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.

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>.cloud.splunk.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/inputs/ad**

https://<host>:<mPort>/services/data/inputs/ad
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.</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.</td>
</tr>
<tr>
<td>targetDc</td>
<td>If not specified, Splunk software attempts to start at the root of the directory tree.</td>
</tr>
</tbody>
</table>

**Example request and response**
XML Request

curl -u admin:pass https://localhost:8089/services/data/inputs/ad

XML Response

...  
<title>win-admon</title>  
{id>https://10.1.5.157:8089/services/data/inputs/ad</i>  
<updated>2011-07-29T19:13:28-07:00</updated>  
<generator version="104976"/>  
<author>  
  <name>Splunk</name>  
</author>  
<link href="/services/data/inputs/ad/_new" rel="create"/>  
<link href="/services/data/inputs/ad/_reload" rel="_reload"/>
... opensearch nodes elided ...
<s:messages/>
<entry>
  <title>NearestDC</title>  
  <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/ad/NearestDC</i>  
  <updated>2011-07-29T19:13:28-07:00</updated>  
  <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC" rel="alternate"/>
  <author>  
    <name>nobody</name>  
  </author>  
  <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC" rel="list"/>
  <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC/edit" rel="edit"/>
  <link href="/servicesNS/nobody/windows/data/inputs/ad/NearestDC/enable" rel="enable"/>
  <content type="text/xml">
    <s:dict>  
      <s:key name="disabled">1</s:key>  
      ... eai:acl node elided ...  
      <s:key name="default">
      <s:key name="monitorSubtree">1</s:key>
      <s:key name="startingNode"/>
      <s:key name="targetDc"/>
    </s:dict>  
  </content>
</entry>
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. If not specified defaults to the default index.</td>
</tr>
<tr>
<td>monitorSubtree</td>
<td>Number</td>
<td></td>
<td>Required. 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></td>
<td>Required. 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>startingNode</td>
<td>String</td>
<td></td>
<td>Where in the Active Directory directory tree to start.</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>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>
  <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>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>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**

```bash
curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/ad/newdc
```

**XML Response**

```xml
...  
<title>win-admon</title>  
<ID>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad</ID>  
<updated>2011-07-29T19:18:18-07:00</updated>  
<generator version="104976"/>  
<author>  
  <name>Splunk</name>  
</author>  
<link href="/servicesNS/nobody/search/data/inputs/ad/_new" rel="create"/>
```
... opensearch nodes elided ...

<entry>
  <title>newdc</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/ad/newdc</id>
  <updated>2011-07-29T19:18:18-07:00</updated>
  <link href="/servicesNS/nobody/search/data/inputs/ad/newdc" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/ad/newdc" rel="list"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/newdc/_reload" rel="_reload"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/newdc/edit" rel="edit"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/newdc/remove" rel="remove"/>
  <link href="/servicesNS/nobody/search/data/inputs/ad/newdc/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="disabled">0</s:key>
      <s:dict name="eai:attributes">
        <s:dict name="optionalFields">
          <s:list>
            <s:item>disabled</s:item>
            <s:item>index</s:item>
            <s:item>startingNode</s:item>
            <s:item>targetDc</s:item>
          </s:list>
        </s:dict>
        <s:dict name="requiredFields">
          <s:list>
            <s:item>monitorSubtree</s:item>
          </s:list>
        </s:dict>
        <s:dict name="wildcardFields">
          </s:dict>
        </s:dict>
      </s:dict>
      <s:key name="index">default</s:key>
      <s:key name="monitorSubtree">0</s:key>
    </s:dict>
  </content>
</entry>
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>host</td>
<td>String</td>
<td>Docs-W8R2-Std7</td>
<td>Baseline objects are objects which currently reside in Active Directory and include previously deleted objects.</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></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>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 specified, attempts to start at the root of</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>targetDc</td>
<td>String</td>
<td></td>
<td>Specifies a fully qualified domain name of a valid, network-accessible DC. 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$  
<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"/>  
... opensearch nodes elided ...
<s:messages/>
**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**

curl -u admin:pass https://localhost:8089/services/data/inputs/all

**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>all</title>
   <id>https://localhost:8089/services/data/inputs/all</id>
   <updated>2012-10-01T16:08:24-07:00</updated>
   <generator build="138753" version="5.0"/>
   <author>
      <name>Splunk</name>
   </author>
   <link href="/services/data/inputs/all/_new" rel="create"/>
   <link href="/services/data/inputs/all/_reload" rel="_reload"/>
   <link href="/services/data/inputs/all/restart" rel="restart"/>
   ... opensearch nodes elided ...
   <s:messages/>
   <entry>
      <title></title>
      <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/all/</id>
      <updated>2012-10-01T16:08:24-07:00</updated>
      <link href="/servicesNS/nobody/system/data/inputs/all/" rel="alternate"/>
      <author>
         <name>nobody</name>
      </author>
      <link href="/servicesNS/nobody/system/data/inputs/all/" rel="list"/>
      <link href="/servicesNS/nobody/system/data/inputs/all/_reload" rel="_reload"/>
      <link href="/servicesNS/nobody/system/data/inputs/all/" rel="edit"/>
      <link href="/servicesNS/nobody/system/data/inputs/all/enable" rel="enable"/>
      <content type="text/xml">
         <s:dict>
            <s:key name="rcvbuf">1572864</s:key>
            ... eai:acl node elided ...
            <s:key name="host">splunks-ombra.sv.splunk.com</s:key>
            <s:key name="index">default</s:key>
         </s:dict>
      </content>
   </entry>
   <entry>
      <title>$SPLUNK_HOME/etc/splunk.version</title>
      <id>https://localhost:8089/servicesNS/nobody/system/data/inputs/all/%24SPLUNK_HOME%252Fetc%252Fsplunk.version</id>
      <updated>2012-10-01T16:08:24-07:00</updated>
      <link href="/servicesNS/nobody/system/data/inputs/all/%24SPLUNK_HOME%252Fetc%252Fsplunk.version" rel="alternate"/>
      <author>
         <name>nobody</name>
      </author>
      ... eai:acl node elided ...
      ... eai:acl node elided ...
      <s:key name="host">splunks-ombra.sv.splunk.com</s:key>
      <s:key name="index">default</s:key>
   </entry>
</feed>
## 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</td>
</tr>
</tbody>
</table>
inputs. These common attributes are as follows.

- app
- disabled
- host
- index
- owner
- source
- sourcetype
- title
- updated

**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**

```xml
...<title>all</title>
<id>https://localhost:8089/services/data/inputs/all</id>
<updated>2012-07-11T08:03:17-07:00</updated>
<generator build="129290" version="5.0"/>
<author>
  <name>Splunk</name>
</author>
<link href="/services/data/inputs/all/restart" rel="restart"/>
... opensearch nodes elided ...
<s:messages/>
<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="name">
              <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>
    </s:key>
  </s:dict>
</content>
data/inputs/http

https://<host>:<mPort>/services/data/inputs/http

Access or update HTTP Event Collector global configuration tokens and application tokens.

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>
<link href="/servicesNS/nobody/system/data/inputs/http/http" rel="alternate"/>
<author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/system/data/inputs/http/http" rel="list"/>
<link href="/servicesNS/nobody/system/data/inputs/http/http/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/system/data/inputs/http/http/edit" rel="edit"/>
<link href="/servicesNS/nobody/system/data/inputs/http/http/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:key name="eai:appName">search</s:key>
    <s:key name="eai:userName">admin</s:key>
    <s:key name="host">$decideOnStartup</s:key>
    <s:key name="index">default</s:key>
  </s:dict>
</content>
</entry>
<entry>
<title>http://%22myapp"</title>
{id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22</id>
<updated>2015-01-26T22:43:26-08:00</updated>
<link href="/servicesNS/nobody/system/data/inputs/http/http%3A%252F%252F%22myapp%22" rel="alternate"/>
<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"/>
</entry>
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>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Adjusting this value may cause</td>
</tr>
</tbody>
</table>
server performance issues and is not generally recommended. Possible values for this setting vary by OS.

| maxThreads | Number | 0 | 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. |
| name | required | String | Token name (inputs.conf key) |
| port | Number | 8088 | HTTP data input IP port. |
| source | String | | Default source for events with this token. |
| sourcetype | String | | Default sourcetype for events with this token. |

**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</td>
<td>required</td>
<td>String</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>sourcetype</td>
<td>String</td>
<td></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>dedicatedIoThreads</td>
<td>Number of threads used by HTTP Input server.</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>enableSSL</td>
<td>Enable SSL protocol for HTTP data input. 1 = SSL enabled, 0 = SSL 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>indexes</td>
<td>Set of indexes allowed for events with this token.</td>
</tr>
<tr>
<td>port</td>
<td>HTTP data input IP port.</td>
</tr>
<tr>
<td>_rcvbuf</td>
<td>Socket receive buffer size (bytes).</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>
</tbody>
</table>

**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 <code>collector/event</code> 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" rel="list"/>
<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/_edit" rel="edit"/>
<link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp/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 ...
<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="token">AABD8B82-2810-4BE8-823F-FE6C15ECB46E</s:key>
</s:dict>
</content>
data/inputs/http/{name}

https://<host>:<mPort>/services/data/inputs/http/{name}

Manage the {name} HTTP Event Collector token. HTTP, as in data/inputs/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
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></td>
</tr>
</tbody>
</table>

23
<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>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>

**Application-level response data keys**

**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
...<title>http</title>
<id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</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>
```
POST

Update token configuration information.

Request parameters

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

25
disabled  Boolean 1  Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.

host  String  Default host.

index  String  Index to store generated events.

indexes  String  Set of indexes allowed for events with this token.

name  String  Required. Token name (inputs.conf key)

source  String  Default source for events with this token.

sourcetype  String  Default sourcetype for events with this token.

<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>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


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"/>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp" rel="list"/>
  <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" rel="edit"/>
  <link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp" rel="remove"/>
  <link href="/servicesNS/nobody/system/data/inputs/http%3A%252F%252Fmyapp/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: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}/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>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

```bash
curl -u admin:pass
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>2015-01-30T12:59:44-08:00</updated>
/generator build="250128" version="20150120"/>
/author>
  /name>Splunk</name>
/author>
/author>
  /link href="/servicesNS/nobody/system/data/inputs/http/_new"
rel="create"/>
/author>
  /link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
/link href="/servicesNS/nobody/system/data/inputs/http/_reload"
rel="_reload"/>
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>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</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**

```bash
curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/http/http%3A%252F%252Fmyapp/enable
```

**XML Response**

```
...<title>http</title>
{id>https://localhost:8089/servicesNS/nobody/system/data/inputs/http</id>
<updated>2015-01-30T12:56:38-08:00</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 ... </entry>
```

31
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

<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/
-X post

XML Response

<?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>
</tbody>
</table>
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.

Example request and response

**XML Request**

curl -u admin:pass https://localhost:8089/services/data/inputs/monitor

**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>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" rel="_reload"/>
  </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></td>
</tr>
<tr>
<td>Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td>If set to true, files that are seen for the first time is read from the end. 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**

```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>monitor</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
  <updated>2011-07-10T14:27:57-07:00</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/>
</feed>
```

**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

```bash
curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog
```

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>monitor</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor</id>
    <updated>2011-07-10T14:35:35-07:00</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/>
</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>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog</id>
    <updated>2011-07-10T14:33:54-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog" rel="list"/>
  </entry>
</feed>
```
<s:dict>
  <s:key name="_rcvbuf">1572864</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>blacklist</s:item>
          <s:item>check-index</s:item>
          <s:item>check-path</s:item>
          <s:item>crc-salt</s:item>
          <s:item>followTail</s:item>
          <s:item>host</s:item>
          <s:item>host_regex</s:item>
          <s:item>host_segment</s:item>
          <s:item>ignore-older-than</s:item>
          <s:item>index</s:item>
          <s:item>recursive</s:item>
          <s:item>rename-source</s:item>
          <s:item>sourcetype</s:item>
          <s:item>time-before-close</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="filecount">108</s:key>
  <s:key name="host">MrT</s:key>
  <s:key name="index">default</s:key>
</s:dict>
POST

Update properties of the named 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 &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></td>
<td></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_regex</td>
<td>String</td>
<td>Use the specified slash-separate segment of the filepath as the host field value.</td>
</tr>
<tr>
<td>host_segment</td>
<td>Number</td>
<td></td>
</tr>
<tr>
<td>ignore-older-than</td>
<td>String</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>index</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>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"
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
<feed xmlns="http://www.w3.org/2005/Atom"
     xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <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>
    <title>/var/log/acpid</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid</id>
    <updated>2011-07-10T14:34:28-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid" rel="alternate"/>
    <author>
      <name>system</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/monitor/%252Fvar%252Flog%252Facpid" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        ... eai:acl node elided ...
      </s:dict>
    </content>
  </entry>
  ... elided ...
</feed>
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.</td>
</tr>
<tr>
<td></td>
<td>This total includes the uncompressed byte count from a source file that is compressed on disk.</td>
</tr>
<tr>
<td></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.</td>
</tr>
<tr>
<td>Offset</td>
<td>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.</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.</td>
</tr>
<tr>
<td></td>
<td>A value of 0 indicates the source file was not compressed.</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>
```

46
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 host field to be applied to data from this file.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>A regex to be used to extract a host field from the path.</td>
</tr>
<tr>
<td>host_regex</td>
<td>String</td>
<td></td>
<td>If the path 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></td>
<td>Use the specified slash-separate segment of the path as the host 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></td>
<td>Required. 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 source 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 sourcetype 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 `{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</td>
<td>Total number of bytes read and sent to the pipeline for indexing</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>---------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Indexed</td>
<td>during a oneshot input.</td>
</tr>
<tr>
<td>Offset</td>
<td>This total includes the uncompressed byte count from a source file that is compressed on disk.</td>
</tr>
<tr>
<td></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.</td>
</tr>
<tr>
<td>Size</td>
<td>You can obtain the percentage of a source file read by calculating offset/size.</td>
</tr>
<tr>
<td>Sources Indexed</td>
<td>Size of the source file, in bytes.</td>
</tr>
<tr>
<td>Spool Time</td>
<td>You can obtain the percentage of a source file read by calculating offset/size.</td>
</tr>
<tr>
<td></td>
<td>Indicates the number of sources read from a file in a compressed format such as tar or zip.</td>
</tr>
<tr>
<td></td>
<td>A value of 0 indicates the source file was not compressed.</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```
curl -u admin:pass
https://localhost:8089/services/data/inputs/oneshot/%252Fvar%252Flog%252Fmessages
```

**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>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>
  <link href="/services/data/inputs/oneshot/_new" rel="create"/>
</feed>
```
... opensearch nodes elided ...

<entry>
  <title>/var/log/messages</title>
  <id>https://localhost:8089/services/data/inputs/oneshot/%252Fvar%252Flog%252Fmessages</id>
  <updated>2011-07-08T01:49:20-07:00</updated>
  <link href="/services/data/inputs/oneshot/%252Fvar%252Flog%252Fmessages" rel="alternate"/>
  <author>
    <name>system</name>
  </author>
  <link href="/services/data/inputs/oneshot/%252Fvar%252Flog%252Fmessages" rel="list"/>
  <content type="text/xml">
    <s:dict>
      <s:dict name="Bytes Indexed">114822</s:dict>
      <s:dict name="Bytes Indexed">114822</s:dict>
      <s:dict name="Size">114822</s:dict>
      <s:dict name="Sources Indexed">0</s:dict>
      <s:dict name="Spool Time">Fri Jul  8 01:48:04 PDT 2011</s:dict>
      ... eai:acl node elided ...
      <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>
  </content>
</entry>
</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>index</td>
<td>Specifies the index that this input should send the data to.</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>It matches against the process name which performed the Registry access.</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/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/Machine%20keys/enable" rel="enable"/>
    <content type="text/xml">
      52
    </content>
  </entry>
</feed>
```
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></td>
<td>Required. 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></td>
<td>Required. Specify the registry hive for monitoring changes.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Required. Name of the configuration stanza.</td>
</tr>
<tr>
<td>proc</td>
<td>String</td>
<td></td>
<td>Required. Specify a regex for collecting changes if a process name matches the regex.</td>
</tr>
<tr>
<td>type</td>
<td>String</td>
<td></td>
<td>Required. List registry event types that you want to monitor. Separate each</td>
</tr>
</tbody>
</table>
### Table

<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 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**

```
<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

curl -u admin:pass --request DELETE
https://localhost:8089/servicesNS/nobody/search/data/inputs/registry/mykeys

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-regmon</title>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/registry</id>
  <updated>2011-07-29T19:36:54-07:00</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"/>
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. Specifies the index that this input should send the data to.</td>
</tr>
<tr>
<td>index</td>
<td>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. Regular expression for processes this input should monitor for Registry access.</td>
</tr>
<tr>
<td>proc</td>
<td>It matches against the process name which performed the Registry access.</td>
</tr>
<tr>
<td></td>
<td>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>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>type</strong></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
```

**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-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/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys/edit" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/registry/mykeys/remove" rel="remove"/>
  </entry>
</feed>
```
<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">
      <s:list>
        <s:item>set</s:item>
        <s:item>create</s:item>
        <s:item>delete</s:item>
        <s:item>rename</s:item>
      </s:list>
    </s:key>
  </s:dict>
</content>
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><strong>Required.</strong> 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><strong>Required.</strong> Specifies the registry hive under which to monitor for changes.</td>
</tr>
<tr>
<td>proc</td>
<td>String</td>
<td></td>
<td><strong>Required.</strong> 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><strong>Required.</strong> A list of registry events types that you want to monitor. Separate each type with a pipe (&quot;</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

```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>2011-07-29T19:36:07-07:00</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/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>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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. An integer or cron schedule.</td>
</tr>
<tr>
<td>interval</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>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::'. 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.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>For more information, see the documentation for the sourcetype parameter for the POST operation.</td>
</tr>
<tr>
<td>starttime</td>
<td>If available, the time the when the script was executed.EHICLE</td>
</tr>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -u admin:pass https://localhost:8089/services/data/inputs/script
```

**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/services/data/inputs/script</id>
</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>Required. 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>Required. 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>source</td>
<td>String</td>
<td></td>
<td>Sets the source key/field for events from this input. Defaults to the input file path. 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>

**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.

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.

Returned values
None

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
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>script</td>
<td>String</td>
<td>Required</td>
<td>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

<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/%252FApplications%252Fsplunk4.3%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh
```

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>2011-07-09T20:29:18-07:00</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>
```

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>Name</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><em>group</em></td>
<td>The name of the inputstatus group, which is always &quot;exec commands.&quot;</td>
</tr>
<tr>
<td><em>host</em></td>
<td>Host these data are identified with.</td>
</tr>
<tr>
<td><em>index</em></td>
<td>Sets the index for events from this input. Defaults to the main index. An integer or cron schedule.</td>
</tr>
<tr>
<td><em>interval</em></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>
</tbody>
</table>

**Example request and response**

**XML Request**

```bash
curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/script/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.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>2011-07-09T21:53:43-07:00</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/>
  <entry>
    <title>/Applications/splunk/etc/apps/myApp/bin/myScript.sh</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/script/%252FApplications%252Fsplunk%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh</id>
    <updated>2011-07-09T21:53:43-07:00</updated>
    <link>
```
<content type="text/xml">
  <s:dict>
    <s:key name="_rcvbuf">1572864</s:key>
    <s:dict name="eai:attributes">
      <s:dict>
        <s:dict name="optionalFields">
          <s:list>
            <s:item>disabled</s:item>
            <s:item>host</s:item>
            <s:item>index</s:item>
            <s:item>interval</s:item>
            <s:item>rename-source</s:item>
            <s:item>source</s:item>
            <s:item>sourcetype</s:item>
          </s:list>
        </s:dict>
        <s:dict name="requiredFields">
          <s:list/>
        </s:dict>
        <s:dict name="wildcardFields">
          <s:list/>
        </s:dict>
      </s:dict>
    </s:dict>
    <s:dict name="group">exec commands</s:dict>
    <s:dict name="host">ombroso-mbp15.splunk.com</s:dict>
    <s:dict name="index">default</s:dict>
    <s:dict name="interval">3600</s:dict>
  </s:dict>
</content>
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>
<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. 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>

**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.

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>sourcetype</td>
<td>String</td>
<td></td>
<td></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/%252FAplications%252Fetc%252Fapps%252FmyApp%252Fbin%252FmyScript.sh -d interval=86400
```

**XML Response**
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 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>
</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"/>
```
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>
<tr>
<td>connection_host</td>
<td>Enum</td>
<td>dns</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</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>disabled</td>
<td>Boolean</td>
<td></td>
<td>remote server sending data.</td>
</tr>
<tr>
<td>host</td>
<td>String</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>none</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>name</td>
<td>Number</td>
<td></td>
<td>Default value is dns.</td>
</tr>
<tr>
<td>restrictToHost</td>
<td>String</td>
<td></td>
<td>Indicates whether the input is disabled.</td>
</tr>
<tr>
<td>Default value is dns.</td>
<td></td>
<td></td>
<td></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>name</td>
<td>Number</td>
<td></td>
<td>Required. The port number of this input.</td>
</tr>
<tr>
<td>queue</td>
<td></td>
<td></td>
<td>Required. The port number of this input.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Specifies where the input processor should deposit the events it reads.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Restrict incoming connections on this port to the host specified here.</td>
</tr>
<tr>
<td>Returned values</td>
<td></td>
<td></td>
<td>None</td>
</tr>
<tr>
<td>Example request and response</td>
<td></td>
<td></td>
<td>XML Request</td>
</tr>
</tbody>
</table>

---

**Example request and response**

**XML Request**
curl -u admin:pass
https://localhost:8089/servicesNS/nobody/search/data/inputs/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/data/inputs/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/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>

data/inputs/tcp/cooked/{name}

https://<host>:{mPort}/services/data/inputs/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
https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/tiny: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/data/inputs/tcp/cooked</id>
    <updated>2011-07-10T14:54:45-07:00</updated>
    <generator version="102807"/>
    <author>
        <name>Splunk</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_new" rel="create"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_reload" rel="_reload"/>
    ... opensearch nodes elided ...
    <s:messages/>
</feed>

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

**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/servicesNS/nobody/search/data/inputs/tcp/cooked</id>
  <updated>2011-07-10T14:52:40-07:00</updated>
  <generator version="102807"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <title>9998</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/9998</id>
    <updated>2011-07-10T14:52:40-07:00</updated>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
  </entry>
</feed>
```
<link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998" rel="list"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998" rel="edit"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998/remove" rel="remove"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998/connections" rel="connections"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/9998/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 node elided ...
  <s:key name="eai:attributes">
    <s:dict>
      <s:key name="optionalFields">
        <s:list>
          <s:item>SSL</s:item>
          <s:item>connection_host</s:item>
          <s:item>disabled</s:item>
          <s:item>host</s:item>
          <s:item>index</s:item>
          <s:item>queue</s:item>
          <s:item>restrictToHost</s:item>
          <s:item>source</s:item>
          <s:item>sourcetype</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="group">listenerports</s:key>
  <s:key name="host">MrT</s:key>
  <s:key name="index">default</s:key>
</s:dict>
</content>
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. Valid values: (ip</td>
</tr>
<tr>
<td>connection_host</td>
<td>Enum</td>
<td>ip</td>
<td>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.</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/
   xmlns:s="http://dev.splunk.com/ns/rest">
   <title>cooked</title>
   <id>https://localhost:8089/servicesNS/nobody/search/data(inputs/tcp/cooked</id>
   <updated>2011-07-10T14:52:54-07:00</updated>
   <generator version="102807"/>
   <author>
      <name>Splunk</name>
   </author>
   <link href="/servicesNS/nobody/search/data(inputs/tcp/cooked/_new"
   rel="create"/>
   <link href="/servicesNS/nobody/search/data(inputs/tcp/cooked/_reload"
   rel="_reload"/>
   ... opensearch nodes elided ...
   <s:messages/>
</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**

```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>cooked</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/</id>
  <generator version="101277"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_new" rel="create"/>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/_reload" rel="_reload"/>
  <opensearch:totalResults>1</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <entry>
    <title>Cooked:9998:127.0.0.1:20089</title>
    <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/cooked/Cooked%3A9998%3A127.0.0.1%3A20089</id>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/Cooked%3A9998%3A127.0.0.1%3A20089/_new" rel="create"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/Cooked%3A9998%3A127.0.0.1%3A20089/_reload" rel="_reload"/>
    <author>
      <name>system</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/cooked/Cooked%3A9998%3A127.0.0.1%3A20089" rel="alternate"/>
  </entry>
</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**

83
### Name Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>_rcvbuf</code></td>
<td>[Deprecated]</td>
</tr>
<tr>
<td><code>disabled</code></td>
<td>Input disabled indicator: 0 = Input Not disabled, 1 = Input disabled.</td>
</tr>
<tr>
<td><code>group</code></td>
<td>Set to <code>listenerports</code> for listening ports.</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>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"/>
  ...
  <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>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44000" rel="list"/>
  </entry>
</feed>
```
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>
<tbody>
<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.
<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>none leaves the host as specified in inputs.conf, which is typically the Splunk system hostname. Default value is ip. Indicates whether the inputs are disabled.</td>
</tr>
<tr>
<td>host</td>
<td>String</td>
<td></td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td>required</td>
<td>The input port which receives raw data.</td>
</tr>
<tr>
<td>queue</td>
<td>Enum</td>
<td></td>
<td>Specifies where the input processor should deposit the events it reads. Defaults to parsingQueue.</td>
</tr>
<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. If a connection over the port specified by name remains idle after receiving data for specified number of seconds, it adds a Done-key. This implies the last event is</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>completely received.</td>
<td></td>
<td></td>
<td></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::'. 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. Set the source type for events from this input.</td>
</tr>
<tr>
<td>sourcetype</td>
<td>String</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

<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}

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
<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>2011-07-08T02:37:09-07:00</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/>
  <entry>
```

90
<title>44343</title>
<id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/raw/44343</id>
<updated>2011-07-08T02:37:09-07:00</updated>
<link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343" rel="alternate"/>
<author>
  <name>nobody</name>
</author>
<link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343" rel="list"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343/_reload" rel="_reload"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343" rel="edit"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343" rel="remove"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343/connections" rel="connections"/>
<link href="/servicesNS/nobody/search/data/inputs/tcp/raw/44343/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 node elided ...
    <s:key name="eai:attributes">
      <s:dict>
        <s:key name="optionalFields">
          <s:list>
            <s:item>SSL</s:item>
            <s:item>connection_host</s:item>
            <s:item>disabled</s:item>
            <s:item>host</s:item>
            <s:item>index</s:item>
            <s:item>queue</s:item>
            <s:item>restrictToHost</s:item>
            <s:item>source</s:item>
            <s:item>sourcetype</s:item>
          </s:list>
        </s:key>
        <s:key name="requiredFields"/>
        <s:list/>
        <s:key name="wildcardFields"/>
        <s:list/>
        <s:key name="group">listenerports</s:key>
      </s:dict>
    </s:dict>
  </s:dict>
</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>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>connection_host</td>
<td>Enum</td>
<td>dns</td>
<td>Default value is ip.</td>
</tr>
<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></td>
<td>Host from which the indexer gets data.</td>
</tr>
<tr>
<td>index</td>
<td>String</td>
<td>default</td>
<td>Index to store generated events.</td>
</tr>
<tr>
<td>queue</td>
<td>Enum</td>
<td></td>
<td>Valid values: (parsingQueue</td>
</tr>
</tbody>
</table>
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 Monitor files and directories with inputs.conf.

Set queue to indexQueue to send your data directly into the index.

Specifies in seconds the timeout value for adding a Done-key. Default value is 10 seconds.

If a connection over the port specified by name remains idle after receiving data for specified number of seconds, it adds a Done-key. This implies the last event is completely received.

Allows for restricting this input to only accept data from the host specified here.

Sets the source key/field for events from this input. Defaults to the input file path.

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::'.

<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>10</td>
<td>Specifies in seconds the timeout value for adding a Done-key. Default value is 10 seconds.</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></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>
</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.

Set the source type for events from this input.

`sourcetype` String

"sourcetype=" is automatically prepended to <string>.

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>sourcetype</td>
<td>String</td>
<td></td>
<td></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>
  <author>
    <name></name>
    <uri></uri>
    <email></email>
  </author>
</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>
<updated>2011-07-13T16:14:33-07:00</updated>
<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 ...
<link href="/services/data/inputs/tcp/raw/_new" rel="create"/>
<link href="/services/data/inputs/tcp/raw/_reload" rel="_reload"/>
... opensearch nodes elided ...
<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>
  <updated>2011-07-13T16:14:33-07:00</updated>
  <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" rel="edit"/>
  <link href="/services/data/inputs/tcp/raw/Raw%3A9998%3A127.0.0.1/remove" rel="remove"/>
  <content type="text/xml">
    <s:dict>
      <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
curl -k -u admin:changeme
https://localhost:8089/services/data/inputs/tcp/splunktcptoken

XML Response

<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>
  <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"/>
  <opensearch:totalResults>2</opensearch:totalResults>
  <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
  <opensearch:startIndex>0</opensearch:startIndex>
  <s:messages/>
  <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>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1" rel="alternate"/>
    <author>
      <name>nobody</name>
    </author>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1" rel="list"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/_reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/edit" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1/remove" rel="remove"/>
    <content type="text/xml">
      <s:dict>
        <98
<entry>
  <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:dict>
          </s:key>
          <s:key name="removable">1</s:key>
          <s:key name="sharing">app</s:key>
        </s:dict>
      </s:key>
      <s:key name="host">$decideOnStartup</s:key>
      <s:key name="index">default</s:key>
      <s?key name="token">4EFFBD13-B26F-4F3A-BED9-03850001EDA1</s?key>
    </s:dict>
  </content>
</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</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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

```
<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"/>
```
data/inputs/tcp/splunktcptoken/{name}

https://<host>:<mPort>/services/data/inputs/tcp/splunktcptoken/{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**

curl -u admin:pass
https://localhost:8089/services/data/inputs/tcp/splunktcptoken

**XML Response**

...<title>splunktcptoken</title>
<id>https://localhost:8089/services/data/inputs/tcp/splunktcptoken</id>
<updated>2015-09-16T09:22:22-07:00</updated>
<generator build="71e3b8d1908254f21434f97320ac5ad7e6b1c16" 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"/>
<opensearch:totalResults>1</opensearch:totalResults>
<opensearch:itemsPerPage>30</opensearch:itemsPerPage>
<opensearch:startIndex>0</opensearch:startIndex>
<s:messages/>
<entry>
  <title>splunktcptoken://tok1</title>
  <id>https://localhost:8089/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3Atok1</id>
  <updated>2015-09-16T09:22:22-07:00</updated>
  <link href="/servicesNS/nobody/search/data/inputs/tcp/splunktcptoken/splunktcptoken%3A%252F%252Ftok1" rel="alternate"/>
  <author>
    <name>nobody</name>
  </author>
</entry>
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

...
<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:key name="eai:attributes">
  <s:dict>
    <s:key name="optionalFields">
      <s:list>
        <s:item>disabled</s:item>
        <s:item>token</s:item>
      </s:list>
    </s:key>
    <s:key name="requiredFields"/>
    <s:key name="wildcardFields">
      <s:list>
        <s:item>.*</s:item>
      </s:list>
    </s:key>
  </s:dict>
</s:key>
<s:key name="host">$decideOnStartup</s:key>
<s:key name="index">default</s:key>
<s:key name="token">99C91C9E-F92E-40AF-BCDC-1A6AD2DC7AEF</s:key>
...
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**

<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>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>
      <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"/>
   <opensearch:totalResults>0</opensearch:totalResults>
   <opensearch:itemsPerPage>30</opensearch:itemsPerPage>
   <opensearch:startIndex>0</opensearch:startIndex>
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>cipherSuit</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
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>_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**

```bash
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 ...
</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>Name</td>
<td>Datatype</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>---------</td>
<td>-----------------------------------------------------</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**

```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>2011-07-12T15:05:42-07:00</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

  <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"/>
  ... opensearch nodes elided ...
  <s:messages/>
</feed>
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>
<tbody>
<tr>
<td>connection_host</td>
<td>Enum</td>
<td>ip</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.

<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 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>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>String</td>
<td></td>
<td>Required. 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.</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>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**

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">
```
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
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

<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/
           _reload" rel="_reload"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/
           edit" rel="edit"/>
    <link href="/servicesNS/nobody/search/data/inputs/udp/44321/
           remove" rel="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:key name="_rcvbuf">1572864</s:key>
        <s:key name="disabled">0</s:key>
        ... eai:acl node elided ...
        <s:key name="eai:attributes">
          ...
        </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: (ip</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ip</td>
<td></td>
<td></td>
<td>Set the host for the remote server that is sending data.</td>
</tr>
<tr>
<td>ip</td>
<td></td>
<td></td>
<td>ip sets the host to the IP address of the remote server sending data.</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>dns</td>
<td></td>
<td></td>
<td><em>sets the host to the reverse DNS entry for the IP address of the remote server sending data.</em></td>
</tr>
<tr>
<td>none</td>
<td></td>
<td></td>
<td><em>leaves the host as specified in inputs.conf, which is typically the Splunk system hostname.</em></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default value is <em>ip.</em></td>
</tr>
<tr>
<td>disabled</td>
<td>Boolean</td>
<td></td>
<td>Indicates if the input is disabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The value to populate in the host field for incoming events.</td>
</tr>
<tr>
<td>host</td>
<td>String</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>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.</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>
<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>source</td>
<td>String</td>
<td></td>
<td>If this is not set, the value specified in [udp://&lt;remote server&gt;:&lt;port&gt;] in inputs.conf is used. 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/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"/>
```
**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**

```bash
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>
</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.</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>
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>
</tbody>
</table>
| logs    | String   |         | List of event log names from which to gather data:  
  • WMI collection format (CSV) example:  
    logs=Application%2CSystem%2CSetup%2CSecurity  
  • Native event log collection format example:  
    logs=Application&logs=System&logs=Setup |
| lookup_host | String |         | Required. Host from which to monitor log events. To specify additional hosts to be monitored using WMI, use the "hosts" parameter. |
| name    | String   |         | 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 "localhost", it uses native event log collection; otherwise, it uses WMI. |

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>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------------------------------------------------------------------</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**

```bash
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**

```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>2011-07-27T11:56:24-07:00</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>2011-07-27T11:56:24-07:00</updated>
    <link href="/servicesNS/nobody/windows/data/inputs/win-event-log-collections/localhost"
```
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.</td>
</tr>
<tr>
<td></td>
<td>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 ...
</s:messages/>
<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>
  <author>
    <name>nobody</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs" rel="alternate"/>
  <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/_edit" rel="edit"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/mylogs/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <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>hosts</s:item>
              <s:item>index</s:item>
              <s:item>logs</s:item>
            </s:list>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</entry>
</s:dict>
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>Name</td>
<td>Datatype</td>
<td>Default</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>----------</td>
<td>---------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>lookup_host</td>
<td>String</td>
<td></td>
<td><strong>Required.</strong> 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>2011-07-27T13:46:07-07:00</updated>
  <generator version="103620"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/servicesNS/nobody/search/data/inputs/win-event-log-collections/_new"/>
</feed>
```
<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">
    <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:key name="lookup_host">localhost</s:key>
      <s:key name="name">localhost</s:key>
    </s:dict>
  </content>
</entry>
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>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
```
<feed xmlns="http://www.w3.org/2005/Atom"
      xmlns:opensearch="http://a9.com/-/spec/opensearch/1.1/">
  <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"
         rel="list"/>
    <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/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:key name="fields">
          <s:list>
            <s:item>PercentProcessorTime</s:item>
          </s:list>
        </s:key>
      </s:dict>
    </content>
  </entry>
</feed>
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><strong>Required.</strong> 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.</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.</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>interval</td>
<td>Number</td>
<td></td>
<td>Specify each instance as a separate argument to the POST operation.</td>
</tr>
<tr>
<td>lookup_host</td>
<td>String</td>
<td></td>
<td>Required. The interval, in seconds, at which the WMI provider(s) is queried.</td>
</tr>
<tr>
<td>name</td>
<td>String</td>
<td></td>
<td>Required. This is the server from which we are 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>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>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

<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"/>
        <author>
            <name>nobody</name>
        </author>
        <link href="/servicesNS/nobody/windows/data/inputs/win-wmi-collections/CPUTime/_list" rel="list"/>
        <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"/>
        <content type="text/xml">
            <s:dict>
                142
            </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
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>
    <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-wmi-collections</id>
    <updated>2011-07-27T14:21:17-07:00</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/>
</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
<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>2011-07-27T14:09:39-07:00</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"
```
... 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>2011-07-27T14:09:39-07:00</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" rel="list"/>
  <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/edit" rel="edit"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu/remove" rel="remove"/>
  <link href="/servicesNS/nobody/search/data/inputs/win-wmi-collections/cpu/disable" rel="disable"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="classes">Win32_PerfFormattedData_PerfOS_Processor</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>fields</s:item>
              <s:item>index</s:item>
              <s:item>instances</s:item>
              <s:item>server</s:item>
            </s:list>
          </s:key>
          <s:key name="requiredFields">
            <s:list>
              <s:item>classes</s:item>
              <s:item>interval</s:item>
              <s:item>lookup_host</s:item>
            </s:list>
          </s:key>
        </s:dict>
      </s:key>
    </s:dict>
  </content>
</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><strong>Required.</strong> A valid WMI class name.</td>
</tr>
<tr>
<td>disabled</td>
<td>Number</td>
<td></td>
<td>Enables 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>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></td>
</tr>
</tbody>
</table>
Instances of a given class for which data is gathered.

Specify each instance as a separate argument to the POST operation.

<table>
<thead>
<tr>
<th>Name</th>
<th>Datatype</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>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>
    <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/_list" rel="list"/>
  </entry>
</feed>
```
<entry>
  <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: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:key name="index">default</s:key>
      <s:key name="instances">
        <s:list/>
      </s:key>
      <s:key name="interval">5</s:key>
      <s:key name="lookup_host">localhost</s:key>
      <s:key name="name">cpu</s:key>
      <s:key name="server"/>
      <s:key name="wql">Select * from Win32_PerfFormattedData_PerfOS_Processor</s:key>
    </s:dict>
  </content>
</entry>

---

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

curl -u admin:pass
https://localhost:8089/services/data/inputs/win-perfmon

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/services/data/inputs/win-perfmon</id>
  <updated>2011-07-29T19:42:06-07:00</updated>
  <generator version="104976"/>
  <author>
    <name>Splunk</name>
  </author>
  <link href="/services/data/inputs/win-perfmon/_new" rel="create"/>
  <link href="/services/data/inputs/win-perfmon/_reload" rel="_reload"/>
  ... opensearch nodes elided ...
</feed>
POST

Update performance monitoring collection settings.
### 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.</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.</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</td>
<td>String</td>
<td>required</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>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-----------------------------------------------------------------------------</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 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
-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/"
     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>2011-07-29T19:40:38-07:00</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>Available Memory</title>
    <id>https://10.1.5.157:8089/servicesNS/nobody/windows/data/inputs/win-perfmon/Available%20Memory</id>
    <updated>2011-07-29T19:40:38-07:00</updated>
    <link
```
data/inputs/win-perfmon/{name}

https://<host>:<mPort>/services/data/inputs/win-perfmon/{name}

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>
  <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>156</td>
<td></td>
</tr>
</tbody>
</table>
counters  List of valid Performance Monitor counters.
disabled  Indicates whether the input is disabled.
          The index that this input should send data to.
index    If no value is present, send data to the default index.
instances List of valid instances for a Performance Monitor counter.
interval How often, in seconds, to poll for new data.
object   A valid Performance Monitor object as defined within Performance Monitor.

Example request and response

XML Request

curl -u admin:pass
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>
  <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"/>
<content type="text/xml">
<s:dict>
  <s:key name="counters"/>
  <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:dict>
  <s:key name="requiredFields"/>
  <s:list/>
  <s:key name="wildcardFields"/>
  <s:list/>
</s:dict>
<s:key name="index">default</s:key>
<s:key name="instances"/>
<s:list/>
<s:key name="interval">4</s:key>
<s:key name="object">Memory</s:key>
</s:dict>
</content>
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.</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.</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. The index that this input should send data to.</td>
</tr>
<tr>
<td>index</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 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/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>
  <id>https://10.1.5.157:8089/servicesNS/nobody/search/data/inputs/win-perfmon</id>
  <updated>2011-07-29T19:45:59-07:00</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>
```
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>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>
  <id>https://localhost:8089/services/data/modular-inputs</id>
  <updated>2012-07-09T09:12:41-07:00</updated>
  <generator build="129290" version="5.0"/>
</feed>
Get data from Amazon S3.

- **Key ID**: Your Amazon key ID. Omitted inline data type: string. Omitted inline description: Your Amazon key ID.
- **Order**: 1
- **Required on Create**: 1
- **Required on Edit**: 0
- **Title**: Key ID

- **Resource name**: 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>
- **Order**: 0
- **Title**: Resource name

- **Secret key**: Your Amazon secret key. Omitted inline data type: string. Omitted inline description: Your Amazon secret key.
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.</td>
</tr>
</tbody>
</table>

The label appears in the Data inputs manager page.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 or simple (plain text).</td>
</tr>
<tr>
<td>title</td>
<td>Contains one or more &lt;arg&gt; elements, which define the parameters to an endpoint.</td>
</tr>
<tr>
<td></td>
<td>The label for a modular input script. The label appears in 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/twitter

**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>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>
  ... opensearch nodes elided ...
  <s:messages/>
  <entry>
    <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"/>  
    <content type="text/xml">
      <s:dict>
Get data from Twitter.

... eai:acl and eai:attribute nodes elided ...

<s:dict>
    <s:dict name="args">
        <s:dict name="name">
            <s:dict name="data_type">string</s:dict>
            <s:dict name="description">Name of the current feed using the user credentials supplied.</s:dict>
            <s:dict name="order">0</s:dict>
            <s:dict name="title">Twitter feed name</s:dict>
        </s:dict>
        <s:dict name="password">
            <s:dict name="data_type">string</s:dict>
            <s:dict name="description">Your twitter password</s:dict>
            <s:dict name="order">2</s:dict>
            <s:dict name="required_on_create">1</s:dict>
            <s:dict name="required_on_edit">0</s:dict>
            <s:dict name="title">Password</s:dict>
        </s:dict>
        <s:dict name="username">
            <s:dict name="data_type">string</s:dict>
            <s:dict name="description">Your Twitter ID.</s:dict>
            <s:dict name="order">1</s:dict>
            <s:dict name="required_on_create">1</s:dict>
            <s:dict name="required_on_edit">0</s:dict>
            <s:dict name="title">Twitter ID/Handle</s:dict>
        </s:dict>
    </s:dict>
    <s:dict name="streaming_mode">simple</s:dict>
    <s:dict name="title">Twitter</s:dict>
</s:dict>
indexing/preview

https://<host>:<mPort>/services/indexing/preview

Preview events from a source file before you index the file.

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>
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
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>Required</td>
<td>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**

```bash
curl -u admin:pass https://localhost:8089/services/indexing/preview -d input.path=/Applications/splunk/var/log/splunk/metrics.log
```

**XML Response**

```xml
<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**

```xml
<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>
  <updated>2011-10-24T15:44:09-07:00</updated>
  <link href="/services/indexing/preview/1319496093.11"
rel="alternate"/>
  <content type="text/xml">
    <s:dict>
      <s:key name="explicit">
        <s:dict>
          <s:key name="PREFERRED_SOURCETYPE">
            <s:dict>
              <s:key name="value">splunkd</s:key>
            </s:dict>
          </s:key>
        </s:dict>
        <s:key name="inherited">
          <s:dict>
            170
          </s:dict>
        </s:key>
      </s:dict>
    </content>
</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>
<tbody>
<tr>
<td>&lt;arbitrary_data&gt;</td>
<td>String</td>
<td></td>
<td><strong>Required.</strong> Raw event text. This is the entirety of the HTTP request body.</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>host</code></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><code>host_regex</code></td>
<td>String</td>
<td></td>
<td>A regular expression used to extract the host value from each event.</td>
</tr>
<tr>
<td><code>index</code></td>
<td>String</td>
<td>default</td>
<td>The destination index where events are sent.</td>
</tr>
<tr>
<td><code>source</code></td>
<td>String</td>
<td></td>
<td>The source value to fill in the metadata for this input's events.</td>
</tr>
<tr>
<td><code>sourcetype</code></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**

curl -u admin:pass  
-d "Sun Jul 10 15:56:02 PDT 2011 User myusername logged in successfully."

**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">
```
receivers/stream

https://<host>:<mPort>/services/receivers/stream

Open a socket to receive streaming data.

Authentication and authorization
The edit_tcp capability is 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><code>&lt;data_stream&gt;</code></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><code>host</code></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><code>host_regex</code></td>
<td>String</td>
<td></td>
<td>A regular expression used to extract the host value from each event.</td>
</tr>
<tr>
<td><code>index</code></td>
<td>String</td>
<td></td>
<td>The index to send events from this input to.</td>
</tr>
<tr>
<td><code>source</code></td>
<td>String</td>
<td></td>
<td>The source value to fill in the metadata for this input's events.</td>
</tr>
<tr>
<td><code>sourcetype</code></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

```python
import httplib, time

conn = httpplib.HTTPSConnection("localhost", 8089)
conn.connect()
conn.putrequest("POST", "/services/receivers/stream?source=www&sourcetype=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))
```

174
time.sleep(1)
i += 1
conn.close()

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. Required. Event payload key-value. Value can be a string or a JSON object.</td>
</tr>
<tr>
<td>event</td>
<td>string</td>
<td>JSON example: {&quot;event&quot;: {&quot;message&quot;:&quot;Access log test message&quot;}} 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</td>
</tr>
</tbody>
</table>
a key to specify the name and include one or more values. Specify multiple values in an array.

In the following example, the "severity" field gets the value "INFO" and the "category" key gets both "foo" and "bar" values.

```json
-d {"event": "something happened", "fields": {
  "severity": "INFO", "category": ["foo", "bar"]
}}
```

<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 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>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>
</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

For index=main | search sourcetype=access

<table>
<thead>
<tr>
<th>Time</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/26/15</td>
<td>[         ]</td>
</tr>
<tr>
<td>10:07:09.000 PM</td>
<td>[         ]</td>
</tr>
<tr>
<td></td>
<td>{ [-]</td>
</tr>
<tr>
<td></td>
<td>message: Access log test message 2</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td>1/26/15</td>
<td>[         ]</td>
</tr>
<tr>
<td>10:07:09.000 PM</td>
<td>[         ]</td>
</tr>
<tr>
<td></td>
<td>{ [-]</td>
</tr>
<tr>
<td></td>
<td>message: Access log test message</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

Request including the fields parameter


Basic auth request

curl -u x:46931F1C-352C-4DF6-820C-F2689CF88494 -k https://localhost:8088/services/collector/JSON -d 'Hello World'
services/collector/ack

<protocol>://<host>:<mPort>/services/collector/ack

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></td>
</tr>
</tbody>
</table>
Contains the key/value pairs for each ACK ID requested. For each key in the "acks" 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.

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**

```bash
```

**JSON response body**

{"acks":{"0":true,"1":true}}

**services/collector/event**

This endpoint works identically to services/collector but introduces a format option for future scalability. For more information, see services/collector.
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/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 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>Name</td>
<td>Datatype</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</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>string or unsigned integer</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**

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-80D1-819F80D7BF0

**MINT Request**

```bash
curl -k http://localhost:8088/services/collector/mint -H 'Authorization: Splunk B5A79AAD-D822-46CC-80D1-819F80D7BF0' -d '{"data":"hello"}1^1og^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 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 <code>channel</code> string parameter or using the <code>x-splunk-request-channel</code> header.</td>
</tr>
<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>string or unsigned integer</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

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.

curl
-k https://localhost:8088/services/collector/raw?channel=934793C0-FC91-467E-965A-7EAA
-H "Authorization: Splunk B5A79AAD-D822-46CC-80D1-819F80D7BF0" -d 'Hello World'}'

Request including a timestamp

curl
-k https://localhost:8088/services/collector/raw?channel=934793C0-FC91-467E-965A-7EAA
-H 'Authorization: Splunk 934793C0-FC91-467E-965A-7EAACEFBC4AB'
-d 'Wed Aug 10 12:27:53 PDT 2016 Hello World'

JSON request with timestamp

curl
-k https://localhost:8088/services/collector/raw?channel=934793C0-FC91-467E-965A-7EAA
-H 'Authorization: Splunk 934793C0-FC91-467E-965A-7EAACEFBC4AB'

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.