splunk>
a CISCO company
Mar 2025

Splunk4Admins - Splunk Cloud Storage

Lab Guide

Overview

This lab guide contains the hands-on exercises for the **Splunk4Admins - Splunk Cloud Storage** workshop. Before proceeding with these exercises, please ensure that you have a copy of the workshop slide deck, which will help to put into context the tasks you are carrying out.

Download the workshop slide deck: https://splk.it/S4A-SCS-Attendee

Prerequisites

In order to complete these exercises, you will need your own Splunk instance. Splunk's hands-on workshops are delivered via the Splunk Show portal and you will need a splunk.com account in order to access this.

If you don't already have a Splunk.com account, please create one here before proceeding with the rest of the workshop.

⚠️ Troubleshooting Connectivity

If you experience connectivity issues with accessing either your workshop environment or the event page, please try the following troubleshooting steps. If you still experience issues please reach out to the team running your workshop.

- **Use Google Chrome** (if you're not already)
- If the event page (i.e. *https://show.splunk.com/event/<eventID>*) didn't load when you clicked on the link, try **refreshing the page**
- **Disconnect from VPN** (if you're using one)
- **Clear your browser cache and restart your browser** (if using Google Chrome, go to: Settings > Privacy and security > Clear browsing data)
- **Try using private browsing mode** (e.g. Incognito in Google Chrome) to rule out any cache issues
- **Try using another computer** such as your personal computer - all you need is a web browser! Cloud platforms like AWS can often be blocked on corporate laptops.

Table of Contents

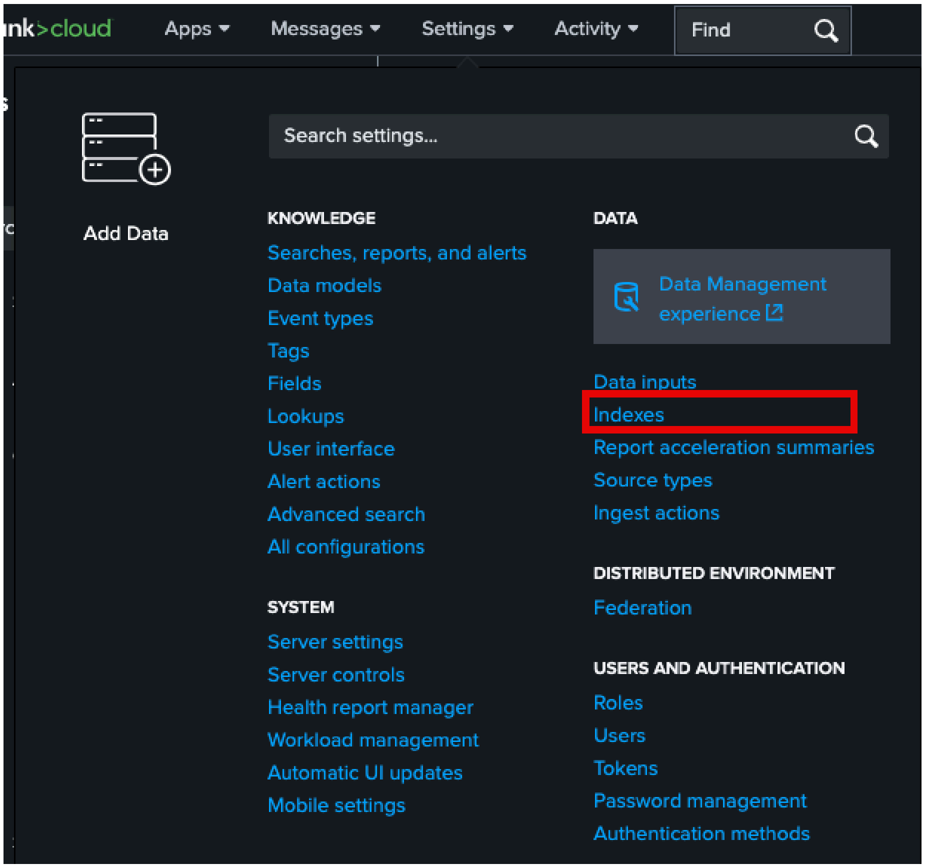
Exercise 1 – Create New Index with DDAA

Description

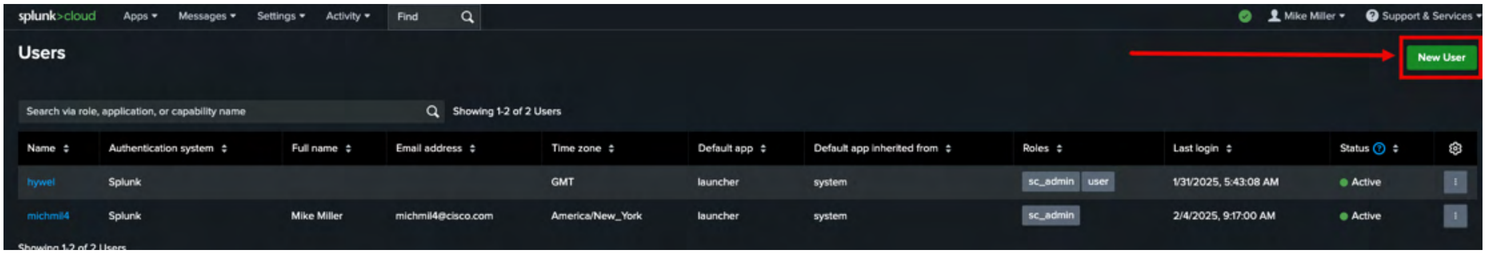
In this exercise we will create a new index called **test_two** and set the searchable retention and the Archive retention periods.

Steps:

1. Log in to your Splunk Cloud instance
2. Click Settings
3. Click Indexes



4. Click New Index



Users

Search via role, application, or capability name

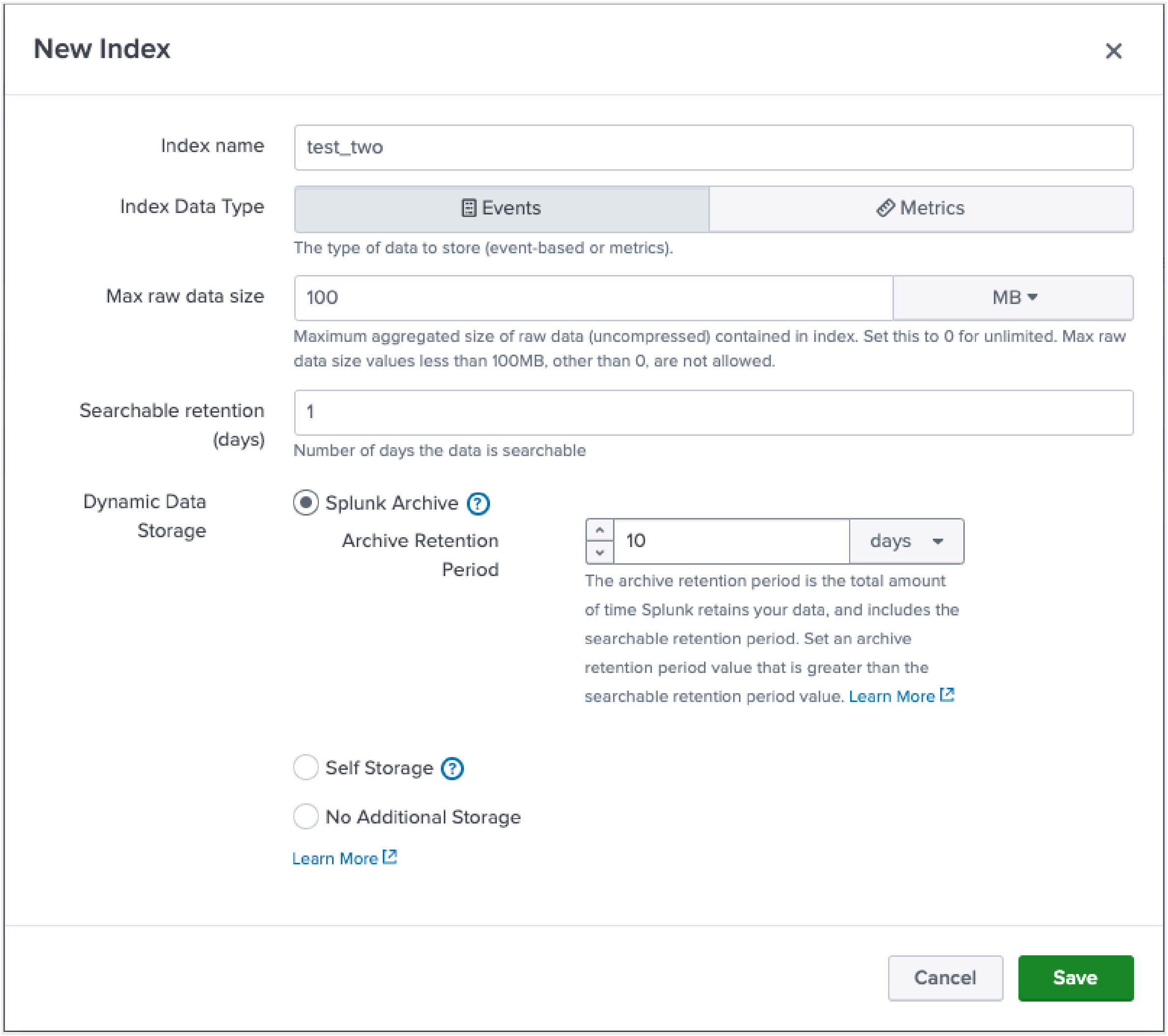
Showing 1-2 of 2 Users

Name	Authentication system	Full name	Email address	Time zone	Default app	Default app inherited from	Roles	Last login	Status
hywel	Splunk			GMT	launcher	system	sc_admin user	1/31/2025, 5:43:08 AM	Active
michmil4	Splunk	Mike Miller	michmil4@cisco.com	America/New_York	launcher	system	sc_admin	2/4/2025, 9:17:00 AM	Active

Showing 1-2 of 2 Users

5. Create the index using the table below:

Index Name	test_two
Data Type	Events
Max Raw Data	100 MB
Searchable Retention	1 day
Archive Retention Period	10 Days



New Index

Index name: test_two

Index Data Type: Events | Metrics

The type of data to store (event-based or metrics).

Max raw data size: 100 MB

Maximum aggregated size of raw data (uncompressed) contained in index. Set this to 0 for unlimited. Max raw data size values less than 100MB, other than 0, are not allowed.

Searchable retention (days): 1

Number of days the data is searchable

Dynamic Data Storage:

● Splunk Archive

Archive Retention Period: 10 days

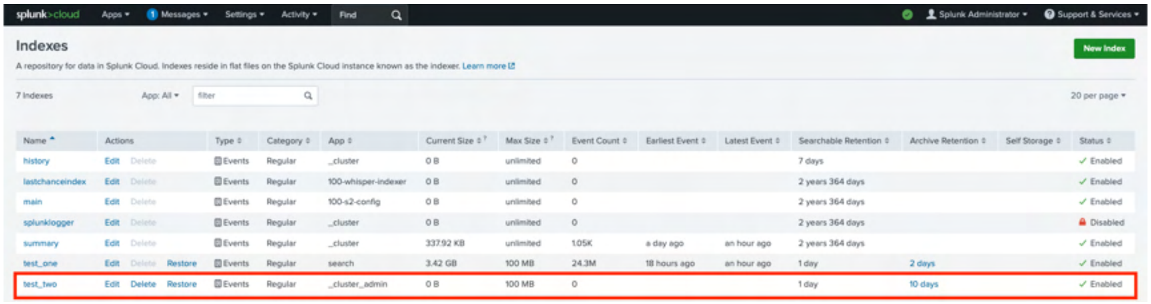
The archive retention period is the total amount of time Splunk retains your data, and includes the searchable retention period. Set an archive retention period value that is greater than the searchable retention period value. Learn More

○ Self Storage

○ No Additional Storage

Learn More

6. Verify the index was created correctly by reviewing the Indexes screen (Note it may take a few moments for the new index to show up in Splunk Cloud. Refresh the page if necessary)



Indexes

A repository for data in Splunk Cloud. Indexes reside in flat files on the Splunk Cloud instance known as the indexer. Learn more

7 Indexes App: All ▾ filter 20 per page ▾

Name	Actions	Type	Category	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Searchable Retention	Archive Retention	Self Storage	Status
history	Edit Delete	Events	Regular	_cluster	0 B	unlimited	0			7 days			✓ Enabled
lastchanceindex	Edit Delete	Events	Regular	100-whisper-indexer	0 B	unlimited	0			2 years 364 days			✓ Enabled
main	Edit Delete	Events	Regular	100-s2-config	0 B	unlimited	0			2 years 364 days			✓ Enabled
splunklogger	Edit Delete	Events	Regular	_cluster	0 B	unlimited	0			2 years 364 days			🔒 Disabled
summary	Edit Delete	Events	Regular	_cluster	337.92 KB	unlimited	1.05K	a day ago	an hour ago	2 years 364 days			✓ Enabled
test_one	Edit Delete Restore	Events	Regular	search	3.42 GB	100 MB	24.3M	18 hours ago	an hour ago	1 day	2 days		✓ Enabled
test_two	Edit Delete Restore	Events	Regular	_cluster_admin	0 B	100 MB	0			1 day	10 days		✓ Enabled

Completion Tracker (Optional):

You can use this drop down to track your progress of each exercise. This is completely optional, but may be a good indicator in more details or complex workshop scenarios.

Incomplete ▾

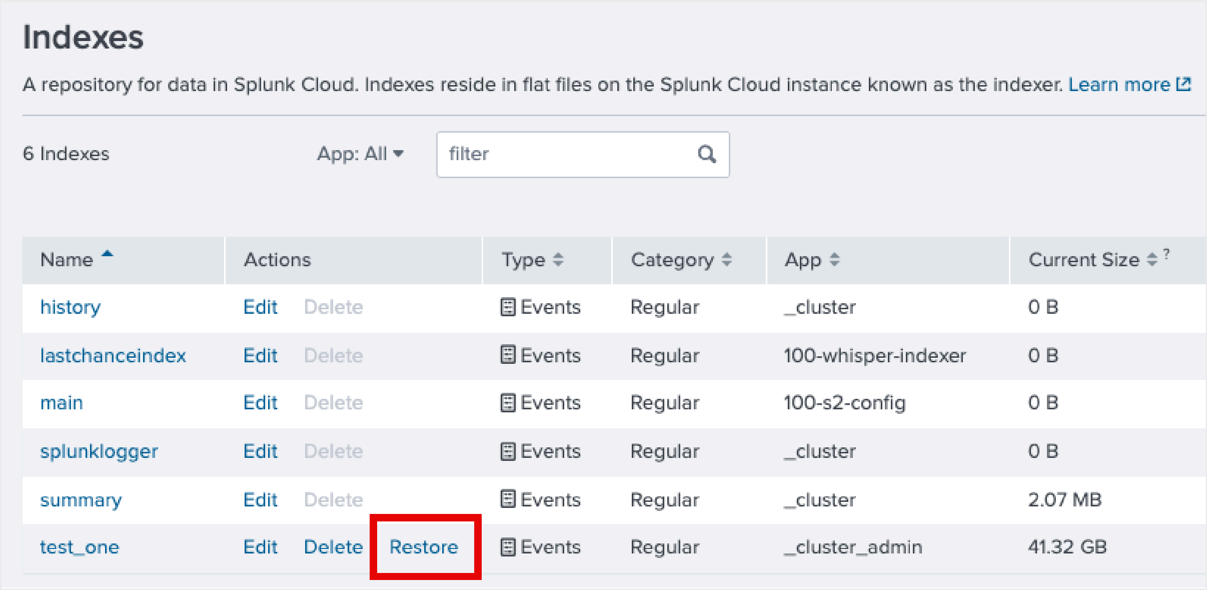
Exercise 2 – Practice Data Restore Process from DDAA

Description

In this exercise explore the process of data restoration for the **test_two** index created above, however we will not actually be restoring data here due to limitations in the workshop environment.

Steps:

1. Log in to your Splunk Cloud Instance
2. Click Settings
3. Click Indexes
4. For the index **test_two**, click the Restore link

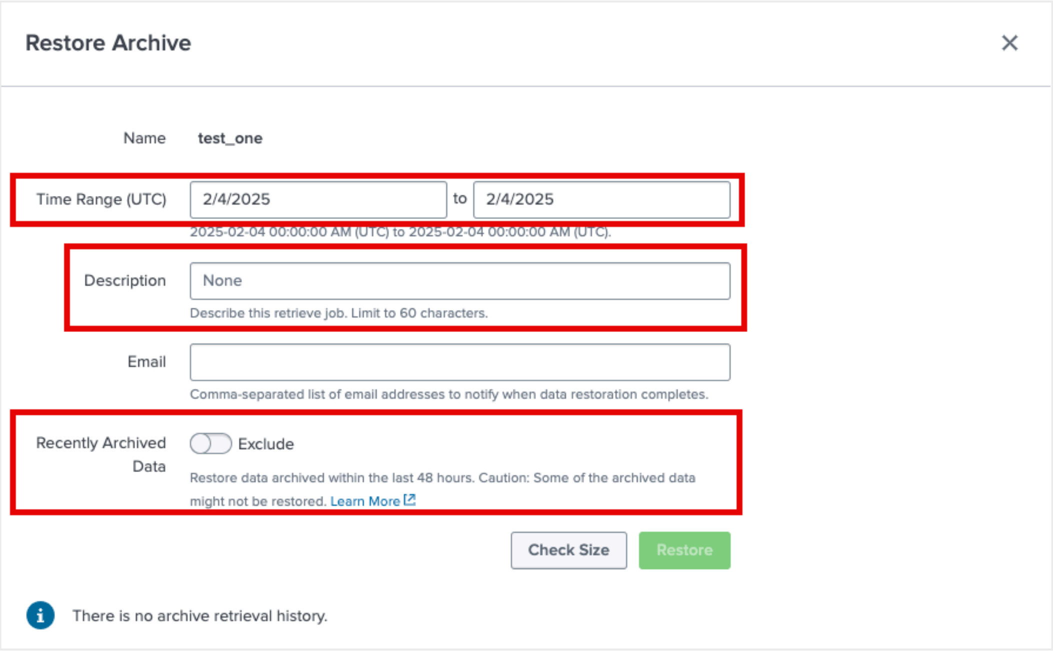


Indexes

A repository for data in Splunk Cloud. Indexes reside in flat files on the Splunk Cloud instance known as the indexer. Learn more

6 Indexes App: All filter

Name	Actions	Type	Category	App	Current Size
history	Edit Delete	Events	Regular	_cluster	0 B
lastchanceindex	Edit Delete	Events	Regular	100-whisper-indexer	0 B
main	Edit Delete	Events	Regular	100-s2-config	0 B
splunklogger	Edit Delete	Events	Regular	_cluster	0 B
summary	Edit Delete	Events	Regular	_cluster	2.07 MB
test_one	Edit Delete Restore	Events	Regular	_cluster_admin	41.32 GB



Restore Archive

Name test_one

Time Range (UTC) 2/4/2025 to 2/4/2025
2025-02-04 00:00:00 AM (UTC) to 2025-02-04 00:00:00 AM (UTC).

Description None
Describe this retrieve job. Limit to 60 characters.

Email
Comma-separated list of email addresses to notify when data restoration completes.

Recently Archived Data ○ Exclude
Restore data archived within the last 48 hours. Caution: Some of the archived data might not be restored. Learn More

Check Size Restore

There is no archive retrieval history.

5. On the Restore Archive set the following:
    a. **Time Range** = 2/3/2025 to 2/3/2025
    b. **Description** = Test Restore
    c. **Recently Archived Data** = Disabled

6. Click the X in the upper right corner to close out the Restore Archive window

Completion Tracker (Optional):

You can use this drop down to track your progress of each exercise. This is completely optional, but may be a good indicator in more details or complex workshop scenarios.

Incomplete ▾

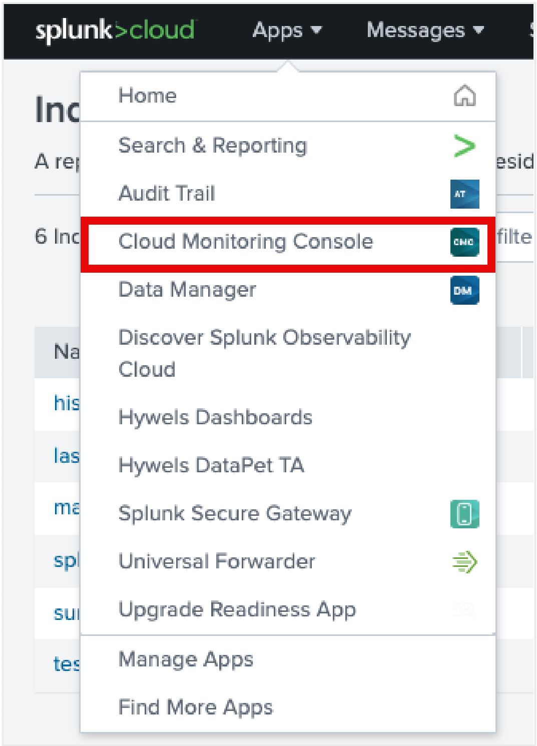
Exercise 3 – Reviewing the CMC

Description:

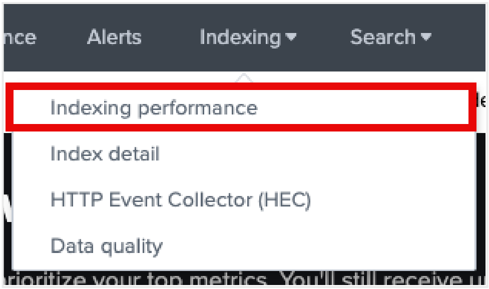
In this exercise we will review storage related dashboards in CMC.

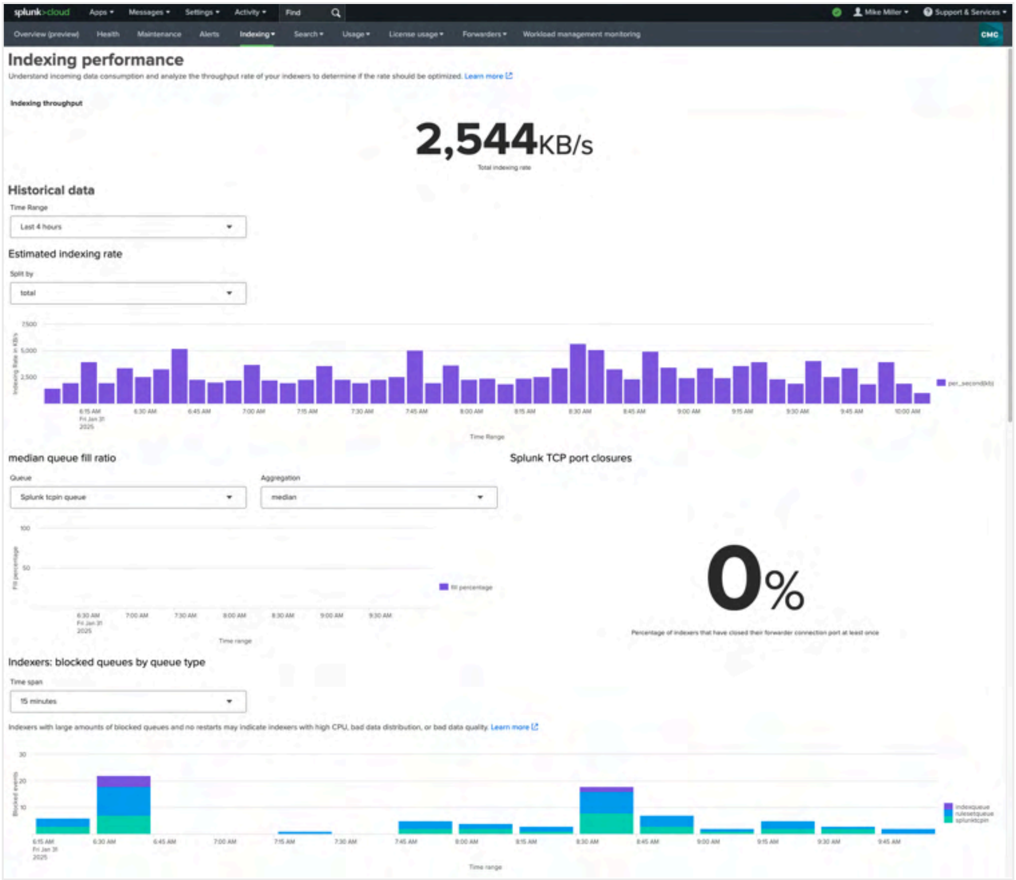
Steps:

1. Log in to your Splunk Cloud instance
2. Click Apps
3. Select Cloud Monitoring Console



4. Click on Indexing > Indexing Performance





Indexing performance

Understand incoming data consumption and analyze the throughput rate of your indexers to determine if the rate should be optimized. Learn more

Indexing throughput

2,544KB/s

Total indexing rate

Historical data

Time Range: Last 4 hours

Estimated indexing rate

Split by: total

median queue fill ratio

Queue: Splunk tcpin queue

Aggregation: median

Splunk TCP port closures

0%

Percentage of indexers that have closed their forwarder connection port at least once

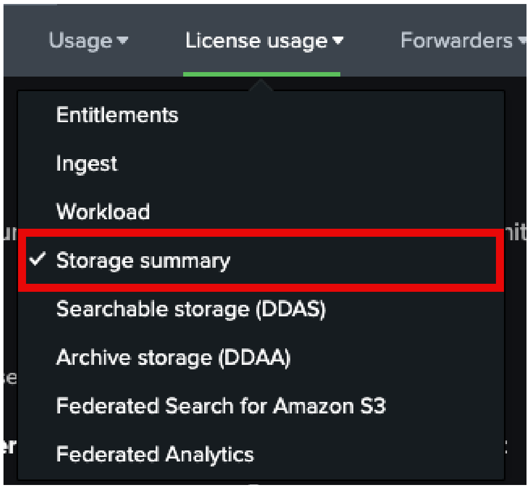
Indexers: blocked queues by queue type

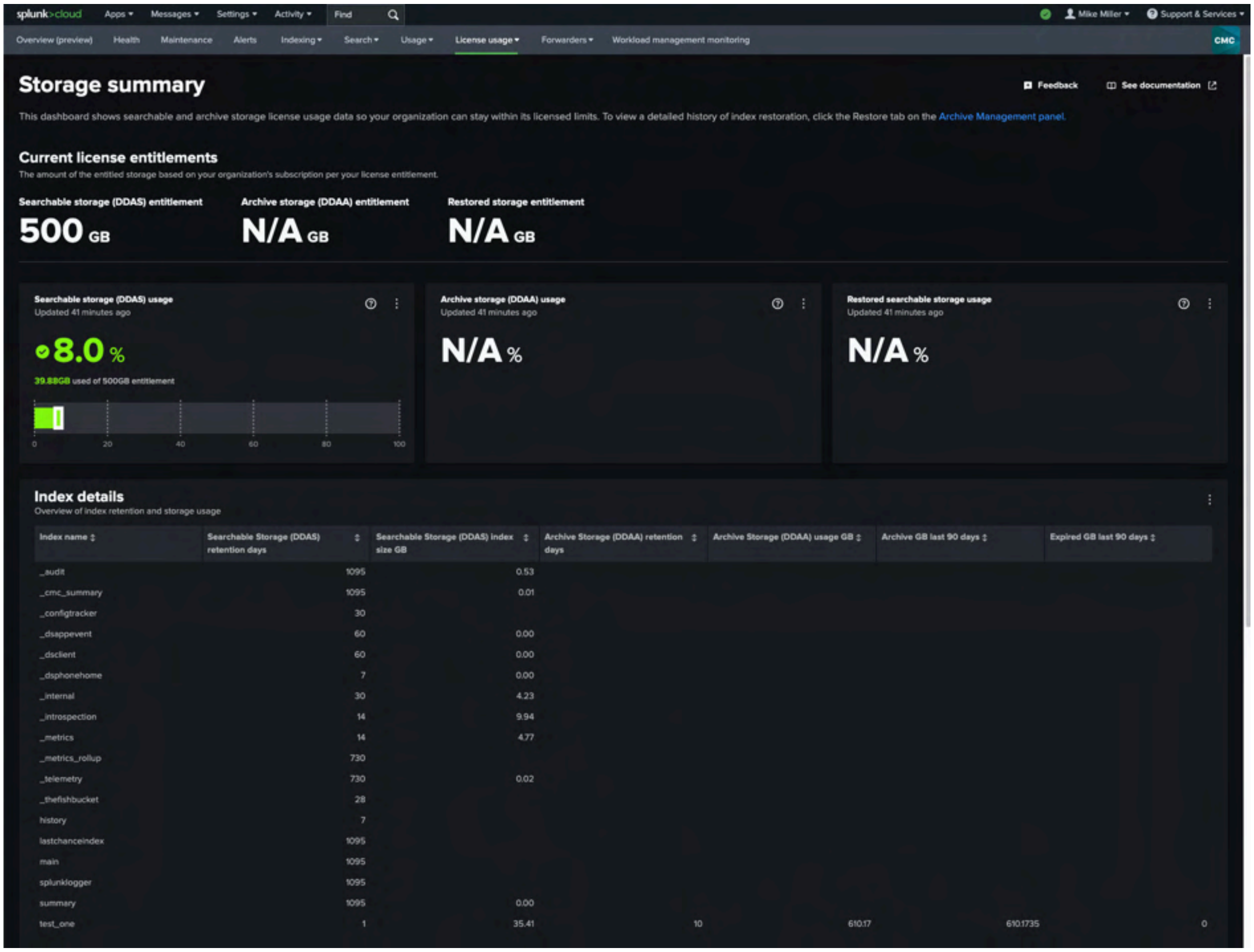
Time span: 15 minutes

Indexers with large amounts of blocked queues and no restarts may indicate indexers with high CPU, bad data distribution, or bad data quality. Learn more

What is the current Indexing throughput?	

5. Next click on Licensing Usage > Storage Summary





Storage summary

This dashboard shows searchable and archive storage license usage data so your organization can stay within its licensed limits. To view a detailed history of index restoration, click the Restore tab on the Archive Management panel.

Current license entitlements

The amount of the entitled storage based on your organization's subscription per your license entitlement.

Searchable storage (DDAS) entitlement	Archive storage (DDAA) entitlement	Restored storage entitlement
500 GB	N/A GB	N/A GB

Searchable storage (DDAS) usage	Archive storage (DDAA) usage	Restored searchable storage usage
Updated 41 minutes ago	Updated 41 minutes ago	Updated 41 minutes ago
8.0 %	N/A %	N/A %
39.88GB used of 500GB entitlement		

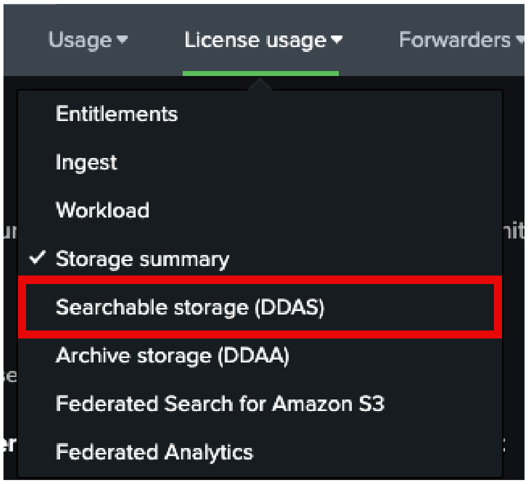
Index details

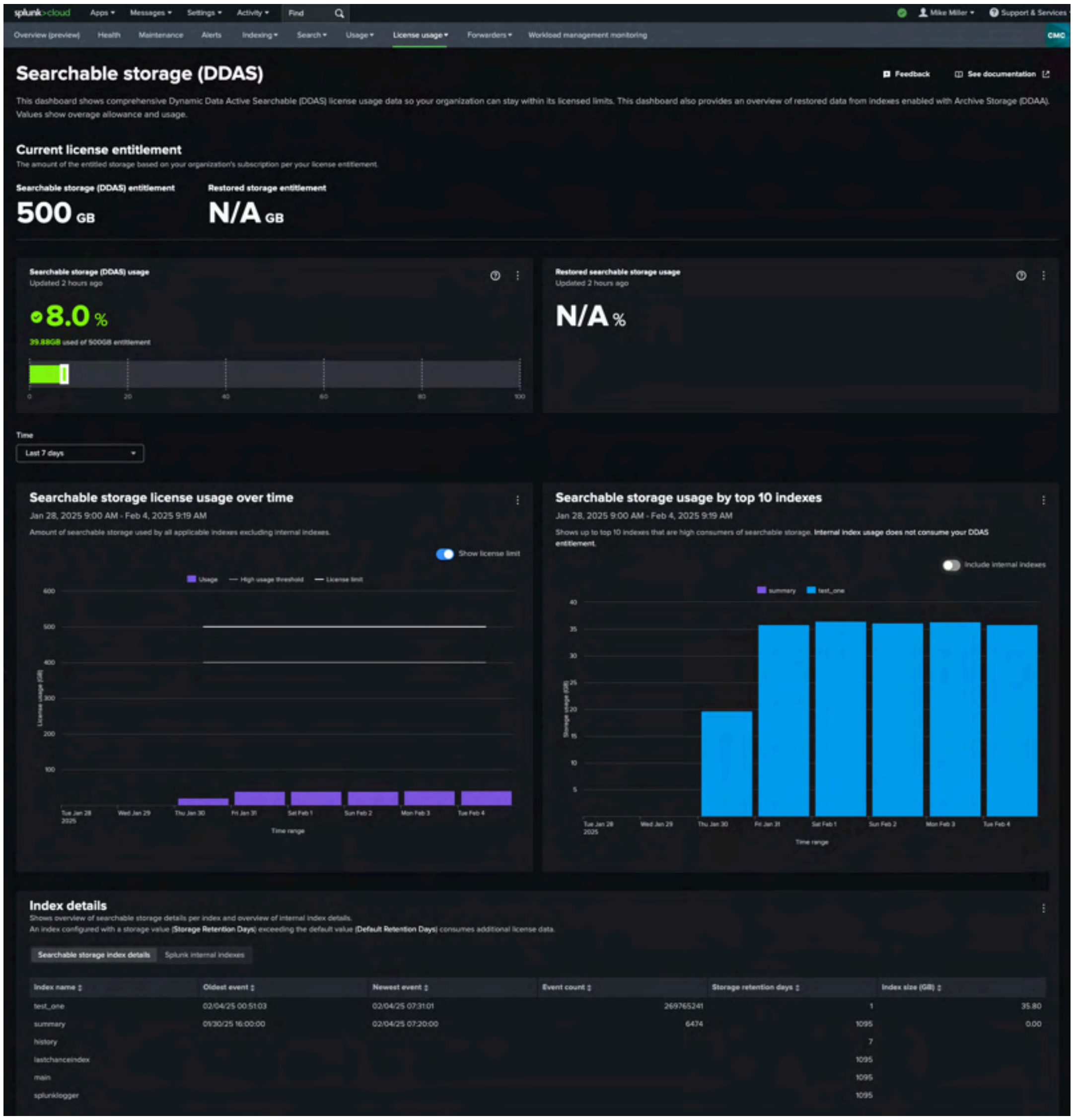
Overview of index retention and storage usage

Index name	Searchable Storage (DDAS) retention days	Searchable Storage (DDAS) index size GB	Archive Storage (DDAA) retention days	Archive Storage (DDAA) usage GB	Archive GB last 90 days	Expired GB last 90 days
_audit	1095	0.53				
_cmc_summary	1095	0.01				
_configtracker	30					
_dsappevent	60	0.00				
_dsclient	60	0.00				
_dsphonehome	7	0.00				
_internal	30	4.23				
_introspection	14	9.94				
_metrics	14	4.77				
_metrics_rollup	730					
_telemetry	730	0.02				
_thefishbucket	28					
history	7					
lastchanceindex	1095					
main	1095					
splunklogger	1095					
summary	1095	0.00				
test_one	1	35.41	10	610.17	610.1735	0

What is the current usage percentage of DDAS?	

6. Next click on LIcense Usage>Searchable Storage DDAS





Searchable storage (DDAS)

This dashboard shows comprehensive Dynamic Data Active Searchable (DDAS) license usage data so your organization can stay within its licensed limits. This dashboard also provides an overview of restored data from indexes enabled with Archive Storage (DDAA). Values show overage allowance and usage.

Current license entitlement

The amount of the entitled storage based on your organization's subscription per your license entitlement.

Searchable storage (DDAS) entitlement
500 GB

Restored storage entitlement
N/A GB

Searchable storage (DDAS) usage
Updated 2 hours ago
8.0 %
39.88GB used of 500GB entitlement

Restored searchable storage usage
Updated 2 hours ago
N/A %

Time: Last 7 days

Searchable storage license usage over time

Jan 28, 2025 9:00 AM - Feb 4, 2025 9:19 AM

Amount of searchable storage used by all applicable indexes excluding internal indexes.

Show license limit

Searchable storage usage by top 10 indexes

Jan 28, 2025 9:00 AM - Feb 4, 2025 9:19 AM

Shows up to top 10 indexes that are high consumers of searchable storage. **Internal index usage does not consume your DDAS entitlement.**

Include internal indexes

Index details

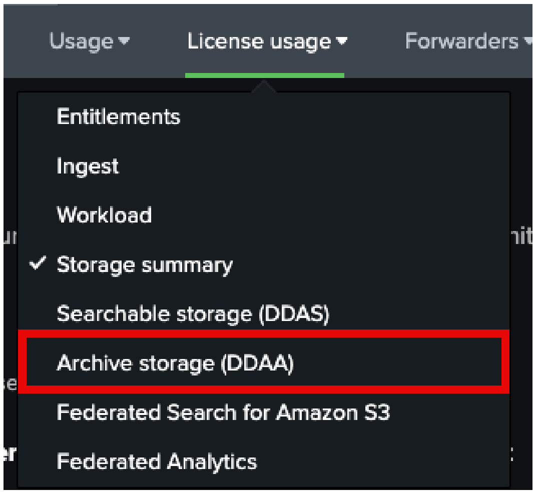
Shows overview of searchable storage details per index and overview of internal index details.
An index configured with a storage value (**Storage Retention Days**) exceeding the default value (**Default Retention Days**) consumes additional license data.

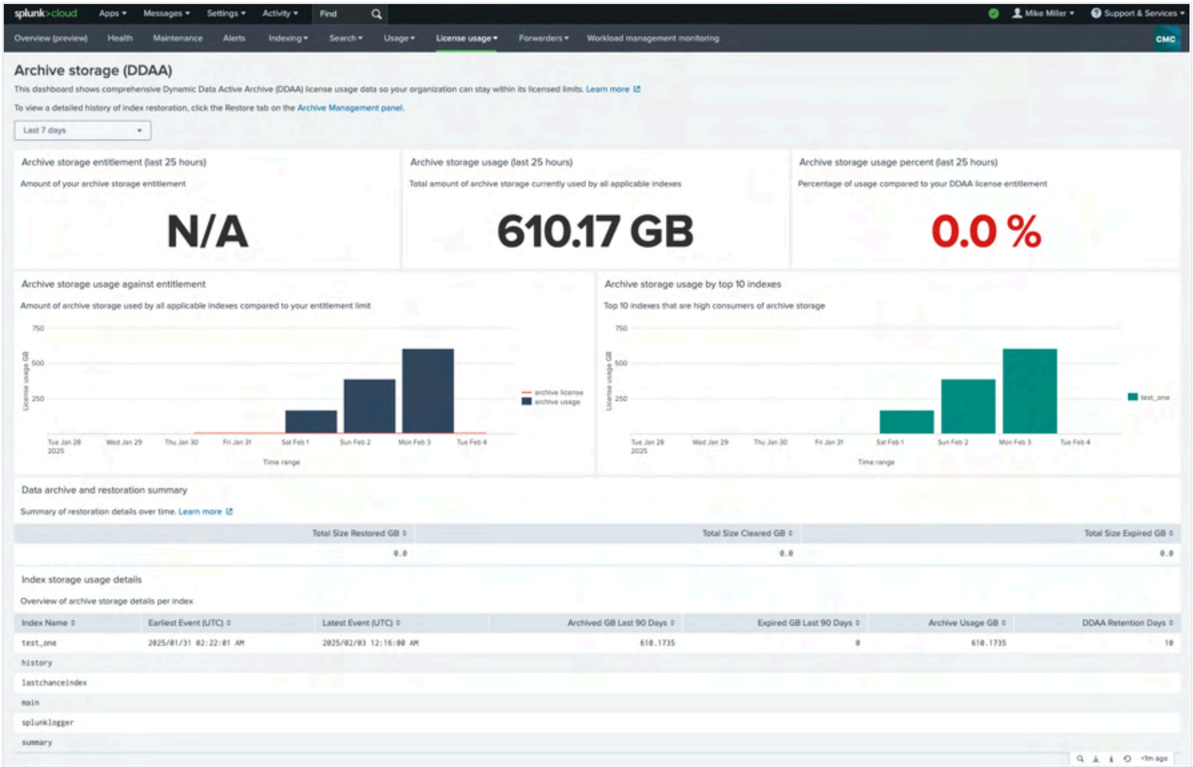
Searchable storage index details | Splunk internal indexes

Index name ↕	Oldest event ↕	Newest event ↕	Event count ↕	Storage retention days ↕	Index size (GB) ↕
test_one	02/04/25 00:51:03	02/04/25 07:31:01	269765241	1	35.80
summary	01/30/25 16:00:00	02/04/25 07:20:00	6474	1095	0.00
history				7	
lastchanceindex				1095	
main				1095	
splunklogger				1095	

What is the value for the number of Storage retention days for the test_one index?	

7. Finally click on License Usage>Archive Storage (DDAA)





Archive storage (DDAA)

This dashboard shows comprehensive Dynamic Data Active Archive (DDAA) license usage data so your organization can stay within its licensed limits. Learn more

To view a detailed history of index restoration, click the Restore tab on the Archive Management panel.

Archive storage entitlement (last 25 hours)

Amount of your archive storage entitlement

N/A

Archive storage usage (last 25 hours)

Total amount of archive storage currently used by all applicable indexes

610.17 GB

Archive storage usage percent (last 25 hours)

Percentage of usage compared to your DDAA license entitlement

0.0 %

Archive storage usage against entitlement

Amount of archive storage used by all applicable indexes compared to your entitlement limit

Archive storage usage by top 10 indexes

Top 10 indexes that are high consumers of archive storage

Data archive and restoration summary

Summary of restoration details over time. Learn more

Total Size Restored GB ⇕	Total Size Cleared GB ⇕	Total Size Expired GB ⇕
0.0	0.0	0.0

Index storage usage details

Overview of archive storage details per index

Index Name ⇕	Earliest Event (UTC) ⇕	Latest Event (UTC) ⇕	Archived GB Last 90 Days ⇕	Expired GB Last 90 Days ⇕	Archive Usage GB ⇕	DDAA Retention Days ⇕
test_one	2025/01/31 02:22:01 AM	2025/02/03 12:16:00 AM	610.1735	0	610.1735	10
history						
lastchanceindex						
main						
splunklogger						
summary						

What is the Archive storage usage (last 25 hours)?	

Completion Tracker (Optional):

You can use this drop down to track your progress of each exercise. This is completely optional, but may be a good indicator in more details or complex workshop scenarios.

Incomplete ▾

Links

Title	Links
Splunk Cloud Platform Service Details	https://docs.splunk.com/Documentation/SplunkCloud/latest/Service/SplunkCloudservice#Storage
Dynamic Data: Data Retention Options in Splunk Cloud	https://www.splunk.com/en_us/blog/platform/dynamic-data-data-retention-options-in-splunk-cloud.html?locale=en_us
Store expired Splunk Cloud Platform data in your private archive	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/DataSelfStorage#Performance
Sizing your Splunk Architecture	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Sizing_your_Splunk_architecture
Optimizing Storage	https://lantern.splunk.com/Splunk_Platform/Splunk_Outcome_Paths/Reduce_Costs/Optimizing_storage
Using Indexing Dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIndexing
Using the License Usage Dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage