



Splunk® Enterprise Analytics Workspace 9.0.2

Generated: 11/02/2022 1:55 pm

Table of Contents

Introduction.....	1
About the Analytics Workspace.....	1
Requirements for the Analytics Workspace.....	1
Getting started with the Analytics Workspace.....	3
Open the Analytics Workspace.....	3
Navigating the Analytics Workspace.....	3
Types of data in the Analytics Workspace.....	4
Using the Analytics Workspace.....	7
Charts in the Analytics Workspace.....	7
Data sources in the Data panel in the Analytics Workspace.....	16
Analytics in the Analytics Workspace.....	16
Alerts in the Analytics Workspace.....	23
Dashboards in the Analytics Workspace.....	27
Use Cases.....	29
Analyzing data in the Analytics Workspace.....	29
Creating a dashboard in the Analytics Workspace.....	31
Resources.....	34
Troubleshoot the Analytics Workspace.....	34

Introduction

About the Analytics Workspace

The Analytics Workspace provides a user interface that enables you to monitor and analyze metrics and other time series without using SPL. Select data sources to create interactive charts in the workspace. Then, apply filters and aggregations to gain insight into your system's metrics and performance. The Analytics Workspace helps you to quickly identify and respond to any issues or anomalies in your data.

Analytics Workspace functions and operations

The Analytics Workspace comes with a set of analytic functions and operations to help you make sense of your data. These functions generate SPL in the background.

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

- Aggregations summarize data points into meaningful values.
- Time shifts modify the time range of a series.
- Splits show results for a specific dimension.
- Filters include or exclude certain results.

After refining your data, use the Analytics Workspace to perform the following actions:

- Set up an alert to be notified of certain behavior in your data.
- Create a dashboard to monitor or share your findings.

To learn about visualizing data, see [Types of data in the Analytics Workspace](#).

To learn about the different parts of the workspace, see [Navigate the Analytics Workspace](#).

To learn more about analytic functions and operations, see [Analytics in the Analytics Workspace](#).

To learn more about alerts, see [Alerts in the Analytics Workspace](#).

To learn more about dashboards, see [Dashboards in the Analytics Workspace](#).

Requirements for the Analytics Workspace

To use the Analytics Workspace, you must meet the following requirements.

Splunk role requirements

To configure the Analytics Workspace in Splunk Enterprise, you must be a member of the `admin` role. You can't change or edit the configuration of the Analytics Workspace in Splunk Cloud Platform.

Splunk capability requirements

To use some functionalities of the Analytics Workspace, you must have certain capabilities assigned at the user level.

Functionality	Capability
Alerts	<code>schedule_search</code>

See About configuring role-based user access in *Securing Splunk Enterprise* for information on Splunk roles and capabilities.

Splunk platform requirements

The Analytics Workspace runs on the following Splunk platforms:

- Splunk Enterprise version 8.0.0 and later
- Splunk Cloud Platform version 8.0.0 and later

For Splunk Enterprise system requirements, see System Requirements in the Splunk Enterprise *Installation Manual*.

Upgrading Splunk Enterprise

Analytics Workspace is installed by default in Splunk Enterprise version 8.0 and later. Prior to Splunk Enterprise 8.0, Metrics Workspace provided similar functionality to Analytics Workspace. In Splunk Enterprise 7.3, Metrics Workspace is installed by default, but in Splunk Enterprise 7.2 and earlier, Metrics Workspace is a standalone app.

If you used Metrics Workspace with Splunk Enterprise version 7.2 or earlier in a search head cluster environment, before you upgrade to Splunk Enterprise version 7.3 or later, remove the `splunk_metrics_workspace` app from the `$SPLUNK_HOME/etc/shcluster/apps` directory. Complete this step before running any configuration deployments.

Getting started with the Analytics Workspace

Open the Analytics Workspace

You can open the Analytics Workspace from the Search & Reporting app or from another app in Splunk Enterprise, depending on the data you want to analyze.

Open the Analytics Workspace from the Search & Reporting app

Open the Analytics Workspace from the Search & Reporting app to visualize and analyze metrics and accelerated datasets.

1. Open the Search & Reporting App in Splunk Web.
2. Click the **Analytics** tab on the Search & Reporting bar.

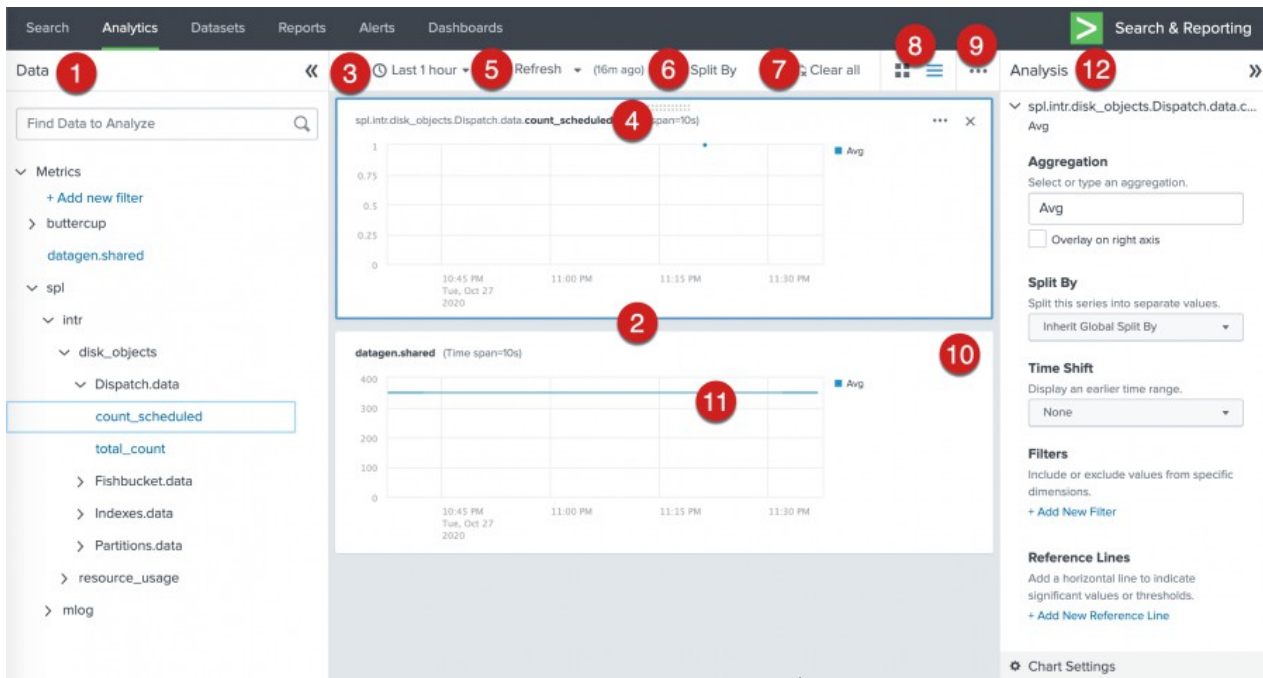
Open the Analytics Workspace from another app in Splunk Enterprise

Open the Analytics Workspace from another app in Splunk Enterprise to analyze metrics and accelerated datasets from that app.

1. Open the app in which you want to use the Analytics Workspace.
2. In your Splunk Web URL, add `/analytics_workspace` after the app's name.
For example, to open the Analytics Workspace in the Splunk App for Infrastructure, enter the following URL:
`http://<splunkhost>:<port>/app/splunk_app_infrastructure/analytics_workspace`.
3. Press Enter.

Navigating the Analytics Workspace

The Analytics 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.



Number	Element	Description
1	Data panel	Search or browse for data to view and analyze.
2	Main (center) panel	View and manipulate time series of your data.
3	Time range picker	Select a common time range to display for all charts.
4	Chart title	Chart titles consist of the data source name.
5	Refresh	Refresh charts to include the most recent data. Refresh manually or enable auto-refresh.
6	Split By	Split a time series by a dimension to view a separate time series for each dimension value.
7	Clear all	Clear all charts from the workspace.
8	Grid layout or stack layout	Display charts in grid layout, which displays multiple charts in each row, or stack layout, which displays one chart per row.
9	More workspace options	Save all charts in the workspace to a dashboard.
10	More chart options	Open chart in search, search for related events, save as alert, save as dashboard panel, save as report, clone panel, or export as PNG or CSV.
11	Pinpoint time range	Hover to view a shared hairline on all charts. Click and drag to zoom in on a narrower time range.
12	Analysis panel	Perform analytic functions and operations.

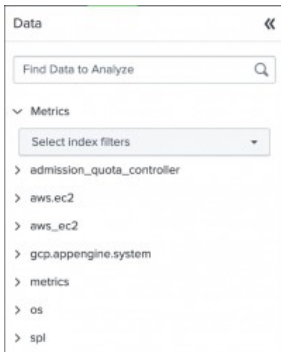
Types of data in the Analytics Workspace

The Analytics Workspace Data panel contains the data sources that you have available for visualization and analysis. These data sources are organized by data type. Supported data types are metrics, datasets, and alerts.

About metrics data

Click the **Metrics** tab in the Data panel to view a list of metrics. Metrics data sources are listed in a tree structure or index according to their `metric_name`.

For example, the following image shows a default view of the **Metrics** data source index list.



If two metrics with the same name are ingested into different indexes, they appear aggregated in the Data panel. To distinguish these metrics in the workspace, see [Distinguish metrics with the same metric name](#).

The Analytics Workspace does not currently support metric roll-ups.

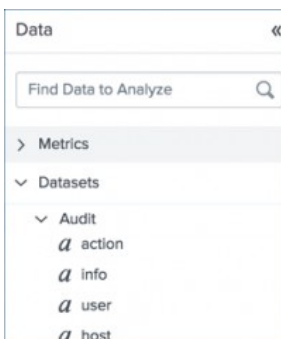
To learn more about metrics data, including metrics ingest, see Overview of Metrics in the *Metrics Manual*.

For information about converting log data into metrics data, see Convert event logs to metric data points in the *Metrics Manual*.

About datasets

Click the **Datasets** tab in the Data panel to view a list of datasets. Datasets are listed in a tree structure according to the dataset name. Click a dataset name to see a list of fields for the dataset. Numeric fields are indicated by the hash (#) icon, whereas string fields are indicated by the alpha (α) icon.

For example, the following image shows a list of fields for the `Audit` dataset.



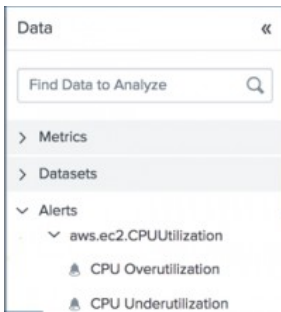
Only accelerated datasets are supported in the Analytics Workspace. See Accelerate data models in the Knowledge Manager Manual for more information.

For more information about datasets, see Dataset types and usage in the *Knowledge Manager Manual*.

About alerts

Click the **Alerts** tab in the Data panel to view a list of alerts that were created in the Analytics Workspace. The **Alerts** tab includes alerts that you created and alerts that have been shared with you. 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.

For example, the following image shows a list of Analytics Workspace alerts for the `aws.ec2.CPUUtilization` metric.



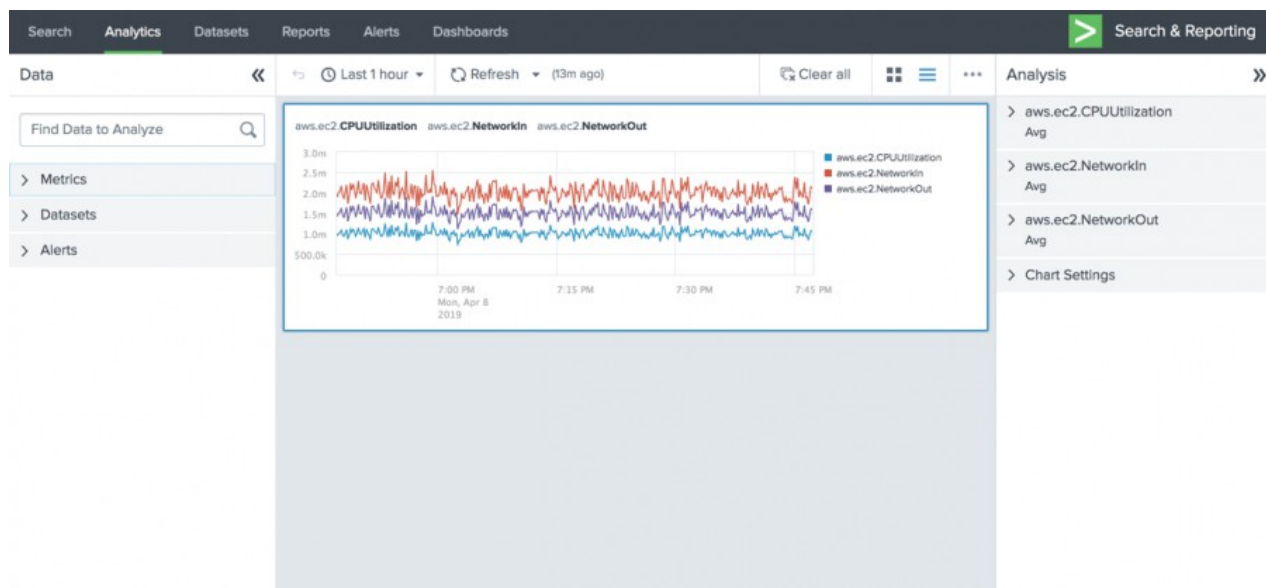
For more information about Analytics Workspace alerts, see [Alerts in the Analytics Workspace](#).

Using the Analytics Workspace

Charts in the Analytics Workspace

Select a source from the Data panel to view your data in a chart in the Analytics Workspace. You can either create a new chart or add additional measurements to an existing chart. Each chart contains one or more time series based on at least one aggregation. Hover over any point on the chart to see the corresponding values in the chart legend.

Charts appear in the main panel of the Analytics Workspace. The following chart shows average values for the `aws.ec2.CPUUtilization`, `aws.ec2.NetworkIn`, and `aws.ec2.NetworkOut` metrics.



To learn how to apply analytic operations to charts, see [Analytics in the Analytics Workspace](#).

View charts in the workspace

View a chart in the Analytics Workspace to see your data represented as a time series.

1. In the Data panel, search or browse for the data source that you want to view in a chart.

Option	What to do
Search for a data source	In the search box, type part or all of the data source name. The list of available data sources for each data type filters to match your criteria.
Browse available data sources	Click the tab for the type of data that you want to visualize in the workspace. Browse through the tree of available data sources.

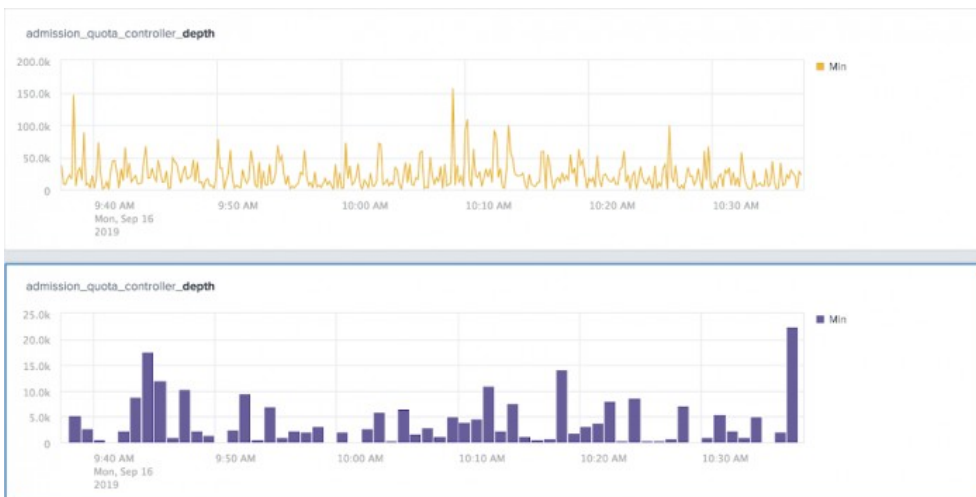
2. Select the data source you want to view as a time series.

The data source appears as a chart in the main panel of the Analytics Workspace. For example, the following chart shows the aggregate average values for the `aws.ec2.CPUUtilization` metric.

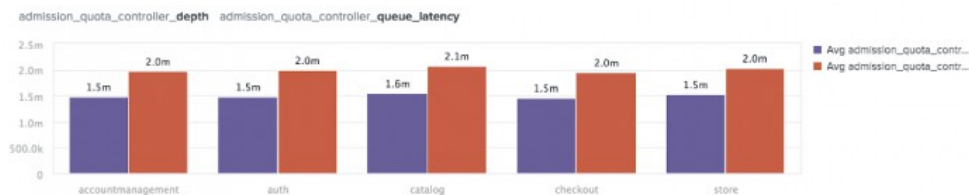


Change the chart type

Two types of charts are available, time and categorical. Time charts show data over time allowing you to quickly visualize trends in your data. The data can be shown as a line, column, area, or heatmap chart. and can be split by dimensions. The following time chart example shows admission_quota_controller_depth values as a line chart and a column chart.



Categorical charts show data over time, grouped by data dimensions, allowing you to analyze and compare different dimensions across multiple metrics. The data can be shown as a column or stacked column chart and can be split by dimensions. The following categorical chart example shows admission_quota_controller_depth and admission_quota_controller_queue_latency as a column chart and a stacked column chart.



Choose a chart type that best displays the data you are viewing.

1. In the main panel of the Analytics Workspace, click the chart that you want to configure.
2. In the Analysis panel, click on Chart Settings.
3. From the drop-down list in the chart type panel, select the chart type you want to use.

Chart type	Chart style	Description
Time charts	Line	A chart showing the data over time as a series of points connected by straight line segments.
	Area	A chart showing the data over time similar to the line chart, with the area between the axis and line filled with a solid color.
	Column	A chart showing the data over time as a series of vertical bars. The span of the columns will automatically scale for readability.
	Heatmap	A chart showing the data over time as a heatmap. The chart is shown as a matrix with values represented as colors.
Categorical charts	Column	A chart showing the data as a series of vertical bars grouped by category. Alerts are disabled for this chart type.
	Stacked Column	A chart showing multi-series data as stacked vertical bars grouped by the common dimension of the series and the respective categories. Alerts are disabled for this chart type.

Set the Time Span for a chart

You can define the time span or size of each bucket of data that is used to plot a data point in your chart. The default is *auto* which is calculated based on the type of chart and the global time setting. For example, a line chart with a 1-hour time range will have an automatically calculated time span of 10 seconds per data point.

Each chart shows the current time span in the top left corner.



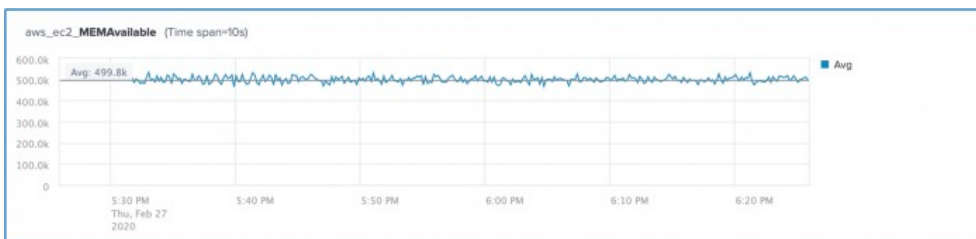
Set a custom time span for your chart:

1. In the main panel of the Analytics Workspace, click the chart that you want to configure.
2. In the Analysis panel, click on Chart Settings.
3. In the Chart Settings panel, select the pencil (✎) icon under **Time Span**.
4. Enter the time span value and select the time units from the drop down list. Time span must be entered as an integer value.
5. Click **Update** and the chart is updated to show the data with the new time span.â ¨

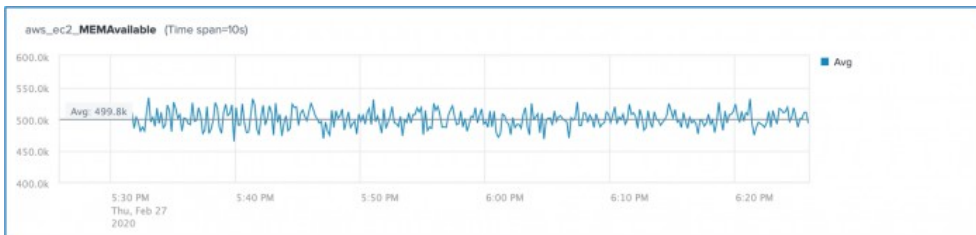
See **<span-length>** in mstats in the *Search Reference* manual for more information about time spans.

Set the Y-Axis scaling on a chart

The data shown in a chart can be clustered within a small range along the y-axis.



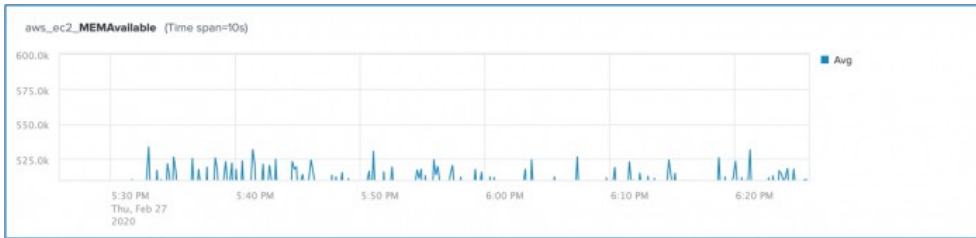
You can set the minimum and maximum values for the left y-axis or the left and right y-axis if **Overlay on right axis** is enabled. The y-axis scaling allows you to zoom in on the data making it easier to draw insights from the data presented. The default is *auto* which sets the Min value to 0, and the Max value is calculated based on reference lines, defined thresholds, and custom padding.



Set the y-axis scaling for your chart:

1. In the main panel of the Analytics Workspace, click the chart that you want to configure.
2. In the Analysis panel, click on Chart Settings.
3. In the Chart Settings panel, select the pencil (✎) icon under **Y-Axis**.
4. Enter the Min Value and Max Value for the Y-Axis.
5. Select Linear or Log scale.
6. Click **Update** and the chart is updated to show the data with the new y-axis scaling. â ¨

If you set a custom Min value that is greater than the smallest value in your data, or you set a Max value less than the largest value in your data, some of the chart data will fall outside the limits you have sent and the data cannot be shown. You can correct this by setting a new Min or Max value or revert the y-axis scaling to the default settings.




View multiple metrics on a chart

View multiple metrics on the same chart to see how your metrics relate to one another. You can add additional metrics to a chart to analyze correlations in your data.

1. In the main panel of the Analytics Workspace, click the chart that you want to add another metric to. Your selected chart appears outlined with a blue border.
2. In the Data panel, search or browse for the data source that you want to add to the chart. Supported data types for multi-series charts include metrics and datasets.

Option	What to do
Search for a data source	In the search box, type part or all of the data source name. The list of available data sources for each data type filters to match your criteria.
Browse available data sources	Click the tab for the type of data that you want to visualize in the workspace. Browse through the tree of available data sources.

3. Hover over the data source that you want to add to the chart. The Add to selected chart () icon appears.

SearchAnalyticsDatasetsReportsAlertsDashboards

Data

Find Data to Analyze

Metrics

aws.ec2

CPUUtilization

MEMAvailable

NetworkIn

NetworkOut

Last 1 hour

Refresh

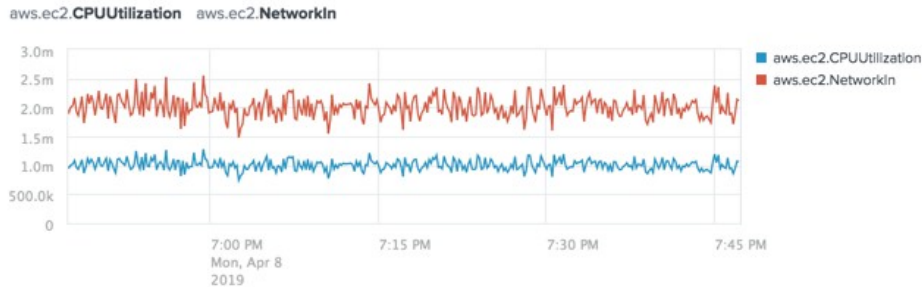
aws.ec2.CPUUtilization

7:00 PM
Mon, Apr 8
2019

12


4. Click the Add to selected chart () icon to add the data source to the chart.

The data source appears as an additional time series on your selected chart. For example, the following chart shows the aggregate average values for the `aws.ec2.CPUUtilization` and `aws.ec2.NetworkIn` metrics:



Remove a time series from a chart

Remove a time series from a chart to modify the metrics for your analysis.

1. In the main panel of the Analytics Workspace, select the chart that contains the time series that you want to remove.
2. In the Analysis panel, locate the name of the time series that you want to remove from the chart.
3. Next to the time series name, click the X () icon.

View chart actions

Click the ellipsis () icon in the top-right corner of a chart to view a list of chart actions.

Action	Description
Open in Search	Show the SPL that drives the chart's time series in the Search & Reporting App.
Search Related Events	View a list of log events that are related to any metric on the chart.
Save as Alert	Save one of the chart's time series as an alert.
Save as Dashboard Panel	Save the chart as a panel on a new or existing dashboard. Heatmap charts are saved as column charts.
Save as Report	Save the chart as a report. Enter report details and click Save . To access the report, click the Reports tab on the Search & Reporting navigation bar. Heatmap charts are saved as column charts.
Clone this Panel	Make a copy of the chart. Clone panels and then make adjustments to compare points in your data. Not available for alert panels.
Export as PNG	Export the chart as a PNG file.
Export as CSV	Export chart values as a CSV file.

Set the workspace time range

To help you compare time series, all charts in the workspace show the same time range. Hover over any chart to view a shared hairline.

The default time range for the workspace is one hour. Adjust the time range to gain more insight from your charts. If you notice a significant change in your data around an approximate time, narrow the time range to refine your analysis. If you

want to see a broader selection of data points, expand the time range to show trends over a longer period of time.

Modifying the workspace time range adjusts the portion of the index that you are analyzing. This change affects how aggregations are calculated on charts. For more information about how the time range affects data point calculations, see [Analytics in the Analytics Workspace](#).

Set the time range through either the time range picker or by zooming in on a chart.

Use the time range picker

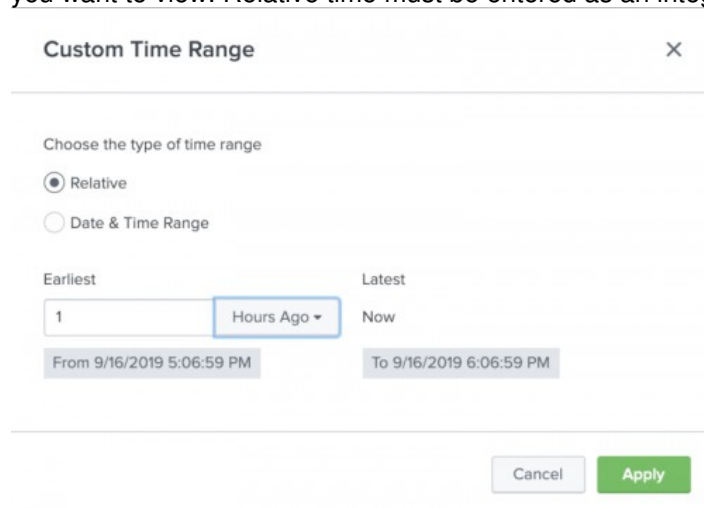
Use the time range picker to adjust the time range for all charts in the Analytics Workspace.

1. From the global actions bar of the Analytics Workspace, click the time range picker.
2. Select a preset time range from the list or when one of the preset time ranges is not precise enough for your search, select **Custom...** and enter a relative or specific date and time range.

Custom time ranges

You can use the Relative option to specify a custom time range relative to the current time. You can use the Date & Time Range option to specify a specific custom time range.

1. Click on the time range drop-down menu and select **Custom....**
2. If you want to view metrics in a time range relative to "now", select **Relative** and enter the earliest date and time you want to view. Relative time must be entered as an integer value.



The screenshot shows a dialog box titled "Custom Time Range" with a close button (X) in the top right corner. Inside the dialog, there is a section "Choose the type of time range" with two radio buttons: "Relative" (which is selected) and "Date & Time Range". Below this, there are two columns of input fields. The left column is labeled "Earliest" and contains a text input with the value "1" and a dropdown menu currently showing "Hours Ago". Below this input is a greyed-out box displaying "From 9/16/2019 5:06:59 PM". The right column is labeled "Latest" and contains a text input with the value "Now". Below this input is a greyed-out box displaying "To 9/16/2019 6:06:59 PM". At the bottom of the dialog, there are two buttons: "Cancel" and "Apply".

3. If you want to view metrics in a specific time range, select **Date & Time Range** and enter the start and end dates and times. Date & Time Range supports all valid date and time formats. See Time modifiers for more information on the supported date and time formats.

Custom Time Range X

Choose the type of time range

☐ Relative

☒ Date & Time Range

Earliest Latest

2019-09-01 12:00 2019-09-10 12:00

From 9/1/2019 12:00:00 PM To 9/10/2019 12:00:00 PM

Cancel Apply

4. Click **Apply**.

See Specifying time ranges for more information on specifying time ranges.

Zoom in to a custom time range

Zoom in to a custom time range to analyze data from a specific time period.

1. Select a chart in the workspace to zoom in on.
2. Click and drag your cursor over the time period you want to view.

All charts show your selected time range.

To undo the zoom, click the back arrow in the top-left corner of the main panel. The time range reverts to the previous setting.

Recover workspace charts

Charts in the Analytics Workspace are automatically backed up to your local system. If you accidentally navigate away from the workspace, you have the option to restore your session in the same browser.

Disable automatic chart recovery

You also have the option to disable automatic chart recovery using the `workspace.conf` file.

1. Navigate to the `packages/splunk_metrics_workspace/src/main/resources/splunk/default` directory on your local file system.
2. Open `workspace.conf`.
3. In the `features` stanza, add the following line: `state_restore = 0`.
4. Restart Splunk Enterprise.

If you are using Splunk Cloud Platform, you cannot disable chart recovery.

For more information about saving charts as dashboard panels, see [Dashboards in the Analytics Workspace](#).

For more information about saving charts as alerts, see [Alerts in the Analytics Workspace](#).

Data sources in the Data panel in the Analytics Workspace

In the Data panel, you can search or browse for the data source that you want to view in a chart in the main panel of the Analytics Workspace. Filter on metrics data sources to narrow down the data sources that you want to use.

Filter on metrics data sources

To more easily find the data source that you want, click **+Add new filter** to filter the available data sources. You can filter by different fields and field values, such as by index or host.

For example, first select one or more metric indexes you want to use to filter. Then, select the specific metric and add the chart to your workspace. The chart header shows your filter selections.

Filter on metrics data source indexes by time range

By default, the number of metrics you can see in the data panel is based on the data ingested in the last 15 minutes. For a metric to show in the data panel, the metric must occur at least once within the set time range and the index must have ingested data for that metric within the same time range.

To change the time range for the data panel metrics click on the **Last 15 minutes** link at the bottom of the data panel, and select a predefined relative time range or set a custom time range using the time range picker. The time range selected here will not affect the global time range for the workspace.

Analytics in the Analytics Workspace

Configure analytic functions and operations in the Analysis panel to gain insight from your charts. All analytic functions generate Splunk Search Processing Language (SPL) in the background.

Perform separate analytics for each time series on a chart. For more information about charts, see [Charts in the Analytics Workspace](#).

View additional time series for a metric

View additional time series for a metric to analyze different facets of your data. You can clone a time series to compare data based on a different aggregation, dimension, time range, or set of filters.

1. In the main panel of the Analytics Workspace, select the chart that you want to modify.
2. In the Analysis panel, locate the name of the time series that you want to clone.
3. Next to the time series name, click the Clone (📄) icon.

A duplicate of the time series appears on the chart. You can modify this time series in the Analysis panel. After you configure the new series, it appears in the chart legend.

Configure aggregations

Charts in the Analytics Workspace contain time series based on aggregated data. To calculate aggregations, data points within the same approximate time frame are categorized into buckets. Aggregations are calculated from data points in the same bucket. The bucket size, or span, is automatically configured based on your specified time range. Increasing the time range causes the span to increase automatically.

You can add multiple time series to a chart to view different aggregations of your data. To maintain a separate scale for an aggregation, display the time series on the right vertical axis of the chart.

The following aggregations are available:

Aggregation	Use	Description
Average (Avg)	Numeric data	Average value from each bucket of data. Default aggregation for numeric data.
Maximum (Max)	Numeric data	Maximum value from each bucket of data.
Minimum (Min)	Numeric data	Minimum value from each bucket of data.
Standard deviation (Std dev)	Numeric data	Standard deviation for each bucket of data.
Sum	Numeric data	Sum of values from each bucket of data.
Percentiles	Numeric data	Percentile values from each bucket of data. Default percentiles are 90 and 99. To configure additional percentiles, enter a percentile value between 1 and 99 in the <code>Aggregation</code> field. For example, to view the 25th percentile, type <code>p25</code> .
Count	String data	Number of values in a dataset field within each bucket of data. Default aggregation for string data.
Distinct count (Dist count)	String data	Number of distinct values in a dataset field within each bucket of data.

Select an aggregation

Select an aggregation to specify which facet of your data to view as a time series.

1. In the main panel of the Analytics Workspace, select the chart that you want to configure.
2. In the Analysis panel, select the time series that you want to modify the aggregation for.
3. Under the `Aggregation` field, select or type the aggregation to apply.
4. (Optional) To move the vertical axis for your selected time series to the right side of the chart, click the **Display on right axis** checkbox.

Examples

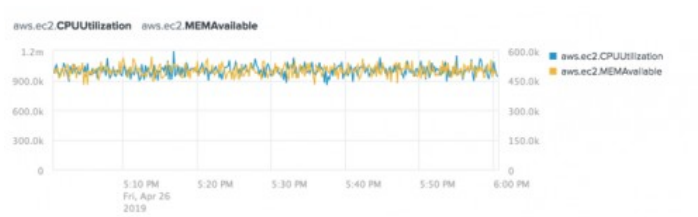
The following chart shows the `Average`, `Maximum`, and `Minimum` aggregations for the `aws.ec2.MEMAvailable` metric.



The following chart shows the 25th, 50th, and 75th Percentile aggregations for the `aws.ec2.CPUUtilization` metric.



The following chart shows the Average aggregation for the `aws.ec2.CPUUtilization` and `aws.ec2.MEMAvailable` metrics. The `aws.ec2.MEMAvailable` metric displays on the right axis of the chart.



Compare time ranges

Shift the time range of a series to investigate whether your data has changed significantly over time.

Shifting the time range is not available for datasets.

Shift the time range of a series

Shift the time range of a series to compare changes in your data over time. Shifting the time range replaces the original series with a series of your selected time range.

Prerequisites

To compare two time ranges for a metric, you first need to clone the original series. For more information, see [View additional time series for a metric](#).

Steps

1. In the main panel of the Analytics Workspace, select the chart that you want to configure.
2. In the Analysis panel, select the time series that you want to shift the time range for.
3. Under the `Time Shift` field, select an earlier time range from the list of preset time shifts or select **Custom** and enter the number and the time shift that you want to display.

Time-shifted series appear as dotted lines on the chart.

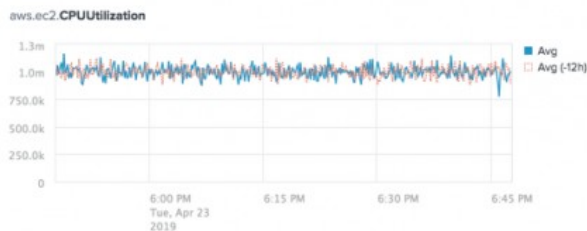
Remove a time shift from a series

Remove a time shift from a series to restore the original time range.

1. In the main panel of the Analytics Workspace, select the chart that you want to configure.
2. In the Analysis panel, select the time series that you want to remove the time shift from.
3. Under the `Time Shift` field, select **None** from the drop-down list.

Examples

The following chart compares current average `aws.ec2.CPUUtilization` values to the values from 12 hours prior.



Split time series by dimension

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

The highest and lowest dimension values are calculated based on the overall highest and lowest data points. Therefore, it is possible for a single dimension value to appear in both the highest and lowest categories. For example, imagine you have two charts in the workspace. The first chart shows CPU utilization split by the top five highest apps, and the second chart shows CPU utilization split by the top five lowest apps. If the data for a particular app contains a high level of variation and has both high and low CPU utilization levels, the app could appear on both charts.

Split a time series by a dimension

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

1. In the main panel of the Analytics Workspace, select the chart that you want to configure.
2. In the Analysis panel, select the time series that you want to split by a dimension.
3. Under the `Split By` field, select the dimension that you want to split.
4. Under the dimension name, select **Highest** or **Lowest** to view either the highest or lowest spikes in data.
5. Select the number of values to display.

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

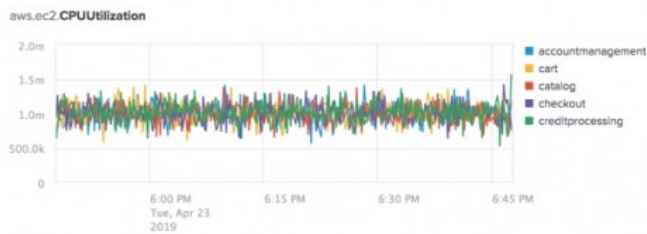
Remove a dimension split

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

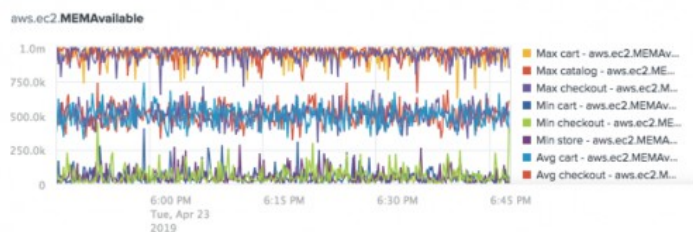
1. In the main panel of the Analytics Workspace, select the chart that you want to configure.
2. In the Analysis panel, select the time series that contains the dimension split that you want to remove.
3. Under the `Split By` field, select **None**.

Examples

The following chart shows the **Average** aggregation for the `aws.ec2.CPUUtilization` metric split by the top five apps.



The following chart shows the **Average**, **Maximum**, and **Minimum** aggregations for the `aws.ec2.MEMAvailable` metric split by the top three apps.



Filter data by dimension

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

Use wildcards from within the filter panel to filter for a dimension with a high number of values. For information about using wildcards in the Splunk platform, see *Wildcards in the Search Manual*.

Filter by dimension value from the Analysis panel

Filter time series data to view a specific subset of dimension values.

1. In the main panel of the Analytics Workspace, select the chart that you want to configure.
2. In the Analysis panel, select the time series that you want to filter by dimension.
3. Under the **Filters** field, click **+ Add New Filter**.
4. From the drop-down list in the filter panel, select the dimension you want to filter.
5. Click the radio button for **Include** or **Exclude** to add or remove the dimension values.
6. From the list of dimension value names, select the dimension values you want to filter in the time series.

If the list contains more than 12 dimension values, a search bar appears. Type part or all of the dimension value name into the search bar to refine the list. Wildcards are supported.

7. After you finish configuring the filter, click **Add**.

The time series shows data for the dimension values that you selected.

Filter by dimension value from the chart legend

If a time series is already split by a dimension, filter by dimension value using the legend to the right of the chart.

Prerequisites

Split a metric by a dimension. See [Split a time series by a dimension](#) for more information.

Steps


1. From the main panel of the Analytics Workspace, select the chart you want to filter by dimension value.
2. In the chart legend, click 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.

Remove or modify dimension value filters

Remove or modify filters to adjust the dimension values that appear in a time series.

1. From the main panel of the Analytics Workspace, select the chart you want to configure.
2. In the Analysis panel, select the time series that you want to remove or modify filters for.
3. Under **Filters**, locate the name of the dimension filter that you want to change.
4. Follow the steps to remove or modify the filter.

Option	What to do
Remove the filter	Next to the filter name, click the X () icon.
Modify the filter	<ol style="list-style-type: none">1. Click the filter name to open the filter panel.2. Adjust the settings for the filter.3. Click Update.

The chart shows data for your updated filters.

Examples

The following chart shows the **Average** aggregation for the `aws.ec2.CPUUtilization` metric split by the `App` dimension and filtered to show time series for the `accountmanagement`, `auth`, and `cart` dimension values.



The following chart shows the **Average** aggregation for the `aws.ec2.NetworkIn` and `aws.ec2.NetworkOut` metrics split by the `App` dimension and filtered to show time series for the `catalog` dimension value.



Stack time series in an area chart

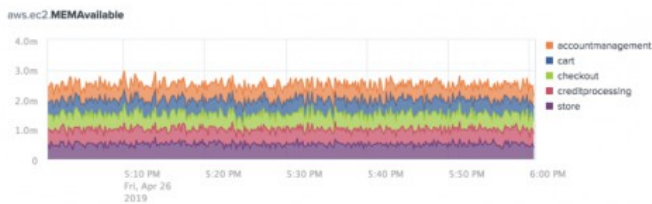
Stack the time series on an area chart to see how each series relates to the chart's data as a whole. Stacking time series in an area chart shows the sum of dimension values. In an area chart, each series appears as a filled-in area on the chart.

Stacking in an area chart is only supported for series using the left vertical axis of the chart.

1. In the main panel of the Analytics Workspace, select the chart that you want to stack the series for.
2. In the Analysis panel, click **Chart Settings**.
3. From the Chart Type drop-down menu, select **Area**.

Examples

The following chart shows the `Average` aggregation for the `aws.ec2.MEMAvailable` metric split by the `App` dimension. The series is stacked to show the sum of the top five apps.



Distinguish metrics with the same metric name

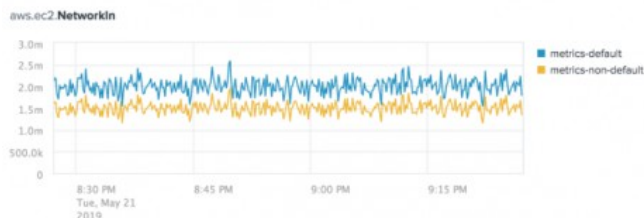
If two metrics with the same name are ingested into different indexes, they appear aggregated in the Analytics Workspace. You can distinguish metrics with the same metric name by either splitting the metric by the index dimension or by creating an index filter.

Split the metric by the index dimension to show a separate time series for each index. To learn more, see [Split a time series by a dimension](#).

Create an index filter to include or exclude metric values from a specific index. For more information, see [Filter data by dimension](#).

Examples

The following image shows a chart of the `Average` aggregation for the `aws.ec2.NetworkIn` metric split by index. There are two indexes with the `aws.ec2.NetworkIn` metric name: `metrics-default` and `metrics-non-default`.



Add reference lines

Add reference lines to compare, reference, or highlight data on your charts. You can add one or more reference lines to your charts.

1. In the main panel of the Analytics Workspace, select the chart that you want to modify.
2. Under the **Reference Lines** field, click **+ Add New Reference Line**.
3. Click the radio button to set the reference line calculation to **Raw Data** which calculates and adds a reference line based on the underlying index data, or **Constant Value** which adds a static reference line to the chart.
4. If you are using raw data calculations, select the calculation method you want to use for your reference line from the **Value** dropdown list.
5. If you are using constant value reference lines, type a constant value in the **Value** field.
6. Enter an optional label for your reference line. If you do not enter a label, the aggregation name is used for the reference line label.
7. Select the **Include Value** checkbox to add the calculated or static value to the reference line label.
8. Click **Add**.

Examples

The following image shows a chart of the `spl.intr.resource_usage.PerProcess.data.pct_cpu` metric, with a reference line indicating the **Average** of the indexed data.



Alerts in the Analytics Workspace

Use alerts to monitor and respond to specific behavior in your data. Analytics Workspace alerts are based on a specific chart. Alerts use a scheduled search of chart data and trigger when search results meet specific conditions.

To create alerts in the workspace, you need specific permissions. See [Requirements for the Analytics Workspace](#) for details.

To learn more about alerting in the Splunk platform, see Getting started with alerts in the *Alerting Manual*.

Parts of an alert

Alerts in the Analytics Workspace consist of alert settings, trigger conditions, and trigger actions.

Alert settings

Configure what you want to monitor in alert settings. Alert settings include:

- Alert title
- Alert description
- Permissions. Whether the alert is private or shared in the workspace.
- Alert Type. Scheduled alerts periodically search for trigger conditions. Streaming alerts continuously search for trigger conditions. Streaming alerts can also reduce search processing load by enabling similar alerts to share the same search process.
- How often you want to check alert conditions. For example, "Evaluate every 10 minutes".

Trigger conditions

Set trigger conditions to manage when an alert triggers. Trigger conditions consist of an aggregation to measure, a threshold value, and a time period to evaluate.

For example, set trigger conditions to "Alert when **Avg** (over 10-second intervals) **cpu.usage** is **greater than 10k** in the last **20 minutes**". The alert triggers when the aggregate average for cpu.usage exceeds 10,000 at any point in the last twenty minutes.

An alert does not have to trigger every time conditions are met. Throttle an alert to control how soon the next alert can trigger after an initial alert.

Trigger actions

Configure trigger actions to manage alert responses. By default, you can view detailed information for triggered alerts on the **Triggered Alerts** page in Splunk. To access the **Triggered Alerts** page, select **Activity > Triggered Alerts** from the top-level navigation bar.

Specify a severity level to assign a level of importance to an alert. Severity levels can help you sort or filter alerts on the **Triggered Alerts** page. Available severity levels include Info, Low, Medium, High, and Critical.

For detailed information about the various actions that can be set up for triggered alerts, see Set up alert actions in the *Alerting Manual*.

The *Alerting Manual* also has instructions for configuring mail server settings so Splunk can send email alerts. See Email notification action.

Create an alert

Create an alert in the Analytics Workspace to monitor your data for certain conditions.


1. In the main panel, select the chart you want to use for the alert.
2. Click the ellipsis (" ") icon.
3. Click **Save as Alert**.
4. If your chart contains more than one time series, select the time series you want to use for the alert from the Source list.
5. Fill in the Settings and Trigger Conditions for your alert.
6. (Optional) Under Trigger Actions, click the **+ Add Actions** drop-down list, and select additional actions for when the alert triggers. Triggered alerts are added to the **Triggered Alerts** page in the Splunk platform by default.

7. Click the **Severity** drop-down list, and select a severity level for the alert.
8. Click **Save**.

Manage alerts



View alerts that were previously created in the Analytics Workspace to monitor and respond to alert activity. Alerts show the same time range and hairline as other charts. Add an alert to the workspace through the Data panel. For more information, see [Types of data in the Analytics Workspace](#).

Alert chart actions

Click the ellipsis () icon in the top-right corner of an alert chart to view a list of alert chart actions.


Action	Description
Edit Alert	Modify alert conditions.
Open in Search	Show the SPL that drives the alert in the Search & Reporting App.
Clone this Panel	Open the alert query in a metrics chart for further analysis.
Search Related Events	View a list of related log events.

Alert details



Select an alert in the Analytics Workspace to view its details. Alert details show in the Analysis panel. These details include the settings, threshold, and severity level configured for the alert. A scheduled alert displays the scheduled alert () badge next to the alert title. A streaming alert displays the streaming alert () badge next to the alert title.

Show triggered instances to see when alert conditions are met.

1. In the main panel, select the alert to show triggered instances.
2. In the Analysis panel under Settings, select **Show triggered instances**.

Triggered instances appear as  annotations on the chart.

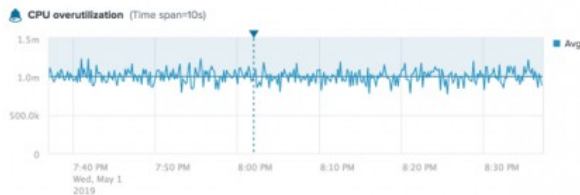
Triggered instance annotations appear at the end of the evaluation window in which the alert triggers, not at the time the alert threshold is crossed.

Use alert badges ( and ) to 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.

Severity level	Badge color
No trigger	Gray
Info	Blue
Low	Green
Medium	Yellow
High	Orange
Critical	Red

Example

The following alert shows CPU overutilization for the `aws.ec2.CPUUtilization` metric.



This alert is based on the aggregate average values for the `aws.ec2.CPUUtilization` metric. The blue alert badge indicates a severity level of Info. The horizontal blue line shows the alert threshold (1.0m). The ▼ annotations show triggered instances for the alert.

Follow up on alerts

Follow up on a triggered alert to perform additional analysis of the underlying data. To investigate a situation highlighted in an alert, open the alert query in a metrics chart.

Analyze a triggered alert in a metrics chart

To perform additional analysis of alert conditions, clone the alert in the Analytics Workspace.

1. In the Data panel, search or browse for the alert that you want to investigate.
2. Click on the alert name to open the alert in the Analytics Workspace.
3. To view a list of alert chart actions, click the ellipsis (" ") icon in the top-right corner of the alert chart.
4. Click **Clone this Panel**.

The alert query opens in a new metrics chart in the Analytics Workspace. You can perform additional analytic functions, such as filtering, modifying the time range, and splitting the chart by a dimension, to follow up on the conditions that triggered the alert.

Streaming metrics alert features not available in the Analytics Workspace

There are a few features for streaming metric alerts that are available only to users who can make direct edits to `metric_alerts.conf`, where streaming metric alert configurations are stored, or engage with the `alerts/metric_alerts` REST API endpoint.

Additional alert feature	Description	Setting
Set multiple group-by dimensions	You can identify a list of group-by dimensions for an alert. This results in a separate aggregation value for each combination of group-by dimensions, instead of just one aggregation value. The Splunk software evaluates the alert against each of these aggregation values.	<code>groupby</code>
Define complex <code>eval</code> expressions for alert conditions	You can set alert conditions that include multiple Boolean operators, <code>eval</code> functions, and metric aggregations. They can also reference dimensions specified in the <code>groupby</code> setting.	<code>condition</code>
Adjust lifespan of triggered streaming metric alert records	By default, records of triggered streaming metric alerts live for 24 hours. You can adjust this time on a per-alert basis for streaming metric alerts.	<code>trigger.expires</code>

Additional alert feature	Description	Setting
Adjust maximum number of triggered alert records for a given streaming metric alert	By default, only 20 triggered alert records of a given streaming metric alert can exist at any given time. You can raise or lower this limit on a per-alert basis according to your needs.	<code>trigger.max_tracked</code>

For more information, see the `metric_alerts.conf` topic in the *Admin Manual*.

The streaming metric alert settings are also documented in the context of the `alerts/metric_alerts` endpoint in the *REST API Reference Manual*.

Dashboards in the Analytics Workspace

Dashboards are saved views that consist of one or more panels. Use dashboards to monitor real-time trends in your data or to share visualizations with your colleagues. Save one or more charts in the Analytics Workspace to new or existing dashboards.

Not all chart types and features are available in dashboards:

- You cannot save alert charts to a dashboard.
- Reference lines do not appear on charts in dashboards.
- Heatmap charts are converted to column charts when you save them to a dashboard.

For more information about dashboards in the Splunk platform, see the Dashboard overview in the *Dashboards and Visualizations Manual*.

Save workspace content as a new dashboard

You can choose to save workspace content to a new XML dashboard in the Analytics Workspace, or export your workspace content to a new dashboard in the Dashboards app (beta). To learn about the Dashboards app (beta), see *What is the new Splunk Dashboards app?* in the *Splunk Dashboards App Manual*.

Save workspace content as a new XML dashboard in the Analytics Workspace

1. Select either the entire workspace or an individual chart.

Option	What to do
Save entire workspace	Click the ellipsis (<code>⋮</code>) icon from the global actions bar, and select Save to Dashboard (XML) .
Save individual panel	Click the ellipsis (<code>⋮</code>) icon from the panel you want to save in a dashboard, and select Save to Dashboard (XML) .

2. For Dashboard, select **New**.
3. Type a **Dashboard Title**.
4. Type a **Dashboard ID**. The ID is used as the file name and cannot be changed.
5. Type a **Dashboard Description**.
6. (Optional) Select **Add interactive time control**. Interactive time control connects all charts to a shared time range picker within the dashboard.
7. Specify permissions.
8. (Optional) If you are saving an individual panel, modify the Panel Title. The default Panel Title is the title of the workspace chart.
9. Click **Save**.

Save workspace content as a new dashboard in the Dashboards app (beta)

1. Select either the entire workspace or an individual chart.

Option	What to do
Save entire workspace	Click the ellipsis (⋮) icon from the global actions bar, and select Save all charts to Dashboards app (beta) .
Save individual panel	Click the ellipsis (⋮) icon from the panel you want to save in a dashboard, and select Save to Dashboards app (beta) .

2. Type a **Dashboard Title**.
3. (Optional) Type a **Dashboard Description**.
4. Select a Layout Option.
5. Specify permissions.
6. Click **Save**.

The Analytics Workspace automatically adds interactive time control when you export charts to the Dashboards app (beta). Interactive time control connects all charts to a shared time range picker within the dashboard.

Save workspace content to an existing dashboard

Add new charts to an existing XML dashboard in the Analytics Workspace. You cannot add new charts to an existing dashboard in the Dashboards app (beta).

1. Select either the entire workspace or an individual chart.

Option	What to do
Save entire workspace	Click the ellipsis (⋮) icon from the global actions bar, and select Save to Dashboard (XML) .
Save individual panel	Click the ellipsis (⋮) icon from the panel you want to save in a dashboard, and select Save to Dashboard (XML) .

2. For Dashboard, select **Existing**.
3. Select a dashboard from the list.
4. (Optional) If you are saving an individual chart, modify the Panel Title. The default Panel Title is the title of the workspace chart.
5. Click **Save**.

Access Analytics Workspace dashboards

Access dashboards created or edited in the Analytics Workspace in Splunk Enterprise.

1. Click the **Dashboard** tab on the Search & Reporting bar in Splunk Enterprise.
2. Select the dashboard you want to view.

For a step-by-step use case for creating a dashboard in the Analytics Workspace, see [Creating a dashboard in the Analytics Workspace](#).

Use Cases

Analyzing data in the Analytics Workspace

Your team manages a bike share program that allows users to check out bicycles using a mobile application.

To gain better insight into your business, you want to analyze the following metrics:

- Inventory status over time
- User availability checks over time
- Social media mentions over time
- User sentiment over time

This use case uses a metrics data source designed to help you get started with the Analytics Workspace. To work through this use case, you need the following:

- Admin-level access
- Unzipped sample data

Create a metrics index and upload the sample data using Splunk Web. Then locate and analyze your data in the Analytics Workspace.

1. [Create a metrics index](#)
2. [Upload data from a CSV file](#)
3. [Locate your data in the Analytics Workspace](#)
4. [Analyze your data in the Analytics Workspace](#)

Create a metrics index

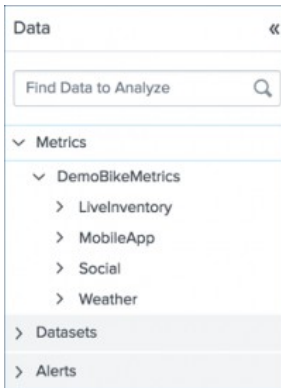
1. In Splunk Web, navigate to **Settings > Indexes** and click **New Index**.
2. For **Index Name**, type "bikes".
3. For **Index Data Type**, click **Metrics**.
4. For the remaining properties of the index, use the default values.
5. Click **Save**.

Upload data from a CSV file

1. In Splunk Web, go to **Settings > Add Data**.
2. Scroll down and click **Upload files from my computer**.
3. Under Select Source, click **Select File**.
4. Locate the `metrics-sample-bikes.csv` file in your file directory system, and click **Open**.
5. After the file uploads to Splunk Web, click **Next**.
6. Under Set Source Type, click the **Source type** drop-down list, and click **Metrics > metrics_csv**. Then click **Next**.
7. (Optional) On the Input Settings page, under Host, specify a host value.
8. On the Input Settings page, under Index, select **bikes**. Then click **Review**.
9. Review your data upload settings. Then click **Submit**.

Locate your data in the Analytics Workspace

1. Navigate to the Search & Reporting app.
2. Click the **Analytics** tab to open the Analytics Workspace.
3. In the Data panel, click **Metrics** to view a list of metrics data sources. DemoBikeMetrics appears in the list of metrics data sources.



Analyze your data in the Metrics Workspace

1. To view a chart showing checked-out bike inventory over time, click **Metrics > DemoBikeMetrics > LiveInventory > CheckedOut**.
2. In the global actions bar, click the time range picker, and select **Last 48 hours**. The workspace time range expands to show a wider range of data.
3. To view a chart showing user availability checks over time, click **Metrics > DemoBikeMetrics > MobileApp > AvailabilityCheckRequests**.



4. To view a chart showing social media mentions over time, click **Metrics > DemoBikeMetrics > Social > News**.
5. To view a chart showing user sentiment over time, click **Metrics > DemoBikeMetrics > Social > Sentiment**.



6. To view how your metrics vary based on location, click **Split By** in the main panel of the Analytics Workspace. Select **city** from the **Split By** menu and click **Apply**.
7. To view the workspace in grid layout, click the grid icon  in the global actions bar.

Summary

From the charts in the workspace, you can deduce that there is a positive correlation between checked-out inventory and user availability requests. There is also a positive correlation between social media mentions and user sentiment. These metrics all peak during certain times of the day, most likely during typical commute hours.

For more information about analyzing data in the Analytics Workspace, see [Analytics in the Analytics Workspace](#).

Creating a dashboard in the Analytics Workspace

Your team runs the online store for [buttercupgames.com](#). This website sells games online and tracks system metrics and logs from its online credit card payment service.

To get the most insight from your metrics, you want to set up a dashboard to monitor this data in real-time.

You have the following metrics:

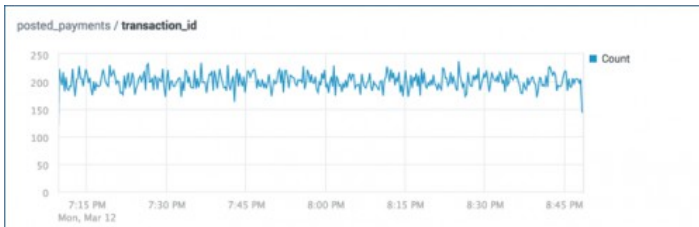
- Number of transactions over time
- Overall revenue over time
- Number of errors for the store and payment service

View each of your metrics as time series in the Analytics Workspace. Then save the charts to a dashboard in the Analytics Workspace.

1. [View number of transactions over time](#)
2. [View overall revenue over time](#)
3. [View number of errors for the store and payment service](#)
4. [Save the workspace to a dashboard](#)

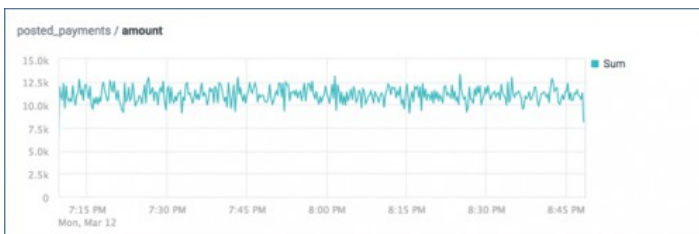
View number of transactions over time

1. In the Data panel, search or browse for the `posted_payments` dataset. This dataset contains the payment logs from your credit card payment provider.
2. Select the `transaction_id` field to create a chart.
3. In the Analysis panel, select the **Count** aggregation. Note that because the `transaction_id` dataset field is a string, the only available aggregations are **Count** and **Distinct count**.



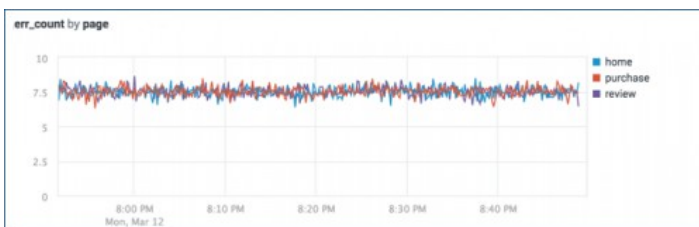
View overall revenue over time

1. In the Data panel, select the `amount` field from the `posted_payments` dataset. This creates a chart of your revenue.
2. In the Analysis panel, change the aggregation to **Sum**. The chart updates to show your aggregated total revenue over time.



View number of errors for the store and payment service

1. In the Data panel, search for `err`. The data hierarchy filters to include only data sources with names that contain `err`.
2. Select the `err_count` metric to create a chart.
3. In the Analysis panel, under **Split By**, select the `page` dimension. This splits the chart to show errors by page.
4. Under **Filters**, click **+ Add New Filter**. Select the `page` dimension. Then select the `home`, `purchase`, and `review` pages. The chart shows errors from these three pages.



Save the workspace to a dashboard

1. From the global actions bar, click the ellipsis (`...`) icon and select **Save to Dashboard (XML)**.
2. Enter the dashboard details. Leave the **Add interactive time control** option selected, so that you can adjust the time range later.
3. Click **Save**.

Save All To Dashboard

Dashboard

NewExisting

Dashboard Title

Buttercup games online store

Dashboard ID ⓘ

buttercup_games_online_store

Can only contain letters, numbers and underscores.

Dashboard Description

This dashboard shows the number of transactions, overall revenue, and error count for the online store.

Add interactive time control

☒

Permissions

PrivateShared in App

Cancel

Save

Summary

You now have a dashboard that monitors the number of transactions over time, overall revenue over time, and the number of store and payment service errors. To view your dashboard, click the **Dashboard** tab on the Search & Reporting bar. Then select the dashboard from the list.

For more information about dashboards in the Splunk platform, see the Dashboard overview in the *Dashboards and Visualizations Manual*.

For more information about dashboards in the Analytics Workspace, see [Dashboards in the Analytics Workspace](#).

Resources

Troubleshoot the Analytics Workspace

You might encounter the following issues while using the Analytics Workspace.

Metrics do not appear in the Data panel

No metrics data sources appear in the Data panel.

Diagnosis

The following issues can cause metrics to not appear in the Data panel:

- No metrics with timestamps in the past 24 hours are available.
- The technical add-ons and agents you use to send and ingest metrics malfunctioned.

Solution

1. Verify that Splunk Web ingested no metrics with timestamps in the past 24 hours.
2. (Optional) Expand the time range for ingested metrics by modifying the `earliest` parameter in the `metadata` stanza located in the app's `workspace.conf` file. Expanding the time range for ingested metrics might have a negative impact on performance.
3. Run the following search in the Search & Reporting app to verify that Splunk software is properly fetching metrics data:

```
| mcatalog values(metric_name) as metrics WHERE NOT ("_dims"="rollup_aggregate" OR
"_dims"="rollup_span" OR "_dims"="rollup_source_index") AND ("index"="*" OR "index"="_*" )
earliest=-1d BY index | mvexpand metrics limit=20000
```

The search results match the list of metric names in the Analytics Workspace Data panel.

4. Investigate whether the technical add-ons and agents you use to ingest metrics are functioning properly.

Data panel does not contain datasets

No datasets are listed in the Data panel.

Diagnosis

Datasets are not accelerated.

Solution

1. Verify that the dataset is shared with you.
2. Click the **Datasets** tab on the Splunk Enterprise Search & Reporting navigation bar.
3. Check whether the dataset is accelerated. Accelerated datasets are designated by the lightning bolt (⚡) icon.

For more information, see Accelerate data models in the *Knowledge Manager Manual*.

Chart does not contain data

You are able to select a data source, but no data appears on the chart.

Diagnosis

The following conditions are possible causes of this issue:

- There is no data within your selected time range.
- There is no data using your selected filters.
- You do not have access to the underlying index for the data.

Solution

1. Expand the time range to view a wider range of data.
2. In the Analysis Panel of the Analytics Workspace, adjust the filters to include a wider range of values.
3. Contact your administrator to verify your permissions.

For more information about Analytics Workspace permissions and capabilities, see [Requirements for the Analytics Workspace](#).

Some metrics are not shown or are missing from the Data panel

Some metrics are not shown or are missing from the list of available data sources in the Data panel.

Diagnosis

The maximum number of metrics that can be displayed in the Data panel is defined by `max_metrics` in `workspace.conf`. If the number of metrics exceeds this limit, an error message is shown.



Solution

Increase the limit for the maximum number of metrics that can be displayed in the Data panel:

1. Edit the following stanza in `workspace.conf` and increase the value for `max_metrics`:

```
[metadata]
max_metrics = 30000
```
2. Restart Splunk.