_type</strong> parameter, which determines whether this set of dimensions is included or excluded from the aggregated rollup metrics that the search head generates for the rollup summary. Defaults to empty string.</td>
</tr>
<tr>
<td><strong>dimension_list_type</strong></td>
<td>[included</td>
<td>excluded]</td>
</tr>
<tr>
<td><strong>metric_overrides</strong></td>
<td>String</td>
<td>Optional. Provides a comma-separated list of exclusion rules for a set of rollup policies. Use this setting to override the default aggregation for one or more metrics. Each metric override pairs a metric name with one or more aggregation functions separated by # characters. Each metric override uses the following syntax: `&lt;metric_name&gt;</td>
</tr>
</tbody>
</table>

---

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregation.&lt;metric_name&gt;</td>
<td>Overrides the default aggregation or set of aggregations for the specified <strong>metric_name</strong> and gives it a different aggregation or set of aggregations instead. Defined by the <strong>metric_overrides</strong> argument.</td>
</tr>
<tr>
<td>defaultAggregation</td>
<td>The default aggregation methods for the rollup policy, separated by # characters.</td>
</tr>
<tr>
<td>dimensionList</td>
<td>Comma-separated list of dimensions to be included or excluded from the aggregations, depending on the value of <strong>dimensionListType</strong>.</td>
</tr>
<tr>
<td>dimensionListType</td>
<td>Indicates whether the <strong>dimensionList</strong> should be <strong>included</strong> or <strong>excluded</strong> from the rollup policy.</td>
</tr>
<tr>
<td>metricList</td>
<td>Comma-separated list of metrics to be included or excluded from the set of metrics rolled up to the summaries, depending on the value of <strong>dimensionListType</strong>.</td>
</tr>
<tr>
<td>metricListType</td>
<td>Indicates whether the <strong>metricList</strong> should be <strong>included</strong> or <strong>excluded</strong> from the rollup policy.</td>
</tr>
<tr>
<td>rollup.&lt;summary number&gt;.rollupIndex</td>
<td>The target rollup index for a specific summary. Summaries are identified by the <strong>&lt;summary number&gt;</strong>.</td>
</tr>
<tr>
<td>rollup.&lt;summary number&gt;.span</td>
<td>The rollup span for a specific summary. Summaries are identified by the <strong>&lt;summary number&gt;</strong>.</td>
</tr>
</tbody>
</table>

---

**Example request and response**

Place this stanza in **metric_rollups.conf**:

```ini
[index:index_s]
aggregation.foo1 = min#avg
aggregation.foo2 = count#avg
defaultAggregation = avg#max
dimensionList = app,region
dimensionListType = included
metricList = foo3,foo4
metricListType = excluded
```

906
curl -k -u admin:changeme https://localhost:8089/services/catalog/metricstore/rollup -d name=index_s -d default_agg=avg#max -d dimension_list="app,region" -d dimension_list_type=included -d metric_overrides="foo2|count#avg,foo1|min#avg" -d summaries="1h|index_d_1h,1d|index_d_1d" -d metric_list="foo3,foo4" -d metric_list_type=excluded

**XML response**

```xml
<entry>
  <title>index_s</title>
  <id>https://127.0.0.1:8101/servicesNS/nobody/search/catalog/metricstore/rollup/index_s</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="list"/>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="edit"/>
  <link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="aggregation.foo1">min#avg</s:key>
      <s:key name="aggregation.foo2">count#avg</s:key>
      <s:key name="defaultAggregation">avg#max</s:key>
      <s:key name="dimensionList">app,region</s:key>
      <s:key name="dimensionListType">included</s:key>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app">search</s:key>
          <s:key name="can_change_perms">1</s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_share_app">1</s:key>
          <s:key name="can_share_global">1</s:key>
          <s:key name="can_share_user">0</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">1</s:key>
          <s:key name="owner">nobody</s:key>
          <s:key name="perms"/>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="metricList">foo3,foo4</s:key>
      <s:key name="metricListType">excluded</s:key>
      <s:key name="minSpanAllowed">300</s:key>
      <s:key name="summaries">
        <s:dict>
          <s:key name="0">
            <s:dict>
              <s:key name="rollupIndex">index_d_1h</s:key>
              <s:key name="span">1h</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
```

907
catalog/metricstore/rollup/{index}

https://<host>:<mPort>/services/catalog/metricstore/rollup/{index}

Use this endpoint to:
- Retrieve a list of the rollup summaries associated with a specific source `{index}`.
- Update a rollup policy for a specific source `{index}`.
- Delete a rollup policy for a specific source `{index}`.

Authentication and Authorization
Use of the GET operation for this endpoint is restricted to roles that have the list_metrics_catalog capability. Usage of the POST and DELETE operations for this endpoint are restricted to roles that have the edit_metrics_rollup capability.

GET

Returns a list of the rollup summaries associated with a specific source `{index}`.

Request parameters
None specific to this method. This method can use pagination and filtering parameters.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summaries</td>
<td>A comma-separated list of the rollup summaries associated with the source metric <code>{index}</code>. Each summary configuration consists of a <code>span</code> and a <code>rollup_index</code>. The <code>span</code> is the interval by which the search head generates the aggregated rollup metric data points that make up the summary. The <code>rollup_index</code> is the target index for the rollup summary. The endpoint uses the following format when it lists summaries: `:&lt;span_1&gt;</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/catalog/metricstore/rollup/index_s
```

XML response

```
...
```

908
<entry>
<title>index_s</title>
<id>https://localhost:8089/servicesNS/nobody/search/catalog/metricstore/rollup/index_s</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="alternate"/>
<author>
<name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="list"/>
<link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="edit"/>
<link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s" rel="remove"/>
<link href="/servicesNS/nobody/search/catalog/metricstore/rollup/index_s/disable" rel="disable"/>
<content type="text/xml">
<s:dict>
<s:key name="aggregation.foo1"> min#avg </s:key>
<s:key name="aggregation.foo2"> count#avg </s:key>
<s:key name="defaultAggregation"> avg#max </s:key>
<s:key name="dimensionList">app,region</s:key>
<s:key name="dimensionListType">included</s:key>
<s:key name="disabled">0</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app">search</s:key>
<s:key name="can_change_perms">1</s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_share_app">1</s:key>
<s:key name="can_share_global">1</s:key>
<s:key name="can_share_user">0</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">1</s:key>
<s:key name="owner">nobody</s:key>
<s:key name="perms"/>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
<s:key name="eai:attributes">
<s:dict>
<s:key name="optionalFields">
<s:list>
<s:item>default_agg</s:item>
<s:item>dimension_list</s:item>
<s:item>dimension_list_type</s:item>
<s:item>isProxyRequest</s:item>
<s:item>metric_overrides</s:item>
<s:item>noProxy</s:item>
<s:item>summaries</s:item>
</s:list>
</s:key>
<s:key name="requiredFields">
<s:list/>
</s:key>
<s:key name="wildcardFields">
<s:list/>
</s:key>
</s:dict>
</s:key>
<s:key name="metricList">foo3,foo4</s:key>
<s:key name="metricListType">excluded</s:key>
<s:key name="minSpanAllowed">300</s:key>
<s:key name="summaries">
</s:key>
</s:dict>
</entry>
POST

Updates a rollup policy for a specific source `{index}`.

Request parameters

At least one argument is required.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default_agg</td>
<td>String</td>
<td>Optional. A list of aggregation functions, separated by # characters. Provides the set of aggregation functions that the rollup search uses when it aggregates the metric data points in the source metric index for a rollup summary. The defaultAggregation can be overruled for specific metrics by the aggregation.&lt;metric_name&gt; setting. This setting supports the following functions: avg, count, max, median, min, perc&lt;int&gt;, and sum. Defaults to avg.</td>
</tr>
<tr>
<td>metric_list</td>
<td>String</td>
<td>Optional. A comma-separated list of metric names. All of the listed metrics must appear in the source metric index identified by the name parameter. This list works in conjunction with the metric_list_type parameter to create a filter at the search head that allows certain metrics to be rolled up but not others. Defaults to empty string.</td>
</tr>
<tr>
<td>metric_list_type</td>
<td>[included</td>
<td>Optional. Works in conjunction with the metric_list parameter to create a filter at the search head that allows certain metrics to be rolled up to the rollup summaries but not others. Defaults to excluded.</td>
</tr>
<tr>
<td></td>
<td>excluded]</td>
<td>• Use included to indicate that the search head should filter out all available metrics from the set of metrics being rolled up to the rollup summaries, except for the metrics listed in metric_list parameter. • Use excluded to indicate that the search head should roll up all available metrics to the rollup summaries except the metrics listed in metric_list parameter.</td>
</tr>
<tr>
<td>dimension_list</td>
<td>string</td>
<td>Optional. A comma-separated list of dimensions that appear in the source index. This list corresponds to the dimension_list_type parameter, which determines whether this set of dimensions is included or excluded from the aggregated rollup metrics that the search head generates for the rollup summary. Defaults to empty string.</td>
</tr>
<tr>
<td>dimension_list_type</td>
<td>[included</td>
<td>Optional. Identifies whether the dimensions specified in the dimension_list parameter are included or excluded from the rollup metrics that are generated by the rollup policies for the rollup summaries.</td>
</tr>
<tr>
<td></td>
<td>excluded]</td>
<td>• Use included to indicate that the rollup metrics produced by the rollup policy filter out all dimensions except the dimensions listed in the dimension_list parameter. • Use excluded to indicate that the rollup metrics produced by the rollup policy include all available dimensions except the dimensions in the dimension_list parameter.</td>
</tr>
<tr>
<td>metric_overrides</td>
<td>String</td>
<td>Optional. Provides a comma-separated list of exclusion rules for a set of rollup policies. Use this setting to override the default aggregation for one or more metrics. Each metric override pairs a metric name with one or more aggregation functions separated by # characters. Each metric override uses the following syntax:</td>
</tr>
</tbody>
</table>

910
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| summaries        | string| Optional. Specify one or more rollup summaries, separated by commas. A rollup summary is a combination of a rollup metric index and a rollup period. The rollup period is the span. It is the interval on which the search head generates the aggregated rollup metric data points that make up the summary. The rollup index is the target index for the rollup summary. The endpoint uses the following format when it lists summaries: 

  <$span_1>|<rollup_index_1>,<$span_2>|<rollup_index_2>...<$span_n>|<rollup_index_n>  |

  Returned values  |

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aggregation.&lt;metric_name&gt;</td>
<td>Overrides the default aggregation or set of aggregations for the specified metric_name and gives it a different aggregation or set of aggregations instead. Defined by the metric_overrides argument.</td>
</tr>
<tr>
<td>defaultAggregation</td>
<td>The default aggregation methods for the rollup policy, separated by # characters.</td>
</tr>
<tr>
<td>dimensionList</td>
<td>Comma-separated list of dimensions to be included or excluded from the aggregations, depending on the value of dimensionListType.</td>
</tr>
<tr>
<td>dimensionListType</td>
<td>Indicates whether the dimensionList should be included or excluded from the rollup policy.</td>
</tr>
<tr>
<td>metricList</td>
<td>Comma-separated list of metrics to be included or excluded from the set of metrics rolled up to the summaries, depending on the value of dimensionListType.</td>
</tr>
<tr>
<td>metricListType</td>
<td>Indicates whether the metricList should be included or excluded from the rollup policy.</td>
</tr>
<tr>
<td>rollup.&lt;summary number&gt;.rollupIndex</td>
<td>The target rollup index for a specific summary. Summaries are identified by the &lt;summary number&gt;.</td>
</tr>
<tr>
<td>rollup.&lt;summary number&gt;.span</td>
<td>The rollup span for a specific summary. Summaries are identified by the &lt;summary number&gt;.</td>
</tr>
</tbody>
</table>

Example request and response

Place this stanza in metric_rollups.conf:

```
[index:index_s]
aggregation.fool = min#avg
aggregation.foolo = count#avg
defaultAggregation = avg#max
dimensionList = app,region
dimensionListType = included
metricList = foo3,foo4
metricListType = excluded
numRollupPolicy = 1
rollup.0.rollupIndex = index_d_30m
rollup.0.span = 30m
```

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/catalog/metricstore/rollup/index_s -d
summaries="30m|index_d_30m"
```

XML response

```
...<entry>
```
Deletes a rollup policy for a specific source {index}.

Request parameters
None specific to this method.

Returned values
None specific to this method.
Example request and response

Remove the `[index:metric_x]` stanza from `metric_rollups.conf`.

XML Request

curl -k -u admin:changeme -X DELETE https://localhost:8089/services/catalog/metricstore/rollup/metric_x

XML response

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      <title>metricstore_rollup</title>
      <id>https://localhost:8089/services/catalog/metricstore/rollup</id>
      <updated>2019-03-20T16:40:00-07:00</updated>
      <generator build="86a463dcd7353fbb093ddacb657f1314fff6529" version="20190319"/>
      <author>
        <name>Splunk</name>
      </author>
      <link href="/services/catalog/metricstore/rollup/_new" rel="create"/>
      <link href="/services/catalog/metricstore/rollup/_reload" rel="_reload"/>
      <link href="/services/catalog/metricstore/rollup/_acl" rel="_acl"/>
      <opensearch:totalResults>0</opensearch:totalResults>
      <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
      <opensearch:startIndex>0</opensearch:startIndex>
      <s:messages/>
    </feed>
```
Output endpoints

Output endpoint descriptions

Manage data from forwarders.

Usage details

*Review ACL information for an endpoint*

To check Access Control List (ACL) properties for an endpoint, append `/acl` to the path. For more information see Access Control List in the *REST API User Manual*.

*Authentication and Authorization*

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as `admin`, can access authorization information in Splunk Web. To view the roles assigned to a user, select *Settings > Access controls* and click *Users*. To determine the capabilities assigned to a role, select *Settings > Access controls* and click *Roles*.

*App and user context*

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the *REST API User Manual*.

*Splunk Cloud URL for REST API access*

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

**Managed Splunk Cloud deployments**

https://<deployment-name>.splunkcloud.com:8089

**Self-service Splunk Cloud deployments**

To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the *Splunk REST API Tutorials* for more information.
data/outputs/tcp/default

https://<host>:<mPort>/services/data/outputs/tcp/default

Access to global tcpout properties.

GET

Returns the current tcpout properties.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoLB</td>
<td>Specifies whether Auto Load balance method is used.</td>
</tr>
<tr>
<td>defaultGroup</td>
<td>Target group names. The forwarder sends all data to the specified groups.</td>
</tr>
<tr>
<td></td>
<td>Starting with 4.2, this attribute is no longer required.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if tcpout settings are disabled.</td>
</tr>
<tr>
<td>forwardedindex.0.whitelist</td>
<td>Specifies 0th whitelist filter. forwardedindex.&lt;n&gt;.whitelist decides which events get forwarded based on the indexes they belong to.</td>
</tr>
<tr>
<td>forwardedindex.1.blacklist</td>
<td>Specifies 1st blacklist filter. forwardedindex.&lt;n&gt;.blacklist specifies index for which events are not forwarded.</td>
</tr>
<tr>
<td>forwardedindex.2.whitelist</td>
<td>Specifies 2nd whitelist filter. forwardedindex.&lt;n&gt;.whitelist decides which events get forwarded based on the indexes they belong to.</td>
</tr>
<tr>
<td>forwardedindex.filter.disable</td>
<td>Specifies whether filtering of forwarded data based on index is disabled.</td>
</tr>
<tr>
<td>indexAndForward</td>
<td>Specifies whether to index all data locally, in addition to forwarding it. Defaults to false. This is known as an “index-and-forward” configuration. This attribute is only available for heavy forwarders. It is available only at the top level [tcpout] stanza in outputs.conf. It cannot be overridden in a target group.</td>
</tr>
<tr>
<td>maxQueueSize</td>
<td>Sets the maximum size of the forwarder output queue. It also sets the maximum size of the wait queue to 3x this value, if you have enabled indexer acknowledgment (useACK=true). See the parameter description for the POST operation for more information.</td>
</tr>
</tbody>
</table>

Example request and response
XML Request

curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/default

XML Response

...<title>tcpout-default</title>

<id>https://localhost:8089/services/data/outputs/tcp/default</id>

<updated>2011-07-10T22:38:23-07:00</updated>

<generator version="102807"/>

<author>
  <name>Splunk</name>
</author>

<link href="/services/data/outputs/tcp/default/_new" rel="create"/>

<link href="/services/data/outputs/tcp/default/_reload" rel="_reload"/>

... opensearch nodes elided ...

<s:messages/>

<entry>
  <title>tcpout</title>
  
  <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/default/tcpout</id>
  
  <updated>2011-07-10T22:38:23-07:00</updated>

  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="alternate"/>

  <author>
    <name>nobody</name>
  </author>

  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout/_reload" rel="_reload"/>

  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="edit"/>

  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout/remove" rel="remove"/>

  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout/disable" rel="disable"/>

  <content type="text/xml">
    
    <s:dict>
      <s:key name="autoLB">1</s:key>
      <s:key name="defaultGroup">spacecake_9998</s:key>
      <s:key name="disabled">0</s:key>
      ... eai:acl nodes elided ...
      <s:key name="forwardedindex.0.whitelist">.*</s:key>
      <s:key name="forwardedindex.1.blacklist">_.*</s:key>
      <s:key name="forwardedindex.2.whitelist">_audit</s:key>
      <s:key name="forwardedindex.filter.disable">0</s:key>
      <s:key name="indexAndForward">0</s:key>
      <s:key name="maxQueueSize">500KB</s:key>
    </s:dict>

    </content>

  </entry>

POST

Configure global tcpout properties.

Request parameters
**defaultGroup**  String  Comma-separated list of one or more target group names, specified later in [tcpout:<target_group>] stanzas of outputs.conf.spec file.

The forwarder sends all data to the specified groups. If you do not want to forward data automatically, do not set this attribute. Can be overridden by an inputs.conf _TCP_ROUTING setting, which in turn can be overridden by a props.conf/transforms.conf modifier.

Starting with 4.2, this attribute is no longer required.

**disabled**  Boolean  Disables default tcpout settings

If set to a positive number, wait the specified number of seconds before throwing out all new events until the output queue has space. Defaults to -1 (do not drop events).

CAUTION: Do not set this value to a positive integer if you are monitoring files.

Setting this to -1 or 0 causes the output queue to block when it gets full, which causes further blocking up the processing chain. If any target group queue is blocked, no more data reaches any other target group.

Using auto load-balancing is the best way to minimize this condition, because, in that case, multiple receivers must be down (or jammed up) before queue blocking can occur.

**dropEventsOnQueueFull**  Number  If set to a positive number, wait the specified number of seconds before throwing out all new events until the output queue has space. Defaults to -1 (do not drop events).

Specifies whether to index all data locally, in addition to forwarding it. Defaults to false.

This is known as an "index-and-forward" configuration. This attribute is only available for heavy forwarders. It is available only at the top level [tcpout] stanza in outputs.conf. It cannot be overridden in a target group.

**heartbeatFrequency**  Number  How often (in seconds) to send a heartbeat packet to the receiving server.

Heartbeats are only sent if sendCookedData=true. Defaults to 30 seconds.

**maxQueueSize**  Number  Specify an integer or integer[KB][MB][GB].

Sets the maximum size of the forwarder output queue. It also sets the maximum size of the wait queue to 3x this value, if you have enabled indexer acknowledgment (useACK=true).

Although the wait queue and the output queues are both configured by this attribute, they are separate queues. The setting determines the maximum size of the queue in-memory (RAM) buffer.

For heavy forwarders sending parsed data, maxQueueSize is the maximum number of events. Since events are typically much shorter than data blocks, the memory consumed by the queue on a parsing forwarder is likely to be much smaller than on a non-parsing forwarder, if you use this version of the setting.

If specified as a lone integer (for example, maxQueueSize=100), maxQueueSize indicates the maximum number of queued events (for parsed
data) or blocks of data (for unparsed data). A block of data is approximately 64KB. For non-parsing forwarders, such as universal forwarders, that send unparsed data, maxQueueSize is the maximum number of data blocks.

If specified as an integer followed by KB, MB, or GB (for example, maxQueueSize=100MB), maxQueueSize indicates the maximum RAM allocated to the queue buffer. Defaults to 500KB (which means a maximum size of 500KB for the output queue and 1500KB for the wait queue, if any).

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Configuration to be edited. The only valid value is &quot;tcpout&quot;.</td>
</tr>
<tr>
<td>sendCookedData</td>
<td>Boolean</td>
<td></td>
<td>If true, events are cooked (processed by Splunk software). If false, events are raw and untouched prior to sending. Defaults to true. Set to false if you are sending to a third-party system.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/default/tcpout -d 'defaultGroup=myIndexers'

XML Response

...<title>tcpout-default</title>
<id>https://localhost:8089/services/data/outputs/tcp/default/tcpout</id>
<updated>2011-07-10T22:43:53-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/default/_new" rel="create"/>
<link href="/services/data/outputs/tcp/default/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>

data/outputs/tcp/default/{name}

https://<host>:<mPort>/services/data/outputs/tcp/default/{name}
Manage forwarder settings.
DELETE

Disable the default forwarding settings.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:changeme --request DELETE https://localhost:8089/services/data/outputs/tcp/default/tcpout

XML Response

...
<title>tcpout-default</title>
<id>https://localhost:8085/services/data/outputs/tcp/default</id>
<updated>2011-07-19T20:09:02-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/default/_new" rel="create"/>
<link href="/services/data/outputs/tcp/default/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>

GET

Retrieve the named configuration.

Usage details
The only valid {name} here is "tcpout".

Request parameters
None

Returned values
None

Example request and response
XML Request

curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/default/tcpout

XML Response

...
<title>tcpout-default</title>
<id>https://localhost:8089/services/data/outputs/tcp/default</id>
<updated>2011-07-10T22:38:23-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/default/_new" rel="create"/>
<link href="/services/data/outputs/tcp/default/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title(tcpout)</title>
  <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/default/tcpout</id>
  <updated>2011-07-10T22:38:23-07:00</updated>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="list"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="edit"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout" rel="remove"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/default/tcpout/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="autoLB">1</s:key>
      <s:key name="defaultGroup">spacecake_9998</s:key>
      <s:key name="disabled">0</s:key>
      ... eai:acl nodes elided ...
      <s:key name="forwardedindex.0.whitelist">.*</s:key>
      <s:key name="forwardedindex.1.blacklist">_.*</s:key>
      <s:key name="forwardedindex.2.whitelist">_audit</s:key>
      <s:key name="forwardedindex.filter.disable">0</s:key>
      <s:key name="indexAndForward">0</s:key>
      <s:key name="maxQueueSize">500KB</s:key>
    </s:dict>
  </content>
</entry>

POST

Configure global forwarding properties.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>920</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute</td>
<td>Type</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>defaultGroup</td>
<td>String</td>
<td>Comma-separated list of one or more target group names, specified later in [tcpout:&lt;target_group&gt;] stanzas of outputs.conf.spec file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>The forwarder sends all data to the specified groups. If you do not want to forward data automatically, do not set this attribute. Can be overridden by an inputs.conf _TCP_ROUTING setting, which in turn can be overridden by a props.conf/transforms.conf modifier. Starting with 4.2, this attribute is no longer required.</td>
<td></td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>Disables default tcpout settings</td>
<td></td>
</tr>
<tr>
<td>dropEventsOnQueueFull</td>
<td>Number</td>
<td>If set to a positive number, wait the specified number of seconds before throwing out all new events until the output queue has space. Defaults to -1 (do not drop events).</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Caution:</strong> Do not set this value to a positive integer if you are monitoring files.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Setting this to -1 or 0 causes the output queue to block when it gets full, which causes further blocking up the processing chain. If any target group queue is blocked, no more data reaches any other target group.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Using auto load-balancing is the best way to minimize this condition, because, in that case, multiple receivers must be down (or jammed up) before queue blocking can occur.</td>
<td></td>
</tr>
<tr>
<td>heartbeatFrequency</td>
<td>Number</td>
<td>How often (in seconds) to send a heartbeat packet to the receiving server. Heartbeats are only sent if sendCookedData=true. Defaults to 30 seconds.</td>
<td></td>
</tr>
<tr>
<td>indexAndForward</td>
<td>Boolean</td>
<td>Specifies whether to index all data locally, in addition to forwarding it. Defaults to false.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>This is known as an &quot;index-and-forward&quot; configuration. This attribute is only available for heavy forwards. It is available only at the top level [tcpout] stanza in outputs.conf. It cannot be overridden in a target group.</td>
<td></td>
</tr>
<tr>
<td>maxQueueSize</td>
<td>Number</td>
<td>Specify an integer or integer[KB][MB][GB].</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sets the maximum size of the forwarder output queue. It also sets the maximum size of the wait queue to 3x this value, if you have enabled indexer acknowledgment (useACK=true). Although the wait queue and the output queues are both configured by this attribute, they are separate queues. The setting determines the maximum size of the queue in-memory (RAM) buffer. For heavy forwards sending parsed data, maxQueueSize is the maximum number of events. Since events are typically much shorter than data blocks, the memory consumed by the queue on a parsing forwarder is likely to be much smaller than on a non-parsing forwarder, if you use this version of the setting. If specified as a lone integer (for example, maxQueueSize=100), maxQueueSize indicates the maximum number of queued events (for parsed data) or blocks of data (for unparsed data). A block of data is approximately 921...</td>
<td></td>
</tr>
</tbody>
</table>
64KB. For non-parsing forwarders, such as universal forwarders, that send unparsed data, maxQueueSize is the maximum number of data blocks. If specified as an integer followed by KB, MB, or GB (for example, maxQueueSize=100MB), maxQueueSize indicates the maximum RAM allocated to the queue buffer. Defaults to 500KB (which means a maximum size of 500KB for the output queue and 1500KB for the wait queue, if any).

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sendCookedData</td>
<td>Boolean</td>
<td>true</td>
<td>If true, events are cooked (processed by Splunk software). If false, events are raw and untouched prior to sending. Defaults to true. Set to false if you are sending to a third-party system.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Name</td>
<td>Indicates if tcpout is disabled for this group.</td>
<td></td>
</tr>
<tr>
<td>method</td>
<td>Type</td>
<td>Default</td>
<td>Specifies the type of output processor. Valid values: (tcpout</td>
</tr>
<tr>
<td>servers</td>
<td>Type</td>
<td>Default</td>
<td>Servers included in this group.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/group

**XML Response**

...<title>tcpout-group</title>
<id>https://localhost:8089/services/data/outputs/tcp/group</id>
<updated>2011-07-10T22:21:07-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/group/_new" rel="create"/>
<link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>spacecake_9998</title>
  <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998</id>
  <updated>2011-07-10T22:21:07-07:00</updated>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998/_new" rel="create"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998/edit"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/group/spacecake_9998/remove"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      ... eai:acl nodes elided ...
      <s:key name="method">autobalance</s:key>
      <s:key name="servers">
        <s:list>
          <s:item>spacecake:9998</s:item>
        </s:list>
      </s:key>
    </s:dict>
  </content>
</entry>...
POST

Configure a group of one or more data forwarding destinations.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>compressed</td>
<td>Boolean</td>
<td>false</td>
<td>If true, forwarder sends compressed data. If set to true, the receiver port must also have compression turned on.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>false</td>
<td>If true, disables the group.</td>
</tr>
<tr>
<td>dropEventsOnQueueFull</td>
<td>Number</td>
<td>-1</td>
<td>If set to a positive number, wait the specified number of seconds before throwing out all new events until the output queue has space. Defaults to -1 (do not drop events). Caution: Do not set this value to a positive integer if you are monitoring files. Setting this to -1 or 0 causes the output queue to block when it gets full, which causes further blocking up the processing chain. If any target group queue is blocked, no more data reaches any other target group. Using auto load-balancing is the best way to minimize this condition, because, in that case, multiple receivers must be down (or jammed up) before queue blocking can occur.</td>
</tr>
<tr>
<td>heartbeatFrequency</td>
<td>Number</td>
<td>30</td>
<td>How often (in seconds) to send a heartbeat packet to the group. Heartbeats are only sent if sendCookedData=true. Defaults to 30 seconds.</td>
</tr>
<tr>
<td>maxQueueSize</td>
<td>Number</td>
<td>auto</td>
<td>Specify either an integer or integer[KB</td>
</tr>
</tbody>
</table>
If specified as an integer followed by KB, MB, or GB (for example, maxQueueSize=100MB), maxQueueSize indicates the maximum RAM allocated to the queue buffer. Defaults to 500KB (which means a maximum size of 500KB for the output queue and 1500KB for the wait queue, if any).

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>method</strong></td>
<td>Enum</td>
<td></td>
<td>Valid values: (tcpout</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the type of output processor.</td>
</tr>
<tr>
<td><strong>name</strong></td>
<td>String</td>
<td>required</td>
<td>The name of the group of receivers.</td>
</tr>
<tr>
<td><strong>sendCookedData</strong></td>
<td>Boolean</td>
<td>true</td>
<td>If true, send cooked events (events processed by Splunk software). If false, events are raw and untouched prior to sending. Set to false if you are sending to a third-party system. Defaults to true.</td>
</tr>
<tr>
<td><strong>servers</strong></td>
<td>String</td>
<td>required</td>
<td>Comma-separated list of servers to include in the group.</td>
</tr>
<tr>
<td><strong>token</strong></td>
<td>GUID</td>
<td></td>
<td>Token value generated by the indexer after configuration.</td>
</tr>
</tbody>
</table>

**Returned values**
None

**Example request and response**

**XML Request**

curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/group -d name=lan_receivers -d method=autobalance -d servers=10.3.3.3:9997,10.4.4.4:9997

**XML Response**

```
...<title>tcpout-group</title>
<id>https://localhost:8089/services/data/outputs/tcp/group/id</id>
<updated>2011-07-10T22:21:23-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/group/_new" rel="create"/>
<link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
```
data/outputs/tcp/group/{name}

https://<host>:<mPort>/services/data/outputs/tcp/group/{name}
Manage the {name} target group.

Authentication and Authorization

- GET requires list_forwarders capability.
- POST and DELETE require edit_forwarders capability.

DELETE

Deletes the target group specified by {name}.

Request parameters

None

Returned values

None

Example request and response

XML Request

curl -k -u admin:changeme --request DELETE
https://localhost:8089/services/data/outputs/tcp/group/lan_receivers

XML Response

...<title>tcpout-group</title>
{id>https://localhost:8089/services/data/outputs/tcp/group</id>
<updated>2011-07-10T22:32:47-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/group/_new" rel="create"/>
<link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
GET

Get configuration information about the target group specified by {name}.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoLB</td>
<td>Indicates if the forwarder performs automatic load balancing. See the description for the autoLB parameter in POST data/outputs/tcp/group for details.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if tcpout is disabled for this group.</td>
</tr>
<tr>
<td>method</td>
<td>Specifies the type of output processor. Valid values: (tcpout</td>
</tr>
<tr>
<td>servers</td>
<td>Servers included in this group.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/group/lan_receivers
```

**XML Response**

```xml
...
<title>tcpout-group</title>
<id>https://localhost:8089/services/data/outputs/tcp/group</id>
<updated>2011-07-10T22:23:10-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/group/_new" rel="create"/>
<link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
<title>lan_receivers</title>
<id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers</id>
<updated>2011-07-10T22:23:10-07:00</updated>
<link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers" rel="alternate"/>
<author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers" rel="list"/>
<link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers" rel="edit"/>
<link href="/servicesNS/nobody/system/data/outputs/tcp/group/lan_receivers" rel="remove"/>
<content type="text/xml">
926
```
POST

Update the configuration of the target group.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>compressed</td>
<td>Boolean</td>
<td>false</td>
<td>If true, forwarder sends compressed data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If set to true, the receiver port must also have compression turned on.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------</td>
<td>---------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>false</td>
<td>If true, disables the group.</td>
</tr>
<tr>
<td>dropEventsOnQueueFull</td>
<td>Number</td>
<td>-1</td>
<td>If set to a positive number, wait the specified number of seconds before throwing out all new events until the output queue has space. Defaults to -1 (do not drop events).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Caution:</strong> Do not set this value to a positive integer if you are monitoring files.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Setting this to -1 or 0 causes the output queue to block when it gets full, which causes further blocking up the processing chain. If any target group queue is blocked, no more data reaches any other target group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Using auto load-balancing is the best way to minimize this condition, because, in that case, multiple receivers must be down (or jammed up) before queue blocking can occur.</td>
</tr>
<tr>
<td>heartbeatFrequency</td>
<td>Number</td>
<td>30</td>
<td>How often (in seconds) to send a heartbeat packet to the group.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Heartbeats are only sent if sendCookedData=true. Defaults to 30 seconds.</td>
</tr>
<tr>
<td>maxQueueSize</td>
<td>Number</td>
<td>auto</td>
<td>Specify either an integer or integer[KB</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sets the maximum size of the forwarder output queue. It also sets the maximum size of the wait queue to 3x this value, if you have enabled indexer acknowledgment (useACK=true).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Although the wait queue and the output queues are both configured by this attribute, they are separate queues. The setting determines the maximum size of the queue in-memory (RAM) buffer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For heavy forwarders sending parsed data, maxQueueSize is the maximum number of events. Since events are typically much shorter than data blocks, the memory consumed by the queue on a parsing forwarder is likely to be much smaller than on a non-parsing forwarder, if you use this version of the setting.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If specified as a lone integer (for example, maxQueueSize=100), maxQueueSize indicates the maximum number of queued events (for parsed data) or blocks of data (for unparsed data). A block of data is approximately 64KB. For non-parsing forwarders, such as universal forwarders, that send unparsed data, maxQueueSize is the maximum number of data blocks.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If specified as an integer followed by KB, MB, or GB (for example, maxQueueSize=100MB), maxQueueSize indicates the maximum RAM allocated to the queue buffer. Defaults to 500KB (which means a maximum size of 500KB for the output queue and 1500KB for the wait queue, if any).</td>
</tr>
<tr>
<td>method</td>
<td>Enum</td>
<td></td>
<td>Valid values: (tcpout</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the type of output processor.</td>
</tr>
<tr>
<td>sendCookedData</td>
<td>Boolean</td>
<td>true</td>
<td>If true, send cooked events (events processed by Splunk software).</td>
</tr>
</tbody>
</table>
If false, events are raw and untouched prior to sending. Set to false if you are sending to a third-party system.

Defaults to true.

## Returned values

None

## Example request and response

### XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/group/lan_receivers -d maxQueueSize=1024KB -d servers=10.3.3.3:9997,10.4.4.4:9997
```

### XML Response

```
...<title>tcpout-group</title>
<id>https://localhost:8089/services/data/outputs/tcp/group</id>
<updated>2011-07-10T22:26:02-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/group/_new" rel="create"/>
<link href="/services/data/outputs/tcp/group/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
```

## data/outputs/tcp/server

https://<host>:<mPort>/services/data/outputs/tcp/server

Access data forwarding configurations.

### GET

List existing forwarded servers.

**Request parameters**

Pagination and filtering parameters can be used with this method.
Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destHost</td>
<td>DNS name of the destination server.</td>
</tr>
<tr>
<td>destIp</td>
<td>IP address of the destination server.</td>
</tr>
<tr>
<td>destPort</td>
<td>Port on which the destination server is listening.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the outputs to the destination server is disabled.</td>
</tr>
<tr>
<td>method</td>
<td>The data distribution method used when two or more servers exist in the same forwarder group. Valid values: (clone</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Port on destination server where data is forwarded.</td>
</tr>
<tr>
<td>status</td>
<td>Indicates the status of the connection to the server.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```bash
curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/server
```

**XML Response**

```xml
...
<title(tcpout-server)</title>
<id>https://localhost:8089/services/data/outputs/tcp/server</id>
<updated>2011-07-10T21:34:59-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/server/_new" rel="create"/>
<link href="/services/data/outputs/tcp/server/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>spacecake:9998</title>
  <id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998</id>
  <updated>2011-07-10T21:34:59-07:00</updated>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998/_list" rel="list"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998/enable" rel="edit"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998/remove" rel="remove"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998/allconnections" rel="allconnections"/>
  <link href="/servicesNS/nobody/system/data/outputs/tcp/server/spacecake%3A9998/disable" rel="disable"/>
```

930
POST

Creates a new forwarder output.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>If true, disables the forwarder.</td>
</tr>
<tr>
<td>method</td>
<td>Enum</td>
<td></td>
<td>Valid values: (clone</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The data distribution method used when two or more servers exist in the same forwarder group.</td>
</tr>
<tr>
<td>name required</td>
<td>String</td>
<td></td>
<td>&lt;host&gt;:&lt;port&gt; of the Splunk receiver. &lt;host&gt; can be either an ip address or server name. &lt;port&gt; is the the port that the Splunk receiver is listening on.</td>
</tr>
<tr>
<td>sslAltNameToCheck</td>
<td>String</td>
<td></td>
<td>The alternate name to match in the remote server's SSL certificate.</td>
</tr>
<tr>
<td>sslCertPath</td>
<td>String</td>
<td></td>
<td>Path to the client certificate. If specified, connection uses SSL.</td>
</tr>
<tr>
<td>sslCipher</td>
<td>String</td>
<td></td>
<td>SSL Cipher in the form ALL:!aNULL:eNULL!:LOW!:EXP:RC4+:RSA:+HIGH:+MEDIUM</td>
</tr>
<tr>
<td>sslCommonNameToCheck</td>
<td>String</td>
<td></td>
<td>Check the common name of the server's certificate against this name. If there is no match, assume that Splunk Enterprise is not authenticated against this server. You must specify this setting if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td>sslPassword</td>
<td>String</td>
<td></td>
<td>The password associated with the CAcert. The default Splunk Enterprise CAcert uses the password &quot;password.&quot;</td>
</tr>
<tr>
<td>sslRootCAPath</td>
<td>String</td>
<td></td>
<td>The path to the root certificate authority file (optional).</td>
</tr>
<tr>
<td>sslVerifyServerCert</td>
<td>Boolean</td>
<td></td>
<td>If true, make sure that the server you are connecting to is a valid one (authenticated). Both the common name and the alternate name of the server are then checked for a match.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response
XML Request

curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/server -d name=tiny:9997

XML Response

<title>tcpout-server</title>
{id>https://localhost:8089/services/data/outputs/tcp/server</id>
<updated>2011-07-10T21:35:13-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/outputs/tcp/server/_new" rel="create"/>
<link href="/services/data/outputs/tcp/server/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>

data/outputs/tcp/server/{name}

https://<host>:<mPort>/services/data/outputs/tcp/server/{name}
Manage the {name} forwarder.

DELETE

Deletes the configuration for the {name} forwarded server.

Request parameters
None

Returned values
None

Example request and response

XML Request


XML Response

... 
<title>tcpout-server</title>
{id>https://localhost:8089/services/data/outputs/tcp/server</id>
<updated>2011-07-10T21:35:41-07:00</updated>
<generator version="102807"/>
GET

Lists information for the `{name}` forwarded server.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Indicates if the outputs to the destination server is disabled.</td>
</tr>
<tr>
<td>method</td>
<td>The data distribution method used when two or more servers exist in the same forwarder group. Valid values: (clone</td>
</tr>
</tbody>
</table>

Example request and response

XML Request


XML Response

...
POST

Configures the forwarded server specified by \{name\}.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

934
<table>
<thead>
<tr>
<th><strong>disabled</strong></th>
<th><strong>Boolean</strong></th>
<th>If true, disables the forwarder.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>method</strong></td>
<td><strong>Enum</strong></td>
<td>Valid values: (clone</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The data distribution method used when two or more servers exist in the same forwarder group.</td>
</tr>
<tr>
<td><strong>sslAltNameToCheck</strong></td>
<td><strong>String</strong></td>
<td>The alternate name to match in the remote server's SSL certificate.</td>
</tr>
<tr>
<td><strong>sslCertPath</strong></td>
<td><strong>String</strong></td>
<td>Path to the client certificate. If specified, connection uses SSL.</td>
</tr>
<tr>
<td><strong>sslCipher</strong></td>
<td><strong>String</strong></td>
<td>SSL Cipher in the form ALL:!aNULL:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Check the common name of the server's certificate against this name.</td>
</tr>
<tr>
<td><strong>sslCommonNameToCheck</strong></td>
<td><strong>String</strong></td>
<td>If there is no match, assume that Splunk Enterprise is not authenticated against this server. You must specify this setting if sslVerifyServerCert is true.</td>
</tr>
<tr>
<td><strong>sslPassword</strong></td>
<td><strong>String</strong></td>
<td>The password associated with the CAcert.</td>
</tr>
<tr>
<td><strong>sslRootCAPath</strong></td>
<td><strong>String</strong></td>
<td>The path to the root certificate authority file (optional).</td>
</tr>
<tr>
<td><strong>sslVerifyServerCert</strong></td>
<td><strong>Boolean</strong></td>
<td>If true, make sure that the server you are connecting to is a valid one (authenticated). Both the common name and the alternate name of the server are then checked for a match.</td>
</tr>
</tbody>
</table>

**Returned values**
None

**Example request and response**

**XML Request**


**XML Response**

```xml
...<title>tcpout-server</title><id>https://localhost:8089/services/data/outputs/tcp/server</id><updated>2011-07-10T21:35:33-07:00</updated><generator version="102807"/><author><name>Splunk</name></author><link href="/services/data/outputs/tcp/server/_new" rel="create"/><link href="/services/data/outputs/tcp/server/_reload" rel="_reload"/>... opensearch nodes elided ...
<s:messages/>
```
**data/outputs/tcp/server/{name}/allconnections**

https://<host>:<mPort>/services/data/outputs/tcp/server/{name}/allconnections

Get {name} forwarder connections.

**GET**

List current connections to the {name} forwarded server.

**Request parameters**
None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destHost</td>
<td>DNS name of the destination server.</td>
</tr>
<tr>
<td>destIp</td>
<td>IP address of the destination server.</td>
</tr>
<tr>
<td>destPort</td>
<td>Port on which the destination server is listening.</td>
</tr>
<tr>
<td>sourcePort</td>
<td>Port on destination server where data is forwarded.</td>
</tr>
<tr>
<td>status</td>
<td>Indicates the status of the connection to the server.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:changeme
https://localhost:8089/services/data/outputs/tcp/server/localhost:9997/allconnections

**XML Response**

...<entry><title>localhost:9997</title>...
data/outputs/tcp/syslog

https://<host>:<mPort>/services/data/outputs/tcp/syslog
Access the configuration of a forwarded server configured to provide data in standard syslog format.

GET
Provides access to syslog data forwarding configurations.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Specifies whether global syslog configuration is disabled.</td>
</tr>
<tr>
<td>server</td>
<td>Specifies server:port where data is forwarded.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies whether tcp or udp is used to forward data. If unspecified, udp is used. Valid values: (tcp</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/syslog

937
XML Response

POST

Configures a forwarder to send data in standard syslog format

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>True</td>
<td>If true, disables global syslog settings.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>NULL</td>
<td>Name of the syslog output group. This is name used when creating syslog configuration in outputs.conf.</td>
</tr>
<tr>
<td>priority</td>
<td>Number</td>
<td>NULL</td>
<td>Sets syslog priority value.</td>
</tr>
<tr>
<td>server</td>
<td>String</td>
<td>NULL</td>
<td>The priority value should specified as an integer. See $SPLUNK_HOME/etc/system/README/outputs.conf.spec for details.</td>
</tr>
</tbody>
</table>

host:port of the server where syslog data should be sent
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>syslogSourceType</td>
<td>String</td>
<td></td>
<td>Specifies a rule for handling data in addition to that provided by the &quot;syslog&quot; sourcetype. By default, there is no value for syslogSourceType.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This string is used as a substring match against the sourcetype key. For example, if the string is set to 'syslog', then all source types containing the</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>string &quot;syslog&quot; receives this special treatment.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To match a source type explicitly, use the pattern &quot;sourcetype::sourcetype_name.&quot; For example</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>syslogSourceType = sourcetype::apache_common</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data that is &quot;syslog&quot; or matches this setting is assumed to already be in syslog format.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Data that does not match the rules has a header, potentially a timestamp, and a hostname added to the front of the event. This is how Splunk</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>software causes arbitrary log data to match syslog expectations.</td>
</tr>
<tr>
<td>timestampformat</td>
<td>String</td>
<td></td>
<td>Format of timestamp to add at start of the events to be forwarded.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The format is a strftime-style timestamp formatting string. See $SPLUNK_HOME/etc/system/README/outputs.conf.spec for details.</td>
</tr>
<tr>
<td>type</td>
<td>String</td>
<td></td>
<td>Protocol to use to send syslog data. Valid values: (tcp</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

**XML Request**


**XML Response**

```xml
...<title>syslog</title><id>https://localhost:22090/services/data/outputs/tcp/syslog</id><updated>2011-07-21T23:00:26-07:00</updated><generator version="104359"/><author><name>Splunk</name></author><link href="/services/data/outputs/tcp/syslog/_new" rel="create"/><opensearch:totalResults>0</opensearch:totalResults><opensearch:itemsPerPage>30</opensearch:itemsPerPage>
```
data/outputs/tcp/syslog/{name}

https://<host>:<mPort>/services/data/outputs/tcp/syslog/{name}
Manage configuration for the {name} forwarder.

DELETE

Deletes the configuration for the {name} forwarder.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:changeme --request DELETE https://localhost:8089/services/data/outputs/tcp/syslog/myServers

XML Response

<opensearch:totalResults>0</opensearch:totalResults><opensearch:itemsPerPage>30</opensearch:itemsPerPage><opensearch:startIndex>0</opensearch:startIndex><s:messages/>

GET

Returns configuration information for the {name} forwarder.
Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Specifies whether global syslog configuration is disabled.</td>
</tr>
<tr>
<td>server</td>
<td>Specifies server:port where data is forwarded.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies whether tcp or udp is used to forward data. If unspecified, udp is used. Valid values : (tcp</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/syslog/myServers

XML Response

...  
<title>syslog</title>  
<id>https://localhost:8089/services/data/outputs/tcp/syslog/myServers</id>  
<generator version="101277"/>  
<author>  
  <name>Splunk</name>  
</author>  
<link href="/services/data/outputs/tcp/syslog/_new" rel="create"/>  
... opensearch nodes elided ...  
<s:messages/>  
<entry>  
<title>myServers</title>  
<id>https://localhost:8089/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers</id>  
<link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="alternate"/>  
<author>  
  <name>nobody</name>  
</author>  
<link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="list"/>  
<link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="edit"/>  
<link href="/servicesNS/nobody/system/data/outputs/tcp/syslog/myServers" rel="remove"/>  
<content type="text/xml">  
  <s:dict>  
    <s:key name="disabled">1</s:key>  
    ... eai:acl nodes elided ...  
    <s:key name="eai:attributes">  
      <s:dict>  
        <s:key name="optionalFields">  
          <s:list/>  
        </s:dict>  
        <s:key name="requiredFields">  
          <s:list/>  
        </s:dict>  
        <s:key name="wildcardFields">  
          <s:list/>  
        </s:dict>  
      </s:dict>  
    </s:dict>  
  </s:dict>  
</content>
POST

Updates the configuration of the `{name}` forwarder.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>If true, disables global syslog settings.</td>
<td>Sets syslog priority value. The priority value should specified as an integer. See $SPLUNK_HOME/etc/system/README/outputs.conf.spec for details.</td>
</tr>
<tr>
<td>priority</td>
<td>Number</td>
<td></td>
<td>This string is used as a substring match against the sourcetype key. For example, if the string is set to 'syslog', then all source types containing the string &quot;syslog&quot; receive this special treatment.</td>
</tr>
<tr>
<td>server</td>
<td>String</td>
<td>host:port of the server where syslog data should be sent</td>
<td>Specifies a rule for handling data in addition to that provided by the &quot;syslog&quot; sourcetype. By default, there is no value for syslogSourceType.</td>
</tr>
<tr>
<td>syslogSourceType</td>
<td>String</td>
<td></td>
<td>Data that is &quot;syslog&quot; or matches this setting is assumed to already be in syslog format. Data that does not match the rules has a header, potentially a timestamp, and a hostname added to the front of the event. This is how Splunk software causes arbitrary log data to match syslog expectations.</td>
</tr>
<tr>
<td>timestampformat</td>
<td>String</td>
<td>Format of timestamp to add at start of the events to be forwarded.</td>
<td>The format is a strftime-style timestamp formatting string. See $SPLUNK_HOME/etc/system/README/outputs.conf.spec for details.</td>
</tr>
<tr>
<td>type</td>
<td>String</td>
<td>Protocol to use to send syslog data. Valid values: (tcp</td>
<td>udp).</td>
</tr>
</tbody>
</table>
Returned values
None

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/data/outputs/tcp/syslog/myServers -d type=udp

XML Response

...
Search endpoints

Search endpoint descriptions

Manage search resources including:

- Alerts triggered by searches.
- Python search command information.
- Saved searches.
- Search results.
- Scheduled view objects.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select Settings > Access controls and click Users. To determine the capabilities assigned to a role, select Settings > Access controls and click Roles.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

Managed Splunk Cloud deployments

https://<deployment-name>.splunkcloud.com:8089

Self-service Splunk Cloud deployments

To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

944
alerts/alert_actions

https://<host>:<mPort>/services/alerts/alert_actions
Access alert actions.

GET
Access a list of alert actions.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values
Varies depending on the type of alert.

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/-/alerts/alert_actions

XML Response

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>alert_actions</title>
  <id>https://localhost:8089/servicesNS/-/-/alerts/alert_actions</id>
  <updated>2018-12-10T16:45:47-05:00</updated>
  <generator build="8c86330ac18" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/-/-/alerts/alert_actions/_reload" rel="_reload"/>
  <link href="/servicesNS/-/-/alerts/alert_actions/_acl" rel="_acl"/>
  <opensearch:totalResults>9</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>email</title>
    <id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/email</id>
    <updated>1969-12-31T19:00:00-05:00</updated>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/email" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/email" rel="list"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/email/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/system/alerts/alert_actions/email/_edit"/>
  </entry>
</feed>
Send an email notification to specified recipients

If you believe you've received this email in error, please see your Splunk administrator.

splunk > the engine for machine data
<s:dict>
  <s:key name="include.view_link">1</s:key>
  <s:key name="inline">0</s:key>
  <s:key name="label">Send email</s:key>
  <s:key name="mailserver">localhost</s:key>
  <s:key name="maxresults">10000</s:key>
  <s:key name="maxtime">5m</s:key>
  <s:key name="message.alert">The alert condition for '$name$' was triggered.</s:key>
  <s:key name="message.report">The scheduled report '$name$' has run.</s:key>
  <s:key name="pdf.footer_center">title</s:key>
  <s:key name="pdf.footer_enabled">1</s:key>
  <s:key name="pdf.footer_left">logo</s:key>
  <s:key name="pdf.footer_right">timestamp,pagination</s:key>
  <s:key name="pdf.header_center">description</s:key>
  <s:key name="pdf.header_enabled">1</s:key>
  <s:key name="pdf.html_image_rendering">1</s:key>
  <s:key name="pdfview"></s:key>
  <s:key name="preprocess_results"></s:key>
  <s:key name="priority">3</s:key>
  <s:key name="reportCIDFontList">gb,cns,jp,kor</s:key>
  <s:key name="reportFileName">$name$-$time:%Y-%m-%d$</s:key>
  <s:key name="reportIncludeSplunkLogo">1</s:key>
  <s:key name="reportPaperOrientation">portrait</s:key>
  <s:key name="reportPaperSize">letter</s:key>
  <s:key name="sendcsv">0</s:key>
  <s:key name="sendpdf">0</s:key>
  <s:key name="sendresults">0</s:key>
  <s:key name="sslVersions">tls1.2</s:key>
  <s:key name="subject">Splunk Alert: $name$</s:key>
  <s:key name="subject.alert">Splunk Alert: $name$</s:key>
  <s:key name="subject.report">Splunk Report: $name$</s:key>
  <s:key name="to"></s:key>
  <s:key name="track_alert">1</s:key>
  <s:key name="ttl">86400</s:key>
  <s:key name="useNSSubject">0</s:key>
  <s:key name="use_ssl">0</s:key>
  <s:key name="use_tls">0</s:key>
  <s:key name="width_sort_columns">1</s:key>
</s:dict>

<entry>
  <title>logevent</title>
  <id>https://localhost:8089/servicesNS/nobody/alert_logevent/alerts/alert_actions/logevent</id>
  <updated>1969-12-31T19:00:00-05:00</updated>
  <link href="/servicesNS/nobody/alert_logevent/alerts/alert_actions/logevent" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <content type="text/xml">
    <s:dict>
      <s:key name="command">sendalert $action_name$ results_file="$results.file$" results_link="$results.url$"</s:key>
      <s:key name="description">Send log event to Splunk receiver endpoint</s:key>
    </s:dict>
  </content>
</entry>
<key name="can_list">1</key>
<key name="can_share_app">1</key>
<key name="can_share_global">1</key>
<key name="can_share_user">0</key>
<key name="can_write">1</key>
<key name="modifiable">1</key>
<key name="owner">nobody</key>
<key name="perms">
  <dict>
    <key name="read">
      <list>
        <item>*</item>
      </list>
    </key>
    <key name="write">
      <list>
        <item>*</item>
      </list>
    </key>
  </dict>
</key>
<key name="removable">0</key>
<key name="sharing">global</key>
</dict>
<key name="eai:appName">alert_logevent</key>
<key name="eai:userName">nobody</key>
<key name="forceCsvResults">auto</key>
<key name="hostname"></key>
<key name="icon_path">logevent.png</key>
<key name="is_custom">1</key>
<key name="label">Log Event</key>
<key name="maxresults">10000</key>
<key name="maxtime">5m</key>
<key name="param.host"></key>
<key name="param.index">main</key>
<key name="param.source">alert:$name$</key>
<key name="param.sourcetype">generic_single_line</key>
<key name="payload_format">json</key>
<key name="track_alert">0</key>
<key name="ttl">10p</key>
</dict>

<entry>
  <title>lookup</title>
  <id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/lookup</id>
  <updated>1969-12-31T19:00:00-05:00</updated>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup" rel="list"/>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup/edit" rel="edit"/>
  <link href="/servicesNS/nobody/system/alerts/alert_actions/lookup/disable" rel="disable"/>
  <content type="text/xml">
    <dict>
      <key name="append">0</key>
      <key name="command">outputlookup "$action.lookup.filename$" append="$action.lookup.append$</key>
      <key name="description">Output the results of the search to a CSV lookup file</key>
      <key name="disabled">0</key>
    </dict>
  </content>
</entry>
"command"><![CDATA[outputtelemetry input=$action.outputtelemetry.param.input$"
Custom action to output results to telemetry endpoint

Anonymous: 1
License: 0
Support: 1
Component: 
Type: event
Optin Required: 1

Disabled: 0
Description:

ACL:
- App: splunk_instrumentation
- Can Change Perms: 1
- Can List: 1
- Can Share App: 1
- Can Share Global: 1
- Can Share User: 0
- Can Write: 1
- Modifiable: 1
- Owner: nobody
- Perms:
  - Read: *
  - Write: admin
- Removable: 0
- Sharing: global

AppName: splunk_instrumentation
UserName: nobody
Force CSV Results: auto
Hostname: 
Icon Path: outputtelemetry.png
Is Custom: 1
Label: Output results to telemetry endpoint
Max Results: 10000
Max Time: 5m
Param Anonymous: 1
Param Component: 
Param Input: 
Param License: 0
Param Optin Required: 1
Param Support: 1
Param Type: event
Track Alert: 0
TTL: 120

Populate lookup

https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/populate_lookup

1969-12-31T19:00:00-05:00

/alternate
<name>nobody</name>
</author>
</entry>
<entry>
<title>rss</title>
<id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/rss</id>
<updated>1969-12-31T19:00:00-05:00</updated>
<link href="/servicesNS/nobody/system/alerts/alert_actions/rss" rel="alternate"/>
<author>
<name>nobody</name>
</author>
</entry>
</content>
<link href="/servicesNS/nobody/system/alerts/alert_actions/rss/disable" rel="disable"/>
<content type="text/xml">
<s:dict>
<s:key name="command">createrss "path=$name$.xml" "name=$name$" "link=$results.url$" "descr=Alert trigger: $name$, results.count=$results.count$ " "count=30" "graceful=$graceful{default=1}$" maxtime="$action.rss.maxtime{default=1m}$"</s:key>
<s:key name="disabled">0</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app">system</s:key>
<s:key name="can_change_perms">1</s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_share_app">1</s:key>
<s:key name="can_share_global">1</s:key>
<s:key name="can_share_user">0</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">1</s:key>
<s:key name="owner">nobody</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>admin</s:item>
</s:list>
</s:key>
</s:dict>
</s:dict>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
<s:key name="eai:appName">system</s:key>
<s:key name="eai:userName">nobody</s:key>
<s:key name="forceCsvResults">auto</s:key>
<s:key name="hostname"></s:key>
<s:key name="maxresults">10000</s:key>
<s:key name="maxtime">1m</s:key>
<s:key name="track_alert">0</s:key>
<s:key name="ttl">86400</s:key>
</s:dict>
</entry>
</content>
</title>
</title>
</id>https://localhost:8089/servicesNS/nobody/system/alerts/alert_actions/script</id>
<updated>1969-12-31T19:00:00-05:00</updated>
<link href="/servicesNS/nobody/system/alerts/alert_actions/script" rel="alternate"/>
<author>
<name>nobody</name>
</author>
<link href="/servicesNS/nobody/system/alerts/alert_actions/script" rel="list"/>
<link href="/servicesNS/nobody/system/alerts/alert_actions/script/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/system/alerts/alert_actions/script/edit" rel="edit"/>
<content type="text/xml">
<s:dict>
<s:key name="command">runshellscript "$action.script.filename$ "$results.count$ "$search$"
<s:dict>
  <s:key name="description">Invoke a custom script</s:key>
  <s:key name="disabled">0</s:key>
  <s:dict name="eai:acl">
    <s:dict>
      <s:key name="app">system</s:key>
      <s:key name="can_change_perms">1</s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_share_app">1</s:key>
      <s:key name="can_share_global">1</s:key>
      <s:key name="can_share_user">0</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">1</s:key>
      <s:key name="owner">nobody</s:key>
      <s:dict name="perms">
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>*</s:item>
            </s:list>
          </s:key>
          <s:key name="write">
            <s:list>
              <s:item>admin</s:item>
            </s:list>
          </s:key>
        </s:dict>
        <s:key name="removable">0</s:key>
        <s:key name="sharing">system</s:key>
      </s:dict>
      <s:key name="eai:appName">system</s:key>
      <s:key name="eai:userName">nobody</s:key>
      <s:key name="filename"></s:key>
      <s:key name="forceCsvResults">auto</s:key>
      <s:key name="hostname"></s:key>
      <s:key name="icon_path">mod_alert_icon_script.png</s:key>
      <s:key name="label">Run a script</s:key>
      <s:key name="maxresults">10000</s:key>
      <s:key name="maxtime">5m</s:key>
      <s:key name="track_alert">1</s:key>
      <s:key name="ttl">600</s:key>
    </s:dict>
  </s:dict>
</s:dict>
<entry>
<title>webhook</title>
<id>https://localhost:8089/servicesNS/nobody/alert_webhook/alerts/alert_actions/webhook</id>
<updated>1969-12-31T19:00:00-05:00</updated>
<author>
<name>nobody</name>
</author>
<content type="text/xml">
<s:dict>
<s:key name="command">sendalert $action_name$ results_file="$results.file$"
</s:dict>
</content>
</entry>

954
alerts/fired_alerts

https://<host>:<mPort>/services/alerts/fired_alerts

Access fired alerts.
GET

Access a fired alerts summary.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>triggered_alert_count</td>
<td>Trigger count for this alert.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/-/alerts/fired_alerts
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
    xmlns:s="http://dev.splunk.com/ns/rest">
  <title>alerts</title>
  <id>https://localhost:8089/services/alerts/fired_alerts</id>
  <updated>2011-07-11T19:27:22-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch nodes elided for brevity. >
  <s:messages/>
  <entry>
    <title>-</title>
    <id>https://localhost:8089/servicesNS/admin/search/alerts/fired_alerts/-</id>
    <updated>2011-07-11T19:22:07:00</updated>
    <link href="/servicesNS/admin/search/alerts/fired_alerts/-" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/alerts/fired_alerts/-" rel="list"/>
    <content type="text/xml">
      <s:dict>
        <eai:acl elided>
          <s:key name="triggered_alert_count">0</s:key>
        </s:dict>
      </content>
    </entry>
</feed>
```
alerts/fired_alerts/{name}

https://<host>:<mPort>/services/alerts/fired_alerts/{name}

Access or delete the {name} triggered alert.

GET

List unexpired triggered instances of this alert.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>actions</td>
<td>Any additional alert actions triggered by this alert.</td>
</tr>
<tr>
<td>alert_type</td>
<td>Indicates if the alert was historical or real-time.</td>
</tr>
<tr>
<td>digest_mode</td>
<td></td>
</tr>
<tr>
<td>expiration_time_rendered</td>
<td></td>
</tr>
<tr>
<td>savedsearch_name</td>
<td>Name of the saved search that triggered the alert.</td>
</tr>
<tr>
<td>severity</td>
<td>Indicates the severity level of an alert.</td>
</tr>
<tr>
<td>sid</td>
<td>The search ID of the search that triggered the alert.</td>
</tr>
<tr>
<td>trigger_time</td>
<td>The time the alert was triggered.</td>
</tr>
<tr>
<td>trigger_time_rendered</td>
<td></td>
</tr>
<tr>
<td>triggered_alerts</td>
<td></td>
</tr>
</tbody>
</table>

Application usage

Specify - for {name} to return all fired alerts.

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/alerts/fired_alerts/MyAlert

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>alerts</title>
</feed>
DELETE

Delete the record of this triggered alert.

Request parameters
None.

Response keys
None.
Example request and response

curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/alerts/fired_alerts/scheduler__admin__search_aGF2ZV9ldmVudHM_at
_1310437740_5d3dfde563194fffd_1310437749

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     xmlns:s="http://dev.splunk.com/ns/rest">
  <title>alerts</title>
  <id>https://localhost:8089/servicesNS/admin/search/alerts/fired_alerts</id>
  <updated>2011-07-11T19:35:25-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <!-- opensearch nodes elided for brevity. -->
  <s:messages/>
</feed>

alerts/metric_alerts

https://<host>:<mPort>/services/alerts/metric_alerts
This endpoint lets you access and create streaming metric alerts.

Authentication and authorization
Only users whose roles have the metric_alerts capability can use this endpoint.

GET
Access streaming metric alert configurations.

Request parameters
None specific to this method. Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| action.<action_name> | Indicates whether the <action_name> is enabled or disabled for a particular metric alert. Valid values for action_name are:  
  - email  
  - logevent  
  - rss  
  - script  
  - webhook  
For more information about the alert action options see the alert_actions.conf file. |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.&lt;action_name&gt;.&lt;parameter&gt;</td>
<td>Overrides the setting defined for an action in the alert_actions.conf file with a new setting that is valid only for the metric alert configuration to which it is applied.</td>
</tr>
<tr>
<td>condition</td>
<td>Specifies an alert condition for one or more metric_name and aggregation pairs. The alert conditions can include multiple Boolean operators, eval functions, and metric aggregations. The Splunk software applies this evaluation to the results of the alert search on a regular interval. When the alert condition evaluates to 'true', the alert is triggered. Must reference at least one 'mstats_aggregation((metric_name))' clause in single quotes. The condition can also reference dimensions specified in the groupby setting.</td>
</tr>
<tr>
<td>description</td>
<td>Description of the metric alert.</td>
</tr>
<tr>
<td>filter</td>
<td>Provides one or more Boolean expressions like &lt;dimension_field&gt;=&lt;value&gt; to define the search result dataset to monitor for the alert condition. Does not support subsearches, macros, tags, event types, or time modifiers such as 'earliest' or 'latest'. Combines with the metric_indexes setting to provide the complete search filter for the alert.</td>
</tr>
<tr>
<td>groupby</td>
<td>The list of dimension fields, delimited by comma, for the group-by clause of the alert search. This leads to multiple aggregation values, one per group, instead of one single value.</td>
</tr>
<tr>
<td>label.&lt;label-name&gt;</td>
<td>Arbitrary key-value pairs for labeling this alert.</td>
</tr>
<tr>
<td>metric_indexes</td>
<td>Specifies one or more metric indexes, delimited by comma. Combines with the filter setting to provide the complete search filter for the alert.</td>
</tr>
<tr>
<td>splunk_ui.&lt;label-name&gt;</td>
<td>An arbitrary key-value pair that is automatically generated by the Splunk software for its internal use only. Do not change it.</td>
</tr>
<tr>
<td>trigger.expires</td>
<td>Sets the period of time that a triggered alert record displays on the Triggered Alerts page.</td>
</tr>
<tr>
<td>trigger.max_tracked</td>
<td>Specifies the maximum number of instances of this alert that can display in the Triggered Alerts page. When this threshold is passed, the Splunk software removes the earliest instances from the Triggered Alerts page to honor this maximum number.</td>
</tr>
<tr>
<td>trigger.suppress</td>
<td>Specifies the suppression period to silence alert actions and notifications. • The suppression period goes into effect when an alert is triggered. • During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out. • When the period elapses, a subsequent triggering of the alert causes alert actions and notifications to take place as usual, and the alert is suppressed again.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

```
$ curl -k -u admin:changeme https://localhost:8089/services/alerts/metric_alerts
```

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>metric_alerts</title>
  <id>https://localhost:8089/services/alerts/metric_alerts</id>
  <updated>2019-09-16T15:03:59-07:00</updated>
</feed>
```
malert-001

mpool used high
<link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high" rel="list"/>
<link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high/_reload" rel="_reload"/>
<link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high" rel="edit"/>
<link href="/servicesNS/admin/search/alerts/metric_alerts/mpool%20used%20high/disable" rel="disable"/>

<content type="text/xml">
<s:dict>
<s:key name="_group_key">streamalert_d8b75eedcf404743</s:key>
<s:key name="action.email">0</s:key>
<s:key name="action.logevent">0</s:key>
<s:key name="action.rss">0</s:key>
<s:key name="action.script">0</s:key>
<s:key name="action.webhook">1</s:key>
<s:key name="action.webhook.command">sendalert $action_name$ results_file="$results.file$" results_link="$results.url$"</s:key>
<s:key name="action.webhook.description">Generic HTTP POST to a specified URL</s:key>
<s:key name="action.webhook.forceCsvResults">auto</s:key>
<s:key name="action.webhook.icon_path">webhook.png</s:key>
<s:key name="action.webhook.is_custom">1</s:key>
<s:key name="action.webhook.label">Webhook</s:key>
<s:key name="action.webhook.maxresults">10000</s:key>
<s:key name="action.webhook.maxtime">5m</s:key>
<s:key name="action.webhook.param.user_agent">Splunk/$server.guid$</s:key>
<s:key name="action.webhook.payload_format">json</s:key>
<s:key name="action.webhook.track_alert">0</s:key>
<s:key name="action.webhook.ttl">10p</s:key>
<s:key name="condition">'max(spl.mlog.mpool.used)' > 10000</s:key>
<s:key name="description">spl.mlog.mpool.used too high</s:key>
<s:key name="disabled">0</s:key>
<s:dict>
<s:key name="app">search</s:key>
<s:key name="can_change_perms">1</s:key>
<s:key name="can_share_app">1</s:key>
<s:key name="can_share_global">1</s:key>
<s:key name="can_share_user">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">1</s:key>
<s:key name="owner">admin</s:key>
<s:key name="perms"/>
<s:key name="removable">1</s:key>
<s:key name="sharing">user</s:key>
</dict>
<s:dict>
<s:key name="eai:appName">search</s:key>
<s:key name="eai:userName">admin</s:key>
<s:key name="filter"/>
<s:key name="metric_indexes">_metrics</s:key>
<s:key name="splunk_ui.displayview">analytics_workspace</s:key>
<s:key name="splunk_ui.managedBy">Analytics Workspace</s:key>
<s:key name="splunk_ui.severity">1</s:key>
<s:key name="splunk_ui.track">1</s:key>
<s:key name="trigger.expires">24h</s:key>
<s:key name="trigger.max_tracked">20</s:key>
<s:key name="trigger.suppress">3m</s:key>
<s:key name="triggered_alert_count">20</s:key>
</dict>
</s:dict>
Create a streaming metric alert.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.&lt;action-name&gt;</td>
<td>Boolean</td>
<td>Indicates whether the <code>&lt;action_name&gt;</code> is enabled or disabled for a particular metric alert. Valid values for <code>&lt;action_name&gt;</code> are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- email&lt;br&gt;- logevent&lt;br&gt;- rss&lt;br&gt;- script&lt;br&gt;- webhook</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more information about the alert action options see the <code>alert_actions.conf</code> file.</td>
</tr>
<tr>
<td>action.&lt;action-name&gt;.&lt;parameter&gt;</td>
<td>String</td>
<td>Override the global setting defined for an <code>&lt;action-name&gt;</code> in the <code>alert_actions.conf</code> file with a new setting that is valid only for the metric alert configuration to which it is applied.</td>
</tr>
<tr>
<td>condition</td>
<td>Boolean</td>
<td>Specifies an alert condition for one or more metric_name and aggregation pairs. You can set alert conditions that include multiple Boolean operators, eval functions, and metric aggregations. The Splunk software applies this evaluation to the results of the alert search on a regular interval. When the alert condition evaluates to 'true', the alert is triggered. Must reference at least one '&lt;mstats_aggregation&gt;(&lt;metric_name&gt;)' clause in single quotes. The condition can also reference dimensions specified in the <code>groupby</code> setting.</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td>Provide a description of the streaming metric alert.</td>
</tr>
<tr>
<td>filter</td>
<td>String</td>
<td>Specify one or more Boolean expressions like <code>&lt;dimension_field&gt;=&lt;value&gt;</code> to define the search result dataset to monitor for an alert condition. Link multiple Boolean expressions with the <code>AND</code> operator. The filter does not support subsearches, macros, tags, event types, or time modifiers such as 'earliest' or 'latest'.&lt;br&gt;This setting combines with the <code>metric_indexes</code> setting to provide the complete search filter for the alert.</td>
</tr>
<tr>
<td>groupby</td>
<td>String</td>
<td>Provide a list of dimension fields, delimited by comma, for the group-by clause of the alert search. This results in multiple aggregation values, one per group, instead of one aggregation value.</td>
</tr>
<tr>
<td>label.&lt;label-name&gt;</td>
<td>String</td>
<td>Provide an arbitrary key-value pair to label or tag this alert. This key-value pair is not used by the Splunk alerting framework. You can design applications that use the alert label when they call the <code>alerts/metric_alerts</code> endpoint.</td>
</tr>
<tr>
<td>metric_indexes</td>
<td>String</td>
<td>Specify one or more metric indexes, delimited by comma. Combinest with the filter setting to define the search result dataset that the alert monitors for the alert condition.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>Specify the name of the streaming metric alert.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>trigger.expires</td>
<td>String</td>
<td>Set the period of time that a triggered alert record displays on the Triggered Alerts page.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Use <code>&lt;positive integer&gt;&lt;time-unit&gt;</code>, where <code>&lt;time-unit&gt;</code> can be 'm' for minutes, 'h' for hours, and 'd' for days.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Set to 0 to make triggered alerts expire immediately so they do not appear on the Triggered Alerts page at all.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default is 24h.</td>
</tr>
<tr>
<td>trigger.max_tracked</td>
<td>Number</td>
<td>Specify the maximum number of instances of this alert that can display in the triggered alerts dashboard. When this threshold is passed, the Splunk software removes the earliest instances from the dashboard to honor this maximum number. Set to 0 to remove the cap.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defaults to 20.</td>
</tr>
<tr>
<td>trigger.suppress</td>
<td>String</td>
<td>Define the suppression period to silence alert actions and notifications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The suppression period goes into effect when an alert is triggered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When the period elapses, a subsequent triggering of the alert causes alert actions and notifications to take place as usual, and the alert is suppressed again.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use <code>&lt;number&gt;m</code> to specify a timespan in minutes. Default is 0m.</td>
</tr>
</tbody>
</table>

Returned values

None.

Example request and response

**XML Request**

```bash
$ curl -k -u admin:changeme https://localhost:8089/services/alerts/metric_alerts -X POST -d name=malert-001 -d condition='sum(spl.intr.resource_usage.Hostwide.data.cpu_count)%3E%3D10' -d filter=region%3Deast -d metric_indexes=_metrics
```

**XML response**

```xml
  <title>metric_alerts</title>
  <id>https://localhost:8089/services/alerts/metric_alerts</id>
  <updated>2019-09-16T15:07:52-07:00</updated>
  <generator build="7170447726604e6ce5018fa5c563f5b631656bdf" version="20190910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/alerts/metric_alerts/_new" rel="create"/>
  <link href="/services/alerts/metric_alerts/_reload" rel="_reload"/>
  <link href="/services/alerts/metric_alerts/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```
alerts/metric_alerts/{alert_name}

https://<host>:<mPort>/services/alerts/metric_alerts/{alert_name}

This endpoint lets you create, update, delete, enable, and disable streaming metric alerts.

Authentication and authorization
Only users whose roles have the metric_alerts capability can use this endpoint.

GET

Access the named streaming metric alert.

Request parameters

None specific to this method. Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.&lt;action_name&gt;</td>
<td>Indicates whether the &lt;action_name&gt; is enabled or disabled for a particular metric alert. Valid values for action_name are:</td>
</tr>
<tr>
<td></td>
<td>• email</td>
</tr>
<tr>
<td></td>
<td>• logevent</td>
</tr>
<tr>
<td></td>
<td>• rss</td>
</tr>
<tr>
<td></td>
<td>• script</td>
</tr>
<tr>
<td></td>
<td>• webhook</td>
</tr>
<tr>
<td></td>
<td>For more information about the alert action options see the alert_actions.conf file.</td>
</tr>
<tr>
<td>action.&lt;action_name&gt;.&lt;parameter&gt;</td>
<td>Overrides the setting defined for an action in the alert_actions.conf file with a new setting that is valid only for the metric alert configuration to which it is applied.</td>
</tr>
<tr>
<td>condition</td>
<td>Specifies an alert condition for one or more metric_name and aggregation pairs. The alert conditions can include multiple Boolean operators, eval functions, and metric aggregations. The Splunk software applies this evaluation to the results of the alert search on a regular interval. When the alert condition evaluates to 'true', the alert is triggered.</td>
</tr>
<tr>
<td></td>
<td>Must reference at least one '&lt;mstats_aggregation&gt;({metric_name})' clause in single quotes. The condition can also reference dimensions specified in the groupby setting.</td>
</tr>
<tr>
<td>description</td>
<td>Description of the metric alert.</td>
</tr>
<tr>
<td>groupby</td>
<td>The list of dimension fields, delimited by comma, for the group-by clause of the alert search. This leads to multiple aggregation values, one per group, instead of one single value.</td>
</tr>
<tr>
<td>filter</td>
<td>Provides one or more Boolean expressions like &lt;dimension_field&gt;=&lt;value&gt; to define the search result dataset to monitor for the alert condition. Does not support subsearches, macros, tags, event types, or time modifiers such as 'earliest' or 'latest'.</td>
</tr>
<tr>
<td></td>
<td>Combines with the metric_indexes setting to provide the complete search filter for the alert.</td>
</tr>
<tr>
<td>label.&lt;label-name&gt;</td>
<td>Arbitrary key-value pairs for labeling this alert.</td>
</tr>
<tr>
<td>metric_indexes</td>
<td></td>
</tr>
</tbody>
</table>

965
Specifies one or more metric indexes, delimited by comma. 
Combines with the filter setting to provide the complete search filter for the alert.

**splunk_ui.<label-name>**
An arbitrary key-value pair that is automatically generated by the Splunk software for its internal use only. Do not change it.

**trigger.expires**
Sets the period of time that a triggered alert record displays on the Triggered Alerts page.

**trigger.max_tracked**
Specifies the maximum number of instances of this alert that can display in the Triggered Alerts page. When this threshold is passed, the Splunk software removes the earliest instances from the Triggered Alerts page to honor this maximum number.

**trigger.suppress**
Specifies the suppression period to silence alert actions and notifications.

- The suppression period goes into effect when an alert is triggered.
- During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out.
- When the period elapses, a subsequent triggering of the alert causes alert actions and notifications to take place as usual, and the alert is suppressed again.

### Example request and response

**XML Request**

```bash
curl -k -u admin:pass123 https://localhost:8089/services/alerts/metric_alerts/malert-001
```

**XML Response**

```xml
>
  <title>malert-001</title>
  <id>https://localhost:8089/services/alerts/metric_alerts/malert-001</id>
  <updated>2019-09-16T14:50:17-07:00</updated>
  <generator build="7170447726604e6ce5018fa5c563f5b631656bdf" version="20190910"/>
  <author>
    <name>admin</name>
  </author>
  <link href="/services/alerts/metric_alerts/malert-001" rel="list"/>
  <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="edit"/>
  <link href="/servicesNS/admin/search/alerts/metric_alerts/malert-001" rel="remove"/>
</feed>
```
Send an email notification to specified recipients.

If you believe you've received this email in error, please see your Splunk administrator.
<s:key name="action.email.to"></s:key>
<s:key name="action.email.track_alert">1</s:key>
<s:key name="action.email.ttl">86400</s:key>
<s:key name="action.email.use NSSubject">0</s:key>
<s:key name="action.email.use_ssl">0</s:key>
<s:key name="action.email.use_tls">0</s:key>
<s:key name="action.email.width_sort_columns">1</s:key>
<s:key name="action.logevent">0</s:key>
<s:key name="action.logevent.command">sendalert $action_name$ results_file="$results.file$" results_link="$results.url$"
</s:key>
<s:key name="action.logevent.description">Send log event to Splunk receiver endpoint</s:key>
<s:key name="action.logevent.forceCsvResults">auto</s:key>
<s:key name="action.logevent.hostname"></s:key>
<s:key name="action.logevent.icon_path">logevent.png</s:key>
<s:key name="action.logevent.is_custom">1</s:key>
<s:key name="action.logevent.label">Log Event</s:key>
<s:key name="action.logevent.maxtime">5m</s:key>
<s:key name="action.logevent.param.host"></s:key>
<s:key name="action.logevent.param.index">main</s:key>
<s:key name="action.logevent.param.source">alert:$name$</s:key>
<s:key name="action.logevent.param.sourcetype">generic_single_line</s:key>
<s:key name="action.logevent.payload_format">json</s:key>
<s:key name="action.logevent.track_alert">0</s:key>
<s:key name="action.logevent.ttl">10p</s:key>
<s:key name="action.lookup">0</s:key>
<s:key name="action.lookup.append">0</s:key>
<s:key name="action.lookup.command">outputlookup "$action.lookup.filename$" append="$action.lookup.append$"
</s:key>
<s:key name="action.lookup.description">Output the results of the search to a CSV lookup file</s:key>
<s:key name="action.lookup.forceCsvResults">auto</s:key>
<s:key name="action.lookup.hostname"></s:key>
<s:key name="action.lookup.icon_path">mod_alert_icon_lookup.png</s:key>
<s:key name="action.lookup.label">Output results to lookup</s:key>
<s:key name="action.lookup.maxresults">10000</s:key>
<s:key name="action.lookup.maxtime">5m</s:key>
<s:key name="action.lookup.track_alert">0</s:key>
<s:key name="action.lookup.ttl">10p</s:key>
<s:key name="action.populate_lookup">0</s:key>
<s:key name="action.populate_lookup.command">copyresults dest="$action.populate_lookup.dest$" sid="$search_id$"
</s:key>
<s:key name="action.populate_lookup.forceCsvResults">auto</s:key>
<s:key name="action.populate_lookup.hostname"></s:key>
<s:key name="action.populate_lookup.maxresults">10000</s:key>
<s:key name="action.populate_lookup.maxtime">5m</s:key>
<s?key name="action.populate_lookup.track_alert">0</s?key>
<s?key name="action.populate_lookup.ttl">10p</s?key>
<s?key name="action.rss">0</s?key>
<s?key name="action.rss.command">createrss "path=$name$.xml" "name=$name$" "link=$results.url$" "descr=Alert trigger: $name$, results.count=$results.count$ " "count=30" "graceful=$graceful{default=1}$" maxtime="$action.rss.maxtime{default=1m}$"
</s?key>
<s?key name="action.rss.forceCsvResults">auto</s?key>
<s?key name="action.rss.hostname"></s?key>
<s?key name="action.rss.maxresults">10000</s?key>
<s?key name="action.rss.maxtime">1m</s?key>
<s?key name="action.rss.track_alert">0</s?key>
<s?key name="action.rss.ttl">86400</s?key>
<s?key name="action.script">0</s?key>
<s?key name="action.script.command">runshellscript "$action.script.filename$ "$results.count$"
Update the named streaming metric alert.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
</table>
| action.<action-name> | Boolean | Indicates whether the `<action_name>` is enabled or disabled for a particular metric alert. Valid values for `<action_name>` are:  
  - email  
  - logevent  
  - rss  
  - script  
  - webhook  
  
  For more information about the alert action options see the `alert_actions.conf` file. |
| action.<action-name>.<parameter> | String  |             |
Override the global setting defined for an `<action-name>` in the `alert_actions.conf` file with a new setting that is valid only for the metric alert configuration to which it is applied.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>condition</td>
<td>Boolean eval</td>
<td>Specifies an alert condition for one or more metric_name and aggregation pairs. You can set alert conditions that include multiple Boolean operators, eval functions, and metric aggregations. The Splunk software applies this evaluation to the results of the alert search on a regular interval. When the alert condition evaluates to 'true', the alert is triggered. Must reference at least one <code>&lt;mstats_aggregation&gt;(&lt;metric_name&gt;)</code> clause in single quotes. The condition can also reference dimensions specified in the groupby setting.</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td>Provide a description of the streaming metric alert.</td>
</tr>
<tr>
<td>groupby</td>
<td>String</td>
<td>Provide a list of dimension fields, delimited by comma, for the group-by clause of the alert search. This results in multiple aggregation values, one per group, instead of one aggregation value.</td>
</tr>
<tr>
<td>filter</td>
<td>String</td>
<td>Specify one or more Boolean expressions like <code>&lt;dimension_field&gt;=&lt;value&gt;</code> to define the search result dataset to monitor for an alert condition. Link multiple Boolean expressions with the 'AND' operator. The filter does not support subsearches, macros, tags, event types, or time modifiers such as 'earliest' or 'latest'. This setting combines with the <code>metric_indexes</code> setting to provide the complete search filter for the alert.</td>
</tr>
<tr>
<td>label.&lt;label-name&gt;</td>
<td>String</td>
<td>Provide an arbitrary key-value pair to label or tag this alert. This key-value pair is not used by the Splunk alerting framework. You can design applications that use the alert label when they call the ‘alerts/metric_alerts’ endpoint.</td>
</tr>
<tr>
<td>metric_indexes</td>
<td>String</td>
<td>Specify one or more metric indexes, delimited by comma. Combines with the filter setting to define the search result dataset that the alert monitors for the alert condition.</td>
</tr>
<tr>
<td>trigger.expires</td>
<td>String</td>
<td>Set the period of time that a triggered alert record displays on the Triggered Alerts page. Use <code>&lt;positive integer&gt;&lt;time-unit&gt;</code>, where <code>&lt;time-unit&gt;</code> can be 'm' for minutes, 'h' for hours, and 'd' for days. Set to 0 to make triggered alerts expire immediately so they do not appear on the Triggered Alerts page at all. Default is 24h.</td>
</tr>
<tr>
<td>trigger.max_tracked</td>
<td>Number</td>
<td>Specify the maximum number of instances of this alert that can display in the triggered alerts dashboard. When this threshold is passed, the Splunk software removes the earliest instances from the dashboard to honor this maximum number. Set to 0 to remove the cap. Defaults to 20.</td>
</tr>
<tr>
<td>trigger.suppress</td>
<td>String</td>
<td>Define the suppression period to silence alert actions and notifications. The suppression period goes into effect when an alert is triggered. During this period, if the alert is triggered again, its actions do not happen and its notifications do not go out. When the period elapses, a subsequent triggering of the alert causes alert actions and notifications to take place as usual, and the alert is suppressed again. Use <code>&lt;number&gt;m</code> to specify a timespan in minutes. Default is 0m.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>------</td>
<td>-------------</td>
</tr>
</tbody>
</table>

**Returned values**

None.

**Example request and response**

**XML Request**

```
$ curl -k -u admin:changeme https://localhost:8089/services/alerts/metric_alerts/malert-002 -d description="updated description of malert-002" -d trigger.expires=1h
```

**XML response**

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>metric_alerts</title>
  <id>https://localhost:8089/services/alerts/metric_alerts</id>
  <updated>2019-09-16T14:38:38-07:00</updated>
  <generator build="7170447726604e6ce5018fa5c563f5b631656bdf" version="20190910"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/alerts/metric_alerts/_new" rel="create"/>
  <link href="/services/alerts/metric_alerts/_reload" rel="_reload"/>
  <link href="/services/alerts/metric_alerts/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

**DELETE**

Deletes the named metric alert.

**Request parameters**

None specific to this method.

**Returned values**

None specific to this method.

**Example request and response**

Remove the [malert-002] stanza from metric_alerts.conf.

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/alerts/metric_alerts/malert-002 -X DELETE
```

**XML response**

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>metric_alerts</title>
</feed>
```
data/commands

https://<host>:<mPort>/services/data/commands
Access Python search commands.

GET
Access Python search commands.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>changes_colorder</td>
<td>Indicates whether the script output should be used to change the column ordering of the fields.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the command is disabled.</td>
</tr>
<tr>
<td>enableheader</td>
<td>Indicate whether or not your script is expecting header information or not.</td>
</tr>
<tr>
<td></td>
<td>Currently, the only thing in the header information is an auth token. If set to true the command expects as input a head section + \ ' then the csv input.</td>
</tr>
<tr>
<td>Note: Should be set to true if you use splunk.Intersplunk</td>
<td></td>
</tr>
<tr>
<td>filename</td>
<td>Name of script file for command.</td>
</tr>
<tr>
<td></td>
<td>&lt;stanza-name&gt;.pl for perl.</td>
</tr>
<tr>
<td></td>
<td>&lt;stanza-name&gt;.py for python.</td>
</tr>
<tr>
<td>generates_timeorder</td>
<td>If generating = false and streaming = true, indicates if the command changes the order of events w/respect to time.</td>
</tr>
<tr>
<td>generating</td>
<td>Indicates if the command generates new events.</td>
</tr>
<tr>
<td>maxinputs</td>
<td>Maximum number of events that can be passed to the command for each invocation. This limit cannot exceed the value of maxresultrows in limits.conf.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>outputheader</td>
<td>If true, the output of script should be a header section + blank line + csv output. If false, script output should be pure csv only.</td>
</tr>
<tr>
<td>passauth</td>
<td>If true, passes an authentication token on the start of input.</td>
</tr>
<tr>
<td>required_fields</td>
<td>A list of fields that this command may use. Informs previous commands that they should retain/extract these fields if possible. No error is generated if a field specified is missing. Defaults to &quot;*&quot;.</td>
</tr>
<tr>
<td>requires_preop</td>
<td>Indicates whether the command sequence specified by the streaming_preop key is required for proper execution or is it an optimization only. Default is false (streaming_preop not required).</td>
</tr>
<tr>
<td>retainsevents</td>
<td>Indicates whether the command retains events (the way the sort/dedup/cluster commands do) or whether the command transforms them (the way the stats command does).</td>
</tr>
<tr>
<td>streaming</td>
<td>Indicates whether the command is streamable.</td>
</tr>
<tr>
<td>supports_getinfo</td>
<td>Indicates whether the command supports dynamic probing for settings (first argument invoked == <strong>GETINFO</strong> or <strong>EXECUTE</strong>).</td>
</tr>
<tr>
<td>supports_rawargs</td>
<td>Indicates whether the command supports raw arguments being passed to it or if it uses parsed arguments (where quotes are stripped).</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the type of command. The only valid value for this attribute is python.</td>
</tr>
</tbody>
</table>

Example request and response

curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/commands

  <title>commandsconf</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/commands</id>
  <updated>2011-07-07T00:52:26-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/commands/_reload" rel="_reload"/>
  <s:messages/>
  <entry>
    <title>bucketdir</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/commands/bucketdir</id>
    <updated>2011-07-07T00:52:26-07:00</updated>
    <link href="/servicesNS/nobody/search/data/commands/bucketdir" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
  </entry>
</feed>
Get information about the `{name}` python search command.

**GET**

Access search command information.

**Request parameters**
None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>changes_colorder</td>
<td>Indicates whether the script output should be used to change the column ordering of the fields.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the command is disabled.</td>
</tr>
<tr>
<td>enableheader</td>
<td>Indicate whether or not your script is expecting header information or not.</td>
</tr>
<tr>
<td>filename</td>
<td>Name of script file for command.</td>
</tr>
</tbody>
</table>

Note: Currently, the only thing in the header information is an auth token. If set to true the command expects as input a head section + \` then the csv input.

Note: Should be set to true if you use splunk.Intersplunk
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;stanza-name&gt;.pl</td>
<td>For Perl.</td>
</tr>
<tr>
<td>&lt;stanza-name&gt;.py</td>
<td>For Python.</td>
</tr>
<tr>
<td>generates_timeorder</td>
<td>If generating = false and streaming = true, indicates if the command changes the order of events w/respect to time.</td>
</tr>
<tr>
<td>generating</td>
<td>Indicates if the command generates new events.</td>
</tr>
<tr>
<td>maxinputs</td>
<td>Maximum number of events that can be passed to the command for each invocation. This limit cannot exceed the value of maxresultrows in limits.conf. 0 indicates no limit. Defaults to 50000.</td>
</tr>
<tr>
<td>outputheader</td>
<td>If true, the output of script should be a header section + blank line + csv output. If false, script output should be pure csv only.</td>
</tr>
<tr>
<td>passauth</td>
<td>If true, passes an authentication token on the start of input.</td>
</tr>
<tr>
<td>required_fields</td>
<td>A list of fields that this command may use. Informs previous commands that they should retain/extract these fields if possible. No error is generated if a field specified is missing. Defaults to &quot;*&quot;.</td>
</tr>
<tr>
<td>requires_preop</td>
<td>Indicates whether the command sequence specified by the streaming_preop key is required for proper execution or is it an optimization only. Default is false (streaming_preop not required).</td>
</tr>
<tr>
<td>retainsevents</td>
<td>Indicates whether the command retains events (the way the sort/dedup/cluster commands do) or whether the command transforms them (the way the stats command does).</td>
</tr>
<tr>
<td>streaming</td>
<td>Indicates whether the command is streamable.</td>
</tr>
<tr>
<td>supports_getinfo</td>
<td>Indicates whether the command supports dynamic probing for settings (first argument invoked == <strong>GETINFO</strong> or <strong>EXECUTE</strong>).</td>
</tr>
<tr>
<td>supports_rawargs</td>
<td>Indicates whether the command supports raw arguments being passed to it or if it uses parsed arguments (where quotes are stripped).</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the type of command. The only valid value for this attribute is python.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/servicesNS/nobody/search/data/commands/input
```

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom"
    xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
    xmlns:s="http://dev.splunk.com/ns/rest">
    <title>commandsconf</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/commands</id>
    <updated>2011-07-07T00:52:26-07:00</updated>
    <generator version="102807"/>
</feed>
```
Access and create saved searches.

**GET**

Access saved search configurations.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest_time</td>
<td>String</td>
<td></td>
<td>For scheduled searches display all the scheduled times starting from this time (not just the next run time)</td>
</tr>
<tr>
<td>latest_time</td>
<td>String</td>
<td></td>
<td>For scheduled searches display all the scheduled times until this time (not just the next run time)</td>
</tr>
<tr>
<td>listDefaultActionArgs</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to list default actions.</td>
</tr>
<tr>
<td>add_orphan_field</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether the response includes a boolean value for each saved search to show whether the search is orphaned, meaning that it has no valid owner. When add_orphan_field is set to true, the response includes the orphaned search indicators, either 0 to indicate that a search is not orphaned or 1 to indicate that the search is orphaned. Admins can use this setting to check for searches without valid owners and resolve related issues.</td>
</tr>
</tbody>
</table>

Pagination and filtering parameters can be used with this method.

This endpoint returns an unusually high number of values. To limit the number of returned values, specify the filtering parameter.

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email</td>
<td>Indicates the state of the email action.</td>
</tr>
<tr>
<td>action.email.sendresults</td>
<td>Indicates whether search results are attached to the email.</td>
</tr>
<tr>
<td>action.email.to</td>
<td>List of addresses for email recipients.</td>
</tr>
<tr>
<td>action.populate_lookup</td>
<td>Indicates the state of the populate lookup action.</td>
</tr>
<tr>
<td>action.rss</td>
<td>Indicates the state of the RSS action.</td>
</tr>
<tr>
<td>action.script</td>
<td>Indicates the state of the script action.</td>
</tr>
<tr>
<td>action.summary_index</td>
<td>Indicates the state of the summary index action.</td>
</tr>
<tr>
<td>alert.digest_mode</td>
<td>Indicates if alert actions are applied to the entire result set or to each individual result.</td>
</tr>
<tr>
<td>alert.expires</td>
<td>Sets the period of time to show the alert in the dashboard. Defaults to 24h.</td>
</tr>
<tr>
<td>alert.expires</td>
<td>Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</td>
</tr>
<tr>
<td>alert.severity</td>
<td>The alert severity level.</td>
</tr>
<tr>
<td>Valid values are:</td>
<td>1 DEBUG</td>
</tr>
<tr>
<td></td>
<td>2 INFO</td>
</tr>
<tr>
<td></td>
<td>3 WARN</td>
</tr>
<tr>
<td></td>
<td>4 ERROR</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>alert.suppress</td>
<td>Indicates whether alert suppression is enabled for this schedules search.</td>
</tr>
<tr>
<td>alert.suppress.period</td>
<td>Specifies the suppression period. Only valid if alert.suppress is enabled. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</td>
</tr>
<tr>
<td>alert.track</td>
<td>Specifies whether to track the actions triggered by this scheduled search. auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions. true - force alert tracking. false - disable alert tracking for this search.</td>
</tr>
<tr>
<td>alert_comparator</td>
<td>One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc.</td>
</tr>
<tr>
<td>alert_condition</td>
<td>A conditional search that is evaluated against the results of the saved search. Defaults to an empty string. Alerts are triggered if the specified search yields a non-empty search result list. Note: If you specify an alert_condition, do not set counttype, relation, or quantity.</td>
</tr>
<tr>
<td>alert_threshold</td>
<td>Valid values are: Integer[%] Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to &quot;rises by perc&quot; or &quot;drops by perc.&quot;</td>
</tr>
<tr>
<td>alert_type</td>
<td>What to base the alert on, overridden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.</td>
</tr>
<tr>
<td>allow_skew</td>
<td>Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods. This setting does not require adjusting in most use cases. Check with an admin before making any updates. When set to a non-zero value for searches with the following cron_schedule values, the search scheduler randomly skews the second, minute, and hour on which the search runs.</td>
</tr>
</tbody>
</table>

    * * * *       Every minute.
    */M * * * *    Every M minutes (M > 0).
    0 * * * *     Every hour.
    0 */H * * *    Every H hours (H > 0).
    0 0 * * *     Every day (at midnight).

When set to a non-zero value for a search that has any other cron_schedule setting, the search scheduler can randomly skew only the second on which the search runs.
The amount of skew for a specific search remains constant between edits of the search.

A value of 0 disallows skew. 0 is the default setting.

**Percentage**

<int> followed by % specifies the maximum amount of time to skew as a percentage of the scheduled search period.

**Duration**

<int><unit> specifies a maximum duration. The <unit> can be omitted only when the <int> is 0.

Valid duration units:

- m
- min
- minute
- mins
- minutes
- h
- hr
- hour
- hrs
- hours
- d
- day
- days

**Examples**

- 100% (for an every-5-minute search) = 5 minutes maximum
- 50% (for an every-minute search) = 30 seconds maximum
- 5m = 5 minutes maximum
- 1h = 1 hour maximum

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cron_schedule</td>
<td>The cron schedule to execute this search.</td>
</tr>
<tr>
<td>description</td>
<td>Description of the saved search.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this saved search is disabled.</td>
</tr>
<tr>
<td>dispatch.buckets</td>
<td>The maximum number of timeline buckets.</td>
</tr>
<tr>
<td>dispatch.earliest_time</td>
<td>A time string that specifies the earliest time for this search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td></td>
<td>If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>dispatch.latest_time</td>
<td>A time string that specifies the latest time for the saved search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td></td>
<td>If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>dispatch.lookups</td>
<td>Indicates if lookups are enabled for this search.</td>
</tr>
<tr>
<td>dispatch.max_count</td>
<td>The maximum number of results before finalizing the search.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dispatch.max_time</td>
<td>Indicates the maximum amount of time (in seconds) before finalizing the search.</td>
</tr>
<tr>
<td>dispatch.reduce_freq</td>
<td>Specifies how frequently the MapReduce reduce phase runs on accumulated map values.</td>
</tr>
<tr>
<td>dispatch.spawn_process</td>
<td>Specifies whether new search process is spawned when this saved search is executed. Searches against indexes must run in a separate process.</td>
</tr>
<tr>
<td>dispatch.time_format</td>
<td>Time format string that defines the time format for specifying the earliest and latest time.</td>
</tr>
<tr>
<td>dispatch.ttl</td>
<td>Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered.</td>
</tr>
<tr>
<td></td>
<td>If an action is triggered, the action ttl is used. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to alert_actions.conf.spec.</td>
</tr>
<tr>
<td></td>
<td>If the integer is followed by the letter 'p', the ttl is interpreted as a multiple of the scheduled search period.</td>
</tr>
<tr>
<td>displayview</td>
<td>Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.</td>
</tr>
<tr>
<td>earliest_time</td>
<td>For scheduled searches display all the scheduled times starting from this time (not just the next run time).</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Indicates if this search is to be run on a schedule.</td>
</tr>
<tr>
<td>is_visible</td>
<td>Indicates if this saved search appears in the visible saved search list.</td>
</tr>
<tr>
<td>latest_time</td>
<td>For scheduled searches display all the scheduled times until this time (not just the next run time).</td>
</tr>
<tr>
<td>listDefaultActionArgs</td>
<td>List default values of actions.*, even though some of the actions may not be specified in the saved search.</td>
</tr>
<tr>
<td>max_concurrent</td>
<td>The maximum number of concurrent instances of this search the scheduler is allowed to run.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>Time when the scheduler runs this search again.</td>
</tr>
<tr>
<td>orphan</td>
<td>If add_orphan_field has been specified in the GET request, indicates whether the search is orphaned.</td>
</tr>
<tr>
<td>qualifiedSearch</td>
<td>The exact search string that the scheduler would run.</td>
</tr>
<tr>
<td>realtime_schedule</td>
<td>Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time.</td>
</tr>
<tr>
<td></td>
<td>If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option.</td>
</tr>
<tr>
<td></td>
<td>If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range.</td>
</tr>
<tr>
<td></td>
<td>The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).</td>
</tr>
<tr>
<td>request.ui.dispatch_app</td>
<td>A field used by Splunk Web to denote the app this search should be dispatched in.</td>
</tr>
<tr>
<td>request.ui.dispatch_view</td>
<td>Specifies a field used by Splunk Web to denote the view this search should be displayed in.</td>
</tr>
<tr>
<td>restart_on_searchpeer_add</td>
<td></td>
</tr>
</tbody>
</table>
Specifies whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search.

Note: The peer can be a newly added peer or a peer down and now available.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>run_on_startup</td>
<td>Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time. This parameter should be set to 1 for scheduled searches that populate lookup tables.</td>
</tr>
</tbody>
</table>
| schedule_priority | Configures the scheduling priority of a specific search. One of the following values.  
|                | [ default | higher | highest ]  
| default        | No scheduling priority increase.                                             |
| higher         | Scheduling priority is higher than other searches of the same scheduling tier. While there are four tiers of priority for scheduled searches, only the following are affected by this property:  
|                | * real-Time-Scheduled (realtime_schedule=1).  
|                | * continuous-Scheduled (realtime_schedule=0).  
| highest        | Scheduling priority is higher than other searches regardless of scheduling tier. However, real-time-scheduled searches with priority = highest always have priority over continuous scheduled searches with priority = highest.  
|                | This is the high-to-low priority order (where RTSS = real-time-scheduled search, CSS = continuous-scheduled search, d = default, h = higher, H = highest).  
|                | RTSS(H) > CSS(H) > RTSS(h) > RTSS(d) > CSS(h) > CSS(d)  
|                | Changing the priority requires the search owner to have the edit_search_schedule_priority capability in order to make non-default settings.  
|                | Defaults to default.                                                        |
|                | For more details, see savedsearches.conf.spec.                             |
| schedule_window | Time window (in minutes) during which the search has lower priority. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. If set to auto, the scheduler prioritizes searches automatically. |
| search         | Search expression to filter the response. The response matches field values against the search expression. For example:  
|                | search=foo matches any object that has “foo” as a substring in a field.  
|                | search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example. |
| vsid           | The viewstate id associated with the UI view listed in 'displayview'.  
|                | Matches to a stanza in viewstates.conf.                                      |

Example requests and responses
**XML Request**

curl -k -u admin:pass https://localhost:8089/services/saved/searches

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>savedsearch</title>
  <id>https://localhost:8089/services/saved/searches</id>
  <updated>2011-07-13T11:56:35-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/saved/searches/_new" rel="create"/>
  <link href="/services/saved/searches/_reload" rel="_reload"/>
  <!-- opensearch nodes elided for brevity. -->
  <s:messages/>
  <entry>
    <title>Errors in the last 24 hours</title>
    <id>https://localhost:8089/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours</id>
    <updated>2011-07-13T11:56:35-07:00</updated>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/edit" rel="edit"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/disable" rel="disable"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/dispatch" rel="dispatch"/>
    <link href="/servicesNS/nobody/search/saved/searches/Errors%20in%20the%20last%2024%20hours/history" rel="history"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">0</s:key>
        <s:key name="action.email.reportServerEnabled">0</s:key>
        <s:key name="action.email.sendresults"/>
        <s:key name="action.email.to"/>
        <s:key name="action.populate_lookup">0</s:key>
        <s:key name="action.rss">0</s:key>
        <s:key name="action.script">0</s:key>
        <s:key name="action.summary_index">0</s:key>
        <s:key name="alert.digest_mode">1</s:key>
        <s:key name="alert.expires">24h</s:key>
        <s:key name="alert.severity">3</s:key>
        <s:key name="alert.suppress"/>
        <s:key name="alert.suppress.period"/>
        <s:key name="alert.track">auto</s:key>
        <s:key name="alert_comparator"/>
        <s:key name="alert_condition"/>
        <s:key name="alert_threshold"/>
        <s:key name="alert_type">always</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```

983
<s:key name="allow_skew">0</s:key>
<s:key name="description"/>
<s:key name="disabled">0</s:key>
<s:key name="dispatch.buckets">0</s:key>
<s:key name="dispatch.earliest_time">-1d</s:key>
<s:key name="dispatch.latest_time"/>
<s:key name="dispatch.lookups">1</s:key>
<s:key name="dispatch.max_count">500000</s:key>
<s:key name="dispatch.max_time">0</s:key>
<s:key name="dispatch.reduce_freq">10</s:key>
<s:key name="dispatch.spawn_process">1</s:key>
<s:key name="dispatch.time_format">%FT%T.%Q%:z</s:key>
<s:key name="dispatch.ttl">2p</s:key>
<s:key name="displayview"/>
<s:key name="is_scheduled">0</s:key>
<s:key name="is_visible">1</s:key>
<s:key name="max_concurrent">1</s:key>
<s:key name="next_scheduled_time"/>
<s:key name="qualifiedSearch">search error OR failed OR severe OR (sourcetype=access_* (404 OR 500 OR 503))</s:key>
<s:key name="realtime_schedule">1</s:key>
<s:key name="request.ui_dispatch_app"/>
<s:key name="request.ui_dispatch_view"/>
<s:key name="restart_on_searchpeer_add">1</s:key>
<s:key name="run_on_startup">0</s:key>
<s:key name="search">error OR failed OR severe OR (sourcetype=access_* (404 OR 500 OR 503))</s:key>
<s:key name="vsid">*:75qh2fwx</s:key>
</s:dict>
</entry>
</feed>

XML Request

curl -s -k -u admin:pass https://localhost:8089/services/saved/searches?f=qualifiedSearch&count=1&f=is_visible"

XML Response

<title>savedsearch</title>
<id>https://localhost:8089/services/saved/searches</id>
<updated>2018-04-09T21:32:11+00:00</updated>
<generator build="00b79c1e9738" version="7.1.0"/>
<author>
  <name>Splunk</name>
</author>
<entry>
<title>Errors in the last 24 hours</title>
</entry>
</feed>

984
POST

Create a saved search.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.&lt;action_name&gt;</td>
<td>String</td>
<td>Enable or disable an alert action. See alert_actions.conf for available alert action types. action_name defaults to the empty string.</td>
</tr>
<tr>
<td>action.&lt;action_name&gt;.&lt;parameter&gt;</td>
<td>String</td>
<td>Use this syntax to configure action parameters. See the following actions and parameter settings.</td>
</tr>
<tr>
<td>action.email</td>
<td>Boolean</td>
<td>The state of the email action. Read-only attribute. Value ignored on POST. Use actions to specify a list of enabled actions. Defaults to 0.</td>
</tr>
<tr>
<td>action.email.auth_password</td>
<td>String</td>
<td>The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here and it is encrypted on the next platform restart. Defaults to empty string.</td>
</tr>
<tr>
<td>action.email.auth_username</td>
<td>String</td>
<td>The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. NOTE: Your SMTP server might reject unauthenticated emails.</td>
</tr>
<tr>
<td>action.email.bcc</td>
<td>String</td>
<td>BCC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>action.email.cc</td>
<td>String</td>
<td>CC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.command</td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.email.format</td>
<td>Enum</td>
<td>Valid values: (plain</td>
</tr>
<tr>
<td>action.email.from</td>
<td>String</td>
<td>Email address from which the email action originates. Defaults to splunk@$LOCALHOST or whatever value is set in alert_actions.conf.</td>
</tr>
<tr>
<td>action.email.hostname</td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a> or <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. When this value begins with &quot;http://&quot;, it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct an externally referencable url, such as SSO environments, other proxies, or when the server hostname is not generally resolvable. Defaults to current hostname provided by the operating system, or if that fails &quot;localhost&quot;. When set to empty, default behavior is used.</td>
</tr>
<tr>
<td>action.email.inline</td>
<td>Boolean</td>
<td>Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.</td>
</tr>
<tr>
<td>action.email.mailserver</td>
<td>String</td>
<td>Set the address of the MTA server to be used to send the emails.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.email.maxresults</td>
<td>Number</td>
<td>Sets the global maximum number of search results to send when email.action is enabled. Defaults to 100.</td>
</tr>
<tr>
<td>action.email.maxtime</td>
<td>Number</td>
<td>Valid values are Integer[m</td>
</tr>
<tr>
<td>action.email.pdfview</td>
<td>String</td>
<td>The name of the view to deliver if sendpdf is enabled.</td>
</tr>
<tr>
<td>action.email.preprocess_results</td>
<td>String</td>
<td>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.</td>
</tr>
<tr>
<td>action.email.reportCIDFontList</td>
<td>Enum</td>
<td>Space-separated list. Specifies the set (and load order) of CID fonts for handling Simplified Chinese(gb), Traditional Chinese(cns), Japanese(jp), and Korean(kor) in Integrated PDF Rendering. If multiple fonts provide a glyph for a given character code, the glyph from the first font specified in the list is used. To skip loading any CID fonts, specify the empty string. Defaults to &quot;gb cns jp kor&quot;</td>
</tr>
<tr>
<td>action.email.reportIncludeSplunkLogo</td>
<td>Boolean</td>
<td>Indicates whether to include the Splunk logo with the report. Valid values: (portrait</td>
</tr>
<tr>
<td>action.email.reportPaperOrientation</td>
<td>Enum</td>
<td>Specifies the paper orientation: portrait or landscape. Defaults to portrait.</td>
</tr>
<tr>
<td>action.email.reportPaperSize</td>
<td>Enum</td>
<td>Valid values: (letter</td>
</tr>
<tr>
<td>action.email.reportServerEnabled</td>
<td>Boolean</td>
<td>Not supported.</td>
</tr>
<tr>
<td>action.email.reportServerURL</td>
<td>String</td>
<td>Not supported. For a default locally installed report server, the URL is <a href="http://localhost:8091/">http://localhost:8091/</a></td>
</tr>
<tr>
<td>action.email.sendpdf</td>
<td>Boolean</td>
<td>Indicates whether to create and send the results as a PDF. Defaults to false.</td>
</tr>
<tr>
<td>action.email.sendresults</td>
<td>Boolean</td>
<td>Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.</td>
</tr>
<tr>
<td>action.email.subject</td>
<td>String</td>
<td>Specifies an alternate email subject.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.email.to</td>
<td>String</td>
<td>A comma or semicolon separated list of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.</td>
</tr>
<tr>
<td>action.email.track_alert</td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.email.ttl</td>
<td>Number</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. Defaults to 86400 (24 hours).</td>
</tr>
<tr>
<td>action.email.use_ssl</td>
<td>Boolean</td>
<td>Indicates whether to use SSL when communicating with the SMTP server. Defaults to false.</td>
</tr>
<tr>
<td>action.email.use_tls</td>
<td>Boolean</td>
<td>Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls). Defaults to false.</td>
</tr>
<tr>
<td>action.email.width_sort_columns</td>
<td>Boolean</td>
<td>Indicates whether columns should be sorted from least wide to most wide, left to right. Only valid if format=text.</td>
</tr>
<tr>
<td>action.populate_lookup</td>
<td>Boolean</td>
<td>The state of the populate lookup action. Read-only attribute. Value ignored on POST. Use actions to specify a list of enabled actions. Defaults to 0.</td>
</tr>
<tr>
<td>action.populate_lookup.command</td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.populate_lookup.dest</td>
<td>String</td>
<td>Lookup name of path of the lookup to populate</td>
</tr>
<tr>
<td>action.populate_lookup.hostname</td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a> or <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.populate_lookup.maxresults</td>
<td>Number</td>
<td>Sets the maximum number of search results sent using alerts. Defaults to 100.</td>
</tr>
<tr>
<td>action.populate_lookup.maxtime</td>
<td>Number</td>
<td>Valid values are: Integer[m</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.populate_lookup.track_alert</td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.populate_lookup.ttl</td>
<td>Number</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, then this specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td>action.rss</td>
<td>Boolean</td>
<td>The state of the rss action. Read-only attribute. Value ignored on POST. Use actions to specify a list of enabled actions. Defaults to 0.</td>
</tr>
<tr>
<td>action.rss.command</td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.rss.hostname</td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms. hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a> or <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.rss.maxresults</td>
<td>Number</td>
<td>Sets the maximum number of search results sent using alerts. Defaults to 100.</td>
</tr>
<tr>
<td>action.rss.maxtime</td>
<td>Number</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 1m.</td>
</tr>
<tr>
<td>action.rss.track_alert</td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.rss.ttl</td>
<td>Number</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td>action.script</td>
<td>Boolean</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.script.command</td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.script.filename</td>
<td>String</td>
<td>File name of the script to call. Required if script action is enabled</td>
</tr>
<tr>
<td>action.script.hostname</td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms. hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a> or <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.script.maxresults</td>
<td>Number</td>
<td>Sets the maximum number of search results sent using alerts. Defaults to 100.</td>
</tr>
<tr>
<td>action.script.maxtime</td>
<td>Number</td>
<td>Valid values are: Integer[m</td>
</tr>
<tr>
<td>action.script.track_alert</td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.script.ttl</td>
<td>Number</td>
<td>Valid values are: Integer[p] Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 600 (10 minutes). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td>action.summary_index</td>
<td>Boolean</td>
<td>The state of the summary index action. Read-only attribute. Value ignored on POST. Use actions to specify a list of enabled actions. Defaults to 0</td>
</tr>
<tr>
<td>action.summary_index._name</td>
<td>String</td>
<td>Specifies the name of the summary index where the results of the scheduled search are saved. Default to &quot;summary.&quot;</td>
</tr>
<tr>
<td>action.summary_index.command</td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.summary_index.hostname</td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in summary-index alert actions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This value accepts two forms:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hostname (for example, splunkserver, splunkserver.example.com)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.summary_index.inline</td>
<td>Boolean</td>
<td>Determines whether to execute the summary indexing action as part of the scheduled search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>NOTE:</strong> This option is considered only if the summary index action is enabled and is always executed (in other words, if counttype = always).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defaults to true.</td>
</tr>
<tr>
<td>action.summary_index.maxresults</td>
<td>Number</td>
<td>Sets the maximum number of search results sent using alerts. Defaults to 100.</td>
</tr>
<tr>
<td>action.summary_index.maxtime</td>
<td>Number</td>
<td>Valid values are: Integer[m</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.</td>
</tr>
<tr>
<td>action.summary_index.track_alert</td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.summary_index.ttl</td>
<td>Number</td>
<td>Valid values are: Integer[p]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 10p.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td>actions</td>
<td>String</td>
<td>A comma-separated list of actions to enable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example: rss,email</td>
</tr>
<tr>
<td>alert.digest_mode</td>
<td>Boolean</td>
<td>Specifies whether alert actions are applied to the entire result set or on each individual result.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defaults to 1.</td>
</tr>
<tr>
<td>alert.expires</td>
<td>Number</td>
<td>Valid values: [number][time-unit]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sets the period of time to show the alert in the dashboard. Defaults to 24h.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>alert.severity</td>
<td>Enum</td>
<td>Use ([number][time-unit]) to specify a time. For example: (60 = 60) seconds, (1m = 1) minute, (1h = 60) minutes = (1) hour. Sets the alert severity level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid values: (1 \mid 2 \mid 3 \mid 4 \mid 5 \mid 6)</td>
</tr>
<tr>
<td>alert.suppress</td>
<td>Boolean</td>
<td>Indicates whether alert suppression is enabled for this scheduled search.</td>
</tr>
<tr>
<td>alert.suppress.fields</td>
<td>String</td>
<td>Indicates whether alert suppression is enabled for this scheduled search.</td>
</tr>
<tr>
<td>alert.suppress.period</td>
<td>Number</td>
<td>Comma delimited list of fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.</td>
</tr>
<tr>
<td></td>
<td>Number</td>
<td>Valid values: ([number][time-unit])</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifies the suppression period. Only valid if alert.suppress is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use ([number][time-unit]) to specify a time. For example: (60 = 60) seconds, (1m = 1) minute, (1h = 60) minutes = (1) hour.</td>
</tr>
<tr>
<td>alert.track</td>
<td>Enum</td>
<td>Specifies whether to track the actions triggered by this scheduled search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>auto - (Default) determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true - force alert tracking.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false - disable alert tracking for this search.</td>
</tr>
<tr>
<td>alert_comparator</td>
<td>String</td>
<td>One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Used with alert_threshold to trigger alert actions.</td>
</tr>
<tr>
<td>alert.condition</td>
<td>String</td>
<td>Contains a conditional search that is evaluated against the results of the saved search. Defaults to an empty string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alerts are triggered if the specified search yields a non-empty search result list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTE: If you specify an alert.condition, do not set counttype, relation, or quantity.</td>
</tr>
<tr>
<td>alert_threshold</td>
<td>Number</td>
<td>Valid values are: (\text{Integer}[%])</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifies the value to compare (see alert_comparator) before</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>alert_type</td>
<td>String</td>
<td>What to base the alert on, overridden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.</td>
</tr>
</tbody>
</table>
| allow_skew     | 0 | <percentage> | <duration> | Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods. Defaults to 0 (skew disabled). <p>This setting does not require adjusting in most use cases. Check with an admin before making any updates.</p> When set to a non-zero value for searches with the following cron_schedule values, the search scheduler randomly skews the second, minute, and hour on which the search runs. <pre>* * * * * Every minute. */M * * * * Every M minutes (M > 0). 0 * * * * Every hour. 0 */H * * * Every H hours (H > 0). 0 0 * * * Every day (at midnight). When set to a non-zero value for a search that has any other cron_schedule setting, the search scheduler can randomly skew only the second on which the search runs. The amount of skew for a specific search remains constant between edits of the search. A value of 0 disallows skew. 0 is the default setting. **Percentage** <p>&lt;int&gt; followed by % specifies the maximum amount of time to skew as a percentage of the scheduled search period.</p> **Duration** <p>&lt;int&gt;&lt;unit&gt; specifies a maximum duration. The &lt;unit&gt; can be omitted only when the &lt;int&gt; is 0.</p> Valid duration units: <ul> <li>m</li> <li>min</li> <li>minute</li> <li>mins</li> <li>minutes</li> <li>h</li> <li>hr</li> <li>hour</li> </ul>

993
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hrs</td>
<td>String</td>
<td>Wildcard argument that accepts any saved search template argument, such as args.username=foobar when the search is search $username$.</td>
</tr>
<tr>
<td>hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td>d</td>
<td></td>
<td></td>
</tr>
<tr>
<td>day</td>
<td></td>
<td></td>
</tr>
<tr>
<td>days</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

- 100% (for an every-5-minute search) = 5 minutes maximum
- 50% (for an every-minute search) = 30 seconds maximum
- 5m = 5 minutes maximum
- 1h = 1 hour maximum

**auto_summarize**

Indicates whether the scheduler should ensure that the data for this search is automatically summarized. Defaults to 0.

**auto_summarize.command**

A search template that constructs the auto summarization for this search. Defaults to summarize override=partial timespan=$auto_summarize.timespan$ max_summary_size=$auto_summarize.max_summary_size$ max_summary_ratio=$auto_summarize.max_summary_ratio$ max_disabled_buckets=$auto_summarize.max_disabled_buckets$ max_time=$auto_summarize.max_time$ [ $search$ ]

**Caution:** Advanced feature. Do not change unless you understand the architecture of auto summarization of saved searches.

**auto_summarize.cron_schedule**

Cron schedule that probes and generates the summaries for this saved search. The default value, */10 * * * *, corresponds to every ten hours.

**auto_summarize.dispatch.earliest_time**

A time string that specifies the earliest time for summarizing this search. Can be a relative or absolute time.

If this value is an absolute time, use the dispatch.time_format to format the value.

**auto_summarize.dispatch.latest_time**

A time string that specifies the latest time for summarizing this saved search. Can be a relative or absolute time.

If this value is an absolute time, use the dispatch.time_format to format the value.

**auto_summarize.dispatch.time_format**

Defines the time format used to specify the earliest and latest time. Defaults to %FT%T.%Q%:z

**auto_summarize.dispatch.ttl**

Valid values: Integer[p]

Indicates the time to live (in seconds) for the artifacts of the summarization of the scheduled search. Defaults to 60.

**auto_summarize.max_disabled_buckets**

The maximum number of buckets with the suspended summarization before the summarization search is completely stopped, and the summarization of the search is suspended for auto_summarize.suspend_period. Defaults to 2.
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto_summarize.max_summary_ratio</td>
<td>Number</td>
<td>The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket. Defaults to 0.1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: The test is only performed if the summary size is larger than auto_summarize.max_summary_size.</td>
</tr>
<tr>
<td>auto_summarize.max_summary_size</td>
<td>Number</td>
<td>The minimum summary size, in bytes, before testing whether the summarization is helpful.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value, 52428800, is equivalent to 5MB.</td>
</tr>
<tr>
<td>auto_summarize.max_time</td>
<td>Number</td>
<td>Maximum time (in seconds) that the summary search is allowed to run. Defaults to 3600.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: This is an approximate time. The summary search stops at clean bucket boundaries.</td>
</tr>
<tr>
<td>auto_summarize.suspend_period</td>
<td>String</td>
<td>Time specifier indicating when to suspend summarization of this search if the summarization is deemed unhelpful. Defaults to 24h.</td>
</tr>
<tr>
<td>auto_summarize.timespan</td>
<td>String</td>
<td>The list of time ranges that each summarized chunk should span. This comprises the list of available granularity levels for which summaries would be available. Specify a comma delimited list of time specifiers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example a timechart over the last month whose granularity is at the day level should set this to 1d. If you need the same data summarized at the hour level for weekly charts, use: 1h,1d.</td>
</tr>
<tr>
<td>cron_schedule</td>
<td>String</td>
<td>Valid values: cron string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td>Human-readable description of this saved search. Defaults to empty string.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>Indicates if the saved search is enabled. Defaults to 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled saved searches are not visible in Splunk Web.</td>
</tr>
<tr>
<td>dispatch.*</td>
<td>String</td>
<td>Wildcard argument that accepts any dispatch related argument.</td>
</tr>
<tr>
<td>dispatch.buckets</td>
<td>Number</td>
<td>The maximum number of timeline buckets. Defaults to 0.</td>
</tr>
<tr>
<td>dispatch.earliest_time</td>
<td>String</td>
<td>A time string that specifies the earliest time for this search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dispatchindexedRealtime</td>
<td>Boolean</td>
<td>Indicates whether to use indexed-realtime mode when doing real-time searches. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>dispatchindexedRealtimeOffset</td>
<td>Integer</td>
<td>Allows for a per-job override of the [search] indexed_realtime_disk_sync_delay setting in limits.conf. Default for saved searches is &quot;unset&quot;, falling back to limits.conf setting.</td>
</tr>
<tr>
<td>dispatchindexedRealtimeMinSpan</td>
<td>Integer</td>
<td>Allows for a per-job override of the [search] indexed_realtime_default_span setting in limits.conf. Default for saved searches is &quot;unset&quot;, falling back to the limits.conf setting.</td>
</tr>
<tr>
<td>dispatchlatest_time</td>
<td>String</td>
<td>A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>dispatchlookups</td>
<td>Boolean</td>
<td>Enables or disables the lookups for this search. Defaults to 1.</td>
</tr>
<tr>
<td>dispatchmax_count</td>
<td>Number</td>
<td>The maximum number of results before finalizing the search. Defaults to 500000.</td>
</tr>
<tr>
<td>dispatchmax_time</td>
<td>Number</td>
<td>Indicates the maximum amount of time (in seconds) before finalizing the search. Defaults to 0.</td>
</tr>
<tr>
<td>dispatchreduce_freq</td>
<td>Number</td>
<td>Specifies, in seconds, how frequently the MapReduce reduce phase runs on accumulated map values. Defaults to 10.</td>
</tr>
<tr>
<td>dispatchrt_backfill</td>
<td>Boolean</td>
<td>Whether to back fill the real time window for this search. Parameter valid only if this is a real time search. Defaults to 0.</td>
</tr>
<tr>
<td>dispatchrt_maximum_span</td>
<td>Integer</td>
<td>Allows for a per-job override of the [search] indexed_realtime_maximum_span setting in limits.conf. Default for saved searches is &quot;unset&quot;, falling back to limits.conf setting.</td>
</tr>
<tr>
<td>dispatchspawn_process</td>
<td>Boolean</td>
<td>Specifies whether to spawn a new search process when this saved search is executed. Defaults to 1. Searches against indexes must run in a separate process.</td>
</tr>
<tr>
<td>dispatchtime_format</td>
<td>String</td>
<td>A time format string that defines the time format for specifying the earliest and latest time. Defaults to %FT%T.%Q%:z.</td>
</tr>
<tr>
<td>dispatchttl</td>
<td>Number</td>
<td>Valid values: Integer[p]. Defaults to 2p. Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If an action is triggered, the action ttl is used. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to alert_actions.conf.spec.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If the integer is followed by the letter 'p', the ttl is interpreted as a...</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>multiple of the scheduled search period.</td>
<td></td>
</tr>
<tr>
<td>displayview</td>
<td>String</td>
<td>Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Boolean</td>
<td>Whether this search is to be run on a schedule</td>
</tr>
<tr>
<td>is_visible</td>
<td>Boolean</td>
<td>Specifies whether this saved search should be listed in the visible saved search list. Defaults to 1.</td>
</tr>
<tr>
<td>max_concurrent</td>
<td>Number</td>
<td>The maximum number of concurrent instances of this search the scheduler is allowed to run. Defaults to 1.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td><strong>Required.</strong> A name for the search.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>String</td>
<td>Read-only attribute. Value ignored on POST. There are some old clients who still send this value</td>
</tr>
<tr>
<td>qualifiedSearch</td>
<td>String</td>
<td>Read-only attribute. Value ignored on POST. This value is computed during runtime.</td>
</tr>
<tr>
<td>realtime_schedule</td>
<td>Boolean</td>
<td>Controls the way the scheduler computes the next execution time of a scheduled search. Defaults to 1. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).</td>
</tr>
<tr>
<td>request.ui_dispatch_app</td>
<td>String</td>
<td>Specifies a field used by Splunk Web to denote the app this search should be dispatched in.</td>
</tr>
<tr>
<td>request.ui_dispatch_view</td>
<td>String</td>
<td>Specifies a field used by Splunk Web to denote the view this search should be displayed in.</td>
</tr>
<tr>
<td>restart_on_searchpeer_add</td>
<td>Boolean</td>
<td>Specifies whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. Defaults to 1. <strong>Note:</strong> The peer can be a newly added peer or a peer down and now available.</td>
</tr>
<tr>
<td>run_on_startup</td>
<td>Boolean</td>
<td>Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time. Defaults to 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set run_on_startup to true for scheduled searches that populate lookup tables.</td>
</tr>
</tbody>
</table>
### Name | Type | Description
--- | --- | ---
**schedule_window** | Number or **auto** | Time window (in minutes) during which the search has lower priority. Defaults to 0. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. Set to **auto** to let the scheduler determine the optimal window value automatically. Requires the **edit_search_schedule_window** capability to override **auto**.

**search** | String | **Required**. The search to save.

**vsid** | String | Defines the viewstate id associated with the UI view listed in 'displayview'. Must match up to a stanza in viewstates.conf.

### Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.*</td>
<td>* represents any custom action.</td>
</tr>
<tr>
<td>action.email</td>
<td>Indicates the state of the email action.</td>
</tr>
<tr>
<td><strong>action.email.auth_password</strong></td>
<td>The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here and it is encrypted on the next restart. Defaults to empty string.</td>
</tr>
<tr>
<td><strong>action.email.auth_username</strong></td>
<td>The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. <strong>Note</strong>: Your SMTP server might reject unauthenticated emails.</td>
</tr>
<tr>
<td>action.email.bcc</td>
<td>BCC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.cc</td>
<td>CC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td><strong>action.email.command</strong></td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.email.format</td>
<td>Specify the format of text in the email. This value also applies to any attachments.&lt; Valid values: (plain</td>
</tr>
<tr>
<td>action.email.from</td>
<td>Email address from which the email action originates. Defaults to splunk@$LOCALHOST or whatever value is set in alert_actions.conf.</td>
</tr>
<tr>
<td>action.email.hostname</td>
<td>Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunksrv.example.com)</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url.</td>
</tr>
<tr>
<td></td>
<td>When this value begins with 'http://', it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct an externally referencable url, such as SSO environments, other proxies, or when the server hostname is not generally resolvable.</td>
</tr>
<tr>
<td></td>
<td>Defaults to current hostname provided by the operating system, or if that fails &quot;localhost&quot;. When set to empty, default behavior is used.</td>
</tr>
<tr>
<td>action.email.inline</td>
<td>Indicates whether the search results are contained in the body of the email.</td>
</tr>
<tr>
<td></td>
<td>Results can be either inline or attached to an email. See action.email.sendresults.</td>
</tr>
<tr>
<td>action.email.mailserver</td>
<td>Set the address of the MTA server to be used to send the emails.</td>
</tr>
<tr>
<td></td>
<td>Defaults to &lt;LOCALHOST&gt; (or whatever is set in alert_actions.conf).</td>
</tr>
<tr>
<td>action.email.maxresults</td>
<td>Sets the global maximum number of search results to send when email.action is enabled.</td>
</tr>
<tr>
<td>action.email.maxtime</td>
<td>Specifies the maximum amount of time the execution of an email action takes before the action is aborted.</td>
</tr>
<tr>
<td>action.email.pdfview</td>
<td>The name of the view to deliver if sendpdf is enabled</td>
</tr>
<tr>
<td>action.email.preprocess_results</td>
<td>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Initially, preprocessing consists of filtering out unwanted internal fields.</td>
</tr>
<tr>
<td>action.email.reportCIDFontList</td>
<td>Space-separated list. Specifies the set (and load order) of CID fonts for handling Simplified Chinese(gb), Traditional Chinese(cns), Japanese(jp), and Korean(kor) in Integrated PDF Rendering.</td>
</tr>
<tr>
<td></td>
<td>If multiple fonts provide a glyph for a given character code, the glyph from the first font specified in the list is used.</td>
</tr>
<tr>
<td></td>
<td>To skip loading any CID fonts, specify the empty string.</td>
</tr>
<tr>
<td></td>
<td>Default value: &quot;gb cns jp kor&quot;</td>
</tr>
<tr>
<td>action.email.includeSplunkLogo</td>
<td>Indicates whether to include the Splunk logo with the report.</td>
</tr>
<tr>
<td>action.email.reportPaperOrientation</td>
<td>Specifies the paper orientation: portrait or landscape.</td>
</tr>
<tr>
<td>action.email.reportPaperSize</td>
<td>Specifies the paper size for PDFs. Defaults to letter.</td>
</tr>
<tr>
<td></td>
<td>Valid values: (letter</td>
</tr>
<tr>
<td>action.email.reportServerEnabled</td>
<td>Not supported.</td>
</tr>
<tr>
<td>action.email.reportServerURL</td>
<td>Not supported.</td>
</tr>
<tr>
<td>action.email.sendpdf</td>
<td>Indicates whether to create and send the results as a PDF.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.email.sendresults</td>
<td>Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.</td>
</tr>
<tr>
<td>action.email.subject</td>
<td>Specifies an email subject. Defaults to SplunkAlert-&lt;savedsearchname&gt;.</td>
</tr>
<tr>
<td>action.email.to</td>
<td>List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.</td>
</tr>
<tr>
<td>action.email.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.email.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows &lt;Integer&gt;, int is the number of scheduled periods. Defaults to 86400 (24 hours).</td>
</tr>
<tr>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td></td>
<td>Valid values are Integer[p].</td>
</tr>
<tr>
<td>action.email.use_ssl</td>
<td>Indicates whether to use SSL when communicating with the SMTP server.</td>
</tr>
<tr>
<td>action.email.use_tls</td>
<td>Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).</td>
</tr>
<tr>
<td>action.email.width_sort_columns</td>
<td>Indicates whether columns should be sorted from least wide to most wide, left to right. Only valid if format=text.</td>
</tr>
<tr>
<td>action.populate_lookup</td>
<td>Indicates the state of the populate lookup action.</td>
</tr>
<tr>
<td>action.populate_lookup.command</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.populate_lookup.dest</td>
<td>Lookup name of path of the lookup to populate.</td>
</tr>
<tr>
<td>action.populate_lookup.hostname</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.populate_lookup.maxresults</td>
<td>The maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>action.populate_lookup.maxtime</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>Valid values are: Integer[m</td>
<td>s</td>
</tr>
<tr>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, then this specifies the number of scheduled periods. Defaults to 10p.</td>
<td><strong>action.populate_lookup.ttl</strong> If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p]</td>
</tr>
<tr>
<td>Indicates the state of the RSS action.</td>
<td><strong>action.rss</strong> The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) See action.email.hostname for details.</td>
<td><strong>action.rss.hostname</strong> Sets the maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Valid values are Integer[m</td>
<td>s</td>
</tr>
<tr>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 86400 (24 hours).</td>
<td><strong>action.rss.ttl</strong> If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]</td>
</tr>
<tr>
<td>Indicates the state of the script for this action.</td>
<td><strong>action.script</strong> The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td><strong>action.script.command</strong></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>action.script.filename</code></td>
<td>File name of the script to call. Required if script action is enabled</td>
</tr>
</tbody>
</table>
| `action.script.hostname` | Sets the hostname used in the web link (url) sent in alert actions.  
This value accepts two forms:  
hostname (for example, splunkserver, splunkserver.example.com)  
See action.email.hostname for details. |
| `action.script.maxresults` | Sets the maximum number of search results sent using alerts.                                                                                                                                               |
| `action.script.maxtime`  | Sets the maximum amount of time the execution of an action takes before the action is aborted.                                                                                                               |
| `action.script.track_alert` | Indicates whether the execution of this action signifies a trackable alert.                                                                                                                                  |
| `action.script.ttl`      | Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 600 (10 minutes).  
If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.  
Valid values are: Integer[p] |
| `action.summary_index`   | Indicates the state of the summary index.                                                                                                                                                                  |
| `action.summary_index._name` | Specifies the name of the summary index where the results of the scheduled search are saved.  
Defaults to "summary."                                                                                                                        |
| `action.summary_index.command` | The search command (or pipeline) which is responsible for executing the action.  
Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$. |
| `action.summary_index.hostname` | Sets the hostname used in the web link (url) sent in alert actions.  
This value accepts two forms:  
hostname (for example, splunkserver, splunkserver.example.com)  
See action.email.hostname for details. |
<p>| <code>action.summary_index.inline</code> | Determines whether to execute the summary indexing action as part of the scheduled search.                                                                                                                 |
|                          | Note: This option is considered only if the summary index action is enabled and is always executed (in other words, if counttype = always).                                                                     |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.summary_index.maxresults</td>
<td>Sets the maximum number of search results sent using alerts.</td>
</tr>
</tbody>
</table>
| action.summary_index.maxtime             | Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.  

Valid values are: Integer[m|s|h|d]  |
| action.summary_index.track_alert         | Indicates whether the execution of this action signifies a trackable alert.  

 Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 10p.  

If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.  

Valid values are: Integer[p]  |
| actions                                   | Actions triggered by this alert.                                                                                                             |
| alert.digest_mode                         | Indicates if the alert actions are applied to the entire result set or to each individual result.                                             |
| alert.expires                             | Sets the period of time to show the alert in the dashboard. Defaults to 24h.  

Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.  

Valid values: [number][time-unit]  |
| alert.severity                            | Sets the alert severity level.  

Valid values are:  

1 DEBUG  
2 INFO  
3 WARN  
4 ERROR  
5 SEVERE  
6 FATAL  |
| alert.suppress                            | Indicates whether alert suppression is enabled for this schedules search.  |
| alert.suppress.fields                     | Fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.  |
| alert.suppress.period                     | Specifies the suppression period. Only valid if alert.suppress is enabled.  

Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.  |
| alert.track                               | Specifies whether to track the actions triggered by this scheduled search.  

auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions.  

true - force alert tracking.  |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>false</td>
<td>- disable alert tracking for this search.</td>
</tr>
<tr>
<td>alert_comparator</td>
<td>One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc</td>
</tr>
<tr>
<td>alert_condition</td>
<td>A conditional search that is evaluated against the results of the saved search. Defaults to an empty string.</td>
</tr>
<tr>
<td></td>
<td>Alerts are triggered if the specified search yields a non-empty search result list.</td>
</tr>
<tr>
<td></td>
<td>Note: If you specify an alert_condition, do not set counttype, relation, or quantity.</td>
</tr>
<tr>
<td>alert_threshold</td>
<td>Valid values are: Integer[%]</td>
</tr>
<tr>
<td></td>
<td>Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to &quot;rises by perc&quot; or &quot;drops by perc.&quot;</td>
</tr>
<tr>
<td>alert_type</td>
<td>What to base the alert on, overridden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.</td>
</tr>
<tr>
<td>allow skew</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.</td>
</tr>
<tr>
<td></td>
<td>This setting does not require adjusting in most use cases. Check with an admin before making any updates.</td>
</tr>
<tr>
<td></td>
<td>When set to a non-zero value for searches with the following cron_schedule values, the search scheduler randomly skews the second, minute, and hour on which the search runs.</td>
</tr>
<tr>
<td></td>
<td><em>/M</em> * * * * Every M minutes (M &gt; 0).</td>
</tr>
<tr>
<td></td>
<td>0 * * * * Every hour.</td>
</tr>
<tr>
<td></td>
<td>0 <em>/H</em> * * Every H hours (H &gt; 0).</td>
</tr>
<tr>
<td></td>
<td>0 0 * * * Every day (at midnight).</td>
</tr>
<tr>
<td></td>
<td>When set to a non-zero value for a search that has any other cron_schedule setting, the search scheduler can randomly skew only the second on which the search runs.</td>
</tr>
<tr>
<td></td>
<td>The amount of skew for a specific search remains constant between edits of the search.</td>
</tr>
<tr>
<td></td>
<td>A value of 0 disallows skew. 0 is the default setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Percentage</strong>&lt;int&gt; followed by % specifies the maximum amount of time to skew as a percentage of the scheduled search period.</td>
</tr>
<tr>
<td></td>
<td><strong>Duration</strong>&lt;int&gt;&lt;unit&gt; specifies a maximum duration. The &lt;unit&gt; can be omitted only when</td>
</tr>
</tbody>
</table>
the `<int>` is 0 (which disables skew).

Valid duration units:

- m
- min
- minute
- mins
- minutes
- h
- hr
- hour
- hrs
- hours
- d
- day
- days

Examples

100% (for an every-5-minute search) = 5 minutes maximum
50% (for an every-minute search) = 30 seconds maximum
5m = 5 minutes maximum
1h = 1 hour maximum

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>args.*</td>
<td>Wildcard argument that accepts any saved search template argument, such as</td>
</tr>
<tr>
<td></td>
<td><code>args.username=foobar</code> when the search is search <code>$username$</code>.</td>
</tr>
<tr>
<td>auto_summarize</td>
<td>Indicates whether the scheduler should ensure that the data for this search</td>
</tr>
<tr>
<td></td>
<td>is automatically summarized.</td>
</tr>
<tr>
<td>auto_summarize.command</td>
<td>A search template that constructs the auto summarization for this search.</td>
</tr>
<tr>
<td></td>
<td><strong>Caution</strong>: Advanced feature. Do not change unless you understand the</td>
</tr>
<tr>
<td></td>
<td>architecture of auto summarization of saved searches.</td>
</tr>
<tr>
<td>auto_summarize.cron_schedule</td>
<td>Cron schedule that probes and generates the summaries for this saved search.</td>
</tr>
<tr>
<td>auto_summarize.dispatch.earliest_time</td>
<td>A time string that specifies the earliest time for summarizing this search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td>auto_summarize.dispatch.latest_time</td>
<td>A time string that specifies the latest time for this saved search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td>auto_summarize.dispatch.time_format</td>
<td>Time format used to specify the earliest and latest times.</td>
</tr>
<tr>
<td>auto_summarize.dispatch.ttl</td>
<td>Indicates the time to live (in seconds) for the artifacts of the summarization of the scheduled search. If the integer is followed by the letter ‘p’, the ttl is interpreted as a multiple of the scheduled search period.</td>
</tr>
<tr>
<td>auto_summarize.max_disabled_buckets</td>
<td>The maximum number of buckets with the suspended summarization before the summarization search is completely stopped, and the summarization of the search is suspended for <code>auto_summarize.suspend_period</code>.</td>
</tr>
<tr>
<td>auto_summarize.max_summary_ratio</td>
<td>The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The test is only performed if the summary size is larger than</td>
</tr>
<tr>
<td></td>
<td><code>auto_summarize.max_summary_size</code>.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>auto_summarize.max_summary_size</strong></td>
<td>The minimum summary size, in bytes, before testing whether the summarization is helpful.</td>
</tr>
<tr>
<td><strong>auto_summarize.max_time</strong></td>
<td>Maximum time (in seconds) that the summary search is allowed to run.</td>
</tr>
<tr>
<td><strong>auto_summarize.suspend_period</strong></td>
<td>Time specifier indicating when to suspend summarization of this search if the summarization is deemed unhelpful.</td>
</tr>
<tr>
<td><strong>auto_summarize.timespan</strong></td>
<td>The list of time ranges that each summarized chunk should span. This comprises the list of available granularity levels for which summaries would be available. For example a timechart over the last month whose granularity is at the day level should set this to 1d. If you need the same data summarized at the hour level for weekly charts, use: 1h,1d.</td>
</tr>
<tr>
<td><strong>cron_schedule</strong></td>
<td>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes. Cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * <em>, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (</em>/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes. Valid values: cron string</td>
</tr>
<tr>
<td><strong>description</strong></td>
<td>Description of this saved search. Defaults to empty string.</td>
</tr>
<tr>
<td><strong>disabled</strong></td>
<td>Indicates if this saved search is disabled.</td>
</tr>
<tr>
<td><strong>dispatch.</strong>*</td>
<td>* represents any custom dispatch field.</td>
</tr>
<tr>
<td><strong>dispatch.buckets</strong></td>
<td>The maximum number of timeline buckets.</td>
</tr>
<tr>
<td><strong>dispatch.earliest_time</strong></td>
<td>A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td><strong>dispatch.indexedRealtime</strong></td>
<td>Indicates whether to used indexed-realtime mode when doing real-time searches.</td>
</tr>
<tr>
<td><strong>dispatch.latest_time</strong></td>
<td>A time string that specifies the latest time for theaved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td><strong>dispatch.lookups</strong></td>
<td>Indicates if lookups are enabled for this search.</td>
</tr>
<tr>
<td><strong>dispatch.max_count</strong></td>
<td>The maximum number of results before finalizing the search.</td>
</tr>
<tr>
<td><strong>dispatch.max_time</strong></td>
<td>Indicates the maximum amount of time (in seconds) before finalizing the search.</td>
</tr>
<tr>
<td><strong>dispatch.reduce_freq</strong></td>
<td>Specifies how frequently the MapReduce reduce phase runs on accumulated map values.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dispatch.rt_backfill</td>
<td>Indicates whether to back fill the real time window for this search. Parameter valid only if this is a real time search.</td>
</tr>
<tr>
<td>dispatch.spawn_process</td>
<td>Indicates whether a new search process spawns when this saved search is executed.</td>
</tr>
<tr>
<td>dispatch.time_format</td>
<td>Time format string that defines the time format for specifying the earliest and latest time.</td>
</tr>
<tr>
<td>dispatch.ttl</td>
<td>Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered. If an action is triggered, the action ttl is used. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to alert_actions.conf.spec. If the integer is followed by the letter 'p', the ttl is interpreted as a multiple of the scheduled search period.</td>
</tr>
<tr>
<td>displayview</td>
<td>Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Indicates if this search is to be run on a schedule.</td>
</tr>
<tr>
<td>is_visible</td>
<td>Indicates if this saved search appears in the visible saved search list.</td>
</tr>
<tr>
<td>max_concurrent</td>
<td>The maximum number of concurrent instances of this search the scheduler is allowed to run.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>The time when the scheduler runs this search again.</td>
</tr>
<tr>
<td>qualifiedSearch</td>
<td>The exact search string that the scheduler would run.</td>
</tr>
<tr>
<td>realtime_schedule</td>
<td>Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).</td>
</tr>
<tr>
<td>request.ui_dispatch_app</td>
<td>A field used by Splunk Web to denote the app this search should be dispatched in.</td>
</tr>
<tr>
<td>request.ui_dispatch_view</td>
<td>Specifies a field used by Splunk Web to denote the view this search should be displayed in.</td>
</tr>
<tr>
<td>restart_on_searchpeer_add</td>
<td>Indicates whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The peer can be a newly added peer or a peer down and now available.</td>
</tr>
<tr>
<td>run_on_startup</td>
<td>Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time.</td>
</tr>
</tbody>
</table>
Splunk recommends that you set run_on_startup to true for scheduled searches that populate lookup tables.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>schedule_window</td>
<td>Time window (in minutes) during which the search has lower priority. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. If set to auto, the scheduler prioritizes searches automatically.</td>
</tr>
<tr>
<td>search</td>
<td>Search expression to filter the response. The response matches field values against the search expression. For example: search=foo matches any object that has &quot;foo&quot; as a substring in a field. search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example.</td>
</tr>
<tr>
<td>vsid</td>
<td>The viewstate id associated with the UI view listed in 'displayview'. Matches to a stanza in viewstates.conf.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches -d name=MySavedSearch --data-urlencode search="index=_internal source=*metrics.log"

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      <title>savedsearch</title>
      <id>https://localhost:8089/servicesNS/admin/search/saved/searches</id>
      <updated>2011-12-09T09:10:21-08:00</updated>
      <generator version="108769"/>
      <author>
        <name>Splunk</name>
      </author>
      <link href="/servicesNS/admin/search/saved/searches/_new" rel="create"/>
      <link href="/servicesNS/admin/search/saved/searches/_reload" rel="_reload"/>
      <opensearch:totalResults>1</opensearch:totalResults>
      <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
      <opensearch:startIndex>0</opensearch:startIndex>
      <s:messages/>
      <entry>
        <title>MySavedSearch</title>
        <id>https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch</id>
        <updated>2011-12-09T09:10:21-08:00</updated>
        <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="alternate"/>
        <author>
          <name>admin</name>
        </author>
        <!-- opensearch nodes elided for brevity. -->
        <content type="text/xml">
          <s:dict>
            <s:key name="action.email">0</s:key>
            <s:key name="action.email.auth_password">$1$o2rN8S6m+0YB</s:key>
          </s:dict>
        </content>
      </entry>
    </feed>
```
<s:key name="action.email.auth_username">myusername</s:key>
<s:key name="action.email.bcc"></s:key>
<s:key name="action.email.cc"></s:key>
<s:key name="action.email.command"><![CDATA[$action.email.preprocess_results{default=""}]
| sendemail "server=$action.email.mailserver{default=localhost}" 
| "use_ssl=$action.email.use_ssl{default=false}" 
| "use_tls=$action.email.use_tls{default=false}" 
| "to=$action.email.to$" 
| "cc=$action.email.cc$" 
| "bcc=$action.email.bcc$"
"from=$action.email.from{default=splunk@localhost}" 
"subject=$action.email.subject{recurse=yes}" 
"format=$action.email.format{default=csv}" 
"sssummary=Saved Search [$(name$): $counttype$($results.count$)]" 
"ssquery=$search$" 
"ssname=$(name$)" 
"sslink=$results.url$" 
"inline=$action.email.inline{default=False}" 
"sendresults=$action.email.sendresults{default=False}" 
"sendpdf=$action.email.sendpdf{default=False}" 
"pdfview=$action.email.pdfview$" 
"searchid=$search_id$" 
"graceful=$graceful{default=True}" 
maxinputs="action.email.maxresults{default=10000}" 
maxtime="action.email.maxtime{default=5m}"
</s:key>
<s:key name="action.email.format">html</s:key>
<s:key name="action.email.from">splunk</s:key>
<s:key name="action.email.hostname"></s:key>
<s:key name="action.email.inline">0</s:key>
<s:key name="action.email.mailserver">localhost</s:key>
<s:key name="action.email.maxresults">10000</s:key>
<s:key name="action.email.maxtime">5m</s:key>
<s:key name="action.email.pdfview"></s:key>
<s:key name="action.email.preprocess_results"></s:key>
<s:key name="action.email.reportPaperOrientation">portrait</s:key>
<s:key name="action.email.reportPaperSize">letter</s:key>
<s:key name="action.email.reportServerEnabled">1</s/key>
<s:key name="action.email.reportServerURL"></s:key>
<s/key name="action.email.sendpdf">0</s:key>
<s/key name="action.email.sendresults">0</s/key>
<s/key name="action.email.subject">Splunk Alert: $(name$)</s/key>
<s/key name="action.email.to"></s/key>
<s/key name="action.email.track_alert">1</s/key>
<s/key name="action.email.ttl">86400</s/key>
<s/key name="action.email.use_ssl">0</s/key>
<s/key name="action.email.use_tls">0</s/key>
<s/key name="action.populate_lookup">0</s/key>
<s/key name="action.populate_lookup.command">copyresults dest="$(action.populate_lookup.dest$"
| sid="$search_id$"
</s:key>
<s/key name="action.populate_lookup.dest$"
</s/key>
<s/key name="action.populate_lookup.hostname"></s/key>
<s/key name="action.populate_lookup.maxresults">10000</s/key>
<s/key name="action.populate_lookup.maxtime">5m</s/key>
<s/key name="action.populate_lookup.track_alert">0</s/key>
<s/key name="action.populate_lookup.ttl">120</s/key>
<s/key name="action.rss">0</s/key>
<s/key name="action.rss.command">createrss "path=$(name$.xml" 
"name=$(name$)" 
"link=$results.url$" 
"desc=Alert trigger: $(name$), results.count=$results.count$"
maxtime="action.rss.maxtime{default=1m}" 
</s/key>
<s/key name="action.rss.hostname"></s/key>
<s/key name="action.rss.maxresults">10000</s/key>
<s/key name="action.rss.maxtime">1m</s/key>
<s/key name="action.rss.track_alert">0</s/key>
<s/key name="action.rss.ttl">86400</s/key>
<s/key name="action.script">0</s/key>
<s/key name="action.script.command">runshellscript $(action.script.filename$ $results.count$ 
"$search$" "$search$" $(name$)"
"Saved Search \[$name$\] \$counttype\($results.count\)" \$results.url$ \$deprecated_arg$

\$search_id$ \$results.file$  

maxtime="\$action.script.maxtime\(default=5m\)"
</s:key>
<s:key name="action.script.filename"></s:key>
<s:key name="action.script.hostname"></s:key>
<s:key name="action.script.maxresults">10000</s:key>
<s:key name="action.script.maxtime">5m</s:key>
<s:key name="action.script.track_alert">1</s:key>
<s:key name="action.script.ttl">600</s:key>
<s:key name="action.summary_index">0</s:key>
</s:key>
<s:key name="action.summary_index._name">summary</s:key>
<s:key name="action.summary_index.command"><![CDATA[summaryindex spool=t uselb=t addtime=t index="\$action.summary_index._name\(required=yes\)"
file="\$name$\$#random$.stash_new" name="\$name$"
marker="\$action.summary_index\*[format=\$KEY=\"\$VAL\",
key_regex="\$action.summary_index.(?!:\(command|inline|maxresults|maxtime|ttl|track_alert|(?:_.*))\$)(.*)"\]>
</s?key>
<s?key name="action.summary_index.hostname"></s?key>
<s?key name="action.summary_index.inline">1</s?key>
<s?key name="action.summary_index.maxresults">10000</s?key>
<s?key name="action.summary_index.maxtime">5m</s?key>
<s?key name="action.summary_index.track_alert">0</s?key>
<s?key name="action.summary_index.ttl">120</s?key>
<s?key name="alert.digest_mode">1</s?key>
<s?key name="alert.expires">24h</s?key>
<s?key name="alert.severity">3</s?key>
<s?key name="alert.suppress"></s?key>
<s?key name="alert.suppress.fields"></s?key>
<s?key name="alert.suppress.period"></s?key>
<s?key name="alert.type">always</s?key>
<s?key name="alert_threshold"></s?key>
<s?key name="alert_comparator"></s?key>
<s?key name="alert_condition"></s?key>
<s?key name="alert_threshold"></s?key>
<s?key name="alert_type">always</s?key>
<s?key name="alert_type"></s?key>
<s?key name="description"></s?key>
<s?key name="disabled">0</s?key>
<s?key name="dispatch.buckets">0</s?key>
<s?key name="dispatch.earliest_time"></s?key>
<s?key name="dispatch.latest_time"></s?key>
<s?key name="dispatch.lookups">1</s?key>
<s?key name="dispatch.max_count">500000</s?key>
<s?key name="dispatch.max_time">0</s?key>
<s?key name="dispatch.reduce_freq">10</s?key>
<s?key name="dispatch.rt_backfill">0</s?key>
<s?key name="dispatch.spawn_process">1</s?key>
<s?key name="dispatch.time_format">%FT%T.%Q%:z</s?key>
<s?key name="dispatch.ttl">2p</s?key>
<s?key name="displayview"></s?key>
<!-- elided -->
<s?key name="is_scheduled">0</s?key>
<s?key name="is_visible">1</s?key>
<s?key name="max_concurrent">1</s?key>
<s?key name="next_scheduled_time"></s?key>
<s?key name="qualifiedSearch">search index=_internal source=*metrics.log\</s?key>
<s?key name="realtime_schedule"></s?key>
<s?key name="request.ui.dispatch_app"></s?key>
<s?key name="request.ui.dispatch_view"></s?key>
<s?key name="restart_on_searchpeer_add">1</s?key>
<s?key name="run_on_startup">0</s?key>
saved/searches/{name}

https://<host>:<mPort>/services/saved/searches/{name}

Manage the {name} saved search.

DELETE

Delete the named saved search.

Request parameters

None

Returned values

None

Example request and response

curl -k -u admin:pass --request DELETE
https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch

GET

Access the named saved search.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1011
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest_time</td>
<td>If the search is scheduled display scheduled times starting from this time.</td>
</tr>
<tr>
<td>latest_time</td>
<td>If the search is scheduled display scheduled times ending at this time.</td>
</tr>
<tr>
<td>listDefaultActionArgs</td>
<td>Indicates whether to list default actions.</td>
</tr>
<tr>
<td>add_orphan_field</td>
<td>Indicates whether the response includes a boolean value for each saved search to show whether the search is orphaned, meaning that it has no valid owner. When add_orphan_field is set to true, the response includes the orphaned search indicators, either 0 to indicate that a search is not orphaned or 1 to indicate that the search is orphaned. Admins can use this setting to check for searches without valid owners and resolve related issues.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email</td>
<td>Indicates the state of the email action.</td>
</tr>
<tr>
<td>action.email.auth_password</td>
<td>The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here that is encrypted on the next restart. Defaults to empty string.</td>
</tr>
<tr>
<td>action.email.auth_username</td>
<td>The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. Note: Your SMTP server might reject unauthenticated emails.</td>
</tr>
<tr>
<td>action.email.bcc</td>
<td>BCC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.cc</td>
<td>CC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.command</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.email.format</td>
<td>Specify the format of text in the email. This value also applies to any attachments. Valid values: (plain</td>
</tr>
<tr>
<td>action.email.from</td>
<td>Email address from which the email action originates.</td>
</tr>
<tr>
<td>action.email.hostname</td>
<td>Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. When this value begins with 'http://', it is used verbatim. Note: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct an externally referencable url.</td>
</tr>
</tbody>
</table>
such as SSO environments, other proxies, or when the server hostname is not generally resolvable.

Defaults to current hostname provided by the operating system, or if that fails "localhost." When set to empty, default behavior is used.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email.inline</td>
<td>Indicates whether the search results are contained in the body of the email.</td>
</tr>
<tr>
<td></td>
<td>Results can be either inline or attached to an email. See action.email.sendresults.</td>
</tr>
<tr>
<td>action.email.mailserver</td>
<td>Set the address of the MTA server to be used to send the emails.</td>
</tr>
<tr>
<td></td>
<td>Defaults to &lt;LOCALHOST&gt; (or whatever is set in alert_actions.conf).</td>
</tr>
<tr>
<td>action.email.maxresults</td>
<td>Sets the global maximum number of search results to send when email.action is enabled.</td>
</tr>
<tr>
<td>action.email.maxtime</td>
<td>Specifies the maximum amount of time the execution of an email action takes before the action is aborted.</td>
</tr>
<tr>
<td>action.email.preprocess_results</td>
<td>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing).</td>
</tr>
<tr>
<td></td>
<td>Usually the preprocessing consists of filtering out unwanted internal fields.</td>
</tr>
<tr>
<td>action.email.reportPaperOrientation</td>
<td>Specifies the paper orientation: portrait or landscape.</td>
</tr>
<tr>
<td>action.email.reportPaperSize</td>
<td>Specifies the paper size for PDFs. Defaults to letter.</td>
</tr>
<tr>
<td></td>
<td>Valid values: (letter</td>
</tr>
<tr>
<td>action.email.reportServerEnabled</td>
<td>Not supported.</td>
</tr>
<tr>
<td>action.email.reportServerURL</td>
<td>Not supported.</td>
</tr>
<tr>
<td>action.email.sendpdf</td>
<td>Indicates whether to create and send the results as a PDF.</td>
</tr>
<tr>
<td>action.email.sendresults</td>
<td>Indicates whether to attach the search results in the email.</td>
</tr>
<tr>
<td></td>
<td>Results can be either attached or inline. See action.email.inline.</td>
</tr>
<tr>
<td>action.email.subject</td>
<td>Specifies an email subject.</td>
</tr>
<tr>
<td></td>
<td>Defaults to SplunkAlert-&lt;savedsearchname&gt;.</td>
</tr>
<tr>
<td>action.email.to</td>
<td>List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.</td>
</tr>
<tr>
<td>action.email.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.email.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows &lt;integer&gt;, int is the number of scheduled periods. Defaults to 86400 (24 hours).</td>
</tr>
<tr>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td></td>
<td>Valid values are Integer[p].</td>
</tr>
<tr>
<td>action.email.use_ssl</td>
<td>Indicates whether to use SSL when communicating with the SMTP server.</td>
</tr>
<tr>
<td>action.email.use_tls</td>
<td>Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.populate_lookup</td>
<td>The state of the populate lookup action.</td>
</tr>
<tr>
<td>action.populate_lookup.command</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.populate_lookup.hostname</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.populate_lookup.maxresults</td>
<td>The maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>action.populate_lookup.maxtime</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m. Valid values are: Integer[m</td>
</tr>
<tr>
<td>action.populate_lookup.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.populate_lookup.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, then this specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p]</td>
</tr>
<tr>
<td>action.rss</td>
<td>The state of the RSS action.</td>
</tr>
<tr>
<td>action.rss.command</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.rss.hostname</td>
<td>Sets the hostname used in the web link (url) sent in alert actions.</td>
</tr>
<tr>
<td>action.rss.maxresults</td>
<td>Sets the maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>action.rss.maxtime</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 1m.</td>
</tr>
<tr>
<td>action.rss.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.rss.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 86400 (24 hours).</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td>action.script</td>
<td>The state of the script action.</td>
</tr>
<tr>
<td>action.script.command</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.script.hostname</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>)</td>
</tr>
<tr>
<td>action.script.maxresults</td>
<td>The maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>action.script.maxtime</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted.</td>
</tr>
<tr>
<td>action.script.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.script.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 600 (10 minutes). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are: Integer[p]</td>
</tr>
<tr>
<td>action.summary_index</td>
<td>The state of the summary index action.</td>
</tr>
<tr>
<td>action.summary_index._name</td>
<td>Specifies the name of the summary index where the results of the scheduled search are saved. Defaults to &quot;summary.&quot;</td>
</tr>
<tr>
<td>action.summary_index.command</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.summary_index.hostname</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms:</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.summary_index.inline</td>
<td>Determines whether to execute the summary indexing action as part of the scheduled search.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This option is considered only if the summary index action is enabled and is always executed (in other words, if counttype = always).</td>
</tr>
<tr>
<td>action.summary_index.maxresults</td>
<td>Sets the maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>action.summary_index.maxtime</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.</td>
</tr>
<tr>
<td>action.summary_index.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.summary_index.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 10p.</td>
</tr>
<tr>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values are:</strong> Integer[p]</td>
</tr>
<tr>
<td>alert.digest_mode</td>
<td>Specifies whether alert actions are applied to the entire result set or to each individual result.</td>
</tr>
<tr>
<td>alert.expires</td>
<td>Sets the period of time to show the alert in the dashboard. Defaults to 24h.</td>
</tr>
<tr>
<td>alert.severity</td>
<td>Sets the alert severity level.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values are:</strong> 1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL</td>
</tr>
<tr>
<td>alert.suppress</td>
<td>Indicates whether alert suppression is enabled for this schedules search.</td>
</tr>
<tr>
<td>alert.suppress.period</td>
<td>Specifies the suppresion period. Only valid if alert.supress is enabled.</td>
</tr>
<tr>
<td></td>
<td>Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</td>
</tr>
<tr>
<td>alert.track</td>
<td>Specifies whether to track the actions triggered by this scheduled search.</td>
</tr>
<tr>
<td></td>
<td><strong>auto</strong> - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions.</td>
</tr>
<tr>
<td></td>
<td><strong>true</strong> - force alert tracking.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| alert_comparator| One of the following strings:  
                        greater than  
                        less than  
                        equal to  
                        rises by  
                        drops by  
                        rises by perc  
                        drops by perc  
                        Used with alert_threshold to trigger alert actions. |
| alert_condition | A conditional search that is evaluated against the results of the saved search. Defaults to an empty string.  
                        Alerts are triggered if the specified search yields a non-empty search result list. |
| alert_threshold | Valid values are: Integer[%]  
                        Specifies the value to compare (see alert_comparator) before triggering the alert actions.  
                        If expressed as a percentage, indicates value to use when alert_comparator is set to “rises by perc” or “drops by perc.” |
| alert_type      | What to base the alert on, overriden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources. Typically, reports return the “always” value, while alerts can return any other value. |
| allow_skew      | 0 | <percentage> | <duration>  
                        Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.  
                        This setting does not require adjusting in most use cases. Check with an admin before making any updates.  
                        When set to a non-zero value for searches with the following cron_schedule values, the search scheduler randomly skews the second, minute, and hour on which the search runs.  
                        * * * * *     Every minute.  
                        */M * * * *    Every M minutes (M > 0).  
                        0 * * * *     Every hour.  
                        0 */H * * *    Every H hours (H > 0).  
                        0 0 * * *     Every day (at midnight).  
                        When set to a non-zero value for a search that has any other cron_schedule setting, the search scheduler can randomly skew only the second on which the search runs.  
                        The amount of skew for a specific search remains constant between edits of the search.  
                        A value of 0 disallows skew. 0 is the default setting. |
### Percentage

<int> followed by % specifies the maximum amount of time to skew as a percentage of the scheduled search period.

### Duration

<int><unit> specifies a maximum duration. The <unit> can be omitted only when the <int> is 0.

**Valid duration units:**

- m
- min
- minute
- mins
- minutes
- h
- hr
- hour
- hrs
- hours
- d
- day
- days

### Examples

100% (for an every-5-minute search) = 5 minutes maximum
50% (for an every-minute search) = 30 seconds maximum
5m = 5 minutes maximum
1h = 1 hour maximum

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cron_schedule</td>
<td>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes.</td>
</tr>
<tr>
<td>description</td>
<td>Description of this saved search.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this saved search is disabled.</td>
</tr>
<tr>
<td>dispatch.buckets</td>
<td>The maximum number of timeline buckets.</td>
</tr>
<tr>
<td>dispatch.earliest_time</td>
<td>A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dispatch.latest_time</td>
<td>A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>dispatch.lookups</td>
<td>Indicates if lookups are enabled for this search.</td>
</tr>
<tr>
<td>dispatch.max_count</td>
<td>The maximum number of results before finalizing the search.</td>
</tr>
<tr>
<td>dispatch.max_time</td>
<td>Indicates the maximum amount of time (in seconds) before finalizing the search.</td>
</tr>
<tr>
<td>dispatch.reduce_freq</td>
<td>Specifies how frequently the MapReduce reduce phase runs on accumulated map values.</td>
</tr>
<tr>
<td>dispatch.spawn_process</td>
<td>Indicates whether a new search process spawns when this saved search is executed.</td>
</tr>
<tr>
<td>dispatch.time_format</td>
<td>A time format string that defines the time format for specifying the earliest and latest time.</td>
</tr>
<tr>
<td>dispatch.ttl</td>
<td>Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered. If an action is triggered, the action ttl is used. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to alert_actions.conf.spec. If the integer is followed by the letter 'p', the ttl is interpreted as a multiple of the scheduled search period.</td>
</tr>
<tr>
<td>displayview</td>
<td>Defines the default Splunk Web view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.</td>
</tr>
<tr>
<td>earliest_time</td>
<td>For scheduled searches display all the scheduled times starting from this time.</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Indicates if this search is to be run on a schedule.</td>
</tr>
<tr>
<td>is_visible</td>
<td>Indicates if this saved search appears in the visible saved search list.</td>
</tr>
<tr>
<td>latest_time</td>
<td>For scheduled searches display all the scheduled times until this time (not just the next run time).</td>
</tr>
<tr>
<td>listDefaultActionArgs</td>
<td>List default values of actions.*, even though some of the actions may not be specified in the saved search.</td>
</tr>
<tr>
<td>max_concurrent</td>
<td>The maximum number of concurrent instances of this search the scheduler is allowed to run.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>The time when the scheduler runs this search again.</td>
</tr>
<tr>
<td>orphan</td>
<td>If the add_orphan_field parameter is passed in with the GET request, this field indicates whether the search is orphaned.</td>
</tr>
<tr>
<td>qualifiedSearch</td>
<td>The exact search command for this saved search.</td>
</tr>
<tr>
<td>realtime_schedule</td>
<td>Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. See the POST parameter for this attribute for details.</td>
</tr>
<tr>
<td>request.ui_dispatch_app</td>
<td>A field used by Splunk Web to denote the app this search should be dispatched in.</td>
</tr>
<tr>
<td>request.ui_dispatch_view</td>
<td>Specifies a field used by Splunk Web to denote the view this search should be displayed in.</td>
</tr>
<tr>
<td>restart_on_searchpeer_add</td>
<td>Indicates whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>run_on_startup</td>
<td>Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time.</td>
</tr>
<tr>
<td></td>
<td>Set run_on_startup to true for scheduled searches that populate lookup tables.</td>
</tr>
<tr>
<td>schedule_priority</td>
<td>One of the following values.</td>
</tr>
<tr>
<td></td>
<td>[ default</td>
</tr>
<tr>
<td></td>
<td>Raises the scheduling priority of the named search.</td>
</tr>
<tr>
<td></td>
<td>default</td>
</tr>
<tr>
<td></td>
<td>higher</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>highest</td>
</tr>
<tr>
<td></td>
<td>The high-to-low priority order (where RTSS = real-time-scheduled search, CSS = continuous-scheduled search, d = default, h = higher, H = highest) is:</td>
</tr>
<tr>
<td></td>
<td>RTSS(H) &gt; CSS(H) &gt; RTSS(h) &gt; RTSS(d) &gt; CSS(h) &gt; CSS(d)</td>
</tr>
<tr>
<td></td>
<td>Requires the search owner to have the edit_search_schedule_priority capability in order to make non-default settings.</td>
</tr>
<tr>
<td></td>
<td>Defaults to default.</td>
</tr>
<tr>
<td></td>
<td>For more details, see savedsearches.conf.spec.</td>
</tr>
<tr>
<td>schedule_window</td>
<td>Time window (in minutes) during which the search has lower priority. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period.</td>
</tr>
<tr>
<td></td>
<td>If set to auto, the scheduler determines the optimal time window automatically.</td>
</tr>
<tr>
<td>search</td>
<td>Search expression to filter the response. The response matches field values against the search expression. For example:</td>
</tr>
<tr>
<td></td>
<td>search=foo matches any object that has &quot;foo&quot; as a substring in a field. search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example.</td>
</tr>
<tr>
<td>vsid</td>
<td>Defines the viewstate id associated with the UI view listed in 'displayview'.</td>
</tr>
<tr>
<td></td>
<td>Must match up to a stanza in viewstates.conf.</td>
</tr>
</tbody>
</table>

**Example request and response**
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch

<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:s="http://dev.splunk.com/ns/rest">
  <title>savedsearch</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/searches</id>
  <updated>2011-07-13T11:57:54-07:00</updated>
  <generator version="102824"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/searches/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/searches/_reload" rel="_reload"/>
  <!-- opensearch nodes elided for brevity. -->
  <s:messages/>
  <entry>
    <title>MySavedSearch</title>
    <id>https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch</id>
    <updated>2011-07-13T11:57:54-07:00</updated>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="list"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/edit" rel="edit"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/remove" rel="remove"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/move" rel="move"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/disable" rel="disable"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/dispatch" rel="dispatch"/>
    <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/history" rel="history"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">0</s:key>
        <s:key name="action.email.auth_password"/>
        <s:key name="action.email.auth_username"/>
        <s:key name="action.email.bcc"/>
        <s:key name="action.email.cc"/>
        <s:key name="action.email.command">
          <![CDATA[
            $sendemail "server=$action.email.mailserver{default=localhost}$" "use_ssl=$action.email.use_ssl{default=false}$" "use_tls=$action.email.use_tls{default=false}$" "to=$action.email.to$" "cc=$action.email.cc$" "bcc=$action.email.bcc$" "from=$action.email.from{default=splunk@localhost}$" "subject=$action.email.subject{recurse=yes}$" "format=$action.email.format{default=csv}$" "assummary=Saved Search [$name$]: $counttypes$($results, count$)
          "sslurl=$results.url$" "ssquery=$search$" "ssname=$name$" "inline=$action.email.inline{default=False}$" "sendresults=$action.email.sendresults{default=False}$" "sendpdf=$action.email.sendpdf{default=False}$" "pdfview=$action.email.pdfview$" "searchid=$search_id$" "graceful=$graceful{default=True}$" maxinputs="$action.email.maxresults{default=10000}$" maxtime="$action.email.maxtime{default=5m}$"
          ]]>"/>
      </s:dict>
    </content>
  </entry>
</feed>
<s:key name="action.email.from">splunk</s:key>
<s:key name="action.email.hostname"/>
<s:key name="action.email.inline">0</s:key>
<s:key name="action.email.mailserver">localhost</s:key>
<s:key name="action.email.maxresults">10000</s:key>
<s:key name="action.email.maxtime">5m</s:key>
<s:key name="action.email.preprocess_results"/>
<s:key name="action.email.reportPaperOrientation">portrait</s:key>
<s:key name="action.email.reportPaperSize">letter</s:key>
<s:key name="action.email.sendpdf">0</s:key>
<s:key name="action.email.sendresults">0</s:key>
<s:key name="action.email.subject">Splunk Alert: $name$</s:key>
<s:key name="action.email.to"/>
<s:key name="action.email.track_alert">1</s:key>
<s:key name="action.email.ttl">86400</s:key>
<s:key name="action.email.use_ssl">0</s:key>
<s:key name="action.email.use_tls">0</s:key>
<s:key name="action.populate_lookup">0</s:key>
<s:key name="action.populate_lookup.command">
  copyresults dest="$action.populate_lookup.command" sid="$search_id$"
</s:key>
<s:key name="action.populate_lookup.hostname"/>
<s:key name="action.populate_lookup.maxresults">10000</s:key>
<s:key name="action.populate_lookup.maxtime">5m</s:key>
<s:key name="action.populate_lookup.track_alert">0</s:key>
<s:key name="action.populate_lookup.ttl">120</s:key>
<s:key name="action.rss">0</s:key>
<s:key name="action.rss.command">
  createrss "path=$name$.xml" "name=$name$" "link=$results.url$" "descr=Alert trigger: $name$, results.count=$results.count$ " "count=30" "graceful=$graceful{default=1}$" maxtime="$action.rss.maxtime{default=1m}$"
</s:key>
<s:key name="action.rss.hostname"/>
<s:key name="action.rss.maxresults">10000</s:key>
<s:key name="action.rss.maxtime">1m</s:key>
<s:key name="action.rss.track_alert">0</s:key>
<s:key name="action.script">0</s:key>
<s:key name="action.script.command">
  runshellscript "$action.script.filename$" "$results.count$" "$search$" "$search$" "$name$" "$results.url$" "$deprecated_arg$" "$search_id$" maxtime="$action.script.maxtime{default=5m}$"
</s:key>
<s:key name="action.script.hostname"/>
<s:key name="action.script.maxresults">10000</s:key>
<s:key name="action.script.maxtime">5m</s:key>
<s:key name="action.script.track_alert">1</s:key>
<s:key name="action.summary_index">0</s:key>
<s:key name="action.summary_index._name">summary</s:key>
<s:key name="action.summary_index.command">
  <![CDATA[summaryindex spool=t uselb=t addtime=t index="$action.summary_index._name{required=yes}$" file="$names_$#random$.stash_new" name="$name$" marker="$action.summary_index{format=SKEY="\"$VAL\\\"", key_regex="action.summary_index.(?!:\$command|inline|maxresults|maxtime|ttl|track_alert|(?:.*))$|\{.*\}|\{.*\})$|\{.*\})$]"]>
</s:key>
<s:key name="action.summary_index.hostname"/>
<s:item>action.populate_lookup.command</s:item>
<s:item>action.populate_lookup.hostname</s:item>
<s:item>action.populate_lookup.maxresults</s:item>
<s:item>action.populate_lookup.maxtime</s:item>
<s:item>action.populate_lookup.track_alert</s:item>
<s:item>action.populate_lookup.ttl</s:item>
<s:item>action.rss.command</s:item>
<s:item>action.rss.hostname</s:item>
<s:item>action.rss.maxresults</s:item>
<s:item>action.rss.maxtime</s:item>
<s:item>action.rss.track_alert</s:item>
<s:item>action.rss.ttl</s:item>
<s:item>action.script.command</s:item>
<s:item>action.script.hostname</s:item>
<s:item>action.script.maxresults</s:item>
<s:item>action.script.maxtime</s:item>
<s:item>action.script.track_alert</s:item>
<s:item>action.script.ttl</s:item>
<s:item>action.summary_index._name</s:item>
<s:item>action.summary_index.command</s:item>
<s:item>action.summary_index.hostname</s:item>
<s:item>action.summary_index.inline</s:item>
<s:item>action.summary_index.maxresults</s:item>
<s:item>action.summary_index.maxtime</s:item>
<s:item>action.summary_index.track_alert</s:item>
<s:item>action.summary_index.ttl</s:item>
<s:item>alert.digest_mode</s:item>
<s:item>alert.expires</s:item>
<s:item>alert.severity</s:item>
<s:item>alert.suppress</s:item>
<s:item>alert.suppress.period</s:item>
<s:item>alert.track</s:item>
<s:item>alert_comparator</s:item>
<s:item>alert_condition</s:item>
<s:item>alert_threshold</s:item>
<s:item>alert_type</s:item>
<s:item>cron_schedule</s:item>
<s:item>description</s:item>
<s:item>disabled</s:item>
<s:item>dispatch.buckets</s:item>
<s:item>dispatch.earliest_time</s:item>
<s:item>dispatch.latest_time</s:item>
<s:item>dispatch.lookups</s:item>
<s:item>dispatch.max_count</s:item>
<s:item>dispatch.max_time</s:item>
<s:item>dispatch.reduce_freq</s:item>
<s:item>dispatch.spawn_process</s:item>
<s:item>dispatch.time_format</s:item>
<s:item>dispatch.ttl</s:item>
<s:item>displayview</s:item>
<s:item>is_scheduled</s:item>
<s:item>is_visible</s:item>
<s:item>max_concurrent</s:item>
<s:item>next_scheduled_time</s:item>
<s:item>qualifiedSearch</s:item>
<s:item>realtime_schedule</s:item>
<s:item>request.ui_dispatch_app</s:item>
<s:item>request.ui_dispatch_view</s:item>
Update the named saved search.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.&lt;action_name&gt;</td>
<td>Boolean</td>
<td>Enable or disable an alert action.&lt;action_name&gt; can be one of the following. [ email</td>
</tr>
<tr>
<td>action.&lt;action_name&gt;.&lt;parameter&gt;</td>
<td></td>
<td>Use this syntax to configure action parameters. See the following parameters for the [ email</td>
</tr>
<tr>
<td>action.email</td>
<td>Boolean</td>
<td>The state of the email action. Read-only attribute. Value ignored on POST. Use actions to specify a list of enabled actions. Defaults to 0.</td>
</tr>
<tr>
<td>action.email.auth_password</td>
<td>String</td>
<td>The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here and it is encrypted on the next restart.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defaults to empty string.</td>
</tr>
<tr>
<td>action.email.auth_username</td>
<td>String</td>
<td>The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.</td>
</tr>
<tr>
<td><strong>Note</strong>: The SMTP server for the Splunk deployment instance might reject unauthenticated emails.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>action.email.bcc</td>
<td>String</td>
<td>BCC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.cc</td>
<td>String</td>
<td>CC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.command</td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.email.format</td>
<td>Enum</td>
<td>Valid values: (plain</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specify the format of text in the email. This value also applies to any attachments.</td>
</tr>
<tr>
<td>action.email.from</td>
<td>String</td>
<td>Email address from which the email action originates.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defaults to splunk@$LOCALHOST or the value set in alert_actions.conf.</td>
</tr>
<tr>
<td>action.email.hostname</td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in email actions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This value accepts two forms:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>hostname (for example, splunkserver, splunkserver.example.com)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When this value begins with &quot;http://&quot;, it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct an externally referencable url, such as SSO environments, other proxies, or when the server hostname is not generally resolvable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defaults to current hostname provided by the operating system, or if that fails &quot;localhost&quot;. When set to empty, default behavior is used.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.email.inline</td>
<td>Boolean</td>
<td>Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.</td>
</tr>
<tr>
<td>action.email.mailserver</td>
<td>String</td>
<td>Set the address of the MTA server to be used to send the emails. Defaults to &lt;LOCALHOST&gt; (or whatever is set in alert_actions.conf).</td>
</tr>
<tr>
<td>action.email.maxresults</td>
<td>Number</td>
<td>Sets the global maximum number of search results to send when email.action is enabled. Defaults to 100.</td>
</tr>
<tr>
<td>action.email.maxtime</td>
<td>Number</td>
<td>Valid values are Integer[m</td>
</tr>
<tr>
<td>action.email.pdfview</td>
<td>String</td>
<td>The name of the view to deliver if sendpdf is enabled</td>
</tr>
<tr>
<td>action.email.preprocess_results</td>
<td>String</td>
<td>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.</td>
</tr>
<tr>
<td>action.email.reportCIDFontList</td>
<td>Enum</td>
<td>Space-separated list. Specifies the set (and load order) of CID fonts for handling Simplified Chinese(gb), Traditional Chinese(cns), Japanese(jp), and Korean(kor) in Integrated PDF Rendering. If multiple fonts provide a glyph for a given character code, the glyph from the first font specified in the list is used. To skip loading any CID fonts, specify the empty string. Defaults to “gb cns jp kor”</td>
</tr>
<tr>
<td>action.email.reportIncludeSplunkLogo</td>
<td>Boolean</td>
<td>Indicates whether to include the Splunk logo with the report.</td>
</tr>
<tr>
<td>action.email.reportPaperOrientation</td>
<td>Enum</td>
<td>Valid values: (portrait</td>
</tr>
<tr>
<td>action.email.reportPaperSize</td>
<td>Enum</td>
<td>Valid values: (letter</td>
</tr>
<tr>
<td>action.email.reportServerEnabled</td>
<td>Boolean</td>
<td>Not supported.</td>
</tr>
<tr>
<td>action.email.reportServerURL</td>
<td>String</td>
<td>Not supported. For a default locally installed report server, the URL is <a href="http://localhost:8091/">http://localhost:8091/</a></td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.email.sendpdf</td>
<td>Boolean</td>
<td>Indicates whether to create and send the results as a PDF. Defaults to false.</td>
</tr>
<tr>
<td>action.email.sendresults</td>
<td>Boolean</td>
<td>Indicates whether to attach the search results in the email.</td>
</tr>
<tr>
<td>action.email.subject</td>
<td>String</td>
<td>Specifies an alternate email subject. Defaults to SplunkAlert-&lt;savedsearchname&gt;.</td>
</tr>
<tr>
<td>action.email.to</td>
<td>String</td>
<td>A comma or semicolon separated list of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.</td>
</tr>
<tr>
<td>action.email.track_alert</td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.email.ttl</td>
<td>Number</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows &lt;Integer&gt;, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td>action.email.use_ssl</td>
<td>Boolean</td>
<td>Indicates whether to use SSL when communicating with the SMTP server. Defaults to false.</td>
</tr>
<tr>
<td>action.email.use_tls</td>
<td>Boolean</td>
<td>Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls). Defaults to false.</td>
</tr>
<tr>
<td>action.email.width_sort_columns</td>
<td>Boolean</td>
<td>Indicates whether columns should be sorted from least wide to most wide, left to right. Only valid if format=text.</td>
</tr>
<tr>
<td>action.populate_lookup</td>
<td>Boolean</td>
<td>The state of the populate lookup action. Read-only attribute. Value ignored on POST. Use actions to specify a list of enabled actions. Defaults to 0.</td>
</tr>
<tr>
<td>action.populate_lookup.command</td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.populate_lookup.dest</td>
<td>String</td>
<td>Lookup name of path of the lookup to populate</td>
</tr>
<tr>
<td>action.populate_lookup.hostname</td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com)</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>action.populate_lookup.maxresults</strong></td>
<td>Number</td>
<td>Sets the maximum number of search results sent using alerts. Defaults to 100.</td>
</tr>
<tr>
<td><strong>action.populate_lookup.maxtime</strong></td>
<td>Number</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m.</td>
</tr>
<tr>
<td><strong>action.populate_lookup.track_alert</strong></td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td><strong>action.populate_lookup.ttl</strong></td>
<td>Number</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, then this specifies the number of scheduled periods. Defaults to 10p.</td>
</tr>
<tr>
<td><strong>action.rss</strong></td>
<td>Boolean</td>
<td>The state of the rss action. Read-only attribute. Value ignored on POST. Use actions to specify a list of enabled actions. Defaults to 0.</td>
</tr>
<tr>
<td><strong>action.rss.command</strong></td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td><strong>action.rss.hostname</strong></td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>)</td>
</tr>
<tr>
<td><strong>action.rss.maxresults</strong></td>
<td>Number</td>
<td>Sets the maximum number of search results sent using alerts. Defaults to 100.</td>
</tr>
<tr>
<td><strong>action.rss.maxtime</strong></td>
<td>Number</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 1m.</td>
</tr>
<tr>
<td><strong>action.rss.track_alert</strong></td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td><strong>action.rss.ttl</strong></td>
<td>Number</td>
<td>Valid values are: Integer[p]</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 86400 (24 hours).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td>action.script</td>
<td>Boolean</td>
<td>The state of the script action. Read-only attribute. Value ignored on POST. Use actions to specify a list of enabled actions. Defaults to 0.</td>
</tr>
<tr>
<td>action.script.command</td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.script.filename</td>
<td>String</td>
<td>File name of the script to call. Required if script action is enabled.</td>
</tr>
<tr>
<td>action.script.hostname</td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in alert actions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This value accepts two forms: hostame (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.script.maxresults</td>
<td>Number</td>
<td>Sets the maximum number of search results sent using alerts. Defaults to 100.</td>
</tr>
<tr>
<td>action.script.maxtime</td>
<td>Number</td>
<td>Valid values are: Integer[m</td>
</tr>
<tr>
<td>action.script.track_alert</td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.script.ttl</td>
<td>Number</td>
<td>Valid values are: Integer[p] Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 600 (10 minutes).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td>action.summary_index</td>
<td>Boolean</td>
<td>The state of the summary index action. Read-only attribute. Value ignored on POST. Use actions to specify a list of enabled actions. Defaults to 0.</td>
</tr>
<tr>
<td>action.summary_index._name</td>
<td>String</td>
<td>Specifies the name of the summary index where the results of the scheduled search are saved.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>---------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.summary_index.command</td>
<td>String</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.summary_index.hostname</td>
<td>String</td>
<td>Sets the hostname used in the web link (url) sent in summary-index alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.summary_index.inline</td>
<td>Boolean</td>
<td>Determines whether to execute the summary indexing action as part of the scheduled search. Defaults to true.</td>
</tr>
<tr>
<td>action.summary_index.maxresults</td>
<td>Number</td>
<td>Sets the maximum number of search results sent using alerts. Defaults to 100.</td>
</tr>
<tr>
<td>action.summary_index.maxtime</td>
<td>Number</td>
<td>Valid values are: Integer[m</td>
</tr>
<tr>
<td>action.summary_index.track_alert</td>
<td>Boolean</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.summary_index.ttl</td>
<td>Number</td>
<td>Valid values are: Integer[p] Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td>actions</td>
<td>String</td>
<td>A comma-separated list of actions to enable. For example: rss,email</td>
</tr>
<tr>
<td>alert.digest_mode</td>
<td>Boolean</td>
<td>Specifies whether alert actions are applied to the entire result set or on each individual result.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>alert.expires</td>
<td>Number</td>
<td>Sets the period of time to show the alert in the dashboard. Defaults to 24h.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid values: [number][time-unit]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</td>
</tr>
<tr>
<td>alert.severity</td>
<td>Enum</td>
<td>Sets the alert severity level. Valid values are: 1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL</td>
</tr>
<tr>
<td>alert.suppress</td>
<td>Boolean</td>
<td>Indicates whether alert suppression is enabled for this scheduled search.</td>
</tr>
<tr>
<td>alert.suppress.fields</td>
<td>String</td>
<td>Comma delimited list of fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.</td>
</tr>
<tr>
<td>alert.suppress.period</td>
<td>Number</td>
<td>Specifies the suppression period. Only valid if alert.suppress is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid values: [number][time-unit]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</td>
</tr>
<tr>
<td>alert.track</td>
<td>Enum</td>
<td>Specifies whether to track the actions triggered by this scheduled search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Valid values: (true</td>
</tr>
<tr>
<td></td>
<td></td>
<td>auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions. Default value.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>true - force alert tracking.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>false - disable alert tracking for this search.</td>
</tr>
<tr>
<td>alert_comparator</td>
<td>String</td>
<td>One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc</td>
</tr>
<tr>
<td>alert_condition</td>
<td>String</td>
<td>Contains a conditional search that is evaluated against the results of the saved search. Defaults to an empty string.</td>
</tr>
</tbody>
</table>
Alerts are triggered if the specified search yields a non-empty search result list.

NOTE: If you specify an alert_condition, do not set counttype, relation, or quantity.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert_threshold</td>
<td>Number</td>
<td>Valid values are: Integer[%] Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to &quot;rises by perc&quot; or &quot;drops by perc.&quot;</td>
</tr>
<tr>
<td>alert_type</td>
<td>String</td>
<td>What to base the alert on, overridden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.</td>
</tr>
<tr>
<td>allow_skew</td>
<td>0</td>
<td>Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods. This setting does not require adjusting in most use cases. Check with an admin before making any updates. When set to a non-zero value for searches with the following cron_schedule values, the search scheduler randomly skews the second, minute, and hour on which the search runs.</td>
</tr>
<tr>
<td></td>
<td>&lt;percentage&gt;</td>
<td>Percentage &lt;int&gt; followed by % specifies the maximum amount of time to skew as a percentage of the scheduled search period. Percentage &lt;int&gt; specifies a maximum duration. The &lt;unit&gt; can be omitted only when the &lt;int&gt; is 0. Valid duration units:</td>
</tr>
<tr>
<td></td>
<td>&lt;duration&gt;</td>
<td>Duration &lt;int&gt;&lt;unit&gt; specifies a maximum duration. The &lt;unit&gt; can be omitted only when the &lt;int&gt; is 0. Valid duration units:</td>
</tr>
</tbody>
</table>
### Examples

100% (for an every-5-minute search) = 5 minutes maximum
50% (for an every-minute search) = 30 seconds maximum
5m = 5 minutes maximum
1h = 1 hour maximum

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>args.*</td>
<td>String</td>
<td>Wildcard argument that accepts any saved search template argument, such as <code>args.username=foobar</code> when the search is <code>search $username$</code>.</td>
</tr>
<tr>
<td>auto_summarize</td>
<td>Boolean</td>
<td>Indicates whether the scheduler should ensure that the data for this search is automatically summarized. Defaults to 0.</td>
</tr>
<tr>
<td>auto_summarize.command</td>
<td>String</td>
<td>An auto summarization template for this search. See auto summarization options in <code>savedsearches.conf</code> for more details.</td>
</tr>
<tr>
<td>auto_summarize.cron_schedule</td>
<td>String</td>
<td>Cron schedule that probes and generates the summaries for this saved search. The default value is <code>*/10 * * * *</code> and corresponds to &quot;every ten hours&quot;.</td>
</tr>
<tr>
<td>auto_summarize.dispatch.earliest_time</td>
<td>String</td>
<td>A time string that specifies the earliest time for summarizing this search. Can be a relative or absolute time. If this value is an absolute time, use the <code>dispatch.time_format</code> to format the value.</td>
</tr>
<tr>
<td>auto_summarize.dispatch.latest_time</td>
<td>String</td>
<td>A time string that specifies the latest time for summarizing this saved search. Can be a relative or absolute time. If this value is an absolute time, use the <code>dispatch.time_format</code> to format the value.</td>
</tr>
<tr>
<td>auto_summarize.dispatch.time_format</td>
<td>String</td>
<td>Defines the time format that Splunk software uses to specify the earliest and latest time. Defaults to <code>%F %T %.Q %z</code>.</td>
</tr>
<tr>
<td>auto_summarize.dispatch.ttl</td>
<td>String</td>
<td>Valid values: Integer[p]. Defaults to 60. Indicates the time to live (in seconds) for the artifacts of the summarization of the scheduled search.</td>
</tr>
<tr>
<td>auto_summarize.max_disabled_buckets</td>
<td>Number</td>
<td>The maximum number of buckets with the suspended summarization before the summarization search is completely stopped, and the summarization of the search is suspended for <code>auto_summarize.suspend_period</code>. Defaults to 2.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>auto_summarize.max_summary_ratio</td>
<td>Number</td>
<td>The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket. Defaults to 0.1.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Note</em>: The test is only performed if the summary size is larger than auto_summarize.max_summary_size.</td>
</tr>
<tr>
<td>auto_summarize.max_summary_size</td>
<td>Number</td>
<td>The minimum summary size, in bytes, before testing whether the summarization is helpful.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The default value is 52428800 and is equivalent to 5MB.</td>
</tr>
<tr>
<td>auto_summarize.max_time</td>
<td>Number</td>
<td>Maximum time (in seconds) that the summary search is allowed to run. Defaults to 3600.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><em>Note</em>: This is an approximate time. The summary search stops at clean bucket boundaries.</td>
</tr>
<tr>
<td>auto_summarize.suspend_period</td>
<td>String</td>
<td>Time specifier indicating when to suspend summarization of this search if the summarization is deemed unhelpful. Defaults to 24h.</td>
</tr>
<tr>
<td>auto_summarize.timespan</td>
<td>String</td>
<td>The list of time ranges that each summarized chunk should span. This comprises the list of available granularity levels for which summaries would be available. Specify a comma delimited list of time specifiers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example a timechart over the last month whose granularity is at the day level should set this to 1d. If you need the same data summarized at the hour level for weekly charts, use: 1h,1d.</td>
</tr>
<tr>
<td>cron_schedule</td>
<td>String</td>
<td>Valid values: cron string</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td>Human-readable description of this saved search. Defaults to empty string.</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>Indicates if the saved search is enabled. Defaults to 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Disabled saved searches are not visible in Splunk Web.</td>
</tr>
<tr>
<td>dispatch.*</td>
<td>String</td>
<td>Wildcard argument that accepts any dispatch related argument.</td>
</tr>
<tr>
<td>dispatch.buckets</td>
<td>Number</td>
<td>The maximum number of timeline buckets. Defaults to 0.</td>
</tr>
<tr>
<td>dispatch.earliest_time</td>
<td>String</td>
<td>A time string that specifies the earliest time for this search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dispatch.indexedRealtime</td>
<td>Boolean</td>
<td>Indicates whether to used indexed-realtime mode when doing real-time searches.</td>
</tr>
<tr>
<td>dispatch.indexedRealtimeOffset</td>
<td>Integer</td>
<td>Allows for a per-job override of the [search] indexed_realtime_disk_sync_delay setting in limits.conf. Default for saved searches is &quot;unset&quot;, falling back to limits.conf setting.</td>
</tr>
<tr>
<td>dispatch.indexedRealtimeMinSpan</td>
<td>Integer</td>
<td>Allows for a per-job override of the [search] indexed_realtime_default_span setting in limits.conf. Default for saved searches is &quot;unset&quot;, falling back to the limits.conf setting.</td>
</tr>
<tr>
<td>dispatch.latest_time</td>
<td>String</td>
<td>A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>dispatch.lookups</td>
<td>Boolean</td>
<td>Enables or disables the lookups for this search. Defaults to 1.</td>
</tr>
<tr>
<td>dispatch.max_count</td>
<td>Number</td>
<td>The maximum number of results before finalizing the search. Defaults to 500000.</td>
</tr>
<tr>
<td>dispatch.max_time</td>
<td>Number</td>
<td>Indicates the maximum amount of time (in seconds) before finalizing the search. Defaults to 0.</td>
</tr>
<tr>
<td>dispatch.reduce_freq</td>
<td>Number</td>
<td>Specifies, in seconds, how frequently the MapReduce reduce phase runs on accumulated map values. Defaults to 10.</td>
</tr>
<tr>
<td>dispatch.rt_backfill</td>
<td>Boolean</td>
<td>Whether to back fill the real time window for this search. Parameter valid only if this is a real time search. Defaults to 0.</td>
</tr>
<tr>
<td>dispatch.rt_maximum_span</td>
<td>Integer</td>
<td>Allows for a per-job override of the [search] indexed_realtime_maximum_span setting in limits.conf. Default for saved searches is &quot;unset&quot;, falling back to the limits.conf setting.</td>
</tr>
<tr>
<td>dispatch.spawn_process</td>
<td>Boolean</td>
<td>Specifies whether a new search process spawns when this saved search is executed. Defaults to 1.</td>
</tr>
<tr>
<td>dispatch.time_format</td>
<td>String</td>
<td>A time format string that defines the time format for specifying the earliest and latest time. Defaults to %FT%T.%Q%:z</td>
</tr>
<tr>
<td>dispatch.ttl</td>
<td>Number</td>
<td>Valid values: Integer[p]. Defaults to 2p.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If an action is triggered, the ttl changes to that action ttl. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to alert_actions.conf.spec.</td>
</tr>
</tbody>
</table>
If the integer is followed by the letter ‘p’, the ttl is handled as a multiple of the scheduled search period.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>displayview</td>
<td>String</td>
<td>Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Boolean</td>
<td>Whether this search is to be run on a schedule</td>
</tr>
<tr>
<td>is_visible</td>
<td>Boolean</td>
<td>Specifies whether this saved search should be listed in the visible saved search list. Defaults to 1.</td>
</tr>
<tr>
<td>max_concurrent</td>
<td>Number</td>
<td>The maximum number of concurrent instances of this search the scheduler is allowed to run. Defaults to 1.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td><strong>Required.</strong> Search name.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>String</td>
<td>Read-only attribute. Value ignored on POST. There are some old clients who still send this value</td>
</tr>
<tr>
<td>qualifiedSearch</td>
<td>String</td>
<td>Read-only attribute. Value ignored on POST. The value is computed during runtime.</td>
</tr>
<tr>
<td>realtime_schedule</td>
<td>Boolean</td>
<td>Defaults to 1. Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).</td>
</tr>
<tr>
<td>request.ui_dispatch_app</td>
<td>String</td>
<td>Specifies a field used by Splunk Web to denote the app this search should be dispatched in.</td>
</tr>
<tr>
<td>request.ui_dispatch_view</td>
<td>String</td>
<td>Specifies a field used by Splunk Web to denote the view this search should be displayed in.</td>
</tr>
<tr>
<td>restart_on_searchpeer_add</td>
<td>Boolean</td>
<td>Specifies whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. Defaults to 1. <strong>Note:</strong> The peer can be a newly added peer or a peer down and now available.</td>
</tr>
<tr>
<td>run_on_startup</td>
<td>Boolean</td>
<td>Indicates whether this search runs at startup. If it does not run on startup, it runs at the next scheduled time. Defaults to 0.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Set to 1 for scheduled searches that populate lookup tables.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>schedule_window</td>
<td>Number or auto</td>
<td>Time window (in minutes) during which the search has lower priority. Defaults to 0. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. Set to auto to let the scheduler determine the optimal window value automatically. Requires the edit_search_schedule_window capability to override auto.</td>
</tr>
<tr>
<td>search</td>
<td>String</td>
<td>Required. The search to save.</td>
</tr>
<tr>
<td>schedule_priority</td>
<td>See description</td>
<td>Raises the scheduling priority of the named search. Use one of the following options.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>default: No scheduling priority increase.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>higher: Scheduling priority is higher than other searches of the same scheduling tier.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>While there are four tiers of priority for scheduled searches, only the following search types are affected by this property.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>real-time scheduled (realtime_schedule=1).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>continuous scheduled (realtime_schedule=0).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>highest: Scheduling priority is higher than other searches regardless of scheduling tier. However, real-time-scheduled searches with priority = highest always have priority over continuous scheduled searches with priority = highest.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requires the search owner to have the edit_search_schedule_priority capability in order to make non-default settings.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defaults to default.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For more details, see savedsearches.conf.spec.</td>
</tr>
<tr>
<td>vsid</td>
<td>String</td>
<td>Defines the viewstate id associated with the UI view listed in 'displayview'.</td>
</tr>
<tr>
<td>workload_pool</td>
<td>String</td>
<td>Specifies the new workload pool where the existing running search will be placed.</td>
</tr>
</tbody>
</table>

## Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.*</td>
<td>* represents any custom action.</td>
</tr>
<tr>
<td>action.email</td>
<td>Indicates the state of the email action.</td>
</tr>
<tr>
<td>action.email.auth_password</td>
<td>The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here that is encrypted on the next restart.</td>
</tr>
<tr>
<td></td>
<td>Defaults to empty string.</td>
</tr>
</tbody>
</table>

1038
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| action.email.auth_username | The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. 

*Note:* Your SMTP server might reject unauthenticated emails. |
| action.email.bcc   | BCC email address to use if action.email is enabled.                                                                                                                                                           |
| action.email.cc   | CC email address to use if action.email is enabled.                                                                                                                                                             |
| action.email.command | The search command (or pipeline) which is responsible for executing the action. 

Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$. |
| action.email.format | Specify the format of text in the email. This value also applies to any attachments. 

Valid values: (plain | html | raw | csv) |
| action.email.from | Email address from which the email action originates. 

Defaults to splunk@$LOCALHOST or whatever value is set in alert_actions.conf. |
| action.email.hostname | Sets the hostname used in the web link (url) sent in email actions. 

This value accepts two forms: 

hostname (for example, splunkserver, splunkserver.example.com) 


When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url. 

When this value begins with 'http://', it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct an externally referencable url, such as SSO environments, other proxies, or when the server hostname is not generally resolvable. 

Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used. |
| action.email.inline | Indicates whether the search results are contained in the body of the email. 

Results can be either inline or attached to an email. See action.email.sendresults. |
| action.email.mailserver | Set the address of the MTA server to be used to send the emails. 

Defaults to &lt;LOCALHOST&gt; (or whatever is set in alert_actions.conf). |
A conditional search that is evaluated against the results of the saved search. Defaults to an empty string.

Alerts are triggered if the specified search yields a non-empty search result list.

**Note:** If you specify an alert_condition, do not set counttype, relation, or quantity.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email.maxtime</td>
<td>Specifies the maximum amount of time the execution of an email action takes before the action is aborted.</td>
</tr>
<tr>
<td>action.email.pdfview</td>
<td>The name of the view to deliver if sendpdf is enabled</td>
</tr>
<tr>
<td>action.email.preprocess_results</td>
<td>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.</td>
</tr>
<tr>
<td>action.email.reportCIDFontList</td>
<td>Space-separated list. Specifies the set (and load order) of CID fonts for handling Simplified Chinese(gb), Traditional Chinese(cns), Japanese(jp), and Korean(kor) in Integrated PDF Rendering. If multiple fonts provide a glyph for a given character code, the glyph from the first font specified in the list is used. To skip loading any CID fonts, specify the empty string. Default value: &quot;gb cns jp kor&quot;</td>
</tr>
<tr>
<td>action.email.reportIncludeSplunkLogo</td>
<td>Indicates whether to include the Splunk logo with the report.</td>
</tr>
<tr>
<td>action.email.reportPaperOrientation</td>
<td>Specifies the paper orientation: portrait or landscape.</td>
</tr>
<tr>
<td>action.email.reportPaperSize</td>
<td>Specifies the paper size for PDFs. Defaults to letter. Valid values: (letter</td>
</tr>
<tr>
<td>action.email.reportServerEnabled</td>
<td>Not supported.</td>
</tr>
<tr>
<td>action.email.reportServerURL</td>
<td>Not supported.</td>
</tr>
<tr>
<td>action.email.sendpdf</td>
<td>Indicates whether to create and send the results as a PDF.</td>
</tr>
<tr>
<td>action.email.sendresults</td>
<td>Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.</td>
</tr>
<tr>
<td>action.email.subject</td>
<td>Specifies an email subject. Defaults to SplunkAlert-&lt;savedsearchname&gt;.</td>
</tr>
<tr>
<td>action.email.to</td>
<td>List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.</td>
</tr>
<tr>
<td>action.email.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.email.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows &lt;Integer&gt;, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td><strong>Name</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.email.use_ssl</td>
<td>Indicates whether to use SSL when communicating with the SMTP server.</td>
</tr>
<tr>
<td>action.email.use_tls</td>
<td>Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).</td>
</tr>
<tr>
<td>action.email.width_sort_columns</td>
<td>Indicates whether columns should be sorted from least wide to most wide, left to right. Only valid if format=text.</td>
</tr>
<tr>
<td>action.populate_lookup</td>
<td>Indicates the state of the populate lookup action.</td>
</tr>
<tr>
<td>action.populate_lookup.command</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.populate_lookup.dest</td>
<td>Lookup name of path of the lookup to populate.</td>
</tr>
<tr>
<td>action.populate_lookup.hostname</td>
<td>Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>) See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.populate_lookup.maxresults</td>
<td>The maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>action.populate_lookup.maxtime</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.populate_lookup.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.populate_lookup.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, then this specifies the number of scheduled periods. Defaults to 10p. If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p]</td>
</tr>
<tr>
<td>action.rss</td>
<td>Indicates the state of the RSS action.</td>
</tr>
<tr>
<td>action.rss.command</td>
<td>The search command (or pipeline) which is responsible for executing the action.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.rss.hostname</td>
<td>Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td></td>
<td>Sets the hostname used in the web link (url) sent in alert actions.</td>
</tr>
<tr>
<td></td>
<td>This value accepts two forms:</td>
</tr>
<tr>
<td></td>
<td>hostname (for example, splunkserver, splunkserver.example.com)</td>
</tr>
<tr>
<td></td>
<td>See action.email.hostname for details.</td>
</tr>
<tr>
<td>action.rss.maxresults</td>
<td>Sets the maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>action.rss.maxtime</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 1m.</td>
</tr>
<tr>
<td>action.rss.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.rss.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 86400 (24 hours).</td>
</tr>
<tr>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td></td>
<td>Valid values are: Integer[p]</td>
</tr>
<tr>
<td>action.script</td>
<td>Indicates the state of the script for this action.</td>
</tr>
<tr>
<td>action.script.command</td>
<td>The search command (or pipeline) which is responsible for executing the action.</td>
</tr>
<tr>
<td></td>
<td>Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.script.filename</td>
<td>File name of the script to call. Required if script action is enabled</td>
</tr>
<tr>
<td></td>
<td>Sets the hostname used in the web link (url) sent in alert actions.</td>
</tr>
<tr>
<td></td>
<td>This value accepts two forms:</td>
</tr>
<tr>
<td></td>
<td>hostname (for example, splunkserver, splunkserver.example.com)</td>
</tr>
<tr>
<td></td>
<td>See action.email.hostname for details.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.script.maxresults</td>
<td>Sets the maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>action.script.maxtime</td>
<td>Sets the maximum amount of time the execution of an action takes before the action is aborted.</td>
</tr>
<tr>
<td>action.script.track_alert</td>
<td>Specifies the name of the summary index where the results of the scheduled search are saved.</td>
</tr>
<tr>
<td></td>
<td>Defaults to &quot;summary.&quot;</td>
</tr>
<tr>
<td>action.script.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 600 (10 minutes).</td>
</tr>
<tr>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td></td>
<td>Valid values are: Integer[p]</td>
</tr>
<tr>
<td>action.summary_index</td>
<td>Indicates the state of the summary index.</td>
</tr>
<tr>
<td>action.summary_index._name</td>
<td>Specifies the name of the summary index where the results of the scheduled search are saved.</td>
</tr>
<tr>
<td></td>
<td>Defaults to &quot;summary.&quot;</td>
</tr>
<tr>
<td>action.summary_index.command</td>
<td>The search command (or pipeline) which is responsible for executing the action.</td>
</tr>
</tbody>
</table>
|                           | Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.

action.summary_index.hostname | Sets the hostname used in the web link (url) sent in alert actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com)
| See action.email.hostname for details. |
| action.summary_index.inline | Determines whether to execute the summary indexing action as part of the scheduled search. Note: This option is considered only if the summary index action is enabled and is always executed (in other words, if counttype = always). |
| action.summary_index.maxresults | Sets the maximum number of search results sent using alerts. |
| action.summary_index.maxtime | Sets the maximum amount of time the execution of an action takes before the action is aborted. Defaults to 5m. Valid values are: Integer[m|s|h|d] |
| action.summary_index.track_alert | Indicates whether the execution of this action signifies a trackable alert. |
| action.summary_index.ttl  | Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows Integer, specifies the number of scheduled periods. Defaults to 10p. |

1043
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>actions</td>
<td>Actions to enable.</td>
</tr>
<tr>
<td>alert.digest_mode</td>
<td>Indicates if alert actions apply to the entire result set or to each individual result.</td>
</tr>
<tr>
<td>alert.expires</td>
<td>Sets the period of time to show the alert in the dashboard. Defaults to 24h. Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour. Valid values: [number][time-unit]</td>
</tr>
<tr>
<td>alert.severity</td>
<td>Valid values: (1</td>
</tr>
<tr>
<td>alert.suppress</td>
<td>Indicates whether alert suppression is enabled for this schedules search.</td>
</tr>
<tr>
<td>alert.suppress.fields</td>
<td>Fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.</td>
</tr>
<tr>
<td>alert.suppress.period</td>
<td>Specifies the suppression period. Only valid if alert.suppress is enabled. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</td>
</tr>
<tr>
<td>alert.track</td>
<td>Specifies whether to track the actions triggered by this scheduled search. auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions. true - force alert tracking. false - disable alert tracking for this search.</td>
</tr>
<tr>
<td>alert_comparator</td>
<td>One of the following strings: greater than, less than, equal to, rises by, drops by, rises by perc, drops by perc Used with alert_threshold to trigger alert actions.</td>
</tr>
<tr>
<td>alert_condition</td>
<td>A conditional search that is evaluated against the results of the saved search. Defaults to an empty string.</td>
</tr>
</tbody>
</table>
### Name | Description
--- | ---
| **alert_threshold** | Alerts are triggered if the specified search yields a non-empty search result list. 
*Note:* If you specify an alert_condition, do not set counttype, relation, or quantity.
Valid values are: Integer[%]
Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to "rises by perc" or "drops by perc."
| **alert_type** | What to base the alert on, overridden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.
| **allow skew** | 0 | <percentage> | <duration>
Allows the search scheduler to distribute scheduled searches randomly and more evenly over their specified search periods.
This setting does not require adjusting in most use cases. Check with an admin before making any updates.
When set to a non-zero value for searches with the following cron_schedule values, the search scheduler randomly skews the second, minute, and hour on which the search runs.

```
* * * * *     Every minute.
*/M * * * *   Every M minutes (M > 0).
0 * * * *     Every hour.
0 */H * * *   Every H hours (H > 0).
0 0 * * *     Every day (at midnight).
```

When set to a non-zero value for a search that has any other cron_schedule setting, the search scheduler can randomly skew only the second on which the search runs.
The amount of skew for a specific search remains constant between edits of the search.
A value of 0 disallows skew. 0 is the default setting.

**Percentage**

<int> followed by % specifies the maximum amount of time to skew as a percentage of the scheduled search period.

**Duration**

<int><unit> specifies a maximum duration. The <unit> can be omitted only when the <int> is 0.
Valid duration units:

- m
- min
- minute

---

1045
### Examples

- 100% (for an every-5-minute search) = 5 minutes maximum
- 50% (for an every-minute search) = 30 seconds maximum
- 5m = 5 minutes maximum
- 1h = 1 hour maximum

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>args.*</code></td>
<td>Wildcard argument that accepts any saved search template argument, such as <code>args.username=foobar</code> when the search is <code>search $username$</code>.</td>
</tr>
<tr>
<td><code>auto_summarize</code></td>
<td>Indicates whether the scheduler should ensure that the data for this search is automatically summarized.</td>
</tr>
<tr>
<td><code>auto_summarize.command</code></td>
<td>An auto summarization template for this search.</td>
</tr>
<tr>
<td><code>auto_summarize.cron_schedule</code></td>
<td>Cron schedule that probes and generates the summaries for this saved search. The default value corresponds to every ten hours.</td>
</tr>
<tr>
<td><code>auto_summarize.dispatch.earliest_time</code></td>
<td>A time string that specifies the earliest time for summarizing this search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td><code>auto_summarize.dispatch.latest_time</code></td>
<td>A time string that specifies the latest time for this saved search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td><code>auto_summarize.dispatch.time_format</code></td>
<td>Defines the time format for specifying earliest and latest time.</td>
</tr>
<tr>
<td><code>auto_summarize.dispatch.ttl</code></td>
<td>Indicates the time to live (in seconds) for the artifacts of the summarization of the scheduled search. If the integer is followed by the letter ‘p’, the ttl is interpreted as a multiple of the scheduled search period.</td>
</tr>
<tr>
<td><code>auto_summarize.max_disabled_buckets</code></td>
<td>The maximum number of buckets with the suspended summarization before the summarization search is completely stopped, and the summarization of the search is suspended for <code>auto_summarize.suspend_period</code>.</td>
</tr>
<tr>
<td><code>auto_summarize.max_summary_ratio</code></td>
<td>The maximum ratio of summary_size/bucket_size, which specifies when to stop summarization and deem it unhelpful for a bucket. <strong>Note:</strong> The test is only performed if the summary size is larger than <code>auto_summarize.max_summary_size</code>.</td>
</tr>
<tr>
<td><code>auto_summarize.max_summary_size</code></td>
<td>The minimum summary size, in bytes, before testing whether the summarization is helpful.</td>
</tr>
<tr>
<td><code>auto_summarize.max_time</code></td>
<td>Maximum time (in seconds) that the summary search is allowed to run. <strong>Note:</strong> This is an approximate time. The summary search stops at clean bucket boundaries.</td>
</tr>
<tr>
<td><code>auto_summarize.suspend_period</code></td>
<td>Time specifier indicating when to suspend summarization of this search if the summarization is deemed unhelpful.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>auto_summarize.timespan</td>
<td>The list of time ranges that each summarized chunk should span. This comprises the list of available granularity levels for which summaries would be available. For example a timechart over the last month whose granularity is at the day level should set this to 1d. If you need the same data summarized at the hour level for weekly charts, use: 1h,1d.</td>
</tr>
<tr>
<td>cron_schedule</td>
<td>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes.</td>
</tr>
<tr>
<td>description</td>
<td>Description of this saved search.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the saved search is disabled.</td>
</tr>
<tr>
<td>dispatch.*</td>
<td>* represents any custom dispatch field.</td>
</tr>
<tr>
<td>dispatch.buckets</td>
<td>The maximum number of timeline buckets.</td>
</tr>
<tr>
<td>dispatch.earliest_time</td>
<td>A time string that specifies the earliest time for this search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td>dispatch.indexedRealtime</td>
<td>Indicates whether to used indexed-realtime mode when doing real-time searches.</td>
</tr>
<tr>
<td>dispatch.latest_time</td>
<td>A time string that specifies the latest time for this saved search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td>dispatch.lookups</td>
<td>Indicates if lookups are enabled for this search.</td>
</tr>
<tr>
<td>dispatch.max_count</td>
<td>The maximum number of results before finalizing the search.</td>
</tr>
<tr>
<td>dispatch.max_time</td>
<td>Indicates the maximum amount of time (in seconds) before finalizing the search.</td>
</tr>
<tr>
<td>dispatch.reduce_freq</td>
<td>Specifies how frequently the MapReduce reduce phase runs on accumulated map values.</td>
</tr>
<tr>
<td>dispatch.rt_backfill</td>
<td>Indicates whether to back fill the real time window for this search. Parameter valid only if this is a real time search.</td>
</tr>
<tr>
<td>dispatch.spawn_process</td>
<td>Indicates whether a new search process spawns when this saved search is executed.</td>
</tr>
<tr>
<td>dispatch.time_format</td>
<td>Time format string that defines the time format for specifying the earliest and latest time.</td>
</tr>
<tr>
<td>dispatch.ttl</td>
<td></td>
</tr>
</tbody>
</table>
Indicates the time to live (in seconds) for the artifacts of the scheduled search, if no actions are triggered.

If an action is triggered, the action ttl is used. If multiple actions are triggered, the maximum ttl is applied to the artifacts. To set the action ttl, refer to `alert_actions.conf.spec`.

If the integer is followed by the letter 'p', the ttl is interpreted as a multiple of the scheduled search period.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>displayview</td>
<td>Defines the default UI view name (not label) in which to load the results. Accessibility is subject to the user having sufficient permissions.</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Indicates if this search is to be run on a schedule.</td>
</tr>
<tr>
<td>is_visible</td>
<td>Indicates if this saved search appears in the visible saved search list.</td>
</tr>
<tr>
<td>max_concurrent</td>
<td>The maximum number of concurrent instances of this search the scheduler is allowed to run.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>The time when the scheduler runs this search again.</td>
</tr>
<tr>
<td>qualifiedSearch</td>
<td>The exact search command for this saved search.</td>
</tr>
<tr>
<td>realtime_schedule</td>
<td>Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).</td>
</tr>
<tr>
<td>request.ui_dispatch_app</td>
<td>A field used by Splunk Web to denote the app this search should be dispatched in.</td>
</tr>
<tr>
<td>request.ui_dispatch_view</td>
<td>Specifies a field used by Splunk Web to denote the view this search should be displayed in.</td>
</tr>
<tr>
<td>restart_on_searchpeer_add</td>
<td>Indicates whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. Note: The peer can be a newly added peer or a peer down and now available.</td>
</tr>
<tr>
<td>run_on_startup</td>
<td>Indicates whether this search on startup. If it does not run on startup, it runs at the next scheduled time. Splunk recommends that you set run_on_startup to true for scheduled searches that populate lookup tables.</td>
</tr>
<tr>
<td>schedule_window</td>
<td>Time window (in minutes) during which the search has lower priority. The scheduler can give higher priority to more critical searches during this window. The window must be smaller than the search period. If set to auto, the scheduler determines the optimal time window automatically. Defaults to 0.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>search</td>
<td>Search expression to filter the response. The response matches field values against the search expression. For example: search=foo matches any object that has “foo” as a substring in a field. search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example.</td>
</tr>
<tr>
<td>vsid</td>
<td>Defines the viewstate id associated with the UI view listed in ‘displayview’. Must match up to a stanza in viewstates.conf.</td>
</tr>
</tbody>
</table>

**Example request and response**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch -d actions=email -d action.email.to="nobody@example.com, info@example.com" -d search="my search here"

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
     <title>savedsearch</title>
     <id>https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch</id>
     <updated>2011-07-26T18:20:14-04:00</updated>
     <generator version="104601"/>
     <author>
       <name>Splunk</name>
     </author>
     <link href="/servicesNS/admin/search/saved/searches/_new" rel="create"/>
     <link href="/servicesNS/admin/search/saved/searches/_reload" rel="_reload"/>
     <opensearch:totalResults>1</opensearch:totalResults>
     <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
     <opensearch:startIndex>0</opensearch:startIndex>
     <s:messages/>
     <entry>
       <title>MySavedSearch</title>
       <id>https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch</id>
       <updated>2011-07-26T18:20:14-04:00</updated>
       <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="alternate"/>
       <author>
         <name>admin</name>
       </author>
       <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="list"/>
       <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/_reload" rel="_reload"/>
       <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="edit"/>
       <link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="remove"/>
       <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/move" rel="move"/>
       <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/disable" rel="disable"/>
       <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/dispatch" rel="dispatch"/>
       <link href="/servicesNS/admin/search/saved/searches/MySavedSearch/history" rel="history"/>
       <content type="text/xml">
         <s:dict>
           <s:key name="action.email">1</s:key>
           <s:key name="action.email.auth_password"></s:key>
           <s:key name="action.email.auth_username"></s:key>
           <s:key name="action.email.bcc"></s:key>
         </s:dict>
       </content>
     </entry>
</feed>
saved/searches/{name}/acknowledge

https://<host>:<mPort>/services/saved/searches/{name}/acknowledge

Acknowledge the {name} saved search alert suppression.

POST

Acknowledge the {name} saved search alert suppression and resume alerting.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>key</td>
<td>String</td>
<td></td>
<td>The suppression key used in field-based suppression. For example, in host-based suppression, with data from 5 hosts, the key is the host, as each host could have different suppression expiration times.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MyAlert/acknowledge -X POST

<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/saved/searches/_new" rel="create"/>
<link href="/servicesNS/admin/search/saved/searches/_reload" rel="_reload"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<a:messages/>
</feed>

saved/searches/{name}/dispatch

https://<host>:<mPort>/services/saved/searches/{name}/dispatch

Dispatch the {name} saved search.
POST

Dispatch the `{name}` saved search.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>args.*</code></td>
<td>String</td>
<td></td>
<td>Arg values to create a saved search is the saved search is a template search. For example, specify arg.index_name to create the following search: search index=$args.index_name$</td>
</tr>
<tr>
<td><code>dispatchAs</code></td>
<td>String</td>
<td>&quot;owner&quot;</td>
<td>Indicate the user context, quota, and access rights for the saved search. The saved search runs according to the context indicated.</td>
</tr>
<tr>
<td><code>dispatch.*</code></td>
<td>String</td>
<td></td>
<td>Any dispatch.* field of the search that needs to be overridden when running the summary search.</td>
</tr>
<tr>
<td><code>dispatch.adhoc_search_level</code></td>
<td>String</td>
<td></td>
<td>Use one of the following search modes. [ verbose</td>
</tr>
<tr>
<td><code>dispatch.now</code></td>
<td>Boolean</td>
<td></td>
<td>Dispatch the search as if the specified time for this parameter was the current time.</td>
</tr>
<tr>
<td><code>force_dispatch</code></td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to start a new search even if another instance of this search is already running.</td>
</tr>
<tr>
<td><code>now</code></td>
<td>String</td>
<td></td>
<td>[Deprecated] Use <code>dispatch.now</code>.</td>
</tr>
<tr>
<td><code>replay_speed</code></td>
<td>Number</td>
<td>greater than 0</td>
<td>Indicate a real-time search replay speed factor. For example, 1 indicates normal speed. 0.5 indicates half of normal speed, and 2 indicates twice as fast as normal. earliest_time and latest_time arguments must indicate a real-time time range to use replay options.</td>
</tr>
<tr>
<td><code>replay_et</code></td>
<td>Time modifier string</td>
<td></td>
<td>Relative &quot;wall clock&quot; start time for the replay.</td>
</tr>
<tr>
<td><code>replay_lt</code></td>
<td>Time modifier string</td>
<td></td>
<td>Relative end time for the replay clock. The replay stops when clock time reaches this time.</td>
</tr>
<tr>
<td><code>trigger_actions</code></td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to trigger alert actions.</td>
</tr>
</tbody>
</table>

Returned values

1053
Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch/dispatch
   -d trigger_actions=1

**XML Response**

```xml
<?xml version='1.0' encoding='UTF-8'?>
<response><sid>admin__admin__search__MySavedSearch_at_1311797437_d831d980832e3e89</sid></response>
```

**saved/searches/{name}/history**

https://<host>:<mPort>/services/saved/searches/{name}/history

List available search jobs created from the `{name}` saved search.

**GET**

List available search jobs created from the `{name}` saved search.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| savedsearch | String triplet consisting of user:app:search_name. The triplet constitutes a unique identifier for accessing saved search history. Passing in this parameter can help you work around saved search access limitations in search head clustered deployments.  
As an example, the following parameter triplet represents an admin user, the search app context, and a search named Splunk errors last 24 hours.  
savedsearch=admin:search:Splunk%20errors%20last%2024%20hours |

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest_time</td>
<td>The earliest time a search job is configured to start.</td>
</tr>
<tr>
<td>isDone</td>
<td>Indicates if the search has completed.</td>
</tr>
<tr>
<td>isFinalized</td>
<td>Indicates if the search was finalized (stopped before completion).</td>
</tr>
<tr>
<td>isRealTimeSearch</td>
<td>Indicates if the search is a real time search.</td>
</tr>
<tr>
<td>isSaved</td>
<td>Indicates if the search is saved indefinitely.</td>
</tr>
<tr>
<td>isScheduled</td>
<td>Indicates if the search is a scheduled search.</td>
</tr>
<tr>
<td>isZombie</td>
<td>Indicates if the process running the search is dead, but with the search not finished.</td>
</tr>
<tr>
<td>latest_time</td>
<td>The latest time a search job is configured to start.</td>
</tr>
<tr>
<td>listDefaultActionArgs</td>
<td>List default values of actions.*, even though some of the actions may not be specified in the saved search.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>ttl</td>
<td>The time to live, or time before the search job expires after it completes.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch/history
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:a9="http://a9.com/-/spec/opensearch/1.1/">
  <title>MySavedSearch</title>
  <id>https://localhost:8089/servicesNS/admin/search/saved/searches</id>
  <updated>2011-07-26T18:13:20-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/saved/searches/_new" rel="create"/>
  <link href="/servicesNS/admin/search/saved/searches/_reload" rel="_reload"/>
  <opensearch:totalResults>2</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>scheduler__admin__search_MySavedSearch_at_1311718380_4270ba99c46128d2</title>
    <id>https://localhost:8089/servicesNS/nobody/search/search/jobs/scheduler__admin__search_MySavedSearch_at_1311718380_4270ba99c46128d2</id>
    <updated>2011-07-26T18:13:18-04:00</updated>
    <link href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_MySavedSearch_at_1311718380_4270ba99c46128d2" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <published>2011-07-26T18:13:01-04:00</published>
    <link href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_MySavedSearch_at_1311718380_4270ba99c46128d2/ _reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_MySavedSearch_at_1311718380_4270ba99c46128d2/ _remove" rel="remove"/>
    <content type="text/xml">
      <!-- eai:acl elided -->
      <s:dict>
        <s:dict>
          <s:Add name="isDone">1</s:Add>
          <s:Add name="isFinalized">0</s:Add>
          <s:Add name="isRealTimeSearch">0</s:Add>
          <s:Add name="isSaved">0</s:Add>
        </s:dict>
      </s:dict>
    </content>
  </entry>
</feed>
```
saved/searches/{name}/reschedule

https://<host>:<mPort>/services/saved/searches/{name}/reschedule

Set {name} scheduled saved search to start at a specific time and then run on its schedule thereafter.

**POST**

Define a new start time for a scheduled saved search.

**Usage details**

If no `schedule_time` argument is specified, the Splunk software runs the search as soon as possible according to its saved search definition. If you restart your Splunk platform implementation, all `schedule_time` values for searches are removed.
Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>schedule_time</td>
<td>Timestamp</td>
<td></td>
<td>The next time to run the search. The timestamp can be in one of three formats: ISO8601 format (adjusted for UTC time), UNIX time format, or relative time format.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass
https://localhost:8089/services/saved/searches/Purchased%20products%2C%20last%2024%20hours/reschedule -d
schedule_time=schedule_time=2018-08-15T14:11:01-08:00

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
  xmlns:s="http://dev.splunk.com/ns/rest"
  xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
><title>savedsearch</title>
<br><id>https://localhost:8089/services/saved/searches</id>
<br><updated>2018-08-15T14:11:01-08:00</updated>
<br><generator build="131547" version="5.0"/>
<br><author>
  <name>Splunk</name>
</author>
<br><link href="/services/saved/searches/_new" rel="create"/>
<br><link href="/services/saved/searches/_reload" rel="_reload"/>
<br><opensearch:totalResults>0</opensearch:totalResults>
<br><opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<br><opensearch:startIndex>0</opensearch:startIndex>
<br><s:messages/>
</feed>

saved/searches/{name}/scheduled_times

https://<host>:<mPort>/services/saved/searches/{name}/scheduled_times
Get the {name} saved search scheduled time.

GET

Access {name} saved search scheduled time.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest_time</td>
<td>String</td>
<td></td>
<td>Absolute or relative earliest time</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>--------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>latest_time</td>
<td>String</td>
<td>Absolute or relative latest time</td>
<td></td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email</td>
<td>Indicates the state of the email action.</td>
</tr>
<tr>
<td>action.email.auth_password</td>
<td>The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here that is encrypted on the next platform restart. Defaults to empty string.</td>
</tr>
<tr>
<td>action.email.auth_username</td>
<td>The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. Note: Your SMTP server might reject unauthenticated emails.</td>
</tr>
<tr>
<td>action.email.pdfview</td>
<td>The name of the view to deliver if sendpdf is enabled.</td>
</tr>
<tr>
<td>action.email.subject</td>
<td>Specifies an email subject. Defaults to SplunkAlert-&lt;savedsearchname&gt;.</td>
</tr>
<tr>
<td>action.email.to</td>
<td>List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.</td>
</tr>
<tr>
<td>action.summary_index</td>
<td>The state of the summary index action.</td>
</tr>
<tr>
<td>action.summary_index._name</td>
<td>The state of the summary index action.</td>
</tr>
<tr>
<td>actions</td>
<td>Actions triggered by this alert.</td>
</tr>
<tr>
<td>alert.digest_mode</td>
<td>Indicates if alert actions are applied to the entire result set or to each individual result.</td>
</tr>
<tr>
<td>alert.expires</td>
<td>Sets the period of time to show the alert in the dashboard. Defaults to 24h. Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</td>
</tr>
<tr>
<td>alert.severity</td>
<td>Valid values: (1</td>
</tr>
<tr>
<td></td>
<td>Sets the alert severity level.</td>
</tr>
<tr>
<td></td>
<td>Valid values are:</td>
</tr>
<tr>
<td></td>
<td>1 DEBUG 2 INFO 3 WARN 4 ERROR 5 SEVERE 6 FATAL</td>
</tr>
<tr>
<td>alert.suppress</td>
<td>Indicates whether alert suppression is enabled for this scheduled search.</td>
</tr>
<tr>
<td>alert.suppress.fields</td>
<td>Fields to use for suppression when doing per result alerting. Required if suppression is turned on and per result alerting is enabled.</td>
</tr>
<tr>
<td>alert.suppress.period</td>
<td>Specifies the suppression period. Only valid if alert.suppress is enabled. Use [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</td>
</tr>
<tr>
<td>alert.track</td>
<td>Specifies whether to track the actions triggered by this scheduled search.</td>
</tr>
</tbody>
</table>
auto - determine whether to track or not based on the tracking setting of each action, do not track scheduled searches that always trigger actions.

true - force alert tracking.

false - disable alert tracking for this search.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert_comparator</td>
<td>Valid values are: Integer[%] Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to &quot;rises by perc&quot; or &quot;drops by perc.&quot;</td>
</tr>
<tr>
<td>alert_condition</td>
<td>A conditional search that is evaluated against the results of the saved search. Defaults to an empty string. Alerts are triggered if the specified search yields a non-empty search result list. Note: If you specify an alert_condition, do not set counttype, relation, or quantity.</td>
</tr>
<tr>
<td>alert_threshold</td>
<td>Valid values are: Integer[%] Specifies the value to compare (see alert_comparator) before triggering the alert actions. If expressed as a percentage, indicates value to use when alert_comparator is set to &quot;rises by perc&quot; or &quot;drops by perc.&quot;</td>
</tr>
<tr>
<td>alert_type</td>
<td>What to base the alert on, overriden by alert_condition if it is specified. Valid values are: always, custom, number of events, number of hosts, number of sources.</td>
</tr>
<tr>
<td>cron_schedule</td>
<td>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * <em>, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (</em>/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes. Valid values: cron string</td>
</tr>
<tr>
<td>description</td>
<td>Description of the saved search.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if this saved search is disabled.</td>
</tr>
<tr>
<td>dispatch_buckets</td>
<td>The maximum number of timeline buckets.</td>
</tr>
<tr>
<td>dispatch.earliest_time</td>
<td>A time string that specifies the earliest time for this search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>dispatch.latest_time</td>
<td>A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>dispatch.lookups</td>
<td>Indicates if lookups are enabled for this search.</td>
</tr>
<tr>
<td>dispatch.max_count</td>
<td>The maximum number of results before finalizing the search.</td>
</tr>
<tr>
<td>dispatch.max_time</td>
<td>Indicates the maximum amount of time (in seconds) before finalizing the search</td>
</tr>
<tr>
<td>earliest_time</td>
<td>For scheduled searches display all the scheduled times starting from this time.</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Indicates if this search is to be run on a schedule.</td>
</tr>
<tr>
<td>is_visible</td>
<td>Indicates if this saved search appears in the visible saved search list.</td>
</tr>
<tr>
<td>latest_time</td>
<td>A time string that specifies the latest time for this saved search. Can be a relative or absolute time. If this value is an absolute time, use the dispatch.time_format to format the value.</td>
</tr>
<tr>
<td>listDefaultActionArgs</td>
<td>List default values of actions.*, even though some of the actions may not be specified in the saved search.</td>
</tr>
<tr>
<td>max_concurrent</td>
<td>The maximum number of concurrent instances of this search the scheduler is allowed to run.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>The time when the scheduler runs this search again.</td>
</tr>
<tr>
<td>qualifiedSearch</td>
<td>The exact search command for this saved search.</td>
</tr>
<tr>
<td>realtime_schedule</td>
<td>Controls the way the scheduler computes the next execution time of a scheduled search. If this value is set to 1, the scheduler bases its determination of the next scheduled search execution time on the current time. If this value is set to 0, the scheduler bases its determination of the next scheduled search on the last search execution time. This is called continuous scheduling. If set to 0, the scheduler never skips scheduled execution periods. However, the execution of the saved search might fall behind depending on the scheduler load. Use continuous scheduling whenever you enable the summary index option. If set to 1, the scheduler might skip some execution periods to make sure that the scheduler is executing the searches running over the most recent time range. The scheduler tries to execute searches that have realtime_schedule set to 1 before it executes searches that have continuous scheduling (realtime_schedule = 0).</td>
</tr>
<tr>
<td>request.ui_dispatch_app</td>
<td>A field used by Splunk Web to denote the app this search should be dispatched in.</td>
</tr>
<tr>
<td>request.ui_dispatch_view</td>
<td>A field used by Splunk Web to denote the app this search should be dispatched in.</td>
</tr>
<tr>
<td>restart_on_searchpeer_add</td>
<td>Indicates whether to restart a real-time search managed by the scheduler when a search peer becomes available for this saved search. Note: The peer can be a newly added peer or a peer down and now available.</td>
</tr>
<tr>
<td>run_on_startup</td>
<td>Indicates whether this search runs on startup. If it does not run on startup, it runs at the next scheduled time. Splunk recommends that you set run_on_startup to true for scheduled searches that populate lookup tables.</td>
</tr>
<tr>
<td>scheduled_times</td>
<td>The times when the scheduler runs the search.</td>
</tr>
<tr>
<td>search</td>
<td>Search expression to filter the response. The response matches field values against the search expression. For example:</td>
</tr>
</tbody>
</table>

1060
search=foo matches any object that has "foo" as a substring in a field.
search=field_name%3Dfield_value restricts the match to a single field. URI-encoding is required in this example.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vsid</td>
<td>The viewstate id associated with the Splunk Web view listed in 'displayview'. Matches to a stanza in viewstates.conf.</td>
</tr>
</tbody>
</table>

**Application usage**
Specify a time range for the data returned using earliest_time and latest_time parameters.

**Example request and response**

**XML Request**
```
curl -k -u admin:pass
https://localhost:8089/services/saved/searches/_ScheduledView__dashboard_live/scheduled_times --get -d earliest_time=-5h -d latest_time=-3h
```

**XML Response**
```
<entry>
<title>_ScheduledView__dashboard_live</title>
<id>https://localhost:8089/servicesNS/admin/search/saved/searches/_ScheduledView__dashboard_live</id>
<updated>2011-12-02T11:55-08:00</updated>
<author>
  <name>Splunk</name>
</author>
<!-- opensearch nodes elided for brevity. -->
<content type="text/xml">
<s:dict>
  <s:key name="action.email">1</s:key>
  <s:key name="action.email.auth_password">$1$02rN856m+$QB</s:key>
  <s:key name="action.email.auth_username">myusername</s:key>
  . . . elided . . .
  <s:key name="action.email.pdfview">dashboard_live</s:key>
  . . . elided . . .
  <s:key name="action.email.subject">Splunk Alert: $name$</s:key>
  <s:key name="action.email.to">myusername@example.com</s:key>
  . . . elided . . .
</s:dict>
```

1061
saved/searches/{name}/suppress

https://<host>:<mPort>/services/saved/searches/{name}/suppress

Get the {name} saved search alert suppression state.

GET

Get the {name} saved search alert suppression state.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>str</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1062
### Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest_time</td>
<td>For scheduled searches display all the scheduled times starting from this time.</td>
</tr>
<tr>
<td>expiration</td>
<td>Sets the period of time to show the alert in the dashboard. Defaults to 24h.</td>
</tr>
<tr>
<td>Uses [number][time-unit] to specify a time. For example: 60 = 60 seconds, 1m = 1 minute, 1h = 60 minutes = 1 hour.</td>
<td></td>
</tr>
<tr>
<td>latest_time</td>
<td>A time string that specifies the latest time for this saved search. Can be a relative or absolute time.</td>
</tr>
<tr>
<td>listDefaultActionArgs</td>
<td>List default values of actions.*, even though some of the actions may not be specified in the saved search.</td>
</tr>
<tr>
<td>suppressed</td>
<td>Indicates if alert suppression is enabled for this search.</td>
</tr>
<tr>
<td>suppressionKey</td>
<td>A combination of all the values of the suppression fields (or the combinations MD5), if fields were specified.</td>
</tr>
</tbody>
</table>

### Example request and response

#### XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch/suppress
```

#### XML Response

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
>
	<id>https://localhost:8089/servicesNS/admin/search/saved/searches</id>
	<updated>2011-07-26T18:22:51Z</updated>
	<generator version="104601"/>
	<author>
		<name>Splunk</name>
	</author>
	<br:totalResults>1</br:totalResults>
	<br:itemsPerPage>30</br:itemsPerPage>
	<br:startIndex>0</br:startIndex>
	<br:messages/>
	<br:entry>
		<br:title>MySavedSearch</br:title>
		<br:id>https://localhost:8089/servicesNS/admin/search/saved/searches/MySavedSearch</br:id>
		<br:author>
			<br:name>admin</br:name>
		</br:author>
		<br:link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="alternate"/>
		<br:link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="list"/>
		<br:link href="/servicesNS/admin/search/saved/searches/MySavedSearch/_edit" rel="edit"/>
		<br:link href="/servicesNS/admin/search/saved/searches/MySavedSearch/_reload" rel="_reload"/>
		<br:link href="/servicesNS/admin/search/saved/searches/MySavedSearch" rel="remove"/>
	</br:entry>
</feed>
```
scheduled/views

https://<host>:<mPort>/services/scheduled/views

Access views scheduled for PDF delivery. Scheduled views are dummy noop scheduled saved searches that email a PDF of a dashboard.

GET

List all scheduled view objects.

Request parameters

Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email</td>
<td>Indicates the state of the email action.</td>
</tr>
<tr>
<td>action.email.pdfview</td>
<td>Name of the view to send as a PDF.</td>
</tr>
<tr>
<td>action.email.sendpdf</td>
<td>Indicates whether to create and send the results as a PDF.</td>
</tr>
<tr>
<td>action.email.sendresults</td>
<td>Indicates whether the search results are included in the email. The results can be attached or inline.</td>
</tr>
<tr>
<td>action.email.to</td>
<td>List of recipient email addresses. Required if the email alert action is enabled.</td>
</tr>
</tbody>
</table>

**action.email.ttl**

Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows <Integer>, int is the number of scheduled periods. Defaults to 86400 (24 hours).

If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.

Valid values are Integer[p].

**cron_schedule**

The cron schedule to use for delivering the view. Scheduled views are dummy/noop scheduled saved searches that email a pdf version of a view

For example: */5 * * * * causes the search to execute every 5 minutes.

cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * runs the search every hour at hh:03, hh:23, hh:43.
Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>description</td>
<td>Description of this scheduled view object.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the scheduled view is disabled.</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Indicates if PDF delivery of this view is scheduled.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>The next time when the view is delivered.</td>
</tr>
</tbody>
</table>

Example request and response

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/scheduled/views

**XML Response**

```xml
  <title>scheduledviews</title>
  <id>https://localhost:8089/servicesNS/admin/search/admin/scheduledviews</id>
  <updated>2011-07-27T16:27:55-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/admin/scheduledviews/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>_ScheduledView__MyView</title>
    <id>https://localhost:8089/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView</id>
    <updated>2011-07-27T16:27:55-04:00</updated>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView" rel="list"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/edit" rel="edit"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/remove" rel="remove"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/move" rel="move"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/disable" rel="disable"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/dispatch" rel="dispatch"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/history" rel="history"/>
    <link href="/servicesNS/admin/search/admin/scheduledviews/_ScheduledView__MyView/notify" rel="notify"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">1</s:key>
        <s:key name="action.email.pdfview">MyView</s:key>
        <s:key name="action.email.sendpdf">1</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
scheduled/views/{name}

https://<host>:<mPort>/services/scheduled/views/{name}

Manage the {name} scheduled view.

DELETE

Delete a scheduled view.

Request parameters
None

Returned values
None

Example request and response
XML Request

curl -k -u admin:pass --request DELETE https://localhost:8089/servicesNS/admin/search/scheduled/views/MyView

XML Response

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
<title>scheduledviews</title>
?id=https://localhost:8089/servicesNS/admin/search/admin/scheduledviews</id>
<updated>2011-07-27T16:16:02-04:00</updated>
<generator version="104601"/>
<author>
  <name>Splunk</name>
</author>
<link href="/servicesNS/admin/search/admin/scheduledviews/_reload" rel="_reload"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
</feed>
GET

Access a scheduled view.

**Request parameters**
None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email</td>
<td>Indicates the state of the email action.</td>
</tr>
<tr>
<td>action.email.auth_password</td>
<td>The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here and it is encrypted on the next restart. Defaults to empty string.</td>
</tr>
<tr>
<td>action.email.auth_username</td>
<td>The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. Note: Your SMTP server might reject unauthenticated emails.</td>
</tr>
<tr>
<td>action.email.bcc</td>
<td>&quot;BCC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.cc</td>
<td>CC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.command</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.email.format</td>
<td>Specify the format of text in the email. This value also applies to any attachments. Valid values: (plain</td>
</tr>
<tr>
<td>action.email.from</td>
<td>Email address from which the email action originates. Defaults to splunk@$LOCALHOST or whatever value is set in alert_actions.conf.</td>
</tr>
<tr>
<td>action.email.hostname</td>
<td>Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com) protocol://hostname:port (for example, <a href="http://splunkserver:8000">http://splunkserver:8000</a>, <a href="https://splunkserver.example.com:443">https://splunkserver.example.com:443</a>)</td>
</tr>
</tbody>
</table>

When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url.

When this value begins with 'http://', it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct an externally referencable url, such as SSO environments, other proxies, or when the server hostname is not generally
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email.inline</td>
<td>Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults.</td>
</tr>
<tr>
<td>action.email.mailserver</td>
<td>Set the address of the MTA server to be used to send the emails. Defaults to <code>&lt;LOCALHOST&gt;</code> (or whatever is set in alert_actions.conf).</td>
</tr>
<tr>
<td>action.email.maxresults</td>
<td>Sets the global maximum number of search results to send when email.action is enabled.</td>
</tr>
<tr>
<td>action.email.maxtime</td>
<td>Specifies the maximum amount of time the execution of an email action takes before the action is aborted.</td>
</tr>
<tr>
<td>action.email.pdfview</td>
<td>The name of the view to deliver if sendpdf is enabled.</td>
</tr>
<tr>
<td>action.email.preprocess_results</td>
<td>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.</td>
</tr>
<tr>
<td>action.email.reportPaperOrientation</td>
<td>Specifies the paper orientation: portrait or landscape.</td>
</tr>
<tr>
<td>action.email.reportPaperSize</td>
<td>Specifies the paper size for PDFs. Defaults to letter.</td>
</tr>
<tr>
<td>action.email.sendpdf</td>
<td>Indicates whether to create and send the results as a PDF.</td>
</tr>
<tr>
<td>action.email.sendresults</td>
<td>Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.</td>
</tr>
<tr>
<td>action.email.subject</td>
<td>Specifies the email subject. Defaults to SplunkAlert-&lt;savedsearchname&gt;.</td>
</tr>
<tr>
<td>action.email.to</td>
<td>List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.</td>
</tr>
<tr>
<td>action.email.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.email.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows &lt;Integer&gt;, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].</td>
</tr>
<tr>
<td>action.email.use_ssl</td>
<td>Indicates whether to use SSL when communicating with the SMTP server</td>
</tr>
<tr>
<td>action.email.use_tls</td>
<td>Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).</td>
</tr>
<tr>
<td>cron_schedule</td>
<td>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes.</td>
</tr>
</tbody>
</table>
cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43.

Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.

Valid values: cron string

description | Description of this saved search for this view.
disabled | Indicates if the saved search for this view is disabled.
is_scheduled | Indicates if this search is to be run on a schedule.
next_scheduled_time | The next time when the view is delivered.

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/scheduled/views/MyView

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:s="http://dev.splunk.com/ns/rest"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>scheduledviews</title>
  <id>https://localhost:8089/servicesNS/admin/search/scheduled/views</id>
  <updated>2011-07-27T17:12:11-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/scheduled/views/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <entry>
    <title>_ScheduledView__MyView</title>
    <id>https://localhost:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView</id>
    <updated>2011-07-27T17:12:11-04:00</updated>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="alternate"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="list"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/edit" rel="edit"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/remove" rel="remove"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/move" rel="move"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/disable" rel="disable"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/dispatch" rel="dispatch"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/history" rel="history"/>
  </entry>
</feed>
<s:dict>
    <s:dict>
        <s:key name="action.email">1</s:key>
        <s:key name="action.email.auth_password"></s:key>
        <s:key name="action.email.auth_username"></s:key>
        <s:key name="action.email.bcc"></s:key>
        <s:key name="action.email.cc"></s:key>
        <s:key name="action.email.command">
            <![CDATA[
                sendemail "server=$action.email.mailserver{default=localhost}$"
                "use_ssl=$action.email.use_ssl{default=false}$"
                "use_tls=$action.email.use_tls{default=false}$" "to=$action.email.to$"
                "cc=$action.email.cc$"
                "bcc=$action.email.bcc$" "from=$action.email.from{default=splunk@localhost}$"
                "subject=$action.email.subject{recurse=yes}$"
                "format=$action.email.format{default=csv}$"
                "sssummary=Saved Search [$name$]: $counttype$($results.count$)"
                "sslink=$results.url$" "ssquery=$search$" "ssname=$name$" "inline=$action.email.inline{default=False}$"
                "sendresults=$action.email.sendresults{default=False}$"
                "sendpdf=$action.email.sendpdf{default=False}$" "pdfview=$action.email.pdfview$"
                "searchid=$search_id$" "graceful=$graceful{default=True}$" "maxinputs=$action.email.maxresults{default=10000}$" "maxtime=$action.email.maxtime{default=5m}$"]]>
            </s:key>
        </s:key>
        <s:key name="action.email.format">html</s:key>
        <s:key name="action.email.from">splunk</s:key>
        <s:key name="action.email.hostname"></s:key>
        <s:key name="action.email.inline">0</s:key>
        <s:key name="action.email.mailserver">localhost</s:key>
        <s:key name="action.email.maxresults">10000</s:key>
        <s:key name="action.email.maxtime">5m</s:key>
        <s:key name="action.email.pdfview">MyView</s:key>
        <s:key name="action.email.preprocess_results"></s:key>
        <s:key name="action.email.reportPaperOrientation">portrait</s:key>
        <s:key name="action.email.reportPaperSize">letter</s:key>
        <s:key name="action.email.reportServerEnabled">0</s:key>
        <s:key name="action.email.reportServerURL"></s:key>
        <s:key name="action.email.sendpdf">1</s:key>
        <s:key name="action.email.sendresults">0</s:key>
        <s:key name="action.email.subject">Splunk Alert: $name$</s:key>
        <s:key name="action.email.to">info@example.com</s:key>
        <s:key name="action.email.track_alert">1</s:key>
        <s:key name="action.email.ttl">10</s:key>
        <s:key name="action.email.use_ssl">0</s:key>
        <s:key name="action.email.use_tls">0</s:key>
        <s:key name="cron_schedule">* * * *</s:key>
        <s:key name="description">scheduled search for view name=MyView</s:key>
        <s:key name="disabled">0</s:key>
    </s:dict>
    <!-- eai:acl elided -->
    <s:dict name="optionalFields">
        <s:list>
            <s:item>description</s:item>
            <s:item>disabled</s:item>
            <s:item>next_scheduled_time</s:item>
        </s:list>
    </s:dict>
</s:dict>
POST

Update a scheduled view.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email.to</td>
<td>String</td>
<td></td>
<td>Comma or semicolon separated list of email addresses to send the view to</td>
</tr>
<tr>
<td>action.email*</td>
<td>String</td>
<td></td>
<td>Wildcard argument that accepts any email action.</td>
</tr>
<tr>
<td>cron_schedule</td>
<td>String</td>
<td></td>
<td>The cron schedule to use for delivering the view. Scheduled views are dummy/noop scheduled saved searches that email a pdf version of a view. For example: */5 * * * * causes the search to execute every 5 minutes. Cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * <em>, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (</em>/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.</td>
</tr>
<tr>
<td>description</td>
<td>String</td>
<td></td>
<td>User readable description of this scheduled view object</td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td>0</td>
<td>Whether this object is enabled or disabled</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Boolean</td>
<td></td>
<td>Whether this pdf delivery should be scheduled</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>String</td>
<td></td>
<td>The next time when the view is delivered. Ignored on edit, here only for backwards compatibility.</td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1071</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>action.email</td>
<td>Indicates the status of the email action.</td>
</tr>
</tbody>
</table>
| action.email.auth_password | The password to use when authenticating with the SMTP server. Normally this value is set when editing  
the email settings, however you can set a clear text password here that is encrypted on the next restart.  
Defaults to empty string. |
| action.email.auth_username | The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string.  
Note: Your SMTP server might reject unauthenticated emails. |
| action.email.bcc     | BCC email address to use if action.email is enabled.                                              |
| action.email.cc      | CC email address to use if action.email is enabled.                                               |
| action.email.command | The search command (or pipeline) which is responsible for executing the action.                  |
|                      | Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$. |
| action.email.format  | Specify the format of text in the email. This value also applies to any attachments.<          |
|                      | Valid values: (plain | html | raw | csv)                                                      |
| action.email.from    | Email address from which the email action originates.                                            |
| action.email.hostname | Sets the hostname used in the web link (url) sent in email actions.  
This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com)  
When this value is a simple hostname, the protocol and port which are configured within splunk are used to construct the base of the url.  
When this value begins with "http://", it is used verbatim. NOTE: This means the correct port must be specified if it is not the default port for http or https. This is useful in cases when the Splunk server is not aware of how to construct an externally referencable url, such as SSO environments, other proxies, or when the server hostname is not generally resolvable.  
Defaults to current hostname provided by the operating system, or if that fails "localhost". When set to empty, default behavior is used. |
<p>| action.email.inline  | Indicates whether the search results are contained in the body of the email. Results can be either inline or attached to an email. See action.email.sendresults. |
| action.email.mailserver | Set the address of the MTA server to be used to send the emails.                                 |</p>
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email.maxresults</td>
<td>Sets the maximum number of search results sent using alerts.</td>
</tr>
<tr>
<td>action.email.maxtime</td>
<td>Specifies the maximum amount of time the execution of an email action takes before the action is aborted.</td>
</tr>
<tr>
<td>action.email.pdfview</td>
<td>The name of the view to deliver if sendpdf is enabled.</td>
</tr>
<tr>
<td>action.email.preprocess_results</td>
<td>Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing). Usually the preprocessing consists of filtering out unwanted internal fields.</td>
</tr>
<tr>
<td>action.email.reportPaperOrientation</td>
<td>Specifies the paper orientation: portrait or landscape.</td>
</tr>
<tr>
<td>action.email.reportPaperSize</td>
<td>Specifies the paper size for PDFs. Defaults to letter.</td>
</tr>
<tr>
<td>action.email.sendpdf</td>
<td>Indicates whether to create and send the results as a PDF.</td>
</tr>
<tr>
<td>action.email.sendresults</td>
<td>Indicates whether to attach the search results in the email. Results can be either attached or inline. See action.email.inline.</td>
</tr>
<tr>
<td>action.email.subject</td>
<td>Specifies an email subject. Defaults to SplunkAlert-&lt;savedsearchname&gt;.</td>
</tr>
<tr>
<td>action.email.to</td>
<td>List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.</td>
</tr>
<tr>
<td>action.email.track_alert</td>
<td>Indicates whether the execution of this action signifies a trackable alert.</td>
</tr>
<tr>
<td>action.email.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows &lt;Integer&gt;, int is the number of scheduled periods. Defaults to 86400 (24 hours).</td>
</tr>
<tr>
<td></td>
<td>If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf.</td>
</tr>
<tr>
<td></td>
<td>Valid values are Integer[p].</td>
</tr>
<tr>
<td>action.email.use_ssl</td>
<td>Indicates whether to use SSL when communicating with the SMTP server.</td>
</tr>
<tr>
<td>action.email.use_tls</td>
<td>Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).</td>
</tr>
<tr>
<td>cron_schedule</td>
<td>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes.</td>
</tr>
<tr>
<td></td>
<td>cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * *, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43.</td>
</tr>
<tr>
<td></td>
<td>Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (*/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>description</td>
<td>Valid values: cron string</td>
</tr>
<tr>
<td>disabled</td>
<td>Description of the saved search for this view.</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Indicates if the saved search for this view is disabled.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>Indicates if this search is to be run on a schedule.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>The next time when the view is delivered.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/scheduled/views/MyView -d action.email.to="info@example.com" -d cron_schedule="0 * * * *" -d is_scheduled=1 -d description="New description"
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>scheduledviews</title>
  <id>https://localhost:8089/servicesNS/admin/search/scheduled/views</id>
  <updated>2011-07-27T17:59:32-04:00</updated>
  <generator version="104601"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/admin/search/scheduled/views/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>_ScheduledView__MyView</title>
    <id>https://localhost:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView</id>
    <updated>2011-07-27T17:59:32-04:00</updated>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView" rel="alternate"/>
    <author>
      <name>admin</name>
    </author>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/_reload" rel="_reload"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/edit" rel="edit"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/remove" rel="remove"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/move" rel="move"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/disable" rel="disable"/>
    <link href="/servicesNS/admin/search/scheduled/views/_ScheduledView__MyView/notify" rel="notify"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="action.email">1</s:key>
        <s:key name="action.email.auth_password"></s:key>
        <s:key name="action.email.auth_username"></s:key>
        <s:key name="action.email.bcc"></s:key>
        <s:key name="action.email.cc"></s:key>
        <s:key name="action.email.command">1074</s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
scheduled/views/{name}/dispatch

https://<host>:<mPort>/services/scheduled/views/{name}/dispatch

Dispatch the scheduled search associated with the {name} scheduled view.
POST

Dispatch the scheduled search associated with the `{name}` scheduled view.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
</table>
| args.*         | String | Wildcard argument that accepts any saved search template argument, such as arg.username=foobar when the search is search $username$.
| dispatch.*     | String | Wildcard argument that accepts any dispatch related argument.               |
| dispatch.now   | Boolean| Dispatch the search as if the specified time for this parameter was the current time. |
| force_dispatch | Boolean| Indicates whether to start a new search even if another instance of this search is already running. |
| now            | String | [Deprecated] Use `dispatch.now`.                                           |
| trigger_actions| Boolean| Indicates whether to trigger alert actions                                 |

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/scheduled/views/MyView/dispatch -d trigger_actions=1
```

XML Response

```
<?xml version='1.0' encoding='UTF-8'?><response><sid>admin__admin__search_X1NjaGVkdWxlZVZpZXdfX015Vmlldw_at_1311805021_c24ff1ea77ad714b</sid></response>
```

scheduled/views/{name}/history

https://<host>:<mPort>/services/scheduled/views/{name}/history

List search jobs used to render the `{name}` scheduled view.

GET

List search jobs used to render the `{name}` scheduled view.

Request parameters

None

Returned values

None
Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/scheduled/views/MyView/history

XML Response

<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
><title>ScheduledView__MyView</title>
   <id>https://localhost:8089/servicesNS/admin/search/scheduled/views</id>
   <updated>2011-07-27T16:25:22-04:00</updated>
   <generator version="104601"/>
   <author>
      <name>Splunk</name>
   </author>
   <link href="/servicesNS/admin/search/scheduled/views/_reload" rel="_reload"/>
   <opensearch:totalResults>1</opensearch:totalResults>
   <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
   <opensearch:startIndex>0</opensearch:startIndex>
   <s:messages/>
   <entry>
      <title>scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a</title>
      <id>https://localhost:8089/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a</id>
      <updated>2011-07-27T16:25:15-04:00</updated>
      <link href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a" rel="alternate"/>
      <author>
         <name>admin</name>
      </author>
      <published>2011-07-27T16:25:15-04:00</published>
      <link href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a" rel="list"/>
      <link href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a/_reload" rel="_reload"/>
      <link href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a/edit"/>
      <link href="/servicesNS/nobody/search/search/jobs/scheduler__admin__search_X1NjaGVkdWxlZFZpZXdfX015Vmlldw_at_1311798300_842d7ca298ab521a/remove"/>
      <content type="text/xml">
         <s:dict>
            <!-- eai:acl elided -->
         </s:dict>
      </content>
   </entry>
</feed>
scheduled/views/{name}/reschedule

https://<host>:<mPort>/services/scheduled/views/{name}/reschedule
Schedule the {name} view PDF delivery.

**POST**

Schedule the {name} view PDF delivery.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>schedule_time</td>
<td>String</td>
<td>Absolute or relative schedule time.</td>
<td></td>
</tr>
</tbody>
</table>

**Returned values**

None

**Application usage**

If schedule_time is not specified, then it is assumed that the delivery should occur as soon as possible.

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/scheduled/views/_ScheduledView__dashboard2/reschedule
-d schedule_time=2013-02-15T14:11:01Z
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
<title>scheduledviews</title>
<id>https://localhost:8089/services/scheduled/views</id>
<updated>2012-10-02T08:48:18-07:00</updated>
<generator build="138753" version="5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/scheduled/views/_reload" rel="_reload"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
</feed>
```
scheduled/views/{name}/scheduled_times

https://<host>:<mPort>/services/scheduled/views/{name}/scheduled_times
Get scheduled view times.

GET
Get scheduled view times.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest_time</td>
<td>String</td>
<td>Absolute or relative earliest time</td>
<td></td>
</tr>
<tr>
<td>latest_time</td>
<td>String</td>
<td>Absolute or relative latest time</td>
<td></td>
</tr>
</tbody>
</table>

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email</td>
<td>Indicates the state of the email action.</td>
</tr>
<tr>
<td>action.email.auth_password</td>
<td>The password to use when authenticating with the SMTP server. Normally this value is set when editing the email settings, however you can set a clear text password here that is encrypted on the next restart. Defaults to empty string.</td>
</tr>
<tr>
<td>action.email.auth_username</td>
<td>The username to use when authenticating with the SMTP server. If this is empty string, no authentication is attempted. Defaults to empty string. Note: Your SMTP server might reject unauthenticated emails.</td>
</tr>
<tr>
<td>action.email.bcc</td>
<td>BCC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.cc</td>
<td>CC email address to use if action.email is enabled.</td>
</tr>
<tr>
<td>action.email.command</td>
<td>The search command (or pipeline) which is responsible for executing the action. Generally the command is a template search pipeline which is realized with values from the saved search. To reference saved search field values wrap them in $, for example to reference the savedsearch name use $name$, to reference the search use $search$.</td>
</tr>
<tr>
<td>action.email.format</td>
<td>Specify the format of text in the email. This value also applies to any attachments.&lt; Valid values: (plain</td>
</tr>
<tr>
<td>action.email.from</td>
<td>Email address from which the email action originates.</td>
</tr>
<tr>
<td>action.email.hostname</td>
<td>Sets the hostname used in the web link (url) sent in email actions. This value accepts two forms: hostname (for example, splunkserver, splunkserver.example.com)</td>
</tr>
</tbody>
</table>
action.email.inline
Indicates whether the search results are contained in the body of the email.

Results can be either inline or attached to an email. See action.email.sendresults.

action.email.mailserver
Set the address of the MTA server to be used to send the emails.

Defaults to <LOCALHOST> (or whatever is set in alert_actions.conf).

action.email.maxresults
Sets the maximum number of search results sent using alerts.

action.email.maxtime
Specifies the maximum amount of time the execution of an email action takes before the action is aborted.

action.email.pdfview
The name of the view to deliver if sendpdf is enabled.

action.email.preprocess_results
Search string to preprocess results before emailing them. Defaults to empty string (no preprocessing).

Usually the preprocessing consists of filtering out unwanted internal fields.

action.email.reportPaperOrientation
Specifies the paper orientation: portrait or landscape.

action.email.reportPaperSize
Specifies the paper size for PDFs. Defaults to letter.

Valid values: (letter | legal | ledger | a2 | a3 | a4 | a5)

action.email.reportServerEnabled
Not supported.

action.email.reportServerURL
Not supported.

action.email.sendpdf
Indicates whether to create and send the results as a PDF.

action.email.sendresults
Indicates whether to attach the search results in the email.

Results can be either attached or inline. See action.email.inline.

action.email.subject
Specifies an email subject.

Defaults to SplunkAlert-<savedsearchname>.

action.email.to
List of recipient email addresses. Required if this search is scheduled and the email alert action is enabled.

action.email.track_alert
Indicates whether the execution of this action signifies a trackable alert.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>action.email.ttl</td>
<td>Specifies the minimum time-to-live in seconds of the search artifacts if this action is triggered. If p follows &lt;integer&gt;, int is the number of scheduled periods. Defaults to 86400 (24 hours). If no actions are triggered, the artifacts have their ttl determined by dispatch.ttl in savedsearches.conf. Valid values are Integer[p].</td>
</tr>
<tr>
<td>action.email.use_ssl</td>
<td>Indicates whether to use SSL when communicating with the SMTP server.</td>
</tr>
<tr>
<td>action.email.use_tls</td>
<td>Indicates whether to use TLS (transport layer security) when communicating with the SMTP server (starttls).</td>
</tr>
<tr>
<td>action.email.width_sort_columns</td>
<td>Indicates whether columns should be sorted from least wide to most wide, left to right. Only valid if format=text.</td>
</tr>
<tr>
<td>cron_schedule</td>
<td>The cron schedule to execute this search. For example: */5 * * * * causes the search to execute every 5 minutes. cron lets you use standard cron notation to define your scheduled search interval. In particular, cron can accept this type of notation: 00,20,40 * * * <em>, which runs the search every hour at hh:00, hh:20, hh:40. Along the same lines, a cron of 03,23,43 * * * * runs the search every hour at hh:03, hh:23, hh:43. Splunk recommends that you schedule your searches so that they are staggered over time. This reduces system load. Running all of them every 20 minutes (</em>/20) means they would all launch at hh:00 (20, 40) and might slow your system every 20 minutes. Valid values: cron string</td>
</tr>
<tr>
<td>description</td>
<td>Description of the saved search for this view.</td>
</tr>
<tr>
<td>disabled</td>
<td>Indicates if the saved search for this view is disabled. Disabled saved searches are not visible in Splunk Web.</td>
</tr>
<tr>
<td>is_scheduled</td>
<td>Indicates if this search is to be run on a schedule.</td>
</tr>
<tr>
<td>next_scheduled_time</td>
<td>The next time when the view is delivered.</td>
</tr>
</tbody>
</table>

**Application usage**
Specify a time range for the data returned using earliest_time and latest_time parameters.

**Example request and response**

**XML Request**

```
curl -k -u admin:admin
https://localhost:8089/services/scheduled/views/_ScheduledView__dashboard_live/scheduled_times --get -d earliest_time=-5h -d latest_time=-3h
```

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">

1081
```
<title>scheduledviews</title>
<id>https://wma-mbp15:8089/services/scheduled/views</id>
<updated>2011-12-01T14:40:18-08:00</updated>
<generator version="112383"/>

<title>_ScheduledView__dashboard_live</title>
<id>https://wma-mbp15:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live</id>
<updated>2011-12-01T14:40:18-08:00</updated>

<title>_ScheduledView__dashboard_live</title>
<id>https://wma-mbp15:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live</id>
<updated>2011-12-01T14:40:18-08:00</updated>

<title>_ScheduledView__dashboard_live</title>
<id>https://wma-mbp15:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live</id>
<updated>2011-12-01T14:40:18-08:00</updated>

<title>_ScheduledView__dashboard_live</title>
<id>https://wma-mbp15:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live</id>
<updated>2011-12-01T14:40:18-08:00</updated>

<title>_ScheduledView__dashboard_live</title>
<id>https://wma-mbp15:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live</id>
<updated>2011-12-01T14:40:18-08:00</updated>

<title>_ScheduledView__dashboard_live</title>
<id>https://wma-mbp15:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live</id>
<updated>2011-12-01T14:40:18-08:00</updated>

<title>_ScheduledView__dashboard_live</title>
<id>https://wma-mbp15:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live</id>
<updated>2011-12-01T14:40:18-08:00</updated>

<title>_ScheduledView__dashboard_live</title>
<id>https://wma-mbp15:8089/servicesNS/admin/search/scheduled/views/_ScheduledView__dashboard_live</id>
<updated>2011-12-01T14:40:18-08:00</updated>
search/concurrency-settings

https://<host>:<mPort>/services/search/concurrency-settings

GET
List search concurrency settings.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_searches_perc</td>
<td>Number</td>
<td>The maximum number of searches the scheduler can run as a percentage of the maximum number of concurrent searches. Default: 50%.</td>
</tr>
<tr>
<td>auto_summary_perc</td>
<td>Number</td>
<td>The maximum number of concurrent searches to be allocated for auto summarization, as a percentage of the concurrent searches that the scheduler can run. Default: 50.</td>
</tr>
<tr>
<td>max_searches_per_cpu</td>
<td>Number</td>
<td>The maximum number of concurrent historical searches allowed per cpu. Default: 1.</td>
</tr>
<tr>
<td>base_max_searches</td>
<td>Number</td>
<td>A baseline constant to add to the max number of searches (computed as multiplier of the CPUs.) Default is 6.</td>
</tr>
<tr>
<td>max_rt_search_multiplier</td>
<td>Number</td>
<td>A number by which the maximum number of historical searches is multiplied to determine the maximum number of concurrent real-time searches. Note: The maximum number of real-time searches is computed as max_RT_searches = max_rt_search_multiplier \times max_hist_searches</td>
</tr>
</tbody>
</table>

Example request and response
XML Request

curl -k -u admin:pass https://localhost:8089/services/search/concurrency-settings

XML Response

      xmlns:dev="http://a9.com/-/spec/opensearch/1.1/dev/"
      xmlns:meta="http://a9.com/-/spec/opensearch/1.1/meta/">
  <title>search-concurrency-settings-handler</title>
  <id>https://localhost:8089/services/search/concurrency-settings</id>
  <updated>2019-04-21T14:46:39-07:00</updated>
  <author>
  </author>
</feed>
<name>Splunk</name>
</author>
<opensearch:totalResults>2</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>scheduler</title>
<id>https://localhost:8089/services/search/concurrency-settings/scheduler</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/services/search/concurrency-settings/scheduler" rel="alternate"/>
<author>
<name>system</name>
</author>
<link href="/services/search/concurrency-settings/scheduler" rel="list"/>
<content type="text/xml">
<s:dict>
<s:key name="auto_summary_perc">50</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">0</s:key>
<s:key name="owner">system</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list/>
</s:key>
</s:dict>
<s:key name="removable">0</s:key>
<s:key name="sharing">system</s:key>
</s:dict>
</s:key>
<s:key name="max_searches_perc">50</s:key>
</s:dict>
</content>
</entry>
<entry>
<title>search</title>
<id>https://localhost:8089/services/search/concurrency-settings/search</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/services/search/concurrency-settings/search" rel="alternate"/>
<author>
<name>system</name>
</author>
<link href="/services/search/concurrency-settings/search" rel="list"/>
<content type="text/xml">
<s:dict>
<s:key name="base_max_searches">10</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app"></s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_write">1</s:key>
</s:dict>
</content>
</entry>

1084
search/concurrency-settings/scheduler

https://<host>:<mPort>/services/search/concurrency-settings/scheduler
Edit settings that determine concurrent scheduled search limits.

Authentication and Authorization
The edit_search_concurrency_scheduled capability is required for this endpoint.

POST
Edit settings that determine concurrent scheduled search limits.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_searches_perc</td>
<td>Number</td>
<td>The maximum number of searches the scheduler can run as a percentage of the maximum number of concurrent searches. Default: 50.</td>
</tr>
<tr>
<td>auto_summary_perc</td>
<td>Number</td>
<td>The maximum number of concurrent searches to be allocated for auto summarization, as a percentage of the concurrent searches that the scheduler can run. Default: 50.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response
XML Request
curl -k -u admin:pass https://localhost:8089/services/search/concurrency-settings/scheduler -d max_searches_perc=40

**XML Response**

```xml
  <title>search-concurrency-settings-handler</title>
  <id>https://localhost:8089/services/search/concurrency-settings</id>
  <updated>2019-04-21T17:17:30-07:00</updated>
  <generator build="efdccca30d13" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>scheduler</title>
    <id>https://localhost:8089/services/search/concurrency-settings/scheduler</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
    <link href="/services/search/concurrency-settings/scheduler" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/services/search/concurrency-settings/scheduler" rel="list"/>
    <link href="/services/search/concurrency-settings/scheduler" rel="edit"/>
    <content type="text/xml">
      <s:dict>
        <s:key name="auto_summary_perc">50</s:key>
        <s:key name="eai:acl">
          <s:dict>
            <s:key name="app"></s:key>
            <s:key name="can_list">1</s:key>
            <s:key name="can_write">1</s:key>
            <s:key name="modifiable">0</s:key>
            <s:key name="owner">system</s:key>
            <s:key name="perms">
              <s:dict>
                <s:key name="read">
                  <s:list>
                    <s:item>*</s:item>
                  </s:list>
                </s:key>
                <s:key name="write">
                  <s:list>
                    <s:item>admin</s:item>
                    <s:item>splunk-system-role</s:item>
                  </s:list>
                </s:key>
                <s:key name="removable">0</s:key>
                <s:key name="sharing">system</s:key>
              </s:dict>
            </s:key>
            <s:key name="max_searches_perc">40</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
```
search/concurrency-settings/search

https://<host>:<mPort>/services/search/concurrency-settings/search

Edit settings that determine the maximum number of concurrent scheduled searches.

Authentication and Authorization

The edit_search_concurrency_all capability is required for this endpoint.

POST

Edit settings that determine the maximum number of concurrent scheduled searches.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_searches_per_cpu</td>
<td>Number</td>
<td>The maximum number of concurrent historical searches allowed per cpu. Default: 1.</td>
</tr>
<tr>
<td>base_max_searches</td>
<td>Number</td>
<td>A baseline constant to add to the max number of searches (computed as multiplier of the CPUs.) Default is 6.</td>
</tr>
<tr>
<td>max_rt_search_multiplier</td>
<td>Number</td>
<td>A number by which the maximum number of historical searches is multiplied to determine the maximum number of concurrent real-time searches. Note: The maximum number of real-time searches is computed as max_rt_searches = max_rt_search_multiplier x max_hist_searches</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/search/concurrency-settings/search -d base_max_searches=5 -d max_searches_per_cpu=4

XML Response

feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
<title>search-concurrency-settings-handler</title>
<id>https://localhost:8089/services/search/concurrency-settings</id>
<updated>2019-04-21T17:31:19-07:00</updated>
<generator build="efdccca30d13" version="7.3.0"/>
<author>
  <name>Splunk</name>
</author>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
search/jobs

https://<host>:<mPort>/services/search/jobs

List search jobs.

For more information about this and other search endpoints, see Creating searches using the REST API in the REST API Tutorial.
GET

Get details of all current searches.

Request parameters
Pagination and filtering parameters can be used with this method.

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cursorTime</td>
<td>The earliest time from which no events are later scanned. Can be used to indicate progress. See description for doneProgress.</td>
</tr>
<tr>
<td>custom</td>
<td>Custom job property. (See the search/jobs POST request for an example of how to create a custom property.)</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> Filtering for custom search jobs fails in a search head cluster environment. Remove the ?search=custom filter to see all search jobs including custom jobs.</td>
</tr>
<tr>
<td>delegate</td>
<td>For saved searches, specifies jobs that were started by the user. Defaults to scheduler.</td>
</tr>
<tr>
<td>diskUsage</td>
<td>The total amount of disk space used, in bytes.</td>
</tr>
<tr>
<td>dispatchState</td>
<td>The state of the search. Can be any of QUEUED, PARSING, RUNNING, PAUSED, FINALIZING, FAILED, DONE.</td>
</tr>
<tr>
<td>doneProgress</td>
<td>A number between 0 and 1.0 that indicates the approximate progress of the search. doneProgress = (latestTime ? cursorTime) / (latestTime ? earliestTime)</td>
</tr>
<tr>
<td>dropCount</td>
<td>For real-time searches only, the number of possible events that were dropped due to the rt_queue_size (default to 100000).</td>
</tr>
<tr>
<td>earliestTime</td>
<td>The earliest time a search job is configured to start. Can be used to indicate progress. See description for doneProgress.</td>
</tr>
<tr>
<td>eventAvailableCount</td>
<td>The number of events that are available for export.</td>
</tr>
<tr>
<td>eventCount</td>
<td>The number of events returned by the search.</td>
</tr>
<tr>
<td>eventFieldCount</td>
<td>The number of fields found in the search results.</td>
</tr>
<tr>
<td>eventIsStreaming</td>
<td>Indicates if the events of this search are being streamed.</td>
</tr>
<tr>
<td>eventIsTruncated</td>
<td>Indicates if events of the search are not stored, making them unavailable from the events endpoint for the search.</td>
</tr>
<tr>
<td>eventPreviewableCount</td>
<td>Number of in-memory events that are not yet committed to disk. Returned if timeline_events_preview is enabled in limits.conf.</td>
</tr>
<tr>
<td>eventSearch</td>
<td>Subset of the entire search that is before any transforming commands. The timeline and events endpoint represents the result of this part of the search.</td>
</tr>
<tr>
<td>eventSorting</td>
<td>Indicates if the events of this search are sorted, and in which order. asc = ascending; desc = descending; none = not sorted</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>---------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>isDone</td>
<td>Indicates if the search has completed.</td>
</tr>
<tr>
<td>isEventPreviewEnabled</td>
<td>Indicates if the <code>timeline_events_preview</code> setting is enabled in <code>limits.conf</code>.</td>
</tr>
<tr>
<td>isFailed</td>
<td>Indicates if there was a fatal error executing the search. For example, invalid search string syntax.</td>
</tr>
<tr>
<td>isFinalized</td>
<td>Indicates if the search was finalized (stopped before completion).</td>
</tr>
<tr>
<td>isPaused</td>
<td>Indicates if the search is paused.</td>
</tr>
<tr>
<td>isPreviewEnabled</td>
<td>Indicates if previews are enabled.</td>
</tr>
<tr>
<td>isRealTimeSearch</td>
<td>Indicates if the search is a real time search.</td>
</tr>
<tr>
<td>isRemoteTimeline</td>
<td>Indicates if the remote timeline feature is enabled.</td>
</tr>
<tr>
<td>isSaved</td>
<td>Indicates that the search job is saved, storing search artifacts on disk for 7 days from the last time that the job was viewed or touched. Add or edit the <code>default_save_ttl</code> value in <code>limits.conf</code> to override the default value of 7 days.</td>
</tr>
<tr>
<td>isSavedSearch</td>
<td>Indicates if this is a saved search run using the scheduler.</td>
</tr>
<tr>
<td>isZombie</td>
<td>Indicates if the process running the search is dead, but with the search not finished.</td>
</tr>
<tr>
<td>keywords</td>
<td>All positive keywords used by this search. A positive keyword is a keyword that is not in a NOT clause.</td>
</tr>
<tr>
<td>label</td>
<td>Custom name created for this search.</td>
</tr>
<tr>
<td>latestTime</td>
<td>The latest time a search job is configured to start. Can be used to indicate progress. See description for doneProgress.</td>
</tr>
<tr>
<td>messages</td>
<td>Errors and debug messages.</td>
</tr>
<tr>
<td>numPreviews</td>
<td>Number of previews generated so far for this search job.</td>
</tr>
<tr>
<td>performance</td>
<td>A representation of the execution costs.</td>
</tr>
<tr>
<td>priority</td>
<td>An integer between 0-10 that indicates the search priority. The priority is mapped to the OS process priority. The higher the number the higher the priority. The priority can be changed using action parameter for POST <code>search/jobs/{search_id}/control</code>. For example, for the action parameter, specify <code>priority=5</code>. Note: In *nix systems, non-privileged users can only reduce the priority of a process.</td>
</tr>
<tr>
<td>remoteSearch</td>
<td>The search string that is sent to every search peer.</td>
</tr>
<tr>
<td>reportSearch</td>
<td>If reporting commands are used, the reporting search.</td>
</tr>
<tr>
<td>request</td>
<td>GET arguments that the search sends to splunkd.</td>
</tr>
<tr>
<td>resultCount</td>
<td>The total number of results returned by the search. In other words, this is the subset of scanned events (represented by the scanCount) that actually matches the search terms.</td>
</tr>
<tr>
<td>resultIsStreaming</td>
<td>Indicates if the final results of the search are available using streaming (for example, no transforming operations).</td>
</tr>
<tr>
<td>resultPreviewCount</td>
<td>The number of result rows in the latest preview results.</td>
</tr>
<tr>
<td>runDuration</td>
<td>Time in seconds that the search took to complete.</td>
</tr>
<tr>
<td>scanCount</td>
<td>The number of events that are scanned or read off disk.</td>
</tr>
<tr>
<td>searchEarliestTime</td>
<td></td>
</tr>
</tbody>
</table>
Specifies the earliest time for a search, as specified in the search command rather than the earliestTime parameter. It does not snap to the indexed data time bounds for all-time searches (something that earliestTime/latestTime does).

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>searchLatestTime</td>
<td>Specifies the latest time for a search, as specified in the search command rather than the latestTime parameter. It does not snap to the indexed data time bounds for all-time searches (something that earliestTime/latestTime does).</td>
</tr>
<tr>
<td>searchProviders</td>
<td>A list of all the search peers that were contacted.</td>
</tr>
<tr>
<td>sid</td>
<td>The search ID number.</td>
</tr>
<tr>
<td>statusBuckets</td>
<td>Maximum number of timeline buckets.</td>
</tr>
<tr>
<td>ttl</td>
<td>The time to live, or time before the search job expires after it completes.</td>
</tr>
</tbody>
</table>

**Application usage**

The user ID is implied by the authentication to the call.

Information returned for each entry includes the search job properties, such as eventCount (number of events returned), runDuration (time the search took to complete), and others. The parameters to POST /search/jobs provides details on search job properties when creating a search. Search job properties are also described in Search job properties in the Knowledge Manager Manual.

You can specify optional arguments based on the search job properties to filter the entries returned. For example, specify search=eventCount>100 as an argument to the GET operation to return searches with event counts greater than 100.

The dispatchState property is of particular interest to determine the state of a search, and can contain the following values:

- QUEUED
- PARSING
- RUNNING
- PAUSED
- FINALIZING
- FAILED
- DONE

This operation also returns performance information for the search.

For more information refer to "View search job properties with the Search Job Inspector" in the Knowledge Manager Manual.

For more information on searches, see the Search Reference.

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/search/jobs --get -d search="eventCount>100"
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
```

1091
<title>jobs</title>
<id>https://localhost:8089/services/search/jobs</id>
<updated>2011-06-21T10:12:22-07:00</updated>
<generator version="100492"/>

<title>search index=_internal (source=*/metrics.log* OR source=*\metrics.log*)
group-per_sourcetype_thruput</title>

<updated>2011-06-21T10:10:31.000-07:00</updated>

<link href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4" rel="alternate"/>
<link href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4/search.log" rel="log"/>
<link href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4/events" rel="events"/>
<link href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4/results" rel="results"/>
<link href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4/results_preview" rel="results_preview"/>
<link href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4/timeline" rel="timeline"/>
<link href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4/summary" rel="summary"/>
<link href="/services/search/jobs/scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4/control" rel="control"/>

<author>
<name>splunk-system-user</name>
</author>

<content type="text/xml">
<s:dict>
<s:key name="cursorTime">1969-12-31T16:00:00.000-08:00</s:key>
<s:key name="delegate">scheduler</s:key>
<s:key name="diskUsage">73728</s:key>
<s:key name="dispatchState">DONE</s:key>
<s:key name="doneProgress">1.00000</s:key>
<s:key name="dropCount">0</s:key>
<s:key name="earliestTime">2011-06-20T10:00:00-07:00</s:key>
<s:key name="eventAvailableCount">1363</s:key>
<s:key name="eventCount">1363</s:key>
<s:key name="eventFieldCount">1</s:key>
<s:key name="eventIsStreaming">1</s:key>
<s:key name="eventIsTruncated">1</s:key>
<s:key name="eventSearch">search index=_internal (source=*/metrics.log* OR source=*\metrics.log*)
group-per_sourcetype_thruput</s:key>
<s:key name="eventSorting">none</s:key>
</s:dict>
</content>

1092
Top five sourcetypes:

```
group::per_sourcetype_thruput
index::_internal
source::*\metrics.log*
```

```
source::*\metrics.log*
```

```
group=per_sourcetype_thruput
  | addinfo  type=count
  | label=prereport_events
  | fields  keepcolorder=t
  | "kb" "prestats_reserved_1" "psrsvd_*" "series"
  | sort  num("kb") | prestats  sum("kb") AS "sum(kb)", by series
```

```
reportSearch=chart  sum("kb") by series  | sort  -sum("kb")  | head  5
```

```
resultCount=4
```

```
resultIsStreaming=0
```

```
resultPreviewCount=4
```

```
runDuration=0.259000
```

```
scanCount=1363
```

```
searchEarliestTime=1308589800.000000000
```

```
searchLatestTime=1308676200.000000000
```

```
sid=scheduler__nobody__search_VG9wIGZpdmUgc291cmNldHlwZXM_at_1308676200_22702c154383bbe4
```

```
ttl=489
```

```
performance=
```

```
command.addinfo=
```
```
  duration_secs=0.005
  invocations=5
  input_count=1363
  output_count=1363
```

```
command.chart=
```
```
  duration_secs=0.003
  invocations=1
  input_count=100000
  output_count=4
```

```
command.convert=
```
```
  duration_secs=0.006
  invocations=5
  input_count=1363
  output_count=1363
```

```
command.fields=
```
```
  duration_secs=0.005
```

```
1093
```
<s:dict><s:key name="command.head"> <s:dict> <s:key name="duration_secs">0.001</s:key> <s:key name="invocations">1</s:key> <s:key name="input_count">4</s:key> <s:key name="output_count">4</s:key> </s:dict> </s:key> <s:key name="command.presort"> <s:dict> <s:key name="duration_secs">0.001</s:key> <s:key name="invocations">1</s:key> <s:key name="input_count">4</s:key> <s:key name="output_count">4</s:key> </s:dict> </s:key> <s:key name="command.prestats"> <s:dict> <s:key name="duration_secs">0.014</s:key> <s:key name="invocations">5</s:key> <s:key name="input_count">1363</s:key> <s:key name="output_count">12</s:key> </s:dict> </s:key> <s:key name="command.search"> <s:dict> <s:key name="duration_secs">0.058</s:key> <s:key name="invocations">5</s:key> <s:key name="input_count">0</s:key> <s:key name="output_count">1363</s:key> </s:dict> </s:key> <s:key name="command.search.fieldalias"> <s:dict> <s:key name="duration_secs">0.003</s:key> <s:key name="invocations">3</s:key> <s:key name="input_count">1363</s:key> <s:key name="output_count">1363</s:key> </s:dict> </s:key> <s:key name="command.search.filter"> <s:dict> <s:key name="duration_secs">0.004</s:key> <s:key name="invocations">3</s:key> </s:dict> </s:key> <s:key name="command.search.index"> <s:dict> <s:key name="duration_secs">0.010</s:key> <s:key name="invocations">5</s:key> </s:dict> </s:key> <s:key name="command.search.kv"> <s:dict> <s:key name="duration_secs">0.011</s:key> <s:key name="invocations">3</s:key> </s:dict> </s:key></s:dict>
<s:dict>
  <s:dict>
    <s:key name="command.search.lookups">
      <s:dict>
        <s:key name="duration_secs">0.003</s:key>
        <s:key name="invocations">3</s:key>
        <s:key name="input_count">1363</s:key>
        <s:key name="output_count">1363</s:key>
      </s:dict>
    </s:key>
  </s:dict>
  <s:dict>
    <s:dict>
      <s:key name="command.search.rawdata">
        <s:dict>
          <s:key name="duration_secs">0.034</s:key>
          <s:key name="invocations">3</s:key>
        </s:dict>
      </s:key>
    </s:dict>
    <s:dict>
      <s:dict>
        <s:key name="command.search.tags">
          <s:dict>
            <s:key name="duration_secs">0.005</s:key>
            <s:key name="invocations">5</s:key>
            <s:key name="input_count">1363</s:key>
            <s:key name="output_count">1363</s:key>
          </s:dict>
        </s:key>
      </s:dict>
      <s:dict>
        <s:dict>
          <s:key name="command.search.typer">
            <s:dict>
              <s:key name="duration_secs">0.005</s:key>
              <s:key name="invocations">5</s:key>
              <s:key name="input_count">1363</s:key>
              <s:key name="output_count">1363</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:dict>
      <s:dict>
        <s:dict>
          <s:key name="command.sort">
            <s:dict>
              <s:key name="duration_secs">0.001</s:key>
              <s:key name="invocations">1</s:key>
              <s:key name="input_count">4</s:key>
              <s:key name="output_count">4</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:dict>
      <s:dict>
        <s:dict>
          <s:key name="dispatch.createProviderQueue">
            <s:dict>
              <s:key name="duration_secs">0.067</s:key>
              <s:key name="invocations">1</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:dict>
      <s:dict>
        <s:dict>
          <s:key name="dispatch.evaluate">
            <s:dict>
              <s:key name="duration_secs">0.038</s:key>
              <s:key name="invocations">1</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:dict>
      <s:dict>
        <s:dict>
          <s:key name="dispatch.evaluate.chart">
            <s:dict>
              <s:key name="duration_secs">0.001</s:key>
              <s:key name="invocations">1</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:dict>
      <s:dict>
        <s:dict>
          <s:key name="dispatch.evaluate.head">
            <s:dict>
              <s:key name="duration_secs">0.001</s:key>
              <s:key name="invocations">1</s:key>
            </s:dict>
          </s:key>
        </s:dict>
      </s:dict>
    </s:dict>
  </s:dict>
</s:dict>
</s:key>
<s:key name="dispatch.evaluate.search">
  <s:dict>
    <s:key name="duration_secs">0.037</s:key>
    <s:key name="invocations">1</s:key>
  </s:dict>
</s:key>
<s:key name="dispatch.evaluate.sort">
  <s:dict>
    <s:key name="duration_secs">0.001</s:key>
    <s:key name="invocations">1</s:key>
  </s:dict>
</s:key>
<s:key name="dispatch.fetch">
  <s:dict>
    <s:key name="duration_secs">0.126</s:key>
    <s:key name="invocations">6</s:key>
  </s:dict>
</s:key>
<s:key name="dispatch.stream.local">
  <s:dict>
    <s:key name="duration_secs">0.070</s:key>
    <s:key name="invocations">5</s:key>
  </s:dict>
</s:key>
</s:dict>
<s:key name="messages">
  <s:dict/>
</s:key>
<s:key name="request">
  <s:dict>
    <s:key name="ui_dispatch_app"></s:key>
    <s:key name="ui_dispatch_view"></s:key>
  </s:dict>
</s:key>
<s:key name="eai:acl">
  <s:dict>
    <s:key name="perms">
      <s:dict>
        <s:key name="read">
          <s:list>
            <s:item>admin</s:item>
          </s:list>
        </s:key>
        <s:key name="write">
          <s:list>
            <s:item>admin</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </s:key>
    <s:key name="owner">nobody</s:key>
    <s:key name="modifiable">true</s:key>
    <s:key name="sharing">global</s:key>
    <s:key name="app">search</s:key>
    <s:key name="can_write">true</s:key>
  </s:dict>
</s:key>
<s:key name="searchProviders">
  <s:list>
    <s:item>mbpl5.splunk.com</s:item>
  </s:list>
</s:key>
Start a new search and return the search ID (<sid>)

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>adhoc_search_level</td>
<td>String</td>
<td></td>
<td>Use one of the following search modes. [ verbose</td>
</tr>
<tr>
<td>allow_partial_results</td>
<td>Boolean</td>
<td>true</td>
<td>Indicates whether the search job can proceed to provide partial results if a search peer fails. When false, the search job fails if a search peer providing results for the search job fails.</td>
</tr>
<tr>
<td>auto.cancel</td>
<td>Number</td>
<td>0</td>
<td>If specified, the job automatically cancels after this many seconds of inactivity. (0 means never auto-cancel)</td>
</tr>
<tr>
<td>auto.finalize_ec</td>
<td>Number</td>
<td>0</td>
<td>Auto-finalize the search after at least this many events are processed. Specify 0 to indicate no limit.</td>
</tr>
<tr>
<td>auto.pause</td>
<td>Number</td>
<td>0</td>
<td>If specified, the search job pauses after this many seconds of inactivity. (0 means never auto-pause)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>To restart a paused search job, specify unpause as an action to POST search/jobs/{search_id}/control.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>auto_pause only goes into effect once. Unpausing after auto_pause does not put auto_pause into effect again.</td>
</tr>
<tr>
<td>custom</td>
<td>String</td>
<td></td>
<td>Specify a custom parameter (see example).</td>
</tr>
<tr>
<td>earliest_time</td>
<td>String</td>
<td></td>
<td>Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a time string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Compare to index_earliest parameter. Also see comment for the search_mode parameter.</td>
</tr>
<tr>
<td>enable_lookups</td>
<td>Boolean</td>
<td>true</td>
<td>Indicates whether lookups should be applied to events.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifying true (the default) may slow searches significantly depending on the nature of the lookups.</td>
</tr>
<tr>
<td>exec_mode</td>
<td>Enum</td>
<td>normal</td>
<td>Valid values: (blocking</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If set to normal, runs an asynchronous search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If set to blocking, returns the sid when the job is complete.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If set to oneshot, returns results in the same call. In this case, you can specify the output (for example, json output) using the output_mode parameter as described in search/jobs/export. Default format for output is xml.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------</td>
<td>---------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>force_bundle_replication</td>
<td>Boolean</td>
<td>false</td>
<td>Specifies whether this search should cause (and wait depending on the value of sync_bundle_replication) bundle synchronization with all search peers.</td>
</tr>
<tr>
<td>id</td>
<td>String</td>
<td></td>
<td>Optional string to specify the search ID (&lt;sid&gt;). If unspecified, a random ID is generated.</td>
</tr>
<tr>
<td>index_earliest</td>
<td>String</td>
<td></td>
<td>Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based on the index time bounds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Compare to earliest_time parameter. Also see comment for the search_mode parameter.</td>
</tr>
<tr>
<td>index_latest</td>
<td>String</td>
<td></td>
<td>Specify a time string. Sets the latest (exclusive), respectively, time bounds for the search, based on the index time bounds.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Compare to latest_time parameter. Also see comment for the search_mode parameter.</td>
</tr>
<tr>
<td>indexedRealtime</td>
<td>Boolean</td>
<td></td>
<td>Indicate whether or not to used indexed-realtime mode for real-time searches.</td>
</tr>
<tr>
<td>indexedRealtimeOffset</td>
<td>Number</td>
<td></td>
<td>Set disk sync delay for indexed real-time search (seconds).</td>
</tr>
<tr>
<td>latest_time</td>
<td>String</td>
<td></td>
<td>Specify a time string. Sets the latest (exclusive), respectively, time bounds for the search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Compare to index_latest parameter. Also see comment for the search_mode parameter.</td>
</tr>
<tr>
<td>max_count</td>
<td>Number</td>
<td>10000</td>
<td>The number of events that can be accessible in any given status bucket. Also, in transforming mode, the maximum number of results to store. Specifically, codeoffset+count max_count.</td>
</tr>
<tr>
<td>max_time</td>
<td>Number</td>
<td>0</td>
<td>The number of seconds to run this search before finalizing. Specify 0 to never finalize.</td>
</tr>
<tr>
<td>namespace</td>
<td>String</td>
<td></td>
<td>The application namespace in which to restrict searches. The namespace corresponds to the identifier recognized in the /services/apps/local endpoint.</td>
</tr>
<tr>
<td>now</td>
<td>String</td>
<td>current system time</td>
<td>Specify a time string to set the absolute time used for any relative time specifier in the search. Default is current system time. You can specify a relative time modifier for this parameter. For example, specify +2d to specify the current time plus two days.</td>
</tr>
</tbody>
</table>
If you specify a relative time modifier both in this parameter and in the search string, the search string modifier takes precedence.

Refer to Time modifiers for search for details on specifying relative time modifiers.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reduce_freq</td>
<td>Number</td>
<td>0</td>
<td>Determines how frequently to run the MapReduce reduce phase on accumulated map values.</td>
</tr>
<tr>
<td>reload_macros</td>
<td>Boolean</td>
<td>true</td>
<td>Specifies whether to reload macro definitions from <code>macros.conf</code>. Default is true.</td>
</tr>
<tr>
<td>remote_server_list</td>
<td>String</td>
<td>empty list</td>
<td>Comma-separated list of (possibly wildcarded) servers from which raw events should be pulled. This server list is to be used in subsearches.</td>
</tr>
<tr>
<td>replay_speed</td>
<td>Number</td>
<td>greater than 0</td>
<td>Indicate a real-time search replay speed factor. For example, 1 indicates normal speed, 0.5 indicates normal speed, and 2 indicates twice as fast as normal. <strong>earliest_time</strong> and <strong>latest_time</strong> arguments must indicate a real-time time range to support replay options. Use <strong>replay_speed</strong> with <strong>replay_et</strong> and <strong>replay_lt</strong> relative times to indicate a speed and time range for the replay. For example, <code>replay_speed = 10</code> <code>replay_et = -d@d</code> <code>replay_lt = -@d</code> specifies a replay at 10x speed, as if the &quot;wall clock&quot; time starts yesterday at midnight and ends when it reaches today at midnight. For more information about using relative time modifiers, see Search time modifiers in the Search reference.</td>
</tr>
<tr>
<td>replay_et</td>
<td>Time modifier</td>
<td>string</td>
<td>Relative &quot;wall clock&quot; start time for the replay.</td>
</tr>
<tr>
<td>replay_lt</td>
<td>Time modifier</td>
<td>string</td>
<td>Relative end time for the replay clock. The replay stops when clock time reaches this time.</td>
</tr>
<tr>
<td>required_field_list</td>
<td>String</td>
<td>empty list</td>
<td>[Deprecated] Use <code>rf</code>. A comma-separated list of required fields that, even if not referenced or used directly by the search, is still included by the events and summary endpoints. Splunk Web uses these fields to prepopulate panels in the Search view.</td>
</tr>
<tr>
<td>reuse_max_seconds_ago</td>
<td>Number</td>
<td></td>
<td>Specifies the number of seconds ago to check when an identical search is started and return the job's search ID instead of starting a new job.</td>
</tr>
<tr>
<td>rf</td>
<td>String</td>
<td></td>
<td>Adds a required field to the search. There can be multiple <code>rf</code> POST arguments to the search. These fields, even if not referenced or used directly by the search, are still included by events and summary endpoints. Splunk Web uses these fields to prepopulate panels in the Search view.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>rt_blocking</td>
<td>Boolean</td>
<td>false</td>
<td>For a real-time search, indicates if the indexer blocks if the queue for this search is full.</td>
</tr>
<tr>
<td>rt_indexfilter</td>
<td>Boolean</td>
<td>true</td>
<td>For a real-time search, indicates if the indexer prefilters events.</td>
</tr>
<tr>
<td>rt_maxblocksecs</td>
<td>Number</td>
<td>60</td>
<td>For a real-time search with rt_blocking set to true, the maximum time to block.</td>
</tr>
<tr>
<td>rt_queue_size</td>
<td>Number</td>
<td>10000 events</td>
<td>For a real-time search, the queue size (in events) that the indexer should use for this search.</td>
</tr>
<tr>
<td>search_required</td>
<td>String</td>
<td></td>
<td>The search language string to execute, taking results from the local and remote servers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Examples:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;search *&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;search *</td>
</tr>
<tr>
<td>search_listener</td>
<td>String</td>
<td></td>
<td>Registers a search state listener with the search.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Use the format:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>search_state;results_condition;http_method;uri;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>search_listener=onResults.true;POST;/servicesNS/admin/search/saved/search/foobar/notify;</td>
</tr>
<tr>
<td>search_mode</td>
<td>Enum</td>
<td>normal</td>
<td>Valid values: (normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If set to real_time, search runs over live data. A real-time search may also be indicated by earliest_time and latest_time variables starting with 'rt' even if the search_mode is normal or is unset. For a real-time search, if both earliest_time and latest_time are exactly 'rt', the search represents all appropriate live data received since the start of the search. In addition, if earliest_time and/or latest_time are 'rt' followed by a relative time specifier, then a sliding window is used where the time bounds of the window are determined by the relative time specifiers and are continuously updated based on the wall-clock time.</td>
</tr>
<tr>
<td>spawn_process</td>
<td>Boolean</td>
<td>true</td>
<td>Specifies whether the search should run in a separate spawned process. Default is true.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Searches against indexes must run in a separate process.</td>
</tr>
<tr>
<td>status_buckets</td>
<td>Number</td>
<td>0</td>
<td>The most status buckets to generate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>0 indicates to not generate timeline information.</td>
</tr>
<tr>
<td>sync_bundle_replication</td>
<td>Boolean</td>
<td></td>
<td>Specifies whether this search should wait for bundle replication to complete.</td>
</tr>
<tr>
<td>time_format</td>
<td>String</td>
<td>%FT%T.%Q%:z</td>
<td>Used to convert a formatted time string from (start,end)_time into UTC seconds. The default value is ISO-8601 format.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>timeout</td>
<td>Number</td>
<td>86400</td>
<td>The number of seconds to keep this search after processing has stopped.</td>
</tr>
<tr>
<td>workload_pool</td>
<td>String</td>
<td></td>
<td>Specifies the new workload pool where the existing running search should be placed.</td>
</tr>
</tbody>
</table>

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sid</td>
<td>Search ID</td>
</tr>
</tbody>
</table>

**Application usage**

Refer to Creating searches using the REST API for information on using this endpoint and other search endpoints.

The search parameter is a search language string that specifies the search. Often you create a search specifying just the search parameter. Use the other parameters to customize a search to specific needs.

Use the returned `<sid>`, in the following endpoints to view and manage the search:

- `search/jobs/{search_id}`: View the status of this search job.
- `search/jobs/{search_id}/control`: Execute job control commands, such as pause, cancel, preview, and others.
- `search/jobs/{search_id}/events`: View a set of untransformed events for the search.
- `search/jobs/{search_id}/results`: View results of the search.
- `search/jobs/{search_id}/results_preview`: Preview results of a search that has not completed.
- `search/jobs/{search_id}/search.log`: View the log file generated by the search.
- `search/jobs/{search_id}/summary`: View field summary information.
- `search/jobs/{search_id}/timeline`: View event distribution over time.

You can also use the custom attribute to create custom job properties (see example).

For more information on searches, see the Splunk Search Reference.

**Example request and response**

**Request**

- **Basic example:**

  ```bash
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/jobs --data-urlencode search="search index=_internal source=*/metrics.log" -d id=mysearch_02151949 -d max_count=50000 -d status_buckets=300
  ``

- **Create custom property example:**

  ```bash
curl -u admin:changeme -k https://localhost:8089/services/search/jobs
  -d search="search *"
  -d custom.foobar="myCustomPropA"
  -d custom.foobaz="myCustomPropB"
  Use the search/jobs GET request to view the custom properties.
  ```

- **Create indexed real-time search with five second disk sync delay example:**

  ```bash
  ```
curl -k -u admin:changed https://localhost:8089/services/search/jobs
   -d search="search index=_* *"
   -d search_mode="realtime"
   -d indexedRealtime="1"
   -d indexedRealtimeOffset="300"

Response

<response><sid>mysearch_02151949</sid></response>

search/jobs/export

https://<host>:<mPort>/services/search/jobs/export

Stream search results as they become available.

The GET and POST operations on this endpoint perform a search identical to a POST to search/jobs. For parameter and returned value descriptions, see search/jobs.

GET

Performs a search identical to POST search/jobs

Request parameters

See the POST operation on search/jobs for parameter descriptions.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto_cancel</td>
<td>Number</td>
<td>See the POST parameter descriptions for search/jobs</td>
<td></td>
</tr>
<tr>
<td>auto_finalize_ec</td>
<td>Number</td>
<td>See the POST parameter descriptions for search/jobs</td>
<td></td>
</tr>
<tr>
<td>auto_pause</td>
<td>Number</td>
<td>See the POST parameter descriptions for search/jobs</td>
<td></td>
</tr>
<tr>
<td>earliest_time</td>
<td>String</td>
<td>See the POST parameter descriptions for search/jobs</td>
<td></td>
</tr>
<tr>
<td>enable_lookups</td>
<td>Bool</td>
<td>See the POST parameter descriptions for search/jobs</td>
<td></td>
</tr>
<tr>
<td>force_bundle_replication</td>
<td>Bool</td>
<td>See the POST parameter descriptions for search/jobs</td>
<td></td>
</tr>
<tr>
<td>id</td>
<td>String</td>
<td>See the POST parameter descriptions for search/jobs</td>
<td></td>
</tr>
<tr>
<td>index_earliest</td>
<td>String</td>
<td>Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based on the index time.</td>
<td></td>
</tr>
<tr>
<td>index_latest</td>
<td>String</td>
<td>Specify a time string. Sets the latest (inclusive), respectively, time bounds for the search, based on the index time.</td>
<td></td>
</tr>
</tbody>
</table>

The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. Refer to Time modifiers for search for information and examples of specifying a time string.
The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string.

Refer to Time modifiers for search for information and examples of specifying a time string.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>latest_time</td>
<td>String</td>
<td></td>
<td>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string.</td>
</tr>
<tr>
<td>max_time</td>
<td>Number</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>namespace</td>
<td>String</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>now</td>
<td>String</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>output_mode</td>
<td>Enum</td>
<td>xml</td>
<td>Valid values: (atom</td>
</tr>
<tr>
<td>reduce_freq</td>
<td>Number</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>reload_macros</td>
<td>Bool</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>remote_server_list</td>
<td>String</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>required_field_list</td>
<td>String</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>rf</td>
<td>String</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>rt_blocking</td>
<td>Bool</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>rt_indexfilter</td>
<td>Bool</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>rt_maxblocksecs</td>
<td>Number</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>rt_queue_size</td>
<td>Number</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>search</td>
<td>String</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>search_listener</td>
<td>String</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>search_mode</td>
<td>Enum</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>sync_bundle_replication</td>
<td>Bool</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>time_format</td>
<td>String</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
<tr>
<td>timeout</td>
<td>Number</td>
<td></td>
<td>See the POST parameter descriptions for search/jobs</td>
</tr>
</tbody>
</table>

**Application usage**

Performs a search identical to POST search/jobs, except the search streams results as they become available. Streaming of results is based on the search string.

For non-streaming searches, previews of the final results are available if preview is enabled. If preview is not enabled, it is better to use search/jobs with exec_mode=oneshot.

If it is too big, you might instead run with the search/jobs (not search/jobs/export) endpoint (it takes POST with the same parameters), maybe using the exec_mode=blocking. Then you can page through the results and request them from the server under your control, which is a better approach for extremely large result sets that need to be chunked.
Example of how to pass a variable to query when using REST API:

This is an example of running a saved search and passing a variable to it. In this case, the variable is host field:

```
$curl -k -u admin:password https://splunkserver:8089/services/search/jobs/export -d search="savedsearch \nMySavedSearch%20host%3Dwolverine"
```

(use "MySavedSearch" and input variable host=wolverine* )

I have a saved search named "MySavedSearch" the query of the search contains:

"index=main $host$ | head 100"

Example request and response

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/jobs/export -d search="search
index%3D_internal | head 1"
```

XML Response

```
<results preview='0'>
<meta>
 <fieldOrder>
 <field>_cd</field>
 <field>_indextime</field>
 <field>_raw</field>
 <field>_si</field>
 <field>_sourcetype</field>
 <field>_subsecond</field>
 <field>_time</field>
 <field>host</field>
 <field>Index</field>
 <field>linecount</field>
 <field>source</field>
 <field>sourcetype</field>
 <field>splunk_server</field>
 </fieldOrder>
</meta>
 <messages>
 <msg type="DEBUG">base lispy: [ AND index:_internal ]</msg>
 <msg type="DEBUG">search context: user="admin", app="search", bs-pathname="/Applications/splunk/etc"
 <msg type="INFO">Your timerange was substituted based on your search string</msg>
 </messages>
 <result offset='0'>
 <field k="_cd">
 <value><text>50:59480</text></value>
 </field>
 <field k="_indextime">
 <value><text>1333739623</text></value>
 </field>
 <field k="_raw">127.0.0.1 - admin [06/Apr/2012:12:13:42.943 -0700] "POST /servicesNS/admin/search/search/jobs/export HTTP/1.1" 200 2063 - - 317ms</value>
 <field k="_serial">
 <value><text>0</text></value>
 </field>
```

1104
POST

Performs a search identical to POST search/jobs. For parameter and returned value descriptions, see the POST parameter descriptions for search/jobs.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>search</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>auto_cancel</td>
<td>Number</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>auto_finalize_ec</td>
<td>Number</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>auto_pause</td>
<td>Number</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>earliest_time</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>enable_lookups</td>
<td>Bool</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>force_bundle_replication</td>
<td>Bool</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>id</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>index_earliest</td>
<td>String</td>
<td></td>
<td>Specify a time string. Sets the earliest (inclusive), respectively, time bounds for the search, based on the index time.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>---------</td>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>index_latest</td>
<td>String</td>
<td></td>
<td>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Refer to Time modifiers for search for information and examples of specifying a time string.</td>
</tr>
<tr>
<td>latest_time</td>
<td>String</td>
<td></td>
<td>Specify a time string. Sets the latest (inclusive), respectively, time bounds for the search, based on the index time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Refer to Time modifiers for search for information and examples of specifying a time string.</td>
</tr>
<tr>
<td>max_time</td>
<td>Number</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>namespace</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>now</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>output_mode</td>
<td>Enum</td>
<td>xml</td>
<td>Valid values: (atom</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the format for the returned output.</td>
</tr>
<tr>
<td>reduce_freq</td>
<td>Number</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>reload_macros</td>
<td>Bool</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>remote_server_list</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>required_field_list</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>rf</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>rt_blocking</td>
<td>Bool</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>rt_indexfilter</td>
<td>Bool</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>rt_maxblocksecs</td>
<td>Number</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>rt_queue_size</td>
<td>Number</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>search_listener</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>search_mode</td>
<td>Enum</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>sync_bundle_replication</td>
<td>Bool</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>time_format</td>
<td>String</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
<tr>
<td>timeout</td>
<td>Number</td>
<td></td>
<td>See the parameters and returned values for search/jobs.</td>
</tr>
</tbody>
</table>

**Returned values**

None

**Application usage**

Streaming of results is based on the search string.
For non-streaming searches, previews of the final results are available if preview is enabled. If preview is not enabled, it is better to use search/jobs with exec_mode=oneshot.

If it is too big, you might instead run with the search/jobs (not search/jobs/export) endpoint (it takes POST with the same parameters), maybe using the exec_mode=blocking. You'll then get back a search id, and then you can page through the results and request them from the server under your control, which is a better approach for extremely large result sets that need to be chunked.

Example of how to pass a variable to query when using REST API:

This is an example of running a saved search and passing a variable to it. In this case, the variable is host field:

```
$curl -k -u admin:password https://splunkserver:8089/services/search/jobs/export -d search="savedsearch \nMySavedSearch%20host%3Dwolverine""
```

(use "MySavedSearch" and input variable host=wolverine* )

I have a saved search named "MySavedSearch" the query of the search contains:

"index=main $host$ | head 100"

---

**search/jobs/{search_id}**

https://<host>:<mPort>/services/search/jobs/{search_id}

Manage the {search_id} search job.

DELETE

Delete the {search_id} search job.

Request parameters

None

Returned values

None

Application usage

{search_id} is the <sid> field returned from the GET operation for the search/jobs endpoint.

Example request and response

XML Request

```
curl -k -u admin:pass --request DELETE https://localhost:8089/services/search/jobs/mysearch_02151949
```

XML Response

```xml
<response><messages><msg type='INFO'>Search job cancelled.</msg></messages></response>
```
GET

Get information about the {search_id} search job.

Request parameters
None

Returned values
None

Application usage
The user ID is implied by the authentication to the call.

Information returned includes the search job properties, such as eventCount (number of events returned), runDuration (time the search took to complete), and others. The parameters to POST /search/jobs provides details on search job properties when creating a search. Search job properties are also described in View search job properties in the Search Manual.

The dispatchState property is of particular interest to determine the state of a search, and can contain the following values:

- QUEUED
- PARSING
- RUNNING
- PAUSED
- FINALIZING
- FAILED
- DONE

This operation also returns performance information for the search. For more information refer to View search job properties in the Search Manual.

For more information on searches in Splunk, refer to the Splunk Search Reference.

POST /search/jobs returns a <sid> for a search. You can also get a search ID from the <sid> field returned from GET search/jobs.

Example request and response
XML Request

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949
```

XML Response

```
<entry
   xmlns="http://www.w3.org/2005/Atom"
   xmlns:s="http://dev.splunk.com/ns/rest"
   xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
   <title>search index</title>
   <id>https://localhost:8089/services/search/jobs/mysearch_02151949</id>
   <updated>2011-07-07T20:49:58.000-07:00</updated>
   <link href="/services/search/jobs/mysearch_02151949" rel="alternate"/>
```
<s:dict>
  <s:key name="cursorTime">1969-12-31T16:00:00.000-08:00</s:key>
  <s:key name="dispatchState">DONE</s:key>
  <s:key name="dropCount">0</s:key>
  <s:key name="earliestTime">2011-07-07T11:18:08.000-07:00</s:key>
  <s:key name="eventAvailableCount">287</s:key>
  <s:key name="eventCount">287</s:key>
  <s:key name="eventFieldCount">6</s:key>
  <s:key name="eventIsStreaming">1</s:key>
  <s:key name="eventIsTruncated">0</s:key>
  <s:key name="eventSearch">search index</s:key>
  <s:key name="eventSorting">desc</s:key>
  <s:key name="isDone">1</s:key>
  <s:key name="isFailed">0</s:key>
  <s:key name="isFinalized">0</s:key>
  <s:key name="isPaused">0</s:key>
  <s:key name="isPreviewEnabled">0</s:key>
  <s:key name="isRealTimeSearch">0</s:key>
  <s:key name="isRemoteTimeline">0</s:key>
  <s:key name="isSaved">0</s:key>
  <s:key name="isSavedSearch">0</s:key>
  <s:key name="isZombie">0</s:key>
  <s:key name="keywords">index</s:key>
  <s:key name="latestTime">1969-12-31T16:00:00.000-08:00</s:key>
  <s:key name="numPreviews">0</s:key>
  <s:key name="priority">5</s:key>
  <s:key name="remoteSearch">litsearch index | fields keepcolororder=t "host" "index" "linecount" "source" "sourcetype" "splunk_server"</s:key>
  <s:key name="reportSearch"></s:key>
  <s:key name="resultCount">287</s:key>
  <s:key name="resultIsStreaming">1</s:key>
  <s:key name="resultPreviewCount">287</s:key>
  <s:key name="runDuration">1.004000</s:key>
  <s:key name="scanCount">287</s:key>
  <s:key name="sid">mysearch_02151949</s:key>
  <s:key name="statusBuckets">0</s:key>
  <s:key name="ttl">516</s:key>
  <s:key name="performance">
    <s:dict>
      <s:key name="duration_secs">0.004</s:key>
      <s:key name="invocations">4</s:key>
      <s:key name="input_count">287</s:key>
      <s:key name="output_count">287</s:key>
    </s:dict>
  </s:key>
</s:dict>
"command.search":
  
  "duration_secs": 0.089,
  "invocations": 4,
  "input_count": 0,
  "output_count": 287,

"command.search.fieldalias":
  
  "duration_secs": 0.002,
  "invocations": 2,
  "input_count": 287,
  "output_count": 287,

"command.search.index":
  
  "duration_secs": 0.005,
  "invocations": 4,

"command.search.kv":
  
  "duration_secs": 0.002,
  "invocations": 2,

"command.search.lookups":
  
  "duration_secs": 0.002,
  "invocations": 2,
  "input_count": 287,
  "output_count": 287,

"command.search.rawdata":
  
  "duration_secs": 0.083,
  "invocations": 2,

"command.search.tags":
  
  "duration_secs": 0.004,
  "invocations": 4,
  "input_count": 287,
  "output_count": 287,

"command.search.typer":
  
  "duration_secs": 0.004,
  "invocations": 4,
  "input_count": 287,
  "output_count": 287,

"dispatch.createProviderQueue":
  
  "duration_secs": 0.059,
<s:key name="invocations">1</s:key>
</s:dict>
<s:key>
<s:dict>
<s:key name="duration_secs">0.037</s:key>
<s:key name="invocations">1</s:key>
</s:dict>
</s:key>
<s:key name="dispatch.evaluate.search">
<s:dict>
<s:key name="duration_secs">0.036</s:key>
<s:key name="invocations">1</s:key>
</s:dict>
</s:key>
<s:key name="dispatch.fetch">
<s:dict>
<s:key name="duration_secs">0.092</s:key>
<s:key name="invocations">5</s:key>
</s:dict>
</s:key>
<s:key name="dispatch.readEventsInResults">
<s:dict>
<s:key name="duration_secs">0.110</s:key>
<s:key name="invocations">1</s:key>
</s:dict>
</s:key>
<s:key name="dispatch.stream.local">
<s:dict>
<s:key name="duration_secs">0.089</s:key>
<s:key name="invocations">4</s:key>
</s:dict>
</s:key>
<s:key name="dispatch.timeline">
<s:dict>
<s:key name="duration_secs">0.359</s:key>
<s:key name="invocations">5</s:key>
</s:dict>
</s:key>
</s:dict>
<s:key name="messages">
<s:dict/>
</s:key>
<s:key name="request">
<s:dict>
<s:key name="id">mysearch_02151949</s:key>
<s:key name="search">search index</s:key>
</s:dict>
</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>admin</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>admin</s:item>
</s:list>
</s:dict>
</s:key>
</s:dict>

1111
Update the \{search_id\} search job.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>custom.</strong>*</td>
<td>String</td>
<td>required</td>
<td>Specify custom job properties for the specified search job.</td>
</tr>
</tbody>
</table>

**Returned values**

None

**search/jobs/{search_id}/control**

https://<host>:[mPort]/services/search/jobs/{search_id}/control

Run a job control command for the \{search_id\} search.

**POST**

Run a job control command for the \{search_id\} search.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>action</strong></td>
<td>Enum</td>
<td></td>
<td>Valid values: (pause</td>
</tr>
</tbody>
</table>

The control action to execute.
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pause</td>
<td></td>
<td></td>
<td>Suspends the execution of the current search.</td>
</tr>
<tr>
<td>unpause</td>
<td></td>
<td></td>
<td>Resumes the execution of the current search, if paused.</td>
</tr>
<tr>
<td>finalize</td>
<td></td>
<td></td>
<td>Stops the search, and provides intermediate results to the /results endpoint.</td>
</tr>
<tr>
<td>cancel</td>
<td></td>
<td></td>
<td>Stops the current search and deletes the result cache.</td>
</tr>
<tr>
<td>touch</td>
<td></td>
<td></td>
<td>Extends the expiration time of the search to now + ttl</td>
</tr>
<tr>
<td>setttl</td>
<td></td>
<td></td>
<td>Change the ttl of the search. Arguments: ttl=&lt;number&gt;</td>
</tr>
<tr>
<td>setpriority</td>
<td></td>
<td></td>
<td>Sets the priority of the search process. Arguments: priority=&lt;0-10&gt;</td>
</tr>
<tr>
<td>enablepreview</td>
<td></td>
<td></td>
<td>Enable preview generation (may slow search considerably).</td>
</tr>
<tr>
<td>disablepreview</td>
<td></td>
<td></td>
<td>Disable preview generation.</td>
</tr>
<tr>
<td>save</td>
<td></td>
<td></td>
<td>saves the search job, storing search artifacts on disk for 7 days. Add or edit the default_save_ttl value in limits.conf to override the default value of 7 days.</td>
</tr>
<tr>
<td>unsave</td>
<td></td>
<td></td>
<td>Disables any action performed by save.</td>
</tr>
</tbody>
</table>

**Returned values**
None

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949/control -d action=pause

**XML Response**

<response><messages><msg type='INFO'>Search job paused.</msg></messages></response>

**search/jobs/{search_id}/events**

https://<host>:<mPort>/services/search/jobs/{search_id}/events

Get {search_id} search events.
## GET

Access `{search_id}` search events.

### Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Number</td>
<td>100</td>
<td>The maximum number of results to return. If value is set to 0, then all available results are returned. Default value is 100.</td>
</tr>
<tr>
<td>earliest_time</td>
<td>String</td>
<td></td>
<td>A time string representing the earliest (inclusive), respectively, time bounds for the results to be returned. If not specified, the range applies to all results found.</td>
</tr>
<tr>
<td>f</td>
<td>String</td>
<td></td>
<td>A field to return for the event set. You can pass multiple POST f arguments if multiple field are required. If field_list and f are provided, the union of the lists is used.</td>
</tr>
<tr>
<td>field_list</td>
<td>String</td>
<td>*</td>
<td>[Deprecated] Use f. A comma-separated list of the fields to return for the event set.</td>
</tr>
<tr>
<td>latest_time</td>
<td>String</td>
<td></td>
<td>A time string representing the latest (exclusive), respectively, time bounds for the results to be returned. If not specified, the range applies to all results found.</td>
</tr>
<tr>
<td>max_lines</td>
<td>Number</td>
<td>0</td>
<td>The maximum lines that any single event _raw field should contain. Specify 0 to specify no limit.</td>
</tr>
<tr>
<td>offset</td>
<td>Number</td>
<td>0</td>
<td>The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0. In 4.1+, negative offsets are allowed and are added to count to compute the absolute offset (for example, offset=-1 is the last available offset. Offsets in the results are always absolute and never negative.</td>
</tr>
<tr>
<td>output_mode</td>
<td>Enum</td>
<td>xml</td>
<td>Valid values: (atom</td>
</tr>
<tr>
<td>output_time_format</td>
<td>String</td>
<td>time_format</td>
<td>Formats a UTC time. Defaults to what is specified in time_format.</td>
</tr>
<tr>
<td>search</td>
<td>String</td>
<td></td>
<td>The post processing search to apply to results. Can be any valid search language string.</td>
</tr>
<tr>
<td>segmentation</td>
<td>String</td>
<td>raw</td>
<td>The type of segmentation to perform on the data. This includes an option to perform k/v segmentation.</td>
</tr>
<tr>
<td>time_format</td>
<td>String</td>
<td>%m/%d/%Y:%H:%M:%S</td>
<td>Expression to convert a formatted time string from {start,end}_time into UTC seconds.</td>
</tr>
<tr>
<td>truncation_mode</td>
<td>Enum</td>
<td>abstract</td>
<td>Valid values: (abstract</td>
</tr>
</tbody>
</table>

### Returned values

None
**Application usage**

These events are the data from the search pipeline before the first "transforming" search command. This is the primary method for a client to fetch a set of UNTRANSFORMED events for the search job.

This endpoint is only valid if the status_buckets > 0 or the search has no transforming commands.

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/search/jobs/1312313809.20/events --get -d f=arch -d f=build -d f=connectionType -d r -d count=3

**XML Response**

```xml
<results preview='0'>
<fieldOrder>
  <field>arch</field>
  <field>build</field>
  <field>connectionType</field>
  <field>date_hour</field>
</fieldOrder>
<meta>
</meta>
  <result offset='0'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
  <result offset='1'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
  <result offset='2'>
    <field k='arch'>
      <value><text>i686</text></value>
    </field>
    <field k='build'>
      <value><text>98164</text></value>
    </field>
    <field k='connectionType'>
      <value><text>cooked</text></value>
    </field>
    <field k='date_hour'>
      <value><text>19</text></value>
    </field>
  </result>
</results>
```

1115
search/jobs/{search_id}/results

https://<host>:<mPort>/services/search/jobs/{search_id}/results

Get {search_id} search results.

GET

Get {search_id} search results.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add_summary_to_metadata</td>
<td>Boolean</td>
<td>false</td>
<td>Set the value to &quot;true&quot; to include field summary statistics in the response.</td>
</tr>
<tr>
<td>count</td>
<td>Number</td>
<td>100</td>
<td>The maximum number of results to return. If value is set to 0, then all available results are returned.</td>
</tr>
<tr>
<td>f</td>
<td>String</td>
<td></td>
<td>A field to return for the event set. You can pass multiple POST f arguments if multiple field are required. If field_list and f are provided the union of the lists is used.</td>
</tr>
<tr>
<td>field_list</td>
<td>String</td>
<td></td>
<td>[Deprecated] Use f. Specify a comma-separated list of the fields to return for the event set.</td>
</tr>
<tr>
<td>offset</td>
<td>Number</td>
<td>0</td>
<td>The first result (inclusive) from which to begin returning data. This value is 0-indexed. Default value is 0. In 4.1+, negative offsets are allowed and are added to count to compute the absolute offset (for example, offset=-1 is the last available offset). Offsets in the results are always absolute and never negative.</td>
</tr>
<tr>
<td>output_mode</td>
<td>Enum</td>
<td>xml</td>
<td>Valid values: (atom</td>
</tr>
<tr>
<td>search</td>
<td>String</td>
<td></td>
<td>The post processing search to apply to results. Can be any valid search language string.</td>
</tr>
</tbody>
</table>

Returned values
None
**Application usage**
This is the table that exists after all processing from the search pipeline has completed.

This is the primary method for a client to fetch a set of TRANSFORMED events. If the dispatched search does not include a transforming command, the effect is the same as get_events, however with fewer options.

**Example request and response**

**JSON request**

```bash
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949/results --get -d f=index -d f=source -d f=sourcetype -d count=3 -d output_mode=json
```

**JSON response**

```json
{
  "init_offset": 0,
  "messages": [{ "text": "base lispy: [ AND index:_internal source::*metrics.log ]", "type": "DEBUG" }, { "text": "search context: user=\"admin\", app=\"search\", bs-pathname=\"/Applications/splunk/etc\"", "type": "DEBUG" }]
},
"preview": false,
"results": [{ "index": "_internal", "source": "/Applications/splunk/var/log/splunk/metrics.log", "sourcetype": "splunkd" }, { "index": "_internal", "source": "/Applications/splunk/var/log/splunk/metrics.log", "sourcetype": "splunkd" }, { "index": "_internal", "source": "/Applications/splunk/var/log/splunk/metrics.log", "sourcetype": "splunkd" }
]
}
```

**search/jobs/{search_id}/results_preview**

https://<host>:<mPort>/services/search/jobs/{search_id}/results_preview

Preview {search_id} search results.

**GET**

Preview {search_id} search results.

**Request parameters**
<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add_summary_to_metadata</td>
<td>Boolean</td>
<td>false</td>
<td>Set the value to &quot;true&quot; to include field summary statistics in the response.</td>
</tr>
<tr>
<td>count</td>
<td>Number</td>
<td>100</td>
<td>The maximum number of results to return.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>If value is set to 0, then all available results are returned.</td>
</tr>
<tr>
<td>f</td>
<td>String</td>
<td></td>
<td>A field to return for the event set.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>You can pass multiple POST f arguments if multiple field are required. If</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>field_list and f are provided the union of the lists is used.</td>
</tr>
<tr>
<td>field_list</td>
<td>String</td>
<td></td>
<td>[Deprecated] Use f.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A comma-separated list of the fields to return for the event set.</td>
</tr>
<tr>
<td>offset</td>
<td>Number</td>
<td>0</td>
<td>The first result (inclusive) from which to begin returning data.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This value is 0-indexed. Default value is 0.</td>
</tr>
<tr>
<td>output_mode</td>
<td>Enum</td>
<td>xml</td>
<td>Valid values: (atom</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies the format for the returned output.</td>
</tr>
<tr>
<td>search</td>
<td>String</td>
<td></td>
<td>The post processing search to apply to results. Can be any valid search</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>language string.</td>
</tr>
</tbody>
</table>

**Returned values**

None

**Application usage**

Returns the intermediate preview results of the search specified by {search_id}. When the job is complete, this gives the same response as /search/jobs/{search_id}/results. Preview is enabled for real-time searches and for searches where status_buckets > 0.

**Example request and response**

**JSON request**

```
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949/results_preview --get -d f=index -d f=source -d f=sourcetype -d count=3 -d output_mode=json
```

**JSON response**

```
{
  "init_offset" : 0,
  "messages" : [
    { "text" : "base lispy: [ AND index:_internal source:*/metrics.log ]",
      "type" : "DEBUG"
    },
    { "text" : "search context: user=admin, app=search, bs-pathname=/Applications/splunk/etc",
      "type" : "DEBUG"
    }
  ],
  "preview" : false,
  "results" : [
    { "index" : "_internal",
      "source" : "/Applications/splunk/var/log/splunk/metrics.log",
      "sourcetype" : "splunkd"
    }
  ]
}
```

1118
search/jobs/{search_id}/search.log

https://<host>:<mPort>/services/search/jobs/{search_id}/search.log

Get the {search_id} search log.

GET

Get the {search_id} search log.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>attachment</td>
<td>Boolean</td>
<td>false</td>
<td>If true, returns search.log as an attachment. Otherwise, streams search.log.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

Request

curl -k -u admin:pass https://localhost:8089/services/search/jobs/mysearch_02151949/search.log

Response

07-07-2011 21:36:22.066 INFO ApplicationManager - Found application directory: /Applications/splunk4.3/etc/apps/user-prefs
07-07-2011 21:36:22.066 INFO ApplicationManager - Initialized at least 12 applications: /Applications/splunk4.3/etc/apps
07-07-2011 21:36:22.066 INFO ApplicationManager - Found 5 application(s) that might have global exports
07-07-2011 21:36:22.073 INFO dispatchRunner - initing LicenseMgr in search process: nonPro=0
07-07-2011 21:36:22.074 INFO LicenseMgr - Initing LicenseMgr
07-07-2011 21:36:22.075 INFO ServerConfig - My GUID is "1F3A34AE-75DA-4680-B184-5BF309843919".
07-07-2011 21:36:22.075 INFO ServerConfig - My hostname is "ombroso-mbp15.local".
07-07-2011 21:36:22.077 INFO SSLCommon - added zlib compression
07-07-2011 21:36:22.077 INFO LMConfig - serverName=mbp15.splunk.com guid=1F3A34AE-75DA-4680-B184-5BF309843919
07-07-2011 21:36:22.077 INFO LMConfig - connection_timeout=30
07-07-2011 21:36:22.077 INFO LMConfig - send_timeout=30

1119
search/jobs/{search_id}/summary

https://<host>:<mPort>/services/search/jobs/{search_id}/summary

Get the getFieldsAndStats output of the events to-date, for the search_id search.

GET

Get the getFieldsAndStats output of the events to-date, for the search_id search.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>earliest_time</td>
<td>String</td>
<td></td>
<td>Time string representing the earliest (inclusive), respectively, time bounds for the search. The time string can be either a UTC time (with fractional seconds), a relative time specifier (to now) or a formatted time string. (Also see comment for the search_mode variable.)</td>
</tr>
<tr>
<td>f</td>
<td>String</td>
<td></td>
<td>A field to return for the event set. You can pass multiple POST f arguments if multiple field are required. If field_list and f are provided, the union of the lists is used.</td>
</tr>
<tr>
<td>field_list</td>
<td>String</td>
<td></td>
<td>[Deprecated] Use f. A comma-separated list of the fields to return for the event set.</td>
</tr>
<tr>
<td>histogram</td>
<td>Boolean</td>
<td>false</td>
<td>Indicates whether to add histogram data to the summary output.</td>
</tr>
<tr>
<td>latest_time</td>
<td>String</td>
<td></td>
<td>Time string representing the latest (exclusive), respectively, time bounds for the search.</td>
</tr>
<tr>
<td>min_freq</td>
<td>Number</td>
<td>0</td>
<td>For each key, the fraction of results this key must occur in to be displayed. Express the fraction as a number between 0 and 1.</td>
</tr>
<tr>
<td>output_time_format</td>
<td>String</td>
<td>time_format</td>
<td>Formats a UTC time.</td>
</tr>
<tr>
<td>search</td>
<td>String</td>
<td>Empty string</td>
<td>Specifies a substring that all returned events should contain either in one of their values or tags.</td>
</tr>
<tr>
<td>time_format</td>
<td>String</td>
<td>%m/%d/%Y:%H:%M:%S</td>
<td>Expression to convert a formatted time string from {start,end}_time into UTC seconds.</td>
</tr>
<tr>
<td>top_count</td>
<td>Number</td>
<td>10</td>
<td>For each key, specifies how many of the most frequent items to return.</td>
</tr>
</tbody>
</table>

Returned values
None

Application usage
This endpoint is only valid when status_buckets > 0. To guarantee a set of fields in the summary, when creating the search, use the required_fields_list or rf parameters.
Example request and response

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mytestsid/summary --get -d f=source -d f=sourcetype -d f=host -d top_count=5
```

**XML Response**

```xml
<?xml version='1.0' encoding='UTF-8'?>
<summary earliest_time='1969-12-31T16:00:00.000-08:00' latest_time='1969-12-31T16:00:00.464-08:00'
duration='0' c='150375'>
  <field k='host' c='150375' nc='0' dc='1' exact='1'>
    <modes>
      <value c='150375' exact='1'><text>tiny</text></value>
    </modes>
  </field>
  <field k='source' c='150375' nc='0' dc='13' exact='1'>
    <modes>
      <value c='136107' exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/metrics.log</text></value>
      <value c='6682' exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/splunkd_access.log</text></value>
      <value c='4656' exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/scheduler.log</text></value>
      <value c='1714' exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/web_access.log</text></value>
      <value c='937' exact='1'><text>/mnt/scsi/steveyz/splunksi/var/log/splunk/splunkd.log</text></value>
    </modes>
  </field>
  <field k='sourcetype' c='150375' nc='0' dc='10' exact='1'>
    <modes>
      <value c='137053' exact='1'><text>splunkd</text></value>
      <value c='6682' exact='1'><text>splunkd_access</text></value>
      <value c='4656' exact='1'><text>scheduler</text></value>
      <value c='1714' exact='1'><text>web_access</text></value>
      <value c='193' exact='1'><text>splunk_web_service</text></value>
    </modes>
  </field>
</summary>
```

**search/jobs/{search_id}/timeline**

https://<host>:<mPort>/services/search/jobs/{search_id}/timeline

Get event distribution over time of the untransformed events read to-date, for the search_id search.

**GET**

Get event distribution over time of the untransformed events read to-date, for the search_id search.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>output_time_format</td>
<td>String</td>
<td>time_format</td>
<td>Formats a UTC time.</td>
</tr>
<tr>
<td>time_format</td>
<td>String</td>
<td>%m%d%Y:%H:%M:%S</td>
<td>Expression to convert a formatted time string from [start,end]_time into UTC seconds.</td>
</tr>
</tbody>
</table>

**Returned values**

None
The output from this endpoint provides values for the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>c</td>
<td>Event count</td>
</tr>
<tr>
<td>a</td>
<td>Available. Not all events in a bucket are retrievable. Generally capped at 10000.</td>
</tr>
<tr>
<td>t</td>
<td>Time in epoch seconds</td>
</tr>
<tr>
<td>d</td>
<td>Bucket size (time)</td>
</tr>
<tr>
<td>f</td>
<td>Indicates if the search finished scanning events from the time range of this bucket.</td>
</tr>
<tr>
<td>etz</td>
<td>Timezone offset, in seconds, for the earliest time of this bucket.</td>
</tr>
<tr>
<td>ltz</td>
<td>Timezone offset, in seconds, for the latest time of this bucket.</td>
</tr>
</tbody>
</table>

**Application usage**

This endpoint is only valid when status_buckets > 0. To guarantee a set of fields in the summary, when creating the search, use the required_fields_list or rf parameters.

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/search/jobs/mytestsid/timeline --get -d
time_format="%c"
```

**XML Response**

```xml
<timeline c='150397' cursor='1312308000'>
  <bucket c='7741' a='7741' t='1312308000.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 11:00:00 2011</bucket>
  <bucket c='7894' a='7894' t='1312311600.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 12:00:00 2011</bucket>
  <bucket c='7406' a='7406' t='1312315200.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 13:00:00 2011</bucket>
  <bucket c='6097' a='6097' t='1312318800.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 14:00:00 2011</bucket>
  <bucket c='6072' a='6072' t='1312322400.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 15:00:00 2011</bucket>
  <bucket c='6002' a='6002' t='1312326000.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 16:00:00 2011</bucket>
  <bucket c='6004' a='6004' t='1312329600.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 17:00:00 2011</bucket>
  <bucket c='5994' a='5994' t='1312333200.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 18:00:00 2011</bucket>
  <bucket c='6037' a='6037' t='1312336800.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 19:00:00 2011</bucket>
  <bucket c='6021' a='6021' t='1312340400.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 20:00:00 2011</bucket>
  <bucket c='6051' a='6051' t='1312344000.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 21:00:00 2011</bucket>
  <bucket c='6006' a='6006' t='1312347600.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 22:00:00 2011</bucket>
  <bucket c='6041' a='6041' t='1312351200.000' d='3600' f='1' etz='-25200' ltz='-25200'>Tue Aug  2 23:00:00 2011</bucket>
</timeline>

1122
search/parser

https://<host>:<mPort>/services/search/parser

Get search language parsing.

**GET**

Parses Splunk search language and returns semantic map.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_lookups</td>
<td>Boolean</td>
<td>false</td>
<td>If true, reverse lookups are done to expand the search expression.</td>
</tr>
<tr>
<td>output_mode</td>
<td>String</td>
<td>xml</td>
<td>Specify output formatting. Select from either:</td>
</tr>
<tr>
<td>parse_only</td>
<td>Boolean</td>
<td>false</td>
<td>If true, disables expansion of search due evaluation of subsearches, time term expansion, lookups, tags, eventtypes, sourcetype alias.</td>
</tr>
<tr>
<td>q required</td>
<td>String</td>
<td></td>
<td>The search string to parse.</td>
</tr>
<tr>
<td>reload_macros</td>
<td>Boolean</td>
<td>true</td>
<td>If true, reload macro definitions from macros.conf.</td>
</tr>
</tbody>
</table>

**Returned values**

None
Example request and response

JSON Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/parser --get -d output_mode=json -d q="search index=os sourcetype=cpu"

JSON Response

```json
{
  "remoteSearch": "litsearch | fields keepcolororder=t \"host\" \"index\" \"linecount\" \"source\" \"sourcetype\" \"splunk_server\"",
  "remoteTimeOrdered": true,
  "eventsSearch": "search ",
  "eventsTimeOrdered": true,
  "eventsStreaming": true,
  "reportsSearch": "",
  "commands": [
    {
      "command": "search",
      "rawargs": "",
      "pipeline": "streaming",
      "args": {
        "search": [""],
      },
      "isGenerating": true,
      "streamType": "SP_STREAM",
    },
  ]
}
```

search/scheduler

https://<host>:<mPort>/services/search/scheduler

GET

Get current search scheduler enablement status.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>saved_searches_disabled</td>
<td>Boolean</td>
<td>0 or 1</td>
<td>A boolean value indicating whether the search scheduler is disabled.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8089/services/search/scheduler

XML Response

<title>scheduler</title>
<id>https://localhost:8089/services/search/scheduler</id>
<updated>2015-06-09T13:23:38-07:00</updated>
<generator build="6cfc0237739f" version="6.3.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/search/scheduler/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>scheduler</title>
<id>https://localhost:8089/services/search/scheduler/scheduler</id>
<updated>2015-06-09T13:23:38-07:00</updated>
<link href="/services/search/scheduler/scheduler" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/search/scheduler/scheduler" rel="list"/>
<link href="/services/search/scheduler/scheduler" rel="edit"/>
<content type="text/xml">
  <s:dict>
    <s:key name="disabled">0</s:key>
    <s:key name="eai:acl">
      <s:dict>
        <s:key name="app"></s:key>
        <s:key name="can_list">1</s:key>
        <s:key name="can_write">1</s:key>
        <s:key name="modifiable">0</s:key>
        <s:key name="owner">system</s:key>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
            <s:key name="write">
              <s:list>
                <s:item>admin</s:item>
                <s:item>splunk-system-role</s:item>
              </s:list>
            </s:key>
            <s:key name="removable">0</s:key>
            <s:key name="sharing">system</s:key>
          </s:dict>
        </s:key>
        <s:key name="saved_searches_disabled">0</s:key>
      </s:dict>
    </s:key>
  </s:dict>
</content>
</entry>
search/scheduler/status

https://<host>:<mPort>/services/search/scheduler/status
Enable or disable the search scheduler.

POST
Enable or disable the search scheduler.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Indicates whether to disable the search scheduler. 0 enables the search scheduler. 1 disables the search scheduler.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

curl -ku admin:pass -XPOST https://localhost:8089/services/search/scheduler/status -d disabled=1

XML Response

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
><title>scheduler</title>
<id>https://localhost:8089/services/search/scheduler</id>
<updated>2015-06-09T13:40:21-07:00</updated>
<generator build="6cfc0237739f" version="6.3.0"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/search/scheduler/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
</feed>
search/timeparser

https://<host>:<mPort>/services/search/timeparser
Get time argument parsing.

GET

Get a lookup table of time arguments to absolute timestamps.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>now</td>
<td>String</td>
<td></td>
<td>The time to use as current time for relative time identifiers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Can itself either be a relative time (from the real &quot;now&quot; time) or an absolute time in the format specified by time_format.</td>
</tr>
<tr>
<td>output_time_format</td>
<td>String</td>
<td>%FT%T.%Q%:z</td>
<td>Used to format a UTC time. Defaults to the value of time_format.</td>
</tr>
<tr>
<td>time</td>
<td>String</td>
<td></td>
<td>The time argument to parse.</td>
</tr>
<tr>
<td>required</td>
<td></td>
<td></td>
<td>Acceptable inputs are either a relative time identifier or an absolute time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Multiple time arguments can be passed by specifying multiple time parameters.</td>
</tr>
<tr>
<td>time_format</td>
<td>String</td>
<td>%FT%T.%Q%:z</td>
<td>The format (strftime) of the absolute time format passed in time.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>This field is not used if a relative time identifier is provided. For absolute times, the default value is the ISO-8601 format.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/timeparser --get -d time=-12h -d time=-24h
```

XML Response

```
<response>
  <dict>
    <key name="-12h">2011-07-06T21:54:23.000-07:00</key>
    <key name="-24h">2011-07-06T09:54:23.000-07:00</key>
  </dict>
</response>
```
search/typeahead

https://<host>:<mPort>/services/search/typeahead

Get search string auto-complete suggestions.

GET

Get a list of words or descriptions for possible auto-complete terms.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>Number</td>
<td></td>
<td>The number of items to return for this term.</td>
</tr>
<tr>
<td>output_mode</td>
<td>String</td>
<td>csv</td>
<td>Specify output formatting. Select from:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>csv: CSV formatting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>xml: XML formatting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>json: JSON formatting</td>
</tr>
<tr>
<td>prefix</td>
<td>String</td>
<td></td>
<td>The term for which to return typeahead results.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

JSON Request

curl -k -u admin:pass https://localhost:8089/servicesNS/admin/search/search/typeahead --get -d count=3 -d prefix=source -d output_mode=json

JSON Response

```json
{
  "results": [
    {
      "content": "source="sampledata.zip:/apache1.splunk.com/access_combined.log"",
      "count": 9199,
      "operator": false
    },
    {
      "content": "source="sampledata.zip:/apache2.splunk.com/access_combined.log"",
      "count": 27705,
      "operator": false
    },
    {
      "content": "source="sampledata.zip:/apache3.splunk.com/access_combined.log"",
      "count": 27888,
      "operator": false
    }
  ]
}
```
System endpoints

System endpoint descriptions

Manage server configuration settings and messages.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select Settings > Access controls and click Users. To determine the capabilities assigned to a role, select Settings > Access controls and click Roles.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

Additional introspection information

See Introspection endpoint descriptions for the system endpoints related to introspection.

Splunk Cloud URL for REST API access

Splunk Cloud has a different host and management port syntax than Splunk Enterprise. Depending on your deployment type, use one of the following options to access REST API resources.

Managed Splunk Cloud deployments

https://<deployment-name>.splunkcloud.com:8089

Self-service Splunk Cloud deployments

To get the required credentials, submit a support case on the Support Portal. After installing the credentials, use the following URL.

https://input-<deployment-name>.cloud.splunk.com:8089

See Using the REST API in Splunk Cloud in the the Splunk REST API Tutorials for more information.
messages

https://<host>:<mPort>/services/messages

Access and create system messages. Most messages are created by splunkd to inform the user of system information, including license quotas, license expirations, misconfigured indexes, and disk space. Splunk Web displays these as bulletin board messages.

GET

Show systemwide messages.

Request parameters

Pagination and filtering parameters can be used with this method.

Response keys

Depending on the system status, messages returned vary. Messages returned in the response include a name and description, as in the following example.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;message_name&gt;</td>
<td>The message name depends on the specific message returned. This field might contain the same text as the message field. In the following example response, this field is &quot;manifest_error&quot;.</td>
</tr>
<tr>
<td>server</td>
<td>Name of the server that generated the error</td>
</tr>
<tr>
<td>severity</td>
<td>One of the following message severity values</td>
</tr>
<tr>
<td></td>
<td>• info</td>
</tr>
<tr>
<td></td>
<td>• warn</td>
</tr>
<tr>
<td></td>
<td>• error</td>
</tr>
<tr>
<td>timeCreated(epochSecs)</td>
<td>Timestamp when the message was posted</td>
</tr>
<tr>
<td>timeCreated_iso</td>
<td>ISO formatted timestamp</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changed https://localhost:8089/services/admin/messages

XML Response

<entry>
...
POST

Create a persistent message displayed at /services/messages.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;name&gt;</td>
<td>String</td>
<td>Required. Message name (key).</td>
</tr>
<tr>
<td>capability</td>
<td>Comma separated list</td>
<td>One or more capabilities that users must have to view the message. Capability names are validated.</td>
</tr>
<tr>
<td>role</td>
<td>Comma separated list</td>
<td>One or more roles that users must have to view the message. Role names are validated.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>value</td>
<td>String</td>
<td>Required. Message text.</td>
</tr>
</tbody>
</table>
| severity | String | One of the following message severity values.  
  • info  
  • warn  
  • error |

Response keys  
None

Example request and response

XML Request

```bash
curl -k -u admin:changeme https://localhost:8089/services/messages -d name=helloMessage -d value="hello world" -d severity="info"
```

XML Response

```xml
tenent type="text/xml">
   <s:dict>
      <s:key name="helloMessage">"hello world"</s:key>
      <s:key name="eai:acl”>
         ... elided ...
      </s:key>
      <s:key name="message">"hello world"</s:key>
      <s:key name="severity">info</s:key>
      <s:key name="timeCreated_epochSecs">1392920642</s:key>
   </s:dict>
</content>
</entry>
```

1132
messages/{name}

https://<host>:<mPort>/services/messages/{name}

Manage the message associated with the {name} message ID.

DELETE

Delete the specified message.

Request parameters
None

Response keys
None. An HTTP status code = 500 is returned if {name} message does not exist.

Example request and response

XML Request

```
curl -k -u admin:changeme --request DELETE https://localhost:8089/services/messages/message
```

XML Response

```
...
<id>https://localhost:8089/services/messages</id>
<updated>2011-07-08T01:14:21-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/messages/_new" rel="create"/>
  ... opensearch elements elided ...
<s:messages/>
```

GET

Get details of the specified message.

Request parameters
None

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1133</td>
<td></td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>help</td>
<td>For internal use only</td>
</tr>
<tr>
<td>&lt;message_name&gt;</td>
<td>The message name depends on the specific message returned. This field might contain the same text as the message field. In the following example response, this field is &quot;manifest_error&quot;.</td>
</tr>
<tr>
<td>message</td>
<td>Message text</td>
</tr>
<tr>
<td>server</td>
<td>One of the server that generated the error</td>
</tr>
<tr>
<td>severity</td>
<td>One of the following message severity values</td>
</tr>
<tr>
<td>timeCreated_epochSecs</td>
<td>Timestamp when the message was posted</td>
</tr>
<tr>
<td>timeCreated_iso</td>
<td>ISO formatted timestamp</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -k -u admin:changed https://localhost:8089/services/admin/messages/manifest_error
```

**XML Response**

```xml
... <title>messages</title>  <id>https://localhost:8089/services/admin/messages</id>  <updated>2016-09-01T13:10:59-07:00</updated>  <generator build="3b17605ee8e3" version="6.5.0"/>  <author>  <name>Splunk</name>  </author>  <link href="/services/admin/messages/_new" rel="create"/>  <link href="/services/admin/messages/_acl" rel="_acl"/>  <opensearch:totalResults>1</opensearch:totalResults>  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>  <opensearch:startIndex>0</opensearch:startIndex>  <s:messages/>  <entry>  <title>manifest_error</title>  <id>https://localhost:8089/services/admin/messages/manifest_error</id>  <updated>2016-09-01T13:10:59-07:00</updated>  <link href="/services/admin/messages/manifest_error" rel="alternate"/>  <author>  <name>system</name>  </author>  <link href="/services/admin/messages/manifest_error" rel="remove"/>  <content type="text/xml">  <s:dict>  <s:key name="eai:acl">  <s:dict>  <s:key name="app"></s:key>  <s:key name="can_list">1</s:key>  <s:key name="can_write">1</s:key>  <s:key name="modifiable">0</s:key>  </s:dict>  </s:dict></s:dict>
```
server/control

https://<host>:<mPort>/services/server/control

List available controls.

GET

List actions that can be performed at this endpoint.

Request parameters
None

Response keys
None

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/control

XML Response


<title>server-control</title>
{id>https://localhost:8089/services/server/control</id>
<updated>2011-07-12T00:17:53-07:00</updated>
<generator version="102807"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/control/restart" rel="restart"/>
  ... opensearch elements elided ...
<s:messages/>

server/control/restart

https://<host>:<mPort>/services/server/control/restart
Restart the splunkd server daemon and Splunk Web interface. The POST operation is equivalent to the splunk restart CLI command.

See also server/control/restart_webui

POST

Restart the splunkd server daemon and Splunk Web interface.

Request parameters
None

Response keys
An HTTP status code 200 indicates successful restart.

Example request and response

XML Request
curl -k -u admin:changeme https://localhost:8089/services/server/control/restart -X POST

XML Response

server/control/restart_webui

https://<host>:<mPort>/services/server/control/restart_webui

Restart the Splunk Web interface. This interface is equivalent to the splunk restart splunkweb CLI command, and restarts the Web interface on servers with the default app server mode set. See also server/control/restart

POST

Restart the Splunk Web interface.

Request parameters
None

Response keys
An HTTP status code 200 indicates successful restart.

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/control/restart_webui -X POST

XML Response

...
server/httpsettings/proxysettings

https://<host>:<mPort>/services/server/httpsettings/proxysettings
Create an HTTP Proxy Server configuration for splunkd.

Authentication and Authorization
Requires the edit_server capability.

POST
Create a HTTP Proxy server configuration stanza for use with splunkd.

The POST request generates a proxyConfig configuration that you can access or update at server/settings/httpsettings/proxysettings/proxyConfig.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>String</td>
<td>Required. Use “proxyConfig” to name the configuration stanza.</td>
</tr>
</tbody>
</table>

Returned values
None

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/httpsettings/proxysettings -d name="proxyConfig"

XML Response

<entry>
  <title>proxyConfig</title>
  <id>https://localhost:8089/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="https://localhost:8089/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
</entry>
server/httpsettings/proxysettings/proxyConfig

https://<host>:<mPort>/services/server/httpsettings/proxysettings/proxyConfig

Access, update, or delete the HTTP Proxy Server configurations for splunkd including http_proxy, https_proxy and no_proxy.

Authentication and Authorization
All operations on this endpoint require the edit_server capability.
GET

Access the `{proxyConfig}` HTTP proxy server configurations for splunkd.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http_proxy</td>
<td>String</td>
<td>Identifies the server proxy. When set, splunkd sends all HTTP requests through the proxy server defined in <code>http_proxy</code> on the proxy. The default value is unset.</td>
</tr>
<tr>
<td>https_proxy</td>
<td>String</td>
<td>Identifies the server proxy. When set, splunkd sends all HTTPS requests through the proxy server defined in <code>https_proxy</code>. If not set, splunkd uses the <code>http_proxy</code> variable instead. The default value is unset.</td>
</tr>
<tr>
<td>no_proxy</td>
<td>String</td>
<td>Identifies the no proxy rules. When set, splunkd uses these rules to decide whether the proxy server needs to be bypassed for matching hosts and IP addresses. Requests going to a localhost/loopback address are not proxied. The default value is localhost, 127.0.0.1, ::1.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:changed https://localhost:8089/services/server/httpsettings/proxysettings -d name="proxyConfig"
``` 

XML Response

```
<entry>
  <title>proxyConfig</title>
  <id>https://localhost:8089/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/edit" rel="edit"/>
  <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/remove" rel="remove"/>
  <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/move" rel="move"/>
  <link href="/servicesNS/nobody/search/server/httpsettings/proxysettings/proxyConfig/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:pair name="disabled" value="0"/>
      <s:pair name="eai:can_change_perms" value="1"/>
      <s:pair name="eai:can_list" value="1"/>
      <s:pair name="eai:can_share_app" value="1"/>
      <s:pair name="eai:can_share_global" value="1"/>
      <s:pair name="eai:can_share_user" value="0"/>
      <s:pair name="eai:can_write" value="1"/>
    </s:dict>
  </content>
</entry>
```
POST

Update the {proxyConfig} HTTP proxy server configurations for splunkd.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>http_proxy</td>
<td>String</td>
<td>Identifies the server proxy. When set, splunkd sends all HTTP requests through the proxy server defined in http_proxy on the proxy. The default value is unset.</td>
</tr>
<tr>
<td>https_proxy</td>
<td>String</td>
<td>Identifies the server proxy. When set, splunkd sends all HTTPS requests through the proxy server defined in https_proxy. If not set, splunkd uses the http_proxy variable instead. The default value is unset.</td>
</tr>
<tr>
<td>no_proxy</td>
<td>String</td>
<td>Identifies the no proxy rules. When set, splunkd uses these rules to decide whether the proxy server needs to be bypassed for matching hosts and IP addresses. Requests going to a localhost/loopback address are not proxied. The default value is localhost, 127.0.0.1, ::1.</td>
</tr>
</tbody>
</table>
Returned values
None

Example request and response

XML Request

curl -k -u admin:changed https://localhost:8089/services/server/httpssettings/proxysettings -d no_proxy="test"

XML Response

<entry>
<title>proxyConfig</title>
<id>https://localhost:8089/servicesNS/nobody/search/server/httpssettings/proxysettings/proxyConfig</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/servicesNS/nobody/search/server/httpssettings/proxysettings/proxyConfig" rel="alternate"/>
<author>
<name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/server/httpssettings/proxysettings/proxyConfig" rel="list"/>
<link href="/servicesNS/nobody/search/server/httpssettings/proxysettings/proxyConfig/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/server/httpssettings/proxysettings/proxyConfig" rel="edit"/>
<link href="/servicesNS/nobody/search/server/httpssettings/proxysettings/proxyConfig" rel="remove"/>
<link href="/servicesNS/nobody/search/server/httpssettings/proxysettings/proxyConfig/move" rel="move"/>
<link href="/servicesNS/nobody/search/server/httpssettings/proxysettings/proxyConfig/disable" rel="disable"/>
<content type="text/xml">  
<s:dict>
  <s:key name="disabled">0</s:key>
  <s:key name="eai:acl">
    <s:key name="app">search</s:key>
    <s:dict>
      <s:key name="can_change_perms">1</s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_share_app">1</s:key>
      <s:key name="can_share_global">1</s:key>
      <s:key name="can_share_user">0</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">1</s:key>
      <s:key name="owner">nobody</s:key>
      <s:dict>
        <s:key name="perms">
          <s:dict>
            <s:key name="read">
              <s:list>
                <s:item>*</s:item>
              </s:list>
            </s:key>
            <s:dict>
              <s:key name="write">
                <s:list>
                  <s:item>*</s:item>
                </s:list>
              </s:key>
            </s:dict>
            <s:key name="removable">1</s:key>
            <s:key name="sharing">app</s:key>
          </s:dict>
        </s:key>
      </s:dict>
    </s:dict>
  </s:dict>
</s:dict>
</content>
DELETE

Delete the {proxyConfig} HTTP proxy server configurations for splunkd.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:changed https://localhost:8089/services/server/httpsettings/proxysettings/proxyConfig -X DELETE

XML Response

<title>proxysettings</title>
<id>https://wimpy.sv.splunk.com:34001/services/server/httpsettings/proxysettings</id>
<updated>2017-04-20T17:14:52-07:00</updated>
<generator build="845bc99189da" version="6.6.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/server/httpsettings/proxysettings/_new" rel="create"/>
<link href="/services/server/httpsettings/proxysettings/_reload" rel="_reload"/>
<link href="/services/server/httpsettings/proxysettings/_acl" rel="_acl"/>
<opensearch:totalResults>0</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>

server/logger

https://<host>:<mPort>/services/server/logger

Access splunkd logging categories specified in code or in $SPLUNK_HOME/etc/log.cfg.
GET

Enumerate splunkd logging categories.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>One of the following valid logger levels for this server.</td>
</tr>
<tr>
<td></td>
<td>• FATAL</td>
</tr>
<tr>
<td></td>
<td>• WARN</td>
</tr>
<tr>
<td></td>
<td>• INFO</td>
</tr>
<tr>
<td></td>
<td>• DEBUG</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/logger

XML Response

...
server/logger/{name}

https://<host>:<mPort>/services/server/logger/{name}

Manage the {name} logging category.

GET

Access information about the specified splunkd logging category.

Request parameters

None

Response keys
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>One of the following valid logger levels for this server.</td>
</tr>
<tr>
<td></td>
<td>• FATAL</td>
</tr>
<tr>
<td></td>
<td>• WARN</td>
</tr>
<tr>
<td></td>
<td>• INFO</td>
</tr>
<tr>
<td></td>
<td>• DEBUG</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:changeme https://localhost:8089/services/server/logger/Application

XML Response

```xml
... elided ...
```
POST

Set the logging level for a specific logging category.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level</td>
<td>Enum</td>
<td>Required. The desired logging level for this category. One of the following valid values. [FATAL</td>
</tr>
</tbody>
</table>

Response keys
None

Example request and response

XML Request

```
curl -k -u admin:changeme https://localhost:8089/services/server/logger/Application -d level=INFO
```

XML Response

```
<title>logger</title>
:id>https://localhost:8089/services/server/logger</id>
 <updated>2011-07-07T00:24:02-07:00</updated>
 <generator version="102807"/>
 <author>
  <name>Splunk</name>
 </author>
 <s:messages/>
```

server/roles

https://<host>[:<mPort>]/services/server/roles

Access server role information.

See also the server-roles attribute in /server/info.
**GET**

Access the roles applicable to this server.

**Request parameters**
None

**Response keys**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;variable&gt;</td>
<td>Zero or more of the following possible server roles.</td>
</tr>
<tr>
<td></td>
<td>• indexer</td>
</tr>
<tr>
<td></td>
<td>• universal_forwarder</td>
</tr>
<tr>
<td></td>
<td>• heavyweight_forwarder</td>
</tr>
<tr>
<td></td>
<td>• lightweight_forwarder</td>
</tr>
<tr>
<td></td>
<td>• license_master</td>
</tr>
<tr>
<td></td>
<td>• license_slave</td>
</tr>
<tr>
<td></td>
<td>• cluster_master</td>
</tr>
<tr>
<td></td>
<td>• cluster_slave</td>
</tr>
<tr>
<td></td>
<td>• cluster_search_head</td>
</tr>
<tr>
<td></td>
<td>• deployment_server</td>
</tr>
<tr>
<td></td>
<td>• deployment_client</td>
</tr>
<tr>
<td></td>
<td>• search_head</td>
</tr>
<tr>
<td></td>
<td>• search_peer</td>
</tr>
<tr>
<td></td>
<td>• shc_captain</td>
</tr>
<tr>
<td></td>
<td>• shc_deployer</td>
</tr>
<tr>
<td></td>
<td>• shc_member</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -k -u admin:changeme https://localhost:8089/services/server/roles
```

**XML Response**

```
<entry>
<title>result</title>
<id>https://localhost:8089/services/server/roles/result</id>
<updated>2014-04-02T12:13:07-07:00</updated>
<link href="/services/server/roles/result" rel="alternate"/>
<author>
</author>
</entry>
```
<name>system</name>
</author>
<content type="text/xml">
  <s:dict>
    <s:key name="eai:acl">
      ... elided ...
    </s:key>
    <s:key name="indexer"/>
    <s:key name="license_master"/>
    <s:key name="license_slave"/>
  </s:dict>
</content>
</entry>

server/security/rotate-splunk-secret

https://<host>:<mPort>/services/server/security/rotate-splunk-secret
Rotates the splunk.secret file on a standalone Splunk Enterprise instance.

POST
Rotates the splunk.secret file on a standalone Splunk Enterprise instance.

Returned values
None

Example request and response

XML Request


XML Response

server/settings

https://<host>:<mPort>/services/server/settings

Access server configuration information for a Splunk platform instance. For additional information about your Splunk platform instance, see the server/info endpoint.
GET

Returns server configuration for a Splunk deployment.

Request parameters
Pagination and filtering parameters can be used with this method.

Response keys

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SPLUNK_DB</td>
<td>Absolute filepath to the default index for this deployment.</td>
</tr>
<tr>
<td>SPLUNK_HOME</td>
<td>Absolute filepath to the local installation of this deployment.</td>
</tr>
<tr>
<td>enableSplunkWebSSL</td>
<td>Indicates if HTTPS and SSL are enabled for Splunk Web.</td>
</tr>
<tr>
<td>host</td>
<td>The default hostname to use for data inputs that do not override this setting.</td>
</tr>
<tr>
<td>httpport</td>
<td>Port on which Splunk Web listens for this instance. Defaults to 8000. If using SSL, set to the HTTPS port number.</td>
</tr>
<tr>
<td>mgmtHostPort</td>
<td>The port on which Splunk Web listens for management operations. Defaults to 8089.</td>
</tr>
<tr>
<td>minFreeSpace</td>
<td>Safe amount of space in MB that must exist for splunkd to continue operating. minFreeSpace affects search and indexing in the following ways.</td>
</tr>
<tr>
<td></td>
<td>• Before attempting to launch a search, the Splunk platform requires this amount of free space on the filesystem where the dispatch directory is stored, $SPLUNK_HOME/var/run/splunk/dispatch.</td>
</tr>
<tr>
<td></td>
<td>• Applied similarly to the search quota values in authorize.conf and limits.conf.</td>
</tr>
<tr>
<td></td>
<td>• For indexing, periodically, the indexer checks space on all partitions that contain splunk indexes as specified by indexes.conf. When you need to clear more disk space, indexing is paused and the Splunk platform posts a UI banner + warning.</td>
</tr>
<tr>
<td>pass4SymmKey</td>
<td>Password string prefixed to the Splunk platform symmetric key, generating the final key to sign all traffic between master/slave licenser.</td>
</tr>
<tr>
<td>serverName</td>
<td>Name identifying this instance for features such as distributed search.</td>
</tr>
<tr>
<td>sessionTimeout</td>
<td>Time range string to indicate the amount of time before a user session times out. Expressed as a search-like time range. The default is 1h (one hour).</td>
</tr>
<tr>
<td></td>
<td>Here are some examples.</td>
</tr>
<tr>
<td></td>
<td>24h (24 hours)</td>
</tr>
<tr>
<td></td>
<td>3d (3 days)</td>
</tr>
<tr>
<td></td>
<td>7200s (7200 seconds, or two hours)</td>
</tr>
<tr>
<td>startwebserver</td>
<td>Indicates whether Splunk Web is configured to start by default.</td>
</tr>
<tr>
<td>trustedIP</td>
<td>IP address of the authenticating proxy. Set to a valid IP address to enable SSO. Disabled by default. Normal value is ‘127.0.0.1’.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request
curl -k -u admin:changeme https://localhost:8089/services/server/settings

XML Response

<entry>
<title>settings</title>
<id>https://localhost:8089/services/server/settings/settings</id>
<updated>2011-07-08T01:56:40-07:00</updated>
<author>
  <name>system</name>
</author>
<link href="/services/server/settings/settings" rel="alternate"/>
<link href="/services/server/settings/settings" rel="list"/>
<link href="/services/server/settings/settings" rel="edit"/>
<content type="text/xml">
  <s:dict>
    <s:key name="SPLUNK_DB">/home/amrit/temp/curl/splunk/var/lib/splunk</s:key>
    <s:key name="SPLUNK_HOME">/home/amrit/temp/curl/splunk</s:key>
    <s:key name="host">MrT</s:key>
    <s:key name="httpport">8001</s:key>
    <s:key name="mgmtHostPort">8085</s:key>
    <s:key name="minFreeSpace">2000000</s:key>
    <s:key name="pass4SymmKey">changeme</s:key>
    <s:key name="serverName">MrT</s:key>
    <s:key name="sessionTimeout">1h</s:key>
    <s:key name="startwebserver">1</s:key>
    <s:key name="trustedIP"/>
  </s:dict>
</content>
</entry>
Workload management endpoints

Workload management endpoint descriptions

Manage system resources for search and indexing processes.

- Create workload pools (CPU and memory resource groups).
- Create workload rules to grant access and prioritize workload pools.
- Assign scheduled and ad hoc searches to workload pools.

For more information, see About workload management in the Workload Management manual.

Usage details

Review ACL information for an endpoint

To check Access Control List (ACL) properties for an endpoint, append /acl to the path. For more information see Access Control List in the REST API User Manual.

Authentication and Authorization

Username and password authentication is required for access to endpoints and REST operations.

Splunk users must have role and/or capability-based authorization to use REST endpoints. Users with an administrative role, such as admin, can access authorization information in Splunk Web. To view the roles assigned to a user, select Settings > Access controls and click Users. To determine the capabilities assigned to a role, select Settings > Access controls and click Roles.

App and user context

Typically, knowledge objects, such as saved searches or event types, have an app/user context that is the namespace. For more information about specifying a namespace, see Namespace in the REST API User Manual.

Splunk Cloud limitations

If you have a managed Splunk Cloud deployment with search head clustering and index clustering, the REST API supports access to the search head only. You can use the REST API to interact with the search head in your deployment. Using the REST API to access any other cluster member nodes is not supported. For example, index cluster management endpoints are not applicable to Splunk Cloud deployments.

Authorized users can access and configure other cluster members, including indexer, cluster master, and license master nodes, in the Splunk Cloud manager user interface.

workloads/categories

https://<host>:<mPort>/services/workloads/categories
List and edit workload categories.
There are three predefined categories: search, ingest, and misc. You cannot create or delete categories. You can only edit and list them.

**Authentication and Authorization**

- GET requires the `list_workload_pools` capability.
- POST requires the `edit_workload_pools` capability.

**GET**

List information about workload categories.

**Request parameters**

None

**Returned values**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_weight</td>
<td>Number</td>
<td>Specifies the fraction of the cpu assigned to this category as a ratio of the total of cpu_weight across all categories. This fraction is then applied to the cpu shares assigned to the parent group. The value must be &gt; 0 and &lt;= 100.</td>
</tr>
<tr>
<td>mem_weight</td>
<td>Number</td>
<td>Specifies the percentage of memory assigned to this category as a percent of the parent group. The total amount of memory limit for this category is a percentage of the value assigned to the parent group. The value must be &gt; 0 and &lt;= 100.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

curl -k -u admin:pass https://localhost:8089/services/workloads/categories/search

**XML Response**

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <title>workload-categories</title>
  <id>https://qa-ubuntu-022:8089/services/workloads/categories</id>
  <updated>2019-03-20T14:11:59-07:00</updated>
  <generator build="8c85c1fbcc8c" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/categories/_reload" rel="_reload"/>
  <link href="/services/workloads/categories/_acl" rel="_acl"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>search</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/system/workloads/categories/search</id>
```

1153
Edit workload categories.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_weight</td>
<td>Number</td>
<td>Specifies the fraction of the CPU assigned to this category as a ratio of the total of cpu_weight across all categories. This fraction is then applied to the CPU shares assigned to the parent group. The value must be &gt; 0 and &lt;= 100.</td>
</tr>
<tr>
<td>mem_weight</td>
<td>Number</td>
<td>Specifies the percentage of memory assigned to this pool as a percent of the parent group. The total amount of memory limit for this pool is a percentage of the value assigned to the parent group. The value must be &gt; 0 and &lt;= 100.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/categories/search -d cpu_weight=40 -d mem_weight=50
```
workloads/pools

https://<host>:<mPort>/services/workloads/pools
Perform CRUD operations on workload pools.

Authentication and Authorization

- GET requires the list_workload_pools capability.
- POST and DELETE require the edit_workload_pools capability.
GET

List information about workload pools.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_weight</td>
<td>Number</td>
<td>Specifies the fraction of the cpu assigned to this pool as a ratio of the total of cpu_weight across all pools in a category. This fraction is then applied to the cpu shares assigned to the category.</td>
</tr>
<tr>
<td>mem_weight</td>
<td>Number</td>
<td>Specifies the percentage of the memory assigned to this pool as a percent of the category. The total amount of memory limit for this pool is a percentage of the value assigned to the category.</td>
</tr>
<tr>
<td>category</td>
<td>string</td>
<td>Specifies the category in which a poll is created. Can be either &quot;search&quot;, &quot;ingest&quot;, or &quot;misc&quot;.</td>
</tr>
<tr>
<td>default_category_pool</td>
<td>Boolean</td>
<td>Specifies the workload pool marked as default pool for its category. This property is defined per workload_pool stanza. Default is 0.</td>
</tr>
<tr>
<td>default_pool</td>
<td>Boolean</td>
<td>Specifies a workload pool defined in the search category as the default pool for the search category.</td>
</tr>
<tr>
<td>ingest_pool</td>
<td>Boolean</td>
<td>Specifies a workload-pool defined in the ingest category as the default pool for the ingest category.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k -u admin:pass https://localhost:8089/services/workloads/pools/search_pool_1
```

XML Response

```
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
><title>workload-pools</title>
  <id>https://qa-ubuntu-022:8089/services/workloads/pools</id>
  <updated>2019-03-21T11:58:38-07:00</updated>
  <generator build="8c85c1fc88c" version="7.3.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/pools/_new" rel="create"/>
  <link href="/services/workloads/pools/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>search_pool_1</title>
    <id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/workloads/pools/search_pool_1</id>
    <updated>1969-12-31T16:00:00-08:00</updated>
  </entry>
</feed>
```

1157
POST

Create and configure workload pools.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_weight</td>
<td>Number</td>
<td>Specifies the fraction of the cpu assigned to this pool as a ratio of the total of cpu_weight across all pools. This fraction is then applied to the cpu shares assigned to the parent group.</td>
</tr>
<tr>
<td>mem_weight</td>
<td>Number</td>
<td>Specifies the fraction of the memory assigned to this pool as a ratio of the total of mem_weight across all pools. This fraction is then applied to the memory limits assigned to the parent group.</td>
</tr>
<tr>
<td>category</td>
<td>string</td>
<td>Specifies the category in which a poll is created. Can be either &quot;search&quot;, &quot;ingest&quot;, or &quot;misc&quot;.</td>
</tr>
<tr>
<td>default_category_pool</td>
<td>Boolean</td>
<td>Specifies the workload pool marked as default pool for its category. This property is defined per workload_pool stanza. Default is 0.</td>
</tr>
<tr>
<td>default_pool</td>
<td>Boolean</td>
<td>Specifies a workload pool defined in the search category as the default pool for the search category.</td>
</tr>
<tr>
<td>ingest_pool</td>
<td>Boolean</td>
<td>Specifies a workload-pool defined in the ingest category as the default pool for the ingest category.</td>
</tr>
</tbody>
</table>

Returned values

None

Example request and response

XML Request

curl -k -u admin:pass -X POST https://localhost:8089/services/workloads/pools -d name=search_pool_3 -d category=search -d cpu_weight=40 -d mem_weight=60 -d default_category_pool=1

XML Response

```xml
  <title>workload-pools</title>
  <id>https://qa-ubuntu-022:8089/services/workloads/pools</id>
  <updated>2019-03-21T12:05:12-07:00</updated>
  <generator build="8a8f51fbc8c" version="7.3.0"/>
</feed>
```
<entry>
<title>search_pool_3</title>
<id>https://qa-ubuntu-022:8089/servicesNS/nobody/search/workloads/pools/search_pool_3</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<author>
<name>nobody</name>
</author>
<content type="text/xml">
<s:dict>
<s:key name="category">search</s:key>
<s:key name="cpu_allocated_percent">28.57</s:key>
<s:key name="cpu_shares">0</s:key>
<s:key name="cpu_weight">40</s:key>
<s:key name="default_category_pool">1</s:key>
<s:key name="eai:acl">
<s:dict>
<s:key name="app">search</s:key>
<s:key name="can_change_perms">1</s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_share_app">1</s:key>
<s:key name="can_share_global">1</s:key>
<s:key name="can_share_user">0</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">1</s:key>
<s:key name="owner">nobody</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="removable">1</s:key>
<s:key name="sharing">app</s:key>
</s:dict>
</s:key>
<s:key name="mem_allocated_percent">36.00</s:key>
<s:key name="mem_limit">0</s:key>
<s:key name="mem_weight">60</s:key>
</s:dict>
</s:messages/>
</opensearch:startIndex>
</opensearch:startIndex>
</opensearch:totalResults>
</opensearch:itemsPerPage>
</opensearch:rel>_reload/
</opensearch:rel>_acl/
</opensearch:rel>_new/
</link>
</s:messages/>
</opensearch:startIndex>
</opensearch:itemsPerPage>
</opensearch:totalResults>
</opensearch:startIndex>
</author>
</link>

Splunk
</name>
workloads/rules

https://<host>:<mPort>/services/workloads/rules
Perform CRUD operations on workload rules.

Authentication and Authorization

- GET requires the list_workload_rules capability.
- POST and DELETE require the edit_workload_rules capability.

GET

List information about workload rules.

Request parameters

None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>predicate</td>
<td>String</td>
<td>The predicate (condition) required to access the workload pool.</td>
</tr>
<tr>
<td>workload_pool</td>
<td>String</td>
<td>Specifies the workload pool associated with the workload rule.</td>
</tr>
<tr>
<td>order</td>
<td>Boolean</td>
<td>Specifies the evaluation order for this workload rule amongst a group of workload rules.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

```
curl -k-u admin:pass https://localhost:8089/services/workloads/rules
```

XML Response

```xml
      xmlns:workload-rules="http://dev.splunk.com/ns/workload-rules">
  <title>workload-rules</title>
  <id>https://localhost:8089/services/workloads/rules</id>
  <updated>2018-08-29T13:18:21-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/rules/_new" rel="create"/>
```
<content type="text/xml">
<s:dict>
<s:key name="eai:acl">
<s:dict>
<s:key name="app">search</s:key>
<s:key name="can_change_perms">1</s:key>
<s:key name="can_list">1</s:key>
<s:key name="can_share_app">1</s:key>
<s:key name="can_share_global">1</s:key>
<s:key name="can_share_user">0</s:key>
<s:key name="can_write">1</s:key>
<s:key name="modifiable">1</s:key>
<s:key name="owner">nobody</s:key>
<s:key name="perms">
<s:dict>
<s:key name="read">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
<s:key name="write">
<s:list>
<s:item>*</s:item>
</s:list>
</s:key>
</s:dict>
<s:key name="removable">1</s:key>
<s:key name="sharing">app</s:key>
</s:dict>
</s:key>
<s:key name="order">1</s:key>
<s:key name="predicate">role=admin</s:key>
<s:key name="workload_pool">pool_1</s:key>
</s:dict>
</content>
POST

Create and configure a workload rule.

Request parameters

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>predicate</td>
<td>String</td>
<td>Specifies a predicate (condition) that must be true for a search to gain access to the workload pool. The syntax is <code>&lt;type&gt;=&lt;value&gt;</code>, with optional AND, OR, NOT, (). For example, <code>app=search AND role=power</code> maps all searches belonging to both the Search app and the power role to the designated workload pool. Valid predicate <code>&lt;type&gt;</code> are <code>app</code>, <code>role</code>, <code>index</code>, <code>user</code>, <code>search_type</code>, <code>search_mode</code>, <code>search_time_range</code>, and <code>runtime</code>. For valid predicate type values, see Predicate type values in the Workload Management manual. You can only specify one predicate for each workload rule. Multiple predicates are not supported.</td>
</tr>
<tr>
<td>action</td>
<td>String</td>
<td>Specifies the action to take when a running search exceeds the specified runtime value. Supported actions are <code>alert</code>, <code>move</code> and <code>abort</code>.</td>
</tr>
<tr>
<td>Name</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>destination</td>
<td>String</td>
<td>Specifies the destination workload pool for the move action.</td>
</tr>
<tr>
<td>workload_pool</td>
<td>String</td>
<td>Specifies the workload pool associated with the workload rule.</td>
</tr>
<tr>
<td>order</td>
<td>Number</td>
<td>Specifies the evaluation order for this workload rule amongst a group of workload rules. For newly created rules, the order cannot be specified. It can only be specified for existing rules.</td>
</tr>
</tbody>
</table>

**Returned values**

None

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass -X POST https://localhost:8089/services/workloads/rules/rule_1 -d predicate="app=splunk_instrumentation"
```

**XML Response**

```xml
<title>workload-rules</title>  
<ID>https://localhost:8089/services/workloads/rules</ID>  
<updated>2018-08-29T13:29:09-07:00</updated>  
<generator build="fc353da83307" version="7.2.0"/>  
<author>  
  <name>Splunk</name>  
</author>  
<link href="/services/workloads/rules/_new" rel="create"/>  
<link href="/services/workloads/rules/_reload" rel="_reload"/>  
<link href="/services/workloads/rules/_acl" rel="_acl"/>  
<opensearch:totalResults>1</opensearch:totalResults>  
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>  
<opensearch:startIndex>0</opensearch:startIndex>  
<s:messages/>  
<entry>  
<title>rule_1</title>  
<ID>https://localhost:8089/servicesNS/nobody/search/workloads/rules/rule_1</ID>  
<updated>1969-12-31T16:00:00-08:00</updated>  
<author>  
  <name>nobody</name>  
</author>  
<link href="/servicesNS/nobody/search/workloads/rules/rule_1" rel="alternate"/>  
<link href="/servicesNS/nobody/search/workloads/rules/rule_1/_reload" rel="_reload"/>  
<link href="/servicesNS/nobody/search/workloads/rules/rule_1/_acl" rel="_acl"/>  
<s:dict>  
  <s:key name="eai:acl">  
    <s:dict>  
      <s:key name="app">search</s:key>  
      <s:key name="can_change_perms">1</s:key>  
      <s:key name="can_list">1</s:key>  
    </s:dict>  
  </s:key>  
</s:dict>  
</entry>
</feed>
```
DELETE

Delete workload rules.

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass -X DELETE https://localhost:8089/services/workloads/rules/rule_1

XML Response

      id=https://localhost:8089/services/workloads/rules/id
      updated=2018-08-29T13:29:47-07:00"/>
<author>

1166
workloads/config/enable

https://<host>:<mPort>/services/workloads/config/enable

Enable workload management.

Authentication and Authorization
Requires the edit_workload_pools capability.

POST
Enable workload management

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass -X POST https://localhost:8089/services/workloads/config/enable

XML Response

  <title>workload-config</title>
  <id>https://localhost:8089/services/workloads/config</id>
  <updated>2018-08-29T13:32:26-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/config/_new" rel="create"/>
  <link href="/services/workloads/config/_reload" rel="_reload"/>
  <link href="/services/workloads/config/_acl" rel="_acl"/>
  <opensearch:totalResults>0</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
</feed>
workloads/config/disable

https://<host>:<mPort>/services/workloads/config/disable
Endpoint to disable workload management.

Authentication and Authorization
Requires the edit_workload_pools capability.

POST
Disable workload management

Request parameters
None

Returned values
None

Example request and response

XML Request

curl -k -u admin:pass -X POST https://localhost:8089/services/workloads/config/disable

XML Response

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
<title>workload-config</title>
<id>https://localhost:8089/services/workloads/config</id>
<updated>2018-08-29T13:33:55-07:00</updated>
<generator build="fc353da83307" version="7.2.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/workloads/config/_reload" rel="_reload"/>
<link href="/services/workloads/config/_acl" rel="_acl"/>
<link href="/services/workloads/config/disable" rel="disable"/>
<link href="/services/workloads/config/enable" rel="enable"/>
<link href="/services/workloads/config/get-base-dirname" rel="get-base-dirname"/>
workloads/config/get-base-dirname

https://<host>:<mPort>/services/workloads/config/get-base-dirname

Get the name of the splunk parent cgroup.

Authentication and Authorization
Requires the edit_workload_pools capability.

GET

Get the name of the splunk parent cgroup.

Request parameters
None

Returned values

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workload_pool_base_dir_name</td>
<td>String</td>
<td>Specifies the parent level cgroup for splunk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This setting applies only to systems running non-systemd setups. With systemd, this setting is ignored.</td>
</tr>
</tbody>
</table>

Example request and response

XML Request

curl -k -u admin:pass https://localhost:8089/services/workloads/config/get-base-dirname

XML Response

<feed xmlns=http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
<title>workload-config</title>
=id>https://localhost:8089/services/workloads/config/id
<updated>2018-08-29T14:49:48-07:00</updated>
<generator build="fc353da83307" version="7.2.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/workloads/config/_reload" rel="_reload"/>
<link href="/services/workloads/config/_acl" rel="_acl"/>
<link href="/services/workloads/config/disable" rel="disable"/>
<link href="/services/workloads/config/enable" rel="enable"/>
<link href="/services/workloads/config/get-base-dirname" rel="get-base-dirname"/>
<link href="/services/workloads/config/set-base-dirname" rel="set-base-dirname"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>workload-pool-base-path</title>
  <id>https://localhost:8089/services/workloads/config/workload-pool-base-path</id>
  <updated>1969-12-31T16:00:00-08:00</updated>
  <link href="/services/workloads/config/workload-pool-base-path" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/workloads/config/workload-pool-base-path" rel="list"/>
  <link href="/services/workloads/config/workload-pool-base-path/_reload" rel="_reload"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="eai:acl">
        <s:dict>
          <s:key name="app"></s:key>
          <s:key name="can_list">1</s:key>
          <s:key name="can_write">1</s:key>
          <s:key name="modifiable">0</s:key>
          <s:key name="owner">system</s:key>
          <s:key name="perms">
            <s:dict>
              <s:key name="read">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>analyst</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
              <s:key name="write">
                <s:list>
                  <s:item>admin</s:item>
                  <s:item>splunk-system-role</s:item>
                </s:list>
              </s:key>
            </s:dict>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="workload_pool_base_dir_name">splunk</s:key>
    </s:dict>
  </content>
</entry>
</feed>

workloads/config/preflight-checks

https://<host>:<mPort>/services/workloads/config/preflight-checks
Run Linux preflight checks for workload management.

1170
Authentication and Authorization
Requires the list_workload_pools and edit_workload_pools capabilities.

GET
Run Linux preflight checks for workload management.

Request parameters
None

Returned values

Example request and response

XML Request
curl -k -u admin:pass https://localhost:8089/services/workloads/config/preflight-checks

XML Response

<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
<title>workload-config</title>
<id>https://localhost:8089/services/workloads/config</id>
<updated>2018-11-30T14:38:15-08:00</updated>
<generator build="611919ba3f87bb18f54b0df1b03fd86a273309c2" version="20181121"/>
<br:title>workload-management-preflight-checks</title>
<id>https://qa-centos7x64-132:8089/services/workloads/config/workload-management-preflight-checks</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<generator build="611919ba3f87bb18f54b0df1b03fd86a273309c2" version="20181121"/>
<author>
<name>Splunk</name>
</author>
<link href="/services/workloads/config/_reload" rel="_reload"/>
<link href="/services/workloads/config/_acl" rel="_acl"/>
<link href="/services/workloads/config/disable" rel="disable"/>
<link href="/services/workloads/config/enable" rel="enable"/>
<link href="/services/workloads/config/get-base-dirname" rel="get-base-dirname"/>
<link href="/services/workloads/config/preflight-checks" rel="preflight-checks"/>
<link href="/services/workloads/config/set-base-dirname" rel="set-base-dirname"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<br:s:messages/>
<br:e:entry>
<title>workload-management-preflight-checks</title>
<id>https://qa-centos7x64-132:8089/services/workloads/config/workload-management-preflight-checks</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<generator build="611919ba3f87bb18f54b0df1b03fd86a273309c2" version="20181121"/>
<br:title>cgroup_version</br:title>
<value>1171</value>
</e:entry>
<s:dict>
  <s:key name="mitigation">Cgroup version must be version 1.</s:key>
  <s:key name="preflight_check_status">1</s:key>
  <s:key name="title">Cgroup Version</s:key>
</s:dict>
<s:dict>
  <s:key name="mitigation">CPU Splunk base directory Splunkd.service requires read and write permissions.</s:key>
  <s:key name="preflight_check_status">1</s:key>
  <s:key name="title">CPU Splunk base directory permissions</s:key>
</s:dict>
<s:dict>
  <s:key name="mitigation">CPU Splunk base directory Splunkd.service is missing.</s:key>
  <s:key name="preflight_check_status">1</s:key>
  <s:key name="title">CPU Splunk base directory present</s:key>
</s:dict>
<s:dict>
  <s:key name="mitigation">The 'Delegate' property in the unit file must be set to 'true'. Restart Splunk then rerun preflight checks.</s:key>
  <s:key name="preflight_check_status">1</s:key>
  <s:key name="title">Delegate property set to true</s:key>
</s:dict>
<s:dict>
  <s:key name="app"></s:key>
  <s:key name="can_list">1</s:key>
  <s:key name="can_write">1</s:key>
  <s:key name="modifiable">0</s:key>
  <s:key name="owner">system</s:key>
  <s:key name="perms">
    <s:dict>
      <s:key name="read">
        <s:list>
          <s:item>admin</s:item>
          <s:item>splunk-system-role</s:item>
        </s:list>
      </s:key>
      <s:key name="write">
        <s:list>
          <s:item>admin</s:item>
          <s:item>splunk-system-role</s:item>
        </s:list>
      </s:key>
      <s:key name="removable">0</s:key>
      <s:key name="sharing">system</s:key>
    </s:dict>
  </s:key>
  <s:key name="general">
    <s:dict>
      <s:key name="preflight_checks_status">1</s:key>
      <s:key name="systemd_present">1</s:key>
    </s:dict>
  </s:key>
</s:dict>
workloads/config/set-base-dirname

https://<host>:<mPort>/services/workloads/config/set-base-dirname
Set the name of the splunk parent cgroup.

Authentication and Authorization
Requires the edit_workload_pools capability.
**POST**

Set the name of the splunk parent cgroup.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>workload_pool_base_dir_name</td>
<td>String</td>
<td>Specifies the parent level cgroup for splunk.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>This setting applies only to systems running non-systemd setups. With systemd, this setting is ignored.</td>
</tr>
</tbody>
</table>

**Returned values**

None

**Example request and response**

**XML Request**

```bash
curl -k -u admin:pass https://localhost:8089/services/workloads/config/set-base-dirname -d "workload_pool_base_dir_name=splunkbase"
```

**XML Response**

```xml
<feed xmlns="http://www.w3.org/2005/Atom" xmlns:s="http://dev.splunk.com/ns/rest"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/"
      xmlns:sw="http://dev.splunk.com/ns/service"
      xmlns:ws="http://dev.splunk.com/ns/workload">
  <title/workload-config<title/>
  <id>https://localhost:8089/services/workloads/config</id>
  <updated>2018-08-29T14:54:31-07:00</updated>
  <generator build="fc353da83307" version="7.2.0"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/workloads/config/_reload" rel="_reload"/>
  <link href="/services/workloads/config/_acl" rel="_acl"/>
  <link href="/services/workloads/config/disable" rel="disable"/>
  <link href="/services/workloads/config/enable" rel="enable"/>
  <link href="/services/workloads/config/get-base-dirname" rel="get-base-dirname"/>
  <link href="/services/workloads/config/set-base-dirname" rel="set-base-dirname"/>
  <sw:totalResults>0</sw:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
</feed>
```

**workloads/status**

https://<host>:<mPort>/services/workloads/status

Get information on the current status of workload management.

**Authentication and Authorization**
Requires the `list_workload_pools` capability.

**GET**

Get information on the current status of workload management.

**Request parameters**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>advanced</td>
<td>Boolean</td>
<td><code>advanced=1</code> returns dispatch time for each process running in each search pool.</td>
</tr>
</tbody>
</table>

**Returned values**

**General information:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default_pool</td>
<td>String</td>
<td>Specifies the workload pool marked as the default pool.</td>
</tr>
<tr>
<td>ingest_pool</td>
<td>Number</td>
<td>Specifies the workload pool marked as the ingest pool.</td>
</tr>
<tr>
<td>error_message</td>
<td>String</td>
<td>Displays the last error message observed while trying to enable workload management. This message is reset to empty on each successful enablement of workload management.</td>
</tr>
<tr>
<td>enabled</td>
<td>Boolean</td>
<td>Specifies whether or not workload management is enabled.</td>
</tr>
<tr>
<td>isSupported</td>
<td>Boolean</td>
<td>Specifies whether or not workload management is supported on this machine.</td>
</tr>
<tr>
<td>os_build</td>
<td>String</td>
<td>Specifies the operating system build information.</td>
</tr>
<tr>
<td>os_extended_name</td>
<td>String</td>
<td>Specifies the extended name of the underlying operating system.</td>
</tr>
<tr>
<td>os_name</td>
<td>String</td>
<td>Specifies the name of the underlying operating system.</td>
</tr>
<tr>
<td>os_version</td>
<td>String</td>
<td>Specifies the operating system version.</td>
</tr>
</tbody>
</table>

**Workload pools:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cpu_weight'</td>
<td>Number</td>
<td>Specifies the fraction of the cpu assigned to this pool as a ratio of the total of cpu_weight across all pools. This fraction is then applied to the cpu shares assigned to the parent group.</td>
</tr>
<tr>
<td>mem_weight</td>
<td>Number</td>
<td>Specifies the fraction of the memory assigned to this pool as a ratio of the total of mem_weight across all pools. This fraction is then applied to the memory limits assigned to the parent group.</td>
</tr>
</tbody>
</table>

**Workload rules:**

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>predicate</td>
<td>String</td>
<td>Specifies the predicate condition that must match to access a workload pool. This must be of the format &quot;app=&lt;value&gt;&quot; or &quot;role=&lt;value&gt;&quot;. For example, app=itsi, role=admin. No other predicate formats are supported.</td>
</tr>
<tr>
<td>workload_pool</td>
<td>String</td>
<td>Specifies the workload pool to associate with the workload rule.</td>
</tr>
<tr>
<td>order</td>
<td>Number</td>
<td>Specifies the evaluation order for this workload rule amongst a group of workload rules.</td>
</tr>
</tbody>
</table>

**Example request and response**

1175
curl -k -u admin:pass https://localhost:8089/services/workloads/status

XML Response

xmlns:workload-status/u/ns/rest"
xmlns:workload-management-status/u/ns/rest">
<title>workload-status</title>
<id>https://localhost:8089/services/workloads/status</id>
<updated>2018-08-29T13:53:48-07:00</updated>
<generator build="fc353da83307" version="7.2.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/workloads/status/_acl" rel="_acl"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
<title>workload-management-status</title>
<id>https://localhost:8089/services/workloads/status/workload-management-status</id>
<updated>1969-12-31T16:00:00-08:00</updated>
<link href="/services/workloads/status/workload-management-status" rel="alternate"/>
<author>
  <name>system</name>
</author>
<link href="/services/workloads/status/workload-management-status" rel="list"/>
<content type="text/xml">
<s:dict>
  <s:key name="eai:acl">
    <s:dict>
      <s:key name="app"> </s:key>
      <s:key name="can_list">1</s:key>
      <s:key name="can_write">1</s:key>
      <s:key name="modifiable">0</s:key>
      <s:key name="owner">system</s:key>
      <s:key name="perms">
        <s:dict>
          <s:key name="read">
            <s:list>
              <s:item>admin</s:item>
              <s:item>analyst</s:item>
              <s:item>splunk-system-role</s:item>
            </s:list>
          </s:key>
          <s:key name="write">
            <s:list/>
          </s:key>
          <s:key name="removable">0</s:key>
          <s:key name="sharing">system</s:key>
        </s:dict>
      </s:key>
      <s:key name="general">
        <s:dict>
          <s:key name="default_pool">default_search_pool</s:key>
          <s:key name="enabled">1</s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </s:key>
</s:dict>
1176