# Table of Contents

**Overview**
- About Splunk IT Service Intelligence ...................................................... 1
- IT Service Intelligence concepts and features ........................................ 1

**Entities**
- Overview of entities in ITSI ................................................................. 6
- Define a single entity in ITSI ............................................................... 7
- Auto-detect entities using ITSI modules .............................................. 8
- Import entities from a CSV file in ITSI ............................................. 8
- Import entities from a Splunk search in ITSI .................................... 12
- Set up a recurring import of entities in ITSI .................................... 14
- Conflict resolution examples in ITSI ............................................... 17
- Bulk delete entities in ITSI ............................................................ 19
- Manage pseudo entities in ITSI .................................................... 21

**Services**
- Overview of services in ITSI .............................................................. 24
- Create a single service in ITSI ............................................................ 25
- Bulk import services in ITSI ............................................................... 26
- Overview of configuring services in ITSI ........................................ 34
- Add entity rules to a service in ITSI ................................................... 36
- Add service dependencies in ITSI .................................................... 38
- Backfill service health scores in ITSI .............................................. 40
- Clone a service in ITSI ................................................................. 41
- How service health scores work in ITSI ........................................ 42

**KPIs**
- Overview of configuring KPIs in ITSI ............................................... 45
- Add a KPI to a service in ITSI ............................................................ 46
- Set KPI importance values in ITSI .................................................... 57
- Create KPI threshold time policies in ITSI ...................................... 59
- Apply adaptive thresholds to a KPI in ITSI ....................................... 65
- Receive alerts when KPI severity changes in ITSI ............................ 70
- Apply anomaly detection to a KPI in ITSI ........................................ 72
- Create KPI base searches in ITSI .................................................... 79
- Schedule KPI searches to update at the same time in ITSI ............. 86
# Table of Contents

## Service Templates

88
- Manage services in bulk with service templates in ITSI
- Create a service template in ITSI
- Configure a service created from a service template in ITSI
- Update a service template in ITSI
- Link a service to a service template in ITSI
- Manage service templates in ITSI

## Predictive Analytics

103
- Predict and prevent outages with ITSI Predictive Analytics
- Set up Predictive Analytics in ITSI
- Access Predictive Analytics in ITSI
- Determine whether your service is a good fit for modeling in ITSI
- Train a predictive model in ITSI
- Test a predictive model in ITSI
- Create an alert for potential service degradation in ITSI
- Add a predictive model to a glass table in ITSI
- Retrain a predictive model in ITSI
- Delete a predictive model in ITSI
- Predictive Analytics performance considerations in ITSI
- ITSI Predictive Analytics use case

## Event Analytics

137
- About ITSI Event Analytics
- Customize Episode Review in ITSI
- Set up custom episode actions in ITSI
- Normalize event fields in ITSI
- Manage notable events in ITSI
- Tune notable event grouping in ITSI
- Enable bidirectional ticketing in ITSI
- Dispatch episode actions to a remote ITSI instance
- Ingest third-party alerts as ITSI notable events
- Ingest SNMP traps in ITSI

## Aggregation Policies

168
- Notable event aggregation policies overview for ITSI
- About the default aggregation policy in ITSI
- Create a custom aggregation policy in ITSI
- Group similar events with Smart Mode in ITSI
# Table of Contents

**Correlation Searches** ................................................................................................. 178  
- Correlation search overview for ITSI ........................................................................ 178  
- Create correlation searches in ITSI .......................................................................... 179  
- Configure correlation searches in ITSI ...................................................................... 179  
- Create multi-KPI alerts in ITSI .................................................................................. 185  

**Managing Content** ................................................................................................... 190  
- Schedule maintenance downtime in ITSI ................................................................ 190  
- Back up and restore ITSI KV store data ................................................................... 193  
- kvstore_to_json.py operations in ITSI ..................................................................... 203  
- Create and manage saved searches in ITSI .............................................................. 217  

**Administer Splunk ITSI with configuration files** ......................................................... 219  
- About configuration files ......................................................................................... 219  
- List of ITSI configuration files .................................................................................. 220  

**Configuration file reference** ..................................................................................... 228  
- alert_actions.conf ..................................................................................................... 228  
- app_common_flags.conf ............................................................................................. 232  
- authorize.conf .......................................................................................................... 233  
- commands.conf ......................................................................................................... 256  
- collections.conf ........................................................................................................ 264  
- datamodels.conf ........................................................................................................ 267  
- deep_dive_drildowns.conf ........................................................................................ 275  
- distsearch.conf ......................................................................................................... 281  
- drilldownsearch_offset.conf .................................................................................... 296  
- fields.conf ................................................................................................................ 297  
- glasstable_icon_library.conf .................................................................................... 300  
- inputs.conf ................................................................................................................ 302  
- itsi_base_service_template.conf .............................................................................. 314  
- itsi_da.conf .............................................................................................................. 316  
- itsi_deep_dive.conf ................................................................................................... 318  
- itsi_event_management.conf ..................................................................................... 320  
- itsi_glass_table.conf ................................................................................................. 321  
- itsi_kpi_base_search.conf ........................................................................................ 323  
- itsi_kpi_template.conf ............................................................................................... 325  
- itsi_kpi_threshold_template.conf .......................................................................... 326  
- itsi_module_settings.conf ....................................................................................... 328  
- itsi_module_viz.conf ............................................................................................... 329
Table of Contents

Configuration file reference
itsi_notable_event_retention.conf ........................................................... 330
itsi_notable_event_severity.conf ............................................................. 332
itsi_notable_event_status.conf ............................................................... 333
itsi_service_analyzer.conf .................................................................. 335
itsi_service_template.conf .................................................................. 337
itsi_settings.conf .............................................................................. 339
itsi_team.conf .................................................................................... 343
limits.conf ........................................................................................... 345
logging.conf ...................................................................................... 431
macros.conf ......................................................................................... 432
mad.conf ............................................................................................. 435
notable_event_actions.conf .................................................................. 441
notable_event_commonality.conf .......................................................... 447
notable_event_correlation.conf ............................................................. 448
props.conf ........................................................................................... 451
restmap.conf ......................................................................................... 491
savedsearches.conf .............................................................................. 500
searchbnf.conf ..................................................................................... 505
service_analyzer_settings.conf ............................................................. 509
threshold_labels.conf .......................................................................... 510
threshold_periods.conf ........................................................................ 512
transforms.conf ................................................................................... 513
ui-tour.conf ......................................................................................... 539
visualizations.conf .............................................................................. 544
web.conf .............................................................................................. 548

Notable Event Action SDK...................................................................... 578
Use the Notable Event Actions SDK ....................................................... 578
Notable Event Actions SDK reference .................................................. 579

Troubleshooting ..................................................................................... 599
Search IT Service Intelligence logs ......................................................... 599
Overview

About Splunk IT Service Intelligence

Splunk IT Service Intelligence (ITSI) is a scalable IT monitoring and analytics solution that provides actionable insight into the performance and behavior of your IT operations.

As an ITSI admin, you can performing the following tasks:

- Ingest and analyze all types of IT event data.
- Create services based on your IT infrastructure for service-level agreement (SLA) monitoring.
- Add KPIs (key performance indicators) with severity-level thresholds to monitor the status of IT processes.
- Predict service health scores and prevent potential service outages.
- Set up service dependencies to identify upstream/downstream causal relationships.
- Build glass table visualizations of KPI search results for any service.
- Create deep dives to compare and analyze time-series events across IT services.
- Create multi-KPI alerts to generate notable events based on multiple KPI threshold trigger conditions.
- Apply anomaly detection to identify statistical outliers and find root cause faster.

See also

- ITSI concepts and features
- Install Splunk IT Service Intelligence

IT Service Intelligence concepts and features

Familiarize yourself with the following concepts and features before deploying Splunk IT Service Intelligence (ITSI).
ITSI workflow overview

The following diagram gives an overview of the basic workflows involved in configuring and using ITSI:

Key ITSI concepts

**Service**

A *service* is a logical mapping of IT objects that applies to your business goals. Splunk ITSI provides for a broad definition of a service. For example, a service can be:

- An application or group of applications
- An infrastructure tier (such as web, database, or network tier)
- A business service, such as an online store, with multiple tiers
- A single process, such as one instance of an application running on a host

ITSI lets you create services that model your IT infrastructure. ITSI services contain KPIs (Key Performance Indicators), which make it possible to monitor service health, perform root cause analysis, receive alerts, and ensure that your IT operations are in compliance with business SLAs (service-level agreements).
Entity

An entity is an IT infrastructure component, such as:

- A physical or virtual server
- A network device (switch, router)
- A user (AD/LDAP)
- A storage system or volume
- An operating system process
- A software application (database, web server, business app)
- An application process instance (for example, 2 instances of the same web server application is 2 separate entities)

Each entity has specific attributes and relationships to other IT processes that uniquely identify it. For example, a server that you define as an entity can have multiple IP addresses, MAC addresses, DNS names, and so on.

Data comes from applications on the entities, log files, and through API data collection processes. You can map data to entities in ITSI through aliases (field/value pairs) that you extract from Splunk searches. For example: host=10.141.24.63. In this way, entities link services to Splunk search results.

An entity is similar to a configuration item in the ITIL framework. However, an entity is never a service itself.

Entities are optional.

KPI

A KPI (Key Performance Indicator) is a recurring saved search that returns the value of an IT performance metric, such as CPU load percentage, memory used percentage, response time, and so on.

ITSI lets you create KPIs and add them to your services. You can then use KPI search result values inside ITSI to monitor service health, check the status of IT components, and troubleshoot trends that might indicate an issue with your IT systems.

For example, cpu_load_percent is a KPI that measures the CPU load percentage on a server. If your organization has a site uptime guarantee of 99.9% per month, you will need to monitor the status of this KPI (and others) to ensure that CPU performance remains within acceptable parameters.
Key ITSI features

**Service Analyzer**

The Service Analyzer provides an overview of ITSI service health scores and KPI search results that are currently trending at the highest severity levels. Use the Service Analyzer to quickly view the status of IT operations and to identify services and KPIs running outside expected norms. Click on any tile in the Service Analyzer to drill down to the deep dives for further analysis and comparison of search results over time.

For more information, see Monitor the health of your services with the ITSI Service Analyzer in the *IT Service Intelligence User Manual*.

**Glass tables**

Glass tables are custom visualizations that let you monitor KPI and service health scores. You can use glass tables to create dynamic contextual views of your IT topology or business processes and monitor them in real time. Glass tables features a drawing canvas where you can draw custom images, upload pre-existing images, and/or add icons from the Splunk icon library.

For more information, see Create a glass table in ITSI in the *Splunk IT Intelligence User Manual*.

**Deep dives**

Deep dives are an investigative tool that let you quickly identify and troubleshoot issues in your IT environment. Deep dives provide swimlane views that let you stack KPI search results over time and create contextual views showing all KPIs in a service. You can use deep dives to quickly zoom in on metric and log events, and visually correlate root cause.

For more information, see Overview of deep dives in ITSI in the *IT Service Intelligence User Manual*.

**Multi-KPI alerts**

A multi-KPI alert is an alert that is based on multiple KPI trigger conditions. When trigger conditions occur simultaneously, a correlation search generates a notable event. Multi-KPI alerts let you correlate the status of multiple KPIs, which can give you insight into system behavior, and help you to identify causal relationships that might negatively impact system performance.
For more information, see Create multi-KPI alerts in ITSI in the IT Service Intelligence User Manual.

**Episode Review**

ITSI provides a notable events management framework that lets you triage and analyze groups of notable events (episodes). ITSI generates notable events when a correlation search or multi-KPI alert meets specific conditions that you define. An episode is a group of events occurring as part of a larger sequence (an incident or period considered in isolation). Use Episode Review to view episode details and identify issues that might impact the performance and availability of your IT services.

Other ITSI notable events management features include a python-based, notable event action SDK, which lets you define secondary, post-notable event actions, such as add tags, add comments, view notable event activities, change owner, change status, change severity, and so on.

For more information, see Overview of Episode Review in ITSI in the IT Service Intelligence User Manual.

**ITSI modules**

ITSI modules provide pre-built KPIs, entity definitions, and dashboard visualizations. ITSI modules are tailored to specific IT use cases, such as monitoring and troubleshooting operating system hosts, load balancers, databases, app servers, and so on. Modules are optimized to process data that you collect using Splunk add-ons.

For more information, see ITSI Modules overview in the IT Service Intelligence Modules Manual.
Entities

Overview of entities in ITSI

In ITSI, an entity is an IT component that requires management to deliver an IT service. Each entity has specific attributes and relationships to other IT processes that uniquely identify it. Entities are usually hosts, but can also be items as diverse as network devices, applications, users, and cell towers.

ITSI entities can be any of the following components:

- Physical or virtual hosts
- Network devices (switches, routers)
- Users (AD/LDAP)
- Storage systems, volumes
- Operating system processes
- Software application (db, web server, business app)
- Application process instances (for example, 2 instances of the same web server application is 2 separate entities)
- Cell towers

Entities contain information that ITSI uses to associate services with information found in Splunk searches. You can use this entity information to filter items according to the entity definition.

An entity is similar to a "configuration item" in the ITIL framework, but an entity is never a service itself.

Define entities before creating services. When you configure a service, you can specify entity matching rules based on entity aliases that automatically add the entities to your service. For more information, see Configure services in ITSI in this manual.

How to define entities

There are four ways to create entities in ITSI:

- Define a single entity
- Auto-detect entities using ITSI modules
- Import entities from a CSV file
- Import entities from searches
All entities exist in the Global team. Only a user with write permissions to the Global team can create a single entity. Only a user with the itoa_admin role can import entities from CSV files or searches.

## Define a single entity in ITSI

This topic describes how to create a single entity in Splunk IT Service Intelligence (ITSI). An entity is an IT component that requires management to deliver an IT service. Each entity has specific attributes and relationships to other IT processes that uniquely identify it. For more information about entities, see [Overview of entities in ITSI](#).

### Prerequisites

You must have the itoa_admin role, or your role must have write access to the Global team, in order to create entities.

### Steps

1. In the ITSI top menu bar, click **Configure > Entities**.
2. Select **Create Entity > Create Single Entity**.
3. Configure the following fields to define your entity:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the entity.</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A brief description of the entity.</td>
</tr>
<tr>
<td>Team</td>
<td>All entities are created in the Global team. You can’t modify this field.</td>
</tr>
<tr>
<td>Aliases</td>
<td>Field-value pairs that identify the entity. For example:</td>
</tr>
<tr>
<td></td>
<td>host=webserver-01</td>
</tr>
<tr>
<td></td>
<td>IP=10.2.1.1</td>
</tr>
<tr>
<td></td>
<td>MAC=C6:4B:B9:E8:E6:2A</td>
</tr>
<tr>
<td>Info Fields</td>
<td>Field-value pairs that associate specific attributes with the entity. For example:</td>
</tr>
<tr>
<td></td>
<td>role=webserver</td>
</tr>
<tr>
<td></td>
<td>owner=Ops</td>
</tr>
</tbody>
</table>

The following characters aren’t supported in fields or values: commas (,), single quotes (’), double quotes (“), ampersand (&), $ (as first character), period (.), equal sign (=), and spaces().

4. Click **Create**. The entity appears in the Entities lister page.
5. (Optional) Click View Health to view detailed entity information, including the health status of associated services and KPIs.

Auto-detect entities using ITSI modules

The modules included with ITSI can help automatically discover entities. For example, when a new server comes online, ITSI can automatically add it as an entity. Entity discovery occurs on a scheduled basis (usually every 4 hours) if the modules included with ITSI are properly configured and the add-ons required for data collection are installed and properly configured.

For example, the OS module automatically detects all the servers that are sending data into the Splunk platform using the Splunk Add-on for Unix and Linux or the Splunk Add-on for Microsoft Windows. Entity types such as OS hosts, virtualization hypervisors, VMs, web servers, database servers, and load balancers can be created and populated as entities in ITSI using module entity discovery searches.

See also

- ITSI module entity discovery

Import entities from a CSV file in ITSI

Import entities from CSV files that contain one or more entity definitions. Importing entities from CSV files is an efficient way to define multiple entities. You can dump data from a change management database (CMDB) or asset inventory database into a CSV file and automate the import for ongoing updates.

Prerequisite

- By default, only a user with the itoa_admin role can bulk import entities.
- To import entities from CSV, you must create a CSV file that contains your entity definitions. Specify column names in the first row. In each subsequent row, specify an entity title, as well as one or more entity aliases, and one or more entity information fields. To associate an entity with a service, provide a column with the name of the service. Import from CSV has a limit of one service and one entity per row. There is no limit on the number of dependent services, entity aliases, or entity rule values per row. A CSV file can contain multiple rows. Import from CSV supports five
different separators: comma (,), semicolon (;), pipe (|), tab (\t), and caret (^).

Scenario

In this example we want to create two entities called appserver-04 and appserver-05, and associate appserver-04 with the Web A service and associate appserver-05 with the Web B service. The Web A service already exists in ITSI but the Web B service does not.

Steps

1. Click Configure > Entities.
2. Click Create Entity > Import from CSV.

If your role does not have write access to Global team, you will not see the New Entity button.
3. Click browse... and select your CSV file, or drop it into the UI. The CSV file uploads and a file preview appears.
4. Click Next.
5. Under Import Column As, select the appropriate column type for each column.

<table>
<thead>
<tr>
<th>Column type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity Title</td>
<td>Makes the column entry the entity title. The column is also added as an Entity Alias using &lt;column name&gt; = &lt;value&gt;.</td>
</tr>
<tr>
<td>Entity Description</td>
<td>Makes the column entry a description of the entity.</td>
</tr>
<tr>
<td>Entity Alias</td>
<td>Makes the column entry a searchable entity identifier.</td>
</tr>
<tr>
<td>Entity Information field</td>
<td>Makes the column entry a tag that provides user-facing validation.</td>
</tr>
<tr>
<td>Service Title</td>
<td>Makes the column entry the name of the service to associate the entity with. The service will be created if it</td>
</tr>
<tr>
<td>Column type</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Service Description</td>
<td>Makes the column entry the description of the service.</td>
</tr>
<tr>
<td>Do Not Import</td>
<td>Removes the column entry from the imported data.</td>
</tr>
</tbody>
</table>

You can edit the Column Name field for columns that you import as Entity Title, Entity Alias, and Entity Information, for custom field mappings.

For this example, we map the columns in the CSV file to the following fields in ITSI:

<table>
<thead>
<tr>
<th>Column Name</th>
<th>Import Column As</th>
<th>Set per ticket from CSV file</th>
</tr>
</thead>
<tbody>
<tr>
<td>service</td>
<td>Service Title</td>
<td>Yes</td>
</tr>
<tr>
<td>service_desc</td>
<td>Service Description</td>
<td>Yes</td>
</tr>
<tr>
<td>desc</td>
<td>Entity Title</td>
<td>Yes, Skip Over Existing Entities</td>
</tr>
<tr>
<td>vendor_name</td>
<td>Entity Alias</td>
<td>Yes, Skip Over Existing Entities</td>
</tr>
<tr>
<td>ip</td>
<td>Entity Information Field</td>
<td>Yes, Skip Over Existing Entities</td>
</tr>
<tr>
<td>port</td>
<td>Entity Information Field</td>
<td>Yes, Skip Over Existing Entities</td>
</tr>
<tr>
<td>net.zone</td>
<td>Entity Information Field</td>
<td>Yes, Skip Over Existing Entities</td>
</tr>
</tbody>
</table>

6. Configure the following options in the Settings section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Team</td>
<td>The team to create the services in.</td>
</tr>
<tr>
<td>(Only displayed if you are importing services.)</td>
<td></td>
</tr>
<tr>
<td>Import Services As</td>
<td>Whether services are enabled or disabled upon import.</td>
</tr>
<tr>
<td>(Only displayed if you are importing services.)</td>
<td></td>
</tr>
<tr>
<td>Conflict Resolution</td>
<td>Determines how ITSI updates and stores your entity data:</td>
</tr>
<tr>
<td></td>
<td>✦ Skip Over Existing Entities: Adds new entity data to the datastore only if the entity does not already exist. If an entity already exists, the entity is not updated.</td>
</tr>
<tr>
<td></td>
<td>✦ Update Existing Entities: Merges the imported data and the existing data associated with the</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>entity. Uses the Conflict Resolution field to identify the entity.</td>
<td></td>
</tr>
<tr>
<td>♦ <strong>Replace Existing Entities:</strong> Replaces existing entity data with new entity data. Uses the Conflict Resolution field to identify the entity.</td>
<td></td>
</tr>
<tr>
<td>Conflict Resolution Field</td>
<td>The field used to merge on. Entities that have the same field value are considered to be the same entity. For example, if there is an entity defined with the same IP then merge into that entity. If Conflict Resolution is set to <strong>Update Existing Entities</strong> or <strong>Replace Existing Entities</strong>, ITSI resolves duplicate entities based on this field.</td>
</tr>
</tbody>
</table>

For this example, we are using **Update Existing Entities** and `host` for the Conflict Resolution field. For more information about Conflict Resolution, see Conflict Resolution examples in ITSI.

7. In the Preview section, click **Entities to be imported** to confirm that your entity import configuration is correct.

The preview shows the entity information you're importing. It doesn't show the final merged entity values.

8. Click **Import**.

9. Click **View all Entities** and **View all Services** to confirm that your imported entities and services appear.

For example, for service Web A (which already existed), an Entity Title matching rule has been added for `appserver-04`. `appserver-04` is listed in the table of matching entities and the aliases and Information fields have been added to the entity from the CSV file.
We also see that the service Web B has been created and that an Entity Title matching rule has been added for appserver-05. We see appserver-05 listed in the table of matching entities at the bottom and we see the aliases and information fields have been added to the entity from the CSV file.

10. (Optional) Click **Set up Recurring Import** to create a modular input for the CSV file. For more information, see **Set up recurring import of entities in ITSI** in this manual.

## Import entities from a Splunk search in ITSI

ITSI lets you import multiple entities from ITSI module searches, saved searches, or ad hoc searches using any data coming into the Splunk platform. The Import from Search workflow is identical to the Import from CSV workflow, except that you specify a search string instead of uploading a CSV file.

For CMDB integration, you can set up the Splunk platform to directly query the database where the CMDB data is stored so that you can use a Splunk search to import the CMDB data into ITSI as entities. You can automate the import from search for ongoing updates.

1. Click **Create Entity > Import from Search**.

   If your role does not have write access to the Global team, you will not see the Create Entity option.

2. Select one of the following search types:

<table>
<thead>
<tr>
<th>Search Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module</td>
<td>Choose from a list of pre-defined entity discovery searches based on ITSI modules.</td>
</tr>
<tr>
<td>Saved Searches</td>
<td>Choose from a list of pre-defined ITSI saved searches.</td>
</tr>
</tbody>
</table>
### Search Type Description

<table>
<thead>
<tr>
<th>Search Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad hoc Search</td>
<td>Enter a custom search string.</td>
</tr>
</tbody>
</table>

3. Enter an ad hoc search string or select a pre-defined module search or saved search. Make sure the results are presented in a table. In this example we want to import entities using an ad hoc search.

4. Click the Search icon to view a preview of the search results.

5. Click **Next**.

6. Use the Select Column page to specify how to classify and store the file column entries that define your entities.
   In this example, we select to import the title column as **Entity Title** and the hostname column as **Entity Alias**.

7. Configure the following options in the Settings section:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Team</td>
<td>The team to create the services in.</td>
</tr>
<tr>
<td>(Only displayed if you</td>
<td></td>
</tr>
<tr>
<td>are importing services.)</td>
<td></td>
</tr>
<tr>
<td>Import Services As</td>
<td>Whether services are enabled or disabled upon import.</td>
</tr>
<tr>
<td>(Only displayed if you</td>
<td></td>
</tr>
<tr>
<td>are importing services.)</td>
<td></td>
</tr>
<tr>
<td>Conflict Resolution</td>
<td>Determines how ITSI updates and stores your entity data:</td>
</tr>
</tbody>
</table>

---

13
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Skip Over Existing Entities:</td>
<td>Adds new entity data to the datastore only if the entity does not already exist. If an entity already exists, the entity is not updated.</td>
</tr>
<tr>
<td>♦ Update Existing Entities:</td>
<td>Merges the imported data and the existing data associated with the entity. Uses the Conflict Resolution field to identify the entity.</td>
</tr>
<tr>
<td>♦ Replace Existing Entities:</td>
<td>Replaces existing entity data with new entity data. Uses the Conflict Resolution field to identify the entity.</td>
</tr>
</tbody>
</table>

The field used to merge on. Entities that have the same field value are considered to be the same entity. For example, if there is an entity defined with the same IP then merge into that entity. If Conflict Resolution is set to Update Existing Entities or Replace Existing Entities, ITSI resolves duplicate entities based on this field.

For more information about Conflict Resolution, see Conflict Resolution examples in ITSI.

8. In the Preview section, click **Entities to be imported** to confirm that your entity import configuration is correct.

The preview shows the entity information you’re importing. It doesn't show the final merged entity values.

9. Click **Import**.

A message appears confirming that the import is complete.

10. Click the **View all Entities** link to confirm your imported entities appear in the Entity viewer page.

11. (Optional) Click **Set up Recurring Import** to create a modular input for the CSV file. See Set up recurring import of entities in ITSI.

### Set up a recurring import of entities in ITSI

After the bulk import process is complete, ITSI gives you the option of creating a modular input that repeats the import function on a recurring basis. This is
convenient if you want to add or update entities or services without repeating the entire import from CSV or search workflow.

You cannot set up a recurring import from the UI in a search head cluster environment. Follow the steps in Set up a recurring import on a search head cluster below.

Prerequisite

Before setting up recurring import, you must import entities from a CSV file or a Splunk search.

- Import entities from a CSV file in ITSI
- Import entities from a Splunk search in ITSI

Set up a recurring import on a single instance

1. After the import from CSV or search process is complete, click Set up Recurring Import.
2. Provide a name for the recurring import.
3. If you're importing a CSV file, enter the full path to the file on the server. The CSV file must be on the same server as your ITSI installation.
4. Set the scheduled time and frequency to run the import.
5. Click Submit. ITSI creates the new modular input in $SPLUNK_HOME/etc/apps/itsi/local/inputs.conf.

The recurring import search executes as splunk-system-user, which returns entities from datasets that exist in indexes that the user creating the import might not have access to.

Set up a recurring import on a search head cluster

You cannot set up a recurring import from the UI in a search head cluster environment. You must configure the modular input manually in inputs.conf and push it to the search peers using the deployer.

1. Follow the steps above to create the modular input through the UI. ITSI adds the input as a new stanza in $SPLUNK_HOME/etc/apps/itsi/local/inputs.conf. It is not replicated across search peers.
Alternatively, if you're familiar with the format of modular inputs, you can create the input yourself.

2. Copy the input stanza from the local version of inputs.conf and add it to shcluster/apps/itsi/local/inputs.conf on the deployer.

3. Let the deployer push the file to the search peers. The file is deployed to the default inputs.conf on each search peer.

4. Remove the modular input stanza from $SPLUNK_HOME/etc/apps/itsi/local/inputs.conf on the search head that created it. Otherwise it will take precedence on the deployer.

Modify or delete a recurring import on a search head cluster

You can't manage recurring imports on a search head cluster through the UI. If you need to change the search, pause or stop the import, or delete the import, you must do it through inputs.conf.

1. Navigate to shcluster/apps/itsi/local/inputs.conf on the deployer.

2. Locate the stanza for the recurring import you want to modify or remove. For example:

   [itsi_csv_import://Recurring entity import]
   entity_field_mapping = title=entity_title
   entity_informational_fields = hostname
   entity_merge_field = title
   entity_title_field = title
   import_from_search = true
   index_earliest = -60m
   index_latest = now
   interval = 0 3 * * *
   search_string = index=main sourcetype=* | dedup hostname | eval title=hostname | table title hostname
   service_security_group = default_itsi_security_group
   update_type = upsert

3. Modify, add, or delete any settings.
   ♦ For descriptions of all possible settings, see the [itsi_csv_import://<string>] stanza of inputs.conf.
   ♦ To pause or stop the import, add the setting disabled = 1 to the stanza.
   ♦ To delete the import, remove the stanza completely.

4. Save the file and let the deployer push the changes to the search peers.

See also

- Modular inputs overview
- Bulk delete entities in ITSI
Conflict resolution examples in ITSI

When you import entities from CSV or search, you must select a conflict resolution type and a conflict resolution field. The conflict resolution field is the field you’d like to use to identify entities. Entities that have the same value for the conflict resolution field are considered to be the same entity. The conflict resolution type determines how ITSI updates and stores your entity data. The following examples demonstrate the behavior of each conflict resolution type.

Skip Over Existing Entities

Adds new entity data to the datastore only if the entity does not already exist. If an entity exists, the information is not updated.

For example, if you import the following CSV file and you use title as the Conflict Resolution field, if Server_1 and Server_2 already exist as entities, they will not be updated with the imported data. If no entities already exist with a title of Server_1 or Server_2, these entities will be created from the imported data.

<table>
<thead>
<tr>
<th>title, IP, host</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server_1, 192.168.1.1, somehostName</td>
</tr>
<tr>
<td>Server_2, 192.168.2.2, anotherhostName</td>
</tr>
</tbody>
</table>

Update Existing Entities

Merges alias and information fields of imported entities with existing entities. Entities that have the same value in the Conflict Resolution field are treated as the same entity.

- Each entity that matches the Conflict Resolution field value receives the merged field values.
- If the Conflict Resolution field doesn't exist in the existing entity, the existing entity isn't affected.
- If the Conflict Resolution field doesn't exist in the CSV or search data, the row data isn't imported.
- If the Conflict Resolution field is an Alias, but in the existing entity the field is an Info field, the existing Info field is preserved.
- If the Conflict Resolution field is an info field, but in the existing entity the field is an Alias, the existing Alias field is preserved.

In this example, the entities in the first example have been created and now you import the following updated entity information using title as the Conflict Resolution field:

<table>
<thead>
<tr>
<th>title, IP, host</th>
</tr>
</thead>
<tbody>
<tr>
<td>newServer_1, 192.168.1.1, newsomehostName</td>
</tr>
<tr>
<td>newServer_2, 192.168.2.2, newanotherhostName</td>
</tr>
</tbody>
</table>
Server_2 will now have two IP addresses, 192.168.2.2 and 192.168.2.3, while no new data is added to Server_1.

Replace Existing Entities

Replaces existing entity data with new entity data. Entities that have the same value in the Conflict Resolution field are treated as the same entity. For example, if you now import this entity information using title as the Conflict Resolution field:

```
title, IP, host
Server_1, 192.168.1.2, somehostName2
Server_2, 192.168.2.2, anotherhostName2
```

The Server_1 and Server_2 entities, which already exist, are replaced with the new entity definitions for Server_1 and Server_2 in the import. The old Alias and Info fields for the entities are replaced with the ones in the import so Server_1 will now have an IP of 192.168.1.2 and a host of somehostName2 and Server_2 will now have an IP of 192.168.2.2 and a host of anotherhostName2.

Example of using a Conflict Resolution field other than Entity Title with Update Existing Entities option

For example, let's say you have two hosts with the same name in different data centers. You import the following columns:

<table>
<thead>
<tr>
<th>Entity Title (Name)</th>
<th>Information Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>host=A</td>
<td>datacenter=A</td>
</tr>
<tr>
<td>host=A</td>
<td>datacenter=B</td>
</tr>
</tbody>
</table>

If you use the host column (Entity Title) as the Conflict Resolution field, and use the Update Existing Entities option, one entity is created because both entities have the same value for host. This means they are treated as the same entity. After importing, entity A will contain both A and B values for datacenter as shown below.

<table>
<thead>
<tr>
<th>Entity Title (Name)</th>
<th>Alias</th>
<th>Information Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>host=A</td>
<td>datacenter=A,B</td>
</tr>
</tbody>
</table>
If instead you use the `datacenter` column (Entity Information Field) as the Conflict Resolution field with the Update Existing Entities option, two entities will be created: the first entity A will be created with an Information field of `datacenter=A` and a second entity A will be created with `datacenter=B` as shown below.

<table>
<thead>
<tr>
<th>Entity Title (Name)</th>
<th>Alias</th>
<th>Information Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>host=A</td>
<td>datacenter=A</td>
</tr>
<tr>
<td>A</td>
<td>host=A</td>
<td>datacenter=B</td>
</tr>
</tbody>
</table>

**Bulk delete entities in ITSI**

Delete entities in bulk if you have a lot of duplicate entities. For example, you might have duplicate entities imported from the Splunk App for Infrastructure (SAI) that you want to get rid of.

The following example shows you how to bulk delete entities from SAI.

1. Use the curl command to spit out the entities that match the ITSI role "SAI".
   ```
   curl -k -u admin:changeme
   https://localhost:8089/servicesNS/nobody/SA-ITOA/itoa_interface/entity?filter='{"itsi_role":"SAI"}'&fields='_key'
   ```
2. Delete the entities.
   ```
   curl -k -u admin:changeme -X DELETE
   https://localhost:8089/servicesNS/nobody/SA-ITOA/itoa_interface/entity?filter='{"itsi_role":"SAI"}'&fields='_key'
   ```

**Disable recurring entity import searches**

After you delete entities, you might still see them populating automatically in the UI. This is most likely because you set up recurring entity imports in the past. These recurring import searches periodically re-populate your entities even after you delete them. For more information, see Set up a recurring import of entities in ITSI.

ITSI saves recurring imports as modular inputs. On a single instance deployment, you can disable or delete these modular inputs through the UI.

1. Click **Settings > Data inputs**.
2. Click **IT Service Intelligence CSV Import**. All recurring imports that you've configured are listed here, in addition to the entity discovery searches that are bundled with ITSI modules.
3. In the Status column, click **Disable** for each recurring import that you want to disable. It is best practice to not delete them altogether, as you might want to enable them again in the future.

**Disable recurring entity import searches in a search head cluster**

ITSI saves recurring entity import searches as modular inputs in a local version of `inputs.conf`. You cannot disable modular inputs using the UI in a search head cluster environment. You must manually disable them through `inputs.conf` on each search head in your environment.

**Prerequisites**

- Only users with file system access, such as system administrators, can disable modular inputs.
- Review the steps in How to edit a configuration file in the *Admin Manual*.

Never change or copy the configuration files in the `default` directory. The files in the `default` directory must remain intact and in their original location.

**Steps**

1. On each search head, navigate to
   
   `$SPLUNK_HOME/etc/apps/itsi/local/inputs.conf`.

2. In each recurring import stanza within the file, add the line **Disabled = 1**.
   
   For example:

   ```plaintext
   [itsi_csv_import://Appservers]
   backfill_enabled = 0
   csv_location = /Users/username/Documents/Entities.csv
   entity_identifier_fields = itsi_role
   entity_informational_fields = IP,host
   entity_title_field = vendor
   import_from_search = false
   interval = 0 8 * * *
   service_description_column = service_desc
   service_enabled = 1
   service_security_group = default_itsi_security_group
   service_title_field = ?ITService
   template = {}
   update_type = upsert
   Disabled = 1
   ```

3. Save and close the file.
Manage pseudo entities in ITSI

A pseudo entity in IT Service Intelligence (ITSI) is an entity that's automatically generated by a KPI split. It's not a real entity because it has no ID and isn't stored anywhere except in the summary index.

You create a pseudo entity if you split a KPI by entity but the entity split field isn't matched in the entity lookup. For more information about splitting a KPI, see Split by entity in the KPI configuration workflow. You won't create a pseudo entity if you split a KPI by entity and filter to entities in the service, unless you do an entity pivot. For instructions, see Entity pivot below.

Pseudo entities appear in the UI as the field value of the entity split field. For example, if you split by host and the host values are A, B, and C, it's possible that A and B match to entities with titles of appserver-01 and appserver-02, but C doesn't match to anything. ITSI displays their names as appserver-01 and appserver-02, and C. Pseudo entities aren't clickable in the Service Analyzer.

The entity key of a pseudo entity is N/A because ITSI can't find a match in the lookup to put a real ID in that field. The entity title field is the only thing that identifies a pseudo entity because alias normalization isn't possible without an entity record.

The following table describes the advantages and disadvantages of using pseudo entities:

<table>
<thead>
<tr>
<th>Advantages of pseudo entities</th>
<th>Disadvantages of pseudo entities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase the speed of setup because you don't have to configure entities</td>
<td>Don't have an entity details page</td>
</tr>
<tr>
<td>Perform better than entities because they don't require a lookup</td>
<td>Can't be displayed in a deep dive swim lane</td>
</tr>
<tr>
<td>Better management of dynamic entities using entity pivot</td>
<td>Don't allow for entity normalization, and you can't use them to filter to anything</td>
</tr>
</tbody>
</table>

Entity pivot

An entity pivot lets you associate pseudo entities to a particular service, even through a shared base search without entity broadcast. To configure an entity pivot, provide a different value for the entity filter field than you do for the entity split field during KPI configuration. Entity pivots are useful because you can filter to entities in the service while still using only pseudo entities.
For example, instead of creating entities that are hosts, you want to create large groups of entities that you can filter on in your data. You have a service called American Southeast and you filter the data with datacenter=Florida and datacenter=Georgia. You make a Florida entity and a Georgia entity and add them to your service. Then you filter a KPI by Georgia and Florida but split it by host. By using entity pivot, you can have relatively static entities that act as pure filters, and lots of highly dynamic small entities that you want to monitor, but you don't have to keep track of them in a CMDB sense.

**When to use entity pivot**

Consider using entity pivot if you dynamically spin up and down virtual machines or you use a system like Kubernetes and you want to split by pod. Virtual machines and pods are difficult to define as entities because they're too dynamic. As pseudo entities, they're defined at the time the KPI search runs. You can filter based on relatively static entities, but split on the dynamic entities.

ITSI allocates service membership in shared base searches based on the filter field, not based on the split by field. Therefore, you don't need to worry about pseudo entities being assigned to the wrong service.

**Entity pivot example**

You configure the following metrics KPI to monitor CPU usage by process:

```
|mstats avg(_value) as alert_value WHERE index=em_metrics metric_name="processmon.cpu.percent" by process_name, host
```

To perform an entity pivot and associate those dynamic processes to a service, you split by `process_name` but filter by `host`. Each host acts as the filter and associates processes to that particular service. Each process is defined at the time the KPI search runs.

The following image shows the entity split and filter configuration:
**Entity broadcast**

If you have pseudo entities but you don’t filter to entities in the service, and you try to use that pseudo entity in a shared base search, the entity is assigned to all services. This functionality is called "entity broadcast".

Entity broadcast occurs because service membership is based on the filter field, not on the split by field. If you use entity pivot and the filter and split fields are the same, all entities and pseudo entities within that filter belongs to that service. However, as soon as an entity belongs to no services, it belongs to all services. This functionality is not ideal except in rare scenarios.

A pseudo entity, even though it has `entity_key=N/A`, will never be broadcasted if it belongs to a service due to the filter field (entity pivot). Defined entities can never be broadcasted.

**Pseudo entities in correlation searches**

If you have a pseudo entity in your correlation search, you need to either statically assign it to a service, or do an entity lookup based on what is traditionally the entity filter field in a pivot scenario. An entity lookup in a correlation search needs to look up on the large group of static entities, if you have that type of entity, instead of looking up on host. For more information, see Entity pivot above. In other words, you must either statically assign the entity to a service, or match against something other than that entity.

No entity relationship option exists in ITSI, and there are no additional metadata fields available for pseudo entities. As a workaround, you can associate two fields to each other using the `eval` command to create the entity title field.
Overview of services in ITSI

This topic provides an overview of how to create services for your Splunk IT Service Intelligence (ITSI) deployment. For instructions on configuring services, see Configure services in ITSI in this manual.

What is an ITSI service?

An ITSI service is a representation of a real-world IT service that lets you monitor the health of IT systems and business processes. For more information on ITSI services, see ITSI concepts and features in this manual.

After you create and configure a service, you can use ITSI to monitor service health, perform root-cause analysis, set up threshold-based alerts, and track compliance with organizational SLAs (service-level agreements).

Services must be assigned to a team. A service is only visible for roles that are assigned read permissions to the team. A service can only be edited by roles that are assigned read and write permissions to the team. If your organization has decided not to create private teams, all services will reside in the Global team. For information about teams, see Implement service-level permissions in ITSI.

Note: Before you create a service, it is a best practice to define the entities that you want the service to contain. You can then add entities to the service when you configure the service. For more information, see Overview of entities in ITSI in this manual.

How to create services

There are three ways to create services:

Create a single service in ITSI
Create new services one at a time in the UI. You can use service templates to quickly configure services.

Import from CSV
Import new services and link them to service templates from a CSV file. This method lets you import a hierarchy of dependent services with entities already associated. You can also create a modular input that runs
automated recurring imports of the CSV file contents.

**Import from search**
Add services and link services to service templates from an ITSI module, saved search, or ad hoc search.

---

**Create a single service in ITSI**

When you create a service, you have three options for populating the service:

- Manually add the KPIs and entity rules.
- Link the service to a service template to populate the KPIs and entity rules from the service template. See Create a service template in ITSI for information about service templates.
- Select prebuilt KPIs from ITSI modules to populate KPIs and entity rules.

**Prerequisite**

By default, users assigned the itoa_admin role or a role that inherits from the itoa_team_admin role can create a new service. You can only create a service in a team for which you have read and write permissions.

**Steps**

1. Click **Configure > Services**.
2. Click **New Service > New Service**.

   If your role does not have write access to any teams, you will not see the New Service option.
3. Provide a title and description for the service.
4. Select the team to associate the service with. This service will only be visible for roles that are assigned read permission to this team. If no private teams have been created for your organization, the only team available will be Global and this is where you will create all services.
5. Select one of the following options:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manually add service content</td>
<td>Manually add entities, KPIs, and other information for this service.</td>
</tr>
<tr>
<td>Link service to a service template</td>
<td>Populate the service with the entity rules and KPIs from a service template.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Add prebuilt KPIs from modules</td>
<td>Populate the service with the entity rules and pre-built KPIs from ITSI modules.</td>
</tr>
</tbody>
</table>

6. If you selected **Link service to a service template**, do the following:
   1. Select the template to link the service to.
   2. Review the entity rules and KPIs in the template. These will be added to the new service.
   3. (Optional) Select **Enable 7 days of backfill for all Service KPIs** if you need to populate the summary index with data in order to use adaptive thresholding or anomaly detection with any of your KPIs. This setting applies to all the KPIs in the service. Individual KPIs cannot be selected for backfill. Note that you cannot enable backfill for a KPI that came from the template in the service later on as this action will unlink the service from the template.

7. If you selected **Add pre-built KPIs from modules**, do the following:
   1. Select any number of ITSI modules from the list. Before using pre-built KPIs, you must configure the specific ITSI module. See About ITSI modules in the *ITSI Modules* manual.)
   2. Select the KPIs to add to the service. Recommended KPIs are pre-selected. Each KPI template populates the new service with specific entity rules and selected KPIs.

8. Click **Create**.

After creating the service, see [Overview of configuring services in ITSI](#) to decide how to configure the newly created service.

### Bulk import services in ITSI

ITSI provides two methods to bulk import service definitions:

- **Import from CSV**
  - Import service definitions from a CSV file.
- **Import from search**
  - Import service definitions from Splunk searches.

You can use either bulk import method to do the following:

- Create multiple services.
- Add service dependencies.
- Link services to service templates (and provide entity rule values for configurable service template entity rules).
• Add associated entities to services.

Do not attempt to import more than a 1,000 services with links to service templates. If you need to import more than 1,000 services and link them to service templates, do the imports in smaller batches. Only import 200-300 services with links to service templates at a time.

Use cases

The rows and columns that your CSV file contains, or the fields that your search contains, depend on your specific use case.

Import new services

Perform the following high-level steps before importing:

1. Create a CSV file or write a search that contains the services to import.
2. In the first row of a CSV, specify the column names.
3. In each subsequent row, specify one service, and, optionally, a service description and one or more service dependencies.

Note that the services created through this method are no populated with KPIs or entities.

Import new services and link them to service templates, or link existing services to service templates

When you link a service to a service template, the service receives the KPIs and entity rules from the template. Note that if a service already exists, ITSI replaces any entity rules in the service with the entity rules in the service template. For more information about service templates, see Create and manage service templates in ITSI.

1. Review the entity rules for the service templates you want to link services to and determine which entity rules have configurable values. You must provide those values for each service in the CSV or search. For information about entity rules, see Add entity rules to a service in ITSI.
2. Create a CSV file or write a search that contains the services to import and the corresponding template to link them to.
3. In the first row of a CSV, specify column names. In each subsequent row, specify one service, and, optionally, a service description, one or more service dependencies, and the name of the service template to link the service to.
4. Include one or more columns that provide values for the configurable entity rules in the service templates.

**Import services with associated entities**

Before importing, create a CSV file or write a search that contains the services and entities to import. ITSI creates an entity rule for the service with `Entity Title matches <value from Entity Title column>` for each entity. See Import ITSI entities from a CSV file for an example.

**Import services, link them to service templates, and import entities**

In the CSV file, include columns to use as values for any configurable entity rules in the templates. To import entities, use either a separate column or the same column that is used for configurable entity rules. In the latter case, entities are created for the column you import as `Entity Title`. However, instead of adding entity rules in the format `Entity Title matches <value from Entity Title column>` to the service, ITSI adds the entity rules from the linked template to the service. Any configurable entity rules use the column(s) you specify as the value for the configurable entity rules.

**Import from CSV**

You can create new services by importing the contents of a CSV file. The rows and columns that your CSV file contains depends on the use case. This section contains an example of importing services and linking them to service templates.

You can import a maximum of one service and one entity per row. There is no limit on the number of dependent services, entity aliases, entity information fields, or entity rule values per row. Import from CSV supports five different separators: comma (,), semicolon (;), pipe (|), tab (\t), and caret (^).

If a service has multiple dependent services, use multiple columns with different names. For example, `Dependent Service 1` and `Dependent Service 2`. Alternatively, you can include multiple rows containing the same service and separate dependencies. Likewise, multiple rows can contain the same service and separate entities to add to it.

**Prerequisites**

- You must be assigned the `itoa_admin` role or have the `write_itsi_service` capability to bulk import services.
• If you plan to link services to service templates, create the service templates first. You cannot create service templates through the bulk import process. For more information, see Create a service template in ITSI.

Steps

1. Create a CSV file that contains your services.
   In this example, we want to create eight services with various dependencies and link them to two different service templates. Three columns (applicationname, app_title, and host) provide entity rule values for the services.

<table>
<thead>
<tr>
<th>Service</th>
<th>Service Description</th>
<th>Dependent Service 1</th>
<th>Dependent Service 2</th>
<th>Template 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web A</td>
<td>This is Web A</td>
<td>App Service 3</td>
<td>App Service 1</td>
<td>Web Store</td>
</tr>
<tr>
<td>Web B</td>
<td>This is Web B</td>
<td>App Service 4</td>
<td>App Service 2</td>
<td>Web Store</td>
</tr>
<tr>
<td>Web C</td>
<td>This is Web C</td>
<td>App Service 1</td>
<td>App Service 5</td>
<td>Middleware</td>
</tr>
<tr>
<td>App Service 1</td>
<td>This is app 1</td>
<td></td>
<td></td>
<td>Middleware</td>
</tr>
<tr>
<td>App Service 2</td>
<td>This is app 2</td>
<td></td>
<td></td>
<td>Middleware</td>
</tr>
<tr>
<td>App Service 3</td>
<td>This is app 3</td>
<td></td>
<td></td>
<td>Middleware</td>
</tr>
<tr>
<td>App Service 4</td>
<td>This is app 4</td>
<td></td>
<td></td>
<td>Middleware</td>
</tr>
<tr>
<td>App Service 5</td>
<td>This is app 5</td>
<td></td>
<td></td>
<td>Middleware</td>
</tr>
</tbody>
</table>

   The following image shows what the final service dependency tree will look like:
2. After you create your CSV file, click **Configure > Services** from the ITSI top menu bar.
3. Click **New Service > Import from CSV**.
4. Click **browse...** and select your CSV file, or drop it into the UI.
   ITSI uploads the CSV file and displays a file preview.
5. Click **Next** to see a table populated by the content of your CSV file.
6. In the **Import Column As** column, choose how to categorize each column in your file.

<table>
<thead>
<tr>
<th>Column type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Title</td>
<td>Makes the column entry the name of the service.</td>
</tr>
<tr>
<td>Service Description</td>
<td>Makes the column entry a description of the service.</td>
</tr>
<tr>
<td>Dependent Services</td>
<td>Makes the column entry a dependent service.</td>
</tr>
<tr>
<td>Service Template Link</td>
<td>Makes the column entry the service template to link the service to. The service template must already exist in ITSI.</td>
</tr>
<tr>
<td>Do Not Import</td>
<td>Removes the column entry from the imported data. Use this setting for columns containing entity rule values if you are linking services to service templates. You will specify the column to use for entity rules later in the import process.</td>
</tr>
</tbody>
</table>

In this example, we are importing the columns in the CSV file as follows. Note that we are not importing the **applicationname**, **app_title**, and **host** columns. These columns contain entity rule values that are different for each service. You will use them later in the import process.
7. In the **Settings** section, configure the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Team</td>
<td>The team that the service belongs to.</td>
</tr>
<tr>
<td>Import Services As</td>
<td>Whether services are enabled or disabled upon import. KPI searches do not run if the service is disabled.</td>
</tr>
<tr>
<td>Enable 7 days of backfill for all service KPIs</td>
<td>This setting appears if you have selected to import columns as Service Title and Service Template Link. Enabling this setting backfills the KPIs in imported services that are linked to service templates. Enable this setting if you do not have at least seven days of data in the ITSI summary index and you want to use anomaly detection or adaptive thresholding for any of the KPIs in the service template.</td>
</tr>
</tbody>
</table>

8. See the Preview section to confirm that your service import configuration is correct.
9. Click **Next**.
10. Perform one of the following tasks:
    - If you selected to import a column as a Service Template Link, go to the Define Entity Rules step (Step 11).
    - If you are not linking services to service templates, skip to the Import step (Step 14).
11. In the Define Entity Rules step, select a service template to complete the template entity rules.
    For the templates that have configurable entity rules, the Entity Rules Complete column displays "Incomplete".

In this example, the Web Store template has four entity rules. One of them has a value defined in the template: `itsi_role matches operating_system_host`. Every service linked to this template receives this field/value pair. The other three entity rules have values in the service template of matches a value to be defined in the service. Therefore, you must provide the value for each service in this step using a column from the CSV file.

12. Click **Select a column** to provide the entity rule value for each configurable entity rule in the template as shown in the following example:
In this example, the Web A service receives *Web* for the applicationname value, New_Relic_Buttercup_Web:8675309 for the app_title value and webserver* for the host value.

13. Preview the entities for each service linked to the template. Note that ITSI can only match existing entities. Any entities being imported do not appear in the preview.

14. Click Import. A message confirms that the import is complete.

15. Click View All Services to confirm that your imported services appear on the Service page. If you linked services to templates, the Service Template column indicates that it's synced with the service template. The template populates the KPIs and entity rules for the services. Any configurable entity rules that came from the template contain the value from the column you specified during the import process.

16. (Optional) Click Set up Recurring Import to create a modular input for the CSV file.

**Import from search**

You can import multiple services from ITSI module searches, saved searches, and ad hoc searches. The Import from Search workflow is identical to the import from CSV workflow, except that you specify a search string instead of uploading a CSV file.

The example in this section shows you how to import services and entities and associate the entities with the services. For an example of importing services and linking them to service templates, see the Import from CSV section.

**Prerequisites**

- You must be assigned the itoa_admin role to bulk import services.
- If you are linking services to service templates, create the service templates first. You cannot create service templates through the bulk import process. They must already exist in ITSI. For more information, see Create service templates in ITSI.
Steps

1. Click **Configure > Services** from the ITSI top menu bar.
2. Click **New Service > Import from search**.
3. Select one of the following search types:

<table>
<thead>
<tr>
<th>Search Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modules</td>
<td>Choose from a list of pre-defined entity discovery searches based on ITSI modules.</td>
</tr>
<tr>
<td>Saved Search</td>
<td>Choose from a list of pre-defined ITSI saved searches.</td>
</tr>
<tr>
<td>Ad hoc Search</td>
<td>Enter a custom search string.</td>
</tr>
</tbody>
</table>

4. Enter an ad hoc search string or select a predefined module search or saved search. Make sure the results are presented in a table. For this example we are using an ad hoc search to import services and entities.

5. Click the Search icon.

The specified search runs and a Search Results Preview appears. We want to create two services called Splunk Search Head Service and Splunk Indexer Service (using the service_title column) and create three entities for the hosts listed in the host column and add these entities to the services.

6. Click **Next**.

The Select Columns page appears, showing a table populated by your search results. Use this page to specify how to classify and store the file column entries that define your entities.

7. For our example, we are importing the columns in our search results as follows.
8. In the **Settings** section, configure the following items:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Team</td>
<td>The team that the service belongs to. Entities are always created in the Global team.</td>
</tr>
<tr>
<td>Import Services As</td>
<td>Whether services are enabled or disabled upon upgrade.</td>
</tr>
<tr>
<td>Conflict Resolution</td>
<td>Determines how ITSI updates and stores your entity data:</td>
</tr>
<tr>
<td></td>
<td>- <strong>Skip Over Existing Entities</strong>: Adds new entity data to the datastore only if the entity does not already exist. If an entity exists, the information is not updated.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Update Existing Entities</strong>: Merges the imported data and the existing data associated with the entity.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Replace Existing Entities</strong>: Replaces existing entity data with new entity data.</td>
</tr>
<tr>
<td>Conflict Resolution Field</td>
<td>The field used to identify entities. Entities that have the same field value are considered the same entity. If Conflict Resolution is set to <strong>Update Existing Entities</strong> or <strong>Replace Existing Entities</strong>, ITSI resolves duplicate entities based on this field.</td>
</tr>
</tbody>
</table>

For more information about Conflict Resolution, see [Conflict Resolution examples in ITSI](#).

9. In the **Preview** section, click **Services to be imported** to confirm that your service import configuration is correct.

10. Click **Import**. A message confirms that the import is complete.

11. Click **View All Services** or **View all Entities** to confirm that your imported services and entities now appear on the respective Service or Entity page.

12. (Optional) Click **Set up Recurring Import** to create a modular input that runs import search on a recurring basis.

---

**Overview of configuring services in ITSI**

This topic provides an overview of how to configure services in IT Service...
Intelligence (ITSI). For more information about ITSI services, see Overview of services in ITSI.

**Prerequisite**

You must have the `write_itsi_service` capability to configure services. The `itoa_admin` and `itoa_team_admin` roles have this capability by default.

**Option 1: Configure a service manually**

The following diagram shows the steps to manually configure an ITSI service:

![Diagram showing the steps to manually configure an ITSI service]

The following table describes the steps to manually configure a service:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Required/Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new service</td>
<td>Either create a single service, import services from a CSV file, or import</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>them from a Splunk search.</td>
<td></td>
</tr>
<tr>
<td>Add entity rules</td>
<td>Entity rules let you dynamically filter KPI searches based on entity alias</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>matches.</td>
<td></td>
</tr>
<tr>
<td>Add KPIs</td>
<td>A Key Performance Indicator (KPI) is a recurring saved search that returns</td>
<td>Required</td>
</tr>
<tr>
<td></td>
<td>the value of an IT performance metric, such as CPU load percentage, memory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>used percentage, response time, and so on.</td>
<td></td>
</tr>
<tr>
<td>Add service dependencies</td>
<td>Adding service dependencies can help you detect if one service is having a</td>
<td>Optional</td>
</tr>
<tr>
<td></td>
<td>negative impact on another service, and can be useful in performing root</td>
<td></td>
</tr>
<tr>
<td></td>
<td>cause analysis.</td>
<td></td>
</tr>
</tbody>
</table>
Option 2: Configure a service created from a service template

If you created a service from a service template, the entity rules and KPIs are populated for you. You still need to configure service dependencies. For more information, see Configure a service created from a service template in ITSI.

Option 3: Configure a service created from pre-built KPIs

If you created a service using pre-built KPIs from modules, the entity rules and KPIs are populated for you. For more information, see Define a source search from a base search and About ITSI modules.

Add entity rules to a service in ITSI

Entity rules let you dynamically filter KPI searches based on entity alias matches. You can use entity rules to associate entities with KPIs at the service level, which makes it unnecessary to specify entity identifying fields for each KPI search.

When to add entity rules

Entity rules are optional and you can add them at any time. Add entity rules if you want to be able to filter a KPI by the entities in the service. There are many scenarios where entity rules can make it easier to configure your services, including the following:

- You want to match entity ID data not recognized inside Splunk Enterprise (such as mapping a naming scheme to specific devices). For example, your organization might use a server naming convention such as server-01, server-02, and so on. These names do not appear as fields inside Splunk searches. Adding rules that match your entity aliases to your server naming scheme lets you apply KPI searches to those servers.
- You want to disambiguate between multiple fields that identify the same machine (such as a host with multiple IP addresses).

How to set up entity rules

You can set up entity rules to match entities based on entity aliases, info, or entity title. You can also create rules based on multiple AND/OR conditions.

For example, if you want to add entity rules that identify your database servers, and those servers have aliases of host=mysql-01, host=mysql-02, host=mysql-03
and so on, you can add an entity rule such as "host matches mysql*" to identify the servers on which to run the KPI search.

This entity rule matches the host field in Splunk data with your mysql* servers and adds each server to all KPI searches in the service.

Entity rule values can be left blank. For example you could specify "web_server does not match" and leave the value field empty to include all values for the web_server field.

**Filter entities out of a service**

Use the "does not match" entity rule to filter entities out of a service rather than in. For example, if you want to filter out your database servers, you could add a rule such as "host does not match mysql*" so the KPI search does not run on those servers.

It is important to note that the "does not match" entity rule always acts as if it has a wildcard (*) at the end of the string you specify, filtering out all possibilities that start with the value rather than just that value.

For example, you have two entities, one with info field location = Z and another with location = ZZZ. If you create an entity rule: location does not match Z, no entities will match the service. Z acts as if it has a wildcard at the end of it, filtering out any info fields that begin with the letter "Z".

This is the default behavior. To work around this behavior, create an OR condition in the entity rules such that the logic works. For example,

**Rule 1:** location does not match A, B, C, ..., Z

OR

**Rule 2:** location matches ZZZ
Add service dependencies in ITSI

After you configure a service, you can add other services as impacting services, or service dependencies. Impacting services have some sort of effect or influence on the primary service. Adding service dependencies can help you detect if one service is having a negative impact on another service, and can be useful in performing root cause analysis.

For example, you might have a web service that has a dependency on a database service. By adding the database service as a dependency, you can monitor the impact that the database service is having on the web service.

When you add a service dependency, you select the specific KPIs from the impacting service that you want ITSI to include in the health score calculation of the primary service.

Avoid creating cyclic service dependencies. A cyclic dependency is a relationship between two or more services which either directly or indirectly depend on each other. Cyclic dependencies can result in infinite loops or other unexpected results. A dotted line between services in the Service Analyzer tree view indicates a cyclic dependency.

1. Click the Service Dependencies tab in the service definition.
2. Click Add Dependencies.
3. Select the service(s) that you want to add as a dependency. You can choose services within the same team as the primary service or from the Global team.
4. Select the specific impacting KPIs that you want to monitor as part of the primary service's health score.
5. Click **Done**.
6. Click **Save** to save the dependency into the service definition.

ITSI adds the selected KPIs to the list of service dependencies, and includes the selected KPIs in the primary service health score calculation.

**Set importance values for service dependencies**

ITSI lets you adjust the importance value of impacting service KPIs on the Settings tab of the service as described in Set KPI importance values in ITSI. Configure the importance value to give impacting KPIs appropriate weights in health score calculations and to generate health score values that more accurately reflect the impact of the dependency on the primary service.

By default, impacting service health scores have an importance value of 11. Regular KPIs have the same importance value that is set for the KPI in the original service.

When an impacting KPI with an importance value of 11 reaches critical, the health score of the primary service will read Critical with a value of 0, regardless of the status of other KPIs.

**Enable or disable a service**

A service must be enabled in order for the KPI searches associated with that service to run. You can enable a service when you first create it, or at a later time from the **Settings** tab of the service definition or the Services lister page.

Disable a service to stop KPI searches at any time. Disabling a service is useful if you are still configuring a service and want to avoid generating inaccurate health scores and false positives. It is also useful for reducing search load for performance purposes.

When you disable a child service, it has no impact on the health of an enabled parent service.

1. Click **Configure > Services**.
2. In the Status column of the service, toggle **Enabled** or **Disabled**.

If you disable a service that has KPI backfill enabled, the backfill will continue and those KPIs will have data for the backfill period.
**Change the team a service belongs to**

You can change the team a service belongs to from the Settings tab in the service definition. In order to move a service from one team to another, you must have write permissions for both teams.

Changing the team a service belongs to might break service dependencies. Check to see if the service has a dependency on another service and note the team that the dependent service belongs to before moving the service to another team.

If a service is dependent on a service in the Global team, the service dependency is not broken. However, if a service is dependent on another service within the same team, and you move one of the services to another team, that dependency breaks. Services in private teams cannot have a dependency on a service in another private team.

To bulk move services to a different team, select the checkboxes on the Services lister page, then click **Bulk Action > Edit Team**.

**Backfill service health scores in ITSI**

Backfill service health scores to fill the summary index, `itsi_summary`, with calculated historical service health scores. Backfill uses past KPI data, including dependent KPIs, to calculate service health scores for a given time period and populate the summary index. In other words, even though the summary index only started collecting service health score data at the start of this week when the service was created, if necessary you can use the backfill option to fill the summary index with data from the past month.

You can’t backfill health scores for multiple services in bulk. You must backfill each service individually.

**Prerequisites**

- You must have the `itoa_admin` or `itoa_team_admin` role, or write access to the service, in order to backfill service health scores.
- To ensure that the health score is backfilled correctly, make sure that all KPIs within the service and all dependent KPIs are already backfilled (or have indexed raw data) for at least the amount of time you plan to backfill the service health score.
Steps

1. Click **Configure > Services**.
2. Open the service whose health score you want to backfill.
3. Click the **Settings** tab.
4. Under Service Health Score, toggle **Backfill**.
5. Use the dropdown to select the number of days of data to backfill. You can choose a predefined time range, like **last 7 days**, or select a custom date prior to the current date. If you choose a specific date, the dropdown dynamically updates with the number of days you’re backfilling to.
6. Click **Save** to begin the backfill process. A message appears when backfill is completed.

The backfill period is the time range of data that’s available after backfill is complete. For example, if you select **last 60 days**, ITSI fills the summary index with data from the past 60 days. You now have 60 days of service health score data available.

See also

- Add a KPI to a service in ITSI (see the "Enable Backfill" section for instructions on backfilling KPI data)
- How service health scores work in ITSI

Clone a service in ITSI

When you clone a service in ITSI, all entities, KPIs, and settings from the original service are cloned into the new service. Cloning a service does not clone summary index content of KPIs within the service. If the original service is linked to a service template, the cloned service is linked to the same service template. Service dependencies and Predictive Analytics models are not copied to the cloned service.

Prerequisite

You must have the write_itsi_service capability to clone a service in ITSI.

Steps

1. From the ITSI top menu bar, click **Configure > Services**.
2. In the Actions column of the service you want to clone, click **Edit > Clone**.
3. Provide a title that is different than the title of the original service (for example, Database 2). Two services cannot have the same title.
4. Select the team that the cloned service will belong to.
5. Click **Clone**.

---

**How service health scores work in ITSI**

ITSI generates a health score for each service that you create. The health score is a good indicator of the status of a service and is a useful metric to display in Service Analyzer, glass tables, and deep dives. A decline in service health score can be the first sign of an issue that might lead to an outage. ITSI continuously monitors and updates service health scores.

**Service health score calculations**

Service health scores range from 0 to 100, with 0 being most critical and 100 being most healthy. The health score calculation is based on the current severity level of service KPIs (Critical, High, Medium, Low, and Normal) and the weighted average of the importance values of all KPIs in a service. For more information, see Set KPI importance values in ITSI.

The **Info** severity level is not included in the service health score calculation.

ITSI does not directly use KPIs or health scores of dependent services to calculate a service’s health score. Service health scores are calculated based on the **score_contribution** value for each severity level. Score contribution values are defined in threshold_labels.conf. Do not modify these values.

For example, a service contains 2 KPIs. One KPI is Critical, so the **score_contribution** value is 0. The other KPI is Normal, so the **score_contribution** value is 100. Assuming both KPIs have the same importance values, the service health score will be 50.

The following formula is used to calculate service health scores:

\[
\text{Service Health Score} = \frac{\sum_{i=1}^{N} K_i \cdot \frac{G_i}{G_{\text{Total}}}}{N}
\]

Where:

- **N** = count of KPIs
- **G** = importance value of one KPI
- **K** = the score contribution of the KPI (Normal=100, Low=70,
For example, if you set KPI importance values as follows:

<table>
<thead>
<tr>
<th>KPI Title</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>KPI1</td>
<td></td>
</tr>
<tr>
<td>KPI2</td>
<td></td>
</tr>
<tr>
<td>KPI3</td>
<td></td>
</tr>
</tbody>
</table>

The service health score is calculated as follows:

Service health score = (100 \cdot 10/22) + (70 \cdot 7/22) + (30 \cdot 5/22) = 45.45 + 22.27 + 6.81 = \mathbf{74.53}

**Impact of per-entity thresholds on service health scores**

When a KPI is split by entity, if any entity has a severity level, based on entity thresholds, that is worse than the service aggregate severity, the service health score is impacted. In some cases, this can cause the overall service health score to change significantly, while the aggregate KPI severity level changes only marginally or not at all.

For example, if you have a CPU % utilization KPI that is running against three entities, and 2 of those entities show normal severity, while the third shows critical, the overall service health score might show critical, while the aggregate KPI severity level remains normal.

For more information about per-entity thresholds, see Set per-entity threshold values in the KPI configuration workflow.

**Impact of service dependencies on service health scores**

Any service dependencies that you add to a service will impact the service health score, based on the importance value that you set for dependent service KPIs. For more information, see Set importance values for service dependencies in this
manual.
KPIs

Overview of configuring KPIs in ITSI

A KPI (Key Performance Indicator) is a recurring saved search that returns the value of an IT performance metric, such as CPU load percentage, memory used percentage, response time, and so on.

ITSI lets you create KPIs and add them to your services. You can then use KPI search result values inside ITSI to monitor service health, check the status of IT components, and troubleshoot trends that might indicate an issue with your IT systems.

For example, `cpu_load_percent` is a KPI that measures the CPU load percentage on a server. If your organization has a site uptime guarantee of 99.9% per month, you will need to monitor the status of this KPI (and others) to ensure that CPU performance remains within acceptable parameters.

When you initially create a KPI search, you configure the following set of search properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source search</td>
<td>A search string that you define as the basis for your KPI, using a <strong>data model</strong>, <strong>ad hoc search</strong>, <strong>metrics</strong> search, or <strong>base search</strong>.</td>
<td>Yes</td>
</tr>
<tr>
<td>Entity Split Field</td>
<td>A field in your data that can be used to break down the KPI. This option lets you apply a KPI search to multiple entities, enabling comparative analysis of search results on a per-entity basis. This field can be different from the Entity Filter Field.</td>
<td>Optional</td>
</tr>
</tbody>
</table>

45
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Required?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity Filter Field</td>
<td>Filter entities in or out of a KPI search.</td>
<td></td>
</tr>
<tr>
<td>Monitoring calculations</td>
<td>The recurring KPI search schedule and statistical operations on search results, including service health score calculations.</td>
<td>Yes</td>
</tr>
<tr>
<td>Backfill</td>
<td>Fills the summary index (itsi_summary) with historical raw service health score data.</td>
<td>Optional</td>
</tr>
<tr>
<td>Severity-level thresholds</td>
<td>Thresholds that you apply to KPI search results. Severity-level thresholds let you monitor KPI status (normal, low, medium, high, and critical) and set trigger conditions for alerts.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

For example, to monitor the CPU load percentage of an entity (machine) in a service, you can create a KPI using an ad hoc base search that returns the value of the field `cpu_load_percent` at 5 minute intervals over a 5 minute time range, then set a range of severity-level thresholds between 0% and 100%.

For a step-by-step guide to adding a KPI to a service, see Add a KPI to a service in ITSI. After you add a KPI to a service, you can perform other configuration tasks, like setting KPI importance values and applying anomaly detection.

**See also**

- Set KPI importance values in ITSI
- Create KPI threshold time policies in ITSI
- Detect anomalous KPI behavior in ITSI

**Add a KPI to a service in ITSI**

A Key Performance Indicator (KPI) is a recurring saved search that returns the value of an IT performance metric, such as CPU load percentage, memory used...
percentage, response time, and so on. Use KPI searches to monitor the performance of your IT services. You must add at least one KPI search to a service to use ITSI. For information on how the number of KPIs can impact performance, see Performance considerations in the ITSI Installation and Upgrade manual.

This topic walks you through the basic KPI search creation modal. These instructions assume that you have already created a service. If not, see Overview of creating services in ITSI in this manual. You must create a service with at least one KPI to run ITSI.

**Prerequisites**

- You must create a service before you can add KPIs to it. For instructions, see Overview of creating services in ITSI.
- To design a KPI search, you need to know the following information:
  - The source search expression, including selection criteria.
  - The specific field in the data that you want to monitor.
  - The time span and frequency for the KPI to update.
  - How to summarize the data over the time span (count, last, sum, average, and so on).
  - Whether you want to split the KPI result values by entities (for example, by host).

**Step 1: Add a new KPI**

1. Click **Configure > Services** from the ITSI top menu bar.
2. Select an existing service.
3. Click **New** in the KPI tab and choose one of the following options:
   - Select **Generic KPI**.
   - Select a KPI template. For example, **Application Server: CPU and Memory > Memory Used**. KPI templates provide pre-configured KPI source searches, including ad hoc searches and base searches, based on ITSI modules. KPI templates are tailored for specific service monitoring use cases, such as operating systems, databases, web servers, load balancers, virtual machines, and so on.
4. In Step 1 of the KPI creation modal, enter the KPI title and optional description. Click **Next**.
Step 2: Define a source search

When you create a KPI, you must define a source search on which to build the KPI. You can choose from four source search types: data model search, metrics search, ad hoc search, and base search.

**Note:** Before you define your source search, consider the performance implications for your particular deployment. While data models are suitable for smaller test environments, base searches generally provide best performance in larger production settings. See Create KPI base searches in ITSI.

**Define a source search from a data model**

1. Configure your data model search.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KPI Source</td>
<td>Data Model</td>
</tr>
<tr>
<td>Data Model</td>
<td>The data model object, child, and attribute fields. For example, Host Operating System &gt; Memory &gt; mem_used_percent.</td>
</tr>
<tr>
<td>Filters (optional)</td>
<td>Click <strong>Add Filter</strong> to add data model filter conditions. Data model filters let you include/exclude search result data based on the filter conditions. For example, the filter condition host Equals ipaddress filters out all values for the data model search field host, except for values that equal ipaddress. Data model filtering can help improve the speed and accuracy of your searches by excluding extraneous data from search results.</td>
</tr>
</tbody>
</table>

2. Click **Generated Search** to preview your KPI search string.

Use the Generated Search box to view changes that ITSI makes to your search string as you build your KPI. Click anywhere on the Generated Search itself to run the search.
3. Click **Next**.

**Define a source search from a metrics search**

1. Configure your metrics search.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KPI Source</td>
<td>Metrics Search</td>
</tr>
<tr>
<td></td>
<td>If there are no metrics indexes configured in your Splunk deployment, you'll see the message &quot;No metrics found&quot;. For more information about metrics, see Get started with Metrics in the Splunk Enterprise Metrics Manual.</td>
</tr>
<tr>
<td>Metrics Index</td>
<td>Select the metrics index from which to choose a metric. The list only populates with indexes defined locally on the search head you are accessing. To use an index defined only on an indexer, enter it manually.</td>
</tr>
<tr>
<td>Metric Name</td>
<td>Select the metric to use for the KPI. For example, memory.used.</td>
</tr>
</tbody>
</table>

2. Click **Generated Search** to preview your KPI search string. Metrics searches begin with the **mstats** command.

3. Click **Next**.

**Define a source search from an ad hoc search**

1. Configure your ad hoc search.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KPI Source</td>
<td>Ad hoc Search</td>
</tr>
<tr>
<td>Search</td>
<td>The ad hoc search string that you create. This is the event gathering search for the KPI.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The use of transforming commands, the <strong>mstats</strong> command, the <code>gettime</code> macro, or time modifiers in your KPI search is not recommended as this may cause issues with KPI backfill, the display of raw data on ITSI views such as glass tables and deep dives that allow you to run KPI searches against raw data, and the KPI threshold preview.</td>
</tr>
<tr>
<td>Threshold Field</td>
<td>The field in your data that the KPI aggregates and monitors. For pure counts use _time.</td>
</tr>
</tbody>
</table>

2. Click **Generated Search** to preview your KPI search string.
Define a source search from a base search

1. Configure your base search.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>KPI Source</strong></td>
<td>Base Search</td>
</tr>
<tr>
<td>Base Search</td>
<td>The base search that you want to associate with the KPI. For example, DA-ITSI-OS:Performance.Memory. Base searches provide preconfigured KPI templates built on ITSI modules.</td>
</tr>
<tr>
<td>Metric</td>
<td>The metric that you want to associate with the KPI. For example, mem_free_percent.</td>
</tr>
</tbody>
</table>

2. *(Optional)* click **Generated Search** to preview your KPI search string.

3. Click **Next**.

**Note:** Most fields in the next window (steps 3 through 6) are pre-populated for the base search by the KPI template. For more information on how to create and configure KPI base searches, see Create KPI base searches.

**Step 3: Filter entities**

Filter entities to have more granular control of your KPI at the entity level.

**Split by Entity**

The Split by Entity option lets you maintain a breakdown of KPI values at the entity level. Split KPI results by a specific entity to monitor each individual entity against which a KPI is running.

You must split KPIs by entity to use the following ITSI features:

- Per-entity thresholds. See Set per entity threshold values in this manual.
- Entity overlays. See Add overlays to a deep dive in ITSI in the ITSI User Manual.
- Maximum severity view in the Service Analyzer. See Aggregate versus maximum severity KPI values in ITSI in the ITSI User Manual.
- Cohesive anomaly detection. See Apply anomaly detection to a KPI in ITSI in this manual.

Configure the following fields:
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Split by Entity</td>
<td>Enable a breakdown of KPI values at the entity level. The KPI must be running against two or more entities.</td>
</tr>
<tr>
<td>Entity Split Field</td>
<td>The field in your data to use to look up the corresponding split by entities. The default lookup field for data model searches and ad hoc searches is <code>host</code>. For metrics searches, select a dimension associated with the metric. This field is case sensitive.</td>
</tr>
<tr>
<td></td>
<td>When filtering a KPI down to entities, you can split by a field other than the field you are using for filtering the entities (specified in the Entity Filter Field). This allows you to filter to the hosts that affect your service, but split out your data by a different field. For example, you might want to filter down to all of your database hosts but split the metric by the processes running on the hosts.</td>
</tr>
</tbody>
</table>

**Entity filtering**

Entity filtering lets you specify the entities against which a KPI search will run. Provide an entity filter field to reduce collection of extraneous data.

For example, if you enable entity filtering for a KPI in the Online Sales service, only entities assigned to that service are used to calculate the KPI search metrics.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter to Entities in Service</td>
<td>Enable/disable entity filtering.</td>
</tr>
<tr>
<td>Entity Filter Field</td>
<td>Specify the field in your data to use to look up the corresponding entities by which to filter the KPI. For metrics searches, select a dimension for the metric. The default field for data model searches, ad hoc searches, and metrics searches is <code>host</code>. This field can be different than the field used for the Entity Split Field.</td>
</tr>
</tbody>
</table>

With the removal of entity alias filtering in version 4.2.x, only the Entity Filter Field determines the entity aliases to use for filtering. ITSI now strictly matches entities against KPI search results using both the alias key and value, whereas before it only used the alias value. The strict entity alias matching also occurs when generating notable events through correlation searches. The entity lookup field must be an actual entity alias field for the match to occur. For more information, see Removed features in Splunk IT Service Intelligence in the ITSI *Release Notes.*
**Step 4: Add monitoring calculations**

Configure the following KPI monitoring calculations:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KPI Search Schedule</td>
<td>Determines the frequency of the KPI search. Avoid scheduling searches at one minute intervals. Running multiple concurrent KPI searches at short intervals can produce lengthy search queues and is not necessary to monitor most KPIs.</td>
</tr>
<tr>
<td>Entity Calculation</td>
<td>The method for calculating aggregate search results on the entity level. Each entity has its own alert value based on this calculation type. For example, Average or Maximum. These entity values are then aggregated to create the overall value, which is the value displayed for the KPI. This setting is only applicable if Split by Entity is set to Yes.</td>
</tr>
<tr>
<td>Service/Aggregate Calculation</td>
<td>The statistical operation that ITSI performs on KPI search results. The correct aggregate calculation to use depends on the type of KPI search. For example, if your search returns results for CPU Load percentage, use Average. If you want a total count of all errors from individual entities, use Sum.</td>
</tr>
<tr>
<td>Calculation Window</td>
<td>The time period over which the calculation applies. For example, Last 5 Minutes.</td>
</tr>
<tr>
<td>Fill Data Gaps with</td>
<td>How to treat gaps in your data. This setting affects how aggregate KPI data gaps are displayed in service analyzers, deep dive KPI lanes, glass table KPI widgets, and other dashboards in ITSI populated by the summary index.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Null values</strong> to fill gaps in data with N/A values. Also select the severity level to use for Null values.</td>
</tr>
<tr>
<td></td>
<td>• Select <strong>Last available value</strong> to use the last reported value in the ITSI summary index. Aggregate KPI data gaps are filled with the last reported aggregate</td>
</tr>
</tbody>
</table>
KPI value. Entity-level data gaps are filled with the corresponding entity’s last available value.

- Select Custom value to specify a specific value to use when there is a gap in data. Enter a positive integer.

Filled gap values are not used in the calculations performed for Anomaly Detection and Adaptive Thresholding.

Click Next.

**Change the stateful KPIs caching period**

Each time the saved search runs for a KPI with Fill Data Gaps with set to Last available value, ITSI caches the alert value for the KPI in the itsi_kpi_summary_cache KV store collection. ITSI uses a lookup named itsi_kpi_alert_value_cache in the KPI saved search to fill entity-level and service-aggregate gaps for the KPI using the cached alert value.

To prevent bloating of the collection with entity and service-aggregate KPI results, a retention policy runs on the itsi_kpi_summary_cache collection using a Splunk modular input. The modular input runs every 15 minutes and removes the entries from cache that have not been updated for more than 30 minutes.

You can change the stateful KPI caching frequency or retention time.

**Prerequisites**

- Only users with file system access, such as system administrators, can change the stateful KPI caching frequency and retention time.
- Review the steps in How to edit a configuration file in the Admin Manual.

Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location.

**Steps**

1. Open or create a local inputs.conf file for the ITSI app at $SPLUNK_HOME/etc/apps/SA-ITOA/local.
2. Under the
   ```
   [itsi_age_kpi_alert_value_cache://age_kpi_alert_value_cache]
   ```
stanza, adjust the `interval` and `retentionTimeInSec` settings.

Filling data gaps with the last reported value occurs for at most 45 minutes, in accordance with the default modular input interval and retention time (15 minutes + 30 minutes). If data gaps for a KPI continue to occur for more than 30 to 45 minutes, the data gaps appear as N/A values.

**Step 5: Unit and Monitoring Lag**

Configure the following optional settings:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unit</strong></td>
<td>The unit of measurement that you want to appear in KPI visualizations. For example, GB, Mbps, secs, and so on.</td>
</tr>
<tr>
<td><strong>Monitoring lag</strong></td>
<td>The monitoring lag time (in seconds) to offset the indexing lag. Monitoring lag is an estimate of the number of seconds it takes for new events to move from the source to the index. When indexing large quantities of data, an indexing lag can occur, which can cause performance issues. Delay the search time window to ensure that events are actually in the index before running the search. In most cases, don’t set this value below 30.</td>
</tr>
</tbody>
</table>

**Step 6: Enable backfill**

Enable backfill to fill the summary index (itsi_summary) with historical raw KPI data. Backfill runs a search in the background that populates the summary index with historical KPI data for a given time range (backfill period) as it would have been populated at a regularly scheduled time by KPI saved searches. In other words, even though the summary index only started collecting data at the start of this week when the KPI was created, if necessary you can use the backfill option to fill the summary index with data from the past month.
Backfill is a one-time operation. Once started, it cannot be redone or undone. For example, if you backfill 60 days of data and then later decide that you want 120 days, you cannot go back and change the backfill period. Think carefully about how many days of data you want to backfill before saving the service.

The backfill option requires you to have indexed adequate raw data for the backfill period you select.

When you enable backfill, you must indicate how many days of data to backfill. You can choose a predefined time range like last 7 days, or select a custom date prior to the current date. If you choose a specific date, the dropdown dynamically updates with the number of days you're backfilling to.

The backfill period is the time range of data that is available after backfill is complete. For example, if you select last 30 days, ITSI fills the summary index with data from the past 30 days. In other words, you now have 30 days of KPI data available.

If you backfill a KPI that uses Last available value to fill data gaps, data gaps are backfilled with filled-in alert values (using the last reported value for the KPI) instead of N/A alert values. If you backfill a KPI that uses a Custom value to fill data gaps, data gaps are backfilled with filled-in alert values (using the custom value provided) instead of N/A alert values. See Step 4: Add monitoring calculations.

You must save the service to initiate the backfill. A message appears in Splunk Web that informs you when the backfill is complete.

ITSI supports a maximum of 60 days of data in the summary index. Therefore, after you configure backfill, you will see one of the following messages:

- "Backfill is not available" - More than 60 days of summary index data already exists.
- "Backfill has been configured for last <#> days of data" - The backfill job is configured but hasn't run yet. This might be because the service has not been saved yet.
- "Backfill completed for last <#> days" - Backfill has completed successfully. This message only shows up until a total of 60 days of data is in the summary index, then it changes to "Backfill is not available".
Step 7: Set thresholds

Severity-level thresholds determine the current status of your KPI. When KPI values meet threshold conditions, the KPI status changes, for example, from high (yellow) to critical (red). The current status of the KPI is reflected in all views across the product, including service analyzers, glass tables, and deep dives.

Manually configure threshold values for your KPIs using the threshold preview window. Alternatively, you can apply threshold time policies, which automatically adapt threshold values based on day and time. See Create KPI threshold time policies in ITSI.

ITSI supports two types of KPI severity-level thresholds: Aggregate thresholds and per-entity thresholds. You can configure adaptive thresholds for aggregate thresholds but not per-entity thresholds.

After you configure KPI thresholds, you can configure alerting on a single KPI so you can be alerted when aggregate KPI threshold values change. ITSI generates notable events in Episode Review based on the alerting rules you configure. For information, see Receive alerts when KPI severity changes in ITSI.

Set aggregate threshold values

Aggregate thresholds are useful for monitoring the status of aggregated KPI values. For example, you might apply aggregate thresholds to monitor the status of KPIs that return the total number of service requests or service errors, based on a calculation that uses the stats count function.

1. Click Aggregate Thresholds.
2. Click Add threshold to add a range of severity-level thresholds to the threshold preview graph.
3. Click **Finish**.

**Set per-entity threshold values**

Per-entity thresholds are useful for monitoring multiple separate entities against which a single KPI is running. For example, you might have a KPI, such as Free Memory %, that is running against three separate servers. Using per-entity thresholds, you can monitor the status of Free Memory % on each individual server.

You can't use adaptive thresholding on a per-entity basis.

**Prerequisites**

To use per-entity thresholds, a KPI must be split by entity. See "Step 3: Filter entities" above.

**Steps**

1. Click **Per-Entity Thresholds**.
2. Click **Add threshold** to add a range of severity-level thresholds to the threshold preview graph.
   The threshold preview shows separate search results for each entity the KPI is running against.

3. Click **Finish**.

**Set KPI importance values in ITSI**

After you create your KPI, you must assign the KPI an importance value. ITSI uses the importance value, along with the KPI severity level, to calculate a service health score.
Importance values range from 0 to 11. KPI importance values from 1-11 are included in the health score calculation, with 1 being the least important and 11 being the most important. KPIs with an importance value of 0 are not included in the health score calculation. The greater the KPI importance value, the greater the impact that KPI has on the service health score.

ITSI considers KPIs that have an importance value of 11 as a special case that represents a "minimum health indicator" for the service. When a KPI with an importance value of 11 reaches the critical state, the overall health score for the service turns critical, regardless of the status of other KPIs in the service.

For more information about how KPI importance values affect service health scores, see How service health scores work in ITSI.

**Prerequisite**

Before you set KPI importance values, you must add the KPI to one of your services. For more information, see Add a KPI to a service in ITSI.

**Steps**

1. Open the service that contains your KPI.
2. Click the **Settings** tab. The Health Score Calculation section shows the importance value of each KPI, along with the simulated health score of the service.
3. Use the slider to set the importance value for your new KPI.
Notice the impact that different severity levels have on the simulated health score given the KPI importance value. Use this feature to help fine-tune your KPI importance values. The simulated health score is for preview purposes only and has no impact on actual severity-level thresholds or service health scores.

Create KPI threshold time policies in ITSI

KPI threshold time policies have threshold values that change over time. Use time policies to accommodate normal variations in usage across your services and improve the accuracy of KPI and service health scores. For example, if your organization's peak activity is during the standard work week, you might create a KPI threshold time policy that accounts for higher levels of usage during work hours, and lower levels of usage during off-hours and weekends.

ITSI stores thresholding information at the KPI level in the KV store. Any updates you make to a KPI threshold template are applied to all KPIs using that template, overriding any changes made to those KPIs.

You can only have one active time policy at any given time. When you create a new time policy, the previous time policy is overwritten and cannot be recovered.

Available KPI threshold templates

ITSI provides a set of 32 default thresholding templates that you can use to build your time policies. You can select templates with different time block combinations, such as work hours, off hours, weekends, AM/PM, 3 hour block, 2 hour block, and so on.

Thresholding templates are either static or adaptive. Use static templates to create time policies that do not change after you configure them. Use adaptive templates to create time policies that generate thresholds dynamically and update daily based on changes in your data. You can use adaptive thresholds with aggregate thresholds but not per-entity thresholds.

The following template types are available:

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantile</td>
<td>Lets you put threshold bounds at various percentiles based on historic data. For example, you might choose to set critical severity</td>
</tr>
<tr>
<td>Algorithm</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Standard deviation</td>
<td>for data points falling below the 1st percentile (0.01) and above the 99th percentile (0.99). Because you must choose percentile threshold values between 0 and 1, this is the only algorithm that will never produce thresholds above or below your historical data minimum and maximum values. Therefore, you are likely to see your threshold bounds crossed repeatedly. This could influence your alerting strategy.</td>
</tr>
</tbody>
</table>
| Range           | Lets you specify thresholds based on multiples of the standard deviation from the mean. Negative values produce thresholds below the mean and positive values produce thresholds above the mean. Standard deviation is most useful for cyclical data, which might include customer traffic volumes. For example, customer traffic increases at 8:00, peaks at 1:00, starts to drop at 5:00, and goes very low in the middle of the night.  
This algorithm is sensitive to outliers in historic data which may cause much larger threshold values than you desire or expect. Additionally, if your data is skewed (larger values and outliers present, but smaller values and outliers not present, such as what you might see with a response time KPI) you might struggle to generate meaningful lower bound thresholds. If your data is well distributed around a mean, this algorithm could be a good choice for you. Moreover, even if your data is skewed, standard deviation is a good choice if you only care about meaningful thresholds in the direction of the skew. |
| Range           | Focuses on the minimum and maximum data points from your historic data and the span between those values (max - min). Your thresholds then become a multiplier of the span added to the minimum. A value of 0 will set a threshold to the historic data minimum, a value of 1 will set a threshold to the historic data maximum. A value of -1 will set the threshold to the minimum minus the span, and a value of 2 will set the threshold to the maximum plus the span.  
Outliers in historical data will directly affect the span value which |
<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>will then affect the thresholds. If you need or want the ability to specify thresholds beyond historic data mins and maxes and standard deviation doesn't work for you, this could be a good choice.</td>
</tr>
</tbody>
</table>

### Apply a threshold time policy to a KPI

Perform the following steps to apply a threshold time policy to a KPI.

1. In the KPIs list, select the specific KPI for which you want to set a threshold time policy.
2. Expand the **Thresholding** panel.
3. Select **Use Thresholding Template**. Then select a thresholding template, such as 3-hour blocks every day (adaptive/stdev) Selecting an adaptive template automatically enables Adaptive Thresholding and Time Policies. The Preview Aggregate Thresholds window opens. ITSI backfills the preview with aggregate data from the past 7 days. If there is data in the summary index it loads the summary data, otherwise it loads raw data. Loading raw data can take some time.
4. Expand the **Configure Thresholds for Time Policies** panel.
5. (Optional) Select a time policy block, then click **Apply Adaptive Thresholding**. For more information, see Apply adaptive thresholds to a KPI in ITSI.

![ITSI generates your new threshold time policy, which you can view in the Preview Aggregate Thresholds window.](image)

ITSI generates your new threshold time policy, which you can view in the Preview Aggregate Thresholds window. Adaptive thresholds update once daily at midnight.

6. Click **Save**.

Time polices cannot overlap. If you attempt to create a policy that overlaps with another policy, a validation error appears.
**Visualize the distribution of your data**

It takes a relatively simple Splunk search to visualize the distribution of your data and see outliers. To do so, you need to ensure the KPI of interest has already been built and backfilled. Once backfilled (or running for several weeks) you’ll have enough data in the *itsi_summary* index to run the search.

Run the following Splunk search from within ITSI. Insert your KPI name as needed at the beginning.

```
index=itsi_summary is_service_aggregate=1 kpi="<YOUR KPI NAME HERE>" | bin alert_value as bin_field | stats max(alert_value) as sort_field count by bin_field | sort sort_field | fields - sort_field | makecontinuous bin_field
```

The above SPL produces the following visualization of your data:

![Visualization of Data Distribution](image)

The search consolidates the many alert_value results down to a smaller set of buckets using the *bin* command. It also leverages the *makecontinuous* command to ensure that any outliers are visually apparent. The results above show a fairly uniform data distribution with no outliers. If necessary, you can add the *span* option to your *bin* command to provide more granularity to your graph.

**Create custom threshold time policies**

You can create custom threshold time policies tailored to your specific monitoring needs and variations in the usage of your services. You can also enable adaptive thresholding for custom time policies, and set a training window over which historical KPI data is analyzed for adaptive threshold adjustments.

Time policies support time zone offsets of 15, 30, and 45 minutes for compatibility with non-hourly time zones (such as (GMT+05:30) Chennai, Kolkata, Mumbai, New Delhi). This allows users in non-hourly time zones to accurately apply time policies created by users in hourly time zones.
**Prerequisite**

You must have the `write_itsi_kpi_threshold_template` capability to create custom threshold time policies. The `itoa_admin` role is assigned this capability by default.

**Steps**

1. In the KPIs list, select the KPI for which you want to set a threshold time policy.
2. Expand the **Thresholding** panel.
3. Select **Set Custom Thresholds**.
4. For Enable Time Policies, select **Yes**.
5. (Optional) Click **Yes** to enable adaptive thresholding. Set the **Training Window**, which is the time window over which historical KPI data is analyzed for adaptive threshold updates.
6. Expand the **Configure Thresholds for Time Policies** panel.
7. Click **Add Time Policy**.
8. Configure your custom time policy:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The name of the threshold time policy.</td>
</tr>
<tr>
<td>Start Time (HH:MM)</td>
<td>The specific hour and minute at which the threshold time policy begins. Note that the threshold start time supports 15, 30, and 45 minute offsets for compatibility with off-hour time zones.</td>
</tr>
<tr>
<td>Duration</td>
<td>The number of hours to which the threshold applies.</td>
</tr>
<tr>
<td>Repeat</td>
<td>The specific days of the week to which the time policy applies.</td>
</tr>
<tr>
<td>Apply the threshold values from an existing time policy?</td>
<td>(Optional). Choose whether to copy the threshold values from an existing policy over to this policy. This option saves you time and effort if your policies have identical or similar thresholds.</td>
</tr>
</tbody>
</table>

9. Click **Add**.
10. (Optional) To apply adaptive thresholding to this specific time policy, select the policy and click **Apply Adaptive Thresholding**. For more information, see **Apply adaptive thresholds to a KPI in ITSI**.

Policy types that support adaptive thresholds include Standard deviation, Quantile, and Range.
Copy threshold values between policies

If you’re creating multiple time policies that require the same threshold values, you can save time by copying the threshold levels and their corresponding values from one policy to another. For example, if you configure Policy 1 with the threshold values Critical=94, High=88, and Medium=75, and you want to use those same levels and values in Policy 2 and Policy 3, you can copy them over rather than inputting the values manually.

1. Click the More Options icon on a policy and choose Copy threshold values.

2. Select the policies to apply the current threshold values to. You can apply aggregate or per-entity thresholds to aggregate and/or per-entity thresholds of the same policy and/or other policies.

3. Click Save. ITSI copies the threshold levels, values, and base severity from the original policy over to the policies you selected.

Create a new KPI threshold template

Create a custom KPI threshold template with specific time block combinations that are tailored to your business case.

Prerequisite

You must have the write_itsi_kpi_threshold_template capability to create KPI threshold templates. The itoa_admin role has this capability by default.

Steps

1. In the ITSI main menu, click Configure > KPI Threshold Templates.
2. Click Create Threshold Template.

If your role does not have write access to the Global team, you will not see the Create Threshold Template option.
3. (Optional) Enter a title and description. KPI threshold templates can only exist in the Global team.
4. Click **Create**.
5. Select the template you just created in the KPI Threshold Templates lister page.
6. Select a **Preview Service** and **Preview KPI**. For example, *Database Service* and *CPU Utilization %*, respectively.
7. (Optional) For **Enable Adaptive Thresholding**, click **Yes** to enable time varying thresholds that update periodically based on historical KPI data.
   ♦ For **Training Window** select the time period over which to evaluate KPI data for adaptive thresholding.
8. Select **Aggregate Thresholds** for the preview to display the single aggregate search value. Or, select **Per Entity Thresholds** for the preview to display KPI values for each individual entity against which the KPI runs.
9. Expand the **Configure Thresholds Time Policies** panel.
10. Define a time policy for this template. Click **Save**.

You can now apply your custom thresholding template to any number of KPIs.

**Edit thresholding templates**

ITSI provides an editing page where you can modify any existing thresholding templates. For example, you might want to change the days and hours for a specific time policy, change the policy type, or apply adaptive thresholding.

1. Select a KPI in the service definition.
2. Expand the **Thresholding** panel.
3. Select **Use Thresholding Template** and select the template you want to edit.
4. Click **Edit Template**.
5. Make your modifications to the thresholding templates.
6. Click **Save**.

**Apply adaptive thresholds to a KPI in ITSI**

Adaptive thresholding uses machine learning techniques to analyze historic data and determine what should be considered normal in your IT environment. Since the shape of your data can vary dramatically, ITSI supports standard deviation, quantile, and range-based thresholds. The adaptive thresholds automatically recalculate on a nightly basis so that slow changes in behavior don't trigger false alerts.
By dynamically calculating time-dependent thresholds, adaptive thresholding allows operations to more closely match alerts to the expected workload on an hour-by-hour basis.

**When to use adaptive thresholds**

Consider the following guidelines when deciding whether to enable adaptive thresholding for a KPI:

- Because adaptive thresholding looks for historic patterns in your data, it is best to enable it for KPIs that have established baselines of data points and show a pattern or trend over time.
- Make sure your historic data isn't too random. If the historic data is noisy, a pattern will be difficult to detect.

**How are thresholds calculated?**

When you click **Apply Adaptive Thresholding** for a KPI, the thresholds are calculated based on the specific KPI that you’re previewing. If you like the calculated thresholds, you can save the template and use it. However, if you apply that same template to other KPIs with different ranges of results, such as results in the 0-100 range versus 1000-2000, you won't see immediately useful thresholds. Instead, the preview displays the KPI scores with the thresholds calculated for the original KPI.

To ensure that other KPIs use a threshold template with adaptive thresholding correctly, you can do one of the following:

- Immediately calculate the thresholds for each individual KPI using the template by clicking **Apply Adaptive Thresholding**.
- Apply the template and let the modular input that runs at midnight calculate and update the thresholds. When the modular input runs, it updates the KPI's local copy of the thresholding template.

Each night at midnight, ITSI calculates adaptive threshold values for a KPI by organizing the data from the training window into distinct buckets and then analyzing each bucket separately. ITSI creates empty buckets for each time block of the threshold template you select. Each bucket is then populated with all data points from that time block for every day of the training window.

After all the data from the last 7 days is distributed and organized into buckets, ITSI applies the selected algorithm to each bucket of data to calculate the threshold value. For descriptions of each algorithm type, see **Create KPI**
Performance considerations

Adaptive thresholds are automatically recalculated on a nightly basis so that gradual changes in behavior don't trigger false alerts. Each time a threshold is recalculated, the service must be re-saved into the its_services KV store collection. This process can moderately impact performance. The performance impact increases if a lot of your services contain KPIs with Adaptive Thresholding enabled.

The individual threshold calculations performed for each KPI do not have a significant impact on ITSI performance.

Prerequisites

- You must have the write_itsi_kpi_threshold_template capability to apply adaptive thresholds to a KPI. The itoa_admin role is assigned this capability by default.
- Before you apply adaptive thresholds, it is best to decide which algorithm you want or need based on the descriptions in Create KPI threshold time policies in ITSI.

Apply adaptive thresholds to a KPI

The following scenario walks through the process of configuring adaptive thresholding for a KPI. The sample KPI represents logins to a web server that exhibits different behaviors each day of the week and each hour of the day.

In this example, the training window is 7 days. However, as you identify smaller and smaller time policies, you might need to increase it to 14, 30, or 60 days to ensure that you have adequate data points in your short time windows to generate meaningful threshold values.

To begin your policy configuration, you must decide on the severity parameters for the chosen adaptive thresholding algorithm that align with your severity definitions. You've determined the following information about your data:

- Quantile is the right algorithm for this KPI.
- >95% is the high threshold.
- <5% is the medium threshold.
You click **Apply Adaptive Thresholding**.

The first thing you’re likely to notice when looking at the week-long KPI graph is that certain times of the day or days of the week are predictably different than other times. Perhaps AM differs from PM, or weekends differ from weekdays. These variations are almost always explainable and expected, but you should work with the service owners to confirm.

Presuming the variation is expected, the next step is to create a time policy to encapsulate that difference. In your case, you expect weekend traffic to your site to be very light. You start by separating weekend traffic from the work week with a new time policy. Apply the same adaptive threshold algorithm and severity values to your new time policy, and apply adaptive thresholds again.
ITSI only uses the historical data points within that time policy to determine the threshold values. Thus the difference is now better accounted for.

It's clear that you've made improvements, but you still see problems. There are some spikes going into the red on Monday. After working with the service team, they tell you that logins predictably spike around 8am and 5pm most every day of the work week. You can create time policies to isolate those spikes. You can also create time policies to isolate the work week evenings where things are quieter.

The thresholds might not be perfect and you'll probably have to continue this process to create the right number of time policies. However, you've applied a methodical approach and can justify the purpose of each time policy.

**Configure alerts for abnormal thresholds**

After you threshold your KPIs with adaptive thresholds, you need to consider what type of alert configurations make sense to transform abnormal KPI results into actionable alerts.
The following are two common alert strategies:

- Alert when a KPI is exhibiting extremely abnormal behavior.
- Alert when multiple KPIs are simultaneously exhibiting abnormal behavior.

However, depending on the algorithm and threshold values you choose, you might not be able to determine that a KPI is extremely abnormal. This is particularly true if you select a quantile algorithm. If that's the case, consider alerting when a KPI spends an excessive amount of time in an abnormal state.

When creating alerts based on the normalcy of multiple KPIs, try to identify two or three KPIs that are highly indicative of service health and create an alert only when most or all of them start to exhibit abnormal behavior. For example, to identify looming service issues, you might alert based on abnormal results from KPIs for count of errors in a log file and the number of successful logins.

You might also want to consider looking at multiple KPIs across two or more critical tiers of your service. For instance, if you’re seeing abnormal error counts in your web tier and your services tier, you might have an issue.

See also

- Create KPI threshold time policies in ITSI

Receive alerts when KPI severity changes in ITSI

Enable alerting on a single key performance indicator (KPI) so you can be alerted when aggregate KPI threshold values change. ITSI generates notable events in Episode Review based on the alerting rules you configure. Use these alerts to investigate and take action on the severity changes of your individual KPIs before they negatively impact the service as a whole.

When you enable alerting on the KPIs in a service template, you must explicitly choose the All KPIs option when you save the template in order for the changes to propagate to the KPIs in the linked services. For more information, see Update a service template in ITSI.

Prerequisites

- You must have write access to the service in order to enable KPI alerting.
You must create the KPI within the service, and configure thresholds for it, before you can enable alerting. For more information, see Set Thresholds.

Steps

1. Click **Configure > Service** and open the service that the KPI belongs to.
2. On the **KPIs** tab, select the KPI you want to receive alerts for.
3. Expand the **Thresholding** panel.
4. Toggle the switch next to **Enable KPI Alerting** in the Aggregate Thresholds section.
5. Configure the specific severity changes you want to monitor:
   - To receive an alert every single time the KPIs severity changes, select **Trigger a notable event for ALL KPI severity changes**.
   - To only receive alerts when specific severity changes occur (for example, a change from **High** to **Critical**), select **Trigger a notable event for specific changes** and configure the alerting rules.
6. When you’re satisfied with your alerting rules, click **Save**.

Example alert configuration

You want your analysts to be alerted when a KPI in the Middleware service degrades so they can take the necessary steps to fix it before it affects the service as a whole. You want them to be notified of each severity change over the course of the degradation so they know if things are getting worse.

You create the following alerts:

**Trigger a notable event for specific changes**

- KPI severity changes to **Critical from High**
- KPI severity changes to **High from Medium**
- KPI severity changes to **Medium from Low**

After an analyst fixes the episode, you want them to receive a final notification that the KPI severity is back to a normal level.

You create the following alert:

- KPI severity changes to **Normal from Critical, High, Medium, Low**
Configure actions for KPI alerts

IT Service Intelligence uses the **KPI Alerting Policy** to group individual KPI alerts into episodes in Episode Review. By default, this notable event aggregation policy does not contain any action rules. Add action rules to take specific actions on each episode.

1. Click **Configure > Notable Event Aggregation Policies**.
2. Open the **KPI Alerting Policy**.
3. Click the **Action Rules** tab.
4. Click **Add Rules** and add one or more action rules for KPI alerts.
5. Click **Save** to save the policy.

For example, you might configure an action rule to make sure an episode’s severity changes to **Critical** when lots of KPI alerts are coming in.

Disable grouping of individual KPI alerts

By default, ITSI uses the **KPI Alerting Policy** to group individual notable events received from KPI alerts into episodes in Episode Review. Events are grouped according to the service they belong to, and ITSI breaks an episode if no events are received for one hour. The severity of each episode is determined by the severity of the first event in the episode.

To view the individual notable events being generated, click the gear icon in Episode Review and disable **Episode View**.

To turn off this grouping behavior altogether and only display individual notable events for KPI alerts, click **Configure > Notable Event Aggregation Policies** to disable the **KPI Alerting Policy**.

The Normalized Policy (Splunk App for Infrastructure) will also create episodes containing individual KPI alerts because it looks for similar event fields when grouping. The Normalized Policy is disabled by default unless you enable it to integrate with the Splunk App for Infrastructure.

Apply anomaly detection to a KPI in ITSI

ITSI anomaly detection generates alerts when a KPI deviates from an expected pattern. If the KPI diverges from the normal pattern, a notable event is generated.
ITSI provides two anomaly detection algorithms that learn KPI patterns continuously in real time, and detect when a KPI departs from its own historical behavior. Enable anomaly detection to identify trends and outliers in KPI search results that might indicate an issue with your system.

**Prerequisite**

Anomaly detection requires Java 8 - 11 to be installed on all search heads running ITSI. For more information, see Install required Java components in the *Install and Upgrade IT Service Intelligence* manual.

**When to enable anomaly detection**

Consider the following guidelines when deciding whether to apply anomaly detection to a KPI:

- Because anomaly detection looks for deviations from a historic pattern, it's best to enable it for KPIs that have established baselines of data points and show a pattern or trend over time.
- Make sure your historic data isn't too random. If the historic data is noisy, a pattern will be difficult to detect, and anomalies will be difficult to find.
- Remember that random spikes are not necessarily anomalies. You can configure regular thresholds to alert on these. Anomaly detection is more useful if the KPI doesn't necessarily spike, but instead begins to behave abnormally.

**Anomaly detection use case**

Online sales typically follow a sine wave each day, with low load in the early morning and peak load in the early evening.
If instead the sales flatline at around medium load, the change would not set off a status-based alert since the KPI isn’t actually spiking. However, anomaly detection notices the change in behavior and generates a notable event.

**Anomaly detection algorithms**

ITSI provides two anomaly detection algorithms: trending and entity cohesion.

**Trending algorithm**

The trending algorithm detects anomalous patterns in a single time series (or metric). A sliding window on the time series is monitored by a scoring function. The scoring function compares patterns in the current window with patterns in historical data, and continuously generates scores to reflect the anomalousness of the current window.

ITSI computes thresholds adaptively without any distribution assumptions. Thresholds are robust to outliers. Anomalously high scores generate notable events.

- Applied to KPI aggregate event results.
- Detects anomalous patterns in the KPI time series.
- Adaptive thresholds applied using machine learning.
- Recent data is compared to historical trends.
- Anomalously high scores generate an alert as a notable event.

Even though the KPI value is in the “normal” range and thus wouldn’t necessarily attract attention, the historic rise and fall pattern changes, so AD indicates an anomaly.
Trending anomaly detection applies to aggregate KPI events, and is useful for tracking anomalous KPI behavior on the service level.

**Entity cohesion algorithm**

Entity cohesion analysis detects anomalous patterns in multiple time series simultaneously. The group of entities the algorithm monitors is assumed to have similar, or "cohesive", behavior and patterns.

A scoring function continuously monitors all time series within a sliding window and generates scores for each time series to reflect its departures in pattern from the rest of the series. Significant departures of a time series from its cohesive peers are indicated by high anomaly scores, which trigger alerts using similar thresholding techniques as the trending algorithm.

- Examines multiple time series (one per entity) simultaneously.
- The KPI must be split by entity, and a minimum of four entities is required.
- If the time series values for a given entity departs significantly from the typical pattern, ITSI generates a notable event.

Entity cohesion anomaly detection applies to KPIs that are shared across multiple entities, and is useful for tracking anomalous behavior on the entity level.

**Enable anomaly detection for a KPI**

Before you enable anomaly detection on a KPI, it is a best practice to use the Analyze KPI Data tool to confirm that anomaly detection is recommended for that KPI. This tool tells you if the algorithms will produce meaningful results for the KPI based on specific criteria. KPIs that do not meet the criteria for the algorithm are likely to generate false positives and are not recommended.
You can enable anomaly detection algorithms for any KPI irrespective of the analysis results. The only scenario in which you cannot enable the algorithm is in the case of entity cohesion, if the KPI is not split by entity.

**Prerequisites**

- You must have the `write_itsi_service` capability to enable anomaly detection. The `itoa_team_admin` and `itoa_admin` roles have this capability by default.
- You need at least 24 hours of data in the summary index to apply anomaly detection to a KPI.
- To enable entity cohesion analysis, the service to which the KPI belongs must contain at least 4 entities.

**Steps**

1. Click **Configure > Services**.
2. Open the service containing the KPI for which you want to apply anomaly detection.
3. Select the KPI.
4. Expand the **Search and Calculate** panel.
5. In the Unit row, click **Edit**.
6. Select **Enable backfill** and define the backfill period over which you want to analyze KPI data.
7. Click **Finish**.
8. Expand the **Anomaly Detection** panel.
9. In **Analysis Time Window**, select the time range for KPI data analysis.
10. Click **Analyze KPI Data**.

   ♦ If Algorithm Analysis Result shows **Recommended**, then the KPI meets the criteria for the algorithm.
   ♦ If Algorithm Analysis Result shows a warning message, then the KPI does not meet the criteria for use with the algorithm. Mouse over the tooltip to learn more about the algorithm requirements. See [Algorithm analysis criteria](#) below.

11. For each recommended algorithm, click **Yes** to enable it.
12. Adjust the **Algorithm Sensitivity** slider to set the algorithm's sensitivity to variance in data. The more sensitive the algorithm is, the more likely it is to generate an anomalous event. The algorithm now evaluates the KPI data continuously and generates anomalous events based on the
algorithm sensitivity threshold.
13. Click **Save**.

**Algorithm analysis criteria**

The following table outlines the specific criteria a KPI must meet to be recommended for use with the respective algorithm.

<table>
<thead>
<tr>
<th>KPI Criteria</th>
<th>Trending algorithm</th>
<th>Entity Cohesion algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum amount of data</td>
<td>24 hours</td>
<td>24 hours</td>
</tr>
<tr>
<td>% of anomalous data points</td>
<td>&lt; 10%</td>
<td>&lt; 10%</td>
</tr>
<tr>
<td>Minimum number of entities</td>
<td>N/A</td>
<td>4 entities minimum</td>
</tr>
<tr>
<td>Maximum number of entities</td>
<td>N/A</td>
<td>30 entities per KPI</td>
</tr>
</tbody>
</table>

**Triage and investigate anomalous events**

An anomalous event is an event that is inconsistent with or deviating from what is usual. ITSI generates a notable event in Episode Review when it detects an anomalous event.

It can take up to 24 hours for anomaly detection to begin generating events. You can then open an event in a deep dive to perform root cause analysis.

- The trending algorithm generates notable events with the heading "Service level alert on KPI."
- The entity cohesion (cohesive) algorithm generates notable events with the heading "Entity level alert on KPI."

The type of algorithm that generated the notable event appears in the **Details** section of the Overview tab.

For more information, see Overview of Episode Review in ITSI in the Splunk ITSI **User Manual**.

**Investigate anomalous events in a deep dive**

You can drill down to a deep dive from any anomalous notable event. This lets you view the event over a default 10 minute time range, and perform root cause analysis in the context of other service KPIs.

1. Select the anomalous notable event in Episode Review.
2. Under Drilldowns, click the **Drilldown to <service_name>** link. A deep dive opens with an overlay of the anomaly in the KPI lane. Anomalous events appear as red icons. The following image shows an example of anomaly overlays:

3. (Optional) Mouse over the alert icon to select options to view notable events or add anomalous entities as new lanes. Add additional KPIs to the deep dive for contextual analysis of the anomalous event.

For more information, see *Add anomaly overlays in the Splunk ITSI User Manual*.  

**Set the maximum entity limit**

The Entity Cohesion algorithm supports a maximum of 30 entities per KPI. Although this limit is configurable, it is recommended that you do not exceed 30 entities. If you run KPI analysis against a KPI that has more than the 30 entities, a warning message appears stating that the KPI has too many entities, and the KPI is not recommended.

You can lower the maximum number of entities at which KPI analysis triggers a warning message.

**Prerequisites**

- Only users with file system access, such as system administrators, can set the maximum entity limit for cohesion analysis.
- Review the steps in How to edit a configuration file in the *Admin Manual*.

Never change or copy the configuration files in the **default** directory. The files in the **default** directory must remain intact and in their original location.

**Steps**

1. Open or create a local *mad.conf* file for the ITSI app at `$SPLUNK_HOME/etc/apps/SA-MetricAD/local/`.
2. Under the *cohesive* stanza, set `metrics_maximum` to a lower value. For example:

   ```
   [cohesive]
   metrics_maximum = 15
   ```
Increase anomaly detection memory requirements

By default, anomaly detection reserves 1GB of memory, which is enough for up to 1000 KPIs for trending analysis or up to 1000 metrics for cohesive analysis. To support more than this, increase the Heap memory size in `SA-ITSI-MetricAD/local/command.conf` on your search heads. To determine the amount of memory you should use, size your analysis requirement first, then calculate your memory requirements based on that.

Trending anomaly detection requires about 600MB per 1000 KPIs. Cohesive anomaly detection requires about 1GB per 1000 metrics (for example, a combination of 10 KPIs with 100 entities or 20 KPIs with 50 entities).

These recommendations are guidelines. Many factors can influence memory usage for anomaly detection, such as the size of historical data, algorithm configurations, and available CPU.

Prerequisites

- Only users with file system access, such as system administrators, can change anomaly detection memory requirements.
- Review the steps in How to edit a configuration file in the Admin Manual.

Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location.

Steps

Perform the following steps on each search head.

1. Open or create a `commands.conf` file at `${SPLUNK_HOME}/etc/apps/SA-ITSI-MetricAD/local/`.
2. Under the [MAD] stanza, change the "1G" part of the `command.arg.1=-J-Xmx1G` setting to increase the memory.
3. Restart Splunk software.

Create KPI base searches in ITSI

KPI base searches let you share a search definition across multiple KPIs. You can create base searches to consolidate multiple similar KPIs, reduce search load, and improve search performance. For example, if you have similar ad hoc
searches whose only difference is an entity or threshold field, you can consolidate these searches into a single base search definition and achieve better search performance.

**ITSI module base searches**

ITSI includes several pre-configured KPI base searches based on ITSI modules that you can use with your services. The titles of these base searches begin with "DA-ITSI". KPI base searches that come with ITSI modules are read-only and cannot be modified or deleted. To customize a base search that comes from an ITSI module, clone the base search, then perform your edits on the clone.

**Service templates and base searches**

Service templates use base searches for their KPIs. When a service template is created from a service, all of the KPIs in the service are imported into the template. Any service KPIs that use ad hoc searches, data model searches, or metrics searches are converted into base searches. These base searches are listed on the KPI Base Searches lister page and are available to use for KPIs in any service, just like any other base search. Base searches that are created for service template KPIs use the following naming standard: `<service name>:<KPI name>_<last 8 digits of KPI ID>`.

**Create a new base search**

You can create new KPI base searches, then use those base searches to build KPIs in the configure services workflow. You can create a base search using an ad hoc search or a metrics search. See Overview of metrics in the Splunk Enterprise Metrics manual for information about Splunk metrics.

**Prerequisites**

Only users with write permissions to the Global team can create a KPI base search. You must also possess the appropriate capabilities to be able to read, create, or delete base searches.

**Steps**

1. Click **Configure > KPI Base Searches**.
2. Click **Create KPI Base Search**.
3. Enter a title for your base search. For example, `CPU load base search`.
4. (Optional) Enter a description for your base search. For example, `This`
base search can be used to build KPIs for CPU metrics.

You can't change the Team field because all KPI base searches exist in the Global team. All users have read access to the Global team.

5. Click **Create**.

6. Configure your base search:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Select either <strong>Ad hoc Search</strong> or <strong>Metrics Search</strong>.</td>
</tr>
<tr>
<td></td>
<td>♦ For an Ad hoc Search, provide the source ad hoc search. For example, <code>index=os source=ps</code>.</td>
</tr>
<tr>
<td></td>
<td>♦ For a Metrics Search, select the metrics index to use and the metric. If you do not have a metrics</td>
</tr>
<tr>
<td></td>
<td>index, you will see the message: &quot;No metrics found&quot;.</td>
</tr>
<tr>
<td>KPI Search Schedule</td>
<td>The frequency of the search (Every 1, 5, or 15 minutes).</td>
</tr>
<tr>
<td>Calculation Window</td>
<td>The time period over which the search applies. (Last 1 min, 5 min, 15 min, or 24 Hours).</td>
</tr>
<tr>
<td>Monitoring Lag</td>
<td>Pushes the search back by the specified number of seconds. This value must match the index lag time.</td>
</tr>
<tr>
<td>Split by Entity</td>
<td>Select <strong>Yes</strong> to maintain a breakdown of KPI values on the entity level.</td>
</tr>
<tr>
<td>Entity Split Field</td>
<td>The field in your search results that is used to look up the corresponding entity to split the KPI.</td>
</tr>
<tr>
<td></td>
<td>For example, you might want to split your KPI by the processes running on the hosts instead of just</td>
</tr>
<tr>
<td></td>
<td>the host.</td>
</tr>
<tr>
<td>Filter to Entities in</td>
<td>Select <strong>Yes</strong> to filter the search based on the entity alias.</td>
</tr>
<tr>
<td>Service</td>
<td>To filter to entities in a service, the service must have associated entities.</td>
</tr>
</tbody>
</table>

7. Click **Add Metric**. The Add Metric modal appears. You can add multiple metrics to your base search. Each metric defines a threshold field (for ad hoc searches only) and the calculation method used to aggregate KPI search results on the entity and service level.

8. Configure your metric:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>The name of the metric. For example, CPU load percent</td>
</tr>
<tr>
<td>-------</td>
<td>------------------------------------------------------</td>
</tr>
<tr>
<td>Threshold Field (Ad hoc search type only)</td>
<td>This is the field in your data that the KPI aggregates and monitors. For pure counts, use _time.</td>
</tr>
<tr>
<td>Unit</td>
<td>The type of measurement that the KPI calculates. For example, %, MB, and so on.</td>
</tr>
<tr>
<td>Entity Calculation</td>
<td>Sets the calculation method for calculating aggregate search results on the entity level if Split by Entity is set to Yes.</td>
</tr>
<tr>
<td>Service/Aggregate Calculation</td>
<td>Sets the calculation method for calculating the service/aggregate level.</td>
</tr>
<tr>
<td>Fill Data Gaps with</td>
<td>How to treat gaps in your data. This setting affects how aggregate KPI data gaps are displayed in service analyzers, deep dive KPI lanes, glass table KPI widgets, and other dashboards in ITSI populated by the summary index.</td>
</tr>
<tr>
<td></td>
<td>♦ Select Null values to fill gaps in data with N/A values. Also select the severity level to use for Null values.</td>
</tr>
<tr>
<td></td>
<td>♦ Select Last available value to use the last reported value in the ITSI summary index. Aggregate KPI data gaps are filled with the last reported aggregate KPI value. Entity-level data gaps are filled with the corresponding entity’s last available value.</td>
</tr>
<tr>
<td></td>
<td>♦ Select Custom value to specify a specific value to use when there is a gap in data. Enter a positive integer. Filled gap values are not used in the calculations performed for Anomaly Detection and Adaptive Thresholding.</td>
</tr>
</tbody>
</table>

9. Click **Add** to add the metric to the list of metrics defined for your base search. When you build a KPI from a base search, you can select one and only one metric for the KPI.

10. Click **Save**. You can now use the base search to build KPIs when configuring services.
Build new KPIs from a base search

You can use KPI base searches to build new KPIs. Each KPI that you build is linked to the base search. If you edit and save a base search, those changes are propagated to all linked KPIs.

KPI base searches contain metric specifications. The metric specification for ad hoc base searches includes a threshold field. The metric specification for both ad hoc base searches and metrics base searches contains a method of calculation for aggregate search results at the service and entity level. When you apply a base search to a new KPI, you must select a metric specification from the base search to complete the new KPI search definition.

For example, if you want to create a new KPI to measure CPU load, you might select a metric specification from the base search that contains `cpu_load_percent` as the threshold field and `average` as the calculation method.

To build a KPI from a KPI base search:

1. Select **Configure > Services** and select a service.
2. In the KPIs tab, select **New > Generic KPI**.
3. Enter a title and description. Click **Next**.
4. For **KPI Source** select **Base Search**.
5. In the **Base Search** dropdown, select the base search for your new KPI. You can choose from base search templates provided by ITSI modules, or from your own custom base searches.
6. Select a metric from the **Metric** menu. Click **Next**.
   - The Entities page appears. All fields are populated from the selected base search. Click **Next**.
   - The Calculation page appears. All fields are populated from the selected base search. Click **Next**.
   - The Optional Setup page appears. All fields are populated from the selected base search, with the exception of **Enable Backfill**.
7. Select the **Enable Backfill** check box, then select a **Backfill Period** (optional). Click **Next**.
8. Set appropriate severity-level thresholds for the KPI. Click **Finish**.
   - The new KPI is created and appears in the list of KPIs for the service.

To unlink a KPI from the base search, edit the KPI and change the search type to adhoc, then save the KPI. This lets you use KPI base searches as a starting point for new KPIs.
Delete a KPI base search

When you delete a base search, any service KPIs that use the base search are converted to ad hoc searches. You can't delete a base search that is being used by a KPI in a service template. You must modify those service templates to remove the dependency before you can delete the base search. Additionally, you can't delete a metric that is being used by a base search in a service template.

By default, you can't edit or delete the module base searches that are shipped with ITSI. However, you can make this content editable so you can tune or delete it through the UI. For more information, see Edit or remove the default content shipped with ITSI in the Splunk ITSI Content Packs manual.

Prerequisites

- Only users with write permissions to the Global team can delete a KPI base search.
- You must have the `delete_itsi_kpi_base_search`. The `itoa_admin` and `itoa_team_admin` roles have this capability by default. For more information, see Configure users and roles in ITSI.

Steps

1. From the ITSI top menu bar, click `Configure > KPI Base Searches`.
2. In the Actions column of the base search you want to delete, click `Edit > Delete`.
3. Click `Delete` to confirm.

KPI base search performance considerations

The performance of KPI base searches is dependent on the following factors:

- The number of KPIs that use the base search.
- The number of services that contain KPIs that use the base search.
- The number of entities matching service entity rules.

Most of the KPI base searches delivered with ITSI are configured to run every minute. Based on testing on a system with 32 cores and 16 GB of memory, a single KPI base search can support up to 5,000 KPIs with 15 entities matched by service entity rules reasonably well.

In general, a KPI base search can support fewer KPIs with many entities or many KPIs with fewer entities. It's not advised to use a single KPI base search for both
a high number of KPIs and a high number of entities. As the number of services or matching entities increases, the search runtime also increases.

You can check the runtime for your KPI base searches on the Activity > Jobs page. The runtime is the actual time it takes to run the search. Check the KPI search schedule, or frequency, of the KPI base search. If a search is scheduled to run every minute, and the runtime of that search is longer than 1 minute, the search is taking too long to run.

To reduce a search's runtime, you need to either reduce the number of KPIs using the base search, reduce the number of services that contain the KPI, or reduce the number of entities for each service accordingly. The easiest solution is to clone the KPI base search and use the cloned base search for some of the KPIs.

**Fix truncated or incorrect KPI values**

Search results are processed, created, and written to the itsi_summary index via an alert action. The default limit on the number of rows that can be written is 50,000 as specified in the $SPLUNK_HOME/etc/system/default/limits.conf file. You can increase this limit if necessary.

Calculate the number of the result rows generated by a shared base search using the following formula:

\[
\text{Number of result rows} = \text{<number of services>} \times \text{<number of KPIs in each service>} \times \text{<number of entities per service entity rule>} + \text{<number of services>} \times 2
\]

For example, for 500 services with 10 KPIs in each service and 15 matching entities, the expected number of result rows is:

\[
500 \times 10 \times 15 + 500 \times 2 = 76,000 \text{ rows}
\]

If the number of result rows expected is more than 50,000, ITSI truncates the results and displays incorrect KPI values. If you think you're running into this limitation perform the following steps:

**Prerequisites**

- Only users with file system access, such as system administrators, can increase write search result limits using a configuration file.
- Review the steps in How to edit a configuration file in the Admin Manual.
Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location.

Steps

1. Open or create a local limits.conf file at $SPLUNK_HOME/etc/apps/SA-ITOA/local.
2. Add the following stanza:

   [scheduler]
   max_action_results = 1000000
3. Set the value for max_action_results to a number higher than 50,000. In the example above it’s set to 100,000.

Increase the KV store bulk get limit

The KPI base search tries to get all the relevant services from the KV store internally for thresholding related operations. When a KPI base search is attached to a lot of services, the bulk get might reach the KV store bulk get size limit. The default limit is 500MB.

As a guideline, for one service with 20 fully populated KPIs in which all KPIs have custom thresholds with time policies configured, as well as cohesive anomaly detection configured, the size is roughly 0.8 MB in the KV store.

If you have a large number of services containing a lot of KPIs and metadata, it is recommended to increase the KV store bulk get limit in $SPLUNK_HOME/etc/apps/SA-ITOA/local/limits.conf. Increase the max_size_per_result_mb value as necessary.

[kvstore]
# The maximum size, in megabytes (MB), of the result that will be returned for a single query to a collection.
# ITSI requires approximately 50MB per 1,000 KPIs. Override this value if necessary.
# Default: 500 MB
max_size_per_result_mb = 500

Schedule KPI searches to update at the same time in ITSI

By default, ITSI staggers the search scheduling of KPIs in order to reduce search load. For example, if you have five KPIs that are scheduled to run every 5 minutes, the search to update the value of each KPI from the summary index is
staggered over the 5 minute interval (the first KPI at minute 1, the second KPI at minute 2, and so on).

You can synchronize KPI searches so they update at the same time during the scheduled interval. For example, if 5 KPIs are scheduled to run every 15 minutes, they ALL run at the 15/30/45/00 mark instead of being staggered over the interval.

Prerequisites

- Only users with file system access, such as system administrators, can synchronize KPI searches.
- Review the steps in How to edit a configuration file in the Admin Manual.

Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location.

Steps

1. Open or create a local itsi_settings.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/local/
2. Add the following stanza:

   [synced_kpi_scheduling]
   disabled = 0

When disabled = 0, newly created KPI saved searches run at the same time during each scheduled interval. After a KPI is updated, its search schedule will be overwritten to follow the synchronized schedule.

To reset the search schedules of all existing KPIs to use the new synchronized search schedule after you set disabled = 0, restart Splunk software and then use mode 4 of the kvstore_to_json.py script. See Regenerate KPI search schedules (mode 4) for details.

This setting affects all KPIs, including base searches, for all services. Enabling synced scheduling can have a significant performance impact because it increases the scheduler load. The increased load can result in a delay in search execution due to the number of searches being dispatched at the same time. You might need to scale up your hardware in order to support the increased load.
Service Templates

Manage services in bulk with service templates in ITSI

Service templates in IT Service Intelligence (ITSI) help you manage services in bulk. Any changes you make to a template are propagated to all linked services. For example, if you add a KPI to a service template, it is added to all the linked services. You can still configure KPIs and entity rules that are unique to a service directly in the service.

Use service templates to do the following:

- Create a single service and link it to a service template to populate the KPIs and entity rules. See Create a single service in ITSI.
- Bulk import many services at once and link them to a service template. See Bulk import services in ITSI.

You can also use the ITSI REST API to link services to service templates. It is best practice to create the service on which to base the template in the UI rather than creating the service through the ITSI REST API. See itoa_interface/service/<_key>/base_service_template in the ITSI REST API Manual for information.

When you update a template, the following changes are propagated to the linked services:

- New KPIs
- Deleted KPIs

For the following properties, you can control how the updates are propagated to linked services:

<table>
<thead>
<tr>
<th>Property</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity rules</td>
<td>Choose whether to overwrite the rules in the linked services or not.</td>
</tr>
<tr>
<td>KPI threshold templates</td>
<td>Choose to update the threshold templates for all KPIs, no KPIs, or only unchanged KPIs in the linked services.</td>
</tr>
<tr>
<td>Health score</td>
<td></td>
</tr>
</tbody>
</table>
Choose whether to overwrite the KPI importance values in the linked services with the importance values in the template. KPIs that exist in the service but not the template and dependent KPI values are not affected by overwriting.

Service templates differ from services in the following ways:

- Templates don’t contain a service health score.
- Template KPIs can only use a base search, not ad hoc or data model searches.
- Templates don’t have service dependencies. You must define dependencies in individual services.
- Templates allow entity values to be defined in the linked services rather than in the template. These are known as configurable entity rules.
- You can’t enable detection for KPIs in a template. You must manually enable it for KPIs in individual services.

Templates exist in the Global team. You must have write access to the Global team and the write capability for service templates in order to create service templates. By default, only the itoa_admin possesses this capability.

Team admins (users with a role that inherits from the itoa_team admin role) can create services for their teams using service templates. The same template can be used for services in different teams. Dependent services do not have to be linked to the same service template as the parent service.

The higher the number of services linked to a service template, the higher the number of KPIs that use the same base search. For example, if a service template has 10 KPIs and is linked to 12 services, each KPI base search in the template is being used 12 times, once for each of the linked services. If the same KPI base search is used by too many services, this can lead to performance issues. See KPI base search performance considerations for information.

**Service template use cases**

The following use cases illustrate how using service templates can streamline the process of creating and maintaining services.
Create one or more services from a service template

In this example, as the ITSI administrator, you need to create multiple services to monitor databases. Each service needs the same set of KPIs: Database Service Errors, Database Service Response Time, Storage Free Space: %, and CPU Utilization: %. However, each service will be monitoring different database servers (entities). One service needs to be filtered to the servers running Oracle database and another service needs to be filtered to the servers running MySQL.

1. A database service already exists that has the KPIs you want your services to have. You use this service to create a Database service template by selecting Edit > Create Service Template from the Services viewer page.
2. You name the template "Database service template" and click Create. The service template receives the entity rules, KPIs, KPI thresholds, and KPI importance values from the service.
3. The Database service didn't have any entity filtering rules, so you decide to add some entity rules to the template. First you add a rule that filters the template down to all entities that have "Category matches database." This helps you narrow down the entities that have a database installed, but you need a way to differentiate between the different services. To do this, you add a configurable entity rule. This allows you to select a key to filter on whose value will be defined in each service linked to the template. You add the following entity rule to the Database template: "host matches a value defined in the service".
4. Save the template and select to overwrite the entity rules so that the entity rules you added in the template will be added to the Database service that you used to create the template. You push the changes immediately and see the new entity rules in the Database service.
5. Now you are ready to create the new services based on the service template. You create a new service named "Oracle database service" and select the option to Link service to a service template and select the Database service template you created. Then you create a "MySQL database service" using the Database service template. These two services are now linked to the template and have received the entity rules and KPIs from the service template.
6. You open the Entity tab of the service definition for the Oracle Database service. You see an empty value for the host entity rule that the service received from the template. Specify the value for the host entity rule as oracle* since all the Oracle hosts begin with "oracle", for example: oracle-01, oracle-02, oracle-03.
   In the service definition of the MySQL service, specify a value of mysql*
since all the MySQL hosts begin with "mysql," for example: mysql-01, mysql-02, mysql-03. Now the KPIs that are filtered to entities (such as Database Service Errors, Storage Free Space: %, and CPU Utilization: %) will be filtered to the appropriate hosts for each service.

7. You decide to go back to the template to make sure that KPI thresholds are set up properly. You select an adaptive threshold template for a KPI and apply it. You look over the preview and toggle it between each linked service to make sure it makes sense for each of the services. You know that if one of the services requires a custom adaptive threshold settings, that you can make that change in the service and choose to only overwrite KPI thresholds for unchanged KPIs when changes are pushed from the template in the future.

8. You also decide to adjust the KPI importance value for one of the KPIs.

9. When you save the template, you choose to overwrite KPI thresholds and overwrite health score so that the KPI thresholds and KPI importance values in the services will be overwritten with the new ones you just added to the template.

10. So as not to cause disruption to the Splunk environment, you schedule the changes to be pushed to the linked services at 12:00am when the system should not be as busy.

11. The next morning, you see that the updates have been propagated to the database services.

See Also

- Create a single service in ITSI
- Create a service template in ITSI

Customize a service that is linked to a service template

The team admin who administers the Oracle database service in ITSI uses a custom plug-in with their Oracle database. She wants to add a KPI that checks the status of the plug-in. Because this KPI does not apply to every service linked to the Database service template, you are hesitant to add it to the Database service template. You tell the team admin to add the KPI to the service.

1. The team admin opens the service definition of the Oracle Database service and adds the KPI to monitor the plug-in and saves it.
2. The next time the ITSI admin updates the Database service template, this unique KPI for the Oracle Database service is not modified.

See Also
Configure a service created from a service template in ITSI
Summary of changes that unlink a service from its service template

Bulk import services and link them to a service template

The director of IT has asked you to create Apache services for every Apache instance in the company. There are dozens of instances and you realize you cannot do this manually. You decide to use the ITSI bulk import feature. An Apache service template already exists with a configurable entity rule to filter entities by a different value for each linked service.

1. You query the CMDB and pull down a list of every Apache service in the company. You export the list as a CSV file and open it in Excel.
2. You add a new column that denotes the template each service will map to. In it you write "Apache Service Template" and copy it for every row.
3. You open up the ITSI bulk import and upload the CSV. You map the proper columns that denote the service name, service dependencies, and service template name.
4. After examining the bulk import preview, you decide the import looks good and move on to the entity configuration step. All of the services have a column called "serviceoid." This makes it very easy to map the entities for each service. You set the configurable entity rule for the Apache template to map to the values in the serviceoid column.
5. You click **Import** and all of your services are created and linked to the Apache service template.

See Also

- Bulk import services in ITSI

Create a service template in ITSI

To create a service template, you must first create a service on which to base the service template. The entity rules, KPIs, KPI importance values, and KPI thresholds of the service are imported into the service template. The service you create the template from is linked to the template by default. After the template is created, you can link multiple services to it. A service can be linked to only one template.

Note that service templates are always created in the Global team, regardless of the team of the service that you use to generate the template.
Prerequisites

♦ To create a service template, you must have the `write_itsi_base_service_template` capability and have write access to the Global team. Users with the `itoa_admin` role have this capability by default.

Users with team admin roles (roles that inherit from the `itoa_team_admin` role) have a read-only view of the Service Templates lister page. Team admins cannot create or change service templates but they can create services for their teams using service templates.

♦ You must first create at least one service to generate a template.

Steps

1. Click **Configure > Service Templates** from the top menu bar.
2. Click **New Service Template**.
3. Select the service on which to base the template. The entity rules, KPIs, KPI importance values, and KPI thresholds of the service will be imported into the template. Additionally, the service you use to create the template will be linked to the template.

   Services with a lock icon are already linked to a template. If you choose a service that is already linked to a template, it is unlinked from its current template and linked to the new template you are creating.

4. Type a name and description for the template and click **Create**.
   The entity rules and KPIs from the service are imported into the template, then the service template definition page opens.
5. Click the **Entities** tab to view the entity rules that have been imported from the service.
   Note that matching entities are not displayed in the service template. You can view matching entities at the bottom of the Entities tab in the service definition.
6. Click the **KPIs** tab to see the KPIs imported from the service. Any KPIs in the service that were based on an ad hoc search, metrics search, or data model are converted to a base search in both the service template and the service.
7. Click the **Settings** tab to see the importance values for the KPIs that were imported from the service.
8. In the **Linked Services** tab, note that the service you used to create the template is listed as a linked service and that the sync status is Synced.

See also:
• To make changes to the service template, see Update a service template in ITSI.
• To create a new service from a service template, see Create a single service in ITSI.

Configure a service created from a service template in ITSI

After creating a service from a service template, review the content the service received from the template. Entity rules, KPIs, KPI threshold values, and KPI importance values are populated from the template. However, you must do some service configuration directly in the service:

• If the service template contains blank entity rules whose values need to be specified in the service, you must provide those in the service entity rules.
• If you want to enable anomaly detection or configure custom thresholds for any of the KPIs, you must do this in the service.
• If the service has service dependencies, you need to specify them in the service.

To finish configuring the service, perform the following steps:

1. Review the entity rules

• The entity rules from the template are added to the service.
• Any entity rules without values that came from the template contain a icon. Provide a value in order to filter the service to a specific set of entities. These entity rule values are meant to be custom for each service. Some entity rules might have blank values intentionally and don’t display the notification icon.
• Add or change entity rules as desired for the service. For more information, see Add entity rules to a service in ITSI. You can choose to preserve any custom entity rules you define in the service when you update the service template.

2. Review the KPIs

• The KPIs in the template are added to the linked service. These KPIs display a lock icon to indicate that they’re linked to the template. Now you can set custom thresholds and enable anomaly detection for linked KPIs. For more information, see Apply anomaly detection in ITSI and Add
a KPI to a service in ITSI.

Making any other changes to a linked KPI, such as deleting it or changing its name, unlinks the service from the template.

- Add any new KPIs that are specific to this service. These KPIs are not overwritten when you update the service template. KPIs added directly to the service do not have a lock icon which indicates they are not tied to the service template. See Add KPIs to a service in ITSI for information.

3. Specify service dependencies

On the Service Dependencies tab, add other services as impacting services, or service dependencies. Dependencies are not included in service templates so you must configure them manually for each service. For more information, see Add service dependencies in ITSI.

4. Set KPI importance values

On the Settings tab, change the team the service belongs to or configure KPI importance values. You can preserve custom KPI importance values for a service, which determine the service health score, when you update the service template. For more information, see Set KPI importance values in ITSI.

Any changes you make to the service apply to the service only. Edit the service template if you want to make changes that propagate to all services linked to the template.

Summary of changes that unlink a service from its service template

When a service is linked to a service template, you generally want to make updates to the template and not the service itself. However, you can customize some attributes of the service that are unique to the service.

You can make the following changes to a service without breaking the link to the service template:

- Add a KPI
- Modify an unlinked KPI (a KPI that does not display a lock icon)
- Update KPI thresholds
- Enable anomaly detection for a KPI
- Update KPI importance values which contribute to the service health score
- Add, modify, or delete entity rules
The following changes to a service will break the link to the service template:

- Modifying the name of a linked KPI
- Modifying the base search of a linked KPI (or modifying any other settings in the Search and Calculate section, including enabling backfill)
- Deleting a linked KPI

Linked KPIs have a lock icon next to the name of the KPI in the KPI tab of the service definition.

If you clone a service that is linked to a template, the clone will also be linked to the service template.

**Update a service template in ITSI**

Make updates to a service template to update all the services linked to the template. You can choose to push updates to the linked services immediately or schedule a specific date and time to push the updates.

1. Click **Configure > Service Templates**.
2. Open a service template.
3. On the **Entities** tab, add, modify, or delete entity rules as desired.
   - Use the **matches a value to be defined in the service** or **does not match a value to be defined in the service** options to specify the value for an entity rule in each service rather than in the template. This is useful if each service linked to the template will be monitoring different entities. For example, you could specify `Alias vm_name matches a value defined in the service`. Then, after the services have been synced with the template, specify the value for `vm_name` in each service. These options are particularly useful if you plan to bulk import services and link them to the template.

If you use the configurable entity rules described above and choose **Overwrite Entity Rules** when you save the service template, any entity rules already defined in the linked services are replaced with the entity rules from the template and have blank values (matching all entities).

4. On the **KPI** tab, add, modify, or delete the KPIs in the template, and set KPI thresholds as desired. Any KPIs you add to the template must use a base search. Template KPIs cannot use ad hoc, metrics, or data model searches.
You cannot enable anomaly detection in a service template. You must enable anomaly detection for a KPI in the service directly.

5. On the **Settings** tab, set importance values for the KPIs and see how they affect the health score of linked services.

6. When you finish making modifications to the service template, click **Save**.

7. In the Save Service Template dialog box, indicate what information to update and select when to push the changes to the linked services.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overwrite entity rules</td>
<td>Replaces the entity rules in the linked services with the entity rules in the template.</td>
</tr>
<tr>
<td>Overwrite KPI thresholds and alerting rules on</td>
<td>Whether to update KPI thresholds and KPI alerting rules.</td>
</tr>
<tr>
<td></td>
<td>♦ Select <strong>All Unchanged KPIs</strong> if you customized some of the KPI thresholds or alerting rules in your services and you want to keep these settings.</td>
</tr>
<tr>
<td></td>
<td>♦ Select <strong>All KPIs</strong> to overwrite customized thresholds and alerting rules in linked services.</td>
</tr>
<tr>
<td></td>
<td>This setting does not affect KPI thresholds or alerting rules for any KPIs that are unique to the service and not linked to the template.</td>
</tr>
<tr>
<td>Overwrite health score calculation</td>
<td>Replaces the KPI importance values used to calculate the health score in the linked services with the values from the template. KPI importance values for any additional KPIs in the service that are not present in the template are not affected. Importance values for dependent services are also not affected.</td>
</tr>
<tr>
<td>Push changes to services</td>
<td>When to push the changes to the linked services. Either push the changes immediately, or select <strong>Later</strong> to choose a date and time to update the linked services. It is considered a best practice to push changes outside of regular business hours to avoid disruption.</td>
</tr>
</tbody>
</table>

8. Click **Save**. The changes in the template are immediately propagated to the linked services if you chose to push the changes now, or scheduled for the date and time you selected.

9. Click the **Linked Services** tab to see the sync status of the services linked to the template.

After the linked services are synced with the template, the status says "Synced". If you elected to push the changes now, you might need to refresh your browser to see the status change. You will also receive a message in Splunk Web with
the status of the sync.

You can only schedule one sync for a service template. If you make additional updates to a service template that is already scheduled, you can keep the scheduled time (the default) or choose to sync now or at a different time. All updates that have been made to the template are pushed at the time you choose.

**Link a service to a service template in ITSI**

You can link multiple services to a service template in order to manage them collectively. A service can be linked to only one service template.

When linking a service to a service template, any existing KPIs in the service are preserved and KPIs in the template are added to the service. You can choose how to update the entity rules in a service: append the template entity rules to the service entity rules, replace the service entity rules with the template entity rules, or keep the entity rules in the service and not import any of the entity rules from the service template.

There is no limit to the number of services that can be linked to a service template. However, the higher the number of services linked to a service template, the longer it will take to sync service template updates with the linked services.

This procedure describes how to link a single service to a service template. To link multiple services to a service template, use the bulk import feature. See Bulk import services in ITSI.

To create a new service from a service template, see Create a single service in ITSI.

**Prerequisites**

- You must have the write_itsi_service capability to link a service to a service template. The itoa_admin and itoa_team_admin roles have this capability by default.
- At least one service template must exist in ITSI.

**Steps**

1. Click Configure > Services from the top menu bar.
2. In the Actions column for the service you want to link, click **Edit > Link to Service Template**.
3. Click **Select...** and choose a template. If the service is already linked to a template, choose a different template to link the service to.
4. In the template details section, review the entity rules, the KPIs that are contained in the template, and the services already linked to the template.

When linking a service to a template for the first time, any KPIs that already exist are retained and new KPIs from the template are added. If any KPIs in the service have the same name as a KPI in the template, the KPI in the service is renamed using a unique identifier.

If the service was already linked to a template and you are linking it to a different template, linked KPIs (those that came from the original template) are removed, unlinked KPIs (KPIs that were added directly to the service) are retained, and KPIs from the newly selected template are added.
5. In the **Settings** section, choose how to update the entity rules in the service:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Append template rules</td>
<td>Adds the entity rules from the template to the service and keeps the ones that were already there.</td>
</tr>
<tr>
<td>Replace with template rule</td>
<td>Deletes the existing entity rules in the service and replaces them with the entity rules from the service template.</td>
</tr>
<tr>
<td>Keep existing service rules</td>
<td>Keeps the existing entity rules in the service and does not add any entity rules from the template.</td>
</tr>
</tbody>
</table>

6. Click **Link**. The Service Template column indicates that the service is synced with the service template.

To review the content updates that the service received from the template, click the name of the service. See **Review updates received from the template and customize the service** for more information.

### Manage service templates in ITSI

Service templates let you update services in bulk. To manage service templates, ITSI administrators can perform these tasks:

- Review content updates received from the template
- Unlink a service from a service template
• Clone a service template
• Delete a service template

Review updates received from a template and customize the service

After linking a service to a template, or changing the template a service is linked to, review the content updates the service received from the template. You can also customize the service to meet your needs. If the service template contains entity rules with values that need to be specified in the service, provide them in the service entity rules.

Review the following tabs within the linked service:

**KPIs**

♦ Make sure the KPIs from the template were added to the service. These KPIs display a lock icon to indicate that they are linked to the template.
♦ Set custom threshold settings and enable anomaly detection for linked KPIs as desired. If you change the threshold settings, or if the adaptive thresholding value is recalculated, a icon appears in the Thresholding section to indicate the KPI threshold settings differ from those in the service template, but the service is still linked. To preserve custom thresholds in the service, make sure to select **Overwrite KPI Thresholds on: All Unchanged KPIs** when saving the template and pushing updates to the services.

Making any other changes to a linked KPI, such as changing the name of the KPI, changing the base search it uses, or enabling backfill, will cause the service to be unlinked from the template.
♦ KPIs that already existed in the service are listed without a lock icon. Any changes you make to the service template will not affect them.
♦ Any existing KPIs in the service that had the same name as a KPI in the template are renamed with _custom and a unique identifier appended to the name of the KPI. For example, if both the service and the template have a KPI called CPU Utilization: %, the KPI in the service is renamed to CPU Utilization: %_custom_02f8cab3-e5d1-11e7-b55a-005056923ff0 and the CPU Utilization: % KPI from the template is added. You can delete the duplicate KPI if desired.
♦ Add any new KPIs to the service as desired. These KPIs will not be overwritten when the service template is updated.

**Entities**

♦ If you selected **Append template rules** when you linked the service to the template, any entity rules that existed in the service are retained and the entity rules from the template are added to a new rule block (with an implicit OR between the rule blocks).

♦ If you selected **Replace with template rules** when you linked the service to the template, any entity rules that were in the service are gone and the entity rules from the service template are added.

♦ If you selected **Keep existing service rules** when you linked the service to the template, the existing entity rules in the service are listed and no new entity rules are added from the template.

Any entity rules with blank values that came from the template contain a ■ icon. Provide a value in order to filter the service to a specific set of entities. These entity rule values are meant to be custom for each service. Some entity rules might have blank values intentionally. These do not display the icon.

Add or change entity rules as desired for the service. You can choose to preserve the entity rules in the service when you update the service template.

**Service Dependencies**

Specify any service dependencies. Service dependencies, or impacting services, have some sort of effect or influence on the primary service. Adding service dependencies can help you detect if one service is having a negative impact on another service, and can be useful in performing root cause analysis.

**Settings**

Enable or disable the service, change the team the service belongs to, and change KPI importance values. Custom KPI importance values for a service, which are used to determine the service health score, can be preserved when the service template is updated.

**Unlink a service from a service template**

There is no direct method to unlink a service from a template. Once a service is linked to a service template, it can only be unlinked from the template by doing one of the following:
- Deleting the service template
- Linking the service to a different service template
- Modifying the name of a linked KPI
- Modifying the base search of a linked KPI (or modifying any other settings in the Search and Calculate section, including enabling backfill)
- Deleting a linked KPI

Linked KPIs have a lock icon next to the name of the KPI in the KPI tab of the service definition.

You can link a service to a different service template from the Linked Services tab of the service template by selecting **Link to another Service Template**.

To enable backfill for a linked KPI in a service, you must delete the service, recreate it using the service template, and enable backfill for all KPIs in the Settings section of the Create Service dialog box.

## Clone or delete a service template

Cloning a service template creates an exact copy of it. However, the cloned template is not linked to the services that are linked to the original service template. Deleting a service template unlinks it from all of its linked services. You can choose to leave them unlinked or link them to another service template.

1. From the IT Service Intelligence main menu, click **Configure > Service Templates**.
2. In the Actions column of the service, click **Edit > Clone/Delete**.

To delete templates in bulk, select all the templates you want to delete and click **Bulk Action > Delete**.
Predictive Analytics

Predict and prevent outages with ITSI Predictive Analytics

ITSI Predictive Analytics uses machine learning algorithms to predict the health score value of a selected service. The models use historical service health score and KPI data to approximate what a service's health might look like in 30 minutes.

ITSI Predictive Analytics allows Splunk users of all skill levels to use machine learning technology. ITSI provides visualization tools that guide you through the process of creating machine learning models without having to learn complex machine learning algorithms and technology. Once your models are ready, ITSI makes it easy to obtain and use service health score predictions.

Use Predictive Analytics if you want to identify and fix service outages before they happen. By receiving a warning that your service is likely to degrade in the next 30 minutes, you can take steps to resolve the problem before it affects other areas of your system.

Use Predictive Analytics if:

- You've had unplanned outages in the past.
- You want to prevent future outages.
- You want to understand and identify patterns in your service.
- You want to understand how future outages can impact your business.
Set up Predictive Analytics in ITSI

Before you can predict service health scores with ITSI Predictive Analytics, you need to configure the Splunk Machine Learning Toolkit application and optionally set up permissions.

Enable Predictive Analytics

To use Predictive Analytics, you need to install the Splunk Machine Learning Toolkit (MLTK) and share the machine learning macros with all apps so ITSI can access them. To minimize memory and disk consumption, configure the Machine Learning Toolkit configuration file. This will allow the MLTK to handle more memory and events.

1. Install the Python for Scientific Computing add-on version 1.3 or later for your operating system:
   ♦ Mac
   ♦ Linux 64-bit
   ♦ Linux 32-bit
   ♦ Windows 64-bit

2. Install the Splunk Machine Learning Toolkit. Follow the steps in Install the Splunk Machine Learning Toolkit in the MLTK User Guide. For compatible MLTK versions, see ITSI compatibility with other apps and add-ons.

3. Give the MLTK app Global permissions:
   1. In ITSI, click App: IT Service Intelligence > Manage Apps.
   2. In the filter bar, enter Splunk Machine Learning Toolkit.
   3. Click Permissions.
   4. Ensure that All apps is selected.
   5. Click Save.

• (Optional) Configure the MLTK to handle more memory and events:

   1. Create a copy of mslsp1.conf in
      $$SPLUNK_HOME/etc/apps/Splunk_ML_Toolkit/local.
   2. Configure the following settings under the [default] stanza and in each algorithm-specific stanza:
### Setting Recommended value

<table>
<thead>
<tr>
<th>Setting</th>
<th>Recommended value</th>
</tr>
</thead>
<tbody>
<tr>
<td>max_inputs</td>
<td>1000000</td>
</tr>
<tr>
<td>max_memory_usage_mb</td>
<td>2000</td>
</tr>
<tr>
<td>max_model_size_mb</td>
<td>30</td>
</tr>
<tr>
<td>max_fit_time</td>
<td>2400</td>
</tr>
</tbody>
</table>

3. Save the file and restart Splunk software.

### Permissions requirements

The following table summarizes the ITSI roles and corresponding Predictive Analytics capabilities:

<table>
<thead>
<tr>
<th>Role</th>
<th>Capabilities</th>
</tr>
</thead>
</table>
| itoa_admin       | • Train a model  
                   • Test a model  
                   • Add a model to a glass table  
                   • Create alerts from a model  
                   • Delete a model |
| itoa_team_admin  | • Train a model (with write access to the service)  
                   • Test a model  
                   • Add a model to a glass table  
                   • Create alerts from a model  
                   • Delete a model |
| itoa_analyst     | • Read models (with read access to the service)  
                   • Test a model  
                   • Add a model to a glass table  
                   • Create alerts from a model |
| itoa_user        | • Read models (with read access to the service)  
                   • Test a model  
                   • Create alerts from a model |
See also

- Configure users and roles in ITSI
- Access Predictive Analytics in ITSI

Access Predictive Analytics in ITSI

ITSI Predictive Analytics is accessible through the service configuration workflow. When you want to create a model for a particular service, edit that service directly.

Prerequisites

You must have the itoa_admin or itoa_team_admin role to train and create a predictive model. After you create a model, open it in the Predictive Analytics dashboard to do root cause analysis.

Steps

1. In the ITSI menu bar, click Configure > Services.
2. Click the name of the service that you want to predict a health score for.
3. Click the Predictive Analytics tab.

See also

- Determine whether your service is a good fit for modeling in ITSI
- Train a predictive model in ITSI

Determine whether your service is a good fit for modeling in ITSI

ITSI provides two visualizations to help you decide whether your service is a good fit for predictive modeling. Experiment with different time periods and review the graphs to determine which time period most accurately represents your data. The key principle is to provide data that reflects what actually happens in your business scenario.
Service Health Score and KPIs over time

The Service Health Score and KPIs over time graph displays the values of service health scores and KPIs over a selected time period. Splunk machine learning algorithms are sensitive to outliers because those values affect statistical significance calculations. If you see unusual values or outliers in your data, confirm whether these data points are relevant and real. If the extreme data points are accurate, predictable, and reoccurring, then your service might be a good candidate for modeling.

The shape of this graph can also help you determine which algorithm to use. For example, if you have cyclical data, which consists of regular rises and falls, a more basic algorithm like linear regression is sufficient. If your data is random and complex, a more robust algorithm like random forest regressor is a better fit.

For example, the following graph has cyclical data:
Distribution of Service Health Score Values

The Distribution of Service Health Score Values graph is a histogram of service health score values over a selected time period. Each bar is a count of how many times your service hits that health score range. Use the graph to confirm that your data is relatively uniformly distributed (that is, the data is spread equally across the entire range). If the data is skewed, with most data points falling near one health score, Splunk machine learning algorithms could produce biased models.

Use the shape of this graph to determine where most of your service health score values fall and how they vary. For example, if most of your service health scores are in the 90-100 range but some are scattered in the lower ranges, this indicates that you've had several outages. This is a perfect use case for predictive modeling.
See also

- Train a predictive model in ITSI
- Test a predictive model in ITSI

Train a predictive model in ITSI

The process of training a machine learning model involves providing a machine learning algorithm with training data to learn from. The term "model" refers to the model artifact that is created by the training process. The learning algorithm finds patterns in the training data and produces a machine learning model that captures these patterns.

To train a model, you need to decide whether the data for the selected service is a good fit for predictive modeling. For more information, see Determine whether your service is a good fit for modeling in ITSI. If you decide to create a model, select the training inputs and train the model. After you train the model, you can save it into the service and create an alert for potential service degradation.

If you have a lot of data in the summary index, the process of training a model can take up to 30 minutes to complete. During this training period, do not navigate away from the page.

The following diagram shows a high-level workflow for training a model:
Check if service has “good” data for training.

I want to train a model.

Train

Select training inputs
To train a predictive model for a selected service, you must do the following:

1. Specify a time period.
2. Choose an algorithm type.
3. Choose a machine learning algorithm.
4. Split your data into training and test sets.

**Specify a time period**

The time period determines how far back ITSI looks when training a predictive model. The amount of data a predictive model needs depends on the complexity and shape of your data within the time period, and the complexity of the algorithm.

Consider the following guidelines when you choose a time period:

- Use at least 14 days of data. 30 days or more is recommended.
- In general, a model needs enough data to reasonably capture the relationships that exist among inputs (past KPI values and service health scores) and between inputs and outputs (future service health scores).
- To encapsulate as much variance in your data as possible, use as much data as you have available to train a model. It is best to operate under the assumption that the more data you provide, the better.

If you don't have enough data in the summary index to adequately train a model, consider backfilling the summary index with service health score data. For more information, see Backfill service health scores in ITSI.

To look more closely at the shape and complexity of your data, consult the following graphs:

- Service Health Score and KPIs Over Time
- Distribution of Service Health Score Values

**Choose an algorithm type**

There are two types of algorithms you can use to train predictive models in ITSI: regression and classification. Fundamentally, regression is about predicting a numerical service health score, and classification is about predicting a service health state.
**Regression algorithms**

Regression algorithms predict numeric values. For example, salary or age. In ITSI Predictive Analytics, regression algorithms predict an actual numeric health score value (for example, health score=89). Such models are useful for determining to what extent peripheral factors, such as historical KPI values, contribute to a particular metric result (service health score). After the regression model is computed, you can use these peripheral values to make a prediction on the metric result.

The following visualization illustrates a scatter plot of actual versus predicted results. The test data is plotted, and the yellow line indicates the best fit line for predicting server power consumption.

![Actual vs. Predicted Scatter Chart](image)

**Classification algorithms**

A classification algorithm predicts a category. For example, diabetic or not diabetic, rather than a discrete numeric value such as cholesterol levels. The algorithm learns the tendency for data to belong to one category or another based on related data. In ITSI Predictive Analytics, a classification algorithm uses the training data to predict a service health state (Normal, Medium, or Critical).

In short, classification classifies data and constructs a model based on the training set, and uses that model in classifying new data.

For example, the following classification table shows the actual state of a field versus the predicted state of the field. The yellow bar highlights an incorrect prediction.
Choose a machine learning algorithm

ITSI provides the following machine learning algorithms:

- Linear regression (Regression)
- Random forest regressor (Regression)
- Gradient boosting regressor (Regression)
- Logistic regression (Classification)

**Linear regression**

The linear regression algorithm creates a model for the relationship between multiple independent input variables (historical KPI and service health score values) and an output dependent variable (future service health score). The model remains linear in the sense that the output is a linear combination of the input variables. The algorithm learns by estimating the coefficient values in the test set using the data available in the training set.

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Useful when the relationship to be modeled is not extremely complex and if you don’t have a lot of data.</td>
<td>Tends to underperform when there are multiple or non-linear decision boundaries.</td>
</tr>
<tr>
<td>Simple to understand, which can be valuable for business decisions.</td>
<td>Sometimes too simple to capture complex relationships between variables.</td>
</tr>
</tbody>
</table>

**Random forest regressor**

The random forest regressor algorithm operates by constructing a multitude of decision trees during training and outputting the mean prediction (regression) of the individual trees. Random forests are a way of averaging multiple deep decision trees, trained on different parts of the same training set, with the goal of
reducing the variance of the prediction.

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Good at learning complex, highly non-linear relationships.</td>
<td>Can be prone to major overfitting.</td>
</tr>
<tr>
<td>Usually achieves high performance.</td>
<td>Slower and requires more memory.</td>
</tr>
</tbody>
</table>

**Gradient boosting regressor**

The gradient boosting regressor algorithm involves three elements: A loss function to optimize, a weak learner to make predictions, and an additive model to add weak learners to minimize the loss function. Decision trees are used as the weak learner. Trees are added to the model one at a time in an effort to correct or improve the final output of the model.

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usually achieves high performance.</td>
<td>A small change in the training data can create radical changes in the model.</td>
</tr>
<tr>
<td>Generally accurate even if the data is very complex or nonlinear in nature.</td>
<td>Can be prone to overfitting.</td>
</tr>
</tbody>
</table>

**Logistic regression**

The logistic regression algorithm is a classification algorithm used to assign observations to a discrete set of classes. For example, logistic regression predicts values like win or lose rather than the actual numeric score of a hockey game. In ITSI Predictive Analytics, the logistic regression algorithm predicts whether a service's health score will be Normal, Medium, or Critical in the next 30 minutes. Unlike linear regression, which outputs continuous numeric values, logistic regression transforms its output to return a probability value, which can be mapped to two or more discrete classes.

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Performs well when the input data is relatively linear.</td>
<td>Tends to underperform when there are multiple or non-linear decision boundaries.</td>
</tr>
<tr>
<td>Avoids overfitting.</td>
<td>Sometimes too simple to capture complex relationships between variables.</td>
</tr>
</tbody>
</table>

Because classification divides your data into separate categories, your data must be highly variable for logistic regression to work. If your data is fairly stable and usually hovers around the same health score, logistic regression cannot divide it.
into three distinct categories.

**Split your data into training and test sets**

Think of your data as a limited resource. You can spend some of this resource to train your model, and some of it to test your model. But you can't reuse the same data for both. If you test your model on the same data you used to train it, your model could be overfit without your knowledge. It is best if a model is judged on its ability to predict new, unseen data. Therefore, ITSI lets you create separate training and testing subsets of your dataset.

A common machine learning strategy is to take all available data and split it into training and testing subsets, usually with a ratio of 70-80 percent for training and 20-30 percent for testing. ITSI uses the training subset to train and predict patterns in the data. The train partition has a single and essential role: it provides the raw material from which the predictive model is generated. ITSI uses the test data to evaluate the performance of the trained model.

For example, if the training data predicts a health score of 60, and the test data shows a score of 62, the model has very high performance. ITSI evaluates predictive performance by comparing predictions on the test data set with actual values using a variety of metrics. Usually, you use the model that performed best on the test subset (the "recommended" model) to make predictions on future health scores.

By default, ITSI selects a random 70 percent of the source data for training and uses the other 30 percent for testing. Use the slider in the training section to specify a custom split ratio.

Consider the following guidelines when splitting your data:

- Always split your data before training a model. This is the best way to get reliable estimates of a model's performance.
- After splitting your data, don't change the "Test Period" until you choose your final model. The test period is meant for retraining purposes.
- When dealing with large datasets (for example, 1 million data points), a
larger split of 90:10 is a good choice.
- With a smaller data set (for example, 10,000 data points), a normal split of 70:30 is sufficient.
- In most cases, the more training data you have, the better the result.

**Test a predictive model in ITSI**

Always evaluate a model to determine if it will do a good job predicting future health scores. When you assess the quality of a predictive model, you determine what will happen if you use that model to make predictions. That is, whether the predictions will be close to the eventual outcomes.

ITSI provides several industry-standard metrics and insights to review the predictive accuracy of your model. Although ITSI provides a recommendation based on the best-performing algorithm, it is important to review the visualizations to decide if your model is performing well enough to match your business requirements.

Select a model to test under **Test a Model**. A checkmark indicates which regression model had the best overall performance. For more information about the difference between regression and classification algorithms, see **Choose an algorithm type** in this manual.

Use these questions to help you choose the best model:

- Which model had the best performance on the test set? ("recommended" model)
- Does the model perform well across various performance metrics?

Do not change the Test Period unless you want to test on all of the available data. Leaving the data in separate train and test partitions, as configured in the training/test split, provides an honest assessment of the model's performance.

After you select the best model for your needs, click **Save** to save the model into your service. You can now use the model to perform root cause analysis in the Predictive Analytics dashboard.

It is advised to only save one service at a time when creating models. Saving multiple models in separate windows might cause an error.
Test a regression model

Use the following metrics to test and evaluate a regression model:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R²</td>
<td>R² represents how well the model explains the variability of the result. 100 percent (a value of 1) means the model fits perfectly. The closer the value is to 1, the better the result.</td>
</tr>
<tr>
<td>RMSE</td>
<td>Root Mean Squared Error (RMSE) is a measure of the difference between values predicted by the model and the values observed. RMSE explains the variability of the result, which is essentially the standard deviation of the residual. This value gives you an idea of how close or far the model is from completely accurate predictions. These values only make sense within one dataset. Do not compare them across datasets.</td>
</tr>
<tr>
<td>Actual vs. Predicted Service Health Score</td>
<td>A sequential overlay that compares the actual service health score to what the model predicted the number will be 30 minutes into the future.</td>
</tr>
<tr>
<td>Residual Error Histogram</td>
<td>A histogram of the residual error of each service health score during the test period. The residual error is the difference between the observed service health score and the estimated score that the model predicted. A graph that is normally distributed with values closer to 0 is most accurate.</td>
</tr>
</tbody>
</table>

Test a classification model

Because classification divides your data into separate categories, your data must be highly variable for logistic regression to work. If your data is fairly stable and usually hovers around the same health score, logistic regression cannot divide it into three distinct categories.

Use the following metrics to test and evaluate a classification model:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision</td>
<td>The percentage of time a model identifies only the relevant data points. For example, of all predicted Severe data points, Precision measures how many of them are actually Severe. Precision is a good metric to use when the cost of a false positive is high. A false positive means that a health score that is Normal was actually predicted to be Severe. In this case, a</td>
</tr>
</tbody>
</table>
user might waste important time investigating a predicted outage that never occurs.

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recall</td>
<td>The percentage of time a model predicts the correct severity. Recall is a good metric to use when there is a high cost associated with a false negative value. For example, if a Severe health score is predicted as Normal, your model might not detect a potential outage, and the consequence can be bad for your business.</td>
</tr>
<tr>
<td>Accuracy</td>
<td>The overall percentage of correct predictions from all predictions made. Sometimes it is desirable to select a model with a lower accuracy because it has a greater overall predictive power. In these cases it is more important that Precision, Recall, or F1 be high.</td>
</tr>
<tr>
<td>F1</td>
<td>The weighted average of Precision and Recall, based on a scale from zero to one. The closer the statistic is to one, the better the fit of the model. The F1 score is a better measure to use if you need to seek a balance between Precision and Recall.</td>
</tr>
<tr>
<td>Classification Results (Confusion Matrix)</td>
<td>The number of actual results against predicted results. The actual severities form the columns, and the predicted severities form the rows. The intersection of the rows and columns show the outcomes. The main diagonal (which generally has larger numbers) gives the correct predictions. That is, the cases where the actual values and the model predictions are the same. It is best if the diagonal numbers are closer to 100 percent of the total values, while the other numbers are closer to 0.</td>
</tr>
</tbody>
</table>

See also

- Train a predictive model in ITSI
- Predictive Analytics dashboard

Create an alert for potential service degradation in ITSI

The predictive models in ITSI can detect when a service's health is about to decline. Create an alert from a model which will generate an event in Episode
Review notifying you when the service health score is predicted to reach a configured threshold.

**Prerequisites**

- To create an alert from a predictive model, a trained model must be saved in the service definition. For more information, see [Train a predictive model in ITSI](#).
- Make sure you're viewing the Predictive Analytics tab from the service definition.

**Steps**

1. From the Predictive Analytics tab, select the model under **Test a Model**.
2. Click the bell icon ( ) in the Worst Case Service Health Score panel.
3. Configure the following fields in the Create Correlation Search box:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Name</td>
<td>The name of the correlation search.</td>
</tr>
<tr>
<td>Create a notable event when predicted health score is</td>
<td>The threshold values used by the search to trigger an alert. When the service's health score drops below or between the values or severities you specify, ITSI generates an event in Episode Review.</td>
</tr>
<tr>
<td>Notable Event Title</td>
<td>The title of the notable event generated in Episode Review.</td>
</tr>
<tr>
<td>Run every</td>
<td>How often the correlation search runs.</td>
</tr>
<tr>
<td>Severity</td>
<td>The initial severity of the notable event. This severity is not tied to the severity of the prediction itself. Rather, it represents the importance of the prediction. For example, the predicted health score might be 60, which is technically in the Medium range for ITSI. However, if this service's health is very important to you, you might make the Severity of the notable event High so that it will be prioritized and investigated sooner.</td>
</tr>
</tbody>
</table>

4. Click **Create**.

   If the service's health score drops to the value or severity you configured, ITSI generates a notable event in Episode Review. Click the drilldown link in the event to open the Predictive Analytics dashboard and perform more granular root cause analysis.
Manage alerts

Alerts are stored with other correlation searches in ITSI. To delete or disable a Predictive Analytics alert, click **Configure > Correlation Searches** from the top menu bar. You can edit the correlation search to change fields such as Time Range, Severity, and Description.

See also:

- Create correlation searches in ITSI

Add a predictive model to a glass table in ITSI

You can add predictive models to glass tables as ad hoc search widgets. This lets you actively monitor service health and troubleshoot imminent issues before they impact your services.

Ad hoc searches are not optimized because each widget runs its own individual search. Thus, the loading time for your glass table visualization is proportional to the number of predictive model widgets you add.

Prerequisite

- To create a glass table widget from a predictive model, you must have a trained model that is saved into the service definition. For more information, see Train a predictive model in ITSI.
- Make sure you're on the Predictive Analytics tab within the service.

Steps

1. On the Predictive Analytics tab, select the model under **Test a Model**.
2. Click the magnifying glass in the Predicted Average Case Service Health Score or Predicted Worst Case Service Health Score panel to open the predictions in the Search app.

   The search is the same whether you select average or worst case.
3. Copy the search string.
4. Open your glass table in Edit mode.
5. Drag **Ad hoc Search** from the Services panel onto the canvas.
6. In the Configurations panel, paste the search string into the **Search** box.
7. In the time range picker, select the end time for your ad hoc search.
8. Expand **Earliest Time** and select the start time for your ad hoc search relative to the end time in the time range picker. This determines the time range over which the ad hoc search applies.

9. In **Threshold Field**, type `next30m_avg_hs` to display the average prediction, or `next30m_min_hs` to display the worst-case prediction.

10. Enable **Thresholds** to display thresholds for the ad hoc search widget:
    1. For Thresholds, click **On**.
    2. Click **Edit** and configure the thresholds for the service health score prediction.
    3. When finished, click **Done**.

11. (Optional) Add a drilldown to the Predictive Analytics dashboard.
    1. For **Drilldown**, click **On**.
    2. Click **Default**, and select **Custom URL**.
    3. In a separate ITSI window, navigate to **Dashboards > Predictive Analytics**.
    4. Select the service and corresponding model to display the health score prediction.
    5. Copy the URL and paste it into the URL field in the glass table.
    6. Edit the URL from `auto_load=false` to `auto_load=true` to automatically load all of the dashboard panels.

12. Select a viz type for your ad hoc search widget. You cannot use the sparkline or trending value viz types because the prediction is a static value.

13. Click **Update** to update the widget to the new visualization and display your search results over the specified time range.

14. Click **Save**.

For more information, see Configure ad hoc search widgets in the *ITSI User Manual*.

---

**Retrain a predictive model in ITSI**

For a model to accurately predict health scores, the data it's making predictions on must have a similar distribution as the data on which the model was trained. Because data distributions are expected to drift over time, deploying a model is not a one-time exercise, but a continuous process.

It is good practice to continuously monitor your incoming data (historical KPI and service health score values) and retrain a model on newer data if KPIs or entities are added, removed, or changed. For example, if you add an Oracle database to a service, it is best practice to retrain the service’s model because the new architecture will create new KPI relationships.
If monitoring your services for changes is too time consuming, a simpler strategy is to train the model periodically. For example, to capture changes to KPIs or service architecture, you might retrain a model every 10 days.

Retrain a service's model in the following situations:

- You added a new KPI or entity to the service.
- You removed or changed a KPI or entity in the service.
- You restored your ITSI configuration (ITSI does not restore MLTK lookup files).
- You notice that the model's performance is starting to degrade.

Before you retrain a model, test it on recent data to evaluate whether it needs to be retrained.

**Prerequisites**

- To retrain a model, the model must be saved in the service definition. For more information, see [Train a predictive model in ITSI](#).
- Make sure you're viewing the Predictive Analytics tab from the service definition.

**Steps**

1. Test the model on recent data:
   1. From the Predictive Analytics tab of the selected service, navigate to the **Test a Model** section.
   2. Change the test period to a recent time range. Changing the time period retests the model on a recent set of data to determine if it needs to be retrained. You must test on at least 90 minutes of data.

   The appropriate test period varies based on your specific data. For example, if a new KPI was added yesterday, test the model on the last 24 hours. If an outage occurred last week, test it on the last seven days.

2. Select the model in the Regression Models or Classification Models table to populate the model's metrics.
3. Analyze the model's metrics. If the metric values have dropped to unacceptable levels for your business, consider retraining the model.

2. Retrain the model on new data:
1. Select the same algorithm and algorithm type as you used to train the model. You can modify the time period and training/test split.
2. Click **Train**. The existing model is replaced by the retrained model.
3. Reevaluate the model's metrics to ensure that they are at acceptable levels. For information about evaluating models, see Test a predictive model in ITSI in this manual.
4. Click **Save** to save the retrained model into the service definition.

The following diagram illustrates the workflow for retraining a model:

**Delete a predictive model in ITSI**

Every time you create a model, it is added to a CSV lookup in Splunk web. CSV lookups are file-based lookups represented by a CSV file. Access, manage, and delete predictive models through Lookups.

1. In ITSI, click **Settings > Lookups**.
2. Select **Lookup table files**.
3. Locate the model you want to delete and click **Delete** in the Actions column.
   
   Services are listed according to service ID. Delete all three models associated with each algorithm, with the following suffixes: `_avg`, `_ss`, and `_worst`.

For information about managing model permissions, see Managing model permissions within Lookups.
Predictive Analytics performance considerations in ITSI

While training and testing models in ITSI, there are several performance considerations to take into account. This topic provides guidance for choosing services to model, selecting training inputs, and retraining models.

While it’s impossible to provide prescriptive advice for maximizing performance in every situation, the following observations and tips can help you tune and improve performance in your unique environment:

1. **Avoid creating models for services that contain more than approximately 20 KPIs and 50 entities.** The training time for a model depends on three factors: the number of KPIs in the service, the number of entities in the service, and the frequency of KPI searches. For a service with 20 total KPIs, 50 total entities, and 1-minute KPI searches, the average training time is 5 minutes. Scaling any of these three factors increases the training time.

2. **Do not create models for more than 75 total services.** Management of models is manual and can be difficult if you create too many.

3. **Configure the MLTK to handle more memory and events.** For more information, see Set up Predictive Analytics in ITSI.

4. **Use at least 14 days worth of data to train your model.** The training period is determined by the time period you specify before training a model. 30 days or more is recommended. In general, it is best to use as much data as you have available to train a model.

5. **Base your training/test split ratio on the size of your dataset.** Use a large split when dealing with large datasets (for example, 1 million data points). Use a smaller split when dealing with smaller datasets (for example, 10,000 data points). For more information, see Split your data into training and test sets.

6. **Do not change the Test Period until you select a final model for the service.** Leaving the data in separate train and test partitions, as configured in the training/test split, provides an honest assessment of the model's performance.

7. **Retrain a service’s model if KPIs or entities are added, removed, or changed.** Changes in service architecture can cause changes in KPI behavior and service health score trends. For more information, see Retrain a predictive model in ITSI.

8. **Before retraining a model, test it on at least 90 minutes of data.** If you test on fewer than 90 minutes, the results could be inaccurate or incomplete.
9. **Do not use the training search as a scheduled search.** Predictive Analytics models do not require repetitive retraining, such as retraining every night. Retraining them too often can cause scale implications. Training is specifically designed to be an intermittent expense.

**More performance help**

If you experience performance issues, or want to receive feedback tailored to your setup, you have the following options:

- Post a request to the community on Splunk Answers.
- Contact Splunk Support.

**ITSI Predictive Analytics use case**

With ITSI Predictive Analytics, you can build and train predictive models and use them to create alerts. This example demonstrates how to use ITSI Predictive Analytics to build a machine learning model, and use the model to generate predictions that you can use to make business decisions.

**Scenario**

You are an IT operations admin for the Middleware team. The Middleware service has experienced several costly outages in the past. To predict and avoid future outages, you want to create a machine learning model of the Middleware service using ITSI's Predictive Analytics capability.

**Use case overview**

This use case includes the following high-level tasks:

1. Determine if the service is a good fit for modeling
2. Train a model
3. Test the model
4. Create an alert from the model
5. Perform root cause analysis using the Predictive Analytics dashboard
6. Retrain the model on new data
Determine if the service is a good fit for modeling

Before you create a predictive model for the Middleware service, you want to make sure that the service is suitable for predictive modeling. You set the time period on the Predictive Analytics tab to Last 14 days so you can get an idea of how the Middleware service's health scores have varied over the last two weeks.

You look at the graph of service health scores and KPIs over time and see that the data is relatively cyclical with no obvious outliers.

You consult the histogram of service health scores and see that the distribution is fairly uniform (the data is spread evenly across the range of health scores). With this even distribution, ITSI's machine learning models are less likely to produce biased results.

Because the Middleware service data contains no outliers and is evenly distributed, you determine that the Middleware service is a good fit for predictive modeling.

Train a model

Now that you've decided to model the Middleware service, it's time to train a predictive model. You go to the Middleware service's Predictive Analytics tab to configure the training inputs.

Time period

You want to provide the model with enough data to capture the relationships that exist among the Middleware service's past KPI values and service health scores. Your last outage occurred two months ago, and you want to provide that data to the model so that it can be trained on the difference between normal and abnormal data. You decide to use the Last 90 days of data.

See also:

- Specify a time period

Algorithm type

There are two types of algorithms you can use to train predictive models in ITSI: regression and classification. Regression algorithms predict a numerical service health score, and classification predicts a service health state.
Regression is best when there is a pattern for health scores in the past, and classification when there is no pattern but rather random drops. Because there is a cyclical pattern to the Middleware service's historical health scores, you decide to go with Regression. When monitoring the Middleware service, you prefer that the health score does not drop below 75.

See also:

- Choose an algorithm type

**Algorithm**

Because you chose regression, you have three algorithms to choose from: linear regression, random forest regressor, and gradient boosting regressor. You already determined that the Middleware service data is fairly cyclical, with regular rises and falls in service health score values. Because the relationships to be modeled are relatively simple, you decide to go with Linear Regression.

See also:

- Choose a machine learning algorithm

**Split for training/test**

A common machine learning strategy is to take all available data and split it into training and testing subsets. The train partition provides the raw data from which the predictive model is generated. The test set is used to evaluate the performance of the trained model.

You know that a larger split works well for large datasets, and a more normal split (like 70/30) works best for small datasets. Your dataset of 90 days is fairly large, especially since the Middleware service contains 8 KPIs and 22 entities. You decide to increase the train/test split to 80/20. This split trains the model on 80% of the data, and uses the remaining 20% to test and evaluate it.

See also:

- Split your data into training and test sets

After everything's configured, your training inputs look like this:
Review the model's predictive performance

It's always a good idea to evaluate a model to determine if it will do a good job predicting future health scores. You want to make sure that the predictions the model generates will be close to the eventual outcomes.

After you click **Train**, the model is created in the Test a Model section.

You select the **LinearRegression** model, the "Recommended" model, to generate the results. The recommended model is the one that had the best performance on the test set. If you don't have a data science or machine learning background and are confused about which model to choose, it is best to choose the recommended model.

ITSI provides the following industry-standard metrics and insights to summarize the predictive accuracy of your model:
$R^2 = 0.96$
You make the following observations about the test results:

- The $R^2$ of 0.96 is very high on a scale of 0 to 1.
- The RMSE of 7.24 is relatively small.
- On the graph of actual versus predicted health scores, most of the points fall close to or exactly on the line. This suggests a large number of correct predictions, which means the model has high performance.
- The residual error histogram has a normal (bell-shaped) distribution with most values close to 0.

Your observations indicate that the linear regression model performs well across various performance metrics. You decide to go with this model, and you click **Save** to save it into the service definition.

**See also:**

- Test a predictive model in ITSI

**Set a score threshold and create an alert**

Now that you’ve saved the model into the service, you want to create an alert so you can be notified if the health score of the Middleware service is predicted to reach a certain worst-case level in the future.

You click the bell icon (ưởng) in the Worst Case Service Health Score panel to open the correlation search modal. You want ITSI to generate a notable event in Episode Review the next time the Middleware service’s health is expected to degrade.

You configure the following inputs:

```
Create Correlation Search

<table>
<thead>
<tr>
<th>Input</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Name</td>
<td>Predicted worst case health score for Middleware service</td>
</tr>
<tr>
<td>Create a notable event when predicted health score is &lt; 75</td>
<td>75</td>
</tr>
<tr>
<td>Notable Event Title</td>
<td>Middleware’s health score is predicted to hit or drop below 75 in 5 to 30 minutes</td>
</tr>
<tr>
<td>Run Every</td>
<td>5 minutes</td>
</tr>
<tr>
<td>Severity</td>
<td>Medium</td>
</tr>
</tbody>
</table>
```

130
Because you want the Middleware service's health score to stay between 75 and 100, you decide to generate an alert when the predicted health score is predicted to be 75 or less.

You configure the initial severity of the notable event to be Medium because a health score of 75 doesn't necessarily indicate a severe outage. You might create another correlation search that generates a Critical event if the health score drops below 30, as this is a more critical situation.

See also:

• Create an alert for potential service degradation in ITSI

Use the model to generate predictions and find root cause

Two days later, one of your IT operations analysts is monitoring Episode Review and sees the following notable event:
The event details indicate that the Middleware service is predicted to degrade to an unacceptable level within the next 30 minutes.

The analyst clicks the **Predictive Analytics Middleware Dashboard** drilldown link. This high-level dashboard lets analysts perform root cause analysis by viewing the top five KPIs contributing to a potential outage and how those KPIs are likely to change in the next 30 minutes.

The analyst sees the following information in the dashboard:

**Predicted Service Health Score in 30 Minutes**

63.48
Along with the predicted health score in 30 minutes, ITSI calculates the top 5 KPIs that are likely contributing to the degraded health score. The analyst determines that the Middleware service is likely to degrade because of an increased amount of 5xx errors, which is the top offending KPI. The analyst opens a ticket with the Middleware team to address the 5xx error count before it becomes a problem.

See also:

- Predictive Analytics dashboard

**Retrain the model on new data**

A month after creating the initial model for the Middleware service, you make a change to one of the KPIs in the service. It is good practice to continuously monitor your incoming data (historical KPI and service health score values) and retrain a model on newer data if KPIs or entities are added, removed, or changed.

You decide to test the existing model on recent data to evaluate whether it needs to be retrained.

On the Middleware service's Predictive Analytics tab, you navigate to the **Test a Model** section where the current model is saved. You change the Test Period to **Last 90 days** and select the **LinearRegression** model. This tests the existing model on the last 90 days of data.

The best metrics to review when retesting a model are $R^2$ and RMSE because they allow you to make a direct numerical comparison to the original values.

You see the following results:
Test a Model

Test Period

Last 90 days

All data within the selected time period will be used for testing.

Regression Models

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>LinearRegression</td>
<td>✓</td>
</tr>
</tbody>
</table>

R^2

0.41
The test results indicate that $R^2$, a measure of how well the model fits, has decreased from 0.96 to 0.41. RMSE, which should be relatively small, has increased from 7.24 to 28.70. These metrics are unacceptably low, so you decide to retrain the model.

You select the same training inputs as before and click **Train**. Training with the same algorithm replaces the existing model with the retrained model.

After the model is trained, you consult the **Test a Model** section to review the new model's predictive performance. The test results display the following metrics:

$$R^2 = 0.97$$
The $R^2$ value has increased significantly and RMSE has dropped significantly. The values are close to what they were when you originally trained the model. The model's performance has increased after you retrained it on recent data, accounting for the recent change to the Middleware service's KPI. You are satisfied with the new model's performance and click **Save** to save it into the service definition.

**See also:**

- Retrain a predictive model in ITSI
**Event Analytics**

**About ITSI Event Analytics**

Splunk IT Service Intelligence (ITSI) Event Analytics ingests events from multiple data sources and creates and manages notable events. A notable event is an enriched event containing metadata to help you investigate issues in your IT environment.

Event Analytics is equipped to handle huge numbers of events coming in at once. Because these events might be related to each other, they must be grouped together so you can identify the underlying problem. Event Analytics provides a simple way to deal with this huge volume and variety of events.

ITSI automatically groups notable events into episodes and organizes them in Episode Review. An episode is a collection of notable events that are grouped together based on predefined rules. You can manage the properties of episodes and determine which services are impacted by each. You can also browse the history of similar episodes to find out what worked to resolve them, and configure automated actions to take on certain types of episodes.

The Event Analytics SDK is shipped with ITSI to help you manage episodes and create custom episode actions programmatically.

**Event Analytics workflow**

ITSI Event Analytics is designed to make event storms manageable and actionable. After data is ingested into ITSI from multiple data sources, events proceed through the following workflow:
**Step 1: Configure a correlation search**

The data itself comes from Splunk indexes, but ITSI only focuses on a subset of all Splunk Enterprise data. This subset is generated by correlation searches. A correlation searches is a specific type of saved search that generates notable events from the search results. For more information, see Correlation search overview for ITSI.

**Step 2: Configure an aggregation policy**

Once notable events start coming in, they need to be organized so you can start gaining value from them. Configure an aggregation policy to define which notable events are related to each other and group them into episodes. An episode contains a chronological sequence of events that tells the story of a problem or issue. In the backend, a component called the Rules Engine executes the aggregation policies you configure. For more information, see Notable event aggregation policies overview for ITSI.

**Step 3: Configure actions**

You can run actions on episodes either automatically or manually. Some actions, like sending an email or pinging a host, are shipped with ITSI. You can also create tickets in external ticketing systems like ServiceNow, Remedy, or VictorOps. Finally, actions can also be modular alerts that are shipped with Splunk add-ons or apps, or custom actions that you configure.

**Customize Episode Review in ITSI**

As a Splunk ITSI administrator, you can customize the way that analysts view and interact with events and episodes in Episode Review.

**Modify which events analysts can see**

By default, ITSI service-level permissions apply to episodes in Episode Review. This means that analysts can only see events from services for which they have read permission. If an event is not associated with a particular service (none of the fields in the event contains service information) then all users can view the event.

You can disable service-level permissions for Episode Review using the itsi_team.conf file.
Prerequisites

- Only users with file system access, such as system administrators, can disable service-level permissions for Episode Review.
- Review the steps in How to edit a configuration file in the Admin Manual.

Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location.

Steps

1. Open or create an itsi_team.conf file at $SPLUNK_HOME/etc/apps/SA-ITOA/local.
2. Under the [notable_event_review_security_group] stanza, set disabled to 1

If service-level permissions are disabled for Episode Review, all ITSI users can see all notable events, regardless of which service they are associated with. However, service information for services that a user does not have read access to are not displayed for notable events. For information about service-level permissions, see Overview of service-level permissions in ITSI.

Modify analyst permissions

Configure read and write permissions on a saved view of Episode Review to restrict permissions for certain roles. By default, read and write permissions are granted to Everyone (all roles) for a newly created view of Episode Review.

Prerequisites

You must have the itoa_admin or itoa_team_admin role, or be assigned the configure_perms capability, to set permissions on a saved Episode Review. For more information, see Configure users and roles in ITSI.

Steps

1. Within Episode Review, click the side arrow to show alternate views.
2. Click **Full Lister Page**.
3. On the Episode Review lister page, click **Edit > Permissions** on the saved view you want to edit.
4. Allow or prevent analysts from reading or writing to the saved Episode Review. Everyone is granted read/write access by default.
5. Click **Save**.

**Change Episode Review columns**

You can change the columns displayed in a saved Episode Review.

1. Click the gear icon to open the View Settings modal.
2. Use the **Columns Shown** section to edit, remove, or change the order of the available columns.
3. Add custom columns by selecting **Add Column**. For example, choose **All Tickets** to display a column with any external tickets linked to the episode.
4. Click **Done**.

**Set up custom episode actions in ITSI**

Unique use cases can require custom alerting functionality and integration. In addition to the default actions you can take on an episode, ITSI also lets you define custom alert actions in `notable_event_actions.conf`.

**Prerequisites**

◊ Only users with file system access, such as system administrators, can `<describe the customization>`.
◊ Review the steps in How to edit a configuration file in the *Admin Manual*.

Never change or copy the configuration files in the `default` directory. The files in the `default` directory must remain intact and in their original location. Make changes to the files in the `local` directory.

**Steps**

1. Open or create a local version of `notable_event_actions.conf` at `SPLUNK_HOME/etc/apps/SA-ITOA/local`.
2. Add a stanza for the action you want to perform. For example:

   ```
   [itsi_sample_event_action_ping]
   ```
3. Set `disabled = 0` to enable the custom action. For example:

```
[itsei_sample_event_action_ping]
disabled = 0
```

For an example configuration, see `notable_event_actions.conf.example`.

Setting up custom alert actions via `notable_event_actions.conf` only allows for a one-way integration. The episode will not contain a drilldown link to the action that was performed.

**Normalize event fields in ITSI**

Normalizing event fields lets you search similar alerts across multiple alert sources much more easily. It also standardizes methods for "grooming" alerts, regardless of their source.

**Normalize entity fields**

Add a new alias field called `entity_name` to every entity which might be used as the Entity Lookup field in a notable event correlation search. As a best practice, add `entity_name` to each entity as an alias containing the title of the entity.

1. Click **Configure > Entities**.
2. Click **Create Entity > Import from Search**.
3. Enter the following ad-hoc search:

   ```
   | inputlookup itsi_entities | eval entity_name=title
   ```
4. Click **Next**.
5. For the `entity_name` row, change the Import Column As field to **Entity Title**. Leave all others as **Do Not Import**.
6. Make sure Conflict Resolution is set to **Update Existing Entities**.
7. Click **Import**.

After the import completes, click **View All Entities**, then select any entity. It should have an alias field `entity_name` which contains the name of the entity itself. This field can be used for all notable event correlation searches as the Entity Lookup Field.
Manage notable events in ITSI

Splunk IT Service Intelligence (ITSI) implements custom indexes for notable event storage. In a single instance deployment, the installation of ITSI creates the indexes in $SPLUNK_HOME/var/lib/splunk.

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>itsi_tracked_alerts</td>
<td>Stores active raw notable event data.</td>
</tr>
<tr>
<td>itsi_notable_audit</td>
<td>Stores all audit events for episodes, including actions, comments, status change, and owner change.</td>
</tr>
<tr>
<td>itsi_grouped_alerts</td>
<td>Stores active episode data.</td>
</tr>
<tr>
<td>itsi_notable_archive</td>
<td>Stores episode tags that have been moved from the KV store after a default 6 month retention period, which begins when you close an episode in the UI. Moving data from the KV store removes extraneous data and helps improve performance.</td>
</tr>
</tbody>
</table>

ITSI uses an indexed real-time search to retrieve notable events from the Splunk platform. Indexed real-time searches have a delay of about 90 seconds before events get processed. Using concurrent real-time search instead of indexed real-time search is not supported for the itsi_event_grouping search because it significantly impacts system performance.

Set the notable event retention policy

In addition to the indexes listed above, ITSI stores the status of notable events and episodes in the KV store collections called itsi_notable_<object type>. By default, notable event metadata is archived after 6 months to keep the KV store from growing too large. If you have a large number of events, use the ITSI Health Check dashboard to check the collection sizes on disk and decide if you need to change the retention policy.

You can tune the retention policy for notable event metadata using an ITSI configuration file. The retention policy determines how long notable event metadata remains in the KV store before it is moved to itsi_notable_archive. Retention policies are based on the mod_time (modify time), not the tag creation time.
Prerequisites

- Only users with file system access, such as system administrators, can set the notable event retention policy.
- Review the steps in How to edit a configuration file in the Admin Manual.

Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location.

Steps

1. Open or create a local itsi_notable_event_retention.conf file in $SPLUNK_HOME/etc/apps/SA-ITOA/local/
2. To set the retention time for all object types, reduce the retentionTimeInSec in the [default] stanza. To individually set retention times for specific object types, add the retentionTimeInSec setting to individual stanzas as needed and reduce the retention time there. The settings in individual stanzas override what’s set in the [default] stanza.

```bash
# default retention policy is 6 months
retentionTimeInSec = 15768000
retentionObjectCount = 50000
disabled = 1

[itsi_notable_event_tag]
# Check retention policy against mod_time (modify time of tags) and move tags to index once they meet the condition
disabled = 0
object_type = notable_event_tag

[itsi_notable_event_ticketing]
# Check retention policy against mod_time (modify time of ticket) and move ticket to index once they meet the condition
disabled = 0
object_type = external_ticket

[itsi_notable_group_user]
# Default is one year
retentionTimeInSec = 31536000
retentionObjectCount = 50000
disabled = 0
object_type = notable_event_group

[itsi_notable_group_system]
# Default is one year
retentionTimeInSec = 31536000
retentionObjectCount = 50000
```
disabled = 0
object_type = notable_group_system

Backfill notable events into episodes

ITSI uses the `itsi_event_grouping` search command to aggregate notable events into episodes. If the search is disabled, either during a restart of Splunk Enterprise or manually by a user, ITSI does not group notable events into episodes.

When the `itsi_event_grouping` search is re-enabled, ITSI looks through notable events that were missed while the search was disabled and backfills them accordingly into episodes.

The default look-back time for missed events is 24 hours. If you want to change the look back time, modify the `group_restore_lookback_time` field in the `itsi_rules_engine.properties` file as follows.

Prerequisites

- Only users with file system access, such as system administrators, can modify the look-back time for missed events using a properties file.
- Review the steps in How to edit a configuration file in the Admin Manual.

Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location.

Steps

1. Open or create a local copy of the `itsi_rules_engine.properties` file at `$SPLUNK_HOME/etc/apps/SA-ITOA/local/`
2. Add the following setting to the file: `group_restore_lookback_time = <number of hours>`.

   For example, to look back two days, add the following setting:

   ```
   group_restore_lookback_time = 48
   ```

Clear all notable events

To permanently delete indexed notable events, use the CLI `clean` command. This command completely deletes the data in one or all indexes or KV store collections, depending on whether you provide an `<index_name>` or `<collection>` argument. For more information, see How to use the clean command in the
Managing Indexers and Clusters of Indexers manual.

The clean command does not work on indexer clusters unless you run it separately on each indexer.

1. In the CLI, to stop Splunk Enterprise type $SPLUNK_HOME/bin/splunk stop
2. On each indexer, run the following commands to clear the indexes:
   
   $SPLUNK_HOME/bin/splunk clean eventdata -index itsi_tracked_alerts;
   $SPLUNK_HOME/bin/splunk clean eventdata -index itsi_notable_audit;
   $SPLUNK_HOME/bin/splunk clean eventdata -index itsi_notable_archive;
   $SPLUNK_HOME/bin/splunk clean eventdata -index itsi_grouped_alerts
3. On a single search head, run the following commands to clear the KV store collections:
   
   $SPLUNK_HOME/bin/splunk clean kvstore -app SA-ITOA -collection itsi_notable_group_system;
   $SPLUNK_HOME/bin/splunk clean kvstore -app SA-ITOA -collection itsi_notable_group_user;
   $SPLUNK_HOME/bin/splunk clean kvstore -app SA-ITOA -collection itsi_notable_event_tag;
   $SPLUNK_HOME/bin/splunk clean kvstore -app SA-ITOA -collection itsi_notable_event_comment;
   $SPLUNK_HOME/bin/splunk clean kvstore -app SA-ITOA -collection itsi_notable_event_group;
   $SPLUNK_HOME/bin/splunk clean kvstore -app SA-ITOA -collection itsi_notable_event_actions_queue;
   $SPLUNK_HOME/bin/splunk clean kvstore -app SA-ITOA -collection itsi_temp_batch_claimed_action_queue;
   $SPLUNK_HOME/bin/splunk clean kvstore -app SA-ITOA -collection itsi_notable_event_ticketing
4. To start Splunk Enterprise type $SPLUNK_HOME/bin/splunk start

Tune notable event grouping in ITSI

Notable event aggregation polices group notable events to organize them in Episode Review. ITSI provides a file called itsi_rules_engine.properties, located at $SPLUNK_HOME/etc/apps/SA-ITOA/default/, where you can tune and customize notable event grouping settings.

Prerequisites
Only users with file system access, such as system administrators, can tune notable event grouping using a configuration file. Review the steps in How to edit a configuration file in the Admin Manual.

Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location.

Steps

1. Open or create a local itsi_rules_engine.properties file at $SPLUNK_HOME/etc/apps/SA-ITOA/local.

2. Modify the following settings as necessary to improve notable event grouping on your deployment.

```properties
# The period, in seconds, at which to fetch aggregation policies from the KV store.
policy_fetch_period = 45

# The HTTP token name.
token_name = itsi_group_alerts_token

# The HTTP sync token name.
# NOTE: If the sync token name and the HTTP token name are the same, a token
# with async functionality is created.
sync_token_name = itsi_group_alerts_token

# The timeout value for receiving an acknowledgement from HEC.
# When processing a notable event and the action criteria is met, this setting
# ensures that the current event is indexed before executing an action.
http_ack_time_out = 10

# The number of split-by hash keys that can exist for a single
aggregation policy that splits events
# by field(s). Split-by hash keys are the possible combinations of
values from individual split-by fields.
# For example, if an aggregation policy is split by 'host' and
'severity', it creates separate hash keys
# for the host-severity combinations of host1 and severity high, host1
and severity low, host2
# and severity low, etc. If episodes are created for 10000 different
host-severity combinations, the limit is reached.
# If you exceed this limit, the hash keys and the episodes associated
with them are cleared from memory. The episodes
# are still saved in the KV store, and events are stored in
itsi_tracked_alerts and itsi_grouped_alerts indexes.
# If you increase this setting, recalculate the
```
'max_event_in_parent_group' setting and increase it accordingly.
sub_group_limit = 10000

# The number of episodes that can be created for each split-by hash key
# for an
# aggregation policy that splits events by field(s).
# If you exceed this limit, the episodes associated with the hash key
# are still saved in the KV store, and events are stored in
# itsi_tracked_alerts and itsi_grouped_alerts indexes.
# If you increase this setting, recalculate the
# 'max_event_in_parent_group' setting and increase it accordingly.
max_groups_per_sub_group = 10000

# The maximum number of events that can be contained within a single
# episode.
# If you exceed this limit, the episode breaks and a new episode is
# created.
# If you increase this setting, recalculate the
# 'max_event_in_parent_group' setting and increase it accordingly.
max_event_in_group = 10000

# The total number of events that can be created by an aggregation
# policy.
# If you exceed this limit, ITSI clears all events associated with this
# aggregation policy from memory. The episodes
# are still saved in the KV store, and events are stored in
# itsi_tracked_alerts and itsi_grouped_alerts indexes.
# This limit is calculated by multiplying 'sub_group_limit' *
# 'max_groups_per_sub_group' * 'max_event_in_group'
max_event_in_parent_group = 1000000000000

# An ACK token ensures that an event is being indexed before running an
# action on it.
# However, events are forwarded to the indexer from the search head,
# which adds another delay.
# This field (in milliseconds) adds an additional delay before running
# an action on events or groups.
action_execution_delay = 0

# When fetching events to perform actions on an episode, the amount of
time, in seconds, to
# subtract from the earliest_time on the search before executing an
# action.
# This setting helps prevent grouping inaccuracies when events are
# milliseconds apart.
earliest_time_lag = 300

# The number of minutes in the past to check for grouping of duplicate
# events.
# For example, if you change this setting to "10", ITSI looks back 10
# minutes prior to the current event. If an
# identical event was added to an episode in the last 10 minutes, the
current event is ignored and not grouped.
`event_grouping_dedup_period = 0`

# The delay, in seconds, to batch update episode state. Otherwise, the
# KV store is accessed too often. # It is recommended that you do not set this to a value below 20.
`group_state_batch_delay = 28`

# The event cache expiration limit. # After this time passes, in seconds, ITSI begins to remove events from
# the cache.
`event_cache_expiry_time = 180`

# The maximum number of events the event cache can contain. # Once the maximum is reached, the cache is cleared.
`event_cache_max_entries = 1000000`

# Whether to validate the current state of the Rules Engine upon
# startup. 
`validate_rules_engine_state_on_startup = true`

# The maximum number of times to restart the Rules Engine if it is not
# in the correct state upon startup.
`max_rt_search_retry_count = 3`

# The various types of error messages to check for at the start of a
# search job.
# The presence of any of these messages could indicate potential
# problems. # If any of these messages are present, the Rules Engine stops.
`exit_condition_message_pattern = (?i).*?nable to distribute to
peer.*|.*?nable to distribute to the peer.*|.*?might have returned
partial results.*|.*?earch results might be incomplete.*`

# The maximum number of times to try a backfill search if any messages
# are detected that
# match those in the 'exit_condition_message_pattern' setting. These
# messages are encountered
# when a peer is unavailable or unreachable, which might cause the Rules
# Engine to miss events.
`backfill_search_retry_count = 3`

# The maximum number of times to try any internal search other than a
# backfill search or a Rules Engine real-time
# search if any messages are detected that match those in the
# 'exit_condition_message_pattern' setting. These messages
# are encountered when a peer is unavailable or unreachable, which might
# cause the Rules Engine to miss data.
`search_retry_count = 3`

# The amount of time to wait, in milliseconds, before retrying a search
job.
search_retryperiod_ms = 500

##########
# ITSI Rules Engine - Resilience Manger Configuration
##########

# A Splunk search to get events that the Rules Engine failed to group.
# Use small timeframes when using this search considering the Splunk
join command limitation of 50,000 rows.
grouping_missed_events_search = search
`itsi_event_management_index_with_close_events` \
 | join type=left event_id search
`itsi_event_management_group_index` | table event_id, itsi_group_id \
 | rename itsi_group_id as backfill_group_id ] \
 | where isnull(backfill_group_id) \
 | fields _time, _raw, source, sourcetype

# The frequency, in seconds, to remind each policy executor to check
time-based policies on their criteria.
# There is a fixed interval between policy check executions to avoid
overlap.
# If the execution of the policy check takes longer than the interval,
# the subsequent execution starts after the prior one completes, plus
the provided interval.
policy_rules_check_frequency = 60

# The frequency, in seconds, that the Rules Engine syncs in-memory
episode state to the KV store.
# Otherwise, the KV store is accessed too often.
# This setting reminds each policy executor to batch update all of an
episode's information in the KV store.
# There is a fixed interval between group state sync executions to avoid
overlap.
policy_group_state_sync_frequency = 28

# The frequency, in seconds, that the resilience manager reprocesses
events that were not grouped.
periodic_backfill_frequency = 720

# The sliding time window, in seconds, used by the resilience manager to
reprocess
# events that were not grouped.
periodic_backfill_time_window = 3600

# The time gap to Rules Engine real-time search, in seconds, used by the
resilience manager
# to reprocess events that were not grouped.
periodic_backfill_to_realtime_gap = 720

# The number of attempts that EventBackfillActor tries before stopping
the periodic backfill search.
Enable bidirectional ticketing in ITSI

Bidirectional ticketing lets you update and close episodes in IT Service Intelligence (ITSI) through an external ticketing system. A bidirectional integration exchanges data between your ITSI instance and a third-party system so that when you make an update to a ticket outside of ITSI, the episode information is also updated within ITSI.

ITSI leverages the Ticket Management data model in the Splunk Common Information Model (CIM) to normalize your data, using the same field names and event tags for equivalent events from your external ticketing system. See Ticket Management in The Splunk Common Information Model Add-on Manual.

This normalization enables you to create action rules for fields like priority, severity, and state without having to remember what they’re called in your external system. See Overview of the Common Information Model in the Common Information Model Add-on Manual for an introduction to the data models and information about the fields and tags they use.

The following image shows how ITSI uses the CIM to update an episode.
ITSI currently only supports bidirectional ticket integration with ServiceNow. Download the Splunk Add-on for ServiceNow from Splunkbase. To configure the app and technical add-on, see Configure ServiceNow to integrate with the Splunk platform in the Splunk Add-on for ServiceNow manual.

Prerequisites

- Any required installations and configurations for your ticketing system.
  - Configure the app and technical add-on for ServiceNow. For instructions, see Configure ServiceNow to integrate with the Splunk platform.
  - Configure data inputs to collect data from your ServiceNow instance. For instructions, see Configure inputs for the Splunk Add-on for ServiceNow.
- The Splunk Common Information Model Add-on (CIM) must be installed.

1. Enable the Bidirectional Ticketing correlation search

ITSI ships with a correlation search that enables bidirectional ticketing. The correlation search queries your ticketing data model and sends an event to the itsi_tracked_alerts index each time an update is made. When sending these events to itsi_tracked_alerts, the correlation search also maps your system’s specific fields to the CIM fields. For more information, see Ticket management in the Common Information Model Add-on Manual.

The Bidirectional Ticketing correlation search is disabled by default. To enable it, perform the following steps:

1. Click Configure > Correlation searches.
2. Toggle the Bidirectional Ticketing correlation search to enable it.

2. (Optional) Specify the index to look at for available fields

When you configure action rules in the next step, ITSI pre-populates all possible fields and values from the main index. If your data is going into a different index, you can specify which index ITSI looks at when populating these fields.

Prerequisites

- Only users with file system access, such as system administrators, can specify a custom index using a configuration file.
- Review the steps in How to edit a configuration file in the Admin Manual.
Never change or copy the configuration files in the default directory. The files in the default directory must remain intact and in their original location.

Steps

1. Open or create a local macros.conf file at $SPLUNK_HOME/etc/apps/SA-ITOA/local/.
2. Under the [itsu_event_management_snow_incidents] stanza, specify the index in the definition setting. For example:

```plaintext
[itsu_event_management_snow_incidents]
args =
definition = index=myspecialindex sourcetype=snow:incident
```

3. Configure action rules

Configure action rules for a notable event aggregation policy that sync the fields in Episode Review with the corresponding fields in your ticketing system. For example, if you already set up an aggregation policy to create incidents in ServiceNow, you must add action rules to update the fields in the ITSI episode when they change in ServiceNow.

If you're integrating with ServiceNow, see Supported arguments for incidents for a table of arguments that ServiceNow supports for incident updates.

Once you configure your aggregation policy action rules and enable the correlation search, any ServiceNow tickets linked through the Link Ticket action in Episode Review has bidirectional functionality enabled by default, as long as you make the ticket system "Service Now" in the Link Ticket modal. For more information, see Link a ticket in the Use Splunk IT Service Intelligence manual.

1. Navigate to Configure > Notable Event Aggregation Policies.
2. Open the existing policy that you use to create tickets in an external system.
3. Click the Action Rules tab.
4. Click Add Rule.
5. Click the If dropdown list and choose the option the <Ticketing System> incident associated with the episode has. The option only appears if you installed the CIM as well as the correct Splunk add-on for your ticketing system.
6. Configure a condition for when a field in an external linked ticket changes. See the following example:
If state matches 6 (Resolved) then change status to Resolved for the episode.

7. Build out your aggregation policy so that each important change in your external ticketing system has an action rule that updates the corresponding episode in ITSI.

For example, the action rules for state changes might look like this:

4. Test the integration

Test the integration to make sure you configured the fields correctly.

1. The next time the aggregation policy creates a ticket in your external ticketing system, update one of the field values for which you created an action rule. For example, change the ticket status from New to In Progress.

2. Go back to Episode Review in ITSI and confirm that the corresponding field was updated in the episode. Note that the field might take several minutes to update.

See also

♦ Create a ticket in ServiceNow or Remedy
♦ Create a custom aggregation policy in ITSI
Dispatch episode actions to a remote ITSI instance

Dispatch episode actions on-premises from a Splunk Cloud instance using hybrid action dispatching. You can configure your on-premises instance to connect to the cloud and get the required information to run the action. Actions include updating the status, severity, and owner of episodes, adding comments, linking tickets, sending an email, pinging a host, and any other custom actions you’ve configured.

Hybrid action dispatching involves configuring your cloud instance as the Master node and your on-premises instance as the Executor node.

<table>
<thead>
<tr>
<th>Node role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Master</td>
<td>The node running core Event Analytics functionality. Configure aggregation policies and trigger actions from the Master node.</td>
</tr>
<tr>
<td>Executor</td>
<td>The node where actions run. The Executor node receives actions dispatched from the Master node and executes them.</td>
</tr>
</tbody>
</table>

The following tasks are meant to configure your cloud instance as the Master node and your on-premises instance as the Executor node. However, you can configure both roles on on-premises instances if needed.

Prerequisites

♦ You must have the admin or itoa_admin role to configure action dispatching.
♦ If an action is configured on the Master node, it must also be configured on the Executor node. If there is a mismatch, the Master node might be able to configure actions that don’t exist on the Executor. For information about configuring ServiceNow, VictorOps, and Remedy actions, see Take action on an episode in ITSI in the User IT Service Intelligence manual.

Configure the cloud search head as the Master node

Configure the cloud search head as the Master node. This is the node running core Event Analytics functionality.
1. **Create an account on the Master node**

Configure a user with the `itoa_admin` role on the cloud search head.

1. Click **Settings > Access controls**.
2. In the Users row, click **+Add New**.
3. Type a name and password.
4. In the Assign to roles **Available item(s) list**, click `itoa_admin` to add it to the Selected Item(s) list.
5. Click **Save**.

2. **Configure the Master node**

Configure the cloud search head as the Master node.

1. On the Master node, click **Configure > Hybrid Action Dispatching**.
2. Set the node’s role to **Master**.
3. Click **Save**.

3. **Disable action execution on the Master node**

The IT Service Intelligence Actions Queue Consumer processes KV store data and executes episode actions. Disable this component on the Master node so that dispatched actions won’t run locally.

1. On the Master node, click **Settings > Data inputs**.
2. Open the **IT Service Intelligence Actions Queue Consumer**.
3. Click **Disable** in the Status column of the **alpha**, **beta**, and **gamma** instances to disable them.

4. **Configure receiving on the Master node**

Configure the master node to receive all action execution information from the Executor node.

1. On the Master node, click **Settings > Forwarding and receiving**.
2. Click **Configure receiving**.
3. Click **New Receiving Port**.
4. Add the TCP port number of the on-premises instance that will execute actions.
5. Click **Save**.
Configure the on-premises search head as the Executor node

Configure the on-premises search head as the Executor node. This is the node that executes episode actions. The Executor makes outbound communication on port 8089 to the cloud search head (Master node), pulling data from the Master node.

You do not need to open any inbound ports. The Executor pushes data to the Master node by configuring forwarding on the port you specify.

5. Configure the Executor node

Assign the on-premises search head as the Executor node and configure the remote instance credentials.

1. On the Executor node, click Configure > Hybrid Action Dispatching.
2. Set the node’s role to Executor.
3. Configure the following settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>URI</td>
<td>The location of the Master node running core Event Analytics services. The URI must point to the management port 8089 (by default) of the Splunk platform instance and include a scheme, host, and port.</td>
</tr>
<tr>
<td>Username</td>
<td>The username that you configured when you created an account on the Master node.</td>
</tr>
<tr>
<td>Password</td>
<td>The password used to log in to the Master node.</td>
</tr>
</tbody>
</table>

4. Click Save.
5. Restart the Executor node to point the Action Queue Consumer to the Master node.

6. Disable Event Analytics on the Executor node

Disable Event Analytics on the Executor node so that this component does not run locally.

1. On the Executor node, click Settings > Searches, reports, and alerts.
2. Change the App: context to All.
3. Search for the itsi_event_grouping search. ITSI Event Analytics runs when this search is enabled.
4. In the Actions column, click Edit > Disable to disable Event Analytics on the Executor node.
7. Configure forwarding on the Executor node

Configure forwarding on the Executor node so that it can send action execution information to the Master node.

1. On the Executor node, click **Settings > Forwarding and receiving**.
2. Click **Configure forwarding**.
3. Click **New Forwarding Host**.
4. Enter the host and port number of the Master node.
5. Click **Save**.

8. Ensure that the Action Queue Consumer is running on the Executor node

Make sure that the Event Analytics saved search is running on the Executor node.

1. On the Executor node, click **Settings > Data inputs**.
2. Open the **IT Service Intelligence Actions Queue Consumer**.
3. Make sure the alpha, beta, and gamma instances show Enabled in the Status column. If not, enable them.

Confirm setup

To confirm that you've successfully configured hybrid action dispatching, execute an action from the Master node. After the action runs, it should appear in the Activity tab of the episode.

- To execute an action from Episode Review, see Take action on an episode in ITSI.
- To execute an action through an aggregation policy, see Create a custom aggregation policy in ITSI.

Ingest third-party alerts as ITSI notable events

ITSI lets you ingest alerts from third-party products, such as Nagios and SCOM, as notable events. You can then manage those notable events in Episode Review. The ability to ingest third-party alerts as notable events lets you use ITSI as an efficient central management console, where you can view, triage, and investigate alerts from integrated products.
**Use a custom integration script**

ITSI provides custom scripts with specific onboarding instructions for you to ingest alerts from common third-party systems. Each blog post provides a script with a custom correlation search and notable event aggregation policy that you can import directly into ITSI. If you use one of these custom scripts, you do not need to follow the regular onboarding steps below.

ITSI provides the following custom onboarding instructions:

- Ingest Netcool Alerts into Splunk ITSI Event Analytics
- Ingest Nagios Alarms into Splunk ITSI Event Analytics
- Ingest AppDynamics and New Relic Alerts into Splunk ITSI Event Analytics

**Step 1: Ingest alerts into ITSI**

There are various methods to get third-party alerts into ITSI. It is recommended that for each alert sender, you have a different source type. Use any of the following methods to ingest alerts into ITSI:

- Set up an email receiver bot. Email alerts are received, parsed, and stored to disk in a directory where a Splunk universal forwarder monitors and collects the data.
- Set up a polling mechanism that uses the third-party service’s API calls to fetch new alerts every minute and store this information into Splunk.
- Use a Splunk universal forwarder to monitor the application logs on the alert-generating servers. The universal forwarder catches the alert in the log files when the tool fires alerts.

**Step 2: Normalize the alert data**

After you ingest alerts into ITSI, you must normalize the fields so that they display properly in Episode Review. Use an ITSI correlation search to normalize third-party alerts as ITSI notable events. A correlation search is an ad hoc Splunk search that enriches, normalizes, and deduplicates raw alerts. Each resulting row from the search becomes an ITSI notable event.

ITSI correlation searches support field substitution with tokens in the format `%fieldname%`. Use field substitution to map third-party alert field values to corresponding notable event fields.
Token variables cannot be the same as correlation search field names. For example, you cannot use "title," "description," "owner," "severity," "status," and so on, as variables. Instead use token variables such as %orig_description%, %orig_owner%, %orig_severity%, %orig_status%, and so on.

1. In ITSI, click **Configure > Correlation Searches.**
2. Click **Create New Search > Create Correlation Search.**
3. Configure a correlation search to ingest third party alerts.

**Search Properties**

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Name</td>
<td>A name that describes the correlation search. For example, &quot;nagios_alert&quot;.</td>
<td>None</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the type of issue the search is intended to detect.</td>
<td>None</td>
</tr>
</tbody>
</table>
| Search Type | Enter an ad hoc search string with appropriate `eval` command expressions to map fields in your third-party alert data to ITSI notable event fields. For example, the following ad hoc search maps Nagios severity-level fields to ITSI severity-level fields:  
  
  ```plaintext
  index="main" sourcetype="csv" | head 100 | eval
  orig_severity=case(severity=="OK", 3, severity=="WARNING", 4, severity=="CRITICAL", 6, severity=="UNKNOWN", 5)
  ```  
  
  Ad hoc | |
<p>| Time range | The time range over which the correlation search applies. Choose <strong>Relative</strong> and run the search over the last 1 minute or last 5 minutes. | Last 15 minutes |</p>
<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>The ITSI services to which this correlation search applies. Leave this field blank.</td>
<td>None</td>
</tr>
</tbody>
</table>
| Entity Lookup Field | The field in the data retrieved by the correlation search that is used to look up corresponding entities. This is usually a host or node field (for example, itsiNode). If the host or node of the alert is listed as a filtered entity in one or more ITSI services, these service names are added to the notable event as "affected service(s)".  

The entity lookup field must be an actual entity alias field for the match to occur. For example, if the entity was created with an alias of hostname but the entity lookup field in the correlation search as a value of myhost, the entity is not matched. The entity lookup field must be hostname as well. | None     |

**Schedule**

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Type</td>
<td>Choose a Basic schedule. Configure the search interval in the Run Every menu to run every 1 minute or 5 minutes (depending on the time range above).</td>
<td>Basic, Every 5 minutes</td>
</tr>
</tbody>
</table>
**Notable Events**

Use this section to configure the notable event that is generated when search results meet a specific condition. The Splunk platform indexes the event object like any other event. You can track, manage, and update notable events in Episode Review.

ITSI correlation searches support field substitution with tokens in the format `%fieldname%`. Use field substitution to map third-party alert field values to corresponding notable event fields. To see the available fields that you can use as tokens, click **Run Search** under Search Properties. You can use any of the fields listed in the left panel.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notable Event Title</td>
<td>The title of the notable event in Episode Review. For example, you might enter %name% to substitute Nagios alert names as notable event titles.</td>
<td>None</td>
</tr>
<tr>
<td>Notable Event Description</td>
<td>A brief phrase to describe the notable event. For example, you might enter %reason% to substitute Nagios descriptions for notable event descriptions.</td>
<td>None</td>
</tr>
<tr>
<td>Owner</td>
<td>The ITSI role to which the notable event is assigned in Episode Review. Click <strong>Advanced Mode</strong>, then enter the owner using a token in the format <code>%fieldname%</code>. For example, %owner_field%. In advanced mode, owners must match the names of owners in the system.</td>
<td>Unassigned</td>
</tr>
<tr>
<td>Severity</td>
<td>The level of importance of the event. Click <strong>Advanced Mode</strong>, then provide a token in the format <code>%fieldname%</code> to substitute the value of a third-party alert field. Values must match an integer specified in the default version of</td>
<td>1 - Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 - Critical</td>
</tr>
<tr>
<td>Field name</td>
<td>Description</td>
<td>Defaults</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>itsi_notable_event_severity.conf (or the local version if you created one).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Status</strong></td>
<td>The triage status of the event in Episode Review. Click Advanced Mode, then provide a token in the format <code>%fieldname%</code> to substitute the value of a third-party alert field. Values must match an integer specified in the default version of itsi_notable_event_status.conf (or the local version if you created one). For incoming third-party alerts the triage status is generally &quot;New&quot;.</td>
<td>0 - Unassigned 1 - New 2 - In Progress 3 - Pending 4 - Resolved 5 - Closed</td>
</tr>
<tr>
<td>Drilldown Name</td>
<td>You can drill down to a specific Splunk search from the All Events tab of Episode Review. Set the name of the drilldown search link.</td>
<td>None</td>
</tr>
<tr>
<td>Drilldown Search</td>
<td>The search you drill down to.</td>
<td>None</td>
</tr>
<tr>
<td>Drilldown earliest offset</td>
<td>Defines how far back from the time of the event to start looking for related events.</td>
<td>Last 5 minutes</td>
</tr>
<tr>
<td>Drilldown latest offset</td>
<td>Defines how far ahead from the time of the event to look for related events.</td>
<td>Next 5 minutes</td>
</tr>
<tr>
<td>Notable Event Identifier Fields</td>
<td>Determine whether a notable event is unique or not, which drives the events timeline. These identifier fields form the event hash field, which is added to every notable event to help identify unique alarm types.</td>
<td>source</td>
</tr>
<tr>
<td>Drilldown link title</td>
<td>You can drill down to a specific website from the All Events tab of</td>
<td>None</td>
</tr>
<tr>
<td>Field name</td>
<td>Description</td>
<td>Defaults</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Drilldown link URI</td>
<td>The website you drill down to.</td>
<td>None</td>
</tr>
</tbody>
</table>

4. Click **Save**.

The correlation search runs as scheduled, mapping third-party alert field values to ITSI notable event fields. Third-party alerts appear as notable events in Episode Review. The events are collected in the itsi_tracked_alerts index.

### Step 3: Aggregate the events

After you ingest and normalize third-party alerts, they are collected in the itsi_tracked_alerts index as notable events and are ready to be grouped into episodes.

A notable event aggregation policy called Splunk App for Infrastructure is delivered with ITSI. This aggregation policy groups all third-party alerts (including alerts from the Splunk App for Infrastructure) that use ITSI normalized fields. Enable this aggregation policy or configure your own aggregation policy to group third-party alert data.

1. In ITSI, click **Configure > Notable Event Aggregation Policies**.
2. Click **New Notable Event Aggregation Policy**, or configure the Default Policy. See Notable event aggregation policies overview for ITSI.

For example, you might configure the Default Policy by enabling Smart Mode, then selecting several notable events to cluster on (such as itsiNode, itsiAlertId, Location, and OS_version).

After you enable an aggregation policy, episodes start appearing in Episode Review.

ITSI can also take automated actions at the beginning or end of an episode. Consider what makes the most sense for a given type of alert. Alert actions might include opening a ServiceNow ticket, sending an email, or running a custom script. For more information, see Take action on an episode in ITSI.
Ingest SNMP traps in ITSI

Simple Network Management Protocol (SNMP) is an application-layer protocol used to manage and monitor network devices and their functions. Learn how to ingest SNMP traps into Splunk enterprise and feed them into ITSI Episode Review for easy review and correlation.

After you configure Splunk enterprise and ITSI to receive and process SNMP traps, enable the default correlation search and aggregation policy to view and triage the traps in Episode Review. For more information, see Triage episodes in ITSI in the Splunk ITSI User Manual.

Prerequisites

1. To ingest SNMP traps in ITSI, you must install and configure snmptrapd, an application that receives and logs SNMP TRAP and INFORM messages and resolves them using vendor Management Information Bases (MIBs). Before you install snmptrapd on your system, see the manual page for snmptrapd.
2. To configure the logging format, open snmptrapd.conf and add the following stanza:

```
# snmptrapd formatting

# SNMPV1
format1 Agent_Address = %A
Agent_Hostname = %B
Date = %y-%m-%d %H:%M:%S
Enterprise_OID = %N
Trap_Type = %w
Trap_SubType = %q
Community_Infosec_Context = %P
Uptime = %T
Description = %W
PDU_Attribute_Value_Pair_Array:
%V
%v
---

# SNMPV2
format2 Agent_Address = %A
Agent_Hostname = %B
Date = %y-%m-%d %H:%M:%S
Enterprise_OID = %N
Trap_Type = %w
Trap_SubType = %q
Community_Infosec_Context = %P
Uptime = %T
Description = %W
PDU_Attribute_Value_Pair_Array:
%V
%v
---
```

Steps
Perform the following steps to ingest SNMP traps into ITSI:

1. Send SNMP events to your Splunk deployment.
2. Configure the snmptrapd index.
3. Enable the SNMP correlation search and aggregation policy.

**Send SNMP events to your Splunk deployment**

For instructions on getting SNMP events into your Splunk deployment, see Send SNMP events to your Splunk deployment in the Splunk Enterprise *Getting Data In* manual.

**Configure the snmptrapd index**

After you install and configure `snmptrapd`, you need to tell Splunk software and ITSI where to find the SNMP data and how to parse it. Use the following ITSI configuration files to instruct Splunk software to monitor the file that `snmptrapd` is writing to, and to parse and extract the key-value pairs that make up important information contained in the traps.

Where you deploy these configurations depends on the type of Splunk deployment you have. For more information, see Overview of installing IT Service Intelligence in a distributed environment.

**inputs.conf**

Add the following stanza to the local version of `inputs.conf`:

```plaintext
[monitor:///var/log/snmptrapd.log]
disabled = false
index = snmptrapd
sourcetype = snmptrapd
```

This stanza tells your Splunk instance where to look for your data. Deploy this configuration on forwarders or Splunk instances co-located with `snmptrapd`.

**props.conf**

Add the following stanza to the local version of `props.conf`:

```plaintext
[snmptrapd]
DATETIME_CONFIG =
KV_MODE = none
```

165
LINE_BREAKER = (\[\r\n\]+)Agent_Address\s=
MAX_TIMESTAMP_LOOKAHEAD = 30
NO_BINARY_CHECK = true
SHOULD_LINEMERGE = false
TIME_FORMAT = %Y-%m-%d %H:%M:%S
TIME_PREFIX = Date\s=\s
TZ = UTC
category = Custom
description = parse snmptrapd logging with custom kvpair splunk formatting
disabled = false
pulldown_type = true
EXTRACT-node = ^[^\[
]*\[(?P<node>[^\]
]+)
REPORT-snmptrapd = snmptrapd_kv

This stanza sets line-breaking rules and extracts the timestamp. In this case, the timestamp is the time that the snmptrapd server received the trap. This stanza also ensures that Splunk knows how to parse the time format.

Deploy this configuration to your heavy forwarder, indexer, and search heads.

*transforms.conf*

Add the following stanza to the local version of *transforms.conf*:

```
[snmptrapd_kv]
DELIMS = "\n", "="
```

This stanza extracts all key-value pairs in the SNMP trap. Deploy this configuration to your heavy forwarder, indexer, and/or search heads.

*default.meta.conf*

Add the following stanza to the local version of *default.meta.conf*:

```
[]
access = read : [ * ], write : [ admin ]
export = system
```

This stanza includes a *local.meta.conf* file in the ITSI application that exports permissions to the system. Deploy this configuration on your search heads.

**Enable the SNMP correlation search and aggregation policy**

ITSI provides the following default correlation search and aggregation policy for processing SNMP traps:
SNMP Traps
A default correlation search that generates a notable event for each SNMP trap received through Splunk.

Default SNMP Policy
A default notable event aggregation policy that aggregates individual SNMP trap events into episodes in Episode Review.

Steps

1. To enable the correlation search, click Configure > Correlation Searches and enable the SNMP Traps search in the Status column.
2. To enable the aggregation policy, click Configure > Notable Event Aggregation Policies and enable the Default SNMP Policy in the Status column.
Aggregation Policies

Notable event aggregation policies overview for ITSI

Notable event aggregation policies help you group notable events into episodes to organize them in Episode Review. ITSI provides a default aggregation policy to group notable events. You can also create your own aggregation policies if you are familiar with your data and want to define very precisely how events are grouped. You can use Smart Mode on any aggregation policy to employ machine learning algorithms to group events. The process of managing notable events through the use of aggregation policies is often referred to as "event analytics."

Aggregation policies group notable events based on rules that you define. You can also consolidate duplicate events, suppress alerts, or close episodes when a clearing event is received.

Aggregated notable events are displayed in Episode Review when event grouping is enabled in View Settings. These episodes have their own title, description, severity, status, and assignee, separate from the individual notable events within the episode.

A notable event can belong to multiple episode if it matches the criteria for those episodes.

The following aggregation policies are delivered with ITSI:

- Default Policy
- Default SNMP Policy
- Normalized Policy (Splunk App for Infrastructure)

See also

- Use the default aggregation policy in ITSI
- Create a custom aggregation policy in ITSI

About the default aggregation policy in ITSI

The ITSI default aggregation policy groups notable events that don't match the filtering criteria of any other policies you create. If you don't want to create your
own aggregation policies, use the default policy to group events. You can't delete or disable the default policy.

Only a user assigned the `itoa_admin` role, or a role that inherits from `itoa_admin`, can modify the default aggregation policy.

The default aggregation policy is defined as follows:

- Does not include any filtering criteria. The default policy catches events not captured by the filtering criteria of any other aggregation policies. None can be added.
- Splits events into multiple episodes by the `source` field. You can change the field that is used to split events, specify more than one field by which to split events, or choose to not split events by not specifying a field name.
- ITSI stops adding events to the episode if the flow of events into the episode is paused for 7200 seconds (2 hours). This can be changed to a different length of time or to different breaking criteria.
- Episode information such as Episode Title, Episode Description, and Episode Severity are set to be the same as the first event in the episode. You can change these if desired.
- No action rules are defined. You can add action rules if desired.

To view or modify the default aggregation policy, click **Configure > Notable Event Aggregation Policies > Default Policy.**

The default policy doesn't have Smart Mode enabled, but you can enable it yourself. For information on enabling Smart Mode, see Group similar events with Smart Mode in ITSI.

For information on modifying the default aggregation policy or creating a new aggregation policy, see Create a custom aggregation policy in ITSI.

---

**Create a custom aggregation policy in ITSI**

You can create one or more customized notable event aggregation policies. By default, users assigned the `itoa_admin` role or `itoa_team_admin` role can create, modify, and delete aggregation policies. Users assigned the `itoa_analyst` role can view notable event aggregation policies but cannot modify or delete them.

If you want to use Smart Mode in a custom aggregation policy, you must first create and save the custom aggregation policy. After you save the policy,
re-open it to turn on and configure Smart Mode.

What aggregation policies do

Notable event aggregation polices help you group notable events into episodes to organize them in Episode Review in the following ways:

1. Group notable events into episodes based on the following criteria:
   - A field matches a string
   - A field does not match a string
   - A field is greater than a number
   - A field is greater than or equal to a number
   - A field is less than a number
   - A field is less than or equal to a number

2. Split events into multiple episodes by one or more fields, such as source or host.

3. Stop grouping when certain criteria are met, such as when a certain number of events is reached, the episode has existed for a certain amount of time, or when a certain event occurs, such as Severity matches Normal.

4. Take automatic actions on an episode when certain trigger conditions are met. Note that not all actions may be available if role-based permissions are set. For information about episode actions, see Take action on an episode in ITSI.

Create an aggregation policy

When creating a new policy, be mindful of the policies that have already been created. Multiple aggregation policies can be created with filtering criteria that capture the same set or subset of events. If the same notable events are captured by more than one policy, the action rules from each policy are applied to the notable events.

To create an aggregation policy:

1. Click Configure > Notable Event Aggregation Policies. The default policy and any other policies that have been created are listed.
2. Click Create Notable Event Aggregation Policy. The Filtering Criteria step opens.
**Filtering Criteria**

You can create rules for determining which notable events are included in the group based on multiple AND/OR conditions. You can use wildcard characters in fields. You must specify at least one rule.

The field names in original events that conflict in the *itsi_tracked_alerts* index are renamed with the prefix `orig_*`. To filter or split by fields in original events, append `orig_` to the field name. For example, use `orig_sourcetype` instead of `sourcetype`. `sourcetype` means the sourcetype of generated notable events in the *itsi_tracked_alerts* index, rather than the sourcetype of original events.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include the events if</td>
<td>Determine when an event is added to this episode. For example, you could specify <code>severity matches Critical</code> to include all critical events in the episode. To include events based on a saved search, type <code>search_name matches &lt;name of saved search&gt;</code>. You can match on any fields in the event. The syntax for the field value does not follow standard SPL. The value must exactly match the field value in the event, including capitalization and spaces. You can use asterisks (*) as wildcards (for example, <code>location does not match webserver*</code>). Click + Add Rule (AND) to add another rule to the rule block, or + Add Rule (OR) to start a new block of rules that is separated from the previous block by an OR condition. For example, if there are three rules in the first block and two rules in the second block, the total clause would read &quot;(Rule1 AND Rule2 AND Rule3) OR (Rule1 AND Rule2)&quot;.</td>
</tr>
<tr>
<td>Split events by field</td>
<td>Split events into separate groups based on one or more raw notable event field names. Each field is considered separately. For example, if you split by <code>name</code> and <code>norm_severity</code> and there are three values for each field, nine episodes are created. A preview shows the events that meet the filtering criteria grouped by the specified fields.</td>
</tr>
<tr>
<td>Break episode</td>
<td>Add breaking conditions to stop grouping. If the conditions are met, the current episode ends and a new episode is started. Use wildcards to search for a string in a field.</td>
</tr>
</tbody>
</table>
For example, you might enter **Break episode if the following event occurs:** `message matches *status Normal`. The breaking event must be included in the episode by meeting the filtering criteria for the episode.

The maximum value for the flow of events into the episode paused for is **86400 seconds** (24 hours).

When an episode is closed, either in Episode Review or through an aggregation policy, it automatically breaks.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Episode Information</strong></td>
<td>Specify how you want episode information to appear in Episode Review. This information is at the episode level and is separate from the information for the underlying notable events in the episode.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Same as the first event</strong> sets the episode fields to the values from the first event in the episode.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Same as the last event</strong> continually updates the episode fields as each new event enters the episode.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Static value</strong> lets you provide specific field values. If you select Static value for Episode Title or Episode Description, you can use a token such as <code>%title%</code> or <code>%description%</code> to insert the value of a field.</td>
</tr>
<tr>
<td></td>
<td>If there are multiple events in an episode with the same timestamp, the policy sorts them by milliseconds to determine the first and last events in an episode.</td>
</tr>
<tr>
<td></td>
<td>Changing a policy’s episode information fields breaks all active episodes associated with that aggregation policy and starts a new episode. Make sure to carefully plan the timing of changes to these fields to mitigate potential risks associated with this behavior.</td>
</tr>
</tbody>
</table>

**Action Rules**

Add action rules to take specific automated actions on each episode created by the aggregation policy. Action rules are optional. You can define more than one action rule per aggregation policy.

- Use the **If** pane to specify the trigger conditions for the action(s).
• Use the **Then** pane to specify the actions to take if the trigger conditions are met.

For example, if you want to close the episode and change the severity level to **Info** when a clearing event comes in, you could specify the following rule:

If the following event occurs: `severity` matches **Normal**, change severity to **Info** for the episode, add a comment **Don't worry** for the episode, and change status to **Closed** for the episode.

Choose from the following default trigger conditions:

<table>
<thead>
<tr>
<th>Trigger condition</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>The following event occurs</td>
<td>Trigger an action when an event containing specific field values is added to the episode. For example, when <code>severity</code> matches <strong>Critical</strong>, you can match on any fields in the event. The syntax for the field value does not follow standard SPL. The value must exactly match the field value in the event, including capitalization and spaces. You can use asterisks (*) as wildcards (for example, <code>service_name</code> does not match <code>BG_*</code>).</td>
</tr>
<tr>
<td>The episode existed for</td>
<td>Trigger an action if the episode has existed for a given amount of time, in seconds. You might close an episode if it's existed for 86400 seconds (one day).</td>
</tr>
<tr>
<td>The number of events in the episode is</td>
<td>Trigger an action if the number of events in the episode exceeds or does not reach a certain limit. By default, an episode breaks when it reaches 10,000 events, and a new episode is created.</td>
</tr>
<tr>
<td>The flow of events into the episode paused for</td>
<td>Trigger an action if the episode hasn't received any events for a given amount of time, in seconds. The maximum value for this field is 86400 seconds (24 hours).</td>
</tr>
</tbody>
</table>

Choose from the following default actions:

<table>
<thead>
<tr>
<th>Action</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change severity</td>
<td></td>
</tr>
</tbody>
</table>
For example, change the severity to Critical when the number of events in the episode is greater than 100.

Change status

For descriptions of each status, see Update the status of an episode.

Changing an episode's status to closed through an aggregation policy action rule also breaks the episode so it no longer receives events.

Change owner

Episodes are unassigned by default.

Add a comment

Does not accept token replacement.

Ping a host

Provide the event field that contains the host that you want to ping in the Host field. For example, %server%.

Send an email

For information on configuring an email, see Send an email in the ITSI User Manual.

Run a script

Provide the file name of the script stored in $SPLUNK_HOME/bin/scripts. For more information, see Configure scripted alerts in the Splunk Enterprise Alerting Manual.

Create an incident in ServiceNow

Requires the Splunk Add-on for ServiceNow. For configuration information, see Create a ticket in ServiceNow or Remedy.

Create an incident in Remedy

Requires the Splunk Add-on for Remedy. For configuration information, see Create a ticket in ServiceNow or Remedy.

Create an incident in VictorOps

Requires VictorOps For Splunk. For configuration information, see Create a ticket in VictorOps.

Policy Info

Specify a title and description for your notable event aggregation policy. The policy is enabled by default and immediately takes effect. Disable it if you do not want it to take effect yet.

Click Next and you will see the message that the policy has been successfully created. After the policy has been created, new incoming notable events are grouped in Episode Review according to the criteria in the policy. Note that notable events that existed before the policy was created are not grouped by the
Enable Smart Mode on an aggregation policy

After creating and saving a custom aggregation policy, you can edit the policy to enable and configure Smart Mode. For information on enabling Smart Mode, see Enable Smart Mode in ITSI.

Set aggregation policy permissions

After you create a notable event aggregation policy, set read/write permissions for it to control who can modify or read it.

1. Click Configure > Notable Event Aggregation Policies.
2. Locate the policy and click Edit > Edit Permissions.
3. Assign read or write permissions to roles as desired.

You cannot assign write permissions unless the role possesses the write_itsi_notable_aggregation_policy capability.
4. Click Save.

Group similar events with Smart Mode in ITSI

Smart Mode groups notable events in Episode Review based on their similarities. It uses machine learning algorithms to compare event field values and group events that are related to each other. Smart Mode reduces noise and detects patterns in your events so you don't have to. You can enable Smart Mode on the default aggregation policy or on a custom policy.

Do not enable Smart Mode on more than five aggregation policies in a minimum environment (12 CPUs, 12 GB of RAM on the search head), or more than 20 aggregation policies in a performance environment (48 CPUs, 65 GB of RAM on the search head).

1. Click Configure > Notable Event Aggregation Policies.
2. Select a custom policy or the Default Policy.
3. Under Smart Mode grouping, enable Smart Mode.
4. Click Select fields. A dialog displays the fields found in your notable events from the last 24 hours.
5. (Optional) Change the time period for the field analysis and click Re-run Analysis.
Choose the fields to compare for event similarity. Recommended fields are selected by default. Do not select more than 15 fields, as this might impact performance.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Category or Text based on the content of the field.</td>
</tr>
<tr>
<td></td>
<td>Category fields have a distinct value, such as a status field.</td>
</tr>
<tr>
<td></td>
<td>Text fields consist of a string, such as a description field.</td>
</tr>
<tr>
<td># of Values</td>
<td>The number of values for each field.</td>
</tr>
<tr>
<td>Event Coverage</td>
<td>The percentage of events that contain the field. In general,</td>
</tr>
<tr>
<td></td>
<td>choose fields with high event coverage.</td>
</tr>
</tbody>
</table>

Click **Apply**. An episode preview uses the last 24 hours of data to illustrate event grouping with Smart Mode enabled. Expand an episode to see the individual notable events.

(Optional) Configure other Smart Mode settings:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Mode grouping</td>
<td>The importance of text similarity versus category similarity. The episodes in the preview update to reflect the importance factors you set. Setting both to 0, half, or 1 gives the factors equal weight.</td>
</tr>
<tr>
<td></td>
<td>Enable <strong>Split by Service</strong> to provide service context for your events. For example, if two events have similar fields but affect different services, they probably shouldn’t be grouped together. If enabled, events are grouped by service first, then by text and category similarity.</td>
</tr>
<tr>
<td></td>
<td>Enable <strong>Split by Entity</strong> to provide entity context for your events. If enabled, ITSI segregates events based on the entity they belong to before applying grouping. Then it groups by text and category similarity. For example, if there are web status errors and disk errors on the same host that occurred in the same time period, those events are now in the same episode.</td>
</tr>
<tr>
<td></td>
<td>If you split by service AND entity, Smart Mode splits by service first (if the event has service association) and does not split further. If the event has no service association, it splits by entity.</td>
</tr>
</tbody>
</table>
### Setting Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Split events by field</td>
<td>Splits events into separate episodes based on a field name. <code>host</code> is a common field to split by so that separate episodes get created for each host. Use commas to separate multiple fields.</td>
</tr>
<tr>
<td>Break episode</td>
<td>The number of seconds that the flow of events is paused before grouping stops.</td>
</tr>
<tr>
<td>Episode information</td>
<td>Determines how the information in each episode is named or assigned. If you select <strong>Static value</strong> for Episode Title or Episode Description, you can use a token such as <code>%title%</code> or <code>%description%</code> to insert the value of a field.</td>
</tr>
</tbody>
</table>

9. Click **Save**.

After you save your aggregation policy, events are grouped in Episode Review according to the policy you configured. Custom aggregation policies take precedence over the Default Policy, so if an event meets the criteria of a custom policy, it is grouped according to that policy's rules.
Correlation Searches

Correlation search overview for ITSI

A correlation search is a recurring search that scans multiple data sources for defined patterns. You can configure a correlation search to generate a notable event (alert) when search results meet specific conditions. Review notable events that your correlation searches generate in Episode Review and initiate the investigative process of determining root cause.

You can use an ITSI correlation search to ingest third-party alerts as ITSI notable events. If you are creating a correlation search to ingest alerts from a third-party product, such as Nagios or SCOM, see Ingest third-party alerts as ITSI notable events for specific instructions.

Do not create correlation searches by manually editing $SPLUNK_HOME/etc/apps/itsi/local/savedsearches.conf. The search will not appear on the correlation search lister page. Always create correlation searches directly in the IT Service Intelligence app.

Predefined correlation searches

The following correlation searches are delivered with ITSI. They are all disabled by default except Splunk App for Infrastructure Alerts. You can enable them and modify them to meet your needs.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bidirectional Ticketing</td>
<td>Maps an external ticketing system's fields to Common Information Model (CIM) fields to enable bidirectional ticketing. See Enable two-way integration with an external ticketing system in ITSI for information.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Monitor Critical Service Based on Health Score</td>
<td>Generates notable events for services with a critical health score.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Normalized Correlation Search</td>
<td>Generates notable events for any third-party alerts being ingested into ITSI that include ITSI normalized fields. See Normalized correlation</td>
<td>Disabled</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default status</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>SNMP Traps</td>
<td>Generates notable events for SNMP traps being ingested into ITSI. See Ingest SNMP traps in ITSI for more information.</td>
<td>Disabled</td>
</tr>
<tr>
<td>Splunk App for Infrastructure Alerts</td>
<td>Generates notable events from Splunk App for Infrastructure alerts when you enable integration between the Splunk App for Infrastructure and ITSI. See Ingest Splunk App for Infrastructure alerts into ITSI as notable events for more information.</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

### Create correlation searches in ITSI

You can create your own correlation searches to generate notable events, throttle events, and perform other actions automatically based on a correlation in events.

Create a correlation search manually if you are an expert with SPL. You can review the included correlation searches for examples of the search methodology and available options. Test your correlation search ideas on the Search page before implementing them.

**Steps:**

1. From the ITSI main menu, click **Configure > Correlation Searches**.
2. Click **Create New Search > Create Correlation Search**.

You can also create a correlation search by cloning an existing one. In the Actions column on the correlation search lister page, click **Edit > Clone**.

For information on configuring correlation searches, see [Configure correlation searches in ITSI](#).

### Configure correlation searches in ITSI

A **correlation search** is a recurring search that scans multiple data sources for defined patterns. You can configure a correlation search to generate a **notable event** (alert) when search results meet specific conditions. Use Episode Review
to review notable events that your correlation searches generate and to initiate
the investigative process of determining root cause.

You can use an ITSI correlation search to ingest third-party alerts as ITSI notable
events. If you are creating a correlation search to ingest alerts from a third-party
product, such as Nagios or SCOM, see Ingest third-party alerts as ITSI notable
events for specific instructions.

Configure correlation searches to update the settings associated with how they
run, change the search logic, and throttle alerts. See Correlation search overview
for ITSI to learn more about correlation searches.

**Search Properties**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search Name</td>
<td>A name that describes the correlation search. For example, &quot;cpu_load_percent&quot;.</td>
<td>None</td>
</tr>
<tr>
<td>Description</td>
<td>(Optional) A description of the type of issue the search is intended to detect.</td>
<td>None</td>
</tr>
<tr>
<td>Search Type</td>
<td>The correlation search type:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>♦ Data Model: Create a search based on a Splunk data model. Click Select to select a data model.</td>
<td>Ad hoc</td>
</tr>
<tr>
<td></td>
<td>♦ Ad hoc: Create a search based on a custom search string that you provide.</td>
<td></td>
</tr>
<tr>
<td>Time range</td>
<td>The time range over which the correlation search applies.</td>
<td>Last 15 minutes</td>
</tr>
</tbody>
</table>
## Association

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Select one or more ITSI services to which this correlation search applies. You can only select services that belong to teams for which you have read access.</td>
<td>None</td>
</tr>
<tr>
<td>Entity Lookup Field</td>
<td>The field in the data retrieved by the correlation search that is used to look up corresponding entities. For example, host.</td>
<td>None</td>
</tr>
</tbody>
</table>

## Schedule

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Schedule Type</td>
<td>Configure the schedule for the correlation search:</td>
<td>Basic, Every 5 minutes</td>
</tr>
<tr>
<td></td>
<td>• <strong>Basic</strong>: Schedule searches to run at regular intervals. Configure the search interval in the Run Every menu.</td>
<td>Basic, Every 5 minutes</td>
</tr>
<tr>
<td></td>
<td>• <strong>Cron</strong>: Schedule searches to run periodically at fixed times, dates, or intervals. Enter a schedule in <strong>Cron Schedule</strong>. For more information, see Use cron expressions for scheduling in the <strong>Alerting Manual</strong></td>
<td>Basic, Every 5 minutes</td>
</tr>
</tbody>
</table>

## Notable Events

Use this section to configure the notable event that is generated when search results meet a specific condition. The Splunk platform indexes the event object like any other event. You can track, manage, and update notable events in Episode Review.
ITSI correlation searches support field substitution with tokens in the format `@fieldname@`. Use field substitution to map third-party alert field values to corresponding notable event fields. See Use ITSI correlation search to ingest alerts for specific examples.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Defaults</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notable Event Title</td>
<td>The title of the notable event in Episode Review. For example, <code>mysql-01 server cpu Load %</code>.</td>
<td>None</td>
</tr>
<tr>
<td>Notable Event Description</td>
<td>A brief phrase to describe the notable event. For example, &quot;This alert triggers when DB CPU load on the mysql-01 server reaches 80%.&quot;</td>
<td>None</td>
</tr>
<tr>
<td>Owner</td>
<td>The ITSI role to which the notable event is assigned in Episode Review. If using advanced mode, the value must resolve to a username in the system.</td>
<td>Unassigned</td>
</tr>
<tr>
<td>Severity</td>
<td>The level of importance of the event. If using advanced mode, the values must resolve to an integer specified in the default version of <code>itsi_notable_event_severity.conf</code> (or the local version if you created one).</td>
<td>1 - Info</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - Normal</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - Low</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - Medium</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - High</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6 - Critical</td>
</tr>
<tr>
<td>Status</td>
<td>The triage status of the event in Episode Review. If using advanced mode, the values must resolve to an integer specified in the default version of <code>itsi_notable_event_status.conf</code> (or the local version if you created one).</td>
<td>0 - Unassigned</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 - New</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 - In Progress</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 - Pending</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 - Resolved</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 - Closed</td>
</tr>
<tr>
<td>Drilldown Search</td>
<td>You can drill down to a specific Splunk search from the Overview.</td>
<td>None</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
<td>Defaults</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Name</td>
<td>tab of Episode Review for an individual notable event or from the Grouped Events tab for a group of notable events. Set the name of the drilldown search link.</td>
<td></td>
</tr>
<tr>
<td>Drilldown Search</td>
<td>The search you drill down to.</td>
<td>None</td>
</tr>
<tr>
<td>Drilldown earliest offset</td>
<td>Defines how far back from the time of the event to start looking for related events.</td>
<td>Last 5 minutes</td>
</tr>
<tr>
<td>Drilldown latest offset</td>
<td>Defines how far ahead from the time of the event to look for related events.</td>
<td>Next 5 minutes</td>
</tr>
<tr>
<td>Notable Event Identifier</td>
<td>Determine whether a notable event is unique or not. These identifier fields form the event hash field, which is added to every notable event to help identify unique alarm types.</td>
<td>source</td>
</tr>
<tr>
<td>Drilldown Website Name</td>
<td>You can drill down to a specific website from the Overview tab of Episode Review. Set the name of the drilldown website link.</td>
<td>None</td>
</tr>
<tr>
<td>Drilldown Website URL</td>
<td>The website you drill down to.</td>
<td>None</td>
</tr>
</tbody>
</table>

**Advanced Options**

**Throttling**

When correlation search results meet specific conditions, the search generates a new notable event (alert). A correlation search can create multiple alerts for the same condition. In most cases, it is best to have a single alert for the same condition. Throttling blocks the correlation search from creating duplicate alerts for the same issue every time it runs.

If you group by one or more fields, throttling is applied to each unique field-value combination. For example, throttling by host once a day means that only one
notable event of this type is created per day, per server.

Throttling applies to any correlation search alert type, including notable events and actions (RSS feed, email, run script, and ticketing).

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suppress Period</td>
<td>During the suppress period, any additional event that matches any of the <strong>Fields to group by</strong> does not create a new alert. After the suppress period passes, the next matching event creates a new alert, and throttling conditions resume. Enter a relative time range in seconds. For example &quot;60s&quot; (60 seconds).</td>
</tr>
<tr>
<td>Fields to group by</td>
<td>Fields to compare for similar events. For example, <code>cpu_load_percent</code>.</td>
</tr>
<tr>
<td></td>
<td>During the suppress period, any additional matches in the correlation search results are compared to the fields defined here. If a field matches, it stops the creation of a new alert. You can define multiple fields. The fields available depend on the search fields that the correlation search returns.</td>
</tr>
</tbody>
</table>

**Actions**

Actions are other alert types that a correlation search can trigger. You configure action alerts independently from other alert types, such as Notable Events and Risk Scoring.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include in RSS feed</td>
<td>Posts the correlation search alert on the Splunk Enterprise RSS feed.</td>
</tr>
<tr>
<td>Send email</td>
<td>Sends an email about the correlation search alert.</td>
</tr>
<tr>
<td></td>
<td>♦ <strong>Email subject</strong>: The email subject defaults to &quot;Splunk Alert: $name$&quot;, where $name$ is the correlation search Search Name.</td>
</tr>
<tr>
<td>Action</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>✦ Email address(es):</td>
<td>Insert email addresses and/or distribution lists that should receive the alert.</td>
</tr>
<tr>
<td>✦ Include entity information:</td>
<td>Apps entity information to the subject of the email.</td>
</tr>
<tr>
<td>✦ Include results in email:</td>
<td>Adds the correlation search results in the body of the email in the format you specify.</td>
</tr>
<tr>
<td>✦ Attach results in a PDF:</td>
<td>Includes the correlation search results as a PDF attachment. The schedule_search capability and the admin_all_objects capability are required for PDF delivery scheduling.</td>
</tr>
<tr>
<td>✦ Attach results in a CSV:</td>
<td>Includes the correlation search results as a CSV attachment.</td>
</tr>
<tr>
<td>Note: Email actions require that you configure the mail server in Splunk Enterprise. See Configure email notification settings in the Alerting Manual.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run a script</td>
<td>Triggers a shell script. See Configure scripted alerts in the Alerting Manual.</td>
</tr>
</tbody>
</table>

**Create multi-KPI alerts in ITSI**

A multi-KPI alert is an alert based on trigger conditions that you define for multiple KPIs. When trigger conditions occur simultaneously for each KPI, a correlation search generates a notable event.

Multi-KPI alerts are useful for correlating the status of multiple KPIs across multiple services. This lets you identify causal relationships, investigate root
cause, and provide insights into behaviors across your infrastructure.

For example, to avoid the negative impact that a large spike in traffic can have on website performance, you might create a multi-KPI alert based on two common KPIs: CPU load percent and web requests. A sudden simultaneous spike in both CPU load percent and web request KPIs might indicate a DDOS (Distributed Denial of Service) attack. Multi-KPI alerts can bring such trending behaviors to your attention early, so that you can take action to minimize any impact on performance.

Multi-KPI alerts can apply to one or more KPIs across one or more services.

**Multi-KPI alert types**

Splunk IT Service Intelligence (ITSI) provides two types of multi-KPI alerts:

<table>
<thead>
<tr>
<th>Alert</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status over time</td>
<td>Based on the severity level of one or more KPIs. If one or more trigger conditions for each KPI are satisfied simultaneously, ITSI triggers an alert and generates a notable event.</td>
</tr>
<tr>
<td>Composite score</td>
<td>Based on a composite score of all KPIs added to the alert. Composite KPI scores are calculated from the KPI severity-level status and an importance value that you assign to the KPI when you create the alert.</td>
</tr>
</tbody>
</table>

Create a multi-KPI alert by selecting **Multi-KPI Alerts** from the top menu bar. You can also create one from a deep dive by selecting one or more KPI swim lanes and then selecting **Bulk Actions > Create Multi KPI Alert**.

**Status over time alerts**

Status over time alerts are multi-KPI alerts based on the severity level status of one or more KPIs. Status over time alerts require you to define one or more trigger conditions per selected KPI.

For example, you select two KPIs for your alert. The first KPI has a trigger for critical 15% of the time and a trigger for high 50% of the time. The second KPI has a single trigger for critical 25% of the time. The boolean expression would read:

\[(\text{kpi1\_perc\_crit} > 15\% \text{ OR kpi1\_perc\_high} > 50\%) \text{ AND (kpi2\_perc\_critical} > 25\%\)\]
Create a status over time alert

Prerequisites

You must have the `write_itsi_correlation_search` capability to create multi-KPI alerts.

Steps

1. On the Multi-KPI Alerts page, click **Status over time**.
2. In the **Services** column, select the service(s) that contain the KPIs for which you want to set up an alert. Note that only services that belong to teams for which you have read access are listed.
3. Optionally, select **Depends on** or **Impacts** to include KPIs from services that impact or depend on that service. All KPIs in each selected service appear in the "KPIs in Selected Services" section.
4. In the "KPIs in Selected Services" section, click **+Add** to add a KPI to the alert.
5. Set trigger conditions for the KPI alert. The condition statement dynamically updates based on the the trigger condition settings.

6. Click **Apply**. The selected KPI appears in the **Selected KPIs** section.
7. Add additional KPIs to the alert. Set one or more trigger conditions for each KPI.

   At least one trigger condition for each KPI must be satisfied simultaneously to trigger the alert and generate a notable event.
8. Click **Save**. The Create Correlation Search modal opens.
9. Configure the correlation search parameters to determine the schedule type, how often the search runs, and the severity of the notable event generated by the alert.
10. Click **Save**. ITSI saves the correlation search in **Settings > Searches, reports, and alerts**. For more information, see **Create correlation searches in ITSI**.

**Composite alerts**

Composite KPI alerts are based on a composite score of all KPIs added to the alert. Unlike service health scores, which give you a weighted average of all KPIs in a service, composite KPI scores give you the weighted average of the selected subset of KPIs only.

Composite KPI scores are calculated from the KPI severity-level status and an importance value that you assign to the KPI when you create the alert. This lets you create unique alerts for different groups of KPIs based on the relative importance of a KPI in the context of the alert.

The Importance value that you set for a KPI when you create a composite KPI alert does not change the Importance value that you set for the KPI (which is used to calculate the service health score) when you first create the KPI.

**Create a composite KPI alert**

**Prerequisites**

You must have the `write_itsi_correlation_search` capability to create multi-KPI alerts.

**Steps**

1. On the Multi-KPI Alerts page, click **Composite score**.
2. In the **Services** column, select the service(s) that contain the KPIs for which you want to set up an alert. Note that only services that belong to teams for which you have read access are listed. The KPIs in each service appear in the "KPIs in Selected Services" section.
3. Click **+Add** to select KPIs that you want to include in the composite KPI alert. The selected KPIs appear in the "Selected KPIs" section.
4. Set an Importance factor for each KPI. The composite score for all selected KPIs dynamically updates based on the selected Importance...
5. Click **Save**. The Create Correlation Search dialog appears.

6. Configure correlation search parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alert me if</td>
<td>Defines the suppression conditions for the alert.</td>
</tr>
<tr>
<td></td>
<td>◊ <strong>Score</strong> - If the composite score value is less than the value you specify, the alert triggers.</td>
</tr>
<tr>
<td></td>
<td>◊ <strong>Status</strong> - If the composite score severity level meets the condition you select, the alert triggers.</td>
</tr>
<tr>
<td>Suppression</td>
<td>Ignores notable events generated for the same alert condition. Enable suppression to minimize the number of duplicate notable events sent to Episode Review.</td>
</tr>
<tr>
<td>Trigger if</td>
<td>Generate notable events based on trigger conditions that occur simultaneously.</td>
</tr>
<tr>
<td></td>
<td>◊ <strong>Count</strong> - If the number of occurrences of the alert condition meets or exceeds the value over time that you specify, the alert triggers.</td>
</tr>
<tr>
<td></td>
<td>◊ <strong>Consecutive Count</strong> - If the number of consecutive occurrences of the alert condition meets or exceeds the value that you specify, the alert triggers.</td>
</tr>
</tbody>
</table>

7. Click **Next** and specify how the alert should appear in Episode Review.

8. Click **Save**.

ITSI saves the correlation search in **Configure > Correlation Searches** and **Settings > searches, reports, and alerts**. For more information, see Create correlation searches in ITSI in this manual.

For an end-to-end troubleshooting scenario that involves creating a multi-KPI alert, see Troubleshoot an outage in ITSI in the *Splunk IT Service Intelligence Use Cases* manual.
Managing Content

Schedule maintenance downtime in ITSI

Splunk IT Service Intelligence (ITSI) lets you put services and entities into maintenance mode for a specific time period. Use maintenance mode to prevent ITSI from triggering alerts from machines and other devices that are undergoing maintenance operations or don't require active monitoring.

For example, if your ticketing system experiences a failure and you start to receive a cascade of identical notable events, you can put the service that is monitoring the ticketing system into maintenance mode to stop ITSI from generating alerts until the issue is resolved.

Create a new maintenance window

Maintenance windows apply to services and entities.

Prerequisites

By default, only users assigned the write-maintenance_calendar capability can create a maintenance window. By default, the itoa_admin and itoa_team_admin roles have this capability.

Steps

1. From the ITSI top menu bar, click Configure > Maintenance Windows.
2. Click Create Maintenance Window.
3. Provide a title for the maintenance window. For example, "DB entity maintenance window."
4. Set the start time, duration, and end time for the maintenance window.
5. Select the Objects for which you want to create a maintenance window: Entities or Services.

If you don't have write access to the Global team, you can't put entities into maintenance mode.

6. Click Next.
7. Select the specific services or entities that you want to place in maintenance mode for the duration of the maintenance window. You can only select services or entities for which you have write access.
8. Click **Create**. The selected entities or services enter maintenance mode according to the defined schedule.

When viewing a scheduled maintenance window, you can only see the services included in the maintenance window for which you have read access. If a maintenance window only contains services for which you don't have read access, you can't view the maintenance window. All users can view a maintenance window that contains only entities.

If you're bulk deleting maintenance windows, you can only delete the maintenance windows that contain services or entities for which you have write access.

**Impact of maintenance windows**

Maintenance windows can have an impact on associated KPIs, service health score calculations, and other ITSI features.

Consider the following when you put a service into maintenance mode:

- All KPIs associated with that service are automatically put into maintenance mode.
- ITSI ignores search results from KPIs in maintenance mode for the purpose of service health score calculation for the duration of the maintenance window.
- Maintenance windows don't affect adaptive threshold calculations. Search results from KPIs in maintenance mode don't count when looking back at past data to calculate threshold values.

Consider the following when you put an entity into maintenance mode:

- If the entity has no KPIs running searches against it, there is no impact on service health scores.
- If the entity has one or more KPIs running searches against it, all search results from all KPIs running against that entity are ignored for the purpose of service health score calculation.
- If a KPI is split by entity, for example if the same KPI is running against two different entities, and one entity is in maintenance mode and one is not, search results generated by the KPI running against the entity in maintenance mode are ignored for the purpose of health score calculation. Search results generated by the same KPI running against the entity that's not in maintenance mode are included as usual in the service health score calculation.
You can put an entity in full or partial maintenance mode without it being explicitly put into maintenance mode, if a service that contains the entity is put in maintenance mode.

**Impact on ITSI features**

Services, entities, and KPIs that are fully or partially impacted by a maintenance window appear in a dark gray color on pages that display health scores, including service analyzers, service and entity details pages, glass tables, multi-KPI alerts, and deep dives.

**View impacted KPIs**

You can view the impact of a maintenance window on associated KPIs.

1. Select a maintenance window from the Maintenance Windows lister page. The maintenance window details page opens, showing the specific services or entities impacted by the maintenance window.
2. Click **Impacted KPIs** to see a list of KPIs impacted by the maintenance window. KPIs that are split by entity, and thus are currently running searches against other entities that are not in maintenance mode, are listed as "Partially" impacted. KPIs that are not split by entity are listed as "Fully" impacted.
When to schedule maintenance windows

It is a best practice to schedule maintenance windows with a 15- to 30-minute time buffer before and after you start and stop your maintenance work. This gives the system an opportunity to catch up with the maintenance state and reduces the chances of ITSI generating false positives during maintenance operations.

For example, if a server will be shut down for maintenance at 1:00PM and restarted at 5:00PM, the ideal maintenance window is 12:30PM to 5:30PM.

The 15- to 30-minute time buffer is a rough estimate based on 15 minutes being the time period over which most KPIs are configured to search data and identify alert triggers.

Back up and restore ITSI KV store data

Regularly backing up the KV store lets you restore your data from a backup in the event of a disaster or if you add a search head to a cluster. You can perform both full backups and partial backups of your data.

When you run a backup job, ITSI saves your data to a set of JSON files compressed into a single ZIP file located in `$SPLUNK_HOME/var/itsi/backups` on the search head. ITSI detects and preserves the application version that it creates a backup from. When you restore from a backup, ITSI detects the correct version of the backup and performs the required migration.

Splunk Cloud customers must use the Backup/Restore Jobs page in the ITSI user interface. All other customers can back up and restore their data from the command line using the `kvstore_to_json.py` script. For more information, see Backup and restore operations (mode 1).

The following table describes the functionality available in each backup and restore method:

<table>
<thead>
<tr>
<th>Method</th>
<th>Backup/Restore UI</th>
<th>Command line script</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full backup</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Partial backup</td>
<td>X</td>
<td>X</td>
<td>If you perform a partial backup using the command line script, the backup does not include</td>
</tr>
</tbody>
</table>
Splunk Enterprise offers an option to back up and restore the KV store. For more information, see Back up and restore KV store in the Splunk Enterprise Admin Manual. However, an ITSI backup is specifically formatted to process the content in the ITSI backup files. The Splunk Enterprise backup is not formatted like an ITSI backup, so you cannot use it to back up your ITSI data.

ITSI processes all backup content. ITSI also triggers many other activities, such as saved search generation and object dependency updates. Directly restoring Splunk Enterprise KV store data does not restore the ITSI system completely. Instead, use the processes described in this topic to back up your ITSI data.

What gets backed up

The following table describes the types of data included and not included in an ITSI backup.

<table>
<thead>
<tr>
<th>Data</th>
<th>Example</th>
<th>Included in backup?</th>
</tr>
</thead>
<tbody>
<tr>
<td>KV store objects</td>
<td>Services, service templates, entities, KPIs, KPI base searches, teams, glass tables, service analyzers, deep dives</td>
<td>Yes</td>
</tr>
<tr>
<td>Indexed data</td>
<td>ITSI summary index, notable events</td>
<td>No</td>
</tr>
</tbody>
</table>
To back up indexed data, use the same approach you use to back up other Splunk indexes. For more information, see Back up indexed data in the Splunk Enterprise Managing Indexers and Clusters of Indexers manual.

**Default scheduled backup**

The default scheduled backup is a full backup that runs daily at 1:00 AM in the server’s local time zone. The time of the backup job is displayed on the Backup/Restore Jobs page. You cannot create additional scheduled backup jobs.

The following limits apply to keeping scheduled backup files in the backup history:

- A minimum of 7 days if running a daily scheduled backup
- A minimum of 14 days if running a weekly scheduled backup
- A maximum of 30 days for all scheduled backup files

The oldest backup file automatically deletes from the backup history after the retention time expires. To set the schedule and retention time period for scheduled backups, edit the settings as defined in the next section.

*Edit the default scheduled backup*

When you edit the default scheduled backup, you can change the name of the scheduled backup, the frequency and time to run the scheduled backup, how many days to keep the backup file, or you can disable the scheduled backup. You cannot delete the scheduled backup job.

**Prerequisites**

You must have the itoa_admin role to view and edit the settings for the default scheduled backup job.

**Steps**

1. Click **Configure > Backup/Restore** from the ITSI top menu bar.
2. Click the default scheduled backup, or in the Actions column, click **Edit > Edit**.
3. (Optional) Change the name and add a description for the default scheduled backup.
4. (Optional) Enable **Include .conf files** to back up the following configuration files located in `$SPLUNK_HOME/etc/apps/SA-ITOA/local` and `$SPLUNK_HOME/etc/apps/itsi/local`.
ITSI only backs up these .conf files if they exist in a non-default directory, such as `~/splunk/etc/apps/itsi/local`. For more information, see About configuration files. When restored, the backed up .conf file overrides the existing local version.

5. Select a daily or weekly schedule, including the time, to run the scheduled backup. The default setting runs the backup job daily at 1:00 AM in the server's local time zone.

6. Set the number of days you want to keep the backup file. The oldest backup file automatically disappears from the backup history after the retention time expires.

7. Click Save.

Create a full backup

Create a full backup to make a copy of all your ITSI configuration information.

Before creating a backup, make sure no service templates are syncing. Check the sync status of service templates by clicking `Configure > Service Templates` from the ITSI top menu bar.

Prerequisites

You must have the `itoa_admin` role or the `write_itsi_backup_restore` capability to create a backup job.

Steps

1. Click `Configure > Backup/Restore` from the ITSI top menu bar.
2. Click `Create Job > Create Backup Job`.
3. Select `Full Backup`.
4. Provide a name and description of the backup job.
5. (Optional) Enable **Include .conf files** to back up the following configuration files located in `$SPLUNK_HOME/etc/apps/SA-ITOA/local` and `$SPLUNK_HOME/etc/apps/itsi/local`:

- `alert_actions.conf`
- `app_common_flags.conf`
- `commands.conf`
- `deep_dive_drilldowns.conf`
- `glasstable_icon_library.conf`
- `inputs.conf`
- `itsi_settings.conf`
- `limits.conf`
- `macros.conf`
- `notable_event_actions.conf`
- `savedsearches.conf` (only in `$SPLUNK_HOME/etc/apps/SA-ITOA/local`)

ITSI backs up these .conf files only if they exist in a non-default directory, such as `$SPLUNK_HOME/etc/apps/itsi/local`. For more information, see About configuration files. When restored, the backed up .conf file overrides the existing local version.

6. Click **Create**.

The backup job appears on the Backup/Restore Jobs page with the status Queued until the job runs. When the backup job finishes, the status changes to Completed and a confirmation message appears in the Messages drop-down list in Splunk Web.

You can run any completed backup job again by clicking **Edit > Start Backup** in the Actions column. You can also modify the completed backup job before running it again.

**Create a partial backup**

Create a partial backup if you want to back up a subset of your KV store objects. You can back up services, service templates, teams, glass tables, and configuration files. When selecting one of these object types, dependent objects are automatically selected to preserve the functionality of the objects after they are restored. In some cases, you can choose whether or not to include dependent objects in the backup.

Before creating a backup, make sure no service templates are syncing. Check the sync status of service templates by clicking **Configure > Service Templates** from the ITSI top menu bar.
What happens when you back up a service

When you back up a service, ITSI also backs up the following objects:

♦ KPI base searches
♦ Threshold templates
♦ Teams

You can also choose whether to back up the following associated objects:

♦ Dependent services
♦ Entities that match service entity rules
♦ A linked service template

If you do not choose to back up an associated object, the dependency between a service and the object breaks when you restore.

What happens when you back up a service template

When you back up a service template, all the services linked to the service template are added to the backup. If you choose to not back up a linked service, it will not exist in the restored environment.

What happens when you back up a team

When you back up a team, all the services associated with that team are added to the backup. You can deselect any services you do not want to back up.

What happens when you back up a glass table

When you back up a glass table, all of the services associated with that glass table are added to the backup. If you choose not to back up a service that the glass table depends on, any visualizations that use KPIs from the service will no longer function.

Glass table images and access control lists (ACLs) are always included in the backup when you back up a glass table.

What happens when you back up a deep dive

When you back up a deep dive, all of the services associated with that deep dive are also added to the backup. If you choose not to back up a service that the deep dive depends on, any KPI swimlanes from the service will no longer
function if the service does not exist in the restored environment.

Prerequisites

You must have the itoa_admin role or the write_itsi_backup_restore capability to create a backup job.

Steps

1. Click Configure > Backup/Restore.
2. Click Create Job > Create Backup Job.
3. Select Partial Backup.
4. Provide a name and description of the backup.
5. (Optional) Toggle Include .conf files to back up the following configuration files located in $SPLUNK_HOME/etc/apps/SA-ITOA/local and $SPLUNK_HOME/etc/apps/itsi/local:
   - alert_actions.conf
   - app_common_flags.conf
   - commands.conf
   - deep_dive_drilldowns.conf
   - glasstable_icon_library.conf
   - inputs.conf
   - itsi_settings.conf
   - limits.conf
   - macros.conf
   - notable_event_actions.conf
   - savedsearches.conf (only in $SPLUNK_HOME/etc/apps/SA-ITOA/local)
   
   ITSI backs up these .conf files only if they exist in a non-default directory, such as $SPLUNK_HOME/etc/apps/itsi/local. For more information, see About configuration files. When restored, the backed up .conf file overrides the existing local version.
6. Click Next.
7. On the partial backup page, select the objects to include in the backup. If you select one object type, it can cause other object types to be automatically selected if there are dependencies between the objects.
8. (Optional) Click Change Settings to change the objects that are selected when you select a service. By default, dependent services are selected. The KPI base searches, threshold templates, and team associated with a service are always included in the backup.
9. (Optional) Although entities are not listed in the partial backup page, you can include them in the backup file by selecting Entities in the Settings dialog box.
10. After making your selections, verify the objects that you selected.
11. Click **Save and Backup**.

The backup job appears on the Backup/Restore Jobs page with the status Queued until the job runs. When the backup job finishes, the status changes to Completed and a confirmation message appears in the Messages drop-down list in Splunk Web.

You can edit any partial backup job before it starts. When the backup job starts, you see a read-only view that lists the objects contained in the partial backup.

You can run any completed backup job again by clicking **Edit > Start Backup** in the Actions column. You can also modify the completed backup job before running it again.

**Restore a full or partial backup**

Restoring a backup merges the JSON data contained in the backup ZIP file with your existing KV store data in the following ways:

- If you added new objects since you created the backup, ITSI keeps these objects.
- If an existing object matches an object in the backup file, the existing object is replaced.
- All other existing objects are preserved.

Use the **command line script** instead of the UI to restore a backup in the following scenarios:

- You want to delete all existing KV store objects in an ITSI instance and replace them with the objects in the backup for a clean restore.
- You want to selectively restore files in a backup. Restoring from the UI restores all of the data in the backup file.

If you restart Splunk software while a backup or restore job is in progress, the job resumes after the restart is complete. Queued jobs automatically time out if they are not completed within 12 hours. You can change the default timeout duration by updating the value of `job_queue_timeout` in the `[backup_restore]` stanza in a local version of `itsi_settings_conf`.
How restoring handles teams

ITSI teams were introduced in version 3.0. If you are restoring from an earlier version of ITSI to version 3.0 or later, all services and service-related objects are placed in the Global team. These objects include entities, KPI templates, KPI base searches, and KPI threshold templates. Backups and subsequent restores on ITSI version 3.0 or later retain team information for services and service-related objects. See Overview of service-level permissions in ITSI for information about teams.

When you restore a backup taken on ITSI version 3.0 or later to another ITSI version 3.0 or later, team ACLs are retained when the teams are restored. The roles assigned to the teams must exist on the system that the backup is restored to. For example, suppose a restore creates teams called “HR” and “Finance”, which have read/write access for the hr_admin and finance_admin roles. If the current system does not have these roles, only the itoa_admin role can access these teams. If the roles assigned to the teams don’t exist on the system, you can create them either before or after restoring.

Prerequisites

♦ Before restoring a backup, make sure no service templates are syncing. Check the sync status of service templates by clicking Configure > Service Templates from the ITSI main menu.
♦ Make sure all technology add-ons (TAs), supporting add-ons (SAs), and domain add-ons (DAs) that exist on the old system are installed on the new system.
♦ If you’ve made modifications to any add-ons on the old system, manually copy those add-ons over the new system before restoring.

Restore from a backup

You can restore from a default scheduled backup or a backup that you created.

1. On the ITSI top menu bar, click Configure > Backup/Restore and find the backup that you want to restore from.
2. Click Edit > Restore Backup.
3. If you are restoring a scheduled backup, select a saved backup from the list. If you are restoring a created backup, go to the next step.
4. Click Start Restore.

Restore from prepends the backup name in the jobs list. A message stating that the restore job successfully completed appears in the
messages drop-down list in Splunk Web.

5. (Optional) If you restore from a backup that contains .conf files, you must restart Splunk software.

**Restore from a backup ZIP file**

You can download any backup ZIP file that is created when you run a backup job in the UI and then restore from that backup ZIP file using the Backup/Restore Jobs UI. The maximum file size supported for uploading a backup file is 500 MB.

Perform the following steps to download a backup ZIP file:

1. On the ITSI top menu bar, click **Configure > Backup/Restore** and find the backup file that you want to download.
2. Click **Edit > Download Backup**. If you are restoring a scheduled backup, select a saved backup from the list. If you are restoring a created backup, the backup file displays.
3. Save the file. The backup ZIP file downloads to your local machine.

Perform the following steps to restore from a downloaded backup ZIP file:

1. On the Backup/Restore Jobs page, click **Create Job > Create Restore Job**.
2. Provide a name and an optional description of the backup.
3. Click **Choose File** and select the previously downloaded backup ZIP file that you want to restore from.
4. (Optional) Toggle **Include .conf files** to restore any configuration files included in the backup.
5. Click **Create**.
   ITSI uploads the backup ZIP file and the new restore job appears in the Backup/Restore Jobs list. A message stating that the restore job has successfully completed appears in the Message drop-down list in Splunk Web.
6. (Optional) If you restore from a backup that contains .conf files, you must restart Splunk software.

**Restore from a backup created using the command line**

If you created a backup of ITSI using the `kvstore_to_json.py` command line option, and you want to restore that data using the Backup/Restore Jobs page, the backup JSON files must be contained in a folder named backup and compressed into a ZIP file. For information, see `kvstore_to_json.py` operations in ITSI.
Back up and restore in a search head cluster environment

You can run backup and restore jobs from the Backup/Restore page in search head cluster environments. You can create a backup on any cluster member and then later restore data from that backup on any cluster member, regardless of where the backup was initiated.

For example, suppose your search head cluster has three cluster members: sh-01, sh-02, and sh-03. If you create a backup on sh-01, you can later restore from that backup on sh-01, sh-02, or sh-03.

When you create a backup on any search head cluster member, the configuration data from all cluster members is backed up. Likewise, when you restore from a backup on any cluster member, configuration data is restored across all cluster members.

In a search head cluster environment, the scheduled backup runs only on the search head cluster captain. However, you can perform a restore of a scheduled backup from any cluster member. If you download the scheduled backup, make sure to download it from the captain because the captain contains the latest backup.

kvstore_to_json.py operations in ITSI

ITSI provides a kvstore_to_json.py script that lets you backup/restore ITSI configuration data, perform bulk service KPI operations, apply time zone offsets for ITSI objects, and regenerate KPI search schedules.

Usage options

The kvstore_to_json.py script is located in $SPLUNK_HOME/etc/apps/SA-ITOA/bin/.

The kvstore_to_json.py script has these 4 modes:

Mode 1: Backup and restore operations
Mode 2: Bulk service KPI operations.
Mode 3: Time zone offset operations.
Mode 4: Regenerate KPI search schedules.

To view all kvstore_to_json.py usage options, specify the -h option.
Usage: kvstore_to_json.py [options]

Options:
  -h, --help     show this help message and exit
  -s SPLUNKDPORT, --splunkdport=SPLUNKDPORT
      splunkd port. If no option is provided, we will
      default to '8089'
  -u USERNAME, --username=USERNAME
      Splunk username
  -p PASSWORD, --password=PASSWORD
      Splunk password
  -n, --no-prompt
      Use this option when you want to disable the
      prompt
  -v, --verbose
      Use this option for verbose logging
  -f FILE_PATH, --filepath=FILE_PATH
      The full path of a directory. Usage depends on
      mode.
      When importing backed up data of version 1.2.0,
      this
      could be a file or a set of files. When working
      with
      service KPIs, this is a directory containing
      input.json on entry and output.json on exit.
  -m MODE, --mode=MODE
      Specify the mode of operation - what kind of
      operations to perform. Mode is set to:
      1 - for
      backup/restore operations.        2 - for
      service KPI
      operations.
      Backup and restore operations. This is mode 1:
      Use this option when you want to perform backup/restore operations.

  -i, --importData
      Use this option when you want to upload data to
      the KV
      Store. When importing data from version 1.2.0,
      you can
      use filepath as wildcard to upload data from
      more than
      one file. However, filepath must be within
      quotes if
      it is being used as a wildcard
  -d, --persist-data
      Use this option when you want to persist
      existing
      configuration in KV Store during import. NOTE:
      Applicable only if importData option is used
-y, --dry-run
    Use this option when you want only to list
    objects for import or backup
-a, --conf-file
    Use this option when you want to back up .conf
    files.
-b BR_VERSION, --base-version=BR_VERSION
    The original ITSI application version user
    intends to backup/restore from.
-l RULE_FILE_PATH, --rule_file_path=RULE_FILE_PATH
    The full path of a file which has rules defined
    for backing up data or importing data
-e DUPNAME_TAG, --dupname-tag=DUPNAME_TAG
    Automatically rename all the duplicated service
    or entity names from restoring with a tag. If this
    option is not set, the restoring will halt if
duplicate names are detected. The default tag is:
    _dup_from_restore_<epoch_timestamp>

Service KPI operations. This is mode 2.:
Use this option when you want to get/create/update/delete KPIs for
existing services.
-g, --get
    For input, specify a list of service keys with
    the keys of KPIs to retrieve. Expected format:
    [{_key:
      <service key>, kpis: [{_key: <KPI key>}]}].
Specify [] to get all KPIs from all services. Specify
[{_key:
  <service key>, kpis: []} to get all KPIs from a
  service. Assumes input is available in
  file_path/input.json
-c, --create
    For input, specify a non-empty list of service
    keys with their KPIs list. Expected format: [{_key:
    <service key>, kpis: [{_key: <KPI key>, <rest
    of KPI structure}>]}]. Note that only existing services
could be updated with new KPIs only with this option.
Assumes input is available in
file_path/input.json
-t, --update
    For input, specify a non-empty list of service
    keys with their KPIs list. Expected format: [{_key:
    <service key>, kpis: [{_key: <KPI key>, <rest

205
of KPI and option.

file_path/input.json: Assumes input is available in

-r, --delete: For input, specify a list of service keys with the keys for the KPIs to delete. Expected format:

[{{_key: <service key>, kpis: {{_key: <KPI key>}}}]].

Assumes input is available in file_path/input.json

Timezone offset operations. This is mode 3:

Use this option when you want to adjust timezone settings for time sensitive fields on object configuration.

-q IS_GET, --is_get=IS_GET: For input, specify if you are trying to read objects or update their timezone offsets.

-o OBJECT_TYPE, --object_type=OBJECT_TYPE: For input, specify a valid object type that contains time sensitive configuration. This option will apply offset to all objects on this type unless scoped to a specific object using object_key parameter. Supported object types are: "maintenance_calendar" for maintenance windows, "service" for Services/KPIs (threshold policies).

-k OBJECT_TITLE, --object_title=OBJECT_TITLE: For input, specify an optional object title of object type that contains time sensitive configuration. Using this option will cause the offset change to only apply to that object.

-z OFFSET_IN_SEC, --offset_seconds=OFFSET_IN_SEC: For input, specify the offset to apply in seconds as a positive or negative number. This offset should be the number of seconds that you want to add or subtract from the current value.
Running the script in a search head cluster environment

When running the `kvstore_to_json.py` script in a replicated KV store environment, the script works on any member of the search head cluster. It does not require execution on the captain.

It is best practice to run the script on the MongoDB captain, which might be different than the captain of the search head cluster.

Backup and restore operations (mode 1)

Use `kvstore_to_json.py` mode 1 to back up and restore your ITSI configuration data to and from JSON files. You can use the `kvstore_to_json` script to do full or partial backups, full or partial restores, and merged or clean restores.

See Backup and restore ITSI configuration data for a summary of the types of data included and not included in an ITSI backup.

You can run the `kvstore_to_json` script in either interactive mode or non-interactive mode. In interactive mode, which is the default, the script prompts you to enter required information. To run the script in non-interactive mode, you must enter the `-n` option to disable the default interactive mode. You can schedule backups through cron by calling the script with all necessary flags for full automation.

Before performing a backup or restore through the CLI, make sure that there are no service template syncs in progress. Check the sync status of service templates in the Service Template viewer by selecting Configure > Service Templates from the top menu.

Perform a full backup using interactive mode

1. Run `kvstore_to_json.py`, where `-s` is the default splunkd port. If you are running `splunkd` on any other port besides 8089, you must specify the port. For example:
   ```bash
   cd $SPLUNK_HOME
   bin/splunk cmd python etc/apps/SA-ITOA/bin/kvstore_to_json.py -s 8089 -u admin -p changeme -m 1 -f /root/backup
   ```
2. Enter the requested information at the prompts. For example:
   ```bash
   >> Enter the splunkd port number OR press the enter key to use [8089]
   >> Do you wish to backup data from KV Store OR restore to KV
   ```

207
You have indicated backup of data from current ITSI version 4.0.3. Proceeding.

The script copies your KV store data to a series of JSON files in the /root/backup directory. If the /root/backup directory does not exist, the script creates it.

3. Go to /root/backup to confirm that your backup JSON files have been created. Backup file names follow the specific format: 
<COLLECTION_NAME>___<OBJECT_TYPE>___<ROLLOVER_NUMBER>. For example:

* itsi_migration___migration___0.json
* itsi_pages___glass_table___0.json
* itsi_services___entity___0.json
* itsi_services___kpi_threshold_template___0.json
* itsi_pages___deep_dive___0.json
* itsi_service_analyzer___home_view___0.json
* itsi_services___kpi_template___0.json
* itsi_services___service___0.json
* itsi_services___correlation_search___0.json

Do not change the JSON file name. If you change the file name you cannot restore the data.

**Perform a full backup using non-interactive mode**

1. Run kvstore_to_json.py, using the appropriate backup options. Enter -n to disable the default interactive mode. Use the -b option to specify the ITSI version that you want to back up. If you do not specify -b, the current ITSI version is used. For example:

   cd $SPLUNK_HOME
   bin/splunk cmd python etc/apps/SA-ITO/bin/kvstore_to_json.py -s 8089 -u admin -p changeme -m 1 -f /root/backup -n -b "4.0.3"

2. Go to /root/backup and confirm that your backup JSON files have been created.

**Restore from a backup using interactive mode**

ITSI supports restore migration from the current backup or an earlier version of the backup. You can migrate backup JSON files based on an earlier ITSI version to the most recent ITSI version. You can restore all the files in a backup or selected files.

**Prerequisite**
Team access control lists are retained when the teams are restored. Therefore, the roles assigned to the teams must exist on the system to which the backup is restored. For example, a restore creates teams called HR and Finance which have read/write access for the roles hr_admin and finance_admin, respectively. If the current system does not have the hr_admin and finance_admin roles, these teams will only be accessible to the itoa_admin role. If the roles assigned to the teams don't already exist on the system, create them either prior to restoring or after restoring.

Steps

1. Run kvstore_to_json.py, using the -i --importData option to upload data from your JSON backup files to the KV store. For example:

   cd $SPLUNK_HOME
   bin/splunk cmd python etc/apps/SA-ITOA/bin/kvstore_to_json.py -s 8089 -u admin -p changeme -m 1 -f /root/backup -i

2. Enter the requested information at the prompt. For example:

   >> Do you wish to backup data from KV Store OR restore to KV store. Press [y|yes|enter] to backup, [n|no] to restore? > n
   >> Do you wish to include .conf files? [y|n|enter]: > y
   You would like to restore data from disk to KV Store. Proceeding.
   >> Enter the previous ITSI version from which you want the data to be restored. Ex: '2.2.0', '2.2.1', '2.2.2' >
   >> Do you wish to persist the existing data in KV Store during the import [y|n]: > y

   Caution: The -i option deletes all existing data from the KV store. If you do not want to delete all data from the KV store on import, enter y at the prompt to use -d --persist data option. This option appends data to the existing data in the KV store.

3. Open the ITSI app and verify that your configuration data has been restored.

Restore from a backup using non-interactive mode

To restore data using non-interactive mode, you must use the -b option to specify the ITSI version of the backup file you plan to restore.

ITSI supports restore migration from the current backup or an earlier version of the backup. You can migrate backup JSON files based on an earlier ITSI version to the most recent ITSI version. You can restore all the files in a backup or selected files.
Prerequisite

Team access control lists are retained when the teams are restored. Therefore, the roles assigned to the teams must exist on the system to which the backup is restored. For example, a restore creates teams called HR and Finance which have read/write access for the roles hr_admin and finance_admin, respectively. If the current system does not have the hr_admin and finance_admin roles, these teams will only be accessible to the itoa_admin role. If the roles assigned to the teams don’t already exist on the system, create them either prior to restoring or after restoring.

Steps

1. Run `kvstore_to_json.py`, using the `--importData` option to upload data from your JSON backup files to the KV store. Use the `-b` option to specify the ITSI version of the backup file. Make sure to include the `-n` option to disable interactive mode. For example:

   ```bash
cd $SPLUNK_HOME
bin/splunk cmd python etc/apps/SA-ITOA/bin/kvstore_to_json.py -s 8089 -u admin -p changeme -m 1 -f /root/backup -i -n -b "4.0.3" -d
```

   The `-i` option deletes all data from the KV store. If you do not want to delete all data from the KV store on import, enter the `-d --persist data` option. This option appends data to the existing data in the KV store.

2. Open the ITSI app and verify that your configuration data has been restored.

Use a wildcard to specify groups of files

You can use a wildcard with the `-f` option to specify a group of files. For example, to import the files

```
itsi_export.json
itsi_export_0.json
itsi_export_1.json
```

you could enter the `-f` path as follows:

```bash
cd $SPLUNK_HOME
bin/splunk cmd python etc/apps/SA-ITOA/bin/kvstore_to_json.py -s 8089 -u admin -p changeme -m 1 -f "/root/itsi_export*" -i
```

The value of `-f` must be in quotes.
Perform a partial backup

Support for partial backups using the `kvstore_to_json.py` script is removed in version 4.3.0. See [Removed features in Splunk IT Service Intelligence](#). Use the Backup/Restore page in the ITSI UI to do partial backups. For information, see [Create a partial backup](#).

Perform a partial restore

You can use the `kvstore_to_json.py` script to perform a partial restore on a subset of your ITSI configuration data.

Prerequisites

To perform a partial restore of ITSI data, you must first create a JSON file that defines rules for the data restore. The rules file has the following schema:

```
[  
    {  
        object_type (required): <object_type>  (Top level objects, valid values are ['service', 'entity', 'home_view', 'kpi_template', 'deep_dive', 'kpi_threshold_template', 'correlation_search', 'glass_table']),  
        title_list (conditional required): regex/string or list of regex/string based titles for import of all objects that match this regex/string (Required or define key_list)  
        key_list (conditional required): list of keys - considered only if title is not defined (Required only if title is empty or not defined)  
        replacement_rules (optional): [  
            {  
                replacement_key (required): title/_key  
                replacement_type (required): (replace, prefix, postfix)  
                replacement_string (required): "regex/string"  
                replacement_pattern (required only for replace type):  
                "regex/string"  
            }  
            .........  
        ]  
    }  
    .........  
}  
```

For example, perform the following steps to restore a single object, such as a service:

1. In any directory, create a JSON rules file. For example:
touch rules.json

2. Edit rules.json to define rules for importing the object. For example:

```
{
  "object_type": "service",
  "title_list": "^Database Service$"
}
```

**Steps**

Use partial restore when you have a full backup of your ITSI configuration data and you want to restore only a few objects, instead of all objects.

For example, to restore a single object, such as a service:

1. In any directory, create a JSON rules file. For example:
   
   ```
touch rules.json
   ```

2. Edit rules.json to define rules for importing the object. For example:

   ```
   {
     "object_type": "service",
     "title_list": "^Database Service$"
   }
   ```

3. Run the `kvstore_to_json.py` command using the dry run (-y) option, where -f is the path to the folder containing your full data backup, -l is the path to the rules.json file, -i is the option to import data, and -d is the option to persist data (to avoid deletion of existing objects). For example:

   ```
   ./bin/splunk cmd python etc/apps/SA-ITOA/bin/kvstore_to_json.py
   -u admin -p changeme -f /root/full_backup_folder -l
   /root/partial_back_up/rules.json -i -d -y -n
   ```

4. After you verify that the list of objects to import in the dry run is correct, run the command without the dry run (-y) option to perform the actual restore operation.

**Use replacement options**

The partial restore rules schema provides replacement options, which let you change the name of an object when you run a partial backup/restore operation. Replacement options are useful for renaming objects when moving from a test environment to a production environment.

For example, to backup a service called `test_database_service`, but change the name to `database_service`; and to backup a deep dive called `test_database_deep_dive`, and change the name to `database_deep_dive`, you
would create a `rules.json` file that contains the following:

```
[
{
  "object_type": "service",
  "title_list": "^test_database_service$",
  "replacement_rules": [ {
    "replacement_key": "title",
    "replacement_type": "replace",
    "replacement_string": "database_service",
    "replacement_pattern": "^test_database_service$"
  }]
},
{
  "object_type": "entity",
  "title_list": ["10.12.*", "*host_database*"]
},
{
  "object_type": "deep_dive",
  "title_list": "^test_database_deep_dive$",
  "replacement_rules": [ {
    "replacement_key": "title",
    "replacement_type": "replace",
    "replacement_string": "database_deep_dive",
    "replacement_pattern": "^test_database_deep_dive$"
  }]
}
]
```

**Service KPI operations (mode 2)**

`kvstore_to_json.py` mode 2 options let you run bulk operations on KPIs, including get (-g), create (-c), update (-t), and delete (-r). Use these options to replicate, edit, and copy KPIs to multiple services, for example, when moving your ITSI deployment from a test environment to a production environment.

All service KPI options require you to specify the mode 2 parameter `-m 2`. You must also specify the file path `-f` parameter as the full path to the directory containing the `input.json` file.

Before you can run service KPI operations, you must create an `input.json` file in the destination directory. The script accepts data input from `input.json` and sends data output to an `output.json` file that the script creates in the same directory.

All service KPI operations, except get `-g`, require you to specify service and/or KPI keys. You can retrieve these keys using the `-g` option in `output.json`.  

213
See the `kvstore_to_json.py` help -h option for proper `input.json` and command syntax.

**Get service and KPI keys**

Use the get -g option to retrieve service and KPI data in JSON format, including service and KPI keys.

1. Create an `input.json` file in the destination directory.

    ```bash
    mkdir <directory_containing_input.json>
touch input.json
    ```

2. Edit `input.json`: Add `[]` to the file to retrieve JSON data for all services and KPIs, or add specific service and kpi keys to the file to retrieve JSON data for those services and KPIs only. For example:

    ```json
    ["_key": "<service_key>", "kpis": [{"_key": "<kpi_key>"} ] ]
    ```

3. Run the `kvstore_to_json` script using the get -g option. Name the full path to the directory containing the `input.json` file as the file path -f parameter. For example:

    ```bash
    cd $SPLUNK_HOME
    bin/splunk cmd python kvstore_to_json.py -u admin -p changeme -m 2
    -g -f <directory_containing_input.json> -n
    ```

4. Review the contents of `output.json` to identify service and KPI keys. For example:

    ```json
    [
    
    "_key": "669c5cec-a492-419d-8659-95a185b4dc5c",
    "kpis": [ 
    
    "_key": "f017cc7b2e67f2b3b9152146",
    ]
    ]
    ```

**Create KPIs**

Use the -c option to create new KPIs.

1. Edit `input.json` to specify the service key of the service for which you want to create the KPI.
2. Add KPI keys for the KPIs that you want to add to the service and any
key-value pairs belonging to the KPI that you want to include in the KPI definition. Leave the key field for each KPI empty for ITSI to auto generate it. For example:

```
[
  {
    "_key": "<service_key>",
    "kpis": [
      {
        "title": "<title_of_kpi_to_create>",
        ...
      }
    ]
  }
]
```

**Update KPIs**

Use the `-t` option to update KPIs.

In `input.json` specify the service and KPI key for each KPI, and any other key/value pair data that you want to update for the KPI.

**Delete KPIs**

Use the `-r` option to delete KPIs.

In `input.json`, specify service and kpi keys for all KPIs that you want to delete.

**Caution:** Make sure to properly validate your JSON input. While the `kvstore_to_json` script does provide some schema validation, incorrect JSON formatting can cause errors.

**Time zone offset operations (mode 3)**

The `kvstore_to_json.py` mode 3 option lets you apply a time offset for time-sensitive fields in object configurations. You can use this option to correct time zone discrepancies for the following object types:

- **maintenance_calendar**: Sets an offset for maintenance window start and end times.
- **service**: Sets an offset for the KPI threshold time policies within a service. See Apply time zone offsets in this manual.
- **kpi_threshold_template**: Sets an offset for a KPI threshold template. After running the command to set an offset for a KPI threshold template,
you must run the command again for each service that uses the KPI threshold template and set the same offset so that they are in sync.

**Apply time zone offset**

Run the following command to set an offset for one of the supported object types.

If you use the command to set an offset for a KPI threshold template, you must run the command again for each service that uses the KPI threshold template and set the same offset so that they are in sync.

1. Run `kvstore_to_json.py`, where `-o` is the object type, `-k` is the title of the specific object, and `-z` is the specific time zone offset in seconds. For example:

   ```bash
   cd $SPLUNK_HOME
   bin/splunk cmd python etc/apps/SA-ITOA/bin/kvstore_to_json.py -m 3 -o service -k "Database Service" -z 1800
   ```

2. Enter the requested information at the prompts (default interactive mode only). For example:

   ```bash
   >> Enter the splunkd port number OR press the enter key to use [8089] > 8089
   >> Enter splunk username or press enter to use "admin" > admin
   >> Enter splunk password for "admin" >
   ```

3. The script applies the time zone offset to the specified object. For example:

   ```bash
   1 object(s) match request
   Applying timezone change on requested object(s): [u'Database Service']
   Timezone offset has been applied on the objects requested.
   ```

ITSI time-sensitive configurations are normalized to UTC.

**Regenerate KPI search schedules (mode 4)**

The `kvstore_to_json.py` mode 4 option regenerates the search schedules for your KPIs. Use this command if you have set your KPI saved search schedules to run at the same time in `itsi_settings.conf`. Run this command to reset the search schedules of all your KPIs to use the new search schedule. See `Schedule KPI searches to update at the same time` for more information.

1. Run `kvstore_to_json.py` in mode 4. For example:
cd $SPLUNK_HOME
bin/splunk cmd python etc/apps/SA-ITOA/bin/kvstore_to_json.py -m 4

2. Enter the requested information at the prompts (default interactive mode only).

3. You will see the following message after the KPI search schedules have been reset:
   Retrieving KPIs to reset their saved search scheduling
   Saving updated KPI scheduling
   Done.

Create and manage saved searches in ITSI

Create a saved search, also called a scheduled report, in Splunk IT Service Intelligence. You can use these saved searches when importing entities and services.

1. Click **Settings > Searches, Reports, and Alerts**.
2. Click **New Report**. When you define a report in Settings, you set it up as a saved search. It appears as a report on the lister page when you're done.
3. Provide a title in the format "IT Service Intelligence - <custom text>". For example, IT Service Intelligence - get my entities. This format is required for the saved search to show up when importing entities and services from a saved search in ITSI.
4. Provide a search string under Search.
5. (Optional) Provide the search **Earliest time** and **Latest time** using **relative time modifiers**. If you want the search to run over all time, leave these fields blank.
6. For **App**, select IT Service Intelligence (its).
7. Click **Save**.
8. After the search saves, locate the search on the lister page and click **Edit > Edit Permissions**.
9. For **Display For**, select **All apps**.
10. Click **Save**.
11. Restart Splunk software to add the search to savedsearches.conf.

The search now appears in the list of predefined ITSI saved searches when you import services and entities.
See also

- Import services from a Splunk search
- Create and edit reports
Administer Splunk ITSI with configuration files

About configuration files

Splunk IT Service Intelligence configuration information is stored in configuration files. These files are identified by the .conf extension and hold the information for different aspects of your ITSI configurations. These aspects include:

- System settings
- Authentication and authorization information
- KPI, glass table, and deep dive configurations
- Notable event configurations
- Module settings

A single Splunk instance typically has multiple versions of configuration files across several directories. You can have configuration files with the same name in your default, local, and app directories. This creates a layering effect that allows Splunk to determine configuration priorities based on factors such as the current user and the current app.

For a list of ITSI configuration files and an overview of the area each file covers, see List of ITSI configuration files in this manual.

Most configuration files come packaged with your ITSI software in the $SPLUNK_HOME/etc/apps/ directory.

Editing a configuration file

Never change, copy, or move the configuration files in the default directory. Default files must remain intact and in their original location. To change settings for a particular ITSI configuration file, you must first create a new version of the file in a non-default directory and then add the settings that you want to change. When you first create this new version of the file, start with an empty file. Do not start from a copy of the file in the default directory.

Before you change any configuration files:
• Learn about how the default configuration files work, and where to put the files that you edit. See Configuration file directories.
• Learn about the structure of the stanzas that comprise configuration files and how the attributes you want to edit are set up. See Configuration file structure.
• Learn how different versions of the same configuration files in different directories are layered and combined. See Configuration file precedence.
• Consult the .spec and .example files for the configuration file. These files reside in the file system in $SPLUNK_HOME/etc/apps/SA-ITOA/README or $SPLUNK_HOME/etc/apps/itsi/README

After you are familiar with the configuration file content and directory structure, and understand how to leverage configuration file precedence, see How to edit a configuration file to learn how to safely modify your files.

List of ITSI configuration files

The following is a list of ITSI configuration files. All files are located under $SPLUNK_HOME/etc/apps/. Most .conf files have accompanying spec and example files located in the README folder that list all supporting attributes. Contact Support before editing a conf file that does not have an accompanying spec or example file.

If you are using Splunk Cloud, you can't edit a .conf file directly. For any task that requires editing a .conf file, submit a ticket using the Support Portal and Splunk Support will work with you to arrange a maintenance window.

Caution: Never change or copy the configuration files in the default directory. Default files must remain intact and in their original location. The upgrade process overwrites the default directory, so any changes that you make in the default directory are lost on upgrade. Create and edit your files in a local directory, for example $SPLUNK_HOME/etc/apps/<app_name>/local. Local directories are not overwritten during upgrades. For more information, see Configuration file directories.

<table>
<thead>
<tr>
<th>File</th>
<th>Purpose</th>
<th>ITSI Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>alert_actions.conf</td>
<td>Generate ITSI notable events and configure episode actions.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>File</td>
<td>Purpose</td>
<td>ITSI Location</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>alert_actions.conf</td>
<td>Summarizing KPI searches into the ITSI summary index.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>app_common_flags.conf</td>
<td>Used to enable or disable certain ITSI features. CAUTION: Do not edit this file.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>authorize.conf</td>
<td>Configure ITSI-specific roles and capabilities, including role-based access controls. Always use /itsi/default. For more information, see Enable/disable ITSI capabilities for a role.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>collections.conf</td>
<td>Configure KV store collections for ITSI.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>commands.conf</td>
<td>Connect search commands to any custom search script.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>datamodels.conf</td>
<td>Attribute/value pairs for configuring data models.</td>
<td>/DA-ITSI-APPSERVER/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/DA-ITSI-LB/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>/DA-ITSI-VIRTUALIZATION/default</td>
</tr>
<tr>
<td>deep_dive_drilldowns.conf</td>
<td>Configure deep dive drilldowns, add new drilldowns.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>File</td>
<td>Purpose</td>
<td>ITSI Location</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>distsearch.conf</td>
<td>Specify behavior for distributed search. Group search peers to facilitate searching on a subset of peers.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>drilldownsearch_offset.conf</td>
<td>Configure time range picker presets for correlation search drilldown offsets.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>fields.conf</td>
<td>Create multivalue fields and add search capability for indexed fields.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>glasstable_icon_library.conf</td>
<td>Add and remove icons from the glass table icon library.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>inputs.conf</td>
<td>Set up data inputs.</td>
<td>/SA-ITOA/default /itsi/default</td>
</tr>
<tr>
<td>itsi_base_service_template.conf</td>
<td>An internal file that determines the templates shipped by default with ITSI for integration with SAI. For information, see Overview of creating an ITSI service using an SAI service template.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>File</td>
<td>Purpose</td>
<td>ITSI Location</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>itsi_da.conf</td>
<td>(Deprecated) Configure an app to export entity searches and service</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td></td>
<td>templates for use within ITSI.</td>
<td></td>
</tr>
<tr>
<td>itsi_deep_dive.conf</td>
<td>Upload deep dives to the KV store.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_event_management.conf</td>
<td>Configure Episode Review default settings.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_glass_table.conf</td>
<td>Upload glass tables to the KV store.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_kpi_base_search.conf</td>
<td>Upload KPI base searches to the KV store.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_kpi_template.conf</td>
<td>Upload KPI templates to the KV store.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_kpi_threshold_template.conf</td>
<td>Upload KPI threshold templates to the KV store.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_module_settings.conf</td>
<td>Define whether a module is editable in the module lister page. Default is false.</td>
<td>/DA-ITSI-EUEM/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-WEBSERVER/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-OS/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-VIRTUALIZATION/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-APPSERVER/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-LB/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-APM/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-DATABASE/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-STORAGE/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-CLOUD/default</td>
</tr>
<tr>
<td>File</td>
<td>Purpose</td>
<td>ITSI Location</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------------------------------------------</td>
</tr>
<tr>
<td>itsi_module_viz.conf</td>
<td>Change tab names and panel titles in a module details dashboard.</td>
<td>/DA-ITSI-EUEM/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-WEBSERVER/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-OS/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-VIRTUALIZATION/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-APPSERVER/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-LB/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-APM/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-DATABASE/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-STORAGE/default</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DA-ITSI-CLOUD/default</td>
</tr>
<tr>
<td>itsi_notable_event_retention.conf</td>
<td>Define how long notable events are retained before they move to the index. Default is 6 months.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_notable_event_severity.conf</td>
<td>Configure the colors associated with different severity levels in Episode Review.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_notable_event_status.conf</td>
<td>Configure label descriptions and event status in Episode Review.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_service_analyzer.conf</td>
<td>Configure auto-refresh interval, or disable auto-refresh.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_service_template.conf</td>
<td>Configure an app to export service</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>File</td>
<td>Purpose</td>
<td>ITSI Location</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------</td>
</tr>
<tr>
<td>itsi_settings.conf</td>
<td>Configure ITSI.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>itsi_team.conf</td>
<td>Upload sample ITSI teams to the KV store.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>limits.conf</td>
<td>Set various limits (such as maximum result size or concurrent real-time searches) for search commands.</td>
<td>/SA-ITOA/default /itsi/default</td>
</tr>
<tr>
<td>macros.conf</td>
<td>Define search macros in Settings.</td>
<td>/SA-ITOA/default /itsi/default</td>
</tr>
<tr>
<td>mad.conf</td>
<td>Configure anomaly detection.</td>
<td>/SA-ITSI-MetricAD/default</td>
</tr>
<tr>
<td>notable_event_actions.conf</td>
<td>Configure actions to take on groups in Episode Review.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>notable_event_commonality.conf</td>
<td>Define fields to include or exclude from the Common Fields tab of Episode Review.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>notable_event_correlation.conf</td>
<td>Set threshold values and limits for Smart Mode event correlation.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>File</td>
<td>Purpose</td>
<td>ITSI Location</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>props.conf</td>
<td>Set indexing property configurations, including timezone offset, custom source type rules, and pattern collision priorities. Also, map transforms to event properties.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>restmap.conf</td>
<td>Create custom REST endpoints.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>savedsearches.conf</td>
<td>Define ordinary reports, scheduled reports, and alerts.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>searchbnf.conf</td>
<td>Configure the search assistant.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>threshold_labels.conf</td>
<td>Configure settings for severity-level thresholds. Change the label, color, threshold level, health weight, minimum and maximum health score, and score contribution.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>threshold_periods.conf</td>
<td>Deprecated. Do not edit.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>File</td>
<td>Purpose</td>
<td>ITSI Location</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------</td>
</tr>
<tr>
<td>transforms.conf</td>
<td>Configure regex transformations to perform on data inputs. Use in tandem with props.conf.</td>
<td>/SA-ITOA/default</td>
</tr>
<tr>
<td>ui-tour.conf</td>
<td>Customize the ITSI product tour.</td>
<td>/itsi/default</td>
</tr>
<tr>
<td>visualizations.conf</td>
<td>Declare common visualizations that other modules can use.</td>
<td>/SA-ITSI-CustomModuleViz/default</td>
</tr>
<tr>
<td>web.conf</td>
<td>Configure Splunk Web, enable HTTPS.</td>
<td>/SA-ITOA/default</td>
</tr>
</tbody>
</table>
Configuration file reference

alert_actions.conf

The following are the spec and example files for alert_actions.conf.

alert_actions.conf.spec

# This file contains possible attributes and values for generating ITSI notable events and configuring episode actions.
#
# There is an alert_actions.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/default/.
# To set custom configurations, place an alert_actions.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local/. You must restart Splunk to enable
# configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the
top
#   of the file.
# * Each .conf file should have at most one default stanza. If there are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
#   the
#   file wins.
# * If an attribute is defined at both the global level and in a
#   specific
#   stanza, the value in the specific stanza takes precedence.

ttl = <integer> [p]
* The minimum time to live (TTL), in seconds, of the search artifacts
  if this action is triggered.
* If p follows the integer, then the integer is the number of scheduled periods.
* Default: 600 (10 minutes)

maxtime = <integer> [m|s|h|d]
* The maximum amount of time that the execution of an action is allowed to take before the action is aborted.
* Use the d, h, m and s suffixes to define the period of time:
  d = day, h = hour, m = minute and s = second.
  For example: 5d means 5 days.
* If you do not include a suffix, the time defaults to seconds.
* Default: 600 (10 minutes)

maxresults = <integer>
* The maximum number of search results sent via the alert.
* Default: 10000

is_custom = <boolean>
* Specifies whether the alert action is based on the custom alert actions framework and is supposed to be listed in the search UI.
* Default: 1

label = <string>
* Defines the label shown in the UI.
* If not specified, the stanza name is used instead.

description = <string>
* Defines the description shown in the UI.

payload_format = [xml|json]
* The format in which the alert script receives the configuration via STDIN.
* Default: json

[itsi_event_generator]

* Generate notable events under this stanza name.
* ITSI sends notable events to the ITSI summary index.
* Follow this stanza name with any number of the following attribute/value pairs.
* If you do not specify an entry for each attribute, Splunk will use the default value.

param.http_token_name = <string>
* The HTTP token name.
* Optional.
* If you do not provide a token name, ITSI obtains one token using the index and sourcetype parameters below.
param.index = <string>
* The index name.
* This setting is required if you do not provide an HTTP
token for the 'param.http_token_name' setting.
* Default: itsi_tracked_alerts

param.sourcetype = <string>
* The sourcetype.
* This setting is used if you do not provide an HTTP
token for the 'param.http_token_name' setting.
* Default: itsi_notable:event

param.event_identifier_fields = <comma-separated list>
* A list of fields that are used to identify event duplication.
* Default: source

param.search_type = <string>
* The search type.
* Default: custom

param.is_use_event_time = <boolean>
* If "1", ITSI uses the actual event time.
* If "0", ITSI uses the time the event was indexed.
* Default: 0

param.event_field_max_length = <integer>
* The maximum field length.
* Default: 10000

[itsi_sample_event_action_ping]

* Ping a host in one or more ITSI episodes under this stanza name.
* Follow this stanza name with any number of the following
  attribute/value pairs.
* If you do not specify an entry for each attribute, Splunk will
  use the default value.

param.host_to_ping = <string>
* The field from the episode representing the host to ping.
* If your event contains the field 'server', set to '%server%'.
* When ITSI executes the alert action, it extracts the value
  corresponding
to the token value from event data and tries to ping it.
* If you set a value that does not begin and end with '%', ITSI
  considers this to be the value to ping. No extractions are done in
  this case.
* Default: %orig_host%
**[itsi_event_action_link_ticket]**

* Set options to associate an episode with a ticket from an external ticketing system under this stanza name.
* Follow this stanza name with any number of the following attribute/value pairs.
* If you do not specify an entry for each attribute, Splunk will use the default value.

**param.ticket_system** = <string>
* The name of the external ticketing system.
* This setting is required to create/update/delete a ticket.
* There is no default.

**param.ticket_id** = <string>
* The ID of the specific ticket to link to.
* This setting is required to create/update/delete a ticket.
* There is no default.

**param.ticket_url** = <string>
* The drilldown link to the ticket in the external ticketing system.
* This setting is required to create/update a ticket.
* There is no default.

**param.operation** = <upsert|delete>
* Specifies the type of action to take on the ticket.
* If "upsert", ITSI inserts or updates existing fields.
* If "delete", ITSI deletes the ticket.
* There is no default.

**param.kwarg** = <dict>
* A dictionary of additional fields to pass to the ticket.
* Optional.
* There is no default.

**[itsi_event_action_send_to_phantom]**

* Set options to send an episode to Phantom under this stanza name.
* Follow this stanza name with any number of the following attribute/value pairs.
* If you do not specify an entry for each attribute, Splunk will use the default value.

**is_custom** = <boolean>
* Specifies whether the alert action is based on the custom alert actions framework and is supposed to be listed in the search UI.
* Default: 1

**label** = <string>
* Defines the label shown in the UI.
* If not specified, the stanza name is used instead.

description = <string>
* Defines the description shown in the UI.

payload_format = [xml|json]
* The format in which the alert script receives
  the configuration via STDIN.
* Default: json

alert_actions.conf.example

No example

app_common_flags.conf

The following are the spec and example files for app_common_flags.conf.

app_common_flags.conf.spec

# This file contains attributes and values for disabling (feature
flagging)
# certain ITSI features.
#
# There is an app_common_flags.conf in
# $SPLUNK_HOME/etc/apps/itsi/default.
# To set custom configurations, place an app_common_flags.conf in
# $SPLUNK_HOME/etc/apps/itsi/local/. You must restart Splunk software
to
# enable configurations.
#
# To learn more about configuration files (including precedence) please
see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
#
# CAUTION: This is an internal configuration file used to turn off
certain ITSI
# features that are incomplete. Do NOT edit or remove this file.
GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
#  * You can also define global settings outside of any stanza, at the top
#    of the file.
#  * Each .conf file should have at most one default stanza. If there are
#    multiple default stanzas, attributes are combined. In the case of
#    multiple definitions of the same attribute, the last definition in
#    the file wins.
#  * If an attribute is defined at both the global level and in a specific
#    stanza, the value in the specific stanza takes precedence.

[<app_common_flag>]

* Each stanza represents a feature within Splunk IT Service Intelligence (ITSI).
* If the feature is disabled, it is currently incomplete and should NOT be enabled.

feature = <string>
* The name of the feature.

description = <string>
* A description of what the feature does.

disabled = <boolean>
* Whether the feature is enabled or disabled.
* If "1", the feature is disabled.
* If "0", the feature is enabled.

app_common_flags.conf.example

No example

authorize.conf

The following are the spec and example files for authorize.conf.
authorize.conf.spec

#   Version 7.3.0
#
# This file contains possible attribute/value pairs for creating roles in
# authorize.conf. You can configure roles and granular access controls by
# creating your own authorize.conf.
#
# There is an authorize.conf in $SPLUNK_HOME/etc/system/default/. To set
# custom configurations, place an authorize.conf in
# $SPLUNK_HOME/etc/system/local/. For examples, see authorize.conf.example.
# You must restart Splunk to enable configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
#
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
#   * You can also define global settings outside of any stanza, at the top
#     of the file.
#   * Each .conf file should have at most one default stanza. If there are
#     multiple default stanzas, attributes are combined. In the case of
#     multiple definitions of the same attribute, the last definition in
#     the file wins.
#   * If an attribute is defined at both the global level and in a specific
#     stanza, the value in the specific stanza takes precedence.

[default]

srchFilterSelecting = <boolean>
* Determines whether a role's search filters are used for selecting or
  eliminating during role inheritance.
* If "true", the search filters are used for selecting. The filters are
  joined
with an OR clause when combined.
* If "false", the search filters are used for eliminating. The filters
  are joined
  with an AND clause when combined.
* Example:
  * role1 srchFilter = sourcetype!=ex1 with selecting=true
  * role2 srchFilter = sourcetype=ex2 with selecting = false
  * role3 srchFilter = sourcetype!=ex3 AND index=main with selecting =
    true
  * role3 inherits from role2 and role 2 inherits from role1
  * Resulting srchFilter = ((sourcetype!=ex1) OR
    (sourcetype!=ex3 AND index=main)) AND ((sourcetype=ex2))
  * Default: true

[capability::<capability>]

* DO NOT edit, remove, or add capability stanzas. The existing
  capabilities
  are the full set of Splunk system capabilities.
* Splunk software adds all of its capabilities this way.
* For the default list of capabilities and assignments, see
  authorize.conf
  under the 'default' directory.
* Only alphanumeric characters and "_" (underscore) are allowed in
  capability names.
Examples:
  * edit_visualizations
  * view_license1
* Descriptions of specific capabilities are listed below.

[role_<roleName>]

<capability> = <enabled>
* A capability that is enabled for this role. You can list many
  capabilities
  for each role.
* NOTE: 'enabled' is the only accepted value here, as capabilities are
  disabled by default.
* Roles inherit all capabilities from imported roles, and you cannot
disable
  inherited capabilities.
* Role names cannot have uppercase characters. Usernames, however, are
  case-insensitive.
* Role names cannot contain spaces, colons, semicolons, or forward
  slashes.

importRoles = <semicolon-separated list>
* A list of other roles and their associated capabilities that Splunk
software should import.
* Importing other roles also imports the other aspects of that role, such as allowed indexes to search.
* By default a role imports no other roles.

grantableRoles = <semicolon-separated list>
* A list of roles that determines which users, roles, and capabilities that a user with a specific set of permissions can manage.
* This setting lets you limit the scope of user, role, and capability management that these users can perform.
* When you set 'grantableRoles', a user that holds a role with the 'edit_roles_grantable' and 'edit_user' capabilities can do only the following with regards to access control management for the Splunk Enterprise instance:
  * They can edit only the roles that contain capabilities that are a union of the capabilities in the roles that you specify with this setting.
  * Any new roles that they create can contain only the capabilities that are a union of these capabilities.
  * Any new roles that they create can search only the indexes that have been assigned to all roles that have been specified with this setting.
  * They can see only users who have been assigned roles that contain capabilities that are a union of these capabilities.
  * They can assign users only to roles whose assigned capabilities are a union of these capabilities.
* For this setting to work, you must assign a user at least one role that:
  * Has both the 'edit_roles_grantable' and 'edit_user' capabilities assigned to it, and
  * Does NOT have the 'edit_roles' capability assigned to it.
* Example:
  Consider a Splunk instance where roles role1-role4 have the following capabilities:

role1: cap1, cap2, cap3
role2: cap4, cap5, cap6
role3: cap1, cap6
role4: cap4, cap8

And users user1-user4 have been assigned the following roles:
user1: role1
user2: role2
user3: role3
user4: role4

If you define the 'grantableRoles' setting as follows for the 'power' role:
grantableRoles = role1;role2

and edit the role so that the 'edit_roles_grantable'
capability is selected, and the 'edit_roles' capability
is not selected,

then a user that has been assigned the 'power' role can make only
the following access control changes on the instance:
* View or edit the following users: user1, user2, user3
* Assign the following roles: role1, role2, role3
* Create roles with the following capabilities: cap1, cap2, cap3,
cap4, cap5, cap6
* Only the 'admin' role holds the 'edit_roles_grantable' capability on
a new Splunk Enterprise installation.
* If you make changes to the 'admin' role, 'grantableRoles' is set to
"admin".
* This setting does not work if you use tokens to authenticate into a
Splunk Enterprise instance.
* Default (if 'admin' role is edited): admin
* Default (otherwise): not set

srchFilter = <semicolon-delimited list>
* A list of search filters for this role.
* To override any search filters from imported roles, set this to "*",
as the 'admin' role does.
* By default, Splunk software does not perform search filtering.

srchTimeWin = <integer>
* Maximum time span, in seconds, of a search.
* This time window limit is applied backwards from the latest time
specified in a search.
* To override any search time windows from imported roles, set this to
"0" (infinite), as the 'admin' role does.
* "-1" is a special value implying that no search window has been set
for this role.
  * This is equivalent to not setting the 'srchTimeWin' setting at
all, which means it can be easily overridden by an imported role.
* By default, searches are not limited to any specific time window.

srchDiskQuota = <integer>
* The maximum amount of disk space, in megabytes, that can be used by
search jobs for a specific user with this role.
* In search head clustering environments, this setting takes effect on a
per-member basis. There is no cluster-wide accounting.
* The dispatch manager checks the quota at the dispatch time of a
  search.
  Additionally, the search process checks the quota at intervals that
  are defined
  in the 'disk_usage_update_period' setting in limits.conf as long as
  the
  search is active.
* A user can occasionally exceed the quota because the search process
  does
  not constantly check the quota.
* Exceeding this quota causes the search to be auto-finalized
  immediately,
  even if there are results that have not yet been returned.
* Default: 100

srchJobsQuota = <integer>
* The maximum number of concurrently running historical searches that a
  user
  with this role can have.
* This setting excludes real-time searches. See the 'rtSrchJobsQuota'
  setting.
* Default: 3

rtSrchJobsQuota = <integer>
* The maximum number of concurrently running real-time searches that a
  user
  with this role can have.
* Default: 6

srchMaxTime = <integer><unit>
* The maximum amount of time that search jobs from specific users with
  this role are
  allowed to run.
* After a search runs for this amount of time, it auto-finalizes.
* If the role inherits from other roles, the value of the 'srchMaxTime'
  setting is
  specified in the included roles.
* This maximum value does not apply to real-time searches.
* Examples: 1h, 10m, 2hours, 2h, 2hrs, 100s
* Default: 100days

srchIndexesDefault = <semicolon-separated list>
* A list of indexes to search when no index is specified.
* These indexes can be wild-carded ("*"), with the exception that "*"
  does not
  match internal indexes.
* To match internal indexes, start with an underscore ("_"). All
  internal indexes are
  represented by "_*".
* The wildcard character "*" is limited to match either all the
  non-internal
indexes or all the internal indexes, but not both at once.
* If you make any changes in the "Indexes searched by default" Settings pane
  for a role in Splunk Web, those values take precedence, and any wildcards
  you specify in this setting are lost.
* No default.

srchIndexesAllowed = <semicolon-separated list>
* A list of indexes that this role is allowed to search.
* Follows the same wildcarding semantics as the 'srchIndexesDefault' setting.
* If you make any changes in the "Indexes" Settings pane for a role in
  Splunk Web,
  those values take precedence, and any wildcards you specify in this
  setting are lost.
* No default.

deleteIndexesAllowed = <semicolon-separated list>
* A list of indexes that this role is allowed to delete.
* This setting must be used in conjunction with the 'delete_by_keyword'
capability.
* Follows the same wildcarding semantics as the 'srchIndexesDefault' setting.
* No default.

cumulativeSrchJobsQuota = <integer>
* The maximum total number of concurrently running historical searches
  across all members of this role.
* For this setting to take effect, you must set the
  'enable_cumulative_quota'
  setting to "true" in limits.conf.
* If a user belongs to multiple roles, the user's searches count against
  the role with the largest cumulative search quota. Once the quota for
  that role is consumed, the user's searches count against the role with
  the next largest quota, and so on.
* In search head clustering environments, this setting takes effect on a
  per-member basis. There is no cluster-wide accounting.
* No default.

cumulativeRTSrchJobsQuota = <integer>
* The maximum total number of concurrently running real-time searches
  across all members of this role.
* For this setting to take effect, you must set the
  'enable_cumulative_quota'
  setting to "true" in limits.conf.
* If a user belongs to multiple roles, the user's searches count against
  the role with the largest cumulative search quota. Once the quota for
  that role is consumed, the user's searches count against the role with
  the next largest quota, and so on.
* In search head clustering environments, this setting takes effect on a
  per-member basis. There is no cluster-wide accounting.
* No default.

[.tokens_auth]

* Settings for token authorization.

expiration = <relative-time-modifier>|never
* The relative time when an authorization token expires.
* The syntax for using time modifiers is:
  * [+]<time_integer><time_unit>@<time_unit>
  * Where time_integer is an integer value and time_unit is relative
time unit in seconds (s), minutes (m), hours (h) or days (d) etc.
* The steps to specify a relative time modifier are:
  * Indicate the time offset from the current time.
  * Define the time amount, which is a number and a unit.
  * Specify a "snap to" time unit. The time unit indicates the nearest
or latest time to which your time amount rounds down.
* For example, if you configure this setting to "+2h@h", the token
expires at
  the top of the hour, two hours from the current time.
* For more information on relative time identifiers, see "Time
Modifiers" in
* The default value indicates that a token never expires. To set token
expiration, you must set this value to a relative time value.
* Your account must hold the admin role to update this setting.
* This setting is optional.
* Default: never

disabled = <boolean>
* Disables and enables Splunk token authorization.
* Defaults to true.

[capability::accelerate_datamodel]

* Lets a user enable or disable data model acceleration.
[capability::accelerate_search]

* Lets a user enable or disable acceleration for reports.
* The assigned role must also be granted the 'schedule_search' capability.

[capability::run_multi_phased_searches]

* Lets a user in a distributed search environment run searches with three or more map-reduce phases.
* Lets users take advantage of the search performance gains related to parallel reduce functionality.
* Multi-phased searches can lead to higher resource utilization on indexers, but they can also reduce resource utilization on search heads.

[capability::admin_all_objects]

* Lets a user access all objects in the system, such as user objects and knowledge objects.
* Lets a user bypass any Access Control List (ACL) restrictions, similar to the way root access in a *nix environment does.
* Splunk software checks this capability when accessing manager pages and objects.

[capability::edit_tokens_settings]

* Lets a user access all token auth settings in the system, such as turning the feature on/off and system-wide expiration.
* Splunk checks this capability when accessing manager pages and objects.

[capability::change_authentication]

* Lets a user change authentication settings through the authentication endpoints.
* Lets the user reload authentication.

[capability::change_own_password]

* Lets a user change their own password. You can remove this capability
to control the password for a user.

[capability::delete_by_keyword]

* Lets a user use the 'delete' command.
* NOTE: The 'delete' command does not actually delete the raw data on disk.
   Instead, it masks the data (via the index) from showing up in search results.

[capability::dispatch_rest_to_indexers]

* Lets a user dispatch the REST search command to indexers.

[capability::edit_deployment_client]

* Lets a user edit the deployment client.
* Lets a user edit a deployment client admin endpoint.

[capability::edit_deployment_server]

* Lets a user edit the deployment server.
* Lets a user edit a deployment server admin endpoint.
* Lets a user change or create remote inputs that are pushed to the forwarders and other deployment clients.

[capability::edit_dist_peer]

* Lets a user add and edit peers for distributed search.

[capability::edit_encryption_key_provider]

* Lets a user view and edit keyprovider properties when using the Server-Side Encryption (SSE) feature for a remote storage volume.

[capability::request_pstacks]

* Lets a user trigger pstacks generation of the main splunkd process using a REST endpoint.
[capability::edit_watchdog]
* Lets a user reconfigure watchdog settings using a REST endpoint.

[capability::edit_forwarders]
* Lets a user edit settings for forwarding data, including settings for SSL, backoff schemes, and so on.
* Also used by TCP and Syslog output admin handlers.

[capability::edit_health]
* Lets a user disable or enable health reporting for a feature in the splunkd health status tree through the server/health-config/{feature_name} endpoint.

[capability::edit_httpauths]
* Lets a user edit and end user sessions through the httpauth-tokens endpoint.

[capability::edit_indexer_cluster]
* Lets a user edit or manage indexer clusters.

[capability::edit_indexerdiscovery]
* Lets a user edit settings for indexer discovery, including settings for master_uri, pass4SymmKey, and so on.
* Also used by Indexer Discovery admin handlers.

[capability::edit_input_defaults]
* Lets a user change the default hostname for input data through the server settings endpoint.
[capability::edit_local_apps]

* Lets a user edit apps on the local Splunk instance through the local apps endpoint.

[capability::edit_monitor]

* Lets a user add inputs and edit settings for monitoring files.
* Also used by the standard inputs endpoint as well as the oneshot input endpoint.

[capability::edit_modinput_winhostmon]

* Lets a user add and edit inputs for monitoring Windows host data.

[capability::edit_modinput_winnetmon]

* Lets a user add and edit inputs for monitoring Windows network data.

[capability::edit_modinput_winprintmon]

* Lets a user add and edit inputs for monitoring Windows printer data.

[capability::edit_modinput_perfmon]

* Lets a user add and edit inputs for monitoring Windows performance.

[capability::edit_modinput_admon]

* Lets a user add and edit inputs for monitoring Active Directory (AD).

[capability::edit_roles]

* Lets a user edit roles.
* Lets a user change the mappings from users to roles.
* Used by both user and role endpoints.
[capability::edit_roles_grantable]

* Lets a user edit roles and change user-to-role mappings for a limited set of roles.
* To limit this ability, also assign the 'edit_roles_grantable' capability
  and configure the 'grantableRoles' setting in authorize.conf.
  * For example:
    
    grantableRoles = role1;role2;role3
  
  This configuration lets a user create roles using the subset of capabilities that the user has in their 'grantable_roles' setting.

[capability::edit_scripted]

* Lets a user create and edit scripted inputs.

[capability::edit_search_head_clustering]

* Lets a user edit and manage search head clustering.

[capability::edit_search_concurrency_all]

* Lets a user edit settings related to maximum concurrency of searches.

[capability::edit_search_concurrency_scheduled]

* Lets a user edit settings related to concurrency of scheduled searches.

[capability::edit_search_scheduler]

* Lets a user disable and enable the search scheduler.

[capability::edit_search_schedule_priority]

* Lets a user assign a search a higher-than-normal schedule priority.
[capability::edit_search_schedule_window]

* Lets a user edit a search schedule window.

[capability::edit_search_server]

* Lets a user edit general distributed search settings like timeouts, heartbeats, and blacklists.

[capability::edit_server]

* Lets a user edit general server and introspection settings, such as the server name, log levels, and so on.
* This capability also inherits the ability to read general server and introspection settings.

[capability::edit_server_crl]

* Lets a user reload Certificate Revocation Lists (CRLs) within Splunk.
* A CRL is a list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted.

[capability::edit_sourcetypes]

* Lets a user create and edit sourcetypes.

[capability::edit_splunktcp]

* Lets a user change settings for receiving TCP input from another Splunk instance.

[capability::edit_splunktcp_ssl]

* Lets a user view and edit SSL-specific settings for Splunk TCP input.
[capability::edit_splunktcp_token]

* Lets a user view or edit splunktcptokens. The tokens can be used on a receiving system to only accept data from forwarders that have been configured with the same token.

[capability::edit_tcp]

* Lets a user change settings for receiving general TCP inputs.

[capability::edit_telemetry_settings]

* Lets a user change settings for opting in and sending telemetry data.

[capability::edit_token_http]

* Lets a user create, edit, display, and remove settings for HTTP token input.
* Enables the HTTP Events Collector feature, which is a way to send data to Splunk Enterprise and Splunk Cloud.

[capability::edit_tokens_all]

* Lets a user issue tokens to all users.

[capability::edit_tokens_own]

* Lets a user issue tokens to themself.

[capability::edit_udp]

* Lets a user change settings for UDP inputs.

[capability::edit_user]

* Lets a user create, edit, or remove other users.
* Also lets a user manage certificates for distributed search.
* To limit this ability, assign the 'edit_roles_grantable' capability
and configure the 'grantableRoles' setting in authorize.conf.
* Example: grantableRoles = role1;role2;role3

[capability::edit_view_html]

* Lets a user create, edit, or otherwise modify HTML-based views.

[capability::edit_web_settings]

* Lets a user change the settings for web.conf through the system settings endpoint.

[capability::export_results_is_visible]

* Lets a user show or hide the Export button in Splunk Web.
* Disable this setting to hide the Export button and prevent users with this role from exporting search results.

[capability::get_diag]

* Lets the user generate a diag on a remote instance through the /streams/diag endpoint.

[capability::get_metadata]

* Lets a user use the metadata search processor.

[capability::get_typeahead]

* Enables typeahead for a user, both the typeahead endpoint and the 'typeahead' search processor.

[capability::indexes_edit]

* Lets a user change any index settings such as file size and memory limits.
[capability::input_file]

* Lets a user add a file as an input through the inputcsv command (except for dispatch=t mode) and the inputlookup command.

[capability::license_tab]

* Lets a user access and change the license.
* DEPRECATED.
* Replaced with the 'license_edit' capability.

[capability::license_edit]

* Lets a user access and change the license.

[capability::license_view_warnings]

* Lets a user see if they are exceeding limits or reaching the expiration date of their license.
* License warnings are displayed on the system banner.

[capability::list_deployment_client]

* Lets a user list the deployment clients.

[capability::list_deployment_server]

* Lets a user list the deployment servers.

[capability::list_pipeline_sets]

* Lets a user list information about pipeline sets.

[capability::list_forwarders]

* Lets a user list settings for data forwarding.
* Used by TCP and Syslog output admin handlers.
[capability::list_health]

* Lets a user monitor the health of various Splunk features (such as inputs, outputs, clustering, and so on) through REST endpoints.

[capability::list_httpauths]

* Lets a user list user sessions through the httpauth-tokens endpoint.

[capability::list_indexer_cluster]

* Lets a user list indexer cluster objects such as buckets, peers, and so on.

[capability::list_indexerdiscovery]

* Lets a user view settings for indexer discovery.
  * Used by indexer discovery handlers.

[capability::list_inputs]

* Lets a user view the list of inputs including files, TCP, UDP, scripts, and so on.

[capability::list_introspection]

* Lets a user read introspection settings and statistics for indexers, search, processors, queues, and so on.

[capability::list_search_head_clustering]

* Lets a user list search head clustering objects such as artifacts, delegated jobs, members, captain, and so on.
[capability::list_search_scheduler]

* Lets a user list search scheduler settings.

[capability::list_settings]

* Lets a user list general server and introspection settings such as the server name and log levels.

[capability::list_metrics_catalog]

* Lets a user list metrics catalog information such as the metric names, dimensions, and dimension values.

[capability::edit_metrics_rollup]

* Lets a user create/edit metrics rollup defined on metric indexes.

[capability::list_storage_passwords]

* Lets a user access the /storage/passwords endpoint.
* Lets the user perform GET operations.
* The 'admin_all_objects' capability must be added to the role in order for the user to perform POST operations to the /storage/passwords endpoint.

[capability::list_tokens_all]

* Lets a user view all tokens.

[capability::list_tokens_own]

* Lets a user view their own tokens.

[capability::never_lockout]

* Allows a user's account to never lockout.
[capability::never_expire]

* Allows a user's account to never expire.

[capability::output_file]

* Lets a user create file outputs, including the 'outputcsv' command (except for dispatch=t mode) and the 'outputlookup' command.

[capability::request_remote_tok]

* Lets a user get a remote authentication token.
* Used for distributing search to old 4.0.x Splunk instances.
* Also used for some distributed peer management and bundle replication.

[capability::rest_apps_management]

* Lets a user edit settings for entries and categories in the Python remote apps handler.
* See restmap.conf.spec for more information.

[capability::rest_apps_view]

* Lets a user list various properties in the Python remote apps handler.
* See restmap.conf.spec for more info

[capability::rest_properties_get]

* Lets a user get information from the services/properties endpoint.

[capability::rest_properties_set]

* Lets a user edit the services/properties endpoint.

[capability::restart_splunkd]

* Lets a user restart Splunk software through the server control
[capability::rtsearch]

* Lets a user run real-time searches.

[capability::run_collect]

* Lets a user run the 'collect' command.

[capability::run_mcollect]

* Lets a user run the 'mcollect' and 'meventcollect' commands.

[capability::run_debug_commands]

* Lets a user run debugging commands, for example 'summarize'.

[capability::schedule_rtsearch]

* Lets a user schedule real-time saved searches.
* You must enable the 'scheduled_search' and 'rtsearch' capabilities for the role.

[capability::schedule_search]

* Lets a user schedule saved searches, create and update alerts, and review triggered alert information.

[capability::search]

* Lets a user run a search.

[capability::search_process_config_refresh]

* Lets a user manually flush idle search processes through the 'refresh search-process-config' CLI command.
**[capability::use_file_operator]**

* Lets a user use the 'file' command.
* The 'file' command is DEPRECATED.

**[capability::upload_lookup_files]**

* Lets a user upload files which can be used in conjunction with lookup definitions.

**[capability::web_debug]**

* Lets a user access /_bump and /debug/** web debug endpoints.

**[capability::edit_statsd_transforms]**

* Lets a user define regular expressions to extract manipulated dimensions out of metric_name fields in statsd metric data using the services/data/transforms/statsdextractions endpoint.
* For example, dimensions can be mashed inside a metric_name field like "dimension1.metric_name1.dimension2" and you can use regular expressions to extract it.

**[capability::edit_metric_schema]**

* Lets a user define the schema of the log data that must be converted to metric format using the services/data/metric-transforms/schema endpoint.

**[capability::list_workload_pools]**

* Lets a user list and view workload pool and workload status information through the workloads endpoint.

**[capability::edit_workload_pools]**

* Lets a user create and edit workload pool and workload configuration information (except workload rule) through the workloads endpoint.
[capability::select_workload_pools]

* Lets a user select a workload pool for a scheduled or ad-hoc search.

[capability::list_workload_rules]

* Lets a user list and view workload rule information from the workloads/rules endpoint.

[capability::edit_workload_rules]

* Lets a user create and edit workload rules through the workloads/rules endpoint.

[capability::apps_restore]

* Lets a user restore configurations from a backup archive through the apps/restore endpoint.

authorize.conf.example

```
#   Version 7.3.0
#
# This is an example authorize.conf. Use this file to configure roles and capabilities.
#
# To use one or more of these configurations, copy the configuration block
# into authorize.conf in $SPLUNK_HOME/etc/system/local/. You must reload auth or restart Splunk to enable configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

[role_ninja]
rtsearch = enabled
importRoles = user
```
srchFilter = host=foo
srchIndexesAllowed = *
srchIndexesDefault = mail;main
srchJobsQuota = 8
rtSrchJobsQuota = 8
srchDiskQuota = 500

# This creates the role 'ninja', which inherits capabilities from the 'user'
# role. ninja has almost the same capabilities as power, except cannot
# schedule searches.
#
# The search filter limits ninja to searching on host=foo.
#
# ninja is allowed to search all public indexes (those that do not start
# with underscore), and will search the indexes mail and main if no
# index is
# specified in the search.
#
# ninja is allowed to run 8 search jobs and 8 real time search jobs
# concurrently (these counts are independent).
#
# ninja is allowed to take up 500 megabytes total on disk for all their
# jobs.

commands.conf

The following are the spec and example files for commands.conf.

commands.conf.spec

#   Version 7.3.0
#
# This file contains possible attribute/value pairs for creating search
# commands for any custom search scripts created. Add your custom
# search
# script to $SPLUNK_HOME/etc/searchscripts/ or
# $SPLUNK_HOME/etc/apps/MY_APP/bin/. For the latter, put a custom
# commands.conf in $SPLUNK_HOME/etc/apps/MY_APP. For the former, put
# your
# custom commands.conf in $SPLUNK_HOME/etc/system/local/.
#
# There is a commands.conf in $SPLUNK_HOME/etc/system/default/ . For
# examples,
# see commands.conf.example. You must restart Splunk to enable
# configurations.
#
# To learn more about configuration files (including precedence) please
# see the
GLOBAL SETTINGS

Use the [default] stanza to define any global settings. You can also define global settings outside of any stanza, at the top of the file. Each conf file should have at most one default stanza. If there are multiple default stanzas, attributes are combined. In the case of multiple definitions of the same attribute, the last definition in the file wins. If an attribute is defined at both the global level and in a specific stanza, the value in the specific stanza takes precedence.

[<STANZA_NAME>]

* Each stanza represents a search command; the command is the stanza name.
* The stanza name invokes the command in the search language.
* Set the following attributes/values for the command. Otherwise, Splunk uses the defaults.
* If the filename attribute is not specified, Splunk searches for an external program by appending extensions (e.g. ".py", ".pl") to the stanza name.
* If chunked = true, in addition to ".py" and ".pl" as above, Splunk searches using the extensions ".exe", ".bat", ".cmd", ".sh", ".js", and no extension (to find extensionless binaries).
* See the filename attribute for more information about how Splunk searches for external programs.

**type = <string>**
* Type of script: python, perl
  * Defaults to python.

**filename = <string>**
* Optionally specify the program to be executed when the search command is used.
  * Splunk looks for the given filename in the app's bin directory.
  * The filename attribute can not reference any file outside of the app's
* If the filename ends in ".py", Splunk's python interpreter is used to invoke the external script.
* If chunked = true, Splunk looks for the given filename in
  `$SPLUNK_HOME/etc/apps/MY_APP/<PLATFORM>/bin` before searching
  `$SPLUNK_HOME/etc/apps/MY_APP/bin`, where `<PLATFORM>` is one of
  "linux_x86_64", "linux_x86", "windows_x86_64", "windows_x86",
  "darwin_x86_64" (depending on the platform on which Splunk is
  running on).
* If chunked = true and if a path pointer file (*.path) is specified,
  the contents of the file are read and the result is used as the
  command to be run. Environment variables in the path pointer
  file are substituted. Path pointer files can be used to reference
  system binaries (e.g. /usr/bin/python).

command.arg.<N> = <string>
* Additional command-line arguments to use when invoking this
  program. Environment variables will be substituted (e.g.
  `$SPLUNK_HOME`).
* Only available if chunked = true.

local = [true|false]
* If true, specifies that the command should be run on the search head
  only
* Defaults to false.

perf_warn_limit = <integer>
* Issue a performance warning message if more than this many input
  events are
  passed to this external command (0 = never)
* Defaults to 0 (disabled)

streaming = [true|false]
* Specify whether the command is streamable.
* Defaults to false.

maxinputs = <integer>
* Maximum number of events that can be passed to the command for each
  invocation.
* This limit cannot exceed the value of maxresultrows in limits.conf.
* 0 for no limit.
* Defaults to 50000.

passauth = [true|false]
* If set to true, splunkd passes several authentication-related facts
  at the start of input, as part of the header (see enableheader).
* The following headers are sent
  * authString: psuedo-xml string that resembles
    `<auth><userId>username</userId><username>username</username><authToken>auth_token</authToken></auth>`
  where the username is passed twice, and the authToken may be used
  to contact splunkd during the script run.
* sessionKey: the session key again.
* owner: the user portion of the search context
* namespace: the app portion of the search context
* Requires enableheader = true; if enableheader = false, this flag will be treated as false as well.
* Defaults to false.
* If chunked = true, this attribute is ignored. An authentication token is always passed to commands using the chunked custom search command protocol.

```
run_in_preview = [true|false]
* Specify whether to run this command if generating results just for preview rather than final output.
* Defaults to true
```

```
enableheader = [true|false]
* Indicate whether or not your script is expecting header information or not.
* Currently, the only thing in the header information is an auth token.
* If set to true it will expect as input a head section + '\n' then the csv input
* NOTE: Should be set to true if you use splunk.Intersplunk
* Defaults to true.
```

```
retainsevents = [true|false]
* Specify whether the command retains events (the way the sort/dedup/cluster commands do) or whether it transforms them (the way the stats command does).
* Defaults to false.
```

```
generating = [true|false]
* Specify whether your command generates new events. If no events are passed to the command, will it generate events?
* Defaults to false.
```

```
generates_timeorder = [true|false]
* If generating = true, does command generate events in descending time order (latest first)
* Defaults to false.
```

```
overrides_timeorder = [true|false]
* If generating = false and streaming=true, does command change the order of events with respect to time?
* Defaults to false.
```

```
requires_preop = [true|false]
* Specify whether the command sequence specified by the 'streaming_preop' key
is required for proper execution or is it an optimization only
* Default is false (streaming_preop not required)

streaming_preop = <string>
* A string that denotes the requested pre-streaming search string.

required_fields = <string>
* A comma separated list of fields that this command may use.
* Informs previous commands that they should retain/extract these fields if
  possible. No error is generated if a field specified is missing.
* Defaults to '**

supports_multivalues = [true|false]
* Specify whether the command supports multivalues.
* If true, multivalues will be treated as python lists of strings, instead of a
  flat string (when using Intersplunk to interpret stdin/stdout).
* If the list only contains one element, the value of that element will be
  returned, rather than a list
  (for example, isinstance(val, basestring) == True).

supports_getinfo = [true|false]
* Specifies whether the command supports dynamic probing for settings
  (first argument invoked == __GETINFO__ or __EXECUTE__).

supports_rawargs = [true|false]
* Specifies whether the command supports raw arguments being passed to it or if
  it prefers parsed arguments (where quotes are stripped).
* If unspecified, the default is false

undo_scheduler_escaping = [true|false]
* Specifies whether the commands raw arguments need to be unesacped.
* This is particularly applies to the commands being invoked by the scheduler.
* This applies only if the command supports raw arguments(supports_rawargs).
* If unspecified, the default is false

requires_srinfo = [true|false]
* Specifies if the command requires information stored in SearchResultsInfo.
* If true, requires that enableheader be set to true, and the full
  pathname of the info file (a csv file) will be emitted in the header under
  the key 'infoPath'
* If unspecified, the default is false

needs_empty_results = [true|false]
* Specifies whether or not this search command needs to be called with
  intermediate empty search results
* If unspecified, the default is true

changes_colorder = [true|false]
* Specify whether the script output should be used to change the column
  ordering of the fields.
* Default is true

outputheader = <true/false>
* If set to true, output of script should be
  a header section + blank line + csv output
* If false, script output should be pure csv only
* Default is false

clear_required_fields = [true|false]
* If true, required_fields represents the *only* fields required.
* If false, required_fields are additive to any fields that may be
  required by
  subsequent commands.
* In most cases, false is appropriate for streaming commands and true
  for
  reporting commands
* Default is false

stderr_dest = [log|message|none]
* What do to with the stderr output from the script
  * 'log' means to write the output to the job's search.log.
  * 'message' means to write each line as an search info message. The
    message
    level can be set to adding that level (in ALL CAPS) to the start of
    the
    line, e.g. "WARN my warning message."
  * 'none' means to discard the stderr output
  * Defaults to log

is_order_sensitive = [true|false]
* Specify whether the command requires ordered input.
* Defaults to false.

is_risky = [true|false]
* Searches using Splunk Web are flagged to warn users when they
  unknowingly run a search that contains commands that might be a
  security risk. This warning appears when users click a link or type
  a URL that loads a search that contains risky commands. This warning
  does not appear when users create ad hoc searches.
* This flag is used to determine whether the command is risky.
* Defaults to false.
  * Specific commands that ship with the product have their own defaults

chunked = [true|false]
* If true, this command supports the new "chunked" custom
search command protocol.
* If true, the only other commands.conf attributes supported are
  is_risky, maxwait, maxchunksize, filename, command.arg.<N>, and
  run_in_preview.
* If false, this command uses the legacy custom search command
  protocol supported by Intersplunk.py.
* Default is false

maxwait = <integer>
* Only available if chunked = true.
* Not supported in Windows.
* The value of maxwait is the maximum number of seconds the custom
  search command can pause before producing output.
* If set to 0, the command can pause forever.
* Default is 0

maxchunksize = <integer>
* Only available if chunked = true.
* The value of maxchunksize is maximum size chunk (size of metadata
  plus size of body) the external command may produce. If the command
  tries to produce a larger chunk, the command is terminated.
* If set to 0, the command may send any size chunk.
* Default is 0

commands.conf.example

# Version 7.3.0
#
# This is an example commands.conf. Use this file to configure settings
# for external search commands.
#
# To use one or more of these configurations, copy the configuration
# block
# into commands.conf in $SPLUNK_HOME/etc/system/local/. You must
# restart
# Splunk to enable configurations.
#
# To learn more about configuration files (including precedence)
# see the documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
#
# Note: These are examples. Replace the values with your own
# customizations.

####################
# defaults for all external commands, exceptions are below in
# individual stanzas
# type of script: 'python', 'perl'
TYPE = python
# default "filename" would be <stanza-name>.py for python,
# <stanza-name>.pl for perl, and
# <stanza-name> otherwise

# is command streamable?
streaming = false

# maximum data that can be passed to command (0 = no limit)
maxinputs = 50000

# end defaults

[createrss]
filename = createrss.py

[diff]
filename = diff.py

[gentimes]
filename = gentimes.py

[head]
filename = head.py

[loglady]
filename = loglady.py

[marklar]
filename = marklar.py

[runshellscript]
filename = runshellscript.py

[sendemail]
filename = sendemail.py

[translate]
filename = translate.py

[transpose]
filename = transpose.py

[uniq]
filename = uniq.py

[windbag]
filename = windbag.py
supports_multivalues = true
collections.conf

The following are the spec and example files for collections.conf.

collections.conf.spec

# Version 7.3.0
#
# This file configures the KV Store collections for a given app in Splunk.
# # To learn more about configuration files (including precedence) please see
# # the documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

[<collection-name>]

enforceTypes = true|false
* Indicates whether to enforce data types when inserting data into the collection.
* When set to true, invalid insert operations fail.
* When set to false, invalid insert operations drop only the invalid field.
* Defaults to false.

field.<name> = number|bool|string|time
* Field type for a field called <name>.
* If the data type is not provided, it is inferred from the provided JSON data type.

accelerated_fields.<name> = <json>
* Acceleration definition for an acceleration called <name>.
* Must be a valid JSON document (invalid JSON is ignored).
* Example: 'acceleration.foo={"a":1, "b":-1}' is a compound acceleration that first sorts 'a' in ascending order and then 'b' in descending order.
* There are restrictions in compound acceleration. A compound acceleration
  must not have more than one field in an array. If it does, KV Store does
  not start or work correctly.
* If multiple accelerations with the same definition are in the same
  collection, the duplicates are skipped.
* If the data within a field is too large for acceleration, you will see a
  warning when you try to create an accelerated field and the acceleration
  will not be created.
* An acceleration is always created on the _key.
* The order of accelerations is important. For example, an acceleration of
  \{ "a":1, "b":1 \} speeds queries on "a" and "a" + "b", but not on "b"
  lone.
* Multiple separate accelerations also speed up queries. For example,
  separate accelerations \{ "a": 1 \} and \{ "b": 1 \} will speed up queries on
  "a" + "b", but not as well as a combined acceleration \{ "a":1, "b":1 \}
* Defaults to nothing (no acceleration).

profilingEnabled = true|false
* Indicates whether to enable logging of slow-running operations, as defined
  in 'profilingThresholdMs'.
* Defaults to false.

profilingThresholdMs = <zero or positive integer>
* The threshold for logging a slow-running operation, in milliseconds.
* When set to 0, all operations are logged.
* This setting is only used when 'profilingEnabled' is true.
* This setting impacts the performance of the collection.
* Defaults to 1000.

replicate = true|false
* Indicates whether to replicate this collection on indexers. When false,
  this collection is not replicated, and lookups that depend on this
  collection will not be available (although if you run a lookup command
  with 'local=true', local lookups will still be available). When true,
  this collection is replicated on indexers.
* Defaults to false.

replication_dump_strategy = one_file|auto
* Indicates how to store dump files. When set to one_file, dump files are
  stored in a single file. When set to auto, dumps are stored in multiple
  files when the size of the collection exceeds the value of
'replication_dump_maximum_file_size'.
* Defaults to auto.

replication_dump_maximum_file_size = <unsigned integer>
* Specifies the maximum file size (in KB) for each dump file when
  'replication_dump_strategy=auto'.
* If this value is larger than 'concerningReplicatedFileSize', which is
  set in distsearch.conf, the value of 'concerningReplicatedFileSize' will
  be used instead.
* KV Store does not pre-calculate the size of the records that will be
  written to disk, so the size of the resulting files can be affected by the
  'max_rows_in_memory_per_dump' setting from 'limits.conf'.
* Defaults to 10240KB.

type = internal_cache|undefined
* Indicates the type of data that this collection holds.
* When set to 'internal_cache', changing the configuration of the
  current instance between search head cluster, search head pool, or standalone
  will erase the data in the collection.
* Defaults to 'undefined'.
* For internal use only.

collections.conf.example

#   Version 7.3.0
#
# The following is an example collections.conf configuration.
#
# To use one or more of these configurations, copy the configuration block
# into collections.conf in $SPLUNK_HOME/etc/system/local/. You must restart
# Splunk to enable configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
#
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
# Note this example uses a compound acceleration. Please check
# collections.conf.spec
# for restrictions on compound acceleration.

[mycollection]
field.foo = number
field.bar = string
accelerated_fields.myacceleration = {"foo": 1, "bar": -1}

datamodels.conf

The following are the spec and example files for datamodels.conf.

datamodels.conf.spec

# Version 7.3.0
#
# This file contains possible attribute/value pairs for configuring
data models. To configure a datamodel for an app, put your custom
datamodels.conf in $SPLUNK_HOME/etc/apps/MY_APP/local/

# For examples, see datamodels.conf.example. You must restart Splunk
to
# enable configurations.

# To learn more about configuration files (including precedence) please see
# the documentation located at
#
http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
#  * You can also define global settings outside of any stanza, at the
top
#    of the file.
#  * Each conf file should have at most one default stanza. If there
are
#    multiple default stanzas, attributes are combined. In the case of
#    multiple definitions of the same attribute, the last definition in
the
#    file wins.
#  * If an attribute is defined at both the global level and in a
specific
#    stanza, the value in the specific stanza takes precedence.
* Each stanza represents a data model. The data model name is the stanza name.

acceleration = `<bool>`
* Set acceleration to true to enable automatic acceleration of this data model.
* Automatic acceleration creates auxiliary column stores for the fields and values in the events for this datamodel on a per-bucket basis.
* These column stores take additional space on disk, so be sure you have the proper amount of disk space. Additional space required depends on the number of events, fields, and distinct field values in the data.
* The Splunk software creates and maintains these column stores on a schedule you can specify with `acceleration.cron_schedule`. You can query them with the `tstats` command.

acceleration.earliest_time = `<relative-time-str>`
* Specifies how far back in time the Splunk software should keep these column stores (and create if acceleration.backfill_time is not set).
* Specified by a relative time string. For example, `-7d` means 'accelerate data within the last 7 days.'
* Defaults to an empty string, meaning 'keep these stores for all time.'

acceleration.backfill_time = `<relative-time-str>`
* ADVANCED: Specifies how far back in time the Splunk software should create its column stores.
* ONLY set this parameter if you want to backfill less data than the retention period set by `acceleration.earliest_time`. You may want to use this parameter to limit your time window for column store creation in a large environment where initial creation of a large set of column stores is an expensive operation.
* WARNING: Do not set 'acceleration.backfill_time' to a narrow time window. If one of your indexers is down for a period longer than this backfill time, you may miss accelerating a window of your incoming data.
* MUST be set to a more recent time than 'acceleration.earliest_time'. For example, if you set 'acceleration.earliest_time' to `-1y` to retain your
column stores for a one year window, you could set 'acceleration.backfill_time' to '-20d' to create column stores that only cover the last 20 days. However, you cannot set 'acceleration.backfill_time' to '-2y', because that goes farther back in time than the 'acceleration.earliest_time' setting of '-1y'.
* Defaults to empty string (unset). When 'acceleration.backfill_time' is unset, the Splunk software always backfills fully to 'acceleration.earliest_time.'

acceleration.max_time = <unsigned int>
* The maximum amount of time that the column store creation search is allowed to run (in seconds).
* Note that this is an approximate time.
* Defaults to: 3600
* An 'acceleration.max_time' setting of '0' indicates that there is no time limit.

acceleration.poll_buckets_until_maxtime = <bool>
* In a distributed environment that consist of heterogenous machines, summarizations might complete sooner on machines with less data and faster resources. After the summarization search is finished with all of the buckets, the search ends. However, the overall search runtime is determined by the slowest machine in the environment.
* When set to "true": All of the machines run for "max_time" (approximately).
  The buckets are polled repeatedly for new data to summarize
* Set this to true if your data model is sensitive to summarization latency delays.
* When this setting is enabled, the summarization search is counted against the number of concurrent searches you can run until "max_time" is reached.
* Default: false

acceleration.cron_schedule = <cron-string>
* Cron schedule to be used to probe/generate the column stores for this data model.
* Defaults to: */5 * * * *

acceleration.manual_rebuilds = <bool>
* ADVANCED: When set to 'true,' this setting prevents outdated summaries from being rebuilt by the 'summarize' command.
* Normally, during the creation phase, the 'summarize' command automatically rebuilds summaries that are considered to be out-of-date, such as when
the configuration backing the data model changes.

* The Splunk software considers a summary to be outdated when:
  * The data model search stored in its metadata no longer matches its current data model search.
  * The search stored in its metadata cannot be parsed.
* NOTE: If the Splunk software finds a partial summary be outdated, it always rebuilds that summary so that a bucket summary only has results corresponding to one datamodel search.
* Defaults to: false

**acceleration.max_concurrent = <unsigned int>**
* The maximum number of concurrent acceleration instances for this data model that the scheduler is allowed to run.
* Defaults to: 3

**acceleration.allow_skew = <percentage>|<duration-specifier>**
* Allows the search scheduler to randomly distribute scheduled searches more evenly over their periods.
* When set to non-zero for searches with the following cron_schedule values, the search scheduler randomly "skews" the second, minute, and hour that the search actually runs on:
  * */ * * * * Every minute.
  * */M * * * * Every M minutes (M > 0).
  * 0 */ * * * Every hour.
  * 0 */H * * * Every H hours (H > 0).
  * 0 0 * * * Every day (at midnight).
* When set to non-zero for a search that has any other cron_schedule setting, the search scheduler can only randomly "skew" the second that the search runs on.
* The amount of skew for a specific search remains constant between edits of the search.
* An integer value followed by '%' (percent) specifies the maximum amount of time to skew as a percentage of the scheduled search period.
* Otherwise, use <int><unit> to specify a maximum duration. Relevant units are: m, min, minute, mins, minutes, h, hr, hour, hrs, hours, d, day, days.
  (The <unit> may be omitted only when <int> is 0.)
* Examples:
  100% (for an every-5-minute search) = 5 minutes maximum
  50% (for an every-minute search) = 30 seconds maximum
5m = 5 minutes maximum
1h = 1 hour maximum
* A value of 0 disallows skew.
* Default is 0.

acceleration.schedule_priority = default | higher | highest
* Raises the scheduling priority of a search:
  + "default": No scheduling priority increase.
  + "higher": Scheduling priority is higher than other data model searches.
  + "highest": Scheduling priority is higher than other searches regardless of
    scheduling tier except real-time-scheduled searches with priority = highest
    always have priority over all other searches.
  + Hence, the high-to-low order (where RTSS = real-time-scheduled search, CSS
    = continuous-scheduled search, DMAS = data-model-accelerated search, d =
    default, h = higher, H = highest) is:
    RTSS(H) > DMAS(H) > CSS(H)
    > RTSS(h) > RTSS(d) > CSS(h) > CSS(d)
    > DMAS(h) > DMAS(d)
* The scheduler honors a non-default priority only when the search owner has
  the 'edit_search_schedule_priority' capability.
* Defaults to: default
* WARNING: Having too many searches with a non-default priority will
  impede the
  ability of the scheduler to minimize search starvation. Use this
  setting
  only for mission-critical searches.

acceleration.allow_old_summaries = <bool>
* Sets the default value of 'allow_old_summaries' for this data model.
* Only applies to accelerated data models.
* When you use commands like 'datamodel', 'from', or 'tstats' to run a
  search
  on this data model, allow_old_summaries=false causes the Splunk
  software to verify that the data model search in each bucket's summary metadata
  matches the scheduled search that currently populates the data model summary.
  Summaries that fail this check are considered "out of date" and are
  not used to deliver results for your events search.
* This setting helps with situations where the definition of an
  accelerated data model has changed, but the Splunk software has not yet updated
  its summaries to reflect this change. When allow_old_summaries=false for a data
model, an event search of that data model only returns results from bucket summaries that match the current definition of the data model. * If you set allow_old_summaries=true, your search can deliver results from bucket summaries that are out of date with the current data model definition. * Default: false

acceleration.hunk.compression_codec = <string>
* Applicable only to Hunk Data models. Specifies the compression codec to be used for the accelerated orc/parquet files.

acceleration.hunk.dfs_block_size = <unsigned int>
* Applicable only to Hunk data models. Specifies the block size in bytes for the compression files.

acceleration.hunk.file_format = <string>
* Applicable only to Hunk data models. Valid options are "orc" and "parquet"

acceleration.workload_pool = <name of workload pool>
* Optional.
* Sets the workload pool to be used by this search.
* There are multiple workload pools defined in workload_pools.conf. Each workload pool has resource limits associated with it. For example, CPU, Memory, etc.
* The specific workload_pool to use is defined in workload_pools.conf. * The search process for this search runs in the specified workload_pool.
* If workload management is enabled and a workload_pool is not specified, the search is put into a proper pool as specified by the workload rules defined in workload_rules.conf. If there is no rule defined for this search, the default_pool defined in workload_pools.conf is used.

******** Dataset Related Attributes ******
# These attributes affect your interactions with datasets in Splunk Web and should not be changed under normal conditions. Do not modify them unless you are sure you know what you are doing.

dataset.description = <string>
* User-entered description of the dataset entity.
dataset.type = [datamodel|table]
* The type of dataset:
  + "datamodel": An individual data model dataset.
  + "table": A special root data model dataset with a search where the
dataset is
    defined by the dataset.commands attribute.
* Default: datamodel

dataset.commands = [<object>(, <object>)*]
* When the dataset.type = "table" this stringified JSON payload is
  created by the
  table editor and defines the dataset.

dataset.fields = [<string>(, <string>)*]
* Automatically generated JSON payload when dataset.type = "table" and
  the root
  data model dataset's search is updated.

dataset.display.diversity = [latest|random|diverse|rare]
* The user-selected diversity for previewing events contained by the
dataset:
  + "latest": search a subset of the latest events
  + "random": search a random sampling of events
  + "diverse": search a diverse sampling of events
  + "rare": search a rare sampling of events based on clustering
* Default: latest

dataset.display.sample_ratio = <int>
* The integer value used to calculate the sample ratio for the dataset
diversity.
  The formula is 1 / <int>.
* The sample ratio specifies the likelihood of any event being included
  in the
  sample.
* For example, if sample_ratio = 500 each event has a 1/500 chance of
  being
  included in the sample result set.
* Default: 1

dataset.display.limiting = <int>
* The limit of events to search over when previewing the dataset.
* Default: 100000

dataset.display.currentCommand = <int>
* The currently selected command the user is on while editing the
  dataset.

dataset.display.mode = [table|datasummary]
* The type of preview to use when editing the dataset:
  + "table": show individual events/results as rows.
  + "datasummary": show field values as columns.
* Default: table
* The earliest time used for the search that powers the datasummary view of the dataset.

* The latest time used for the search that powers the datasummary view of the dataset.

* A comma-separated list of tag fields that the data model requires for its search result sets.

* This is a search performance setting. Apply it only to data models that use a significant number of tag field attributes in their definitions. Data models without tag fields cannot use this setting. This setting does not recognize tags used in constraint searches.

* Only the tag fields identified by tags_whitelist (and the event types tagged by them) are loaded when searches are performed with this data model.

* When you update tags_whitelist for an accelerated data model, the Splunk software rebuilds the data model unless you have enabled acceleration.manual_rebuild for it.

* If tags_whitelist is empty, the Splunk software attempts to optimize out unnecessary tag fields when searches are performed with this data model.

* Defaults to empty.

datamodels.conf.example

#   Version 7.3.0
#
# Configuration for example datamodels
#

# An example of accelerating data for the 'mymodel' datamodel for the past five days, generating and checking the column stores every 10 minutes
[mymodel]
acceleration = true
acceleration.earliest_time = -5d
acceleration.poll_buckets_until_maxtime = true
acceleration.cron_schedule = */10 * * * *
acceleration.hunk.compression_codec = snappy
acceleration.hunk.dfs_block_size = 134217728
acceleration.hunk.file_format = orc
deep_dive_drilldowns.conf

The following are the spec and example files for deep_dive_drilldowns.conf.

deep_dive_drilldowns.conf.spec

# Copyright (C) 2005-2019 Splunk Inc. All Rights Reserved.
# This file contains all possible attribute/value pairs for configuring
# drilldown options for deep dive lanes.
#
# A unique drilldown options is represented by a stanza in this file.
# The name of the stanza is the name that will appear in the UI.
# ITSI currently supports a maximum of 22 drilldown stanzas in this
# file.
# Default values are provided for most settings and are defined in
# the [default] stanza of the configuration file.
#
# Other more complex drilldown options are not defined in this file
# because they are only represented in the deep dive code and cannot
# be disabled.
#
# There is a deep_dive_drilldowns.conf in
# $SPLUNK_HOME/etc/apps/itsi/default.
# To set custom configurations, place a deep_dive_drilldowns.conf in
# $SPLUNK_HOME/etc/apps/itsi/local/. You must restart Splunk software
to
# enable configurations.
#
# To learn more about configuration files (including precedence) please
# see the documentation located at
# https://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the
top of
#   the file.
# * Each conf file should have at most one default stanza. If there
are
#   multiple default stanzas, settings are combined. In the case of
#   multiple definitions of the same setting, the last definition in
the
#   file wins.
# If a setting is defined at both the global level and in a specific stanza, the value in the specific stanza takes precedence.

[<name>]

* Each stanza represents a unique drilldown option. Use these settings to configure properties for all types of drilldowns.

type = uri|search
* Represents whether this drilldown is meant to redirect to a new URI or open a Splunk search.
* Required.

replace_tokens = true|false
* Enables token replacement in the search string or URI.
* Optional.
* If "true", the search or URI is token replaced by properties of the drilldown.
* Token replacement is similar to token replacement in simpleXML. Tokens are represented in tokenized strings as a sub-string key surrounded by '$'.
  * For example, search=index=_internal | stats count | where count>$value$
* The following tokens are available for replacement by default:
  * lane_title - the title of the lane
  * lane_subtitle - the subtitle of the lane
  * lane_search - the search that powered the primary graph in the lane
  * earliest - the earliest epoch time stamp of the entire lane
  * latest - the latest epoch time stamp of the entire lane
  * bucket_earliest - the earliest epoch time stamp of the time bucket clicked
  * bucket_latest - the latest epoch time stamp of the time bucket clicked
* The following tokens are available for KPI lanes only:
  * kpi.service_id - the ID of the service to which the KPI belongs
  * kpi.service_title - the title of the service to which the KPI belongs
  * kpi.kpi_id - the ID of the KPI represented in the lane
  * kpi.kpi_title - the title of the KPI represented in the lane
  * kpi.single_value_search - the raw data alert search for the KPI
  * kpi.timeseries_search - the raw data time series search for the KPI
  * kpi.base_search - the event gathering/filtering search for the KPI
* Default: false

metric_lane_enabled = true|false
* Whether to enable drilldowns on metric lanes.
* Optional.
* If "true", drilldown is available on metric lanes.
* If "false", drilldown is unavailable on metric lanes.
kpi_lane_enabled = true|false
* Whether to enable drilldowns on KPI lanes.
* Optional.
* If "true", drilldown is available on KPI lanes.
* If "false", drilldown is unavailable on KPI lanes.
* Default: false

event_lane_enabled = true|false
* Whether to enable drilldowns on event lanes.
* Optional.
* If "true", drilldown is available on event lanes.
* If "false", drilldown is unavailable on event lanes.
* Default: false

####
# Entity-based features
####
# Entity-based features are only available on KPI lanes because KPI lanes are the only
# lanes that understand entities. Note that KPIs must have 'Split by Entity' enabled.

default: false

entity_level_only = true|false
* Whether to enable drilldowns only on lanes that surface entity-level information.
* Optional.
* If "true", drilldown is only available on lanes that surface entity-level information.
* If "false", drilldown is available on all lanes.
* Entity-level drilldowns make additional tokens and information available based
  on the entities clicked. See the 'entity_tokens' setting for more details.
* Default: false

entity_tokens = <csv>
* A CSV file of entity attributes to include on a drilldown.
* Optional.
* Only definition entities will be available on entity-level drilldowns. Pseudo-entities are ignored.
* If the 'replace_tokens' setting is "true", this setting will generate additional token replacements.
* Attributes can be either info fields or aliases.
* If the 'uri_payload_type' setting is set to "json", these entity attributes
  are added to the JSON payload per entity.
* Tokens from the first entity are replaced. If there are multiple entities,
  they all appear in a JSON payload.
* Tokens have the format "entity.<attribute name>".
* If any entity tokens are set to "all" (required to make drilldown work),
  entity.id and entity.title will always be available as tokens.

entity_activation_rules = <JSON blob of entity rules>|all
* Determines which entities to consider for drilldown.
* Optional.
* If "all", all entities are considered valid for drilldown.
* If set to a JSON blob of entity rules, entities will be tested for compliance with those rules. If no entities match, drilldown will not be available. If some or all all entities match, only those matching will be passed down to drilldown.

###
# Properties for search type drilldowns
###
search = <tokenized search string>
* The search to use in the new lane or on the search page.
* Required for search type drilldowns.
* If the 'replace_tokens' setting is "true", the search is token replaced
  by properties from the drilldown itself.

add_lane_enabled = true|false
* Whether users can activate the drilldown as a search.
* Required for search type drilldowns
* If "true", users can activate the drilldown as a search.
* If "false", users cannot activate the drilldown as a search.
* Default: false

use_bucket_timerange = true|false
* Whether to use only the time range of the selected bucket when redirected to a Splunk search.
* Optional.
* If "true", the drilldown search uses only the time range from which the user clicked in the deep dive.
* If "false", the drilldown search uses the entire search timerange.
* Default: true

new_lane_settings = <tokenized JSON for lane settings properties>
* A tokenized JSON string that represents a model to use for new lanes.
* Required for search type drilldowns with the 'add_lane_enabled' setting
  set to "true".
* The "search" setting is overridden by the search property in this stanza.
* If the 'replace_tokens' setting is "true", the string is token replaced
  by properties from the drilldown itself.
* Default lane settings are applied if you do not specify any values.

###
# Properties for URI type drilldowns

* uri = <str>
* The URI to redirect to on the drilldown.
* Required for URI type drilldowns.
* If the 'replace_tokens' setting is "true" and the 'uri_payload_type' setting is "simple", the URI string is replaced by tokens.
* Follows the format of an href:
  * A leading protocol allows a change in domain.
  * A leading slash changes the full path on the same domain.
  * Any other string only replaces the last segment of the URI with that string.

* uri_payload_type = simple|json
* If "simple", token replacement is performed on the URI as if it were a search.
* If "json", no token replacement is performed and a query string parameter 'drilldown_payload' is appended to the URI with a JSON representation of the context of a drilldown. This payload will always contain the context portion of the JSON blob, which contains the basic properties.
* If it is entity level and the entity properties of the drilldown are specified, the entities portion will exist and consist of the entity ID and title as well as all attributes specified in as 'entity_tokens'. A JSON payload format will look like the following (assumes 'entity_tokens' was host,family):

```json
{
    "context": {
        "earliest": <earliest time of full lane>,
        "latest": <latest time of full lane>,
        "bucket_earliest": <earliest time of bucket clicked>,
        "bucket_latest": <latest time of the bucket clicked>,
        "return_url": <URI of the current deep dive>,
        "service_id": "158bdaf4-6b0c-433e-9c24-c3a36c0e8eea",
        "kpi_id": "65ec30c5e1dd5046ac5416f5",
        "service_title": "Production Webservers",
        "kpi_title": "Total Request Latency (ms)"
    },
    "entities": [
        {
            "id": "5303377f-162c-45cc-809a-d1e3254ea4a1",
            "title": "Host Title 1",
            "host": "Host1",
            "family": "Linux"
        },
        {
            "id": "7aefd044-0f46-4ba4-ab13-f31e5797a3bf",
            "title": "Host Title 2",
```
* Default: simple

---

**deep_dive_drilldowns.conf.example**

# This is an example deep_dive_drilldowns.conf. Use this file to # configure custom drilldowns.
# # To use one or more of these configurations, copy the configuration block # into deep_dive_drilldowns.conf in $SPLUNK_HOME/etc/apps/itsi/local. # You must restart Splunk to enable configurations.
# # To learn more about configuration files (including precedence) please see # the documentation located at # http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles # # This example alert includes showing raw events at selected time buckets, # showing raw events from a displayed time range, showing KPI events for # a host, and showing all events for a host.

[Show raw events at selected time bucket]
type = uri
kpi_lane_enabled = true
type = uri
kpi_lane_enabled = true
type = uri
kpi_lane_enabled = true

[Show raw events from displayed time range]
type = uri
ekpi_lane_enabled = true
entity_level_only = false
uri = /app/itsi/search?q=search$kpi.base_search$&earliest=$bucket_earliest$&latest=$bucket_latest$&display.page.search.mode=smart&dispatch.sample_ratio=1
replace_tokens = true

[Show KPI events for this host]
type = uri
kpi_lane_enabled = true
entity_level_only = true
replace_tokens = true
distsearch.conf

The following are the spec and example files for distsearch.conf.

distsearch.conf.spec

#  Version 7.3.0
# This file contains possible attributes and values you can use to configure distributed search.
#
# To set custom configurations, place a distsearch.conf in $SPLUNK_HOME/etc/system/local/. For examples, see distsearch.conf.example.
# You must restart Splunk to enable configurations.
#
# To learn more about configuration files (including precedence) please see the documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
#
# These attributes are all configured on the search head, with the exception of
# the optional attributes listed under the SEARCH HEAD BUNDLE MOUNTING OPTIONS
# heading, which are configured on the search peers.

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
#   * You can also define global settings outside of any stanza, at the top of the file.
#   * Each conf file should have at most one default stanza. If there are multiple default stanzas, attributes are combined. In the case of multiple definitions of the same attribute, the last definition in the file wins.
#   * If an attribute is defined at both the global level and in a specific stanza, the value in the specific stanza takes precedence.

[distributedSearch]
* Set distributed search configuration options under this stanza name.
* Follow this stanza name with any number of the following attribute/value pairs.
* If you do not set any attribute, Splunk software uses the default value (if there is one listed).

disabled = <boolean>
* Toggle distributed search off ("true") and on ("false").
  * Default: false (distributed search is enabled by default)

```
heartbeatMcastAddr = <IP address>
* DEPRECATED.
```

```
heartbeatPort = <port>
* DEPRECATED.
```

```
ttl = <integer>
* DEPRECATED.
```

```
heartbeatFrequency = <integer>
* DEPRECATED.
```

```
statusTimeout = <integer>
* Set connection timeout when gathering a search peer's basic info (/services/server/info).
* Increasing this value on the Distributed Monitoring Console (DMC) can result in fewer peers showing up as "Down" in /services/search/distributed/peers/.
* Note: Read/write timeouts are automatically set to twice this value.
  * Default: 10
```

```
removedTimedOutServers = <boolean>
* This setting is no longer supported, and will be ignored.
```

```
checkTimedOutServersFrequency = <integer>
* This setting is no longer supported, and will be ignored.
```

```
autoAddServers = <boolean>
* DEPRECATED.
```

```
bestEffortSearch = <boolean>
* This setting determines whether a search peer that's missing the knowledge bundle participates in the search.
* If set to "true", the peer participates in the search even if it doesn't have the knowledge bundle. The peers that don't have any common bundles are simply not searched.
  * Default: false
```

```
skipOurselves = <boolean>
* DEPRECATED.
```

```
servers = <comma-separated list>
* An initial list of servers.
  * Each member of this list must be a valid URI in the format of scheme://hostname:port
```

```
disabled_servers = <comma-separated list>
* A list of disabled search peers. Peers in this list are not monitored
```
or searched.
* Each member of this list must be a valid URI in the format of
  scheme://hostname:port

quarantined_servers = <comma-separated list>
* A list of quarantined search peers.
* Each member of this list must be a valid URI in the format of
  scheme://hostname:port
* The admin might quarantine peers that seem unhealthy and are degrading
  search
  performance of the whole deployment.
* Quarantined peers are monitored but not searched by default.
* A user might use the splunk_server arguments to target a search
  to quarantined peers at the risk of slowing the search.
* When you quarantine a peer, any real-time searches that are running
  are NOT
  restarted. Currently running real-time searches continue to return
  results
  from the quarantined peers. Any real-time searches started after the
  peer
  has been quarantined will not contact the peer.
* Whenever a quarantined peer is excluded from search, appropriate
  warnings
  are displayed in the search.log and in the Job Inspector.

useDisabledListAsBlacklist = <boolean>
* Whether or not the search head treats the 'disabled_servers' setting
  as
  a blacklist.
* If set to "true", search peers that appear in both the 'servers'
  and 'disabled_servers' lists are disabled and do not participate in
  search.
* If set to "false", search peers that appear in both lists are enabled
  and participate in search.
* Default: false

shareBundles = <boolean>
* Indicates whether this server will use bundle replication to share
  search-time
  configurations with search peers.
* If set to "false", the search head assumes that all the search peers
  can
  access the correct bundles via shared storage and have configured the
  options listed under the "SEARCH HEAD BUNDLE MOUNTING OPTIONS"
  heading.
* Default: true

useSHPBundleReplication = [true|false|always]
* Whether the search heads in the pool compete with each other to decide
  which
  one handles the bundle replication (every time bundle replication
  needs
to happen), or whether each of them individually replicates the bundles.
* This setting is only relevant in search head pooling environments.
* When set to "always" and you have configured mounted bundles, use the search head pool GUID rather than each individual server name to identify bundles (and search heads to the remote peers).
* Default: true

trySSLFirst = <boolean>
* This setting is no longer supported, and will be ignored.

peerResolutionThreads = <integer>
* This setting is no longer supported, and will be ignored.

defaultUriScheme = [http|https]
* The default URI scheme to use if you add a new peer without specifying a scheme for the URI to its management port.
* Default: https

serverTimeout = <integer>
* This setting is no longer supported, and will be ignored.
* It has been replaced by the following settings:
  'connectionTimeout', 'sendTimeout', 'receiveTimeout'.

connectionTimeout = <integer>
* The maximum amount of time to wait, in seconds, when the search head is attempting to establish a connection to the search peer.

sendTimeout = <integer>
* The maximum amount of time to wait, in seconds, when the search head is attempting to write or send data to a search peer.

receiveTimeout = <integer>
* The maximum amount of time to wait, in seconds, when the search head is attempting to read or receive data from a search peer.

authTokenConnectionTimeout = <integer>
* The maximum amount of time to wait, in seconds, for the search head to connect to a remote search peer when reading its authentication token.
* Fractional seconds are allowed (for example, 10.5 seconds).
* Default: 5

authTokenSendTimeout = <integer>
* The maximum amount of time to wait, in seconds, for the search head to send a request to a remote peer when getting its authentication token.
* Fractional seconds are allowed (for example, 10.5 seconds).
* Default: 10

authTokenReceiveTimeout = <integer>
* The maximum amount of time to wait, in seconds, for the search head to receive a response from a remote peer when getting its authentication token.
* Fractional seconds are allowed (for example, 10.5 seconds).
* Default: 10

bcs = <string>
* Currently not supported. This setting is related to a feature that is still under development.
* A string that represents the URL for the Bucket Catalog Service.
* Optional.
* There is no default.

bcsPath = <path>
* Currently not supported. This setting is related to a feature that is still under development.
* Optional.
* Default: /bcs/v1/buckets

**DISTRIBUTED SEARCH KEY PAIR GENERATION OPTIONS**

[tokenExchKeys]
certDir = <directory>
* This directory contains the local Splunk Enterprise instance's distributed search key pair.
* This directory also contains the public keys of servers that distribute searches to this Splunk Enterprise instance.
* Default: $SPLUNK_HOME/etc/auth/distServerKeys

publicKey = <string>
* The name of the public key file for this Splunk Enterprise instance.
* Default: trusted.pem

privateKey = <string>
* The name of private key file for this Splunk Enterprise instance.
* Default: private.pem

genKeyScript = <string>
* The command used to generate the two files above.
* Default: $SPLUNK_HOME/bin/splunk, createssl, audit-keys
REPLICATION SETTING OPTIONS

[replicationSettings]

connectionTimeout = <integer>
* The maximum amount of time to wait, in seconds, before a search head's initial connection to a peer times out.
* Default: 60

sendRcvTimeout = <integer>
* The maximum amount of time to wait, in seconds, when a search head is sending a full replication to a peer.
* Default: 60

replicationThreads = <positive integer>|auto
* The maximum number of threads to use when performing bundle replication to peers.
* If set to "auto", the peer auto-tunes the number of threads it uses for bundle replication.
  * If the peer has 3 or fewer CPUs, it allocates 2 threads.
  * If the peer has 4-7 CPUs, it allocates up to '# of CPUs - 2' threads.
  * If the peer has 8-15 CPUs, it allocates up to '# of CPUs - 3' threads.
  * If the peer has 16 or more CPUs, it allocates up to '# of CPUs - 4' threads.
* Default: 5

maxMemoryBundleSize = <integer>
* The maximum size, in megabytes, of bundles to hold in memory.
* If a bundle is larger than this value, Splunk software reads and encodes the bundle on the fly for each peer on which the replication is taking place.
* Default: 10

maxBundleSize = <integer>
* The maximum bundle size, in megabytes, for which replication can occur.
* If a bundle is larger than this value, bundle replication does not occur and Splunk logs an error message.
* Default: 2048 (2GB)
concerningReplicatedFileSize = <integer>
* The maximum allowable file size, in megabytes, within a bundle.
* Any individual file within a bundle that is larger than this value triggers a splunkd.log message.
* Where possible, avoid replicating such files by customizing your blacklists.
* Default: 500

excludeReplicatedLookupSize = <integer>
* The maximum allowable lookup file size, in megabytes, during knowledge bundle replication.
* Any lookup file larger than this value is excluded from the knowledge bundle
  that the search head replicates to its search peers.
* When this value is set to "0", this feature is disabled. All file sizes are included.
* Default: 0

allowStreamUpload = [auto|true|false]
* Whether to enable streaming bundle replication for peers.
* If set to "auto", search heads use streaming bundle replication when
  connecting to peers with a complete implementation of this feature
  (Splunk Enterprise 6.0 or higher).
* If set to "true", search heads use streaming bundle replication when
  connecting to peers with a complete or experimental implementation
  of this feature (Splunk Enterprise 4.2.3 or higher).
* If set to "false", streaming bundle replication is never used.
* Whatever the value of this setting, streaming bundle replication is not used for peers that completely lack support for this feature.
* Default: auto

allowSkipEncoding = <boolean>
* Whether to skip over URL-encoded bundled data on upload.
* Default: true

allowDeltaUpload = <boolean>
* Whether to enable delta-based bundle replication.
* Delta-based replication keeps the bundle compact, with the search head only
  replicating the changed portion of the bundle to its search peers.
* Default: true

sanitizeMetaFiles = <boolean>
* Whether to sanitize or filter *.meta files before replication.
* Use this setting to avoid unnecessary replications triggered by writes to *.meta files that have no real effect on search behavior.
* The types of stanzas that "survive" filtering are configured via the replicationSettings:refineConf stanza.
* The filtering process removes comments and cosmetic white space.
* Default: true
RFS (AKA S3/REMOTE FILE SYSTEM) REPLICATION-SPECIFIC SETTINGS

enableRFSReplication = <boolean>
* Currently not supported. This setting is related to a feature that is still under development.
* If set to "true", remote file system bundle replication is enabled.
* When search heads generate bundles, these bundles are uploaded to the configured remote file system.
* When search heads delete their old bundles, they subsequently attempt to delete the bundle from the configured remote file system.
* Required on search heads.
* Default: false

enableRFSMonitoring = <boolean>
* Currently not supported. This setting is related to a feature that is still under development.
* If set to "true", remote file system bundle monitoring is enabled.
* Search peers periodically monitor the configured remote file system and download any bundles that they do not have on disk.
* Required on search peers.
* Default: false

rfsMonitoringPeriod = <unsigned integer>
* Currently not supported. This setting is related to a feature that is still under development.
* The amount of time, in seconds, that a search peer waits between polling attempts. You must also configure this setting on search heads, whether or not the 'enableRFSMonitoring' setting is enabled on them.
* For search heads when the 'rfsSyncReplicationTimeout' setting is set to "auto", this setting automatically adapts the 'rfsSyncReplicationTimeout' setting to the monitoring frequency of the search peers.
* If you set this value to less than "60", it automatically defaults to 60.
* Default: 60

rfsSyncReplicationTimeout = <unsigned integer>
* Currently not supported. This setting is related to a feature that is still under development.
* The amount of time, in seconds, that a search head waits for synchronous replication to complete. Only applies to RFS bundle replication.
* The default value is computed from the 'rfsMonitoringPeriod' setting. For example, (rfsMonitoringPeriod + 60) * 5, where 60 is the non-configurable polling interval from search heads to search peers, and 5 is an
arbitrary multiplier.
* If you do not modify the 'rfsMonitoringPeriod' setting, the default
  value is 600.
* Default: auto

path = <path>
* Currently not supported. This setting is related to a feature that is
  still under development.
* The remote storage location where bundles reside.
  * Required.
  * The format for this attribute is:
    <scheme>://<remote-location-specifier>
    * The "scheme" identifies a supported external storage system type.
    * The "remote-location-specifier" is an external system-specific
      string
      for identifying a location inside the storage system.
* The following external systems are supported:
  * Object stores that support AWS's S3 protocol. These use the scheme
    "s3".
    Example: "path=s3://mybucket/some/path"
  * POSIX file system, potentially a remote file system mounted over
    NFS.
    These use the scheme "file".
    Example: "path=file:///mnt/cheap-storage/some/path"

remote.s3.endpoint = <URL>
* Currently not supported. This setting is related to a feature that is
  still under development.
* The URL of the remote storage system supporting the S3 API.
* The protocol, http or https, can be used to enable or disable SSL
  connectivity with the endpoint.
* If not specified and the indexer is running on EC2, the endpoint is
  constructed automatically based on the EC2 region of the instance
  where
  the indexer is running, as follows: https://s3-<region>.amazonaws.com
* Example: https://s3-us-west-2.amazonaws.com

remote.s3.encryption = [sse-s3|none]
* Currently not supported. This setting is related to a feature that is
  still under development.
* Specifies the schema to use for Server-Side Encryption (SSE) for data
  at rest.
  * sse-s3: See:
  * none: Server-side encryption is disabled. Data is stored unencrypted
    on the
    remote storage.
  * Optional.
  * Default: none

[replicationSettings:refineConf]
replicate.<conf_file_name> = <boolean>
* Controls whether Splunk software replicates a particular type of
  *.conf file, along with any associated permissions in *.meta files.
* These settings on their own do not cause files to be replicated. You
  must still whitelist a file (via the 'replicationWhitelist' setting) in
  order for
  it to be eligible for inclusion via these settings.
* In a sense, these settings constitute another level of filtering that
  applies
  specifically to *.conf files and stanzas with *.meta files.
* Default: false

**REPLICATION WHITELIST OPTIONS**

[replicationWhitelist]

<name> = <whitelist_pattern>
* Controls Splunk software's search-time configuration replication from
  search heads to search peers.
* Only files that match a whitelist entry are replicated.
* Conversely, files that do not match a whitelist entry are not
  replicated.
* Only files located under $SPLUNK_HOME/etc will ever be replicated in
  this way.
* The regex is matched against the file name, relative to
  $SPLUNK_HOME/etc.
  Example: For a file
  "$SPLUNK_HOME/etc/apps/fancy_app/default/inputs.conf",
  this whitelist should match
  "apps/fancy_app/default/inputs.conf"
  * Similarly, the etc/system files are available as system/...
    User-specific files are available as users/username/appname/...
  * The 'name' element is generally descriptive, with one exception:
    If <name> begins with "refine.", files whitelisted by the given
    pattern will
    also go through another level of filtering configured in the
    [replicationSettings:refineConf] stanza.
  * The whitelist_pattern is the Splunk style pattern matching, which is
    primarily regex-based with special local behavior for '...' and '*'.
    * '...' matches anything, while '*' matches anything besides
      directory separators. See props.conf.spec for more detail on these.
    * Note: '.' will match a literal dot, not any character.
  * These lists are applied globally across all configuration data, not to
    any
    particular application, regardless of where they are defined. Be
    careful to
pull in only your intended files.

REPLICATION BLACKLIST OPTIONS

[replicationBlacklist]

<name> = <blacklist_pattern>
* All comments from the replication whitelist notes above also apply here.
* Replication blacklist takes precedence over the whitelist, meaning that a file that matches both the whitelist and the blacklist is NOT replicated.
* Use this setting to prevent unwanted bundle replication in two common scenarios:
  * Very large files which part of an application might not want to be replicated, especially if they are not needed on search nodes.
  * Frequently updated files (for example, some lookups) will trigger retransmission of all search head data.
* These lists are applied globally across all configuration data. Especially for blacklisting, be sure to constrain your blacklist to match only data that your application does not need.

BUNDLE ENFORCER Whitelist OPTIONS

[bundleEnforcerWhitelist]

<name> = <whitelist_pattern>
* Peers use this setting to make sure knowledge bundles sent by search heads and masters do not contain alien files.
* If this stanza is empty, the receiver accepts the bundle unless it contains files matching the rules specified in the [bundleEnforcerBlacklist] stanza.
  Hence, if both [bundleEnforcerWhitelist] and [bundleEnforcerBlacklist] are empty (which is the default), then the receiver accepts all bundles.
* If this stanza is not empty, the receiver accepts the bundle only if it...
contains only files that match the rules specified here but not those in the
[bundleEnforcerBlacklist] stanza.
* All rules are regular expressions.
* No default.

**BUNDLE ENFORCER BLACKLIST OPTIONS**

[bundleEnforcerBlacklist]

<name> = <blacklist_pattern>
* Peers use this setting to make sure knowledge bundle sent by search heads and
  masters do not contain alien files.
* This list overrides the [bundleEnforceWhitelist] stanza above. This means that
  the receiver removes the bundle if it contains any file that matches the
  rules specified here even if that file is allowed by [bundleEnforcerWhitelist].
* If this stanza is empty, then only [bundleEnforcerWhitelist] matters.
* No default.

**SEARCH HEAD BUNDLE MOUNTING OPTIONS**

# Configure these settings on the search peers only, and only if you also
# configure shareBundles=false in the [distributedSearch] stanza on the search
# head. Use these settings to access bundles that are not replicated.
The search
# peers use a shared
# storage mount point to access the search head bundles
($SPLUNK_HOME/etc).
#*****************************************************************************

[searchhead:<searchhead-splunk-server-name>]
* <searchhead-splunk-server-name> is the name of the related search head
  installation.
* The server name is located in server.conf: serverName = <name>

mounted_bundles = <boolean>
* Determines whether the bundles belonging to the search head specified in the
  stanza name are mounted.
* You must set this value to "true" to use mounted bundles.
* Default: false

bundles_location = <path>
* The path to where the search head's bundles are mounted.
* This path must be the mount point on the search peer, not on the search head.
* The path should point to a directory that is equivalent to $SPLUNK_HOME/etc/.
* The path must contain at least the following subdirectories: system, apps,
  users

**DISTRIBUTED SEARCH GROUP DEFINITIONS**

# These settings are the definitions of the distributed search groups. A search
# group is a set of search peers as identified by thier host:management-port. A
# search can be directed to a search group using the splunk_server_group argument.
# The search is dispatched to only the members of the group.
#******************************************************************************

[distributedSearch:<splunk-server-group-name>]
* <splunk-server-group-name> is the name of the Splunk server group
  that is defined in this stanza

servers = <comma-separated list>
* A list of search peers that are members of this group.
* The list must use peer identifiers (i.e. hostname:port).

default = <boolean>
* Whether or not this group is the default group of peers against which all
  searches are run, unless a server group is not explicitly specified.

distsearch.conf.example

#   Version 7.3.0
These are example configurations for distsearch.conf. Use this file to configure distributed search. For all available attribute/value pairs, see distsearch.conf.spec.

There is NO DEFAULT distsearch.conf.

To use one or more of these configurations, copy the configuration block into distsearch.conf in $SPLUNK_HOME/etc/system/local/. You must restart Splunk to enable configurations.

To learn more about configuration files (including precedence) please see the documentation located at http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

[distributedSearch]

# This entry distributes searches to 192.168.1.1:8059,192.168.1.2:8059. These machines will be contacted on port 8059 using https. Attributes not set here will use the defaults listed in distsearch.conf.spec.

# this stanza controls the timing settings for connecting to a remote peer and the send timeout
[replicationSettings]
connectionTimeout = 10
sendRcvTimeout = 60

# this stanza controls what files are replicated to the other peer each is a regex
[replicationWhitelist]
allConf = *.conf

# Mounted bundles example.
# This example shows two distsearch.conf configurations, one for the search head and another for each of the search head's search peers. It shows only the attributes necessary to implement mounted bundles.

# On a search head whose Splunk server name is "searcher01":
[distributedSearch]
... shareBundles = false
# On each search peer:
[searchhead:searcher01]
mounted_bundles = true
bundles_location = /opt/shared_bundles/searcher01

drilldownsearch_offset.conf

The following are the spec and example files for drilldownsearch_offset.conf.

drilldownsearch_offset.conf.spec

# This file contains attributes and values for configuring time range picker
# presets for correlation search drilldown offsets.
#
# There is a drilldownsearch_offset.conf in
# $SPLUNK_HOME/etc/apps/itsi/default/.
# To set custom configurations, place a drilldownsearch_offset.conf in
# $SPLUNK_HOME/etc/apps/itsi/local/. You must restart Splunk to enable
# configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the
top
#   of the file.
# * Each .conf file should have at most one default stanza. If there are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
#   the
#   file wins.
# * If an attribute is defined at both the global level and in a
#   specific
#   stanza, the value in the specific stanza takes precedence.
timeInSecs = <integer>
* The offset time, in seconds.
* Required.

description = <string>
* The description that is shown in the UI for the earliest and latest offset
dropdown. The earliest offset prepends "Last" to the description and the
latest offset prepends "Next" to the description.
* Required if the 'earliest_description' and 'latest_description' settings
are not defined below.

earliest_description = <string>
* A description for the earliest offset dropdown.
* Optional.

latest_description = <string>
* A description for the latest offset dropdown.
* Optional.

drilldownsearch_offset.conf.example

No example

fields.conf

The following are the spec and example files for fields.conf.

fields.conf.spec

# Version 7.3.0
#
# This file contains possible attribute and value pairs for:
# * Telling Splunk how to handle multi-value fields.
# * Distinguishing indexed and extracted fields.
# * Improving search performance by telling the search processor how to
# handle field values.

# Use this file if you are creating a field at index time (not advised).
#
# There is a fields.conf in $SPLUNK_HOME/etc/system/default/. To set
custom
# configurations, place a fields.conf in
$SPLUNK_HOME/etc/system/local/. For
# examples, see fields.conf.example. You must restart Splunk to enable
# configurations.
#
# To learn more about configuration files (including precedence) please
# see the
documentation located at#
http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
#   * You can also define global settings outside of any stanza, at the
top of
#     the file.
#   * Each conf file should have at most one default stanza. If there
are
#     multiple default stanzas, attributes are combined. In the case of
#     multiple definitions of the same attribute, the last definition in
the
#     file wins.
#   * If an attribute is defined at both the global level and in a
specific
#     stanza, the value in the specific stanza takes precedence.

[field name>]

* Name of the field you're configuring.
* Follow this stanza name with any number of the following
attribute/value
  pairs.
* Field names can only contain a-z, A-Z, 0-9, and _, but cannot begin
  with a
  number or _

# TOKENIZER indicates that your configured field's value is a smaller
part of a
# token. For example, your field's value is "123" but it occurs as
"foo123" in
# your event.
TOKENIZER = <regular expression>
* Use this setting to configure multivalue fields (refer to the online
documentation for multivalue fields).
* A regular expression that indicates how the field can take on multiple values
  at the same time.
* If empty, the field can only take on a single value.
* Otherwise, the first group is taken from each match to form the set of values.
* This setting is used by the "search" and "where" commands, the summary and
  XML outputs of the asynchronous search API, and by the top, timeline and
  stats commands.
* Tokenization of indexed fields (INDEXED = true) is not supported so this
  attribute is ignored for indexed fields.
* Default to empty.

INDEXED = [true|false]
* Indicate whether a field is indexed or not.
* Set to true if the field is indexed.
* Set to false for fields extracted at search time (the majority of
  fields).
* Defaults to false.

INDEXED_VALUE = [true|false|<sed-cmd>|<simple-substitution-string>]
* Set this to true if the value is in the raw text of the event.
* Set this to false if the value is not in the raw text of the event.
* Setting this to true expands any search for key=value into a search of
  value AND key=value (since value is indexed).
* For advanced customization, this setting supports sed style
  substitution.
  For example, 'INDEXED_VALUE=s/foo/bar/g' would take the value of the
  field,
  replace all instances of 'foo' with 'bar,' and use that new value as
  the
  value to search in the index.
* This setting also supports a simple substitution based on looking for
  the
  literal string '<VALUE>' (including the '<' and '>' characters).
  For example, 'INDEXED_VALUE=source::*<VALUE>*' would take a search
  for
  'myfield=myvalue' and search for 'source::*myvalue*' in the index as
  a
  single term.
* For both substitution constructs, if the resulting string starts with
  a '[',
  Splunk interprets the string as a Splunk LISPY expression. For
  example,
  'INDEXED_VALUE=[OR <VALUE> source::*<VALUE>]' would turn
  'myfield=myvalue'
  into applying the LISPY expression '[OR myvalue source::*myvalue]' (meaning
  it matches either 'myvalue' or 'source::*myvalue' terms).
* Defaults to true.
* NOTE: You only need to set indexed_value if indexed = false.

**fields.conf.example**

```
#   Version 7.3.0
#
# This file contains an example fields.conf. Use this file to configure
# dynamic field extractions.
#
# To use one or more of these configurations, copy the configuration
# block into
# fields.conf in $SPLUNK_HOME/etc/system/local/. You must restart
# Splunk to
# enable configurations.
#
# To learn more about configuration files (including precedence) please
# see the
# documentation located at
#
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
#
# These tokenizers result in the values of To, From and Cc treated as a
# list,
# where each list element is an email address found in the raw string of
data.

[To]
TOKENIZER = (\w[\w.\-]*@[\w.\-]*\w)

[From]
TOKENIZER = (\w[\w.\-]*@[\w.\-]*\w)

[Cc]
TOKENIZER = (\w[\w.\-]*@[\w.\-]*\w)
```

**glasstable_icon_library.conf**

The following are the spec and example files for `glasstable_icon_library.conf`.

**glasstable_icon_library.conf.spec**

```
# This file contains possible attributes and values for adding
# and removing icons from the glass table icon library.
#
# There is a glasstable_icon_library.conf in
$SPLUNK_HOME/etc/apps/itsi/default/.
# To set custom configurations, place a glasstable_icon_library.conf in
# $SPLUNK_HOME/etc/apps/itsi/local/. You must restart Splunk to enable
# configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
#
http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the top
#   of the file.
# * Each .conf file should have at most one default stanza. If there are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
#   the file wins.
# * If an attribute is defined at both the global level and in a specific
#   stanza, the value in the specific stanza takes precedence.

[default]

iconThumbnailSrc = <string>
* The file path of the icon.
* Required.

[<stanza name>]

iconId = <string>
* An internal unique identifier for the icon.
* Required.

iconLabel = <string>
* The name or label for the icon that appears in the UI.

iconThumbnailSrc = <string>
* The file path of the icon.
* Required.
iconCategory = ['Application'|'Splunk'|'Network'|'General']
* The assigned category for the icon.
* Required.

svgPath = <string>
* The SVG path for the icon.
* The same path used for the icon library thumbnail.

defaultWidth = <positive integer>
* The initial width of the icon.

defaultHeight = <positive integer>
* The initial height of the icon.

**glasstable_icon_library.conf.example**

No example

**inputs.conf**

The following are the spec and example files for **inputs.conf**.

**inputs.conf.spec**

# This file contains possible settings you can use to configure ITSI inputs, register user access roles, and import services and entities from CSV files or search strings.
#
# There is an inputs.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/default. To set custom configurations, place an inputs.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/local.
# You must restart ITSI to enable new configurations.
#
# To learn more about configuration files (including precedence), see the # documentation located at
#
http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

###
# GLOBAL SETTINGS
###
# Use the [default] stanza to define any global settings.
#   * You can also define global settings outside of any stanza, at the
# Each conf file should have at most one default stanza. If there are multiple default stanzas, settings are combined. In the case of multiple definitions of the same setting, the last definition in the file wins.

# If a setting is defined at both the global level and in a specific stanza, the value in the specific stanza takes precedence.

# log_level = <DEBUG|INFO|WARN|ERROR>
# * This setting sets the logging level of each modular input.
# * The logging level describes the type and/or quantity of output that an application writes to a log file.
# * Set the logging verbosity of each modular input to specify how much and what kind of information it writes to the log file.
# * Setting a log level gets you messages at that level and higher, so default settings are typically INFO or WARN.

[itsi_user_access_init://<name>]

* A modular input that runs once during startup (or at the user's request) to register user access roles and capabilities with the SA-UserAccess module.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: WARN

app_name = <name>
* The Splunk application that has the user access roles and capabilities.
* Default: itsi

registered_capabilities = [true|false]
* Indicates whether or not capabilities have already been registered with ITSI.
* If true, the 'itsi_user_access_init' input does not re-register capabilities.
* If false, 'itsi_user_access_init' registers ITSI capabilities again.
* Default: false

[configure_itsi://<name>]

* A configuration input that runs once (or at the user's request) to
pull entities from the configuration file system into the App Key Value (KV) Store.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: WARN

is_configured = ""
* Left it for backwards compatibility.

[itsi_csv_import://<string>]

* A modular input that periodically uploads CSV data into the KV Store.
* The CSV file must contain headers for the import to work properly.
* This input runs every 4 hours or after a Splunk software restart.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: WARN

import_from_search = <boolean>
* Indicates whether to import data from a CSV file or a Splunk search.
* If "true", this input imports data from the search specified by 'search_string'.
* If "false", this input imports CSV data from the path specified by 'csv_location'.
* This setting is required, and the input does not run if the setting is not present.
* There is no default.

csv_location = <path>
* The location on disk of the CSV file to import.
* NOTE: The disk must be local to the search head. Cloud storage is unacceptable.
* This setting is required if you import data from a CSV file
  (if you set 'import_from_search' to "false").
* There is no default.

search_string = <string>
* The Splunk search string that generates the data to import.
* This setting is required if you import from a search string
  (if you set 'import_from_search' to "true").
* There is no default.

service_security_group = <string>
* The ITSI team that the imported services belong to.
* Use teams to group services by department, organization, or type of service and control access to the services.
* This setting is required, and the input does not run if the setting is
index_earliest = <integer>
* Specify the earliest _indextime, in minutes, for the time range of your search.
* This setting is required if you import from a search string (if you set 'import_from_search' to "true").
* Default: -15m

index_latest = <integer>
* Specify the latest _indextime, in minutes, for the time range of your search.
* This setting is required if you import from a search string (if you set 'import_from_search' to "true").
* Default: now

entity_title_field = <string>
* The column name in the CSV file, or the field in the search, to import the entity title from.
* This field serves as the informal identifier of the entity.
* There is no default.

entity_merge_field = <string>
* The column name in the CSV file, or the field in the search, to import the entity merge field from.
* There is no default.

entity_relationship_spec = <dict>
* A dictionary of key:value pairs that specifies how 'entity_title_field' associates with other fields and in what relationship.
* NOTE: This setting is unused.
* For example, 
  {
  "hosts": "vm1, vm2", "hostedBy": "host_id"}, or
  {
  "hosts": [{"vm1", "vm2"}, "hostedBy": "host_id"}.
  
  * For a record that has values for fields: vm1, vm2, host_id, 'entity_title_field' value>, three relationships are extracted:
    <value for 'entity_title_field'> hosts <value for vm1>
    <value for 'entity_title_field'> hosts <value for vm2>
    <value for 'entity_title_field'> hostedBy <value for host_id>
  * There is no default.

selected_services = <comma-separated list>
* A list of existing services to associate the imported entities with.
* DEPRECATED.
* There is no default.

service_rel = <comma-separated list>
* A list of existing service relationships.
* DEPRECATED.
* Use this setting to represent service dependencies in ITSI.
* There is no default.

`service_dependents = <comma-separated list>`
* A list of child columns in the CSV file, or child fields in the search, that indicate service dependencies.
* There is no default.

`entity_service_columns = <comma-separated list>`
* A list of services found in the CSV file or search that are to be associated with the entity for the row.
* DEPRECATED.
* There is no default.

`entity_identifier_fields = <comma-separated list>`
* A list of columns found in the CSV file or fields in the search that identify the entities (entity aliases).
* There is no default.

`entity_description_column = <comma-separated list>`
* A list of columns found in the CSV file or fields in the search that describe the entities.
* There is no default.

`entity_informational_fields = <comma-separated list>`
* A list of informational columns in the CSV file or fields in the search.
* These are non-identifying fields for the entities.
* There is no default.

`entity_field_mapping = <key-value pairs>`
* A key-value mapping of fields to re-map to other fields in your data.
* Follows a `<CSV field> = <Splunk search field>` format.
* For example, `ip1 = dest, ip2 = dest, storage_type = volume`
* Use this setting to rename a field or column to an alias or info value.
* There is no default.

`service_title_field = <string>`
* The field to import the service title from.
* This field is the informal identifier of the service.
* There is no default.
* This setting is required if you import services.

`service_description_column = <comma-separated list>`
* A list of columns in the CSV file or fields in the search that describe the services.
* There is no default.

`service_enabled = <boolean>`
* Whether or not imported services are enabled.
* Default: false
service_template_field = <string>
* This setting determines which service template a service is linked to.
* There is no default.

template = <dict>
* A dictionary of key:value pairs that maps entity rules to service
templates.
* For example,
  
  
  {
    "test_template_2": {
      "entity_rules": [
        {
          "rule_items": [
            {
              "rule_type": "matches",
              "field_type": "alias",
              "field": "whoa",
              "value": "doe"
            }
          ],
          "rule_condition": "AND"
        }
      ]
    },
    "test_template_1": {
      "entity_rules": [
        {
          "rule_items": [
            {
              "rule_type": "matches",
              "field_type": "alias",
              "field": "blah",
              "value": "da"
            }
          ],
          "rule_condition": "AND"
        }
      ]
    }
  }
  
  * CAUTION: Do not change this setting.
  * There is no default.

backfill_enabled = <boolean>
* This setting determines whether to enable backfill on all
  Key Performance Indicators (KPIs) in linked service templates.
* Backfill is the process of getting historical KPI data.
* ITSI backfills the KPI summary index (itsi_summary). You must have
  indexed adequate raw data for the backfill period.
* There is no default.

update_type = <APPEND|UPSERT|REPLACE>
* The update/insertion method when uploading entities.
* This setting is required, and the input will not run if the setting is
  not present.
* APPEND: ITSI makes no attempt to identify commonalities between
  entities. All information is appended to the table.
* UPSERT: ITSI appends new entries. Existing entries (based on the
  value found in the title_field) have additional information appended
  to the existing record.
* REPLACE: ITSI appends new entries. Existing entries (based on the
  value found in the title_field) are replaced by the new record value.
* There is no default.

interval = <integer>
* The interval, in seconds, that determines how often this input runs.
* There is no default.

[[itsi_async_csv_loader://<name>]]

* A modular input that periodically uploads CSV data into the KV store.
* The file must contain headers for the import to work properly.
log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: WARN

import_from_search = <boolean>
* Indicates whether to import data from a CSV file or a Splunk search.
* If "true", this input imports data from the search specified by 'search_string'.
* If "false", this input imports CSV data from the path specified by 'csv_location'.
* This setting is required, and the input does not run if the setting is not present.
* There is no default.

csv_location = <path>
* The location on disk of the CSV file to import.
* NOTE: The disk must be local to the search head. Cloud storage is unacceptable.
* This setting is required if you import data from a CSV file (if you set 'import_from_search' to "false").
* There is no default.

search_string = <string>
* The Splunk search string that generates the data to import.
* This setting is required if you import from a search string (if you set 'import_from_search' to "true").
* There is no default.

index_earliest = <integer>
* Specify the earliest _indextime, in minutes, for the time range of your search.
* This setting is required if you import from a search string (if you set 'import_from_search' to "true").
* Default: -15m

index_latest = <integer>
* Specify the latest _indextime, in minutes, for the time range of your search.
* This setting is required if you import from a search string (if you set 'import_from_search' to "true").
* Default: now

entity_title_field = <string>
* The column name in the CSV file, or the field in the search, to import the entity title from.
* This field serves as the informal identifier of the entity.
* There is no default.

entity_merge_field = <string>
* The column name in the CSV file, or the field in the search, to import the entity merge field from.
* There is no default.
entity_relationship_spec = <dict>
* A dictionary of key:value pairs that specifies how
  'entity_title_field' associates with other fields and in what
  relationship.
* NOTE: This setting is unused.
* For example,
  {"hosts": "vm1, vm2", "hostedBy": "host_id"}, or
  {"hosts": ["vm1", "vm2"], "hostedBy": "host_id"}.
* For a record that has values for fields: vm1, vm2, host_id,
  <'entity_title_field' value>, three relationships are extracted:
  <value for 'entity_title_field'> hosts <value for vm1>
  <value for 'entity_title_field'> hosts <value for vm2>
  <value for 'entity_title_field'> hostedBy <value for host_id>
* There is no default.

selected_services = <comma-separated list>
* A list of existing services to associate the imported entities with.
  * DEPRECATED.
  * There is no default.

service_rel = <comma-separated list>
* A list of existing service relationships.
  * DEPRECATED.
  * Use this setting to represent service dependencies in ITSI.
  * There is no default.

service_dependents = <comma-separated list>
* A list of child columns in the CSV file, or child fields in the
  search, that indicate service dependencies.
  * There is no default.

entity_service_columns = <comma-separated list>
* A list of services found in the CSV file or search that are to be
  associated with the entity for the row.
  * DEPRECATED.
  * There is no default.

entity_identifier_fields = <comma-separated list>
* A list of columns found in the CSV file or fields in the search
  that identify the entities (entity aliases).
  * There is no default.

entity_description_column = <comma-separated list>
* A list of columns found in the CSV file or fields in the search
  that describe the entities.
  * There is no default.

entity_informational_fields = <comma-separated list>
* A list of informational columns in the CSV file or fields in the search.
* These are non-identifying fields for the entities.
  * There is no default.

entity_field_mapping = <key-value pairs>
* A key-value mapping of fields to re-map to other fields in your data.
  * Follows a <CSV field> = <Splunk search field> format.
  * For example, ip1 = dest, ip2 = dest, storage_type = volume
  * Use this setting to rename a field or column to an alias or info value.
  * There is no default.

service_title_field = <string>
* The field to import the service title from.
  * This field is the informal identifier of the service.
  * There is no default.
  * This setting is required if you import services.

service_description_column = <comma-separated list>
* A list of columns in the CSV file or fields in the search that describe the services.
  * There is no default.

update_type = <APPEND|UPSERT|REPLACE>
* The update/insertion method when uploading entities.
  * This setting is required, and the input will not run if the setting is not present.
  * APPEND: ITSI makes no attempt to identify commonalities between entities.
    All information is appended to the table.
  * UPSERT: ITSI appends new entries. Existing entries (based on the value found in the title_field) have additional information appended to the existing record.
  * REPLACE: ITSI appends new entries. Existing entries (based on the value found in the title_field) are replaced by the new record value.
  * There is no default.

[itstsi_upgrade://<name>]

* A modular input that checks the ITSI version when Splunk Enterprise starts.
  * If the version does not match, Splunk Enterprise locks the UI and performs a version-based migration.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
  * Default: DEBUG
[**itsi_refresher://<name>**]

* A modular input that processes deferred methods using a single queue processor.
* Tracks relational objects and dependencies.
* This input detects conflicts and ensures consistency across ITSI.

`log_level = <DEBUG|INFO|WARN|ERROR>`
* The logging level of this input.
* Default: INFO

[**itsi_consumer://<name>**]

* A modular input that processes deferred methods using multiple queues across the Splunk environment.

`log_level = <DEBUG|INFO|WARN|ERROR>`
* The logging level of this input.
* Default: INFO

[**itsi_backup_restore://<name>**]

* A modular input that performs backup and restore operations by managing backup/restore jobs.
* If you restore ITSI from a backup of an older version of ITSI, migration begins during the restore process.
* The input runs every 5 seconds to check for the scheduled job.

`log_level = <DEBUG|INFO|WARN|ERROR>`
* The logging level of this input.
* Default: INFO

[**itsi_scheduled_backup_caller://<name>**]

* A modular input that manages ITSI backup schedules.
* For example, you might use this input if you want to backup ITSI every night at 1 am.

`log_level = <DEBUG|INFO|WARN|ERROR>`
* The logging level of this input.
* Default: INFO
[itsi_service_template_update_scheduler://<name>]

* A modular input that performs a scheduled sync from service templates to services every 15 minutes.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: INFO

[itsi_backfill://<name>]

* A modular input that manages KPI backfill jobs.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: INFO

[itsi_notable_event_archive://<name>]

* A modular input that moves notable events from the KV store to the index every hour.

owner = <string>
* Splunk cannot read the modular name unless a parameter is specified. Therefore, ITSI passes 'owner = <string>'.

[maintenance_minder://<name>]

* A modular input that runs every 60 seconds and populates the operative maintenance log based on configured maintenance windows.
* This input is responsible for putting services into maintenance mode.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: INFO

[itsi_default_aggregation_policy_loader://<name>]

* A modular input that loads the default aggregation policy.
* The default aggregation policy receives notable events that do not match the filtering criteria of any other aggregation policies.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: INFO

[itsi_default_correlation_search_acl_loader://<name>]

* A modular input that loads the Access Control List (ACL) for the default correlation searches provided with ITSI:
  "Monitor Critical Services Based on Health Score",
  "Splunk App for Infrastructure Alerts", and
  "Normalized Correlation Search".
* This input pulls ACL information from the KV store.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: INFO

[itsi_notable_event_hec_init://<name>]

* A modular input that initializes HEC client on a search head by creating and showing pertinent HEC tokens.
* A new HEC token is acquired during a Splunk restart.
* The internal system populates the new HEC token automatically.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: INFO

[itsi_notable_event_actions_queue_consumer://name]

* A modular input that acts as a consumer of the queue for executing notable event actions, such as pinging a host or running a script.
* This setting is primarily used by the rules engine.

exec_delay_time = <integer>
* The amount of time, in seconds, to delay execution of a notable event action.
* Default: 0

batch_size = <integer>
* The number of jobs to pick up in a single request from the notable event actions queue.
* Default: 5

timeout = <integer>
* The timeout period, in seconds, that ITSI uses when a user reclaimed an expired job.
* Default: 7200 (2 hours)
system_user_name = <string>
* The username of the system.
* Default: splunk-system-user

[itsi_entity_exchange_consumer://name]

* A modular input that consumes entities from the entity exchange module.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of the modular input.
* Default: DEBUG

interval = <value>
* The interval, in seconds, at which the modular input should run.
* Optional
* Default: 300 (5 minutes)

[itsi_age_kpi_alert_value_cache://<name>]

* A modular input that cleans up the aged entries in the KPI summary cache.

retentionTimeInSec = <integer>
* Aging/retention time for entries present in the KPI summary cache.

log_level = <DEBUG|INFO|WARN|ERROR>
* The logging level of this input.
* Default: INFO

inputs.conf.example

No example

itsu_base_service_template.conf

The following are the spec and example files for
itsu_base_service_template.conf.

itsu_base_service_template.conf.spec

# This file contains possible settings you can use to upload sample
# base service templates to the KV store.
#
# There is an itsi_base_service_template.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/default. To set custom
# configurations, place an itsi_base_service_template.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local.
# You must restart ITSI to enable new configurations.
#
# To learn more about configuration files (including precedence), see
# the
# documentation located at
#
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

[[<name>]]

title = <string>
* The title of the service template.

description = <string>
* A description of the service template.

_owner = <string>
* The owner of the service template.
* Default: itsi

_immutable = <boolean>
* Whether the service template can be edited or deleted.
* If "true", the service template cannot be edited or deleted.
* If "false", the service template can be edited or deleted.
* Default: false

entity_rules = <json>
* A list of entity rules (rules specification) used to associate
  entities
to services created from this service template.
* This setting is the same as the 'entity_rules' setting in
itsi_service.conf.spec.
* Example:

```json
[
  {
    "rule_condition": "AND", 
    "rule_items": [
      {
        "field": "app_title", 
        "field_type": "alias", 
        "rule_type": "not", 
        "value": ""
      },
      {
        "field": "another_field", 
        "field_type": "number", 
        "rule_type": "lt", 
        "value": 10
      }
    ]
  }
]
```
kpis = <json>
* A JSON blob that specifies the array of KPI definitions.
* For an example, see itsi_base_service_template.conf.

itsi_base_service_template.conf.example

No example

itsi_da.conf

The following are the spec and example files for itsi_da.conf.

itsi_da.conf.spec

# Copyright (C) 2005-2019 Splunk Inc. All Rights Reserved.
#
# This configuration file is DEPRECATED.
#
# For [entity_source_template://<string>], use
inputs.conf/[itsi_csv_import://<name>] instead.
# For [service_template://<string>], use
itsi_service_template.conf/[string] instead.
#
# This file contains possible settings you can use to configure an
itsi_da.conf file. Use this
# file to configure an app to export entity searches and service
templates for use within the
# IT Service Intelligence (ITSI) app.
#
# To learn more about configuration files (including precedence), see
the
# documentation located at
#
316
http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

# CAUTION: You can drastically affect your Splunk installation by changing these settings.
# Consult technical support (http://www.splunk.com/page/submit_issue) if you are not sure how
# to configure this file.

```
[entity_source_template://<string>]
```

title = <string>
* The display name of the search.

description = <string>
* A human-readable description of this search.

saved_search = <string>
* The actual Splunk saved search that outputs a table. This will be enforced by client-side code.

title_field = <string>
* A single field that acts as the title for the entity.

description_fields = <comma-separated list>
* A list of fields that describe the entity.

identifier_fields = <comma-separated list>
* A list of fields that identify the entity.

informational_fields = <comma-separated list>
* A list of fields that act as additional entity metadata.

```
[service_template://<string>]
```

title = <string>
* A title for the service template.

description = <string>
* The full description of the service being created.

entity_sourceTemplates = <comma-separated list>
* The list of entity searches that create entities that can be used with this service.
* The list is used to populate the list of entity searches in the combined entity-service creation workflow.
entity_rules = <string>
* A list of entity rules (rules specification) used to associate
entities to service
    created from this template.
* This field is the same as the entity_rules field in
itsi_service.conf.spec.

recommended_kpis = <comma-separated list>
* A list of KPIs that are automatically added when a service is created
with this template.

informational_kpis = <comma-separated list>
* A list of informational (no threshold) KPIs that are automatically
added when a
    service is created with this template.

optional_kpis = <comma-separated list>
* A list of KPIs that are available for this service (but not added
automatically).

itsi_da.conf.example

No example

itsi_deep_dive.conf

The following are the spec and example files for itsi_deep_dive.conf.

itsi_deep_dive.conf.spec

# This file contains possible attributes and values for uploading sample
# deep dives to the KV store.
#
# To upload deep dives to the KV store, place an
# itsi_deep_dive.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/local.
# You must restart Splunk software to enable configurations, unless you
# are
# editing them through the Splunk manager.
# To learn more about configuration files (including precedence) please
# see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
# WARNING: Manual editing of this file is not recommended. Contact
Support before proceeding.

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the
top
#   of the file.
# * Each conf file should have at most one default stanza. If there
are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
the
#   file wins.
# * If an attribute is defined at both the global level and in a
specific
#   stanza, the value in the specific stanza takes precedence.

[<name>]

* A name or primary identifier for the deep dive.

  focus_id = <string>
  * The ID of the entity or service that is in focus in the deep dive.
  * When an entity or service has focus, you see a list of metrics
    (performance metrics, event counts) for that entity/service.
  * Any particular deep dive can have a particular IT context
    in focus at any given time.
  * You can change the IT context in focus at any time. However,
    changing the focus has implications for historical tracking
    if not in a named deep dive.

  title = <string>
  * The title of the deep dive that is displayed in the UI.

  lane_settings_collection = <array>
  * An array of lane settings specifying each lane's configuration.

  acl = <value>
  * The team Access Control List (ACL) settings.

  mod_time = <value>
  * The last time the 'acl' setting was modified.

  description = <value>
  * Optional. The description of the deep dive.
is_named = <true|false>
* Whether or not this deep dive is named.
* A deep dive is considered "named" if you save it in the UI
  and give it a name. You might name a deep dive if you find it
  particularly useful and want to save it for future use.
* A deep dive is considered "unnamed" if you dynamically generated
  it (for example, from a drilldown) and did not save it.

_owner = <string>
* The user's KV store account in which to store the deep dive.
* In nearly all cases this value is "nobody".

source_itsi_da = <string>
* Optional. The ITSI module that acts as the source to define
  the deep dive.
* This attribute is used by the domain add-ons.

itsi_deep_dive.conf.example

No example

itsi_event_management.conf

The following are the spec and example files for itsi_event_management.conf.

itsi_event_management.conf.spec

# This file contains attributes and values for configuring the
# default selected fields for the similar episodes pane in
# Episode Review
#
# There is an itsi_event_management.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/default/.
# To set custom configurations, place an itsi_event_management.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local/. You must restart Splunk to
# enable
# configurations.
#
# To learn more about configuration files (including precedence) please
# see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
#  * You can also define global settings outside of any stanza, at the
top
#    of the file.
#  * Each .conf file should have at most one default stanza. If there
are
#    multiple default stanzas, attributes are combined. In the case of
multiple definitions of the same attribute, the last definition in
the
#    file wins.
#  * If an attribute is defined at both the global level and in a
specific
#    stanza, the value in the specific stanza takes precedence.

[<stanza_name>]

* A setting that you want to enable for Episode Review.
* Currently, 'similar_episodes' is the only supported setting.

default_fields = [<comma-separated list>]
* The list of field names selected by default in Similar Episodes pane
* For example, ["title","description","host"]
* Default: ["title"]

itsi_event_management.conf.example

No example

itsi_glass_table.conf

The following are the spec and example files for itsi_glass_table.conf.

itsi_glass_table.conf.spec

# This file contains possible attributes and values for uploading sample
glass tables to the KV store.
#
# To upload glass tables to the KV store, place an
# itsi_glass_table.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/local.
#
# You must restart Splunk software to enable configurations, unless you
are
# editing them through the Splunk manager.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
#
# WARNING: Manual editing of this file is not recommended. Contact Support before proceeding.

[<name>]

svg_content = <value>
* The SVG content settings.

latest = <value>
* The latest time in the time range.

earliest = <value>
* The earliest time in the time range.

svg_coordinates = <value>
* The SVG coordinate settings.

title = <string>
* The user-defined title of the glass table.

description = <string>
* The user defined description of the glass table.

mod_time = <value>
* Last modified time.

acl = <value>
* Access control information.

_owner = <string>
* The user account this deep dive belongs to.

source_itsi_da = <string>
* The ITSI module which is the source defining this glass table.

itsi_glass_table.conf.example

No example
itsi_kpi_base_search.conf

The following are the spec and example files for itsi_kpi_base_search.conf.

itsi_kpi_base_search.conf.spec

# This file contains possible settings you can use to upload sample 
# KPI base searches to the KV store.
#
# There is an itsi_kpi_base_search.conf in
#$SPLUNK_HOME/etc/apps/SA-ITOA/default. To set custom
# configurations, place an itsi_kpi_base_search.conf in
#$SPLUNK_HOME/etc/apps/SA-ITOA/local.
# You must restart ITSI to enable new configurations.
#
# To learn more about configuration files (including precedence), see
# the
# documentation located at
#
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

[<name>]

description = <string>
* A description of the KPI base search.

title = <string>
* The title of the KPI base search

_owner = <string>
* The owner of this KPI base search
* Default: itsi

base_search = <search>
* The search to execute in the KPI base search. This search is the 
  source 
  for the fields defined in metrics.
* Set the search to "*" if the 'is_metric' setting is set to "true".

metrics = <json>
* A JSON blob that specifies the array of metrics to be collected.
* Example item in the blob:
  * { 
    *   "unit": "%",
    *   "title": "CPU Utilization: %",
    *   "entity_statop": "avg",
    *   "aggregate_statop": "avg",
  }
* _key": "620b26a6f286a508fd356d94",
* "threshold_field": "cpu_load_percent"
* }
* The threshold_field in the item corresponds to a field from the base search.

is_metric = <boolean>
* Whether the KPI base search is a metric search.

metric = <json>
* A JSON blob that specifies the metric index and metric name to search on.
* Example item in the blob:
* 
* {  
*     "metric_index": "em_metrics",
*     "metric_name": "cpu.user"
* }

is_entity_breakdown = <boolean>
* Whether the metrics should be broken down by entities for threshold calculations.
* If "1", metrics are broken down by entities.
* If "0", metrics are not broken down by entities.

is_service_entity_filter = <boolean>
* Whether metrics should filter out entities not in the service.
* If "1", entities that don't belong to the service are filtered out.
* If "0", entities that don't belong to the service are still included.

entity_id_fields = <string>
* The field in the base search used to look up the corresponding entity to filter KPIs.
* For example, host, ip, and so on.
* This field is required if the 'is_service_entity_filter' setting is set to "true".

entity_breakdown_id_fields = <string>
* The field in the base search used to look up the corresponding entity to split KPIs.
* For example, host, ip, and so on.
* This field is required if the 'is_entity_breakdown' setting is set to "true".

entity_alias_filtering_fields = <comma-separated list>
* A list of alias attributes to be used to filter out entities not in the service.
* Optional.
* This field is required if the 'is_service_entity_filter' setting is set to "true".

alert_period = <integer>
* The frequency, in minutes, at which to run the search.
search_alert_earliest = <integer>
* The time window, in minutes, over which to evaluate the metrics.

alert_lag = <integer>
* The amount of time, in seconds, to push back the metric evaluation.
* This setting corresponds to the data indexing lag.
* Default: 30

metric_qualifier = <string>
* The field in the base search used to further split metrics.
* CAUTION: You cannot modify this setting in the UI.

source_itsi_da = <string>
* The ITSI module that is the source defining this KPI base search.

**itsi_kpi_base_search.conf.example**

No example

**itsi_kpi_template.conf**

The following are the spec and example files for *itsi_kpi_template.conf*.

**itsi_kpi_template.conf.spec**

```
# This file contains possible settings you can use to upload sample
# KPI templates to the KV store.
#
# There is an itsi_kpi_template.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/default. To set custom
# configurations, place an itsi_kpi_template.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local.
# You must restart ITSI to enable new configurations.
#
# To learn more about configuration files (including precedence), see
# the
documentation located at
#
http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

[<name>]
```

description = <string>
* The description of the KPI template bundle.
title = <string>
* The title of the bundle.

_owner = <string>
* The owner of the bundle.

kpis = <json>
* A JSON blob that specifies the array of KPI definitions.

source_itsi_da = <string>
* The ITSI module that is the source defining this KPI template.

itsi_kpi_template.conf.example

No example

itsi_kpi_threshold_template.conf

The following are the spec and example files for
itsi_kpi_threshold_template.conf.

itsi_kpi_threshold_template.conf.spec

# This file contains possible settings you can use to upload sample
# KPI threshold templates to the KV store.
#
# There is an itsi_kpi_threshold_template.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/default. To set custom
# configurations, place an itsi_kpi_threshold_template.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local.
# You must restart ITSI to enable new configurations.
#
# To learn more about configuration files (including precedence), see
# the
# documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

[<kpi_threshold_template>]

* Each stanza represents a KPI threshold template.
* Use threshold templates to build your time policies.
* You can create different policies with different time block
  combinations, such as work hours, off hours, or weekends.
title = <string>
* The title of the KPI threshold template.

description = <string>
* A description of the KPI threshold template.

time_variate_thresholds_specification = <JSON>
* A JSON blob containing the detailed time variant threshold object.

cacl = <JSON>
* A JSON blob containing the ACL information for the KPI threshold template.
* Use the following format:
  {
    "perms":{
      "read":[<LIST_OF_ROLES>],
      "write":[<LIST_OF_ROLES>]
    },
    "can_share_user":true|false,
    "can_share_app":true|false,
    "modifiable":true|false,
    "sharing":app|global,
    "can_change_perms":true|false,
    "can_share_global":true|false,
    "owner":<OWNER_NAME_STRING>,
    "can_write":true|false
  }

time_variate_thresholds = [True|False]
* Whether to enable time-variant thresholds.
* Time-variant thresholds accommodate normal variations in usage across your services and improve the accuracy of KPI and service health scores.
* For example, a time-variant threshold might take into account higher levels of usage during work hours, and lower levels of usage during off-hours and weekends.
* Default: True

adaptive_thresholding_training_window = <-7|-14|-30|-60>[d]
* The time window over which historical KPI data is analyzed for adaptive threshold updates.
* You must have 7 days of summary data in the summary index for adaptive thresholding to work properly.
* Default: -7 days

adaptive_thresholds_is_enabled = [True|False]
* Whether to enable adaptive thresholding for policies in time-variate thresholds.
* Adaptive thresholding lets you create time polices that generate thresholds
dynamically and update daily based on changes in your data.
* If you set this value to "true", the 'time_variate_thresholds' setting must
  also be set to "true".
* Default: False

itsi_kpi_threshold_template.conf.example

No example

itsi_module_settings.conf

The following are the spec and example files for itsi_module_settings.conf.

itsi_module_settings.conf.spec

# This file contains a setting for determining whether a module is editable
# in the module lister page.
#
# There is an itsi_module_settings.conf in each individual module
directory (for example,
# $SPLUNK_HOME/etc/apps/DA-ITSI-OS/default for the Operating System module). To change this
# setting for a specific module, place an itsi_module_settings.conf in
# $SPLUNK_HOME/etc/apps/<module>/local.
# You must restart Splunk software to enable configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

[settings://<app>]

* "app" is the ID for the app that contains this configuration file.

is_read_only = <boolean>
* Whether the module shows as editable in the module lister page.
* If "1", the module is not editable in the module lister page.
* If "0", the module is editable in the module lister page.
  * Default: 1

**itsi_module_settings.conf.example**

No example

**itsi_module_viz.conf**

The following are the spec and example files for **itsi_module_viz.conf**.

**itsi_module_viz.conf.spec**

```
# This file contains possible attributes and values for changing tab
# names and panel titles in a module details dashboard.
#
# There is an itsi_module_viz.conf in each module-specific directory
within ITSI (for example,
# $SPLUNK_HOME/etc/apps/DA-ITSI-OS/default for the Operating System
module). To edit these
# configurations, place an itsi_module_viz.conf in
$SPLUNK_HOME/etc/apps/DA-ITSI-OS/local.
# You must restart Splunk software to enable configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
#
http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
#
# WARNING: Manual editing of this file is not recommended. Contact Support before proceeding.
```

**[<view_name>]**

* The name of the deep dive drilldown view within the ITSI module.

```
tabs = <comma-separated list>
```

* A list of tab IDs that will be included in this drilldown view.

```
<tabId>.control_token = <string>
```

* Used to run all the panel searches in a given tab.
* When the tab is shown, a list of search tokens are retrieved, the search tokens for
all inactive tabs are removed from the list, and the search token for the active tab is added to the list. This guarantees that only the shown tab's panels are displayed.

<tabId>.title = <string>
* The title of the tab that is displayed in the UI.

<tabId>.row.<int> = <comma-separated list>
* A list of panels that are displayed on each row on a tab.
* The panels are formatted as follows: <module_name>:<panel_name>.
* These settings start at 'row.0' and go up to any number of rows that is needed for a tab.
* Example:
  
  row.0 = DA-ITSI-OS:panel1,DA-ITSI-LB:panel2

<tabId>.extendable_tab = <boolean>
* Whether the tab is considered an extendable tab.
* This setting is for user-created tabs so that a delete button appears on the tab in the UI.
* Any tabs that ship with the module default to "false".

<tabId>.activation_rule = <comma-separated list>
* A list of KPI elements that are associated with a given tab so that context-aware drilldown is enabled based on the selected KPI from the deep dive.
* Each element here is defined as the content from the "target_field" parameter from each selected KPI from the file itsi_kpi_template.conf.

entity_search_filter = <JSON>
* A JSON blob of entity rules to use to filter entities for entity dropdown.

requested_entity_tokens = <comma-separated list>
* A list of entity attributes that are submitted as tokens.

itsi_module_viz.conf.example

No example

itsi_notable_event_retention.conf

The following are the spec and example files for
itsi_notable_event_retention.conf.
itsi_notable_event_retention.conf.spec

# This file contains attributes and values for defining how long notable event metadata remains 
# in the KV store before it moves to the 'itsi_notable_archive' index.
# 
# There is an itsi_notable_event_retention.conf in 
# $SPLUNK_HOME/etc/apps/SA-ITOA/default/. 
# To set custom configurations, place an 
# itsi_notable_event_retention.conf in 
# $SPLUNK_HOME/etc/apps/SA-ITOA/local/. You must restart Splunk to 
# enable 
# configurations. 
# 
# To learn more about configuration files (including precedence) please see 
# the documentation located at 
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings. 
# * You can also define global settings outside of any stanza, at the 
#   top 
#   of the file. 
# * Each .conf file should have at most one default stanza. If there 
#   are 
#   multiple default stanzas, attributes are combined. In the case of 
#   multiple definitions of the same attribute, the last definition in 
#   the 
#   file wins. 
# * If an attribute is defined at both the global level and in a 
# specific 
#   stanza, the value in the specific stanza takes precedence.

[<collection_name>]

retentionTimeInSec = <seconds>  
* The amount of time, in seconds, to retain the notable event object type.  
* Default: 15768000 (6 months)

retentionObjectCount = <number of objects>  
* The maximum number of a single object type (for example,
notable_event_comment) to retain in the KV store.
* The retention policy runs every hour. If the retention count is 50,000
  and a KV store collection exceeds 50,000 objects,
* the oldest objects are moved to the archive index so the collection
  only has 50,000 objects.
* Default: 50000

disabled = 0|1
* Whether this stanza is enabled or disabled.
* If "1", the stanza is disabled.
* If "0", the stanza is enabled.

object_type = <string>
* The notable event object type to retain.
* For example, comments, tags, external tickets, and so on.
* Required.
* If 'object_type' is not specified, the entire stanza is ignored.

itsi_notable_event_retention.conf.example

No example

itsi_notable_event_severity.conf

The following are the spec and example files for
itsi_notable_event_severity.conf.

itsi_notable_event_severity.conf.spec

# This file contains attributes and values for defining the colors
# associated with
# different severity levels in Episode Review.
#
# There is an itsi_notable_event_severity.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/default/.
# To set custom configurations, place an
# itsi_notable_event_severity.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local/. You must restart Splunk to
# enable
# configurations.
#
# To learn more about configuration files (including precedence) please
# see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the
top
#   of the file.
# * Each .conf file should have at most one default stanza. If there
are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
#   the
#   file wins.
# * If an attribute is defined at both the global level and in a
specific
#   stanza, the value in the specific stanza takes precedence.

[name]

color = <string>
* A valid color code to represent the color of an episode with this
severity.
* Required.

lightcolor = <string>
* A valid color code to represent the severity in Splunk Light.
* Required.

label = <string>
* The severity label.
* For example, Info, Medium, Critical.

default = 0|1
* Set this flag to indicate the default severity of an event or episode.

itsi_notable_event_severity.conf.example

No example

itsi_notable_event_status.conf

The following are the spec and example files for
itsi_notable_event_status.conf.
itsi_notable_event_status.conf.spec

# This file contains attributes and values for configuring label
descriptions
# and episode status in Episode Review.
#
# There is an itsi_notable_event_status.conf in
#$SPLUNK_HOME/etc/apps/SA-ITOA/default/.
# To set custom configurations, place an itsi_notable_event_status.conf
# in
#$SPLUNK_HOME/etc/apps/SA-ITOA/local/. You must restart Splunk to enable
# configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the top
#   of the file.
# * Each .conf file should have at most one default stanza. If there are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
#   the
#   file wins.
# * If an attribute is defined at both the global level and in a
#   specific
#   stanza, the value in the specific stanza takes precedence.

[id]

label = <string>
* A valid label for the episode status.
* Required.

default = <boolean>
* Indicates the initial status of an episode when it is generated in
  Episode Review.
* Set this value to "1" if this label is the default label.

description = <string>
* A description of the episode label.

end = <boolean>
* Indicates the last status in the Episode Review workflow.
* Set this value to "1" if this label is the end of the episode management workflow.
* If a status has an end flag enabled, any episode with that status is automatically broken. This means that no more events will flow into that episode.
This rule applies to status changes in Episode Review as well as through aggregation policy action rules.
* CAUTION: If you remove the "end" tag from the "Closed" status, you will no longer be able to close episodes through the Episode Review UI. It is recommended that you do not remove or change the location of this tag.

itsi_notable_event_status.conf.example

No example

itsi_service_analyzer.conf

The following are the spec and example files for itsi_service_analyzer.conf.

itsi_service_analyzer.conf.spec

# This file contains attributes and values for configuring the auto-refresh interval, or disabling auto-refresh.
# There is an itsi_service_analyzer.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/default/.
# To set custom configurations, place an itsi_service_analyzer.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/local/. You must restart Splunk to enable configurations.
# To learn more about configuration files (including precedence) please see the documentation located at
GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the top
#   of the file.
# * Each .conf file should have at most one default stanza. If there
#   are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
#   the
#   file wins.
# * If an attribute is defined at both the global level and in a
#   specific
#   stanza, the value in the specific stanza takes precedence.

[<stanza_name>]

* A setting that you want to enable for the Service Analyzer.
* Currently, 'auto_refresh' is the only supported setting.
* NOTE: Auto-refresh is automatically disabled in real-time search mode
  for the Service Analyzer.

disabled = 0|1
* Whether this setting is disabled for the Service Analyzer.
* Required.
* If "1", the setting is disabled.
* If "0", the setting is enabled.
* Default: 1

interval = <seconds>
* The interval, in seconds, at which auto-refresh occurs for Service
  Analyzer.
* Required.
* Default: 120 (2 minutes)

itsi_service_analyzer.conf.example

No example
itsi_service_template.conf

The following are the spec and example files for itsi_service_template.conf.

itsi_service_template.conf.spec

# Copyright (C) 2005-2019 Splunk Inc. All Rights Reserved.
#
# This file contains attributes and values for creating and uploading
# modules
# in Splunk IT Service Intelligence (ITSI).
#
# To set custom configurations, place an itsi_service_template.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local/ . You must restart Splunk
# software to
# enable configurations.
#
# To learn more about configuration files (including precedence) please
# see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
#
# CAUTION: You can drastically affect your Splunk installation by
# changing these settings.
# Consult technical support (http://www.splunk.com/page/submit_issue)
# if you are not sure how
# to configure this file.

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the
top
#   of the file.
# * Each .conf file should have at most one default stanza. If there
are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
the
#   file wins.
# * If an attribute is defined at both the global level and in a
specific
#   stanza, the value in the specific stanza takes precedence.
[<stanza_name>]

title = <string>
* A title of the module.

description = <string>
* The full description of the module being created.

description = <string>
* A JSON blob of entity rules (rules specification) used to associate
* entities to services created from this module.
* This setting is the same as the 'entity_rules' setting in itsi_service.conf.spec.
* Example:

```json
{
  "rule_condition": "AND",
  "rule_items": [
    {
      "field": "app_title",
      "field_type": "alias",
      "rule_type": "not",
      "value": ""
    },
    {
      "field": "itsi_role",
      "field_type": "info",
      "rule_type": "matches",
      "value": "apm"
    },
    {
      "field": "type",
      "field_type": "info",
      "rule_type": "matches",
      "value": "application"
    }
  ]
}
```

recommended_kpis = <json>
* A list of KPIs that are automatically added when a service
  is created with this module.

optional_kpis = <json>
* A list of KPIs that are available with this module but
  not added automatically when a service is created with it.
itsi_service_template.conf.example

No example

itsi_settings.conf

The following are the spec and example files for itsi_settings.conf.

itsi_settings.conf.spec

# Copyright (C) 2005-2019 Splunk Inc. All Rights Reserved.
# This file contains attributes and values for configuring the IT Service
# Intelligence (ITSI) app.
#
# There is an itsi_settings.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/default/.
# To set custom configurations, place an itsi_settings.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local/. You must restart Splunk software to enable
# configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
#
# CAUTION: You can drastically affect your Splunk installation by changing these settings.
# Consult technical support (http://www.splunk.com/page/submit_issue) if you are not sure how
# to configure this file.

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
#   * You can also define global settings outside of any stanza, at the top
#     of the file.
#   * Each .conf file should have at most one default stanza. If there
#     are
#     multiple default stanzas, attributes are combined. In the case of
#     multiple definitions of the same attribute, the last definition in
the
#    file wins.
#  If an attribute is defined at both the global level and in a
#    specific
#  stanza, the value in the specific stanza takes precedence.

[datamodels://<app>]

* 'app' is the ID for the app containing the datamodel.

blacklist = <datamodel_names_list>
* A pipe-separated list of data model external authentication interface
  (EAI) names (IDs) to blacklist.
* NOTE: Data model names do not contain pipe characters.
* The blacklisted data models will not be supported and remain hidden
  from the ITSI UI.

[cloud]

show_migration_message = <boolean>
* Removes Cloud migration messages about deprecated files or apps from
  the logs because this process is done internally.

[backup_restore]

* Defines settings related to ITSI backup/restore.

job_queue_timeout = <seconds>
* The amount of time, in seconds, before the backup/restore job queue
  times out if the node owning the job has been down for too long to
  allow other jobs to proceed.
* The minimum supported timeout period is 3600 seconds (1 hour). The
  system
  sets the timeout to 3600 seconds when a value lower than this is set.
* Default: 43200 (12 hours)

[import]

* Defines limits for import behavior.

import_batch_size = <integer>
* The number of rows or objects that the importer should analyze before
  attempting a save to the KV store.
* Default: 750
preview_sample_limit = <integer>
* The maximum number of rows that are returned from a preview request for a pending import.
* Default: 100

asynchronous_processing_threshold = <integer>
* The number of rows after which the bulk importer reads and stores the inbound content so that it can be processed at a more convenient time, rather than processing it immediately.

[metric_backfill]

* Defines backfill settings.

pre_calculation_window = <seconds>
* The size, in seconds, of the pre-calculation window for metric backfill.
* The smallest accepted value is 1. Increasing this value makes the backfill search faster, but less accurate.
* Default: 1

[sai_integration]

* Defines Splunk App for Infrastructure (SAI) settings.

show_detection_modal = <boolean>
* Whether or not to show the Splunk App for Infrastructure integration modal when the Service Analyzer loads.
* If "1", ITSI displays the integration modal.
* If "0", ITSI does not display the integration modal.
* Default: 1

[synced_kpi_scheduling]

disabled = <boolean>
* Indicates whether KPI saved searches have a randomized schedule or the same schedule.
* If "1", KPI saved searches run at staggered times throughout the scheduled interval.
* If "0", KPI saved searches all run at the same time during each scheduled interval.
* CAUTION: Changing this value to "0" can have a significant performance impact. KPI saved searches are designed to run at different times to prevent the search scheduler from becoming overloaded.
* Default = 1
[customsearch]

timeout_read = <seconds>
* The maximum number of seconds that an ITSI custom search command will attempt to
  read a chunk from the "chunked" custom search command protocol.
* Default: 60

[episode_action_dispatch]

* Enables the ability to dispatch actions from a Splunk instance to be executed on another instance.
* Configure these settings in this stanza if you want to specify whether this Splunk instance will read actions and execute actions from another instance or dispatch actions to anotherSplunk instance.
* The settings in this stanza define the host's role. If configured as an 'executor' they also define the URI and username of the host for consuming Event Analytics episode actions.

role = <executor|master|both>
* Whether the machine is executing actions, running core event analytics services, or both.
* If "executor", the host is only executing actions.
* If "master", the host is only running core event analytics services.
* Default: both

remote_ea_mgmt_uri = <string>
* The Splunkd management URI from which to pull action jobs, in addition to other core event analytics services.
* The URI must include a scheme, host, and port.
* If an empty string, ITSI uses the local Splunk address to avoid the necessity of an update if a custom port or scheme is in use on the local Splunk instance.
* This setting is only required if 'role' is set to "executor".
* Default: empty string

remote_ea_username = <string>
* The username to use when communicating with the remote host for actions and updates.
* If you're on localhost, ITSI always uses the past session from Splunkd (the provided username is ignored in this case).
* This setting is only required if 'role' is set to "executor".
* Default: empty string
**service_template_sync_in_progress = <boolean>**
* Whether a service template is currently syncing.
* If "1", at least one service template is syncing and it is not safe to upgrade.
* If "0", no service templates are syncing and it is safe to upgrade.
* CAUTION: Do not change this setting. It is updated dynamically by ITSI.
* Default: 0

**itsi_settings.conf.example**

No example

**itsi_team.conf**

The following are the spec and example files for itsi_team.conf.

**itsi_team.conf.spec**

```plaintext
# This file contains attributes and values for uploading ITSI teams
# to the KV store. By default, only the Global team ships with ITSI.
#
# There is an itsi_team.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/default.
# To set custom configurations, place an itsi_team.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local/. You must restart Splunk
software to
# enable configurations.
#
# To learn more about configuration files (including precedence) please
see
# the documentation located at
#
http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
#
# CAUTION: You can drastically affect your Splunk installation by
changing these settings.
# Consult technical support (http://www.splunk.com/page/submit_issue)
if you are not sure how
# to configure this file.
```
GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the
top
#   of the file.
# * Each .conf file should have at most one default stanza. If there
are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
the
#   file wins.
# * If an attribute is defined at both the global level and in a
specific
#   stanza, the value in the specific stanza takes precedence.

[default_itsi_security_group]

title = <value>
* The name of the team.
* Duplicate team names are allowed, but be aware of other team names
  and use naming conventions to avoid confusion.

description = <value>
* A meaningful description of the team.

 Immutable = <boolean>
* Whether users can edit the team.
  * If "1", the team cannot be edited.
  * If "0", the team can be edited.
  * Default: 0

acl = <dictionary>
* An Access Control List (ACL) associating ITOA roles with permissions
  within that team.
* Assign read or write access to the listed ITOA roles as appropriate.
  If a role has write permissions for a team, a user with this role can
  create and modify services in the team. The user can't delete a
  service
  in the team unless the role has the delete capability for a service.

[notable_event_review_security_group]

disable = <boolean>
* Use this setting to turn off Role-Based Access Control (RBAC) for
Episode
Review only.
* If you set this flag to "1", all users will be able to see all events within Episode Review, regardless of their team.
* If "1", RBAC is disabled for Episode Review.
* If "0", RBAC is enabled for Episode Review.
* Default: 0

itsi_team.conf.example

No example

limits.conf

The following are the spec and example files for limits.conf.

limits.conf.spec

# Version 7.3.0
#

OVERVIEW

# This file contains descriptions of the settings that you can use to configure limitations for the search commands.
# Each stanza controls different search commands settings.
# There is a limits.conf file in the $SPLUNK_HOME/etc/system/default/ directory.
# Never change or copy the configuration files in the default directory.
# The files in the default directory must remain intact and in their original location.
# To set custom configurations, create a new file with the name limits.conf in
# the $SPLUNK_HOME/etc/system/local/ directory. Then add the specific settings
# that you want to customize to the local configuration file.
# For examples, see limits.conf.example. You must restart the Splunk instance
# to enable configuration changes.
# To learn more about configuration files (including file precedence)
see the
documentation located at
http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

About Distributed Search
Unlike most settings which affect searches, limits.conf settings are not
provided by the search head to be used by the search peers. This means
that if you need to alter search-affecting limits in a distributed
environment, typically you will need to modify these settings on the
relevant peers and search head for consistent results.

GLOBAL SETTINGS

Use the [default] stanza to define any global settings.
* You can also define global settings outside of any stanza, at the top of
  the file.
* Each .conf file should have at most one default stanza. If there are
  multiple default stanzas, settings are combined. In the case of
  multiple definitions of the same setting, the last definition in the
  file takes precedence.
* If a setting is defined at both the global level and in a specific
  stanza, the value in the specific stanza takes precedence.

CAUTION: Do not alter the settings in the limits.conf file unless you
know what you are doing. Improperly configured limits might result in
splunkd crashes, memory overuse, or both.

[default]

DelayArchiveProcessorShutdown = <boolean>
* Specifies whether during splunk shutdown archive processor should finish
  processing archive file under process.
* When set to "false": The archive processor abandons further processing of
  the archive file and will process again from start again.
* When set to "true": The archive processor will complete processing of
  the archive file. Shutdown will be delayed.
max_mem_usage_mb = <non-negative integer>

* Default: false

* Provides a limitation to the amount of RAM, in megabytes (MB), a batch of
  events or results will use in the memory of a search process.
* Operates on an estimation of memory use which is not exact. The estimation can
  deviate by an order of magnitude or so to both the smaller and larger sides.
* The limitation is applied in an unusual way; if the number of results or
  events exceeds maxresults, AND the estimated memory exceeds this limit, the
  data is spilled to disk.
* This means, as a general rule, lower limits will cause a search to use more
  disk I/O and less RAM, and be somewhat slower, but should cause the same
  results to typically come out of the search in the end.
* This limit is applied currently to a number, but not all search processors.
  However, more will likely be added as it proves necessary.
* The number is thus effectively a ceiling on batch size for many components of
  search for all searches run on this system.
* When set to "0": Specifies that the size is unbounded. Searches might be
  allowed to grow to arbitrary sizes.

NOTE:
* The mvexpand command uses the 'max_mem_usage_mb' value in a different way.
  * The mvexpand command has no combined logic with 'maxresults'.
  * If the memory limit is exceeded, output is truncated, not spilled to disk.
* The stats command processor uses the 'max_mem_usage_mb' value in the following way.
  * If the estimated memory usage exceeds the specified limit, the results are
    spilled to disk.
  * If 0 is specified, the results are spilled to the disk when the number of
    results exceed the 'maxresultrows' setting.
* The eventstats command processor uses the 'max_mem_usage_mb' value in the following way.
  * Both the 'max_mem_usage_mb' and the 'maxresultrows' settings are used to
    determine the maximum number of results to return. If the limit for one
    setting is reached, the eventstats processor continues to return results
until the limit for the other setting is reached. When both limits are reached, the eventstats command processor stops adding the requested fields to the search results.
* If you set 'max_mem_usage_mb' to 0, the eventstats command processor uses only the 'maxresultrows' setting as the threshold. When the number of results exceeds the 'maxresultrows' setting, the eventstats command processor stops adding the requested fields to the search results.
* Default: 200

min_batch_size_bytes = <integer>
* Specifies the size, in bytes, of the file/tar after which the file is handled by the batch reader instead of the trailing processor.
* Global parameter, cannot be configured per input.
* NOTE: Configuring this to a very small value could lead to backing up of jobs at the tailing processor.
* Default: 20971520

regex_cpu_profiling = <boolean>
* Enable CPU time metrics for RegexProcessor. Output will be in the metrics.log file.
  Entries in metrics.log will appear per_host_regex_cpu, per_source_regex_cpu, per_sourcetype_regex_cpu, per_index_regex_cpu.
* Default: false

file_and_directory_eliminator_reaper_interval = <integer>
* Specifies how often, in seconds, to run the FileAndDirectoryEliminator reaping process.
* The FileAndDirectoryEliminator eliminates files and directories by moving them to a location that is reaped periodically. This reduces the chance of encountering issues due to files being in use.
* On Windows, the FileAndDirectoryEliminator is used by the deployment client to delete apps that have been removed or that are being redeployed.
* A value of 0 disables the FileAndDirectoryEliminator.
* NOTE: Do not change this setting unless instructed to do so by Splunk Support.
* Default (on Windows): 60
* Default (otherwise): 0
[searchresults]

* This stanza controls search results for a variety of Splunk search commands.

compression_level = <integer>
* Compression level to use when writing search results to .csv.gz files.
* Default: 1

maxresultrows = <integer>
* Configures the maximum number of events are generated by search commands
  which grow the size of your result set (such as multikv) or that create
  events. Other search commands are explicitly controlled in specific stanzas
  below.
* This limit should not exceed 50000.
* Default: 50000

tocsv_maxretry = <integer>
* Maximum number of times to retry the atomic write operation.
* When set to "1": Specifies that there will be no retries.
* Default: 5

tocsv_retryperiod_ms = <integer>
* Period of time to wait before each retry.
* Default: 500

* These settings control logging of error messages to the info.csv file.
  All messages will be logged to the search.log file regardless of these settings.

[search_info]

* This stanza controls logging of messages to the info.csv file.
* Messages logged to the info.csv file are available to REST API clients and Splunk Web. Limiting the messages added to info.csv will mean
  that these messages will not be available in the UI and/or the REST API.

filteredindexes_log_level = [DEBUG|INFO|WARN|ERROR]
* Log level of messages when search returns no results because user has no permissions to search on queried indexes.

infocsv_log_level = [DEBUG|INFO|WARN|ERROR]
* Limits the messages which are added to the info.csv file to the stated level and above.
* For example, if "infocsv_log_level" is WARN, messages of type WARN
and higher will be added to the info.csv file.

max_infocsv_messages  = <positive integer>
* If more than max_infocsv_messages log entries are generated, additional
  entries will not be logged in the info.csv file. All entries will still be
  logged in the search.log file.

show_warn_on_filtered_indexes = <boolean>
* Log warnings if search returns no results because user has no permissions to search on queried indexes.

[subsearch]

* This stanza controls subsearch results.
* NOTE: This stanza DOES NOT control subsearch results when a subsearch is
  called by commands such as join, append, or appendcols.
* Read more about subsearches in the online documentation:
  http://docs.splunk.com/Documentation/Splunk/latest/Search/Aboutsubsearches

maxout = <integer>
* Maximum number of results to return from a subsearch.
  * This value cannot be greater than or equal to 10500.
  * Default: 10000

maxtime = <integer>
* Maximum number of seconds to run a subsearch before finalizing
  * Default: 60

ttl = <integer>
* The time to live (ttl), in seconds, of the cache for the results of a given
  subsearch.
  * Do not set this below 120 seconds.
  * See the definition in the [search] stanza under the "TTL" section for more
    details on how the ttl is computed.
  * Default: 300 (5 minutes)

SEARCH COMMAND

# This section contains the limitation settings for the search command.
# The settings are organized by type of setting.
# The settings under the [search] stanza are organized by type of setting.

# Batch search
# This section contains settings for batch search.

allow_batch_mode = <boolean>
* Specifies whether or not to allow the use of batch mode which searches
  in disk based batches in a time insensitive manner.
* In distributed search environments, this setting is used on the search
  head.
* Default: true

batch_search_max_index_values = <integer>
* When using batch mode, this limits the number of event entries read
  from the
  index file. These entries are small, approximately 72 bytes. However
  batch
  mode is more efficient when it can read more entries at one time.
* Setting this value to a smaller number can lead to slower search
  performance.
* A balance needs to be struck between more efficient searching in batch
  mode
* and running out of memory on the system with concurrently running
  searches.
* Default: 10000000

batch_search_max_pipeline = <integer>
* Controls the number of search pipelines that are
  launched at the indexer during batch search.
* Increasing the number of search pipelines should help improve search
  performance, however there will be an increase in thread and memory
  usage.
* This setting applies only to searches that run on remote indexers.
* Default: 1

batch_search_max_results_aggregator_queue_size = <integer>
* Controls the size, in MB, of the search results queue to which all
  the search pipelines dump the processed search results.
* Increasing the size can lead to search performance gains.
  Decreasing the size can reduce search performance.
* Do not specify zero for this setting.
* Default: 100

batch_search_max_serialized_results_queue_size = <integer>
* Controls the size, in MB, of the serialized results queue from which
the serialized search results are transmitted.
* Increasing the size can lead to search performance gains.
  Decreasing the size can reduce search performance.
* Do not specify zero for this setting.
  Default: 100

NOTE: The following batch search settings control the periodicity of retries
to search peers in the event of failure (Connection errors, and others).
The interval exists between failure and first retry, as well as successive retries in the event of further failures.

batch_retry_min_interval = <integer>
* When batch mode attempts to retry the search on a peer that failed,
  specifies the minimum time, in seconds, to wait to retry the search.
  Default: 5

batch_retry_max_interval = <integer>
* When batch mode attempts to retry the search on a peer that failed,
  specifies the maximum time, in seconds, to wait to retry the search.
  Default: 300 (5 minutes)

batch_retry_scaling = <double>
* After a batch retry attempt fails, uses this scaling factor to increase
  the time to wait before trying the search again.
  The value should be > 1.0.
  Default: 1.5

##########################################################################
# Bundles
##########################################################################
# This section contains settings for bundles and bundle replication.

load_remote_bundles = <boolean>
* On a search peer, allow remote (search head) bundles to be loaded in splunkd.
  Default: false.

replication_file_ttl = <integer>
* The time to live (ttl), in seconds, of bundle replication tarballs,
  for example: *.bundle files.
  Default: 600 (10 minutes)

replication_period_sec  = <integer>
* The minimum amount of time, in seconds, between two successive bundle replications.
  Default: 60

sync_bundle_replication = [0|1|auto]
* A flag that indicates whether configuration file replication blocks
searches or is run asynchronously.
* When set to "auto": The Splunk software uses asynchronous
  replication only if all of the peers support asynchronous bundle
  replication.
  Otherwise synchronous replication is used.
* Default: auto

# Concurrency
# This section contains settings for search concurrency limits.

base_max_searches = <integer>
* A constant to add to the maximum number of searches, computed as a
  multiplier of the CPUs.
* Default: 6

max_rt_search_multiplier = <decimal number>
* A number by which the maximum number of historical searches is
  multiplied
to determine the maximum number of concurrent real-time searches.
* NOTE: The maximum number of real-time searches is computed as:
  max_rt_searches = max_rt_search_multiplier x max_hist_searches
* Default: 1

max_searches_per_cpu = <integer>
* The maximum number of concurrent historical searches for each CPU.
The system-wide limit of historical searches is computed as:
  max_hist_searches =  max_searches_per_cpu x number_of_cpus +
  base_max_searches
* NOTE: The maximum number of real-time searches is computed as:
  max_rt_searches = max_rt_search_multiplier x max_hist_searches
* Default: 1

# Distributed search
# This section contains settings for distributed search connection
# information.

addpeer_skew_limit = <positive integer>
* Absolute value of the largest time skew, in seconds, that is allowed
  when
  configuring a search peer from a search head, independent of time.
* If the difference in time (skew) between the search head and the peer
  is
greater than "addpeer_skew_limit", the search peer is not added.
* This is only relevant to manually added peers. This setting has no
  effect
  on index cluster search peers.
* Default: 600 (10 minutes)
fetch_remote_search_log = [enabled|disabledSavedSearches|disabled]
* When set to "enabled": All remote search logs are downloaded barring the oneshot search.
* When set to "disabledSavedSearches": Downloads all remote logs other than saved search logs and oneshot search logs.
* When set to "disabled": Irrespective of the search type, all remote search log download functionality is disabled.
* NOTE:
  * The previous Boolean values:[true|false] are still supported, but are not recommended.
  * The previous value of "true" maps to the current value of "enabled".
  * The previous value of "false" maps to the current value of "disabled".
  * Default: disabledSavedSearches

max_chunk_queue_size = <integer>
* The maximum size of the chunk queue.
  * default: 10000000

max_combiner_memevents = <integer>
* Maximum size of the in-memory buffer for the search results combiner. The <integer> is the number of events.
  * Default: 50000

max_tolerable_skew = <positive integer>
* Absolute value of the largest time skew, in seconds, that is tolerated between the native clock on the search head and the native clock on the peer (independent of time zone).
* If this time skew is exceeded, a warning is logged. This estimate is approximate and tries to account for network delays.
  * Default: 60

max_workers_searchparser = <integer>
* The number of worker threads in processing search result when using round robin policy.
  * default: 5

results_queue_min_size = <integer>
* The minimum size, of search result chunks, that will be kept from peers for processing on the search head before throttling the rate that data is accepted.
* The minimum queue size in chunks is the "results_queue_min_size" value and the number of peers providing results, which ever is greater.
  * Default: 10

result_queue_max_size = <integer>
* The maximum size, in MB, that will be kept from peers for processing on
the search head before throttling the rate that data is accepted.
* The "results_queue_min_size" value takes precedence. The number of
search
results chunks specified by "results_queue_min_size" will always be
retained in the queue even if the combined size in MB exceeds the
"result_queue_max_size" value.
* Default: 100

results_queue_read_timeout_sec = <integer>
* The amount of time, in seconds, to wait when the search executing on
the
search head has not received new results from any of the peers.
* Cannot be less than the 'receiveTimeout' setting in the
distsearch.conf
  file.
* Default: 900

batch_wait_after_end = <integer>
* DEPRECATED: Use the 'results_queue_read_timeout_sec' setting instead.

# Field stats
# This section contains settings for field statistics.

fieldstats_update_freq = <number>
* How often to update the field summary statistics, as a ratio to the
  elapsed
    run time so far.
* Smaller values means update more frequently.
* When set to "0": Specifies to update as frequently as possible.
* Default: 0

fieldstats_update_maxperiod = <number>
* The maximum period, in seconds, for updating field summary statistics.
* When set to "0": Specifies that there is not maximum period. The
  period
    is dictated by the calculation:
      current_run_time x fieldstats_update_freq
* Fractional seconds are allowed.
* Default: 60

min_freq = <number>
* Minimum frequency of a field that is required for the field to be
  included
  in the /summary endpoint.
* The frequency must be a fraction >=0 and <=1.
* Default: 0.01 (1%)

# History

355
# This section contains settings for search history.

`enable_history = <boolean>`
* Specifies whether to keep a history of the searches that are run.
  * Default: true

`max_history_length = <integer>`
* Maximum number of searches to store in history for each user and application.
  * Default: 1000

# Memory tracker

# This section contains settings for the memory tracker.

`enable_memory_tracker = <boolean>`
* Specifies if the memory tracker is enabled.
  * When set to "false" (disabled): The search is not terminated even if the search exceeds the memory limit.
  * When set to "true": Enables the memory tracker.
  * Must be set to "true" to enable the "search_process_memory_usage_threshold"
    setting or the "search_process_memory_usage_percentage_threshold" setting.
  * Default: false

`search_process_memory_usage_threshold = <double>`
* To use this setting, the "enable_memory_tracker" setting must be set to "true".
  * Specifies the maximum memory, in MB, that the search process can consume in RAM.
  * Search processes that violate the threshold are terminated.
  * If the value is set to 0, then search processes are allowed to grow unbounded in terms of in memory usage.
  * Default: 4000 (4GB)

`search_process_memory_usage_percentage_threshold = <decimal>`
* To use this setting, the "enable_memory_tracker" setting must be set to "true".
  * Specifies the percent of the total memory that the search process is entitled to consume.
  * Search processes that violate the threshold percentage are terminated.
  * If the value is set to zero, then splunk search processes are allowed to grow unbounded in terms of percentage memory usage.
  * Any setting larger than 100 or less than 0 is discarded and the default value is used.
  * Default: 25%
# Meta search

This section contains settings for meta search.

allow_inexact_metasearch = <boolean>
* Specifies if a metasearch that is inexact be allowed.
* When set to "true": An INFO message is added to the inexact metasearches.
* When set to "false": A fatal exception occurs at search parsing time.
* Default: false

indexed_as_exact_metasearch = <boolean>
* Specifies if a metasearch can process <field>=<value> the same as <field>::<value>, if <field> is an indexed field.
* When set to "true": Allows a larger set of metasearches when the "allow_inexact_metasearch" setting is "false". However, some of the metasearches might be inconsistent with the results of doing a normal search.
* Default: false

# Misc

This section contains miscellaneous search settings.

disk_usage_update_period = <number>
* Specifies how frequently, in seconds, should the search process estimate the artifact disk usage.
* The quota for the amount of disk space that a search job can use is controlled by the 'srchDiskQuota' setting in the authorize.conf file.
* Exceeding this quota causes the search to be auto-finalized immediately, even if there are results that have not yet been returned.
* Fractional seconds are allowed.
* Default: 10

dispatch_dir_warning_size = <integer>
* Specifies the number of jobs in the dispatch directory that triggers when to issue a bulletin message. The message warns that performance might be impacted.
* Default: 5000

do_not_use_summaries = <boolean>
* Do not use this setting without working in tandem with Splunk support.
* This setting is a very narrow subset of "summary_mode=none".
* When set to "true": Disables some functionality that is necessary for report acceleration.
* In particular, when set to "true", search processes will no longer query
the main splunkd's /admin/summarization endpoint for report acceleration
  summary IDs.
  * In certain narrow use-cases this might improve performance if report acceleration (savedsearches.conf:auto_summarize) is not in use, by lowering
    the main splunkd's process overhead.
  * Default: false

enable_datamodel_meval = <boolean>
  * Enable concatenation of successively occurring evals into a single comma-separated eval during the generation of datamodel searches.
  * default: true

enable_conditional_expansion = <boolean>
  * Determines whether or not scoped conditional expansion of knowledge objects occurs during search string expansion. This only applies on the search head.
  * NOTE: Do not change unless instructed to do so by Splunk Support.
  * Default: true

force_saved_search_dispatch_as_user = <boolean>
  * Specifies whether to overwrite the "dispatchAs" value.
  * When set to "true": The "dispatchAs" value is overwritten by "user" regardless of the [user|owner] value in the savedsearches.conf file.
  * When set to "false": The value in the savedsearches.conf file is used.
  * You might want to set this to "true" to effectively disable "dispatchAs = owner" for the entire install, if that more closely aligns
    with security goals.
  * Default: false

max_id_length = <integer>
  * Maximum length of the custom search job ID when spawned by using REST API argument "id".

search_keepalive_frequency = <integer>
  * Specifies how often, in milliseconds, a keepalive is sent while a search is running.
  * Default: 30000 (30 seconds)

search_keepalive_max = <integer>
  * The maximum number of uninterrupted keepalives before the connection is closed.
  * This counter is reset if the search returns results.
  * Default: 100

search_retry = <boolean>
  * Specifies whether the Splunk software retries parts of a search within a currently-running search process when there are indexer failures in
the indexer clustering environment.
* Indexers can fail during rolling restart or indexer upgrade when indexer clustering is enabled. Indexer reboots can also result in failures.
* This setting applies only to historical search in batch mode, real-time search, and indexed real-time search.
* When set to true, the Splunk software attempts to rerun searches on indexer cluster nodes that go down and come back up again. The search process on the search head maintains state information about the indexers and buckets.
* NOTE: Search retry is on a best-effort basis, and it is possible for Splunk software to return partial results for searches without warning when you enable this setting.
* When set to false, the search process will stop returning results from a specific indexer when that indexer undergoes a failure.
* Default: false

**stack_size = <integer>**
* The stack size, in bytes, of the thread that executes the search.
* Default: 4194304 (4MB)

**summary_mode = [all|only|none]**
* Specifies if precomputed summary data are to be used.
* When set to "all": Use summary data if possible, otherwise use raw data.
* When set to "only": Use summary data if possible, otherwise do not use any data.
* When set to "none": Never use precomputed summary data.
* Default: all

**track_indextime_range = <boolean>**
* Specifies if the system should track the _indextime range of returned search results.
* Default: true

**use_bloomfilter = <boolean>**
* Controls whether to use bloom filters to rule out buckets.
* Default: true

**use_metadata_elimination = <boolean>**
* Control whether to use metadata to rule out buckets.
* Default: true

**results_serial_format = [csv|srs]**
* The internal format used for storing serialized results on disk.
* Options:
  * csv: Comma-separated values format
  * srs: Splunk binary format
results_compression_algorithm = [gzip|zstd|none]
* The compression algorithm used for storing serialized results on disk.
* Options:
  * gzip: gzip
  * zstd: zstd
  * none: No compression
* NOTE: Do not change this setting unless instructed to do so by Splunk Support.
* Default: zstd

record_search_telemetry = <boolean>
* Controls whether to record search related metrics in search_telemetry.json in the dispatch dir. It also indexes this file to the _introspection index.
* NOTE: Do not change this setting unless instructed to do so by Splunk Support.
* Default: true

always_include_indexedfield_lispy = <boolean>
* Whether or not search always looks for a field that does not have "INDEXED = true" set in fields.conf using both the indexed and non-indexed forms.
* If set to "true", when searching for <field>=<value>, the lexicon is searched for both "<field>::<value>" and "<value>".
* If set to "false", when searching for <field>=<val>, the lexicon is searched only for "<value>".
* Set to "true" if you have fields that are sometimes indexed and sometimes not indexed.
* For field names that are always indexed, it is much better for performance to set "INDEXED = true" in fields.conf for that field instead.
* Default: false

auto_cancel_after_pause = <integer>
* Specifies the amount of time, in seconds, that a search must be paused before the search is automatically cancelled.
* If set to 0, a paused search is never automatically cancelled.
* Default: 0

max_searchinfo_map_size = <integer>
* Maximum number of entries in each SearchResultsInfo data structure map that are used to track information about search behavior
**Default:** 50000

`track_matching_sourcetypes = <bool>`
* If true, keeps track of the number of events of each sourcetype that match a search, and store that information in info.csv
* **Default:** true

`max_audit_sourcetypes = <integer>`
* If `track_matching_sourcetypes = true`, the matching sourcetypes for a search will be written to the info=completed audit.log message upon completion of the search, up to `max_audit_sourcetypes`.
* If `max_audit_sourcetypes` is set to 0, sourcetype information will not be added to audit.log.
* If the number of matching sourcetypes exceeds the `max_audit_sourcetypes` setting, the sourcetypes with the greatest number of matching events will be included.
* **Default:** 100

`execute_postprocess_in_search = <bool>`
* If true, try to run postprocess searches ahead of time in the search process instead of the main splunkd process.
* **Default:** true

# Parsing

This section contains settings related to parsing searches.

`max_macro_depth = <integer>`
* Maximum recursion depth for macros. Specifies the maximum levels for macro expansion.
* It is considered a search exception if macro expansion does not stop after this many levels.
* **Value must be greater than or equal to 1.**
* **Default:** 100

`max_subsearch_depth = <integer>`
* Maximum recursion depth for subsearches. Specifies the maximum levels for subsearches.
* It is considered a search exception if a subsearch does not stop after this many levels.
* **Default:** 8

`min_prefix_len = <integer>`
* The minimum length of a prefix before a wildcard (*) to use in the query
to the index.
* Default: 1

use_directives = <boolean>
* Specifies whether a search can take directives and interpret them
  into arguments.
* This is used in conjunction with the search optimizer in order to
  improve search performance.
* Default: true

########################################################################
# Phased execution settings
########################################################################
# This section contains settings for multi-phased execution

phased_execution = <boolean>
DEPRECATED This setting has been deprecated.

phased_execution_mode = [multithreaded|auto|singlethreaded]
* Controls whether searches use the multiple-phase method of search
  execution,
  which is required for parallel reduce functionality as of Splunk
  Enterprise
  7.1.0.
* When set to 'multithreaded' the Splunk platform uses the
  multiple-phase
  search execution method. Allows usage of the 'redistribute' command.
* When set to 'auto', the Splunk platform uses the multiple-phase search
  execution method when the 'redistribute' command is used in the search
  string. If the 'redistribute' command is not present in the search
  string,
  the single-phase search execution method is used.
* When set to 'singlethreaded' the Splunk platform uses the
  single-threaded
  search execution method, which does not allow usage of the
  'redistribute'
  command.
* NOTE: Do not change this setting unless instructed to do so by Splunk
  Support.
* Default: multithreaded

########################################################################
# Preview
########################################################################
# This section contains settings for previews.

max_preview_period = <integer>
* The maximum time, in seconds, between previews.
* Used with the preview interval that is calculated with the
  "preview_duty_cycle" setting.
* When set to "0": Specifies unlimited time between previews.
* Default: 0
min_preview_period = <integer>
* The minimum time, in seconds, required between previews. When the calculated
  interval using "preview_duty_cycle" indicates previews should be run frequently. This setting is used to limit the frequency with which previews run.
* Default: 1

preview_duty_cycle = <number>
* The maximum time to spend generating previews, as a fraction of the total
  search time.
* Must be > 0.0 and < 1.0
* Default: 0.25

preview_freq = <timespan> or <ratio>
* Minimum amount of time between results preview updates.
* If specified as a number, between > 0 and < 1, the minimum time between
  previews is computed as a ratio of the amount of time that the search has been running, or as a ratio of the length of the time window for real-time windowed searches.
* Default: a ratio of 0.05

#=================================================================#
# Quota or queued searches
#=================================================================#
# This section contains settings for quota or queued searches.

default_allow_queue = [0|1]
* Unless otherwise specified by using a REST API argument, specifies if an
  asynchronous job spawning request should be queued on quota violation.
  If not, an http error of server too busy is returned.
* Default: 1 (true)

dispatch_quota_retry = <integer>
* The maximum number of times to retry to dispatch a search when the quota has
  been reached.
* Default: 4

dispatch_quota_sleep_ms = <integer>
* The time, in milliseconds, between retrying to dispatch a search when a
  quota is reached.
* Retries the given number of times, with each successive wait 2x longer than
  the previous wait time.
* Default: 100
enable_cumulative_quota = <boolean>
* Specifies whether to enforce cumulative role based quotas.
* Default: false

queued_job_check_freq = <number>
* Frequency, in seconds, to check queued jobs to determine if the jobs can
  be started.
* Fractional seconds are allowed.
* Default: 1.

chunk_multiplier = <integer>
* A multiplier that the "max_results_perchunk", "min_results_perchunk", and
  "target_time_perchunk" settings are multiplied by for a long running search.
* Default: 5

long_search_threshold = <integer>
* The time, in seconds, until a search is considered "long running".
* Default: 2

max_rawsize_perchunk = <integer>
* The maximum raw size, in bytes, of results for each call to search
  (in dispatch).
* When set to "0": Specifies that there is no size limit.
* This setting is not affected by the "chunk_multiplier" setting.
* Default: 100000000 (100MB)

max_results_perchunk = <integer>
* The maximum number of results to emit for each call to the preview data
  generator.
* Default: 2500

max_results_perchunk = <integer>
* Maximum results for each call to search (in dispatch).
* Must be less than or equal to the "maxresultrows" setting.
* Default: 2500

min_results_perchunk = <integer>
* The minimum results for each call to search (in dispatch).
* Must be less than or equal to the "max_results_perchunk" setting.
* Default: 100

target_time_perchunk = <integer>
* The target duration, in milliseconds, of a particular call to fetch search results.
* Default: 2000 (2 seconds)

# Real-time
# This section contains settings for real-time searches.

check_splunkd_period = <number>
* Amount of time, in seconds, that determines how frequently the search process
  (when running a real-time search) checks whether the parent process
  (splunkd) is running or not.
* Fractional seconds are allowed.
* Default: 60 (1 minute)

realtime_buffer = <integer>
* Maximum number of accessible events to keep for real-time searches in Splunk Web.
* Acts as circular buffer after this buffer limit is reached.
* Must be greater than or equal to 1.
* Default: 10000

# Remote storage
# This section contains settings for remote storage.

bucket_localize_acquire_lock_timeout_sec = <integer>
* The maximum amount of time, in seconds, to wait when attempting to acquire a
  lock for a localized bucket.
* When set to 0, waits indefinitely.
* This setting is only relevant when using remote storage.
* Default: 60 (1 minute)

bucket_localize_max_timeout_sec = <integer>
* The maximum amount of time, in seconds, to spend localizing a bucket stored
  in remote storage.
* If the bucket contents (what is required for the search) cannot be localized
  in that timeframe, the bucket will not be searched.
* When set to "0": Specifies an unlimited amount of time.
* This setting is only relevant when using remote storage.
* Default: 300 (5 minutes)

bucket_localize_status_check_period_ms = <integer>
* The amount of time, in milliseconds, between consecutive status checks to see
  if the needed bucket contents required by the search have been
localized.
* This setting is only relevant when using remote storage.
* The minimum and maximum values are 10 and 60000, respectively. If the
  specified value falls outside this range, it is effectively set to the
  nearest value within the range. For example, if you set the value to
  70000, the effective value will be 60000.
* Default: 50 (.05 seconds)

bucket_localize_status_check_backoff_start_ms = <integer>
* When explicitly set, and different from
bucket_localize_status_check_period_ms,
  enables exponential backoff between consecutive status checks for
bucket
  localization. Starting from the specified amount of time, in
milliseconds, up to
  bucket_localize_status_check_period_ms.
* This setting is only relevant when using remote storage.
* Setting this option is beneficial when bucket contents localize
quickly (e.g., in
  less time than the minimal allowed value for
bucket_localize_status_check_period_ms),
  or with high variability.
* The minimum and maximum values are 1 and
bucket_localize_status_check_period_ms,
  respectively. If the specified value falls outside this range, it is
effectively
  set to the nearest value within the range.
* NOTE: Do not change this setting unless instructed to do so by Splunk
  Support.
* Default: 0 (no backoff)

bucket_localize_max lookahead = <integer>
* Specifies the maximum number of buckets the search command localizes
  for look-ahead purposes, in addition to the required bucket.
* Increasing this value can improve performance, at the cost of
  additional
  network/io/disk utilization.
* Valid values are 0-64. Any value larger than 64 will be set to 64.
Other
  invalid values will be discarded and the default will be substituted.
* This setting is only relevant when using remote storage.
* Default: 5

bucket_localize_lookahead_priority_ratio = <integer>
* A value of N means that lookahead localizations will occur only 1 out
  of N
  search localizations, if any.
* Default: 5

bucket_predictor = [consec_not_needed|everything]
* Specifies which bucket file prediction algorithm to use.
* Do not change this unless you know what you are doing.
* Default: consec_not_needed

# Results storage
# This section contains settings for storing final search results.

max_count = <integer>
* The number of events that can be accessible in any given status bucket
  (when status_buckets = 0).
* The last accessible event in a call that takes a base and count.
* NOTE: This value does not reflect the number of events displayed in
  the UI after the search is evaluated or computed.
* Default: 500000

max_events_per_bucket = <integer>
* For searches with "status_buckets>0", this setting limits the number of
  events retrieved for each timeline bucket.
* Default: 1000 in code.

status_buckets = <integer>
* The approximate maximum number buckets to generate and maintain in the
  timeline.
* Default: 0, which means do not generate timeline information

truncate_report = [1|0]
* Specifies whether or not to apply the "max_count" setting to report output.
* Default: 0 (false)

write_multifile_results_out = <boolean>
* At the end of the search, if results are in multiple files, write out the
  multiple files to the results_dir directory, under the search results
directory.
* This setting speeds up post-processing search, since the results will
  already be split into appropriate size files.
* Default: true

# Search process
# This section contains settings for search process configurations.

idle_process_cache_search_count = <integer>
* The number of searches that the search process must reach, before
  purging older data from the cache. The purge is performed even if the
  "idle_process_cache_timeout" has not been reached.
* When a search process is allowed to run more than one search, the
search
   process can cache some data between searches.
* When set to a negative value: No purge occurs, no matter how many
   searches are run.
* Has no effect on Windows if "search_process_mode" is not "auto"
   or if "max_searches_per_process" is set to 0 or 1.
* Default: 8

idle_process_cache_timeout = <number>
* The amount of time, in seconds, that a search process must be idle
   before
   the system purges some older data from these caches.
* When a search process is allowed to run more than one search, the
   search
   process can cache some data between searches.
* When set to a negative value: No purge occurs, no matter on how long
   the
   search process is idle.
* When set to "0": Purging always occurs, regardless of whether the
   process
   has been idle or not.
* Has no effect on Windows if "search_process_mode" is not "auto" or
   if "max_searches_per_process" is set to 0 or 1.
* Default: 0.5 (seconds)

idle_process_regex_cache_hiwater = <integer>
* A threshold for the number of entries in the regex cache. If the regex
   cache
   grows to larger than this number of entries, the systems attempts to
   purge some of the older entries.
* When a search process is allowed to run more than one search, the
   search
   process can cache compiled regex artifacts.
* Normally the "idle_process_cache_search_count" and the
   "idle_process_cache_timeout" settings will keep the regex cache a
   reasonable size. This setting is to prevent the cache from growing
   extremely large during a single large search.
* When set to a negative value: No purge occurs, not matter how large
   the cache.
* Has no effect on Windows if "search_process_mode" is not "auto" or
   if "max_searches_per_process" is set to 0 or 1.
* Default: 2500

idle_process_reaper_period = <number>
* The amount of time, in seconds, between checks to determine if there
   are
   too many idle search processes.
* When a search process is allowed to run more than one search, the
   system
   checks if there are too many idle search processes.
* Has no effect on Windows if "search_process_mode" is not "auto" or
   if "max_searches_per_process" is set to 0 or 1.
launcher_max_idle_checks = <integer>
* Specifies the number of idle processes that are inspected before
giving up
    and starting a new search process.
* When allowing more than one search to run for each process, the system
    attempts to find an appropriate idle process to use.
* When set to a negative value: Every eligible idle process is
    inspected.
* Has no effect on Windows if "search_process_mode" is not "auto" or
    if "max_searches_per_process" is set to 0 or 1.
* Default: 5

launcher_threads = <integer>
* The number of server thread to run to manage the search processes.
* Valid only when more than one search is allowed to run for each
    process.
* Has no effect on Windows if "search_process_mode" is not "auto" or
    if "max_searches_per_process" is set to 0 or 1.
* Default: -1 (a value is selected automatically)

max_old_bundle_idle_time = <number>
* The amount of time, in seconds, that a process bundle must be idle
    before
    the process bundle is considered for reaping.
* Used when reaping idle search processes and the process is not
    configured
    with the most recent configuration bundle.
* When set to a negative value: The idle processes are not reaped sooner
    than normal if the processes are using an older configuration bundle.
* Has no effect on Windows if "search_process_mode" is not "auto" or
    if "max_searches_per_process" is set to 0 or 1.
* Default: 5

max_searches_per_process = <integer>
* On UNIX, specifies the maximum number of searches that each search
    process
    can run before exiting.
* After a search completes, the search process can wait for another
    search to
    start and the search process can be reused.
* When set to "0" or "1": The process is never reused.
* When set to a negative value: There is no limit to the number of
    searches
    that a process can run.
* Has no effect on Windows if search_process_mode is not "auto".
* Default: 500

max_time_per_process = <number>
* Specifies the maximum time, in seconds, that a process can spend
    running
searches.
* When a search process is allowed to run more than one search, limits how much time a process can accumulate running searches before the process must exit.
* When set to a negative value: There is no limit on the amount of time a search process can spend running.
* Has no effect on Windows if "search_process_mode" is not "auto" or if "max_searches_per_process" is set to 0 or 1.
* NOTE: A search can run longer than the value set for "max_time_per_process" without being terminated. This setting ONLY prevents the process from being used to run additional searches after the maximum time is reached.
* Default: 300 (5 minutes)

process_max_age = <number>
* Specifies the maximum age, in seconds, for a search process.
* When a search process is allowed to run more than one search, a process is not reused if the process is older than the value specified.
* When set to a negative value: There is no limit on the the age of the search process.
* This setting includes the time that the process spends idle, which is different than "max_time_per_process" setting.
* Has no effect on Windows if "search_process_mode" is not "auto" or if "max_searches_per_process" is set to 0 or 1.
* NOTE: A search can run longer than the the time set for "process_max_age" without being terminated. This setting ONLY prevents that process from being used to run more searches after the search completes.
* Default: 7200 (120 minutes or 2 hours)

process_min_age_before_user_change = <number>
* The minimum age, in seconds, of an idle process before using a process from a different user.
* When a search process is allowed to run more than one search, the system tries to reuse an idle process that last ran a search by the same Splunk user.
* If no such idle process exists, the system tries to use an idle process from a different user. The idle process from a different user must be idle for at least the value specified for the "process_min_age_before_user_change" setting.
* When set to "0": Any idle process by any Splunk user can be reused.
* When set to a negative value: Only a search process by same Splunk user can be reused.
* Has no effect on Windows if "search_process_mode" is not "auto" or
if "max_searches_per_process" is set to 0 or 1.
* Default: 4

search_process_mode = [auto|traditional|debug <debugging-command><debugging-args>]
* Controls how search processes are started.
* When set to "traditional": Each search process is initialized completely
  from scratch.
* When set to "debug": When set to a string beginning with "debug",
  searches are routed through the <debugging-command>, where the user can
  "plug in" debugging tools.
* The <debugging-command> must reside in one of the following
  locations:
  * $SPLUNK_HOME/etc/system/bin/
  * $SPLUNK_HOME/etc/apps/$YOUR_APP/bin/
  * $SPLUNK_HOME/bin/scripts/
* The <debugging-args> are passed, followed by the search command it
  would normally run, to <debugging-command>
* For example, given the following setting:
  search_process_mode = debug
$SPLUNK_HOME/bin/scripts/search-debugger.sh 5
A command similar to the following is run:
$SPLUNK_HOME/bin/scripts/search-debugger.sh 5 splunkd search \
  --id=... --maxbuckets=... --ttl=... [...]
* Default: auto

############################################################################
# Search reuse
############################################################################
# This section contains settings for search reuse.

allow_reuse = <boolean>
* Specifies whether to allow normally executed historical searches to be
  implicitly re-used for newer requests if the newer request allows it.
* Default: true

reuse_map_maxsize = <integer>
* Maximum number of jobs to store in the reuse map.
* Default: 1000

############################################################################
# Splunk Analytics for Hadoop
############################################################################
# This section contains settings for use with Splunk Analytics for
# Hadoop.

reduce_duty_cycle = <number>
* The maximum time to spend performing the reduce, as a fraction of
  total search time.
reduce_freq = <integer>
* When the specified number of chunks is reached, attempt to reduce
  the intermediate results.
* When set to "0": Specifies that there is never an attempt to reduce
  the intermediate result.
* Default: 10

remote_reduce_limit = <unsigned long>
* The number of results processed by a streaming search before a reduce
  is forced.
* NOTE: this option applies only if the search is run with
  --runReduce=true
  (currently only Splunk Analytics for Hadoop does this)
* When set to "0": Specifies that there is no limit.
* Default: 1000000

unified_search = <boolean>
* Specifies if unified search is turned on for hunk archiving.
* Default: false

status_cache_size = <integer>
* The number of status data for search jobs that splunkd can cache in
  RAM.
  This cache improves performance of the jobs endpoint.
* Default: 10000

status_period_ms = <integer>
* The minimum amount of time, in milliseconds, between successive
  status/info.csv file updates.
* This setting ensures that search does not spend significant time just
  updating these files.
* This is typically important for very large number of search peers.
* It could also be important for extremely rapid responses from search
  peers, when the search peers have very little work to do.
* Default: 1000 (1 second)

remote_event_download_finalize_pool = <integer>
* Size of the pool, in threads, responsible for writing out the full
remote events.
* Default: 5

remote_event_download_initialize_pool = <integer>
* Size of the pool, in threads, responsible for initiating the remote event fetch.
* Default: 5

remote_event_download_local_pool = <integer>
* Size of the pool, in threads, responsible for reading full local events.
* Default: 5

remote_timeline = [0|1]
* Specifies if the timeline can be computed remotely to enable better map/reduce scalability.
* Default: 1 (true)

remote_timeline_connection_timeout = <integer>
* Connection timeout, in seconds, for fetching events processed by remote peer timeliner.
* Default: 5.

remote_timeline_fetchall = [0|1]
* When set to "1" (true): Splunk fetches all events accessible through the timeline from the remote peers before the job is considered done.
* Fetching of all events might delay the finalization of some searches, typically those running in verbose mode from the main Search view in Splunk Web.
* This potential performance impact can be mitigated by lowering the "max_events_per_bucket" settings.
* When set to "0" (false): The search peers might not ship all matching events to the search head, particularly if there is a very large number of them.
* Skipping the complete fetching of events back to the search head will result in prompt search finalization.
* Some events may not be available to browse in the UI.
* This setting does NOT affect the accuracy of search results computed by reporting searches.
* Default: 1 (true)

remote_timeline_max_count = <integer>
* Maximum number of events to be stored per timeline bucket on each search peer.
* Default: 10000
remote_timeline_max_size_mb = <integer>
* Maximum size of disk, in MB, that remote timeline events should take
  on each peer.
* If the limit is reached, a DEBUG message is emitted and should be
  visible in the job inspector or in messages.
* Default: 100

remote_timeline_min_peers = <integer>
* Minimum number of search peers for enabling remote computation of
  timelines.
* Default: 1

remote_timeline_parallel_fetch = <boolean>
* Specifies whether to connect to multiple peers at the same time when
  fetching remote events.
* Default: true

remote_timeline_prefetch = <integer>
* Specifies the maximum number of full eventuate that each peer should
  proactively send at the beginning.
* Default: 100

remote_timeline_receive_timeout = <integer>
* Receive timeout, in seconds, for fetching events processed by remote
  peer
timeliner.
* Default: 10

remote_timeline_send_timeout = <integer>
* Send timeout, in seconds, for fetching events processed by remote peer
timeliner.
* Default: 10

remote_timeline_thread = [0|1]
* Specifies whether to use a separate thread to read the full events
  from
  remote peers if "remote_timeline" is used and
"remote_timeline_fetchall"
is set to "true".
  Has no effect if "remote_timeline" or "remote_timeline_fetchall" is
set to
"false".
* Default: 1 (true)

remote_timeline_touchperiod = <number>
* How often, in seconds, while a search is running to touch remote
timeline
artifacts to keep the artifacts from being deleted by the remote peer.
* When set to "0": The remote timelines are never touched.
* Fractional seconds are allowed.
* Default: 300 (5 minutes)
**timeline_events_preview = <boolean>**

* When set to "true": Display events in the Search app as the events are scanned, including events that are in-memory and not yet committed, instead of waiting until all of the events are scanned to see the search results.
  
  You will not be able to expand the event information in the event viewer until events are committed.
* When set to "false": Events are displayed only after the events are committed (the events are written to the disk).
* This setting might increase disk usage to temporarily save uncommitted events while the search is running. Additionally, search performance might be impacted.
  
  * Default: false

**timeline_freq = <timespan> or <ratio>**

* The minimum amount of time, in seconds, between timeline commits.
* If specified as a number < 1 (and > 0), minimum time between commits is computed as a ratio of the amount of time that the search has been running.
  
  * Default: 0

---

**TTL**

---

# This section contains time to live (ttl) settings.

**cache_ttl = <integer>**

* The length of time, in seconds, to persist search cache entries.
  
  * Default: 300 (5 minutes)

**default_save_ttl = <integer>**

* How long, in seconds, the ttl for a search artifact should be extended in response to the save control action.
* When set to 0, the system waits indefinitely.
  
  * Default: 604800 (1 week)

**failed_job_ttl = <integer>**

* How long, in seconds, the search artifacts should be stored on disk after a job has failed. The ttl is computed relative to the modtime of the status.csv file of the job, if the file exists, or the modtime of the artifact directory for the search job.
* If a job is being actively viewed in the Splunk UI then the modtime of...
the status.csv file is constantly updated such that the reaper does not remove the job from underneath.
* Default: 86400 (24 hours)

remote_ttl = <integer>
* How long, in seconds, the search artifacts from searches run in behalf of a search head should be stored on the indexer after completion.
* Default: 600 (10 minutes)

ttl = <integer>
* How long, in seconds, the search artifacts should be stored on disk after the job completes. The ttl is computed relative to the modtime of the status.csv file of the job, if the file exists, or the modtime of the artifact directory for the search job.
* If a job is being actively viewed in the Splunk UI then the modtime of the status.csv file is constantly updated such that the reaper does not remove the job from underneath.
* Default: 600 (10 minutes)

check_search_marker_done_interval = <integer>
* The amount of time, in seconds, that elapses between checks of search marker files, such as hot bucket markers and backfill complete markers.
* This setting is used to identify when the remote search process on the indexer completes processing all hot bucket and backfill portions of the search.
* Default: 60

check_search_marker_sleep_interval = <integer>
* The amount of time, in seconds, that the process will sleep between subsequent search marker file checks.
* This setting is used to put the process into sleep mode periodically on the indexer, then wake up and check whether hot buckets and backfill portions of the search are complete.
* Default: 1

srtemp_dir_ttl = <integer>
* The time to live, in seconds, for the temporary files and directories within the intermediate search results directory tree.
* These files and directories are located in $SPLUNK_HOME/var/run/splunk/srtemp.
* Every 'srtemp_dir_ttl' seconds, the reaper removes files and directories within this tree to reclaim disk space.
* The reaper measures the time to live through the newest file modification time
within the directory.
* When set to 0, the reaper does not remove any files or directories in this
tree.
* Default: 86400 (24 hours)

# Unsupported settings
# This section contains settings that are no longer supported.

```plaintext
enable_status_cache = <boolean>
```
* This is not a user tunable setting. Do not use this setting without
  working in tandem with Splunk personnel. This setting is not tested at
  non-default.
* This controls whether the status cache is used, which caches
  information
  about search jobs (and job artifacts) in memory in main splunkd.
* Normally this caching is enabled and assists performance. However,
  when
  using Search Head Pooling, artifacts in the shared storage location
  will be
  changed by other search heads, so this caching is disabled.
* Explicit requests to jobs endpoints, eg /services/search/jobs/<sid>
  are
  always satisfied from disk, regardless of this setting.
* Default (when search head pooling is not enabled): true
* Default (when search head pooling is enabled): false

```plaintext
status_cache_in_memory_ttl = <positive integer>
```
* This is not a user tunable setting. Do not use this setting without
  working
  in tandem with Splunk personnel. This setting is not tested at
  non-default.
* This setting has no effect unless search head pooling is enabled, AND
  enable_status_cache has been set to true.
* If set, controls the number of milliseconds which a status cache entry
  may be
  used before it expires.
* Default: 60000 (60 seconds)

# Unused settings
# This section contains settings that have been deprecated. These
# settings
# remain listed in this file for backwards compatibility.

```plaintext
max_bucket_bytes = <integer>
```
* This setting has been deprecated and has no effect.
rr_min_sleep_ms = <integer>
* REMOVED. This setting is no longer used.

rr_max_sleep_ms = <integer>
* REMOVED. This setting is no longer used.

rr_sleep_factor = <integer>
* REMOVED. This setting is no longer used.

OTHER COMMAND SETTINGS

# This section contains the stanzas for the SPL commands, except for the
# search command, which is in separate section.

[anomalousvalue]

maxresultrows = <integer>
* Configures the maximum number of events that can be present in memory
at one
time.
* Default: The value set for 'maxresultrows' in the [searchresults]
stanza,
  which is 50000 by default.

maxvalues = <integer>
* Maximum number of distinct values for a field.
  * Default: 100000

maxvaluesize = <integer>
* Maximum size, in bytes, of any single value (truncated to this size if
larger).
  * Default: 1000

[associate]

maxfields = <integer>
* Maximum number of fields to analyze.
  * Default: 10000

maxvalues = <integer>
* Maximum number of values for any field to keep track of.
  * Default: 10000

maxvaluesize = <integer>
* Maximum length of a single value to consider.
* Default: 1000

[autoregress]

maxp = <integer>
* Maximum number of events for auto regression.
* Default: 10000

maxrange = <integer>
* Maximum magnitude of range for p values when given a range.
* Default: 1000

[concurrency]

batch_search_max_pipeline = <integer>
* Controls the number of search pipelines launched at the indexer during batch search.
* Increasing the number of search pipelines should help improve search performance but there will be an increase in thread and memory usage.
* This value applies only to searches that run on remote indexers.
* Default: 1

max_count = <integer>
* Maximum number of detected concurrencies.
* Default: 10000000

[correlate]

maxfields = <integer>
* Maximum number of fields to correlate.
* Default: 1000

[ctable]

* This stanza controls settings for the contingency command.
* Aliases for the contingency command are: ctable and counttable.

maxvalues = <integer>
* Maximum number of columns/rows to generate (the maximum number of distinct values for the row field and column field).
* Default: 1000
[discretize]

* This stanza contains the settings for the bin command.
* Aliases for the bin command are: bucket and discretize.

default_time_bins = <integer>
* When discretizing time for timechart or explicitly via bin, the
default bins
to use if no span or bins is specified.
* Default: 100

maxbins = <integer>
* Maximum number of bins to discretize into.
* If 'maxbins' is not specified or = 0, 'maxbins' uses the value set for
'maxresultrows' in the [searchresults] stanza, which is 50000 by
default.
* Default: 50000

[findkeywords]

maxevents = <integer>
* Maximum number of events used by the findkeywords command and the
Patterns tab.
* Default: 50000

[geomfilter]

enable_clipping = <boolean>
* Whether or not polygons are clipped to the viewport provided by the
render client.
* Default: true

enable_generalization = <boolean>
* Whether or not generalization is applied to polygon boundaries to
reduce
point count for rendering.
* Default: true

[geostats]

filterstrategy = <integer>
* Controls the selection strategy on the geoviz map.
* Valid values are 1 and 2.

maxzoomlevel = <integer>
* Controls the number of zoom levels that geostats will cluster events on.

\[
zl_0\text{gridcell_latspan} = \langle\text{decimal}\rangle
\]
* Controls what is the grid spacing in terms of latitude degrees at the lowest zoom level, which is zoom-level 0.
* Grid-spacing at other zoom levels are auto created from this value by reducing by a factor of 2 at each zoom-level.

\[
zl_0\text{gridcell_longspan} = \langle\text{decimal}\rangle
\]
* Controls what is the grid spacing in terms of longitude degrees at the lowest zoom level, which is zoom-level 0
* Grid-spacing at other zoom levels are auto created from this value by reducing by a factor of 2 at each zoom-level.

[inputcsv]

\[
mkdir\_max\_retries = \langle\text{integer}\rangle
\]
* Maximum number of retries for creating a tmp directory (with random name as subdir of SPLUNK\_HOME/var/run/splunk)
* Default: 100

[iplocation]

\[
db\_path = \langle\text{path}\rangle
\]
* The absolute path to the GeoIP database in the MMDB format.
* The "db_path" setting does not support standard Splunk environment variables such as SPLUNK\_HOME.
* Default: The database that is included with the Splunk platform.

[join]

\[
subsearch\_maxout = \langle\text{integer}\rangle
\]
* Maximum result rows in output from subsearch to join against.
* Default: 50000

\[
subsearch\_maxtime = \langle\text{integer}\rangle
\]
* Maximum search time, in seconds, before auto-finalization of subsearch.
* Default: 60

\[
subsearch\_timeout = \langle\text{integer}\rangle
\]
* Maximum time, in seconds, to wait for subsearch to fully finish.
* Default: 120
**[kmeans]**

maxdatapoints = <integer>
* Maximum data points to do kmeans clusterings for.
* Default: 100000000 (100 million)

maxkrange = <integer>
* Maximum number of k values to iterate over when specifying a range.
* Default: 100

maxkvalue = <integer>
* Maximum number of clusters to attempt to solve for.
* Default: 1000

**[lookup]**

batch_index_query = <boolean>
* Should non-memory file lookups (files that are too large) use batched queries
to possibly improve performance?
* Default: true

batch_response_limit = <integer>
* When doing batch requests, the maximum number of matches to retrieve.
* If more than this limit of matches would otherwise be retrieved, the lookup
  falls back to non-batch mode matching.
* Default: 5000000

max_lookup_messages = <positive integer>
* If more than "max_lookup_messages" log entries are generated, additional
  entries will not be logged in info.csv. All entries will still be logged in
  search.log.

max_matches = <integer>
* DEPRECATED: Use this setting in transforms.conf for lookup definitions.

max_memtable_bytes = <integer>
* Maximum size, in bytes, of static lookup file to use an in-memory index for.
* Lookup files with size above max_memtable_bytes will be indexed on disk
* CAUTION: Setting this to a large value results in loading large lookup files in memory. This leads to a bigger process memory footprint.
* Default: 10000000 (10MB)
indexed_csv_ttl = <positive integer>
* Specifies the amount of time, in seconds, that a indexed CSV lookup table can exist without update before it is removed by Splunk software.
* On a period set by 'indexed_csv_keep_alive_timeout', Splunk software checks the CSV lookup table to see if it has been updated. If it has been updated, Splunk software modifies a special token file.
* At the end of the 'indexed_csv_ttl' period Splunk software looks at the token file. If the token file shows that its CSV lookup table has been updated, Splunk software does not delete that CSV lookup table.
* Default: 300

indexed_csv_keep_alive_timeout = <positive integer>
* Sets the period, in seconds, for an activity check that Splunk software performs on indexed CSV lookup tables.
* When Splunk software performs a CSV lookup table check and finds that the table has been updated, it marks this activity on a token file. The token file update prevents the CSV lookup table from being deleted after 'indexed_csv_ttl' seconds of inactivity have passed.
* Default: 30

indexed_csv_inprogress_max_timeout = <positive integer>
* Sets the maximum time, in seconds, for Splunk software to wait for ongoing indexing of a CSV lookup table to finish before failing any search that is awaiting the lookup table.
* Default: 300

max_reverse_matches = <integer>
* maximum reverse lookup matches (for search expansion)
* Default: 50

[metadata]

bucket_localize_max_lookahead = <integer>
* This setting is only relevant when using remote storage.
* Specifies the maximum number of buckets the metadata command localizes for look-ahead purposes, in addition to the required bucket.
* Increasing this value can improve performance, at the cost of additional network/io/disk utilization.
* Valid values are 0-64. Any value larger than 64 will be set to 64.
Other invalid values will be discarded and the default will be substituted.  
* Default: 10

maxcount = <integer>  
* The total number of metadata search results returned by the search head;  
  after the 'maxcount' is reached, any additional metadata results received from  
  the search peers will be ignored (not returned).  
* A larger number incurs additional memory usage on the search head.  
* Default: 100000

maxresultrows = <integer>  
* The maximum number of results in a single chunk fetched by the metadata  
  command  
* A smaller value will require less memory on the search head in setups with  
  large number of peers and many metadata results, though, setting this too  
  small will decrease the search performance.  
* NOTE: Do not change this setting unless instructed to do so by Splunk Support.  
* Default: 10000

[mvexpand]

* This stanza allows for fine tuning of mvexpand search command.  

max_mem_usage_mb = <non-negative integer>  
* Overrides the default value for "max_mem_usage_mb".  
* Limits the amount of RAM, in megabytes (MB), a batch of events or results will  
  use in the memory of a search process.  
* See definition in the [default] stanza for "max_mem_usage_mb"  
  for more details.  
* Default: 500

[mvcombine]

* This stanza allows for fine tuning of mvcombine search command.  

max_mem_usage_mb = <non-negative integer>  
* Overrides the default value for "max_mem_usage_mb"  
* Limits the amount of RAM, in megabytes (MB), a batch of events or results  
  use in the memory of a search process.
* See definition in the [default] stanza for "max_mem_usage_mb"
  for more details.
* Default: 500

**[outputlookup]**

outputlookup_check_permission = <boolean>
* Specifies whether the outputlookup command should verify that users
  have write permissions to CSV lookup table files.
* outputlookup_check_permission is used in conjunction with the
  transforms.conf setting check_permission.
* The system only applies outputlookup_check_permission to .csv lookup
  configurations in transforms.conf that have check_permission=true.
* You can set lookup table file permissions in the .meta file for each
  lookup
  file, or through the Lookup Table Files page in Settings. By default,
  only
  users who have the admin or power role can write to a shared CSV
  lookup
  file.
* Default: false

**[rare]**

maxresultrows = <integer>
* Maximum number of result rows to create.
* If not specified, defaults to the value set for 'maxresultrows' in the
  [searchresults] stanza, which is 50000 by default.
* Default: 50000

maxvalues = <integer>
* Maximum number of distinct field vector values to keep track of.
* Default: 100000

maxvaluesize = <integer>
* Maximum length of a single value to consider.
* Default: 1000

**[set]**

maxresultrows = <integer>
* The maximum number of results the set command will use from each
  result
  set to compute the required set operation.
* Default: 50000
[sort]

maxfiles = <integer>
* Maximum files to open at once. Multiple passes are made if the number of
  result chunks exceeds this threshold.
* Default: 64.

[spath]

extract_all = <boolean>
* Controls whether to respect automatic field extraction when spath is
  invoked manually.
* If set to "true", all fields are extracted regardless of settings.
* If set to "false", only fields used by later search commands are
  extracted.
* Default: true

extraction_cutoff = <integer>
* For 'extract-all' spath extraction mode, this setting applies
  extraction only
  to the first <integer> number of bytes. This setting applies both the
  auto kv
  extraction and the spath command, when explicitly extracting fields.
* Default: 5000

[stats|sistats]

approx_dc_threshold = <integer>
* When using approximate distinct count (i.e. estdc(<field>) in
  stats/chart/timechart), do not use approximated results if the actual
  number
  of distinct values is less than this number
* Default: 1000

dc_digest_bits = <integer>
* The size of the digest used for approximating distinct count.
* The digest is configured to be 2 ^ 'dc_digest_bits' bytes in size.
* Must be >= 8 (128B) and <= 16 (64KB)
* Default: 10 (equivalent to 1KB)

default_partitions = <integer>
* Number of partitions to split incoming data into for
  parallel/multithreaded
  reduce.
* Default: 1

386
list_maxsize = <integer>
* Maximum number of list items to emit when using the list() function
stats/sistats
* Default: 100

maxmem_check_freq = <integer>
* How frequently, in number of rows, to check if the in-memory data
structure size limit is exceeded, as specified by the
'max_mem_usage_mb' setting.
* Default: 50000

maxresultrows = <integer>
* Maximum number of rows allowed in the process memory.
* When the search process exceeds "max_mem_usage_mb" and
"maxresultrows",
  data is sent to the disk.
* If not specified, uses the value set for 'maxresultrows' in the
  [searchresults] stanza, which is 50000 by default.
* Default: 50000

max_stream_window = <integer>
* For the streamstats command, the maximum allow window size.
* Default: 10000

maxvalues = <integer>
* Maximum number of values for any field to keep track of.
* When set to "0": Specifies an unlimited number of values.
* Default: 0

maxvaluesize = <integer>
* Maximum length of a single value to consider.
* When set to "0": Specifies an unlimited number of values.
* Default: 0

max_valuemap_bytes = <integer>
* For the sistats command, the maximum encoded length of the valuemap,
  per result written out.
* If limit is exceeded, extra result rows are written out as needed.
* 0 = no limit per row
* Default: 100000

natural_sort_output = <boolean>
* Whether or not to perform a natural sort on the output of 'stats'
  if the output size is greater than or equal to the 'maxresultrows' setting.
* A natural sort means that numbers are sorted numerically and
  non-numbers
  are sorted lexicographically.
* Default: true

partitions_limit = <integer>
* Maximum number of partitions to split into that can be specified with
the 'partitions' option.
* When exceeded, the number of partitions is reduced to this limit.
* Default: 100

perc_method = nearest-rank|interpolated
* Which method to use for computing percentiles (and medians=50 percentile).
  * nearest-rank picks the number with 0-based rank \( R = \text{floor}\left(\frac{\text{percentile}}{100}\right)\times \text{count} \)
  * interpolated means given \( F = \frac{\text{percentile}}{100}\times (\text{count}-1), \)
    pick ranks \( R1 = \text{floor}(F) \) and \( R2 = \text{ceiling}(F) \).
    Answer = \( (R2 \times (F - R1)) + (R1 \times (1 - (F - R1))) \)
* See wikipedia percentile entries on nearest rank and "alternative methods"
* Default: nearest-rank

perc_digest_type = rdigest|tdigest
* Which digest algorithm to use for computing percentiles (and medians=50 percentile).
  * rdigest picks the rdigest_k, rdigest_maxnodes and perc_method properties.
  * tdigest picks the tdigest_k and tdigest_max_buffer_size properties.
* Default: tdigest

sparkline_maxsize = <integer>
* Maximum number of elements to emit for a sparkline
* Default: The value of the "list_maxsize" setting

sparkline_time_steps = <time-step-string>
* Specify a set of time steps in order of decreasing granularity. Use an integer and one of the following time units to indicate each step.
  * s = seconds
  * m = minutes
  * h = hours
  * d = days
  * month
* A time step from this list is selected based on the <sparkline_maxsize> setting.
* The lowest <sparkline_time_steps> value that does not exceed the maximum number of bins is used.
* Example:
  * If you have the following configurations:
    * <sparkline_time_steps> = 1s,5s,10s,30s,1m,5m,10m,30m,1h,1d,1month
    * <sparkline_maxsize> = 100
  * The timespan for 7 days of data is 604,800 seconds.
  * Span = 604,800/<sparkline_maxsize>.
  * If sparkline_maxsize = 100, then span = (604,800 / 100) = 6,048 sec == 1.68 hours.
  * The "1d" time step is used because it is the lowest value that does
not exceed the maximum number of bins.
* Default: 1s, 5s, 10s, 30s, 1m, 5m, 10m, 30m, 1h, 1d, 1month

NOTE: The following are rdigest and tdigest settings.
rdigest is a data structure used to compute approximate order
statistics (such as median and percentiles) using sublinear space.

rdigest_k = <integer>
* rdigest compression factor
* Lower values mean more compression
* After compression, number of nodes guaranteed to be greater than or
equal to
  11 times k.
* Must be greater than or equal to 2.
* Default: 100

digest_maxnodes = <integer>
* Maximum rdigest nodes before automatic compression is triggered.
* When set to "1": Specifies to automatically configure based on k
  value.
* Default: 1

tdigest_k = <integer>
* tdigest compression factor
* Higher values mean less compression, more mem usage, but better
  accuracy.
* Must be greater than or equal to 1.
* Default: 50

tdigest_max_buffer_size = <integer>
* Maximum number of elements before automatic reallocation of buffer
  storage
  is triggered.
* Smaller values result in less memory usage but is slower.
* Very small values (<100) are not recommended as they will be very
  slow.
* Larger values help performance up to a point after which it actually
  hurts performance.
* Recommended range is around 10tdigest_k to 30tdigest_k.
* Default: 1000

maxresultrows = <integer>
* Maximum number of result rows to create.
* If not specified, uses the value set for 'maxresultrows' in the
  [searchresults] stanza, which is 50000 by default.
maxvalues = <integer>
* Maximum number of distinct field vector values to keep track of.
* Default: 100000

maxvaluesize = <integer>
* Maximum length of a single value to consider.
* Default: 1000

[transactions]

maxopentxn = <integer>
* Specifies the maximum number of not yet closed transactions to keep in the open pool before starting to evict transactions.
* Default: 5000

maxopenevents = <integer>
* Specifies the maximum number of events (which are) part of open transactions before transaction eviction starts happening, using LRU policy.
* Default: 100000

[tscollect]

squashcase = <boolean>
* The default value of the 'squashcase' argument if not specified by the command
* Default: false

keepresults = <boolean>
* The default value of the 'keepresults' argument if not specified by the command
* Default: false

optimize_max_size_mb = <unsigned integer>
* The maximum size in megabytes of files to create with optimize
* Specify 0 for no limit (may create very large tsidx files)
* Default: 1024

[tstats]

allow_old_summaries = <boolean>
* Whether or not the 'tstats' command, when run on an accelerated datamodel, confirms that the datamodel search in each bucket's summary metadata
is considered to be up to date with the current datamodel search.
* Only bucket summaries that are considered "up to date" are used to deliver results.
* This value is the default value of the 'allow_old_summaries' setting, if that argument is not specified in the command.
* When set to "false", 'tstats' always confirms that the datamodel search in each bucket's summary metadata is considered up to date with the current datamodel search.
* When set to "true", 'tstats' delivers results even from bucket summaries that are considered out of date with the current datamodel.
* Default: false

apply_search_filter = <boolean>
* Whether or not 'tstats' applies role-based search filters when users run the command on normal index data.
* If set to "true", 'tstats' applies role-based search filters.
* NOTE: Regardless of this setting value, 'tstats' never applies search filters to data collected with 'tscollect', or with datamodel acceleration.
* Default: true

bucket_localize_max_lookahead = <integer>
* This setting is only relevant when using remote storage.
* Specifies the maximum number of buckets the tstats command localizes for look-ahead purposes, in addition to the required bucket.
* Increasing this value can improve performance, at the cost of additional network/io/disk utilization.
* Valid values are 0-64. Any value larger than 64 will be set to 64. Other invalid values will be discarded and the default will be substituted.
* Default: 10

chunk_size = <unsigned integer>
* ADVANCED: The default value of 'chunk_size' arg if not specified by the command
* This argument controls how many events are retrieved at a time within a single TSIDX file when answering queries
* Consider lowering this value if tstats queries are using too much memory (cannot be set lower than 10000)
* Larger values will tend to cause more memory to be used (per search) and might have performance benefits.
* Smaller values will tend to reduce performance and might reduce memory used (per search).
* Altering this value without careful measurement is not advised.
  * Default: 10000000

**summariesonly = <boolean>**
* Whether or not 'tstats' employs a mixed mode when running against an accelerated datamodel.
  * This value is the default value for the 'summariesonly' setting, if that argument is not specified in the command.
  * In mixed mode, 'tstats' falls back to search if it encounters missing tsidx data.
  * If set to "true", 'tstats' overrides this mixed mode, and only generates results from available tsidx data, which might be incomplete.
  * If set to "false", 'tstats' uses mixed mode, and falls back to search for tsidx data that is missing.
  * Default: false

**warn_on_missing_summaries = <boolean>**
* ADVANCED: Only meant for debugging 'summariesonly=true' searches on accelerated datamodels.
  * When set to "true", search will issue a warning for a tstats 'summariesonly=true' search for the following scenarios:
    a) If there is a non-hot bucket that has no corresponding datamodel acceleration summary whatsoever.
    b) If the bucket's summary does not match with the current datamodel acceleration search.
  * Default: false

**[typeahead]**

**cache_ttl_sec = <integer>**
* How long, in seconds, the typeahead cached results are valid.
  * Default 300

**fetch_multiplier = <integer>**
* A multiplying factor that determines the number of terms to fetch from the index, fetch = fetch_multiplier x count.
  * Default: 50

**max_concurrent_per_user = <integer>**
* The maximum number of concurrent typeahead searches per user. Once this maximum is reached only cached typeahead results might be available.
  * Default: 3

**maxcount = <integer>**
* Maximum number of typeahead results to find.
* Default: 1000

min_prefix_length = <integer>
* The minimum length of the string prefix after which to provide typeahead.
* Default: 1

use_cache = [0|1]
* Specifies whether the typeahead cache will be used if use_cache is not specified in the command line or endpoint.
* Default: true or 1

[typer]

maxlen = <integer>
* In eventtyping, pay attention to first <integer> characters of any attribute
  (such as _raw), including individual tokens. Can be overridden by supplying
  the typer operator with the argument maxlen (for example,
  "|typer maxlen=300").
* Default: 10000

[xyseries]

* This stanza allows for fine tuning of xyseries search command.

max_mem_usage_mb = <non-negative integer>
* Overrides the default value for 'max_mem_usage_mb'
* See definition in [default] max_mem_usage_mb for more details

GENERAL SETTINGS

# This section contains the stanzas for a variety of general settings.

[authtokens]

expiration_time = <integer>
* Expiration time, in seconds, of auth tokens.
* Default: 3600 (60 minutes)
[auto_summarizer]

allow_event_summarization = <boolean>
* Whether auto summarization of searches whose remote part returns events rather than results will be allowed. * Default: false

cache_timeout = <integer>
* The minimum amount of time, in seconds, to cache auto summary details and search hash codes. * The cached entry expires randomly between 'cache_timeout' and 2 * "cache_timeout" seconds. * Default: 600 (10 minutes)

detailed_dashboard = <boolean>
* Turn on/off the display of both normalized and regular summaries in the Report Acceleration summary dashboard and details. * Default: false

maintenance_period = <integer>
* The period of time, in seconds, that the auto summarization maintenance happens * Default: 1800 (30 minutes)

max_run_stats = <integer>
* Maximum number of summarization run statistics to keep track and expose via REST. * Default: 48

max_verify_buckets = <integer>
* When verifying buckets, stop after verifying this many buckets if no failures have been found * 0 means never * Default: 100

max_verify_bucket_time = <integer>
* Maximum time, in seconds, to spend verifying each bucket. * Default: 15

max_verify_ratio = <number>
* Maximum fraction of data in each bucket to verify * Default: 0.1 (10%)
* Maximum total time in seconds to spend doing verification, regardless if any buckets have failed or not
  * When set to "0": Specifies no limit.
  * Default: 0

normalized_summaries = <boolean>
* Turn on/off normalization of report acceleration summaries.
* Default: true

return_actions_with_normalized_ids = [yes|no|fromcontext]
* Report acceleration summaries are stored under a signature/hash which can be regular or normalized.
  * Normalization improves the re-use of pre-built summaries but is not supported before 5.0. This config will determine the default value of how normalization works (regular/normalized)
  * When set to "fromcontext": Specifies that the end points and summaries would be operating based on context.
* Normalization strategy can also be changed via admin/summarization REST calls with the "use_normalization" parameter which can take the values "yes"/"no"/"fromcontext"
* Default: fromcontext

search_2_hash_cache_timeout = <integer>
* The amount of time, in seconds, to cache search hash codes
* Default: The value of the "cache_timeout" setting

shc_accurate_access_counts = <boolean>
* Only relevant if you are using search head clustering
* Turn on/off to make acceleration summary access counts accurate on the captain.
* by centralizing

verify_delete = <boolean>
* Should summaries that fail verification be automatically deleted?
* Default: false

[export]

add_offset = <boolean>
* Add an offset/row number to JSON streaming output
* Default: true

add_timestamp = <boolean>
* Add a epoch time timestamp to JSON streaming output that reflects the time
the results were generated/retrieved
* Default: false

[extern]

perf_warn_limit = <integer>
* Warn when external scripted command is applied to more than this many events
* When set to "0": Specifies for no message (message is always INFO level)
* Default: 10000

[http_input]

max_number_of_tokens = <unsigned integer>
* The maximum number of tokens reported by logging input metrics.
* Default: 10000

max_content_length = <integer>
* The maximum length, in bytes, of HTTP request content that is accepted by the HTTP Event Collector server.
* Default: 838860800 (~ 800 MB)

max_number_of_ack_channel = <integer>
* The maximum number of ACK channels accepted by HTTP Event Collector server.
* Default: 1000000 (~ 1 million)

max_number_of_acked_requests_pending_query = <integer>
* The maximum number of ACKed requests pending query on HTTP Event Collector server.
* Default: 10000000 (~ 10 million)

max_number_of_acked_requests_pending_query_per_ack_channel = <integer>
* The maximum number of ACKed requested pending query per ACK channel on HTTP Event Collector server.
* Default: 1000000 (~ 1 million)

metrics_report_interval = <integer>
* The interval, in seconds, of logging input metrics report.
* Default: 60 (1 minute)

[indexpreview]

max_preview_bytes = <integer>
* Maximum number of bytes to read from each file during preview
* Default: 2000000 (2 MB)

max_results_perchunk = <integer>
* Maximum number of results to emit per call to preview data generator
* Default: 2500

soft_preview_queue_size = <integer>
* Loosely-applied maximum on number of preview data objects held in memory
* Default: 100

[inputproc]

file_tracking_db_threshold_mb = <integer>
* The size, in megabytes, at which point the file tracking database, otherwise known as the "fishbucket" or "btree", rolls over to a new file.
* The rollover process is as follows:
  * After the fishbucket reaches 'file_tracking_db_threshold_mb' megabytes
  in size, a new database file is created.
  * From this point forward, the processor writes new entries to the new database.
  * Initially, the processor attempts to read entries from the new database,
    but upon failure, falls back to the old database.
  * Successful reads from the old database are written to the new database.
* NOTE: During migration, if this setting doesn't exist, the initialization code in splunkd triggers an automatic migration step that reads in the current value for "maxDataSize" under the "_thefishbucket" stanza in indexes.conf and writes this value into etc/system/local/limits.conf.

learned_sourcetypes_limit = <0 or positive integer>
* Limits the number of entries added to the learned app for performance reasons.
* If nonzero, limits two properties of data added to the learned app by the file classifier. (Code specific to monitor:: stanzas that auto-determines sourcetypes from content.)
  * The number of sourcetypes added to the learned app's props.conf file will be limited to approximately this number.
  * The number of file-content fingerprints added to the learned app's sourcetypes.conf file will be limited to approximately this number.
* The tracking for uncompressed and compressed files is done separately, so in some cases this value may be exceeded.
* This limit is not the recommended solution for auto-identifying sourcetypes.
  The usual best practices are to set sourcetypes in input stanzas, or alternatively to apply them based on filename pattern in props.conf [source::<pattern>] stanzas.
  * Default: 1000

max_fd = <integer>
* Maximum number of file descriptors that a ingestion pipeline in Splunk will keep open, to capture any trailing data from files that are written to very slowly.
* Note that this limit will be applied per ingestion pipeline. For more information about multiple ingestion pipelines see parallelIngestionPipelines in the server.conf.spec file.
  * With N parallel ingestion pipelines the maximum number of file descriptors that can be open across all of the ingestion pipelines will be N * max_fd.
  * Default: 100

monitornohandle_max_heap_mb = <integer>
* The maximum amount of memory, in megabytes, used by the MonitorNoHandle modular input in user mode.
  * The memory of this input grows in size when the data being produced by applications writing to monitored files comes in faster than the Splunk instance can accept it.
  * When set to 0, the heap size (memory allocated in the modular input) can grow without limit.
  * If this size is limited, and the limit is encountered, the input drops some data to stay within the limit.
  * This setting is valid only on Windows machines.
  * Default: 0

tailing_proc_speed = <integer>
  * REMOVED. This setting is no longer used.

monitornohandle_max_driver_mem_mb = <integer>
* The maximum amount of NonPaged memory, in megabytes, used by the kernel driver of the MonitorNoHandle modular input.
  * The memory of this input grows in size when the data being produced by applications writing to monitored files comes in faster than the Splunk instance can accept it.
  * When set to 0, the NonPaged memory size (memory allocated in the kernel driver of the modular input) can grow without limit.
* If this size is limited, and the limit is encountered, the input drops some data to stay within the limit.
* This setting is valid only on Windows machines.
* Default: 0

```
monitornohandle_max_driver_records = <integer>
```
* The maximum number of in-memory records that the kernel module for the MonitorNoHandle modular input stores.
* This setting controls memory growth by limiting the amount of memory that the MonitorNoHandle input kernel module uses.
* When 'monitornohandle_max_driver_mem_mb' is set to > 0, this setting is ignored.
* The 'monitornohandle_max_driver_mem_mb' and 'monitornohandle_max_driver_records' settings are mutually exclusive.
* If the limit is encountered, the input drops some data to remain within the limit.
* Default: 500.

```
time_before_close = <integer>
```
* MOVED. This setting is now configured per-input in inputs.conf.
* Specifying this setting in limits.conf is DEPRECATED, but overrides the setting for all inputs, for now.

```
[journal_compression]
```

```
threads = <integer>
```
* Specifies the maximum number of indexer threads which will be work on compressing hot bucket journal data.
* This setting does not typically need to be modified.
* Default: The number of CPU threads of the host machine

```
[kv]
```

```
avg_extractor_time = <integer>
```
* Maximum amount of CPU time, in milliseconds, that the average (over search results) execution time of a key-value pair extractor will be allowed to take before warning. Once the average becomes larger than this amount of time a warning will be issued
* Default: 500 (.5 seconds)

```
limit = <integer>
```
* The maximum number of fields that an automatic key-value field extraction (auto kv) can generate at search time.
* The summary fields 'host', 'index', 'source', 'sourcetype',
indexed_kv_limit = <integer>
* The maximum number of fields that can be extracted at index time from a data source.
* Fields that can be extracted at index time include default fields, custom fields, and structured data header fields.
* The summary fields 'host', 'index', 'source', 'sourcetype', 'eventtype', 'linecount', 'splunk_server', and 'splunk_server_group' do not count against this limit and are always returned.
* Increase this setting if, for example, you have indexed data with a large number of columns and want to ensure that searches display all fields from the data.
* Set this value to 0 if you do not want to limit the number of fields that can be extracted at index time.
* Default: 200

maxchars = <integer>
* Truncate _raw to this size and then do auto KV.
* Default: 10240 characters

maxcols = <integer>
* When non-zero, the point at which kv should stop creating new fields.
* Default: 512

max_extractor_time = <integer>
* Maximum amount of CPU time, in milliseconds, that a key-value pair extractor will be allowed to take before warning. If the extractor exceeds this execution time on any event a warning will be issued.
* Default: 1000 (1 second)

[kvstore]

max_accelerations_per_collection = <unsigned integer>
* The maximum number of accelerations that can be assigned to a single collection
* Valid values range from 0 to 50
* Default: 10

max_documents_per_batch_save = <unsigned integer>
* The maximum number of documents that can be saved in a single batch
* Default: 1000

max_fields_per_acceleration = <unsigned integer>
* The maximum number of fields that can be part of a compound acceleration
  (i.e. an acceleration with multiple keys)
* Valid values range from 0 to 50
* Default: 10

max_queries_per_batch = <unsigned integer>
* The maximum number of queries that can be run in a single batch
* Default: 1000

max_rows_in_memory_per_dump = <unsigned integer>
* The maximum number of rows in memory before flushing it to the CSV projection of KVStore collection.
* Default: 200

max_rows_per_query = <unsigned integer>
* The maximum number of rows that will be returned for a single query to a collection.
* If the query returns more rows than the specified value, then returned result set will contain the number of rows specified in this value.
* Default: 50000

max_size_per_batch_result_mb = <unsigned integer>
* The maximum size, in megabytes (MB), of the result set from a set of batched queries
* Default: 100

max_size_per_batch_save_mb = <unsigned integer>
* The maximum size, in megabytes (MB), of a batch save query.
* Default: 50

max_size_per_result_mb = <unsigned integer>
* The maximum size, in megabytes (MB), of the result that will be returned for a single query to a collection.
* Default: 50

max_threads_per_outputlookup = <unsigned integer>
* The maximum number of threads to use during outputlookup commands on KVStore
* If the value is 0 the thread count will be determined by CPU count
* Default: 1
[input_channels]

max_inactive = <integer>
* Internal setting, do not change unless instructed to do so by Splunk Support.

lowater_inactive = <integer>
* Internal setting, do not change unless instructed to do so by Splunk Support.

inactive_eligibility_age_seconds = <integer>
* Internal setting, do not change unless instructed to do so by Splunk Support.

[ldap]

allow_multiple_matching_users = <boolean>
* Whether or not Splunk Enterprise allows login when it finds multiple entries in LDAP with the same value for the 'username' attribute.
* When multiple entries are found, it chooses the first Distinguished Name (DN) lexicographically.
* Setting this to false is more secure as it does not allow any ambiguous login, but users with duplicate entries will be unable to login.
* Default: true

max_users_to_precache = <unsigned integer>
* The maximum number of users that are pre-cached from LDAP after reloading auth.
* Set this to 0 to turn off pre-caching.

[metrics]

interval = <integer>
* Number of seconds between logging splunkd metrics to metrics.log.
* Minimum of 10.
* Default: 30

maxseries = <integer>
* The number of series to include in the per_x_thruput reports in metrics.log.
* Default: 10
[metrics:tcpin_connections]

aggregate_metrics = <boolean>
* For each splunktcp connection from forwarder, splunk logs metrics information
every metrics interval.
* When there are large number of forwarders connected to indexer, the amount of
  information logged can take lot of space in metrics.log. When set to true, it
  will aggregate information across each connection and report only once per
  metrics interval.
* Default: false

suppress_derived_info = <boolean>
* For each forwarder connection, _tcp_Bps, _tcp_KBps, _tcp_avg_thruput, _tcp_Kprocessed is logged in metrics.log.
* This can be derived from kb. When set to true, the above derived info will not be emitted.
* Default: false

[pdf]

max_rows_per_table = <unsigned integer>
* The maximum number of rows that will be rendered for a table within integrated PDF rendering.
* Default: 1000

render_endpoint_timeout = <unsigned integer>
* The number of seconds after which the pdfgen render endpoint will timeout if it has not yet finished rendering the PDF output.
* Default: 3600 (60 minutes)

[realtime]

# Default options for indexer support of real-time searches
# These can all be overridden for a single search via REST API arguments

alerting_period_ms = <integer>
* The time, in milliseconds, to wait between triggering alerts during a realtime search.
* This setting limits the frequency at which alerts are triggered during realtime search.
* A value of 0 means that alerts are triggered for every batch of events
that are read. In dense realtime searches with expensive alerts, this can overwhelm the alerting system.

* Precedence: Searchhead
* Default: 0

**blocking** = <boolean>
* Whether or not the indexer should block if a queue is full.
* Default: false

**default_backfill** = <boolean>
* Whether or not windowed real-time searches should backfill events.
* Default: true

**enforce_time_order** = <boolean>
* Whether or not real-time searches should ensure that events are sorted in ascending time order.
* Splunk Web automatically reverses the order that it displays events for real-time searches. If set to "true", the latest events will be shown first.
* Default: true

**indexfilter** = <boolean>
* Whether or not the indexer should pre-filter events for efficiency.
* Default: 1 (true)

**indexed_realtime_update_interval** = <integer>
* When you run an indexed realtime search, the list of searchable buckets needs to be updated. If the Splunk software is installed on a cluster, the list of allowed primary buckets is refreshed. If not installed on a cluster, the list of buckets, including any new hot buckets are refreshed.
  This setting controls the interval for the refresh. The setting must be less than the "indexed_realtime_disk_sync_delay" setting. If your realtime buckets transition from new to warm in less time than the value specified for the "indexed_realtime_update_interval" setting, data will be skipped by the realtime search in a clustered environment.
* Precedence: Indexers
* Default: 30

**indexed_realtime_cluster_update_interval** = <integer>
* This setting is deprecated. Use the "indexed_realtime_update_interval" setting instead.
* While running an indexed realtime search on a cluster, the list of allowed
primary buckets is updated. This controls the interval at which the list is updated. This value must be less than the 'indexed_realtime_disk_sync_delay' setting. If your buckets transition from Brand New to warm in less than the interval time specified, indexed realtime will lose data in a clustered environment.

* Precedence: Indexers
* Default: 30

indexed_realtime_default_span = <integer>
* An indexed realtime search is made up of many component historical searches that by default will span this many seconds. If a component search is not completed in this many seconds the next historical search will span the extra seconds. To reduce the overhead of running an indexed realtime search you can change this span to delay longer before starting the next component historical search.
* Precedence: Indexers
* Default: 1

indexed_realtime_disk_sync_delay = <integer>
* The number of seconds to wait for disk flushes to finish when using indexed/continuous/pseudo realtime search, so that all data can be seen.
* After indexing there is a non-deterministic period where the files on disk, when opened by other programs, might not reflect the latest flush to disk, particularly when a system is under heavy load.
* Precedence: SearchHead overrides Indexers
* Default: 60

indexed_realtime_maximum_span = <integer>
* While running an indexed realtime search, if the component searches regularly take longer than 'indexed_realtime_default_span' seconds, then indexed realtime search can fall more than 'indexed_realtime_disk_sync_delay' seconds behind realtime.
* Use this setting to set a limit after which search drops data to catch back up to the specified delay from realtime, and only search the default span of seconds.
* Precedence: API overrides SearchHead overrides Indexers
* Default: 0 (unlimited)

indexed_realtime_use_by_default = <boolean>
* Whether or not the indexedRealtime mode should be used by default.
* Precedence: SearchHead
* Default: false
local_connect_timeout = <integer>
* Connection timeout, in seconds, for an indexer's search process when connecting to that indexer's splunkd.
* Default: 5

local_receive_timeout = <integer>
* Receive timeout, in seconds, for an indexer's search process when connecting to that indexer's splunkd.
* Default: 5

local_send_timeout = <integer>
* Send timeout, in seconds, for an indexer's search process when connecting to that indexer's splunkd.
* Default: 5

max_blocking_secs = <integer>
* Maximum time, in seconds, to block if the queue is full (meaningless if blocking = false)
* 0 means no limit
* Default: 60

queue_size = <integer>
* Size of queue for each real-time search (must be >0).
* Default: 10000

[restapi]

maxresultrows = <integer>
* Maximum result rows to be returned by /events or /results getters from REST API.
* Default: 50000

jobscontentmaxcount = <integer>
* Maximum length of a property in the contents dictionary of an entry from /jobs getter from REST API
* Value of 0 disables truncation
* Default: 0

time_format_reject = <regular expression>
* HTTP parameters for time_format and output_time_format which match this regex will be rejected (blacklisted).
* The regex will be satisfied by a substring match anywhere in the parameter.
* Intended as defense-in-depth against XSS style attacks against browser users by crafting specially encoded URLs for them to access splunkd.

406
* If unset, all parameter strings will be accepted.
* To disable this check entirely, set the value to empty.
  * Example of disabling: time_format_reject =
  * Default: [<>!], which means that the less-than '<', greater-than '>',
  and exclamation point '!' are not allowed.

[reversedns]

rdnsMaxDutyCycle = <integer>
* Generate diagnostic WARN in splunkd.log if reverse dns lookups are
taking more than this percent of time
* Range 0-100
* Default: 10

[sample]

maxsamples = <integer>
* Default: 10000

maxtotalsamples = <integer>
* Default: 100000

[scheduler]

action_execution_threads = <integer>
* Number of threads to use to execute alert actions, change this number if your
  alert actions take a long time to execute.
* This number is capped at 10.
* Default: 2

actions_queue_size = <integer>
* The number of alert notifications to queue before the scheduler starts
  blocking, set to 0 for infinite size.
* Default: 100

actions_queue_timeout = <integer>
* The maximum amount of time, in seconds, to block when the action queue
  size is full.
* Default: 30

alerts_expire_period = <integer>
* The amount of time, in seconds, between expired alert removal
* This period controls how frequently the alerts list is scanned, the
only benefit from reducing this is better resolution in the number of
alerts fired
at the savedsearch level.
* Change not recommended.
* Default: 120

alerts_max_count = <integer>
* Maximum number of unexpired alerts information to keep for the alerts
  manager, when this number is reached Splunk will start discarding the
  oldest alerts.
* Default: 50000

alerts_max_history = <integer>[s|m|h|d]
* Maximum time to search in the past for previously triggered alerts.
* splunkd uses this property to populate the Activity -> Triggered
  Alerts page at startup.
* Values greater than the default may cause slowdown.
* Relevant units are: s, sec, second, secs, seconds, m, min, minute, mins,
  minutes, h, hr, hour, hrs, hours, d, day, days.
* Default: 7d

alerts_scoping = host|splunk_server|all
* Determines the scoping to use on the search to populate the triggered alerts
  page. Choosing splunk_server will result in the search query
  using splunk_server=local, host will result in the search query using
  host=<search-head-host-name>, and all will have no scoping added to the
  search query.
* Default: splunk_server

auto_summary_perc = <integer>
* The maximum number of concurrent searches to be allocated for auto
  summarization, as a percentage of the concurrent searches that the
  scheduler can run.
* Auto summary searches include:
  * Searches which generate the data for the Report Acceleration
    feature.
  * Searches which generate the data for Data Model acceleration.
  * NOTE: user scheduled searches take precedence over auto summary
    searches.
* Default: 50

auto_summary_perc.<n> = <integer>
auto_summary_perc.<n>.when = <cron string>
* The same as auto_summary_perc but the value is applied only when the
  cron
string matches the current time. This allows 'auto_summary_perc' to have
different values at different times of day, week, month, etc.
* There may be any number of non-negative <n> that progress from least
  specific
to most specific with increasing <n>.
* The scheduler looks in reverse-<n> order looking for the first match.
* If either these settings aren't provided at all or no "when" matches the
current time, the value falls back to the non-<n> value of
'auto_summary_perc'.

concurrency_message_throttle_time = <integer>[s|m|h|d]
* Amount of time controlling throttling between messages warning about
  scheduler
  concurrency limits.
* Relevant units are: s, sec, second, secs, seconds, m, min, minute,
  mins,
  minutes, h, hr, hour, hrs, hours, d, day, days.
* Default: 10m

introspection_lookback = <duration-specifier>
* The amount of time to "look back" when reporting introspection
  statistics.
* For example: what is the number of dispatched searches in the last 60
  minutes?
* Use [<integer>]<unit> to specify a duration;
  a missing <integer> defaults to 1.
* Relevant units are: m, min, minute, mins, minutes, h, hr, hour, hrs,
  hours,
  d, day, days, w, week, weeks.
* For example: "5m" = 5 minutes, "1h" = 1 hour.
* Default: 1h

max_action_results = <integer>
* The maximum number of results to load when triggering an alert action.
* Default: 50000

max_continuous_scheduled_search_lookback = <duration-specifier>
* The maximum amount of time to run missed continuous scheduled searches
  for
  once Splunk Enterprise comes back up, in the event it was down.
* Use [<integer>]<unit> to specify a duration;
  a missing <integer> defaults to 1.
* Relevant units are: m, min, minute, mins, minutes, h, hr, hour, hrs,
  hours,
  d, day, days, w, week, weeks, mon, month, months.
* For example: "5m" = 5 minutes, "1h" = 1 hour.
* A value of 0 means no lookback.
* Default: 24h

max_lock_files = <integer>
* The number of most recent lock files to keep around.
* This setting only applies in search head pooling.

```
max_lock_file_ttl = <integer>
* Time, in seconds, that must pass before reaping a stale lock file.
* Only applies in search head pooling.
```

```
max_per_result_alerts = <integer>
* Maximum number of alerts to trigger for each saved search instance (or
  real-time results preview for RT alerts)
* Only applies in non-digest mode alerting. Use 0 to disable this limit
* Default: 500
```

```
max_per_result_alerts_time = <integer>
* Maximum amount of time, in seconds, to spend triggering alerts for
  each saved search instance (or real-time results preview for RT alerts)
* Only applies in non-digest mode alerting. Use 0 to disable this limit.
* Default: 300 (5 minutes)
```

```
max_searches_perc = <integer>
* The maximum number of searches the scheduler can run, as a percentage
  of the maximum number of concurrent searches, see [search]
  max_searches_per_cpu for how to set the system wide maximum number of searches.
* Default: 50
```

```
max_searches_perc.<n> = <integer>
max_searches_perc.<n>.when = <cron string>
* The same as max_searches_perc but the value is applied only when the cron
  string matches the current time. This allows 'max_searches_perc' to have
  different values at different times of day, week, month, etc.
* There may be any number of non-negative <n> that progress from least specific
  to most specific with increasing <n>.
* The scheduler looks in reverse-<n> order looking for the first match.
* If either these settings aren't provided at all or no "when" matches the
current time, the value falls back to the non-<n> value of 'max_searches_perc'.
```

```
persistence_period = <integer>
* The period, in seconds, between scheduler state persistence to disk. The
  scheduler currently persists the suppression and fired-unexpired alerts to
  disk.
* This is relevant only in search head pooling mode.
* Default: 30
```
persistance_period = <integer>
* DEPRECATED: Use the 'persistence_period' setting instead.

priority_runtime_factor = <double>
* The amount to scale the priority runtime adjustment by.
* Every search's priority is made higher (worse) by its typical running time.
   Since many searches run in fractions of a second and the priority is integral, adjusting by a raw runtime wouldn't change the result; therefore, it's scaled by this value.
* Default: 10

priority_skipped_factor = <double>
* The amount to scale the skipped adjustment by.
* A potential issue with the priority_runtime_factor is that now longer-running searches may get starved. To balance this out, make a search's priority lower (better) the more times it's been skipped. Eventually, this adjustment will outweigh any worse priority due to a long runtime. This value controls how quickly this happens.
* Default: 1

dispatch_retry_delay = <unsigned integer>
* The amount of time, in seconds, to delay retrying a scheduled search that failed to dispatch (usually due to hitting concurrency limits).
* Maximum value: 30
* Default: 0

saved_searches_disabled = <boolean>
* Whether saved search jobs are disabled by the scheduler.
* Default: false

scheduled_view_timeout = <integer>[s|m|h|d]
* The maximum amount of time that a scheduled view (pdf delivery) would be allowed to render
* Relevant units are: s, sec, second, secs, seconds, m, min, minute, mins, minutes, h, hr, hour, hrs, hours, d, day, days.
* Default: 60m

shc_role_quota_enforcement = <boolean>
* When this attribute is enabled, the search head cluster captain enforces user-role quotas for scheduled searches globally (cluster-wide).
* A given role can have (n *number_of_members) searches running
cluster-wide,
where n is the quota for that role as defined by srchJobsQuota and
rtSrchJobsQuota on the captain and number_of_members include the
capable of running scheduled searches.
* Scheduled searches will therefore not have an enforcement of user role
quota on a per-member basis.
* Role-based disk quota checks (srchDiskQuota in authorize.conf) can be
enforced only on a per-member basis.
These checks are skipped when shc_role_quota_enforcement is enabled.
* Quota information is conveyed from the members to the captain. Network
delays
can cause the quota calculation on the captain to vary from the actual
values
in the members and may cause search limit warnings. This should clear
up as
the information is synced.
* Default: false

shc_syswide_quota_enforcement = <boolean>
* When this is enabled, Maximum number of concurrent searches is
enforced
globally (cluster-wide) by the captain for scheduled searches.
Concurrent searches include both scheduled searches and ad hoc
searches.
* This is (n * number_of_members) where n is the max concurrent searches
per
node (see max_searches_per_cpu for a description of how this is
computed) and
number_of_members include members capable of running scheduled
searches.
* Scheduled searches will therefore not have an enforcement of
instance-wide
concurrent search quota on a per-member basis.
* Note that this does not control the enforcement of the scheduler
quota.
For a search head cluster, that is defined as
(max_searches_perc * number_of_members)
and is always enforced globally on the captain.
* Quota information is conveyed from the members to the captain. Network
delays
can cause the quota calculation on the captain to vary from the actual
values
in the members and may cause search limit warnings. This should clear
up as
the information is synced.
* Default: false

shc_local_quota_check = <boolean>
* DEPRECATED. Local (per-member) quota check is enforced by default.
* To disable per-member quota checking, enable one of the cluster-wide
quota
checks (shc_role_quota_enforcement or shc_syswide_quota_enforcement).
* For example, setting 'shc_role_quota_enforcement=true' turns off
  local role
  quota enforcement for all nodes in the cluster and is enforced
  cluster-wide
  by the captain.

shp_dispatch_to_slave = <boolean>
* By default the scheduler should distribute jobs throughout the pool.
* Default: true

search_history_load_timeout = <duration-specifier>
* The maximum amount of time to defer running continuous scheduled
  searches
  while waiting for the KV Store to come up in order to load historical
  data.
  This is used to prevent gaps in continuous scheduled searches when
  splunkd
  was down.
* Use [<integer>]<unit> to specify a duration; a missing <integer>
  defaults to 1.
* Relevant units are: s, sec, second, secs, seconds, m, min, minute,
  mins,
  minutes.
* For example: "60s" = 60 seconds, "5m" = 5 minutes.
* Default: 2m

search_history_max_runtimes = <unsigned integer>
* The number of runtimes kept for each search.
* Used to calculate historical typical runtime during search
  prioritization.
* Default: 10

[search_metrics]

debuge_metrics = <boolean>
* This indicates whether to output more detailed search metrics for
  debugging.
* This will do things like break out where the time was spent by peer,
  and might
  add additional deeper levels of metrics.
* This is NOT related to "metrics.log" but to the "Execution Costs" and
  "Performance" fields in the Search inspector, or the count_map in the
  info.csv file.
* Default: false
[show_source]

distributed = <boolean>
* Whether or not a distributed search is performed to get events from all
  servers and indexes.
* Turning this off results in better performance for show source, but events
  will only come from the initial server and index.
* NOTE: event signing and verification is not supported in distributed mode
* Default: true

distributed_search_limit = <unsigned integer>
* The maximum number of events that are requested when performing a search
  for distributed show source.
* As this is used for a larger search than the initial non-distributed show
  source, it is larger than max_count
* Splunk software rarely returns anywhere near this number of results, as excess results are pruned.
* The point is to ensure the distributed search captures the target event in an
  environment with many events.
* Default: 30000

max_count = <integer>
* Maximum number of events accessible by show_source.
* The show source command will fail when more than this many events are in the
  same second as the requested event.
* Default: 10000

max_timeafter = <timespan>
* Maximum time after requested event to show.
* Default: '1day' (86400 seconds)

max_timebefore = <timespan>
* Maximum time before requested event to show.
* Default: '1day' (86400 seconds)

[rex]

match_limit = <integer>
* Limits the amount of resources that are spent by PCRE when running patterns that will not match.
* Use this to set an upper bound on how many times PCRE calls an internal
function, match(). If set too low, PCRE might fail to correctly match
a pattern.
* Default: 100000

depth_limit = <integer>
* Limits the amount of resources that are spent by PCRE
  when running patterns that will not match.
* Use this to limit the depth of nested backtracking in an internal PCRE
  function, match(). If set too low, PCRE might fail to correctly match
  a pattern.
* Default: 1000

[slc]

maxclusters = <integer>
* Maximum number of clusters to create.
* Default: 10000.

[slow_peer_disconnect]

# This stanza contains settings for the heuristic that will detect and
# disconnect slow peers towards the end of a search that has returned a
# large volume of data.

batch_search_activation_fraction = <decimal>
* The fraction of peers that must have completed before disconnection
  begins.
* This is only applicable to batch search because the slow peers will
  not hold back the fast peers.
* Default: 0.9

bound_on_disconnect_threshold_as_fraction_of_mean = <decimal>
* The maximum value of the threshold data rate that is used to determine
  if a peer is slow.
* The actual threshold is computed dynamically at search time but never
  exceeds
  \( (100 \times \text{maximum_threshold_as_fraction_of_mean}) \% \)
  on either side of the mean.
* Default: 0.2

disabled = <boolean>
* Whether or not this feature is enabled.
* Default: true

grace_period_before_disconnect = <decimal>
* How long, in seconds, when multiplied by life_time_of_collector, to
  wait
  while the heuristic claims that a peer is slow, before disconnecting
the peer.
* If the heuristic consistently claims that the peer is slow for at least
  \(<\text{grace\_period\_before\_disconnect}>*\text{life\_time\_of\_collector}\) seconds, then the
  peer is disconnected.
* Default: 0.1

\text{packets\_per\_data\_point} = <\text{unsigned\ integer}>
* Rate statistics will be sampled once every \text{packets\_per\_data\_point}
  packets.
* Default: 500

\text{sensitivity} = <\text{decimal}>
* Sensitivity of the heuristic to newer values. For larger values of
  sensitivity the heuristic will give more weight to newer statistic.
* Default: 0.3

\text{threshold\_connection\_life\_time} = <\text{unsigned\ integer}>
* All peers will be given an initial grace period of at least these many
  seconds before they are considered in the heuristic.
* Default: 60

\text{threshold\_data\_volume} = <\text{unsigned\ integer}>
* The volume of uncompressed data that must have accumulated, in
  kilobytes (KB), from a peer before it is considered in the heuristic.
* Default: 1024

\textbf{[summarize]}

\text{bucket\_refresh\_interval} = <\text{integer}>
* When \text{poll\_buckets\_until\_maxtime} is enabled in a non-clustered
  environment, this is the minimum amount of time (in seconds)
  between bucket refreshes.
* Default: 30

\text{bucket\_refresh\_interval\_cluster} = <\text{integer}>
* When \text{poll\_buckets\_until\_maxtime} is enabled in a clustered
  environment, this is the minimum amount of time (in seconds)
  between bucket refreshes.
* Default: 120

\text{hot\_bucket\_min\_new\_events} = <\text{integer}>
* The minimum number of new events that need to be added to the hot
  bucket (since last summarization) before a new summarization can take place.
To disable hot bucket summarization set this value to a * large positive
  number.
* Default: 100000

indextime_lag = <unsigned integer>
* The amount of lag time, in seconds, to give indexing to ensure that 
it has synced any received events to disk.
* Effectively, the data that has been received in the past 
'indextime_lag' 
seconds is NOT summarized.
* NOTE: Do not change this setting unless instructed to do so by Splunk 
Support.
* Default: 90

max_hot_bucket_summarization_idle_time = <unsigned integer>
* Maximum amount of time, in seconds, a hot bucket can be idle. When the 
time exceeds the maximum, all of the events are summarized even if 
there 
are not enough events (determined by the hot_bucket_min_new_events 
attribute).
* Default: 900 (15 minutes)

max_replicated_hot_bucket_idle_time = <unsigned integer>
* The maximum amount of time, in seconds, that a replicated hot bucket 
can remain idle before 'indextime_lag' is no longer applied to it.
* This applies only to idle replicated hot buckets. When new events 
arrive, 
the default behavior of applying 'indextime_lag' resumes.
* Default: 150

max_summary_ratio = <decimal>
* A number in the [0-1] range that indicates the maximum ratio of 
summary data / bucket size at which point the summarization of that 
bucket, for the particular search, will be disabled.
* Set to 0 to disable.
* Default: 0

max_summary_size = <integer>
* Size of summary, in bytes, at which point we'll start applying the 
max_summary_ratio.
* Set to 0 to disable.
* Default: 0

max_time = <integer>
* The maximum amount of time, seconds, that a summary search process is 
allowed to run.
* Set to 0 to disable.
* Default: 0

poll_buckets_until_maxtime = <boolean>
* Only modify this setting when you are directed to do so by Support.
* Use the datamodels.conf setting 
'acceleration.poll_buckets_until_maxtime'
  for individual data models that are sensitive to summarization latency
delays.
* Default: false

sleep_seconds = <integer>
* The amount of time, in seconds, to sleep between polling the summarization complete status.
* Default: 5

stale_lock_seconds = <integer>
* The amount of time, in seconds, to have elapse since the mod time of a .lock file before summarization considers that lock file stale and removes it.
* Default: 600

[system_checks]

insufficient_search_capabilities = enabled | disabled
* Enables/disables automatic daily logging of scheduled searches by users who have insufficient capabilities to run them as configured.
* Such searches are those that:
  + Have schedule_priority set to a value other than "default" but the owner does not have the edit_search_schedule_priority capability.
  + Have schedule_window set to a value other than "auto" but the owner does not have the edit_search_schedule_window capability.
* This check and any resulting logging occur on system startup and every 24 hours thereafter.
* Default: enabled

installed_files_integrity = enabled | log_only | disabled
* Enables/disables automatic verification on every startup that all the files that were installed with the running Splunk version are still the files that should be present.
* Effectively this finds cases where files were removed or changed that should not be removed or changed, whether by accident or intent.
* The source of truth for the files that should be present is the manifest file in the $SPLUNK_HOME directory that comes with the release, so if this file is removed or altered, the check cannot work correctly.
* Reading of all the files provided with the install has some I/O cost, though it is paid out over many seconds and should not be severe.
* When "enabled", detected problems will cause a message to be posted to the bulletin board (system UI status message).
* When "enabled" or "log_only", detected problems will cause details to be
  written out to the splunkd.log file.
* When "disabled", no check will be attempted or reported.
* Default: enabled

orphan_searches = enabled|disabled
* Enables/disables automatic UI message notifications to admins for
  scheduled saved searches with invalid owners.
* Scheduled saved searches with invalid owners are considered
  "orphaned".
  They cannot be run because Splunk cannot determine the roles to use
  for
  the search context.
* Typically, this situation occurs when a user creates scheduled searches
  then departs the organization or company, causing their account to be
  deactivated.
* Currently this check and any resulting notifications occur on system
  startup and every 24 hours thereafter.
* Default: enabled

[thruput]

maxKBps = <integer>
* The maximum speed, in kilobytes per second, that incoming data is
  processed through the thruput processor in the ingestion pipeline.
* To control the CPU load while indexing, use this setting to throttle
  the number of events this indexer processes to the rate (in
  kilobytes per second) that you specify.
* NOTE:
  * There is no guarantee that the thruput processor
    will always process less than the number of kilobytes per
    second that you specify with this setting. The status of
    earlier processing queues in the pipeline can cause
    temporary bursts of network activity that exceed what
    is configured in the setting.
  * The setting does not limit the amount of data that is
    written to the network from the tcpoutput processor, such
    as what happens when a universal forwarder sends data to
    an indexer.
  * The thruput processor applies the 'maxKBps' setting for each
    ingestion pipeline. If you configure multiple ingestion
    pipelines, the processor multiplies the 'maxKBps' value
    by the number of ingestion pipelines that you have
    configured.
  * For more information about multiple ingestion pipelines, see
    the 'parallelIngestionPipelines' setting in the
    server.conf.spec file.
* Default (Splunk Enterprise): 0 (unlimited)
* Default (Splunk Universal Forwarder): 256

**[viewstates]**

enable_reaper = <boolean>
* Controls whether the viewstate reaper runs.
* Default: true

reaper_freq = <integer>
* Controls how often, in seconds, the viewstate reaper runs.
* Default: 86400 (24 hours)

reaper_soft_warn_level = <integer>
* Controls what the reaper considers an acceptable number of viewstates.
* Default: 1000

ttl = <integer>
* Controls the age, in seconds, at which a viewstate is considered eligible for reaping.
* Default: 86400 (24 hours)

**[scheduled_views]**

# Scheduled views are hidden [saved searches / reports] that trigger PDF generation for a dashboard. When a user enables scheduled PDF delivery # in the dashboard UI, scheduled views are created.
#
# The naming pattern for scheduled views is _ScheduledView__<view_name>_,
# where <view_name> is the name of the corresponding dashboard.
#
# The scheduled views reaper, if enabled, runs periodically to look for scheduled views that have been orphaned. A scheduled view becomes orphaned when its corresponding dashboard has been deleted. The scheduled views reaper deletes these orphaned scheduled views. The reaper only deletes scheduled views if the scheduled views have not been disabled and their permissions have not been modified.

enable_reaper = <boolean>
* Controls whether the scheduled views reaper runs, as well as whether scheduled views are deleted when the dashboard they reference is
deleted.
* Default: true

reaper_freq = <integer>
* Controls how often, in seconds, the scheduled views reaper runs.
* Default: 86400 (24 hours)

**OPTIMIZATION**

# This section contains global and specific optimization settings

[search_optimization]

enabled = <boolean>
* Enables search optimizations
* Default: true

[search_optimization::search_expansion]

enabled = <boolean>
* Enables optimizer-based search expansion.
* This enables the optimizer to work on pre-expanded searches.
* Default: true

# NOTE: Do not edit the below configurations unless directed by support

[search_optimization::replace_append_with_union]

enabled = <boolean>
* Enables replace append with union command optimization
* Default: true

[search_optimization::merge_union]

enabled = <boolean>
* Merge consecutive unions
* Default: true
**[search_optimization::predicate_merge]**

enabled = <boolean>
* Enables predicate merge optimization
  * Default: true

inputlookup_merge = <boolean>
* Enables predicate merge optimization to merge predicates into inputlookup
  * predicate_merge must be enabled for this optimization to be performed
  * Default: true

merge_to_base_search = <boolean>
* Enable the predicate merge optimization to merge the predicates into the first search in the pipeline.
  * Default: true

fields_black_list = <fields_list>
* A comma-separated list of fields that will not be merged into the first search in the pipeline.
  * If a field contains sub-tokens as values, then the field should be added to fields_black_list
  * Default: no default

**[search_optimization::predicate_push]**

enabled = <boolean>
* Enables predicate push optimization
  * Default: true

**[search_optimization::predicate_split]**

enabled = <boolean>
* Enables predicate split optimization
  * Default: true

**[search_optimization::projection_elimination]**

enabled = <boolean>
* Enables projection elimination optimization
  * Default: true
cmds_black_list = <Commands List>
* A comma-separated list of commands that are not affected by projection elimination optimization.
* Default: no default

[search_optimization::required_field_values]

enabled = <boolean>
* Enables required field value optimization
* Default: true

fields = <comma-separated-string>
* Provide a comma-separated-list of field names to optimize.
* Currently the only valid field names are eventtype and tag.
* Optimization of event type and tag field values applies to transforming searches. This optimization ensures that only the event types and tags necessary to process a search are loaded by the search processor.
* Only change this setting if you need to troubleshoot an issue.
* Default: eventtype, tag

[search_optimization::search_flip_normalization]

enabled = <boolean>
* Enables predicate flip normalization.
* This type of normalization takes 'where' command statements in which the value is placed before the field name and reverses them so that the field name comes first.
* Predicate flip normalization only works for numeric values and string values where the value is surrounded by quotes.
* Predicate flip normalization also prepares searches to take advantage of predicate merge optimization.
* Disable search_flip_normalization if you determine that it is causing slow search performance.
* Default: true

[search_optimization::reverse_calculated_fields]

enabled = <boolean>
* Enables reversing of calculated fields optimization.
* Default: true

[search_optimization::search_sort_normalization]

enabled = <boolean>
* Enables predicate sort normalization.
* This type of normalization applies lexicographical sorting logic to 'search' command expressions and 'where' command statements, so they are consistently ordered in the same way.
* Disable search_sort_normalization if you determine that it is causing slow search performance.
* Default: true

[search_optimization::eval_merge]

enabled = <boolean>
* Enables a search language optimization that combines two consecutive "eval" statements into one and can potentially improve search performance.
* There should be no side-effects to enabling this setting and need not be changed unless you are troubleshooting an issue with search results.
* Default: true

[search_optimization::replace_table_with_fields]

enabled = <boolean>
* Enables a search language optimization that replaces the table command with the fields command in reporting or stream reporting searches
* There should be no side-effects to enabling this setting and need not be changed unless you are troubleshooting an issue with search results.
* Default: true

[search_optimization::replace_stats_cmds_with_tstats]

enabled = <bool>
* If you are not using summary indexing, enable this setting to improve performance for searches that perform statistical operations only on indexed fields.
* Do not enable this setting if you are dependent on summary indexes. When it is enabled, searches that perform stats operations on summary indexes and which only reference indexed fields will return incorrect results. This occurs because the 'tstats' command does not respect the fields created by summary indexing commands. If you are using summary indexing but still choose
to enable this optimization globally, this optimization can be
disabled on
a per-search basis by appending
'| noop search_optimization.replace_stats_cmds_with_tstats=f' to the
search
string.
* Default: false

[directives]

required_tags = enabled|disabled
* Enables the use of the required tags directive, which allows the
search
processor to load only the required tags from the conf system.
* Disable this setting only to troubleshoot issues with search results.
* Default: true

required_eventtypes = enabled|disabled
* Enables the use of the required eventtypes directive, which allows the
search
processor to load only the required event types from the conf system.
* Disable this setting only to troubleshoot issues with search results.
* Default: true

read_summary = enabled|disabled
* Enables the use of the read summary directive, which allows the search
processor to leverage existing data model acceleration summary data
when it
performs event searches.
* Disable this setting only to troubleshoot issues with search results.
* Default: true

[parallelreduce]

maxReducersPerPhase = <positive integer>
* The maximum number of valid indexers that can be used as intermediate
reducers in the reducing phase of a parallel reduce operation. Only
healthy
search peers are valid indexers.
* If you specify a number greater than 200 or an invalid value, parallel
reduction does not take place. All reduction processing moves to the
search
head.
* Default: 4

maxRunningPrdSearches = <unsigned integer>
* DEPRECATED. Use the 'maxPrdSearchesPerCpu' setting instead.
maxPrdSearchesPerCpu = <unsigned integer>
* The maximum number of parallel reduce searches that can run, per CPU core,
on an indexer that has been configured as an intermediate reducer.
* If you specify 0, there is no limit. The indexer runs as many parallel reduce searches as the indexer hardware permits.
* Default: 1

reducers = <string>
* Use this setting to configure one or more valid indexers as dedicated intermediate reducers for parallel reduce search operations. Only healthy search peers are valid indexers.
* For <string>, specify the indexer host and port using the following format -
  host:port. Separate each host:port pair with a comma to specify a list of intermediate reducers.
* If the 'reducers' list includes one or more valid indexers, all of those indexers (and only these indexers) are used as intermediate reducers when you run a parallel reduce search. If the number of valid indexers in the 'reducers' list exceeds 'maxReducersPerPhase', the Splunk software randomly selects the set of indexers that are used as intermediate reducers.
* If all of the indexers in the 'reducers' list are invalid, the search runs without parallel reduction. All reduce operations for the search are processed on the search head.
* If 'reducers' is empty or not configured, all valid indexers are potential intermediate reducer candidates. The Splunk software randomly selects valid indexers as intermediate reducers with limits determined by the 'winningRate' and 'maxReducersPerPhase' settings.
* Default: ""

winningRate = <positive integer>
* The percentage of valid indexers that can be selected from the search peers as intermediate reducers for a parallel reduce search operation.
* This setting is only respected when the 'reducers' setting is empty or not configured.
* If 100 is specified, the search head attempts to use all of the indexers.
* If 1 is specified, the search head attempts to use 1% of the indexers.
* The minimum number of indexers used as intermediate reducers is 1.
* The maximum number of indexers used as intermediate reducers is the value of
'maxReducersPerPhase'.
* Default: 50

[rollup]

minSpanAllowed = <integer>
* Sets the minimum timespan for the scheduled searches that generate metric
  rollup summaries.
* Each rollup summary uses a scheduled search to provide its metric data point
  aggregations. The interval of the search matches the span defined for the
  rollup summary.
* However, when you run large numbers of scheduled searches with short
  intervals, you can encounter search concurrency problems, where some
  searches
  skip scheduled runs.
* To reduce the risk of search concurrency issues, this setting ensures
  that
  the the rollup summaries created for your have longer spans.
* Do not set below 60 seconds.
* Default: 300

limits.conf.example

#   Version 7.3.0
# CAUTION: Do not alter the settings in limits.conf unless you know what
# you are doing.
# Improperly configured limits may result in splunkd crashes and/or
# memory overuse.

[searchresults]
maxresultrows = 50000
# maximum number of times to try in the atomic write operation (1 = no
retries)
tocsv_maxretry = 5
# retry period is 1/2 second (500 milliseconds)
tocsv_retryperiod_ms = 500

[subsearch]
# maximum number of results to return from a subsearch
maxout = 100
# maximum number of seconds to run a subsearch before finalizing
maxtime = 10
# time to cache a given subsearch's results
ttl = 300

[anomalousvalue]
maxresultrows = 50000
# maximum number of distinct values for a field
maxvalues = 100000
# maximum size in bytes of any single value (truncated to this size if larger)
maxvaluesize = 1000

[associate]
maxfields = 10000
maxvalues = 10000
maxvaluesize = 1000

# for the contingency, ctable, and counttable commands
[ctable]
maxvalues = 1000

[correlate]
maxfields = 1000

# for bin/bucket/discretize
[discretize]
maxbins = 50000
# if maxbins not specified or = 0, defaults to searchresults::maxresultrows

[inputcsv]
# maximum number of retries for creating a tmp directory (with random name in
# SPLUNK_HOME/var/run/splunk)
mkdir_max_retries = 100

[kmeans]
maxdatapoints = 100000000

[kv]
# when non-zero, the point at which kv should stop creating new columns
maxcols = 512

[rare]
maxresultrows = 50000
# maximum distinct value vectors to keep track of
maxvalues = 100000
maxvaluesize = 1000

[restapi]
# maximum result rows to be returned by /events or /results getters from REST
# API
maxresultrows = 50000

[search]
# how long searches should be stored on disk once completed
ttl = 86400

# the approximate maximum number of timeline buckets to maintain
status_buckets = 300

# the last accessible event in a call that takes a base and bounds
max_count = 10000

# the minimum length of a prefix before a * to ask the index about
min_prefix_len = 1

# the length of time to persist search cache entries (in seconds)
cache_ttl = 300

# By default, we will not retry searches in the event of indexer
# failures with indexer clustering enabled.
# Hence, the default value for search_retry here is false.
search_retry = false

# Timeout value for checking search marker files like hotbucketmarker or
# backfill
# marker.
check_search_marker_done_interval = 60

# Time interval of sleeping between subsequent search marker files
# checks.
check_search_marker_sleep_interval = 1

# If number of cpu's in your machine is 14 then total system wide number
# of
# concurrent searches this machine can handle is 20.
# which is base_max_searches + max_searches_per_cpu x num_cpus = 6 + 14
# x 1 = 20
base_max_searches = 6
max_searches_per_cpu = 1

[scheduler]

# Percent of total concurrent searches that will be used by scheduler is
# total concurrency x max_searches_perc = 20 x 60% = 12 scheduled
# searches
# User default value (needed only if different from system/default
# value) when
# no max_searches_perc.<n>.when (if any) below matches.
max_searches_perc = 60

# Increase the value between midnight-5AM.
max_searches_perc.0 = 75
max_searches_perc.0.when = * 0-5 * * *

# More specifically, increase it even more on weekends.
max_searches_perc.1 = 85
max_searches_perc.1.when = * 0-5 * * 0,6

# Maximum number of concurrent searches is enforced cluster-wide by the
# captain for scheduled searches. For a 3 node SHC total concurrent
# searches = 3 x 20 = 60. The total searches (adhoc + scheduled) = 60,
then
# no more scheduled searches can start until some slots are free.
shc_syswide_quota_enforcement = true

[s1c]
# maximum number of clusters to create
maxclusters = 10000

[findkeywords]
#events to use in findkeywords command (and patterns UI)
maxevents = 50000

[stats]
maxresultrows = 50000
maxvalues = 10000
maxvaluesize = 1000

[top]
maxresultrows = 50000
# maximum distinct value vectors to keep track of
maxvalues = 100000
maxvaluesize = 1000

[search_optimization]
enabled = true

[search_optimization::predicate_split]
enabled = true

[search_optimization::predicate_push]
enabled = true

[search_optimization::predicate_merge]
enabled = true
inputlookup_merge = true
merge_to_base_search = true

[search_optimization::projection_elimination]
enabled = true
cmds_black_list = eval, rename

[search_optimization::search_flip_normalization]
enabled = true
The following are the spec and example files for `logging.conf`.

**logging.conf.spec**

# The format and semantics of this file are described in this article at Python.org:
#
# [Configuration file format](https://docs.python.org/2/library/logging.config.html#configuration-file-format)
# This file must contain sections called [loggers], [handlers] and [formatters] which identify by name the entities of each type which are defined in the file. For each such entity, there is a separate section which identifies how that entity is configured.

keys = <a list of available keys separated by comma>
* appears in [loggers], [handlers] or [formatters]
* describes the available [logger_<name>], [handler_<name>] or [formatter_<name>]

level = <DEBUG|INFO|WARNING|ERROR|CRITICAL|NOTSET>
* For the root logger only, NOTSET means that all messages will be logged.

handlers = <comma-separated list>
* A comma-separated list of handler names, which must appear in the [handlers] section.
* These names must appear in the [handlers] section and have corresponding
sections in the configuration file.

**qualname = <string>**  
* The hierarchical channel name of the logger (the name used by the application to get the logger).

**propagate = <0|1>**  
* Set to "1" to indicate that messages must propagate to handlers higher up the logger hierarchy from this logger.  
* Set to "0" to indicate that messages are not propagated to handlers up the hierarchy.

**class = <string>**  
* Indicates the handler's class, as determined by eval() in the logging package's namespace.

**args = <comma-separated list>**  
* The list of arguments to the constructor for the handler class, when eval()uated in the context of the logging package's namespace.

**formatter = <string>**  
* The key name of the formatter for this handler.  
* If blank, a default formatter (logging._defaultFormatter) is used.  
* If a name is specified, it must appear in the [formatters] section and have a corresponding section in the configuration file.

**format = <logger format pattern>**  
* for pattern format see:  
https://docs.python.org/2/library/logging.config.html#user-defined-objects

logging.conf.example

No example

macros.conf

The following are the spec and example files for macros.conf.

macros.conf.spec

```python
#   Version 7.3.0
#   This file contains possible attribute/value pairs for search language macros.
#
# To learn more about configuration files (including precedence) please
```
**[<STANZA_NAME>]**

* Each stanza represents a search macro that can be referenced in any search.
  * The stanza name is the name of the macro if the macro takes no arguments.
    Otherwise, the stanza name is the macro name appended with 
    "(<numargs>)"
    where <numargs> is the number of arguments that this macro takes.
  * Macros can be overloaded. In other words, they can have the same name but a 
    different number of arguments. If you have [foobaz], [foobaz(1)], 
    [foobaz(2)], etc., they are not the same macro.
  * Macros can be used in the search language by enclosing the macro name and any 
    argument list within tick marks, for example:`foobar(arg1,arg2)` or 
    'footer`.
  * Splunk does not expand macros when they are inside of quoted values, for 
    example: "foo`bar`baz".

**args = <string>,<string>,...**
* A comma-delimited string of argument names.
* Argument names can only contain alphanumeric characters, underscores 
  '_', and hyphens '-'.
* If the stanza name indicates that this macro takes no arguments, this 
  attribute will be ignored.
* This list cannot contain any repeated elements.

**definition = <string>**
* The string that the macro will expand to, with the argument substitutions 
  made. (The exception is when iseval = true, see below.)
* Arguments to be substituted must be wrapped by dollar signs ($), for example: 
  "the last part of this string will be replaced by the value of argument foo $foo$".
* Splunk replaces the $<arg>$ pattern globally in the string, even inside of 
  quotes.

**validation = <string>**
* A validation string that is an 'eval' expression. This expression must
evaluate to a boolean or a string.
* Use this to verify that the macro's argument values are acceptable.
* If the validation expression is boolean, validation succeeds when it returns
  true. If it returns false or is NULL, validation fails, and Splunk returns
  the error message defined by the attribute, errormsg.
* If the validation expression is not boolean, Splunk expects it to return a
  string or NULL. If it returns NULL, validation is considered a success.
  Otherwise, the string returned is the error string.

errmsg = <string>
* The error message to be displayed if validation is a boolean expression and
  it does not evaluate to true.

iseval = <true/false>
* If true, the definition attribute is expected to be an eval expression that
  returns a string that represents the expansion of this macro.
* Defaults to false.

description = <string>
* OPTIONAL. Simple english description of what the macro does.

macros.conf.example

#    Version 7.3.0
#
# Example macros.conf
#

# macro foobar that takes no arguments can be invoked via `foobar`
[foobar]
# the definition of a macro can invoke another macro. nesting can be indefinite
# and cycles will be detected and result in an error
definition = `foobar(foo=defaultfoo)`

# macro foobar that takes one argument, invoked via `foobar(someval)`
[foobar(1)]
args = foo
# note this is definition will include the leading and trailing quotes,
# i.e.
# something `foobar(someval)`
# would expand to
# something "foo = someval"
definition = "foo = $foo$"

# macro that takes two arguments
# note that macro arguments can be named so this particular macro could be
# invoked equivalently as `foobar(1,2)` `foobar(foo=1,bar=2)` or
# `foobar(bar=2,foo=1)`
[foobar(2)]
args = foo, bar
definition = "foo = $foo$, bar = $bar$"

# macro that takes one argument that does validation
[foovalid(1)]
args = foo
definition = "foovalid = $foo$"
# the validation eval function takes any even number of arguments (>=2)
# where
# the first argument is a boolean expression, the 2nd a string, the third
# boolean, 4th a string, etc etc etc
validation = validate(foo>15,"foo must be greater than 15",foo<=100,"foo must be <= 100")

# macro showing simple boolean validation, where if foo > bar is not true,
# errmsg is displayed
[foovalid(2)]
args = foo, bar
definition = "foo = $foo$ and bar = $bar$"
validation = foo > bar
errmsg = foo must be greater than bar

# example of an eval-based definition. For example in this case
# `fooeval(10,20)` would get replaced by 10 + 20
[fooeval(2)]
args = foo, bar
definition = if (bar > 0, "$foo$ + $bar$", "$foo$ - $bar$")
iseval = true

mad.conf

The following are the spec and example files for mad.conf.

mad.conf.spec

# This file contains possible settings you can use to configure metric anomaly detection.
# Use anomaly detection to identify trends and outliers in KPI search
results that might
# indicate an issue with your system.
#
# There is a mad.conf in
$SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/default. To set custom
# configurations, place a mad.conf in
$SPLUNK_HOME/etc/apps/SA-ITSI-MetricAD/local.
#
# To learn more about configuration files (including precedence), see
the
# documentation located at
#
http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
#
# To learn more about metric anomaly detection, see
#
http://docs.splunk.com/Documentation/ITSI/latest/Configure/Enableanomalydetection
#
# In most situations, the default values specified in mad.conf should
work as-is.
# Modifying this file can result in negative changes to anomaly
detection accuracy.
# Do NOT remove any stanzas or settings in the configuration file.
#
# For <duration> format, this configuration file accepts the following
units:
#   * ms => milliseconds
#   * s, sec, secs, second, seconds => second
#   * m, min, mins, minute, minutes => minute
#   * h, hr, hrs, hour, hours => hour
#   * d, day, days => day
#
[service]

unbounded_buffer_size = <duration>
* The size of the data buffer used in batch mode.
* For example, "4d" stores a maximum of 4 days of data.
* Default: 400d

kvstore_connect_interval = <duration>
* How often to retry connecting to the KV store when the connection is
lost.
* Default: 30s

rest_ssl_permissive_trustmanager = <boolean>
* Whether to enable PermissiveX509TrustManager with HTTPS connection to
Splunk REST API.
* Do not modify this setting unless Splunk is not running in HTTPS mode.
* Default: true
rest_ssl_permissive_hostnameverifier = <boolean>
* Whether hostname verification is strict or permissive.
* If set to "true", hostname verification is permissive.
* If set to "false", hostname verification is strict.
* This setting can be disabled when the Splunk certificate is not self-signed.
* Default: true

trending_bounded_buffer_size = <duration>
* The size of the data buffer for the trending algorithm in real-time mode.
* This setting MUST be larger than the value of the 'training_period' setting in the [trending] stanza.
* Default: 15d

cohesive_bounded_rt_buffer_size = <duration>
* The size of the real-time data buffer for the cohesive algorithm in real-time mode.
* Default: 12h

cohesive_bounded_backfill_buffer_size = <duration>
* The size of the backfill data buffer for the cohesive algorithm in real-time mode.
* Default: 25h

[trending]

* Use this stanza to configure the 'mad' command for the trending algorithm.

periods.days = <positive integer>
* How many days to look back for normal patterns in the data.
* Must be a value greater than zero.
* Default: 6

periods.weeks = <integer>
* How many weeks to look back for normal patterns in the data.
* Must be a value greater than or equal to zero.
* Default: 2

window_size = <positive integer>
* How many data points to use to construct an analysis window.
* Must be a value greater than 1.
* Default: 60

step_size = <positive integer>
* The offset size of two consecutive analysis window.
* Must be a value greater than 0.
* Default: 1
training_period = <duration>
* The amount of time used to train the algorithm.
* Must be a value greater than 1.
* Default: 7d

max_NA_ratio = <float>
* The maximum possible ratio of NaN (undefined) data points.
* Must be a decimal between 0.0 and 1.0.
* Default: 0.5

na_rm = <boolean>
* Whether or not to remove NaN (undefined) data points.
* If set to "true", NaN data points are removed.
* Default: true

Nkeep = <duration>
* How much data to keep in memory for analysis.
* Default: 50h

Naccum = <float>
* The accumulation score for anomaly alerting.
* Must be a value greater than zero.
* Default: 35.0

[trending:limits]

* Use this stanza to configure the 'naccum' command for trending algorithm.

Naccum_max = <float>
* The maximum accumulation score to use for detecting anomalies.
* This value MUST be larger than the 'Naccum' setting in the [trending] stanza.
* Default: 50.0

Naccum_min = <float>
* The minimum accumulation score to use for detecting anomalies.
* This value MUST be smaller than the 'Naccum' in the [trending] stanza.
* Default: 30.0

sensitivity_max = <integer>
* The number of sensitivity levels.
* Must be a value greater than 1.
* Default: 10

[cohesive]

* Use this stanza to configure the 'mad' command for the cohesive
algorithm.

window_size = <positive integer>
* How many data points to use to construct an analysis window.
* Must be a value greater than 1.
* Default: 60

step_size = <positive integer>
* The offset size of two consecutive analysis windows.
* Must be a value greater than 0.
* Default: 1

training_period = <duration>
* The amount of time used to train the algorithm.
* Must be a value greater than 1.
* Default: 7d

max_NA_ratio = <float>
* The maximum possible ratio of NaN (undefined) data points.
* Must be a decimal between 0.0 and 1.0.
* Default: 0.5

na_rm = <boolean>
* Whether or not to remove NaN (undefined) data points.
* If set to "true", NaN data points are removed.
* Default: true

Nkeep = <duration>
* How much data to keep in memory for analysis.
* Default: 10h

Naccum = <float>
* The accumulation score for anomaly alerting.
* Must be a number greater than zero.
* Default: 35.0

norm_Ntrend = <integer>
* The window of moving median for normalization of incoming data.
* Default: 10

norm_maxNAratio = <float>
* The maximum ratio of NaN data points allowed in the dataset for normalization of incoming data.
* Must be a decimal between 0.0 and 1.0.
* Default: 0.5

norm_trendOnly = <boolean>
* Whether to use only the trend of the data for normalization.
* Default: false

norm_MAratio = 0.8
* The moving average ratio of the normalization window.
* Must be a decimal between 0.0 and 1.0.
* Default: 0.8

norm_NArm = <boolean>
* Whether to remove NaN (undefined) data points for normalization.
* Default: false

norm_Nwindow = <integer>
* The size, in data points, of the normalization buffer.
* Default: 10080

norm_Nshift = <integer>
* The interval at which the normalization constants are recalculated.
* After receiving this many data points, the constants are recalculated.
* Default: 1440

norm_Ninit = <integer>
* The number of data points needed to calculate the normalization constants.
* Default: 30

norm_batch = <boolean>
* Deprecated option
* Enable/disable batch normalization

metrics_maximum = <integer>
* The maximum number of metrics that can be analyzed for the cohesive algorithm.
* Default: 30

[cohesive:limits]

* Use this stanza to configure the 'naccum' command for the cohesive algorithm.

Naccum_max = <float>
* The maximum accumulation score that can be used for detecting anomalies.
* This value MUST be larger than the 'Naccum' setting in the [cohesive] stanza.
* Default: 50.0

Naccum_min = <float>
* The minimum accumulation score that can be used for detecting anomalies.
* This value MUST be smaller than the 'Naccum' setting in the [cohesive] stanza.
* Default: 30.0

sensitivity_max = <integer>
* The number of sensitivity levels.
* Must be a value greater than 1.
* Default: 10

[logging]

* Use this stanza to configure logging.

metric_registry = <boolean>
* Enable logging metrics of the 'mad' command.
* CAUTION: Enabling this setting will have a significant performance impact.
* Default: false

[alerting]

* Use this stanza to configure external HTTP endpoint connections for posting alerts.

rest_ssl_permissive_trustmanager = <boolean>
* Whether to enable PermissiveX509TrustManager with HTTPS connection to the Splunk REST API.
* Default: true

rest_ssl_permissive_hostnameverifier = <boolean>
* Whether to be strict or permissive in hostname verification.
* If set to "true", hostname verification is permissive.
* If set to "false", hostname verification is strict.
* Default: true

max_http_connection = 100
* How many simultaneous HTTP connections are allowed.
* Default: 100

mad.conf.example

No example

notable_event_actions.conf

The following are the spec and example files for notable_event_actions.conf.
notable_event_actions.conf.spec

# This file contains attributes and values for taking actions on episodes
# in Episode Review.
#
# There is a notable_event_actions.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/default/.
# To set custom configurations, place a notable_event_actions.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local/. You must restart Splunk to enable
# configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the top
#   of the file.
# * Each conf file should have at most one default stanza. If there are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in the
#   file wins.
# * If an attribute is defined at both the global level and in a
#   specific
#   stanza, the value in the specific stanza takes precedence.

disabled = <boolean>
* Disable a notable event action by setting to 1.
* Optional.
* Default: 0

is_group_compatible = <boolean>
* Make an action available for episodes by setting to 1.
* Default: 1

is_bulk_compatible = <boolean>
* Make an action available for bulk episodes by setting to 1.
* Default: 0
run_bulk_action_iteratively = <boolean>
* If set to "1", bulk episode actions run iteratively rather than simultaneously.
* This value only takes effect if the 'is_bulk_compatible' setting is set to "1".
* For custom ServiceNow add-ons, this setting must be set to "1" in order for bulk episode actions to function properly.
* Default: 0

[<action_name>]

* Each stanza represents an episode action. The action name is the type of action you want to configure.
* Options are email, script, itsi_sample_event_action_ping, itsi_event_action_link_ticket, snow_incident, and remedy_incident.

execute_in_sync = <boolean>
* If 1, ITSI executes the action synchronously.
* The UI notifies you when the action is truly complete, rather than requiring you to check back later to confirm.
* It is recommended that you set this value to 1 for an external ticket created by a Splunk custom search command or modular alert.
* Default: 0

execute_once_per_group = <boolean>
* If 1, ITSI executes the action exactly once in the case of a bulk action.
* In special cases (like if this alert action has 'type' set to "external_ticket"), the result of a refresh is associated with all the events in the group.
* Default: 0

type = <string>
* The type of action to take on the episode.
* Use this setting if you are creating a ServiceNow or Remedy ticket from an episode.
* The only supported value for this setting is "external_ticket", which creates a ticket in the external ticketing system you choose.
* If you set the value to "external_ticket", ITSI runs a refresh action right after execution.
* The attribute-value pairs below are applicable when 'type' is "external_ticket".

ticket_system_name = <string>
* The name of the external ticketing system in which to create the ticket.
relative_refresh_uri = <string>
* A relative URI for the search head where ITSI is installed.
* https://localhost:8089/ or something similar is prepended to the URI.
* ITSI constructs this link so you can navigate directly to the external ticket.
* ITSI issues a GET call on this URI and outputs JSON data.
* 'refresh_response_json_path' indicates the path to walk through the received JSON output.
* Do not change this from the default value or refresh will not work.

correlation_key = <string>
* Optional. The query parameter to be appended to 'relative_refresh_uri'.
* The parameter is also saved in the KV store collection that contains all created tickets.
* Do not change this from the default value or refresh will not work.
* Default: correlation_id

correlation_value = <string>
* The key in the raw notable event whose value to append to the refresh URI.
* If a 'correlation_key' exists, ITSI appends this value to the refresh URI instead.
* Do not change this from the default value or refresh will not work.
* Default: $result.event_id$

correlation_value_for_group = <string>
* The key in the episode whose value to append to the refresh URI.
* By default, ITSI uses the value corresponding to 'itsi_group_id'.
* Do not change this from the default value or refresh will not work.
* Default: $result.itsi_group_id$

refresh_response_json_path = <string>
* Because the JSON output of 'relative_refresh_uri' can be nested and complex, this setting indicates the path to walk through the received output.
* Do not change this from the default value or refresh will not work.
* Default: entry.(0).content

refresh_response_ticket_id_key = <string>
* After traversing the JSON path specified in 'refresh_response_json_path'
  and fetching a JSON blob, the key corresponding to the external ticket ID.
* Do not change this from the default value or refresh will not work.

refresh_response_ticket_url_key = <string>
* After traversing the JSON path specified in 'refresh_response_json_path'
  and fetching a JSON blob, the key corresponding to the external ticket
URL.
* Do not change this from the default value or refresh will not work.

bulk_max = <string>
* The maximum number of episodes that this action can be executed on.
* Default: 25

notable_event_actions.conf.example

# This is an example notable_event_actions.conf. Use this file to configure
# episode actions.
#
# To use one or more of these configurations, copy the configuration block
# into notable_event_actions.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/local.
# You must restart Splunk to enable configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
#
http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
#
# This example alert includes running a script, sending an email, and
# creating an incident in ServiceNow.

[email]
disabled = 0

[script]
disabled = 0

[snow_incident]
disabled = 0
type = external_ticket
extecute_in_sync = 1
extecute_once_per_group = 1
tickt_system_name = ServiceNow
relative_refresh_uri = /servicesNS/nobody/-/service_now_incident/snow_incident
correlation_key = correlation_id
    * Refresh URI now becomes
    /servicesNS/nobody/-/service_now_incident/snow_incident?correlation_id
correlation_value = $result.event_id$
    * Assuming we are dealing with an event whose event_id is 'myevent1234',


the URI now becomes:
/servicesNS/nobody/-/service_now_incident/snow_incident?correlation_id=myevent1234
* Final URI with output_mode:
/servicesNS/nobody/-/service_now_incident/snow_incident?correlation_id=myevent1234&output_mode=json
* If there is no 'correlation_key' specified, the final URI looks like:
/servicesNS/nobody/-/service_now_incident/snow_incident/myevent1234?output_mode=json

correlation_value_for_group = $result.itsi_group_id$
* When operating on an episode, we will use the value corresponding to 'itsi_group_id'
as the correlation_id. Similar to correlation_value mentioned above.

refresh_response_json_path = entry[0].content
* Assuming the JSON response looks like the following:
{
...
"entry": [ 
{
...
"content": { 
   "number": "INC0047495", 
   "url": 
... 
} 
],
...
}
...
... the path value is indicative of how to extract the ticket_id and ticket_url.

refresh_response_ticket_id_key = number
* After extracting the JSON blob we are interested in, which looks like the following:
{
...
"number": "INC0047495",
"url": 
"https://abc.service-now.com/incident.do?sysparm_query=correlation_id=myevent1234"
} 
... 'number' is the value we are interested in.

refresh_response_ticket_url_key = url
* After extracting the JSON blob we are interested in, which looks like the following:
{
...
"number": "INC0047495",
"url": 
"https://abc.service-now.com/incident.do?sysparm_query=correlation_id=myevent1234"
} 

... 'url' is the value we are interested in.

notable_event_commonality.conf

The following are the spec and example files for notable_event_commonality.conf.

notable_event_commonality.conf.spec

# This file contains possible attribute/value pairs for blacklisting
# notable event fields from the Common Fields section of episodes.
#
# There is a notable_event_commonality.conf in
# $SPLUNK_HOME/etc/apps/SA-ITOA/default/.
# To set custom configurations, place a notable_event_commonality.conf
# in
# $SPLUNK_HOME/etc/apps/SA-ITOA/local. You must restart Splunk software
# to enable
# configurations.
#
# To learn more about configuration files (including precedence) please
# see
# the documentation located at
#
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

[common_event_fields]

black_list_fields = <comma-separated list>
* A list of field names in a notable event that will not appear in the
  Common Fields section of an episode.
* By default, ITSI blacklists fields that are not core to the raw event
  itself, or ones that are mainly used internally.
* Add fields here that you don't necessarily care about, but that you
  know
  will probably appear in most of your events.

notable_event_commonality.conf.example

No example
notable_event_correlation.conf

The following are the spec and example files for notable_event_correlation.conf.

notable_event_correlation.conf.spec

# This file contains attributes and values that ITSI Smart Mode uses to correlate
# notable events.
#
# There is a notable_event_correlation.conf in
# SPLUNK_HOME/etc/apps/SA-ITOA/default/.
# To set custom configurations, place a notable_event_correlation.conf in
# SPLUNK_HOME/etc/apps/SA-ITOA/local. You must restart Splunk software to enable
# configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
#
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the top
#   of the file.
# * Each .conf file should have at most one default stanza. If there are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
#   the file wins.
# * If an attribute is defined at both the global level and in a
#   specific stanza, the value in the specific stanza takes precedence.
[<smart_mode_correlation_engine>]

* The settings under this stanza determine how ITSI Smart Mode analyzes notable event fields to determine whether they contain textual or categorical content.
  * Smart Mode uses machine learning to compare event field values and group events that are related to each other.
* CAUTION: This configuration file does not support adding any additional stanzas. Do not add, remove, or change any of the settings or stanzas in this file unless specifically instructed to by a Splunk support specialist.

**BLACKLIST FIELDS**

black_list_fields = <comma-separated list>
* A list of field names in a notable event whose values to discard from consideration for Smart Mode event correlation.

**TEXTUAL FIELDS**

text_field_names = <comma-separated list>
* A list of field names in a notable event that usually represent textual content.
  * A text field is a data structure that holds alphanumeric data, such as name and address.
  * Defaults: comment, description, summary, review, message

ignore_fields_that_contain = <comma-separated list>
* A list of field names to implicitly ignore because they are not useful for event correlation.
  * ITSI ignores field names that contain any of the words in this list.
  * For example, with the default "time", ITSI ignores fields that represent time, like alert_triggertime, alerttriggertime, lasttimeup, etc.
  * Default: time

threshold_event_coverage_perc = <int>
* A threshold value for considering a notable event field as a text field.
  * If the count (total number of occurrences) of a field divided by
the total number of events processed in the time frame is less than the percentage specified in 'threshold_event_coverage_perc', then the notable event field is a text field.
* Default: 10

**CATEGORICAL FIELDS**

threshold_distinct_value_perc = <int>
* A threshold value for considering a notable event field as a categorical field.
* If the distinct_count (count of distinct values) of a field divided by the count (total number of occurrences) of the field is less than the percentage specified, then the notable event field is a categorical field.
* Categorical fields have a distinct value, such as a status field, as opposed to textual data, descriptions, numerical values, and comments.
* If this setting determines that a field is NOT a categorical field, ITSI uses the two settings below ('min_distinct_value_perc' and 'max_count_perc') in a second calculation to check whether the field is a categorical field.
* Default: 35

min_distinct_value_perc = <int>
* Helps confirm whether a notable event field is a categorical field.
* Sets the minimum distinctive value percentage that a notable event field must be to be considered a categorical field.
* If the cumulative sum of 'min_distinct_value_perc' of distinct_count (count of unique values) of a field is at least 'max_count_perc' of the count (total number of occurrences) of the field, then the notable event field is considered a categorical field.
* For example, consider the following field:value pairs:
  {field:value1 count:34}, {field:value2 count:31}, {field:value3 count:5},
  {field:value4 count:5}, ..., {field:value18 count:1}, {field:value19 count:1},
  {field:value20 count:1}
  There are 20 different values listed for this field, so distinct_count = 20.
  ITSI sums the counts of all the values, so count = 80.
  80% of count = 64
  10% of distinct_count = 2, so you add the counts of the first two values above (34 + 31).
{field:value1 count:34} + {field:value2 count:31} = 34 + 31 = 65 > 64
Because 65 is at least 64, "field" is a categorical field.
* Default: 10

max_count_perc = <int>
* Helps confirm whether a notable event field is a categorical field.
* Sets the maximum count percentage that a notable event field must be to be considered a categorical field.
* If the cumulative sum of 'min_distinct_value_perc' of distinct_count (count of unique values) of a field is at least 'max_count_perc' of the count (total number of occurrences) of the field, then the notable event field is considered a categorical field.
* See the example for the 'min_distinct_value_perc' setting to understand how this setting works.
* Default: 80

notable_event_correlation.conf.example

No example

props.conf

The following are the spec and example files for props.conf.

props.conf.spec

#   Version 7.3.0
#
# This file contains possible setting/value pairs for configuring Splunk software's processing properties through props.conf.
#
# Props.conf is commonly used for:
#
# * Configuring line breaking for multi-line events.
# * Setting up character set encoding.
# * Allowing processing of binary files.
# * Configuring timestamp recognition.
# * Configuring event segmentation.
# * Overriding automated host and source type matching. You can use props.conf to:
#   * Configure advanced (regular expression-based) host and source type overrides.
#   * Override source type matching for data from a particular source.
#   * Set up rule-based source type recognition.
* Rename source types.
* Anonymizing certain types of sensitive incoming data, such as credit card or social security numbers, using sed scripts.
* Routing specific events to a particular index, when you have multiple indexes.
* Creating new index-time field extractions, including header-based field extractions.
  NOTE: Do not add to the set of fields that are extracted at index time unless it is absolutely necessary because there are negative performance implications.
* Defining new search-time field extractions. You can define basic search-time field extractions entirely through props.conf, but a transforms.conf component is required if you need to create search-time field extractions that involve one or more of the following:
  * Reuse of the same field-extracting regular expression across multiple sources, source types, or hosts.
  * Application of more than one regular expression (regex) to the same source, source type, or host.
  * Delimiter-based field extractions (they involve field-value pairs that are separated by commas, colons, semicolons, bars, or something similar).
  * Extraction of multiple values for the same field (multivalued field extraction).
  * Extraction of fields with names that begin with numbers or underscores.
* Setting up lookup tables that look up fields from external sources.
* Creating field aliases.

NOTE: Several of the above actions involve a corresponding transforms.conf configuration.

You can find more information on these topics by searching the Splunk documentation (http://docs.splunk.com/Documentation/Splunk).

There is a props.conf in $SPLUNK_HOME/etc/system/default/. To set custom configurations, place a props.conf in $SPLUNK_HOME/etc/system/local/. For help, see props.conf.example.

You can enable configurations changes made to props.conf by typing the following search string in Splunk Web:

| extract reload=T

To learn more about configuration files (including precedence) see
GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the top
#   of the file.
# * Each conf file should have at most one default stanza. If there are
#   multiple default stanzas, settings are combined. In the case of
#   multiple definitions of the same setting, the last definition in the
#   file wins.
# * If a setting is defined at both the global level and in a specific
#   stanza, the value in the specific stanza takes precedence.

[<spec>]
* This stanza enables properties for a given <spec>.
* A props.conf file can contain multiple stanzas for any number of
different <spec>.
* Follow this stanza name with any number of the following setting/value pairs, as appropriate for what you want to do.
* If you do not set a setting for a given <spec>, the default is used.

<spec> can be:
1. <sourcetype>, the source type of an event.
2. host::<host>, where <host> is the host, or host-matching pattern, for an event.
3. source::<source>, where <source> is the source, or source-matching pattern, for an event.
4. rule::<rulename>, where <rulename> is a unique name of a source type classification rule.
5. delayedrule::<rulename>, where <rulename> is a unique name of a delayed source type classification rule.

These are only considered as a last resort before generating a new source type based on the source seen.

**[<spec>] stanza precedence:**
For settings that are specified in multiple categories of matching `<spec>` stanzas, `[host::<host>]` settings override `[<sourcetype>]` settings. Additionally, `[source::<source>]` settings override both `[host::<host>]` and `[<sourcetype>]` settings.

**Considerations for Windows file paths:**

When you specify Windows-based file paths as part of a `[source::<source>]` stanza, you must escape any backslashes contained within the specified file path.

Example: `[source::c:\path_to\file.txt]`

**[<spec>] stanza patterns:**

When setting a `<spec>` stanza, you can use the following regex-type syntax:
- ... recurses through directories until the match is met or equivalently, matches any number of characters.
- * matches anything but the path separator 0 or more times. The path separator is '/' on unix, or '\' on Windows. Intended to match a partial or complete directory or filename.
- | is equivalent to 'or'
- ( ) are used to limit scope of |.
- "\" = matches a literal backslash '\'.

Example: `[source::....(?<!tar.)(gz|bz2)]`

This matches any file ending with '.gz' or '.bz2', provided this is not preceded by 'tar.', so tar.bz2 and tar.gz would not be matched.

**[source::<source>] and [host::<host>] stanza match language:**

Match expressions must match the entire name, not just a substring. Match expressions are based on a full implementation of Perl-compatible regular expressions (PCRE) with the translation of "...", "*", and "." Thus, "." matches a period, "*" matches non-directory separators, and "..." matches any number of any characters.

For more information search the Splunk documentation for "specify input paths with wildcards".

**[<spec>] stanza pattern collisions:**

Suppose the source of a given input matches multiple [source::<source>]
patterns. If the [<spec>] stanzas for these patterns each supply distinct settings, Splunk software applies all of these settings.

However, suppose two [<spec>] stanzas supply the same setting. In this case, Splunk software chooses the value to apply based on the ASCII order of the patterns in question.

For example, take this source:

    source::az

and the following colliding patterns:

    [source::...a...]  
    sourcetype = a

    [source::...z...]  
    sourcetype = z

In this case, the settings provided by the pattern [source::...a...] take precedence over those provided by [source::...z...], and sourcetype ends up with "a" as its value.

To override this default ASCII ordering, use the priority key:

    [source::...a...]  
    sourcetype = a  
    priority = 5

    [source::...z...]  
    sourcetype = z  
    priority = 10

Assigning a higher priority to the second stanza causes sourcetype to have the value "z".

**Case-sensitivity for [<spec>] stanza matching:**

By default, [source::<source>] and [<sourcetype>] stanzas match in a case-sensitive manner, while [host::<host>] stanzas match in a case-insensitive manner. This is a convenient default, given that DNS names are case-insensitive.

To force a [host::<host>] stanza to match in a case-sensitive manner use the
"(?-i)" option in its pattern.

For example:

```
[host::foo]
FIELDALIAS-a = a AS one

[host::(?-i)bar]
FIELDALIAS-b = b AS two
```

The first stanza actually applies to events with host values of "FOO" or "Foo". The second stanza, on the other hand, does not apply to events with host values of "BAR" or "Bar".

**Building the final [<spec>] stanza:**

The final [<spec>] stanza is built by layering together (1) literal-matching stanzas (stanzas which match the string literally) and (2) any regex-matching stanzas, according to the value of the priority field.

If not specified, the default value of the priority key is:

* 0 for pattern-matching stanzas.
* 100 for literal-matching stanzas.

NOTE: Setting the priority key to a value greater than 100 causes the pattern-matched [<spec>] stanzas to override the values of the literal-matching [<spec>] stanzas.

The priority key can also be used to resolve collisions between [<sourcetype>] patterns and [host::<host>] patterns. However, be aware that the priority key does *not* affect precedence across <spec> types. For example, [spec] stanzas with [source::<source>] patterns take priority over stanzas with [host::<host>] and [<sourcetype>] patterns, regardless of their respective priority key values.

#****************************************************************************
# The possible setting/value pairs for props.conf, and their default values, are:
#****************************************************************************

```
priority = <number>
* Overrides the default ASCII ordering of matching stanza names

# International characters and character encoding.
```
**Line breaking**

# Use the following settings to define the length of a line.

**TRUNCATE** = <non-negative integer>
* The default maximum line length, in bytes.
* Although this is in bytes, line length is rounded down when this would otherwise land mid-character for multi-byte characters.
* Set to 0 if you never want truncation (very long lines are, however, often a sign of garbage data).
* Default: 10000

**LINE_BREAKER** = <regular expression>
* Specifies a regex that determines how the raw text stream is broken into initial events, before line merging takes place. (See the
SHOULD_LINEMERGE setting, below.)
* The regex must contain a capturing group -- a pair of parentheses which
defines an identified subcomponent of the match.
* Wherever the regex matches, Splunk software considers the start of the first
capturing group to be the end of the previous event, and considers the end
of the first capturing group to be the start of the next event.
* The contents of the first capturing group are discarded, and are not present in any event. You are telling Splunk software that this text comes between lines.
* NOTE: You get a significant boost to processing speed when you use LINE_BREAKER to delimit multi-line events (as opposed to using SHOULD_LINEMERGE to reassemble individual lines into multi-line events).
* When using LINE_BREAKER to delimit events, SHOULD_LINEMERGE should be set to false, to ensure no further combination of delimited events occurs.
* Using LINE_BREAKER to delimit events is discussed in more detail in the documentation. Search the documentation for "configure event line breaking" for details.
* Default: ((\r\n)+) (Data is broken into an event for each line, delimited by any number of carriage return or newline characters.)

** Special considerations for LINE_BREAKER with branched expressions **

When using LINE_BREAKER with completely independent patterns separated by pipes, some special issues come into play.
EG. LINE_BREAKER = pattern1|pattern2|pattern3

NOTE: This is not about all forms of alternation. For instance, there is nothing particularly special about example: LINE_BREAKER = ([\r\n])+{one|two|three}
where the top level remains a single expression.

CAUTION: Relying on these rules is NOT encouraged. Simpler is better, in both regular expressions and the complexity of the behavior they rely on.
If possible, reconstruct your regex to have a leftmost capturing group that always matches.

It might be useful to use non-capturing groups if you need to express a group
before the text to discard.
Example: LINE_BREAKER = (?:one|two){[\r\n]+}
* This matches the text one, or two, followed by any amount of
  newlines or carriage returns. The one-or-two group is
non-capturing
  via the ?: prefix and is skipped by LINE_BREAKER.

* A branched expression can match without the first capturing group
  matching, so the line breaker behavior becomes more complex.
Rules:
  1: If the first capturing group is part of a match, it is considered
    the
    linebreak, as normal.
  2: If the first capturing group is not part of a match, the leftmost
    capturing group which is part of a match is considered the
    linebreak.
  3: If no capturing group is part of the match, the linebreaker assumes
    that the linebreak is a zero-length break immediately preceding the
    match.

Example 1: LINE_BREAKER = end(\n)begin|end2(\n)begin2|begin3

* A line ending with 'end' followed a line beginning with 'begin'
  would
  match the first branch, and the first capturing group would have a
  match
  according to rule 1. That particular newline would become a break
  between lines.
* A line ending with 'end2' followed by a line beginning with 'begin2'
  would match the second branch and the second capturing group would
  have
  a match. That second capturing group would become the linebreak
  according to rule 2, and the associated newline would become a break
  between lines.
* The text 'begin3' anywhere in the file at all would match the third
  branch, and there would be no capturing group with a match. A
  linebreak
  would be assumed immediately prior to the text 'begin3' so a
  linebreak
  would be inserted prior to this text in accordance with rule 3.
This
  means that a linebreak occurs before the text 'begin3' at any
  point in the text, whether a linebreak character exists or not.

Example 2: Example 1 would probably be better written as follows. This
is
  not equivalent for all possible files, but for most real
files
  would be equivalent.

LINE_BREAKER = end2?(\n)begin(2|3)?
LINE_BREAKER_LOOKBEHIND = <integer>
* The number of bytes before the end of the raw data chunk
to which Splunk software should apply the 'LINE_BREAKER' regex.
* When there is leftover data from a previous raw chunk,
  LINE_BREAKER_LOOKBEHIND indicates the number of bytes before the end
  of
  the raw chunk (with the next chunk concatenated) where Splunk software
  applies the LINE_BREAKER regex.
* You might want to increase this value from its default if you are
dealing with especially large or multi-line events.
* Default: 100

# Use the following settings to specify how multi-line events are
handled.

SHOULD_LINEMERGE = <boolean>
* Whether or not to combine several lines of data into a single
multiline event, based on the configuration settings listed in
this subsection.
* When you set this to "true", Splunk software combines several lines of
data
  into a single multi-line event, based on values you configure
in the following settings.
* When you set this to "false", Splunk software does not combine lines
  of
data into multiline events.
* Default: true

# When SHOULD_LINEMERGE is set to true, use the following settings to
# define how Splunk software builds multi-line events.

BREAK_ONLY_BEFORE_DATE = <boolean>
* Whether or not to create a new event if a new line with a date is
encountered
  in the data stream.
* When you set this to "true", Splunk software creates a new event only
if it
  encounters a new line with a date.
  * NOTE: When using DATETIME_CONFIG = CURRENT or NONE, this setting is
    not
    meaningful, as timestamps are not identified.
  * Default: true

BREAK_ONLY_BEFORE = <regular expression>
* When set, Splunk software creates a new event only if it encounters a
new
  line that matches the regular expression.
* Default: empty string

MUST_BREAK_AFTER = <regular expression>
* When set, Splunk software creates a new event for the next input line
  only
if the regular expression matches the current line.
* It is possible for the software to break before the current line if
  another rule matches.
* Default: empty string

MUST_NOT_BREAK_AFTER = <regular expression>
* When set, and the current line matches the regular expression, Splunk
  software does not break on any subsequent lines until the MUST_BREAK_AFTER
  expression matches.
* Default: empty string

MUST_NOT_BREAK_BEFORE = <regular expression>
* When set, and the current line matches the regular expression, Splunk
  software does not break the last event before the current line.
* Default: empty string

MAX_EVENTS = <integer>
* The maximum number of input lines to add to any event.
* Splunk software breaks after it reads the specified number of lines.
* Default: 256

# Use the following settings to handle better load balancing from UF.
# NOTE: The EVENT_BREAKER properties are applicable for Splunk Universal
# Forwarder instances only.

EVENT_BREAKER_ENABLE = <boolean>
* Whether or not a universal forwarder (UF) uses the
  'ChunkedLBProcessor'
  data processor to improve distribution of events to receiving
  indexers for a given source type.
* When set to true, a UF splits incoming data with a
  light-weight chunked line breaking processor ('ChunkedLBProcessor')
  so that data is distributed fairly evenly amongst multiple indexers.
* When set to false, a UF uses standard load-balancing methods to
  send events to indexers.
* Use this setting on a UF to indicate that data
  should be split on event boundaries across indexers, especially
  for large files.
* This setting is only valid on universal forwarder instances.
* Default: false

# Use the following to define event boundaries for multi-line events
# For single-line events, the default settings should suffice

EVENT_BREAKER = <regular expression>
* A regular expression that specifies the event boundary for a
  universal forwarder to use to determine when it can send events
  to an indexer.
* The regular expression must contain a capturing group
  (a pair of parentheses that defines an identified sub-component
of the match.)
* When the UF finds a match, it considers the first capturing group to be the end of the previous event, and the end of the capturing group to be the beginning of the next event.
* At this point, the forwarder can then change the receiving indexer based on these event boundaries.
* This setting is only active if you set 'EVENT_BREAKER_ENABLE' to "true", only works on universal forwarders, and works best with multiline events.
* Default: "\r\n"

**Timestamp extraction configuration**

**DATETIME_CONFIG = [<filename relative to $SPLUNK_HOME> | CURRENT | NONE]**
* Specifies which file configures the timestamp extractor, which identifies timestamps from the event text.
* This setting may also be set to "NONE" to prevent the timestamp extractor from running or "CURRENT" to assign the current system time to each event.
* "CURRENT" sets the time of the event to the time that the event was merged from lines, or worded differently, the time it passed through the aggregator processor.
* "NONE" leaves the event time set to whatever time was selected by the input layer.
* For data sent by Splunk forwarders over the Splunk-to-Splunk protocol, the input layer is the time that was selected on the forwarder by its input behavior (as below).
* For file-based inputs (monitor, batch) the time chosen is the modification timestamp on the file being read.
* For other inputs, the time chosen is the current system time when the event is read from the pipe/socket/etc.
* Both "CURRENT" and "NONE" explicitly disable the per-text timestamp identification, so the default event boundary detection (BREAK_ONLY_BEFORE_DATE = true) is likely to not work as desired. When using these settings, use 'SHOULD_LINEMERGE' and/or the 'BREAK_ONLY_*', 'MUST_BREAK_*' settings to control event merging.
* For more information on 'DATETIME_CONFIG' and datetime.xml, see "Configure advanced timestamp recognition with datetime.xml" in the Splunk Documentation.
* Default: /etc/datetime.xml (for example,
TIME_PREFIX = <regular expression>
* If set, Splunk software scans the event text for a match for this regex
  in event text before attempting to extract a timestamp.
* The timestamping algorithm only looks for a timestamp in the text
  following the end of the first regex match.
* For example, if 'TIME_PREFIX' is set to "abc123", only text following the
  first occurrence of the text abc123 is used for timestamp extraction.
* If the 'TIME_PREFIX' cannot be found in the event text, timestamp
  extraction
  does not occur.
* Default: empty string

MAX_TIMESTAMP_LOOKAHEAD = <integer>
* The number of characters into an event Splunk software should look
  for a timestamp.
* This constraint to timestamp extraction is applied from the point of
  the
  'TIME_PREFIX'-set location.
* For example, if 'TIME_PREFIX' positions a location 11 characters into the
  event, and MAX_TIMESTAMP_LOOKAHEAD is set to 10, timestamp extraction
  is
  constrained to characters 11 through 20.
* If set to 0 or -1, the length constraint for timestamp recognition is
  effectively disabled. This can have negative performance implications
  which scale with the length of input lines (or with event size when
  'LINE_BREAKER' is redefined for event splitting).
* Default: 128

TIME_FORMAT = <strptime-style format>
* Specifies a "strptime" format string to extract the date.
* "strptime" is an industry standard for designating time formats.
* For more information on strftime, see "Configure timestamp
  recognition" in
  the online documentation.
* TIME_FORMAT starts reading after the TIME_PREFIX. If both are
  specified,
  the TIME_PREFIX regex must match up to and including the character
  before
  the TIME_FORMAT date.
* For good results, the <strptime-style format> should describe the day
  of
  the year and the time of day.
* Default: empty string

TZ = <timezone identifier>
* The algorithm for determining the time zone for a particular event is
  as
follows:
* If the event has a timezone in its raw text (for example, UTC, -08:00),
  use that.
* If TZ is set to a valid timezone string, use that.
* If the event was forwarded, and the forwarder-indexer connection uses
  the version 6.0 and higher forwarding protocol, use the timezone provided
  by the forwarder.
* Otherwise, use the timezone of the system that is running splunkd.
* Default: empty string

TZ_ALIAS = <key=value>[,<key=value>]...
* Provides Splunk software admin-level control over how timezone strings
  extracted from events are interpreted.
  * For example, EST can mean Eastern (US) Standard time, or Eastern
    (Australian) Standard time. There are many other three letter
  timezone
    acronyms with many expansions.
  * There is no requirement to use 'TZ_ALIAS' if the traditional Splunk
    software
    default mappings for these values have been as expected. For example, EST
    maps to the Eastern US by default.
  * Has no effect on the 'TZ' value. This only affects timezone strings
    from event
    text, either from any configured 'TIME_FORMAT', or from pattern-based
    guess
    fallback.
* The setting is a list of key=value pairs, separated by commas.
  * The key is matched against the text of the timezone specifier of the
    event, and the value is the timezone specifier to use when mapping
    the
    timestamp to UTC/GMT.
  * The value is another TZ specifier which expresses the desired
    offset.
  * Example: TZ_ALIAS = EST=GMT+10:00 (See props.conf.example for
    more/full
    examples)
  * Default: not set

MAX_DAYS_AGO = <integer>
* The maximum number of days in the past, from the current date as
  provided by the input layer (For example forwarder current time, or
  modtime
  for files), that an extracted date can be valid.
* Splunk software still indexes events with dates older than
  'MAX_DAYS_AGO'
  with the timestamp of the last acceptable event.
* If no such acceptable event exists, new events with timestamps older
  than 'MAX_DAYS_AGO' uses the current timestamp.
* For example, if MAX_DAYS_AGO = 10, Splunk software applies the
timestamp
of the last acceptable event to events with extracted timestamps older
than 10 days in the past. If no acceptable event exists, Splunk
software
applies the current timestamp.
* If your data is older than 2000 days, increase this setting.
* Highest legal value: 10951 (30 years).
* Default: 2000 (5.48 years).

MAX_DAYS_HENCE = <integer>
* The maximum number of days in the future, from the current date as
provided by the input layer (for e.g. forwarder current time, or
modtime for files), that an extracted date can be valid.
* Splunk software still indexes events with dates more than
'MAX_DAYS_HENCE'
in the future with the timestamp of the last acceptable event.
* If no such acceptable event exists, new events
with timestamps after 'MAX_DAYS_HENCE' use the current timestamp.
* For example, if MAX_DAYS_HENCE = 3, Splunk software applies the
timestamp of
the last acceptable event to events with extracted timestamps more
than 3
days in the future. If no acceptable event exists, Splunk software
applies
the current timestamp.
* The default value includes dates from one day in the future.
* If your servers have the wrong date set or are in a timezone that is one
day ahead, increase this value to at least 3.
* NOTE: False positives are less likely with a smaller window. Change
with
cautions.
* Highest legal value: 10950 (30 years).
* Default: 2

MAX_DIFF SECS_AGO = <integer>
* This setting prevents Splunk software from rejecting events with
timestamps
that are out of order.
* Do not use this setting to filter events. Splunk software uses
complicated heuristics for time parsing.
* Splunk software warns you if an event timestamp is more than
'MAX_DIFF SECS_AGO' seconds before the previous timestamp and does not
have the same time format as the majority of timestamps from the
source.
* After Splunk software throws the warning, it only rejects an event if it
cannot apply a timestamp to the event. (For example, if Splunk
software
cannot recognize the time of the event.)
* If your timestamps are wildly out of order, consider increasing
this value.
* NOTE: If the events contain time but not date (date determined another way,
such as from a filename) this check only considers the hour. (No one second granularity for this purpose.)
* Highest legal value: 2147483646 (68.1 years).
* Defaults: 3600 (one hour).

MAX_DIFF_SECS_HENCE = <integer>
* This setting prevents Splunk software from rejecting events with timestamps
  that are out of order.
* Do not use this setting to filter events. Splunk software uses complicated heuristics for time parsing.
* Splunk software warns you if an event timestamp is more than 'MAX_DIFF_SECS_HENCE' seconds AFTER the previous timestamp and does not
  have the same time format as the majority of timestamps from the source.
* After Splunk software throws the warning, it only rejects an event if it
cannot apply a timestamp to the event. (For example, if Splunk software
cannot recognize the time of the event.)
* If your timestamps are wildly out of order, or you have logs that are written less than once a week, consider increasing this value.
* Highest legal value: 2147483646 (68.1 years).
* Default: 604800 (one week).

ADD_EXTRA_TIME_FIELDS = [none | subseconds | all | <boolean>]
* Whether or not Splunk software automatically generates and indexes the following keys with events:
  * date_hour, date_mday, date_minute, date_month, date_second, date_wday,
    date_year, date_zone, timestartpos, timeendpos, timestamp.
* These fields are never required, and may be turned off as desired.
* If set to "none" (or false), all indextime data about the timestamp is stripped out. This removes the above fields but also removes information
  about the sub-second timestamp granularity. When events are searched, only the second-granularity timestamp is returned as part of the
  "_time" field.
* If set to "subseconds", the above fields are stripped out but the data about
  subsecond timestamp granularity is left intact.
* If set to "all" (or true), all of the indextime fields from the time parser are included.
* Default: true (Enabled for most data sources.)
Structured Data Header Extraction and configuration

* This setting applies at input time, when data is first read by Splunk software, such as on a forwarder that has configured inputs acquiring the data.

# These special string delimiters, which are single ASCII characters, can be used in the settings that follow, which state "You can use the delimiters for structured data header extraction with this setting."
# You can only use a single delimiter for any setting. It is not possible to configure multiple delimiters or characters per setting.
# Example of using the delimiters:
# FIELD_DELIMITER=space
# * Tells Splunk software to use the space character to separate fields in the specified source.
# space - Space separator (separates on a single space)
# tab / \t - Tab separator
# fs - ASCII file separator
# gs - ASCII group separator
# rs - ASCII record separator
# us - ASCII unit separator
# \xHH - HH is two hexadecimal digits to use as a separator
# Example : \x14 - select 0x14 as delimiter
# none - (Valid for FIELD_QUOTE and HEADER_FIELD_QUOTE only)
# whitespace / ws - (Valid for FIELD_DELIMITER and HEADER_FIELD_DELIMITER only)
# treats any number of spaces and tabs as a single delimiter

INDEXED_EXTRACTIONS = <CSV|TSV|PSV|W3C|JSON|HEC>
* The type of file that Splunk software should expect for a given source type, and the extraction and/or parsing method that should be used on the file.
* The following values are valid for 'INDEXED_EXTRACTIONS':
  CSV - Comma separated value format
  TSV - Tab-separated value format
  PSV - pipe ("|")-separated value format
  W3C - World Wide Web Consortium (W3C) Extended Extended Log File Format
  JSON - JavaScript Object Notation format
  HEC - Interpret file as a stream of JSON events in the same format as the HTTP Event Collector (HEC) input.
* These settings change the defaults for other settings in this subsection to appropriate values, specifically for these formats.
* The HEC format lets events overrided many details on a per-event basis, such as the destination index. Use this value to read data which you know to be well-formatted and safe to index with little or no processing, such as data generated by locally written tools.
* Default: not set

METRICS_PROTOCOL = <STATSD|COLLECTD_HTTP>
* Which protocol the incoming metric data is using:
  STATSD: Supports the statsd protocol, in the following format:
  <metric name>:<value>|<metric type>
  Use the 'STATSD-DIM-TRANSFORMS' setting to manually extract dimensions for the above format. Splunk software auto-extracts dimensions when the data has "#" as dimension delimiter as shown below:
  <metric name>:<value>|<metric type>|#<dim1>:<val1>, <dim2>:<val2>...
  COLLECTD_HTTP: This is data from the write_http collectd plugin being parsed as streaming JSON docs with the _value living in "values" array and the dimension names in "dsnames" and the metric type (for example, counter vs gauge) is derived from "dstypes".
* Default (for event (non-metric) data): not set

STATSD-DIM-TRANSFORMS = <statsd_dim_stanza_name1>,<statsd_dim_stanza_name2>..
* Valid only when 'METRICS_PROTOCOL' is set to "statsd".
* A comma separated list of transforms stanza names which are used to extract dimensions from statsd metric data.
* Optional for sourcetypes which have only one transforms stanza for extracting dimensions, and the stanza name is the same as that of sourcetype name.
* Default: not set

METRIC-SCHEMA-TRANSFORMS = <metric-schema:stanza_name>[,<metric-schema:stanza_name>]...
* A comma-separated list of metric-schema stanza names from transforms.conf that the Splunk platform uses to create multiple metrics from index-time
field extractions of a single log event.
* NOTE: This setting is valid only for index-time field extractions.
You can set up the TRANSFORMS field extraction configuration to create index-time field extractions. The Splunk platform always applies METRIC-SCHEMA-TRANSFORMS after index-time field extraction takes place.
* Optional.
* Default: empty

PREAMBLE_REGEX = <regex>
* A regular expression that lets Splunk software ignore "preamble lines",
  or lines that occur before lines that represent structured data.
* When set, Splunk software ignores these preamble lines,
  based on the pattern you specify.
* Default: not set

FIELD_HEADER_REGEX = <regex>
* A regular expression that specifies a pattern for prefixed headers.
* The actual header starts after the pattern. It is not included in
  the header field.
* This setting supports the use of the special characters described above.
* The default can vary if 'INDEXED_EXTRACTIONS' is set.
* Default (if 'INDEXED_EXTRACTIONS' is not set): not set

HEADER_FIELD_LINE_NUMBER = <integer>
* The line number of the line within the specified file or source that
  contains the header fields.
* If set to 0, Splunk software attempts to
  locate the header fields within the file automatically.
* Default: 0

FIELD_DELIMITER = <character>
* Which character delimits or separates fields in the
  specified file or source.
* You can use the delimiters for structured data header extraction with
  this setting.
* This setting supports the use of the special characters described above.
* The default can vary if 'INDEXED_EXTRACTIONS' is set.
* Default (if 'INDEXED_EXTRACTIONS' is not set): not set

HEADER_FIELD_DELIMITER = <character>
* Which character delimits or separates header fields in
  the specified file or source.
* The default can vary if 'INDEXED_EXTRACTIONS' is set.
* Default (if 'INDEXED_EXTRACTIONS' is not set): not set

FIELD_QUOTE = <character>
* The character to use for quotes in the specified file
  or source.
* You can use the delimiters for structured data header extraction with this setting.
* The default can vary if 'INDEXED_EXTRACTIONS' is set.
* Default (if 'INDEXED_EXTRACTIONS' is not set): not set

**HEADER_FIELDQUOTE** = <character>
* The character to use for quotes in the header of the specified file or source.
* You can use the delimiters for structured data header extraction with this setting.
* The default can vary if 'INDEXED_EXTRACTIONS' is set.
* Default (if 'INDEXED_EXTRACTIONS' is not set): not set

**TIMESTAMP_FIELDS** = [ <string>,..., <string>]
* Some CSV and structured files have their timestamp encompass multiple fields in the event separated by delimiters.
* This setting tells Splunk software to specify all such fields which constitute the timestamp in a comma-separated fashion.
* If not specified, Splunk software tries to automatically extract the timestamp of the event.
* The default can vary if 'INDEXED_EXTRACTIONS' is set.
* Default (if 'INDEXED_EXTRACTIONS' is not set): not set

**FIELD_NAMES** = [ <string>,..., <string>]
* Some CSV and structured files might have missing headers.
* This setting tells Splunk software to specify the header field names directly.
* The default can vary if 'INDEXED_EXTRACTIONS' is set.
* Default (if 'INDEXED_EXTRACTIONS' is not set): not set

**MISSING_VALUE_REGEX** = <regex>
* The placeholder to use in events where no value is present.
* The default can vary if 'INDEXED_EXTRACTIONS' is set.
* Default (if 'INDEXED_EXTRACTIONS' is not set): not set

**JSON_TRIM_BRACES_IN_ARRAY_NAMES** = <boolean>
* Whether or not the JSON parser for 'INDEXED_EXTRACTIONS' strips curly braces from names of fields that are defined as arrays in JSON events.
* When the JSON parser extracts fields from JSON events, by default, it extracts array field names with the curly braces that indicate they are arrays ("{}") intact.
* For example, given the following partial JSON event:
  
  ```json
  {"datetime":"08-20-2015 10:32:25.267 -0700","log_level":"INFO",...,
   data:{...,"fs_type":"ext4","mount_point":['/disk48','/disk22'],...}}
  ```

  Because the "mount_point" field in this event is an array of two values ("/disk48" and "/disk22"), the JSON parser sees the field as an array, and extracts it as such, including the braces that identify it as an array. The resulting field name is "data.mount_point{}").
* Set 'JSON_TRIM_BRACES_IN_ARRAY_NAMES' to "true" if you want the JSON parser to strip these curly braces from array field names. (In this example, the resulting field is instead "data.mount_point").
* CAUTION: Setting this to "true" makes array field names that are
  extracted  
at index time through the JSON parser inconsistent with search-time
  extraction of array field names through the 'spath' search command.
* Default: false

**Field extraction configuration**

NOTE: If this is your first time configuring field extractions in
  props.conf, review the following information first. Additional
  information is also available in the Getting Data In Manual
  in the Splunk Documentation.

There are three different "field extraction types" that you can use to
  configure field extractions: TRANSFORMS, REPORT, and EXTRACT. They
differ in
two significant ways: 1) whether they create indexed fields (fields
extracted at index time) or extracted fields (fields extracted at search
time), and 2), whether they include a reference to an additional
component
called a "field transform," which you define separately in
  transforms.conf.

**Field extraction configuration: index time versus search time**

Use the TRANSFORMS field extraction type to create index-time field
  extractions. Use the REPORT or EXTRACT field extraction types to create
search-time field extractions.

NOTE: Index-time field extractions have performance implications.
  Create additions to the default set of indexed fields ONLY
  in specific circumstances. Whenever possible, extract
  fields only at search time.

There are times when you may find that you need to change or add to your
  set
of indexed fields. For example, you may have situations where certain
search-time field extractions are noticeably impacting search
performance.
This can happen when the value of a search-time extracted field exists
outside of the field more often than not. For example, if you commonly
search a large event set with the expression company_id=1 but the value
1
occurs in many events that do *not* have company_id=1, you may want to
add
  company_id to the list of fields extracted by Splunk software at index
time.
This is because at search time, Splunk software checks each
instance of the value 1 to see if it matches company_id, and that kind of thing slows down performance when you have Splunk searching a large set of data.

Conversely, if you commonly search a large event set with expressions like company_id!=1 or NOT company_id=1, and the field company_id nearly *always* takes on the value 1, you may want to add company_id to the list of fields extracted by Splunk software at index time.

For more information about index-time field extraction, search the documentation for "index-time extraction." For more information about search-time field extraction, search the documentation for "search-time extraction."

**Field extraction configuration: field transforms vs. "inline" (props.conf only) configs**

The TRANSFORMS and REPORT field extraction types reference an additional component called a field transform, which you define separately in transforms.conf. Field transforms contain a field-extracting regular expression and other settings that govern the way that the transform extracts fields. Field transforms are always created in conjunction with field extraction stanzas in props.conf; they do not stand alone.

The EXTRACT field extraction type is considered to be "inline," which means that it does not reference a field transform. It contains the regular expression that Splunk software uses to extract fields at search time. You can use EXTRACT to define a field extraction entirely within props.conf, no transforms.conf component is required.

**Search-time field extractions: Why use REPORT if EXTRACT will do?**

This is a good question. And much of the time, EXTRACT is all you need for search-time field extraction. But when you build search-time field extractions, there are specific cases that require the use of REPORT and the field transform that it references. Use REPORT if you want to:

* Reuse the same field-extracting regular expression across multiple sources, source types, or hosts. If you find yourself using the same regex to extract fields across several different sources, source types, and hosts, set it up as a transform, and then reference it in REPORT
extractions in those stanzas. If you need to update the regex you only have to do it in one place. Handy!
* Apply more than one field-extracting regular expression to the same source, source type, or host. This can be necessary in cases where the field or fields that you want to extract from a particular source, source type, or host appear in two or more very different event patterns.
* Set up delimiter-based field extractions. Useful if your event data presents field-value pairs (or just field values) separated by delimiters such as commas, spaces, bars, and so on.
* Configure extractions for multivalued fields. You can have Splunk software append additional values to a field as it finds them in the event data.
* Extract fields with names beginning with numbers or underscores. Ordinarily, the key cleaning functionality removes leading numeric characters and underscores from field names. If you need to keep them, configure your field transform to turn key cleaning off.
* Manage formatting of extracted fields, in cases where you are extracting multiple fields, or are extracting both the field name and field value.

**Precedence rules for TRANSFORMS, REPORT, and EXTRACT field extraction types**

* For each field extraction, Splunk software takes the configuration from the highest precedence configuration stanza (see precedence rules at the beginning of this file).
* If a particular field extraction is specified for a source and a source type, the field extraction for source wins out.
* Similarly, if a particular field extraction is specified in ../local/ for a <spec>, it overrides that field extraction in ../default/.

TRANSFORMS-<class> = <transform_stanza_name>, <transform_stanza_name2>, ...
* Used for creating indexed fields (index-time field extractions).
* <class> is a unique literal string that identifies the namespace of the field you're extracting.

**Note:** <class> values do not have to follow field name syntax restrictions. You can use characters other than a-z, A-Z, and 0-9, and spaces are allowed. <class> values are not subject to key cleaning.
* <transform_stanza_name> is the name of your stanza from transforms.conf.
* Use a comma-separated list to apply multiple transform stanzas to a single
TRANSFORMS extraction. Splunk software applies them in the list order. For example, this sequence ensures that the [yellow] transform stanza gets applied first, then [blue], and then [red]:
[source::color_logs]
TRANSFORMS-colorchange = yellow, blue, red

REPORT-<class> = <transform_stanza_name>, <transform_stanza_name2>,...
* Used for creating extracted fields (search-time field extractions) that reference one or more transforms.conf stanzas.
* <class> is a unique literal string that identifies the namespace of the field you're extracting.
NOTE: <class> values do not have to follow field name syntax restrictions. You can use characters other than a-z, A-Z, and 0-9, and spaces are allowed. <class> values are not subject to key cleaning.
* <transform_stanza_name> is the name of your stanza from transforms.conf.
* Use a comma-separated list to apply multiple transform stanzas to a single REPORT extraction.

Splunk software applies them in the list order. For example, this sequence insures that the [yellow] transform stanza gets applied first, then [blue], and then [red]:
[source::color_logs]
REPORT-colorchange = yellow, blue, red

EXTRACT-<class> = [<regex>|<regex> in <src_field>]
* Used to create extracted fields (search-time field extractions) that do not reference transforms.conf stanzas.
* Performs a regex-based field extraction from the value of the source field.
* <class> is a unique literal string that identifies the namespace of the field you're extracting.
NOTE: <class> values do not have to follow field name syntax restrictions. You can use characters other than a-z, A-Z, and 0-9, and spaces are allowed. <class> values are not subject to key cleaning.
* The <regex> is required to have named capturing groups. When the <regex> matches, the named capturing groups and their values are added to the event.
* dotall (?s) and multi-line (?m) modifiers are added in front of the regex.
So internally, the regex becomes (?ms)<regex>.
* Use '<regex> in <src_field>' to match the regex against the values of a specific field. Otherwise it just matches against _raw (all raw event
* NOTE: <src_field> has the following restrictions:
  * It can only contain alphanumeric characters and underscore (a-z, A-Z, 0-9, and _).
  * It must already exist as a field that has either been extracted at index time or has been derived from an EXTRACT-<class> configuration whose <class> ASCII value is *higher* than the configuration in which you are attempting to extract the field. For example, if you have an EXTRACT-ZZZ configuration that extracts <src_field>, then you can only use 'in <src_field>' in an EXTRACT configuration with a <class> of 'aaa' or lower, as 'aaa' is lower in ASCII value than 'ZZZ'.
  * It cannot be a field that has been derived from a transform field extraction (REPORT-<class>), an automatic key-value field extraction (in which you configure the KV_MODE setting to be something other than 'none'), a field alias, a calculated field, or a lookup, as these operations occur after inline field extractions (EXTRACT-<class>) in the search-time operations sequence.
  * If your regex needs to end with 'in <string>' where <string> is *not* a field name, change the regex to end with '[i]n <string>' to ensure that Splunk software doesn't try to match <string> to a field name.

KV_MODE = [none|auto|auto_escaped|multi|json|xml]
  * Used for search-time field extractions only.
  * Specifies the field/value extraction mode for the data.
  * Set KV_MODE to one of the following:
    * none: if you want no field/value extraction to take place.
    * auto: extracts field/value pairs separated by equal signs.
    * auto_escaped: extracts fields/value pairs separated by equal signs and honors \" and \\ as escaped sequences within quoted values, e.g field="value with \"nested\" quotes"
    * multi: invokes the multikv search command to expand a tabular event into multiple events.
    * xml: automatically extracts fields from XML data.
    * json: automatically extracts fields from JSON data.
  * Setting to 'none' can ensure that one or more user-created regexes are not overridden by automatic field/value extraction for a particular host, source, or source type, and also increases search performance.
  * The 'xml' and 'json' modes do not extract any fields when used on data that isn't of the correct format (JSON or XML).
  * Default: auto

MATCH_LIMIT = <integer>
  * Only set in props.conf for EXTRACT type field extractions.
    * For REPORT and TRANSFORMS field extractions, set this in transforms.conf.
* Optional. Limits the amount of resources spent by PCRE when running patterns that do not match.
* Use this to set an upper bound on how many times PCRE calls an internal function, match(). If set too low, PCRE may fail to correctly match a pattern.
* Default: 100000

DEPTH_LIMIT = <integer>
* Only set in props.conf for EXTRACT type field extractions.
  For REPORT and TRANSFORMS field extractions, set this in transforms.conf.
* Optional. Limits the amount of resources spent by PCRE when running patterns that do not match.
* Use this to limit the depth of nested backtracking in an internal PCRE function, match(). If set too low, PCRE might fail to correctly match a pattern.
* Default: 1000

AUTO_KV_JSON = <boolean>
* Used for search-time field extractions only.
* Specifies whether to try json extraction automatically.
* Default: true

KV_TRIM_SPACES = <boolean>
* Modifies the behavior of KV_MODE when set to auto, and auto_escaped.
* Traditionally, automatically identified fields have leading and trailing whitespace removed from their values.
* Example event: 2014-04-04 10:10:45 myfield="apples"
  would result in a field called 'myfield' with a value of 'apples'.
* If this value is set to false, then external whitespace then this outer space is retained.
* Example: 2014-04-04 10:10:45 myfield="apples"
  would result in a field called 'myfield' with a value of 'apples'.
* The trimming logic applies only to space characters, not tabs, or other whitespace.
* NOTE: Splunk Web currently has limitations with displaying and interactively clicking on fields that have leading or trailing whitespace. Field values with leading or trailing spaces may not look distinct in the event viewer, and clicking on a field value typically inserts the term into the search string without its embedded spaces.
* The limitations are not specific to this feature. Any embedded spaces
  behave this way.
* The Splunk search language and included commands respect the spaces.
* Default: true

CHECK_FOR_HEADER = <boolean>
* Used for index-time field extractions only.
* Set to true to enable header-based field extraction for a file.
* If the file has a list of columns and each event contains a field value
  (without field name), Splunk software picks a suitable header line to use for extracting field names.
* Can only be used on the basis of [<sourcetype>] or [source::<spec>], not [host::<spec>].
* Disabled when LEARN_SOURCETYPE = false.
* Causes the indexed source type to have an appended numeral; for example, sourcetype-2, sourcetype-3, and so on.
* The field names are stored in etc/apps/learned/local/props.conf.
  * Because of this, this feature does not work in most environments where the data is forwarded.
* This setting applies at input time, when data is first read by Splunk software, such as on a forwarder that has configured inputs acquiring the data.
* Default: false

SEDCMD-<class> = <sed script>
* Only used at index time.
* Commonly used to anonymize incoming data at index time, such as credit card or social security numbers. For more information, search the online documentation for "anonymize data."
* Used to specify a sed script which Splunk software applies to the _raw field.
* A sed script is a space-separated list of sed commands. Currently the following subset of sed commands is supported:
  * replace (s) and character substitution (y).
* Syntax:
  * replace - s/regex/replacement/flags
    * regex is a perl regular expression (optionally containing capturing groups).
  * replacement is a string to replace the regex match. Use \n for back references, where "n" is a single digit.
  * flags can be either: g to replace all matches, or a number to replace a specified match.
  * substitute - y/string1/string2/
    * substitutes the string1[i] with string2[i]
* No default.

FIELDALIAS-<class> = (orig_field_name) AS|ASNEW (new_field_name)+
* Use FIELDALIAS configurations to apply aliases to a field. This lets you search for the original field using one or more alias field names.
* <orig_field_name> is the original name of the field. It is not removed by this configuration.
* `<new_field_name>` is the alias to assign to the `<orig_field_name>`.
* You can create multiple aliases for the same field.
* You can include multiple field alias renames in the same stanza.
* Avoid applying the same alias field name to multiple original field names.
  * If you must do this, set it up as a calculated field (an EVAL-* statement) that uses the 'coalesce' function to create a new field that takes the value of one or more existing fields. This method lets you be explicit about ordering of input field values in the case of NULL fields. For example: EVAL-ip = coalesce(clientip,ipaddress)
* The following is true if you use AS in this configuration:
  * If the alias field name `<new_field_name>` already exists, the Splunk software replaces its value with the value of `<orig_field_name>`.
  * If the `<orig_field_name>` field has no value or does not exist, the `<new_field_name>` is removed.
* The following is true if you use ASNEW in this configuration:
  * If the alias field name `<new_field_name>` already exists, the Splunk software does not change it.
  * If the `<orig_field_name>` field has no value or does not exist, the `<new_field_name>` is kept.
* Field aliasing is performed at search time, after field extraction, but before calculated fields (EVAL-* statements) and lookups. This means that:
  * Any field extracted at search time can be aliased.
  * You can specify a lookup based on a field alias.
  * You cannot alias a calculated field.
* No default.

```
EVAL-<fieldname> = <eval statement>
```
* Use this to automatically run the `<eval statement>` and assign the value of the output to `<fieldname>`. This creates a "calculated field." When multiple EVAL-* statements are specified, they behave as if they are run in parallel, rather than in any particular sequence. For example say you have two statements: EVAL-x = y*2 and EVAL-y=100. In this case, "x" is assigned the original value of "y * 2," not the value of "y" after it is set to 100.
* Splunk software processes calculated fields after field extraction and field aliasing but before lookups. This means that:
  * You can use a field alias in the eval statement for a calculated field.
  * You cannot use a field added through a lookup in an eval statement for a calculated field.
* No default.
LOOKUP-<class> = $TRANSFORM (<match_field> (AS <match_field_in_event>)?)+ (OUTPUT|OUTPUTNEW (<output_field> (AS <output_field_in_event>)? )+)?

* At search time, identifies a specific lookup table and describes how that lookup table should be applied to events.
* <match_field> specifies a field in the lookup table to match on.
  * By default Splunk software looks for a field with that same name in the event to match with (if <match_field_in_event> is not provided)
  * You must provide at least one match field. Multiple match fields are allowed.
* <output_field> specifies a field in the lookup entry to copy into each matching event in the field <output_field_in_event>.
  * If you do not specify an <output_field_in_event> value, Splunk software uses <output_field>.
  * A list of output fields is not required.
* If they are not provided, all fields in the lookup table except for the match fields (and the timestamp field if it is specified) are output for each matching event.
* If the output field list starts with the keyword "OUTPUTNEW" instead of "OUTPUT", then each output field is only written out if it did not previous exist. Otherwise, the output fields are always overridden. Any event that has all of the <match_field> values but no matching entry in the lookup table clears all of the output fields. NOTE that OUTPUTNEW behavior has changed since 4.1.x (where *none* of the output fields were written to if *any* of the output fields previously existed).
* Splunk software processes lookups after it processes field extractions, field aliases, and calculated fields (EVAL-* statements). This means that you can use extracted fields, aliased fields, and calculated fields to specify lookups. But you can't use fields discovered by lookups in the configurations of extracted fields, aliased fields, or calculated fields.
* The LOOKUP- prefix is actually case-insensitive. Acceptable variants include:
  * LOOKUP_<class> = [...] 
  * LOOKUP<class> = [...] 
  * lookup_<class> = [...] 
  * lookup<class> = [...] 
* No default.
**Binary file configuration**

NO_BINARY_CHECK = <boolean>
* When set to true, Splunk software processes binary files.
* Can only be used on the basis of \[<sourcetype>\], or \[source::<source>\], not \[host::<host>\].
* Default: false (binary files are ignored).
* This setting applies at input time, when data is first read by Splunk software, such as on a forwarder that has configured inputs acquiring the data.

detect_trailing_nulls = [auto|true|false]
* When enabled, Splunk software tries to avoid reading in null bytes at the end of a file.
* When false, Splunk software assumes that all the bytes in the file should be read and indexed.
* Set this value to false for UTF-16 and other encodings (CHARSET) values that can have null bytes as part of the character text.
* Subtleties of 'true' vs 'auto':
  * 'true' is the historical behavior of trimming all null bytes when Splunk software runs on Windows.
  * 'auto' is currently a synonym for true but may be extended to be sensitive to the charset selected (i.e. quantized for multi-byte encodings, and disabled for unsafe variable-width encodings)
* This feature was introduced to work around programs which foolishly preallocate their log files with nulls and fill in data later. The well-known case is Internet Information Server.
* This setting applies at input time, when data is first read by Splunk software, such as on a forwarder that has configured inputs acquiring the data.
* Default (on *nix machines): false
* Default (on Windows machines): true

**Segmentation configuration**

SEGMENTATION = <segmenter>
* Specifies the segmenter from segmenters.conf to use at index time for the host, source, or sourcetype specified by <spec> in the stanza heading.
* Default: indexing
SEGMENTATION-<segment selection> = <segmenter>
* Specifies that Splunk Web should use the specific segmenter (from
  segmenters.conf) for the given <segment selection> choice.
* Default <segment selection> choices are: all, inner, outer, raw. For
  more
    information see the Admin Manual.
* Do not change the set of default <segment selection> choices, unless
  you
    have some overriding reason for doing so. In order for a changed set
    of
    <segment selection> choices to appear in Splunk Web, you need to edit
    the Splunk Web UI.

File checksum configuration

CHECK_METHOD = [endpoint_md5|entire_md5|modtime]
* Set CHECK_METHOD to "endpoint_md5" to have Splunk software perform a
  checksum
    of the first and last 256 bytes of a file. When it finds matches,
    Splunk
    software lists the file as already indexed and indexes only new data,
    or
    ignores it if there is no new data.
* Set CHECK_METHOD to "entire_md5" to use the checksum of the entire
  file.
* Set CHECK_METHOD to "modtime" to check only the modification time of
  the
  file.
* Settings other than "endpoint_md5" cause Splunk software to index the
  entire
  file for each detected change.
* This option is only valid for [source::<source>] stanzas.
* This setting applies at input time, when data is first read by Splunk
  software, such as on a forwarder that has configured inputs acquiring
  the
  data.
* Default: endpoint_md5

initCrcLength = <integer>
* See documentation in inputs.conf.spec.

Small file settings
PREFIX_SOURCETYPE = <boolean>
* NOTE: this setting is only relevant to the "[too_small]" sourcetype.
* Determines the source types that are given to files smaller than 100
  lines, and are therefore not classifiable.
* PREFIX_SOURCETYPE = false sets the source type to "too_small."
* PREFIX_SOURCETYPE = true sets the source type to
  "<sourcename>-too_small",
  where "<sourcename>" is a cleaned up version of the filename.
  * The advantage of PREFIX_SOURCETYPE = true is that not all small
    files
    are classified as the same source type, and wildcard searching is
    often
    effective.
* For example, a Splunk search of "sourcetype=access*" retrieves
  "access" files as well as "access-too_small" files.
* This setting applies at input time, when data is first read by Splunk
  software, such as on a forwarder that has configured inputs acquiring
  the
  data.
* Default: true

### Sourcetype configuration

sourcetype = <string>
* Can only be set for a [source::...:] stanza.
* Anything from that <source> is assigned the specified source type.
* Is used by file-based inputs, at input time (when accessing logfiles)
  such
  as on a forwarder, or indexer monitoring local files.
* sourcetype assignment settings on a system receiving forwarded Splunk
  data
  are not be applied to forwarded data.
* For log files read locally, data from log files matching <source> is
  assigned the specified source type.
* Default: empty string

# The following setting/value pairs can only be set for a stanza that
# begins with [<sourcetype>]:

rename = <string>
* Renames [<sourcetype>] as <string> at search time
* With renaming, you can search for the [<sourcetype>] with
  sourcetype=<string>
* To search for the original source type without renaming it, use the
  field _sourcetype.
* Data from a renamed sourcetype only uses the search-time
  configuration for the target sourcetype. Field extractions
invalid_cause = <string>
* Can only be set for a [<sourcetype>] stanza.
* If invalid_cause is set, the Tailing code (which handles uncompressed
  logfiles) does not read the data, but hands it off to other components
  or
  throws an error.
* Set <string> to "archive" to send the file to the archive processor
  (specified in unarchive_cmd).
* When set to "winevt", this causes the file to be handed off to the
  Event Log input processor.
* Set to any other string to throw an error in the splunkd.log if you
  are
  running Splunklogger in debug mode.
* This setting applies at input time, when data is first read by Splunk
  software, such as on a forwarder that has configured inputs acquiring
  the
  data.
* Default: empty string

is_valid = <boolean>
* Automatically set by invalid_cause.
* This setting applies at input time, when data is first read by Splunk
  software, such as on a forwarder that has configured inputs acquiring
  the
  data.
* DO NOT SET THIS.
* Default: true

force_local_processing = <boolean>
* Forces a universal forwarder to process all data tagged with this
  sourcetype
  locally before forwarding it to the indexers.
* Data with this sourcetype is processed by the linebreaker, aggerator,
  and the regexreplacement processors in addition to the
  existing
  utf8 processor.
* Note that switching this property potentially increases the cpu
  and memory consumption of the forwarder.
* Applicable only on a universal forwarder.
* Default: false

unarchive_cmd = <string>
* Only called if invalid_cause is set to "archive".
* This field is only valid on [source::<source>] stanzas.
* <string> specifies the shell command to run to extract an archived
  source.
* Must be a shell command that takes input on stdin and produces output
  on
  stdout.
Use _auto for Splunk software's automatic handling of archive files (tar, tar.gz, tgz, tbz, tbz2, zip)

This setting applies at input time, when data is first read by Splunk software, such as on a forwarder that has configured inputs acquiring the data.

Default: empty string

unarchive_sourcetype = <string>

Sets the source type of the contents of the matching archive file. Use this field instead of the sourcetype field to set the source type of archive files that have the following extensions: gz, bz, bz2, Z.

If this field is empty (for a matching archive file props lookup) Splunk software strips off the archive file's extension (.gz, bz etc) and lookup another stanza to attempt to determine the sourcetype.

This setting applies at input time, when data is first read by Splunk software, such as on a forwarder that has configured inputs acquiring the data.

Default: empty string

LEARN_SOURCETYPE = <boolean>

Determines whether learning of known or unknown sourcetypes is enabled.

For known sourcetypes, refer to LEARN_MODEL.

For unknown sourcetypes, refer to the rule:: and delayedrule:: configuration (see below).

Setting this field to false disables CHECK_FOR_HEADER as well (see above).

This setting applies at input time, when data is first read by Splunk software, such as on a forwarder that has configured inputs acquiring the data.

Default: true

LEARN_MODEL = <boolean>

For known source types, the file classifier adds a model file to the learned directory.

To disable this behavior for diverse source types (such as source code, where there is no good example to make a sourcetype) set LEARN_MODEL = false.

This setting applies at input time, when data is first read by Splunk software, such as on a forwarder that has configured inputs acquiring the data.

Default: true

maxDist = <integer>

484
* Determines how different a source type model may be from the current file.
* The larger the 'maxDist' value, the more forgiving Splunk software is with differences.
  * For example, if the value is very small (for example, 10), then files
    of the specified sourcetype should not vary much.
  * A larger value indicates that files of the given source type can vary
    quite a bit.
* If you're finding that a source type model is matching too broadly, reduce
  its 'maxDist' value by about 100 and try again. If you're finding that a
  source type model is being too restrictive, increase its 'maxDist
  value by
  about 100 and try again.
* This setting applies at input time, when data is first read by Splunk
  software, such as on a forwarder that has configured inputs acquiring
  the data.
* Default: 300

# rule:: and delayedrule:: configuration

MORE_THAN<optional_unique_value>_<number> = <regular expression>
(empty)
LESS_THAN<optional_unique_value>_<number> = <regular expression>
(empty)

* This setting applies at input time, when data is first read by Splunk
  software, such as on a forwarder that has configured inputs acquiring
  the data.

An example:

```
[rule::bar_some]
sourcetype = source_with_lots_of_bars
  # if more than 80% of lines have "----", but fewer than 70% have
  "####"
  # declare this a "source_with_lots_of_bars"
MORE_THAN_80 = ----
LESS_THAN_70 = ####
```

A rule can have many MORE_THAN and LESS_THAN patterns, and all are
required
for the rule to match.
**Annotation Processor configured**

ANNOTATE_PUNCT = <boolean>
* Determines whether to index a special token starting with "punct::"
  * The "punct::" key contains punctuation in the text of the event.
    It can be useful for finding similar events
  * If it is not useful for your dataset, or if it ends up taking too much space in your index it is safe to disable it
  * Default: true

**Header Processor configuration**

HEADER_MODE = <empty> | always | firstline | none
* Determines whether to use the inline ***SPLUNK*** directive to rewrite index-time fields.
  * If "always", any line with ***SPLUNK*** can be used to rewrite index-time fields.
  * If "firstline", only the first line can be used to rewrite index-time fields.
  * If "none", the string ***SPLUNK*** is treated as normal data.
  * If <empty>, scripted inputs take the value "always" and file inputs take the value "none".
  * This setting applies at input time, when data is first read by Splunk software, such as on a forwarder that has configured inputs acquiring the data.
  * Default: <empty>

**Internal settings**

# NOT YOURS. DO NOT SET.

__actions = <string>
* Internal field used for user-interface control of objects.
  * Default: "new,edit,delete".

pulldown_type = <boolean>
* Internal field used for user-interface control of source types.
  * Default: empty

given_type = <string>
* Internal field used by the CHECK_FOR_HEADER feature to remember the
original sourcetype.
* This setting applies at input time, when data is first read by Splunk
  software, such as on a forwarder that has configured inputs acquiring
  the
  data.
* Default: not set

**Sourcetype Category and Descriptions**

description = <string>
* Field used to describe the sourcetype. Does not affect indexing
  behavior.
  * Default: not set

category = <string>
* Field used to classify sourcetypes for organization in the front end.
  Case
  sensitive. Does not affect indexing behavior.
  * Default: not set

**props.conf.example**

# Version 7.3.0
#
# The following are example props.conf configurations. Configure
# properties for
# your data.
#
# To use one or more of these configurations, copy the configuration
# block into
# props.conf in $SPLUNK_HOME/etc/system/local/. You must restart Splunk
to
# enable configurations.
#
# To learn more about configuration files (including precedence) please
# see the
# documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

########
# Line merging settings
########
# The following example line-merges source data into multi-line events for
# apache_error sourcetype.

[apache_error]
SHOULD_LINEMERGE = True

########
# Settings for tuning
########

# The following example limits the amount of characters indexed per event from
# host::small_events.

[host::small_events]
TRUNCATE = 256

# The following example turns off DATETIME_CONFIG (which can speed up indexing)
# from any path that ends in /mylogs/*.log.
# In addition, the default splunk behavior of finding event boundaries via per-event timestamps can't work with NONE, so we disable
# SHOULD_LINEMERGE, essentially declaring that all events in this file are
# single-line.

[source:.../mylogs/*.log]
DATETIME_CONFIG = NONE
SHOULD_LINEMERGE = false

########
# Timestamp extraction configuration
########

# The following example sets Eastern Time Zone if host matches nyc*.

[host::nyc*]
TZ = US/Eastern

# The following example uses a custom datetime.xml that has been created and
# placed in a custom app directory. This sets all events coming in from hosts
# starting with dharma to use this custom file.
[host::dharma*]
DATETIME_CONFIG = <etc/apps/custom_time/datetime.xml>

########
## Timezone alias configuration
########

# The following example uses a custom alias to disambiguate the Australian
# meanings of EST/EDT
TZ_ALIAS = EST=GMT+10:00,EDT=GMT+11:00

# The following example gives a sample case wherein, one timezone field is
# being replaced by/interpreted as another.
TZ_ALIAS = EST=AEST,EDT=AEDT

########
# Transform configuration
########

# The following example creates a search field for host::foo if tied to a
# stanza in transforms.conf.
[host::foo]
TRANSFORMS-foo=foobar

# The following stanza extracts an ip address from _raw
[my_sourcetype]
EXTRACT-extract_ip = {(?<ip>\d{1,3}\./\d{1,3}\./\d{1,3}\./\d{1,3})}

# The following example shows how to configure lookup tables
[my_lookuptype]
LOOKUP-foo = mylookuptable userid AS myuserid OUTPUT username AS myusername

# The following shows how to specify field aliases
FIELDALIAS-foo = user AS myuser id AS myid

########
# Sourcetype configuration
########

# The following example sets a sourcetype for the file web_access.log
for a
# unix path.
[source::.../web_access.log]
sourcetype = splunk_web_access

# The following example sets a sourcetype for the Windows file iis6.log.
# Note:
# Backslashes within Windows file paths must be escaped.
[source::...\iis\iis6.log]
sourcetype = iis_access

# The following example extracts syslog events.
[syslog]
invalid_cause = archive
unarchive_cmd = gzip -cd -

# The following example learns a custom sourcetype and limits the range between
# different examples with a smaller than default maxDist.
[custom_sourcetype]
LEARN_MODEL = true
maxDist = 30

# rule:: and delayedrule:: configuration
# The following examples create sourcetype rules for custom sourcetypes with
# regex.

[rule::bar_some]
sourcetype = source_with_lots_of_bars
MORE_THAN_80 = ----

[delayedrule::baz_some]
sourcetype = my_sourcetype
LESS_THAN_70 = ####

#######
# File configuration
#######

# Binary file configuration
# The following example eats binary files from the sourcetype
# "imported_records".
[imported_records]
NO_BINARY_CHECK = true
# File checksum configuration
# The following example checks the entirety of every file in the
web_access
directory rather than skipping files that appear to be the same.

[source::.../web_access/*]
CHECK_METHOD = entire_md5

########
# Metric configuration
########

# A metric sourcetype of type statsd with 'regex_stanza1',
'regex_stanza2' to
# extract dimensions
[metric_sourcetype_name]
METRICS_PROTOCOL = statsd
STATSD-DIM-TRANSFORMS = regex_stanza1, regex_stanza2

#Convert a single log event into multiple metrics using
METRIC-SCHEMA-TRANSFORMS
#and index time extraction feature.
[logtometrics]
METRIC-SCHEMA-TRANSFORMS = metric-schema:logtometrics
TRANSFORMS-group = extract_group
TRANSFORMS-name = extract_name
TRANSFORMS-max_size_kb = extract_max_size_kb
TRANSFORMS-current_size_kb = extract_current_size_kb
TRANSFORMS-current_size = extract_current_size
TRANSFORMS-largest_size = extract_largest_size
TRANSFORMS-smallest_size = extract_smallest_size
category = metrics
should_linemerge = false

restmap.conf

The following are the spec and example files for restmap.conf.

restmap.conf.spec

# Version 7.3.0
#
# This file contains possible attribute and value pairs for creating new
# Representational State Transfer (REST) endpoints.
#
# There is a restmap.conf in $SPLUNK_HOME/etc/system/default/. To set custom
# configurations, place a restmap.conf in
# $SPLUNK_HOME/etc/system/local/. For
# help, see restmap.conf.example. You must restart Splunk to enable
# configurations.
#
# To learn more about configuration files (including precedence) please
# see the
# documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
#
# NOTE: You must register every REST endpoint via this file to make it
# available.
#
# Global stanza
#
[global]
* This stanza sets global configurations for all REST endpoints.
* Follow this stanza name with any number of the following
  attribute/value
  pairs.

allowGetAuth=[true|false]
* Allow user/password to be passed as a GET parameter to endpoint
  services/auth/login.
* Setting this to true, while convenient, may result in user/password
  getting
  logged as cleartext in Splunk's logs *and* any proxy servers in
  between.
* Defaults to false.

allowRestReplay=[true|false]
* POST/PUT/DELETE requests can be replayed on other nodes in the
  deployment.
* This enables centralized management.
* Turn on or off this feature. You can also control replay at each
  endpoint
  level. This feature is currently INTERNAL and should not be turned on
  without
  consulting splunk support.
* Defaults to false

defaultRestReplayStanza=<string>
* Points to global rest replay configuration stanza.
* Related to allowRestReplay
* Defaults to "restreplayshc"

pythonHandlerPath=<path>
* Path to 'main' python script handler.
* Used by the script handler to determine where the actual 'main' script
  is
located.
* Typically, you should not need to change this.
* Defaults to $SPLUNK_HOME/bin/rest_handler.py.

#############################
# Applicable to all REST stanzas
# Stanza definitions below may supply additional information for these.
#

[
    <rest endpoint name>:<endpoint description string>]
match=<path>
* Specify the URI that calls the handler.
* For example if match=/foo, then https://$SERVER:$PORT/services/foo
    calls this
    handler.
* NOTE: You must start your path with a /.

requireAuthentication=[true|false]
* This optional attribute determines if this endpoint requires
    authentication.
* Defaults to 'true'.

authKeyStanza=<stanza>
* This optional attribute determines the location of the pass4SymmKey in
    the
    server.conf to be used for endpoint authentication.
* Defaults to 'general' stanza.
* Only applicable if the requireAuthentication is set true.

restReplay=[true|false]
* This optional attribute enables rest replay on this endpoint group
* Related to allowRestReplay
* This feature is currently INTERNAL and should not be turned on without
    consulting
    splunk support.
* Defaults to false

restReplayStanza=<string>
* This points to stanza which can override the
    [global]/defaultRestReplayStanza
    value on a per endpoint/regex basis
* Defaults to empty

capability=<capabilityName>
capability.<post|delete|get|put>=<capabilityName>
* Depending on the HTTP method, check capabilities on the authenticated
    session user.
* If you use 'capability.post|delete|get|put,' then the associated
    method is
    checked against the authenticated user's role.
* If you just use 'capability,' then all calls get checked against this
    capability (regardless of the HTTP method).
* Capabilities can also be expressed as a boolean expression. Supported operators
  include: or, and, ()

acceptFrom=<network_acl> ...
* Lists a set of networks or addresses to allow this endpoint to be accessed
  from.
* This shouldn't be confused with the setting of the same name in the
  [httpServer] stanza of server.conf which controls whether a host can
  make HTTP requests at all
* Each rule can be in the following forms:
  1. A single IPv4 or IPv6 address (examples: "10.1.2.3", "fe80::4a3")
  2. A CIDR block of addresses (examples: "10/8", "fe80:1234/32")
  3. A DNS name, possibly with a '*' used as a wildcard (examples:
     "myhost.example.com", "*.splunk.com")
  4. A single '*' which matches anything
* Entries can also be prefixed with '!' to cause the rule to reject the
  connection. Rules are applied in order, and the first one to match is
  used. For example, "!10.1/16, *" will allow connections from
  everywhere except the 10.1.*.* network.
* Defaults to "*" (accept from anywhere)

includeInAccessLog=[true|false]
* If this is set to false, requests to this endpoint will not appear
  in splunkd_access.log
* Defaults to 'true'.

########################################################################
# Per-endpoint stanza
# Specify a handler and other handler-specific settings.
# The handler is responsible for implementing arbitrary namespace
# underneath
# each REST endpoint.

[script:<uniqueName>]
* NOTE: The uniqueName must be different for each handler.
* Call the specified handler when executing this endpoint.
* The following attribute/value pairs support the script handler.

scripttype=python
* Tell the system what type of script to execute when using this
  endpoint.
* Defaults to python.
* If set to "persist" it will run the script via a persistent-process
  that
    uses the protocol from persistconn/appserver.py.

handler=<SCRIPT>.<CLASSNAME>
* The name and class name of the file to execute.
* The file *must* live in an application's bin subdirectory.
* For example, `$SPLUNK_HOME/etc/apps/<APPNAME>/bin/TestHandler.py` has a class
called MyHandler (which, in the case of python must be derived from a base
class called 'splunk.rest.BaseRestHandler'). The tag/value pair for this is:
"handler=TestHandler.MyHandler".

xsl=<path to XSL transform file>
* Optional.
* Perform an optional XSL transform on data returned from the handler.
* Only use this if the data is XML.
* Does not apply to scripttype=persist.

script=<path to a script executable>
* For scripttype=python this is optional. It allows you to run a script which is *not* derived from 'splunk.rest.BaseRestHandler'. This is rarely used. Do not use this unless you know what you are doing.
* For scripttype=persist this is the path with is sent to the driver to execute. In that case, environment variables are substituted.

script.arg.<N>=<string>
* Only has effect for scripttype=persist.
* List of arguments which are passed to the driver to start the script.
* The script can make use of this information however it wants.
* Environment variables are substituted.

script.param=<string>
* Optional.
* Only has effect for scripttype=persist.
* Free-form argument that is passed to the driver when it starts the script.
* The script can make use of this information however it wants.
* Environment variables are substituted.

output_modes=<csv list>
* Specifies which output formats can be requested from this endpoint.
* Valid values are: json, xml.
* Defaults to xml.

passSystemAuth=<bool>
* Specifies whether or not to pass in a system-level authentication token on each request.
* Defaults to false.

driver=<path>
* For scripttype=persist, specifies the command to start a persistent server for this process.
* Endpoints that share the same driver configuration can share processes.
* Environment variables are substituted.
* Defaults to using the persistconn/appserver.py server.

driver.arg.<n> = <string>
* For scripttype=persist, specifies the command to start a persistent server for this process.
* Environment variables are substituted.
* Only takes effect when "driver" is specifically set.

driver.env.<name>=<value>
* For scripttype=persist, specifies an environment variable to set when running the driver process.

passConf=<bool>
* If set, the script is sent the contents of this configuration stanza as part of the request.
* Only has effect for scripttype=persist.
* Defaults to true.

passPayload=[true | false | base64]
* If set to true, sends the driver the raw, unparsed body of the POST/PUT as a "payload" string.
* If set to "base64", the same body is instead base64-encoded and sent as a "payload_base64" string.
* Only has effect for scripttype=persist.
* Defaults to false.

passSession=<bool>
* If set to true, sends the driver information about the user's session. This includes the user's name, an active authtoken, and other details.
* Only has effect for scripttype=persist.
* Defaults to true.

passHttpHeaders=<bool>
* If set to true, sends the driver the HTTP headers of the request.
* Only has effect for scripttype=persist.
* Defaults to false.

passHttpCookies=<bool>
* If set to true, sends the driver the HTTP cookies of the request.
* Only has effect for scripttype=persist.
* Defaults to false.

#############################
# 'admin'
# The built-in handler for the Extensible Administration Interface.
# Exposes the listed EAI handlers at the given URL.
#
[admin:<uniqueName>]
match=<partial URL>
* URL which, when accessed, will display the handlers listed below.

members=<csv list>
* List of handlers to expose at this URL.
* See https://localhost:8089/services/admin for a list of all possible handlers.

# 'admin_external'
# Register Python handlers for the Extensible Administration Interface.
# Handler will be exposed via its "uniqueName".
#

[admin_external:<uniqueName>]

handlertype=<script type>
* Currently only the value 'python' is valid.

handlerfile=<unique filename>
* Script to execute.
* For bin/myAwesomeAppHandler.py, specify only myAwesomeAppHandler.py.

handlerpersistentmode=[true|false]
* Set to true to run the script in persistent mode and keep the process running between requests.

handleractions=<comma separated list>
* List of EAI actions supported by this handler.
* Valid values are: create, edit, list, delete, _reload.

# Validation stanzas
# Add stanzas using the following definition to add arg validation to the appropriate EAI handlers.

[validation:<handler-name>]

<field> = <validation-rule>
* <field> is the name of the field whose value would be validated when an object is being saved.
* <validation-rule> is an eval expression using the validate() function to evaluate arg correctness and return an error message. If you use a boolean returning function, a generic message is displayed.
* <handler-name> is the name of the REST endpoint which this stanza applies to
  handler-name is what is used to access the handler via
/servicesNS/</user>/<app/admin/<handler-name>.
* For example:
  action.email.sendresult = validate(isbool('action.email.sendresults'), "'action.email.sendresults' must be a boolean value").
* NOTE: use ' or $ to enclose field names that contain non alphanumeric characters.

#############################
# 'eai'
# Settings to alter the behavior of EAI handlers in various ways.
# These should not need to be edited by users.
#
[eai:<EAI handler name>]

showInDirSvc = [true|false]
* Whether configurations managed by this handler should be enumerated via the
directory service, used by SplunkWeb's "All Configurations" management page.
  Defaults to false.
desc = <human readable string>
* Allows for renaming the configuration type of these objects when enumerated
  via the directory service.

#############################
# Miscellaneous
# The un-described parameters in these stanzas all operate according to the
# descriptions listed under "script:", above.
# These should not need to be edited by users - they are here only to quiet
# down the configuration checker.
#
[input:...]
dynamic = [true|false]
* If set to true, listen on the socket for data.
* If false, data is contained within the request body.
* Defaults to false.

[peerupload:...]
path = <directory path>
* Path to search through to find configuration bundles from search peers.
untar = [true|false]
* Whether or not a file should be untarred once the transfer is
[restreplayshc]
methods = <comma separated strings>
* REST methods which will be replayed. POST, PUT, DELETE, HEAD, GET are the available options

nodelists = <comma separated string>
* strategies for replay. Allowed values are shc, nodes, filternodes
  * shc - replay to all other nodes in Search Head Cluster
  * nodes - provide raw comma separated URIs in nodes variable
  * filternodes - filter out specific nodes. Always applied after other strategies

nodes = <comma separated management uris>
* list of specific nodes that you want the REST call to be replayed to

filternodes = <comma separated management uris>
* list of specific nodes that you do not want the REST call to be replayed to

[proxy:appsbrowser]
destination = <splunkbaseAPIURL>
* protocol, subdomain, domain, port, and path of the splunkbase api used to browse apps
  * Defaults to https://splunkbase.splunk.com/api

restmap.conf.example

# Version 7.3.0
#
# This file contains example REST endpoint configurations.
#
# To use one or more of these configurations, copy the configuration block into
# restmap.conf in $SPLUNK_HOME/etc/system/local/. You must restart Splunk to
# enable configurations.
#
# To learn more about configuration files (including precedence) please see the
# documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

# The following are default REST configurations. To create your own
endpoints,
# modify the values by following the spec outlined in restmap.conf.spec.

#
/////////////////////////////////////////////////////////////////////////
#  global settings
#
/////////////////////////////////////////////////////////////////////////

[global]

# indicates if auths are allowed via GET params
allowGetAuth=false

#The default handler (assuming that we have PYTHONPATH set)
pythonHandlerPath=$SPLUNK_HOME/bin/rest_handler.py

#
/////////////////////////////////////////////////////////////////////////
#  internal C++ handlers
# NOTE: These are internal Splunk-created endpoints. 3rd party
developers can
# only use script or search can be used as handlers.
# (Please see restmap.conf.spec for help with configurations.)
#
/////////////////////////////////////////////////////////////////////////

[SBA:sba]
match=/properties
capability=get_property_map

[asyncsearch:asyncsearch]
match=/search
capability=search

[indexing-preview:indexing-preview]
match=/indexing/preview
capability=(edit_monitor or edit_sourcetypes) and (edit_user and
edit_tcp)

savedsearches.conf

The following are the spec and example files for savedsearches.conf.
# This file contains possible attribute/value pairs for saved search entries in
# savedsearches.conf. You can configure saved searches by creating your own
# savedsearches.conf.
# There is a default savedsearches.conf in
#$SPLUNK_HOME/etc/apps/SA-ITOA/default. To
# set custom configurations, place a savedsearches.conf in
#$SPLUNK_HOME/etc/apps/SA-ITOA/local/. For examples, see
# savedsearches.conf.example. You must restart Splunk to enable configurations.
# To learn more about configuration files (including precedence) please see the
# documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

**Ping**

action.itsi_sample_event_action_ping.param.host = <string>
* Field in the event indicating the host to ping.
* Required. If no value is provided, no host will be pinged.
* Set to $result.host$ or $result.server$ etc...

**Event generator settings**

action.itsi_event_generator = <boolean>
* Whether the alert is enabled.

action.itsi_event_generator.param.title = <string>
* The title of the notable event in Episode Review.
* Optional. If title is not provided then the search name becomes the title.

action.itsi_event_generator.param.description = <string>
* A description of the notable event.
* Optional. If a description is not provided then the search description becomes the event description.

action.itsi_event_generator.param.owner = <string>
* The initial owner of the notable event.
Optional. If an owner is not provided then default_owner is assigned.

action.itsi_event_generator.param.status = <string>
* The triage status of the event in Episode Review.
* Values must match an integer specified in the default version of itsi_notable_event_status.conf (or the local version if you created one).
* Optional. If a status is not provided then default_status is assigned.

action.itsi_event_generator.param.severity = <string>
* The level of importance of the event.
* Values must match an integer specified in the default version of itsi_notable_event_severity.conf (or the local version if you created one).
* Optional. If a severity is not provided then default_severity is assigned.

action.itsi_event_generator.param.drilldown_search_title = <string>
* You can drill down to a specific Splunk search from an event or episode.
* The name of the drilldown search link.
* Optional.

action.itsi_event_generator.param.drilldown_search_search= <string>
* The drilldown search string.
* Optional.

action.itsi_event_generator.param.drilldown_search_latest_offset = <seconds>
* Defines how far ahead from the time of the event, in seconds, to look for related events.
* This offset is added to the event time.
* Optional.

action.itsi_event_generator.param.drilldown_search_earliest_offset = <string>
* Defines how far back from the time of the event, in seconds, to start looking for related events.
* This offset is subtracted from the event time.
* Optional.

action.itsi_event_generator.param.drilldown_title = <string>
* You can drill down to a specific website from an event or episode.
* The name of the drilldown website link.
* Optional.

action.itsi_event_generator.param.drilldown_uri = <string>
* The URI of the website you drill down to.
* Optional.

action.itsi_event_generator.param.event_identifier_fields = <comma-separated list>
* A list of fields used to identify if a notable event is unique.
  * Optional.
  * This setting is useful for identifying if a given notable event is already present.
  * ITSI usually builds a hash using this set of fields.

```python
action.itsi_event_generator.param.service_ids = <comma-separated list>
```
* A list of service IDs representing one or more ITSI services to which this correlation search applies.
  * Optional.

```python
action.itsi_event_generator.param.entity_lookup_field = <string>
```
* The field in the data retrieved by the correlation search that is used to look up corresponding entities. For example, host.
  * Optional.

```python
action.itsi_event_generator.param.search_type = <string>
```
* The search type.
  * Optional.
  * Default: custom

```python
action.itsi_event_generator.param.meta_data = <string>
```
* The search type of any stored metadata.
  * Optional.

```python
action.itsi_event_generator.param.is_ad_at = <boolean>
```
* Whether this correlation is created by enabling adaptive thresholding or anomaly detection (AT/AD) for KPIs or services.
  * Optional.
  * If "1", the correlation is created by AT/AD.
  * If "0", the correlation is not created by AT/AD.

```python
action.itsi_event_generator.param.ad_at_kpi_ids = <comma-separated list>
```
* A list of KPIs where AT/AD is enabled.
  * Optional.

**savedsearches.conf.example**

```python
# This is an example savedsearches.conf. Use this file to configure saved searches.
# To use one or more of these configurations, copy the configuration block
# into savedsearches.conf in $SPLUNK_HOME/etc/apps/SA-ITOA/local. 
# You must restart Splunk to enable configurations.
# To learn more about configuration files (including precedence) please see
```

503
# the documentation located at
#
http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

[Test ITSI Reporting Search]

cron_schedule                      = */5 * * * *
disabled                           = False
dispatch.earliest_time             = -5m
dispatch.latest_time               = now
enableSched                        = True
search                             = | stats count | eval demo="Demo Search" | fields - count

action.itsi_event_generator = 1

action.itsi_event_generator.param.title = "Host $result.host$ is down"
action.itsi_event_generator.param.description = Test if host $result.host$ is down or not
action.itsi_event_generator.param.owner = admin
action.itsi_event_generator.param.status = 1
action.itsi_event_generator.param.severity = 2
action.itsi_event_generator.param.drilldown_search_title = Raw search of seeing $result.host$ events
action.itsi_event_generator.param.drilldown_search_search= index=_internal host="$result.host$"

action.itsi_event_generator.param.drilldown_search_latest_offset = 30
action.itsi_event_generator.param.drilldown_search_earliest_offset = -30
action.itsi_event_generator.param.drilldown_title = Go to deep dive "$result.sourcetype$"
action.itsi_event_generator.param.drilldown_uri = "/en-US/app/itsi/search/"

[Test ITSI Notable Event Search]

cron_schedule                      = */5 * * * *
disabled                           = False
dispatch.earliest_time             = -5m
dispatch.latest_time               = now
enableSched                        = True
search                             = index=_internal | head 4
alert.digest_mode = 0

action.itsi_event_generator = 1

action.itsi_event_generator.param.title = "Host $result.host$ is down"

action.itsi_event_generator.param.description = Test if host $result.host$ is down or not

action.itsi_event_generator.param.owner = admin

action.itsi_event_generator.param.status = 1

action.itsi_event_generator.param.severity = 2

action.itsi_event_generator.param.drilldown_search_title = Raw search of seeing $result.host$ events

action.itsi_event_generator.param.drilldown_search_search = index=_internal host=$result.host$

action.itsi_event_generator.param.drilldown_search_latest_offset = 30

action.itsi_event_generator.param.drilldown_search_earliest_offset = -30

action.itsi_event_generator.param.drilldown_title = Go to deep dive "$result.sourcetype$"

action.itsi_event_generator.param.drilldown_uri = "/en-US/app/itsi/search/"

searchbnf.conf

The following are the spec and example files for searchbnf.conf.

searchbnf.conf.spec

# Version 7.3.0
#
#
# This file contain descriptions of stanzas and attribute/value pairs for
# configuring search-assistant via searchbnf.conf
#
# There is a searchbnf.conf in $SPLUNK_HOME/etc/system/default/. It should
# not be modified. If your application has its own custom python search
# commands, your application can include its own searchbnf.conf to describe
# the commands to the search-assistant.
# To learn more about configuration files (including precedence) please see
# the documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

**GLOBAL SETTINGS**

# Use the [default] stanza to define any global settings.
# * You can also define global settings outside of any stanza, at the top
#   of the file.
# * Each conf file should have at most one default stanza. If there are
#   multiple default stanzas, attributes are combined. In the case of
#   multiple definitions of the same attribute, the last definition in
#   the file wins.
# * If an attribute is defined at both the global level and in a
#   specific stanza, the value in the specific stanza takes precedence.

**[<search-commandname>-command]**

* This stanza enables properties for a given <search-command>.
* A searchbnf.conf file can contain multiple stanzas for any number of
  commands. * Follow this stanza name with any number of the following
  attribute/value pairs.
* If you do not set an attribute for a given <spec>, the default is
  used.
  The default values are empty.
* An example stanza name might be "geocode-command", for a "geocode"
  command.
* Search command stanzas can refer to definitions defined in others
  stanzas,
  and they do not require "-command", appended to them. For example:

**[geocode-command]**

    syntax = geocode <geocode-option>*

...
[geocode-option]

syntax = (maxcount=<int>) | (maxhops=<int>)
...

#*****************************************************************************
# The possible attributes/value pairs for searchbnf.conf
#*****************************************************************************
syntax = <string>
* Describes the syntax of the search command. See the head of
  searchbnf.conf for details.
  * Required

simplesyntax = <string>

* Optional simpler version of the syntax to make it easier to
  understand at the expense of completeness. Typically it removes
  rarely used options or alternate ways of saying the same thing.
  * For example, a search command might accept values such as
  "m|min|mins|minute|minutes", but that would unnecessarily
  clutter the syntax description for the user. In this case, the
  simplesyntax can just pick the one (e.g., "minute").

alias = <commands list>
* Alternative names for the search command. This further cleans
  up the syntax so the user does not have to know that
  'savedsearch' can also be called by 'macro' or 'savedsplunk'.

description = <string>
* Detailed text description of search command. Description can continue
  on
  the next line if the line ends in "\"
  * Required

shortdesc = <string>
* A short description of the search command. The full DESCRIPTION
  may take up too much screen real-estate for the search assistant.
  * Required

e.example<index> = <string>

comment<index> = <string>
* 'example' should list out a helpful example of using the search
  command, and 'comment' should describe that example.
* 'example' and 'comment' can be appended with matching indexes to
  allow multiple examples and corresponding comments.
  * For example:
      example2 = geocode maxcount=4
command2 = run geocode on up to four values
example3 = geocode maxcount=-1
comment3 = run geocode on all values

usage = public|private|deprecated
* Determines if a command is public, private, depreciated. The search assistant only operates on public commands.
* Required

tags = <tags list>
* List of tags that describe this search command. Used to find commands when the use enters a synonym (e.g. "graph" -> "chart")

related = <commands list>
* List of related commands to help user when using one command to learn about others.

#****************************************************************************
# Optional attributes primarily used internally at Splunk
#***************************************************************************

appears-in = <string>
category = <string>
maintainer = <string>
note = <string>
optout-in = <string>
supports-multivalue = <string>

# searchbnf.conf.example

# Version 7.3.0
#
# The following are example stanzas for searchbnf.conf configurations.
#

##################
# selfjoin
##################
[selfjoin-command]
syntax = selfjoin (<selfjoin-options>)* <field-list>
shortdesc = Join results with itself.
description = Join results with itself. Must specify at least one field to join on.
usage = public
example1 = selfjoin id
comment1 = Joins results with itself on 'id' field.
related = join
tags = join combine unite
[selfjoin-options]
syntax = overwrite=<bool> | max=<int> | keepsingle=<int>
description = The selfjoin joins each result with other results that have the same value for the join fields. 'overwrite' controls if fields from these 'other' results should overwrite fields of the result used as the basis for the join (default=true). max indicates the maximum number of 'other' results each main result can join with. (default = 1, 0 means no limit). 'keepsingle' controls whether or not results with a unique value for the join fields (and thus no other results to join with) should be retained. (default = false)

**service_analyzer_settings.conf**

The following are the spec and example files for service_analyzer_settings.conf.

**service_analyzer_settings.conf.spec**

```plaintext
# This file contains a setting for determining whether or not to always display the First Time Run modal in the Service Analyzer.
# To set custom configurations, place a service_analyzer_settings.conf in $SPLUNK_HOME/etc/apps/itsi/local/. You must restart Splunk to enable configurations.
# To learn more about configuration files (including precedence) please see the documentation located at
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles

[settings]

ftr_override = [0|1]
* Whether or not to always display the First Time Run (FTR) modal in the Service Analyzer.
* If "1", every time you navigate to the Service Analyzer, the First Time Run modal is displayed.
* If "0", the behavior defaults to showing the FTR modal only when services are not present.
* Default: 0 (false)

show_cycles_warning = [0|1]
* Whether to display a warning banner on the Service Analyzer
```
when there are one or more cyclic dependencies in the service topology.

* After the warning is ignored in the UI, this flag is set to "0" and the warning is never shown again unless manually changed.
* If "1", every time a cyclic dependency exists, a warning banner appears on the Service Analyzer.
* If "0", the banner never appears on the Service Analyzer.
* Default: 1 (true)

**service_analyzer_settings.conf.example**

No example

**threshold_labels.conf**

The following are the spec and example files for `threshold_labels.conf`.

**threshold_labels.conf.spec**

```plaintext
# Copyright (C) 2005-2019 Splunk Inc. All Rights Reserved.
#
# This file contains all possible attribute/value pairs for configuring settings
# for severity-level thresholds. Use this file to configure
# threshold names and color mappings.
#
# To map threshold names and colors, place a threshold_label.conf in
# $SPLUNK_HOME/etc/apps/itsi/local/. For examples, see
# threshold_label.conf.example.
#
# To learn more about configuration files (including precedence) see the
documentation
# located at
http://www.splunk.com/base/Documentation/latest/Admin/Aboutconfigurationfiles
#
# CAUTION: You can drastically affect your Splunk installation by changing
# any settings in
# this file other than the colors. Consult technical support
(http://www.splunk.com/page/submit_issue)
# if you are not sure how to configure this file.

[<name>]

color = <string>
* A valid color code.
```
lightcolor = <string>
* A valid color code to display for Episode Review "prominent mode".
* When you view Episode Review in prominent mode, the entire row is colored
  rather than just the colored band on the side.
* Required.

threshold_level = <integer>
* A threshold level that is used to create an ordered list of the labels.
* For example, if you set the 'Normal' threshold level to "1", it appears
  first when the levels are listed in the UI.
* Optional.

health_weight = <integer>
* The weight or importance of this status.
* This value should be between 0 and 1.
* In general, regular levels like Normal and Critical have a weight of
  "1", while
  less important levels like Maintenance and Info have a weight of "0".
* Required.

health_min = <integer>
* The minimum threshold value.
* This value must be a number between 0 and 100. 0 and 100 are inclusive
  but
  the minimum threshold value is exclusive.
* Required.

health_max = <integer>
* The maximum threshold value.
* This value must be a number between 0 and 100. 0 and 100 are inclusive
  but
  the maximum threshold value is exclusive.
* Required.

score_contribution = <integer>
* The number, traditionally from 0 to 100, that this particular level will
  contribute towards health score calculations.
* Required.

threshold_labels.conf.example

# Copyright (C) 2005-2019 Splunk Inc. All Rights Reserved.
# This is an example threshold_labels.conf. Use this file to
# configure settings for severity-level thresholds.
#
# To use one or more of these configurations, copy the color code
# into threshold_labels.conf in $SPLUNK_HOME/etc/apps/itsi/local.
# You must restart Splunk to enable configurations.
#
# To learn more about configuration files (including precedence) please
# see
# the documentation located at
#
# http://docs.splunk.com/Documentation/ITSI/latest/Configure/ListofITSIconfigurationfiles
#
# This example alert includes showing raw events at selected time
# buckets,
# showing raw events from a displayed time range, showing KPI events for
# a host, and showing all events for a host.
#
# This file contains examples of brighter severity colors, with "Normal"
# severity
# being replaced with "Low" severity.

[info]
color = #6AB7C7
threshold_level = 1

[low]
color = #65A637
threshold_level = 2

[medium]
color = #FAC51C
threshold_level = 3

[high]
color = #F7902B
threshold_level = 4

[critical]
color = #D85D3C
threshold_level = 5

**threshold_periods.conf**

The following are the spec and example files for **threshold_periods.conf**.

**threshold_periods.conf.spec**

# threshold_periods.conf is DEPRECATED and should not be edited.
[<threshold-period-number>]

color = <value>
* Label for how far in the past.

description=<value>
* The description.

relative=<value>
* Relative time range.

**threshold_periods.conf.example**

No example

**transforms.conf**

The following are the spec and example files for **transforms.conf**.

**transforms.conf.spec**

```plaintext
#   Version 7.3.0
#
# This file contains settings and values that you can use to configure
# data transformations.
#
# Transforms.conf is commonly used for:
# * Configuring host and source type overrides that are based on regular
#   expressions.
# * Anonymizing certain types of sensitive incoming data, such as credit
#   card or social security numbers.
# * Routing specific events to a particular index, when you have
#   multiple
#   indexes.
# * Creating new index-time field extractions. NOTE: We do not recommend
#   adding to the set of fields that are extracted at index time unless
#   it
#   is absolutely necessary because there are negative performance
#   implications.
# * Creating advanced search-time field extractions that involve one or
#   more
#   of the following:
# * Reuse of the same field-extracting regular expression across
#   multiple
#   sources, source types, or hosts.
```

513
# * Application of more than one regular expression to the same source,
#     source type, or host.
# * Using a regular expression to extract one or more values from the values
#     of another field.
# * Delimiter-based field extractions, such as extractions where the field-value pairs are separated by commas, colons, semicolons, bars, or something similar.
# * Extraction of multiple values for the same field.
# * Extraction of fields with names that begin with numbers or underscores.
# * NOTE: Less complex search-time field extractions can be set up entirely in props.conf.
# * Setting up lookup tables that look up fields from external sources.

# All of the above actions require corresponding settings in props.conf.
# You can find more information on these topics by searching the Splunk documentation (http://docs.splunk.com/Documentation).

# There is a transforms.conf file in $SPLUNK_HOME/etc/system/default/.
To set custom configurations, place a transforms.conf file in $SPLUNK_HOME/etc/system/local/.
# For examples of transforms.conf configurations, see the transforms.conf.example file.

# You can enable configuration changes made to transforms.conf by running this search in Splunk Web:
# | extract reload=t
#
# To learn more about configuration files (including precedence) please see the documentation located at http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
# You can also define global settings outside of any stanza, at the top of the file.
* Each conf file should have at most one default stanza. If there are multiple default stanzas, settings are combined. In the case of multiple definitions of the same setting, the last definition in the file wins.
* If a setting is defined at both the global level and in a specific stanza, the value in the specific stanza takes precedence.

[<unique_transform_stanza_name>]
* Name your stanza. Use this name when you configure field extractions, lookup tables, and event routing in props.conf. For example, if you are setting up an advanced search-time field extraction, in props.conf you would add REPORT-<class> = <unique_transform_stanza_name> under the [<spec>] stanza that corresponds with a stanza you've created in transforms.conf.
* Follow this stanza name with any number of the following setting/value pairs, as appropriate for what you intend to do with the transform.
* If you do not specify an entry for each setting, Splunk software uses the default value.

REGEX = <regular expression>
* Enter a regular expression to operate on your data.
* NOTE: This setting is valid for index-time and search-time field extraction.
* REGEX is required for all search-time transforms unless you are setting up an ASCII-only delimiter-based field extraction, in which case you can use DELIMS (see the DELIMS setting description, below).
* REGEX is required for all index-time transforms.
* REGEX and the FORMAT setting:
  * Name-capturing groups in the REGEX are extracted directly to fields. This means that you do not need to specify the FORMAT setting for simple field extraction cases (see the description of FORMAT, below).
  * If the REGEX extracts both the field name and its corresponding field value, you can use the following special capturing groups if you want to skip specifying the mapping in FORMAT:
    * _KEY_<string>, _VAL_<string>.
  * For example, the following are equivalent:
    * Using FORMAT:
      * REGEX = ([a-z]+)=([a-z]+)
      * FORMAT = $1::$2
    * Without using FORMAT
      * REGEX = (?< KEY_1>[a-z]+)=(?<VAL_1>[a-z]+)
  * When using either of the above formats, in a search-time extraction, the regular expression attempts to match against the source text,
extracting as many fields as can be identified in the source text.
* Default: empty string

FORMAT = <string>
* NOTE: This option is valid for both index-time and search-time field extraction. However, FORMAT behaves differently depending on whether the extraction is performed at index time or search time.
* This setting specifies the format of the event, including any field names or values you want to add.
* FORMAT for index-time extractions:
  * Use $n (for example $1, $2, etc) to specify the output of each REGEX match.
  * If REGEX does not have n groups, the matching fails.
  * The special identifier $0 represents what was in the DEST_KEY before the REGEX was performed.
  * At index time only, you can use FORMAT to create concatenated fields:
    * Example: FORMAT = ipaddress::$1.$2.$3.$4
    * When you create concatenated fields with FORMAT, "$" is the only special character. It is treated as a prefix for regular expression capturing groups only if it is followed by a number and only if the number applies to an existing capturing group. So if REGEX has only one capturing group and its value is "bar", then:
      * "FORMAT = foo$1" yields "foobar"
      * "FORMAT = foo$bar" yields "foo$bar"  
      * "FORMAT = foo$1234" yields "foo$1234"
      * "FORMAT = foo$1$2" yields "foobar$2"
  * At index-time, FORMAT defaults to <stanza-name>::$1
* FORMAT for search-time extractions:
  * The format of this field as used during search time extractions is as follows:
    * FORMAT = <field-name>::<field-value>(<field-name>::<field-value>)*
where:
  * field-name = [<string>|$<extracting-group-number>]
  * field-value = [<string>|$<extracting-group-number>]
* Search-time extraction examples:
  * 1. FORMAT = first::$1 second::$2 third::other-value
  * 2. FORMAT = $1::$2
* If you configure FORMAT with a variable <field-name>, such as in the second example above, the regular expression is repeatedly applied to the source text.
key to match and extract all field/value pairs in the event.
* When you use FORMAT to set both the field and the value (such as
  FORMAT =
    third::other-value), and the value is not an indexed token, you
must set the
  field to INDEXED_VALUE = false in fields.conf. Not doing so can
cause
  inconsistent search results.
* NOTE: You cannot create concatenated fields with FORMAT at search
time.
  That functionality is only available at index time.
* At search-time, FORMAT defaults to an empty string.

MATCH_LIMIT = <integer>
* Only set in transforms.conf for REPORT and TRANSFORMS field
  extractions.
  For EXTRACT type field extractions, set this in props.conf.
* Optional. Limits the amount of resources that are spent by PCRE
  when running patterns that do not match.
* Use this to set an upper bound on how many times PCRE calls an
  internal
  function, match(). If set too low, PCRE may fail to correctly match a
  pattern.
* Default: 100000

DEPTH_LIMIT = <integer>
* Only set in transforms.conf for REPORT and TRANSFORMS field
  extractions.
  For EXTRACT type field extractions, set this in props.conf.
* Optional. Limits the amount of resources that are spent by PCRE
  when running patterns that do not match.
* Use this to limit the depth of nested backtracking in an internal PCRE
  function, match(). If set too low, PCRE might fail to correctly match a
  pattern.
* Default: 1000

CLONE_SOURCETYPE = <string>
* This name is wrong; a transform with this setting actually clones and
  modifies events, and assigns the new events the specified source type.
* If CLONE_SOURCETYPE is used as part of a transform, the transform
  creates a
  modified duplicate event for all events that the transform is applied
  to via
  normal props.conf rules.
* Use this setting when you need to store both the original and a
  modified
  form of the data in your system, or when you need to to send the
  original and
  a modified form to different outbound systems.
* A typical example would be to retain sensitive information according
  to
one policy and a version with the sensitive information removed according to another policy. For example, some events may have data that you must retain for 30 days (such as personally identifying information) and only 30 days with restricted access, but you need that event retained without the sensitive data for a longer time with wider access.

* Specifically, for each event handled by this transform, a near-exact copy is made of the original event, and the transformation is applied to the copy. The original event continues along normal data processing unchanged.

* The <string> used for CLONE_SOURCETYPE selects the source type that is used for the duplicated events.

* The new source type MUST differ from the the original source type. If the original source type is the same as the target of the CLONE_SOURCETYPE, Splunk software makes a best effort to log warnings to splunkd.log, but this setting is silently ignored at runtime for such cases, causing the transform to be applied to the original event without cloning.

* The duplicated events receive index-time transformations & sed commands for all transforms that match its new host, source, or source type.

* This means that props.conf matching on host or source will incorrectly be applied a second time.

* Can only be used as part of of an otherwise-valid index-time transform. For example REGEX is required, there must be a valid target (DEST_KEY or WRITE_META), etc as above.

LOOKAHEAD = <integer>

* NOTE: This option is valid for all index time transforms, such as index-time field creation, or DEST_KEY modifications.

* Optional. Specifies how many characters to search into an event.

* Default: 4096

* You may want to increase this value if you have event line lengths that exceed 4096 characters (before linebreaking).

WRITE_META = [true|false]

* NOTE: This setting is only valid for index-time field extractions.

* Automatically writes REGEX to metadata.

* Required for all index-time field extractions except for those where DEST_KEY = _meta (see the description of the DEST_KEY setting, below)

* Use instead of DEST_KEY = _meta.
* Default: false

DEST_KEY = <KEY>
* NOTE: This setting is only valid for index-time field extractions.
* Specifies where Splunk software stores the expanded FORMAT results in accordance with the REGEX match.
* Required for index-time field extractions where WRITE_META = false or is not set.
* For index-time extractions, DEST_KEY can be set to a number of values mentioned in the KEYS section at the bottom of this file.
* If DEST_KEY = _meta (not recommended) you should also add $0 to the start of your FORMAT setting. $0 represents the DEST_KEY value before Splunk software performs the REGEX (in other words, _meta).
* The $0 value is in no way derived *from* the REGEX match. (It does not represent a captured group.)
* KEY names are case-sensitive, and should be used exactly as they appear in the KEYS list at the bottom of this file. (For example, you would say DEST_KEY = MetaData:Host, *not* DEST_KEY = metadata:host.)

DEFAULT_VALUE = <string>
* NOTE: This setting is only valid for index-time field extractions.
* Optional. The Splunk software writes the DEFAULT_VALUE to DEST_KEY if the REGEX fails.
* Default: empty string

SOURCE_KEY = <string>
* NOTE: This setting is valid for both index-time and search-time field extractions.
* Optional. Defines the KEY that Splunk software applies the REGEX to.
* For search time extractions, you can use this setting to extract one or more values from the values of another field. You can use any field that is available at the time of the execution of this field extraction.
* For index-time extractions use the KEYS described at the bottom of this file.
* KEYs are case-sensitive, and should be used exactly as they appear in the KEYS list at the bottom of this file. (For example, you would say
  
  SOURCE_KEY = MetaData:Host, *not* SOURCE_KEY = metadata:host.)
* If <string> starts with "field:" or "fields:" the meaning is changed. Instead of looking up a KEY, it instead looks up an already indexed field.
  
  For example, if a CSV field name "price" was indexed then
  "SOURCE_KEY = field:price" causes the REGEX to match against the
of that field. It's also possible to list multiple fields here with "SOURCE_KEY = fields:name1,name2,name3" which causes MATCH to be run against a string comprising of all three values, separated by space characters.
* SOURCE_KEY is typically used in conjunction with REPEAT_MATCH in index-time field transforms.
* Default: _raw
  * This means it is applied to the raw, unprocessed text of all events.

REPEAT_MATCH = [true|false]
* NOTE: This setting is only valid for index-time field extractions.
* Optional. When set to true, Splunk software runs the REGEX multiple times on the SOURCE_KEY.
* REPEAT_MATCH starts wherever the last match stopped, and continues until no more matches are found. Useful for situations where an unknown number of REGEX matches are expected per event.
* Default: false

INGEST_EVAL = <comma-separated list of evaluator expressions>
* NOTE: This setting is only valid for index-time field extractions.
* Optional. When you set INGEST_EVAL, this setting overrides all of the other index-time settings (such as REGEX, DEST_KEY, etc) and declares the index-time extraction to be evaluator-based.
* The expression takes a similar format to the search-time "|eval" command.
  For example "a=b+c*d" Just like the search-time operator, you can string multiple expressions together, separated by commas like "len=length(_raw), length_category=floor(log(len,2))".
* Keys which are commonly used with DEST_KEY or SOURCE_KEY (like "_raw", "queue", etc) can be used directly in the expression.
  Also available are values which would be populated by default when this event is searched ("source", "sourcetype", "host", "splunk_server", "linecount", "index"). Search-time calculated fields (the "EVAL-" settings in props.conf) are NOT available.
* When INGEST_EVAL accesses the ".time" variable, subsecond information is included. This is unlike regular-expression-based index-time extractions, where ".time" values are limited to whole seconds.
* By default, other variable names refer to index-time fields which are populated in ".meta" So an expression 'event_category=if(_raw LIKE "WARN \%", "warning", "normal")' would append a new indexed field to .meta like "event_category::warning".
* You can force a variable to be treated as a direct KEY name by prefixing it with "pd:". You can force a variable to be always
treated as a "_meta" field by prefixing it with "field:" Therefore the above expression could also be written as
'$field:event_category$=if($pd:_raw$ LIKE "WARN %", "warning", "normal")'
* When writing to a _meta field, the default behavior is to add a new index-time field even if one exists with the same name, the same way WRITE_META works for regular-expression-based extractions. For example, "a=5,
a=a+2" adds two index-time fields to _meta: "a::5 a::7". You can change this
by using "::=" after the variable name. For example, setting "a=5,
a::=a+2"
causes Splunk software to add a single "a::7" field.
* NOTE: Replacing index-time fields is slower than adding them. It is best to
only use "::=" when you need this behavior.
* The "::=" operator can also be used to remove existing fields in _meta by assigning the expression null() to them.
* When reading from an index-time field that occurs multiple times inside the
_meta key, normally the first value is used. You can override this by
prefixing the name with "mv:" which returns all of the values into a "multival" object. For example, if _meta contains the keys "v::a v::b" then
'mvjoin(v,"",")' returns "a" while 'mvjoin($mv:v$,","",")' returns "a,b".
* Note that this "mv:" prefix does not change behavior when it writes to a
_meta field. If the value returned by an expression is a multivalue, it
always creates multiple index-time fields. For example,
'x=mvappend("a","b","c")' causes the string "x::a x::b x::c" to be appended
to the _meta key.
* Internally, the _meta key can hold values with various numeric types.Splunk software normally picks a type appropriate for the value that the
expression returned. However, you can override this this choice by specifying
a type in square brackets after the destination field name. For example,
'my_len[int]=length(source)' creates a new field named "my_len" and forces it
to be stored as a 64-bit integer inside _meta. You can force Splunk software
to store a number as floating point by using the type "[float]". You can
request a smaller, less-precise encoding by using "[float32]". If you want to
store the value as floating point but also ensure that the Splunk software
remembers the significant-figures information that the evaluation expression
deduced, use "[float-sf]" or "[float32-sf]". Finally, you can force the
result to be treated as a string by specifying "[string]".
* The capability of the search-time |eval operator to name the destination
field based on the value of another field (like "| eval {destname}=1")
is NOT available for index-time evaluations.
* Default: empty

DELIMS = <quoted string list>
* NOTE: This setting is only valid for search-time field extractions.
* IMPORTANT: If a value may contain an embedded unescaped double quote character, such as "foo"bar", use REGEX, not DELIMS. An escaped double quote (\") is ok. Non-ASCII delimiters also require the use of REGEX.
* Optional. Use DELIMS in place of REGEX when you are working with ASCII-only delimiter-based field extractions, where field values (or field/value pairs)
are separated by delimiters such as colons, spaces, line breaks, and so on.
* Sets delimiter characters, first to separate data into field/value pairs,
and then to separate field from value.
* Each individual ASCII character in the delimiter string is used as a delimiter to split the event.
* Delimiters must be specified within double quotes (eg. DELIMS="|,;"). Special escape sequences are \t (tab), \n (newline), \r (carriage return),
\\ (backslash) and \" (double quotes).
* When the event contains full delimiter-separated field/value pairs, you
enter two sets of quoted characters for DELIMS:
* The first set of quoted delimiters extracts the field/value pairs.
* The second set of quoted delimiters separates the field name from its corresponding value.
* When the event only contains delimiter-separated values (no field names),
use just one set of quoted delimiters to separate the field values. Then use
the FIELDS setting to apply field names to the extracted values.
* Alternately, Splunk software reads even tokens as field names and odd
tokens as field values.
* Splunk software consumes consecutive delimiter characters unless you specify a list of field names.
* The following example of DELIMS usage applies to an event where field/value pairs are separated by '|' symbols and the field names are separated from their corresponding values by '=' symbols:
[pipe_eq]
DELIMS = "|", "="
* Default: ""
FIELDS = <quoted string list>
* NOTE: This setting is only valid for search-time field extractions.
* Used in conjunction with DELIMS when you are performing
delimiter-based
    field extraction and only have field values to extract.
* FIELDS enables you to provide field names for the extracted field values,
    in list format according to the order in which the values are
extracted.
* NOTE: If field names contain spaces or commas they must be quoted with
    " "
    To escape, use \
* The following example is a delimiter-based field extraction where
three
    field values appear in an event. They are separated by a comma and
then a
    space.
    [commalist]
    DELIMS = ", ",
    FIELDS = field1, field2, field3
* Default: ""

MV_ADD = [true|false]
* NOTE: This setting is only valid for search-time field extractions.
* Optional. Controls what the extractor does when it finds a field which
    already exists.
* If set to true, the extractor makes the field a multivalued field and
    appends the newly found value, otherwise the newly found value is
    discarded.
* Default: false

CLEAN_KEYS = [true|false]
* NOTE: This setting is only valid for search-time field extractions.
* Optional. Controls whether Splunk software "cleans" the keys (field
    names) it
    extracts at search time. "Key cleaning" is the practice of replacing
any
    non-alphanumeric characters (characters other than those falling
between the
    a-z, A-Z, or 0-9 ranges) in field names with underscores, as well as
the
    stripping of leading underscores and 0-9 characters from field names.
* Add CLEAN_KEYS = false to your transform if you need to extract field
    names that include non-alphanumeric characters, or which begin with
underscores or 0-9 characters.
* Default: true

KEEP_EMPTY_VALS = [true|false]
* NOTE: This setting is only valid for search-time field extractions.
* Optional. Controls whether Splunk software keeps field/value pairs
when
    the value is an empty string.
* This option does not apply to field/value pairs that are generated by Splunk software autokv extraction. Autokv ignores field/value pairs with empty values.
* Default: false

CAN_OPTIMIZE = [true|false]
* NOTE: This setting is only valid for search-time field extractions.
* Optional. Controls whether Splunk software can optimize this extraction out (another way of saying the extraction is disabled).
* You might use this if you are running searches under a Search Mode setting that disables field discovery—it ensures that Software always discovers specific fields.
* Splunk software only disables an extraction if it can determine that none of the fields identified by the extraction will ever be needed for the successful evaluation of a search.
* NOTE: This option should be rarely set to false.
* Default: true

### Lookup tables

# NOTE: Lookup tables are used ONLY during search time

filename = <string>
* Name of static lookup file.
* File should be in $SPLUNK_HOME/etc/system/lookups/, or in $SPLUNK_HOME/etc/<app_name>/lookups/ if the lookup belongs to a specific app.
* If file is in multiple 'lookups' directories, no layering is done.
* Standard conf file precedence is used to disambiguate.
* Only file names are supported. Paths are explicitly not supported. If you specify a path, Splunk software strips the path to use the value after the final path separator.
* Splunk software then looks for this filename in $SPLUNK_HOME/etc/system/lookups/ or $SPLUNK_HOME/etc/<app_name>/lookups/.
* Default: empty string

collection = <string>
* Name of the collection to use for this lookup.
* Collection should be defined in $SPLUNK_HOME/etc/<app_name>/collections.conf for some <app_name>
* If collection is in multiple collections.conf file, no layering is done.
* Standard conf file precedence is used to disambiguate.
* Defaults to empty string (in which case the name of the stanza is used).

```
max_matches = <integer>
* The maximum number of possible matches for each input lookup value (range 1 - 1000).
* If the lookup is non-temporal (not time-bounded, meaning the time_field setting is not specified), Splunk software uses the first <integer> entries,
  in file order.
* If the lookup is temporal, Splunk software uses the first <integer> entries in descending time order. In other words, only <max_matches> lookup entries are allowed to match. If the number of lookup entries exceeds <max_matches>,
  only the ones nearest to the lookup value are used.
* Default: 100 matches if the time_field setting is not specified for the lookup. If the time_field setting is specified for the lookup, the default is 1 match.
```

```
min_matches = <integer>
* Minimum number of possible matches for each input lookup value.
* Default = 0 for both temporal and non-temporal lookups, which means that Splunk software outputs nothing if it cannot find any matches.
* However, if min_matches > 0, and Splunk software gets less than min_matches,
  it provides the default_match value provided (see below).
```

```
default_match = <string>
* If min_matches > 0 and Splunk software has less than min_matches for any given input, it provides this default_match value one or more times until the min_matches threshold is reached.
* Defaults to empty string.
```

```
case_sensitive_match = <bool>
* NOTE: To disable case-sensitive matching with input fields and values from events, the KV Store lookup data must be entirely in lower case. The input data can be of any case, but the KV Store data must be lower case.
* If set to false, case insensitive matching is performed for all fields in a
```
lookup table
* Defaults to true (case sensitive matching)

match_type = <string>
* A comma and space-delimited list of \(<match_type>\{<field_name>\) specification to allow for non-exact matching
* The available match_type values are WILDCARD, CIDR, and EXACT. Only fields that should use WILDCARD or CIDR matching should be specified in this list.
* Default: EXACT

external_cmd = <string>
* Provides the command and arguments to invoke to perform a lookup. Use this for external (or "scripted") lookups, where you interface with with an external script rather than a lookup table.
* This string is parsed like a shell command.
* The first argument is expected to be a python script (or executable file) located in $SPLUNK_HOME/etc/<app_name>/bin (or ../etc/searchscripts).
* Presence of this field indicates that the lookup is external and command based.
* Default: empty string

fields_list = <string>
* A comma- and space-delimited list of all fields that are supported by the external command.

index_fields_list = <string>
* A comma- and space-delimited list of fields that need to be indexed for a static .csv lookup file.
* The other fields are not indexed and not searchable.
* Restricting the fields enables better lookup performance.
* Defaults to all fields that are defined in the .csv lookup file header.

external_type = [python|executable|kvstore|geo|geo_hex]
* This setting describes the external lookup type.
* Use 'python' for external lookups that use a python script.
* Use 'executable' for external lookups that use a binary executable, such as a C++ executable.
* Use 'kvstore' for KV store lookups.
* Use 'geo' for geospatial lookups.
* 'geo_hex' is reserved for the geo_hex H3 lookup.
* Default: python

time_field = <string>
* Used for temporal (time bounded) lookups. Specifies the name of the
field
  in the lookup table that represents the timestamp.
* Default: empty string
  * This means that lookups are not temporal by default.

time_format = <string>
* For temporal lookups this specifies the 'strptime' format of the
  field.
* You can include subseconds but Splunk software ignores them.
* Default: %s.%Q (seconds from unix epoch in UTC and optional
  milliseconds)

max_offset_secs = <integer>
* For temporal lookups, this is the maximum time (in seconds) that the
  event
  timestamp can be later than the lookup entry time for a match to
  occur.
* Default: 2000000000

min_offset_secs = <integer>
* For temporal lookups, this is the minimum time (in seconds) that the
  event
  timestamp can be later than the lookup entry timestamp for a match to
  occur.
* Default: 0

batch_index_query = <bool>
* For large file-based lookups, batch_index_query determines whether
  queries
  can be grouped to improve search performance.
* Default is unspecified here, but defaults to true (at global level in
  limits.conf)

allow_caching = <bool>
* Allow output from lookup scripts to be cached
* Default: true

cache_size = <integer>
* Cache size to be used for a particular lookup. If a previously looked
  up
  value is already present in the cache, it is applied.
* The cache size represents the number of input values for which to
  cache
  output values from a lookup table.
* Do not change this value unless you are advised to do so by Splunk
  Support or
  a similar authority.
* Default: 10000

max_ext_batch = <integer>
* The maximum size of external batch (range 1 - 1000).
filter = <string>
* Filter results from the lookup table before returning data. Create this filter like you would a typical search query using Boolean expressions and/or comparison operators.
* For KV Store lookups, filtering is done when data is initially retrieved to improve performance.
* For CSV lookups, filtering is done in memory.

feature_id_element = <string>
* If the lookup file is a kmz file, this field can be used to specify the xml path from placemark down to the name of this placemark.
* This setting applies only to geospatial lookup configurations.
* Default: /Placemark/name

check_permission = <bool>
* Specifies whether the system can verify that a user has write permission to a lookup file when that user uses the outputlookup command to modify that file.
  If the user does not have write permissions, the system prevents the modification.
* The check_permission setting is only respected when output_check_permission is set to "true" in limits.conf.
* You can set lookup table file permissions in the .meta file for each lookup file, or through the Lookup Table Files page in Settings. By default, only users who have the admin or power role can write to a shared CSV lookup file.
* This setting applies only to CSV lookup configurations.
* Default: false

replicate = true|false
* Indicates whether to replicate CSV lookups to indexers.
  When false, the CSV lookup is replicated only to search heads in a search head cluster so that input lookup commands can use this lookup on the search heads.
  When true, the CSV lookup is replicated to both indexers and search heads.
* Only for CSV lookup files.
* Note that replicate=true works only if it is included in replication whitelist, See distSearch.conf/[replicationWhitelist] option.
* Default: true
**METRICS - STATSD DIMENSION EXTRACTION**

**Metrics**

[statsd-dims:<unique_transforms_stanza_name>]
* 'statsd-dims' prefix indicates this stanza is applicable only to statsd metric type input data.
* This stanza is used to define regular expression to match and extract dimensions out of statsd dotted name segments.
* By default, only the unmatched segments of the statsd dotted name segment become the metric_name.

REGEX = <regular expression>
* Splunk software supports a named capturing group extraction format to provide dimension names of the corresponding values being extracted out. For example:
  (?<dim1>group)(?<dim2>group).. REMOVE_DIMS_FROM_METRIC_NAME = <boolean>
* If set to false, the matched dimension values from the REGEX above would also be a part of the metric name.
* If true, the matched dimension values would not be a part of metric name.
* Default: true

[metric-schema:<unique_transforms_stanza_name>]
* The 'metric-schema' stanza transforms index-time field extractions from a single log event into metrics.
* Each metric created has its own metric_name and _value.
* The other fields extracted from the log event become dimensions in the generated metrics.
* You must provide one of the following two settings:
  METRIC-SCHEMA-MEASURES-<unique_metric_name_prefix> or METRIC-SCHEMA-MEASURES. These settings determine how values for the metric_name and _value fields are obtained.

METRIC-SCHEMA-MEASURES-<unique_metric_name_prefix> = (_ALLNUMS_ |
(_NUMS_EXCEPT_ )? <field1>, <field2>,... }
* Optional.
* <unique_metric_name_prefix> should match the value of a field extracted from
  the event.
* If this setting is exactly equal to _ALLNUMS_, the Splunk software treats
  all numeric fields as measures.
* If this setting starts with _NUMS_EXCEPT_, the Splunk software treats all
  numerical fields except those that match the given field names as measures.
  * NOTE: a space is required between the '_NUMS_EXCEPT_' prefix and
    '<field1>'.
* Otherwise, the Splunk software treats all fields that are listed and which
  have a numerical value as measures.
* If the value of the 'metric_name' index-time extraction matches with the
  <unique_metric_name_prefix>, the Splunk platform:
  * Creates a metric with a new metric_name for each measure field where
    the
    metric_name value is the name of the field prefixed by the
    <unique_metric_name_prefix>.
  * Saves the corresponding numeric value for each measure field as
    '_value'
    within each metric.
  * The Splunk platform saves the remaining index-time field extractions as
    dimensions in each of the created metrics.
  * Default: empty

METRIC-SCHEMA-BLACKLIST-DIMS-<unique_metric_name_prefix> =
<dimension_field1>, <dimension_field2>,...
* Optional
* This configuration enables the Splunk platform to omit unnecessary dimensions
  when it transforms log data to metrics data. You might set this up if you
  have high-cardinality dimensions that are unnecessary for your metrics.
* Use this configuration in conjunction with a corresponding
  METRIC-SCHEMA-MEASURES-<unique_metric_name_prefix> configuration.
* <unique_metric_name_prefix> should match the value of a field extracted from
  the log event.
* <dimension_field> should match the name of a field in the log event that is
  not extracted as a measure field in the corresponding METRIC-SCHEMA-
  MEASURES-<unique_metric_name_prefix> configuration.
* Default: empty
METRIC-SCHEMA-MEASURES = (_ALLNUMS_ | (!_NUMS_EXCEPT_)? <field1>, <field2>,...) * Optional.
* This configuration has a lower precedence over
METRIC-SCHEMA-MEASURES-<unique_metric_name_prefix>
  if event has a match for unique_metric_name_prefix
* When no prefix can be identified, this configuration is active
  to create a new metric for each measure field in the event data, as defined
  in the previous description for
METRIC-SCHEMA-MEASURES-<unique_metric_name_prefix>
* The Splunk platform saves the remaining index-time field extractions
  as dimensions in each of the created metrics.
* Default: empty

METRIC-SCHEMA-BLACKLIST-DIMS = <dimension_field1>, <dimension_field2>,...
* Optional
* This configuration enables the Splunk platform to omit unnecessary dimensions
  when it transforms log data to metrics data. You might set this up if you
  have high-cardinality dimensions that are unnecessary for your metrics.
* Use this configuration in conjunction with a corresponding
  METRIC-SCHEMA-MEASURES configuration.
* <dimension_field> should match the name of a field in the log event that is
  not extracted as a <measure_field> in the corresponding METRIC-SCHEMA-
  MEASURES configuration.
* Default: empty

**KEYS:**

* NOTE: Keys are case-sensitive. Use the following keys exactly as they appear.

queue : Specify which queue to send the event to (can be nullQueue, indexQueue).
  * indexQueue is the usual destination for events going through the
  transform-handling processor.
  * nullQueue is a destination which causes the events to be dropped entirely.
_raw : The raw text of the event.
_meta : A space-separated list of metadata for an event.
_time : The timestamp of the event, in seconds since 1/1/1970 UTC.
MetaData:Host : The host associated with the event.
The value must be prefixed by "host::"

_MetaData:Index : The index where the event should be stored.

MetaData:Source : The source associated with the event.
The value must be prefixed by "source::"

MetaData:Sourcetype : The source type of the event.
The value must be prefixed by "sourcetype::"

_TCP_ROUTING : Comma separated list of tcpout group names (from outputs.conf)

_SYSLOG_ROUTING : Comma separated list of syslog-stanza names (from outputs.conf)

* NOTE: Any KEY (field name) prefixed by '_ ' is not indexed by Splunk software, in general.

[accepted_keys]

<name> = <key>

* Modifies the list of valid SOURCE_KEY and DEST_KEY values. Splunk software
  checks the SOURCE_KEY and DEST_KEY values in your transforms against
  this list when it performs index-time field transformations.
* Add entries to [accepted_keys] to provide valid keys for specific environments, apps, or similar domains.
* The 'name' element disambiguates entries, similar to -class entries in props.conf.
* The 'name' element can be anything you choose, including a description of
  the purpose of the key.
* The entire stanza defaults to not being present, causing all keys not
documented just above to be flagged.

transforms.conf.example

#  Version 7.3.0
#
# This is an example transforms.conf. Use this file to create regexes
and
# rules for transforms. Use this file in tandem with props.conf.
#
# To use one or more of these configurations, copy the configuration
# block
# into transforms.conf in $SPLUNK_HOME/etc/system/local/. You must
# restart
# Splunk to enable configurations.
#
# To learn more about configuration files (including precedence) please
# see
# the documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
#
# Note: These are examples. Replace the values with your own
# customizations.
#
# Indexed field:

[netscreen-error]
REGEX = device_id=\[w+\](?<err_code>[^:]+)
FORMAT = err_code::$1
WRITE_META = true

# Override host:

[hostoverride]
DEST_KEY = MetaData:Host
REGEX = \s(\w*)$
FORMAT = host::$1

# Extracted fields:

[netscreen-error-field]
REGEX = device_id=\[w+\](?<err_code>[^:]+)
FORMAT = err_code::$1

# Index-time evaluations:

[discard-long-lines]
INGEST_EVAL = queue=if(length(_raw) > 500, "nullQueue", ")"

[split-into-sixteen-indexes-for-no-good-reason]
INGEST_EVAL = index="split_" . substr(md5(_raw),1,1)

[add-two-numeric-fields]
INGEST_EVAL = loglen_raw=ln(length(_raw)),
loglen_src=ln(length(source))
# In this example we only create the new index-time field if the host
# had a dot in it; assigning null() to a new field is a no-op:
[add-hostdomain-field]
INGEST_EVAL = hostdomain=if(host LIKE "%.%",
replace(host,"^[^\./]+\./",""), null())

# Static lookup table
[mylookuptable]
filename = mytable.csv

# one to one lookup
# guarantees that we output a single lookup value for each input value,
if
# no match exists, we use the value of "default_match", which by default
is
# "NONE"
[mylook]
filename = mytable.csv
max_matches = 1
min_matches = 1
default_match = nothing

# Lookup and filter results
[myfilteredlookup]
filename = mytable.csv
filter = id<500 AND color="red"

# external command lookup table
[myexternaltable]
external_cmd = testadapter.py blah
fields_list = foo bar

# Temporal based static lookup table
[staticwtime]
filename = mytable.csv
time_field = timestamp
time_format = %d/%m/%y %H:%M:%S

# Mask sensitive data:
[session-anonymizer]
REGEX = (?m)^(.*)SessionId=\w{4}([&"].*$)
FORMAT = $1SessionId=#####$2
DEST_KEY = _raw

# Route to an alternate index:
# Extract comma-delimited values into fields:

```
[extract_csv]
DELIMS = ",," 
FIELDS = "field1", "field2", "field3"
```

# This example assigns the extracted values from _raw to field1, field2 and
# field3 (in order of extraction). If more than three values are
# extracted
# the values without a matching field name are ignored.

```
[pipe_eq]
DELIMS = "|", "="
```

# The above example extracts key-value pairs which are separated by '|' 
# while the key is delimited from value by '='.

```
[multiple_delims]
DELIMS = "|;", "=:"
```

# The above example extracts key-value pairs which are separated by '|' 
# or
# ';', while the key is delimited from value by '=' or ':'.

##### BASIC MODULAR REGULAR EXPRESSIONS DEFINITION START #######

# When adding a new basic modular regex please add a comment that lists
# the fields that it extracts (named capturing groups), or whether it
# provides a placeholder for the group name as:
# Extracts: field1, field2...
#
# [all_lazy]
REGXEX = .*?

# [all]
REGXEX = .*

# [nspaces]
# matches one or more NON space characters
REGXEX = \S+
[alphas]
# matches a string containing only letters a-zA-Z
REGEX = [a-zA-Z]+

[alnums]
# matches a string containing letters + digits
REGEX = [a-zA-Z0-9]+

[qstring]
# matches a quoted "string" - extracts an unnamed variable
# name MUST be provided as in [[qstring:name]]
# Extracts: empty-name-group (needs name)
REGEX = "(?<>[^"]*+)"

[sbstring]
# matches a string enclosed in [] - extracts an unnamed variable
# name MUST be provided as in [[sbstring:name]]
# Extracts: empty-name-group (needs name)
REGEX = \[(?<>[^\]\]*+)\]

[digits]
REGEX = \d+

[int]
# matches an integer or a hex number
REGEX = 0x[a-fA-F0-9]+|\d+

[float]
# matches a float (or an int)
REGEX = \d*\.\d+|[[]int]]

[octet]
# this would match only numbers from 0-255 (one octet in an ip)
REGEX = (?:2(?:5[0-5]|0-4)[0-9])|[0-1][0-9][0-9]|0-9[0-9]?

[ipv4]
# matches a valid IPv4 optionally followed by :port_num the octets in the ip
# would also be validated 0-255 range
# Extracts: ip, port
REGEX = (?<ip>[[octet]](?:\.[[octet]][3])?::[[int:port]])?

[simple_url]
# matches a url of the form proto://domain.tld/uri
# Extracts: url, domain
REGEX = (?<url>\w++://(?<domain>[a-zA-Z0-9\-.:]+)?(\s+)?([^\s]*))?

[url]
# matches a url of the form proto://domain.tld/uri
# Extracts: url, proto, domain, uri
REGEX = (?<url>[[alphas:proto]]://(?<domain>[a-zA-Z0-9\-.:]+)?(?<url>\s+)?([^\s]*))?
# matches a uri of the form /path/to/resource?query
# Extracts: uri, uri_path, uri_query
REGEX = (?<uri>({[^\s?]+}\+)?(?:\:\\?({[^\s]+})?))?

uri
# uri = path optionally followed by query
[/this/path/file.js?query=part&other=var]
# path = root part followed by file
# Extracts: uri, uri_path, uri_root, uri_file, uri_query, uri_domain
(optional if in proxy mode)
REGEX = (?<uri>(?:\w++://(?<uri_domain>[^\s/]+)+)?(?<uri_path>({[^\s?;=]+})(?<!\d+)(?:\?(?<uri_query>[^\s"]+))?)?

[hide-ip-address]
# Make a clone of an event with the sourcetype masked_ip_address. The
# clone
# will be modified; its text changed to mask the ip address.
# The cloned event will be further processed by index-time transforms
# and
# SEDCMD expressions according to its new sourcetype.
# In most scenarios an additional transform would be used to direct the
# masked_ip_address event to a different index than the original data.
REGEX = ^(.*?src=\d+\.\d+\.\d+\.\d+.*)$ FORMAT = $1src=XXXXX$2 DEST_KEY = _raw CLONE_SOURCETYPE = masked_ip_addresses

#Set REPEAT_MATCH to true to repeatedly match the regex in the data.
#example sample data - 1483382050 a=1 b=2 c=3 d=4 e=5
#Since REPEAT_MATCH is set to true, the regex will matched for a=1, then
#b=2, then c=3 and so on
#if REPEAT_MATCH is set to false, the match will stop at a=1
#if WRITE_META is set to false, these will added as indexed fields -
a, b, c, d, e

[repeat_regex]
REGEX = ([a-z])=(\d+)
FORMAT = $1::$2 REPEAT_MATCH = true WRITE_META = true

#Regex with $0 in FORMAT
#example sample data -
# #52 +(6295)- [X]
# <Tsk> idfdgdfdhgfjhgjdsdfjhkiuk;'''
# <Tsk> sorry.. this is a test
[bash]
REGEX = #([0-9]+) \+\{(-?[0-9]+)\} - \[X\]
FORMAT = $0 bash_quote_id::$1 bash_quote_score::$2 WRITE_META=true

537
# Statsd dimensions extraction

# For example, below two stanzas would extract dimensions as
# ipv4=10.2.3.4
# and os=windows from statsd
data=mem.percent.used.10.2.3.4.windows:33|g
[statsd-dims:regex_stanza1]
REGEX = (?<ipv4>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})
REMOVE_DIMS_FROM_METRIC_NAME = true

[statsd-dims:regex_stanza2]
REGEX = \S+\.(?<os>\w+):
REMOVE_DIMS_FROM_METRIC_NAME = true

# In most cases we need only one regex to be run per sourcetype. By default
# Splunk would look for the sourcetype name in transforms.conf in such scenario.
# Hence, there is no need to provide STATSD-DIM-TRANSFORMS setting in props.conf.
[statsd-dims:metric_sourcetype_name]
REGEX = (?<ipv4>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})\.(?<os>\w+):
REMOVE_DIMS_FROM_METRIC_NAME = true

# In this metrics example, we start with this log line:
#
# 01-26-2018 07:49:49.030 -0800 INFO  Metrics - group=queue,
# name=aggqueue, max_size_kb=1024, current_size_kb=1,
# current_size=3, largest_size=49, smallest_size=0,
dc_latitude=37.3187706, dc_longitude=-121.9515042
#
# The following stanza converts that single event into multiple metrics
# at
# index-time. It blacklists the dc_latitude and dc_longitude dimensions, which
# means they are omitted from the generated metrics.
[metric-schema:logtometrics]
METRIC-SCHEMA-MEASURES-queue =
max_size_kb,current_size_kb,current_size,largest_size,smallest_size
METRIC-SCHEMA-BLACKLIST-DIMS-queue = dc_latitude,dc_longitude

# Here are the metrics generated by that stanza:
# {'metric_name' : 'queue.max_size_kb',    '_value' : 1024, 'name':
# 'aggqueue'},
# {'metric_name' : 'queue.current_size_kb', '_value' : 1,    'name':
# 'aggqueue'},
# {'metric_name' : 'queue.current_size',   '_value' : 3,    'name':
# 'aggqueue'},

538
# {'metric_name': 'queue.largest_size', '_value': 49, 'name': 'aggqueue'},
# {'metric_name': 'queue.smallest_size', '_value': 0, 'name': 'aggqueue'}

# In the sample log above, group=queue represents the unique metric name prefix. Hence, it needs to be
# formatted and saved as metric_name::queue for Splunk to identify queue as a metric name prefix.

[extract_group]
REGEX = group=(\w+)
FORMAT = metric_name::$1
WRITE_META = true

[extract_name]
REGEX = name=(\w+)
FORMAT = name::$1
WRITE_META = true

[extract_max_size_kb]
REGEX = max_size_kb=(\w+)
FORMAT = max_size_kb::$1
WRITE_META = true

[extract_current_size_kb]
REGEX = current_size_kb=(\w+)
FORMAT = current_size_kb::$1
WRITE_META = true

[extract_max_size_kb]
REGEX = max_size_kb=(\w+)
FORMAT = max_size_kb::$1
WRITE_META = true

[extract_largest_size]
REGEX = largest_size=(\w+)
FORMAT = largest_size::$1
WRITE_META = true

[extract_smallest_size]
REGEX = smallest_size=(\w+)
FORMAT = smallest_size::$1
WRITE_META = true

ui-tour.conf

The following are the spec and example files for ui-tour.conf.
ui-tour.conf.spec

# Version 7.3.0
#
# This file contains the tours available for Splunk Onboarding
#
# There is a default ui-tour.conf in $SPLUNK_HOME/etc/system/default.
# To create custom tours, place a ui-tour.conf in
# $SPLUNK_HOME/etc/system/local/. To create custom tours for an app, place
# ui-tour.conf in $SPLUNK_HOME/etc/apps/<app_name>/local/.
# #
# To learn more about configuration files (including precedence) see the
# documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
#

GLOBAL SETTINGS

# Use the [default] stanza to define any global settings.
#   * You can also define global settings outside of any stanza, at the
top of
#     the file.
#   * This is not a typical conf file for configurations. It is used to
set/create
#     tours to demonstrate product functionality to users.
#   * If an attribute is defined at both the global level and in a
specific
#     stanza, the value in the specific stanza takes precedence.

[<stanza name>]
* Stanza name is the name of the tour

useTour = <string>
* Used to redirect this tour to another when called by Splunk.
* Optional

nextTour = <string>
* String used to determine what tour to start when current tour is
finished.
* Optional

intro = <string>
* A custom string used in a modal to describe what tour is about to be
taken.
* Optional
type = <image || interactive>
* Can either be "image" or "interactive" to determine what kind of tour it is.
* Required

label = <string>
* The identifying name for this tour used in the tour creation app.
* Optional in general
* Required only if this tour is being linked from another tour (nextTour)

tourPage = <string>
* The Splunk view this tour is associated with (only necessary if it is linked to).
* Optional

managerPage = <boolean>
* Used to signify that the tourPage is a manager page. This will change the url of
* when the tourPage is rendered to "/manager/{app}/{view}" rather than "/app/{app}/{view}"
* Optional

viewed = <boolean>
* A boolean to determine if this tour has been viewed by a user.
* Set by Splunk

skipText = <string>
* The string for the skip button (interactive and image)
* Defaults to "Skip tour"
* Optional

doneText = <string>
* The string for the button at the end of a tour (interactive and image)
* Defaults to "Try it now"
* Optional

doneURL = <string>
* The Splunk URL of where the user will be directed once the tour is over.
* The user will click a link/button.
* Helpful to use with above doneText attribute to specify location.
* Splunk link is formed after the localization portion of the full URL.
* For example if the link is localhost:8000/en-US/app/search/reports, the doneURL will be "app/search/reports"
* Optional

forceTour = <boolean>
* Used with auto tours to force users to take the tour and not be able to skip
* Optional

**For image based tours**

# Users can list as many images with captions as they want. Each new image is created by
# incrementing the number.

imageName<int> = <string>
* The name of the image file (example.png)
* Required but Optional only after first is set

imageCaption<int> = <string>
* The caption string for corresponding image
* Optional

imgPath = <string>
* The subdirectory relative to Splunk's 'img' directory in which users put the images.
  This will be appended to the url for image access and not make a server request within Splunk.
  EX) If user puts images in a subdirectory 'foo': imgPath = foo.
  EX) If within an app, imgPath = foo will point to the app's img path of
    appserver/static/img/foo
* Required only if images are not in the main 'img' directory.

canvas = <specific app name>
* String consisting of either 'system' or the app name the tour images are to be stored.
* If set to 'system', it will revert to Splunk's native img path.
* Required

**For interactive tours**

# Users can list as many steps with captions as they want. Each new step is created by
# incrementing the number.

urlData = <string>
* String of any querystring variables used with tourPage to create full url executing this tour.
* Don't add the "?" to the beginning of this string
* Optional
stepText<int> = <string>
* The string used in specified step to describe the UI being showcased.
* Required but Optional only after first is set

stepElement<int> = <selector>
* The UI Selector used for highlighting the DOM element for corresponding step.
* Optional

stepPosition<int> = <bottom || right || left || top>
* String that sets the position of the tooltip for corresponding step.
* Optional

stepClickEvent<int> = <click || mousedown || mouseup>
* Sets a specific click event for an element for corresponding step.
* Optional

stepClickElement<int> = <string>
* The UI selector used for a DOM element used in conjunction with click above.
* Optional

**ui-tour.conf.example**

```
#  Version 7.3.0
#
#  This file contains the tours available for Splunk Onboarding
#
#  To update tours, copy the configuration block into
#  ui-tour.conf in $SPLUNK_HOME/etc/system/local/. Restart the Splunk software to
#  see the changes.
#
#  To learn more about configuration files (including precedence) see the
#  documentation located at
#  http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles
#
#  Image Tour
[tour-name]
type = image
imageName1 = TourStep1.png
imageCaption1 = This is the first caption
imageName2 = TourStep2.png
imageCaption2 = This is the second caption
imgPath = /testtour
context = system
doneText = Continue to Tour Page
```
doneURL = app/toursapp/home

# Interactive Tour
[test-interactive-tour]
type = interactive
tourPage = reports
urlData = data=foo&moredata=bar
label = Interactive Tour Test
stepText1 = Welcome to this test tour
stepText2 = This is the first step in the tour
stepElement2 = .test-selector
stepText3 = This is the second step in the tour
stepElement3 = .test-selector
stepClickEvent3 = mousedown
stepClickElement3 = .test-click-element
forceTour = 1

visualizations.conf

The following are the spec and example files for visualizations.conf.

visualizations.conf.spec

# Version 7.3.0
#
# This file contains definitions for visualizations an app makes available
# to the system. An app intending to share visualizations with the system
# should include a visualizations.conf in $SPLUNK_HOME/etc/apps/<appname>/default
#
# visualizations.conf should include one stanza for each visualization to be shared
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
#
http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

*******
# The possible attribute/value pairs for visualizations.conf are:
*******
* Create a unique stanza name for each visualization. It should match the name of the visualization
* Follow the stanza name with any number of the following attribute/value pairs.
* If you do not specify an attribute, Splunk uses the default.

disabled = <bool>
* Optional.
* Disable the visualization by setting to true.
* If set to true, the visualization is not available anywhere in Splunk
* Defaults to false.

allow_user_selection = <bool>
* Optional.
* Whether the visualization should be available for users to select
* Defaults to true

label = <string>
* Required.
* The human-readable label or title of the visualization
* Will be used in dropdowns and lists as the name of the visualization
* Defaults to <app_name>.<viz_name>

description = <string>
* Required.
* The short description that will show up in the visualization picker
* Defaults to ""

search_fragment = <string>
* Required.
* An example part of a search that formats the data correctly for the viz. Typically the last pipe(s) in a search query.
* Defaults to ""

default_height = <int>
* Optional.
* The default height of the visualization in pixels
* Defaults to 250

default_width = <int>
* Optional.
* The default width of the visualization in pixels
* Defaults to 250

min_height = <int>
* Optional.
* The minimum height the visualizations can be rendered in.
  * Defaults to 50.

  \[
  \text{min\_width} = \text{<int>}
  \]
  * Optional.
  * The minimum width the visualizations can be rendered in.
  * Defaults to 50.

  \[
  \text{max\_height} = \text{<int>}
  \]
  * The maximum height the visualizations supports.
  * Optional.
  * Default is unbounded.

  \[
  \text{max\_width} = \text{<int>}
  \]
  * The maximum width the visualizations supports.
  * Optional.
  * Default is unbounded.

  \[
  \text{trellis\_default\_height} = \text{<int>}
  \]
  * Default is 400

  \[
  \text{trellis\_min\_widths} = \text{<string>}
  \]
  * Default is undefined

  \[
  \text{trellis\_per\_row} = \text{<string>}
  \]
  * Default is undefined

# Define data sources supported by the visualization and their initial fetch params for search results data

```
\[
\text{data\_sources} = \text{<csv\-list>}
\]
```
* Comma separated list of data source types supported by the visualization.
* Currently the visualization system provides these types of data sources:
  * - primary: Main data source driving the visualization.
  * - annotation: Additional data source for time series visualizations to show discrete event annotation on the time axis.
  * Defaults to "primary"

```
\[
\text{data\_sources.<data\-source\-type>\text{.params.output_mode} = [\text{json\_rows}|\text{json\_cols}|\text{json}]}
\]
```
* Optional.
* the data format that the visualization expects. One of:
  * - "$\text{json\_rows}$": corresponds to SplunkVisualizationBase.\text{ROW\_MAJOR\_OUTPUT\_MODE}
  * - "$\text{json\_cols}$": corresponds to SplunkVisualizationBase.\text{COLUMN\_MAJOR\_OUTPUT\_MODE}
  * - "$\text{json}$": corresponds to SplunkVisualizationBase.\text{RAW\_OUTPUT\_MODE}
* Defaults to undefined and requires the javascript implementation to supply initial data params.
data_sources.<data-source-type>.params.count = <int>
* Optional.
* How many rows of results to request, default is 1000

data_sources.<data-source-type>.params.offset = <int>
* Optional.
* The index of the first requested result row, default is 0

data_sources.<data-source-type>.params.sort_key = <string>
* Optional.
* The field name to sort the results by

data_sources.<data-source-type>.params.sort_direction = [asc|desc]
* Optional.
* The direction of the sort
* - asc: sort in ascending order
* - desc: sort in descending order
* Defaults to desc

data_sources.<data-source-type>.params.search = <string>
* Optional.
* A post-processing search to apply to generate the results

data_sources.<data-source-type>.mapping_filter = <bool>
data_sources.<data-source-type>.mapping_filter.center = <string>
data_sources.<data-source-type>.mapping_filter.zoom = <string>
supports_trellis = <bool>
* Optional.
* Indicates whether trellis layout is available for this visualization
* Defaults to false

supports_drilldown = <bool>
* Optional.
* Indicates whether the visualization supports drilldown (responsive actions triggered when users click on the visualization).
* Defaults to false

supports_export = <bool>
* Optional.
* Indicates whether the visualization supports being exported to PDF.
* This setting has no effect in third party visualizations.
* Defaults to false

# Internal settings for bundled visualizations. They are ignored for third party visualizations.
core.type = <string>
core.viz_type = <string>
core.charting_type = <string>
core.mapping_type = <string>
core.order = <int>
core.icon = <string>
The following are the spec and example files for `web.conf`.

### web.conf.spec

```plaintext
#   Version 7.3.0
#
# This file contains possible attributes and values you can use to configure
# the Splunk Web interface.
# There is a web.conf in $SPLUNK_HOME/etc/system/default/. To set custom
# configurations, place a web.conf in $SPLUNK_HOME/etc/system/local/.
# For examples, see web.conf.example. You must restart Splunk software to enable
# configurations.
#
# To learn more about configuration files (including precedence) please see
# the documentation located at
#
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

[settings]
* Set general Splunk Web configuration options under this stanza name.
* Follow this stanza name with any number of the following setting/value pairs.
* If you do not specify an entry for each setting, Splunk Web uses the default value.

startwebserver = [0 | 1]
* Set whether or not to start Splunk Web.
* 0 disables Splunk Web, 1 enables it.
* Default: 1
```

No example
httpPort = <positive integer>
* The TCP port on which Splunk Web listens for incoming connections.
* Must be present for Splunk Web to start.
* If omitted or 0 the server will NOT start an http listener.
* If using SSL, set to the HTTPS port number.
* Default: 8000

gmtHostPort = <IP address:port>
* The IP address and host port of the splunkd process.
* Don’t include "http[s]://" when specifying this setting. Only include the IP address and port.
* Default: 0.0.0.0:8089

appServerPorts = <positive integer>[, <positive integer>, <positive integer> ...]
* Port number(s) for the python-based application server to listen on.
  This port is bound only on the loopback interface -- it is not exposed to the network at large.
* If set to "0", prevents the application server from being run from splunkd. Instead, Splunk Web starts as a separate python-based service which directly listens to the 'httpPort'. This is how Splunk 6.1.X and earlier behaved.
* Generally, you should only set one port number here. For most deployments a single application server won't be a performance bottleneck. However you can provide a comma-separated list of port numbers here and splunkd will start a load-balanced application server on each one.
* Set this setting to a non-zero value unless you experience compatibility problems. The new separate application server configuration is faster and supports more configuration options. Also, setting this to "0" can cause problems with new functionality, such as using the Search Head Clustering feature. See the [shclustering] stanza in server.conf for more information.
* Default: 8065

splunkdConnectionTimeout = <integer>
* The amount of time, in seconds, to wait before timing out when communicating with splunkd.
* Must be at least 30. If not
* Values smaller than 30 will be ignored, resulting in the use of the default value
* Default: 30

enableSplunkWebClientNetloc = <boolean>
* Control if the splunk web client can override the client network location
* Default: false
enableSplunkWebSSL = <boolean>
* Toggle between http or https.
* Set to true to enable https and SSL.
* Default: false

privKeyPath = <path>
* The path to the file containing the web server SSL certificate private key.
* A relative path is interpreted relative to $SPLUNK_HOME and may not refer
  outside of $SPLUNK_HOME (e.g., no ../*somewhere).
* You can also specify an absolute path to an external key.
* See also 'enableSplunkWebSSL' and 'serverCert'.
* No default.

serverCert = <path>
* Full path to the Privacy Enhanced Mail (PEM) format Splunk web server certificate file.
* The file may also contain root and intermediate certificates, if required.
  They should be listed sequentially in the order:
  [ Server SSL certificate ]
  [ One or more intermediate certificates, if required ]
  [ Root certificate, if required ]
* See also 'enableSplunkWebSSL' and 'privKeyPath'.
* Default: $SPLUNK_HOME/etc/auth/splunkweb/cert.pem

sslPassword = <password>
* Password that protects the private key specified by 'privKeyPath'.
* If encrypted private key is used, do not enable client-authentication on splunkd server. In [sslConfig] stanza of server.conf, 'requireClientCert' must be 'false'.
* Optional.
* Default: The unencrypted private key.

caCertPath = <path>
* DEPRECATED.
* Use 'serverCert' instead.
* A relative path is interpreted relative to $SPLUNK_HOME and may not refer
  outside of $SPLUNK_HOME (e.g., no ../*somewhere).
* No default.

requireClientCert = <boolean>
* Requires that any HTTPS client that connects to the Splunk Web HTTPS server has a certificate that was signed by the CA cert installed on this server.
* If "true", a client can connect ONLY if a certificate created by our certificate authority was used on that client.
* If "true", it is mandatory to configure splunkd with same root CA in server.conf.
  This is needed for internal communication between splunkd and
splunkweb.
* Default: false

sslCommonNameToCheck = <commonName1>, <commonName2>, ...
* Checks the common name of the client's certificate against this list
  of names.
* 'requireClientCert' must be set to "true" for this setting to work.
  * Optional.
  * Default: empty string (No common name checking).

sslAltNameToCheck = <alternateName1>, <alternateName2>, ...
* If this value is set, and 'requireClientCert' is set to true, Splunk Web will verify certificates which have a so-called
  "Subject Alternate Name" that matches any of the alternate names in
  this list.
* Subject Alternate Names are effectively extended descriptive
  fields in SSL certs beyond the commonName. A common practice for
  HTTPS certs is to use these values to store additional valid
  hostnames or domains where the cert should be considered valid.
* Accepts a comma-separated list of Subject Alternate Names to consider
  valid.
  * Optional.
  * Default: empty string (no alternate name checking).

serviceFormPostURL = http://docs.splunk.com/Documentation/Splunk
* DEPRECATED.
* This setting has been deprecated since Splunk Enterprise version
  5.0.3.

userRegistrationURL = https://www.splunk.com/page/sign_up
updateCheckerBaseURL = http://quickdraw.Splunk.com/js/
docsCheckerBaseURL = http://quickdraw.splunk.com/help
* These are various Splunk.com urls that are configurable.
* Setting 'updateCheckerBaseURL' to 0 stops Splunk Web from pinging
  Splunk.com for new versions of Splunk software.

enable_insecure_login = <boolean>
* Whether or not the GET-based "/account/insecurelogin" REST endpoint
  is enabled.
* Provides an alternate GET-based authentication mechanism.
  * If "true", the following url is available:
  * If "false", only the main /account/login endpoint is available
  * Default: false

simple_error_page = <boolean>
* Whether or not to display a simplified error page for HTTP errors that
  only contains the error status.
* If set to "true", Splunk Web displays a simplified error page for
  errors (404, 500, etc.) that only contain the error status.
* If set to "false", Splunk Web displays a more verbose error page that
  contains the home link, message, a more_results_link, crashes, referrer,
debug output, and byline
* Default: false

login_content = <string>
* Lets you add custom content to the login page.
* Supports any text including HTML.
* No default.

sslVersions = <comma-separated list>
* A comma-separated list of SSL versions to support.
* The versions available are "ssl3", "tls1.0", "tls1.1", and "tls1.2"
* The special version "*" selects all supported versions. The version "tls"
  selects all versions tls1.0 or newer
* If you prefix a version with "-", it is removed from the list.
* SSLv2 is always disabled; "-ssl2" is accepted in the version list, but does nothing.
* When 'appServerPorts'="0" only supported values are "all", "ssl3", "tls"
  and "tls"
* When configured in FIPS mode, "ssl3" is always disabled regardless of this configuration.
* NOTE: this setting only takes effect when 'appServerPorts' is set to a non-zero value.
* For the default, see $SPLUNK_HOME/etc/system/default/web.conf.

supportSSLV3Only = <boolean>
* When 'appServerPorts' is set to a non-zero value (the default mode), this setting is DEPRECATED. SSLv2 is now always disabled.
* The exact set of SSL versions allowed is now configurable via the 'sslVersions' setting above.
* When 'appServerPorts' is set to 0, this controls whether SSLv2 connections are disallowed.
* Default (when 'appServerPorts' is set to 0): false

cipherSuite = <cipher suite string>
* If set, uses the specified cipher string for the HTTP server.
* If not set, uses the default cipher string provided by OpenSSL. This is
  used to ensure that the server does not accept connections using weak encryption protocols.
* Must specify 'dhFile' to enable any Diffie-Hellman ciphers.
* The default can vary. See the cipherSuite setting in
  * $SPLUNK_HOME/etc/system/default/web.conf for the current default.

ecdhCurveName = <string>
* DEPRECATED.
* Use the 'ecdhCurves' setting instead.
* This setting specifies the Elliptic Curve Diffie-Hellman (ECDH) curve to
  use for ECDH key negotiation.
* Splunk only supports named curves that have been specified by their
SHORT name.
* The list of valid named curves by their short and long names can be obtained by running this CLI command:
  `$SPLUNK_HOME/bin/splunk cmd openssl ecparam -list_curves`
* Default: empty string.

ecdhCurves = <comma-separated list>
* A list of ECDH curves to use for ECDH key negotiation.
* The curves should be specified in the order of preference.
* The client sends these curves as a part of an SSL Client Hello.
* The server supports only the curves specified in the list.
* Splunk software only supports named curves that have been specified by their SHORT names.
* The list of valid named curves by their short and long names can be obtained by running this CLI command:
  `$SPLUNK_HOME/bin/splunk cmd openssl ecparam -list_curves`
* Example setting: "ecdhCurves = prime256v1,secp384r1,secp521r1"
* The default can vary. See the 'ecdhCurves' setting in `$SPLUNK_HOME/etc/system/default/web.conf` for the current default.

dhFile = <path>
* Full path to the Diffie-Hellman parameter file.
* Relative paths are interpreted as relative to $SPLUNK_HOME, and must not refer to a location outside of $SPLUNK_HOME.
* This file is required in order to enable any Diffie-Hellman ciphers.
* Default: not set.

root_endpoint = <URI_prefix_string>
* Defines the root URI path on which the appserver will listen
* For example, if you want to proxy the splunk UI at http://splunk:8000/splunkui,
  then set root_endpoint = /splunkui
* Default: /

static_endpoint = <URI_prefix_string>
* Path to static content.
* The path here is automatically appended to root_endpoint defined above
* Default: /static

static_dir = <relative_filesystem_path>
* The directory that holds the static content
* This can be an absolute URL if you want to put it elsewhere
* Default: share/splunk/search_mrsparkle/exposed

rss_endpoint = <URI_prefix_string>
* Path to static rss content
* The path here is automatically appended to what you defined in the 'root_endpoint' setting
* Default: /rss

embed_uri = <URI>
* Optional URI scheme/host/port prefix for embedded content
* This presents an optional strategy for exposing embedded shared 
  content that does not require authentication in a reverse proxy/single 
  sign on environment.
* Default: empty string, resolves to the client
  window.location.protocol + "//" + window.location.host

embed_footer = <html_string>
* A block of HTML code that defines the footer for an embedded report.
* Any valid HTML code is acceptable.
* Default: "splunk>"

tools.staticdir.generate_indexes = [1 | 0]
* Whether or not the webserver serves a directory listing for static 
  directories.
* Default: 0 (false)

template_dir = <relative_filesystem_path>
* The base path to the Mako templates.
* Default: "share/splunk/search_mrsparkle/templates"

module_dir = <relative_filesystem_path>
* The base path to Splunk Web module assets.
* Default: "share/splunk/search_mrsparkle/modules"

enable_gzip = <boolean>
* Whether or not the webserver applies gzip compression to responses.
* Default: true

use_future_expires = <boolean>
* Whether or not the Expires header of /static files is set to a 
  far-future date
* Default: true

flash_major_version = <integer>
flash_minor_version = <integer>
flash_revision_version = <integer>
* Specifies the minimum Flash plugin version requirements
* Flash support, broken into three parts.
* We currently require a min baseline of Shockwave Flash 9.0 r124

override_JSON_MIME_type_with_text_plain = <boolean>
* Whether or not to override the MIME type for JSON data served up 
  by Splunk Web endpoints with content-type="text/plain; charset=UTF-8"
* If "true", Splunk Web endpoints (other than proxy) that serve JSON 
  data will 
  serve as "text/plain; charset=UTF-8"
* If "false", Splunk Web endpoints that serve JSON data will serve as 
  "application/json; charset=UTF-8"

enable_proxy_write = <boolean>
* Indicates if the /splunkd proxy endpoint allows POST operations.
* If "true", both GET and POST operations are proxied through to splunkd.
* If "false", only GET operations are proxied through to splunkd.
* Setting to "false" prevents many client-side packages (such as the Splunk JavaScript SDK) from working correctly.
* Default: true

js_logger_mode = [None | Firebug | Server]
* The JavaScript Logger mode.
* Available modes: None, Firebug, Server
* Mode None: Does not log anything.
* Mode Firebug: Use firebug by default if it exists, or defer to the older less promiscuous version of firebug lite.
* Mode Server: Log to a defined server endpoint.
* See js/logger.js Splunk.Logger.Mode for mode implementation details and if you would like to author your own.
* Default: None

js_logger_mode_server_end_point = <URI_relative_path>
* The server endpoint to post JavaScript log messages
* Used when js_logger_mode = Server
* Default: util/log/js

js_logger_mode_server_poll_buffer = <integer>
* The interval, in milliseconds, to check, post, and cleanse the JavaScript log buffer
* Default: 1000

js_logger_mode_server_max_buffer = <integer>
* The maximum size threshold, in megabytes, to post and cleanse the JavaScript log buffer
* Default: 100

ui_inactivity_timeout = <integer>
* The length of time lapsed, in minutes, for notification when there is no user interface clicking, mouseover, scrolling, or resizing.
* Notifies client side pollers to stop, resulting in sessions expiring at the 'tools.sessions.timeout' value.
* If less than 1, results in no timeout notification ever being triggered (Sessions stay alive for as long as the browser is open).
* Default: 60

js_no_cache = <boolean>
* DEPRECATED.
* Toggles the JavaScript cache control.
* Default: false
cacheBytesLimit = <integer>
* When appServerPorts is set to a non-zero value, splunkd can keep a small cache of static assets in memory.
* When the total size of the objects in cache grows larger than this setting, in bytes, splunkd begins ageing entries out of the cache.
* If set to zero, disables the cache.
* Default: 4194304

cacheEntriesLimit = <integer>
* When appServerPorts is set to a non-zero value, splunkd can keep a small cache of static assets in memory.
* When the number of the objects in cache grows larger than this, splunkd begins ageing entries out of the cache.
* If set to zero, disables the cache.
* Default: 16384

staticCompressionLevel = <integer>
* When appServerPorts is set to a non-zero value, splunkd can keep a small cache of static assets in memory.
* Splunkd stores these assets in a compressed format, and the assets can usually be served directly to the web browser in compressed format.
* This level can be a number between 1 and 9. Lower numbers use less CPU time to compress objects, but the resulting compressed objects will be larger.
* There is not much benefit to decreasing the value of this setting from its default. Not much CPU time is spent compressing the objects.
* Default: 9

enable_autocomplete_login = <boolean>
* Indicates if the main login page lets browsers autocomplete the username.
* If "true", browsers may display an autocomplete drop down in the username field.
* If "false", browsers may not show autocomplete drop down in the username field.
* Default: false

verifyCookiesWorkDuringLogin = <boolean>
* Normally, the login page makes an attempt to see if cookies work properly in the user's browser before allowing them to log in.
* If you set this to "false", this check is skipped.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* Do not set to "false" in normal operations.
* Default: true

minify_js = <boolean>
* Whether the static JavaScript files for modules are consolidated and minified.
* Setting this to "true" improves client-side performance by reducing the number of HTTP
requests and the size of HTTP responses.

minify_css = <boolean>
* Indicates whether the static CSS files for modules are consolidated and minified
* Setting this to "true" improves client-side performance by reducing the number of HTTP requests and the size of HTTP responses.
* Due to browser limitations, disabling this when using Internet Explorer version 9 and earlier might result in display problems.

trap_module_exceptions = <boolean>
* Whether or not the JavaScript for individual modules is wrapped in a try/catch
* If "true", syntax errors in individual modules do not cause the UI to hang, other than when using the module in question.
* Set to "false" when developing apps.

enable_pivot_adhoc_acceleration = <boolean>
* DEPRECATED in version 6.1 and later, use 'pivot_adhoc_acceleration_mode' instead
* Whether or not the pivot interface uses its own ad-hoc acceleration when a data model is not accelerated.
* If "true", the pivot interface uses ad-hoc acceleration to make reporting in pivot faster and more responsive.
* In situations where data is not stored in time order, or where the majority of events are far in the past, disabling this behavior can improve the pivot experience.

pivot_adhoc_acceleration_mode = [Elastic | AllTime | None]
* Specifies the type of ad-hoc acceleration used by the pivot interface when a data model is not accelerated.
* If "Elastic", the pivot interface only accelerates the time range specified for reporting, and dynamically adjusts when this time range is changed.
* If "AllTime", the pivot interface accelerates the relevant data over all time. This makes the interface more responsive to time-range changes but places a larger load on system resources.
* If "None", the pivot interface does not use any acceleration. This means any change to the report requires restarting the search.
* Default: Elastic

jschart_test_mode = <boolean>
* Whether or not the JSChart module runs in Test Mode.
* If "true", JSChart module attaches HTML classes to chart elements for introspection.
* This negatively impacts performance and should be disabled unless you are actively using JSChart Test Mode.

#
# To avoid browser performance impacts, the JSChart library limits
# the amount of data rendered in an individual chart.

jschart_truncation_limit = <integer>
* Cross-browser truncation limit.
* If set, takes precedence over the browser-specific limits below

jschart_truncation_limit.chrome = <integer>
* Chart truncation limit.
* For Chrome only.
* Default: 50000

jschart_truncation_limit.firefox = <integer>
* Chart truncation limit.
* For Firefox only.
* Default: 50000

jschart_truncation_limit.safari = <integer>
* Chart truncation limit.
* For Safari only.
* Default: 50000

jschart_truncation_limit.ie11 = <integer>
* Chart truncation limit.
* For Internet Explorer version 11 only
* Default: 50000

jschart_series_limit = <integer>
* Chart series limit for all browsers.
* Default: 100

jschart_results_limit = <integer>
* DEPRECATED.
* Use 'data_sources.primary.params.count' in visualizations.conf instead.
* Chart results per series limit for all browsers.
* Overrides the results per series limit for individual visualizations.
* Default: 10000

choropleth_shape_limit = <integer>
* Choropleth map shape limit for all browsers.
* Default: 10000

dashboard_html_allow_inline_styles = <boolean>
* Whether or not to allow style attributes from inline HTML elements in dashboards.
* If "false", style attributes from inline HTML elements in dashboards will be removed to prevent potential attacks.
* Default: true

```
dashboard_html_allow_iframes = <boolean>
* Whether or not to allow iframes from HTML elements in dashboards.
* If "false", iframes from HTML elements in dashboards will be removed to prevent potential attacks.
* Default: true
```

```
splunk_dashboard_app_name = <string>
* Please do not change.
* Set the name for the Splunk Dashboard App.
* Default: splunk-dashboard-app
```

```
max_view_cache_size = <integer>
* The maximum number of views to cache in the appserver.
* Default: 1000
```

```
pdfgen_is_available = [0 | 1]
* Specifies whether Integrated PDF Generation is available on this search head.
* This is used to bypass an extra call to splunkd.
* Default (on platforms where node is supported): 1
* Default (on platforms where node is not supported): 0
```

```
version_label_format = <printf_string>
* Internal configuration.
* Overrides the version reported by the UI to *.splunk.com resources
* Default: %s
```

```
auto_refresh_views = [0 | 1]
* Specifies whether the following actions cause the appserver to ask splunkd to reload views from disk.
* Logging in through Splunk Web
* Switching apps
* Clicking the Splunk logo
* Default: 0
```

```#
# Splunk bar options
#
# Internal config. May change without notice.
# Only takes effect if 'instanceType' is 'cloud'.
#
```

```
showProductMenu = <boolean>
* Used to indicate visibility of product menu.
```
* Default: False.

**productMenuUriPrefix = <string>**
* The domain product menu links to.
* Required if 'showProductMenu' is set to "true".

**productMenuLabel = <string>**
* Used to change the text label for product menu.
* Default: 'My Splunk'

**showUserMenuProfile = <boolean>**
* Used to indicate visibility of 'Profile' link within user menu.
* Default: false

# # Header options #
## x_frame_options_sameorigin = <boolean>##
* adds a X-Frame-Options header set to "SAMEORIGIN" to every response served
* by cherrypy
* Default: true

# # Single Sign On (SSO) #
## remoteUser = <http_header_string>##
* Remote user HTTP header sent by the authenticating proxy server.
* This header should be set to the authenticated user.
* CAUTION: There is a potential security concern regarding the treatment of HTTP headers.
* Your proxy provides the selected username as an HTTP header as specified above.
* If the browser or other HTTP agent were to specify the value of this header, probably any proxy would overwrite it, or in the case that the username cannot be determined, refuse to pass along the request or set it blank.
* However, Splunk Web (specifically, cherrypy) normalizes headers containing the dash and the underscore to the same value. For example, USER-NAME and USER_NAME are treated as the same in Splunk Web.
* This means that if the browser provides REMOTE-USER and Splunk Web accepts REMOTE_USER, theoretically the browser could dictate the username.
* In practice, however, the proxy adds its headers last, which causes them to take precedence, making the problem moot.
* See also the 'remoteUserMatchExact' setting which can enforce more
exact
  header matching when running with 'appServerPorts' enabled.
* Default: 'REMOTE_USER'

remoteGroups = <http_header_string>
* Remote groups HTTP header name sent by the authenticating proxy server.
* This value is used by Splunk Web to match against the header name.
* The header value format should be set to comma-separated groups that the user belongs to.
* Example of header value: Products,Engineering,Quality Assurance
* No default.

remoteGroupsQuoted = <boolean>
* Whether or not the group header value can be comma-separated quoted entries.
* This setting is considered only when 'remoteGroups' is set.
* If "true", the group header value can be comma-separated quoted entries.
* NOTE: Entries themselves can contain commas.
* Example of header value with quoted entries:
  "Products","North America, Engineering","Quality Assurance"
* Default: false (group entries should be without quotes.)

remoteUserMatchExact = [0 | 1]
* Whether or not to consider dashes and underscores in a remoteUser header
to be distinct.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* When set to "1", considers dashes and underscores distinct (so "Remote-User" and "Remote_User" are considered different headers.)
* When set to 0, dashes and underscores are not considered to be distinct,
to retain compatibility with older versions of Splunk software.
* Set to 1 when you set up SSO with 'appServerPorts' enabled.
* Default: 0

remoteGroupsMatchExact = [0 | 1]
* Whether or not to consider dashes and underscores in a remoteGroup header
to be distinct.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* When set to 1, considers dashes and underscores distinct (so "Remote-Groups" and "Remote_Groups" are considered different headers)
* When set to 0, dashes and underscores are not considered to be distinct,
to retain compatibility with older versions of Splunk software.
* Set to 1 when you set up SSO with 'appServerPorts' enabled.
* Default: 0
SSOMode = [permissive | strict]
* Whether SSO behaves in either permissive or strict mode.
* When set to "permissive": Requests to Splunk Web that originate from an
  untrusted IP address are redirected to a login page where they can log into
  Splunk Web without using SSO.
* When set to "strict": All requests to Splunk Web will be restricted to those
  originating from a trusted IP except those to endpoints that do not require
  authentication.
* Default: strict

trustedIP = <ip_address>
* The IP address of the authenticating proxy (trusted IP).
* Splunk Web verifies it is receiving data from the proxy host for all SSO requests.
* Set to a valid IP address to enable SSO.
* If 'appServerPorts' is set to a non-zero value, this setting can accept a
  richer set of configurations, using the same format as the 'acceptFrom'
  setting.
* Default: not set; the normal value is the loopback address (127.0.0.1).

allowSsoWithoutChangingServerConf = [0 | 1]
* Whether or not to allow SSO without setting the 'trustedIP' setting in
  server.conf as well as in web.conf.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* If set to 1, enables web-based SSO without a 'trustedIP' setting configured
  in server.conf.
* Default: 0

testing_endpoint = <relative_uri_path>
* The root URI path on which to serve Splunk Web unit and integration testing resources.
* NOTE: This is a development only setting, do not use in normal operations.
* Default: /testing

testing_dir = <relative_file_path>
* The path relative to $SPLUNK_HOME that contains the testing files to be served at endpoint defined by 'testing_endpoint'.
* NOTE: This is a development only setting, do not use in normal operations.
* Default: share/splunk/testing

ssoAuthFailureRedirect = <scheme>://<URL>
* The redirect URL to use if SSO authentication fails.
  * Examples:
    * http://www.example.com
    * https://www.example.com
  * Default: empty string; Splunk Web shows the default unauthorized error page if SSO authentication fails.

# Results export server config

export_timeout = <integer>
  * When exporting results, the number of seconds the server waits before closing the connection with splunkd.
  * If you do not set a value for export_timeout, Splunk Web uses the value for the 'splunkdConnectionTimeout' setting.
  * Set 'export_timeout' to a value greater than 30 in normal operations.
  * No default.

# cherrypy HTTP server config

server.thread_pool = <integer>
  * The minimum number of threads the appserver is allowed to maintain.
  * Default: 20

server.thread_pool_max = <integer>
  * The maximum number of threads the appserver is allowed to maintain.
  * Default: -1 (unlimited)

server.thread_pool_min_spare = <integer>
  * The minimum number of spare threads the appserver keeps idle.
  * Default: 5

server.thread_pool_max_spare = <integer>
  * The maximum number of spare threads the appserver keeps idle.
  * Default: 10

server.socket_host = <ip_address>
  * Host values may be any IPv4 or IPv6 address, or any valid hostname.
  * The string 'localhost' is a synonym for '127.0.0.1' (or '::1', if your hosts file prefers IPv6).
  * The string '0.0.0.0' is a special IPv4 entry meaning "any active interface" (INADDR_ANY), and "::" is the similar IN6ADDR_ANY for IPv6.
  * Default (if 'listenOnIPV6' is set to "no"): 0.0.0.0
  * Default (otherwise): "::"

server.socket_timeout = <integer>
  * The timeout, in seconds, for accepted connections between the browser and Splunk Web
listenOnIPv6 = <no | yes | only>
* By default, Splunk Web listens for incoming connections using IPv4 only.
* To enable IPv6 support in splunkweb, set this to "yes". Splunk Web simultaneously listens for connections on both IPv4 and IPv6 protocols.
* To disable IPv4 entirely, set to "only", which causes Splunk Web to exclusively accept connections over IPv6.
* To listen on an IPV6 address, also set 'server.socket_host' to "::".

max_upload_size = <integer>
* The hard maximum limit, in megabytes, of uploaded files.
* Default: 500

log.access_file = <filename>
* The HTTP access log filename.
* This file is written in the default $SPLUNK_HOME/var/log directory.
* Default: web_access.log

log.access_maxsize = <integer>
* The maximum size, in bytes, that the web_access.log file can be.
* Comment out or set to 0 for unlimited file size.
* Splunk Web rotates the file to web_access.log.0 after the 'log.access_maxsize' is reached.
* See the 'log.access_maxfiles' setting to limit the number of backup files created.
* Default: 0 (unlimited size).

log.access_maxfiles = <integer>
* The maximum number of backup files to keep after the web_access.log file has reached its maximum size.
* CAUTION: Setting this to very high numbers (for example, 10000) can affect performance during log rotation.
* Default (if 'access_maxsize' is set): 5

log.error_maxsize = <integer>
* The maximum size, in bytes, the web_service.log can be.
* Comment out or set to 0 for unlimited file size.
* Splunk Web rotates the file to web_service.log.0 after the max file size is reached.
* See 'log.error_maxfiles' to limit the number of backup files created.
* Default: 0 (unlimited file size).

log.error_maxfiles = <integer>
* The maximum number of backup files to keep after the web_service.log file has reached its maximum size.
* CAUTION: Setting this to very high numbers (for example, 10000) can affect
performance during log rotations
* Default (if 'access_maxsize' is set): 5

log.screen = <boolean>
* Whether or not runtime output is displayed inside an interactive TTY.
  * Default: true

request.show_tracebacks = <boolean>
* Whether or not an exception traceback is displayed to the user on fatal
  exceptions.
  * Default: true

engine.autoreload_on = <boolean>
* Whether or not the appserver will auto-restart if it detects a python file
  has changed.
  * Default: false

tools.sessions.on = true
* Whether or not user session support is enabled.
  * Always set this to true.

tools.sessions.timeout = <integer>
* The number of minutes of inactivity before a user session is expired.
  * The countdown for this setting effectively resets every minute through
    browser activity until the 'ui_inactivity_timeout' setting is reached.
  * Use a value of 2 or higher, as a value of 1 causes a race condition with
    the browser refresh, producing unpredictable behavior.
  * Low values are not useful except for testing.
  * Default: 60

tools.sessions.restart_persist = <boolean>
* Whether or not the session cookie is deleted from the browser when the
  browser quits.
  * If set to "false", then the session cookie is deleted from the browser
    upon the browser quitting.
  * If set to "true", then sessions persist across browser restarts, assuming
    the 'tools.sessions.timeout' has not been reached.
  * Default: true

tools.sessions.httponly = <boolean>
* Whether or not the session cookie is available to running JavaScript scripts.
  * If set to "true", the session cookie is not available to running
    JavaScript scripts. This improves session security.
  * If set to "false", the session cookie is available to running
JavaScript scripts.
* Default: true

tools.sessions.secure = <boolean>
* Whether or not the browser must transmit session cookies over an HTTPS connection when Splunk Web is configured to serve requests using HTTPS (the 'enableSplunkWebSSL' setting is "true").
* If set to "true" and 'enableSplunkWebSSL' is also "true", then the browser must transmit the session cookie over HTTPS connections. This improves session security.
* See the 'enableSplunkWebSSL' setting for details on configuring HTTPS session support.
* Default: true

tools.sessions.forceSecure = <boolean>
* Whether or not the secure bit of a session cookie that has been sent over HTTPS is set.
* If a client connects to a proxy server over HTTPS, and the back end connects to Splunk over HTTP, then setting this to "true" forces the session cookie being sent back to the client over HTTPS to have the secure bit set.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* Default: false

response.timeout = <integer>
* The timeout, in seconds, to wait for the server to complete a response.
* Some requests, such as uploading large files, can take a long time.
* Default: 7200 (2 hours).

tools.sessions.storage_type = [file]
tools.sessions.storage_path = <filepath>
* Specifies the session information storage mechanisms.
* Set 'tools.sessions.storage_type' and 'tools.sessions.storage_path' to use RAM based sessions instead.
* Use an absolute path to store sessions outside of $SPLUNK_HOME.
* Default: storage_type=file, storage_path=var/run/splunk

tools.decode.on = <boolean>
* Whether or not all strings that come into CherryPy controller methods are decoded as unicode (assumes UTF-8 encoding).
* CAUTION: Setting this to false will likely break the application, as all incoming strings are assumed to be unicode.
* Default: true

tools.encode.on = <boolean>
* Whether or not to encode all controller method response strings into UTF-8 str objects in Python.
* CAUTION: Disabling this will likely cause high byte character encoding to fail.
* Default: true

tools.encode.encoding = <codec>
* Forces all outgoing characters to be encoded into UTF-8.
* This setting only takes effect when 'tools.encode.on' is set to "true".
* By setting this to "utf-8", CherryPy default behavior of observing the Accept-Charset header is overwritten and forces utf-8 output.
* Only change this if you know a particular browser installation must receive some other character encoding (Latin-1 iso-8859-1, etc)
* CAUTION: Change this setting at your own risk.
* Default: utf-8

tools.proxy.on = <boolean>
* Used for running Apache as a proxy for Splunk Web, typically for SSO configurations.
* Search the CherryPy website for "apache proxy" for more information.
* For Apache 1.x proxies only, set to "true". This configuration tells CherryPy (the Splunk Web HTTP server) to look for an incoming X-Forwarded-Host header and to use the value of that header to construct canonical redirect URLs that include the proper host name. For more information, refer to the CherryPy documentation on running behind an Apache proxy. This setting is only necessary for Apache 1.1 proxies.
* For all other proxies, you must set to "false".
* Default: false

tools.proxy.base = <scheme>://<URL>
* The proxy base URL in Splunk Web.
* Default: empty string

pid_path = <filepath>
* Specifies the path to the Process IDentification (pid) number file.
* Must be set to "var/run/splunk/splunkweb.pid".
* CAUTION: Do not change this parameter.

enabled_decomposers = <intention> [, <intention>]...
* Added in Splunk 4.2 as a short term workaround measure for apps which happen to still require search decomposition, which is deprecated with 4.2.
* Search decomposition will be entirely removed in a future release.
* A comma-separated list of allowed intentions.
* Modifies search decomposition, which is a Splunk Web internal behavior.
* Can be controlled on a per-app basis.
* If set to an empty string, no search decomposition occurs, which causes
some usability problems with Report Builder.
* The current possible values are: addcommand, stats, addterm,
  addtermlt, setfields, excludefields, audit, sort, plot
* Default: "plot", leaving only the plot intention enabled.

simple_xml_perf_debug = <boolean>
* Whether or not Simple XML dashboards log performance metrics to the
  browser console.
* If set to "true", Simple XML dashboards log some performance metrics
to the browser console.
* Default: false

job_min_polling_interval = <integer>
* The minimum polling interval, in milliseconds, for search jobs.
* This is the initial wait time for fetching results.
* The poll period increases gradually from the minimum interval
to the maximum interval when search is in a queued or parsing
state (and not a running state) for some time.
* Set this value between 100 and 'job_max_polling_interval'
  milliseconds.
* Default: 100

job_max_polling_interval = <integer>
* The maximum polling interval, in milliseconds, for search jobs.
* This is the maximum wait time for fetching results.
* In normal operations, set to 3000.
* Default: 1000

acceptFrom = <network_acl> ...
* Lists a set of networks or addresses from which to accept connections.
* This setting only takes effect when 'appServerPorts' is set to a
  non-zero value.
* Separate multiple rules with commas or spaces.
* Each rule can be in one of the following formats:
  1. A single IPv4 or IPv6 address (examples: "10.1.2.3", "fe80::4a3")
  2. A Classless Inter-Domain Routing (CIDR) block of addresses
     (examples: "10/8", "192.168.1/24", "fe80:1234/32")
  3. A DNS name, possibly with a "*" used as a wildcard
     (examples: "myhost.example.com", "*.splunk.com")
  4. "*", which matches anything
* You can also prefix an entry with '!' to cause the rule to reject the
  connection. The input applies rules in order, and uses the first one
  that matches.
  For example, "!10.1/16, *" allows connections from everywhere except
  the 10.1.*.* network.
* Default: "*" (accept from anywhere)

maxThreads = <integer>
* The number of threads that can be used for active HTTP transactions.
* This setting only takes effect when appServerPorts is set to a non-zero value.
* This value can be limited to constrain resource usage.
* If set to 0, a limit is automatically picked based on estimated server capacity.
* If set to a negative number, no limits are enforced.
* Default: 0

`maxSockets = <integer>`
* The number of simultaneous HTTP connections that Splunk Web can accept.
* This setting only takes effect when appServerPorts is set to a non-zero value.
* This value can be limited to constrain resource usage.
* If set to 0, a limit is automatically picked based on estimated server capacity.
* If set to a negative number, no limits are enforced.
* Default: 0

`keepAliveIdleTimeout = <integer>`
* How long, in seconds, that the Splunk Web HTTP server lets a keep-alive connection remain idle before forcibly disconnecting it.
* If this number is less than 7200, it will be set to 7200.
* Default: 7200

`busyKeepAliveIdleTimeout = <integer>`
* How long, in seconds, that the Splunk Web HTTP server lets a keep-alive connection remain idle while in a busy state before forcibly disconnecting it.
* CAUTION: Too large a value that can result in file descriptor exhaustion due to idling connections.
* If this number is less than 12, it will be set to 12.
* Default: 12

`forceHttp10 = auto|never|always`
* How the HTTP server deals with HTTP/1.0 support for incoming clients.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* When set to "always", the REST HTTP server does not use some HTTP 1.1 features such as persistent connections or chunked transfer encoding.
* When set to "auto", it limits HTTP 1.1 features only if the client sent no User-Agent header, or if the user agent is known to have bugs in its HTTP/1.1 support.
* When set to "never", it always allows HTTP 1.1, even to clients it suspects might be buggy.
* Default: auto
crossOriginSharingPolicy = <origin_acl> ... 
* A list of HTTP Origins for which to return Access-Control-Allow-* 
  (CORS) headers.
* This setting only takes effect when 'appServerPorts' is set to a 
  non-zero value.
* These headers tell browsers that Splunk Web trusts web applications 
  at those sites to make requests to the REST interface.
* The origin is passed as a URL without a path component (for example 
  "https://app.example.com:8000")
* This setting can take a list of acceptable origins, separated 
  by spaces and/or commas
* Each origin can also contain wildcards for any part. Examples:
  *://app.example.com:* (either HTTP or HTTPS on any port)
  https://*.example.com (any host under example.com, including 
  example.com itself)
* An address can be prefixed with a '!' to negate the match, with 
  the first matching origin taking precedence. For example,
  "!://evil.example.com:* *://*.example.com:*" to not avoid 
  matching one host in a domain.
* "*" can also be used to match all origins.
* Default: empty string

allowSslCompression = <boolean>
* Whether or not the server lets clients negotiate SSL-layer data 
  compression.
* This setting only takes effect when 'appServerPorts' is set 
  to a non-zero value. When 'appServerPorts' is zero or not set, this 
  setting 
  is "true".
* If set to "true", the server lets clients negotiate SSL-layer 
  data compression.
* The HTTP layer has its own compression layer which is usually 
  sufficient.
* Default (if 'appServerPorts' is set and not 0): false 
* Default (if 'appServerPorts' is 0 or not set): true

allowSslRenegotiation = <boolean>
* Whether or not the server lets clients renegotiate SSL connections.
* This setting only takes effect when 'appServerPorts' is set to a 
  non-zero value.
* In the SSL protocol, a client may request renegotiation of the 
  connection 
  settings from time to time.
* Setting this to "false" causes the server to reject all renegotiation 
  attempts, breaking the connection.
* This limits the amount of CPU a single TCP connection can use, but it 
  can cause connectivity problems especially for long-lived connections.
* Default: true

sendStrictTransportSecurityHeader = <boolean>
* Whether or not the REST interface sends a "Strict-Transport-Security"
header with all responses to requests made over SSL.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* If set to "true", the REST interface sends a "Strict-Transport-Security" header with all responses to requests made over SSL.
* This can help avoid a client being tricked later by a Man-In-The-Middle attack to accept a non-SSL request.
* This requires a commitment that no non-SSL web hosts will ever be run on this hostname on any port. For example, if splunkweb is in default non-SSL mode this can break the ability of browser to connect to it.
* Enable this setting with caution.
* Default: false

dedicatedIoThreads = <integer>
* The number of dedicated threads to use for HTTP input/output operations.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* If set to zero, HTTP I/O is performed in the same thread that accepted the TCP connection.
* If set set to a non-zero value, separate threads run to handle the HTTP I/O, including SSL encryption.
* Typically this does not need to be changed. For most usage scenarios using the same the thread offers the best performance.
* Default: 0

replyHeader.<name> = <string>
* Adds a static header to all HTTP responses that this server generates.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* For example, "replyHeader.My-Header = value" causes Splunk Web to include the response header "My-Header: value" in the reply to every HTTP request to it.
* No default.

termsOfServiceDirectory = <directory>
* The directory to look in for a "Terms of Service" document that each user must accept before logging into Splunk Web.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* Inside the directory the TOS should have a filename in the format "<number>.html"
* <number> is in the range 1 to 18446744073709551615.
* The active TOS is the filename with the larger number. For example, if there are two files in the directory named "123.html" and "456.html", then
456 will be the active TOS version.
* If a user has not accepted the current version of the TOS, they must accept it the next time they try to log in. The acceptance times will be recorded inside a "tos.conf" file inside an app called "tos".
* If the "tos" app does not exist, you must create it for acceptance times to be recorded.
* The TOS file can either be a full HTML document or plain text, but it must have the ".html" suffix.
* You do not need to restart Splunk Enterprise when adding files to the TOS directory.
* Default: empty string (no TOS)

appServerProcessShutdownTimeout = <nonnegative integer>[smhd]
* The amount of time splunkd waits for a Python-based application server process to handle outstanding or existing requests.
* This setting only takes effect when 'appServerPorts' is set to a non-zero value.
* If a Python-based application server process "outlives" this timeout, splunkd forcibly terminates the process.
* Default: '10m' (10 minutes).

enableWebDebug = <boolean>
* Whether or not the debug REST endpoints are accessible, for example., /debug/**splat.
* Default: false

allowableTemplatePaths = <directory> [, <directory>][...]
* A comma-separated list of template paths that may be added to the template lookup whitelist.
* Paths are relative to $SPLUNK_HOME.
* Default: empty string

enable_risky_command_check = <boolean>
* Whether or not checks for data-exfiltrating search commands are enabled.
* default true

customFavicon = <pathToMyFile, myApp:pathToMyFile, or blank for default>
* Customizes the favicon image across the entire application.
* If no favicon image file, the favicon default: the Splunk favicon.
  * Supported favicon image files are .ico files, and should be square images.
  * Place the favicon image file in the default or manual location:
    * Default destination folder: $SPLUNK_HOME/etc/apps/search/appserver/static/customfavicon.
    * Example: If your favicon image is located at $SPLUNK_HOME/etc/apps/search/appserver/static/customfavicon/favicon.ico, set 'customFavicon' to "customfavicon/favicon.ico".
    * Manual location: Place the file in $SPLUNK_HOME/etc/apps/<myApp>/appserver/static/<pathToMyFile>, and set
'customFavicon' to
"<myApp:pathToMyFile>".
* Default: not set, Splunk Web uses the Splunk favicon.

loginCustomLogo = <fullUrl, pathToMyFile, myApp:pathToMyFile, or blank for default>
* Customizes the logo image on the login page.
* If no image file, the logo Default: the Splunk logo.
* Supported images are:
  * Full URL image file (secured or not secured), such as
  * Image file, such as .jpg or .png. All image formats are supported.
    * Place logo image file in default or manual location:
      * Default destination folder:
        $SPLUNK_HOME/etc/apps/search/appserver/static/logincustomlogo.
        * Example: If your logo image is located at
          $SPLUNK_HOME/etc/apps/search/appserver/static/logincustomlogo/logo.png,
          type loginCustomLogo = logincustomlogo/logo.png.
      * Manual location:
        $SPLUNK_HOME/etc/apps/<myApp>/appserver/static/<pathToMyFile>, and type
        loginCustomLogo = <myApp:pathToMyFile>.
    * The maximum image size is 485px wide and 100px high. If the image
      exceeds these limits, the image is automatically resized.
    * Default: not set, Splunk Web uses the Splunk logo.

loginBackgroundImageOption = [default| custom | none]
* Controls display of the background image of the login page.
  * "default" displays the Splunk default background image.
  * "custom" uses the background image defined by the
    backgroundImageCustomName setting.
  * "none" removes any background image on the login page. A dark
    background color is applied.
  * Default: "default".

loginCustomBackgroundImage = <pathToMyFile or myApp:pathToMyFile>
* Customizes the login page background image.
  * Supported image files include .jpg, .jpeg or .png with a maximum
    file size of 20MB.
  * A landscape image is recommended, with a minimum resolution of
    1024x640 pixels.
  * Using Splunk Web:
    * Upload a custom image to a manager page under General Settings.
    * The login page background image updates automatically.
  * Using the CLI or a text editor:
    * Set 'loginBackgroundImageOption' to "custom".
    * Place the custom image file in the default or manual location:
      * Default destination folder:
        $SPLUNK_HOME/etc/apps/search/appserver/static/logincustombg.
        * Example: If your image is located at
          $SPLUNK_HOME/etc/apps/search/appserver/static/logincustombg/img.png, set
          'loginCustomBackgroundImage' to "logincustombg/img.png".
* Manual location: 
  ${SPLUNK_HOME/etc/apps/<myApp>/appserver/static/<pathToMyFile>}, and set
  'loginCustomBackgroundImage' to
  "<myApp:pathToMyFile>".
  * The login page background image updates automatically.
  * Default: not set (If no custom image is used, the default Splunk
    background image displays).

loginFooterOption = [default | custom | none]
* Controls display of the footer message of the login page.
  * "default" displays the Splunk copyright text.
  * "custom" uses the footer text defined by the loginFooterText setting.
  * "none" removes any footer text on the login page.
  * NOTE: This option is made available only to OEM customers
    participating in
    the Splunk OEM Partner Program and is subject to the relevant terms of
    the Master OEM Agreement. All other customers or partners are prohibited
    from
    removing or altering any copyright, trademark, and/or other
    intellectual
    property or proprietary rights notices of Splunk placed on or embedded
    in any Splunk materials.
  * Default: "default".

loginFooterText = <footer_text>
* The text to display in the footer of the login page.
  * Supports any text, including HTML.
  * To display, the parameter 'loginFooterOption' must be set to "custom".

loginDocumentTitleOption = [default | custom | none]
* Controls display of the document title of the login page.
  * Default: "default".
  * "default" displays: "<page_title> | Splunk".
  * "none" removes the branding on the document title of the login page:
    "<page_title>".
  * "custom" uses the document title text defined by the
    loginDocumentTitleText setting.
  * NOTE: This option is made available only to OEM customers
    participating in
    the Splunk OEM Partner Program and is subject to the relevant terms of
    the
    Master OEM Agreement. All other customers or partners are prohibited
    from
    removing or altering any copyright, trademark, and/or other
    intellectual
    property or proprietary rights notices of Splunk placed on or embedded
    in any Splunk materials.
  * Default: "default".

loginDocumentTitleText = <document_title_text>
* The text to display in the document title of the login page.
  * Text only.
* To display, the parameter 'loginDocumentTitleOption' must be set to "custom".

loginPasswordHint = <default_password_hint>
* The text to display the password hint at first time login on the login page.
* Text only.
* Default: "changeme"

appNavReportsLimit = <integer>
* Maximum number of reports to fetch to populate the navigation drop-down menu of an app.
* An app must be configured to list reports in its navigation XML configuration before it can list any reports.
* Set to -1 to display all the available reports in the navigation menu.
* NOTE: Setting to either -1 or a value that is higher than the default might result in decreased browser performance due to listing large numbers of available reports in the drop-down menu.
* Default: 500

# The Django bindings component and all associated [framework] settings have been removed. Configuring these settings no longer has any effect, and Splunk Enterprise ignores any existing settings that are related to the component.

# custom cherrypy endpoints

[endpoint:<python_module_name>]
* Registers a custom python CherryPy endpoint.
* The expected file must be located at:
  $SPLUNK_HOME/etc/apps/<APP_NAME>/appserver/controllers/<PYTHON_NODULE_NAME>.py
* This module's methods will be exposed at
  /custom/<APP_NAME>/<PYTHON_NODULE_NAME>/<METHOD_NAME>

# exposed splunkd REST endpoints

[expose:<unique_name>]
* Registers a splunkd-based endpoint that should be made available to the UI under the "/splunkd" and "/splunkd/__raw" hierarchies.
* The name of the stanza does not matter as long as it begins with "expose:"
* Each stanza name must be unique.

pattern = <url_pattern>
* The pattern to match under the splunkd /services hierarchy.
* For instance, "a/b/c" would match URIs "/services/a/b/c" and "/servicesNS/*/a/b/c",
* The pattern cannot include leading or trailing slashes.
* Inside the pattern an element of "*" matches a single path element. For example, "a/*/c" would match "a/b/c" but not "a/1/2/c".
* A path element of "**" matches any number of elements. For example, "a/**/c" would match both "a/1/c" and "a/1/2/3/c".
* A path element can end with a "*" to match a prefix. For example, "a/elem-*//b" would match "a/elem-123/c".

methods = <method_lists>
* A comma-separated list of methods to allow from the web browser (example: "GET,POST,DELETE").
* Default: "GET"

oidEnabled = [0 | 1]
* Whether or not a REST endpoint is capable of taking an embed-id as a query parameter.
* If set to 1, the endpoint is capable of taking an embed-id as a query parameter.
* This is only needed for some internal splunk endpoints, you probably should not specify this for app-supplied endpoints
* Default: 0

skipCSRFProtection = [0 | 1]
* Whether or not Splunk Web can safely post to an endpoint without applying Cross-Site Request Forgery (CSRF) protection.
* If set to 1, tells Splunk Web that it is safe to post to this endpoint without applying CSRF protection.
* This should only be set on the login endpoint (which already contains sufficient auth credentials to avoid CSRF problems).
* Default: 0

---

**web.conf.example**

# Version 7.3.0
#
# This is an example web.conf. Use this file to configure data web settings.
#
# To use one or more of these configurations, copy the configuration block
# into web.conf in $SPLUNK_HOME/etc/system/local/. You must restart Splunk
# to enable configurations.
#
# To learn more about configuration files (including precedence) please
# the documentation located at
# http://docs.splunk.com/Documentation/Splunk/latest/Admin/Aboutconfigurationfiles

# This stanza heading must precede any changes.
[settings]

# Change the default port number:
httpport = 12800
# Also run the python application server on a non-default port:
appServerPorts = 12801

# Turn on SSL:
enableSplunkWebSSL = true
# absolute paths may be used here.
privKeyPath = /home/user/certs/myprivatekey.pem
serverCert = /home/user/certs/mycacert.pem
# NOTE: non-absolute paths are relative to $SPLUNK_HOME

# First party apps:
splunk_dashboard_app_name = splunk-dashboard-app
Notable Event Action SDK

Use the Notable Event Actions SDK

The Notable Events Action SDK comes packaged with ITSI and is located in $SPLUNK_HOME/etc/apps/SA-ITOA/lib/itsi/event_management/sdk. The SDK is implemented in Python and includes:

1. Methods for custom actions on ITSI episodes: class CustomGroupActionBase in custom_group_action_base.py
2. Methods for working on an ITSI episode post-custom action: class EventGroup in grouping.py
3. Methods for finding metadata for ITSI notable events: class EventMeta in eventing.py
4. Methods for finding metadata for ITSI episodes: class GroupMeta in grouping.py

Custom actions require a class that derives from CustomGroupActionBase and implements the execute() method. The __init__() method of your class needs to initialize the base class CustomGroupActionBase.

For more information, see the Notable events action SDK reference in this manual.

The following is a summary of the custom action Ping Host that ships with ITSI:

class Ping(CustomGroupActionBase):
    def __init__(self, settings):
        # initialize CustomGroupActionBase
        super(Ping, self).__init__(settings, self.logger)

    def get_host_to_ping(self):
        # from input settings, fetch host to ping
        # some logic is abstracted in custom_event_action_base.py
        ...
        return host

    def ping(self, host):
        # does the act of pinging the host
        ...

    def execute(self):
        # has all the logic of ping in here...
        host = self.get_host_to_ping()
std_out, std_err = self.ping(host)

# do other stuff here, like add a comment to an ITSI episode
# or add a few tags, and so on....
# change the state of the episode....
for data in self.get_group():
    group_id = data.get('itsi_group_id')
    group = EventGroup(self.get_session_key(), self.logger)
    group.create_comment(itsi_group_id, comment)
    group.create_comment(itsi_group_id, out)
    group.create_tag(itsi_group_id, 'ping')
return

if __name__=='__main__':
    if len(sys.argv) > 1 and sys.argv[1] == '--execute':
        input_params = sys.stdin.read()
        ping = Ping(input_params)
        ping.execute()

Notable Event Actions SDK reference

The Notable Events Action SDK contains three main modules.

- custom_group_action_base
- eventing
- grouping

Use the custom_group_action_base module when you want to consume the output of your moderator alerts (modalert).

Use the eventing module to get information about your events in ITSI. This module must reside on the same host where ITSI is installed. All classes in this module inherit from the EventBase class. This base class tracks the session key, username, password, and logger info.

Use the grouping module to operate on your episodes in ITSI. This module must reside on the same host where ITSI is installed.

```python
class custom_group_action_base.CustomGroupActionBase(settings, logger)
```

Import the custom_group_action_base module when you want to consume the output of your modalert. In your script, inherit your class from the CustomGroupActionBase class. Use the get_group() method to work on the episode that triggered your script.
**Parameter** | **Type** | **Description**
--- | --- | ---
settings | basestring or dictionary | Incoming parameters passed to the script using stdin. 
logger | logger | The logger instance of the inherited class. 

**Raises**

**Type Error** - Raised when settings is not a serialized JSON string.

**Returns**

A CustomGroupActionBase instance.

**Return type**

CustomGroupActionBase.

**execute()**

Implement this method to configure the actions to take based on the alert output. Derived classes must implement this method.

**Raises**

**Not Implemented Error** - Raised when the execute() method is not implemented in the derived class.

**extract_group_or_event_id(notable_data)**

Use this method to get the ID of the event or episode that triggered the action.

**Parameter** | **Type** | **Description**
--- | --- | ---
notable_data | basestring | Notable event or episode object from which the event_ID or itsi_group_id is extracted. 

**Raises**

**Type Error** - Raised if notable_data is of type None.

**Exception** - Raised if notable_data is not JSON type data.

**Returns**

The event_id or itsi_group_id.

**Return type**

basestring.
get_config()

Gets the configuration based on the settings.

Returns

The configuration that comes with the settings.

Return type
Configuration.

get_group()

Gets the episode that triggered the custom action. This method relies on get_results_file() and expects the returned file path to be a .csv.gz format.

The method is implemented as a generator because there can be thousands of episodes.

Raises

Value Error - Raised when there is not a valid .csv.gz results file. It prints out what file format was returned instead.

Returns

A dictionary type object until all received episodes are returned.

Return type
dictionary

get_results_file()

Gets the results file, which is where results are temporarily stored.

Raises

Attribute Error - Raised when no results file is returned.

Returns

The results file.

Return type
Results file.

get_session_key()

Gets the Splunk session key.
Raises

**Attribute Error** - Raised when no session key is returned.

**Returns**
The session key.

**Return type**
basestring.

class eventing.EventMeta(*args)

Import this class to get information about ITSI events, such as status, owner, and severities.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_key</td>
<td>basestring</td>
<td>The session key that is given by splunkd when you log in. If you do not have a session key, pass in None, but you will need to provide username and password credentials.</td>
</tr>
<tr>
<td>username</td>
<td>basestring</td>
<td>Your username.</td>
</tr>
<tr>
<td>password</td>
<td>basestring</td>
<td>Your password.</td>
</tr>
<tr>
<td>logger</td>
<td>logger</td>
<td>A place to log actions in an existing logger. If you do not have a logger, then the ITSI logger is used.</td>
</tr>
</tbody>
</table>

Raises

**Type Error** - Raised when the `session_key` is not a basestring type or when the `session_key` is not valid.

**Value Error** - Raised when the `session_key` is a zero-length string, or when the `username` and `password` are empty strings and the `session_key` is of type None.

**Returns**
An EventMeta instance.

**Return type**
EventMeta.

get_all_owners()

Get all valid owner values for a notable event.

**Returns**
A list of all configured owners.  

Return type  
list.

get_all_severities()  
Get all severity values for a notable event.  

Returns  
A list of all configured severities.  
Return type  
list.

get_all_statuses()  
Get all status values for a notable event.  

Returns  
A list of all configured statuses.  
Return type  
list.

class eventing.Event(session_key, *args, **kwargs)  
Import this class to get information about ITSI events.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_key</td>
<td>basestring</td>
<td>The session key that is given by splunkd when you log in. If you do not have a session key, pass in None, but you will need to provide username and password credentials.</td>
</tr>
<tr>
<td>username</td>
<td>basestring</td>
<td>Your username.</td>
</tr>
<tr>
<td>password</td>
<td>basestring</td>
<td>Your password.</td>
</tr>
<tr>
<td>logger</td>
<td>logger</td>
<td>A place to log actions in an existing logger. If you do not have a logger, then the ITSI logger is used.</td>
</tr>
</tbody>
</table>

Raises
**Type Error** - Raised when the `session_key` is not a basestring type or when the `session_key` is not valid.

**Value Error** - Raised when the `session_key` is a zero-length string, or when the `username` and `password` are empty strings and the `session_key` is of type None.

**Returns**

An Event instance.

**Return type**

Event.

`get_owner(*args, **kwargs)`

Return the owners, given a list of events or event IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>events</code></td>
<td>list of dictionaries</td>
<td>Each dictionary in the list represents an event that was sent by Splunk as an outcome of a custom action. The <code>get_event()</code> method in the CustomGroupActionBase class generates such an item.</td>
</tr>
<tr>
<td><code>event_ids</code></td>
<td>basestring or list</td>
<td>The unique ID of an event.</td>
</tr>
<tr>
<td><code>split_by</code></td>
<td>basestring</td>
<td>If <code>event_ids</code> is of type basestring, then it is split into a list of event IDs. By default, ',' separates the event IDs.</td>
</tr>
<tr>
<td><code>**kwargs</code></td>
<td>dict</td>
<td>A dictionary with the keys <code>earliest_time</code> and <code>latest_time</code> with corresponding values.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when `events` is not of type basestring or of type list.

**Value Error** - Raised when both `events` and `event_ids` are of type None.

**Returns**

The event IDs and corresponding owners.

**Return type**

list of tuples.
**get_status(*args, **kwargs)**

Return the statuses, given a list of events or event IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>list of dicts</td>
<td>Each dictionary in the list represents an event that was sent by Splunk as an outcome of a custom action. The get_event() method in the CustomGroupActionBase class generates such an item.</td>
</tr>
<tr>
<td>event_ids</td>
<td>basestring or list</td>
<td>The unique ID of an event.</td>
</tr>
<tr>
<td>split_by</td>
<td>basestring</td>
<td>If event_ids is of type basestring, then it is split into a list of event IDs. By default, ',' separates the event IDs.</td>
</tr>
<tr>
<td>**kwargs</td>
<td>dict</td>
<td>A dictionary with the keys earliest_time and latest_time with corresponding values.</td>
</tr>
</tbody>
</table>

**Raises**

- **Type Error** - Raised when events is not of type list.
- **Value Error** - Raised when both events and event_ids are of type None.

**Returns**

The event IDs and corresponding statuses.

**Return type**

list of tuples.

**get_severity(*args, **kwargs)**

Return the severities, given a list of events or event IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>events</td>
<td>list of dicts</td>
<td>Each dictionary in the list represents an event that was sent by ITSI as an outcome of a custom action. The get_event() method in the CustomGroupActionBase class generates such an event.</td>
</tr>
<tr>
<td>event_ids</td>
<td>basestring / list</td>
<td>The unique ID of an event.</td>
</tr>
<tr>
<td>split_by</td>
<td>basestring</td>
<td>If event_ids is of type basestring, then it is split into a list of event IDs. By default, ',' separates the event IDs.</td>
</tr>
</tbody>
</table>

585
Parameter | Type | Description
---|---|---
**kwargs | dict | A dictionary with the keys `earliest_time` and `latest_time` with corresponding values.

*Raises*

**Type Error** - Raised when `events` is not of type basestring or of type list.
**Value Error** - Raised when both `events` and `event_ids` are of type `None`.

*Returns*

The event IDs and corresponding severities.

*Return type*

list of tuples.

class grouping.GroupMeta(*args)*

Import this class to get information about ITSI episodes, such as all available statuses, owners, and severities.

Parameter | Type | Description
---|---|---
session_key | basestring | The session key that is given by splunkd when you log in. If you do not have a session key, pass in `None`, but you will need to provide username and password credentials.
username | basestring | Your username.
password | basestring | Your password.
logger | logger | A place to log actions in an existing logger. If you do not have a logger, then the ITSI logger is used.

*Raises*

**Type Error** - Raised when the `session_key` is not a basestring type or when the `session_key` is not valid.
**Value Error** - Raised when the `session_key` is a zero-length string, or when the `username` and `password` are empty strings and the `session_key` is of type `None`.

*Returns*

An `GroupMeta` instance.
Return type
GroupMeta.

get_all_owners()
Get all valid owner values for an episode.

Returns
A list of all configured owners.
Return type
list.

get_all_severities()
Get all severity values for an episode.

Returns
A list of all configured severities.
Return type
list.

get_all_statuses()
Get all status values for an episode.

Returns
A list of all configured statuses.
Return type
list.

class grouping.EventGroup(session_key, *args, **kwargs)
Import this class to operate on ITSI episodes.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>session_key</td>
<td>basestring</td>
<td>The session key that is given by splunkd when you log in. If you do not have a session key, pass in None, but you will need to provide username and password credentials.</td>
</tr>
</tbody>
</table>
### create_tag(*args)

Create a tag, given an episode ID.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_id</td>
<td>basestring</td>
<td>An episode ID.</td>
</tr>
<tr>
<td>tag_value</td>
<td>basestring</td>
<td>New value for the tag.</td>
</tr>
<tr>
<td>raise_exceptions</td>
<td>bool</td>
<td>Raise an exception. By default this value is False</td>
</tr>
</tbody>
</table>

**Raises**

- **Type Error** - Raised when the `group_id` or `tag_value` is an empty string.
- **Value Error** - Raised when the `group_id` is a zero-length string, or when the `username` and `password` are empty strings and the `session_key` is of type None.

**Returns**

The episode ID, the new tag, and the tag ID.

**Return type**

dictionary.
**delete_all_tags(group_id)**

Delete all of the tags associated with an episode, given an episode ID.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_id</td>
<td>basestring</td>
<td>An episode ID.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when the `group_id` is an empty string.

**Returns**

Nothing.

**delete_tag(tag_id)**

Delete the tag value, given a tag ID.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag_id</td>
<td>basestring</td>
<td>The ID of the tag to be retrieved.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when the `tag_id` is an empty string.

**Returns**

Nothing.

**delete_ticket_info(group_ids, ticket_system, ticket_id)**

Delete external ticket information, given a list of episode IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_ids</td>
<td>basestring or list</td>
<td>A comma-separated string of episode IDs, or a list of episode IDs.</td>
</tr>
<tr>
<td>ticket_system</td>
<td>basestring</td>
<td>The name of an external ticket system.</td>
</tr>
<tr>
<td>ticket_id</td>
<td>basestring</td>
<td>The external ticket ID.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when `group_ids` is not of type basestring or of type list.
**Value Error** - Raised when `group_ids` is an empty string or list.

**Returns**
The episode IDs of successful and failed deletions.

**Return type**
dictionary.

`get_all_comments(group_id)`

Get all of the comments associated with an episode, given an episode ID.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_id</td>
<td>basestring</td>
<td>An episode ID.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when the `group_id` is an empty string.

**Returns**
All of the comments corresponding to the episode ID.

**Return type**
list.

`get_all_tags(group_id)`

Get all of the tags, given an episode ID.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_id</td>
<td>basestring</td>
<td>An episode ID.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when `group_id` is an empty string.

**Returns**
All of the existing tags for a given episode.

**Return type**
list.

`get_comment(comment_id)`

Get the comment, given a comment ID.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>comment_id</td>
<td>basestring</td>
<td>The ID of the comment to get.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when the `comment_id` is an empty string.

**Returns**

The comment corresponding to the ID.

**Return type**

basestring.

**get_owner(**args, **kwargs)**

Return the owners, given a list of episodes or episode IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>list of dicts</td>
<td>Each dictionary in the list represents an episode that was sent by Splunk as an outcome of a custom action. The <code>get_group()</code> method in the <code>CustomGroupActionBase</code> class generates such an item.</td>
</tr>
<tr>
<td>group_ids</td>
<td>basestring or list</td>
<td>The unique ID of an episode.</td>
</tr>
<tr>
<td>split_by</td>
<td>basestring</td>
<td>If <code>group_ids</code> is of type basestring, then it is split into a list of episode IDs. By default, ',' separates the episode IDs.</td>
</tr>
<tr>
<td>**kwargs</td>
<td>dict</td>
<td>A dictionary with the keys <code>earliest_time</code> and <code>latest_time</code> with corresponding values.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when `groups` is not of type basestring or of type list.

**Value Error** - Raised when both `groups` and `group_ids` are of type `None`.

**Returns**

The episode IDs and corresponding owners.

**Return type**

list of tuples.
**get_status(*args, **kwargs)**

Return the statuses, given a list of episodes or episode IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>list of dicts</td>
<td>Each dictionary in the list represents an episode that was sent by Splunk as an outcome of a custom action. The <code>get_group()</code> method in the CustomGroupActionBase class generates such an item.</td>
</tr>
<tr>
<td>group_ids</td>
<td>basestring or list</td>
<td>The unique ID of an episode.</td>
</tr>
<tr>
<td>split_by</td>
<td>basestring</td>
<td>If <code>group_ids</code> is of type basestring, then it is split into a list of episodes IDs. By default, ',' separates the episode IDs.</td>
</tr>
<tr>
<td>**kwargs</td>
<td>dict</td>
<td>A dictionary with the keys <code>earliest_time</code> and <code>latest_time</code> with corresponding values.</td>
</tr>
</tbody>
</table>

**Raises**

- **TypeError** - Raised when `groups` is not of type list.
- **Value Error** - Raised when both `groups` and `groups_ids` are of type None.

**Returns**
The episode IDs and corresponding statuses.

**Return type**
list of tuples.

**get_severity(*args, **kwargs)**

Return the severities, given a list of episodes or episode IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groups</td>
<td>list of dicts</td>
<td>Each dictionary in the list represents an episode that was sent by ITSI as an outcome of a custom action. The <code>get_group()</code> method in the CustomGroupActionBase class generates such an episode.</td>
</tr>
<tr>
<td>group_ids</td>
<td>basestring or list</td>
<td>The unique ID of an episode.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Type</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>split_by</td>
<td>basestring</td>
<td>If group_ids is of type basestring, then it is split into a list of episode IDs. By default, ',' separates the episode IDs.</td>
</tr>
<tr>
<td>**kwargs</td>
<td>dict</td>
<td>A dictionary with the keys earliest_time and latest_time with corresponding values.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when groups is not of type basestring or of type list.

**Value Error** - Raised when both groups and group_ids are of type None.

**Returns**

The episode IDs and corresponding severities.

**Return type**

list of tuples.

**get_tag(tag_id)**

Get the value of a tag, given a tag ID.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tag_id</td>
<td>basestring</td>
<td>The ID of the tag to be retrieved.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when the tag_id is an empty string.

**Returns**

The tag value corresponding to the tag ID.

**Return type**

basestring.

**update(*args, **kwargs)**

Update the status, severity, and owner of each episode individually.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>blob</td>
<td>list / dict</td>
<td>A list of dicts containing episode IDs and the severity, status, and/or owner that they should be updated to.</td>
</tr>
</tbody>
</table>
Parameter | Type | Description
---|---|---
split_by | basestring | If the `group_ids` in `blob` is of type basestring, then it is split into a list of episode IDs. By default, ',' separates the episode IDs.
**kwargs | dict | A dictionary with the keys `earliest_time` and `latest_time` with corresponding values.

**Raises**

- **Key Error** - Raised when the `group_ids` key is missing from the `blob` dictionary.
- **Type Error** - Raised when `blob` is neither of type list nor of type dictionary.
- **Value Error** - Raised when `blob` is empty.

**Returns**
The episode ID schemas with updated fields, in the order of input.

**Return type**
dictionary.

`update_owner(*args, **kwargs)`

Update the owner of each episode, given a list of episode IDs.

Parameter | Type | Description
---|---|---
group_ids | basestring or list | A comma-separated string of episode IDs or a list of episode IDs.
owner | basestring | The owner of the episode.
split_by | basestring | If the `group_ids` is of type basestring, then it is split into a list of episode IDs. By default, ',' separates the episode IDs.
**kwargs | dict | A dictionary with the keys `earliest_time` and `latest_time` with corresponding values.

**Raises**

- **Type Error** - Raised when `group_ids` is neither of type basestring nor of type list.
- **Value Error** - Raised when `group_ids` is an empty list, or when `owner` is not a valid string.
**Returns**

The episode ID schemas with updated owners, in the order of input.

**Return type**

dictionary.

**update_severity(*args, **kwargs)**

Update the severity value of each episode, given a list of episode IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_ids</td>
<td>basestring or list</td>
<td>A comma-separated string of episode IDs, or a list of episode IDs.</td>
</tr>
<tr>
<td>severity</td>
<td>basestring</td>
<td>One of the supported severity values.</td>
</tr>
<tr>
<td>split_by</td>
<td>basestring</td>
<td>If the <code>group_ids</code> is of type basestring, then it is split into a list of episode IDs. By default, ',' separates the episode IDs.</td>
</tr>
<tr>
<td>**kwargs</td>
<td>dict</td>
<td>A dictionary with the keys <code>earliest_time</code> and <code>latest_time</code> with corresponding values.</td>
</tr>
</tbody>
</table>

**Raises**

**Type Error** - Raised when `group_ids` is neither of type basestring nor of type list.

**Value Error** - Raised when `group_ids` is an empty list, or when `severity` is not a valid string.

**Returns**

The episode ID schemas with updated severities, in the order of input.

**Return type**

dictionary.

**update_status(*args, **kwargs)**

Update the status of each episode, given a list of episode IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_ids</td>
<td>basestring or list</td>
<td>A comma-separated string of episode IDs, or a list of episode IDs.</td>
</tr>
<tr>
<td>status</td>
<td>basestring</td>
<td>One of the supported statuses.</td>
</tr>
</tbody>
</table>
Parameter | Type | Description
---|---|---
split_by | basestring | If the `group_ids` is of type basestring, then it is split into a list of episode IDs. By default, ',' separates the episode IDs.

**kwargs | dict | A dictionary with the keys `earliest_time` and `latest_time` with corresponding values.

** Raises

** Type Error ** - Raised when `group_ids` is neither of type basestring nor of type list.
** Value Error ** - Raised when `group_ids` is an empty list, or when `status` is not a valid string.

** Returns **
The episode ID schemas with updated statuses, in the order of input.

** Return type **
dictionary.

** update_tag(*args) **
Update the tag, given an episode ID and a tag ID.

Parameter | Type | Description
---|---|---
group_id | basestring | An episode ID.
tag_id | basestring | The tag ID.
tag_value | basestring | The new value for the tag.

** Raises

** Type Error ** - Raised when the `group_id` or `tag_id` are empty strings.

** Returns **
The committed value.

** Return type **
dictionary.
**update_ticket_info(*args, **kwargs)**

Update episodes with external ticket information, given a list of episode IDs.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_ids</td>
<td>basestring or list</td>
<td>A comma-separated string of episode IDs, or a list of episode IDs.</td>
</tr>
<tr>
<td>ticket_system</td>
<td>basestring</td>
<td>The name of an external ticket system.</td>
</tr>
<tr>
<td>ticket_id</td>
<td>basestring</td>
<td>The external ticket ID.</td>
</tr>
<tr>
<td>ticket_url</td>
<td>basestring</td>
<td>The URL to reach the external ticket.</td>
</tr>
<tr>
<td>**kwargs</td>
<td>dict</td>
<td>A dictionary of additional parameters to add to the ticket information.</td>
</tr>
</tbody>
</table>

**Raises**

- **Type Error** - Raised when the `group_ids` is not of type basestring or of type list.
- **Value Error** - Raised when the `group_ids` is an empty string or list.

**Returns**

The episode IDs of successful and failed updates.

**Return type**

dictionary.

**add_drilldown(self, group_id, drilldown)**

Adds drilldown to an episode.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_id</td>
<td>basestring</td>
<td>The ID of the episode where add_drilldown is operated on.</td>
</tr>
<tr>
<td>drilldown</td>
<td>dict</td>
<td>The drilldown data that is added.</td>
</tr>
</tbody>
</table>

**Raises**

- **Attribute Error** - Raised when the `group_id` not available.
- **Value Error** - Raised when drilldown data is not a dictionary with link and name.

**Returns**

Return dictionary which holds updated keys.
**Return type**
dictionary.

**update_drilldown(self, group_id, drilldown)**

Updates a drilldown for an episode.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_id</td>
<td>basestring</td>
<td>The ID of the episode that owns the updated drill down.</td>
</tr>
<tr>
<td>drilldown</td>
<td>dict</td>
<td>The drilldown that is updated.</td>
</tr>
</tbody>
</table>

**Raises**

**Value Error** - Raised when drilldown data is not a dictionary with link and name.

**Returns**

Return dictionary which holds updated keys.

**Return type**
dictionary.

**delete_drilldown(self, group_id, drilldown)**

Deletes a drilldown for an episode.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group_id</td>
<td>basestring</td>
<td>The ID of the episode that owns the deleted drill down.</td>
</tr>
<tr>
<td>drilldown</td>
<td>dict</td>
<td>The drilldown that is deleted.</td>
</tr>
</tbody>
</table>

**Raises**

**Value Error** - Raised when drilldown data is not a dictionary with link and name.

**Returns**

Return dictionary which holds updated keys.

**Return type**
dictionary.
Troubleshooting

Search IT Service Intelligence logs

IT Service Intelligence log files have a prefix of itsi_.

- IT Service Intelligence search command logs are located in
  \$SPLUNK_HOME/var/run/splunk/dispatch/<session_id>/itsi_search.log.
- All other ITSI logs are located in \$SPLUNK_HOME/var/log/splunk.

All ITSI logs have a source type of itsi_internal_log to make them easy to search.

Steps

1. Run the following Splunk search to search ITSI logs:

   ```
   index = _internal sourcetype=itsi_internal_log
   ```

2. Click the **source** field under Selected Fields to see specific log files.

For Windows deployments, the ITSI search command log, itsi_search.log, cannot be searched in Splunk Web. You must open the file on the Windows host using a text editor.

See also

- See ITSI Health Check dashboard for IT Service Intelligence log messages.
- See What Splunk software logs about itself for general information about Splunk logging.