Splunk® Common Information Model Add-on
Common Information Model Add-on Manual 4.20.0

Table of Contents

Table of Contents

Introduction

Overview of the Splunk Common Information Model

The Splunk **Common Information Model (CIM)** is a shared semantic model focused on extracting value from data. The CIM is implemented as an add-on that contains a collection of data models, documentation, and tools that support the consistent, normalized treatment of data for maximum efficiency at search time.

The CIM add-on contains a collection of preconfigured **data models** that you can apply to your data at search time. Each data model in the CIM consists of a set of field names and tags that define the least common denominator of a domain of interest. You can use these data models to normalize and validate data at search time, accelerate key data in searches and dashboards, or create new reports and visualizations with Pivot.

The add-on also contains several tools that are intended to make analysis, validation, and alerting easier and more consistent. These tools include a custom command for CIM validation and a common action model, which is the common information model for custom alert actions. See Approaches to using the CIM for more information about the tools available in the CIM add-on.

Why the CIM exists

The CIM helps you to normalize your data to match a common standard, using the same field names and event tags for equivalent events from different sources or vendors. The CIM acts as a search-time schema ("schema-on-the-fly") to allow you to define relationships in the event data while leaving the raw machine data intact.

After you have normalized the data from multiple different source types, you can develop reports, correlation searches, and dashboards to present a unified view of a data domain. You can display your normalized data in the dashboards provided by other Splunk applications such as Splunk Enterprise Security and the Splunk App for PCI Compliance. The dashboards and other reporting tools in apps that support CIM compliance display only the data that is normalized to the tags and fields defined by the Common Information Model.

The Splunk Common Information Model add-on is packaged with Splunk Enterprise Security and the Splunk App for PCI Compliance.

How to use this manual

The Data Models chapter of this manual provides reference documentation for the fields and tags that make up each data model. Refer to the reference tables to determine what tags and fields are expected for each dataset in a data model as you work to normalize a new data source to the CIM. See How to use these reference tables.

This manual also provides a step-by-step guide for how to apply the CIM to your data at search time. The Using the Common Information Model chapter of the manual includes a walkthrough of the procedure you should follow to

- Use the CIM to normalize data at search time
- Use the CIM to validate your data
- Use the CIM to create reports and dashboards
- Use the common action model to build a custom alert action.

The manual also includes two detailed examples that further demonstrate how to use the CIM to normalize data at search time.

- Use the CIM to normalize CPU performance metrics

What data models are included

The data models are included in the Splunk Common Information Model Add-on. You can find the JSON implementations of the data models in `$SPLUNK_HOME/etc/apps/Splunk_SA_CIM/default/data/models`.

For a list of data models, see CIM fields per associated data model.

For cloud purposes, there is not one specific data model. Most of the cloud data fields are mapped to existing data models. For example, authentication is authentication regardless if it's in the cloud or not. For samples of how events map differently from various cloud providers such as AWS, Azure, and GCP to CIM data model field names, see the following field mappings:

- Authentication Field Mapping
- Change Field Mapping
- Network Traffic Field Mapping
- Data Access Field Mapping

For use cases on cloud data sources, see the following resources:

- Security
    ◆ Splunk Security Essentials
    ◆ Use Analytic Stories for actionable guidance in Splunk Enterprise Security
- IT
    ◆ Splunk IT Essentials
    ◆ Splunk IT Service Intelligence
- Observability
    ◆ Splunk Observability Cloud

How the Splunk CIM compares to the DMTF CIM

The Splunk Common Information Model is an independent standard, unaffiliated with the Distributed Management Task Force CIM.

The DMTF CIM is different from the Splunk CIM. The DMTF is more hierarchical, more complex, and more comprehensive than the Splunk CIM. In the DMTF CIM, all models inherit from a single parent node, with child nodes for each model, then additional branching child nodes for sub-concepts. Thus, the DMTF's individual sub-nodes can be very complex with multiple branches in order to define most possible configurations.

In contrast, the Splunk CIM is relatively flat, simple, and flexible, because it defines only the least common denominator of concepts in a given domain rather than all possible concepts in the domain. The Splunk CIM defines fewer concepts than the DMTF CIM in order to give the developer maximum flexibility.

Prerequisites

This manual assumes you are familiar with the full data lifecycle in the Splunk platform. If you are not yet sure how to get your data in, see *Getting Data In* for more information on how to set up the Splunk platform to accept new data or to learn about the types of data the Splunk platform can index.

Get started

To get started, see Install the Common Information Model Add-on.

Install the Splunk Common Information Model Add-on

1. Download the Common Information Model add-on from Splunkbase at https://apps.splunk.com/app/1621/.
2. Review the indexes defined in CIM.
    1. The previously deprecated `cim_summary` index definition is now removed. If you have a custom configuration for this in your local `indexes.conf` file, it will persist as-defined.
        1. If you are no longer using this index definition, remove the stanza from your local `indexes.conf` file before installation.
        2. If you are still using it, you will need to revise the stanza if you were previously relying on parts of the deprecated default `cim_summary` index definition.
    2. The `cim_modactions` index definition is used with the common action model alerts and auditing. Make sure that the index exists and assign the appropriate Roles to search the index.
3. Install the Splunk Common Information Model Add-on to your search heads only.

    Refer to Installing add-ons for detailed instructions describing how to install a Splunk add-on in the following deployment scenarios:

    - Single-instance Splunk Enterprise
    - Distributed Splunk Enterprise
    - Splunk Cloud Platform
    - Splunk Light

Next: See Set up the Splunk Common Information Model Add-on to perform optional configurations to improve performance.

Set up the Splunk Common Information Model Add-on

Perform optional configurations on the Splunk Common Information Model Add-on Setup page.

- Constrain the indexes that each data model searches in order to improve performance.
- Configure the tag whitelist that each data model searches.
- Enable or adjust the acceleration of each data model.

Access the setup page by selecting **Apps > Manage Apps** and then clicking **Set up** in the row for Splunk Common Information Model. You can only use the setup page on Splunk platform version 6.4.x or later. With Splunk_SA_CIM version 4.11.0 and lower, you need to have the admin_all_objects capability. With Splunk_SA_CIM version 4.12.0 and higher, you need to have the accelerate_datamodel capability. If you do not see a link to set up the app, you can access the setup page directly by going to `https://<URL of your Splunk deployment>/en-US/app/search/cim_setup`.

Set index constraints

Improve performance by constraining the indexes that each data model searches. By default, each data model searches all indexes.

1. In Splunk Web, access the CIM Setup page:

- ♦ Select **Apps > Manage Apps** and then click **Set up** in the row for Splunk Common Information Model.
- ♦ Access the setup page directly by going to `https://<URL of your Splunk deployment>/en-US/app/search/cim_setup`.

2. Select the data model that you want to modify.
3. In **Indexes whitelist**, type the index that the data model should search. You can type the names of indexes that are defined only on indexers.
4. Click **Save**.

If you constrain a data model to selected indexes and then later add another index to your environment that is also relevant to the data model, return to this page and add the new index to the data model constraints.

Accelerating CIM data models

Enable acceleration for data models to return results faster for searches, reports, and dashboard panels that reference the data model.

The summary range settings of a data model affect the size of the data models on disk and also affect the processing load on the indexers due to the load of creating accelerated data alongside the index buckets. See Enable data model acceleration in the *Knowledge Manager Manual* for Splunk Enterprise.

All data models included in the CIM add-on have data model acceleration disabled by default.

If you have Splunk Enterprise Security or the Splunk App for PCI Compliance installed, configuration settings automatically accelerate some of the data models in the CIM. If you use these apps, do not make changes to acceleration settings on the CIM setup page because your changes do not persist. Instead, make changes in the **Data Model Acceleration Enforcement** modular input on your search head. The modular input overrides the acceleration status that you set on the CIM setup page to make sure that the apps continue to work.

If you use the CIM without these apps installed, you can choose to accelerate one or more of the data models manually.

Enable data model acceleration

Configure the acceleration parameters of the CIM data models in the CIM Setup view.

1. In Splunk Web, access the CIM Setup page:
   - ♦ Select **Apps > Manage Apps** and then click **Set up** in the row for Splunk Common Information Model.
   - ♦ Access the setup page directly by going to `https://<URL of your Splunk deployment>/en-US/app/search/cim_setup`.
2. Select a data model that you want to accelerate.
3. Select the check box next to **Accelerate** to accelerate the model.
4. (Optional) Configure the advanced acceleration settings.

Parameter	Description	More information
Backfill range	How far back in time the Splunk platform creates its column stores, specified as a relative time string. Only set this parameter if you want to backfill less data than the retention period set by Earliest time. Refer to `datamodels.conf.spec` for warnings and limitations.	See `datamodels.conf.spec` and Advanced configurations for persistently accelerated data models in the *Knowledge*
Summary range	How far back in time the Splunk platform keeps these column stores, specified as a relative time string. Backfill Range should be more	

Parameter	Description	
	recent than Summary Range.	*Manager Manual* in the Splunk Enterprise documentation.
Max summarization search time	The maximum amount of time that the column store creation search is allowed to run, in seconds.	
Accelerate until maximum time	When selected, runs the acceleration search until the maximum time is reached.	**More information**
Max concurrent summarization searches	The maximum number of concurrent acceleration instances for this data model that the scheduler is allowed to run.	
Manual rebuilds	When selected, prevents the summarize command from rebuilding outdated summaries. Admins can manually rebuild a data model in Settings. Select **Settings > Data Models** and locate the row for the data model. Click **Rebuild** to rebuild the data model.	
Schedule priority	Raises the scheduling priority of a summary search, as follows: ♦ 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. This field is only available in Splunk platform 6.5.x or later.	
Indexes whitelist	Restricts the index attribute of the data model to specified index values to improve performance.	
Tags whitelist	Restricts the tag attribute of the data model to specified tag values to improve performance. By default, the whitelists for each CIM data model contain the tags used as constraints for the child datasets as well as the tags used in any searches within the model. Do not remove these tags, or data model searches that rely on these tags will fail. You can add additional tags to this whitelist to accommodate how you have applied tags to your data. Add additional tags that you need to use to search and filter within searches for a data model.	The tags_whitelist setting is only available in Splunk Enterprise 6.6.0 and above. For organizations running Splunk Enterprise 6.6.4 and above, there is a UI component to manage the tags_whitelist setting via the Splunk Web UI. For organizations running Splunk Enterprise 6.6.0 - 6.6.3, the tags_whitelist setting must be managed manually via conf file access. See datamodels.conf.spec and Set a tag whitelist for better data model search performance in the *Knowledge Manager Manual* in the Splunk Enterprise documentation.

5. Click **Save**.

For more information about accelerated data models and data model acceleration jobs, see Check the status of data model accelerations in this topic.

Disable acceleration for a data model

If you have Splunk Enterprise Security or the Splunk App for PCI Compliance installed, some of the data models in the CIM are automatically accelerated by configuration settings in these apps. If you want to change which data models are accelerated by these apps, access the **Data Model Acceleration Enforcement** modular input on your search head and make your changes there. If you attempt to de-accelerate a data model using any other method, including using the Settings tab in the CIM Setup page, your changes will not persist because the the app acceleration enforcement re-accelerates the data models automatically.

If you do not have an app installed that enforces the acceleration of any CIM data models, you can edit the acceleration settings on the CIM Setup page.

1. In Splunk Web, access the CIM Setup page:
     - Select **Apps > Manage Apps** and then click **Set up** in the row for Splunk Common Information Model.
     - Access the setup page directly by going to `https://<URL of your Splunk deployment>/en-US/app/search/cim_setup`.
2. Select the data model for which you want to disable acceleration.
3. Deselect the check box next to **Enable acceleration** to stop accelerating the data model.
4. Click **Save**.

Change the summary range for data model accelerations

A data model's summary range setting affects the size of the data models on disk, and the processing load of creating accelerated data alongside the index buckets.

1. In Splunk Web, access the CIM Setup page:
     - Select **Apps > Manage Apps** and then click **Set up** in the row for Splunk Common Information Model.
     - Access the setup page directly by going to `https://<URL of your Splunk deployment>/en-US/app/search/cim_setup`.
2. Select the data model you want to change.
3. Set a summary range:
     1. Make sure that **Enable acceleration** is checked. A summary range only applies to accelerated data models.
     2. Review the **Earliest time** setting to determine the current summary range.
     3. Change the **Earliest time** setting.
        For example, -1y, -3mon, -1mon, -1w, -1d, or 0 for "All Time".
4. Click **Save**.

The CIM Setup page only displays CIM data models. You cannot change the settings of a custom data model on the CIM Setup page. To change the summary range or other settings on a custom data model, manually edit the `datamodels.conf` provided with the app or add-on. For more information, see the datamodels.conf spec file in the Splunk Enterprise *Admin Manual*.

Check the status of data model accelerations

Use the Data Model Audit dashboard to display information about the state of data model accelerations in your environment. Alternatively, use the `` `cim_datamodelinfo` `` macro to search the data model statuses from the search bar.

To access the dashboard:

1. Open the **Search and Reporting** app.
2. In the menu bar, click **Dashboards**.

3. Select the **Data Model Audit** dashboard.

Panel	Description
Top Accelerations By Size	Displays the accelerated data models sorted in descending order by MB on disk
Top Accelerations By Run Duration	Displays the accelerated data models sorted in descending order by the time spent on running acceleration tasks.
Acceleration Details	Displays a table of the accelerated data models with additional information.

Data model acceleration can be in progress and 100% complete at the same time. The process running and the status completing are not directly tied together.

Release notes for the Splunk Common Information Model Add-on

Version 4.20.0 of the Splunk Common Information Model Add-on was released on June 30, 2021.

New features

Version 4.20.0 of the Splunk Common Information Model Add-on includes the following new features.

Enhancement	Description
New Data Access data model.	The Data Access data model is for monitoring shared data access user activity. It helps you detect a user's unauthorized data access, misuse, exfiltration, and more. See Data Access.
The Endpoint data model has a new field.	The new field in the data model is `original_file_name`. Certain EDR products include this field to help discover if a file is renamed. See Endpoint.
jQuery 3.5.0 migration.	Starting in CIM 4.20.0 to enhance product security, jQuery is migrated from 2.1.0 to 3.5.0 and some Splunk Web Core UI components are deprecated. Library updates have been made that may impact some dashboards with CustomJS.

Upgrade requirements

Splunk platform version	Upgrade activity
8.0.x or later	If you apply custom tags to data mapped to CIM data models and you use these tags in searches and search filters, add these tags to the whitelists for those models. See Set up the Splunk Common Information Model Add-on for details about the tags whitelist field.

Compatibility

Version 4.20.x of the Splunk Common Information Model Add-on requires Splunk platform version 8.0.x or later. Some workarounds, such as the datamodels spec workaround for tags_whitelist and poll_buckets, are no longer available in version 7.0.x and later. This might lead to btool check warnings at startup.

Fixed issues

This version of the Splunk Common Information Model Add-on fixes the following issues. If this section is empty, this release has no reported fixed issues.

Date resolved	Issue number	Description
2021-06-29	CIM-1033, CIM-978	CIM Setup: "An error occurred fetching assets"
2021-03-16	CIM-990	Adaptive response actions creates duplicate Invocations.

Known issues

This version of the Splunk Common Information Model Add-on has the following reported known issues. If this section is empty, this release has no reported known issues.

Date filed	Issue number	Description
2021-07-02	CIM-1040	CIM 4.20.0 Setup link returns 404 Workaround: Access the setup page directly by going to https://<URL of your Splunk deployment>/en-US/app/search/cim_setup

Deprecated or removed features

The following are deprecated or removed features for the last seven versions.

As of version 4.20.0:

- N/A

As of version 4.19.0:

- N/A

As of version 4.18.0:

- The `body` field is deprecated in favor of the `description` field in the Alerts data model and will be removed in a future version.
- The `subject` field is deprecated in favor of the `signature` field in the Alerts data model and will be removed in a future version.

As of version 4.15.0:

- The Predictive Analytics dashboard is removed in favor of Machine Learning Toolkit functionality.

As of version 4.14.0:

- The Predictive Analytics dashboard is deprecated in favor of Machine Learning Toolkit functionality and will be removed in a future version.

As of version 4.13.0:

- N/A

As of version 4.12.0:

- The modaction_invocations_rest_handler.py (alerts/modaction_invocations) is deprecated and will be removed in a future version.
- The following previously deprecated configurations are removed.
    - `search_activity` macro
    - `search_typer` macro
- Deprecated data models: Application State and Change Analysis

Third-party software attributions

The Splunk Common Information Model Add-on does not incorporate any third-party software or libraries.

Support and resource links for the Splunk Common Information Model Add-on

Download

Download the Splunk Common Information Model Add-on at http://apps.splunk.com/app/1621/

Questions and answers

Access questions and answers specific to the Splunk Common Information Model Add-on at http://answers.splunk.com/app/questions/1621.html

Support

For general Splunk platform support, see the Splunk Support Programs page: http://www.splunk.com/support

If you have specific questions about the Splunk Common Information Model Add-on, log a case using the Splunk Support Portal at https://www.splunk.com/index.php/submit_issue.

More resources

Access these Splunk platform resources for more help:

- The Splunk Enterprise documentation at http://docs.splunk.com/Documentation/Splunk/latest
- The Splunk Cloud Platform documentation at http://docs.splunk.com/Documentation/SplunkCloud
- The Splunk Light documentation at http://docs.splunk.com/Documentation/SplunkLight
- The #splunk IRC channel on EFNET

Data models

How to use the CIM data model reference tables

Each topic in this section contains a use case for the data model, a breakdown of the required tags for the event datasets or search datasets in that model, and a listing of all extracted and calculated fields included in the model.

A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

How to read the tags tables

The tags tables communicate which tags you must apply to your events in order to make them CIM-compliant. These tags act as **constraints** to identify your events as relevant to this data model, so that this data is included in Pivot reports, searches, and dashboards based on this model.

There might be additional constraints outside the scope of these tables. Refer to the data model itself using its editor view in Splunk Web for required fields, field=value combinations, or base searches that the model depends on.

Apply tags to your events to ensure your data is populated in the correct dashboards, searches, and Pivot reports.

1. Identify the CIM data model relevant to your events.
2. Identify the dataset within that model that is relevant to your events.
3. Observe which tags are required for that dataset.
4. Observe which tags are required for any parent datasets.
5. Observe any other constraints relevant to the dataset or its parents.
6. Apply those tags and other constraints to your events using event types.
7. Repeat for any additional relevant CIM datasets.

For a detailed walkthrough of these steps, see Use the CIM to normalize data at search time.

How to read the fields tables

The fields tables list the **extracted fields** and **calculated fields** for the event and search datasets in the model and provide descriptions and expected values (if relevant) for these fields.

How to find a field

The table presents the fields in alphabetical order, starting with the fields for the root datasets in the model, then proceeding to any unique fields for child datasets. The table does not repeat any fields that a child dataset inherits from a parent dataset, so refer to the parent dataset to see the description and expected values for that field.

Because the fields tables exclude inherited fields, many child datasets have no fields listed in the table at all. Those child datasets include only inherited fields from one or more of their parent datasets, so there are no unique extracted or calculated fields to display. All data models inherit the fields `_time`, `host`, `source`, and `sourcetype`, so those fields are always available to you for use in developing Pivot reports, searches, and dashboards.

How to interpret the expected values

For some fields, the tables include one or more expected values for that field. These expected values include:

- values that are used in knowledge objects in downstream applications such as Splunk Enterprise Security (in the table as "ES expects")
- values that are used in the CIM model as constraints for a dataset (in the table as "Other")

In some cases, the expected values also include additional values that Splunk suggests as the normalized standards for a field. The expected values are provided to help you make normalization decisions when developing add-ons. They are not exhaustive or exclusive.

Use the tables to apply the Common Information Model to your data

The tables in this section of documentation are intended to be supplemental reference for the data models themselves. Use the documentation and the data model editor in Splunk Web together. You can also access all of the information about a data model's dataset hierarchy, fields, field descriptions, and expected values in the JSON file of the model. You can browse the JSON in the `$SPLUNK_HOME/etc/apps/Splunk_SA_CIM/default/data/models` directory.

Prerequisite

You need Write access to a data model in order to browse it in its editor view. If you do not have this access, request it from your Splunk administrator.

Steps

1. In Splunk Web, go to **Settings > Data Models** to open the **Data Models** page.
2. Click a data model to view it in an editor view. There, you can see the full dataset hierarchy, a complete listing of constraints for each dataset, and full listing of all inherited, extracted, and calculated fields for each dataset.
3. Compare this information with the reference tables in the documentation for descriptions and expected values of the fields in each datasets.
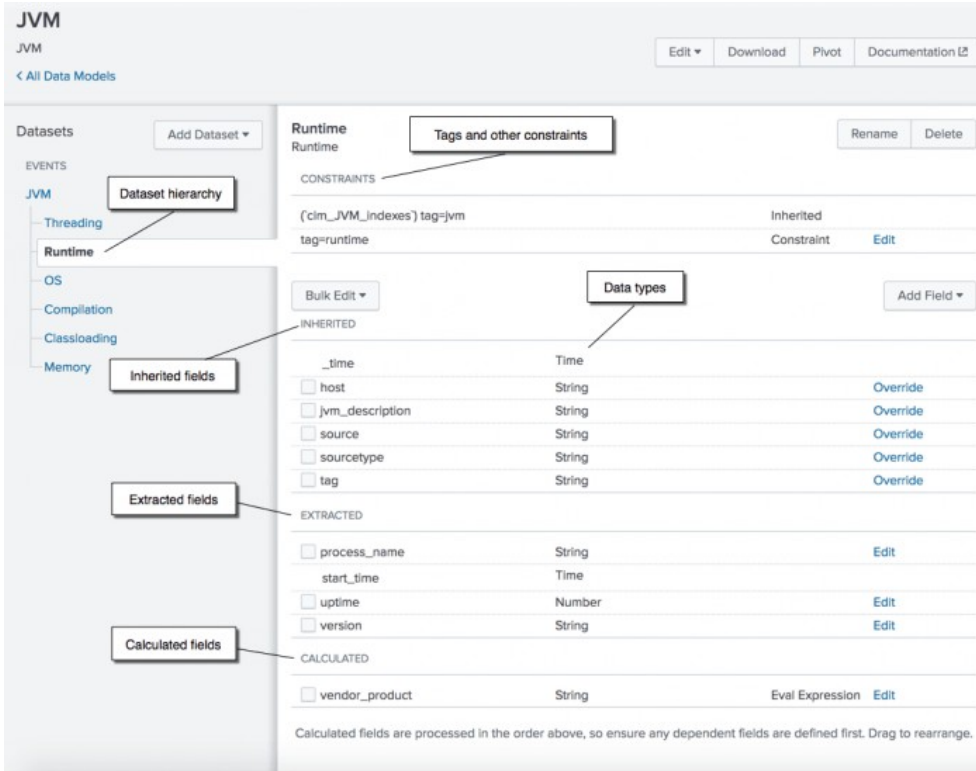
	Information available in documentation	**Information available in Data Model Editor in Splunk Web**	**Information available in JSON file of the model**
Required tags	YES	YES	YES
Other constraints	NO	YES	YES
Full dataset hierarchy	NO	YES	YES
Inherited fields	NO	YES	YES
Extracted fields	YES	YES	YES
Calculated fields	YES	YES	YES
Data types	YES	YES	YES
Descriptions	YES	NO	YES
Expected values	YES	NO	YES
TA relevance	NO	NO	YES

How to access information directly from the JSON files

As shown in the table in the previous section, each data model's JSON file contains all the information about the model structure and its fields, so you can access this information programmatically. Several parameters formerly available only in the documentation are now available in the JSON's `comment` field. The format for this field is `{"description": "Description of the field.", "expected_values": ["val 1", "val 2"], "ta_relevant": true|false}`.

Parameter	**Description**

Parameter	Description
description	A description of the field.
expected_values	Optional. The values that applications such as Splunk Enterprise Security or Splunk App for PCI Compliance expect this field to contain. Use this for validation to ensure that your data populates correctly in the dashboards for these apps.
ta_relevant	Optional. A boolean indicator, signaling whether developers of add-ons need to populate this field. The default is true. A false value is given for fields that Splunk Enterprise Security or Splunk App for PCI Compliance automatically populate through the asset and identity correlation framework of those apps, or for other fields that are not intended to be populated by incoming data, such as the tag fields in each model.

CIM fields per associated data model

Single page view of all the CIM fields and the associated models. See where the overlapping models use the same fields and how to join across different datasets.

Field name	Data model
access_count	Splunk Audit Logs
access_time	Splunk Audit Logs
action	Authentication, Change, Data Access, Data Loss Prevention, Email, Endpoint, Intrusion Detection, Malware, Network Sessions, Network Traffic, Performance, Web
action_mode	Splunk Audit Logs
action_name	Splunk Audit Logs
action_status	Splunk Audit Logs
additional_answer_count	Network Resolution (DNS)
affect_dest	TicketManagement
answer	Network Resolution (DNS)
answer_count	Network Resolution (DNS)
app	Alerts, Authentication, Data Access, Data Loss Prevention, Network Traffic, Splunk Audit Logs, Web
app_id	Data Access
array	Inventory, Performance
authentication_method	Authentication
authentication_service	Authentication
authority_answer_count	Network Resolution (DNS)
availability	Databases
avg_executions	Databases
blocksize	Inventory, Performance
body	Alerts Deprecated in favor of description.
buckets	Splunk Audit Logs
buckets_size	Splunk Audit Logs
buffer_cache_hit_ratio	Databases
bugtraq	Vulnerabilities

Field name	Data model
bytes	Network Traffic, Web
bytes_in	Network Traffic, Web
bytes_out	Network Traffic, Web
cached	Web
category	Data Loss Prevention, Intrusion Detection, Malware, Vulnerabilities, Web
cert	Vulnerabilities
change	TicketManagement
change_type	Change
channel	Network Traffic
cluster	Inventory, Performance
cm_enabled	Java Virtual Machines (JVM)
cm_supported	Java Virtual Machines (JVM)
command	Change
comments	TicketManagement
commits	Databases
committed_memory	Java Virtual Machines (JVM)
compilation_time	Java Virtual Machines (JVM)
complete	Splunk Audit Logs
component	Splunk Audit Logs
cookie	Web
cpu_cores	Inventory
cpu_count	Inventory
cpu_load_mhz	Performance
cpu_load_percent	Endpoint, Performance
cpu_mhz	Inventory
cpu_time	Java Virtual Machines (JVM), Performance
cpu_time_enabled	Java Virtual Machines (JVM)
cpu_time_supported	Java Virtual Machines (JVM)
cpu_used	Databases
cpu_user_percent	Performance
creation_time	Endpoint
cron	Splunk Audit Logs
current_cpu_time	Java Virtual Machines (JVM)
current_loaded	Java Virtual Machines (JVM)

Field name	Data model
current_user_time	Java Virtual Machines (JVM)
cursor	Databases
cve	Vulnerabilities
cvss	Vulnerabilities
daemon_thread_count	Java Virtual Machines (JVM)
datamodel	Splunk Audit Logs
date	Malware
delay	Email
description	Alerts, Endpoint, Inventory, TicketManagement
dest	Alerts, Authentication, Certificates, Change, Data Access, Data Loss Prevention, Databases, Email, Endpoint, Event Signatures, Interprocess Messaging, Intrusion Detection, Inventory, Malware, Network Resolution (DNS), Network Traffic, Performance, TicketManagement, Updates, Vulnerabilities, Web
dest_bunit	Alerts, Authentication, Certificates, Change, Data Loss Prevention, Databases, Email, Endpoint, Event Signatures, Interprocess Messaging, Intrusion Detection, Inventory, Malware, Network Resolution (DNS), Network Sessions, Network Traffic, Performance, TicketManagement, Updates, Vulnerabilities, Web
dest_category	Alerts, Authentication, Certificates, Change, Data Loss Prevention, Databases, Email, Endpoint, Event Signatures, Interprocess Messaging, Intrusion Detection, Inventory, Malware, Network Resolution (DNS), Network Sessions, Network Traffic, Performance, TicketManagement, Updates, Vulnerabilities, Web
dest_dns	Network Sessions
dest_interface	Network Traffic
dest_ip	Inventory, Network Sessions, Network Traffic
dest_ip_range	Change
dest_is_expected	Endpoint
dest_mac	Network Sessions, Network Traffic
dest_name	Data Access
dest_nt_domain	Authentication, Change, Malware
dest_nt_host	Network Sessions
dest_port	Certificates, Endpoint, Intrusion Detection, Network Resolution (DNS), Network Traffic, Web
dest_port_range	Change
dest_priority	Alerts, Authentication, Certificates, Change, Data Loss Prevention, Databases, Email, Endpoint, Event Signatures, Interprocess Messaging, Intrusion Detection, Inventory, Malware, Network Resolution (DNS), Network Sessions, Network Traffic, Performance, TicketManagement, Updates, Vulnerabilities, Web
dest_requires_av	Endpoint, Malware
dest_should_timesync	Endpoint, Performance
dest_should_update	Endpoint, Performance, Updates
dest_translated_ip	Network Traffic
dest_translated_port	Network Traffic

Field name	Data model
dest_type	Alerts
dest_url	Data Access
dest_zone	Data Loss Prevention, Network Traffic
digest	Splunk Audit Logs
direction	Change, Network Traffic
dlp_type	Data Loss Prevention
dns	Inventory
dump_area_used	Databases
duration	Authentication, Certificates, Databases, Email, Interprocess Messaging, Network Resolution (DNS), Network Sessions, Network Traffic, Splunk Audit Logs, Web
dvc	Change, Data Access, Data Loss Prevention, Intrusion Detection, Network Traffic, Updates, Vulnerabilities
dvc_bunit	Data Loss Prevention, Intrusion Detection, Network Traffic, Vulnerabilities
dvc_category	Data Loss Prevention, Intrusion Detection, Network Traffic, Vulnerabilities
dvc_ip	Network Traffic
dvc_mac	Network Traffic
dvc_priority	Data Loss Prevention, Intrusion Detection, Network Traffic, Vulnerabilities
dvc_zone	Data Loss Prevention, Network Traffic
earliest	Splunk Audit Logs
elapsed_time	Databases
email	Data Access
enabled	Inventory
endpoint	Interprocess Messaging
endpoint_version	Interprocess Messaging
error_code	Web
event_id	Splunk Audit Logs
family	Inventory
fan_speed	Performance
fd_max	Inventory, Performance
fd_used	Performance
file_access_time	Endpoint
file_acl	Endpoint
file_create_time	Endpoint
file_hash	Email, Endpoint, Intrusion Detection, Malware, Updates
file_modify_time	Endpoint
file_name	Email, Endpoint, Intrusion Detection, Malware, Updates

Field name	Data model
file_path	Endpoint
file_path	Intrusion Detection
file_path	Malware
file_size	Email
file_size	Endpoint
filter_action	Email
filter_score	Email
flow_id	Network Traffic
free_bytes	Databases
free_physical_memory	Java Virtual Machines (JVM)
free_swap	Java Virtual Machines (JVM)
heap_committed	Java Virtual Machines (JVM)
heap_initial	Java Virtual Machines (JVM)
heap_max	Java Virtual Machines (JVM)
heap_used	Java Virtual Machines (JVM)
host	Splunk Audit Logs
http_content_type	Web
http_method	Web
http_referrer	Web
http_referrer_domain	Web
http_user_agent	Web
http_user_agent_length	Web
hypervisor	Inventory
hypervisor_id	Inventory, Performance
icmp_code	Network Traffic
icmp_type	Network Traffic
id	Alerts
ids_type	Intrusion Detection
image_id	Change
incident	TicketManagement
indexes_hit	Databases
info	Splunk Audit Logs
inline_nat	Inventory
instance_name	Databases

Field name	Data model
instance_reads	Databases
instance_type	Change
instance_version	Databases
instance_writes	Databases
interactive	Inventory
interface	Inventory
internal_message_id	Email
ip	Inventory
is_inprogress	Splunk Audit Logs
jvm_description	Java Virtual Machines (JVM)
last_call_minute	Databases
last_error	Splunk Audit Logs
last_sid	Splunk Audit Logs
latency	Inventory, Performance
latest	Splunk Audit Logs
lb_method	Inventory
lease_duration	Network Sessions
lease_scope	Network Sessions
lock_mode	Databases
lock_session_id	Databases
logical_reads	Databases
logon_time	Databases
mac	Inventory
machine	Databases
max_file_descriptors	Java Virtual Machines (JVM)
mem	Inventory, Performance
mem_committed	Performance
mem_free	Performance
mem_used	Endpoint
mem_used	Performance
memory_sorts	Databases
message	Interprocess Messaging
message_consumed_time	Interprocess Messaging
message_correlation_id	Interprocess Messaging

Field name	Data model
message_delivered_time	Interprocess Messaging
message_delivery_mode	Interprocess Messaging
message_expiration_time	Interprocess Messaging
message_id	Email, Interprocess Messaging
message_info	Email
message_priority	Interprocess Messaging
message_properties	Interprocess Messaging
message_received_time	Interprocess Messaging
message_redelivered	Interprocess Messaging
message_reply_dest	Interprocess Messaging
message_type	Interprocess Messaging, Network Resolution (DNS)
mitre_technique_id	Alerts
mod_time	Splunk Audit Logs
mount	Inventory, Performance
msft	Vulnerabilities
mskb	Vulnerabilities
name	Inventory, Network Resolution (DNS)
node	Inventory
node_port	Inventory
non_heap_committed	Java Virtual Machines (JVM)
non_heap_initial	Java Virtual Machines (JVM)
non_heap_max	Java Virtual Machines (JVM)
non_heap_used	Java Virtual Machines (JVM)
number_of_users	Databases
obj_name	Databases
object	Change, Data Access, Data Loss Prevention, Databases
object_attrs	Change
object_category	Change, Data Access, Data Loss Prevention
object_id	Change, Data Access
object_path	Change, Data Access, Data Loss Prevention
object_size	Data Access
objects_pending	Java Virtual Machines (JVM)
omu_supported	Java Virtual Machines (JVM)
open_file_descriptors	Java Virtual Machines (JVM)

Field name	Data model
operation	Web
orig_dest	Email
orig_recipient	Email
orig_rid	Splunk Audit Logs
orig_sid	Splunk Audit Logs
orig_src	Email
original_file_name	Endpoint
os	Endpoint, Inventory, Java Virtual Machines (JVM)
os_architecture	Java Virtual Machines (JVM)
os_pid	Databases
os_version	Java Virtual Machines (JVM)
owner	Data Access
owner_email	Data Access
owner_id	Data Access
packets	Network Traffic
packets_in	Network Traffic
packets_out	Network Traffic
parameters	Interprocess Messaging
parent	Inventory, Performance
parent_object	Data Access
parent_object_category	Data Access
parent_object_id	Data Access
parent_process	Endpoint
parent_process_exec	Endpoint
parent_process_guid	Endpoint
parent_process_id	Endpoint
parent_process_name	Endpoint
parent_process_path	Endpoint
password	Inventory
payload	Interprocess Messaging
payload_type	Interprocess Messaging
peak_thread_count	Java Virtual Machines (JVM)
physical_memory	Java Virtual Machines (JVM)
physical_reads	Databases

Field name	Data model
power	Performance
priority	TicketManagement
problem	TicketManagement
process	Email, Endpoint
process_current_directory	Endpoint
process_exec	Endpoint
process_guid	Endpoint
process_hash	Endpoint
process_id	Email, Endpoint, Network Traffic
process_integrity_level	Endpoint
process_limit	Databases
process_name	Endpoint, Java Virtual Machines (JVM)
process_path	Endpoint
processes	Databases
product_version	Malware
protocol	Change, Email, Network Traffic
protocol_version	Network Traffic
query	Databases, Network Resolution (DNS)
query_count	Network Resolution (DNS)
query_id	Databases
query_plan_hit	Databases
query_time	Databases
query_type	Network Resolution (DNS)
read_blocks	Inventory, Performance
read_latency	Inventory, Performance
read_ops	Inventory, Performance
reason	Authentication
recipient	Email
recipient_count	Email
recipient_domain	Email
recipient_status	Email
record_type	Network Resolution (DNS)
records_affected	Databases
registry_hive	Endpoint

Field name	Data model
registry_key_name	Endpoint
registry_path	Endpoint
registry_value_data	Endpoint
registry_value_name	Endpoint
registry_value_text	Endpoint
registry_value_type	Endpoint
reply_code	Network Resolution (DNS)
reply_code_id	Network Resolution (DNS)
request_payload	Interprocess Messaging
request_payload_type	Interprocess Messaging
request_sent_time	Interprocess Messaging
resource_type	Performance
response_code	Interprocess Messaging
response_payload_type	Interprocess Messaging
response_received_time	Interprocess Messaging
response_time	Authentication, Certificates, Databases, Email, Interprocess Messaging, Network Resolution (DNS), Network Sessions, Network Traffic, Web
result	Change
result_id	Change
retention	Splunk Audit Logs
retries	Email
return_addr	Email
return_message	Interprocess Messaging
rid	Splunk Audit Logs
rpc_protocol	Interprocess Messaging
rule	Network Traffic
rule_action	Change
savedsearch_name	Splunk Audit Logs
search	Splunk Audit Logs
search_et	Splunk Audit Logs
search_lt	Splunk Audit Logs
search_name	Splunk Audit Logs
search_type	Splunk Audit Logs
seconds_in_wait	Databases

Field name	Data model
sender	Malware
serial	Inventory
serial_num	Databases
service	Endpoint
service_dll	Endpoint
service_dll_hash	Endpoint
service_dll_path	Endpoint
service_dll_signature_exists	Endpoint
service_dll_signature_verified	Endpoint
service_exec	Endpoint
service_hash	Endpoint
service_id	Endpoint
service_name	Endpoint
service_path	Endpoint
service_signature_exists	Endpoint
service_signature_verified	Endpoint
session_id	Databases, Network Traffic
session_limit	Databases
session_status	Databases
sessions	Databases
severity	Alerts, Data Loss Prevention, Intrusion Detection, TicketManagement, Updates, Vulnerabilities
severity_id	Alerts, Data Loss Prevention, Intrusion Detection, Malware, TicketManagement, Updates,Vulnerabilities
sga_buffer_cache_size	Databases
sga_buffer_hit_limit	Databases
sga_data_dict_hit_ratio	Databases
sga_fixed_area_size	Databases
sga_free_memory	Databases
sga_library_cache_size	Databases
sga_redo_log_buffer_size	Databases
sga_shared_pool_size	Databases
sga_sql_area_size	Databases
shell	Inventory
sid	Splunk Audit Logs, Splunk Audit Logs
signature	Alerts, Authentication, Data Loss Prevention, Email, Event Signatures, Intrusion Detection, Malware, Network Sessions, Performance, Splunk Audit Logs, Updates, Vulnerabilities

Field name	Data model
signature_extra	Email
signature_id	Alerts, Authentication, Email, Event Signatures, Data Loss Prevention, Intrusion Detection, Malware, Network Sessions, Performance, Updates, Vulnerabilities
signature_version	Malware
site	Web
size	Email, Inventory, Splunk Audit Logs
snapshot	Inventory
source	Splunk Audit Logs
sourcetype	Splunk Audit Logs
spent	Splunk Audit Logs
splunk_id	TicketManagement
splunk_realm	TicketManagement
splunk_server	Splunk Audit Logs
src	Alerts, Authentication, Certificates, Change, Data Access, Data Loss Prevention, Databases, Email, Endpoint, Intrusion Detection, Malware, Network Resolution (DNS), Network Traffic, Web
src_bunit	Alerts, Authentication, Certificates, Change, Data Loss Prevention, Databases, Email, Intrusion Detection, Malware, Network Resolution (DNS), Network Sessions, Network Traffic, Web
src_category	Alerts, Authentication, Certificates, Change, Data Loss Prevention, Databases, Email, Endpoint, Intrusion Detection, Malware, Network Resolution (DNS), Network Sessions, Network Traffic, Web
src_dns	Network Sessions
src_interface	Network Traffic
src_ip	Inventory, Network Sessions, Network Traffic
src_ip_range	Change
src_mac	Network Sessions, Network Traffic
src_nt_domain	Authentication, Change
src_nt_host	Network Sessions
src_port	Certificates, Endpoint, Network Resolution (DNS), Network Traffic
src_port_range	Change
src_priority	Alerts, Authentication, Certificates, Change, Data Loss Prevention, Databases, Email, Endpoint, Intrusion Detection, Malware, Network Resolution (DNS), Network Sessions, Network Traffic, Web
src_requires_av	Endpoint
src_should_timesync	Endpoint
src_should_update	Endpoint
src_translated_ip	Network Traffic
src_translated_port	Network Traffic
src_type	Alerts

Field name	Data model
src_user	Authentication, Change, Data Loss Prevention, Email, TicketManagement
src_user_bunit	Authentication, Change, Data Loss Prevention, Email, TicketManagement
src_user_category	Authentication, Change, Data Loss Prevention, Email, TicketManagement
src_user_domain	Email
src_user_id	Authentication
src_user_name	Change
src_user_priority	Authentication, Change, Data Loss Prevention, Email, TicketManagement
src_user_role	Authentication
src_user_type	Authentication, Change
src_zone	Data Loss Prevention, Network Traffic
ssid	Network Traffic
ssl_end_time	Certificates
ssl_engine	Certificates
ssl_hash	Certificates
ssl_is_valid	Certificates
ssl_issuer	Certificates
ssl_issuer_common_name	Certificates
ssl_issuer_email	Certificates
ssl_issuer_email_domain	Certificates
ssl_issuer_locality	Certificates
ssl_issuer_organization	Certificates
ssl_issuer_state	Certificates
ssl_issuer_street	Certificates
ssl_issuer_unit	Certificates
ssl_name	Certificates
ssl_policies	Certificates
ssl_publickey	Certificates
ssl_publickey_algorithm	Certificates
ssl_serial	Certificates
ssl_session_id	Certificates
ssl_signature_algorithm	Certificates
ssl_start_time	Certificates
ssl_subject	Certificates
ssl_subject_common_name	Certificates

Field name	Data model
ssl_subject_email	Certificates
ssl_subject_email_domain	Certificates
ssl_subject_locality	Certificates
ssl_subject_organization	Certificates
ssl_subject_state	Certificates
ssl_subject_street	Certificates
ssl_subject_unit	Certificates
ssl_validity_window	Certificates
ssl_version	Certificates
start_mode	Endpoint
start_time	Databases, Java Virtual Machines (JVM)
state	Endpoint
status	Change, Endpoint, Interprocess Messaging, Inventory, Splunk Audit Logs, TicketManagement, Updates, Web
status_code	Email
storage	Inventory, Performance
storage_free	Performance
storage_free_percent	Performance
storage_name	Web
storage_used	Performance
storage_used_percent	Performance
stored_procedures_called	Databases
subject	Alerts Deprecated in favor of `signature`, Email
summary_id	Splunk Audit Logs
swap	Performance
swap_free	Performance
swap_space	Java Virtual Machines (JVM)
swap_used	Performance
synch_supported	Java Virtual Machines (JVM)
system_load	Java Virtual Machines (JVM)
table_scans	Databases
tables_hit	Databases
tablespace_name	Databases
tablespace_reads	Databases
tablespace_status	Databases

Field name	Data model
tablespace_used	Databases
tablespace_writes	Databases
tag	Alerts, Authentication, Certificates, Change, Data Loss Prevention, Databases, Email, Endpoint, Event Signatures, Interprocess Messaging, Intrusion Detection, Inventory, Java Virtual Machines (JVM), Malware, Network Resolution (DNS), Network Sessions, Network Traffic, Performance, TicketManagement, Updates, Vulnerabilities, Web
tcp_flag	Network Traffic
temperature	Performance
tenant_id	Data Access
thread_count	Java Virtual Machines (JVM)
threads_started	Java Virtual Machines (JVM)
thruput	Performance
thruput_max	Performance
ticket_id	TicketManagement
time	Inventory
time_submitted	TicketManagement
tos	Network Traffic
total_loaded	Java Virtual Machines (JVM)
total_processors	Java Virtual Machines (JVM)
total_unloaded	Java Virtual Machines (JVM)
transaction_id	Network Resolution (DNS)
transport	Certificates, Endpoint, Intrusion Detection, Network Resolution (DNS), Network Traffic
transport_dest_port	Endpoint
ttl	Network Resolution (DNS), Network Traffic
type	Alerts
uptime	Java Virtual Machines (JVM), Performance
uri	Splunk Audit Logs
uri_path	Web
uri_query	Web
url	Email, Malware, Vulnerabilities, Web
url_domain	Web
url_length	Web
user	Alerts, Authentication, Change, Data Access, Data Loss Prevention, Databases, Email, Endpoint, Intrusion Detection, Inventory, Malware, Network Sessions, Network Traffic, Splunk Audit Logs, TicketManagement, Vulnerabilities, Web
user_agent	Authentication, Change, Data Access

Field name	Data model
user_bunit	Alerts, Authentication, Data Loss Prevention, Databases, Email, Endpoint, Intrusion Detection, Inventory, Malware, Network Sessions, Network Traffic, Splunk Audit Logs, TicketManagement, Vulnerabilities, Web
user_category	Alerts, Authentication, Data Loss Prevention, Databases, Email, Endpoint, Intrusion Detection, Inventory, Malware, Network Sessions, Network Traffic, Splunk Audit Logs, TicketManagement, Vulnerabilities, Web
user_group	Data Access
user_id	Authentication, Endpoint, Inventory
user_name	Alerts, Change
user_priority	Alerts, Authentication, Data Loss Prevention, Databases, Email, Endpoint, Intrusion Detection, Inventory, Malware, Network Sessions, Network Traffic, Splunk Audit Logs, TicketManagement, Vulnerabilities, Web
user_role	Authentication, Data Access
user_type	Authentication, Change
vendor_account	Alerts, Authentication, Change, Network Traffic
vendor_product	Authentication, Change, Data Access, Data Loss Prevention, Databases, Email, Endpoint, Event Signatures, Intrusion Detection, Inventory, Java Virtual Machines (JVM), Malware, Network Resolution (DNS), Network Sessions, Network Traffic, Updates, Vulnerabilities, Web
vendor_product_id	Alerts, Change
vendor_region	Alerts, Change
version	Inventory, Java Virtual Machines (JVM)
view	Splunk Audit Logs
vip_port	Inventory
vlan	Network Traffic
wait_state	Databases
wait_time	Databases
wifi	Network Traffic
write_blocks	Inventory, Performance
write_latency	Inventory, Performance
write_ops	Inventory, Performance
xdelay	Email
xref	Email
xref	Vulnerabilities

Alerts

The fields and tags in the Alerts data model describe the alerts produced by alerting systems, such as Nagios or NetCool, for use in Splunk correlation searches or dashboards. They are not to be used to describe Splunk Alerts or Notable Events, which are already modeled in other contexts.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with the Alerts event dataset

The following tag acts as constraint to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
Alerts	alert

Fields for the Alerts event dataset

The following table lists the extracted and calculated fields for the event dataset in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Alerts	app	string	The system, service, or application that generated the alert event. Examples include, but are not limited to the following: GuardDuty, SecurityCenter, 3rd party services, win:app:trendmicro, vmware, nagios.	• recommended • required for pytest-splunk-addon
Alerts	body	string	The body of a message. This field is deprecated in favor of `description`.	required for pytest-splunk-addon
Alerts	description	string	The description of the alert event.	
Alerts	dest	string	The object that is the target of the alert event. Examples include an email address, SNMP trap, or virtual machine id. You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	• recommended • required for pytest-splunk-addon
Alerts	dest_bunit	string	The business unit associated with the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Alerts	dest_category	string	The category of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Alerts	dest_priority	string	The priority of the destination. This field is automatically provided by asset and identity	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Alerts	dest_type	string	The type of the destination object, such as instance, storage, firewall.	
Alerts	id	string	The unique identifier of the alert event.	required for pytest-splunk-addon
Alerts	mitre_technique_id	string	The MITRE ATT&CK technique ID of the alert event, searchable at https://attack.mitre.org/techniques.	
Alerts	severity	string	The severity of the alert event. **Note:** This field is a string. Specific values are required. Use the severity_id field for severity ID fields that are integer data types. Specific values are required. Use vendor_severity for the vendor's own human-readable strings (such as Good, Bad, Really Bad, and so on).	• recommended • required for pytest-splunk-addon • prescribed values: critical, high, medium, low, informational, unknown
Alerts	severity_id	string	The numeric or vendor specific severity indicator corresponding to the event severity.	
Alerts	signature	string	The human-friendly title of the alert event, such as 'API GetAccountPasswordPolicy was invoked using root credentials.' Split by signature_id when aggregating alert events by types.	
Alerts	signature_id	string	The vendor specific policy or rule that generated the alert event, such as 'Policy:IAMUser/RootCredentialUsage.'	recommended
Alerts	src	string	The object that is the actor of the alert event. You can **alias** this from more specific fields, such as src_host, src_ip, or src_name.	recommended
Alerts	src_bunit	string	The business unit associated with the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Alerts	src_category	string	The category of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Alerts	src_priority	string	The priority of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Alerts	src_type	string	The type of the source object, such as instance, storage, firewall.	
Alerts	subject	string	The message subject. This field is deprecated in favor of signature.	
Alerts	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
Alerts	type	string	The alert event type.	• recommended • required for pytest-splunk-addon • prescribed values: alarm, alert, event, task, warning, unknown
Alerts	user	string	The user involved in the alert event.	recommended
Alerts	user_bunit	string	The business unit of the user involved in the alert event. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Alerts	user_category	string	The category of the user involved in the alert event. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Alerts	user_name	string	The name of the user involved in the alert event.	
Alerts	user_priority	string	The priority of the user involved in the alert event. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Alerts	vendor_account	string	The account associated with the alert event.	
Alerts	vendor_region	string	The data center region involved in the alert event, such as us-west-2.	

Application State (deprecated)

This data model is deprecated as of software version 4.12.0. Use the Endpoint data model instead.

The fields and tags in the Application State data model describe service or process inventory and state, such as Unix daemons, Windows services, running processes on any OS, or similar systems.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Application State event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Application_State	(listening, port) OR (process, report) OR (service, report)
|_____ Ports	listening
	port
|_____ Processes	process
	report
|_____ Services	service
	report

Fields for Application State event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

Dataset name	Field name	Data type	Description	Expected values
All_Application_State	dest	string	The compute resource where the service is installed. You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	
All_Application_State	dest_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Application_State	dest_category	string		
All_Application_State	dest_priority	string		
All_Application_State	dest_requires_av	boolean		
All_Application_State	dest_should_timesync	boolean		
All_Application_State	dest_should_update	boolean		
All_Application_State	process	string	The name of a process or service file, such as `sqlsrvr.exe` or `httpd`. **Note:** This field is not appropriate for service or daemon names, such as `SQL Server` or `Apache Web Server`. Service or daemon names belong to the `service` field (see below).	
All_Application_State	process_name	string	The name of a process.	
All_Application_State	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this	

Dataset name	Field name	Data type	Description	Expected values
			field when writing add-ons.	
All_Application_State	`user`	string	The user account the service is running as, such as `System` or `httpdsvc`.	
All_Application_State	`user_bunit`	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Application_State	`user_category`	string		
All_Application_State	`user_priority`	string		
Ports	`dest_port`	number	Network ports communicated to by the process, such as 53.	
Ports	`transport`	string	The network ports listened to by the application process, such as tcp, udp, etc.	
Ports	`transport_dest_port`	string	Calculated as transport/dest_port, such as tcp/53.	
Processes	`cpu_load_mhz`	number	CPU Load in megahertz	
Processes	`cpu_load_percent`	number	CPU Load in percent	
Processes	`cpu_time`	string	CPU Time	
Processes	`mem_used`	number	Memory used in bytes	
Services	`service`	string	The name of the service, such as `SQL Server` or `Apache Web Server`. **Note:** This field is not appropriate for filenames, such as `sqlsrvr.exe` or `httpd`. Filenames should belong to the `process` field instead. Also, note that field is a string. Use the `service_id` field for service ID fields that are integer data types.	
Services	`service_id`	string	A numeric indicator for a service.	
Services	`start_mode`	string	The start mode for the service.	`disabled`, `manual`, `auto`.
Services	`status`	string	The status of the service.	`critical`, `started`, `stopped`, `warning`

Authentication

The fields and tags in the Authentication data model describe login activities from any data source.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Authentication event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name

Dataset name	Tag name
Authentication	authentication
|____ Default_Authentication	default
|____ Insecure_Authentication	cleartext OR insecure
|____ Privileged_Authentication	privileged

Fields for Authentication event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

For even more examples, see Authentication Field Mapping.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Authentication	`action`	string	The action performed on the resource.	• recommended • required for pytest-splunk-addon • prescribed values: `success`, `failure`, `pending`, `error`
Authentication	`app`	string	The application involved in the event (such as `ssh`, `splunk`, `win:local`, `signin.amazonaws.com`).	• recommended • required for pytest-splunk-addon
Authentication	`authentication_method`	string	The method used to authenticate the request such as `SAML`, `FIDO`, `MFA`, `Kerberos`, `NTLM`, `LM`, `NTLMv2`, `PSK`, `Password`.	
Authentication	`authentication_service`	string	The service used to authenticate the request such as `Okta`, `ActiveDirectory`, `AzureAD`.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Authentication	dest	string	The target involved in the authentication. You can **alias** this from more specific fields, such as dest_host, dest_ip, dest_nt_host.	• recommended • required for pytest-splunk-addon
Authentication	dest_bunit	string	The business unit of the authentication target. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	dest_category	string	The category of the authentication target, such as email_server or SOX-compliant. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	dest_nt_domain	string	The name of the Active Directory used by the authentication target, if applicable.	
Authentication	dest_priority	string	The priority of the authentication target. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	duration	number	The amount of time for the completion of the authentication event, in seconds.	
Authentication	reason	string	The human-readable message associated with the authentication action (success or failure). Used when differentiating from event name (signature). Often used to describe the reason of the logon failure, such as "wrong password"".	
Authentication	response_time	number	The amount of time it took to receive a response in the authentication event, in seconds.	
Authentication	signature	string	A human-readable signature name.	
Authentication	signature_id	string	The unique identifier or event code of the event signature.	
Authentication	src	string	The source involved in the authentication. In the case of endpoint protection authentication the src is the client. You can **alias** this from more specific fields, such as src_host, src_ip, or src_nt_host. Do not confuse src with the event source or sourcetype fields.	recommended
Authentication	src_bunit	string	The business unit of the authentication source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	src_category	string		

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			The category of the authentication source, such as `email_server` or `SOX-compliant`. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	src_nt_domain	string	The name of the Active Directory used by the authentication source, if applicable.	
Authentication	src_priority	string	The priority of the authentication source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	src_user	string	In privilege escalation events, `src_user` represents the user who initiated the privilege escalation. This field is unnecessary when an escalation has not been performed.	recommended
Authentication	src_user_bunit	string	The business unit of the user who initiated the privilege escalation. This field is unnecessary when an escalation has not been performed. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	src_user_category	string	The category of the user who initiated the privilege escalation. This field is unnecessary when an escalation has not been performed. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	src_user_id	string	The unique id of the user who initiated the privilege escalation. This field is unnecessary when an escalation has not been performed.	
Authentication	src_user_priority	string	The priority of the user who initiated the privilege escalation. This field is unnecessary when an escalation has not been performed. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	src_user_role	string	The role of the user who initiated the privilege escalation. This field is unnecessary when an escalation has not been performed.	
Authentication	src_user_type	string	The type of the user who initiated the privilege escalation. This field is unnecessary when an escalation has not been performed.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Authentication	tag	string	This automatically-generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
Authentication	user	string	The actual string or identifier that a user is logging in with. This is the user involved in the event, or who initiated the event. For authentication privilege escalation events, this should represent the user string or identifier targeted by the escalation.	• recommended • required for pytest-splunk-addon
Authentication	user_agent	string	The user agent through which the request was made, such as `Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6)` or `aws-cli/2.0.0 Python/3.7.4 Darwin/18.7.0 botocore/2.0.0dev4`.	
Authentication	user_bunit	string	The business unit of the user involved in the event, or who initiated the event. For authentication privilege escalation events this should represent the user targeted by the escalation. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	user_category	string	The category of the user involved in the event, or who initiated the event. For authentication privilege escalation events, this should represent the user targeted by the escalation. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	user_id	string	The unique id of the user involved in the event. For authentication privilege escalation events, this should represent the user targeted by the escalation.	
Authentication	user_priority	string	The priority of the user involved in the event, or who initiated the event. For authentication privilege escalation events, this should represent the user targeted by the escalation. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Authentication	user_role	string	The role of the user involved in the event, or who initiated the event. For authentication privilege escalation events, this should represent the user role targeted by the escalation.	
Authentication	user_type	string	The type of the user involved in the event or who initiated the event, such as IAMUser, Admin, or System. For authentication privilege escalation events, this should represent the user type targeted by the escalation.	
Authentication	vendor_account	string	The account that manages the user that initiated the request.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values

Certificates

The fields and tags in the Certificates data model describe key and certificate management events from a variety of secure servers and IAM systems.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Certificates event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Certificates	certificate
|____ SSL	ssl OR tls

Fields for Certificates event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Certificates	dest	string	The target in the certificate management event.	
All_Certificates	dest_bunit	string	The business unit of the target. This field is automatically provided by Asset and Identity correlation features of applications like Splunk Enterprise Security.	
All_Certificates	dest_category	string	The category of the target. This field is automatically provided by Asset and Identity correlation features of applications like	other: email_server, SOX-compliant

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			the Splunk Enterprise Security.	
All_Certificates	`dest_port`	number	The port number of the target.	
All_Certificates	`dest_priority`	string	The priority of the target.	
All_Certificates	`duration`	number	The amount of time for the completion of the certificate management event, in seconds.	
All_Certificates	`response_time`	number	The amount of time it took to receive a response in the certificate management event, if applicable.	
All_Certificates	`src`	string	The source involved in the certificate management event. You can **alias** this from more specific fields, such as `src_host`, `src_ip`, or `src_nt_host`. **Note:** Do not confuse `src` with the event `source` or `sourcetype` fields.	
All_Certificates	`src_bunit`	string	The business unit of the certificate management source. This field is automatically provided by Asset and Identity correlation features of applications like Splunk Enterprise Security.	
All_Certificates	`src_category`	string	The category of the certificate management source. This field is automatically provided by Asset and Identity correlation features of applications like the Splunk Enterprise Security.	other: `email_server`, `SOX-compliant`
All_Certificates	`src_port`	number	The port number of the source.	
All_Certificates	`src_priority`	string	The priority of the certificate management source.	
All_Certificates	`tag`	string	This automatically generated field is used to access tags from within datamodels. Add-on builders do not need to populate it.	
All_Certificates	`transport`	string	The transport protocol of the Network Traffic involved with this certificate.	
SSL	`ssl_end_time`	time	The expiry time of the certificate. Needs to be converted to UNIX time for calculations in dashboards.	recommended
SSL	`ssl_engine`	string	The name of the signature engine that created the certificate.	
SSL	`ssl_hash`	string	The hash of the certificate.	recommended
SSL	`ssl_is_valid`	boolean	Indicator of whether the ssl certificate is valid or not.	prescribed values: `true`, `false`, `1`, `0`
SSL	`ssl_issuer`	string	The certificate issuer's RFC2253 Distinguished Name.	• recommended

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				• required for pytest-splunk-addon
SSL	ssl_issuer_common_name	string	The certificate issuer's common name.	• recommended • required for pytest-splunk-addon
SSL	ssl_issuer_email	string	The certificate issuer's email address.	
SSL	ssl_issuer_email_domain	string	The domain name contained within the certificate issuer's email address.	recommended
SSL	ssl_issuer_locality	string	The certificate issuer's locality.	
SSL	ssl_issuer_organization	string	The certificate issuer's organization.	
SSL	ssl_issuer_state	string	The certificate issuer's state of residence.	
SSL	ssl_issuer_street	string	The certificate issuer's street address.	
SSL	ssl_issuer_unit	string	The certificate issuer's organizational unit.	
SSL	ssl_name	string	The name of the ssl certificate.	
SSL	ssl_policies	string	The Object Identification Numbers's of the certificate's policies in a comma separated string.	
SSL	ssl_publickey	string	The certificate's public key.	
SSL	ssl_publickey_algorithm	string	The algorithm used to create the public key.	
SSL	ssl_serial	string	The certificate's serial number.	• recommended • required for pytest-splunk-addon
SSL	ssl_session_id	string	The session identifier for this certificate.	
SSL	ssl_signature_algorithm	string	The algorithm used by the Certificate Authority to sign the certificate.	
SSL	ssl_start_time	time	This is the start date and time for this certificate's validity. Needs to be converted to UNIX time for calculations in dashboards.	recommended
SSL	ssl_subject	string	The certificate owner's RFC2253 Distinguished Name.	• recommended • required for pytest-splunk-addon
SSL	ssl_subject_common_name	string	This certificate owner's common name.	• recommended • required for pytest-splunk-addon
SSL	ssl_subject_email	string	The certificate owner's e-mail address.	
SSL	ssl_subject_email_domain	string	The domain name contained within the certificate subject's email address.	recommended
SSL	ssl_subject_locality	string	The certificate owner's locality.	
SSL	ssl_subject_organization	string	The certificate owner's organization.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				required for pytest-splunk-addon
SSL	`ssl_subject_state`	string	The certificate owner's state of residence.	
SSL	`ssl_subject_street`	string	The certificate owner's street address.	
SSL	`ssl_subject_unit`	string	The certificate owner's organizational unit.	
SSL	`ssl_validity_window`	number	The length of time (in seconds) for which this certificate is valid.	required for pytest-splunk-addon
SSL	`ssl_version`	string	The ssl version of this certificate.	

Examples for Certificates event datasets

The following is a sample of a certificate event from zeek/corelight:

```
{
  "ts": 1586817752.481357,
  "id": "FBKnzp4LVE2thdglSe",
  "certificate.version": 3,
  "certificate.serial": "0B1641AEAE93F5DB71B36C977B7FCF63",
  "certificate.subject": "CN=Outlook.live.com,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US",
  "certificate.issuer": "CN=DigiCert Cloud Services CA-1,O=DigiCert Inc,C=US",
  "certificate.not_valid_before": 1585008000.0,
  "certificate.not_valid_after": 1648123200.0,
  "certificate.key_alg": "rsaEncryption",
  "certificate.sig_alg": "sha256WithRSAEncryption",
  "certificate.key_type": "rsa",
  "certificate.key_length": 2048,
  "certificate.exponent": "65537",
  "san.dns": ["Outlook.live.com", "outlook-sdf.live.com", "attachment.outlook.office.net",
"attachment.outlook.officeppe.net", "hotmail.com", "*.calendar.live.com", "*.hotmail.com", "*.live.com",
"*.mail.live.com", "afd-a-acdc-direct.office.com", "live.com", "*.nrb.footprintdns.com",
"*.fp.measure.office.com", "premium.outlook.com"],
  "basic_constraints.ca": false
}
```

The following are CIM fields extracted from this sample:

```
"ssl_start_time" = "1585008000"
"ssl_end_time" = "1648123200"
"ssl_validity_window" = "63115200"
"ssl_issuer" = "CN=DigiCert Cloud Services CA-1,O=DigiCert Inc,C=US"
"ssl_issuer_common_name" = "DigiCert Cloud Services CA-1"
"ssl_issuer_locality" = "Redmond"
"ssl_issuer_state" = "Washington
"ssl_issuer_organization" = "DigiCert Inc"
"ssl_subject" = "CN=Outlook.live.com,O=Microsoft Corporation,L=Redmond,ST=Washington,C=US"
"ssl_subject_common_name" = "Outlook.live.com"
"ssl_subject_organization" = "Microsoft Corporation"
"ssl_subject_locality" = "Redmond"
"ssl_subject_state" = "Washington"
"ssl_subject_organization" = "Microsoft Corporation"
"ssl_is_valid" = "true"
"ssl_version" = "3"
```

```
"ssl_serial" = "0B1641AEAE93F5DB71B36C977B7FCF63"
"ssl_publickey_algorithm" = "rsaEncryption"
"ssl_signature_algorithm" = "sha256WithRSAEncryption"
```

Change

The Change data model replaces the Change Analysis data model, which is deprecated as of software version 4.12.0.

Change.Endpoint is for administrative and policy types of changes to infrastructure security devices, servers, and endpoint detection and response (EDR) systems. The Endpoint data model is for monitoring endpoint clients including, but not limited to, end user machines, laptops, and bring your own devices (BYOD). If an event is about an endpoint process, service, file, port, and so on, see the Endpoint data model.

The fields in the Change data model describe `Create`, `Read`, `Update`, and `Delete` activities from any data source.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Change event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Changes	change
|____ Auditing_Changes	audit
|____ Endpoint_Changes	endpoint
|____ Network_Changes	network
|____ Account_Management	account
|____ Instance_Changes	instance

Fields for Change event datasets

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.

- **Other values**: Other example values that you might see.

For even more examples, see Change Field Mapping.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Changes	action	string	The action attempted on the resource, regardless of success or failure.	• recommended • required for pytest-splunk-addon • prescribed values: `created`, `deleted`, `acl_modified`, `cleared`, `modified`, `read`, `stopped`, `started`, `restarted`
All_Changes	change_type	string	The type of change, such as `filesystem` or `AAA` (authentication, authorization, and accounting).	• recommended • required for pytest-splunk-addon • prescribed values: `restart`
All_Changes	command	string	The command that initiated the change.	• recommended • required for pytest-splunk-addon
All_Changes	dest	string	The resource where change occurred. You can **alias** this from more specific fields not included in this data model, such as `dest_host`, `dest_ip`, or `dest_name`.	• recommended • required for pytest-splunk-addon
All_Changes	dest_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Changes	dest_category	string		
All_Changes	dest_priority	string		
All_Changes	dvc	string	The device that reported the change, if applicable, such as a FIP or CIM server. You can **alias** this from more specific fields not included in this data model, such as `dvc_host`, `dvc_ip`, or `dvc_name`.	• recommended • required for pytest-splunk-addon
All_Changes	object	string	Name of the affected object on the resource (such as a router interface, user account, or server volume).	• recommended • required for pytest-splunk-addon
All_Changes	object_attrs	string	The object's attributes and their values. The attributes and values can be those that are updated on a resource object, or those that are not updated but are essential attributes.	• recommended • required for pytest-splunk-addon
All_Changes	object_category	string	Generic name for the class of the updated resource object. Expected values may be specific to an app, for example: registry, directory, file, group, user, bucket, instance.	• recommended • required for pytest-splunk-addon

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Changes	object_id	string	The unique updated resource object ID as presented to the system, if applicable (for instance, a SID, UUID, or GUID value).	• recommended • required for pytest-splunk-addon
All_Changes	object_path	string	The path of the modified resource object, if applicable (such as a file, directory, or volume).	• recommended • required for pytest-splunk-addon
All_Changes	result	string	The vendor-specific result of a change, or clarification of an `action` status. For instance, `status=failure` may be accompanied by `result=blocked by policy` or `result=disk full`. `result` is a string. Please use a `msg_severity_id` field (not included in the data model) for severity ID fields that are integer data types.	• recommended • prescribed values: `lockout`
All_Changes	result_id	string	A result indicator for an `action` status.	recommended
All_Changes	src	string	The resource where the change was originated. You can **alias** this from more specific fields not included in the data model, such as `src_host`, `src_ip`, or `src_name`.	recommended
All_Changes	src_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Changes	src_category	string		
All_Changes	src_priority	string		
All_Changes	status	string	Status of the update.	• recommended • required for pytest-splunk-addon • prescribed values: `success`, `failure`
All_Changes	tag	string	This automatically generated field is used to access tags from within datamodels. Do not define extractions for this field when writing add-ons.	
All_Changes	user	string	The user or entity performing the change. For account changes, this is the account that was changed. See `src_user` for user or entity performing the change. Fill out and normalize first to `user` & `src_user`, for example when using Assets and Identities in Enterprise Security.	• recommended • required for pytest-splunk-addon
All_Changes	user_agent	string	The user agent through which the request was made, such as `Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6)` or `aws-cli/2.0.0 Python/3.7.4 Darwin/18.7.0 botocore/2.0.0dev4`.	
All_Changes	user_name	string	The user name of the user or entity performing the change. For account changes, this is the account that was changed (see `src_user_name`). Use this field for a friendlier name, for example, with AWS	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			events if you do not have Assets and Identities configured in Enterprise Security and are not getting a friendly name from `user`.	
All_Changes	`user_type`	string	The type of the user involved in the event or who initiated the event, such as IAMUser, Admin, or System. For account management events, this should represent the type of the user changed by the request.	
All_Changes	`vendor_account`	string	The account that manages the user that initiated the request.	
All_Changes	`vendor_product`	string	The vendor and product or service that detected the change. This field can be automatically populated by `vendor` and `product` fields in your data.	• recommended • required for pytest-splunk-addon
All_Changes	`vendor_region`	string	The data center region where the change occurred, such as us-west-2.	
Account_Management	`dest_nt_domain`	string	The NT domain of the destination, if applicable.	recommended
Account_Management	`src_nt_domain`	string	The NT domain of the source, if applicable.	recommended
Account_Management	`src_user`	string	For account changes, the user or entity performing the change. Fill out and normalize first to `user` & `src_user`, for example when using Assets and Identities in Enterprise Security.	recommended
Account_Management	`src_user_bunit`	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Account_Management	`src_user_category`	string		
Account_Management	`src_user_priority`	string		
Account_Management	`src_user_name`	string	For account changes, the user name of the user or entity performing the change. Use this field for a friendlier name, for example, with AWS events if you do not have Assets and Identities configured in Enterprise Security and are not getting a friendly name from `src_user`.	
Account_Management	`src_user_type`	string	For account management events, this should represent the type of the user changed by the request.	
Instance_Changes	`image_id`	string	For create instance events, this field represents the image ID used for creating the instance such as the OS, applications, installed libraries, and more.	recommended
Instance_Changes	`instance_type`	string	For create instance events, this field represents the type of instance to build such as the combination of CPU, memory, storage, and network capacity.	recommended
Network_Changes	`dest_ip_range`	string	For network events, the outgoing traffic for a specific destination IP address range. Specify a single IP address or an IP address range in CIDR notation. For example, 203.0.113.5 or 203.0.113.5/32.	
Network_Changes	`dest_port_range`	string	For network events, this field represents destination port or range. For example, 80 or 8000 - 8080 or	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			80,443.	
Network_Changes	direction	string	For network events, this field represents whether the traffic is inbound or outbound.	
Network_Changes	protocol	string	This field represents the protocol for the network event rule.	
Network_Changes	rule_action	string	For network events, this field represents whether to allow or deny traffic.	
Network_Changes	src_ip_range	string	For network events, this field represents the incoming traffic from a specific source IP address or range. Specify a single IP address or an IP address range in CIDR notation. For example, 203.0.113.5 or 203.0.113.5/32.	
Network_Changes	src_port_range	string	For network events, this field represents source port or range. For example, 80 or 8000 - 8080 or 80,443.	

Change Analysis (deprecated)

This data model is deprecated as of software version 4.12.0. Use the Change data model instead.

The fields in the Change Analysis data model describe `Create`, `Read`, `Update`, and `Delete` activities from any data source.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Change Analysis event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Changes	change
|____ Auditing_Changes	audit
|____ Endpoint_Changes	endpoint
|____ Network_Changes	network
|____ Account_Management	account

Fields for Change Analysis event dataset

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

Dataset name	Field name	Data type	Description	Expected values
All_Changes	action	string	The action performed on the resource.	acl_modified, cleared, created, deleted, modified, read, stopped, updated
All_Changes	change_type	string	The type of change, such as filesystem or AAA (authentication, authorization, and accounting).	restart
All_Changes	command	string	The command that initiated the change.	
All_Changes	dest	string	The resource where change occurred. You can **alias** this from more specific fields not included in this data model, such as dest_host, dest_ip, or dest_name.	
All_Changes	dest_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Changes	dest_category	string		
All_Changes	dest_priority	string		
All_Changes	dvc	string	The device that reported the change, if applicable, such as a FIP or CIM server. You can **alias** this from more specific fields not included in this data model, such as dvc_host, dvc_ip, or dvc_name.	
All_Changes	object	string	Name of the affected object on the resource (such as a router interface, user account, or server volume).	
All_Changes	object_attrs	string	The attributes that were updated on the updated resource object, if applicable.	
All_Changes	object_category	string	Generic name for the class of the updated resource object. Expected values may be specific to an app.	directory, file, group, registry, user
All_Changes	object_id	string	The unique updated resource object ID as presented to the system, if applicable (for instance, a SID, UUID, or GUID value).	
All_Changes	object_path	string	The path of the modified resource object, if applicable (such as a file, directory, or volume).	
All_Changes	result	string	The vendor-specific result of a change, or clarification of an action status. For instance, status=failure may be accompanied by result=blocked by policy or result=disk full. result is a string. Please use a msg_severity_id field (not included in the data model) for severity ID fields that are integer data types.	lockout
All_Changes	result_id	string	A result indicator for an action status.	
All_Changes	src	string	The resource where the change was originated. You can **alias** this from more specific fields not included in the data model, such as src_host, src_ip, or src_name.	

Dataset name	Field name	Data type	Description	Expected values
All_Changes	`src_bunit`	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Changes	`src_category`	string		
All_Changes	`src_priority`	string		
All_Changes	`status`	string	Status of the update.	`success`, `failure`
All_Changes	`tag`	string	This automatically generated field is used to access tags from within datamodels. Do not define extractions for this field when writing add-ons.	
All_Changes	`user`	string	The user or entity performing the change. For account changes, this is the account that was changed. See `src_user` for user or entity performing the change.	
All_Changes	`vendor_product`	string	The vendor and product or service that detected the change. This field can be automatically populated by `vendor` and `product` fields in your data.	
Account_Management	`dest_nt_domain`	string	The NT domain of the destination, if applicable.	
Account_Management	`src_nt_domain`	string	The NT domain of the source, if applicable.	
Account_Management	`src_user`	string	For account changes, the user or entity performing the change.	
Account_Management	`src_user_bunit`	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Account_Management	`src_user_category`	string		
Account_Management	`src_user_priority`	string		
Filesystem_Changes	`file_access_time`	time	The time the file (the object of the event) was accessed.	
Filesystem_Changes	`file_acl`	string	Access controls associated with the file affected by the event.	
Filesystem_Changes	`file_create_time`	time	The time the file (the object of the event) was created.	
Filesystem_Changes	`file_hash`	string	A cryptographic identifier assigned to the file object affected by the event.	
Filesystem_Changes	`file_modify_time`	time	The time the file (the object of the event) was altered.	
Filesystem_Changes	`file_name`	string	The name of the file that is the object of the event (without location information related to local file or directory structure).	
Filesystem_Changes	`file_path`	string	The location of the file that is the object of the event, in local file and directory structure terms.	
Filesystem_Changes	`file_size`	number	The size of the file that is the object of the event, in kilobytes.	

Data Access

The Data Access data model is for monitoring shared data access user activity. It helps you detect a user's unauthorized data access, misuse, exfiltration, and more. It applies to events about users accessing data on servers that are shared by many other users, such as: The "file abc" on the "server xyz" was accessed (read, created, modified, shared, and so on) by a "user Bob".

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Data Access event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
Data_Access	data
	access

Fields for Data Access event datasets

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

For even more examples, see Data Access Field Mapping.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Data_Access	`action`	string	The data access action taken by the user.	• recommended • prescribed values: `copied`, `created`, `deleted`, `modified`, `read`, `stopped`, `updated`, `downloaded`, `uploaded`, `shared`
Data_Access	`app`	string	The application involved in the event.	recommended
Data_Access	`app_id`	string	Application ID as defined by the vendor.	
Data_Access	`dest`	string	The destination where the data resides or where it is being accessed, such as the product or application. You can alias this from more specific fields not included in this data model, such as `dest_host`, `dest_ip`, `dest_url`, or `dest_name`.	recommended
Data_Access	`dest_name`	string	Name of the destination as defined by the vendor.	
Data_Access	`dest_url`	string	Url of the product, application, or object.	
Data_Access	`dvc`	string	The device that reported the data access event.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Data_Access	email	string	The email address of the user involved in the event, or who initiated the event.	
Data_Access	object	string	Resource object name on which the action was performed by a user.	recommended
Data_Access	object_category	string	Generic name for the class of the updated resource object. Expected values may be specific to an app. For example, collaboration, file, folder, comment, task, note, and so on.	recommended
Data_Access	object_id	string	The unique updated resource object ID as presented to the system, if applicable. For example, a source_folder_id, doc_id.	recommended
Data_Access	object_path	string	The path of the modified resource object, if applicable, such as a file, directory, or volume.	
Data_Access	object_size	string	The size of the modified resource object.	recommended
Data_Access	owner	string	Resource owner.	
Data_Access	owner_email	string	Email of the resource owner.	
Data_Access	owner_id	string	ID of the owner as defined by the vendor.	
Data_Access	parent_object	string	Parent of the object name on which the action was performed by a user.	
Data_Access	parent_object_id	string	Parent object ID	
Data_Access	parent_object_category	string	Object category of the parent object on which action was performed by a user.	
Data_Access	src	string	The endpoint client host.	recommended
Data_Access	tenant_id	string	Tenant ID in multi-tenant environments.	recommended
Data_Access	user	string	The user involved in the event, or who initiated the event.	recommended
Data_Access	user_agent	string	The user agent through which the request was made, such as Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) or aws-cli/2.0.0 Python/3.7.4 Darwin/18.7.0 botocore/2.0.0dev4	recommended
Data_Access	user_group	string	The group of the user involved in the event, or who initiated the event.	
Data_Access	user_role	string	The role of the user involved in the event, or who initiated the event.	
Data_Access	vendor_product	string	The vendor and product name of the vendor.	recommended
Data_Access	vendor_product_id	string	The vendor and product name ID as defined by the vendor.	

Databases

The fields and tags in the Databases data model describe events that pertain to structured and semi-structured data storage.

50

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Databases event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Databases	database
|____ Database_Instance	instance
|____ Instance_Stats	stats
|____ Session_Info	session
|____ Lock_Info	lock
|____ Database_Query	query
|____ Tablespace	tablespace
|____ Query_Stats	stats

Fields for Databases event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data	Description	Abbreviated list of

		type		example values
All_Databases	dest	string	The destination of the database event. You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	
All_Databases	dest_bunit	string	The business unit of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Databases	dest_category	string	The category of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Databases	dest_priority	string	The priority of the destination, if applicable. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Databases	duration	number	The amount of time for the completion of the database event, in seconds.	
All_Databases	object	string	The name of the database object.	
All_Databases	response_time	number	The amount of time it took to receive a response in the database event, in seconds.	
All_Databases	src	string	The source of the database event. You can **alias** this from more specific fields, such as `src_host`, `src_ip`, or `src_name`.	
All_Databases	src_bunit	string	The business unit of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Databases	src_category	string	The category of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Databases	src_priority	string	The priority of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Instance_Stats	avg_executions	number	database instance.	
Instance_Stats	dump_area_used	string	The amount of the database dump area that has been used.	
Instance_Stats	instance_reads	number	The total number of reads for the database instance.	
Instance_Stats	instance_writes	number	The total number of writes for the database instance.	
Instance_Stats	number_of_users	number	The total number of users for the database instance.	
Instance_Stats	processes	number	The number of processes currently running for the database instance.	
Instance_Stats	sessions	number	The total number of sessions currently in use for the database instance.	
Instance_Stats	sga_buffer_cache_size	number	The total size of the buffer cache for the database instance, in bytes.	
Instance_Stats	sga_buffer_hit_limit	number	The maximum number of number of buffers that can be hit in the database instance without finding a free buffer.	
Instance_Stats	sga_data_dict_hit_ratio	number	The hit-to-miss ratio for the database instance's data dictionary.	
Instance_Stats	sga_fixed_area_size	number	The size of the fixed area (also referred to as the fixed SGA) for the database instance, in bytes.	
Instance_Stats	sga_free_memory	number	The total amount of free memory in the database instance SGA, in bytes.	
Instance_Stats	sga_library_cache_size	number	The total library cache size for the database instance, in bytes.	
Instance_Stats	sga_redo_log_buffer_size	number	The total size of the redo log buffer for the database instance, in bytes.	
Instance_Stats	sga_shared_pool_size	number	The total size of the shared pool for this database instance, in bytes.	
Instance_Stats	sga_sql_area_size	number	The total size of the SQL area for this database instance, in bytes.	
Instance_Stats	start_time	time	The total amount of uptime for the database instance.	
Instance_Stats	tablespace_used	string	The total amount of tablespace used for the database instance, in bytes.	
Session_Info	buffer_cache_hit_ratio	number	The percentage of logical reads from the buffer during the session (1-physical reads/session logical reads*100).	
Session_Info	commits	number	The number of commits per second performed by the user associated with the session.	
Session_Info	cpu_used	number	The number of CPU centiseconds used by the session. Divide this value by 100 to get the CPU seconds.	
Session_Info	cursor	number	The number of the cursor currently in use by the session.	
Session_Info	elapsed_time	number	The total amount of time elapsed since the user started the session by logging into the database server, in seconds.	
Session_Info	logical_reads	number		

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Lock_Info	last_call_minute	number	status. The definition of this field depends on the `session_status` value. If `session_status = ONLINE`, the `last_call_minute` value represents the time elapsed since the session became active. If `session_status = OFFLINE`, the `last_call_minute` value represents the time elapsed since the session became inactive.	
Lock_Info	lock_mode	string	The mode of the lock on the object.	
Lock_Info	lock_session_id	string	The session identifier of the locked object.	
Lock_Info	logon_time	number	The database logon time for the session.	
Lock_Info	obj_name	string	The name of the locked object.	
Lock_Info	os_pid	string	The process identifier for the operating system.	
Lock_Info	serial_num	string	The serial number of the object.	
Database_Query	query	string	The full database query.	
Database_Query	query_id	string	The identifier for the database query.	
Database_Query	query_time	time	The time the system initiated the database query.	
Database_Query	records_affected	number	The number of records affected by the database query.	
Tablespace	free_bytes	number	The total amount of free space in the tablespace, in bytes.	
Tablespace	tablespace_name	string	The name of the tablespace.	
Tablespace	tablespace_reads	number	The number of tablespace reads carried out by the query.	
Tablespace	tablespace_status	string	The status of the tablespace.	prescribed values: `Offline`, `Online`, `Read Only`
Tablespace	tablespace_writes	number	The number of tablespace writes carried out by the query.	
Query_Stats	indexes_hit	string	The names of the indexes hit by the database query.	
Query_Stats	query_plan_hit	string	The name of the query plan hit by the query.	
Query_Stats	stored_procedures_called	string	The names of the stored procedures called by the query.	
Query_Stats	tables_hit	string	The names of the tables hit by the query.	

Data Loss Prevention

The fields in the Data Loss Prevention (DLP) data model describe events gathered from DLP tools used to identify, monitor and protect data.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with DLP event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
DLP_Incidents	dlp
	incident

Fields for DLP event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
DLP_Incidents	action	string	The action taken by the DLP device.	• recommended • required for pytest-splunk-addon
DLP_Incidents	app	string	The application involved in the event.	required for pytest-splunk-addon
DLP_Incidents	category	string	The category of the DLP event.	• recommenderd • required for pytest-splunk-addon
DLP_Incidents	dest	string	The target of the DLP event.	• recommended • required for pytest-splunk-addon
DLP_Incidents	dest_bunit	string	The business unit of the DLP target. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	dest_category	string	The category of the DLP target. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	dest_priority	string	The priority of the DLP target. This field is automatically provided by asset and identity	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	dest_zone	string	The zone of the DLP target.	
DLP_Incidents	dlp_type	string	The type of DLP system that generated the event.	• recommended • required for pytest-splunk-addon
DLP_Incidents	dvc	string	The device that reported the DLP event.	• recommended • required for pytest-splunk-addon
DLP_Incidents	dvc_bunit	string	The business unit of the DLP target. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	dvc_category	string	The category of the DLP device. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	dvc_priority	string	The priority of the DLP device. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	dvc_zone	string	The zone of the DLP device.	
DLP_Incidents	object	string	The name of the affected object.	• recommended • required for pytest-splunk-addon
DLP_Incidents	object_category	string	The category of the affected object.	• recommended • required for pytest-splunk-addon
DLP_Incidents	object_path	string	The path of the affected object.	• recommended • required for pytest-splunk-addon
DLP_Incidents	severity	string	The severity of the DLP event.	• recommended • required for pytest-splunk-addon
DLP_Incidents	severity_id	string		

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			The numeric or vendor specific severity indicator corresponding to the event severity.	
DLP_Incidents	signature	string	The name of the DLP event.	• recommended • required for pytest-splunk-addon
DLP_Incidents	signature_id	string	The unique identifier or event code of the event signature.	
DLP_Incidents	src	string	The source of the DLP event.	recommended
DLP_Incidents	src_bunit	string	The business unit of the DLP source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	src_category	string	The category of the DLP source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	src_priority	string	The priority of the DLP source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	src_user	string	The source user of the DLP event.	• recommended • required for pytest-splunk-addon
DLP_Incidents	src_user_bunit	string	The business unit of the DLP source user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	src_user_category	string	The category of the DLP source user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	src_user_priority	string	The priority of the DLP source user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	src_zone	string	The zone of the DLP source.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
DLP_Incidents	tag	string	This automatically generated field is used to access tags from within datamodels. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	user	string	The target user of the DLP event.	recommended
DLP_Incidents	user_bunit	string	The business unit of the DLP user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	user_category	string	The category of the DLP user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	user_priority	string	The priority of the DLP user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DLP_Incidents	vendor_product	string	The vendor and product name of the DLP system.	recommended

Email

The fields and tags in the Email data model describe email traffic, whether server:server or client:server.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Email event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Email	email
|____ Delivery	delivery
|____ Content	content
	filter

Dataset name	Tag name
|____ Filtering	

Fields for the Email event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values

All_Email	`action`	string	Action taken by the reporting device.	• recommended
				• required for pytest-splunk-addon
				• prescribed values:
				  `delivered`, `blocked`,
				  `quarantined`, `deleted`

All_Email	`delay`	number	Total sending delay in milliseconds.	
All_Email	`dest`	string	The endpoint system to which the message was delivered. You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	• recommended • required for pytest-splunk-addon
All_Email	`dest_bunit`	string	The business unit of the endpoint system to which the message was delivered. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	`dest_category`	string	The category of the endpoint system to which the message was delivered. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	`dest_priority`	string	The priority of the endpoint system to which the message was delivered.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	`duration`	number	The amount of time for the completion of the messaging event, in seconds.	
All_Email	`file_hash`	string	The hashes for the files attached to the message, if any exist.	
All_Email	`file_name`	string	The names of the files attached to the message, if any exist.	
All_Email	`file_size`	number	The size of the files attached the message, in bytes.	
All_Email	`internal_message_id`	string	Host-specific unique message identifier.	• required for pytest-splunk-addon • other: Such as `aid` in sendmail, `IMI` in Domino, `Internal-Message-ID` in Exchange, and `MID` in Ironport).
All_Email	`message_id`	string	The globally-unique message identifier.	required for pytest-splunk-addon
All_Email	`message_info`	string	Additional information about the message.	
All_Email	`orig_dest`	string	The original destination host of the message. The message destination host can change when a message is relayed or bounced.	
All_Email	`orig_recipient`	string	The original recipient of the message. The message recipient can change when the original email address is an alias and has to be resolved to the actual recipient.	
All_Email	`orig_src`	string	The original source of the message.	
All_Email	`process`	string	The name of the email executable that carries out the message transaction.	other: `sendmail`, `postfix`, or the name of an email client
All_Email	`process_id`	number	The numeric identifier of the process invoked to send the message.	
All_Email	`protocol`	string	The email protocol involved, such as `SMTP` or `RPC`.	• required for pytest-splunk-addon • prescribed values: `smtp`, `imap`, `pop3`, `mapi`

All_Email	`recipient`	string	A field listing individual recipient email addresses.	• recommended
				• required for pytest-splunk-addon
				• other:
				  `recipient="foo@splunk.com"`,
				  `recipient="bar@splunk.com"`

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Email	recipient_count	number	The total number of intended message recipients.	required for pytest-splunk-addon
All_Email	recipient_domain	string	The domain name contained within the recipient email addresses.	recommended
All_Email	recipient_status	string	The recipient delivery status, if available.	
All_Email	response_time	number	The amount of time it took to receive a response in the messaging event, in seconds.	
All_Email	retries	number	The number of times that the message was automatically resent because it was bounced back, or a similar transmission error condition.	
All_Email	return_addr	string	The return address for the message.	
All_Email	size	number	The size of the message, in bytes.	
All_Email	src	string	The system that sent the message. You can **alias** this from more specific fields, such as src_host, src_ip, or src_name.	• recommended • required for pytest-splunk-addon
All_Email	src_bunit	string	The business unit of the system that sent the message. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	src_category	string	The category of the system that sent the message. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	src_priority	string	The priority of the system that sent the message. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	src_user	string	The email address of the message sender.	• recommended • required for pytest-splunk-addon
All_Email	src_user_bunit	string	The business unit of the message sender.	

61

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	src_user_category	string	The category of the message sender. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	src_user_domain	string	The domain name contained within the email address of the message sender.	recommended
All_Email	src_user_priority	string	The priority of the message sender. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	status_code	string	The status code associated with the message.	
All_Email	subject	string	The subject of the message.	
All_Email	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
All_Email	url	string	The URL associated with the message, if any.	
All_Email	user	string	The user context for the process. This is not the email address for the sender. For that, look at the src_user field.	required for pytest-splunk-addon
All_Email	user_bunit	string	The business unit of the user context for the process. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	user_category	string	The category of the user context for the process. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Email	user_priority	string	The priority of the user context for the `process.` This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Email	vendor_product	string	The vendor and product of the email server used for the email transaction. This field can be automatically populated by `vendor` and `product` fields in your data.	recommended
All_Email	xdelay	string	Extended delay information for the message transaction. May contain details of all the delays from all the servers in the message transmission chain.	
All_Email	xref	string	An external reference. Can contain message IDs or recipient addresses from related messages.	
Filtering	filter_action	string	The status produced by the filter.	other: `accepted`, `rejected`, `dropped`
Filtering	filter_score	number	Numeric indicator assigned to specific emails by an email filter.	
Filtering	signature	string	The name of the filter applied.	recommended
Filtering	signature_extra	string	Any additional information about the filter.	
Filtering	signature_id	string	The id associated with the filter name.	

Search Example

An example follows for the root dataset of All_Email and datamodel of Email:

```
| tstats summariesonly=t count from datamodel="Email" by All_Email.file_name
```

Endpoint

The Endpoint data model replaces the Application State data model, which is deprecated as of software version 4.12.0. The architecture of this data model is different than the data model it replaces. Each data set is directly searchable as `DataModel.DataSet` rather than by node name.

The Endpoint data model is for monitoring endpoint clients including, but not limited to, end user machines, laptops, and bring your own devices (BYOD). If an event is about an endpoint process, service, file, port, and so on, then it relates to the Endpoint data model. For administrative and policy types of changes to infrastructure security devices, servers, and endpoint detection and response (EDR) systems, see Change.Endpoint in the Change data model.

The fields and tags in the Endpoint data model describe service or process inventory and state, such as Unix daemons, Windows services, running processes on any OS, or similar systems.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Dataset name	Tag name
Endpoint	
|____ Ports	listening
	port
|____ Processes	process
	report
|____ Services	service
	report
|____ Filesystem	endpoint
	filesystem
|____ Registry	endpoint
	registry

Fields for the Endpoint event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Ports

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Ports	creation_time	timestamp	The time at which the network port started listening on the endpoint.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Ports	dest	string	The endpoint on which the port is listening. Expression: `if(isnull(dest) OR dest=\"\",\"unknown\",dest)`	• recommended • required for pytest-splunk-addon
Ports	dest_bunit	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	dest_category	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	dest_port	number	Network port listening on the endpoint, such as 53.	• recommended • required for pytest-splunk-addon
Ports	dest_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	dest_requires_av	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	dest_should_timesync	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	dest_should_update	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	process_guid	string	The globally unique identifier of the process assigned by the vendor_product.	
Ports	process_id	string	The numeric identifier of the process assigned by the operating system.	
Ports	src	string	The "remote" system connected to the listening port (if applicable). Expression: `if(isnull(src) OR src=\"\",\"unknown\",src)`	• recommended • required for pytest-splunk-addon
Ports	src_category	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	src_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			add-ons.	
Ports	`src_port`	number	The "remote" port connected to the listening port (if applicable). Expression: `if(isnum(src_port),src_port,0)`	• recommended • required for pytest-splunk-addon
Ports	`src_requires_av`	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	`src_should_timesync`	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	`src_should_update`	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	`state`	string	The status of the listening port, such as established, listening, etc.	required for pytest-splunk-addon
Ports	`tag`	string	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Ports	`transport`	string	The network transport protocol associated with the listening port, such as tcp, udp, etc."	• recommended • required for pytest-splunk-addon
Ports	`transport_dest_port`	string	Calculated as transport/dest_port, such as tcp/53.	
Ports	`user`	string	The user account associated with the listening port. Expression: `if(isnull(user) OR user=\"\",\"unknown\",user)`	recommended
Ports	`user_bunit`	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	`user_category`	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Ports	`user_priority`	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	

Processes

Dataset name	Field name	Data type	Description

66

Processes	`action`	string	The action taken by the endpoint, such as allowed, blocked, deferred.
Processes	`cpu_load_percent`	number	CPU load consumed by the process (in percent).
Processes	`dest`	string	The endpoint for which the process was spawned. Expression: `if(isnull(dest) OR dest=\"\",\"unknown\",dest)`
Processes	`dest_bunit`	string	This field is automatically provided by asset and identity correlation features of applications like S Enterprise Security. Do not define extractions for this fields when writing add-ons.
Processes	`dest_category`	string	This field is automatically provided by asset and identity correlation features of applications like S Enterprise Security. Do not define extractions for this fields when writing add-ons.
Processes	`dest_is_expected`	boolean	This field is automatically provided by asset and identity correlation features of applications like S Enterprise Security. Do not define extractions for this field when writing add-ons.
Processes	`dest_priority`	string	This field is automatically provided by asset and identity correlation features of applications like S Enterprise Security. Do not define extractions for this fields when writing add-ons.
Processes	`dest_requires_av`	boolean	This field is automatically provided by asset and identity correlation features of applications like S Enterprise Security. Do not define extractions for this fields when writing add-ons.
Processes	`dest_should_timesync`	boolean	This field is automatically provided by asset and identity correlation features of applications like S Enterprise Security. Do not define extractions for this fields when writing add-ons.
Processes	`dest_should_update`	boolean	This field is automatically provided by asset and identity correlation features of applications like S Enterprise Security. Do not define extractions for this fields when writing add-ons.
Processes	`mem_used`	number	Memory used by the process (in bytes).
Processes	`original_file_name`	string	Original name of the file, not including path. Sometimes this field is similar to process name but t do not always match, such as `process_name=pwsh` and `original_file_name=powershel` to detect renamed instances of any process executing.
Processes	`os`	string	The operating system of the resource, such as Microsoft Windows Server 2008r2.
Processes	`parent_process`	string	The full command string of the parent process. Expression: `if(isnull(parent_process) OR parent_process=\"\",\"unknown\"` `parent_process)`
Processes	`parent_process_exec`	string	The executable name of the parent process.
Processes	`parent_process_id`	number	The numeric identifier of the parent process assigned by the operating system.
Processes	`parent_process_guid`	string	The globally unique identifier of the parent process assigned by the vendor_product.
Processes	`parent_process_name`	string	The friendly name of the parent process, such as notepad.exe. Expression: `case(isnotnull(parent_process_name) AND` `parent_process_name!=\"\",parent_process_name, isnotnull(parent_process` `parent_process!=\"\",replace(parent_process,` `\"^\\s*([^\\s]+).*\",\"\\1\"),1=1,\"unknown\")"`
Processes	`parent_process_path`	string	The file path of the parent process, such as C:\Windows\System32\notepad.exe.
Processes	`process`	string	The full command string of the spawned process. Such as C:\\WINDOWS\\system32\\cmd.exe \/ \"\"C:\\Program Files\\SplunkUniversalForwarder\\etc\\system\\bin\\powershell.cmd\" --scheme\"".

Processes	vendor_product	string	The vendor and product name of the Endpoint solution that reported the event, such as Carbon B Response. This field can be automatically populated by vendor and product fields in your data." Expression: case(isnotnull(vendor_product),vendor_product, isnotnull(ven AND vendor!=\"unknown\" AND isnotnull(product) AND product!=\"unknown\",vendor.\" \".product,isnotnull(vendor) AND vendor!=\"unknown\" AND (isnull(product) OR product=\"unknown\"),vendor unknown\",(isnull(vendor) OR vendor=\"unknown\") AND isnotnull(product) product!=\"unknown\",\"unknown \" **Description** isnotnull(sourcetype),sourcet 1=1,\"unknown\")	
Dataset name	**Field name**	**Data type**	

Services

Dataset name	**Field name**	**Data type**	**Description**	**Abbreviated list of example values**
Services	description	string	The description of the service.	
Services	dest	string	The endpoint for which the service is installed. Expression: if(isnull(dest) OR dest=\"\",\"unknown\",dest)	• recommended • required for pytest-splunk-ad
Services	dest_bunit	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Services	dest_category	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Services	dest_is_expected	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Services	dest_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Services	dest_requires_av	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Services	dest_should_timesync	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Services	dest_should_update	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Services	process_guid	string	The globally unique identifier of the process assigned by the vendor_product.	
Services	process_id	string	The numeric identifier of the process assigned by the operating system.	
Services	service	string	The full service name. Expression: if(isnull(service) OR service=\"\",\"unknown\",service)	• recommended • required for

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				pytest-splunk-ad
Services	`service_dll`	string	The dynamic link library associated with the service.	
Services	`service_dll_path`	string	The file path to the dynamic link library assocatied with the service, such as C:\Windows\System32\comdlg32.dll.	
Services	`service_dll_hash`	string	The digests of the dynamic link library associated with the service, such as <md5>, <sha1>, etc.	
Services	`service_dll_signature_exists`	boolean	Whether or not the dynamic link library associated with the service has a digitally signed signature.	
Services	`service_dll_signature_verified`	boolean	Whether or not the dynamic link library associated with the service has had its digitally signed signature verified.	
Services	`service_exec`	string	The executable name of the service.	
Services	`service_hash`	string	The digest(s) of the service, such as <md5>, <sha1>, etc.	
Services	`service_id`	string	The unique identifier of the service assigned by the operating system. Expression: `if(isnull(service_id) OR service_id=\"\",\"unknown\",service_id)`	recommended
Services	`service_name`	string	The friendly service name. Expression: `if(isnull(service_name) OR service_name=\"\",\"unknown\",service_name)`	• recommended • required for pytest-splunk-ad
Services	`service_path`	string	The file path of the service, such as C:\WINDOWS\system32\svchost.exe.	required for pytest-splunk-addon
Services	`service_signature_exists`	boolean	Whether or not the service has a digitally signed signature.	
Services	`service_signature_verified`	boolean	Whether or not the service has had its digitally signed signature verified.	
Services	`start_mode`	string	The start mode for the service. Expression: `if(isnull(start_mode) OR start_mode=\"\",\"unknown\",start_mode)`	• recommended • required for pytest-splunk-ad • prescribed values: `disabled, manual, auto`
Services	`status`	string	The status of the service. Expression: `if(isnull(dest) OR dest=\"\",\"unknown\",dest)`	• recommended • required for pytest-splunk-ad • prescribed values: `critical, started,`

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				stopped, warning
Services	tag	string	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Services	user	string	The user account associated with the service. Expression: `if(isnull(user) OR user=\"\",\"unknown\",user)`	• recommended • required for pytest-splunk-ad
Services	user_bunit	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Services	user_category	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Services	user_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Services	vendor_product	string	The vendor and product name of the Endpoint solution that reported the event, such as Carbon Black Cb Response. This field can be automatically populated by vendor and product fields in your data. Expression: `case(isnotnull(vendor_product),vendor_product, isnotnull(vendor) AND vendor!=\"unknown\" AND isnotnull(product) AND product!=\"unknown\",vendor.\" \".product,isnotnull(vendor) AND vendor!=\"unknown\" AND (isnull(product) OR product=\"unknown\"),vendor.\" unknown\",(isnull(vendor) OR vendor=\"unknown\") AND isnotnull(product) AND product!=\"unknown\",\"unknown \".product,isnotnull(sourcetype),sourcetype, 1=1,\"unknown\")`	recommended

Filesystem

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Filesystem	action	string	The action performed on the resource. Expression: `if(isnull(action) OR action=\"\",\"unknown\",action)`	• recommended • required for pytest-splunk-addon

70

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				• prescribed values: `acl_modified`, `created`, `deleted`, `modified`, `read`
Filesystem	`dest`	string	The endpoint pertaining to the filesystem activity. Expression: `if(isnull(dest) OR dest=\"\",\"unknown\",dest)`	• recommended • required for pytest-splunk-addon
Filesystem	`dest_bunit`	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Filesystem	`dest_category`	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Filesystem	`dest_priority`	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Filesystem	`dest_requires_av`	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Filesystem	`dest_should_timesync`	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Filesystem	`dest_should_update`	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Filesystem	`file_access_time`	timestamp	The time that the file (the object of the event) was accessed.	recommended
Filesystem	`file_create_time`	timestamp	The time that the file (the object of the event) was created.	recommended
Filesystem	`file_hash`	string	A cryptographic identifier assigned to the file object affected by the event. Expression: `if(isnull(file_hash) OR file_hash=\"\",\"unknown\",file_hash)`	recommended
Filesystem	`file_modify_time`	timestamp	The time that the file (the object of the event) was altered.	recommended
Filesystem	`file_name`	string	The name of the file, such as notepad.exe. Expression: `if(isnull(file_name) OR file_name=\"\",\"unknown\",file_name`	• recommended • required for pytest-splunk-addon

71

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Filesystem	file_path	string	The path of the file, such as C:\Windows\System32\notepad.exe. Expression: `if(isnull(file_path) OR file_path=\"\",\"unknown\",file_path)`	• recommended • required for pytest-splunk-addon
Filesystem	file_acl	string	Access controls associated with the file affected by the event. Expression: `if(isnull(file_acl) OR file_acl=\"\",\"unknown\",file_acl)`	recommended
Filesystem	file_size	string	The size of the file that is the object of the event, in kilobytes. Expression: `if(isnum(file_size),file_size,null())`	recommended
Filesystem	process_guid	string	The globally unique identifier of the process assigned by the vendor_product.	
Filesystem	process_id	string	The numeric identifier of the process assigned by the operating system.	
Filesystem	tag	string	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Filesystem	user	string	The user account associated with the filesystem access. Expression: `if(isnull(user) OR user=\"\",\"unknown\",user)`	• recommended • required for pytest-splunk-addon
Filesystem	user_bunit	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Filesystem	user_category	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Filesystem	user_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Filesystem	vendor_product	string	The vendor and product name of the Endpoint solution that reported the event, such as Carbon Black Cb Response. This field can be automatically populated by vendor and product fields in your data. Expression: `case(isnotnull(vendor_product),vendor_product, isnotnull(vendor) AND vendor!=\"unknown\" AND isnotnull(product) AND product!=\"unknown\",vendor.\" \".product,isnotnull(vendor) AND vendor!=\"unknown\" AND (isnull(product) OR product=\"unknown\"),vendor.\" unknown\",(isnull(vendor) OR vendor=\"unknown\")`	recommended

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			AND isnotnull(product) AND product!=\"unknown\",\"unknown \".product,isnotnull(sourcetype),sourcetype, 1=1,\"unknown\")	

Registry

Dataset name	Field name	Data type	Description	Abbrev
Registry	action	string	The action performed on the resource. Expression: `if(isnull(action) OR action=\"\",\"unknown\",action)`	• r • r p • p c m
Registry	dest	string	The endpoint pertaining to the registry events. Expression: `if(isnull(dest) OR dest=\"\",\"unknown\",dest)`	• r • r p
Registry	dest_bunit	string	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Registry	dest_category	string	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Registry	dest_priority	string	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Registry	dest_requires_av	boolean	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Registry	dest_should_timesync	boolean	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Registry	dest_should_update	boolean	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Registry	process_guid	string	The globally unique identifier of the process assigned by the vendor_product.	
Registry	process_id	string	The numeric identifier of the process assigned by the operating system.	
Registry	registry_hive	string	The logical grouping of registry keys, subkeys, and values.	• r p • p H H H H H H H
Registry	registry_path	string	The path to the registry value, such as \win\directory\directory2\{676235CD-B656-42D5-B737-49856E97D072}\PrinterDriverData.	• r

73

Dataset name	Field name	Data type	Description	Abbrev
			Expression: `if(isnull(registry_path) OR registry_path=\"\",\"unknown\",registry_path)`	• r p
Registry	registry_key_name	string	The name of the registry key, such as PrinterDriverData. Expression: `if(isnull(registry_key_name) OR registry_key_name=\"\",\"unknown\", registry_key_name)`	• r • r p
Registry	registry_value_data	string	The unaltered registry value. Expression: `if(isnull(registry_value_data) OR registry_value_data=\"\",\"unknown\", registry_value_data)`	• r • r p
Registry	registry_value_name	string	The name of the registry value. Expression: `if(isnull(registry_value_name) OR registry_value_name=\"\",\"unknown\", registry_value_name)`	• r • r p
Registry	registry_value_text	string	The textual representation of registry_value_data (if applicable).	required fo

Registry	registry_value_type	string	The type of the registry value.
			
			Expression: `if(isnull(registry_value_type) OR registry_value_type=\"\",\"unknown\", registry_value_type)`
				• r
				• r
				p
				• p
				  R
				  R
				  R
				  R
				  R
				  R
				  R
				  R
				  R

Registry	status	string	The outcome of the registry action.	• r p • p f
Registry	tag	string	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	
Registry	user	string	The user account associated with the registry access. Expression: `if(isnull(user) OR user=\"\",\"unknown\",user)`	• r • r p
Registry	user_bunit	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Registry	user_category	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Registry	user_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	

74

Dataset name	Field name	Data type	Description	Abbrev
Registry	vendor_product	string	The vendor and product name of the Endpoint solution that reported the event, such as Carbon Black Cb Response. This field can be automatically populated by vendor and product fields in your data. Expression: `case(isnotnull(vendor_product),vendor_product, isnotnull(vendor) AND vendor!=\"unknown\" AND isnotnull(product) AND product!=\"unknown\",vendor.\" \".product,isnotnull(vendor) AND vendor!=\"unknown\" AND (isnull(product) OR product=\"unknown\"),vendor.\" unknown\",(isnull(vendor) OR vendor=\"unknown\") AND isnotnull(product) AND product!=\"unknown\",\"unknown \".product,isnotnull(sourcetype),sourcetype, 1=1,\"unknown\")`	recommen

Search Example

The Endpoint data model is not directly searchable. Searching the Endpoint data model directly may show the following error: "Error in 'DataModelCache': Invalid or unaccelerable root object for datamodel." Instead, search for one or more of the data sets within the Endpoint data model: Endpoint.Ports, Endpoint.Processes, Endpoint.Services, or Endpoint.Filesystem.

An example follows for the new versus old search for summary count of ports by destination port:

Endpoint
```
    | tstats `summariesonly` count from datamodel=Endpoint.Ports by Ports.dest
```
Application State
```
    | tstats count from datamodel=Application_State.All_Application_State where
    nodename="All_Application_State.Ports" by All_Application_State.dest
```

Event Signatures

Event Signatures is a standard location to store Windows EventID. This data model is searchable as DataModel.DataSet. It is not accelerated by default, but the appropriate acceleration settings have been defined.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Dataset name	Tag name
Event_Signatures	
|____ Signatures	track_event_signatures

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Event Signatures

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Signatures	dest	string	System affected by the signature.	
Signatures	dest_bunit	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Signatures	dest_category	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Signatures	dest_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this fields when writing add-ons.	
Signatures	signature	string	The human readable event name.	
Signatures	signature_id	string	The event name identifier (as supplied by the vendor).	
Signatures	tag	string	This automatically generated field is used to access tags from within data models. Add-on builders do not need to populate it.	

Calculations

Calculation ID	Field name	Data type	Description	Abbreviated list of example values
Signatures_vendor_product	vendor_product	string	The vendor and product name of the technology that reported the event, such as Carbon Black Cb Response. This field can be automatically populated by vendor and product fields in your data. Expression: `case(isnotnull(vendor_product),vendor_product,` isnotnull(vendor) AND vendor!=\"unknown\" AND isnotnull(product) AND product!=\"unknown\",vendor.\" \".product,isnotnull(vendor) AND vendor!=\"unknown\" AND (isnull(product) OR product=\"unknown\"),vendor.\" unknown\",(isnull(vendor) OR vendor=\"unknown\") AND isnotnull(product) AND product!=\"unknown\",\"unknown	recommended

Calculation ID	Field name	Data type	Description	Abbreviated list of example values
			\".product,isnotnull(sourcetype),sourcetype, 1=1,\"unknown\")"	

Search Example

An example follows for the summary count of signatures by destination ID:

```
| tstats count from datamodel=Event_Signatures.Signatures by Signatures.signature_id,Signatures.dest
```

Interprocess Messaging

The fields in the Interprocess Messaging data model describe transactional requests in programmatic interfaces. This enables you to establish the data requirements for a domain and create apps that support each other. The Interprocess Messaging data model enables reporting on

- messaging queues such as Tibco, MSMQ, Apache ESB, IBM MQ, and XMPP.
- IPC interfaces like RPC and WMI.
- Web interfaces such as SOAP and REST.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with the Interprocess Messaging event dataset

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Interprocess_Messaging	messaging

Fields for the Interprocess Messaging event dataset

The following table lists the extracted and calculated fields for the event dataset in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Interprocess_Messaging	dest	string	The destination of the message. You can **alias** this from more specific fields, such as dest_host, dest_ip, or dest_name.	
All_Interprocess_Messaging	dest_bunit	string	The business unit of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Interprocess_Messaging	dest_category	string	The type of message destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	prescribed values: queue, topic
All_Interprocess_Messaging	dest_priority	string	The priority of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Interprocess_Messaging	duration	number	The number of seconds from message call to message response. Can be derived by getting the difference between the request_sent_time and the message_received_time.	
All_Interprocess_Messaging	endpoint	string	The endpoint that the message accessed during the RPC (remote procedure call) transaction.	
All_Interprocess_Messaging	endpoint_version	string	The version of the endpoint accessed during the RPC (remote procedure call) transaction, such as 1.0 or 1.22.	
All_Interprocess_Messaging	message	string	A command or reference that an RPC (remote procedure call) reads or responds to.	
All_Interprocess_Messaging	message_consumed_time	time	The time that the RPC (remote procedure call) read the message and was prepared to take some sort of action.	
All_Interprocess_Messaging	message_correlation_id	string	The message correlation identification value.	
All_Interprocess_Messaging	message_delivered_time	time	The time that the message producer sent the message.	
All_Interprocess_Messaging	message_delivery_mode	string	The message delivery mode. Possible values depend on the type of message-oriented middleware (MOM) solution in use. They can be words like Transient (meaning the message is stored in memory and is lost if the server dies or restarts) or Persistent (meaning the message is stored both in memory and on disk and is preserved if the server dies or restarts). They can also be numbers like 1, 2, and so on.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Interprocess_Messaging	message_expiration_time	time	The time that the message expired.	
All_Interprocess_Messaging	message_id	string	The message identification.	
All_Interprocess_Messaging	message_priority	string	The priority of the message. Important jobs that the message queue should answer no matter what receive a higher message_priority than other jobs, ensuring they are completed before the others.	
All_Interprocess_Messaging	message_properties	string	An arbitrary list of message properties. The set of properties displayed depends on the message-oriented middleware (MOM) solution that you are using.	
All_Interprocess_Messaging	message_received_time	time	The time that the message was received by a message-oriented middleware (MOM) solution.	
All_Interprocess_Messaging	message_redelivered	boolean	Indicates whether or not the message was redelivered.	
All_Interprocess_Messaging	message_reply_dest	string	The name of the destination for replies to the message.	
All_Interprocess_Messaging	message_type	string	The type of message, such as call or reply.	
All_Interprocess_Messaging	parameters	string	Arguments that have been passed to an endpoint by a REST call or something similar. A sample parameter could be something like foo=bar.	
All_Interprocess_Messaging	payload	string	The message payload.	
All_Interprocess_Messaging	payload_type	string	The type of payload in the message. The payload type can be text (such as json, xml, and raw) or binary (such as compressed, object, encrypted, and image).	
All_Interprocess_Messaging	request_payload	string	The content of the message request.	
All_Interprocess_Messaging	request_payload_type	string	The type of payload in the message request. The payload type can be text (such as json, xml, and raw) or binary (such as compressed, object, encrypted, and image).	
All_Interprocess_Messaging	request_sent_time	time	The time that the message request was sent.	
All_Interprocess_Messaging	response_code	string	The response status code sent by the receiving server. Ranges between 200 and 404.	
All_Interprocess_Messaging	response_payload_type	string	The type of payload in the message response. The payload type can be text (such as json, xml, and raw) or binary (such as compressed, object, encrypted, and image).	
All_Interprocess_Messaging	response_received_time	time	The time that the message response was received.	
All_Interprocess_Messaging	response_time	number	The amount of time it took to receive a response, in seconds.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Interprocess_Messaging	`return_message`	string	The response status message sent by the message server.	
All_Interprocess_Messaging	`rpc_protocol`	string	The protocol that the message server uses for remote procedure calls (RPC). Possible values include `HTTP REST`, `SOAP`, and `EJB`.	
All_Interprocess_Messaging	`status`	boolean	The status of the message response.	prescribed values: `pass`, `fail`
All_Interprocess_Messaging	`tag`	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	

Intrusion Detection

The fields in the Intrusion Detection data model describe attack detection events gathered by network monitoring devices and apps.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Intrusion Detection event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
IDS_Attacks	ids
	attack

Fields for Intrusion Detection event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name		Description	

		Data type		Abbreviated list of example values
IDS_Attacks	action	string	The action taken by the intrusion detection system (IDS).	• required for pytest-splunk-addon • prescribed values: allowed, blocked
IDS_Attacks	category	string	The vendor-provided category of the triggered signature, such as spyware. This field is a string. Use a category_id field (not included in this data model) for category ID fields that are integer data types.	• recommended • required for pytest-splunk-addon
IDS_Attacks	dest	string	The destination of the attack detected by the intrusion detection system (IDS). You can **alias** this from more specific fields not included in this data model, such as dest_host, dest_ip, or dest_name.	recommended
IDS_Attacks	dest_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
IDS_Attacks	dest_category	string		
IDS_Attacks	dest_priority	string		
IDS_Attacks	dest_port	number	The destination port of the intrusion.	
IDS_Attacks	dvc	string	The device that detected the intrusion event. You can **alias** this from more specific fields not included in this data model, such as dvc_host, dvc_ip, or dvc_name.	• recommended • required for pytest-splunk-addon
IDS_Attacks	dvc_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
IDS_Attacks	dvc_category	string		
IDS_Attacks	dvc_priority	string		
IDS_Attacks	file_hash	string	A cryptographic identifier assigned to the file object affected by the event.	
IDS_Attacks	file_name	string	The name of the file, such as notepad.exe.	
IDS_Attacks	file_path	string	The path of the file, such as C:\\Windows\\System32\\notepad.exe.	
IDS_Attacks	ids_type	string	The type of IDS that generated the event.	• recommended • required for pytest-splunk-addon • prescribed values: network, host, application, wireless
IDS_Attacks	severity	string	The severity of the network protection event. This field is a string. Use a severity_id field (not included in this data model) for severity ID fields that are integer data types. Also,	• recommended • required for pytest-splunk-addon

source, along with network infrastructure inventory and topology. This model was formerly labeled and documented as "Compute Inventory." The internal name of the datamodel has not changed, to support backward compatibility.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Inventory event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Dataset name			Tag name	
All_Inventory			inventory	
			cpu OR memory OR network OR storage OR (system, version) OR user OR virtual	
|____ CPU			cpu	
|____ Memory			memory	
|____ Network			network	
|____ Storage			storage	
|____ OS			system	
			version	
|____ User			user	
|____ Cleartext_Passwords			password=*	
|____ Default_Accounts			default	
|____ Virtual_OS			virtual	
|____ Snapshot			snapshot	
|____ Tools			tools	

Fields for Inventory event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Inventory	description	string	The description of the inventory system.	
All_Inventory	dest	string	The system where the data is going, the target of the event. You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	
All_Inventory	dest_bunit	string	The business unit of the system where the data is going. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Inventory	dest_category	string	The category of the system where the data is going, such as `email_server` or `SOX-compliant`. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Inventory	dest_priority	string	The priority of the system where the data is going. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Inventory	enabled	boolean	Indicates whether the resource is enabled or disabled.	
All_Inventory	family	string	The product family of the resource, such as `686_64` or `RISC`.	
All_Inventory	hypervisor_id	string	The hypervisor identifier, if applicable.	
All_Inventory	serial	string	The serial number of the resource.	
All_Inventory	status	string	The current reported state of the resource.	
All_Inventory	tag	string	Splunk uses this automatically generated field to access tags from within data models. You do not need to populate it.	
All_Inventory	vendor_product	string	The vendor and product name of the resource, such as `Cisco Catalyst 3850`. This field can be automatically populated by `vendor` and `product` fields in your data.	
All_Inventory	version	string	The version of a computer resource, such as `2008r2` or `3.0.0`.	
CPU	cpu_cores	number	The number of CPU cores reported by the resource (total, not per CPU).	
CPU	cpu_count	number	The number of CPUs reported by the resource.	
CPU	cpu_mhz	number	The maximum speed of the CPU reported by the resource (in megahertz).	
Memory	mem	number	The total amount of memory installed in or allocated to the resource, in megabytes.	
Network	dest_ip	string	The IP address for the system that the data is going to.	
Network	dns	string	The domain name server for the resource.	
Network	inline_nat	string	Identifies whether the resource is a network address translation pool.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Network	interface	string	The network interfaces of the computing resource, such as `eth0`, `eth1` or `Wired Ethernet Connection, Teredo Tunneling Pseudo-Interface`.	
Network	ip	string	The network addresses of the computing resource, such as `192.168.1.1` or `E80:0000:0000:0000:0202:B3FF:FE1E:8329`.	
Network	lb_method	string	The load balancing method used by the computing resource such as `method`, `round robin`, or `least weight`.	
Network	mac	string	A MAC (media access control) address associated with the resource, such as `06:10:9f:eb:8f:14`. **Note:** Always force lower case on this field. **Note:** Always use colons instead of dashes, spaces, or no separator.	
Network	name	string	A name field provided in some data sources.	
Network	node	string	Represents a node hit.	
Network	node_port	number	The number of the destination port on the server that you requested from.	
Network	src_ip	string	The IP address for the system from which the data originates.	
Network	vip_port	number	The port number for the virtual IP address (VIP). A VIP allows multiple MACs to use one IP address. VIPs are often used by load balancers.	
OS	os	string	The operating system of the resource, such as `Microsoft Windows Server 2008r2`. This field is constructed from `vendor_product` and `version` fields.	
Storage	array	string	The array that the storage resource is a member of, if applicable	
Storage	blocksize	number	The block size used by the storage resource, in kilobytes.	
Storage	cluster	string	The index cluster that the resource is a member of, if applicable.	
Storage	fd_max	number	The maximum number of file descriptors available.	
Storage	latency	number	The latency reported by the resource, in milliseconds.	
Storage	mount	string	The path at which a storage resource is mounted.	
Storage	parent	string	A higher level object that this resource is owned by, if applicable.	
Storage	read_blocks	number	The maximum possible number of blocks read per second during a polling period .	
Storage	read_latency	number	For a polling period, the average amount of time elapsed until a read request is filled by the host disks (in ms).	
Storage	read_ops	number	The total number of read operations in the polling period.	
Storage	storage	number	The amount of storage capacity allocated to the resource, in megabytes.	
Storage	write_blocks	number	The maximum possible number of blocks written per second during a polling period.	
Storage	write_latency	number	For a polling period, the average amount of time elapsed until a write request is filled by the host disks (in ms).	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Storage	write_ops	number	The total number of write operations in the polling period.	
User	interactive	boolean	Indicates whether a locally defined account on a resource can be interactively logged in.	
User	password	string	Displays the stored password(s) for a locally defined account, if it has any. For instance, an add-on may report the password column from /etc/passwd in this field.	
User	shell	string	Indicates the shell program used by a locally defined account.	
User	user	string	The full name of a locally defined account.	
User	user_bunit	string	The business unit of the locally-defined user account. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
User	user_category	string	The category of the system where the data originated, such as email_server or SOX-compliant. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
User	user_id	number	The user identification for a locally defined account.	
User	user_priority	string	The priority of a locally-defined account. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Virtual_OS	hypervisor	string	The hypervisor parent of a virtual guest OS.	
Snapshot	size	number	The snapshot file size, in megabytes.	
Snapshot	snapshot	string	The name of a snapshot file.	
Snapshot	time	time	The time at which the snapshot was taken.	

Java Virtual Machines (JVM)

The fields in the JVM data model describe generic Java server platforms.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with JVM event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name

Dataset name	Tag name
JVM	jvm
|____ Threading	threading
|____ Runtime	runtime
|____ OS	os
|____ Compilation	compilation
|____ Classloading	classloading
|____ Memory	memory

Fields for JVM event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
JVM	`jvm_description`	string	A description field provided in some data sources.	
JVM	`tag`	string	This automatically generated field is used to access tags from within datamodels. Add-on builders do not need to populate it.	
Threading	`cm_enabled`	boolean	Indicates whether thread contention monitoring is enabled.	prescribed values: `true, false, 1, 0`
Threading	`cm_supported`	boolean	Indicates whether the JVM supports thread contention monitoring.	prescribed values: `true, false, 1, 0`
Threading	`cpu_time_enabled`	boolean	Indicates whether thread CPU time measurement is enabled.	prescribed values: `true, false, 1, 0`

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Threading	`cpu_time_supported`	boolean	Indicates whether the Java virtual machine supports CPU time measurement for the current thread.	prescribed values: `true`, `false`, `1`, `0`
Threading	`current_cpu_time`	number	CPU-space time taken by the JVM, in seconds.	
Threading	`current_user_time`	number	User-space time taken by the JVM, in seconds.	
Threading	`daemon_thread_count`	number	The JVM's current daemon count.	
Threading	`omu_supported`	boolean	Indicates whether the JVM supports monitoring of object monitor usage.	prescribed values: `true`, `false`, `1`, `0`
Threading	`peak_thread_count`	number	The JVM's peak thread count.	
Threading	`synch_supported`	boolean	Indicates whether the JVM supports monitoring of ownable synchronizer usage.	prescribed values: `true`, `false`, `1`, `0`
Threading	`thread_count`	number	The JVM's current thread count.	
Threading	`threads_started`	number	The total number of threads started in the JVM.	
Runtime	`process_name`	string	Process name of the JVM process.	
Runtime	`start_time`	timestamp	Start time of the JVM process.	
Runtime	`uptime`	number	Uptime of the JVM process, in seconds.	
Runtime	`vendor_product`	string	The JVM product or service. This field can be automatically populated by the the `vendor` and `product` fields in your raw data.	
Runtime	`version`	string	Version of the JVM.	
OS	`committed_memory`	number	Amount of memory committed to the JVM, in bytes.	
OS	`cpu_time`	number	Amount of CPU time taken by the JVM, in seconds.	
OS	`free_physical_memory`	number	Amount of free physical memory remaining to the JVM, in bytes.	
OS	`free_swap`	number	Amount of free swap memory remaining to the JVM, in bytes.	
OS	`max_file_descriptors`	number	Maximum file descriptors available to the JVM.	
OS	`open_file_descriptors`	number	Number of file descriptors opened by the JVM.	
OS	`os`	string	OS that the JVM is running on.	
OS	`os_architecture`	string	OS architecture that the JVM is running on.	
OS	`os_version`	string	OS version that the JVM is running on.	
OS	`physical_memory`	number	Physical memory available to the OS that the JVM is running on, in bytes.	
OS	`swap_space`	number	Swap memory space available to the OS that the JVM is running on, in bytes.	
OS	`system_load`	number	System load of the OS that the JVM is running on.	
OS	`total_processors`	number	Total processor cores available to the OS that the JVM is running on.	
Compilation	`compilation_time`	number	Time taken by JIT compilation, in seconds.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Classloading	current_loaded	number	The current count of classes loaded in the JVM.	
Classloading	total_loaded	number	The total count of classes loaded in the JVM.	
Classloading	total_unloaded	number	The total count of classes unloaded from the JVM.	
Memory	heap_committed	number	Committed amount of heap memory used by the JVM, in bytes.	
Memory	heap_initial	number	Initial amount of heap memory used by the JVM, in bytes.	
Memory	heap_max	number	Maximum amount of heap memory used by the JVM, in bytes.	
Memory	heap_used	number	Heap memory used by the JVM, in bytes.	
Memory	non_heap_committed	number	Committed amount of non-heap memory used by the JVM, in bytes.	
Memory	non_heap_initial	number	Initial amount of non-heap memory used by the JVM, in bytes.	
Memory	non_heap_max	number	Maximum amount of non-heap memory used by the JVM, in bytes.	
Memory	non_heap_used	number	Non-heap memory used by the JVM, in bytes.	
Memory	objects_pending	number	Number of objects pending in the JVM, in bytes.	

Malware

The fields in the Malware data model describe malware detection and endpoint protection management.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Malware event and search datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
Malware_Attacks	malware
	attack
Malware_Operations	malware
	operations

Fields for the Malware_Attacks event datasets and Malware_Operations search dataset

Malware_Attacks is mainly for searching against and creating alerts for potential malware infections in your environment. Malware_Operations is mainly for monitoring the health and operational status of your anti-virus or anti-malware solution.

The following table lists the extracted and calculated fields for the event dataset and search dataset in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Malware_Attacks	`action`	string	The action taken by the reporting device.	• recommended • required for pytest-splunk-addon • prescribed values: `allowed`, `blocked`, `deferred`
Malware_Attacks	`category`	string	The category of the malware event, such as `keylogger` or `ad-supported program`. **Note:** This is a string value. Use a `category_id` field for category ID fields that are integer data types (`category_id` fields are optional, so they are not included in this table).	• recommended • required for pytest-splunk-addon
Malware_Attacks	`date`	string	The date of the malware event.	recommended
Malware_Attacks	`dest`	string	The system that was affected by the malware event. You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	• recommended • required for pytest-splunk-addon
Malware_Attacks	`dest_bunit`	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Malware_Attacks	`dest_category`	string		
Malware_Attacks	`dest_priority`	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Malware_Attacks	`dest_requires_av`	boolean		
Malware_Attacks	`file_hash`	string	The hash of the file with suspected malware.	
Malware_Attacks	`file_name`	string	The name of the file with suspected malware.	required for pytest-splunk-addon
Malware_Attacks	`file_path`	string	The full file path of the file with suspected malware.	required for pytest-splunk-addon
Malware_Attacks	`severity`	string	The severity of the network protection event. Note: This field is a string. Use severity_id for severity ID fields that are integer data types. Also, specific values are required	• recommended

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			for this field. Use `vendor_severity` for the vendor's own human readable severity strings, such as Good, Bad, and Really Bad.	• prescribed values: `critical`, `high`, `medium`, `low`, `informational`
Malware_Attacks	`severity_id`	string	The numeric or vendor specific severity indicator corresponding to the event severity.	
Malware_Attacks	`signature`	string	The name of the malware infection detected on the client (the `dest`). **Note:** This is a string value. Use a `signature_id` field for signature ID fields that are integer data types.	• recommended • required for pytest-splunk-addon • other: such as `Trojan.Vundo`, `Spyware.Gaobot`, `W32.Nimbda`
Malware_Attacks	`signature_id`	string	The unique identifier or event code of the event signature.	
Malware_Attacks	`src`	string	The source of the event, such as a DAT file relay server. You can **alias** this from more specific fields, such as `src_host`, `src_ip`, or `src_name`.	
Malware_Attacks	`src_bunit`	string	The business unit of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Malware_Attacks	`src_category`	string	The category of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Malware_Attacks	`src_priority`	string	The priority of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Malware_Attacks	`src_user`	string	The reported sender of an email-based attack.	
Malware_Attacks	`tag`	string	This automatically generated field is used to access tags from within datamodels. Do not define extractions for this field when writing add-ons.	
Malware_Attacks	`user`	string	The user involved in the malware event.	recommended
Malware_Attacks	`user_bunit`	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Malware_Attacks	`user_category`	string		
Malware_Attacks	`user_priority`	string		

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Malware_Attacks	`url`	string	A URL containing more information about the vulnerability.	
Malware_Attacks	`vendor_product`	string	The vendor and product name of the endpoint protection system, such as `Symantec AntiVirus`. This field can be automatically populated by `vendor` and `product` fields in your data.	recommended
Malware_Operations	`dest`	string	The system where the malware operations event occurred.	• recommended • required for pytest-splunk-addon
Malware_Operations	`dest_bunit`	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Malware_Operations	`dest_category`	string		
Malware_Operations	`dest_nt_domain`	string	The NT domain of the `dest` system, if applicable.	recommended
Malware_Operations	`dest_priority`	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Malware_Operations	`dest_requires_av`	boolean	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Malware_Operations	`product_version`	string	The product version of the malware operations product.	recommended
Malware_Operations	`signature_version`	string	The version of the malware signature bundle in a signature update operations event.	• recommended • required for pytest-splunk-addon
Malware_Operations	`tag`	string	The tag associated with the malware operations event.	
Malware_Operations	`vendor_product`	string	The vendor product name of the malware operations product.	• recommended • required for pytest-splunk-addon

Network Resolution (DNS)

The fields and tags in the Network Resolution (DNS) data model describe DNS traffic, both server:server and client:server.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with the DNS event dataset

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see the topic How to use these reference tables in this manual.

Dataset name	Tag name

DNS	network			
	resolution			
	dns			

Fields for the Network Resolution event dataset

The following table lists the extracted and calculated fields for the event dataset in the model. The table does not include any inherited fields. For more information, see the topic How to use these reference tables in this manual.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
DNS	additional_answer_count	number	Number of entries in the "additional" section of the DNS message.	required for pytest-splunk-addon
DNS	answer	string	Resolved address for the query.	• recommended • required for pytest-splunk-addon
DNS	answer_count	number	Number of entries in the answer section of the DNS message.	required for pytest-splunk-addon
DNS	authority_answer_count	number	Number of entries in the 'authority' section of the DNS message.	required for pytest-splunk-addon
DNS	dest	string	The destination of the network resolution event. You can **alias** this from more specific fields, such as dest_host, dest_ip, or dest_name.	• recommended • required for pytest-splunk-addon
DNS	dest_bunit	string	The business unit of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DNS	dest_category	string	The category of the network resolution target, such as email_server or SOX-compliant. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
DNS	dest_port	number	The destination port number.	
DNS	dest_priority	string	The priority of the destination, if applicable. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DNS	duration	number	The time taken by the network resolution event, in seconds.	
DNS	message_type	string	Type of DNS message.	• recommended • required for pytest-splunk-addon • prescribed values: `Query`, `Response`
DNS	name	string	The name of the DNS event.	
DNS	query	string	The domain which needs to be resolved. Applies to messages of type "Query".	• recommended • required for pytest-splunk-addon
DNS	query_count	number	Number of entries that appear in the "Questions" section of the DNS query.	required for pytest-splunk-addon
DNS	query_type	string	The field may contain DNS OpCodes or Resource Record Type codes. For details, see the Domain Name System Parameters on the Internet Assigned Numbers Authority (IANA) web site. If a value is not set, the `DNS.record_type` field is referenced.	• required for pytest-splunk-addon • prescribed values: `Query, IQuery, Status, Notify, Update, A, MX, NS, PTR`
DNS	record_type	string	The DNS resource record type. For details, see the List of DNS record types on the Wikipedia web site.	• required for pytest-splunk-addon • prescribed values: `A, DNAME, MX, NS, PTR`
DNS	reply_code	string	The return code for the response. For details, see the Domain Name System Parameters on the Internet Assigned Numbers Authority (IANA) web site.	• recommended • required for pytest-splunk-addon • prescribed values: `No Error, Format Error, Server Failure, Non-Existent Domain` • other: `NoError, FormErr, ServFail, NXDomain, NotImp, Refused, YXDomain, YXRRSet, NotAuth, NotZone, BADVERS, BADSIG, BADKEY, BADTIME,`

93

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				BADMODE, BADNAME, BADALG
DNS	reply_code_id	number	The numerical id of a return code. For details, see the Domain Name System Parameters on the Internet Assigned Numbers Authority (IANA) web site.	• recommended • required for pytest-splunk-addon • prescribed values: 0, NoError, 1, FormErr,2, ServFail, 3, NXDomain,
DNS	response_time	number	The amount of time it took to receive a response in the network resolution event, in seconds if consistent across all data sources, if applicable.	required for pytest-splunk-addon
DNS	src	string	The source of the network resolution event. You can **alias** this from more specific fields, such as src_host, src_ip, or src_name.	required for pytest-splunk-addon
DNS	src_bunit	string	The business unit of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DNS	src_category	string	The category of the source, such as email_server or SOX-compliant. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DNS	src_port	number	The port number of the source.	
DNS	src_priority	string	The priority of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
DNS	tag	string	This automatically generated field is used to access tags from within datamodels. Do not define extractions for this field when writing add-ons.	
DNS	transaction_id	number	The unique numerical transaction id of the network resolution event.	required for pytest-splunk-addon
DNS	transport	string	The transport protocol used by the network resolution event.	required for pytest-splunk-addon
DNS	ttl	number	The time-to-live of the network resolution event.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
DNS	vendor_product	string	The vendor product name of the DNS server. The Splunk platform can derive this field from the fields vendor and product in the raw data, if they exist.	recommended

Network Sessions

The fields in the Network Sessions data model describe Dynamic Host Configuration Protocol (DHCP) and Virtual Private Network (VPN) traffic, whether server:server or client:server, and network infrastructure inventory and topology.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Network Session event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Sessions	network
	session
|____ Session_Start	start
|____ Session_End	end
|____ DHCP	dhcp
|____ VPN	vpn

Fields for Network Sessions event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Sessions	action	string	The action taken by the reporting device.	required for pytest-splunk-addon
All_Sessions	dest_bunit	string	The business unit of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	dest_category	string	The category of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	dest_dns	string	The domain name system address of the destination for a network session event.	recommended
All_Sessions	dest_ip	string	The internal IP address allocated to the client initializing a network session. For DHCP and VPN events, this is the IP address leased to the client.	• recommended • required for pytest-splunk-addon
All_Sessions	dest_mac	string	The internal MAC address of the network session client. For DHCP events, this is the MAC address of the client acquiring an IP address lease. For VPN events, this is the MAC address of the client initializing a network session. **Note:** Always force lower case on this field. **Note:** Always use colons instead of dashes, spaces, or no separator.	• recommended • required for pytest-splunk-addon
All_Sessions	dest_nt_host	string	The NetBIOS name of the client initializing a network session.	recommended
All_Sessions	dest_priority	string	The priority of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	duration	number	The amount of time for the completion of the network session event, in seconds.	
All_Sessions	response_time	number	The amount of time it took to receive a response in the network session event, if applicable.	
All_Sessions	signature	string	An indication of the type of network session event.	required for pytest-splunk-addon
All_Sessions	signature_id	string	The unique identifier or event code of the event signature.	
All_Sessions	src_bunit	string	The business unit of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing	

96

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			add-ons.	
All_Sessions	src_category	string	The category of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	src_dns	string	The external domain name of the client initializing a network session. Not applicable for DHCP events.	
All_Sessions	src_ip	string	The IP address of the client initializing a network session. Not applicable for DHCP events.	
All_Sessions	src_mac	string	The MAC address of the client initializing a network session. Not applicable for DHCP events. **Note:** Always force lower case on this field. **Note:** Always use colons instead of dashes, spaces, or no separator.	
All_Sessions	src_nt_host	string	The NetBIOS name of the client initializing a network session. Not applicable for DHCP events.	
All_Sessions	src_priority	string	The priority of the source. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
All_Sessions	user	string	The user in a network session event, where applicable. For example, a VPN session or an authenticated DHCP event.	• recommended • required for pytest-splunk-addon
All_Sessions	user_bunit	string	The business unit associated with the user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	user_category	string	The category of the user. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	user_priority	string	The priority of the user. This field is automatically provided by asset and identity	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Sessions	`vendor_product`	string	The full name of the DHCP or DNS server involved in this event, including vendor and product name. For example, `Microsoft DHCP` or `ISC BIND`. Create this field by combining the values of the `vendor` and `product` fields, if present in the events.	recommended
DHCP	`lease_duration`	number	The duration of the DHCP lease, in seconds.	
DHCP	`lease_scope`	string	The consecutive range of possible IP addresses that the DHCP server can lease to clients on a subnet. A `lease_scope` typically defines a single physical subnet on your network to which DHCP services are offered.	required for pytest-splunk-addon

Network Traffic

The fields and tags in the Network Traffic data model describe flows of data across network infrastructure components.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Network Traffic event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Traffic	network
	communicate

Fields for Network Traffic event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

For even more examples, see NetworkTrafficFieldMapping.

Dataset name	Field name		Description	

		Data type		Abbreviated list of example values
All_Traffic	action	string	The action taken by the network device.	• recommended • required for pytest-splunk-addon • prescribed values: `allowed` `blocked`, `teardown`
All_Traffic	app	string	The application protocol of the traffic.	required for pytest-splunk-addon
All_Traffic	bytes	number	Total count of bytes handled by this device/interface (`bytes_in + bytes_out`).	recommended
All_Traffic	bytes_in	number	How many bytes this device/interface received.	recommended
All_Traffic	bytes_out	number	How many bytes this device/interface transmitted.	recommended
All_Traffic	channel	number	The 802.11 channel used by a wireless network.	
All_Traffic	dest	string	The destination of the network traffic (the remote host). You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	• recommended • required for pytest-splunk-addon
All_Traffic	dest_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Traffic	dest_category	string		
All_Traffic	dest_interface	string	The interface that is listening remotely or receiving packets locally. Can also be referred to as the "egress interface."	
All_Traffic	dest_ip	string	The IP address of the destination.	
All_Traffic	dest_mac	string	The destination TCP/IP layer 2 Media Access Control (MAC) address of a packet's destination, such as `06:10:9f:eb:8f:14`. **Note:** Always force lower case on this field. **Note:** Always use colons instead of dashes, spaces, or no separator.	
All_Traffic	dest_port	number	The destination port of the network traffic. **Note:** Do not translate the values of this field to strings (`tcp/80` is `80`, not `http`). You can set up the corresponding string value in a `dest_svc` field by extending the data model.	recommended
All_Traffic	dest_priority	string	The destination priority, if applicable. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Traffic	dest_translated_ip	string	The NATed IPv4 or IPv6 address to which a packet has been sent.	
All_Traffic	dest_translated_port	number		

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Traffic	packets_in	number	The total count of packets received by this device/interface.	
All_Traffic	packets_out	number	The total count of packets transmitted by this device/interface.	
All_Traffic	process_id	string	The numeric identifier of the process (PID) or service generating the network traffic.	
All_Traffic	protocol	string	The OSI layer 3 (network) protocol of the traffic observed, in lower case. For example, ip, appletalk, ipx.	
All_Traffic	protocol_version	string	Version of the OSI layer 3 protocol.	
All_Traffic	response_time	number	The amount of time it took to receive a response in the network event, if applicable.	
All_Traffic	rule	string	The rule that defines the action that was taken in the network event. **Note:** This is a string value. Use a rule_id field for rule fields that are integer data types. The rule_id field is optional, so it is not included in this table.	recommended
All_Traffic	session_id	string	The session identifier. Multiple transactions build a session.	
All_Traffic	src	string	The source of the network traffic (the client requesting the connection). You can **alias** this from more specific fields, such as src_host, src_ip, or src_name.	• recommended • required for pytest-splunk-addon
All_Traffic	src_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Traffic	src_category	string		
All_Traffic	src_interface	string	The interface that is listening locally or sending packets remotely. Can also be referred to as the "ingress interface."	
All_Traffic	src_ip	string	The ip address of the source.	
All_Traffic	src_mac	string	The source TCP/IP layer 2 Media Access Control (MAC) address of a packet's destination, such as 06:10:9f:eb:8f:14. **Note:** Always force lower case on this field. **Note:** Always use colons instead of dashes, spaces, or no separator.	
All_Traffic	src_port	number	The source port of the network traffic. **Note:** Do not translate the values of this field to strings (tcp/80 is 80, not http). You can set up the corresponding string value in the src_svc field.	recommended
All_Traffic	src_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Traffic	src_translated_ip	string	The NATed IPv4 or IPv6 address from which a packet has been sent..	required for pytest-splunk-addon
All_Traffic	src_translated_port	number	The NATed port from which a packet has been sent. **Note:** Do not translate the values of this field to strings (tcp/80 is 80, not http).	
All_Traffic	src_zone	string	The network zone of the source.	required for pytest-splunk-addon
All_Traffic	ssid	string	The 802.11 service set identifier (ssid) assigned to a wireless session.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Performance	performance			
	cpu OR facilities OR memory OR storage OR network OR (os, (uptime OR (time, synchronize)))			
|____CPU	cpu			
|____Facilities	facilities			
|____Memory	memory			
|____Storage	storage			
|____Network	network			
|____OS	os			
|____Uptime	uptime			
|____Timesync	time			
	synchronize			

Fields for Performance event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Object name	Field name	Data type	Description	Abbreviated list of example values
All_Performance	dest	string	The system where the event occurred, usually a facilities resource such as a rack or room. You can **alias** this from more specific fields in your event data, such as `dest_host`, `dest_ip`, or `dest_name`.	recommended
All_Performance	dest_bunit	string	The business unit of the system where the event occurred. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Performance	dest_category	string	The category of the system where the event occurred. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Performance	dest_priority	string	The priority of the system where the performance event occurred.	

101

Object name	Field name	Data type	Description	Abbreviated list of example values
All_Performance	dest_should_timesync	boolean	Indicates whether or not the system where the performance event occurred should time sync. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Performance	dest_should_update	boolean	Indicates whether or not the system where the performance event occurred should update. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Performance	hypervisor_id	string	The ID of the virtualization hypervisor.	
All_Performance	resource_type	string	The type of facilities resource involved in the performance event, such as a rack, room, or system.	
All_Performance	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
CPU	cpu_load_mhz	number	The amount of CPU load reported by the controller in megahertz.	
CPU	cpu_load_percent	number	The amount of CPU load reported by the controller in percentage points.	recommended
CPU	cpu_time	number	The number of CPU seconds consumed by processes.	
CPU	cpu_user_percent	number	Percentage of CPU user time consumed by processes.	
Facilities	fan_speed	number	The speed of the cooling fan in the facilities resource, in rotations per second.	
Facilities	power	number	Amount of power consumed by the facilities resource, in kW/h.	
Facilities	temperature	number	Average temperature of the facilities resource, in °C.	recommended
Memory	mem	number	The total amount of memory capacity reported by the resource, in megabytes.	recommended
Memory	mem_committed	number	The committed amount of memory reported by the resource, in megabytes.	
Memory	mem_free	number	The free amount of memory reported by the resource, in megabytes.	recommended
Memory	mem_used	number	The used amount of memory reported by the resource, in megabytes.	recommended
Memory	swap	number	The total swap space size, in megabytes, if applicable.	
Memory	swap_free	number	The free swap space size, in megabytes, if applicable.	
Memory	swap_used	number	The used swap space size, in megabytes, if applicable.	
Storage	array	number	The array that the resource is a member of, if applicable.	

Object name	Field name	Data type	Description	Abbreviated list of example values
Storage	`blocksize`	number	Block size used by the storage resource, in kilobytes.	
Storage	`cluster`	string	The cluster that the resource is a member of, if applicable.	
Storage	`fd_max`	number	The maximum number of available file descriptors.	
Storage	`fd_used`	number	The current number of open file descriptors.	
Storage	`latency`	number	The latency reported by the resource, in milliseconds.	
Storage	`mount`	string	The mount point of a storage resource.	
Storage	`parent`	string	A generic indicator of hierarchy. For instance, a disk event might include the array ID here.	
Storage	`read_blocks`	number	Number of blocks read.	
Storage	`read_latency`	number	The latency of read operations, in milliseconds.	
Storage	`read_ops`	number	Number of read operations.	
Storage	`storage`	number	The total amount of storage capacity reported by the resource, in megabytes.	
Storage	`storage_free`	number	The free amount of storage capacity reported by the resource, in megabytes.	recommended
Storage	`storage_free_percent`	number	The percentage of storage capacity reported by the resource that is free.	recommended
Storage	`storage_used`	number	The used amount of storage capacity reported by the resource, in megabytes.	recommended
Storage	`storage_used_percent`	number	The percentage of storage capacity reported by the resource that is used.	recommended
Storage	`write_blocks`	number	The number of blocks written by the resource.	
Storage	`write_latency`	number	The latency of write operations, in milliseconds.	
Storage	`write_ops`	number	The total number of write operations processed by the resource.	
Network	`thruput`	number	The current throughput reported by the service, in bytes.	recommended
Network	`thruput_max`	number	The maximum possible throughput reported by the service, in bytes.	
OS	`signature`	string	The event description signature, if available.	recommended
OS	`signature_id`	string	The unique identifier or event code of the event signature.	
Timesync	`action`	string	The result of a time sync event.	• recommended • prescribed values: `success`, `failure`
Uptime	`uptime`	number	The uptime of the compute resource, in seconds.	recommended

103

Splunk Audit Logs

The fields in the Splunk Audit Logs data model describe audit information for systems producing event logs.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with the Audit event datasets

The following tags act as constraints to identify your events as being relevant to the Modular_Actions dataset in this data model. For more information, see How to use these reference tables.

Although it is not part of the data model shipped in the CIM add-on, the common information model expects the tag `modaction_result` for events produced by custom alert actions.

Dataset name	Tag name
Modular_Actions	modaction
|____ Modular Action Invocations	invocation

Fields for the event dataset and the search datasets

The following table lists the extracted and calculated fields for the event dataset and search datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
View_Activity	app	string	The app name which contains the view.	
View_Activity	spent	number	The amount of time spent loading the view (in milliseconds).	
View_Activity	uri	string	The uniform resource identifier of the view activity.	
View_Activity	user	string	The username of the user who accessed the view.	
View_Activity	view	string	The name of the view.	
Datamodel_Acceleration	access_count	number	The number of times the data model summary has been accessed since it was created.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Datamodel_Acceleration	access_time	time	The timestamp of the most recent access of the data model summary.	
Datamodel_Acceleration	app	string	The application context in which the data model summary was accessed.	
Datamodel_Acceleration	buckets	number	The number of index buckets spanned by the data model acceleration summary.	
Datamodel_Acceleration	buckets_size	number	The total size of the bucket(s) spanned by the data model acceleration summary.	
Datamodel_Acceleration	complete	number	The percentage of the data model summary that is currently complete.	other: `0-100`
Datamodel_Acceleration	cron	string	The cron expression used to accelerate the data model.	
Datamodel_Acceleration	datamodel	string	The name of the data model accelerated.	
Datamodel_Acceleration	digest	string	A hash of the current data model constraints.	
Datamodel_Acceleration	earliest	time	The earliest time that the data model summary was accessed.	
Datamodel_Acceleration	is_inprogress	boolean	Indicates whether the data model acceleration is currently in progress.	prescribed values: `true, false, 1, 0`
Datamodel_Acceleration	last_error	string	The text of the last error reported during the data model acceleration.	
Datamodel_Acceleration	last_sid	string	The search id of the last acceleration attempt.	
Datamodel_Acceleration	latest	time	The most recent acceleration timestamp of the data model.	
Datamodel_Acceleration	mod_time	time	The timestamp of the most recent modification to the data model acceleration.	
Datamodel_Acceleration	retention	number	The length of time that data model accelerations are retained, in seconds.	
Datamodel_Acceleration	size	number	The amount of storage space the data model's acceleration summary takes up, in bytes.	
Datamodel_Acceleration	summary_id	string	The unique id of the data model acceleration summary.	
Search_Activity	host	string	The host on which the search occurred.	
Search_Activity	info	string	The action of the search (granted, completed, cancelled, failed).	
Search_Activity	search	string	The search string.	
Search_Activity	search_et	string	The earliest time of the search.	
Search_Activity	search_lt	string	The latest time of the search.	
Search_Activity	search_type	string	The type of search.	
Search_Activity	source	string	The source associated with the search.	
Search_Activity	sourcetype	string	The source types included in the search.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Search_Activity	user	string	The name of the user who ran the search.	
Search_Activity	user_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Search_Activity	user_category	string		
Search_Activity	user_priority	string		
Scheduler_Activity	app	string	The app context in which the scheduled search was run.	
Scheduler_Activity	host	string	The host on which the scheduled search was run.	
Scheduler_Activity	savedsearch_name	string	The name of the saved search.	
Scheduler_Activity	sid	string	The search id.	
Scheduler_Activity	source	string	The source associated with the scheduled search.	
Scheduler_Activity	sourcetype	string	The source type associated with the scheduled search.	
Scheduler_Activity	splunk_server	string	The Splunk Server on which the scheduled search runs.	
Scheduler_Activity	status	string	The status of the scheduled search.	
Scheduler_Activity	user	string	The user who scheduled the search.	
Web_Service_Errors	host	string	The host on which the web service error occurred.	
Web_Service_Errors	source	string	The source where the web service error occurred.	
Web_Service_Errors	sourcetype	string	The source type associated with the web service error.	
Web_Service_Errors	event_id	string	The unique event_id for the web service error event.	
Modular_Actions	action_mode	string	Specifies whether the action was executed as an ad hoc action or from a saved search, based on whether a search_name exists.	prescribed values: saved, adhoc
Modular_Actions	action_status	string	The status of the action. For example, "success", "failure", or "pending".	
Modular_Actions	app	string	The app ID of the app or add-on that owns the action.	
Modular_Actions	duration	number	How long the action took to complete, in milliseconds.	
Modular_Actions	component	string	The component of the modular action script involved in the event. Often used in conjunction with duration.	
Modular_Actions	orig_rid	string	The rid value of a source action result, automatically added to an event if it is the product of a previously executed action.	
Modular_Actions	orig_sid	string	The original sid value of a source action, automatically added to an event if it is the product of a previously executed action.	
Modular_Actions	rid	string	The id associated with the result of a specific sid. By default, this is the row number of the search, starting with 0.	
Modular_Actions	search_name	string		

106

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			The name of the correlation search that triggered the action. Blank for ad hoc actions.	
Modular_Actions	action_name	string	The name of the action.	
Modular_Actions	signature	string	The logging string associated with alert action introspection events.	
Modular_Actions	sid	string	The search id, automatically assigned by splunkd.	
Modular_Actions	user	string	The user who triggered an ad hoc alert. Not relevant for actions triggered by searches.	

Ticket Management

The fields and tags in the Ticket Management data model describe service requests and their states in ITIL-influenced service desks, bug trackers, simple ticket systems, or GRC systems. They can help you establish a domain's data requirements so you can create apps that support each other.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with Ticket Management event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Ticket_Management	ticketing
|____Change	change
|____Incident	incident
|____Problem	problem

Fields for Ticket Management event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Ticket_Management	affect_dest	string	Destinations affected by the service request.	
All_Ticket_Management	comments	string	Comments about the service request.	
All_Ticket_Management	description	string	The description of the service request.	
All_Ticket_Management	dest	string	The destination of the service request. You can **alias** this from more specific fields, such as dest_host, dest_ip, or dest_name.	
All_Ticket_Management	dest_bunit	string	The business unit associated with the destination user or entity of the triggering events, if applicable. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Ticket_Management	dest_category	string	The category of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Ticket_Management	dest_priority	string	The priority of the destination. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Ticket_Management	priority	string	The relative priority of the service request.	
All_Ticket_Management	severity	string	The relative severity of the service request.	
All_Ticket_Management	severity_id	string	The numeric or vendor specific severity indicator corresponding to the event severity.	
All_Ticket_Management	splunk_id	string	The unique identifier of the service request as it pertains to Splunk. For example, 14DA67E8-6084-4FA8-9568-48D05969C522@@_internal@@0533eff241db0d892509be46cd3126e30e0f6046.	
All_Ticket_Management	splunk_realm	string	The Splunk application or use case associated with the unique identifier (splunk_id). For example, es_notable.	
All_Ticket_Management	src_user	string	The user or entity creating or triggering the ticket, if applicable.	
All_Ticket_Management	src_user_bunit	string	The business unit associated with the source user or entity within the triggering events, if applicable. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Ticket_Management	src_user_category	string	The category associated with the user or entity that triggered the service request. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Ticket_Management	src_user_priority	string	The priority associated with the user or entity that triggered the service request. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Ticket_Management	status	string	The relative status of the service request.	
All_Ticket_Management	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
All_Ticket_Management	ticket_id	string	An identification name, code, or number for the service request.	
All_Ticket_Management	time_submitted	time	The time that the src_user submitted the service request.	
All_Ticket_Management	user	string	The name of the user or entity that is assigned to the ticket, if applicable.	
All_Ticket_Management	user_bunit	string	The business unit associated with the user or entity that is carrying out the service request, if applicable. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Ticket_Management	user_category	string	The category associated with the user or entity that is assigned to carry out the service request, if applicable. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Ticket_Management	user_priority	string	The priority of the user or entity that is assigned to carry out the service request, if applicable. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
Change	change	string	Designation for a request for change (RFC) that is raised to modify an IT service to resolve an incident or problem.	
Incident	incident	string	The incident that triggered the service request. Can be a rare occurrence, or something that happens more frequently. An incident that occurs on a frequent basis can also be classified as a problem.	
Problem	problem	string	When multiple occurrences of related incidents are observed, they are collectively designated with a single problem value. Problem management differs from the process of managing an isolated incident. Often problems are managed by a specific set of staff and through a problem management process.	

Updates

The fields in the Updates data model describe patch management events from individual systems or central management tools.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with the Updates event and search datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
Updates	update
	status
Update_Errors	update
	error

Fields for the Updates event datasets and Update_Errors search dataset

The following table lists the extracted and calculated fields for the event datasets and search dataset in the model. The table does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Updates	`dest`	string	The system that is affected by the patch change. You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	• recommended • required for pytest-splunk-addon
Updates	`dest_bunit`	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Updates	`dest_category`	string		
Updates	`dest_priority`	string		
Updates	`dest_should_update`	boolean		
Updates	`dvc`	string	The device that detected the patch event, such as a patching or configuration management server. You can **alias** this from more specific fields, such as	required for pytest-splunk-addon

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			dvc_host, dvc_ip, or dvc_name.	
Updates	file_hash	string	The checksum of the patch package that was installed or attempted.	
Updates	file_name	string	The name of the patch package that was installed or attempted.	required for pytest-splunk-addon
Updates	severity	string	The severity associated with the patch event.	prescribed values: critical, high, medium, low, informational
Updates	severity_id	string	The numeric or vendor specific severity indicator corresponding to the event severity.	
Updates	signature	string	The name of the patch requirement detected on the client (the dest), such as MS08-067 or RHBA-2013:0739. **Note:** This is a string value. Use signature_id for numeric indicators.	• recommended • required for pytest-splunk-addon
Updates	signature_id	int	The ID of the patch requirement detected on the client (the src). **Note:** Use signature for human-readable signature names.	• recommended • required for pytest-splunk-addon
Updates	status	string	Indicates the status of a given patch requirement.	• recommended • required for pytest-splunk-addon • prescribed values: available, installed, invalid, "restart required"
Updates	tag	string	This automatically generated field is used to access tags from within datamodels. Do not define extractions for this field when writing add-ons.	
Updates	vendor_product	string	The vendor and product of the patch monitoring product, such as Lumension Patch Manager. This field can be automatically populated by vendor and product fields in your data.	recommended

Vulnerabilities

The fields in the Vulnerabilities data model describe vulnerability detection data.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with the Vulnerabilities event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
Vulnerabilities	report
	vulnerability

Fields for Vulnerabilities event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Vulnerabilities	bugtraq	string	Corresponds to an identifier in the vulnerability database provided by the Security Focus website (searchable at http://www.securityfocus.com/).	
Vulnerabilities	category	string	The category of the discovered vulnerability, such as `DoS`. **Note:** This field is a string. Use `category_id` for numeric values. The `category_id` field is optional and thus is not included in the data model.	• recommended • required for pytest-splunk-addon
Vulnerabilities	cert	string	Corresponds to an identifier in the vulnerability database provided by the US Computer Emergency Readiness Team (US-CERT, searchable at http://www.kb.cert.org/vuls/).	
Vulnerabilities	cve	string	Corresponds to an identifier provided in the Common Vulnerabilities and Exposures index (searchable at http://cve.mitre.org).	• recommended • required for pytest-splunk-addon
Vulnerabilities	cvss	number	Numeric indicator of the common vulnerability scoring system.	required for pytest-splunk-addon
Vulnerabilities	dest	string	The host with the discovered vulnerability. You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	• recommended • required for pytest-splunk-addon
Vulnerabilities	dest_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Vulnerabilities	dest_category	string		
Vulnerabilities	dest_priority	string		
Vulnerabilities	dvc	string	The system that discovered the vulnerability. You can **alias** this from more specific fields, such as `dvc_host`, `dvc_ip`, or `dvc_name`.	• recommended • required for pytest-splunk-addon

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Vulnerabilities	dvc_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Vulnerabilities	dvc_category	string		
Vulnerabilities	dvc_priority	string		
Vulnerabilities	msft	string	Corresponds to a Microsoft Security Advisory number (http://technet.microsoft.com/en-us/security/advisory/).	
Vulnerabilities	mskb	string	Corresponds to a Microsoft Knowledge Base article number (http://support.microsoft.com/kb/).	
Vulnerabilities	severity	string	The severity of the vulnerability detection event. Specific values are required. Use `vendor_severity` for the vendor's own human readable strings (such as `Good`, `Bad`, and `Really Bad`). **Note:** This field is a string. Use `severity_id` for numeric data types.	• recommended • required for pytest-splunk-addon • prescribed values: `critical`, `high`, `medium`, `informational`, `low`
Vulnerabilities	severity_id	string	The numeric or vendor specific severity indicator corresponding to the event severity.	
Vulnerabilities	signature	string	The name of the vulnerability detected on the host, such as `HPSBMU02785 SSRT100526 rev.2 – HP LoadRunner Running on Windows, Remote Execution of Arbitrary Code, Denial of Service (DoS)`. **Note:** This field has a string value. Use `signature_id` for numeric indicators.	• recommended • required for pytest-splunk-addon
Vulnerabilities	signature_id	string	The unique identifier or event code of the event signature.	
Vulnerabilities	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
Vulnerabilities	url	string	The URL involved in the discovered vulnerability.	
Vulnerabilities	user	string	The user involved in the discovered vulnerability.	
Vulnerabilities	user_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
Vulnerabilities	user_category	string		
Vulnerabilities	user_priority	string		
Vulnerabilities	vendor_product	string	The vendor and product that detected the vulnerability. This field can be automatically populated by `vendor` and `product` fields in your data.	recommended
Vulnerabilities	xref	string	A cross-reference identifier associated with the vulnerability. In most cases, the `xref` field contains both the short name of the database being cross-referenced and the unique identifier used in the external database.	

Web

The fields in the Web data model describe web server and/or proxy server data in a security or operational context.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Tags used with the Web event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
Web	web
|____ Proxy	proxy
|____ Storage	storage

Fields for Web event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Web	action	string	The action taken by the server or proxy.	• recommended • required for pytest-splunk-addon
Web	app	string	The application detected or hosted by the server/site such as WordPress, Splunk, or Facebook.	
Web	bytes	number	The total number of bytes	• recommended

Dataset name	Field name	Data type	Description	Abbreviated list of example values
			transferred (`bytes_in` + `bytes_out`).	• required for pytest-splunk-addon
Web	`bytes_in`	number	The number of inbound bytes transferred.	• recommended • required for pytest-splunk-addon
Web	`bytes_out`	number	The number of outbound bytes transferred.	• recommended • required for pytest-splunk-addon
Web	`cached`	boolean	Indicates whether the event data is cached or not.	prescribed values: `true`, `false`, `1`, `0`
Web	`category`	string	The category of traffic, such as may be provided by a proxy server.	required for pytest-splunk-addon
Web	`cookie`	string	The cookie file recorded in the event.	
Web	`dest`	string	The destination of the network traffic (the remote host). You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	• recommended • required for pytest-splunk-addon
Web	`dest_bunit`	string	These fields are automatically provided by asset and identity correlation featu applications like Splunk Enterprise Security. Do not define extractions for thes fields when writing add-ons.	
Web	`dest_category`	string		
Web	`dest_priority`	string		
Web	`dest_port`	number	The destination port of the web traffic.	required for pytest-splunk-addon
Web	`duration`	number	The time taken by the proxy event, in milliseconds.	
Web	`http_content_type`	string	The content-type of the requested HTTP resource.	recommended
Web	`http_method`	string	The HTTP method used in the request.	• recommended • prescribed values: `GET`, `PUT`,`POST`, `DELETE`, `HEAD`, `OPTIONS`, `CONNECT`, `TRACE`

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Web	http_referrer	string	The HTTP referrer used in the request. The W3C specification and many implementations misspell this as http_referer. Use a FIELDALIAS to handle both key names.	recommended
Web	http_referrer_domain	string	The domain name contained within the HTTP referrer used in the request.	recommended
Web	http_user_agent	string	The user agent used in the request.	• recommended • required for pytest-splunk-addon
Web	http_user_agent_length	number	The length of the user agent used in the request.	required for pytest-splunk-addon
Web	response_time	number	The amount of time it took to receive a response, if applicable, in milliseconds.	
Web	site	string	The virtual site which services the request, if applicable.	
Web	src	string	The source of the network traffic (the client requesting the connection).	• recommended • required for pytest-splunk-addon
Web	src_bunit	string	These fields are automatically provided by asset and identity correlation featu applications like Splunk Enterprise Security. Do not define extractions for thes fields when writing add-ons.	
Web	src_category	string		
Web	src_priority	string		
Web	status	string	The HTTP response code indicating the status of the proxy request.	• recommended • required for pytest-splunk-addon • prescribed values: 100, 101, 102, 200, 201, 202, 203, 204, 205, 206, 207, 208, 300, 301, 302, 303, 304, 305, 306, 307, 308, 400, 401, 402, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 417, 422, 423, 424, 426, 428, 429, 431, 500, 501, 502, 503,

116

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				505, 506, 507, 508, 510, 511
Web	`tag`	string	This automatically generated field is used to access tags from within datamodels. Do not define extractions for this field when writing add-ons.	

Web	`uri_path`	string	The path of the resource served by the webserver or proxy.	other:
				`/CertEnroll/Blue%20Coat%20Systems`
				`%20Internal.crl`
				
				/CertEnroll/PWSVL-NETSVC-01.internal.cacheflow.com _Blue%20Coat%20Systems %20Internal.crt /MFAwTqADAgEAMEcwRTBDMAkGBSsOAw... laBQAEFOoaVMtyzC9gObESY9g1eXf1VM8VBBTl1mBq2WF... 4cYqBl6c08kr4S302gIKUCIZd gAAAAAnQA%3D%3D /bag /en-US/account/login /en-US/account/login /en-US/app/simple_xml_examples/custom_viz _ forcedirected /en-US/config /en-US/splunkd/__raw/services/apps/local/simple _xml_examples /en-US/splunkd/_ _raw/services/configs/conf-web/settings /en-US/splunkd/__raw/services/data/user-prefs/general /en-US/splunkd/__raw /services/messages /en-US/splunkd/__raw/services/messages /en-US/splunkd/__raw/services/messages /en-US/splunkd/_ _raw/services/messages /en-US/splunkd/__raw/services/saved/searches/_new /en-US/splunkd/__raw/services/server/info /server-info /en-US/splunkd/__raw/servicesNS/-/-/search/jobs

Web	`uri_query`	string	The path of the resource requested by the client.	other:
				`?return_to=%2Fen-US%2Fapp%2Fsimple_xml_examples%2Fcust...`
				`_`
				`forcedirected%3Fearliest%3D0%26latest%3D`
				
				?earliest=0&latest= ?autoload=1 ?output_mode=json& _=1424960631223 ?output_mode=json&_=1424960631232 ?output_mode=json&_=1424960631225 ?output _mode=json&sort_key=timeCreated_ epochSecs&sort_dir=desc&_=1424960631236 ?output_mode=json&sort _key=timeCreated_ epochSecs&sort_dir=desc&count= 1000&_=1424933765618 ?output_mode=json&sort _key=timeCreated_ epochSecs&sort_dir=desc&count= 1000&_=1424933765619 ?output_mode=json&sort

117

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				key=timeCreated epochSecs&sort_dir=desc&count= 1000&_=1424960631233 ?output_mode=json& _=14249606 ?output_mode=json&_=1424960631224 ?id=admin__admin_c2ltcGxlX3htbF9leGFtcGxlcw__ search1 _1424960633.67&count=1& output_mode=json&_=1424960631243
Web	url	string	The URL of the requested HTTP resource.	• recommended • required for pytest-splunk-addon • other: http://0.channel36.facebook.com/x/1746719903/ false/p_1243021868=11 http://0.channel36.facebook.com/x /3833188787/ false/p_1243021868=11 http://0.channel37.facebook.com/x/3598566724/ false/p_576766886=1 http:/ /01275269302.channel11.facebook.com/x/ 832619022/false/p_792194432=2 http://03978257738.channel38.facebook.com/x / 3905575759/false/p_1576492095=0 http://1.gravatar.com/avatar /72f230f80 db7d667952d596cafbaf928?s=16&d=identicon&r=PG http://10.0.26.105:8080/secars /secars.dll?h=33 EC64FCE11F15337B7BE75CF1EF7443FFA8 E58454580830E8D41D695469C01E8D128BF891F4D 0438A70BE3E 0A0D7BABD610DE3A588DF1804F823 CD509F0A2177AD97F7B9F3D09BEDA005C241B873 349D525C0264A9F1655FD408F70DD465574D5E8 E BE0DC29030A6365C1F025CB2954E2C38E0404CE4 D24970B2613EB394E2611FD7EC8EB2AD84318421CD 40DF01E6DF002AFF77565303 0012EF432D59072C0 5F1A939A6C1467CC3A129801587BE559CB16653513 3EAA6C78D3C4BDEC6D795C2934A176DACBB3839 8ED4903 037DDB59101EE725138FF8534D89657F4 43F084ACE66DF159581AEF495F317536C34477D005 49B514A81CC689BFB7ACA7C10399C2C7B D76319876 C9890FB4172BBC7CBDF50F7CE0B164BE7F8D8228E9 555E39EE9D0F50B6CE3F610533544A959087F03FCD 16D8FDF0F9C5EB 692E3C7EE61B75272961CC29A05D 5F3A1629BBF7C70044BBC65D30812B8EB3E0C7510C DA0F636808B32925481602F702714C60ADC704 0F58 CACA4BDD61D776C796D5344495B93AC08F16FC851E 3FB157CEBB563CC1 http://10.10.8.60/ http://10.120.109.82/en-US /static/@255606:0/app/simple_ xml_examples/components/forcedirected/ forcedirected.js?_=1424960631242 http:/ /10.120.251.250/en-US/account/login
Web	url_domain	string	The domain name contained within the URL of the requested HTTP resource.	recommended

Dataset name	Field name	Data type	Description	Abbreviated list of example values
Web	url_length	number	The length of the URL.	
Web	user	string	The user that requested the HTTP resource.	recommended
Web	user_bunit	string	These fields are automatically provided by asset and identity correlation featu... applications like Splunk Enterprise Security. Do not define extractions for thes... fields when writing add-ons.	
Web	user_category	string		
Web	user_priority	string		
Web	vendor_product	string	The vendor and product of the proxy server, such as Squid Proxy Server. This field can be automatically populated by vendor and product fields in your data.	recommended
Storage	error_code	string	The error code that occurred while accessing the storage account.	other: NoSuchBucket
Storage	operation	string	The operation performed on the storage account.	other: REST.PUT.OBJECT
Storage	storage_name	string	The name of the bucket or storage account.	other: es-csm-files

Using the Common Information Model

Approaches to using the CIM

This chapter provides a comprehensive overview of how Splunk platform app and add-on developers, knowledge managers, or administrators can use the Common Information Model to work with data at search time.

Not all sections apply for all users and use cases.

If you want to normalize some newly indexed data from a source type that is unfamiliar to the Splunk platform, see Use the CIM to normalize data at search time.

If you want to validate that your indexed data conforms to the CIM for all the models that you expect, see Use the CIM to validate your data.

If you are using Pivot to work with data that has already been normalized to the CIM, see Use the CIM to generate reports and dashboards.

If you want to create a new custom alert action or adaptive response action that conforms to the common action model, see Use the common action model to build a custom alert action.

Use the CIM to normalize data at search time

If you are working with a new data source, you can manipulate your already-indexed data at search time so that it conforms to the common standard used by other Splunk applications and their dashboards. Your goal might be to create a new application or add-on specific to this data source for use with Splunk Enterprise Security or other existing applications, or you might just want to normalize the data for your own dashboards.

This topic guides you through the steps to normalize your data to the Common Information Model, following established best practices.
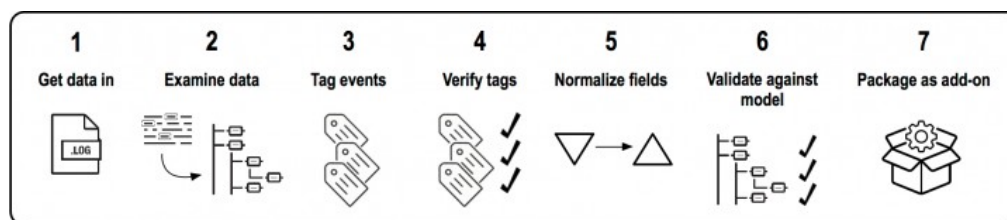
To see these steps applied in a real use case, see Use the CIM to normalize CPU performance metrics.

Before you start, keep in mind that someone else may have already built an add-on to normalize the data you have in mind. Check Splunkbase for CIM-compatible apps and add-ons that match your requirements.

1. Get your data in

If you have not already done so, get your data in to the Splunk platform.

Do not be concerned about making your data conform to the CIM in the parsing or indexing phase. You normalize your data to be CIM compliant at search time. See Getting Data In if you need more direction for capturing and indexing your data.

2. Examine your data in the context of the CIM

Determine which data models are relevant for the data source you are working with.

Use the CIM reference tables to find fields that are relevant to your domain and your data. You might need to normalize data from a single event or source of events against more than one data model. Some events may be logs tracking create, read, update, delete (CRUD) changes to a system, others may log the login/logout activities for that system. For each different kind of event, look for data models that match the context of your data. For example, CRUD events map to the Change data model. Login events map to the Authentication data model.

You might see the `app` field in the Authentication, Network Traffic, or Web data models. Consider the source and purpose of the events. If the primary purpose is login activities, then Authentication is the data model to match against, even though the `app` field exists in multiple data models. Do not force-fit based solely on field name.

Refer to How to use these reference tables for a description of how to compare the information in the reference tables with the data models in the Data Model Editor page in Splunk Web. Keep both the documentation and the Data Model Editor open for reference, because you need to refer to them in the following steps.

3. Configure CIM-compliant event tags

Apply tags to categorize your event data according to type.

Categorizing your data allows you to specify the dashboards in which the data should appear, something that cannot necessarily be determined just by field names and sources. Many of the CIM data models have the same field names, so the tags act as constraints to filter the data to just the relevant events for that model. Also, many different sources may produce events relevant to a particular data model. For example, web applications, VPN servers, and email servers all have authentication events, yet the source and structure of these authentication events are considerably different for each type of device. Tagging all of the authentication related events appropriately makes it possible for your dashboards to pull data from the correct events automatically.

To apply the CIM-compliant tags to your data, follow these steps.

1. Determine which tags are necessary for your data. Refer to the data models that use similar domain data to choose the tags from the Common Information Model that are needed. Remember to look for inherited tags from parent datasets. See How to use these reference tables for more information.
2. Create the appropriate event types in Splunk Web by selecting **Settings > Event types**.
3. Click **New** and create a new event type.
4. Add or edit tags for the event type. Separate tags with spaces or commas.
5. Click **Save** to save the new event type and tags.

If an event type already exists, add tags to the event type.

1. In Splunk Web, click **Settings > Event types**.
2. Locate the event type that you want to tag and click its name.
3. On the detail page for the event type, add or edit tags in the **Tags** field. Separate tags with spaces or commas.
4. Click **Save**.

Repeat this process for each of the tags needed to map your events to the correct datasets in the data models.

If you have access to the file system, you can add an event type by editing the local version of the `eventtypes.conf` file directly. You can also add tags for an event type using the file system. Edit the local version of the `tags.conf` file. For example:

[eventtype=nessus]
vulnerability = enabled
report = enabled
The event type and tag modifications that you make are saved in
`$SPLUNK_HOME/etc/users/$USERNAME$/$APPNAME$/local/eventtypes.conf` and
`$SPLUNK_HOME/etc/users/$USERNAME$/$APPNAME$/local/tags.conf`.

For more information about event typing, see the Data Classification: Event types and transactions section in the Splunk Enterprise *Knowledge Manager Manual*. For more information about managing tags in Splunk Web, see Data normalization: tags and aliases in the Splunk Enterprise *Knowledge Manager Manual*.

4. Verify tags

To verify that the data is tagged correctly, display the event type tags and review the events.

1. Search for the source type.
2. Use the field picker to display the field `tag::eventtype` at the bottom of each event.
3. Look at your events to verify that they are tagged correctly.
4. If you created more than one event type, also check that each event type is finding the events you intended.

5. Make your fields CIM-compliant

Examine the fields available in the data model, and look for the equivalent fields in your indexed data. Some of the fields might already be present with the correct field names and value types that match the expectations of the Common Information Model. If you are not certain that your values match what is expected by the model, check the description of that field in the data model reference tables in this documentation.

Fields from different sources can use different names for similar events. You can map the names to CIM-compliant fields. For example, the following diagram shows login events from two different sources as mapped to CIM-compliant fields.

a. Use the following search results to help prioritize field mapping

Use the following search results to help prioritize which fields to map when normalizing. The "recommended=true" fields are both commonly available in data sources of the intended type, and highly useful for security monitoring and investigations. Make a concerted effort to map appropriate fields from your source to these "recommended=true" data model fields. Without tagging for the recommended fields, an event may not be as useful.

```
| rest splunk_server=local count=0 /services/data/models | rename title as model,eai:data as data | spath
input=data output=objects path=objects{} | mvexpand objects | spath input=objects output=object_name
path=objectName | spath input=objects output=fields path=fields{} | appendpipe [| spath input=objects
output=fields path=calculations{}.outputFields{}] | mvexpand fields | spath input=fields output=field_name
path=fieldName | spath input=fields output=recommended path=comment.recommended | table
model,object_name,field_name,recommended | sort model,object_name,field_name
```

You can also narrow down the search results by changing `/services/data/models` to one model, such as `/services/data/models/Alerts`.

Make note of all fields in the data model that do not correspond exactly to your event data. Some might not exist in your data, have different field names, or have the correct field names but have values that do not match the expected type of the model. Normalize your data for each of these fields using a combination of field aliases, field extractions, and lookups.

b. Create field aliases to normalize field names

First, look for opportunities to add aliases to fields. Determine whether any existing fields in your data have different names than the names expected by the data models. For example, the Web data model has a field called `http_referrer`. This field may be misspelled as `http_referer` in your source data. Define field aliases to capture the differently-named field in your original data and map it to the field name that the CIM expects.

Also check your existing fields for field names that match the CIM field names but do not match the expected values as described in the data model reference tables. Your event may have an extracted field such as `id` that refers to the name of a completely different entity than the description of the field `id` in the CIM data model. Define a field alias to copy the `id` field from your indexed data to a different field name, such as `vendor_id`. The field alias is only part of the solution for preventing that data from appearing in reports and dashboards that expect the CIM `id` field. To capture the correct `id` field that you need for CIM compliance, you can either extract the field from elsewhere in your event, or write a lookup file to add that field from a CSV file.

See Add aliases to fields in the Splunk Enterprise documentation for more information about adding aliases to fields.

c. Create field extractions to extract new fields

After you have added aliases to all the fields that you can, add missing fields. When the values that you need for the CIM data model exist in the event data, extract the necessary fields using the field extraction capabilities of the Splunk platform. Name the fields to exactly match the field names in the CIM data models.

See Build field extractions with the field extractor and Create and maintain search-time field extractions through configuration files in the Splunk Enterprise documentation.

d. Write lookups to add fields and normalize field values

After you have aliased or extracted all the fields that you can in your indexed data, you might have to create lookup files to finish normalizing your data.

There are two reasons to create lookup files:

- Add fields that cannot be extracted from the event data. For example, your events might not contain the name of the `vendor`, `product`, or `app` of the system logging the event, but the data model you are mapping the data to expects all three of these fields. In this case, populate a CSV file with the source types generating the events and map each to the appropriate vendor name, product name, and application name.
- Normalize field values to make them compliant with the CIM. For example, the Network Traffic data model includes a `rule` field that expects string values that define the action taken in the network event. If your network traffic data contains a numeric value for the field `rule`, create a field alias for that field to something like `rule_id` so that it does not conflict with the `rule` field expected by the data model, which must be a string. Then, add a lookup to map the `rule_id` values to a new `rule` field with their corresponding string values.

See About lookups in the *Knowledge Manager Manual*.

e. Verify fields and values

After you finish normalizing your fields and values, validate that the fields appear in your events as you intended.

1. Search for the source type containing the data you are working to map to the CIM.
2. Use the field picker to select all the fields you just aliased, extracted, or looked up in your data.
3. Scan your events and verify that each field is populated correctly.
4. If one of the normalized fields has an incorrect value, edit the extraction, update the field alias, or correct your lookup file to correct the value.

6. Validate your data against the data model

After you have added your event tags and normalized your data by extracting fields, adding field aliases, and writing lookups, the data from your source type should map to the CIM data models that you targeted. You can validate that your data is fully CIM compliant by using the data model itself, using Pivot or Datasets, or by searching the data model directly.

Validate your data with specific goals in mind. For each field that you normalized within each unique event type, think of a useful metric that you can build with Pivot or Datasets to assess whether your data appears as you expect. Whether you use Pivot or Datasets depends on the apps installed in your deployment.

- If you use a version of Splunk Enterprise prior to 6.5.0, or do not have the Splunk Datasets Add-on installed, use Pivot to validate that your data is CIM compliant.
- If you use Splunk Cloud Platform or version 6.5.0 or later of Splunk Enterprise and have the Splunk Datasets Add-on installed, use Datasets to validate that your data is CIM compliant.

a. Validate using Datasets

If you have the Splunk Datasets Add-on installed, you can use Datasets to check whether your own login activity appears in your authentication data.

1. In the Search and Reporting app, click **Datasets**.
2. Select the data model and dataset in the model that you want to visualize with Pivot. For this example, locate **Authentication > Authentication > Successful Authentication** and click **Explore > Visualize with Pivot**.
3. Set the time range to an appropriate range to speed up the search. For this example, select **Last 15 minutes** if you recently logged in to a system.
4. Apply a filter to match your source type.
5. Split rows and columns by other relevant attributes in the model. For example, you might split the rows by `user` to

see a list of usernames that have logged in during the past 15 minutes.

b. Validate using Pivot

If you do not have the Splunk Datasets Add-on installed and are not a Splunk Cloud Platform customer, use Pivot. In this example, check whether your own login activity appears in your authentication data.

1. In the Search and Reporting app, click **Pivot**.
2. Select the data model against which you want to validate your data, then click into a relevant dataset in the model. For this example, select **Authentication**, then **Successful Authentication**.
3. Set the time range to an appropriate time range to speed up the search. For this example, set it to **Last 15 minutes** if you recently logged in to a system.
4. Apply a filter to match your source type.
5. Split rows and columns by other relevant attributes in the model. For example, you might split the rows by `user` to see a list of usernames that have logged in during the past 15 minutes.

c. Validate by searching the data model

You can search the data model using the `datamodel` command or the `| from datamodel` search syntax.

1. Open the Search and Reporting app.
2. Construct a search referencing the data model, including a filter for your source type, the `table` command, and the `field summary` command.
   For example, format a search using the `datamodel` command as follows:

   ```
   | datamodel <Data_Model> <Data_Model_Dataset> search | search sourcetype=<your:sourcetype> | table *
   | fields – <List any statistics columns that you do not want to display> | fieldsummary
   ```

   To use the `| from datamodel` syntax, format your search as follows:

   ```
   | from datamodel:<Data_Model>.<Data_Model_Dataset> | search sourcetype=<your:sourcetype> | table * |
   fields – <List any statistics columns that you do not want to display> | fieldsummary
   ```
3. Observe the results of the search. To identify problems with your field normalizations, scan this table to look for empty values, incorrect values, or statistics that do not match your expectations.
   The `datamodel` command performs a search against the data model and returns a list of all fields in the model, some statistics about them, and sample output from your data in the values column. You can remove statistics columns by specifying them after the `| fields –` portion of the search string.
   The `from` command does the same search, but flattens the results, so the field names are not prefaced with the name of the data model.
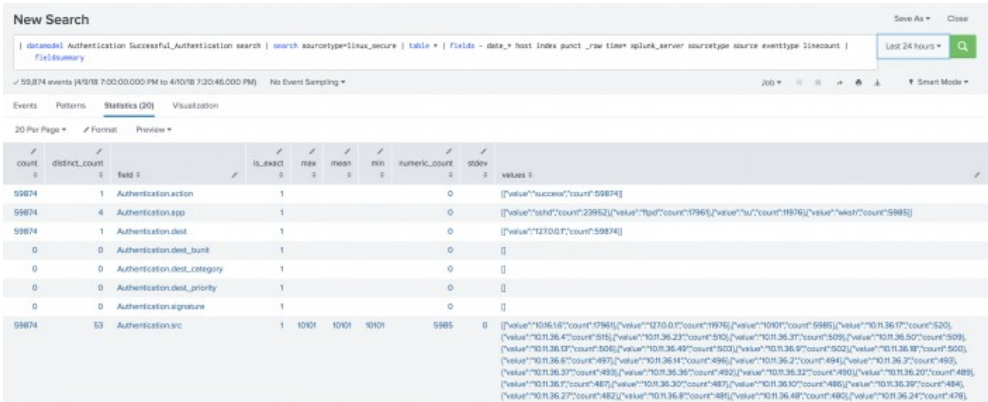
You can use these example searches to check for problems with your source type and field normalizations.

Normalization	Description
Source Type	You can use this example search to check for problems with your source type normalizations. For example, where your source type is a Cisco device, you can search for the following: `| datamodel Network_Traffic All_Traffic search	search sourcetype=cisco:*	stats count by sourcetype`

Normalization	Description
	If you don't see all the `sourcetype` results that you expect, then you may need to revisit the corresponding add-on details. See Supported Add-ons.
Field	You can use this example search to check for problems with your field normalizations. For example, where your source type is a Linux Secure device, you can use this example search to check that Linux Secure data maps as expected to the Authentication data model for successful login activities. `| datamodel Authentication Successful_Authentication search | search sourcetype=linux_secure | table * | fields – date_* host index punct _raw time* splunk_server sourcetype source eventtype linecount | fieldsummary` Here is the result using the example search string above.

For more information about the datamodel command, see the datamodel in the *Search Reference* manual.

7. (Optional) Extend the CIM definition with custom fields

If some of the fields that you want to use are not defined in the data model by default, you can add fields to a dataset. As a precaution, consider keeping a record of your modifications, so that they can be reapplied if models are updated or restored in the future. You can do this by selecting **download** from the datamodel editor page, after you have made your modifications.

Add new fields as follows:

1. From the Splunk ES menu bar, click **Search > Datasets**.
2. Find the name of the Data Model and click **Manage > Edit Data Model**.
3. From the Add Field drop-down, select a method for adding the field, such as **Auto-Extracted**.
   1. If you see the field name, check the check box for it, enter a display name, and select a type.
   2. If you don't see the field name, click **Add by Name**, enter the field name, enter a display name, and select a type.

Then you can search the dataset again:

1. From the Splunk ES menu bar, click **Search > Datasets**.
2. Find the name of the Data Model and click **Explore > Investigate in Search**.
3. The search displays in the search bar:

```
| from datamodel:"Web.Web"
```

and the new field displays in the results.

> It is not considered a best practice to clone the data model and to keep the original for record keeping purposes. Cloning would create an entirely new model that wouldn't be referenced in any downstream searches.

8. (Optional) Package your configurations as an add-on

Now that you have tested your field extractions, lookups, and tags, you can choose to package the search-time configurations as an add-on and publish it to the community. Using your add-on, other Splunk platform users with the same data source can map their data to the CIM without having to repeat the steps you completed above.

See Package and publish a Splunk app on the Splunk Developer Portal.

Use the CIM to validate your data

The Common Information Model offers several built-in validation tools.

Use the `datamodelsimple` command

To determine the available fields for a data model, you can run the custom command `datamodelsimple`. Use or automate this command to recursively retrieve available fields for a given dataset of a data model.

You can use `datamodelsimple` in scenarios such as exploring the structure of data models or using the output of the command to create custom dashboards. This is helpful for technology add-on developers and dashboard content writers.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

The following format is expected by the command.

```
| datamodelsimple type=<models|objects|attributes> datamodel=<model name> object=<dataset name>
nodename=<dataset lineage>
```
Syntax for datamodelsimple

```
datamodelsimple [datamodelsimple-options]
```

Parameters for datamodelsimple

The following parameters are optional unless otherwise specified.

[datamodelsimple-options]
  Optional parameters for datamodelsimple command.
  syntax: `type=<datamodelsimple-option-type> <datamodelsimple-option-datamodel>`
  `<datamodelsimple-option-object> <datamodelsimple-option-nodename>`

[datamodelsimple-option-type]
  The list that will be returned.
  syntax: `models|objects|attributes`
  examples:

◊ models = returns a list of model names, such as `Authentication`
◊ objects = returns a list of object names, such as `Authentication.Failed_Authentication`
◊ attributes = returns a list of attribute names, such as `host, authentication_method, dest_bunit, reason`

[datamodelsimple-option-datamodel]
The datamodel name. Required for `type=objects` and `type=attributes`.
syntax: `datamodel=<string>`

[datamodelsimple-option-object]
The datamodel object name. Required for `type=attributes`.
syntax: `object=<string>`

[datamodelsimple-option-nodename]
The datamodel object name including lineage. Required for `type=attributes` in lieu of object.
syntax: `nodename=<string>`

Examples for datamodelsimple

You can use the datamodelsimple command in Splunk Web UI searches.

- List all the data models in the environment.

```
| datamodelsimple type=models
```

- List the objects in the Authentication data model.

```
| datamodelsimple type=objects datamodel=Authentication
```

- List attributes for the Failed_Authentication object in the Authentication data model.

```
| datamodelsimple type=attributes datamodel=Authentication
nodename=Authentication.Failed_Authentication
```

Use the CIM Validation (S.o.S.) datamodel

Version 4.2.0 of the Common Information Model moves the CIM Validation datasets into their own data model. Previously, the validation datasets were located within each relevant model.

Access the CIM Validation (S.o.S.) model in Pivot. From there, you can select a top-level dataset, a Missing Extractions search, or an Untagged Events search for a particular category of data. See Introduction to Pivot in the Splunk Enterprise *Pivot Manual*.

From the Splunk Enterprise menu bar, access the model from the following steps:

1. Select **Settings > Data models**
2. Locate the CIM Validation (S.o.S.) data model and in the Actions column, click Pivot.
3. Click one of the following to create the Pivot:
   ♦ Top level dataset
   ♦ Missing extractions
   ♦ Untagged events
4. Click **Save As...** to save your changes as a report or a dashboard panel.

Top level datasets

Top level datasets such as **Authentication** tell you what is feeding the model. Pivot allows you to validate that you are getting what you expect from your available source types. For best results, split rows by source type and add a column to the table to show counts for how many events in that source type are missing extractions. The following screenshot shows an example of how that looks using Authentication as an example.

If you see values in the missing extractions column, and the data model is accelerated, you can go to the Datamodel Audit Dashboard in Splunk Enterprise Security. See Datamodel Audit Dashboard for more information. Alternatively, you can access the appropriate Missing Extractions dataset in Pivot to drill further into the attributes.

Missing extractions

Missing extractions run searches that return all missing field extractions. There are certain field extractions that are expected in order to fully populate that dataset of the data model, and the names display here if the data is missing. In other words, Splunk Enterprise finds tagged events for this dataset in this model, but there are field extractions for this event type that Splunk Enterprise expects, but they are not present. If you get results, split rows by source type to find which data source is contributing events for this model but is not fully mapping to the CIM.

Untagged events

Untagged events runs a search for events that have a strong potential for CIM compliance but are not tagged with the appropriate tag or tags. For example, the Untagged Authentication search is:

```
(login OR "log in" OR authenticated) sourcetype!=stash NOT tag=authentication
```

For best results, split by source type. Click the results to drill into the untagged events.

Use the CIM to create reports and dashboards

If you are working with data that has already been normalized to the Common Information Model, you can use the CIM data models to generate visualizations, reports, and dashboards the same way you would use any other data model in the Splunk platform.

Your data is normalized if you or someone else in your organization have completed the normalizing steps described in Use the CIM to normalize data at search time, or you are using an add-on that normalizes data to the CIM data models.

Example: Create a report to analyze authorization events using CIM data models

For example, you want to create a report to monitor authorization events on your systems. Both the Authentication and Change data models contain authorization-relevant fields. You can create reports using search or using Pivot. This example uses Pivot.

Start by opening the Change data model in Pivot. You can open a data model in Pivot two different ways, depending on if you use the Splunk Datasets Add-on or not.

- If you use Splunk Cloud Platform or you have the Splunk Datasets Add-on, open a data model in Pivot with the following steps:
  1. In the Search and Reporting App, click **Datasets**.
  2. Locate the **Change > All Changes > Account Management** data model and datasets.
  3. Click **>** to review the fields available in the dataset of the data model.
  4. Click **Explore > Visualize with Pivot** to open Pivot to explore the data model and dataset.
- If you do not have the Splunk Datasets Add-on, or do not use Splunk Cloud Platform, you can open a data model in Pivot with the following steps:
  1. In the Search and Reporting App, click **Pivot**.
  2. Select the **Change** data model. Observe that it has a child dataset called Account Management.
  3. Click **>** next to the Account Management dataset and its child datasets to browse the available events and fields contained in the model.

Then, create a report in Pivot. This report uses the Account Management dataset of the Change data model.

For example, to see the number of account lockouts over the past hour, create a report as follows.

1. In Pivot, select the **Area Chart** option.
2. Set the time range to **Last 60 minutes**.
3. If the `dest_category` field is in use, you can filter based on the destination category to review account lockouts only on specifically-categorized machines. Otherwise, leave the filter blank.
4. Leave the X-axis as the default of time.
5. Select a field of `is_Account_Lockouts` for the Y-axis.
6. (Optional) Modify additional settings.
7. Select **Save As > Report** to save the chart as a report.

After creating the report, you can add the report to a dashboard and adjust the permissions so that others can view it.

Resources for using Pivot with data models

To learn more about using Pivot with data models, use the following resources.

- See About Data Models in the Splunk Enterprise *Knowledge Manager Manual*.
- See the Introduction to Pivot in the Splunk Enterprise documentation.

Use the Data Model Audit dashboard and Machine Learning ToolKit

You can use the dashboard included with the Common Information Model to monitor your data model accelerations and searches. The Common Information Model includes the Data Model Audit dashboard to help you analyze the performance of your data model accelerations.

Access these dashboard by going to the Search and Reporting app. From there, click **Dashboards** to view your list of dashboards. When the Splunk Common Information Model Add-on is installed, the dashboard appear in the list.

For more detail on the data model audit dashboard, see Check the status of data model accelerations in this manual.

You can also use MLTK to find different varieties of anomalous events in your data. See Machine Learning Toolkit Overview in Splunk Enterprise Security in the Splunk Enterprise Security *Administer Splunk Enterprise Security* manual.

Use the CIM Filters to exclude data

The CIM Filter macros are available to help exclude data from your search results. The macros are a way to reduce false positives by whitelisting categories from lookups, data model objects, event severities, or extracted fields. They are available by default and located in the `CIM Filters` section of the `$SPLUNK_HOME/etc/apps/Splunk_SA_CIM/default/macros.conf` file for reference. There is no need to modify the stanzas in this section.

Usage

To use the `cim_filter_known_scanners` macro, for example, the most common use case is with Splunk Enterprise Security.

In this case, a known scanner is a device on your network that is purposely doing active or passive vulnerability scans. You might get a lot of false positive alerts about this device because the scanning activity is generating a lot of notable events. You know that these events can be ignored because it's your own scanner. You can categorize this device as a **known_scanner** in the assets and identities system. Then you can use the macro to filter out that category, so you no longer see the device in the search results.

See the "Asset lookup header" section of Format an asset or identity list as a lookup in Splunk Enterprise Security in the *Administer Splunk Enterprise Security* manual for more information about where to add **known_scanner** as a category.

Example

The macros are for use with piped searches or where clauses. For the example of `cim_filter_known_scanners`, you can see in the `macros.conf` file that you can use it in two ways.

One way to use the macro is with search:

```
... | search `cim_filter_known_scanners` | ...
```

The other way to use the macro allows you to pass the DataModel.DataSet object lineage with tstats:

```
| tstats count from datamodel="Intrusion_Detection.IDS_Attacks" where
`cim_filter_known_scanners(IDS_Attacks)`
```

See Define search macros in Settings in the Splunk Enterprise *Knowledge Manager Manual* for further information on how to navigate to and edit the macro definition in Splunk Web.

Accelerate CIM data models

You can accelerate a data model to speed up the data set represented by that data model for reporting purposes. After you accelerate a data model, your reports and dashboard panels that reference the accelerated data model will return results faster. A data model's summary range setting impacts the size of the data models on disk, and the processing load of creating accelerated data alongside the index buckets. For more information about accelerating data models, see Enable data model acceleration in the *Knowledge Manager Manual* for Splunk Enterprise.

On the Splunk Cloud Platform, running accelerated data models might impact the performance of the search head since these heavy searches that collect the data for the data acceleration model can cause the search head to run out of processing power.

Additionally, when a time summary range of over 3 months is selected, it might cause searches to run on a loop. This implies that even though the search head is unable to finish the first search and build a data model, it repeats the same search that creates incomplete data models since accelerated data models are searches that run in the background to build a data model. For more information on how to change the summary time range, see Change the summary time range for data model accelerations.

Enable data model acceleration

By default, the data model acceleration for all models included in the Splunk Common Information Model Add-on are disabled.

Configure the acceleration parameters of the CIM data models in the CIM Setup view.

1. In Splunk Web, go to **Apps > Manage Apps**.
2. Click on **Set up** in the row for Splunk Common Information Model.
3. Click on the **Settings** tab.
4. Select a data model that you want to accelerate.
5. Click the box next to acceleration.enabled to accelerate the model.
6. (Optional) Configure the advanced acceleration settings.

Parameter	Description
acceleration.backfill_time	How far back in time the Splunk platform should create its column stores, specified as a relative time string. Only set this parameter if you want to backfill less data than the retention period set by 'acceleration.earliest_time'. Refer to `datamodels.conf.spec` for warnings and limitations.
acceleration.earliest_time	How far back in time the Splunk software should keep these column stores, specified as a relative time string.
acceleration.max_time	The maximum amount of time that the column store creation search is allowed to run, in seconds.
acceleration.max_concurrent	The maximum number of concurrent acceleration instances for this data model that the scheduler is allowed to run.
acceleration.manual_rebuilds	When checked, this setting prevents outdated summaries from being rebuilt by the 'summarize' command. Admins can manually rebuild a data model through the Data Model Manager page by expanding the row for the affected data model and clicking **Rebuild**.

For more detailed reference information on these fields, see Advanced configurations for persistently accelerated data models in the *Knowledge Manager Manual* in the Splunk Enterprise documentation.

7. Click **Save**.

For more information about accelerated data models and data model acceleration jobs, see Use the data model audit dashboard in this topic.

Disable acceleration for a data model

If you have Splunk Enterprise Security or the Splunk App for PCI Compliance installed, some of the data models in the CIM are automatically accelerated by configuration settings in these apps. If you want to change which data models are accelerated by these apps, access the **Data Model Acceleration Enforcement** modular input on your search head and make your changes there. If you attempt to unaccelerate a data model using any other method, including using the **Settings** tab in the CIM Setup page, your changes will not persist because the the app acceleration enforcement re-accelerates the data models automatically.

If you do not have an app installed that enforces any CIM data models to be accelerated, you can edit the acceleration settings on the CIM Setup page.

1. In Splunk Web, go to Apps > Manage Apps
2. Click on **Set up** in the row for Splunk Common Information Model.
3. Click on the **Settings** tab.
4. Select the data model for which you want to disable acceleration.
5. Uncheck the box next to acceleration.enabled to stop accelerating this data model.
6. Click **Save**.

Change the summary range for data model accelerations

A data model's summary range setting impacts the size of the data models on disk, and the processing load of creating accelerated data alongside the index buckets.

1. In Splunk Web, go to **Apps > Manage Apps**.
2. Find the Splunk Common Information Model add-on.
3. Click **Set up** to open the CIM Setup page.
4. Click the **Settings** tab.
5. Select the data model you want to change.
6. Set a summary range:
    1. Review the **acceleration.enabled** setting. A summary range only applies to accelerated data models.
    2. Review the **acceleration.earliest_time** setting to determine the current summary range.
    3. Change the **acceleration.earliest_time** setting. Examples: -1y, -3mon, -1mon, -1w, -1d, or 0 for "All Time".
7. Select **Save**.

The CIM Setup page will only display CIM data models. A custom data model will not be displayed and cannot have its settings changed from the CIM Setup page. To change the summary range or other settings on a custom data model, manually edit the `datamodels.conf` provided with the app or add-on. For more information, see the datamodels.conf spec file in the Splunk Enterprise *Admin Manual*.

Use the Data Model Audit dashboard

Use the Data Model Audit dashboard to display information about the state of data model accelerations in your environment. Alternatively, use the `` `cim_datamodelinfo` `` macro to search the data model statuses from the search bar.

To access the dashboard:

1. Go to the **Search and Reporting** app.
2. In the menu bar, click **Dashboards**.
3. Select the **Data Model Audit** dashboard.

Check the status of data model accelerations

Panel	Description
Top Accelerations By Size	Displays the accelerated data models sorted in descending order by MB on disk
Top Accelerations By Run Duration	Displays the accelerated data models sorted in descending order by the time spent on running acceleration tasks.
Acceleration Details	Displays a table of the accelerated data models with additional information.

Use the common action model to build custom alert actions

The common action model is a common information model for alert actions. It is not a data model. Rather, it is a set of tools and best practices for creating alert actions that are consistent, robust, and easy to introspect. Splunk developed the common action model to support the adaptive response framework in Splunk Enterprise Security, but it is not exclusive to that use case.

The common action model consists of three components:

- a `cim_actions.py` library, which assists developers with building alert actions in a way that conforms to the common action model.
- a JSON spec in `alert_actions.conf.spec`, which classifies actions and specifies other metadata expected by the adaptive response framework.
- an extension to the Splunk Audit Logs data model that describes the introspection event data produced by alert actions that conform to the common action model.

Developers can use these components to design new alert actions or adaptive response actions or refactor existing custom actions to comply with the model. You can incorporate the common action model into your manual development process, or you can use the Splunk Add-on Builder, which incorporates the common action model in its custom alert action creation wizard. The Splunk Enterprise Security developer documentation contains a detailed walkthrough of both of these methods of creating an adaptive response action, which is an alert action with special functionality in Splunk Enterprise Security. See Create an adaptive response action on the Splunk developer portal.

Using the `cim_actions.py` library

The `cim_actions.py` library is located at `$SPLUNK_HOME/etc/apps/Splunk_SA_CIM/lib/cim_actions.py`. If you are creating your action manually, import this library so that you can use the methods provided in it. If you are using Add-on Builder to create your action, the code snippet provided on the code editor imports the library for you and provides sample code for the methods available.

Incorporating the JSON spec

The JSON spec is located at `$SPLUNK_HOME/etc/apps/Splunk_SA_CIM/README/alert_actions.conf.spec`. It defines the `param._cam` attribute and provides its documentation. The same folder also contains `alert_actions.conf.example`, which contains two examples of how to follow the specification in your `alert_actions.conf` file.

Parameter	Description	Examples

category	The category or categories the action belongs to. See `cam_categories.csv` for recommended values.	Information Conveyance, Information Gathering, Information Tracking, Permissions Control, Device Control
task	The function or functions performed by the action. See `cam_tasks.csv` for recommended values.	block, allow, create, update, delete, scan
subject	The object or objects that the action's task or tasks can be performed on. See `cam_subjects.csv` for recommended values.	endpoint.file, network.proxy, process.sandbox

technology	The technology vendor(s), product(s), and version(s) that the action supports.	`{ "vendor":  "Splunk",`
		`"product": "Enterprise",`
		`"version": ["6.4.3", "6.5.0"]`
		`}`

supports_adhoc	Specifies if the action supports ad-hoc invocation from the Actions menu on the Incident Review dashboard in Splunk Enterprise Security. This parameter is only relevant within Splunk Enterprise Security, and defaults to false. See Adaptive Response framework in Splunk ES on the Splunk developer portal.	true
drilldown_uri	An optional customized drilldown for the link that appears in the detailed view of a notable event on the Incident Review dashboard in Splunk Enterprise Security. This parameter is only relevant within Splunk Enterprise Security. If you do not want to specify a custom drilldown link, remove this parameter. Do not leave this parameter blank. If the parameter is not included, the default drilldown URL leads to a search for the result events created by this response action. If you want to specify a target in an app outside Enterprise Security, use the format `../<app_context>/<viewname>?<additional drilldown parameters>`. If you are redirecting to a custom view within Enterprise Security, use the format `/<viewname>?<additional drilldown parameters>`.	`"../my_app/my_view?` `form.orig_sid=$sid$&form.orig_rid=$rid$"`
field_name_params	The param or params which represent the name of a result field. This parameter is only relevant within Splunk Enterprise Security. Incident Review uses the specified field name parameters to render a dropdown with field names present in the notable event.	["param.my_param"]
required_params	Parameter(s) required for successful action execution. This parameter is only relevant within Splunk Enterprise Security. Incident Review uses the specified field name parameters to render a * on the user interface to indicate that the parameter is required.	["param.my_param"]

Modeling introspection data

The Splunk Audit Logs data model includes the `Modular_Actions` dataset. The `message()` method in the `cim_actions.py` library automatically creates and tags introspection events for this data model. See Splunk Audit Logs for details of the fields.

If you have Splunk Enterprise Security installed, select the Adaptive Response Action Center to view introspection data for all actions compliant with the common action model.

Examples

Use the CIM to normalize OSSEC data

This example demonstrates how to create an add-on for OSSEC, an open-source host-based intrusion detection system (IDS).

Note: Splunk offers an add-on that provides the capabilities in this example for OSSEC data, so you do not need to build one yourself. Find the add-on on Splunkbase at https://splunkbase.splunk.com/app/2808/.

This example illustrates how to perform the following tasks:

- Evaluate data in the context of the CIM and Splunk Enterprise Security requirements.
- Use regular expressions to extract the necessary fields.
- Convert the values in the severity field to match the format required in the Common Information Model.
- Create multiple event types to identify different types of events within a single data source.
- Package the results as an add-on to share with the community.

Step 1: Get the data in

To get started, set up a data input in order to get OSSEC data into Splunk Enterprise Security. OSSEC submits logs via `syslog` over port UDP:514, so you can use a network-based data input. Once you have built and installed the add-on, it will detect OSSEC data and automatically assign it the correct source type when it receives data over UDP port 514.

1. Configure folder and source type naming. Create a folder for the new add-on at `$SPLUNK_HOME/etc/apps/Splunk_TA-ossec`. (The name of this add-on is `Splunk_TA-ossec`.) For this add-on, use the source type `ossec` to identify data associated with the OSSEC intrusion detection system.

2. Configure line breaking. Because each log message separates itself with an end-line, you must disable line-merging to prevent the add-on from combining multiple messages. To do so, set `SHOULD_LINEMERGE` to false in the `default/props.conf`.

For example:

```
[source::....ossec]
sourcetype=ossec

[ossec]

SHOULD_LINEMERGE = false

[source::udp:514]
TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec
```

3. Restart the Splunk platform so that it recognizes the add-on and source type you defined.

Step 2: Examine your data to identify relevant IT security events

1. Identify which events you want to display in the **Intrusion Center** dashboard in Splunk Enterprise Security. Use the CIM reference tables to find fields that are relevant for intrusion detection data. The data maps to the Intrusion Detection data model.

137

2. Open the reference table for that model to use as a reference. In Splunk Web, open the Data Model Editor for the IDS model to refer to the dataset structure and constraints.

Step 3: Tag events

1. Identify the tags you must create. The Common Information Model dictates that you must tag intrusion detection data with "`attack`" and "`ids`" to indicate that the data comes from an attack detection event.

2. Create the event types to which you can assign tags. To do so, create an event type in the `eventtypes.conf` file that assigns the "ossec_attack" event type to all data with the source type `ossec` and a `severity_id` greater than or equal to 6.

```
[ossec_attack]
search = sourcetype=ossec severity_id >=6
#tags = ids attack
```

3. Assign the tags in the `tags.conf` file.

```
  [eventtype=ossec_attack]
   attack = enabled
   ids = enabled
```

Step 4: Verify tags

1. Verify that your Splunk platform applies the tags correctly. In the Searching and Reporting app, search for the source type as follows:

```
sourcetype="ossec"
```

2. Review the entries to find the tag statements under the log message.

Step 5: Normalize fields

1. Create the field extractions that populate the fields according to the Common Information Model. First, review the Common Information Model and the Dashboard requirements matrix for Splunk Enterprise Security in *Administer Splunk Enterprise Security* to determine that the OSSEC add-on needs to include the following fields in order to populate the Intrusion Center and Intrusion Search dashboards in Splunk Enterprise Security:

Domain	Field Name	Data Type
Intrusion Detection	signature	string
Intrusion Detection	category	string
Intrusion Detection	severity	string
Intrusion Detection	src	string
Intrusion Detection	dest	string
Intrusion Detection	ids_type **Note:** ids_type of host is necessary to include this in the host root model	string

You can also populate additional CIM fields, if they are available in your data.

2. Create extractions. OSSEC data is in a proprietary format that does not use key-value pairs or any kind of standard delimiter between the fields. Therefore, you have to write a regular expression to parse the individual fields. The following outlines a log message highlighting the relevant fields.

The severity field includes an integer, while the Common Information Model requires a string. Therefore, extract this into a different field, `severity_id`, then perform the necessary conversion later to produce the severity field.

3. Extract the Location, Message, severity_id, signature and src_ip fields. To do so, edit the `default/transforms.conf` file to add a stanza that extracts the fields you need to the following:

```
[force_sourcetype_for_ossec]
DEST_KEY = MetaData:Sourcetype
REGEX = ossec\:
FORMAT = sourcetype::ossec

[kv_for_ossec]
REGEX = Alert Level\:\s+([^;]+)\;\s+Rule\:\s+([^\s]+)\s+-
\s+([^\.]+)\.{0,1}\;\s+Location\:\s+([^;]+)\;\s*(srcip\:\s+(\d{1,3}
\.\d{1,3}\.\d{1,3}\.\d{1,3})\;){0,1}\s*(user\:\s+([^;]+)\;){0,1}\s*(.*)
FORMAT = severity_id::"$1" signature_id::"$2" signature::"$3"
Location::"$4" src_ip::"$6" user::"$8" Message::"$9"
```

4. Enable the statement in the `default/props.conf` file in your add-on folder.

```
[source::....ossec]
sourcetype=ossec

[ossec]
SHOULD_LINEMERGE = false
REPORT-0kv_for_ossec = kv_for_ossec

[source::udp:514]
TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec
```

5. Extract the `dest` field. Some of the fields need additional field extraction to fully match the Common Information Model. The `Location` field includes several separate fields within a single field value. Create the following stanza in the `default/props.conf` file to extract the destination DNS name, destination IP address, and original source address.

```
[source::....ossec]
sourcetype=ossec

[ossec]
SHOULD_LINEMERGE = false

[source::udp:514]
TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec

[kv_for_ossec]
REGEX = Alert Level\:\s+([^;]+)\;\s+Rule\:\s+([^\s]+)\s+-
\s+([^\.]+)\.{0,1}\;\s+Location\:\s+([^;]+)\;\s*(srcip\:\s+(\d{1,3
}\.\d{1,3}\.\d{1,3}\.\d{1,3})\;){0,1}\s*(user\:\s+([^;]+)\;){0,1}\s*(.*)
```

```
FORMAT = severity_id::"$1" signature_id::"$2" signature::"$3"
Location::"$4" src_ip::"$6" user::"$8" Message::"$9"

[Location_kv_for_ossec]
SOURCE_KEY = Location
REGEX = (\((([^\)]+)\))*\s*(.*?)(->)(.*)
FORMAT = dest_dns::"$2" dest_ip::"$3" orig_source::"$5"
```

6. Enable the statement in the `default/props.conf` file in the add-on folder:

```
[source::....ossec]
sourcetype=ossec

[ossec]
SHOULD_LINEMERGE = false
REPORT-0kv_for_ossec = kv_for_ossec, Location_kv_for_ossec

[source::udp:514]
TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec
```

7. The "`Location_kv_for_ossec`" stanza creates two fields that represent the destination (either by the DNS name or destination IP address). You need a single field named "`dest`" that represents the destination. To handle this, add stanzas to `default/transforms.conf` that populate the destination field if the `dest_ip` or `dest_dns` is not empty. Note that the regular expressions below work only if the string has at least one character. This ensures that the destination is not an empty string.

```
[source::....ossec]
sourcetype=ossec

[ossec]
SHOULD_LINEMERGE = false

[source::udp:514]
TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec

[kv_for_ossec]
REGEX = Alert Level\:\s+([^;]+)\;\s+Rule\:\s+([^\s]+)\s+-
\s+([^\.]+)\.\{0,1}\;\s+Location\:\s+([^;]+)\;\s*(srcip\:\s+(\d{1,3}\.\d{1,3
}\.\d{1,3}\.\d{1,3})\;){0,1}\s*(user\:\s+([^;]+)\;){0,1}\s*(.*)
FORMAT = severity_id::"$1" signature_id::"$2" signature::"$3"
Location::"$4" src_ip::"$6" user::"$8" Message::"$9"

[Location_kv_for_ossec]
SOURCE_KEY = Location
REGEX = (\((([^\)]+)\))*\s*(.*?)(->)(.*)
FORMAT = dest_dns::"$2" dest_ip::"$3" orig_source::"$5"

[dest_ip_as_dest]
SOURCE_KEY = dest_ip
REGEX = (.+)
FORMAT = dest::"$1"

[dest_dns_as_dest]
SOURCE_KEY = dest_dns
REGEX = (.+)
FORMAT = dest::"$1"
```

8. Enable the field extractions you created in the `default/transforms.conf` file by adding them to the `default/props.conf` file. Set up your field extractions to ensure that you get the DNS name instead of the IP address if both are available. To

140

do so, place the "`dest_dns_as_dest`" transform first; the Splunk platform processes field extractions in order, stopping on the first one that matches.

```
[source::....ossec]
sourcetype=ossec

[ossec]
SHOULD_LINEMERGE = false
REPORT-0kv_for_ossec = kv_for_ossec, Location_kv_for_ossec
REPORT-dest_for_ossec = dest_dns_as_dest,dest_ip_as_dest

[source::udp:514]
TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec
```

9. Extract the `src` field. You populated the source IP into the field "`src_ip`", but the CIM requires a separate "`src`" field as well. To create the separate field, add a field alias in the `default/props.conf` file that populates the "`src`" field with the value in "`src_ip`".

```
[source::....ossec]
sourcetype=ossec

[ossec]
SHOULD_LINEMERGE = false
REPORT-0kv_for_ossec = kv_for_ossec, Location_kv_for_ossec
REPORT-dest_for_ossec = dest_dns_as_dest,dest_ip_as_dest
FIELDALIAS-src_for_ossec = src_ip as src

[source::udp:514]
TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec
```

10. Normalize the severity field. The OSSEC data includes a field that contains an integer value for the severity. However, the Common Information Model requires a string value for the severity. Therefore, you need to convert the input value to a value that matches the Common Information Model. Do this using a lookup table. Map the "`severity_id`" values to the corresponding severity string, then create a CSV file in `lookups/ossec_severities.csv`.

```
severity_id,severity
 0,informational
 1,informational
 2,informational
 3,informational
 4,error
 5,error
 6,low
 7,low
 8,low
 9,medium
10,medium
11,medium
12,high
13,high
14,high
15,critical
```

11. Add the lookup file definition to the `default/transforms.conf` file.

```
[source::....ossec]
sourcetype=ossec

[ossec]
```

```
  SHOULD_LINEMERGE = false

  [source::udp:514]
  TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec

  [kv_for_ossec]
  REGEX = Alert Level\:\s+([^;]+)\;\s+Rule\:\s+([^\s]+)\s+-
  \s+([^\.]+)\.\{0,1}\;\s+Location\:\s+([^]+)\;\s*(srcip\:\s+(\d{1,3
  }\.\d{1,3}\.\d{1,3}\.\d{1,3})\;){0,1}\s*(user\:\s+([^;]+)\;){0,1}\s*(.*)
  FORMAT = severity_id::"$1" signature_id::"$2" signature::"$3"
  Location::"$4" src_ip::"$6" user::"$8" Message::"$9"

  [Location_kv_for_ossec]
  SOURCE_KEY = Location
  REGEX = (\(([^\)]+)\))*\s*(.*?)(->)(.*)
  FORMAT = dest_dns::"$2" dest_ip::"$3" orig_source::"$5"

  [dest_ip_as_dest]
  SOURCE_KEY = dest_ip
  REGEX = (.+)
  FORMAT = dest::"$1"

  [dest_dns_as_dest]
  SOURCE_KEY = dest_dns
  REGEX = (.+)
  FORMAT = dest::"$1"

  [ossec_severities_lookup]
  filename = ossec_severities.csv
```

12. Add the lookup to `default/props.conf`:

```
  [source::....ossec]
  sourcetype=ossec

  [ossec]
  SHOULD_LINEMERGE = false
  REPORT-0kv_for_ossec = kv_for_ossec, Location_kv_for_ossec
  REPORT-dest_for_ossec = dest_dns_as_dest,dest_ip_as_dest
  FIELDALIAS-src_for_ossec = src_ip as src
  LOOKUP-severity_for_ossec = ossec_severities_lookup severity_id OUTPUT severity

  [source::udp:514]
  TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec
```

13. Define the vendor and product fields. The last fields to populate are the vendor and product fields. To populate these, add stanzas to the `default/transforms.conf` file to statically define them:

```
  [source::....ossec]
  sourcetype=ossec

  [ossec]
  SHOULD_LINEMERGE = false

  [source::udp:514]
  TRANSFORMS-force_sourcetype_for_ossec_syslog = force_sourcetype_for_ossec

  [kv_for_ossec]
  REGEX = Alert Level\:\s+([^;]+)\;\s+Rule\:\s+([^\s]+)\s+-
  \s+([^\.]+)\.\{0,1}\;\s+Location\:\s+([^]+)\;\s*(srcip\:\s+(\d{1,3}\.\d{1,3}\.\d{1,3
  }\.\d{1,3})\;){0,1}\s*(user\:\s+([^;]+)\;){0,1}\s*(.*)
```

```
    FORMAT = severity_id::"$1" signature_id::"$2" signature::"$3"
    Location::"$4" src_ip::"$6" user::"$8" Message::"$9"

    [Location_kv_for_ossec]
    SOURCE_KEY = Location
    REGEX = (\((([^\)]+)\)))*\s*(.*?)(->)(.*)
    FORMAT = dest_dns::"$2" dest_ip::"$3" orig_source::"$5"

    [dest_ip_as_dest]
    SOURCE_KEY = dest_ip
    REGEX = (.+)
    FORMAT = dest::"$1"

    [dest_dns_as_dest]
    SOURCE_KEY = dest_dns
    REGEX = (.+)
    FORMAT = dest::"$1"

    [ossec_severities_lookup]
     filename = ossec_severities.csv

    [product_static_hids]
    REGEX = (.)
    FORMAT = product::"HIDS"

    [vendor_static_open_source_security]
    REGEX = (.)
    FORMAT = vendor::"Open Source Security"
```

14. Enable the stanzas in the `default/props.conf` file.

```
  [source::....ossec]
  sourcetype=ossec

  [ossec]
  SHOULD_LINEMERGE = false
  REPORT-0kv_for_ossec = kv_for_ossec, Location_kv_for_ossec
  REPORT-dest_for_ossec = dest_dns_as_dest,dest_ip_as_dest
  FIELDALIAS-src_for_ossec = src_ip as src
  LOOKUP-severity_for_ossec = ossec_severities_lookup severity_id OUTPUT severity
  REPORT-product_for_ossec = product_static_hids
  REPORT-vendor_for_ossec = vendor_static_open_source_security
```

Step 6: Validate your CIM compliance

1. Verify that your field extractions function correctly. First, restart the Splunk platform so that it recognizes the lookups you created.

2. In the **Searching and Reporting** app, search for the source type.

```
sourcetype="ossec"
```

3. From the search results, select **Pick Fields** to choose the fields that the Splunk platform ought to populate. Hover over the field name to display the values (see example below).
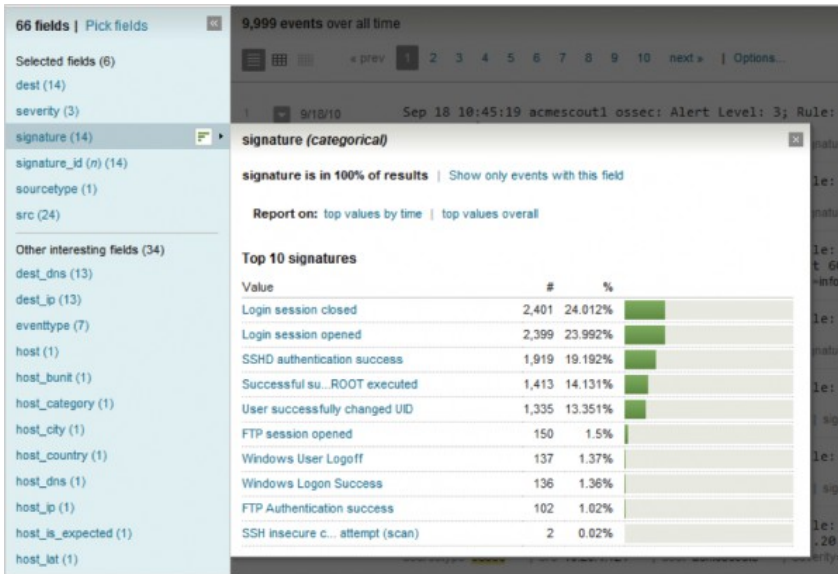
Optional You can further validate using one of the following methods:

◊ Use Pivot. See Validate using Pivot for details.
◊ Use the `datamodel` command. See Validate using the `datamodel` command for details.
◊ Use the Splunk Enterprise Security dashboard in which you expect the data to appear. In this example, the OSSEC data ought to display in the Intrusion Center dashboard. The OSSEC data is not immediately available in the dashboard because Splunk Enterprise Security uses summary indexing. Therefore, the data may not be available on the dashboard for up to an hour after you have completed the add-on.

Step 7: (Optional) Document and package your configurations as an add-on

1. Create a README file. In the file, include information necessary for others to use the add-on. Create the following README.txt file under the root add-on directory.

```
===OSSEC add-on===

  Author: John Doe
  Version/Date: 1.3 September 2013

  Supported product(s):
  This add-on supports Open Source Security (OSSEC) IDS 2.5

  Source type(s): This add-on will process data that is source typed
  as "ossec".

  Input requirements: Syslog data sent to port UDP\514

  ===Using this add-on===

  Configuration: Automatic
  Syslog data sent to port UDP\514 will automatically be detected as OSSEC
  data and processed accordingly.

  To process data that is sent to another
  port, configure the data input with a source type of "ossec".
```

2. Package the OSSEC add-on by converting it into a zip archive named `Splunk_TA-ossec.zip`.

3. To share your add-on, go to https://splunkbase.splunk.com/develop/, then click **Submit your app**.

Use the CIM to normalize CPU performance metrics

This example illustrates how to normalize data for CIM-compliance for an IT Service Intelligence use case. This example provides two variations: one using Splunk Web, and another using configuration files from the command line.

Normalize data for CIM-compliance using Splunk Web

Step 1. Get your data in

For the purposes of this example, assume that you have already added data to your Splunk platform deployment. For instructions on adding data, see *Getting Data In*.

Step 2. Examine your data in context of the CIM

Make sure that the data that you want to extract has a dataset specified in the CIM. For example, if you want to build a KPI search based on a specific CPU performance metric, such as `cpu_load_percent`, review the Performance data model to make sure that the data model lists `CPU` as a dataset.

If the CIM does not contain the specific data that you want to extract for your KPI searches, you can use a Splunk add-on or apply the Common Information Model to your own data. See Design data models in the Splunk Enterprise *Knowledge Manager Manual*.

Step 3. Configure CIM-compliant event types

1. From Splunk Web, select **Settings > Data Models**.
2. Find the data model dataset that you want to map your data to, then identify its associated tags.
   For example, the `CPU` dataset in the `Performance` data model has the following tags associated with it:
   tag = performance
   tag = cpu
3. Create an event type.
      1. Select **Settings > Event types**.
      2. Click **New.**
      3. In the **Add new** dialog, type the following values for the following fields.

Destination App:	ITSI
Name:	Type the name of the event type. For example, `cpu_metrics`.
Search String:	Type a search string for the event type. For example, `sourcetype=test_cpu_log`.
Tag(s):	Type the tags associated with the data model dataset you are mapping to. For example, `performance`, `cpu`.
Field aliases:	Type the field name as found in your data, then enter the field alias. For example, `cpu_percent = cpu_load_percent`

4. Click **Save**.

For more information, see Configure event types in Splunk Web in the Splunk Enterprise *Knowledge Manager Manual*.

Step 4. Verify your tags

See Use the CIM to normalize data at search time for details.

Step 5. Make fields CIM-compliant

Create field aliases to make fields CIM-compliant.

Note: Field aliases do not support multi-value fields. For more information, see Create aliases for fields.

1. From Splunk Web, select **Settings > Fields > Field Aliases**.
2. Click **New**.
3. In the **Add New** window, type the following:
    1. For **Destination App:**, select ITSI.
    2. For **Name:**, type a name for your field alias.
    3. For **Apply to:**, select **Sourcetype**.
    4. For **named:**, type the name of the source type. For example, `test_cpu_log`.
4. Restart the Splunk platform for your changes to take effect.
5. Create search-time field extractions.
   If your event data contains fields that are not found in existing data models or search-time field extractions, you can add those fields using the Field Extractions page in Splunk Web. See Use the Field extractions page in the *Knowledge Manager Manual*.
6. Write lookups to add fields and normalize field values.
7. Verify fields and values.

Step 6. Validate normalized data against the data model

Now that you have mapped your data to the CIM, you can validate that your data is CIM-compliant. See 6. Validate your data against the data model.

Normalize data for CIM-compliance using configuration files

This section demonstrates how to normalize data for CIM-compliance at search-time using Splunk configuration files.

Step 1. Get your data in

For the purposes of this example, assume that you have already added data to your Splunk platform deployment. For instructions on adding data, see *Getting Data In*.

Step 2. Examine your data in context of the CIM

Make sure that the data that you want to extract has a dataset specified in the CIM. For example, if you want to build a KPI search based on a specific CPU performance metric, such as `cpu_load_percent`, review the Performance data model to make sure that the data model lists `CPU` as a dataset.

If the CIM does not contain the specific data that you want to extract for your KPI searches, you can use a Splunk add-on or apply the Common Information Model to your own data. See Design data models in the Splunk Enterprise *Knowledge Manager Manual*.

Step 3. Configure CIM-compliant event tags

1. Determine which tags are associated with the data model dataset. In Splunk Web, select **Settings > Data Models**.
2. Find the data model dataset that you want to map your data to, then identify its associated tags.
   For example, the `cpu_load_percent` attribute in the `CPU` dataset in the `Performance` data model has the following tags associated with it:
   tag = performance
   tag = cpu
3. On the search head, edit or create an `$SPLUNK_HOME/etc/apps/$APPNAME$/local/eventtypes.conf` file, then manually add the event type.
   For example:

   ```
   [cpu_metrics]
   search = sourcetype=test_cpu_log
   ```
4. On the search head, edit or create a `$SPLUNK_HOME/etc/apps/$APPNAME$/local/tags.conf` file, then manually add the appropriate tags for the data model dataset. For example:

   ```
   [eventtype=cpu_metrics]
   performance = enabled
   cpu = enabled
   ```
5. Restart the Splunk platform.

For more information, see Configure event types in eventtypes.conf.

Step 4. Verify your tags

See Use the CIM to normalize data at search time.

Step 5. Make fields CIM-compliant

Create field aliases to make fields CIM-compliant, then add search-time field extractions for additional fields as needed.

1. Create field aliases in `props.conf`. You can create multiple field aliases in a single stanza. Create your field alias by adding the following line to a stanza in the `$SPLUNK_HOME/etc/apps/$APPNAME$/local/props.conf` file.
   FIELDALIAS-<class> = <orig_field_name> AS <new_field_name>
   For example:

   ```
   [test_cpu_log]
   FIELDALIAS-cpu_percent = cpu_percent AS cpu_load_percent
   ```
2. Restart the Splunk platform for your changes to take effect.
3. Create basic search-time field extractions in `props.conf` by adding an EXTRACT stanza to
   `$SPLUNK_HOME/etc/apps/$APPNAME$/local/props.conf`:
   EXTRACT-<class> = [<regular_expression>|<regular_expression> in <source_field>]

For more information about field aliases, see Create aliases for fields in the *Knowledge Manager Manual*.

For more information about search-time field extractions, see Create basic search-time field extractions with props.conf edits.

Step 6. Validate normalized data against the data model

Now that you have mapped your data to the CIM, you can validate that your data is CIM-compliant. See 6. Validate your data against the data model.

Field Mappings

Authentication Field Mapping

The following shows an example of how authentication events map differently from various cloud providers to CIM data model field names.

See the Authentication data model for full field descriptions.

Login success example

The login success event from Google Cloud Platform (GCP), Microsoft Office 356 (MS o365), and Amazon Web Services (AWS) is a good way to see a common event and how each cloud provider maps to CIM data model field names.

GCP success

A sample GCP successful user login follows:

Click **expand** or **collapse** to show or hide the example.

```
{
   "actor":{
      "email":"name@gmail.com",                /** -----  user_id
      "profileId":"104465715494659475645"
   },
   "etag":"\"JDMC8884sebSczDxOtZ17CIssbQ/Pau_EbIGF8FWZWC7W8Ti1uoCfjc\"",
   "events":[
      {
         "name":"login_success",              /** -----  action
         "parameters":[
            {
               "name":"login_type",
               "value":"google_password"
            },
            {
               "multiValue":[
                  "password"                   /** -----  authentication_method
               ],
               "name":"login_challenge_method"
            },
            {
               "boolValue":false,
               "name":"is_suspicious"
            }
         ],
         "type":"login"                        /** -----  signature
      }
   ],
   "id":{
      "applicationName":"login",
      "customerId":"C035c27ok",                /** -----  vendor_account
      "time":"2020-02-24T23:31:48.090Z",
      "uniqueQualifier":"529462392776"
   },
```

```
   "ipAddress":"4.14.104.185",                   /** -----   src, src_ip
   "kind":"admin#reports#activity"               /** -----   user_agent
}
```

MS o365 success

A sample MS o365 successful user login follows:

Click **expand** or **collapse** to show or hide the example.

```
{ [-]
   Actor: [ [-]
      { [-]
        ID: df22f023-9e0f-4d78-bdd5-d496688af11e          /** -----   user_id
        Type: 0
      }
      { [-]
        ID: admin@a830edad9050849NDA3079.onmicrosoft.com /** -----   user_id
        Type: 5
      }
      { [-]
        ID: 10037FFE8EC1E08E                              /** -----   user_id
        Type: 3
      }
   ]
   ActorContextId: 2ed28a74-1f6f-4829-8530-fe359c77d35c  /** -----   vendor_account
   ActorIpAddress: 4.14.104.185                          /** -----   src, src_ip
   ApplicationId: c44b4083-3bb0-49c1-b47d-974e53cbdf3c
   AzureActiveDirectoryEventType: 1
   ClientIP: 4.14.104.185
   CreationTime: 2020-02-27T00:49:21
   ExtendedProperties: [ [-]
      { [-]
        Name: UserAgent
        Value: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/80.0.3987.116 Safari/537.36                       /** -----   user_agent
      }
      { [-]
        Name: FlowTokenScenario
        Value: Login
      }
      { [-]
        Name: UserAuthenticationMethod
        Value: 1                                          /** -----   authentication_method
      }
      { [-]
        Name: RequestType
        Value: Login:login
      }
      { [-]
        Name: ResultStatusDetail
        Value: Success
      }
   ]
   Id: 6c7bb43a-4fc5-403e-9e20-a1e6d4fdc7b3
   InterSystemsId: a2c96557-09ee-4be2-9d8a-a13c7326ff0e
   IntraSystemId: 4bc7a6ba-fabb-4bcc-9663-2a1be0a11a00
   ModifiedProperties: [ [-]
   ]
   ObjectId: 797f4846-ba00-4fd7-ba43-dac1f8f63013
   Operation: UserLoggedIn                               /** -----   signature
```

150

```
   OrganizationId: 2ed28a74-1f6f-4829-8530-fe359c77d35c
   RecordType: 15
   ResultStatus: Succeeded                      /** -----  action
   SupportTicketId:
   Target: [ [-]
     { [-]
       ID: 797f4846-ba00-4fd7-ba43-dac1f8f63013
       Type: 0
     }
   ]
   TargetContextId: 2ed28a74-1f6f-4829-8530-fe359c77d35c
   UserId: admin@a830edad9050849NDA3079.onmicrosoft.com
   UserKey: 10037FFE8EC1E08E@a830edad9050849NDA3079.onmicrosoft.com
   UserType: 0
   Version: 1
   Workload: AzureActiveDirectory
}
```

AWS success

A sample AWS successful user login follows:

Click **expand** or **collapse** to show or hide the example.

```
{
   additionalEventData: {
     LoginTo: https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true
     MFAUsed: No                              /** -----  authentication_method
     MobileVersion: No
   }
   awsRegion: us-east-1
   eventID: 040eb5f3-1132-4325-b06b-022e580c44fe
   eventName: ConsoleLogin                    /** -----  signature
   eventSource: signin.amazonaws.com
   eventTime: 2020-02-21T23:06:26Z
   eventType: AwsConsoleSignIn
   eventVersion: 1.05
   recipientAccountId: 772089552793
   requestParameters: null
   responseElements: {
     ConsoleLogin: Success                    /** -----  action
   }
   sourceIPAddress: 4.14.104.185              /** -----  src
   userAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/79.0.3945.130 Safari/537.36                        /** -----  user_agent
   userIdentity: {
     accountId: 772089552793                  /** -----  vendor_account
     arn: arn:aws:iam::772089552793:user/example_user
     principalId: AIDA3HRA7T6MUVQJRHPKV
     type: IAMUser
     userName: example_user                   /** -----  user_id, user, src_user
   }
}
```

Login success field mapping

Using the login success from GCP as a base sample, and comparing it to a similar event from MS o365 and AWS is a good way to see the similarities and differences per common CIM field names.

User id example data	Provider field name	CIM field name

151

	Provider field name	CIM field name
GCP `name@gmail.com`	actor.email	user_id
MS o365 • `df22f023-9e0f-4d78-bdd5-d496688af11e` • `admin@a830edad9050849NDA3079.onmicrosoft.com` • `10037FFE8EC1E08E`	Id	user_id
AWS `example_user`	userIdentity.userName	• user_id • user • src_user
Action example data	**Provider field name**	**CIM field name**
GCP `login_success`	events.name	action
MS o365 `Succeeded`	ResultStatus	action
AWS `Success`	responseElements.ConsoleLogin	action
Signature example data	**Provider field name**	**CIM field name**
GCP `login`	events.type	signature
MS o365 `UserLoggedIn`	Operation	signature
AWS `ConsoleLogin`	eventName	signature
Authentication method example data	**Provider field name**	**CIM field name**
GCP `password`	• multiValue • events.parameters.name.login_challenge_method	authentication_method
MS o365 `1`	UserAuthenticationMethod	authentication_method
AWS `No`	MFAUsed	authentication_method
Vendor account example data	**Provider field name**	**CIM field name**
GCP `C035c27ok`	id.customerId	vendor_account

```
      authenticationInfo": {
        "principalEmail": "example_user@gmail.com"              /** -----  user_id
      },
      "requestMetadata": {
        "callerIp": "2601:646:8400:b0:a991:7135:7879:6cea"      /** -----  src, src_ip
      },
      "serviceName": "login.googleapis.com",                    /** -----  app, dest
      "methodName": "google.login.LoginService.loginFailure",   /** -----  signature
      "resourceName": "organizations/809036120291",
      "metadata": {
```

User id example data	Provider field name	CIM field name

```
        "activityId": {
          "timeUsec": "1588189783734201",
          "uniqQualifier": "1023108278221"
        },
        "event": [
          {
            "eventType": "login",
            "eventName": "login_failure",
            "parameter": [
              {
                "name": "login_type",
                "value": "unknown",
                "label": "LABEL_OPTIONAL",
                "type": "TYPE_STRING"
              },
              {
                "name": "login_challenge_method",          /** -----  authentication_method
                "multiStrValue": [                          /** -----  reason
                  "password",
                  "password"
                ],
                "label": "LABEL_REPEATED",
                "type": "TYPE_STRING"
              },
              {
                "name": "dusi",
                "value": "IMyb8fehs77-gQE",
                "label": "LABEL_OPTIONAL",
                "type": "TYPE_STRING"
              }
            ]
          }
        ],
        "@type": "type.googleapis.com/ccc_hosted_reporting.ActivityProto"
      }
    },
    "insertId": "mh9fqkc4a2",
    "resource": {
      "type": "audited_resource",
      "labels": {
        "method": "google.login.LoginService.loginFailure",
        "service": "login.googleapis.com"
      }
    },
    "timestamp": "2020-04-29T19:49:43.734201Z",
    "severity": "NOTICE",                                 /** -----  action
    "logName": "organizations/809036120291/logs/cloudaudit.googleapis.com%2Fdata_access",
    "receiveTimestamp": "2020-04-29T20:43:00.836830467Z"
}
```

MS o365 failure

A sample MS o365 failed user login follows:

Click **expand** or **collapse** to show or hide the example.

```
{ [-]
   Actor: [ [-]
      { [-]
```

```
      ID: 1d48684f-70ea-41e7-8459-9a7a24a8690a
      Type: 0
    }
    { [-]
      ID: jc3@a830edad9050849NDA3079.onmicrosoft.com          /** -----  user_id
      Type: 5
    }
    { [-]
      ID: 10030000AEF912F2
      Type: 3
    }
  ]
  ActorContextId: 2ed28a74-1f6f-4829-8530-fe359c77d35c
  ActorIpAddress: 13.67.186.66
  ApplicationId: 00000002-0000-0ff1-ce00-000000000000
  AzureActiveDirectoryEventType: 1
  ClientIP: 13.67.186.66                                      /** -----  src_ip,  src
  CreationTime: 2020-02-27T07:46:00
  ExtendedProperties: [ [-]
    { [-]
      Name: UserAgent                                         /** -----  user_agent
      Value: python-requests/2.12.4
    }
    { [-]
      Name: RequestType
      Value: OrgIdWsTrust2:process
    }
    { [-]
      Name: ResultStatusDetail
      Value: UserError
    }
  ]
  Id: 8498834c-4ca4-4300-9351-099f917bd2e7
  InterSystemsId: 3f3bd815-8d38-48c8-aa71-445216d908de
  IntraSystemId: c3b22bc6-14c4-4b41-9aee-f4fb7f1e1000
  LogonError: InvalidUserNameOrPassword                       /** -----  reason
  ModifiedProperties: [ [-]
  ]
  ObjectId: Unknown
  Operation: UserLoginFailed                                  /** -----  signature
  OrganizationId: 2ed28a74-1f6f-4829-8530-fe359c77d35c        /** -----  vendor_account
  RecordType: 15
  ResultStatus: Failed                                        /** -----  action
  SupportTicketId:
  Target: [ [-]
    { [-]
      ID: Unknown
      Type: 0
    }
  ]
  TargetContextId: 2ed28a74-1f6f-4829-8530-fe359c77d35c
  UserId: jc3@a830edad9050849NDA3079.onmicrosoft.com          /** -----  user, user_id
  UserKey: 10030000AEF912F2@a830edad9050849NDA3079.onmicrosoft.com
  UserType: 0                                                 /** -----  user_type
  Version: 1
  Workload: AzureActiveDirectory                              /** -----  app
}
```

154

AWS failure

A sample AWS failed user login follows:

Click **expand** or **collapse** to show or hide the example.

```
{
  additionalEventData: {
    LoginTo: https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true
    MFAUsed: No                                            /** -----  authentication_method
    MobileVersion: No
  }
  awsRegion: us-east-1
  errorMessage: Failed authentication                      /** -----  reason
  eventID: 9c6005a8-def1-4075-a1b8-daba01c8150b
  eventName: ConsoleLogin                                  /** -----  signature
  eventSource: signin.amazonaws.com                        /** -----  app, dest
  eventTime: 2020-02-21T23:06:11Z
  eventType: AwsConsoleSignIn
  eventVersion: 1.05
  recipientAccountId: 772089552793
  requestParameters: null
  responseElements: {
    ConsoleLogin: Failure                                  /** -----  action
  }
  sourceIPAddress: 4.14.104.185                            /** -----  src
  userAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36     /** -----  user_agent
  userIdentity: {
    accessKeyId:
    accountId: 772089552793                                /** -----  vendor_account
    principalId: AIDA3HRA7T6MUVQJRHPKV
    type: IAMUser                                          /** -----  user_type
    userName: example_user                                 /** -----  user_id
  }
}
```

Login failure field mapping

Using the login failure from GCP as a base sample, and comparing it to a similar event from MS o365 and AWS is a good way to see the similarities and differences per common CIM field names.

User id example data	Provider field name	CIM field name
GCP example_user@gmail.com	protoPayload.authenticationInfo.principalEmail	user_id
MS o365 jc3@a830edad9050849NDA3079.onmicrosoft.com	UserId	user_id
AWS example_user	userIdentity.userName	user_id
User type example data	**Provider field name**	**CIM field name**
MS o365 0	UserType	user_type

155

User id example data	Provider field name	CIM field name
AWS `IAMUser`	userIdentity.type	user_type
App example data	**Provider field name**	**CIM field name**
GCP `login.googleapis.com`	protoPayload.serviceName	app
MS o365 `AzureActiveDirectory`	Workload	app
AWS `signin.amazonaws.com`	eventSource	app
Action example data	**Provider field name**	**CIM field name**
GCP `NOTICE`	severity	action
MS o365 `Failed`	ResultStatus	action
AWS `Failure`	responseElements.ConsoleLogin	action
Signature example data	**Provider field name**	**CIM field name**
GCP `google.login.LoginService.loginFailure`	protoPayload.methodName	signature
MS o365 `UserLoginFailed`	Operation	signature
AWS `ConsoleLogin`	eventName	signature
Authentication method example data	**Provider field name**	**CIM field name**
GCP `login_challenge_method`	events.parameters.name.login_challenge_method	authentication_method
AWS `No`	additionalEventData.MFAUsed	authentication_method
Vendor account example data	**Provider field name**	**CIM field name**
MS o365	OrganizationId	vendor_account

156

User id example data	Provider field name	CIM field name
2ed28a74-1f6f-4829-8530-fe359c77d35c		
AWS 772089552793	userIdentity.accountId	vendor_account
Source example data	**Provider field name**	**CIM field name**
GCP 2601:646:8400:b0:a991:7135:7879:6cea	requestMetadata.callerIp	• src • src_ip
MS o365 13.67.186.66	ClientIP	• src • src_ip
AWS 4.14.104.185	sourceIPAddress	src
Reason example data	**Provider field name**	**CIM field name**
GCP password	event.parameter.multiStrValue	reason
MS o365 InvalidUserNameOrPassword	LogonError	reason
AWS Failed authentication	errorMessage	reason
User agent data	**Provider field name**	**CIM field name**
MS o365 python-requests/2.12.4	UserAgent	user_agent
AWS Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.130 Safari/537.36	userAgent	user_agent

Privilege escalation example

The privilege escalation event from AWS is a good way to see a common event and how a cloud provider maps to CIM data model field names.

Privilege escalations include scenarios such as when a user, app, or agent logs in with one set of privileges, and then assumes a new set of privileges (such as `sudo su -` or short-lived credentials for service accounts).

AWS privilege escalation

A sample AssumeRoleWithSAML follows:

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": "SAMLUser",
        "principalId": "g4RD/xcF3dcnEghdegAhfaPo+ow=:example_user@aws.com",
        "userName": "example_user@aws.com",              /** -----   src_user
        "identityProvider": "g4RD/xcF3dcnEghdegAhfaPo+ow="
    },
    "eventTime": "2020-03-02T20:25:30Z",
    "eventSource": "sts.amazonaws.com",                   /** -----   app, dest
    "eventName": "AssumeRoleWithSAML",                    /** -----   signature
    "awsRegion": "us-east-1",
    "sourceIPAddress": "12.26.0.2",
    "userAgent": "aws-sdk-go/2.0.0-preview.2 (go1.9.6; darwin; amd64)",
    "requestParameters": {
        "sAMLAssertionID": "id29525874074479896480891647",
        "roleSessionName": "example_user@aws.com",
        "durationSeconds": 43200,
        "roleArn": "arn:aws:iam::671568874969:role/splunkcloud_account_metadata_read",
        "principalArn": "arn:aws:iam::671568874969:saml-provider/SplunkcloudOkta"
    },
    "responseElements": {
        "subjectType": "unspecified",
        "issuer": "http://www.okta.com/exksfwc0mwQGJQoJ62p6",
        "credentials": {
            "accessKeyId": "ASIAZYXE7ZXMXCVFRGMO",
            "expiration": "Mar 3, 2020 8:25:30 AM",
            "sessionToken":
"FwoGZXIvYXdzEG4aDKrC390jc4wlJW7kpyLnAWpYPA0uT1YdeIogg1iol1J0mdHQkIy1QmETyBa8o8KWXP7ptMeilV1UiPmtPQppTu0iXsMOp
UM25WOaPioornDWpHwY3ieOhJl1gVODA9cjlLu3pH8j9q4nFXxelkhieBdguExhUslmDSmGLoI94IPOn27bISDZW8vRJwnj9
/7WupIM6g4zOOipstGNbWfgTE4
/6fkc4HRxdrfS5c1c7ijFxfSaCoT134vhEA1xxhrKLn896ydbFuiIcxsYggDBe886NHKY+DNq1aYPKEiTrJKfWDLLs97sq0ZTi79fOW7arjtNccyKqyi
        },
        "nameQualifier": "g4RD/xcF3dcnEghdegAhfaPo+ow=",
        "assumedRoleUser": {
            "assumedRoleId": "AROAIDCBHGVCTRIEIG2X2:example_user@aws.com",
            "arn":
"arn:aws:sts::671568874969:assumed-role/splunkcloud_account_metadata_read/example_user@aws.com"  /** -----
 user
        },
        "subject": "example_user@aws.com",
        "audience": "https://signin.aws.amazon.com/saml"
    },
    "requestID": "7c7ac23a-fc2d-4c76-976e-8e2b40073d7d",
    "eventID": "84dd288a-bdc0-4708-ad61-cde4f45dcc64",
    "resources": [
        {
            "ARN": "arn:aws:iam::671568874969:role/splunkcloud_account_metadata_read",
            "accountId": "671568874969",
            "type": "AWS::IAM::Role"
        },
        {
            "ARN": "arn:aws:iam::671568874969:saml-provider/SplunkcloudOkta",
            "accountId": "671568874969",
            "type": "AWS::IAM::SAMLProvider"
        }
    ],
    "eventType": "AwsApiCall",
    "recipientAccountId": "671568874969"
}
```

GCP short-lived credentials

A sample GCP short-lived credentials follows:

```
{
  "logName": "projects/my-project/logs/cloudaudit.googleapis.com%2Fdata_access",
  "protoPayload": {
    "@type": "type.googleapis.com/google.cloud.audit.AuditLog",
    "authenticationInfo": {
      "principalEmail": "example_user@gmail.com"                    /** -----  src_user
    },
    "methodName": "GenerateAccessToken",                           /** -----  signature
    "request": {
      "@type": "type.googleapis.com/google.iam.credentials.v1.GenerateAccessTokenRequest",
      "name": "projects/-/serviceAccounts/my-service-account@my-project.iam.gserviceaccount.com"
    },
    "serviceName": "iamcredentials.googleapis.com"                 /** -----  app, dest
  },
  "resource": {
    "labels": {
      "email_id": "my-service-account@my-project.iam.gserviceaccount.com",  /** -----  user
      "project_id": "my-project",                                  /** -----  vendor_account
      "unique_id": "123456789012345678901"
    },
    "type": "service_account"
  }
}
```

Privilege escalation field mapping

Using the privilege escalation from AWS as a base sample is a good way to see the similarities and differences per common CIM field names.

Vendor account example data	Provider fiel
AWS `671568874969`	userIdentity.accountId
GCP `my-project`	resource.labels.project_id
Source user example data	**Provider fiel**
AWS `example_user@aws.com`	userIdentity.userName
GCP `example_user@gmail.com`	protoPayload.authenticatio
App, dest example data	**Provider fiel**
AWS	eventSource

159

Vendor account example data	Provider fiel
`sts.amazonaws.com`	
GCP	protoPayload.serviceName
`iamcredentials.googleapis.com`	

Signature example data	Provider fiel
AWS	eventName
`AssumeRoleWithSAML`	
GCP	protoPayload.methodName
`GenerateAccessToken`	

User example data	Provider fiel
AWS	assumedRoleUser.arn
`arn:aws:sts::671568874969:assumed-role/splunkcloud_account_metadata_read/example_user@aws.com`	
GCP	resource.labels.email_id
`my-service-account@my-project.iam.gserviceaccount.com`	

Change Field Mapping

The following shows an example of how change events map differently from various cloud providers to CIM data model field names.

See the Change data model for full field descriptions.

Update user example

The update user event from Amazon Web Services (AWS) and Azure is a good way to see a common event and how each cloud provider maps to CIM data model field names. An example case is where an admin creates or updates an IAMUser. The admin is the source user and source type.

AWS update user

A sample AWS update user action follows:

Click **expand** or **collapse** to show or hide the example.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",                      /** -----  user_type, src_user_type
    "principalId": "AIDA3HRA7T6MUVQJRHPKV", /** -----  user, user_id
    "arn": "arn:aws:iam::772089552793:user/example_name",
    "accountId": "772089552793",            /** -----  vendor_account
```

```
    "accessKeyId": "AKIA3HRA7T6MVC4EBVOG",
    "userName": "example_name"                 /** ----- user_name
  },
  "eventTime": "2020-06-25T16:56:12Z",
  "eventSource": "iam.amazonaws.com",          /** ----- app, dest
  "eventName": "UpdateUser",                    /** ----- action, command
  "awsRegion": "us-east-1",
  "sourceIPAddress": "72.83.94.230",            /** ----- src, src_ip
  "userAgent": "aws-cli/2.0.0 Python/3.7.4 Darwin/19.5.0 botocore/2.0.0dev4", /** -----  user_agent
  "requestParameters": {                        /** ----- object, object_attrs, object_category, object_id,
object_path
    "userName": "user_change_dm",
    "newUserName": "user_change"
  },
  "responseElements": null,
  "requestID": "7e371c54-8df7-4f1f-b3b8-03d1298a52fd",
  "eventID": "74f66cee-7fe3-48f1-97ee-9c59efc40a5f",
  "eventType": "AwsApiCall",
  "recipientAccountId": "772089552793"
}
```

Azure update user

A sample Azure update user action follows:

Click **expand** or **collapse** to show or hide the example.

```
{
  "id": "Directory_5c4d6b97-3e18-4565-ad44-3c20ee2c70ab_1CKOF_99617149",
  "category": "UserManagement",                 /** ----- object_category
  "correlationId": "5c4d6b97-3e18-4565-ad44-3c20ee2c70ab",
  "result": "success",                          /** ----- status
  "resultReason": "",                           /** ----- result
  "activityDisplayName": "Disable Strong Authentication", /** -----  command
  "activityDateTime": "2020-06-11T23:07:51.971036Z",
  "loggedByService": "Core Directory",          /** ----- dest, dvc
  "operationType": "Update",                    /** ----- action
  "initiatedBy": {
    "app": null,
    "user": {
      "id": "df22f023-9e0f-4d78-bdd5-d496688af11e",
      "displayName": null,
      "userPrincipalName": "admin@a830edad9050849NDA3079.onmicrosoft.com",  /** -----  src_user
      "ipAddress": null,
      "userType": null
    }
  },
  "targetResources": [
    {
      "id": "93a565f6-d0fc-4ac3-9d2a-8c1de9aeed3c", /** -----  object_id
      "displayName": null,
      "type": "User",                           /** ----- change_type, object_category
      "userPrincipalName": "es_csm_change_model@a830edad9050849nda3079.onmicrosoft.com",  /** -----  user,
user_id
      "groupType": null,
      "modifiedProperties": [
        {
          "displayName": "StrongAuthenticationRequirement",
          "oldValue":
"[{\"RelyingParty\":\"*\",\"State\":1,\"RememberDevicesNotIssuedBefore\":\"2020-06-11T23:07:35+00:00\"}]",
          "newValue": "[]"
```

```
      },
      {
        "displayName": "Included Updated Properties",
        "oldValue": null,
        "newValue": "\"StrongAuthenticationRequirement\"" /** -----  object_attrs
      }
    ]
  }
  ],
  "additionalDetails": []
}
```
User update field mapping

Using the user update from AWS as a base sample, and comparing it to a similar event from Azure is a good way to see the similarities and differences per common CIM field names.

User example data	Provider field name	CIM field name
AWS `AIDA3HRA7T6MUVQJRHPKV`	userIdentity.principalId	• user • user_id
Azure `es_csm_change_model@a830edad9050849nda3079.onmicrosoft.com`	targetResources.userPrincipalName	• user • user_id
Destination example data	**Provider field name**	**CIM field name**
AWS `iam.amazonaws.com`	eventSource	• app • dest
Azure `Core Directory`	loggedByService	• dest • dvc
Action example data	**Provider field name**	**CIM field name**
AWS `UpdateUser`	eventName	• action • command
Azure `Update`	operationType	action
Object example data	**Provider field name**	**CIM field name**

AWS
`"requestParameters": {`
`    "userName": "user_change_dm",`
`    "newUserName": "user_change"`
`  },`
	requestParameters	• object
		• object_attrs
		• object_category
		• object_id
		• object_path

Azure `UserManagement`	category	object_category
Azure	targetResources.id	object_id

User example data	Provider field name	CIM field name
`93a565f6-d0fc-4ac3-9d2a-8c1de9aeed3c`		
Azure `"StrongAuthenticationRequirement\"`	targetResources.modifiedProperties	object_attrs

Reboot example

The login success event from Amazon Web Services (AWS) and Azure is a good way to see a common event and how each cloud provider maps to CIM data model field names.

AWS EC2 instance reboot

A sample AWS EC2 instance reboot action follows:

Click **expand** or **collapse** to show or hide the example.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",                         /** -----  user_type, src_user_type
    "principalId": "AIDA3HRA7T6MRJYJZSGXO",    /** -----  user, user_id
    "arn": "arn:aws:iam::772089552793:user/example_name",
    "accountId": "772089552793",              /** -----  vendor_account
    "accessKeyId": "ASIA3HRA7T6MR2NXOREA",
    "userName": "example_name",               /** -----  user_name
    "sessionContext": {
      "sessionIssuer": {},
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2020-06-08T21:51:29Z"
      }
    }
  },
  "eventTime": "2020-06-09T01:05:55Z",
  "eventSource": "ec2.amazonaws.com",         /** -----  app, dest
  "eventName": "RebootInstances",             /** -----  action, command
  "awsRegion": "us-east-2",                   /** -----  vendor_region
  "sourceIPAddress": "73.162.147.20",         /** -----  src, src_ip
  "userAgent": "console.ec2.amazonaws.com",   /** -----  user_agent
  "requestParameters": {                      /** -----  object, object_attrs, object_category,
object_id, object_path
    "instancesSet": {
      "items": [
        {
          "instanceId": "i-09b1f332093983cc1"
        }
      ]
    }
  },
  "responseElements": {
    "requestId": "b09c7d96-645e-45db-aa6f-e09c32ad076e",
    "_return": true
  },
  "requestID": "b09c7d96-645e-45db-aa6f-e09c32ad076e",
  "eventID": "43a8628d-5fc7-42f7-8666-b71664cefbac",
```

163

```
    "eventType": "AwsApiCall",
    "recipientAccountId": "772089552793"
}
```

Azure virtual machine reboot

A sample Azure virtual machine reboot action follows:

Click **expand** or **collapse** to show or hide the example.

```
{
  "time": "2020-06-18T22:31:41.7234475Z",
  "resourceId":
"/SUBSCRIPTIONS/AE4AB7C9-DCDF-4427-9729-48E8C7551BE9/RESOURCEGROUPS/ES_CSM_CHANGE_MODEL/PROVIDERS/MICROSOFT.COMPUTE
/VIRTUALMACHINES/ES-CSM-CHNAGE-VM-1",                            /** -----  object_id, object, app,
object_category
  "operationName": "MICROSOFT.COMPUTE/VIRTUALMACHINES/RESTART/ACTION",    /** -----  app, dest
  "category": "Administrative",
  "resultType": "Success",
  "resultSignature": "Succeeded.",                              /** -----  status
  "durationMs": 0,
  "callerIpAddress": "174.62.106.48",
  "correlationId": "3cdcca7c-a98c-46b6-b3f9-9ce2d27c5fe4",
  "identity": {
    "authorization": {
      "scope":
"/subscriptions/ae4ab7c9-dcdf-4427-9729-48e8c7551be9/resourceGroups/es_csm_change_model/providers/Microsoft.Compute
/virtualMachines/es-csm-chnage-vm-1",
      "action": "Microsoft.Compute/virtualMachines/restart/action",       /** -----  action, command
      "evidence": {
        "role": "Contributor",
        "roleAssignmentScope": "/subscriptions/ae4ab7c9-dcdf-4427-9729-48e8c7551be9",
        "roleAssignmentId": "8eb22423e5cc461592fda56f5b5dc2aa",
        "roleDefinitionId": "b24988ac618042a0ab8820f7382dd24c",
        "principalId": "149ec7a11f3a4878a1d558f4a1e67655",
        "principalType": "User"
      }
    },
    "claims": {
      "aud": "https://management.core.windows.net/",
      "iss": "https://sts.windows.net/2ed28a74-1f6f-4829-8530-fe359c77d35c/",
      "iat": "1592517408",
      "nbf": "1592517408",
      "exp": "1592521308",
      "http://schemas.microsoft.com/claims/authnclassreference": "1",
      "aio": "ATQAy/8PAAAAtikpFkPjCTjg0x5DI7ch1Ki6e2TVeKzmZrn2OnJ5GchOOfM/PN7RfBss5uGIecXp",
      "http://schemas.microsoft.com/claims/authnmethodsreferences": "pwd",
      "appid": "c44b4083-3bb0-49c1-b47d-974e53cbdf3c",
      "appidacr": "2",
      "ipaddr": "174.62.106.48",                                /** -----  src, src_ip

      "name": "Example_Name",
      "http://schemas.microsoft.com/identity/claims/objectidentifier":
"149ec7a1-1f3a-4878-a1d5-58f4a1e67655",
      "puid": "10032000C9954D8E",
      "http://schemas.microsoft.com/identity/claims/scope": "user_impersonation",
      "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier":
"nZAgSAB9HehKWTDa3J1iIqTLWNzipERZJYScR7qzot4",
      "http://schemas.microsoft.com/identity/claims/tenantid": "2ed28a74-1f6f-4829-8530-fe359c77d35c",
      "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name":
"admin@a830edad9050849nda3079.onmicrosoft.com", /** -----  user_id
```

```
      "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn":
"admin@a830edad9050849nda3079.onmicrosoft.com",
      "uti": "Ka0FzSYrf02er9SWaHN9AA",
      "ver": "1.0"
    }
  },
  "level": "Information",
  "properties": {
    "category": "Administrative"
  }
}
```

Reboot field mapping

Using the reboot from AWS as a base sample, and comparing it to a similar event from Azure is a good way to see the similarities and differences per common CIM field names.

User example data	
AWS AIDA3HRA7T6MRJYJZSGXO	userIdentity.principalId
Azure admin@a830edad9050849nda3079.onmicrosoft.com	identity.claims.http://sch
User type example data	
AWS IAMUser	userIdentity.type
Azure n/a	n/a
Destination example data	
AWS ec2.amazonaws.com	eventSource
Azure Microsoft.Compute	operationName
Action example data	
AWS RebootInstances	eventName
Azure MICROSOFT.COMPUTE/VIRTUALMACHINES/RESTART/ACTION	operationName
Source example data	
AWS 73.162.147.20	sourceIPAddress

User example data	
Azure 174.62.106.48	claims.ipaddr
Object example data	

AWS
``
"requestParameters": {
        "force": false,
        "instancesSet": {
        "items": [{
                "instanceId": "i-c103dcc9"
                }]
            }
},
``
	requestParameters

Azure /SUBSCRIPTIONS/AE4AB7C9-DCDF-4427-9729-48E8C7551BE9/RESOURCEGROUPS/ES_CSM_CHANGE_MODEL/PROVIDERS /MICROSOFT.COMPUTE/VIRTUALMACHINES/ES-CSM-CHNAGE-VM-1	resourceId

Network Traffic Field Mapping

The following shows an example of how network traffic events map differently from various cloud providers to CIM data model field names.

See the Network Traffic data model for full field descriptions.

Source flow example

The source flow event from Google Cloud Platform (GCP) and Amazon Web Services (AWS) is a good way to see a common event and how each cloud provider maps to CIM data model field names.

GCP source flow

A sample GCP source flow follows:

Click **expand** or **collapse** to show or hide the example.

```
{
   "resource":{
      "labels":{
         "subnetwork_id":"4884528796030499819",
         "subnetwork_name":"default",
         "location":"us-central1-c",
         "project_id":"gsa-project-151018"
      },
      "type":"gce_subnetwork"
   },
   "timestamp":"2020-05-13T18:10:27.15490124Z",
   "jsonPayload":{
      "src_vpc":{
         "subnetwork_name":"default",
```

```
          "vpc_name":"default",
          "project_id":"gsa-project-151018"
      },
      "dest_location":{
          "country":"usa",gce_subnetwork
          "asn":15169,
          "continent":"America"
      },
      "src_instance":{
          "region":"us-central1",
          "vm_name":"gke-cluster-1-default-pool-cc3d3622-09nt",
          "zone":"us-central1-c",
          "project_id":"gsa-project-151018"          /** -----  vendor_account
      },
      "start_time":"2020-05-13T18:10:22.594437852Z", /** -----  duration start time
      "rtt_msec":"0",                                /** -----  response_time
      "bytes_sent":"5300",                           /** -----  bytes_out, bytes_in, bytes
      "reporter":"SRC",                              /** -----  direction
      "packets_sent":"40",                           /** -----  packets_out, packets_in, packets
      "end_time":"2020-05-13T18:10:22.614528620Z",   /** -----  duration end time
      "connection":{
          "protocol":6,                              /** -----  transport
          "src_port":44114,                          /** -----  src_port
          "dest_ip":"173.255.116.127",               /** -----  dest_ip, dest, dvc
          "src_ip":"10.128.15.212",                  /** -----  src_ip, src, dvc
          "dest_port":443                            /** -----  dest_port
      }
  },
  "insertId":"atlo5sg16t94yf",
  "logName":"projects/gsa-project-151018/logs/compute.googleapis.com%2Fvpc_flows",
  "receiveTimestamp":"2020-05-13T18:10:27.15490124Z"
}
```

AWS source flow

A sample AWS source flow follows:

Click **expand** or **collapse** to show or hide the example.

```
2
772089552793          /** -----  account-id
eni-099b0af8dd18f05bd /** -----  dvc
103.137.144.25        /** -----  src_ip, src
103.137.144.26        /** -----  dest_ip, dest
443                   /** -----  src_port
22271                 /** -----  dest_port
6                     /** -----  transport
19                    /** -----  packets
10984                 /** -----  bytes
1589294114            /** -----  duration
1589294114            /** -----  duration
ACCEPT
OK
```

Source flow field mapping

Using the login success from GCP as a base sample, and comparing it to a similar event from AWS is a good way to see the similarities and differences per common CIM field names.

Source example data	Provider field name	CIM field name

	Provider field name	CIM field name
GCP `10.128.15.212`	data.jsonPayload.connection.src_ip	• src_ip • src • dvc if reporter=SRC
AWS `103.137.144.25`	srcaddr	• src_ip • src
Device example data	**Provider field name**	**CIM field name**
GCP `10.128.15.212`	data.jsonPayload.connection.src_ip	dvc if reporter=SRC
AWS `eni-099b0af8dd18f05bd`	interface-id	dvc
Source port example data	**Provider field name**	**CIM field name**
GCP `44114`	data.jsonPayload.connection.src_port	src_port
AWS `443`	srcport	src_port
Destination example data	**Provider field name**	**CIM field name**
GCP `173.255.116.127`	data.jsonPayload.connection.dest_ip	• dest_ip • dest • dvc if reporter=DEST
AWS `103.137.144.26`	dstaddr	• dest • dest_ip
Destination port example data	**Provider field name**	**CIM field name**
GCP `443`	data.jsonPayload.connection.dest_port	dest_port
AWS `22271`	dstport	dest_port
Transport example data	**Provider field name**	**CIM field name**
GCP `6`	data.jsonPayload.connection.protocol	transport
AWS `6`	protocol	transport
Duration start time example data	**Provider field name**	**CIM field name**

Source example data	Provider field name	CIM field name
GCP `2020-05-13T18:10:22.594437852Z`	data.jsonPayload.start_time	duration, calculated from start_time and end_time
AWS `1589294114`	start	duration, calculated from start_time and end_time
Duration end time example data	**Provider field name**	**CIM field name**
GCP `2020-05-13T18:10:22.614528620Z`	data.jsonPayload.end_time	duration, calculated from start_time and end_time
AWS `1589294114`	end	duration, calculated from start_time and end_time
Bytes example data	**Provider field name**	**CIM field name**
GCP `5300`	data.jsonPayload.bytes_sent	• bytes_out if reporter=SRC • bytes_in • bytes
AWS `10984`	bytes	bytes
Packets example data	**Provider field name**	**CIM field name**
GCP `40`	data.jsonPayload.packets_sent	• packets_out if reporter=SRC • packets_in • packets
AWS `19`	packets	packets
Direction example data	**Provider field name**	**CIM field name**
GCP `SRC`	data.jsonPayload.reporter	direction
AWS n/a	n/a	n/a
Vendor account example data	**Provider field name**	**CIM field name**
GCP `gsa-project-151018`	data.jsonPayload.src_instance.project_id	vendor_account if reporter=SRC
AWS `772089552793`	account-id	vendor_account

Data Access Field Mapping

The following shows an example of how data access events map differently from various cloud providers to CIM data model field names.

See the Data Access data model for full field descriptions.

File upload success example

The file upload success event from Google Drive and Box is a good way to see a common event and how each cloud provider maps to CIM data model field names.

Google Drive upload success

A sample Google Drive user successfully uploading a file follows:

Click **expand** or **collapse** to show or hide the example.

```
{
  "kind": "admin#reports#activity",
  "id": {
    "time": "2021-01-27T20:55:22.553Z",
    "uniqueQualifier": "-5126288301746458201",
    "applicationName": "drive",                    /** -----  app, dest_name, vendor_product, dvc
    "customerId": "C01yel9ht"                      /** -----   tenant_id
  },
  "etag": "\"fhmPGI5aiiS0KGD55zBI3n4f0Di-XQVRRMmqt75xUJc/Qtt_cFE351_xxWrZD43B_hFtj7I\"",
  "actor": {
    "email": "name@example.com",                   /** -----  email, user
    "profileId": "110778908138668363959"           /** -----  user_id
  },
  "ipAddress": "96.231.134.130",                    /** -----  src
  "events": [
    {
      "type": "access",
      "name": "upload",                            /** -----  action
      "parameters": [
        {
          "name": "primary_event",
          "boolValue": true
        },
        {
          "name": "billable",
          "boolValue": true
        },
        {
          "name": "doc_id",                        /** -----  object_id
          "value": "1s2ww0PVPGuuKXAzdjg6jGgmZtcxGchH7"
        },
        {
          "name": "doc_type",                      /** -----  object_type
          "value": "unknown"
        },
        {
```

```
        "name": "doc_title",                          /** ----- object
        "value": "quickstart.py"
      },
      {
        "name": "visibility",
        "value": "private"
      },
      {
        "name": "originating_app_id",
        "value": "691301496089"
      },
      {
        "name": "actor_is_collaborator_account",        /** ----- user_role
        "boolValue": false
      },
      {
        "name": "owner",                              /** ----- owner
        "value": "name@example.com"
      },
      {
        "name": "owner_is_shared_drive",
        "boolValue": false
      },
      {
        "name": "owner_is_team_drive",
        "boolValue": false
      }
    ]
  }
    ]
  }
  ]
}
```

Box upload success

A sample Box user successfully uploading a file follows:

Click **expand** or **collapse** to show or hide the example.

```
source_item_type="file",                                              /** -----  object_type
source_item_id="782729174962",                                        /** -----  object_id
source_item_name="Consolidated Quarter-VII-IV Schedule -
    Participants.xlsx",                                               /** -----  object
source_parent_type="folder",
source_parent_name="Test",
source_parent_id="132755355986",
source_owned_by_type="user",
source_owned_by_id="15230886095",                                     /** -----  owner_id
source_owned_by_name="Example Name",                                  /** -----  owner
source_owned_by_login="name@example.com",                             /** -----  owner_email
created_by_type="user",
created_by_id="15230886095",                                          /** -----  user_id
created_by_name="Example Name",                                       /** -----  user
created_by_login="name@example.com",                                  /** -----  email
action_by="",
created_at="2021-03-03T10:10:40-08:00",
event_id="30fe6b3e-41ea-40a5-894d-38c575c0be5f",
event_type="UPLOAD",                                                  /** -----  action
ip_address="103.226.185.0",                                           /** -----  src
type="event",
```

```
session_id="",
additional_details_size="22564",                                        /** -----  object_size
additional_details_ekm_id="b03b4375-03c9-4c03-9559-9cedddab801d",
additional_details_version_id="836198952562",
additional_details_service_id="231318",
additional_details_service_name="Multiput Uploads",
account_id=15230886095                                                   /** -----  user_id
```

Upload field mapping

Using the file upload success from Google Drive as a base sample, and comparing it to a similar event from Box is a good way to see the similarities and differences per common CIM field names.

Source example data	Provider field name	CIM field name
Google Drive `name@example.com`	actor.email	• email • user
Box `name@example.com`	created_by_login	email
Device example data	**Provider field name**	**CIM field name**
Google Drive `name@example.com`	actor.email	• email • user
Box `Example Name`	created_by_name	user
Device example data	**Provider field name**	**CIM field name**
Google Drive `110778908138668363959`	actor. profileId	user_id
Box `15230886095`	• created_by_id • account_id	user_id
Device example data	**Provider field name**	**CIM field name**
Google Drive `96.231.134.130`	ipAddress	src
Box `103.226.185.0`	ip_address	src
Device example data	**Provider field name**	**CIM field name**
Google Drive `upload`	name	action
Box `UPLOAD`	event_type	action

172

Source example data	Provider field name	CIM field name
Device example data	**Provider field name**	**CIM field name**
Google Drive `1s2ww0PVPGuuKXAzdjg6jGgmZtcxGchH7`	"name": "doc_id"	object_id
Box `782729174962`	source_item_id	object_id
Device example data	**Provider field name**	**CIM field name**
Google Drive `unknown`	"name": "doc_type"	object_type
Box `file`	source_item_type	object_type
Device example data	**Provider field name**	**CIM field name**
Google Drive `quickstart.py`	"name": "doc_title"	object
Box `Consolidated Quarter-VII-IV Schedule – Participants.xlsx`	source_item_name	object
Device example data	**Provider field name**	**CIM field name**
Google Drive `name@example.com`	"name": "owner"	owner
Box `Example Name`	source_owned_by_name	owner

Additional Normalizations

ITSI Normalization

The following table describes field and field definitions in support of Universal Alerting in ITSI. See the details About the Content Pack for Monitoring and Alerting in *Splunk ITSI Content Packs*.

The key for using the column titled "Abbreviated list of example values" follows. It is relevant for TA developers and ITSI implementors such as customers, SEs, and PSEs:

- **Required**: Required Fields must be included.
- **Recommended**: Recommended Fields are helpful, but the Universal Correlation Search does not require them.
- **Optional**: Optional Fields are available for more advanced integrations, such as providing drilldowns.

Field name	Data type	Description	Abbreviated list of example values
app	string	The system, service, or application that generated the alert event. Examples include "Nagios Host", "Solarwinds", "Splunk Infra Mon".	recommended for ITSI
description	string	The description of the alert event. Adds more detail to the `signature` field.	recommended for ITSI
entity_name	string	Used for the 'Entity Lookup Field' in the Universal Correlation Search. Default is `<src>`.	optional for ITSI
itsiDrilldownSearch	string	SPL to drill down into the details of this alert. Default is `"index=* signature="<signature>" src="<src>"`.	optional for ITSI
itsiDrilldownURI	string	External link for this alert, such as "https://bakookanet.com/alerts&alertid=1234567".	optional for ITSI
itsiDrilldownWeb	string	Optional Name for the link included in `itsiDrilldownURI`. Default is "External Drilldown for <itsiNotableTitle>"	optional for ITSI
itsiInclude	string	Boolean indicating whether this alert is automatically brought into ITSI as a Notable Event. If absent, ITSI assumes `itsiInclude="true"`. If `itsiInclude="false"`, ITSI does not onboard the alert. This is useful for testing or for specifically selecting which raw alerts to onboard as Notable Events.	recommended for ITSI
itsi_instruction	string	Text or markdown instructions for a human on how to handle this type of alert; can handle a link if encoded as markdown. See https://www.markdownguide.org.	optional for ITSI
itsiNotableTitle	string	Specifies which fields the Notable Event Title includes. Default is `"<signature> - <src> (<subcomponent>)"`.	optional for ITSI
severity_id	string	The numeric or vendor-specific severity indicator corresponding to the event severity. For ITSI, `severity_id` is one of the following values: 1 = Info or Unknown 2 = Normal or Cleared 3 = Low 4 = Medium 5 = High 6 = Critical	required for ITSI

Field name	Data type	Description	Abbreviated list of example values
signature	string	The human-friendly title of the alert event, such as 'Device Not Responding,' 'Disk Full,' or 'CPU usage too high.'	required for ITSI
src	string	The object that is the target, host, or object of the alert event. You can **alias** this field from existing fields such as src_host, src_ip, or src_name.	required for ITSI
subcomponent	string	Sub-component object for this alert. Further defines the src field. For example, for a "Filesystem Full" alert on "server42" for "/var": • signature = "Filesystem Full" • src = "server42" • subcomponent = "/var" Most alerts will not have a sub-component object. However, if the alert does contain a sub-component object, you must include this field.	recommended for ITSI
vendor_severity	string	The original vendor-specific severity/health/status string for this alert, such as up/down/ok/normal/critical/warning/red/green/minor/major.	required by ITSI