

Rubrik Splunk Add-On

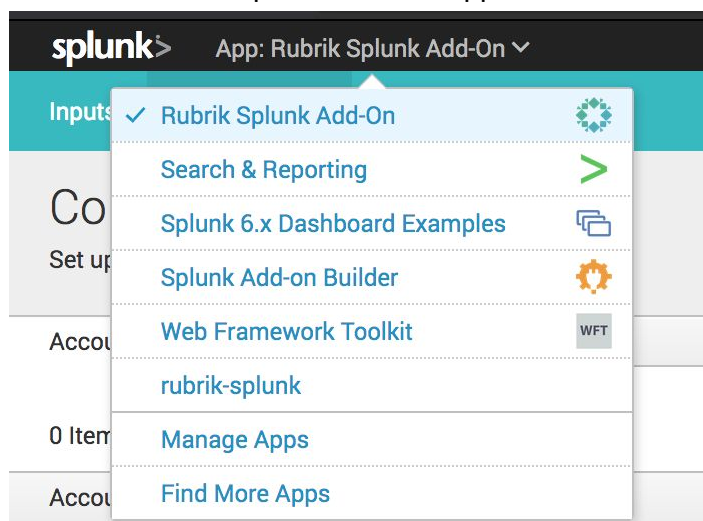
Installation and Setup Guide

Installing and Upgrading the Add-On

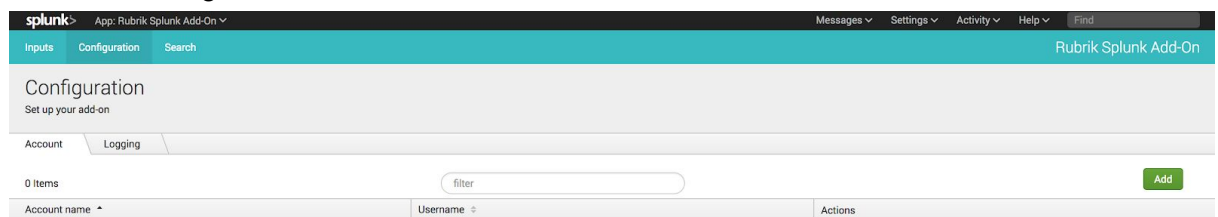
This is now taken care of via Splunkbase from within the Splunk application.

Credentials and Logging

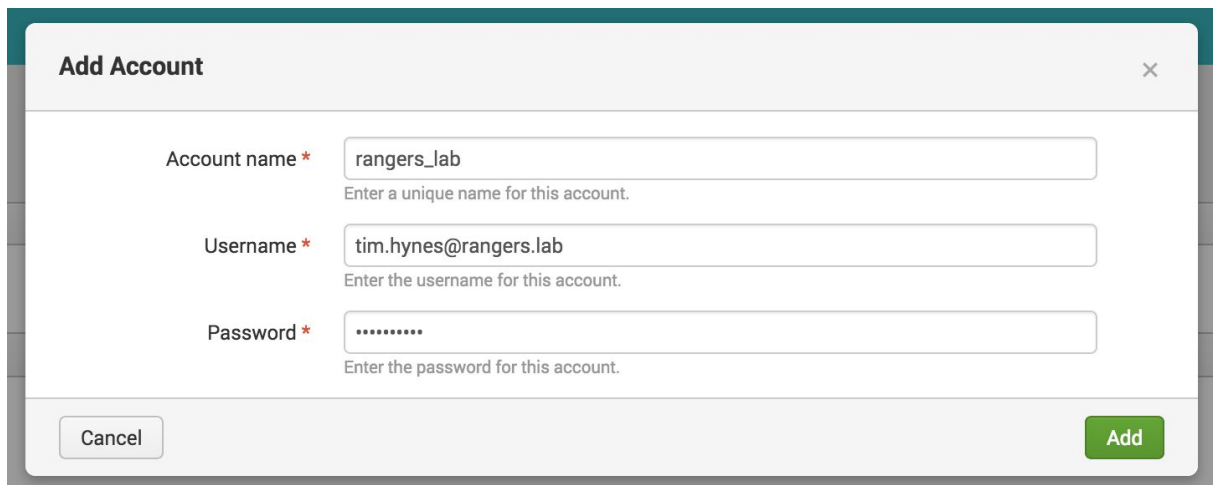
1. Go to the 'Rubrik Splunk Add-On' application:



2. Click the 'Configuration' tab, and click the 'Add' button:



3. Enter a name for the credential, and the username and password:

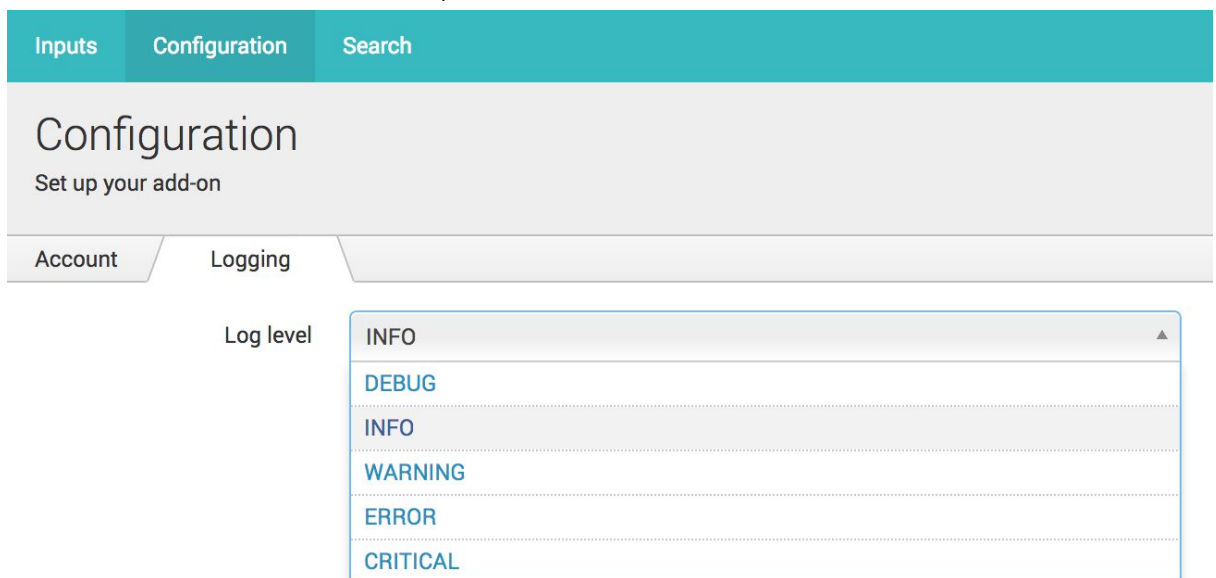


The 'Add Account' dialog box contains three input fields. The first field is labeled 'Account name *' and contains the text 'rangers_lab'. Below it is a hint: 'Enter a unique name for this account.' The second field is labeled 'Username *' and contains the text 'tim.hynes@rangers.lab'. Below it is a hint: 'Enter the username for this account.' The third field is labeled 'Password *' and contains seven dots. Below it is a hint: 'Enter the password for this account.' At the bottom left is a 'Cancel' button, and at the bottom right is a green 'Add' button.

4. Press Add.

NOTE: steps 1-4 can be repeated for your Polaris username and password if Polaris Radar is available and you would like to add this to Splunk.

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



The 'Configuration' page has three tabs: 'Inputs', 'Configuration', and 'Search'. The 'Configuration' tab is active. Below the tabs, there are two sub-tabs: 'Account' and 'Logging'. The 'Logging' sub-tab is selected. Under the 'Logging' sub-tab, there is a 'Log level' label and a dropdown menu. The dropdown menu is open, showing a list of log levels: 'INFO' (selected), 'DEBUG', 'INFO', 'WARNING', 'ERROR', and 'CRITICAL'.

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	300
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

Optional - for customers with Polaris Radar:

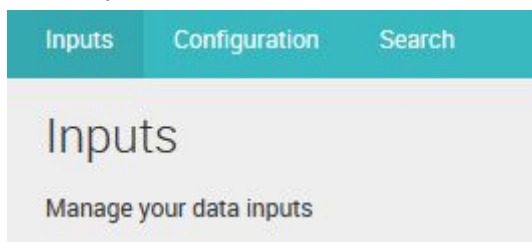
Name	polaris_radar_anomalies
Interval	900
Index	main
Global Account	<Polaris global account if present>
Polaris URL	https://<your_polaris_url>.my.rubrik.com
Input Type	Polaris - Radar Anomalies

How to create an Input

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



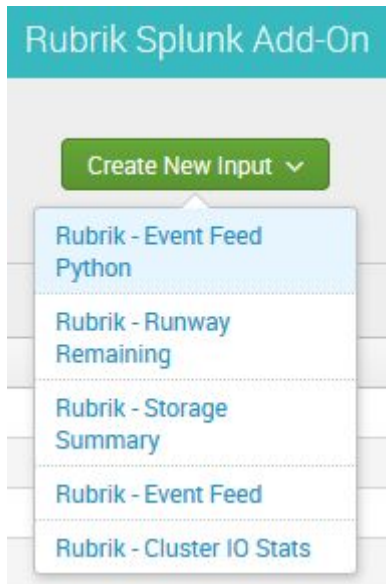
2. Ensure you are on the 'Inputs' tab



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

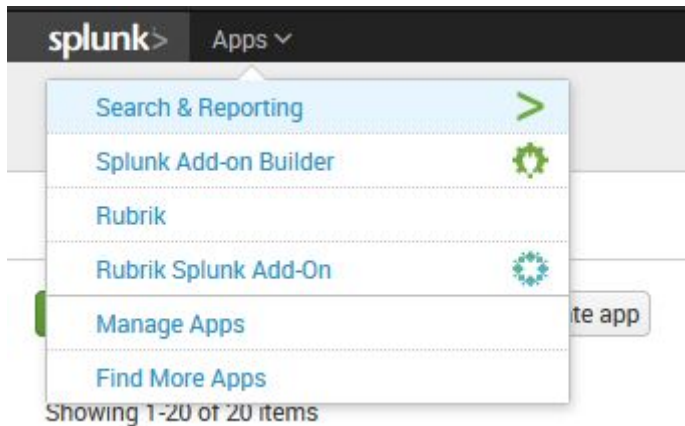
A screenshot of the 'Add Rubrik - Runway Remaining' form. The form has a title bar with the text 'Add Rubrik - Runway Remaining' and a close button (X). The form contains five input fields: 'Name *' with a placeholder 'Enter a unique name for the data input', 'Interval *' with a placeholder 'Time interval of input in seconds.', 'Index *' with a dropdown menu showing 'default', 'Global Account *' with a dropdown menu, and 'Rubrik Node *' with a text input field. At the bottom of the form are two buttons: 'Cancel' and 'Add'.

Importing the Rubrik application - Fresh Install

NOTE: The Rubrik application file is currently located in the Rubrik Splunk Add-On GitHub repo here: <https://github.com/rubrik-devops/rubrik-splunk-addon/tree/master/App>.

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'

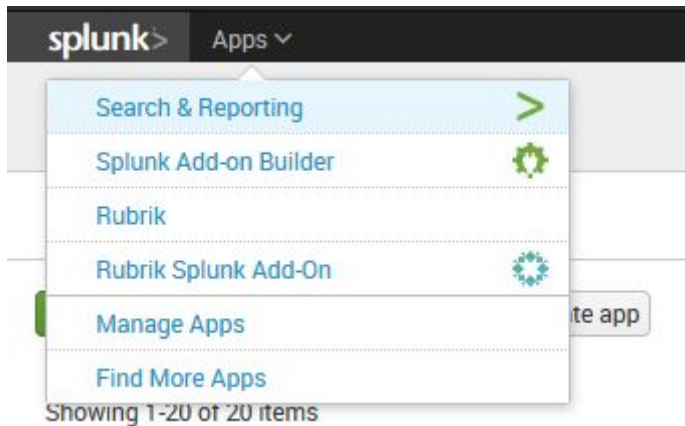
A screenshot of the 'Upload an app' form in the Splunk interface. The form has a title 'Upload an app' in green. Below it, text says: 'If you have a .spl or .tar.gz app file to install, you can upload it using this form.' and 'You can replace an existing app via the Splunk CLI. [Learn more.](#)'. There is a 'File' section with a 'Browse...' button and the text 'No file selected.'. Below that is a checkbox labeled 'Upgrade app. Checking this will overwrite the app if it already exists.'. At the bottom are 'Cancel' and 'Upload' buttons.

Importing the Rubrik application - Upgrade

NOTE: The Rubrik application file is currently located in the Rubrik Splunk Add-On GitHub repo here: <https://github.com/rubrik-devops/rubrik-splunk-addon/tree/master/App>.

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'

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 = strptime(time, "%a %b %d %H:%M:%S %Z %Y")
Table ID	rubrik_dataset_security_audit_events
Fields	_time clusterName eventStatus eventType message username

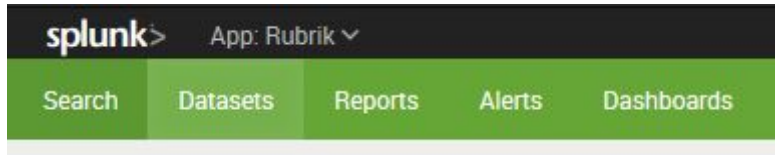
Table Title	Rubrik - Storage Summary
Search String	(index="main") (sourcetype="rubrik:storagesummary")
Table ID	rubrik_dataset_storage_summary
Fields	_time available clusterName liveMount miscellaneous snapshot

	total used
--	---------------

Table Title	Rubrik - Cluster IO Stats
Search String	(index="main") (sourcetype="rubrik:clusteriostats") eval _time = strptime(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

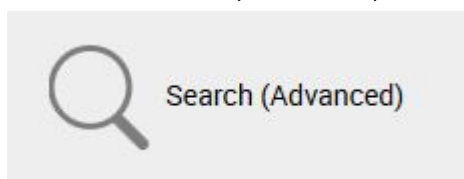
1. If you do not have the 'Splunk Datasets Add-on' installed or enabled, you will need to install this from the app store in Splunk and enable it, or download and install it from [here](#).
2. Go to the 'Datasets' tab under the 'Rubrik' application



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

New Table Dataset Cancel

Select one: Indexes & Source Types Existing Datasets Search (Advanced)

`{index="main"} (sourcetype="rubrik_rest_storage_summary") | fields _time, "available", "lastUpdateTime", "total", "used", "_raw"`

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

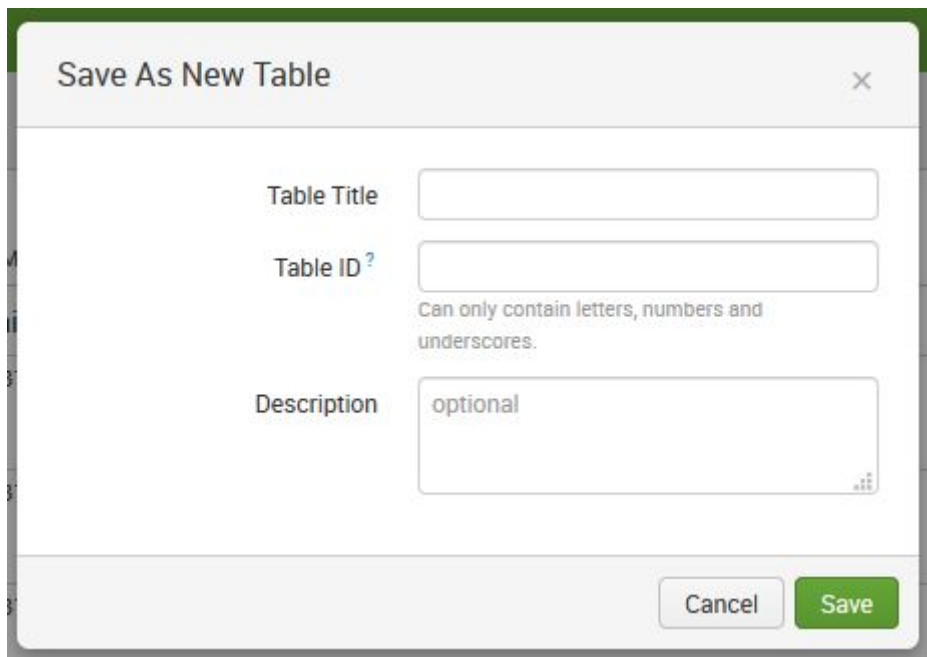
7. Click the 'Save As' button in the top right hand side

✓ Find

Rubrik

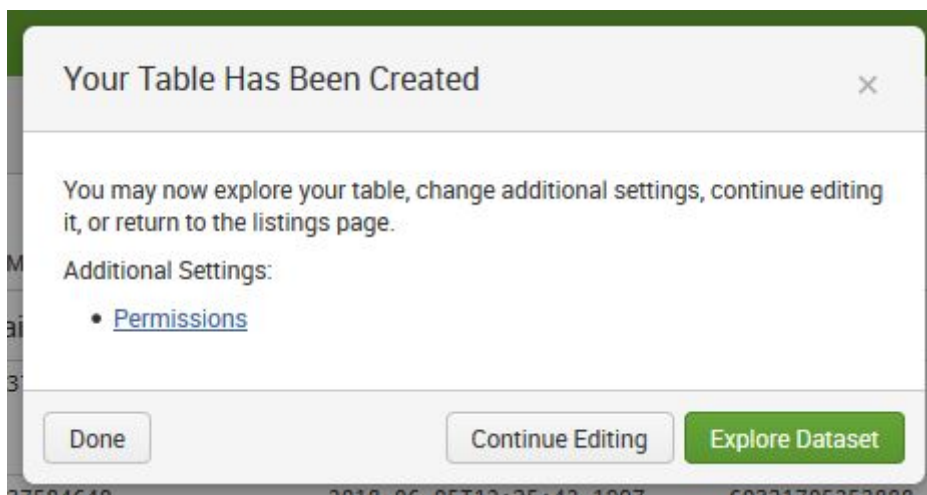
Save Save As

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



A dialog box titled "Save As New Table" with a close button (X) in the top right corner. It contains three input fields: "Table Title" (empty), "Table ID" (empty) with a question mark icon and a note below it stating "Can only contain letters, numbers and underscores.", and "Description" (containing the text "optional"). At the bottom right, there are two buttons: "Cancel" and "Save".

9. Click 'Done'



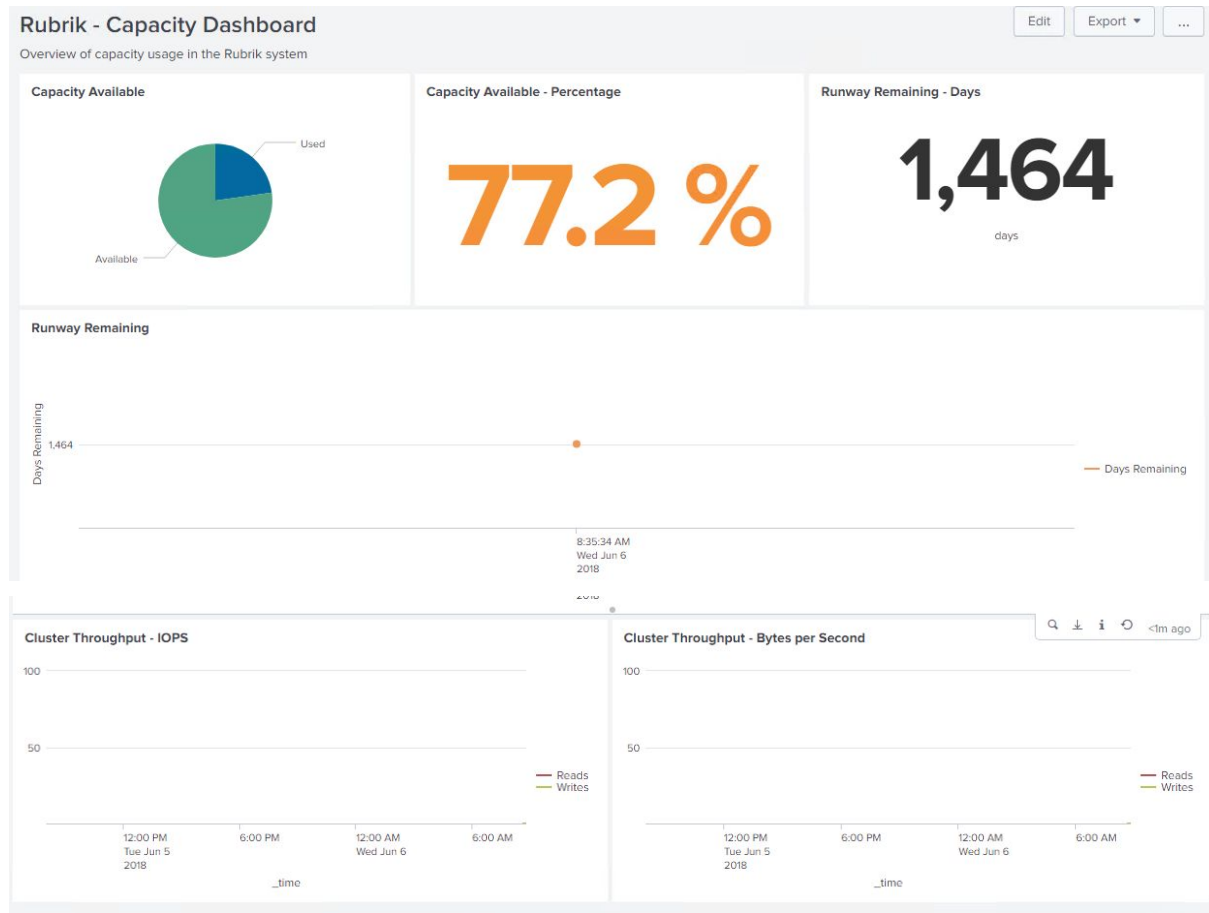
A dialog box titled "Your Table Has Been Created" with a close button (X) in the top right corner. It contains the text: "You may now explore your table, change additional settings, continue editing it, or return to the listings page." Below this, it says "Additional Settings:" followed by a bullet point and a link: "• [Permissions](#)". At the bottom, there are three buttons: "Done", "Continue Editing", and "Explore Dataset".

Dashboards

Overview

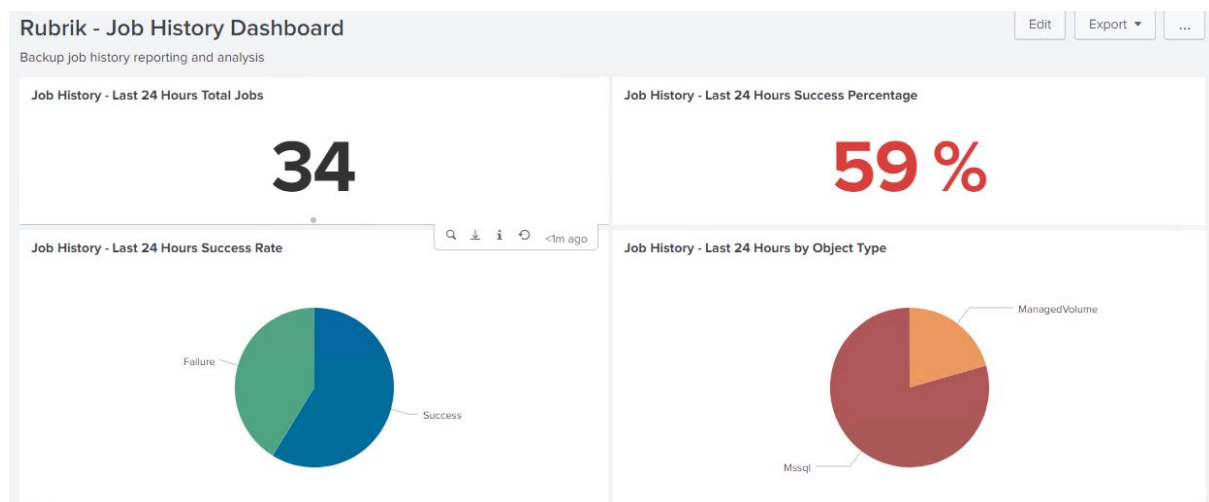
There are three dashboards which should now be populated in the Rubrik application, these are as follows:

Capacity Dashboard



This dashboard shows capacity and throughput statistics for the cluster.

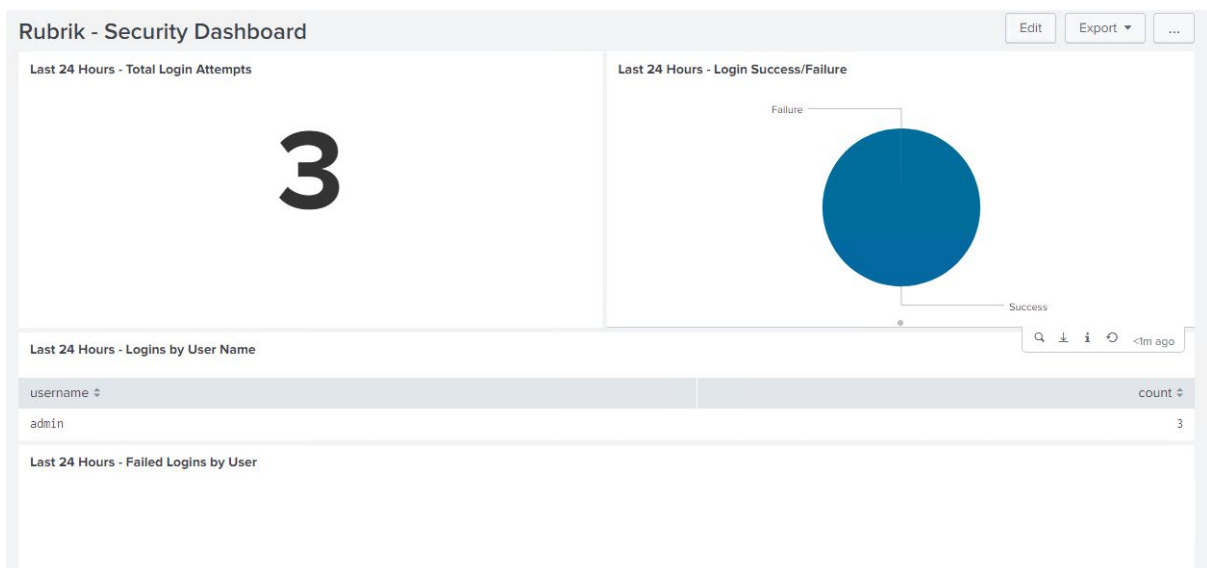
Job History Dashboard



Job History - Last 24 Hours Failed Backups		
time ↕	objectName ↕	message ↕
Wed Jun 06 07:40:46 UTC 2018	ora-devops-rac	Failed to copy data for managed volume 'ora-devops-rac' based on snapshot taken at 'Sat Apr 21 12:03:09 UTC 2018'. 'Internal server error' requirement failed: Directory already exists. groupId: 3913e1cb-b850-4354-950b-95a00820ae67/f53e49ef-47ac-458d-958e-2da089233f74/772a5b15-8e45-4734-bdd9-ec8a9cfe051b relContentDir: f53e49ef-47ac-458d-958e-2da089233f74/772a5b15-8e45-4734-bdd9-ec8a9cfe051b/74eb6151-f79c-43e5-a642-61a8a221200f fileSystemOps: com.scaledata.blobstore.TranslatingFileSystemOps@49065aac''
Wed Jun 06 07:46:34 UTC 2018	ora-devops-rac	Failed to copy data for managed volume 'ora-devops-rac' based on snapshot taken at 'Sat Apr 21 12:03:09 UTC 2018'. 'Internal server error' requirement failed: Directory already exists. groupId: 3913e1cb-b850-4354-950b-95a00820ae67/f53e49ef-47ac-458d-958e-2da089233f74/772a5b15-8e45-4734-bdd9-ec8a9cfe051b relContentDir: f53e49ef-47ac-458d-958e-2da089233f74/772a5b15-8e45-4734-bdd9-ec8a9cfe051b/c4b1fb23-5ca3-4644-892e-cae0f2b271ac fileSystemOps: com.scaledata.blobstore.TranslatingFileSystemOps@705c852c''
Wed Jun 06 07:46:56 UTC 2018	model	Failed backup of the transaction log for database 'model' from 'msfsql16-poc-01'. Reason: Could not open a connection to msfsql16-poc-01:12800. Error while resolving hostname
Wed Jun 06 07:44:30 UTC 2018	ora-devops-rac	Failed to copy data for managed volume 'ora-devops-rac' based on snapshot taken at 'Sat Apr 21 12:03:09 UTC 2018'. 'Internal server error' requirement failed: Directory already exists. groupId: 3913e1cb-b850-4354-950b-95a00820ae67/f53e49ef-47ac-458d-958e-2da089233f74/772a5b15-8e45-4734-bdd9-ec8a9cfe051b relContentDir: f53e49ef-47ac-458d-958e-2da089233f74/772a5b15-8e45-4734-bdd9-ec8a9cfe051b/374e31e7-5445-4718-85c1-0dc79dea8384 fileSystemOps: com.scaledata.blobstore.TranslatingFileSystemOps@eb21f2b''
Wed Jun 06 07:37:40 UTC 2018	TPCH_SF100G	Failed backup of the transaction log for database 'TPCH_SF100G' from Availability group 'msfsql16-poc-ag'. Reason: Cannot find a valid replica of the availability database.
Wed Jun 06 07:35:11 UTC 2018	TPCH_2F100G	Failed backup of the transaction log for database 'TPCH_2F100G' from 'poc-sql02'. Reason: Could not download file 'VDI d0fa7177-2a7f-4d87-8def-da7fc7f339d1' from 'poc-sql02':12801

This shows the last 24 hours of backup histories, breaking them down by succeeded and failed, and by object type, as well as showing failure logs for any missed backup jobs.

Security Dashboard

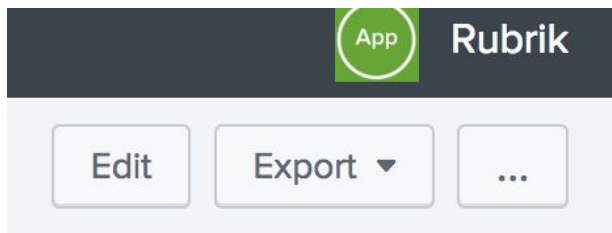


This dashboard shows the last 24 hours of login information, breaking down the top 10 logins by name and count, and the top 10 failed logins by name and count

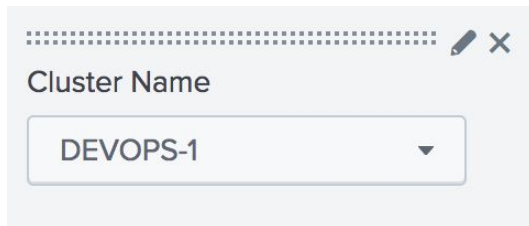
Setting a Default Rubrik Cluster

The Dashboards built in to the application have a dropdown to select the cluster for which to display statistical information. By default this will be blank on loading the dashboard, to set this to a default value follow the steps below:

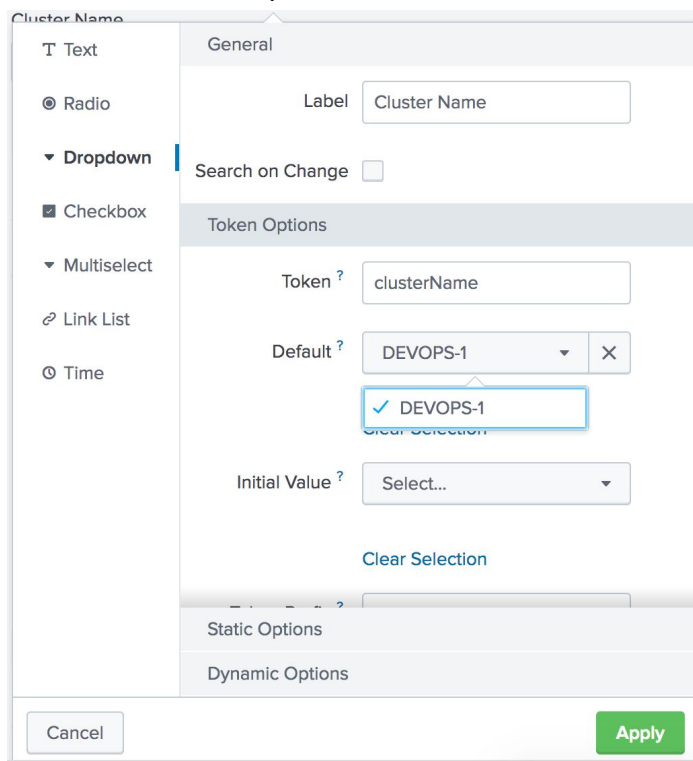
1. Go to the dashboard you wish to configure
2. Click the 'Edit' button in the top right of the page:



3. Select the pencil next to 'Cluster Name' in the top left of the page:



4. Use the 'Default' dropdown to select the default cluster you want to display:



5. Click the 'Apply' button to save the change and then the Save button in the top right of the dashboard to save all changes:



NOTE: The list populating the 'Default' dropdown is generated by the events ingested by Splunk, so this may take a while to populate after you have added new data inputs.