Splunk® App for Infrastructure Use Splunk App for Infrastructure 1.2.2

Generated: 2/06/2019 11:14 am
# Table of Contents

## Getting started
- About Splunk App for Infrastructure .......................................................... 1
- Get started using Splunk App for Infrastructure ........................................ 4

## Monitor and investigate
- Monitor Entity Health with Splunk App for Infrastructure .......................... 6
- Analyze Entities and Groups with Splunk App for Infrastructure ................ 7

## Alerts and notifications
- Monitor and investigate alerts in Splunk App for Infrastructure ................... 9

## Use cases
- Monitor CPU usage using Splunk App for Infrastructure ............................ 13
- Monitor CPU resource utilization using Splunk App for Infrastructure .......... 16

## Videos
- Videos for how to use Splunk App for Infrastructure ................................. 21

## Toolkit
- Using the Infrastructure Overview in Splunk App for Infrastructure ............. 23
- Using the List View in Splunk App for Infrastructure ................................. 25
- Using the Analysis Workspace in Splunk App for Infrastructure ................. 26
- Using the Entity Overview in Splunk App for Infrastructure ........................ 31
- About Analytics in the Analysis Workspace in Splunk App for Infrastructure .. 33
- Using Groups in Splunk App for Infrastructure ........................................ 40
- Glossary of terms for Splunk App for Infrastructure .................................. 43

## Support
- Support for Splunk App for Infrastructure ............................................... 44
Getting started

About Splunk App for Infrastructure

Splunk App for Infrastructure is a tool that provides insight into the performance of Linux servers, Microsoft Windows servers, and Amazon EC2, ELB and EBS instances. Splunk App for Infrastructure utilizes metrics for performance monitoring, and log data for deep understanding and troubleshooting of your server infrastructure.

For a video overview of Splunk App for Infrastructure, see Video: Introducing Splunk App for Infrastructure.

Core Features

Splunk App for Infrastructure provides everything you need for deploying metric and log data collection, entity discovery, server monitoring, and performance analysis and troubleshooting. The Insight has the following primary sections.

- The Add Data view gets you started with data collection. From this view you can set up data collection on Linux, Windows, and Mac OS X servers for both system metrics and logs. You can also create accounts for polling critical performance metrics for your Amazon EC2, ELB and EBS entities. See How to add data to Splunk App for Infrastructure below.
- The Investigate views allow you to browse a list of discovered entities, create groups using entity metadata, view the Entity Overview to monitor the health of an entity, link to Group and Entity Analysis Workspaces for deeper insight, and view all of your server entities as tiles in the Infrastructure Overview. See Investigate Your Infrastructure below.
- The Alerts view displays the most recent 100 triggered alert conditions. From this view you can drill down into the Entity Analysis Workspace to perform root cause analysis on a particular alert. See View and Manage Alerts below.

Investigate Your Infrastructure

Use the Investigate views, including the Infrastructure Overview, List View, and Analysis Workspace to monitor your infrastructure.
Investigate the Infrastructure Overview

Monitor the health of your system using the **Infrastructure Overview**. This view is used to quickly understand availability and performance of your server infrastructure. You can choose a specific performance metric and set a threshold to better understand your high and low performing systems. From this view you can access quick information including hostname and IP address, as well as drill down into the Analysis Workspace for a specific server where you can continue to analyze and understand server performance. For more information, see Using the Infrastructure Overview in Splunk App for Infrastructure.

---

**Investigate the List View**

Use the **List View** to view your entities or groups, their status as active or inactive, and sort them by dimensions. You can also drill down into the Analysis Workspace of an entity or group being monitored to review details or troubleshoot an issue. For more information, see Using the List View in Splunk App for Infrastructure.
**Investigate the Entity Overview**

Use the Entity Overview to view performance charts that give a quick view of the performance of Infrastructure entities. From this overview, get a summary of metrics being used by the entity, such as CPU, network, memory, disk, system information, dimensions and more. For more information, see Monitor Entity Health with Splunk App for Infrastructure and Using the Entity Overview in Splunk App for Infrastructure.

**Investigate the Analysis Workspace**

Use the Analysis Workspace to analyze performance metrics for a single entity or a group of entities. Determine poor performing entities by metrics, or determine a point in time when multiple entities began performing in a similar way. Create alert conditions and search logs collected from your servers to perform root cause analysis and understand why your infrastructure is performing the way it is. View and search for entities in a group, or view all groups an entity is a part of for easy navigation. For more information, see Analyze Entities and Groups with Splunk App for Infrastructure and Using the Analysis Workspace in Splunk App for Infrastructure.
View and Manage Alerts

Admin privileges are required to create and manage alerts.

Use Alerts to monitor triggered events and perform root cause analysis. The Alerts page displays a list of the last 100 triggered alerts. From here you can link to the Analysis Workspace, where you can continue to investigate performance issues during the time of the alert, modify or delete the alert condition. For more information about alerts, see Using Alerts in Splunk App for Infrastructure.

Get started using Splunk App for Infrastructure

To get started using Splunk App for Infrastructure, see the topics in this guide for information about how to:

- Monitor entity health
- Investigate entities and groups
- Analyze performance
- Monitor and investigate alerts
• Use notifications to notify you when an alert is triggered
• Follow use cases for example workflows for monitoring your system
• Watch videos for a tour and instructions about how to use the application
• Use the toolkit for information about navigating views, using groups, understanding analytics, and so on.

Where to start

For instructions on how to install and set up Splunk App for Infrastructure in a single-instance or distributed deployment environment, see Install and Upgrade Splunk App for Infrastructure.

For instructions on how to administer Splunk App for Infrastructure, including including adding data, advanced data collection tasks, creating alerts, configuring notifications, managing users and roles, and troubleshooting, see Administer Splunk App for Infrastructure.

For instructions on how to use an already configured instance of Splunk App for Infrastructure, see the sections in this guide, Use Splunk App for Infrastructure.

For information about new features, fixed issues, and known issues in this version of Splunk App for Infrastructure, see Release Notes for Splunk App for Infrastructure.
Monitor and investigate

Monitor Entity Health with Splunk App for Infrastructure

Monitor the overall health of an entity with the **Entity Overview**. The Entity Overview contains performance charts that give a quick view of the performance of Infrastructure entities.

The Entity Overview is available for the single entities only, and is not available for groups at this time.

**Steps**

1. From the Investigate page, click an entity for which you want to view overall health.

   ![Entity Overview](image)

   This action drills down to the Entity Overview page.

2. On the Entity Overview page, view an overall summary of metrics being used by the entity, for example CPU, network, memory, disk, system information, dimensions and more. Each chart represents a metric area, and metrics vary depending on the operating system you are using.
Click a metric area to display detailed charts for the selected metric area.
Hover over an area or select a metric from list in the chart to display isolated metric information.
For more information about using the Entity Overview, see Using the Entity Overview in Splunk App for Infrastructure.

Analyze Entities and Groups with Splunk App for Infrastructure

Analyze performance metrics and log sources for a single entity, or a specific group of entities, using the Analysis Workspace. Understand why your infrastructure is performing the way it is, and quickly identify and respond to any issues or anomalies in your data.

Steps

1. On the Investigate page, select the entity or group you want to analyze.
   • If you select an entity, you will drill down to the Entity Overview page. Click the Analysis tab to access the Analysis Workspace.
   • If you select a group, you will drill down to the Analysis Workspace.
2. Investigate your entities and groups.

- Determine poor performing entities for a set of metrics, or determine a point in time when multiple entities began performing in a similar way.
- Create alert conditions and search logs collected from your servers to perform root cause analysis.
- Select data sources to create interactive charts in the workspace.
- Apply filters and aggregations to gain insight into your system’s metrics and performance.

For more information about using the Analysis Workspace, see Using the Analysis Workspace in Splunk App for Infrastructure and About Analytics in the Analysis Workspace in Splunk Insights for Infrastructure.
Alerts and notifications

Monitor and investigate alerts in Splunk App for Infrastructure

Admin privileges are required to create and manage alerts.

Use alerts to monitor triggered events and perform root cause analysis for a specific behavior in your data. The Alerts page displays a list of the last 100 triggered alerts. From here you can link to the Analysis Workspace, where you can continue to investigate performance issues during the time of the alert. This topic includes information about how to:

- Video: Setting up and using alerts
- Monitor and investigate alerts in the Analysis Workspace
- Monitor and investigate alerts from the Alerts tab
- View alert notifications
- View alert details

Video: Setting up and using alerts

For a video demonstration about setting up and using alerts, see Video: Setting up and using alerts. Alerts must be configured and created by an administrator.

Monitor and investigate alerts in the Analysis Workspace

View and investigate alerts in the Analysis Workspace:

- Click an alert or group from the Investigate page to access the Analysis Workspace.
- Click Alerts in the left Data panel to view a list of alerts that were created for an entity or group.
- Alerts are listed in a tree structure according to the data source they use.
- Click a data source name to see a list of alerts that are based on it, and to view the alert details in the workspace.
- The chart displays color-coded severity levels based upon thresholds set when creating the alert.

For example, the following image shows an Analysis Workspace alert for the cpu.idle metric.
Monitor and investigate alerts from the Alerts tab

Click the Alerts tab in the menu bar to launch the Alerts page and to view a list of alerts. The Alerts page lists the last 100 triggered alerts.

- When you click an alert, a slideout panel displays on the right of the screen with detailed information about the alert.
- In the slideout panel, click the ✤ to access the Investigate button to drilldown to the Analysis Workspace and investigate the alert further.
- The Alerts page displays a color-coded severity status for the state of the alert. This allows you to easily view the state of the alert by color. Severity colors include: Green for Information, Yellow for Medium, and Red for Critical.
- A severity status arrow displays alongside the severity status color in the Currently Severity column, indicating whether the alert has improved or degraded.
- The row size in the Alerts view is limited to two rows per entity. If resizing the window, or if the slide-out panel is activated, the dimensions column truncates and only displays dimensions that fit into the available two-row column size. The row does not expand or wrap to more than two rows, so all dimensions might not display. To view all of the dimensions for each entity or group, close the slide-out panel or resize your window to a larger view.
Alert notifications

When an alert is created by an administrator, there is an option to include an alert notification. This can be an alert notification sent by email or using VictorOps for Splunk. When the alert triggers, one or more notifications are sent depending on the type of alert notification and recipients selected during the alert creation, including:

- an email notification with details of the alert.
- a VictorOps notification, with the details displaying in your VictorOps account timeline. In your VictorOps account, click Alert Payload link to view details of the alert.

Alert details

Select an alert in the Alerts View or the Analysis Workspace to view its details. These details include the threshold conditions and severity levels configured for the alert, settings, and triggered instances.

- Triggered instances appear as annotations on the chart, and up to 100 annotations can display on the chart. Triggered instance annotations appear at the time the alert triggers, not the precise time the alert threshold is crossed.
Alert badges gauge the alert severity level. To help you monitor alert activity, badge colors are based on the most recent severity level of a triggered alert.

<table>
<thead>
<tr>
<th>Severity level</th>
<th>Badge color</th>
</tr>
</thead>
<tbody>
<tr>
<td>No trigger</td>
<td>Gray</td>
</tr>
<tr>
<td>Info</td>
<td>Green</td>
</tr>
<tr>
<td>Medium</td>
<td>Yellow</td>
</tr>
<tr>
<td>Critical</td>
<td>Red</td>
</tr>
</tbody>
</table>

**Example**

The following alert shows CPU user average for the cpu.user metric.

This alert is based on the aggregate average of cpu.user metric values. The green alert badge indicates a severity level of Info, yellow for medium, and red for critical. The horizontal lines show the alert threshold values. The annotations show triggered instances for the alert.
Use cases

Monitor CPU usage using Splunk App for Infrastructure

There are multiple CPU metrics that provide insight into how your infrastructure is performing. CPU utilization metrics indicate the following:

- **If a system is being over-utilized**: If your system is being over-utilized, it does not have enough capacity for the CPU demand. A high cpu system, cpu user and low cpu.idle measurements indicate over-utilization.
- **If a system is being under-utilized**: Your system is expected to handle consistent workloads, but a high cpu.idle, low cpu.system and cpu.user measurements indicate under-utilization.
- **Is disk I/O causing a bottleneck?** A high cpu.wait measurement indicates that the CPU is unable to move on because it is waiting for a disk operation to finish.

A single Linux host is a server or entity. A group of Linux hosts is a logical clustering of entities based on a data center, operating system, or tier of infrastructure so that you can monitor them in aggregate.

Steps

**Step 1: View your entities**

1. Click the **Investigate** tab. The Investigate view displays the entities you have added. You can select to view your entities using the Infrastructure Overview (tile view) or List View.

**Step 2: Explore Entities in the Entity Analysis Workspace**

1. Click the **Entities** button.
2. Click the **Entity Name** for the host you want to explore. The Analysis Workspace displays.
3. Under **Metrics**, click **cpu**. This menu tree contains metrics used to analyze your system.

- **Click** **user**. A cpu:user chart is added to the workspace.
- **Click** **system**. A cpu:system chart is added to the workspace.
Step 3: View per CPU breakdown

1. In the workspace menu bar, select **Split all by?**.
2. Select **cpu**. This enables monitoring cpu usage per core for all your charts.

Step 4: Pinpoint a specific timerange to investigate

1. Drag over an area of the chart to pinpoint a time range to investigate.
Summary

You now have a workspace that monitors your cpu usage for your single Linux hosts. On your workspace, you can also:

- Create alerts to notify you when conditions for critical issues are met. Admin privileges required to configure and manage alerts.
- Select the time period you want to display, from the last 15 minutes to the last 30 days.
- Use advanced aggregation and filtering options available in the Analysis panel.
- Select to view your charts by grid layout or stack layout
- Click the refresh button to refresh the screen.

Monitor CPU resource utilization using Splunk App for Infrastructure

You can create an alert to notify you when your CPU.system is running at a high level. For example, a server is running at 100% of CPU.system utilization for the past 15 minutes. This is affecting the performance of server, and degrading application delivery and user experience.

Problem: Too many duplicated processes and threads are running at the same time, due to a bug in a patch that was deployed. The server is running 100% on cpu.system for the past 15 minutes.

Resolution: Set up an alert to issue a warning when the average CPU.system utilization is greater than 89 percent, for a period of 15 minutes or more.

Admin privileges required to configure and manage alerts.

Steps

Step 1: Investigate the entity for which you want to set an alert

1. Click the Investigate tab to display a list of your entities.
2. Click the entity for which you want to set an alert and drilldown to the Analysis Workspace
Step 2: Select the metric to set the alert

1. On the Analysis Workspace, click the Metrics tab.
2. Select cpu > system. A new chart displays.

Step 3: Save the chart as an alert

1. In the chart, click the ... and select Create Alert. This launches the Create Alert dialog.
**Step 4: Configure the alert**

1. Enter information to create an alert:
   - **Name**: The alert is automatically given an alert name. Change the name if desired, following the character requirements.
   - **Type Id**: The entity or group name is displayed.
   - **Metric**: The type of metric selected for the chart, along with data analysis information.
   - **Trigger Actions**: Enter thresholds for alert trigger conditions.
   - **Notify if**: Select to notify a recipient if the alert severity improves or degrades.
   - **Send email**: Check the box next to the envelope to send an email when the alert triggers.
   - **Enter Recipients**: Enter email address(es) for alert notification recipients.

2. Click **Submit**.
**Step 5: Display alerts as a chart in the Analysis Workspace**

1. Click the **Alerts** tab to display the created alert.
2. Click the alert from the list to display the alert as a chart. This allows you to monitor the alert in the main panel view. When an alert triggers, the icon and chart displays the alert color, and alert details display in the right Analysis panel.

**Step 6: View triggered alerts from the Alerts List View**

You can view your most recent triggered alerts from the Alerts List View.

1. Click **Alerts** in the menu bar at the top of the user interface.
2. Click an entity or group to view more details about the alert in the right slide-out panel. The following screen shows akron.usa.com
Summary

You now have an alert that will notify you by email if your entity’s cpu.system reaches 89% or more.
Videos

Videos for how to use Splunk App for Infrastructure

The Splunk App for Infrastructure videos provide quick tutorials to help you understand, navigate, or configure your instance. These videos are useful tools to get you up and running fast, and to help answer any questions you might have about using this product and monitoring your infrastructure. Click on any of the videos listed below to help guide you in using this product.

**Introducing Splunk App for Infrastructure**

This video gives a full demonstration and overview of Splunk App for Infrastructure. See Introducing Splunk App for Infrastructure.

**Install to Insight in Minutes**

This video demonstrates how to install Splunk App for Infrastructure on Linux. See Install to Insight in Minutes.

**Configuring log and metrics collection for Linux**

This video demonstrates how to configure and install the Agent Installation Script on a host machine, and making the connection with Splunk App for Infrastructure to start collecting data to monitor and investigate your infrastructure. See Configuring log and metrics collection for Linux.

**Configuring AWS Data Collection**

This video demonstrates how to collect metric data from your AWS entities, such as EC2, EBS, ELB, and CloudWatch logs, and making the connection with Splunk App for Infrastructure to monitor and investigate your AWS accounts. See Configuring AWS collection.

**Using Entities and Dimensions**

This video demonstrates defining dimensions to allow you to easily group and filter entities, giving you the flexibility to view your infrastructure the ways you want to. See Entities and Dimensions.
**Using Groups**

This video demonstrates working with groups in Splunk App for Infrastructure. See Monitoring and Investigating Groups of Systems.

**Using Alerts**

This video demonstrates working with alerts in Splunk App for Infrastructure. See Setting and Using Alerts.

**Windows Support**

This video demonstrates how Splunk App for Infrastructure 1.1 works with Windows Server 2012/2016 and Windows 12, both for deployment and data collection. See Windows Deployment and Data Collection Support.
Toolkit

Using the Infrastructure Overview in Splunk App for Infrastructure

Monitor the health of your system using the **Infrastructure Overview**. This view is used to quickly understand availability and performance of your server infrastructure. Choose a specific performance metric and set a threshold to better understand your high and low performing systems.

From this view you can quickly access information including hostname and IP address, as well as drill down to the Overview Dashboard and Analysis Workspace for a specific server where you can continue to analyze and understand server performance.
<table>
<thead>
<tr>
<th>Number</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Get details of an active entity</td>
<td>Hover your mouse over a tile to display the name of the entity, time of activity for the entity, IP address, and operating system information. Click the tile to drilldown to the Analysis Workspace to further monitor the entity.</td>
</tr>
<tr>
<td>2</td>
<td>Active entity</td>
<td>Green tiles indicate the entity is active. The name of the entity is displayed in the tile, and you can hover your mouse over the tile to display more information about the entity.</td>
</tr>
<tr>
<td>3</td>
<td>Inactive entity</td>
<td>Red tiles indicate the entity is inactive. The name of the entity is displayed, along with the time the entity has been inactive, the operating system, and the IP address. Click the tile to drilldown to the Analysis Workspace to troubleshoot the reason why the entity is inactive.</td>
</tr>
<tr>
<td>4</td>
<td>Number of Entities</td>
<td>Number of monitored entities available to in your infrastructure.</td>
</tr>
<tr>
<td>5</td>
<td>Display Entities or Groups</td>
<td>Select to display entities or groups in the Infrastructure Overview.</td>
</tr>
<tr>
<td>6</td>
<td>Filter by metric</td>
<td>Click the dropdown menu and select to display the entities by metric.</td>
</tr>
<tr>
<td>7</td>
<td>Filter by dimensions</td>
<td>Filter the display by dimensions. Start typing in the field to filter through all dimensions and display them in the Infrastructure Overview. Click the star to save your selections as a group, for easier monitoring.</td>
</tr>
<tr>
<td>8</td>
<td>Set threshold value for selected metric</td>
<td>Set the minimum and maximum metric thresholds values for the entities or groups displayed in the overview workspace. This allows you to visually monitor healthy and unhealthy entities or groups as they display as green or red in the workspace, based upon their threshold setting.</td>
</tr>
<tr>
<td>9</td>
<td>Unhealthy, healthy, and inactive entity or group count</td>
<td>The number of unhealthy, healthy, or inactive entities or groups are displayed by count.</td>
</tr>
<tr>
<td>Number</td>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>10</td>
<td>Refresh</td>
<td>Select how often to refresh the overview workspace. You can set to Auto Refresh, refresh in seconds or minutes, or set refresh to off.</td>
</tr>
<tr>
<td>11</td>
<td>Save as group</td>
<td>Click the star icon to create a group based upon the dimensions you select in the filter bar. Saving entities that have similar dimensions as a group allows you to easily monitor them.</td>
</tr>
<tr>
<td>12</td>
<td>Display the Infrastructure Overview or List View</td>
<td>Select to display the Infrastructure Overview by tile view or list view. The display shown is the Infrastructure Overview.</td>
</tr>
<tr>
<td>13</td>
<td>Minimize of maximize tiles in view</td>
<td>Minimize or maximize the tile size in the Infrastructure Overview. If you minimize the tiles, you can see more tiles in the overview for easy visualization of your infrastructure. If you maximize the tiles, you will not see as many entities, although you will see more details about each entity.</td>
</tr>
<tr>
<td>14</td>
<td>No metric available for entity</td>
<td>A grey tile indicates there is no metric available for the entity.</td>
</tr>
</tbody>
</table>

**Using the List View in Splunk App for Infrastructure**

Use the **List View** to view your entities or groups, view their status as active or inactive, sort by dimensions, create groups, and perform bulk actions. You can also drilldown to the Overview Dashboard of an entity, and the Analysis Workspace of an entity or group to review details or troubleshoot an issue.
<table>
<thead>
<tr>
<th>Number</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Drilldown to the Analysis Workspace</td>
<td>Click an entity or group in the list to drilldown to the Analysis Workspace to further explore details of the entity or group metrics and alarms.</td>
</tr>
<tr>
<td>2</td>
<td>Bulk Actions</td>
<td>Click the Bulk Actions dropdown and select bulk actions for all entities or groups in the List View, such as deleting.</td>
</tr>
<tr>
<td>3</td>
<td>Number of Entities</td>
<td>Number of monitored entities available to in your infrastructure.</td>
</tr>
<tr>
<td>4</td>
<td>Entities or Groups</td>
<td>Select to display entities or groups in the List View.</td>
</tr>
<tr>
<td>5</td>
<td>Filter by dimensions</td>
<td>Filter the display by dimensions. Start typing in the field to filter through all dimensions and display them in the Infrastructure Overview. Click the star to save your selections as a group, for easier monitoring.</td>
</tr>
<tr>
<td>6</td>
<td>Save as group</td>
<td>Click the star icon to create a group based upon the dimensions you select in the filter bar. Saving entities that have similar dimensions as a group allows you to easily monitor them.</td>
</tr>
<tr>
<td>7</td>
<td>Infrastructure Overview or List View</td>
<td>Select to display the Infrastructure Overview (tiles) or the List View. The display shown is the List View.</td>
</tr>
<tr>
<td>8</td>
<td>Actions</td>
<td>Perform actions to delete an entity and/or edit or delete a group.</td>
</tr>
</tbody>
</table>

### Using the Analysis Workspace in Splunk App for Infrastructure

Use the **Analysis Workspace** to analyze performance metrics and log sources for a single entity, or a specific group of entities. Determine poor performing entities for a set of metrics, or determine a point in time when multiple entities began performing in a similar way. Create alert conditions and search logs collected from your servers to perform root cause analysis and understand why your infrastructure is performing the way it is.

Select data sources to create interactive charts in the workspace. Then, apply filters and aggregations to gain insight into your system?ś metrics and
performance. The Analysis Workspace helps you quickly identify and respond to any issues or anomalies in your data.

**Navigating the Analysis Workspace**

From the Infrastructure Overview or the List View, access the Analysis Workspace by clicking an entity or group:

- If clicking an entity, you drilldown to the Entity Overview. Click the Analysis tab to access the Analysis Workspace.
- If clicking a group, you drilldown to the Analysis Workspace.

You can also navigate groups or entities in the Analysis Workspace by clicking the group or entity navigation dropdown to view what entities are in a group, or what groups an entity is a part of.

The workspace contains three panels.

- The left-side Data panel shows all data sources that are available for analysis.
- The Main panel in the center is where you see your data represented in charts.
- The right-side Analysis panel lists the aggregations and analytic functions that you can apply to your data. For more information about the Analysis panel, see About Analytics in the Analysis Workspace in Splunk App for Infrastructure.

To add a chart to your workspace to view data represented as a time series, use the search box to find metrics, event, or alerts, or browse through the hierarchy of available data sources. Click the data source, and a chart displays in the workspace. Use the workspace analysis tools customize your charts. The chart must have data to access chart actions, and you must have admin privileges to perform chart actions. For more information about chart actions, see Use Chart Actions to create an alert, open in search, or save as a dashboard panel.
<table>
<thead>
<tr>
<th>Number</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Search metrics, events, or alerts</strong></td>
<td>Search available metrics, events or alerts to analyze and display in the workspace charts. Manage alerts that you have created, and perform actions such as deleting an alert. See Using Alerts in Splunk App for Infrastructure for detailed information about using alerts.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Data panel</strong></td>
<td>The Data panel contains all of the data sources that you have available for visualization and analysis. Search metrics, events, or alerts, or browse for data to view and analyze in the workspace.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Every data source that you select in the Data panel appears as a separate chart in the workspace. Each chart contains a time series based on at least one aggregation. Hover over any point on the series to see the corresponding values in the chart legend to the right of the chart.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Group and Entity navigation</strong></td>
<td>View entities contained in a group, or view what groups an entity is a part of, by expanding the group or entity navigation dropdown. For example when viewing a group in the Analysis Workspace, click the down arrow next to the group name and a list of entities contained in the group display. Click an entity in the group to view the entity in the Analysis Workspace, or use the search field to search for an entity in the group. If viewing an entity in the Analysis</td>
</tr>
<tr>
<td>Number</td>
<td>Element</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4</td>
<td>Pinpoint time range</td>
<td>Hover to view a shared hairline on all charts. Click and drag to zoom in on a narrower time range.</td>
</tr>
<tr>
<td>5</td>
<td>Time range picker</td>
<td>Select a common time range to display for all charts. The default time range for time series is one hour. Adjust the time range to gain more insight from your charts. Adjust the time range by either the time range picker, or by zooming in on a chart. You can select a custom time range by clicking and dragging your cursor over the time period you want to view.</td>
</tr>
<tr>
<td>6</td>
<td>Split by</td>
<td>Split charts to show a separate time series for each value of a dimension. Click a dimension in a chart and select an action such as <em>Investigate Entity</em> to drilldown to further details.</td>
</tr>
<tr>
<td>7</td>
<td>Refresh</td>
<td>Refresh charts to include the most recent data. Refresh manually or enable auto-refresh.</td>
</tr>
<tr>
<td>8</td>
<td>Chart actions</td>
<td>Click the ellipsis to view the chart action menu. Perform chart actions such as creating an alert, saving a chart as a dashboard panel, opening the chart in Search, saving the chart as a Report, and other tasks. See <em>Use Chart Actions</em> to create an alert, open in search, or save as a dashboard panel.</td>
</tr>
<tr>
<td>9</td>
<td>Entity Overview or Analysis Workspace</td>
<td>Select to display the Analysis Workspace or display system information about the selected host, including operating system, IP address, version information, and associate dimensions.</td>
</tr>
<tr>
<td>10</td>
<td>Clear all</td>
<td>Clear all charts from the workspace.</td>
</tr>
<tr>
<td>11</td>
<td>Grid layout or stack layout</td>
<td>Display charts in grid layout, which displays multiple charts in each row, or stack layout, which displays one chart per row.</td>
</tr>
<tr>
<td>12</td>
<td>Save all charts to a dashboard</td>
<td>Save all charts to a dashboard.</td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Select analysis tools, such as aggregation, time comparison, split by, and filters, to display in the Analysis Workspace.

Depending on your data source, the following operations are available:

- Aggregations summarize data points into meaningful values.
- Time comparisons overlay a previous time period on the chart.
- Split by shows results for a specific dimension.
- Filters include or exclude certain results.

See Analytics in the Analysis Workspace for detailed information about the different operations you can use to analyze your data.

<table>
<thead>
<tr>
<th>Number</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Main panel</td>
<td>The Main panel is contains charts. Every data source that you select in the Data panel appears as a separate chart in the workspace, or Main panel. Each chart contains a time series based on at least one aggregation. Hover over any point on the series to see the corresponding values in the chart legend to the right of the chart.</td>
</tr>
</tbody>
</table>

**Use Chart Actions to create an alert, open in search, or save as a dashboard panel**

Perform chart actions using the chart action menu, such as creating an alert, saving a chart as a dashboard panel, opening the chart in Search, saving the chart as a Report, and other tasks. Click the ellipsis to access the chart action menu. You must have admin privileges and data in the chart to access this menu and perform actions.

If you create a dashboard panel, click the Dashboard tab to view your dashboards in Splunk Enterprise. See the Splunk Enterprise Dashboards and Visualizations guide.

If you open your chart in Search, see the Splunk Enterprise Search Manual.
Using the Entity Overview in Splunk App for Infrastructure

The **Entity Overview** contains performance charts that give a quick view of the performance of Infrastructure entities. From this overview, get a summary of metrics being used by the entity, including CPU, network, memory, disk, system information, dimensions and more. Click a metric area to display detailed charts for the selected metric area, and hover over an area or select a metric from list in the chart to display isolated metric information.

The Entity Overview is available for the single entities only, and is not available for groups at this time.
<table>
<thead>
<tr>
<th>Number</th>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Entity</td>
<td>The name of the entity for which the details are displayed in the overview.</td>
</tr>
<tr>
<td>2</td>
<td>Refresh</td>
<td>Select how often to refresh the overview. You can set to Auto Refresh, refresh in seconds or minutes, or set refresh to off and manually refresh.</td>
</tr>
<tr>
<td>3</td>
<td>Time picker</td>
<td>Select the time period for which you want to display in the overview.</td>
</tr>
</tbody>
</table>
| 4      | Metric tabs | Metrics tabs identify the areas of metrics displayed in the overview charts.  
- The Overview tab displays a chart for each metric area listed.  
- Click a metric tab, such as CPU, and the overview updates to display charts for the selected metric area. Each chart displays a list of metrics shown in the visualization, and values for a selected time period.  
- The tabs and associated charts are by default and cannot be modified. |
| 5      | Metric area | Tabs identify an individual metric area. A numeric value displays beneath the name of the metric area, and represents values such as disk free percent. The arrow next to the value displays values increasing or decreasing, and the number value represents the activity in the given time period. |
| 6      | Overview tab or Analysis tab | Click the Overview tab to display the Entity Overview and view metric details of an entity. Click the Analysis tab to drill down to the Analysis Workspace. |
| 7      | System Information | Displays system information for the entity displayed in the overview. |
| 8      | Dimensions | Displays dimensions of the entity displayed in the overview. |
| 9      | List of metrics in a chart | Every chart displays a color-coded list of metrics. Each metric displays as a visual data value in the chart, such as a line chart or stack chart. Hover over a specific metric to isolate and display that selected metric in the chart. |
## Overview

A chart contains a visualization representing data. Each chart is identified by the name of the metric area or metric. The chart displays a list of metrics as a visualization, and each metric value is represented by a color-coded visual identifier. Hover or click an area to isolate details of a selected metric, or click a metric in the chart list to isolate data in the visualization and display details only for that metric. The charts are view only and cannot be edited.

### About Analytics in the Analysis Workspace in Splunk App for Infrastructure

Configure analytic functions and operations in the Analysis panel in the Analysis Workspace. These options help you gain insight from your charts.

### Aggregations

Aggregations are groups of data points within the same approximate time frame. Charts in the Analysis Workspace contain time series based on aggregated data. Select one or more aggregations in the Analysis panel to generate a time series on the chart.

The following aggregations are available:

<table>
<thead>
<tr>
<th>Aggregation</th>
<th>Use</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average (Avg)</strong></td>
<td>Numeric data</td>
<td>Aggregated averages of the values in your data. Default aggregation for numeric data.</td>
</tr>
<tr>
<td><strong>Maximum (Max)</strong></td>
<td>Numeric data</td>
<td>Aggregated maximum values in your data.</td>
</tr>
<tr>
<td><strong>Minimum (Min)</strong></td>
<td>Numeric data</td>
<td>Aggregated minimum values in your data.</td>
</tr>
<tr>
<td><strong>Standard deviation (Std dev)</strong></td>
<td>Numeric data</td>
<td>Standard deviation of each time bucket in your data.</td>
</tr>
<tr>
<td><strong>Sum</strong></td>
<td>Numeric data</td>
<td>Aggregated sum of values in your data.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Use</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Percentiles</td>
<td>Numeric data</td>
<td>Aggregated percentile values in your data. View a maximum of five percentiles. Default percentiles are 90, 75, 50, 25, and 15. To remove a percentile, click the X icon next to the percentile you want to remove. To configure additional percentiles, enter a number between 1 and 100 in the box under the percentiles option.</td>
</tr>
</tbody>
</table>

To configure aggregations:

1. In the Main panel, select the chart you want to modify.
2. In the Analysis panel, select the aggregations to apply.

**Examples**

The following chart shows the Average, Maximum, and Minimum aggregations of system.cpu values for collectd metrics.

The following chart shows the 25th, 50th, and 75th Percentile aggregations of system.cpu values for collectd metrics.

**Time comparisons**

Time comparisons overlay a previous time period on a chart to investigate whether a time series has changed significantly between two related time ranges.

Time comparisons are not available for datasets or when splitting charts by dimension.
**Add a time comparison to a chart**

Add a time comparison to a chart to investigate changes in your data over time.

1. From the Main panel of the Analysis Workspace, select a chart to add the time overlay to.
2. In the Analysis panel of the Analysis Workspace, click the **Compare to** list under Time Comparison.
3. Select from the list of preset time overlays, or select **custom**.
4. (Optional) If you selected **custom**, enter the time comparison you want to use.

Time comparisons appear as dotted lines on the chart.

**Remove a time comparison from a chart**

Remove a time comparison from a chart to show data from only the current time range.

1. In the Analysis panel of the Analysis Workspace, click the **Compare to** list.
2. Select **None**.

**Examples**

The following chart compares current average system.cpu values to the values from 24 hours before.

![Chart example](image)

**Splitting and stacking**

Split a chart by a dimension to view a separate time series for each dimension value. Splitting a chart by a dimension shows the values with the highest or lowest values in data for the selected time range.

Stack the series to show the sum of dimension values on the chart. In a stacked series, each series appears as a colored area of the stacked chart.
Splitting by dimension is not supported for charts with multiple aggregations or time comparisons.

**Split a chart by dimension**

Split a chart by a dimension to show a separate time series for each dimension value.

1. From the Main panel of the Analysis Workspace, select the chart you want to split by dimension.
2. In the Analysis panel, click the **Split by** list.
3. Select the dimension that you want to split.
4. For Display, select either the **Highest** or **Lowest** spikes in data.
5. Select the number of values to display.
6. (Optional) Select **Stack Series**.

The chart shows a new time series for each value of the split dimension.

**Remove a dimension split**

Remove a dimension split to view data for all dimensions in a single time series.

1. In the Analysis panel of the Analysis Workspace, click the **Split by** list.
2. Select **None**.

**Split all charts in the workspace**

Split all charts by a single dimension to view the top five values of that dimension for each chart in the workspace. Splitting all charts by a dimension overrides any other splits you have in place. New charts that you add to the workspace will automatically apply the split.

Split all charts by a dimension:

1. Click the **Split all by** drop-down list in the global actions bar of the Analysis Workspace.
2. Select a dimension from the list.

All charts appear split by your selected dimension. If a chart does not apply the split, it is because that dimension is not present in your data.

Splitting all charts only applies the split once. If you split by a different dimension for one or more charts in the workspace, this overrides the global split.
Remove dimension splitting from all charts:

1. Click the **Split all by** drop-down list in the global actions bar of the Analysis Workspace.
2. Select **None**.

**Examples**

The following chart shows the `apache.response_time` metric split by the top five pages.

The following chart shows the `apache.active_connections` metric split by the top three extracted hosts. The series is stacked to show the total number of active connections.

**Filters**

Filter data to view specific dimension values on the chart. If a chart is already split by a dimension, use filters to add or remove time series for selected dimension values.

To filter for a dimension with a high number of values, use wildcard searches from within the Filter panel. For more information about wildcard searches in the Splunk platform, see Wildcards in the *Splunk Enterprise Search Manual*.

**Filter by dimension value from the Analysis panel**

Filter chart data to view a specific subset of dimension values.

1. From the Main panel of the Analysis Workspace, select the chart you want to filter by dimension value.
2. In the Analysis panel under Filters, click the name of the dimension you want to filter by.
3. Select whether to **Include** or **Exclude** the specified dimension values.
4. (Optional) For dimensions with a high number of values, type part or all of the dimension value name into the search bar on the Filter panel.
5. From the list of dimension value names, select the dimension values you want to filter on the chart.

The chart shows data for the dimension values that you selected.

*Filter by dimension value from the chart legend*

If a chart is already split by a dimension, filter by dimension value using the chart legend.

**Prerequisites**
Split the chart by a dimension. See Splitting and stacking.

**Steps**

1. From the Main panel of the Analysis Workspace, select the chart you want to filter by dimension value.
2. In the chart legend, click the the name of the dimension value that you want to filter.
3. From the options that appear, click either **Keep Only** or **Exclude**.

The chart shows data for the dimension values that you selected.

*Example*

*Filter a group by entity and dimension value from the chart legend*

Filter group chart data to view a specific entity based on dimension values.

**Prerequisites**
Split the group chart by a dimension. See Splitting and stacking.
**Steps**

1. From the Main panel of a Group Analysis Workspace, select the chart you want to filter to view an entity based on a dimension value.
2. Select **Split all by?** and select the dimension you want to filter the chart by. For example, `host`.
3. In the chart, click the entity from the chart legend to display the action menu.
4. Select the action to **Investigate Entity** to open a separate analysis workspace for that entity, or select to **Keep Only**, **Exclude**, or **Copy Series Name** for the chart you are viewing.

**Example**

![Chart Example]

**Clear all dimension value filters**

Clear all dimension value filters to view data from all values of a dimension on the chart.

1. From the Main panel of the Analysis Workspace, select the chart you want to clear filters for.
2. In the Analysis panel under Filters, click the name of the dimension you want to clear filters for.
3. In the top-right corner of the list of dimension values, click the \( \times \) icon.

The chart shows data for all values of that dimension.

**Examples**

The following chart shows the average, maximum, and minimum aggregations for the `aws.ec2.CPUUtilization` metric filtered by IP address.
The following chart shows the system.memory.usage metric split by App and filtered to show time series for the cart, catalog, and checkout dimension values.

Using Groups in Splunk App for Infrastructure

Use groups to monitor and analyze performance across multiple hosts, and to quickly find relevant log events for the entire group. When creating a group, logically group hosts together by choosing one or more dimension filters that are common across a similar entities. You can also use wildcards, so that you can look across multiple hosts that might match a certain portion of the criteria.

For a video demonstration about using groups, see Video: Monitoring and Investigating Groups of Systems.

Create a group from an entity list

To create a group of entities, select from your list of entities hosts that have similar dimensions to reflect your infrastructure. Logically group these hosts together for troubleshooting and monitoring. You must have multiple entities already added to your instance in order to group them.

1. Click the Investigate tab to see your list of entities.
2. Click in the filter bar. Dimensions, or key/value pairs, that you created when configuring agents display in the dropdown list.
   1. When creating groups, multiple values with the same key are treated as an OR condition, values with different keys are treated as an AND condition.
3. Select the dimensions you want to use to filter your entities into a group.
4. After selecting filter dimensions for your group, click the star icon/Save as group to the right of the filter bar. The create group dialog displays, with
the group name pre-populated. You can edit the group name before saving. **Note:** A Group name cannot contain a pipe (|) or an equals sign (=).

5. Click **Save** to create the group. Your group is saved.
6. Click **View group now** to view your list of groups.
7. Click the **Groups** button on the upper left to view all of your saved groups.

**Using the Analysis Workspace to view and analyze group performance metrics**

Use the Analysis Workspace to access a group analysis view and analyze performance metrics across all the entities for a specific group. The Analysis Workspace aggregates performance across all hosts in a group. Determine poor performing entities for a set of metrics, or determine a point in time when multiple entities began performing in a similar way. View what entities are contained in a group from the group navigation dropdown.

Explore the status of a group using the Analysis Workspace.

1. Click the **Investigate** tab.
2. Click **Groups** to display your list of groups.
3. Click a group to drilldown and display in the Analysis Workspace.
4. Click the dropdown arrow next to the group name in the header of the Analysis Workspace to view or search for entities within the group.

**Monitor the health of groups using the Infrastructure Overview**

Monitor the health of your system using the Infrastructure Overview. This view displays critical information about your groups, such as hostname and IP address of entities, status of your groups (indicated by color), time indicating when status was last updated, or drilldown into the Analysis Workspace.

1. Click the **Investigate** tab.
2. Click **Groups**.
3. Click the **tile view** icon in the upper right of the page.
   - The tile view displays groups in your environment.
   - The color of each tile indicates if the group is active (green) or inactive (red).
   - The time the group has been active is noted in the center of the tile.
4. Click the group you want to explore to drilldown to the Analysis Workspace. See Using the Analysis Workspace in Splunk App for Infrastructure.
Update group settings

Update group settings, including group dimensions and details, fixing errors or changing the scope of a group.

1. Click the **Investigate** tab.
2. Click the **Groups** button.
3. Click the checkbox for the group or groups you want to update or edit.
4. Click the **Action** dropdown for the selected group(s) and click **Edit**.
5. Makes your changes in the filter bar.

Viewing the status of servers in a group

Explore the status of servers in a group to view if they are active or inactive.

1. Click the **Investigate** tab.
2. Click **Groups** to display your list of groups.
3. Click a group to drilldown and display in the Analysis Workspace.
4. Rollover the Entity Breakdown Indicator to display information about the group. The Entity Breakdown Indicator is the icon to the left of the group name, and displays if servers in the group are active or inactive.
   1. If less than 20% of servers in your group are active, a green checkmark displays.
   2. If greater than 20% of servers in your group are inactive, the Entity Breakdown indicator displays as a red exclamation icon.

Delete a group or groups

Delete a group or multiple groups. Deleting a group will only remove the group from the list, and will not delete any of the entities contained in the group.

**To delete a single group**

1. Click the checkbox for the group you want to delete.
2. Click **Bulk Actions > Delete Selected Groups**. Or, you can select the group and **Action > Delete**.

**To delete multiple groups**

1. Click the checkbox in the Name header, which populates all group checkboxes.
2. Click **Bulk Actions > Delete Selected Groups**. Or, you can select the
Glossary of terms for Splunk App for Infrastructure

Splunk App for Infrastructure basic components and feature descriptions include:

- **Agent** is the agent script which performs the following upon execution on the host machine/agent/entity:
  - ♦ Detects the operating system (for example, Ubuntu).
  - ♦ Based on the machine type, installs dependencies.
  - ♦ Updates collectd.conf with the necessary plugin.
  - ♦ Adds a custom plugin that sends data to Splunk App for Infrastructure.
  - ♦ Starts the collectd service.
  - ♦ Runs collectd and establishes a data connection.

- **Collectd** is a system statistic collection daemon, see https://collectd.org/

- **Dimension** is a key/value pair used for troubleshooting, analysis, and filtering hosts, for example location:seattle or role:webserver. Dimension keys and values cannot begin with an underscore.

- **Entity** is the machine or host that has the data you want to forward to Splunk App for Infrastructure to monitor.

- **Metrics** is a set of measurements containing a timestamp, a metric name, a value, and a dimension. Metrics is a feature for system administrators and IT tools engineers that focuses on collecting, investigating, monitoring, and sharing metrics from your technology infrastructure, security systems, and business applications in real time.

- **Status** is the status for each entity is calculated by determining if data has been sent from the entity and is available for analysis in the last 60 seconds. An offset is set for this search to allow for time to index and store the metric measurements.
Support

Support for Splunk App for Infrastructure

If you need additional support or help with your Splunk App for Infrastructure instance, there are different resources based upon the type of license or version you have:

- Paid license instance, contact your Splunk representative.
- Free-tier instance, find help using the Splunk Community at:
  ♦ Splunk Answers
  ♦ User groups
  ♦ Blogs
  ♦ Community Portal