Splunk4Admins - Cloud Monitoring Console

Lab Guide

Overview

This lab guide contains the hands-on exercises for the **Splunk4Admins - Cloud Monitoring Console** 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-CMC-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 when accessing 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

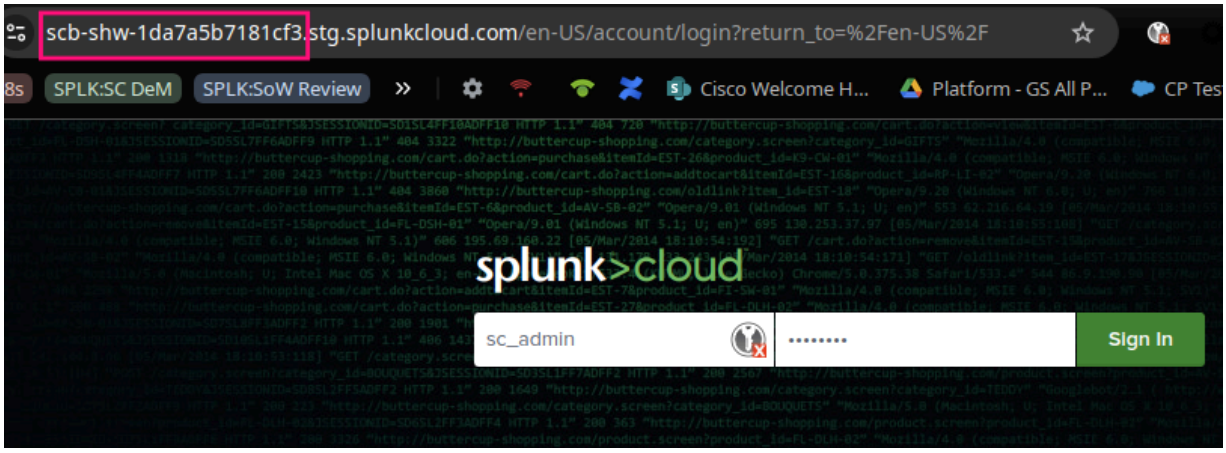
Exercise 1 – Explore Overview / Health / Maintenance / Alerts

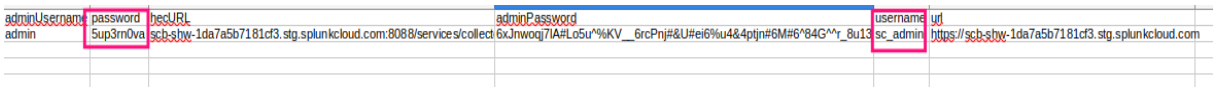
Description

Explore the CMC Overview, Health, Maintenance, and Alerts dashboards.

Steps

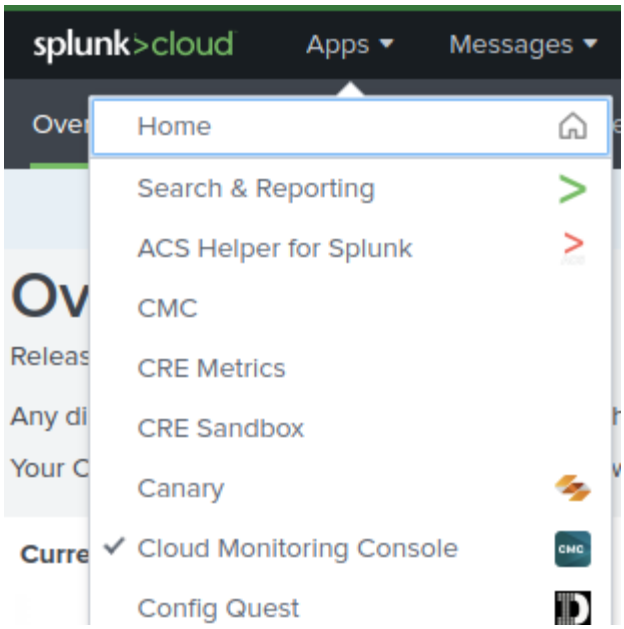
1. Access the Cloud instance assigned to each attendee
2. Login with “sc_admin” and the password “5up3rn0va”. At login, the user will be required to generate a new password, any password that passes the standard Splunk password minimums is fine, but it is recommended to record the password somewhere, just in case.



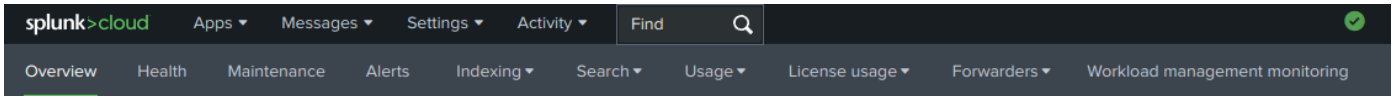


adminUsername	password	hecURL	adminPassword	username	url
admin	5up3rn0va	scb-shw-1da7a5b7181cf3.stg.splunkcloud.com:8088/services/collect	6xJnwoqj7lA#Lo5u^%KV__6rcPnj#&U#ei6%u4&4ptjn#6M#6^84G^^r_8u13	sc_admin	https://scb-shw-1da7a5b7181cf3.stg.splunkcloud.com

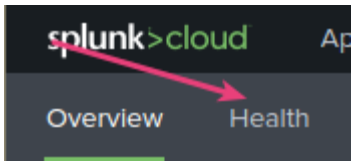
3. Find the Cloud Monitoring Console App



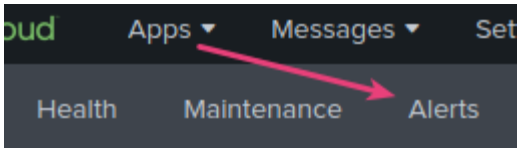
4. Observe the dashboards available, select and explore the Overview dashboard



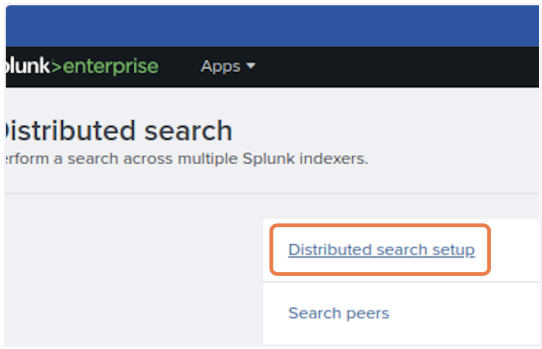
5. Select and explore the Health dashboard



6. Select and explore the Alerts dashboard



7. Select and explore the Health dashboard


lunk>enterprise
Apps
istributed search
erform a search across multiple Splunk indexers.
Distributed search setup
Search peers

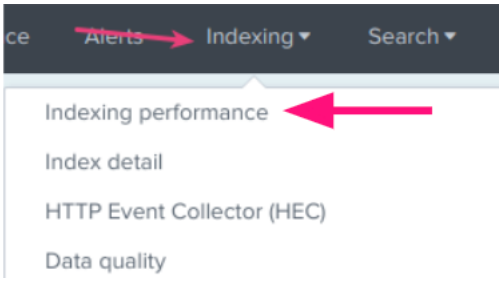
Exercise 2 – Explore the Indexing dashboards

Description

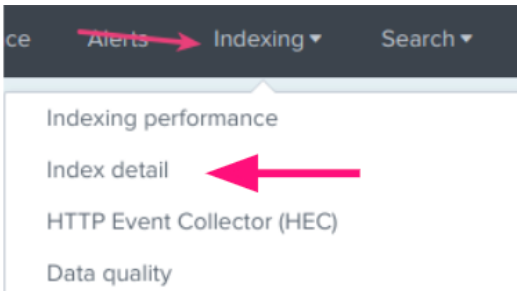
There are four dashboards in the Indexing menu, Indexing performance, Index detail, HTTP Event Collector (HEC), and Data quality. Explore these to understand what can be discovered on them.

Steps

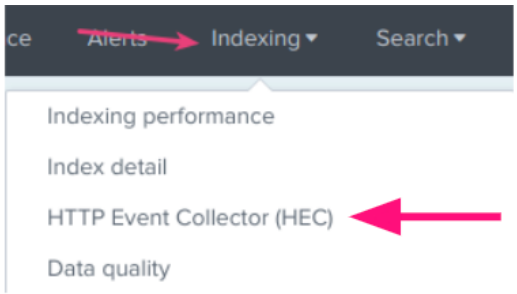
1. Select "**Indexing**" and then "**Indexing performance**"



2. Select "**Indexing**" and then "**Index detail**"

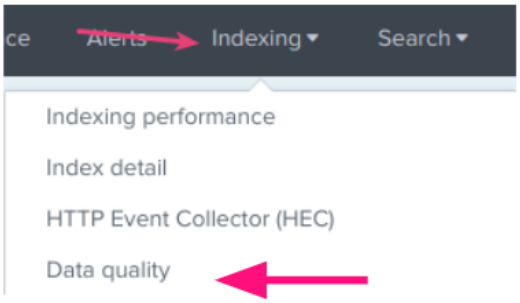


3. Select "**Indexing**" and then "**HTTP Event Collector (HEC)**"



splunk>

4. Select “**Indexing**” and then “**Data quality**”



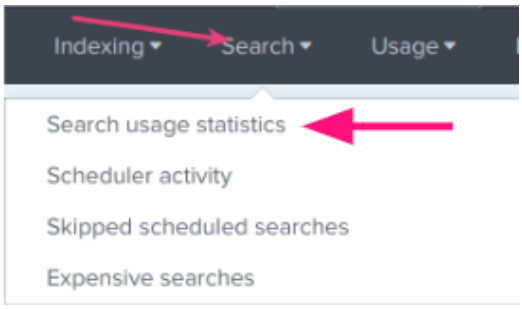
Exercise 3 – Explore the Search dashboards

Description

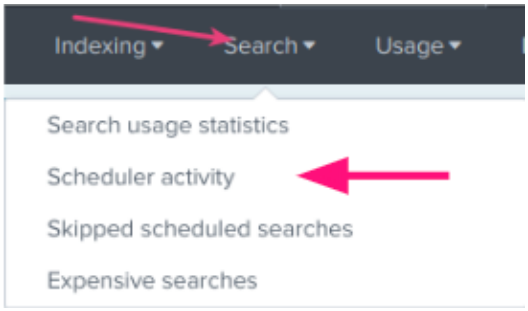
Explore the four dashboards associated with Search, Search usage statistics, Scheduler activity, Skipped scheduled searches, and Expensive searches.

Steps

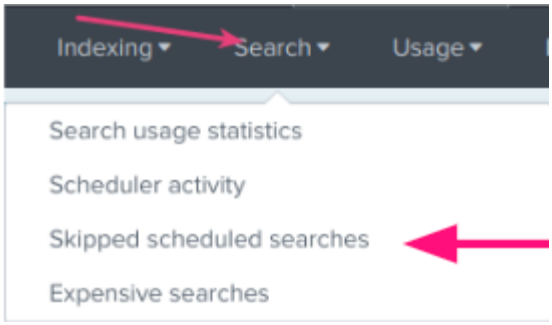
1. Click on "**Search**" and then "**Search usage statistics**"



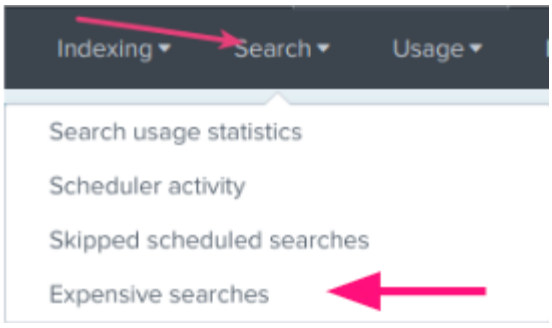
2. Click on "**Search**" and then "**Scheduler activity**"



3. Click on "**Search**" and then "**Skipped scheduled searches**"



4. Click on “**Search**” and then “**Expensive searches**”



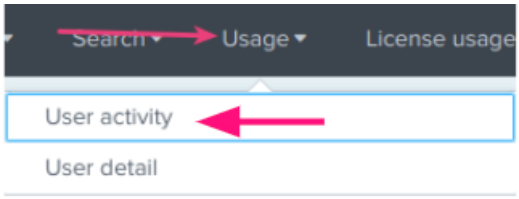
Exercise 4 – Explore the Usage dashboards

Description

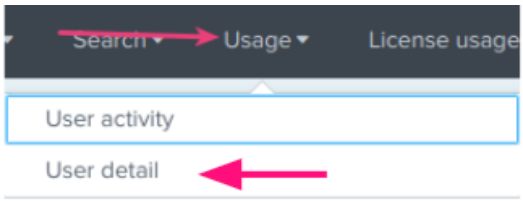
Explore the two dashboards under the Usage menu, “User activity” and “User detail”

Steps

1. Click on “**Usage**” and then “**User activity**”



2. Click on “**Usage**” and then “**User activity**”



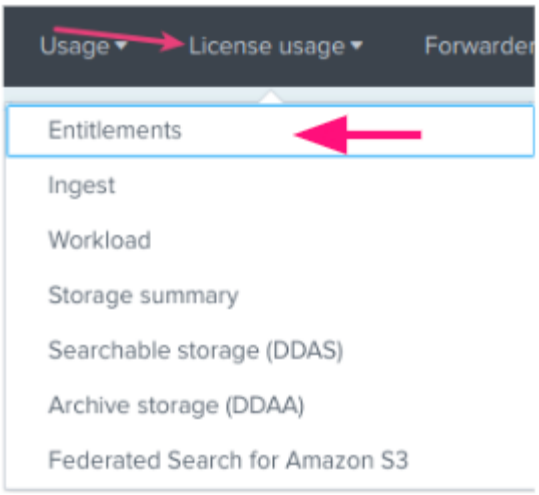
Exercise 5 – Explore the License Usage dashboards

Description

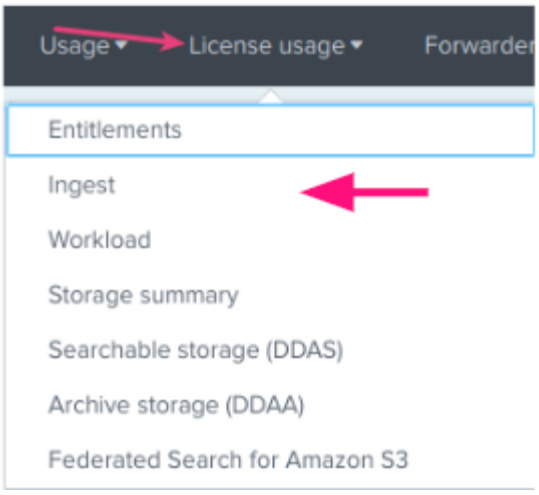
Explore the seven dashboards under the “License Usage” menu, “Entitlements”, “Ingest”, “Workload”, “Storage summary”, “Searchable storage (DDAS)”, “Archive storage (DDAA)”, and “Federated Search for Amazon S3”

Steps

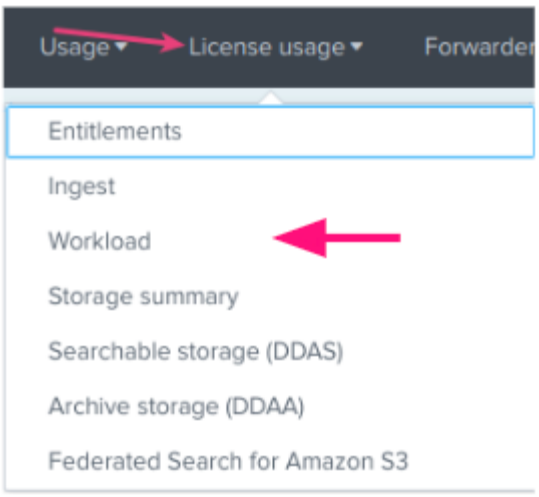
1. Click on “**License Usage**” then “**Entitlements**”



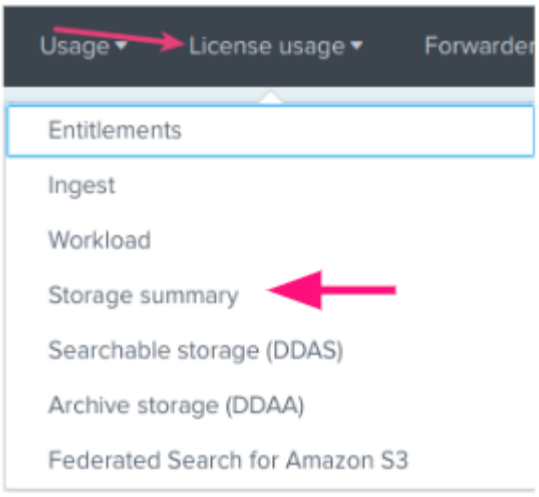
2. Click on **“License Usage**” then “**Ingest**”



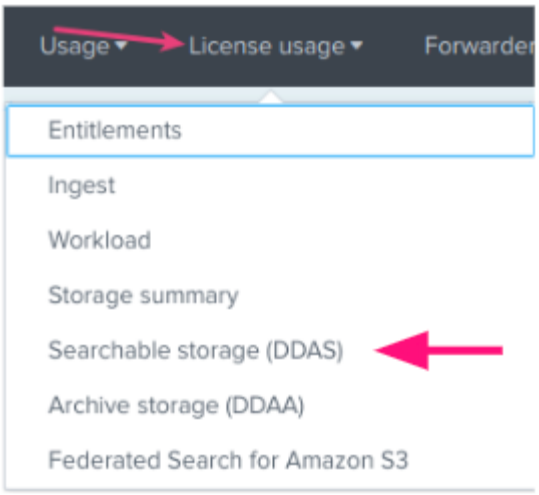
3. Click on “**License Usage**” then “**Workload**”



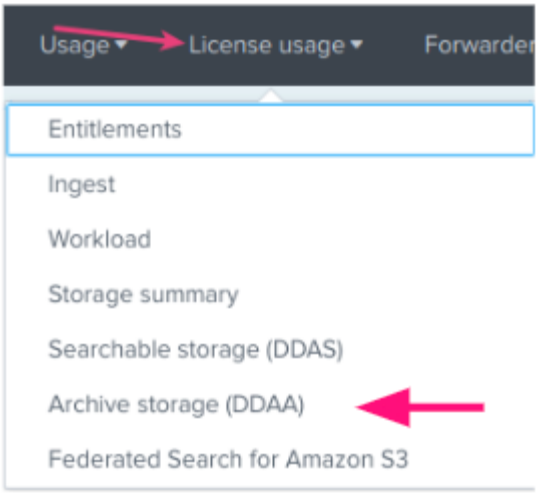
4. Click on **“License Usage**” then “**Storage summary**”



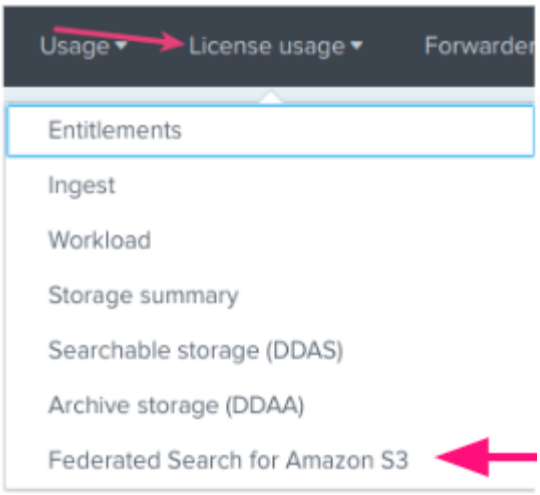
5. Click on “**License Usage**” then “**Searchable storage (DDAS)**”



6. Click on **“License Usage**” then “**Archive storage (DDAA)**”



7. Click on “**License Usage**” then “**Federated Search for Amazon S3**”



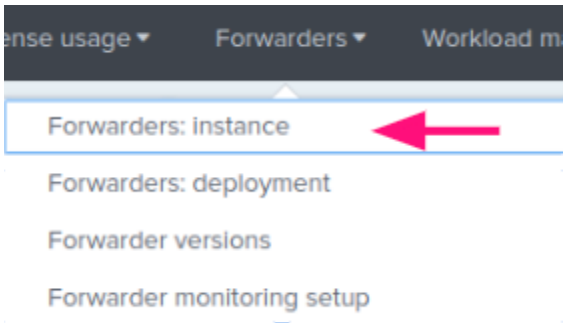
Exercise 6 – Explore Forwarders

Description

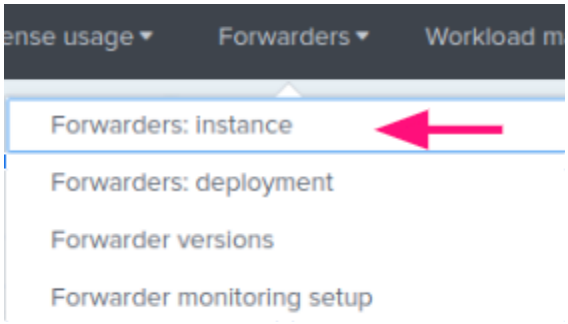
Explore the four dashboards under the “Forwarders” menu, “Forwarders:Instance”, “Forwarders:deployment”, “Forwarder versions”, “Forwarder monitoring setup”

Steps

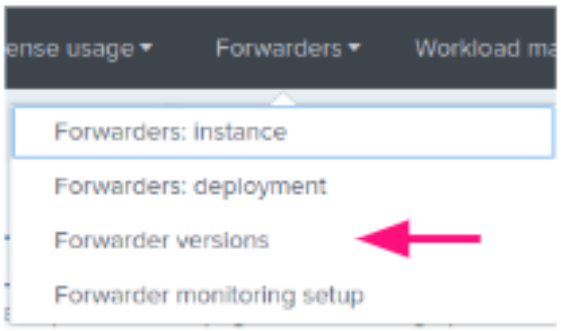
1. Click on “**Forwarders**” then “**Forwarders:Instance**”



2. Click on “**Forwarders**” then “**Forwarders:deployment**”

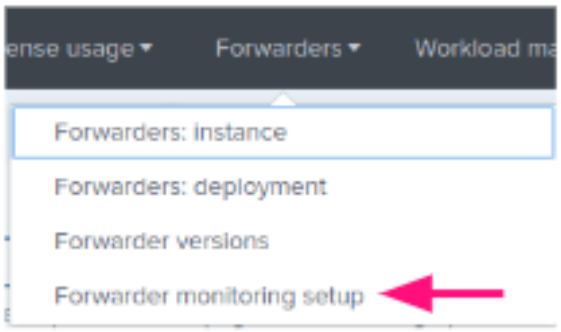


3. Click on “**Forwarders**” then “**Forwarder versions**”



splunk>

4. Click on “**Forwarders**” then “**Forwarder monitoring setup**”



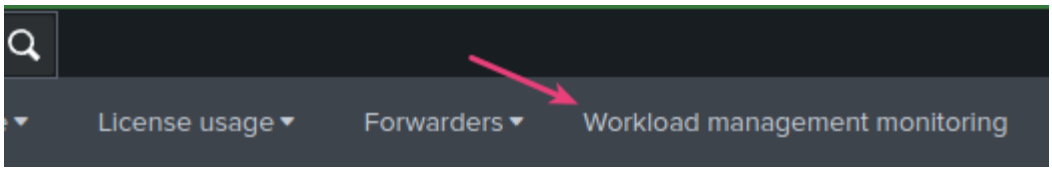
Exercise 7 – Explore Workload Management

Description

The CMC provides monitoring capabilities related to Splunk Workload Management via the “Workload management monitoring” dashboard.

Steps

1. Click on “**Workload management monitoring**”



Summary of All CMC Dashboards

This section contains a summary of the menu and dashboards available under each menu, with panels defined that appear on each dashboard. The highlighted panels are called out as useful in the Presentation and Lab Guide.

Overview

- Current active users (last hour)
- Average daily users (last 7 days)
- Search count (yesterday)
- Indexes with events (last 15 minutes)
- Total Indexes (last 15 minutes)
- Total Ingest volume (yesterday)
- Searches by type (last 24 hours)
- Throughput by Index (last 24 hours)
- Splunk TCP Closures (last 24 hours)
- Long running searches (last 24 hours)
- Scheduled search skipped (last hour)
- Data parsing Issues (last hour)

Health

Indicators:

- Universal forwarder software version
- Heavy forwarder software version
- Bucket size and range
- Skipped search percentage
- Cache transfer activity
- High memory searches

Maintenance

Maintenance window and change freeze

- Maintenance
- Change freeze
- (All, Upcoming, Past)

Alerts

- Triggered Alerts
- Configured Alerts

Indexing

Indexing performance

- Indexing throughput
- Historical data
    - Estimated indexing rate
    - Median queue fill ratio
    - Splunk TCP port closures
    - Indexers: blocked queues by queue type

Index detail

- Uncompressed Raw Data Size
- Total Bucket Count
- Total Event Count
- Earliest Event
- Latest Event
- Throughput: last 24 hours (GB)

HTTP Event Collector (HEC)

- HEC token usage (last 7 days)
- Requests - Events per second, Valid requests per second, Invalid requests per second
- Data - Data received (MB) per second, Data indexed (MB) per second
- Activity (last 30 minutes)
- HIstorical data
    - Request overview - Event count, Valid request count, Invalid request count
    - Data overview - MB Received, MB Indexed
    - Events and valid requests Count
    - Errors
    - Data received and indexed
    - Data delay

Data quality

- Event processing issues by source type

Search

Search usage statistics

- Overview - Searches finished, Successful Searches, Unsuccessful Searches, Total Search Runtime
- Searches - Number of searches over time
- Search activity by search type
- Cache activity (across all search heads)
- Search details (10000)

Scheduler activity

- Skip ratio (last hour)
- Average execution (last hour)
- Scheduler executions detail
- Scheduler executions
- Scheduled report completions
- Scheduler errors and warnings
- Median concurrency of completed scheduled searches
- Execution latency

Skipped scheduled activities

- Total skipped searches
- Scheduled search skip ratio
- Skipped scheduled searches detail
- Skipped searches
- Skipped searches by name and reason
- Scheduler errors and warnings

Expensive searches

- Maximum runtime searches
- Top 20 most memory consuming searches
- Top 20 most expensive ad hoc searches
- Top 20 most expensive scheduled searches
- Potentially inefficient searches

Usage

User activity

- Distinct users
- Distinct apps
- Total pageviews
- Pageviews - Top Apps, App access
- Activity by page

User detail

By user:

- Name
- Username
- Roles assigned to <Username>
- User logins
- Search count
- Average search runtime
- Total search time
- Searches by type
- Pageviews by app
- User search detail

License usage

Entitlements

- Ingest license entitlement
- Searchable storage (DDAS) entitlement
- Archive storage (DDAA) entitlement

Ingest

- License entitlement
- Daily license usage summary

Workload

- License entitlement
- SVC usage
- SVC consumers
- Search seconds by search type
- Search seconds by top 10 apps
- SVC usage by ingestion
- Data ingestion
- Dispatched and skipped search count

Storage Summary

- Searchable storage (DDAS) entitlement (last 25 hours)
- Searchable storage (DDAS) usage (last 25 hours)
- Searchable storage (DDAS) usage percentage (last 25 hours)
- Archive storage (DDAA) entitlement (last 25 hours)
- Archive storage (DDAA) usage (last 25 hours)
- Archive storage (DDAA) usage percent (last 25 hours)

- Restored entitlement
- Restored searchable storage (DDAS) usage
- Restored searchable storage (DDAS) usage percent
- Index details

Searchable storage (DDAS)

- Searchable storage entitlement (last 25 hours)
- Searchable storage usage (last 25 hours)
- Searchable storage usage percent (last 25 hours)
- Restored entitlement
- Restored searchable storage (DDAS) usage
- Resoted searchable storage (DDAS) usage percent
- Searchable storage usage against entitlement
- Searchable storage usage by top 10 indexes
- Searchable storage index details
- Splunk internal index details

Archive storage (DDAA)

- Archive storage entitlement (last 25 hours)
- Archive storage usage (last 25 hours)
- Archive storage usage percent (last 25 hours)
- Archive storage usage against entitlement
- Archive storage usage by top 10 indexes
- Data archive restoration summary
- Index storage usage details

Federated Search for Amazon S3

- Total data scan entitlement
- Data scan entitlement usage
- Percentage of data scan entitlement usage

Forwarders

Forwarders:instance

- Status and Configuration
- Outgoing Data Rate

Forwarders:deployment

- Forwarders by Status
- Status and Configuration
- Historical:Total Count of Forwarders and Receivers
- Forwarder Connection Count Over Time

Forwarder versions

- Version summary
- Current Splunk Cloud Platform version
- Upgrade Recommendations

Workload management monitoring

- Searches filtered
- Searches aborted
- Searches reclassified
- Searches triggering an alert

Links

Introduction to the Cloud Monitoring Console	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIntro
Use the Overview dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringOverview
Use the Health dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringHealth
Use the Maintenance dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringComms
Use the Alerts dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringAlerts
Use the Indexing dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIndexing
Check indexing performance	Use the Indexing dashboards - Splunk Documentation
Check index detail	Use the Indexing dashboards - Splunk Documentation
Verify data quality	Use the Indexing dashboards - Splunk Documentation
Check the status of HTTP event collection	Use the Indexing dashboards - Splunk Documentation
Use the Search dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringSearch
Use the Usage dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringUsage
Use the License Usage dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage
Use the Workload (preview) dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/Workload
Use the Forwarder dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringForwarders
Use the Workload Management Monitoring dashboard	https://docs.splunk.com/Documentation/SplunkCloud/9.2.2403/Admin/MonitoringWrkldMgmt
How is SVC Utilization Measured	What is Splunk Virtual Compute (SVC)?
Optimzing Search	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Searching_and_Reporting/Optimizing_search
Write better searches	https://docs.splunk.com/Documentation/Splunk/latest/Search/Writebettersearches
Remediate long-running searches	https://community.splunk.com/t5/Knowledge-Management/help-optimise-a-long-running-search/m-p/551040
Search Optimization	https://docs.splunk.com/Documentation/Splunk/latest/Search/Built-inoptimization
Search Head Clustering	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCarchitecture
Communities: Skipped Searches	https://community.splunk.com/t5/Splunk-Search/Skipped-Searches/m-p/

	563180
Reducing skipped searches	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Searching_and_Reporting/Reducing_skipped_searches
Communities: Skipped Saved Searches	https://community.splunk.com/t5/Reporting/Skipped-Saved-Searches/td-p/55288
Are You Skipping? Please Read!	https://www.splunk.com/en_us/blog/tips-and-tricks/are-you-skipping-please-read.html
About search optimization	https://docs.splunk.com/Documentation/Splunk/latest/Search/Aboutoptimization
Identify and triage indexing performance problems	https://docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/Troubleshootindexingperformance
Clone and manage dashboards	https://docs.splunk.com/Documentation/Splunk/latest/Viz/DashboardCloneHome
Splunk Supported Versions: Core and Forwarder	https://www.splunk.com/en_us/legal/splunk-software-support-policy.html#:~:text=in%20English%20only.-,Core,-Splunk%20Enterprise%20/%20Splunk