Splunk4Admins

Splunk Cloud Storage Workshop

splunk>
a CISCO company

Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

splunk> a CISCO company

Please introduce yourself!

- Name
- Company/organisation
- Role
- Are you currently using Splunk?
- What are you interested in using Splunk for?

Enroll in Today's Workshop

Tasks

1. Get a splunk.com account if you don't have one yet:
   https://splk.it/SignUp
2. Enroll in the Splunk Show workshop event:
   https://show.splunk.com/event/<eventID>
3. Download the hands-on lab guide:
   https://splk.it/S4A-SCS-Lab-Guide

   > Contains step-by-step instructions for all of today's exercises!

4. Download a copy of today's slide deck:
   https://splk.it/S4A-SCS-Attendee

Goal

> Enroll in today's event

Workshop Agenda

- Overview
- Storage Options for Splunk Cloud
- Dynamic Data: Active Searchable (DDAS)
- Dynamic Data: Active Archive (DDAA)
- Dynamic Data: Self Storage (DDSS)
- Best Practices for Splunk Cloud Storage
- Monitoring and Troubleshooting
- Summary

Overview

Splunk Cloud Storage

The goal of this workshop is to review options for monitoring the Splunk Cloud Storage, as well as provide general tips and tricks to optimize performance.

General Expectations

- Duration 60 to 90 Minutes
- Understanding of Splunk Cloud storage configurations and options
- Monitoring Splunk Cloud Storage
- Understanding of Splunk Cloud Storage operations

Audience

Audience	Recommendation
Those who are interested in how to observe and detect issues within Splunk Enterprise Search	
Splunk Admins	
Power User Certified	**Required**
Splunk Admin enabled \ Splunk Admin Certified	**Preferred**

Workshop Agenda

- Overview
- Storage Options for Splunk Cloud
- Dynamic Data: Active Searchable (DDAS)
- Dynamic Data: Active Archive (DDAA)
- Dynamic Data: Self Storage (DDSS)
- Best Practices for Splunk Cloud Storage
- Monitoring and Troubleshooting
- Summary

Storage Options for Splunk Cloud

Overview of Storage Options

Dynamic Data Active Searchable	DDAS	• Set per Index • Default Storage for Splunk Cloud • Initial landing area for all indexed data • Optimized for fast search and analysis
Dynamic Data Active Archive	DDAA	• Set per Index • Long-term lower cost storage • Optimized for data that is less frequently access but needs to remain searchable • Suitable for Legal and compliance purposes • Managed by Splunk
Dynamic Data Self-Storage	DDSS	• Set per index • Long term archiving solution • Stored on customers cloud storage (AWS S3, GCP) • Customer owned and managed

https://docs.splunk.com/Documentation/SplunkCloud/latest/Service/SplunkCloudservice#Storage

Workshop Agenda

- Overview
- Storage Options for Splunk Cloud
- Dynamic Data: Active Searchable (DDAS)
- Dynamic Data: Active Archive (DDAA)
- Dynamic Data: Self Storage (DDSS)
- Best Practices for Splunk Cloud Storage
- Monitoring and Troubleshooting
- Summary

Diving Deeper on DDAS

Dynamic Data Active Searchable - Use Case Examples

Use Case:

- **Data must be stored and retrieved in the index as fast as possible with little to no latency.**
- Data must be stored, for compliance purposes, for 180 Days then it can be purged
- Uncompressed data is estimated to be between 500 GB and **700 GB** per day.

- **Fastest storage**
- Most Expensive
- **Intended for fast search and retrieval**
- **Intended for short term storage**
- Directly attached to Splunk Cloud Instance.

- Slower storage
- More Cost effective
- Intended for long term archival and compliance
- Directly attached to Splunk Cloud instance

- Slower storage
- Costs vary
- Intended for long term archival and compliance
- Cannot be restored to Splunk Cloud
- Customer Managed

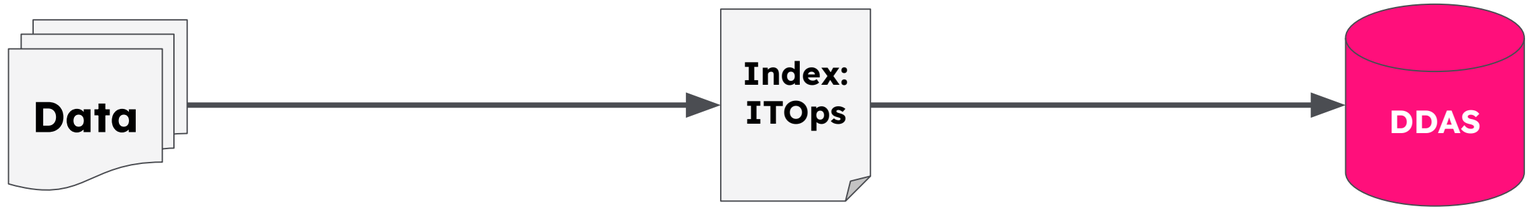
Dynamic Data: Data Retention Options in Splunk Cloud Platform
Splunk Cloud Platform Service Details

Diving Deeper on DDAS

Dynamic Data Active Searchable - Use Case Examples

Use Case:

- Data must be stored and retrieved in the index as fast as possible with little to no latency.
- **Data must be stored, for compliance purposes, for 180 Days then it can be purged**
- **Uncompressed data is estimated to be between 500 GB and 700 GB per day.**



Uncompressed Data:
700 GB per day

✖

Retention Requirement:
180 Days

=

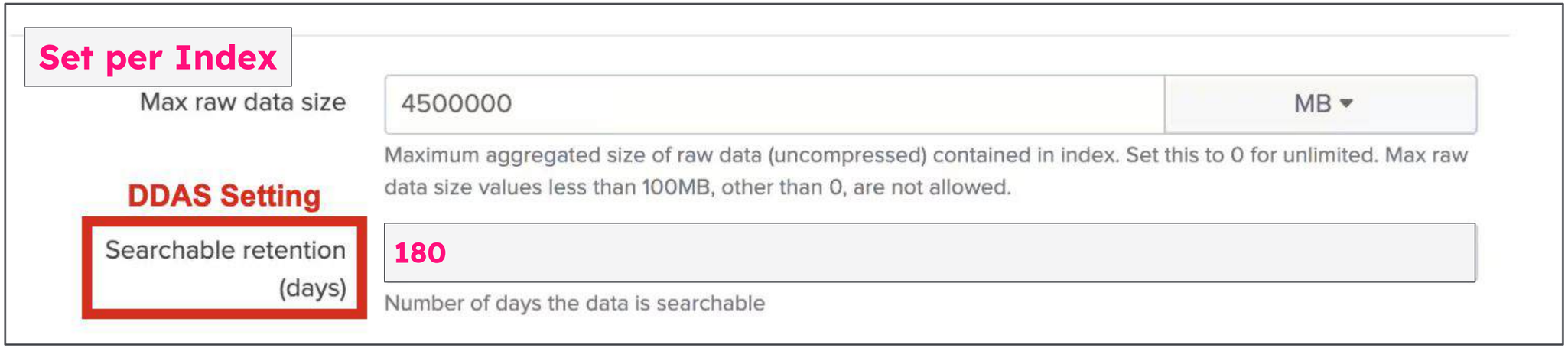
Storage Needed:
126 TB + 10% = **138.6 TB**
(adjusted 139 TB DDAS)

Dynamic Data: Data Retention Options in Splunk Cloud Platform
Splunk Cloud Platform Service Details

Diving Deeper on DDAS

Dynamic Data Active Searchable - Data Retention Configuration

Setting DDAS Searchable Retention for an index. Using our previous example we will use **180 Days** as the value for the number of days the data is searchable



Dynamic Data: Data Retention Options in Splunk Cloud Platform

Exercise 1

Create a new index with DDAA

In this exercise you will:

- Create a new index in Splunk Cloud called test_two
- Attach DDAA to the index

Workshop Agenda

- Overview
- Storage Options for Splunk Cloud
- Dynamic Data: Active Searchable (DDAS)
- Dynamic Data: Active Archive (DDAA)
- Dynamic Data: Self Storage (DDSS)
- Best Practices for Splunk Cloud Storage
- Monitoring and Troubleshooting
- Summary

Diving Deeper on DDAA

Dynamic Data Active Archive - Data Retention

Use Case:

- Data must be stored into an archive for 3 years
- Archive data must be able to be restored as quickly as possible to meet legal requirements
- Archival solution must be more cost effective than DDAS

- Fastest storage
- Most Expensive
- Intended for fast search and retrieval
- Intended for short term storage
- Directly attached to Splunk Cloud Instance.

- Slower storage
- More Cost effective
- Intended for long term archival and compliance
- Directly attached to Splunk Cloud instance

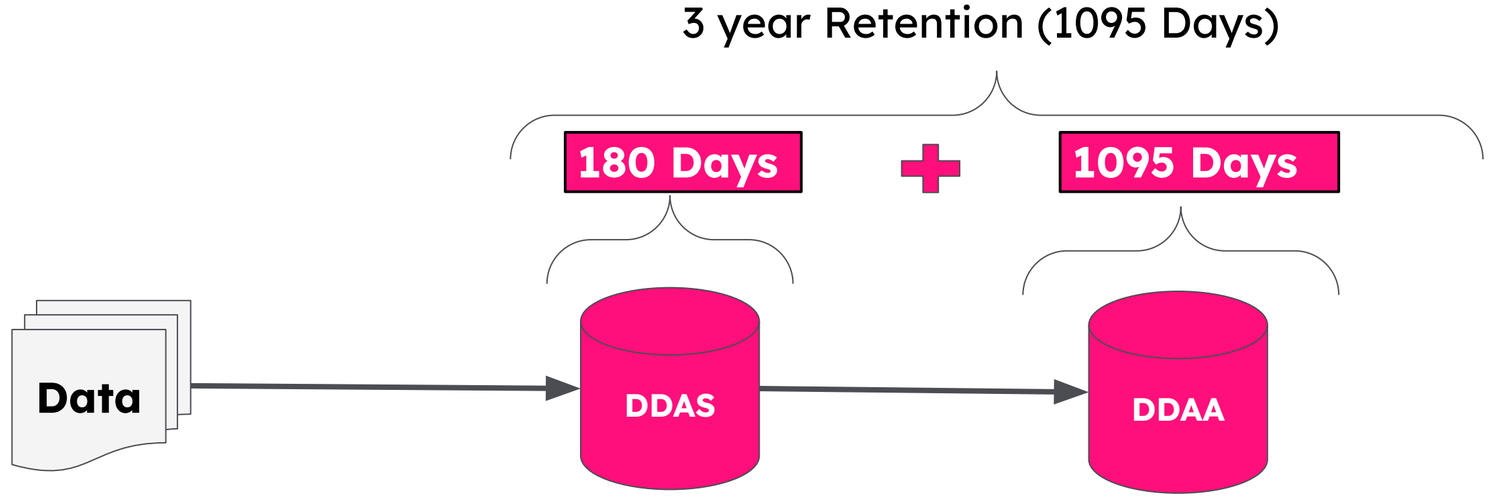
- Slower storage
- Costs vary
- Intended for long term archival and compliance
- Cannot be restored to Splunk Cloud
- Customer Managed

Dynamic Data: Data Retention Options in Splunk Cloud Platform
Splunk Cloud Platform Service Details

Diving Deeper on DDAA

Dynamic Data Active Archive - How DDAA and DDAS work together

Data Storage Process:



Data is ingested and stored in DDAS based on the searchable retention setting (slide 18)

Once the retention setting is reached (in this configuration) data is moved to DDAA for archival storage

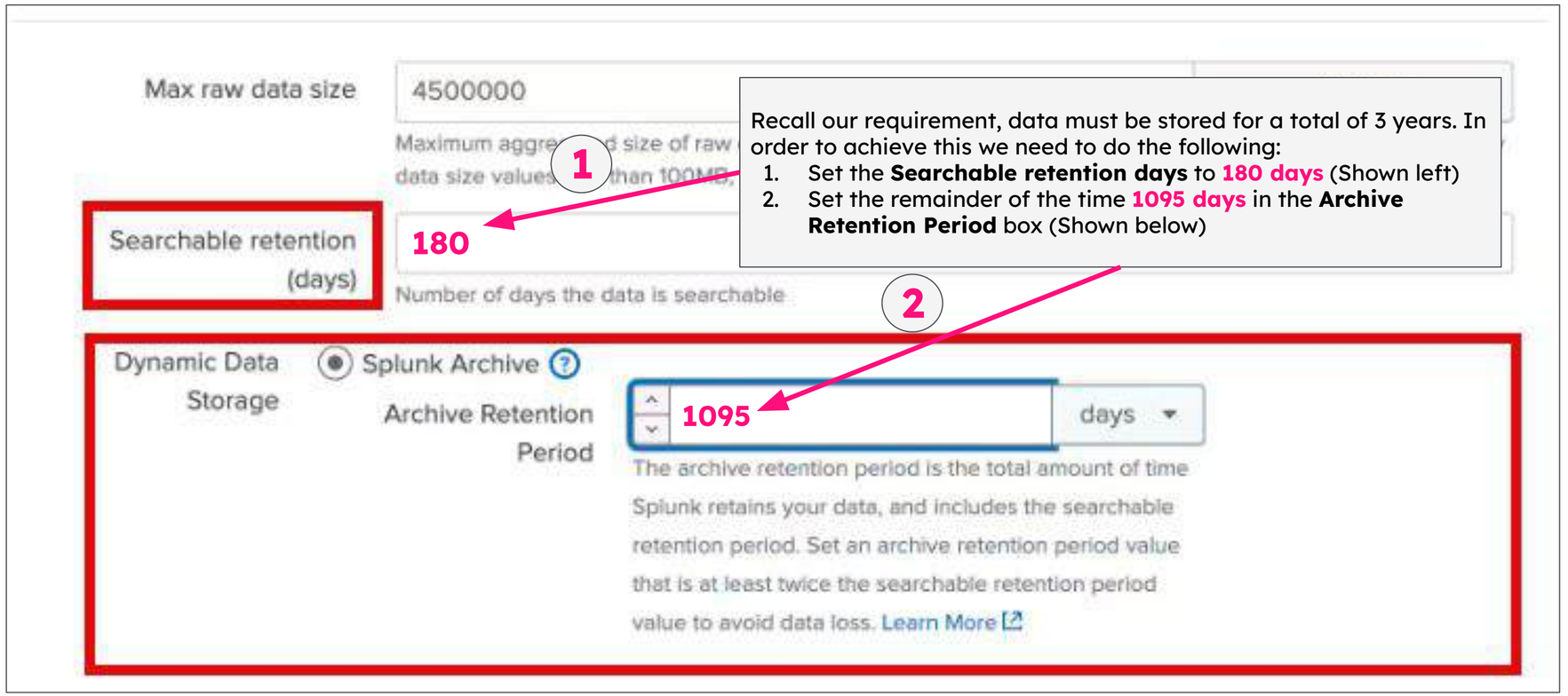
- Data must be restored from archive
- The restored data is then placed into DDAS cache in the source index

Dynamic Data: Data Retention Options in Splunk Cloud Platform
Splunk Cloud Platform Service Details

Diving Deeper on DDAA

Dynamic Data Active Searchable - Data Retention Configuration

Setting DDAA Archive Retention for an index. Using our previous example we will use **180 Days** as the value for the number of days the data is searchable



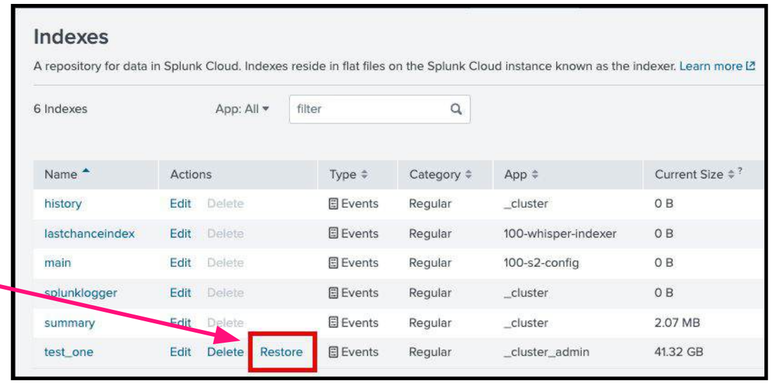
Dynamic Data: Data Retention Options in Splunk Cloud Platform
Store expired Splunk Cloud Platform data in a Splunk-managed archive

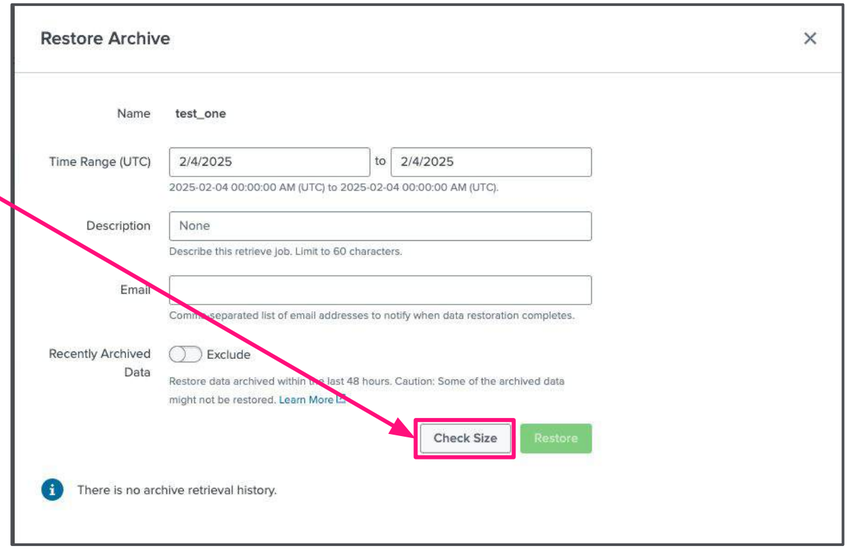
Diving Deeper on DDAA

Dynamic Data Active Searchable - Data restoration process

Steps to restore archived data to Splunk Cloud Platform

1. In Splunk Cloud, go to **Settings > Indexes**.
2. For the index where you want to restore data, click **Restore**. The menu displays the restore history for the specified index. You can see the history of data restoration and file size for the data restored.
3. Use the date picker to select a time range to retrieve.
4. Click **Check size**. Splunk Cloud Platform checks to see if the size of the file might impact performance. If the file size is too large, Splunk Cloud Platform blocks you from restoring data. If there is a potential performance impact, Splunk Cloud Platform displays a warning. Splunk Cloud Platform also prevents you from restoring data that overlaps with existing restored data.
5. Enter an email address to send job status notifications. Splunk Cloud Platform will notify you when the restoration is complete.
6. (Optional) If your time range includes data archived within the last 48 hours, toggle the **Recently Archived Data** switch to disable the default **Exclude** mode. When set to "Exclude" mode, DDAA skips restoration of data archived within the last 48 hours. Note that attempting to restore data that is not fully archived can cause data restoration to fail. For more information, see Troubleshoot Dynamic Data Active Archive.
7. Click **Restore** when you have refined the file size or date range to acceptable limits.





After you initiate data restoration, it can take up to 24 hours before data is restored. If it takes longer than 24 hours, contact Splunk Technical Support.

- Dynamic Data: Data Retention Options in Splunk Cloud Platform
- Store expired Splunk Cloud Platform data in a Splunk-managed archive

Workshop Agenda

- Overview
- Storage Options for Splunk Cloud
- Dynamic Data: Active Searchable (DDAS)
- Dynamic Data: Active Archive (DDAA)
- Dynamic Data: Self Storage (DDSS)
- Best Practices for Splunk Cloud Storage
- Monitoring and Troubleshooting
- Summary

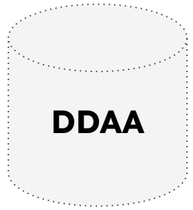
Diving Deeper on DDSS

Dynamic Data Self Storage - Data Retention

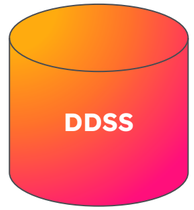
Use Case:

- Data must be stored into an archive for 3 years
- Data in the archive is rarely recalled
- Archive storage must stay under customer management

- Fastest storage
- Most Expensive
- Intended for fast search and retrieval
- Intended for short term storage
- Directly attached to Splunk Cloud Instance.



- Slower storage
- More Cost effective
- Intended for long term archival and compliance
- Directly attached to Splunk Cloud instance



- Slower storage
- Costs vary
- **Intended for long term archival and compliance**
- **Cannot be restored to Splunk Cloud**
- **Customer Managed**

NOTE: Data stored into a customers DDSS archive must be restored to a separate instance of Splunk Enterprise. This instance is not in any way connected to Splunk Cloud and must be either an existing or new instance of Splunk Enterprise. This can be either located on-premises but ideally should be in AWS/GCP in the same region for faster recovery.

Dynamic Data: Data Retention Options in Splunk Cloud Platform

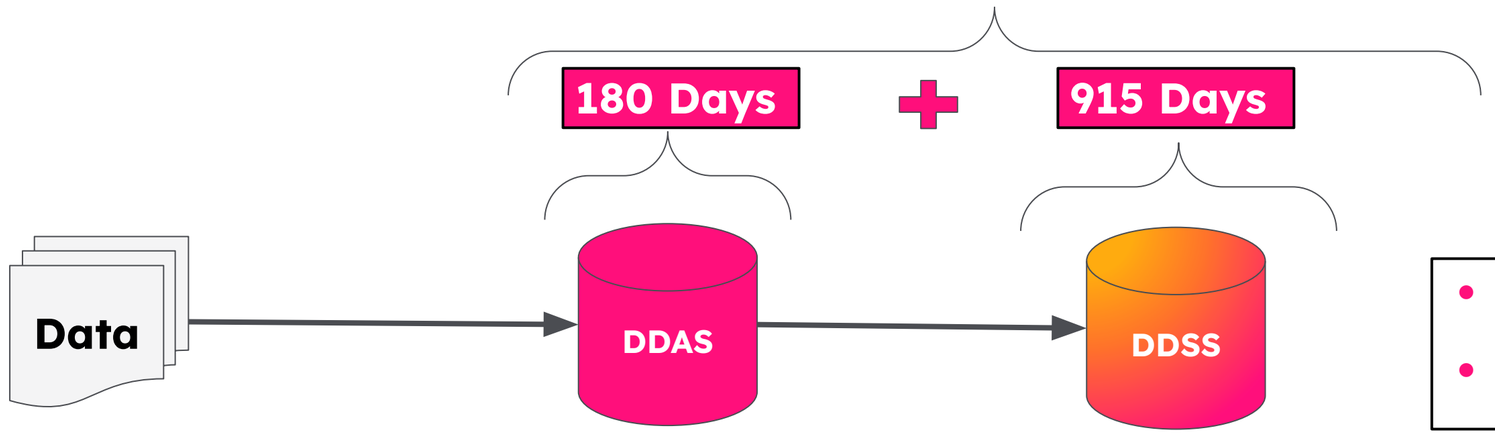
Splunk Cloud Platform Service Details

Diving Deeper on DDSS

Dynamic Data Active Archive - Planning Retention on DDSS

Data Storage Process:

3 year Retention (1095 Days)



- **Data is not searchable from Splunk Cloud**
- **Data cannot be directly restored to Splunk Cloud**

Data is ingested and stored in DDAS based on the searchable retention setting (slide 18)

Once the retention setting is reached (in this configuration) data is moved to DDSS for archival storage

Dynamic Data: Data Retention Options in Splunk Cloud Platform
Splunk Cloud Platform Service Details

Diving Deeper on DDSS

Dynamic Data Active Searchable - Leveraging AWS S3

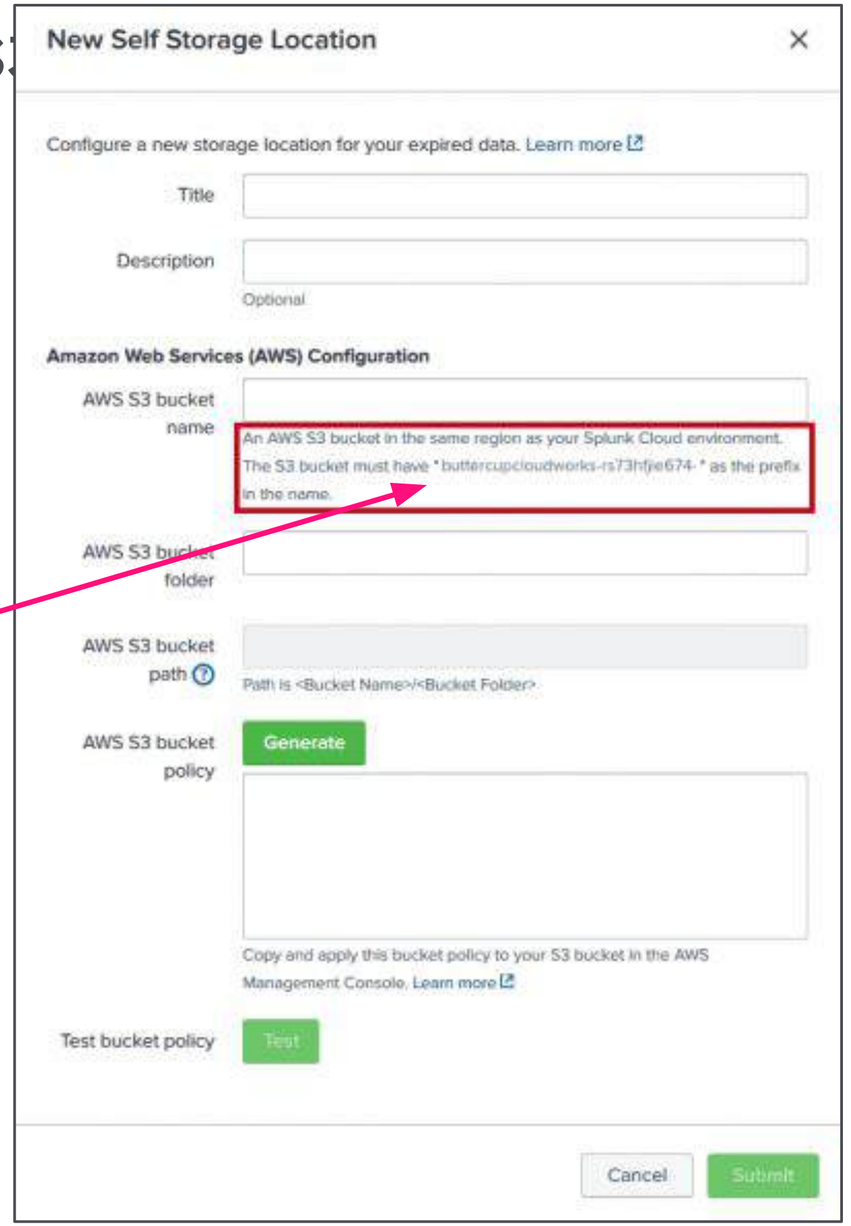
Part 1: Create an Amazon S3 bucket in your AWS Environment

Region: You must provision your Amazon S3 bucket in the same region as your Splunk Cloud Platform environment.

Object Lock: Do not activate AWS S3 Object Lock when creating a bucket. Locking the bucket prevents DDSS from moving data to the bucket. For more information, see https://docs.aws.amazon.com/AmazonS3/latest/user-guide/object-lock.html

Naming: When you name the S3 bucket, it **must include the Splunk prefix provided to you** and displayed in the UI under the **AWS S3 bucket name** field. Enter the prefix *before* the rest of the bucket name. This prefix contains your organization's Splunk Cloud ID, which is the first part of your organization's Splunk Cloud URL, and a 12-character string. The complete S3 bucket name has the following syntax:

```
Splunk Cloud ID-{12-character string}-{your bucket name}
```



https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/DataSelfStorage#Performance

Diving Deeper on DDSS

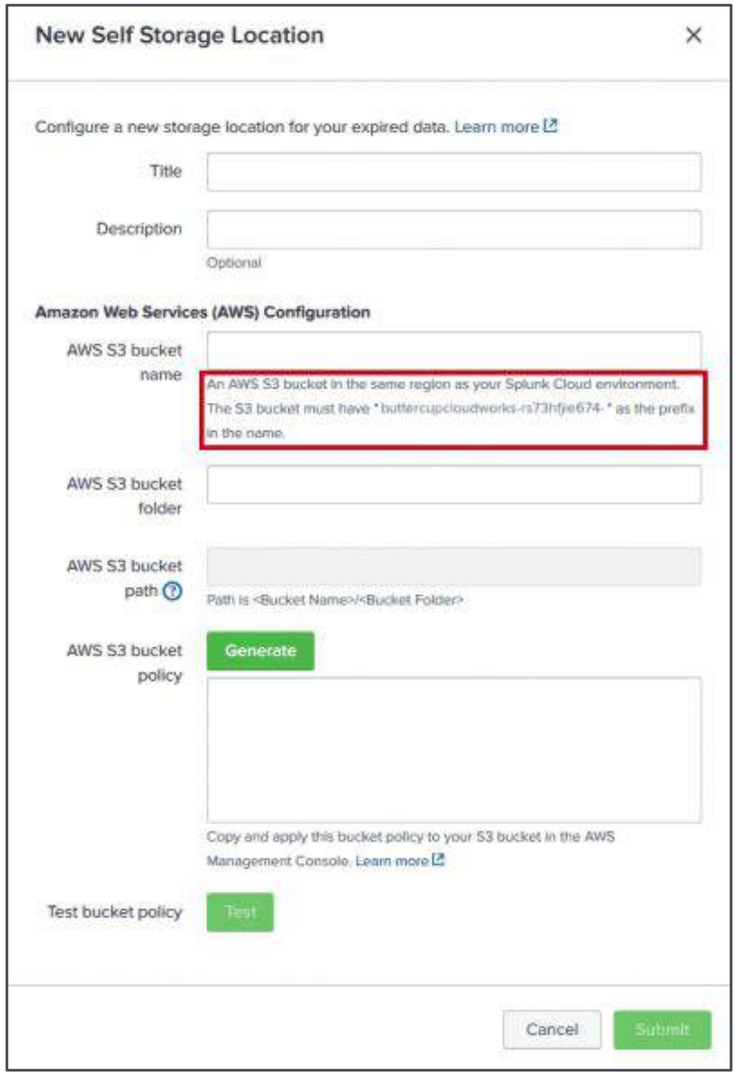
Dynamic Data Active Searchable - Leveraging AWS S3

https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/DataSelfStorage#Performance

Part 2: Configure a self storage location for the Amazon S3 bucket

1. In Splunk Web, click **Settings > Indexes > New Index**.
2. In the **Dynamic Data Storage** field, click the radio button for **Self Storage**.
3. Click **Create a self storage location**.
   The Dynamic Data Self Storage page opens.
4. Give your location a **Title** and an optional **Description**.
5. In the **Amazon S3 bucket name** field, enter the name of the S3 bucket that you created.
6. (Optional) Enter the bucket folder name.
7. Click **Generate**. Splunk Cloud Platform generates a bucket policy.
8. Copy the bucket policy to your clipboard. Note: Customers with an SSE-S3 encrypted bucket must use the default policy and not modify the policy in any way.
9. In a separate window, navigate to your AWS Management console and apply this policy to the S3 bucket you created earlier.
10. In the Self Storage Locations dialog, click **Test**.
    Splunk Cloud writes a 0 KB test file to the root of your S3 bucket to verify that Splunk Cloud Platform has permissions to write to the bucket. A success message displays, and the **Submit** button is enabled.
11. Click **Submit**.
12. In the AWS Management Console, verify that the 0 KB test file appears in the root of your bucket.

You cannot edit or delete a self storage location after it is defined, so verify the name and description before you save it.



Exercise 2

Practice data restore process from DDAA

In this exercise you will:

- Follow the process for restoration of data from DDAA to the target index test_two

NOTE: No data restoration will take place in this lab due to limitations in the lab environment, however this is still good practice.

Workshop Agenda

- Overview
- Storage Options for Splunk Cloud
- Dynamic Data: Active Searchable (DDAS)
- Dynamic Data: Active Archive (DDAA)
- Dynamic Data: Self Storage (DDSS)
- Best Practices for Splunk Cloud Storage
- Monitoring and Troubleshooting
- Summary

Optimizing Storage

Click Here 

Creating Data Retention Policies

This section outlines the following steps to help you create a balance between data availability, compliance requirements, and storage efficiency. In the next few slides we will cover the following items.

1. **Understanding compliance requirements and business needs**
2. **Categorizing data types**
3. **Determining appropriate retention periods**
4. **Setting bucket roll behavior**
5. **Implementing automatic data archival**
6. **Testing and validating**
7. **Communicating and documenting**

Click Here →

Monitoring and alerting in storage

Being informed in real-time when your storage approaches crucial limits is vital. Proactive alerting mechanisms can make the difference between business-as-usual and an unforeseen outage. This article details how you can set up effective safeguards, plan for future needs, and ensure data is managed through its entire lifecycle efficiently in the Splunk platform

- **Understanding storage demands**
- **Understanding the benefits of proactive storage monitoring and alerting**
- **Monitoring storage capacity**
- **Alerting for storage capacity**
- **Planning and managing capacity proactively**
- **Following best practices for proactive monitoring and alerting**

Platform Capacity Considerations	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/DataSelfStorage#Performance
Sizing you 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

Workshop Agenda

- Overview
- Storage Options for Splunk Cloud
- Dynamic Data: Active Searchable (DDAS)
- Dynamic Data: Active Archive (DDAA)
- Dynamic Data: Self Storage (DDSS)
- Best Practices for Splunk Cloud Storage
- Monitoring and Troubleshooting
- Summary

Cloud Monitoring Console

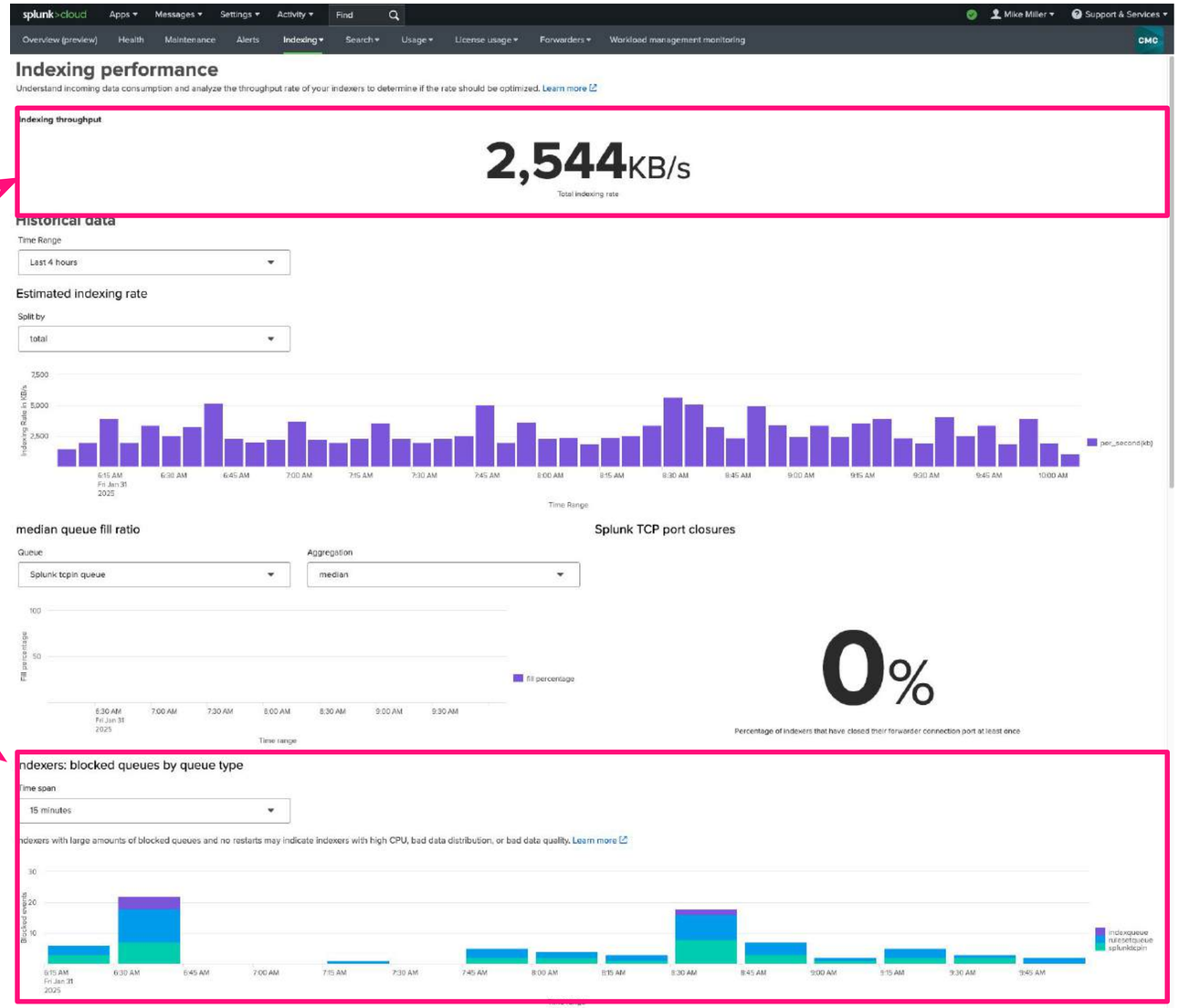
Splunk Cloud CMC Dashboards for Storage Monitoring

Indexing Performance:
While the Indexing Performance dashboard does not directly address storage, it is critical to understand your Splunk Cloud instances throughput.

Key Sections to monitor:

- Indexing Performance
- Indexers: blocked queues by type

If your throughput volume is higher than expected it could negatively impact your storage forecasting and performance.



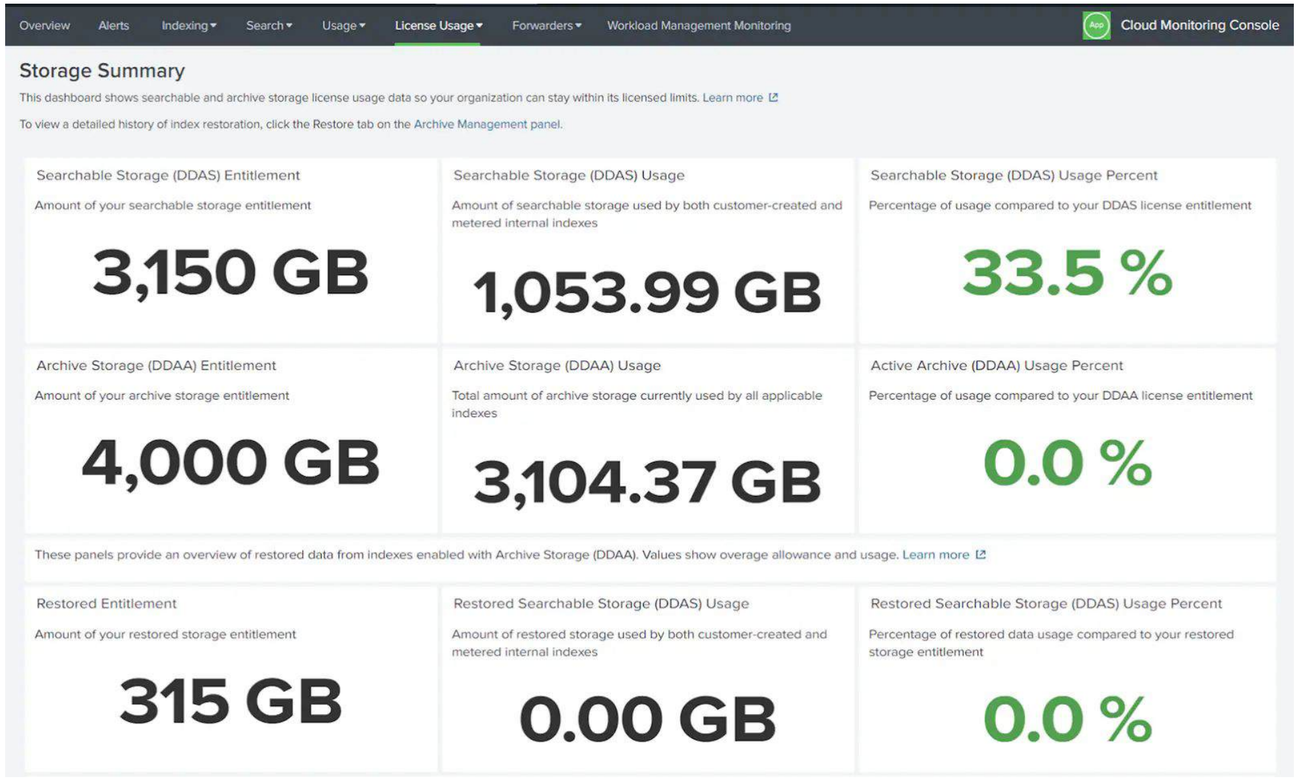
CMC - Monitoring Indexing	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIndexing

Cloud Monitoring Console

Storage Summary Dashboard

Location:
Cloud Monitoring Console>Licensing Usage>Storage Summary

Overview:
The screenshot shows an example of the Dynamic Data Active Searchable (DDAA) dashboard. The Storage Summary dashboard highlights important information that also displays on the Entitlements, Searchable Storage (DDAS), and Archive Storage (DDAA) dashboards. This dashboard provides insights into your data retention based on the uncompressed data you have indexed.



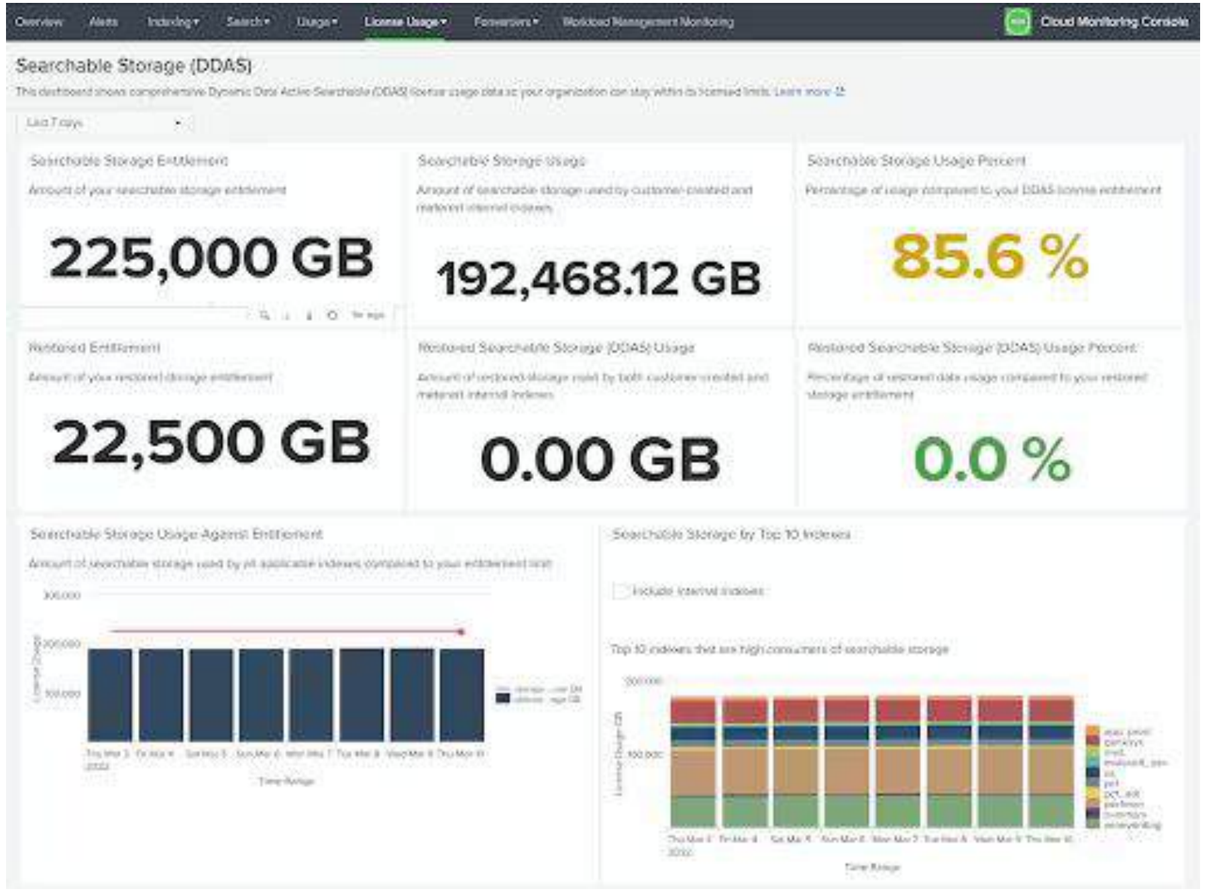
Monitoring License Usage:	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage

Cloud Monitoring Console

Search Storage (DDAS)

Location:
Cloud Monitoring Console>Licensing Usage>Searchable Storage (DDAS)

Overview:
The screenshot shows an example of the Dynamic Data Active Searchable (DDAA) dashboard. This dashboard shows details about your DDAS storage entitlement in GB.



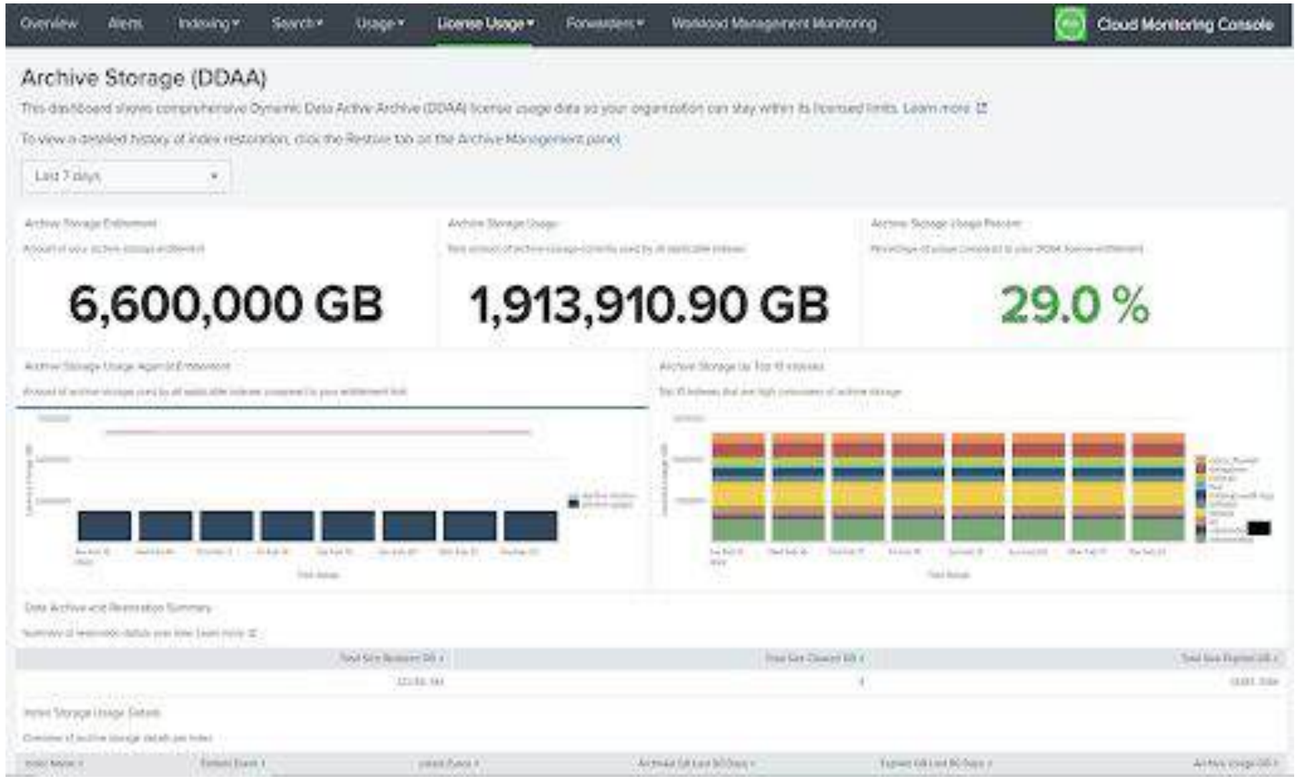
Monitoring License Usage:	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage

Cloud Monitoring Console

Archive Storage (DDAA)

Location:
Cloud Monitoring Console>Licensing Usage>Archive Storage (DDAA)

Overview:
The screenshot shows an example of the Dynamic Data Active Archive (DDAA) dashboard. This dashboard shows details about your DDAA storage entitlement in GB.



Monitoring License Usage:	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage

Exercise 3

Reviewing the Splunk Cloud - Cloud Monitoring Console

In this exercise you will:

- Navigate to the storage and indexing related CMC dashboards
- Review the data associated with each of the dashboards.

Workshop Agenda

- Overview
- Storage Options for Splunk Cloud
- Dynamic Data: Active Searchable (DDAS)
- Dynamic Data: Active Archive (DDAA)
- Dynamic Data: Self Storage (DDSS)
- Best Practices for Splunk Cloud Storage
- Monitoring and Troubleshooting
- Summary

Summary

- Review of Splunk Cloud Storage Options
- Storage Use Case reviews
- Retention calculation
- Best practices for Splunk Cloud Storage
- Monitoring and troubleshooting of Splunk Cloud storage

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

Thank you

splunk> a CISCO company