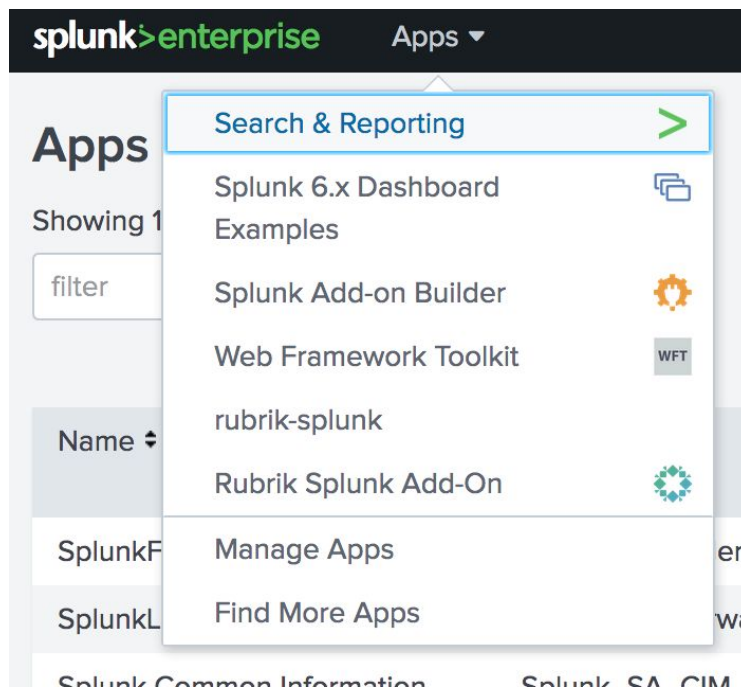


Rubrik Splunk Add-On

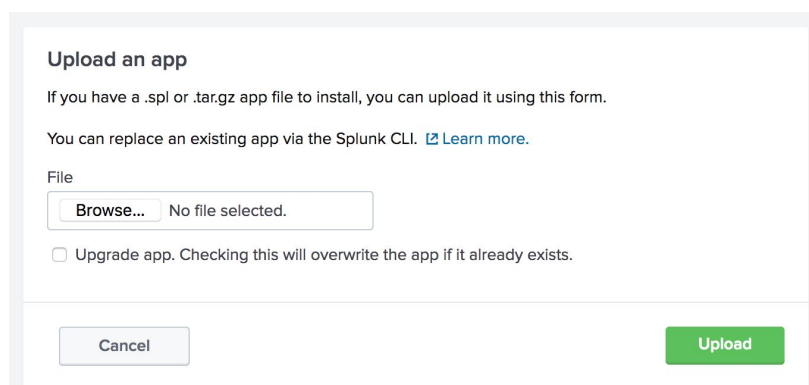
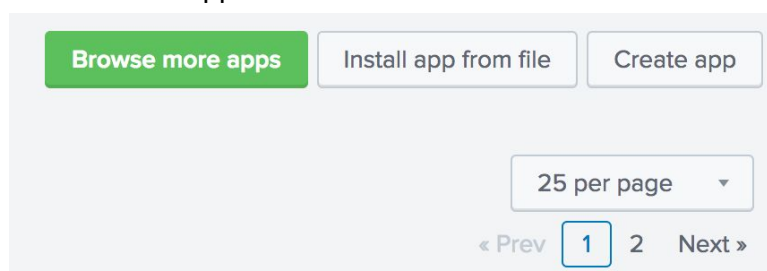
Installation and Setup Guide

Installing the Add-On - Fresh Install

1. Go to the 'Manage Apps' page in Splunk:



2. Select 'Install app from File':



3. Click 'Browse' and browse to the location of the exported add-on. Select the file and click 'Upload'. Splunk may ask to be restarted after upload.

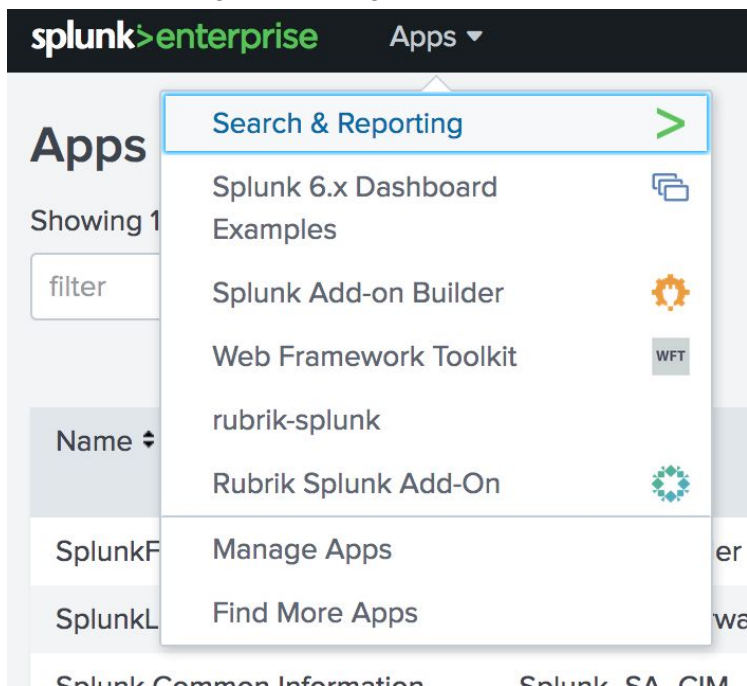
Restart Required
You must restart Splunk Enterprise to complete the update.

Restart Now

Restart Later

Installing the Add-On - Upgrade

- Go to the 'Manage Apps' page in Splunk:



- Select 'Install app from File':

Browse more apps

Install app from file

Create app

25 per page

« Prev

1

2

Next »

Upload an app
If you have a .spl or .tar.gz app file to install, you can upload it using this form.
You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

Browse...

No file selected.

☐ Upgrade app. Checking this will overwrite the app if it already exists.

Cancel

Upload

6. Click 'Browse' and browse to the location of the exported add-on, check the 'Upgrade app' box. Select the file and click 'Upload'. Splunk may ask to be restarted after upload.

The image shows two screenshots from the Splunk interface. The top screenshot is the 'Upload an app' form. It has a title 'Upload an app' and a description: 'If you have a .spl or .tar.gz app file to install, you can upload it using this form.' Below this, it says 'You can replace an existing app via the Splunk CLI. [Learn more.](#)'. There is a 'File' section with a 'Browse...' button and a text input field containing 'TA-rubrik-splunk-add-on-0.0.2.spl.gz'. Below the file input, there is a checkbox labeled 'Upgrade app. Checking this will overwrite the app if it already exists.' which is checked. At the bottom of the form are 'Cancel' and 'Upload' buttons. The bottom screenshot is a 'Restart Required' notification. It has a green checkmark icon and the text 'Restart Required'. Below this, it says 'You must restart Splunk Enterprise to complete the update.' At the bottom are 'Restart Now' and 'Restart Later' buttons.

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

TA-rubrik-splunk-add-on-0.0.2.spl.gz

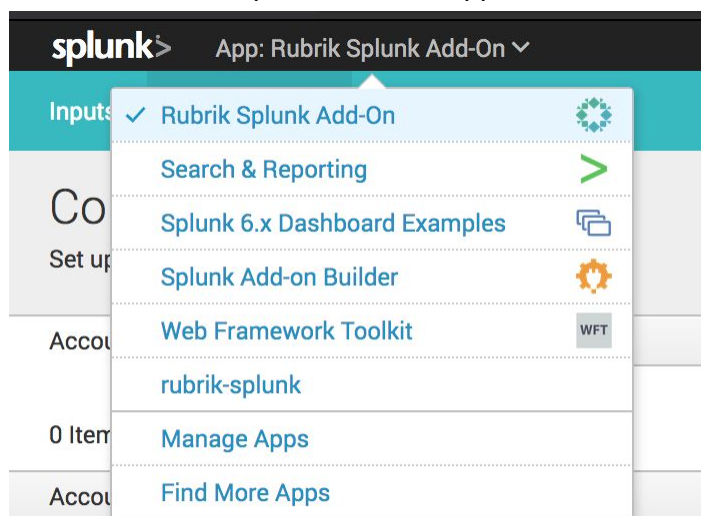
☒ Upgrade app. Checking this will overwrite the app if it already exists.

Restart Required

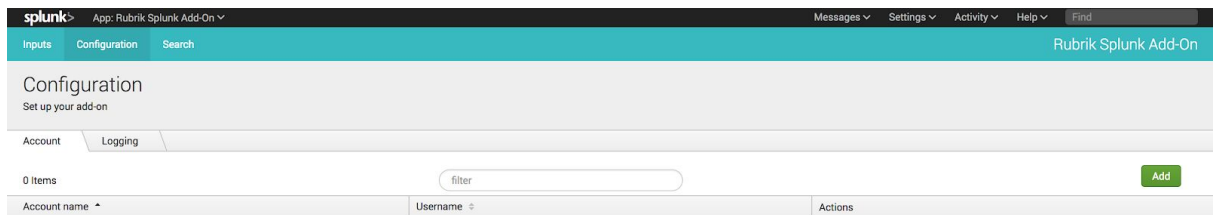
You must restart Splunk Enterprise to complete the update.

Credentials and Logging

1. Go to the 'Rubrik Splunk Add-On' application:



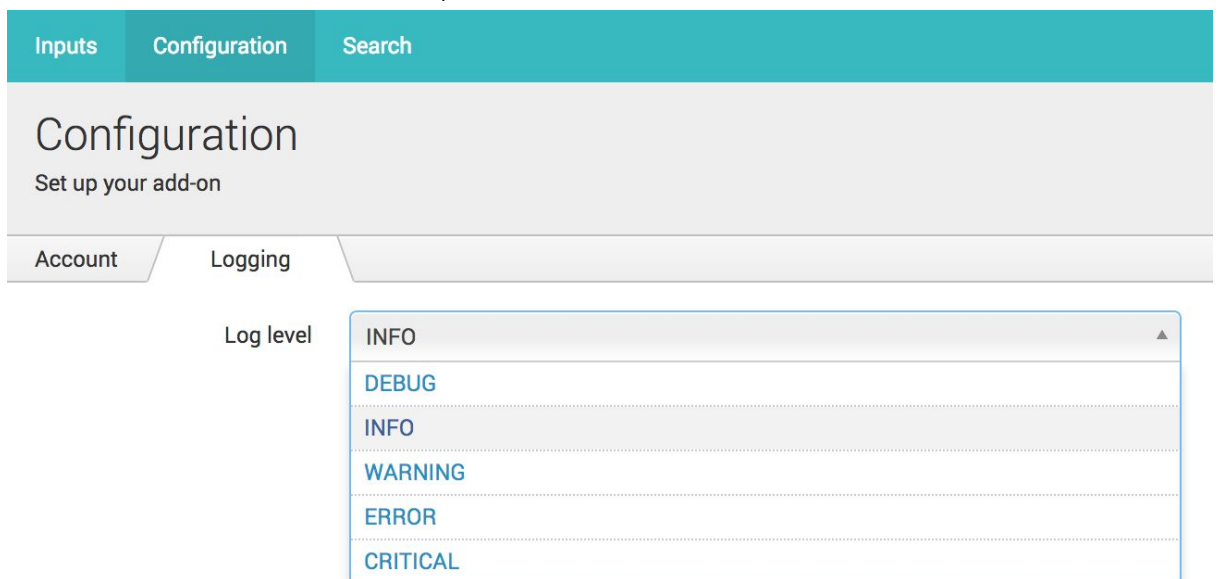
- Click the 'Configuration' tab, and click the 'Add' button:



- Enter a name for the credential, and the username and password:

The screenshot shows the 'Add Account' dialog box. It has a title bar with a close button. Inside, there are three input fields: 'Account name' with the value 'rangers_lab', 'Username' with the value 'tim.hynes@rangers.lab', and 'Password' with masked characters. Each field has a red asterisk indicating it's required. Below each field is a small instruction: 'Enter a unique name for this account.', 'Enter the username for this account.', and 'Enter the password for this account.' respectively. At the bottom, there are 'Cancel' and 'Add' buttons.

- Press Add.
- Click on the 'Logging' tab, and set the desired log level (INFO is the default, and should be fine for most use cases)



Creating Inputs

Inputs will be created for each of the input types, for each cluster to be monitored, these will define the systems to collect data from using the REST API.

There are four inputs required for the Rubrik Splunk application, the specifications for these are detailed below, followed by instructions on how to create an input:

Required Inputs

NOTE: If you are adding multiple Rubrik clusters, then it is a good idea to include a short version of the cluster name in the 'Name' field, in this case, replace 'rubrik' with the short name of your cluster.

NOTE: It is a good idea to use a floating IP address for the 'Rubrik Node' value - this will ensure that in the case of a node being unavailable, the data points can still be gathered. Instructions on setting up floating IPs can be found in the Rubrik User Guide.

Name	rubrik_runway_remaining
Interval	3600
Index	main
Global Account	<i><as defined in previous section></i>
Rubrik Node	<i><node or floating ip as desired></i>
Input Type	Rubrik - Runway Remaining

Name	rubrik_storage_summary
Interval	600
Index	main
Global Account	<i><as defined in previous section></i>
Rubrik Node	<i><node or floating ip as desired></i>
Input Type	Rubrik - Storage Summary

Name	rubrik_event_feed
Interval	60
Index	main
Global Account	<i><as defined in previous section></i>
Rubrik Node	<i><node or floating ip as desired></i>

Input Type	Rubrik - Event Feed
-------------------	---------------------

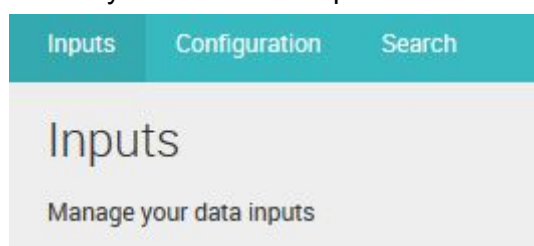
Name	rubrik_cluster_io_stats
Interval	60
Index	main
Global Account	<as defined in previous section>
Rubrik Node	<node or floating ip as desired>
Input Type	Rubrik - Cluster IO Stats

How to create an Input

1. Go to the 'Rubrik Splunk Add-On' in the application picker



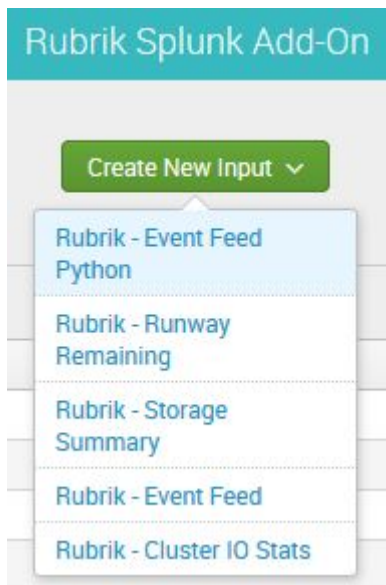
2. Ensure you are on the 'Inputs' tab



3. Click 'Create New Input'



4. Select the input type, as defined in the table in the last section, from the dropdown



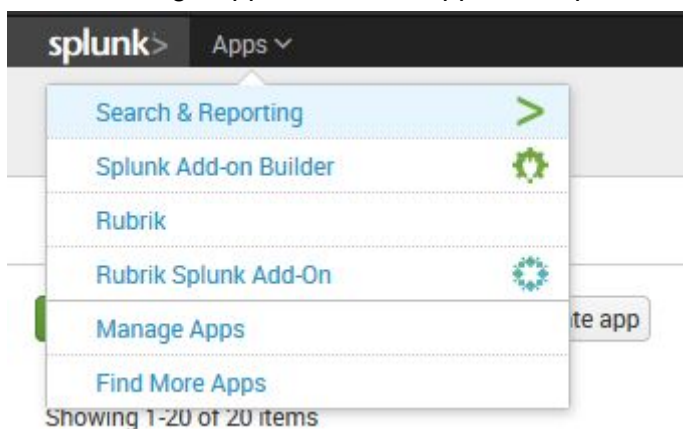
5. Enter the details as defined in the last section, and click Add

 A screenshot of a configuration dialog box titled 'Add Rubrik - Runway Remaining'. It contains five input fields, each with an asterisk indicating it's required: 'Name' (with a hint 'Enter a unique name for the data input'), 'Interval' (with a hint 'Time interval of input in seconds'), 'Index' (a dropdown menu currently showing 'default'), 'Global Account' (a dropdown menu), and 'Rubrik Node'. At the bottom left is a 'Cancel' button, and at the bottom right is a green 'Add' button.

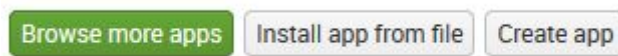
Importing the Rubrik application - Fresh Install

The Rubrik application will be used to contain the datasets and dashboards imported through the Rubrik Add-On. The steps below detail how to import the application file.

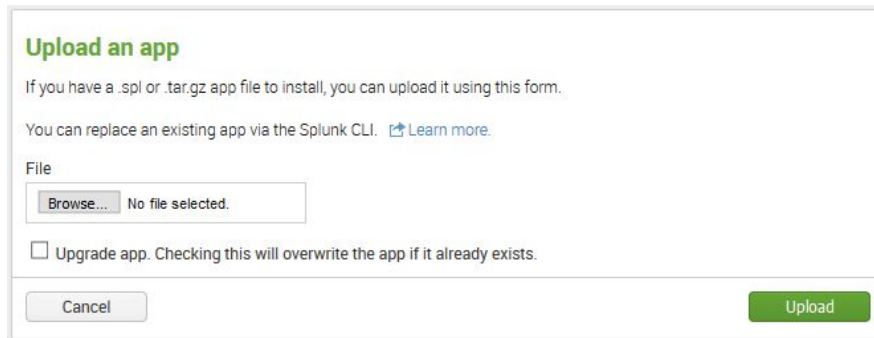
1. Go to 'Manage Apps' under the application picker



2. Click the 'Install app from file' button



3. Click 'Browse' and select the 'Rubrik.spl' file, click 'Upload'



Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

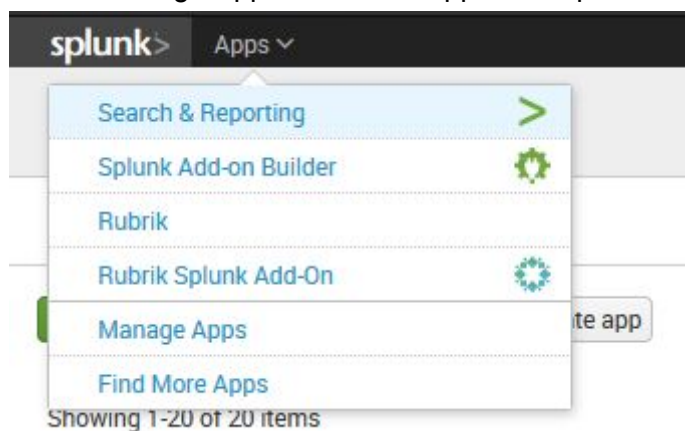
No file selected.

☐ Upgrade app. Checking this will overwrite the app if it already exists.

Importing the Rubrik application - Upgrade

The Rubrik application will be used to contain the datasets and dashboards imported through the Rubrik Add-On. The steps below detail how to import the application file.

4. Go to 'Manage Apps' under the application picker



5. Click the 'Install app from file' button



6. Click 'Browse' and select the 'Rubrik.spl' file, check the 'Upgrade app' box, click 'Upload'

Upload an app

If you have a .spl or .tar.gz app file to install, you can upload it using this form.

You can replace an existing app via the Splunk CLI. [Learn more.](#)

File

☒ Upgrade app. Checking this will overwrite the app if it already exists.

Creating/Updating Datasets

Datasets are used to store the gathered data in a table in Splunk. These need to be created once the add-on and application have been imported so that the dashboards can consume the filtered data.

NOTE: If this is an upgrade, then modify the existing datasets to match the below.

There are five datasets required for the Rubrik Splunk application, the specifications for these are detailed below, followed by instructions on how to create a dataset:

Required Datasets

The following datasets are required:

Table Title	Rubrik - Backup Job Events
Search String	(index="main") (sourcetype="rubrik:eventfeed") where eventType="Backup" eval _time = strptime(time, "%a %b %d %H:%M:%S %Z %Y") dedup id
Table ID	rubrik_dataset_backup_job_events
Fields	_time, clusterName, eventStatus, locationName, message, objectName, objectType

Table Title	Rubrik - Runway Remaining
Search String	(index="main") (sourcetype="rubrik:runwayremaining")
Table ID	rubrik_dataset_runway_remaining
Fields	_time clusterName

	daysRemaining
--	---------------

Table Title	Rubrik - Security Audit Events
Search String	(index="main") (sourcetype="rubrik:eventfeed") where eventType="Audit" eval _time = strftime(time, "%a %b %d %H:%M:%S %Z %Y")
Table ID	rubrik_dataset_security_audit_events
Fields	_time clusterName eventStatus eventType message username

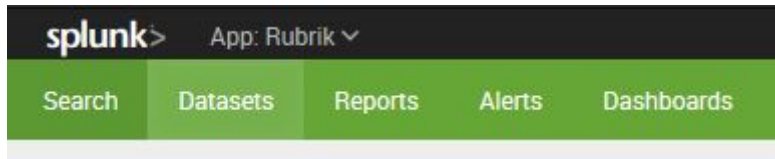
Table Title	Rubrik - Storage Summary
Search String	(index="main") (sourcetype="rubrik:storagesummary")
Table ID	rubrik_dataset_storage_summary
Fields	_time available clusterName liveMount miscellaneous snapshot total used

Table Title	Rubrik - Cluster IO Stats
Search String	(index="main") (sourcetype="rubrik:clusteriostats") eval _time = strftime(time, "%Y-%m-%dT%H:%M:%S.%f%Z")
Table ID	rubrik_dataset_cluster_io_stats
Fields	_time clusterName readBytePerSecond readsPerSecond writeBytePerSecond writesPerSecond

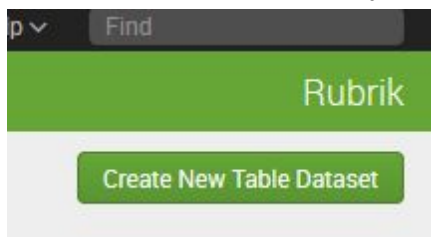
How to create a Dataset

1. If you do not have the 'Splunk Datasets Add-on' installed or enabled, you will need to install this from the app store in Splunk and enable it, or download and install it from [here](#).

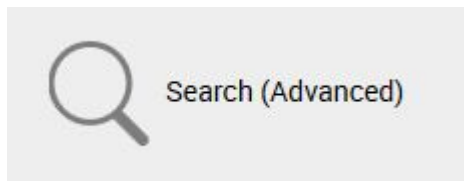
2. Go to the 'Datasets' tab under the 'Rubrik' application



3. Click the 'Create New Table Dataset' button (if you do not have the Splunk Datasets Add-on enabled or installed you will not see this button)



4. Click the 'Search (Advanced)' link



5. Enter the search string as defined in the tables in the last section, and hit the search button on the far right



6. Select the fields as defined in the 'Fields' section of the tables in the last section, click 'Done'

Select existing fields

☒ Field name Q

- ✓ _time
- ✓ _raw
- ✓ available
- eventtype
- host
- index
- ✓ lastUpdateTime
- linecount
- liveMount
- miscellaneous
- punct
- snapshot
- source
- sourcetype
- splunk_server
- timestamp
- ✓ total
- ✓ used

[+ Add a missing existing field](#)

Done

7. Click the 'Save As' button in the top right hand side

Find

Rubrik

Save
Save As

8. Enter the title and ID as defined in the table in the last section, and click 'Save'

Save As New Table X

Table Title

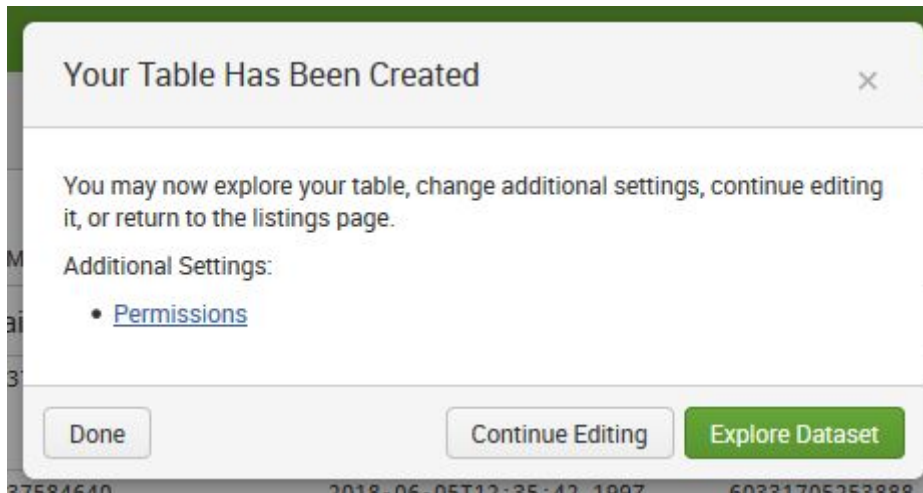
Table ID [?]

Can only contain letters, numbers and underscores.

Description

Cancel
Save

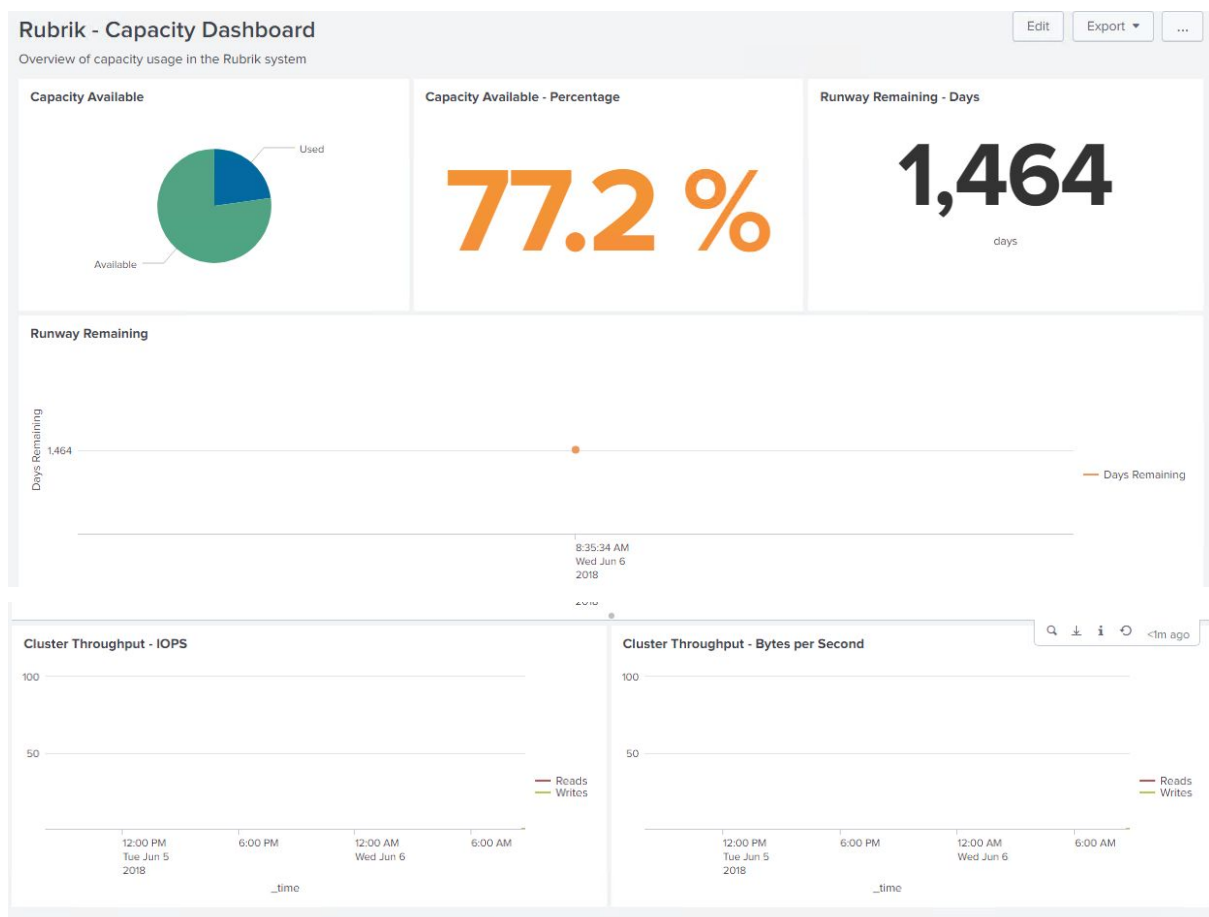
9. Click 'Done'



Dashboards

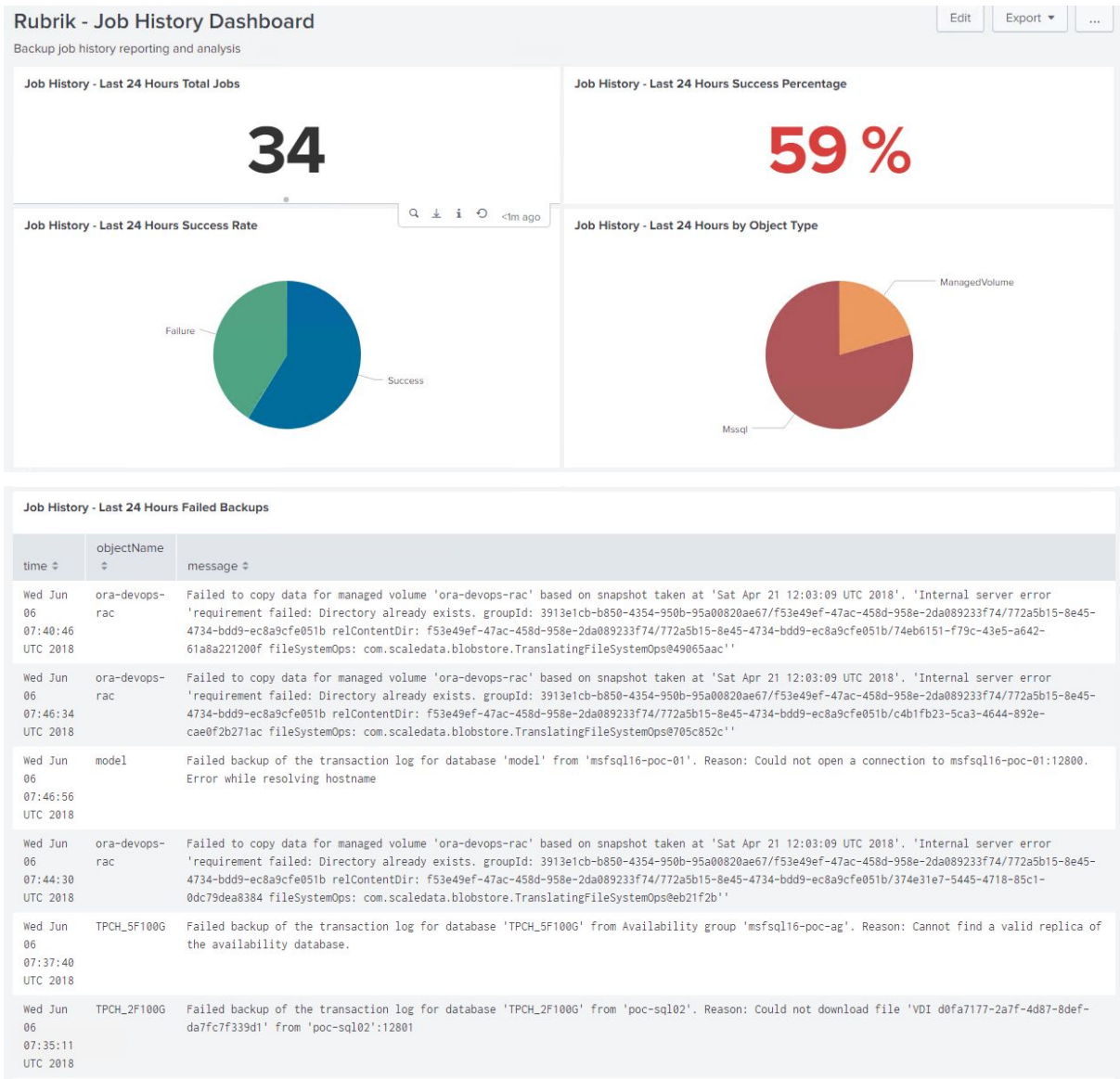
There are three dashboards which should now be populated in the Rubrik application, these are as follows:

Capacity Dashboard

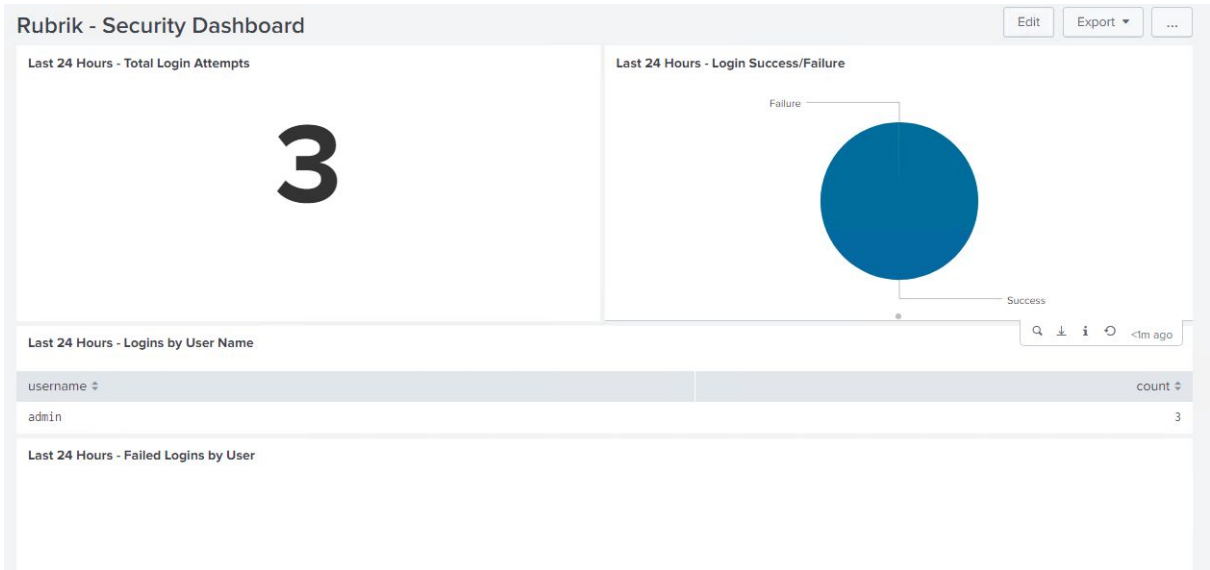


This dashboard shows capacity and throughput statistics for the cluster.

Job History Dashboard



Security Dashboard



This dashboard shows the last 24 hours of login information, breaking down the top 10 logins by name and count, and the top 10 failed logins by name and count