Splunk4Admins

Cloud Monitoring Console

<Customer Name>

splunk>
a CISCO company

Forward-looking statements

This presentation may be deemed to contain forward-looking statements, which are subject to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995. Any statements that are not statements of historical fact (including statements containing the words “will,” “believes,” “plans,” “anticipates,” “expects,” “estimates,” “strives,” “goal,” “intends,” “may,” “endeavors,” “continues,” “projects,” “seeks,” or “targets,” or the negative of these terms or other comparable terminology, as well as similar expressions) should be considered to be forward-looking statements, although not all forward-looking statements contain these identifying words. Readers should not place undue reliance on these forward-looking statements, as these statements are management’s beliefs and assumptions, many of which, by their nature, are inherently uncertain, and outside of management’s control. Forward-looking statements may include statements regarding the expected benefits to Cisco, Splunk and their respective customers from the completed transaction, the integration of Splunk’s and Cisco’s complementary capabilities and products to create an end-to-end platform designed to unlock greater digital resilience for customers, our expectations regarding greater resiliency and better product outcomes, including for security and observability, plans for future investment, our development and use of AI and the role that our innovation plays as our customers adopt AI. Statements regarding future events are based on Cisco’s current expectations, estimates, and projections and are necessarily subject to associated risks related to, among other things, (i) the ability of Cisco to successfully integrate Splunk’s market opportunities, technology, personnel and operations and to achieve expected benefits, (ii) Cisco’s ability to implement its plans, forecasts and other expectations with respect to Splunk’s business and realize expected synergies, (iii) the outcome of any legal proceedings related to the transaction, (iv) the effects on the accounting relating to the acquisition of Splunk, (v) legislative, regulatory, and economic developments, (vi) general economic conditions, and (vii) the retention of key personnel. Therefore, actual results may differ materially and adversely from the anticipated results or outcomes indicated in any forward-looking statements. For information regarding other related risks, see 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 reports on Form 10-Q filed with the SEC on February 20, 2024 and November 21, 2023, respectively. The parties undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about 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. We undertake no 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.

REGISTRATION 5 MINS

Enroll in Today’s Workshop

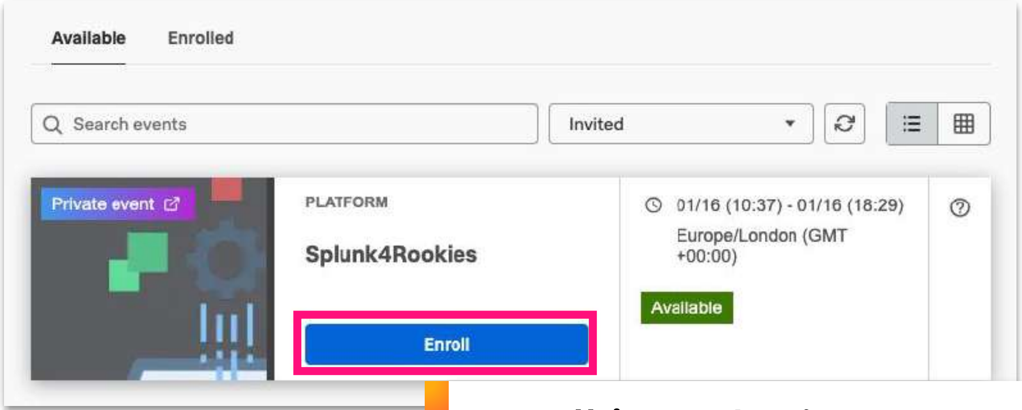
Tasks

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-CMC-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-CMC-Attendee

Goal



Enroll in today’s event

Please introduce yourself!

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

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Dashboard Modification
- Summary

Audience

Who is this Workshop for?

- Those who are interested in how to observe and detect issues within Splunk …
  - Splunk Admins
  - “Required”: Power User Certified
  - “Preferred”: Splunk Admin enabled (at least started …), Certified

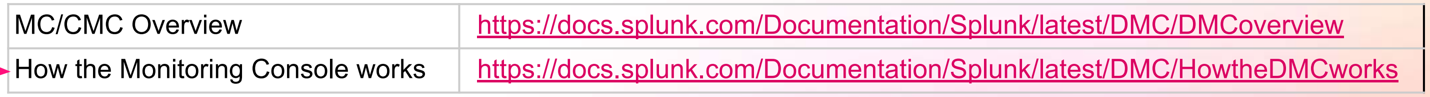
Expectations for Workshop

Hereinafter “CMC” …

- Last roughly 60 - 75 minutes
- Effectively a short survey of what is available in the CMC
- Experience setup and configuration of CMC (forwarders)
- Understand the dashboards in CMC
    - Indexing
    - Search
    - Usage
    - Forwarders
- Understand how to use CMC to adhere more closely to Best Practices
- Discover issues with CMC

What is the CMC?

- CMC - Splunk Cloud
  - Set of dashboards providing information about customer-influenceable resources - more limited than the MC for OnPremise Enterprise
- MC - Enterprise, customer-managed cloud
  - Set of dashboards providing information about OnPremise resources
- Understanding what the CMC has available can help Admins diagnose and remediate more quickly
- Integrated on customer search head as an App



MC/CMC Overview	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
How the Monitoring Console works	https://docs.splunk.com/Documentation/Splunk/latest/DMC/HowtheDMCworks

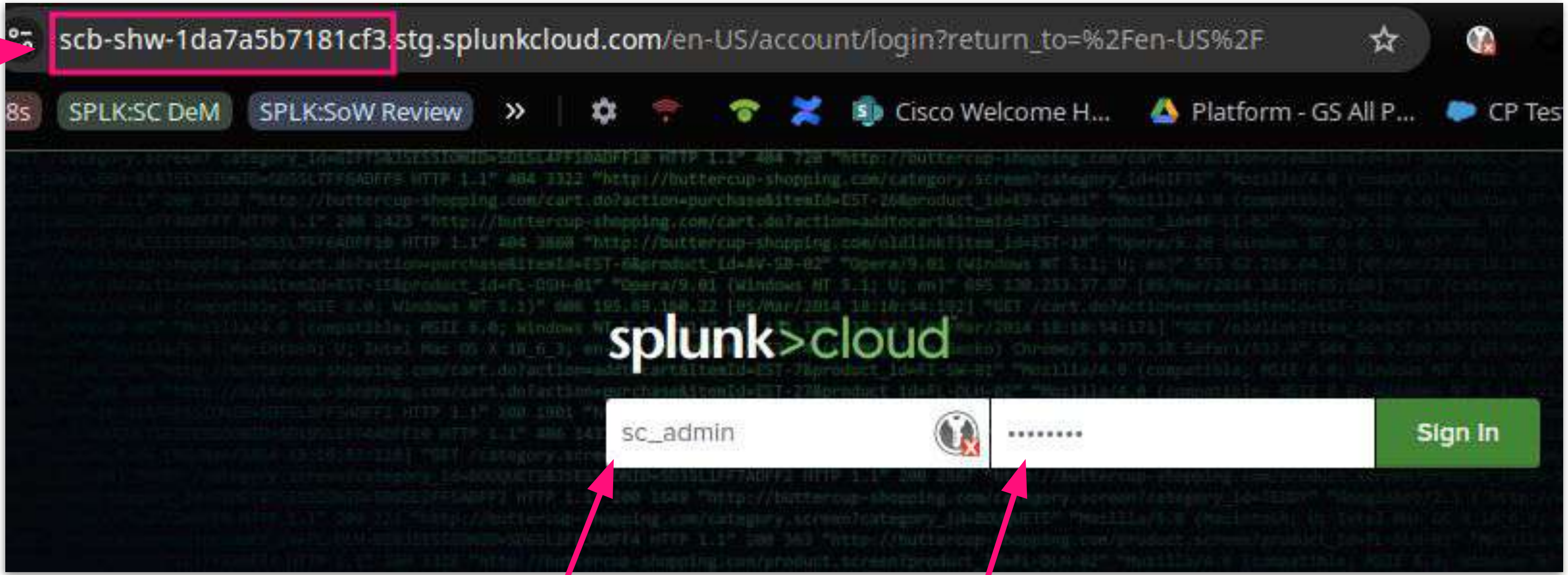
Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is a Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Dashboard Modification
- Summary

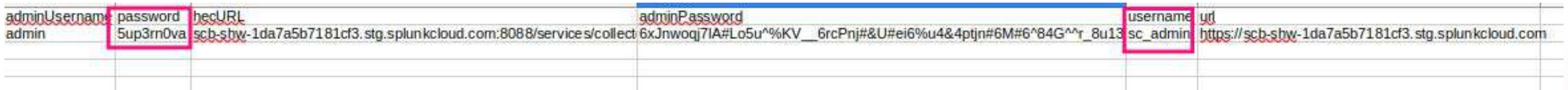
Explore Dashboards

Get to Cloud Monitoring Console

Each attendee instance is in the workbook provided with the username and password indicated.
This is an example …
and login with “sc_admin” and “5up3rn0va”



scb-shw-1da7a5b7181cf3.stg.splunkcloud.com/en-US/account/login?return_to=%2Fen-US%2F



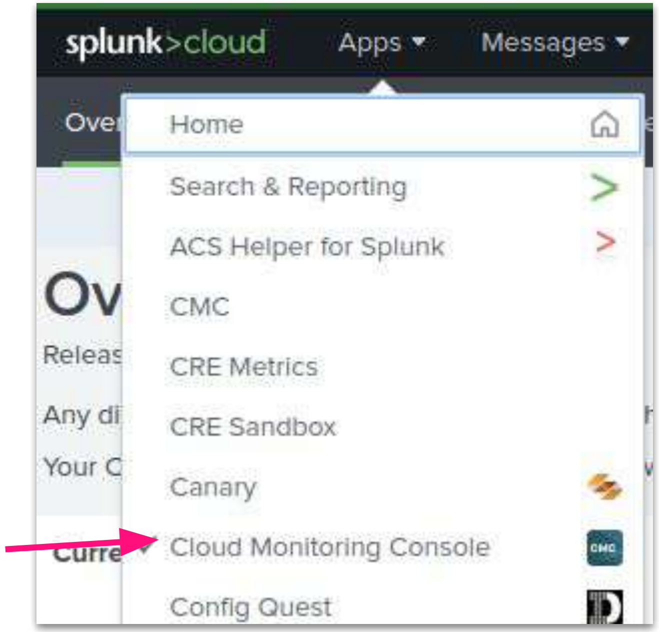
adminUsernam	password	hecURL	adminPassword	username	url
admin	5up3rn0va	scb-shw-1da7a5b7181cf3.stg.splunkcloud.com:8088/services/collect	6xJnwoqj7IA#Lo5u^%KV__6rcPnj#&U#ei6%u4&4ptjn#6M#6^84G^^r_8u13	sc_admin	https://scb-shw-1da7a5b7181cf3.stg.splunkcloud.com

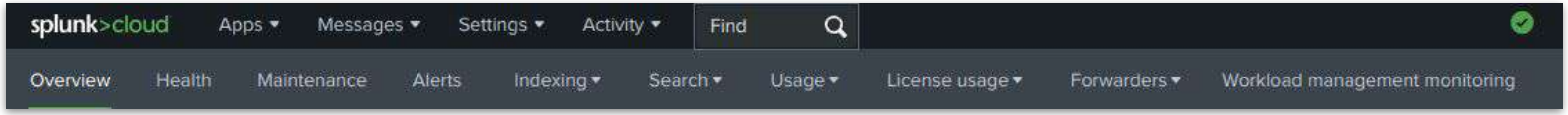
Introduction to the Cloud Monitoring Console	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIntro

Explore Dashboards

Lab1

Get to Cloud Monitoring Console



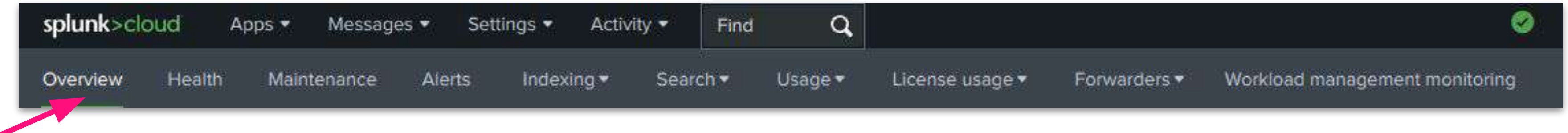


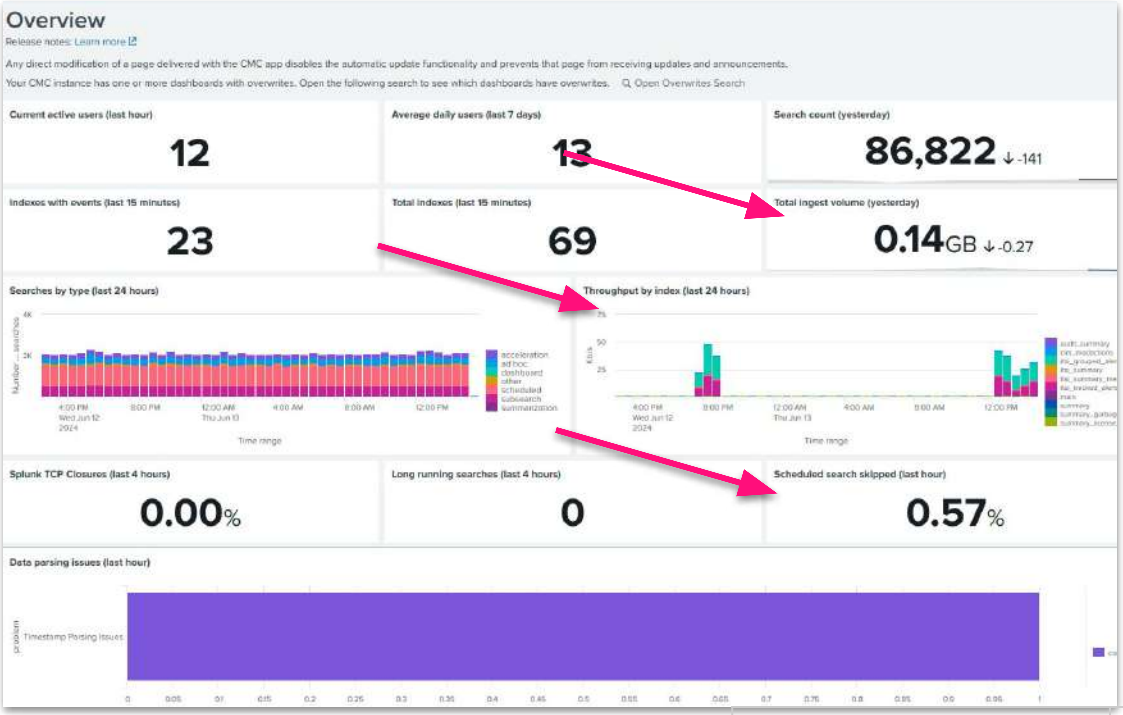
Introduction to the Cloud Monitoring Console	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIntro

Explore Dashboards

Lab1

Overview





Overview

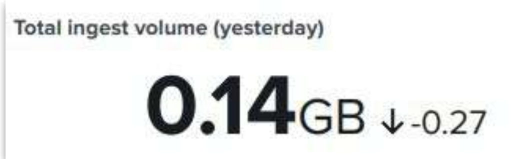
Release notes: Learn more

Any direct modification of a page delivered with the CMC app disables the automatic update functionality and prevents that page from receiving updates and announcements.

Your CMC instance has one or more dashboards with overwrites. Open the following search to see which dashboards have overwrites. Open Overwrites Search

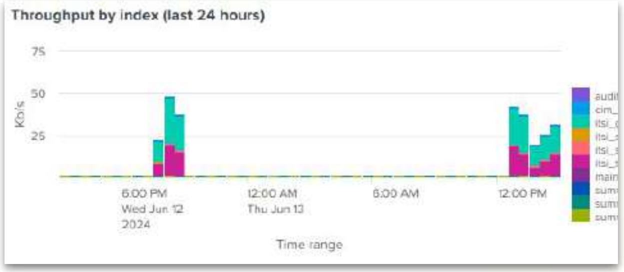
Current active users (last hour) 12	Average daily users (last 7 days) 13	Search count (yesterday) 86,822 ↓ -141
Indexes with events (last 15 minutes) 23	Total indexes (last 15 minutes) 69	Total ingest volume (yesterday) 0.14GB ↓ -0.27
Splunk TCP Closures (last 4 hours) 0.00%	Long running searches (last 4 hours) 0	Scheduled search skipped (last hour) 0.57%

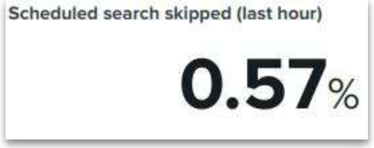
Searches by type (last 24 hours)
Throughput by index (last 24 hours)
Time range
Data parsing issues (last hour)
Timestamp Parsing Issues



Total ingest volume (yesterday)

0.14GB ↓ -0.27





Scheduled search skipped (last hour)

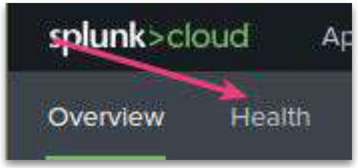
0.57%

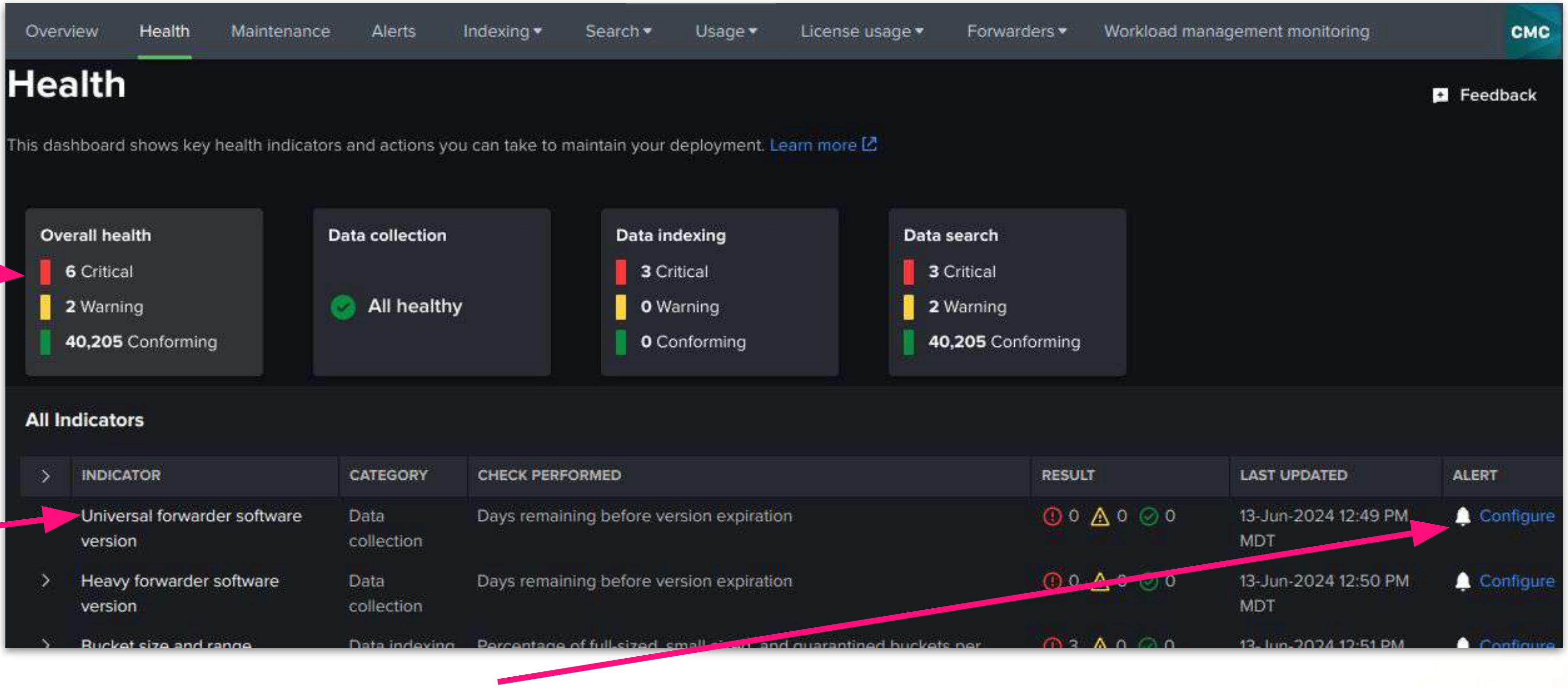
Use the Overview dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringOverview

Explore Dashboards

Lab1

Health





Health

This dashboard shows key health indicators and actions you can take to maintain your deployment. Learn more

Overall health	Data collection	Data indexing	Data search
🟥 6 Critical 🟨 2 Warning 🟩 40,205 Conforming	✓ All healthy	🟥 3 Critical 🟨 0 Warning 🟩 0 Conforming	🟥 3 Critical 🟨 2 Warning 🟩 40,205 Conforming

All Indicators

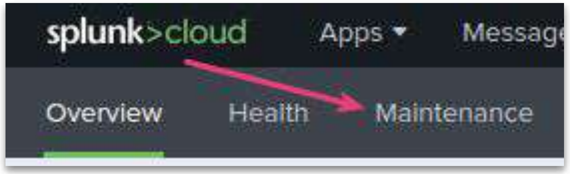
>	INDICATOR	CATEGORY	CHECK PERFORMED	RESULT	LAST UPDATED	ALERT
	Universal forwarder software version	Data collection	Days remaining before version expiration	ⓘ 0 ⚠ 0 ✓ 0	13-Jun-2024 12:49 PM MDT	Configure
>	Heavy forwarder software version	Data collection	Days remaining before version expiration	ⓘ 0 ⚠ 0 ✓ 0	13-Jun-2024 12:50 PM MDT	Configure
>	Bucket size and range	Data indexing	Percentage of full-sized, small-sized, and quarantined buckets per	ⓘ 3 ⚠ 0 ✓ 0	13-Jun-2024 12:51 PM	Configure

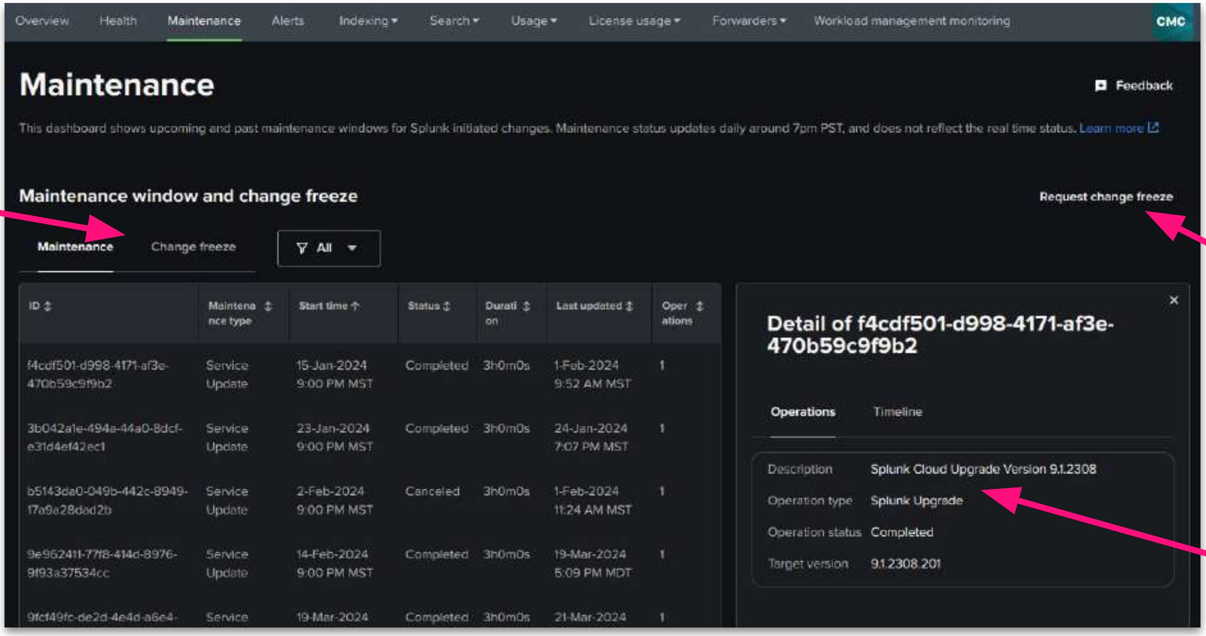
Use the Health dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringHealth

Explore Dashboards

Lab1

Maintenance





Maintenance

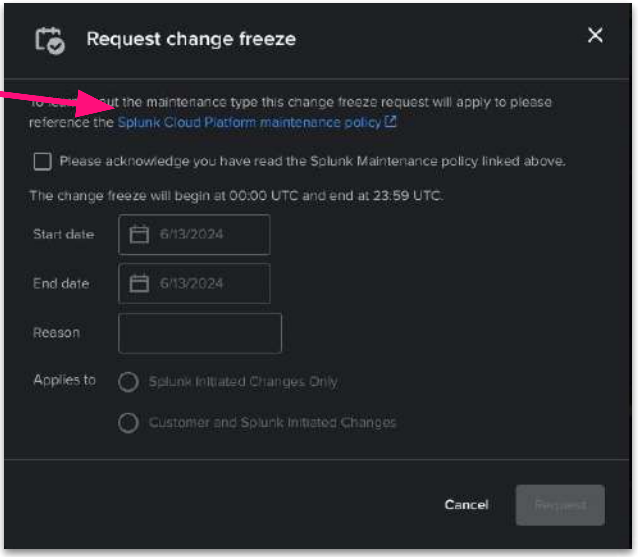
This dashboard shows upcoming and past maintenance windows for Splunk initiated changes. Maintenance status updates daily around 7pm PST, and does not reflect the real time status. Learn more

Maintenance window and change freeze

ID	Maintenance type	Start time	Status	Duration	Last updated	Operations
f4cdf501-d998-4171-af3e-470b59c9f9b2	Service Update	15-Jan-2024 9:00 PM MST	Completed	3h0m0s	1-Feb-2024 9:52 AM MST	1
3b042a1e-494a-44a0-8dcf-e31d4ef42ec1	Service Update	23-Jan-2024 9:00 PM MST	Completed	3h0m0s	24-Jan-2024 7:07 PM MST	1
b5143da0-049b-442c-8949-17a9a28dad2b	Service Update	2-Feb-2024 9:00 PM MST	Canceled	3h0m0s	1-Feb-2024 11:24 AM MST	1
9e962411-77f8-414d-8976-9f93a37534cc	Service Update	14-Feb-2024 9:00 PM MST	Completed	3h0m0s	19-Mar-2024 5:09 PM MDT	1
9fcf49fc-de2d-4e4d-a6e4-	Service	19-Mar-2024	Completed	3h0m0s	21-Mar-2024	1

Detail of f4cdf501-d998-4171-af3e-470b59c9f9b2

Description	Splunk Cloud Upgrade Version 9.1.2308
Operation type	Splunk Upgrade
Operation status	Completed
Target version	9.1.2308.201



Request change freeze

To learn about the maintenance type this change freeze request will apply to please reference the Splunk Cloud Platform maintenance policy

□ Please acknowledge you have read the Splunk Maintenance policy linked above.

The change freeze will begin at 00:00 UTC and end at 23:59 UTC.

Start date: 6/13/2024

End date: 6/13/2024

Reason:

Applies to: ○ Splunk Initiated Changes Only ○ Customer and Splunk Initiated Changes

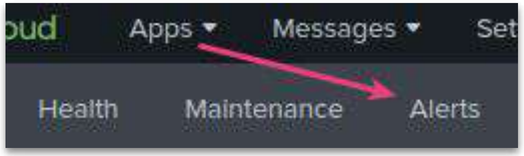
Button “Request change freeze”

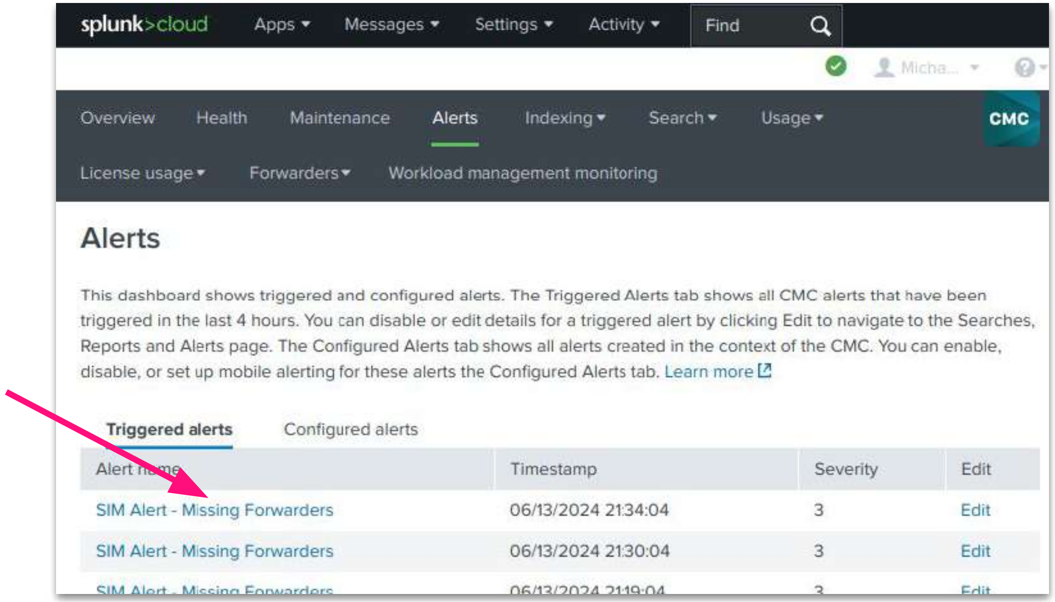
Use the Maintenance dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringComms

Explore Dashboards

Lab1

Alerts



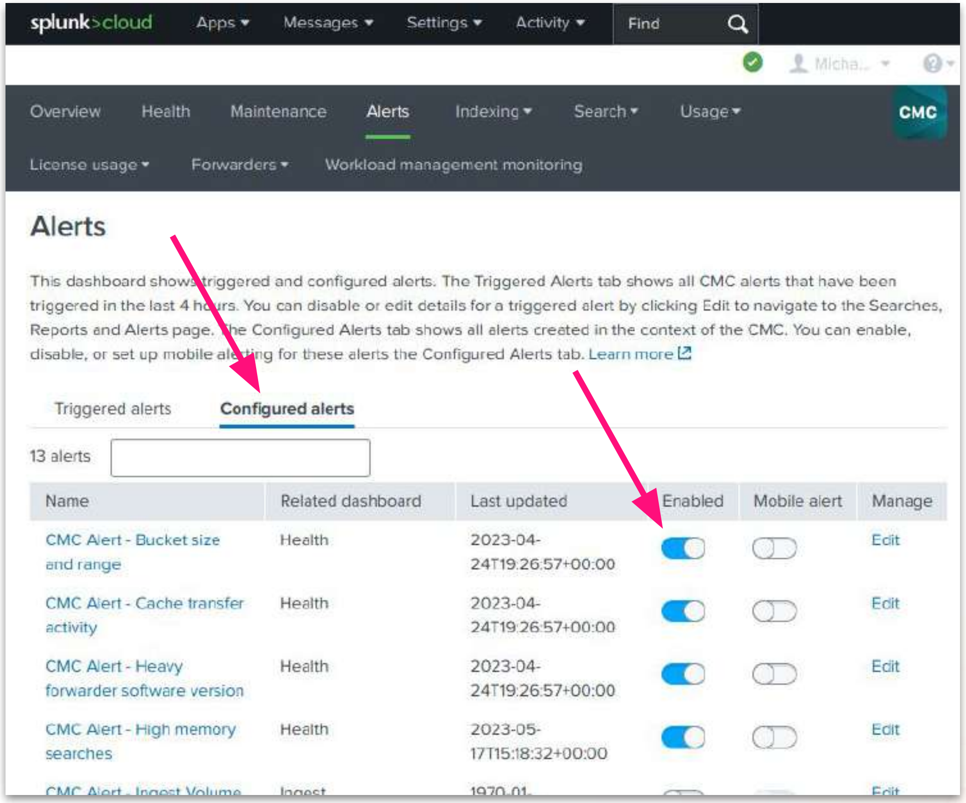


Alerts

This dashboard shows triggered and configured alerts. The Triggered Alerts tab shows all CMC alerts that have been triggered in the last 4 hours. You can disable or edit details for a triggered alert by clicking Edit to navigate to the Searches, Reports and Alerts page. The Configured Alerts tab shows all alerts created in the context of the CMC. You can enable, disable, or set up mobile alerting for these alerts the Configured Alerts tab. Learn more

Triggered alerts | Configured alerts

Alert name	Timestamp	Severity	Edit
SIM Alert - Missing Forwarders	06/13/2024 21:34:04	3	Edit
SIM Alert - Missing Forwarders	06/13/2024 21:30:04	3	Edit
SIM Alert - Missing Forwarders	06/13/2024 21:19:04	3	Edit



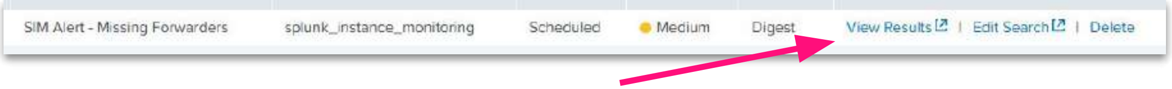
Alerts

This dashboard shows triggered and configured alerts. The Triggered Alerts tab shows all CMC alerts that have been triggered in the last 4 hours. You can disable or edit details for a triggered alert by clicking Edit to navigate to the Searches, Reports and Alerts page. The Configured Alerts tab shows all alerts created in the context of the CMC. You can enable, disable, or set up mobile alerting for these alerts the Configured Alerts tab. Learn more

Triggered alerts | **Configured alerts**

13 alerts

Name	Related dashboard	Last updated	Enabled	Mobile alert	Manage
CMC Alert - Bucket size and range	Health	2023-04-24T19:26:57+00:00	●	○	Edit
CMC Alert - Cache transfer activity	Health	2023-04-24T19:26:57+00:00	●	○	Edit
CMC Alert - Heavy forwarder software version	Health	2023-04-24T19:26:57+00:00	●	○	Edit
CMC Alert - High memory searches	Health	2023-05-17T15:18:32+00:00	●	○	Edit
CMC Alert - Ingest Volume	Ingest	1970-01-			Edit



SIM Alert - Missing Forwarders	splunk_instance_monitoring	Scheduled	● Medium	Digest	View Results | Edit Search | Delete

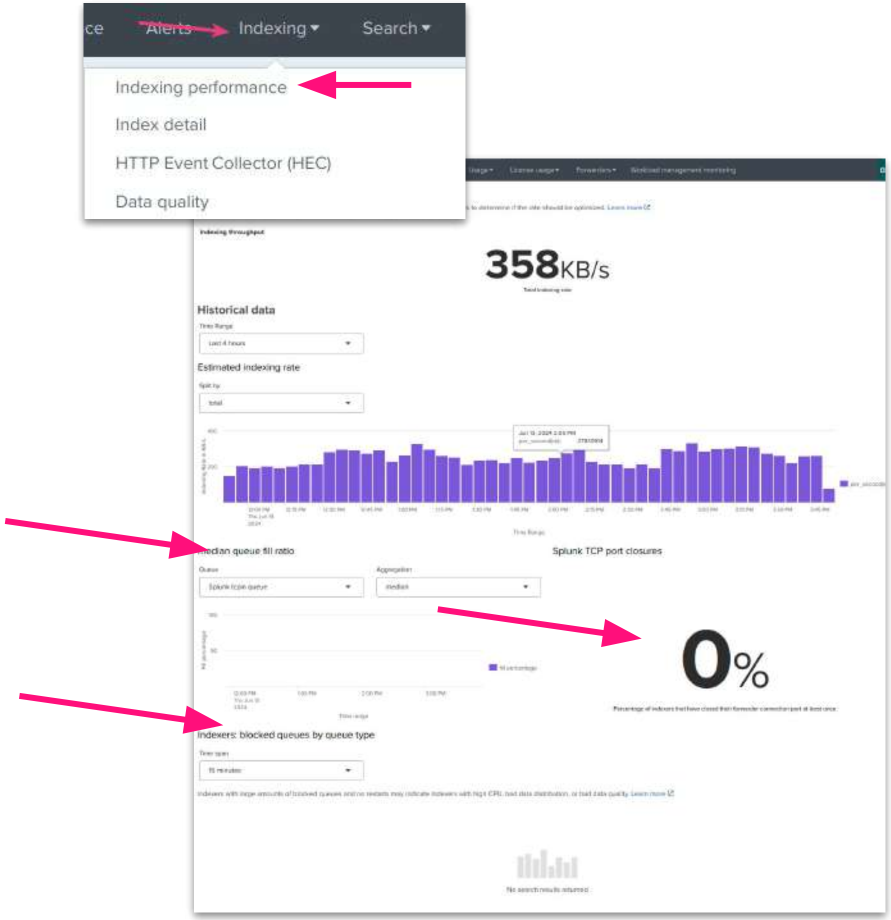
Use the Alerts dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringAlerts

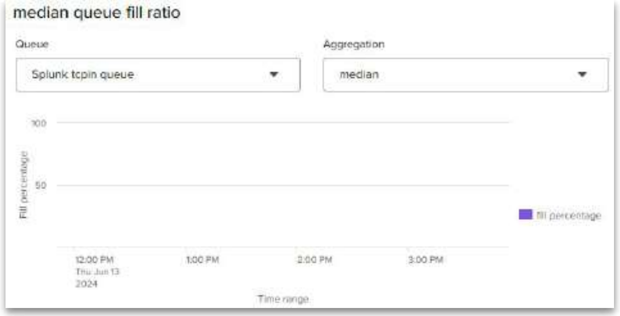
Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Dashboard Modification
- Summary

Explore Dashboards

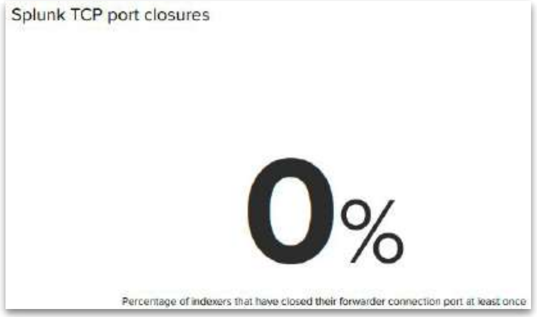
Indexing - Indexing performance



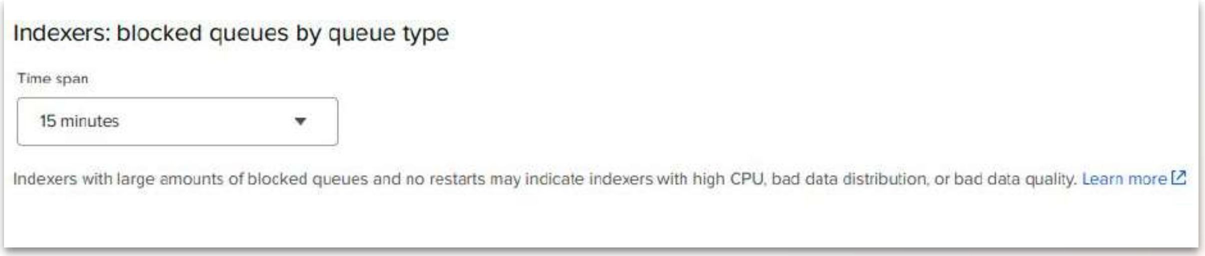


Queue: Splunk tcpin queue

Aggregation: median



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



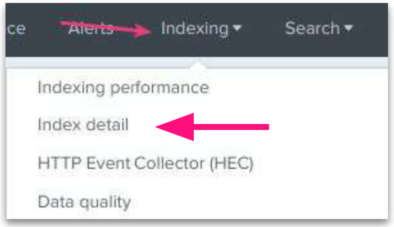
Time span: 15 minutes

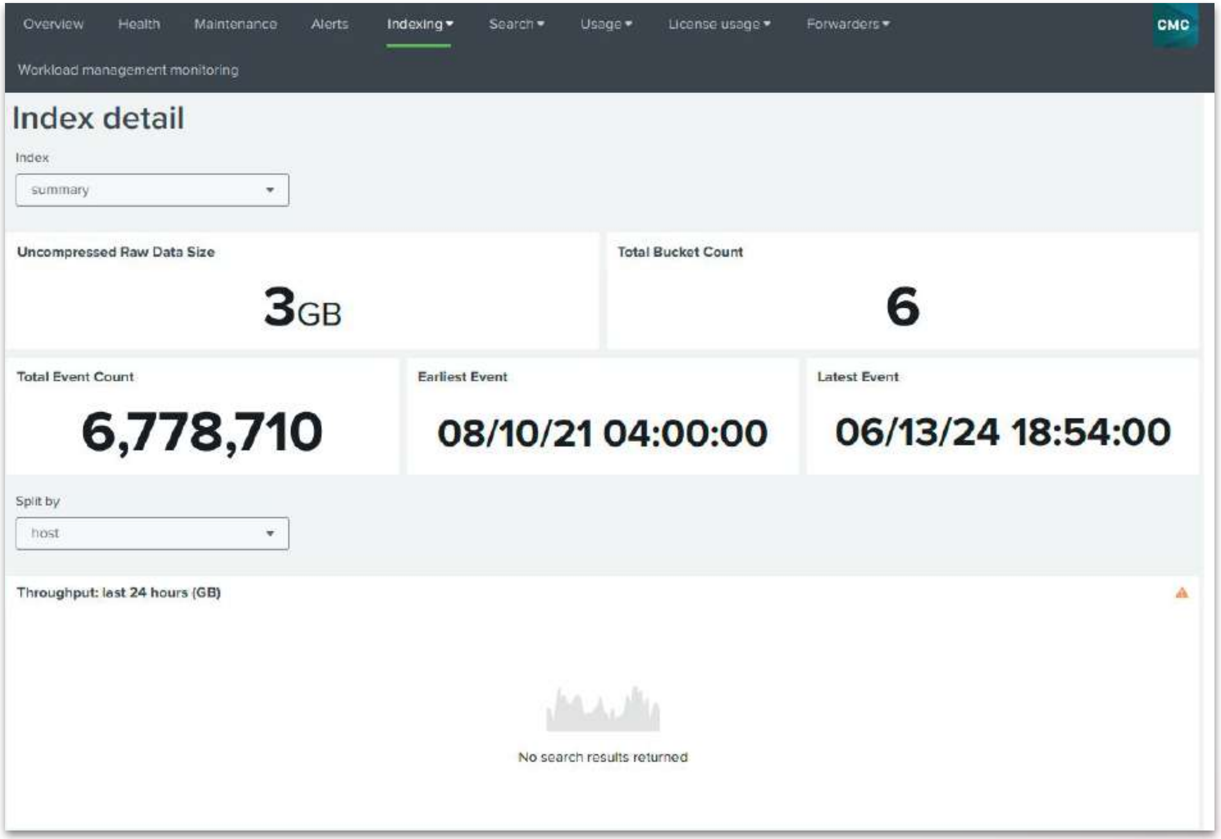
Indexers with large amounts of blocked queues and no restarts may indicate indexers with high CPU, bad data distribution, or bad data quality. Learn more

Use the Indexing dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIndexing

Explore Dashboards

Indexing - Index detail





Index detail

Index: summary

Uncompressed Raw Data Size: 3GB

Total Bucket Count: 6

Total Event Count: 6,778,710

Earliest Event: 08/10/21 04:00:00

Latest Event: 06/13/24 18:54:00

Split by: host

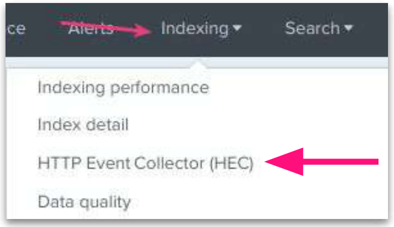
Throughput: last 24 hours (GB)

No search results returned

Use the Indexing dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIndexing

Explore Dashboards

Indexing - HTTP Event Collector (HEC)

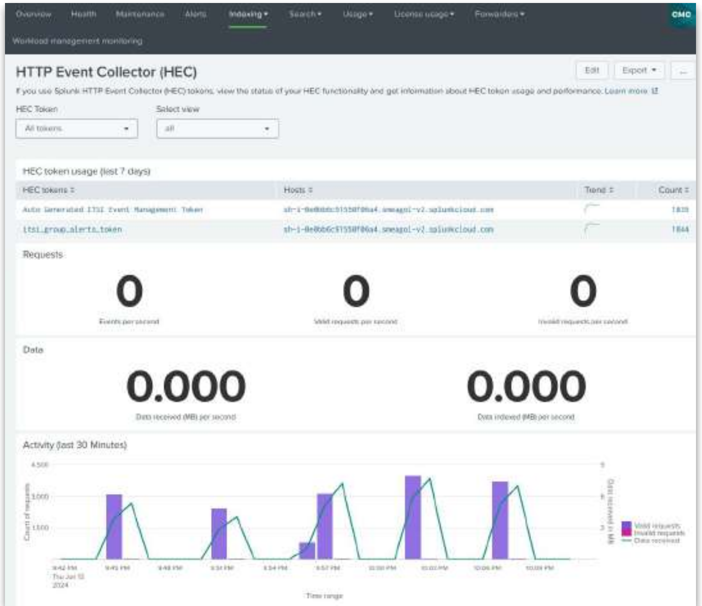


Indexing performance

Index detail

HTTP Event Collector (HEC)

Data quality



HTTP Event Collector (HEC)

If you use Splunk HTTP Event Collector (HEC) tokens, view the status of your HEC functionality and get information about HEC token usage and performance. Learn more

HEC Token: All tokens

Select view: all

HEC token usage (last 7 days)

HEC tokens	Hosts	Trend	Count
Auto Generated ITSI Event Management Token	sh-i-0e0bb6c91550f06a4.smeagol-v2.splunkcloud.com		1839
itsi_group_alerts_token	sh-i-0e0bb6c91550f06a4.smeagol-v2.splunkcloud.com		1844

Requests

0 Events per second

0 Valid requests per second

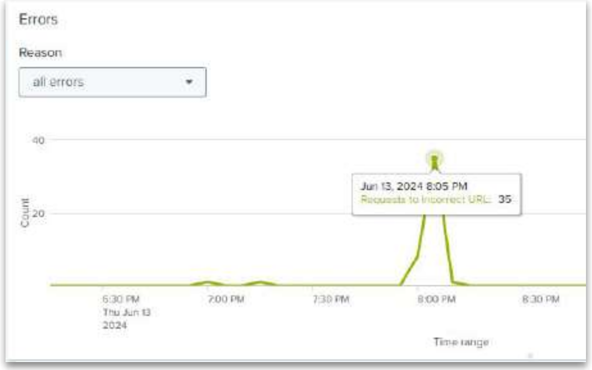
0 Invalid requests per second

Data

0.000 Data received (MB) per second

0.000 Data indexed (MB) per second

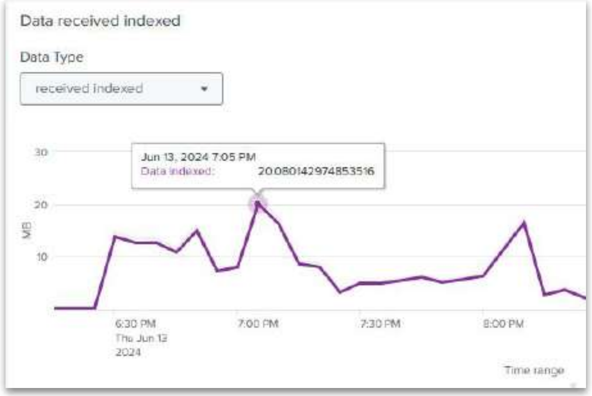
Activity (last 30 Minutes)



Errors

Reason: all errors

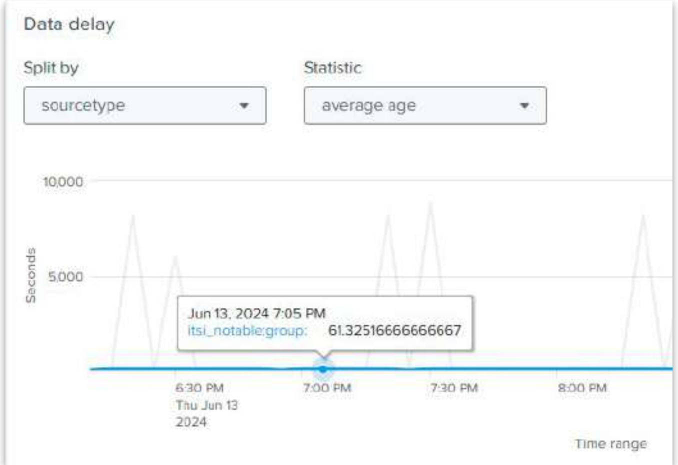
Jun 13, 2024 8:05 PM
Requests to Incorrect URL: 35



Data received indexed

Data Type: received indexed

Jun 13, 2024 7:05 PM
Data indexed: 20.080142974853516



Data delay

Split by: sourcetype

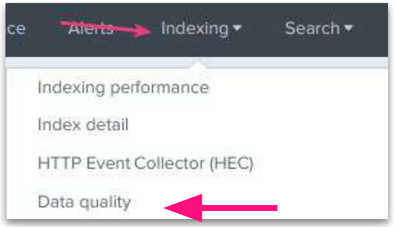
Statistic: average age

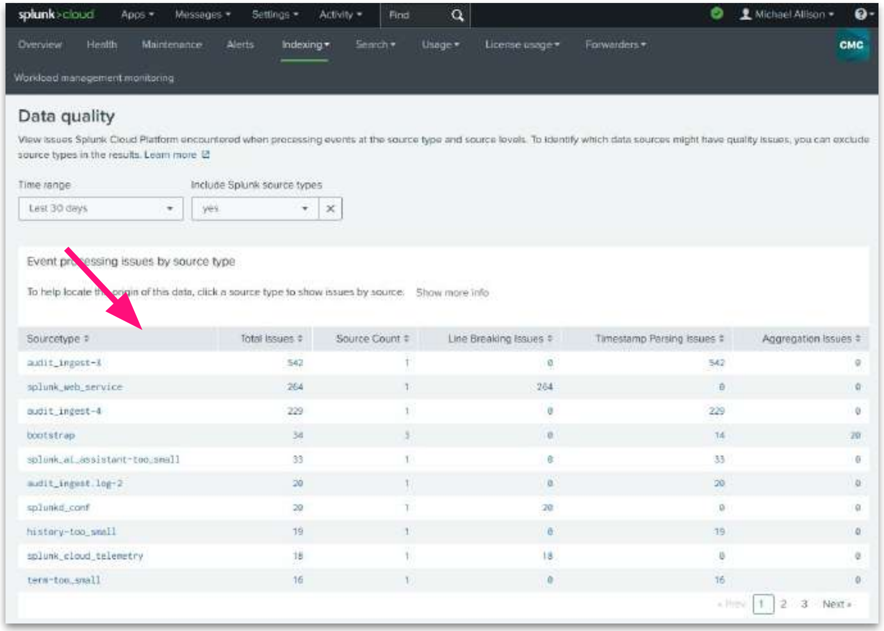
Jun 13, 2024 7:05 PM
itsi_notable:group: 61.32516666666667

Use the Indexing dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIndexing

Explore Dashboards

Indexing - Data quality





Data quality

View issues Splunk Cloud Platform encountered when processing events at the source type and source levels. To identify which data sources might have quality issues, you can exclude source types in the results. Learn more

Time range: Last 30 days

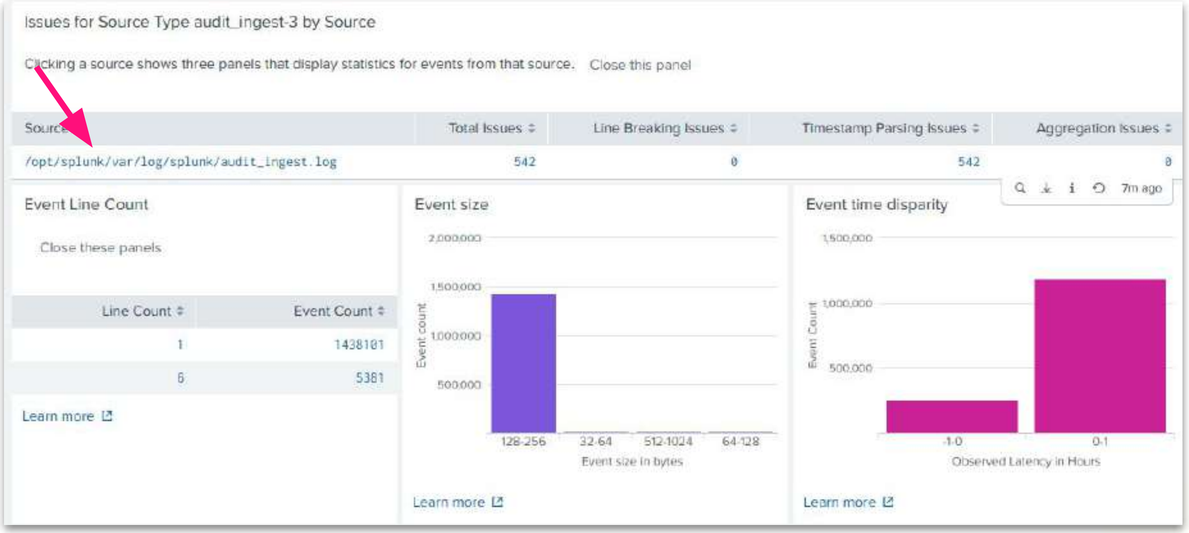
Include Splunk source types: yes

Event processing issues by source type

To help locate the origin of this data, click a source type to show issues by source. Show more info

Sourcetype	Total Issues	Source Count	Line Breaking Issues	Timestamp Parsing Issues	Aggregation Issues
audit_ingest-3	542	1	0	542	0
splunk_web_service	264	1	264	0	0
audit_ingest-4	229	1	0	229	0
bootstrap	34	3	0	14	20
splunk_ai_assistant-too_small	33	1	0	33	0
audit_ingest.log-2	20	1	0	20	0
splunkd_conf	20	1	20	0	0
history-too_small	19	1	0	19	0
splunk_cloud_telemetry	18	1	18	0	0
term-too_small	16	1	0	16	0

« Prev 1 2 3 Next »



Issues for Source Type audit_ingest-3 by Source

Clicking a source shows three panels that display statistics for events from that source. Close this panel

Source	Total Issues	Line Breaking Issues	Timestamp Parsing Issues	Aggregation Issues
/opt/splunk/var/log/splunk/audit_ingest.log	542	0	542	0

Event Line Count

Close these panels

Line Count	Event Count
1	1438101
6	5381

Learn more

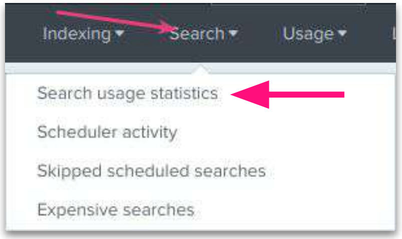
Use the Indexing dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringIndexing

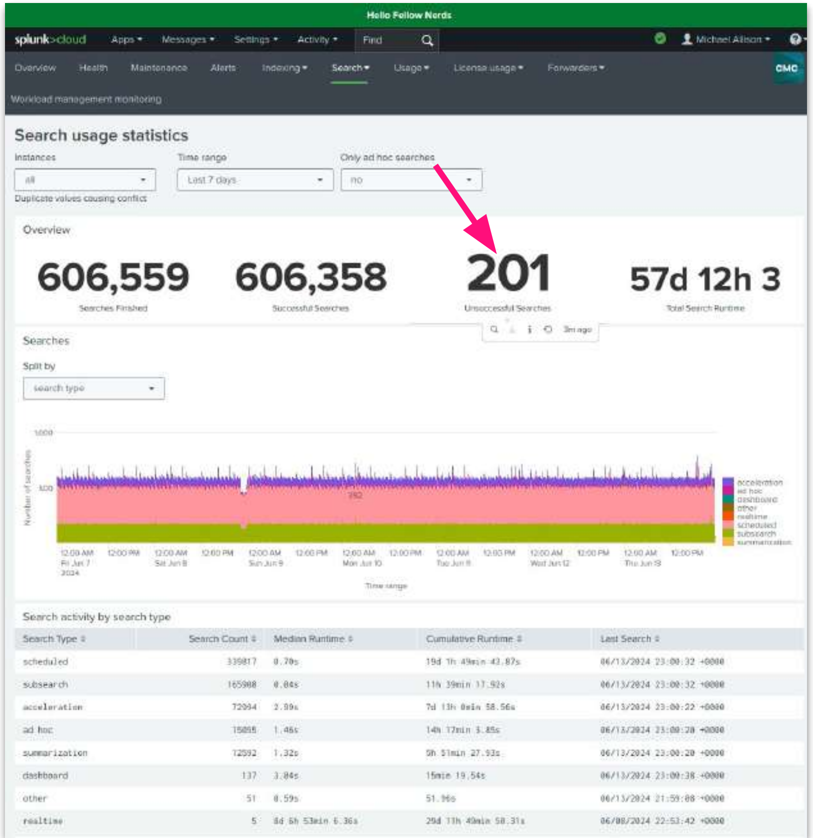
Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Dashboard Modification
- Summary

Explore Dashboards

Search - Search usage statistics





Search usage statistics

Instances: all
Duplicate values causing conflict

Time range: Last 7 days

Only ad hoc searches: no

Overview

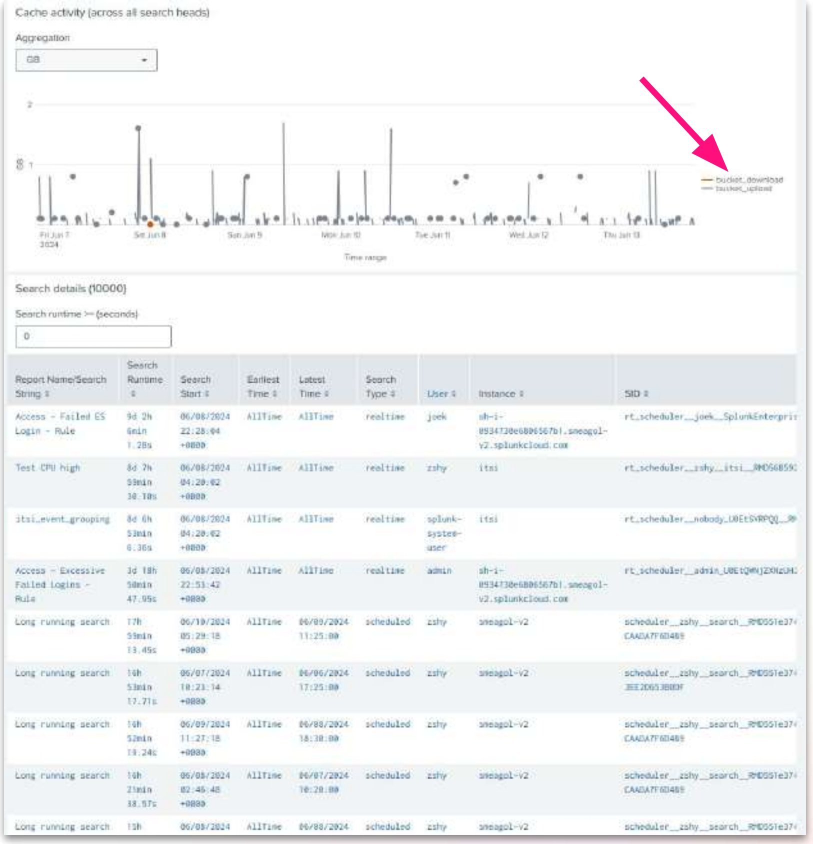
606,559	606,358	201	57d 12h 3
Searches Finished	Successful Searches	Unsuccessful Searches	Total Search Runtime

Searches

Split by: search type

Search activity by search type

Search Type	Search Count	Median Runtime	Cumulative Runtime	Last Search
scheduled	339817	0.70s	19d 1h 49min 43.87s	06/13/2024 23:00:32 +0000
subsearch	165908	0.04s	11h 39min 17.92s	06/13/2024 23:00:32 +0000
acceleration	72094	2.99s	7d 13h 0min 58.56s	06/13/2024 23:00:22 +0000
ad hoc	15095	1.46s	14h 17min 3.85s	06/13/2024 23:00:20 +0000
summarization	12592	1.32s	5h 51min 27.93s	06/13/2024 23:00:20 +0000
dashboard	137	3.04s	15min 19.54s	06/13/2024 23:00:38 +0000
other	51	0.59s	51.96s	06/13/2024 21:59:08 +0000
realtime	5	8d 6h 53min 6.36s	29d 11h 49min 50.31s	06/08/2024 22:53:42 +0000



Cache activity (across all search heads)

Aggregation: GB

Search details (10000)

Search runtime >= (seconds): 0

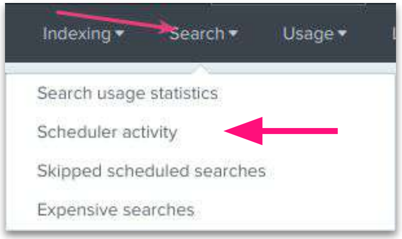
Report Name/Search String	Search Runtime	Search Start	Earliest Time	Latest Time	Search Type	User	Instance	SID
Access - Failed ES Login - Rule	9d 2h 6min 1.28s	06/08/2024 22:28:04 +0000	AllTime	AllTime	realtime	joek	sh-i-0934730e6806567b1.smeagol-v2.splunkcloud.com	rt_scheduler__joek__SplunkEnterpri
Test CPU high	8d 7h 59min 30.10s	06/08/2024 04:20:02 +0000	AllTime	AllTime	realtime	zshy	itsi	rt_scheduler__zshy__itsi__RMD56859
itsi_event_grouping	8d 6h 53min 6.36s	06/08/2024 04:20:02 +0000	AllTime	AllTime	realtime	splunk-system-user	itsi	rt_scheduler__nobody_U0EtSVRPQQ__R
Access - Excessive Failed Logins - Rule	3d 18h 50min 47.95s	06/08/2024 22:51:42 +0000	AllTime	AllTime	realtime	admin	sh-i-0934730e6806567b1.smeagol-v2.splunkcloud.com	rt_scheduler__admin_U0EtQWNjZXNzUH
Long running search	17h 59min 13.45s	06/10/2024 05:29:18 +0000	AllTime	06/09/2024 11:25:00	scheduled	zshy	smeagol-v2	scheduler__zshy__search__RMD5Te37 CAADA7F6D489
Long running search	16h 53min 17.71s	06/07/2024 10:21:14 +0000	AllTime	06/06/2024 17:25:00	scheduled	zshy	smeagol-v2	scheduler__zshy__search__RMD5Te37 3EE2D653B0DF
Long running search	16h 52min 19.24s	06/09/2024 11:27:18 +0000	AllTime	06/08/2024 18:30:00	scheduled	zshy	smeagol-v2	scheduler__zshy__search__RMD5Te37 CAADA7F6D489
Long running search	16h 21min 38.57s	06/08/2024 02:46:48 +0000	AllTime	06/07/2024 10:20:00	scheduled	zshy	smeagol-v2	scheduler__zshy__search__RMD5Te37 CAADA7F6D489
Long running search	13h	06/08/2024	AllTime	06/08/2024	scheduled	zshy	smeagol-v2	scheduler__zshy__search__RMD5Te37

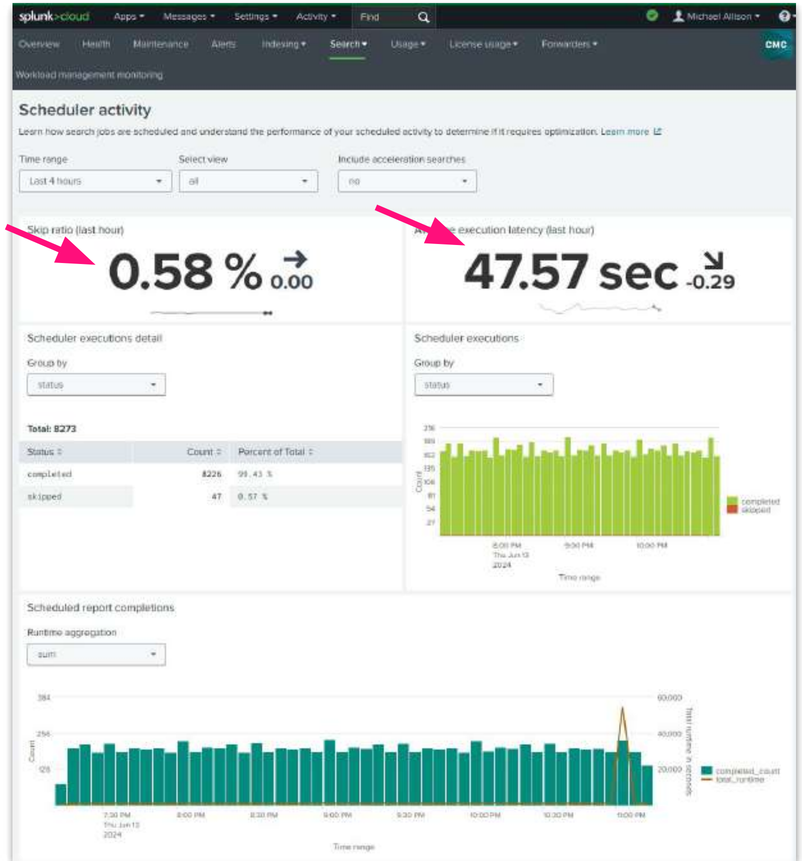
Use the Search dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringSearch

Explore Dashboards

Lab3

Search - Search activity





Scheduler activity

Learn how search jobs are scheduled and understand the performance of your scheduled activity to determine if it requires optimization. Learn more

Time range: Last 4 hours

Select view: all

Include acceleration searches: no

Skip ratio (last hour): 0.58 % → 0.00

A... execution latency (last hour): 47.57 sec ↘ -0.29

Scheduler executions detail

Group by: status

Total: 8273

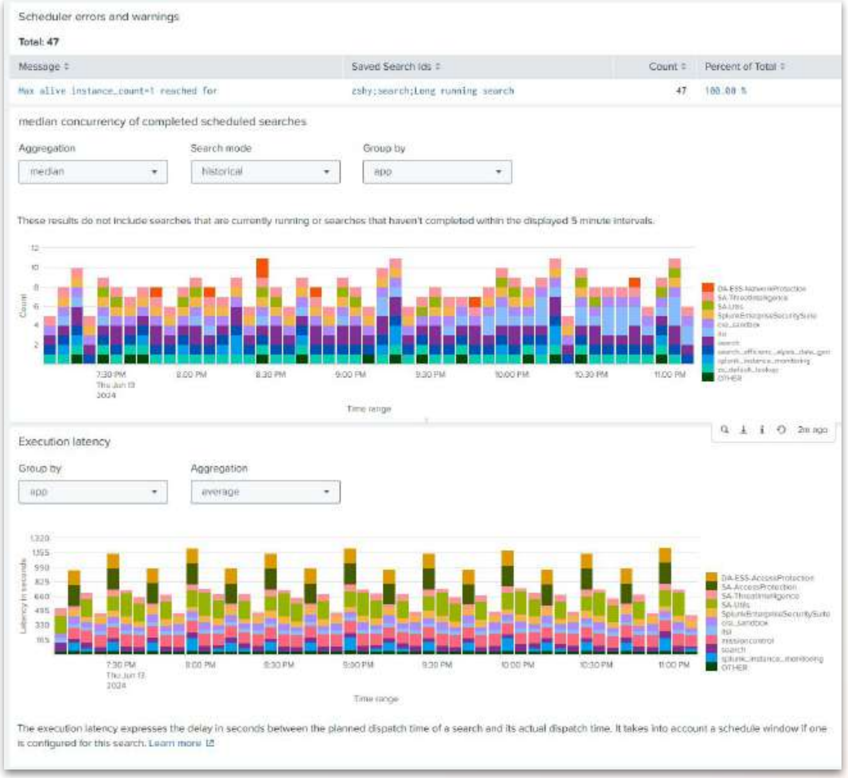
Status	Count	Percent of Total
completed	8226	99.43 %
skipped	47	0.57 %

Scheduler executions

Group by: status

Scheduled report completions

Runtime aggregation: sum



Scheduler errors and warnings

Total: 47

Message	Saved Search Ids	Count	Percent of Total
Max alive instance_count=1 reached for	zshy;search;Long running search	47	100.00 %

median concurrency of completed scheduled searches

Aggregation: median

Search mode: historical

Group by: app

These results do not include searches that are currently running or searches that haven't completed within the displayed 5 minute intervals.

Execution latency

Group by: app

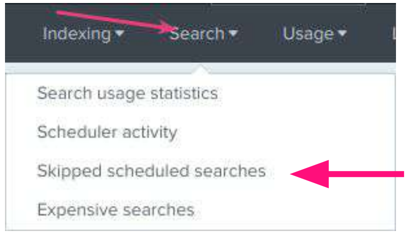
Aggregation: average

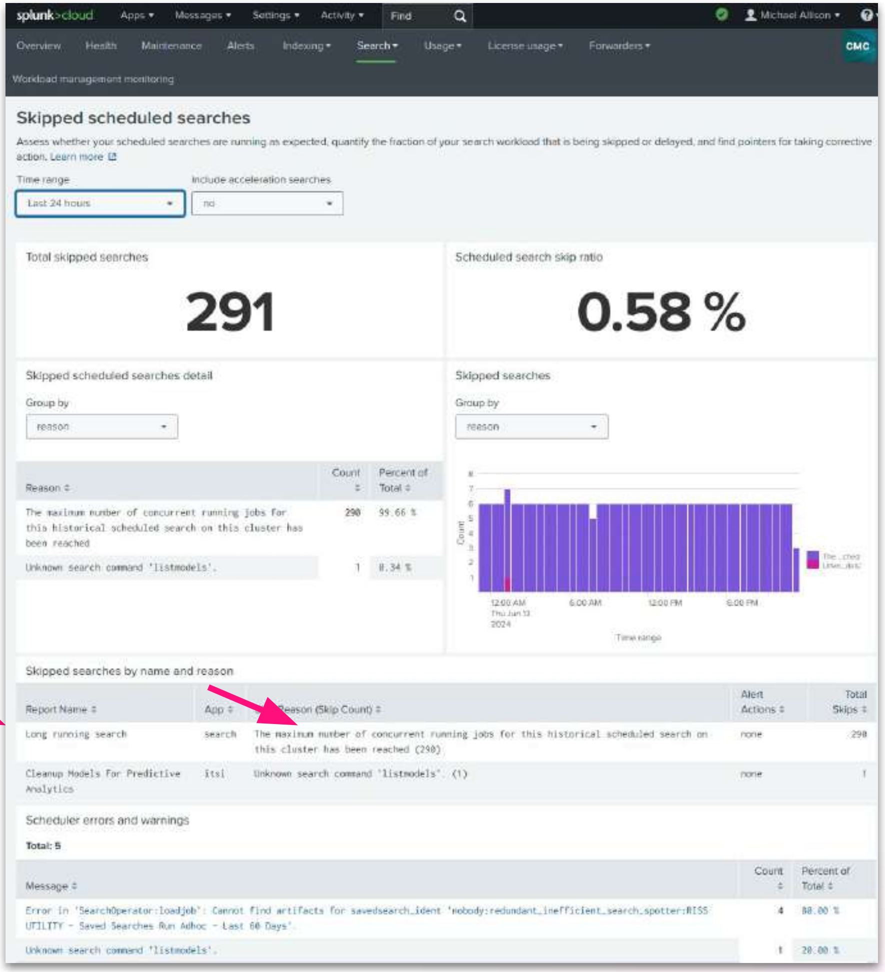
The execution latency expresses the delay in seconds between the planned dispatch time of a search and its actual dispatch time. It takes into account a schedule window if one is configured for this search. Learn more

Use the Search dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringSearch

Explore Dashboards

Search - Skipped scheduled searches





Skipped scheduled searches

Assess whether your scheduled searches are running as expected, quantify the fraction of your search workload that is being skipped or delayed, and find pointers for taking corrective action. Learn more

Time range: Last 24 hours

Include acceleration searches: no

Total skipped searches: **291**

Scheduled search skip ratio: **0.58 %**

Skipped scheduled searches detail

Group by: reason

Reason ⇕	Count ⇕	Percent of Total ⇕
The maximum number of concurrent running jobs for this historical scheduled search on this cluster has been reached	290	99.66 %
Unknown search command 'listmodels'.	1	0.34 %

Skipped searches

Group by: reason

Skipped searches by name and reason

Report Name ⇕	App ⇕	Reason (Skip Count) ⇕	Alert Actions ⇕	Total Skips ⇕
Long running search	search	The maximum number of concurrent running jobs for this historical scheduled search on this cluster has been reached (290)	none	290
Cleanup Models For Predictive Analytics	itsi	Unknown search command 'listmodels'. (1)	none	1

Scheduler errors and warnings

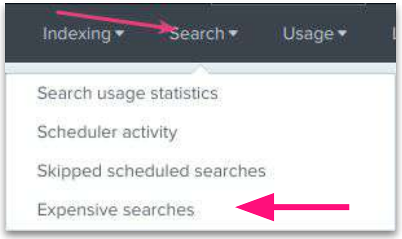
Total: 5

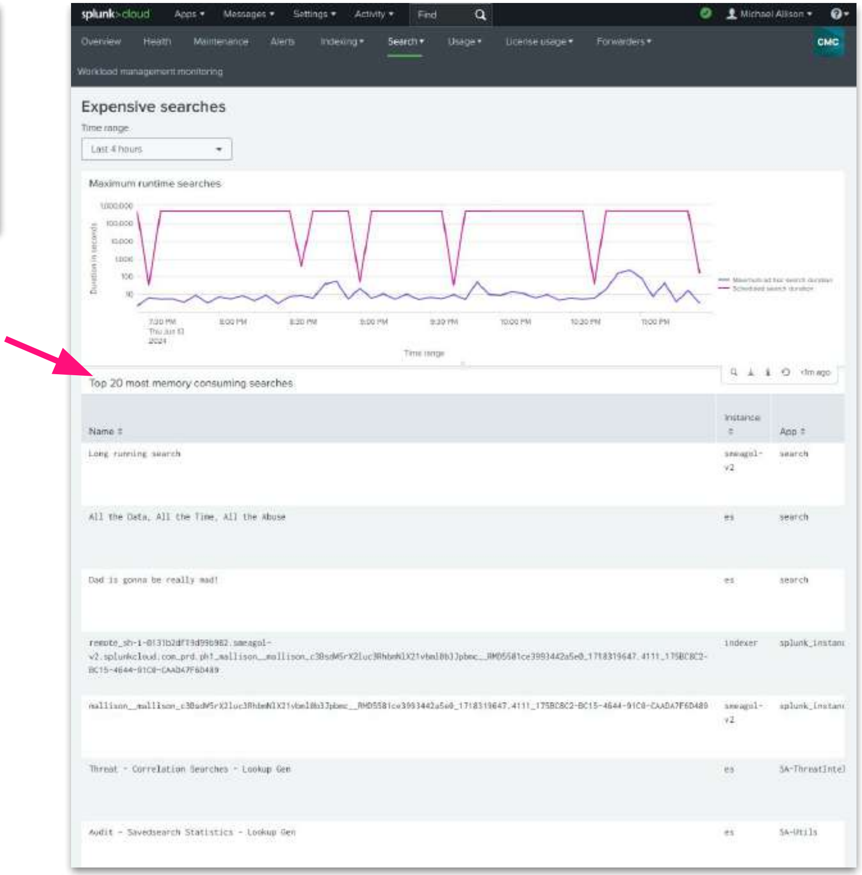
Message ⇕	Count ⇕	Percent of Total ⇕
Error in 'SearchOperator:loadjob': Cannot find artifacts for savedsearch_ident 'nobody:redundant_inefficient_search_spotter:RISS UTILITY - Saved Searches Run Adhoc - Last 60 Days'.	4	80.00 %
Unknown search command 'listmodels'.	1	20.00 %

Use the Search dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringSearch

Explore Dashboards

Expensive searches



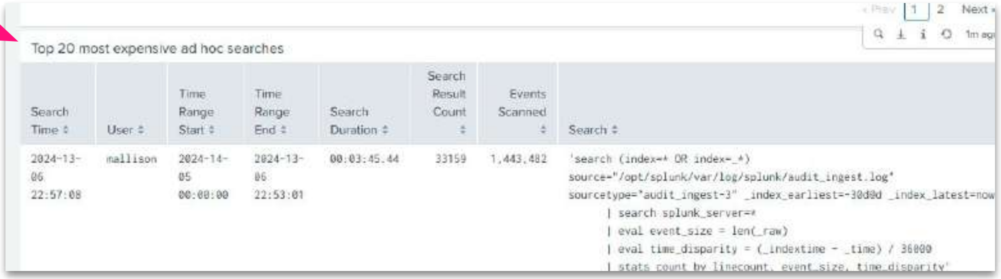


Expensive searches

Time range: Last 4 hours

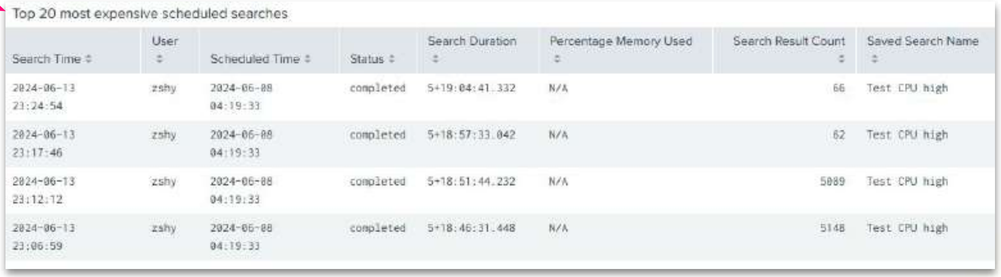
Top 20 most memory consuming searches

Name ⇕	Instance ⇕	App ⇕
Long running search	smeagol-v2	search
All the Data, All the Time, All the Abuse	es	search
Dad is gonna be really mad!	es	search
remote_sh-i-0131b2df19d99b982.smeagol-v2.splunkcloud.com_prd.ph1_mallison__mallison_c3BsdW5rX2luc3RhbmN1X21vbml0b3Jpbmc__RMD5581ce3993442a5e0_1718319647.4111_175BC8C2-BC15-4644-91C0-CAAD47F6D489	indexer	splunk_instan
mallison__mallison_c3BsdW5rX2luc3RhbmN1X21vbml0b3Jpbmc__RMD5581ce3993442a5e0_1718319647.4111_175BC8C2-BC15-4644-91C0-CAAD47F6D489	smeagol-v2	splunk_instan
Threat - Correlation Searches - Lookup Gen	es	SA-ThreatIntel
Audit - Savedsearch Statistics - Lookup Gen	es	SA-Utils



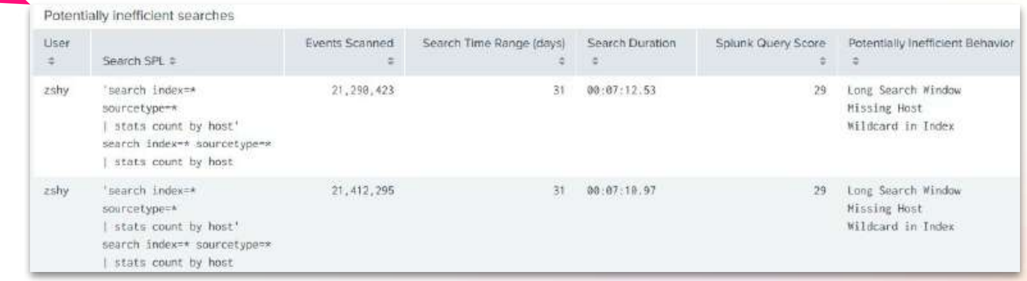
Top 20 most expensive ad hoc searches

<table>
<tr><th>Search Time ⇕</th><th>User ⇕</th><th>Time Range Start ⇕</th><th>Time Range End ⇕</th><th>Search Duration ⇕</th><th>Search Result Count ⇕</th><th>Events Scanned ⇕</th><th>Search ⇕</th></tr>
<tr><td>2024-13-06 22:57:08</td><td>mallison</td><td>2024-14-05 00:00:00</td><td>2024-13-06 22:53:01</td><td>00:03:45.44</td><td>33159</td><td>1,443,482</td><td>'search (index=* OR index=_*)
source="/opt/splunk/var/log/splunk/audit_ingest.log"
sourcetype="audit_ingest-3" _index_earliest=-30d0d _index_latest=now
| search splunk_server=*
| eval event_size = len(_raw)
| eval time_disparity = (_indextime - _time) / 36000
| stats count by linecount, event_size, time_disparity'</td></tr>
</table>



Top 20 most expensive scheduled searches

Search Time ⇕	User ⇕	Scheduled Time ⇕	Status ⇕	Search Duration ⇕	Percentage Memory Used ⇕	Search Result Count ⇕	Saved Search Name ⇕
2024-06-13 23:24:54	zshy	2024-06-08 04:19:33	completed	5+19:04:41.332	N/A	66	Test CPU high
2024-06-13 23:17:46	zshy	2024-06-08 04:19:33	completed	5+18:57:33.042	N/A	62	Test CPU high
2024-06-13 23:12:12	zshy	2024-06-08 04:19:33	completed	5+18:51:44.232	N/A	5089	Test CPU high
2024-06-13 23:06:59	zshy	2024-06-08 04:19:33	completed	5+18:46:31.448	N/A	5148	Test CPU high



Potentially inefficient searches

<table>
<tr><th>User ⇕</th><th>Search SPL ⇕</th><th>Events Scanned ⇕</th><th>Search Time Range (days) ⇕</th><th>Search Duration ⇕</th><th>Splunk Query Score ⇕</th><th>Potentially Inefficient Behavior ⇕</th></tr>
<tr><td>zshy</td><td>'search index=*
sourcetype=*
| stats count by host'
search index=* sourcetype=*
| stats count by host</td><td>21,290,423</td><td>31</td><td>00:07:12.53</td><td>29</td><td>Long Search Window
Missing Host
Wildcard in Index</td></tr>
<tr><td>zshy</td><td>'search index=*
sourcetype=*
| stats count by host'
search index=* sourcetype=*
| stats count by host</td><td>21,412,295</td><td>31</td><td>00:07:10.97</td><td>29</td><td>Long Search Window
Missing Host
Wildcard in Index</td></tr>
</table>

Use the Search dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringSearch

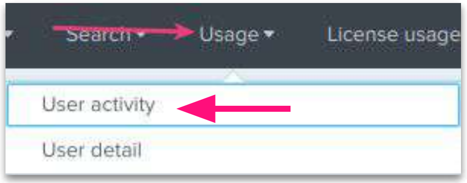
Workshop Agenda

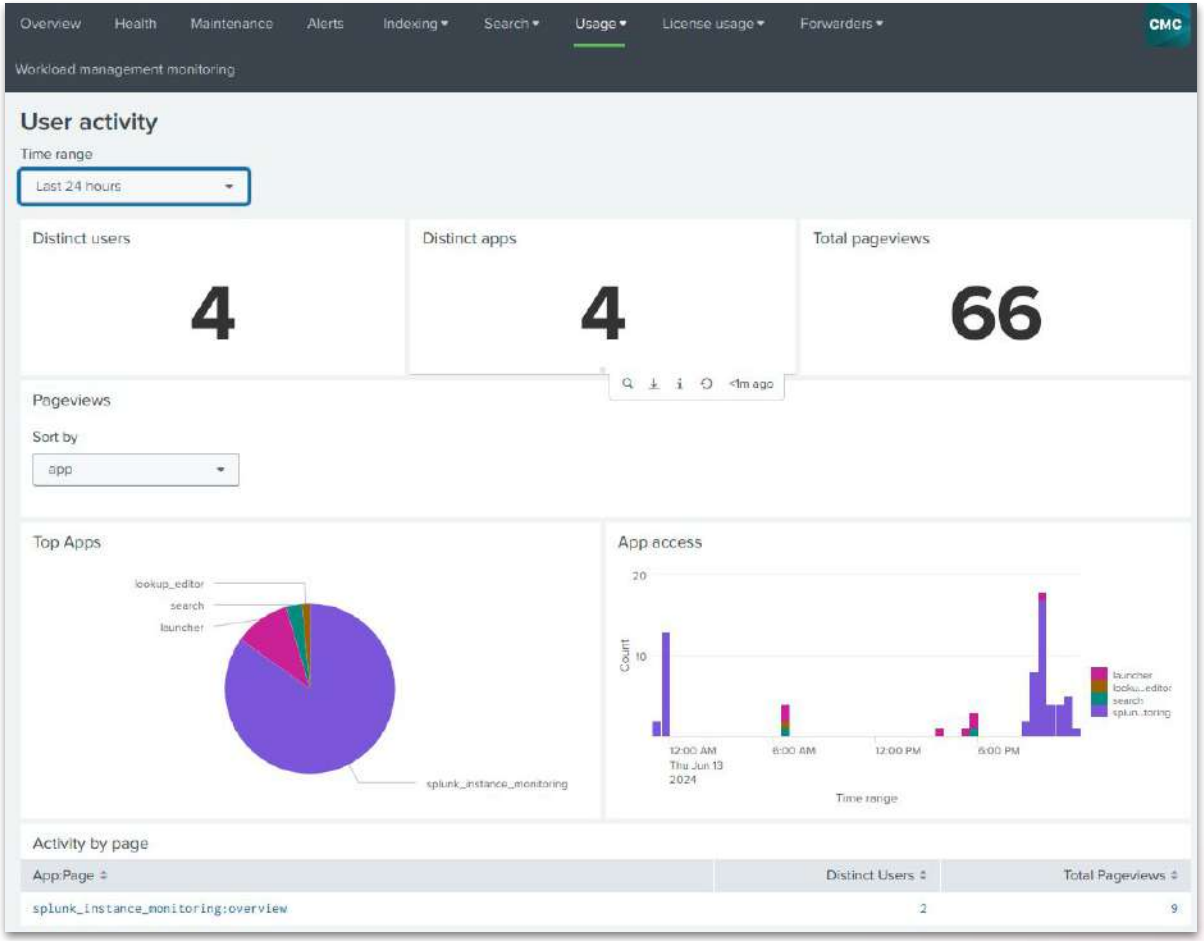
- Discuss Who? What? Why?
- Expectations
- What is an Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Dashboard Modification
- Summary

Explore Dashboards

Lab4

Usage - User activity





User activity

Time range: Last 24 hours

Distinct users: 4

Distinct apps: 4

Total pageviews: 66

Pageviews

Sort by: app

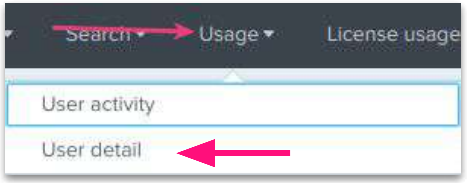
Activity by page

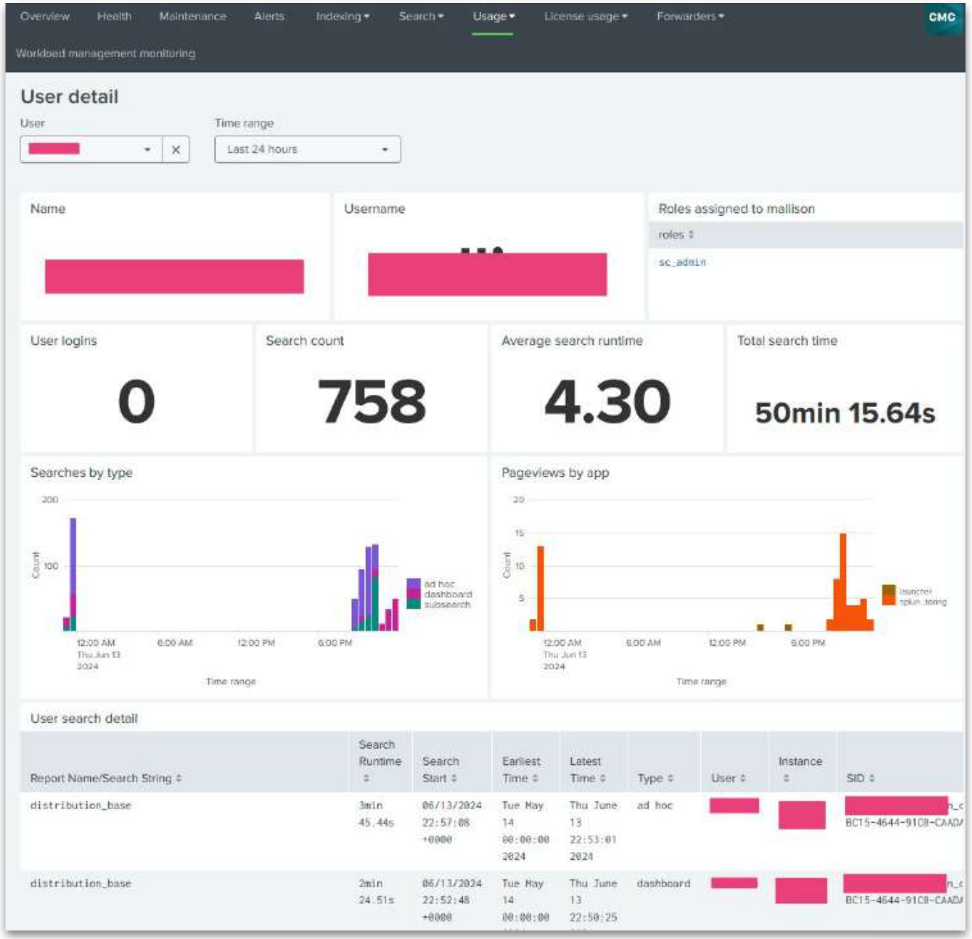
App:Page	Distinct Users	Total Pageviews
splunk_instance_monitoring:overview	2	9

Use the Usage dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringUsage

Explore Dashboards

Usage - User detail





User detail

User: [redacted]

Time range: Last 24 hours

Name: [redacted]

Username: [redacted]

Roles assigned to mallison

roles ⇕
sc_admin

User logins	Search count	Average search runtime	Total search time
0	758	4.30	50min 15.64s

Searches by type

Pageviews by app

User search detail

Report Name/Search String ⇕	Search Runtime ⇕	Search Start ⇕	Earliest Time ⇕	Latest Time ⇕	Type ⇕	User ⇕	Instance ⇕	SID ⇕
distribution_base	3min 45.44s	06/13/2024 22:57:08 +0000	Tue May 14 00:00:00 2024	Thu June 13 22:53:01 2024	ad hoc	[redacted]	[redacted]	[redacted] n_c BC15-4644-91C8-CAAD
distribution_base	2min 24.51s	06/13/2024 22:52:48 +0000	Tue May 14 00:00:00	Thu June 13 22:50:25	dashboard	[redacted]	[redacted]	[redacted] n_c BC15-4644-91C8-CAAD

Use the Usage dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringUsage

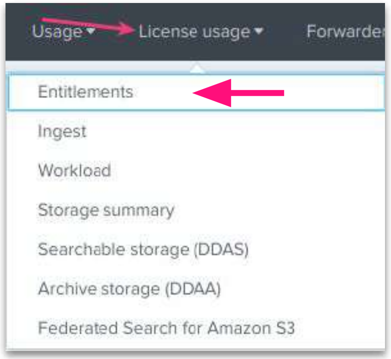
Workshop Agenda

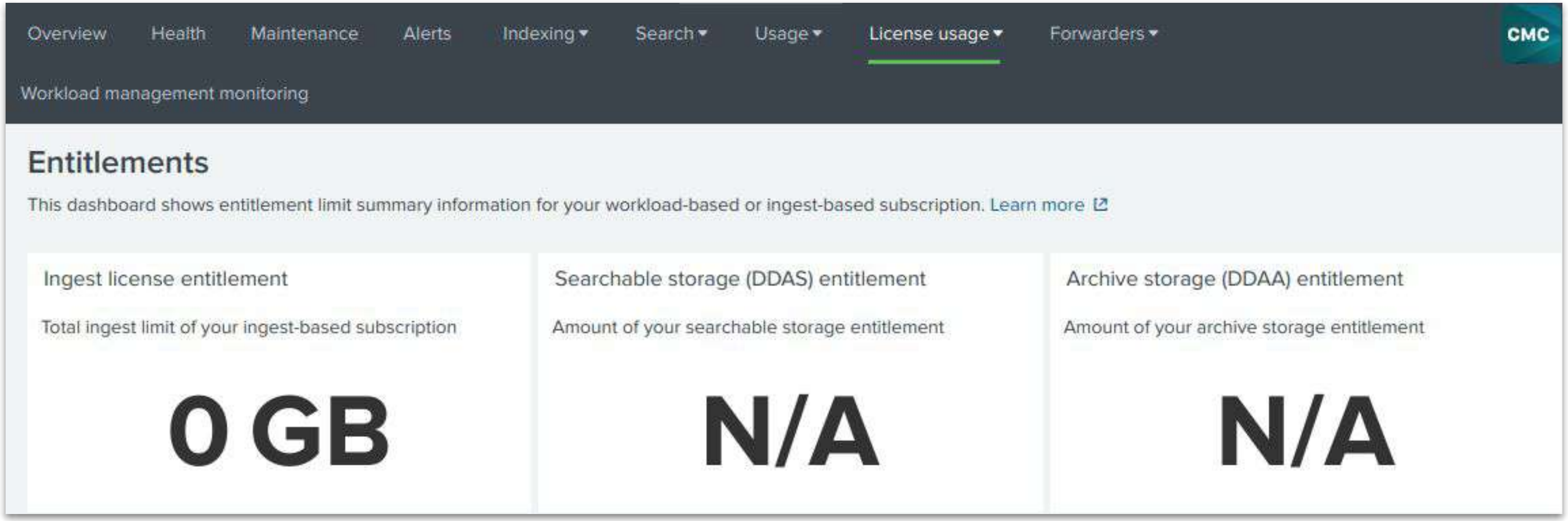
- Discuss Who? What? Why?
- Expectations
- What is an Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Dashboard Modification
- Summary

Explore Dashboards

Lab5

License Usage - Entitlements





Entitlements

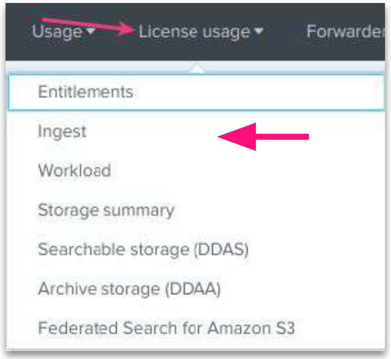
This dashboard shows entitlement limit summary information for your workload-based or ingest-based subscription. Learn more

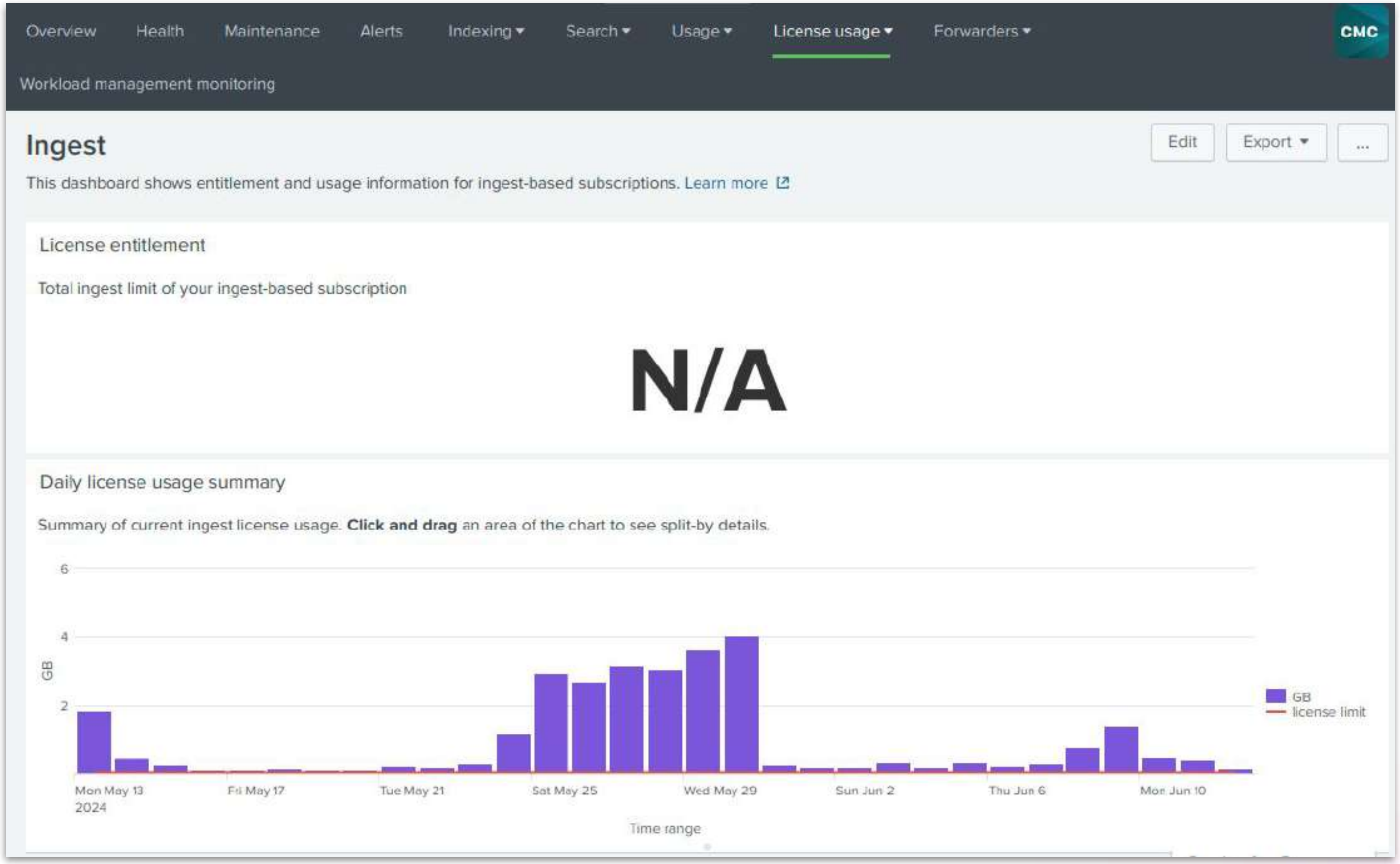
Ingest license entitlement	Searchable storage (DDAS) entitlement	Archive storage (DDAA) entitlement
Total ingest limit of your ingest-based subscription	Amount of your searchable storage entitlement	Amount of your archive storage entitlement
0 GB	N/A	N/A

Use the License Usage dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage

Explore Dashboards

License Usage - Ingest





Ingest

This dashboard shows entitlement and usage information for ingest-based subscriptions. Learn more

License entitlement

Total ingest limit of your ingest-based subscription

N/A

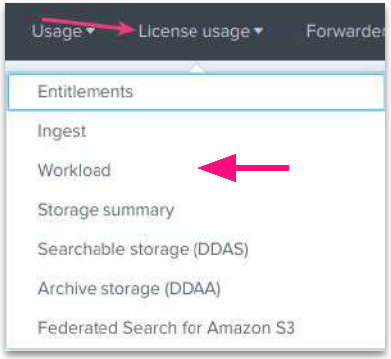
Daily license usage summary

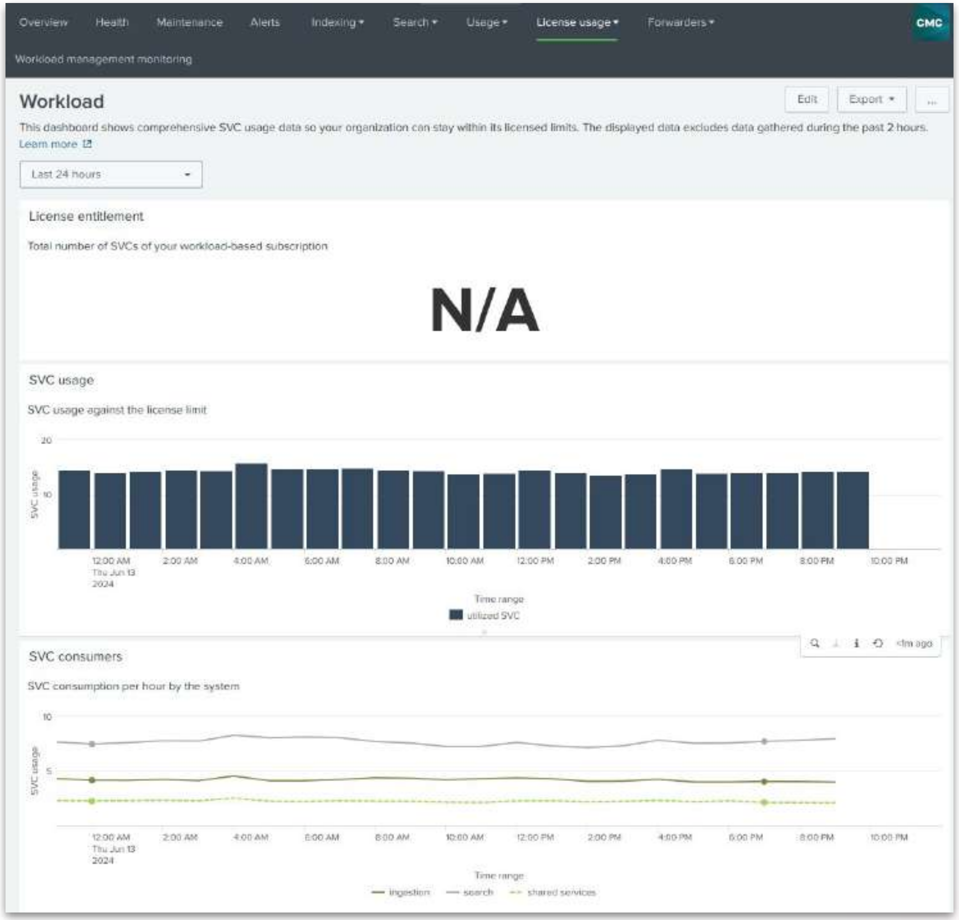
Summary of current ingest license usage. **Click and drag** an area of the chart to see split-by details.

Use the License Usage dashboards https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage

Explore Dashboards

License Usage - Ingest





Workload

This dashboard shows comprehensive SVC usage data so your organization can stay within its licensed limits. The displayed data excludes data gathered during the past 2 hours. Learn more

License entitlement

Total number of SVCs of your workload-based subscription

N/A

SVC usage

SVC usage against the license limit

SVC consumers

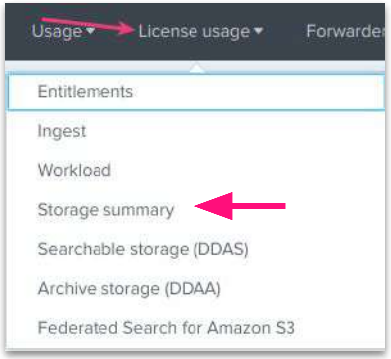
SVC consumption per hour by the system

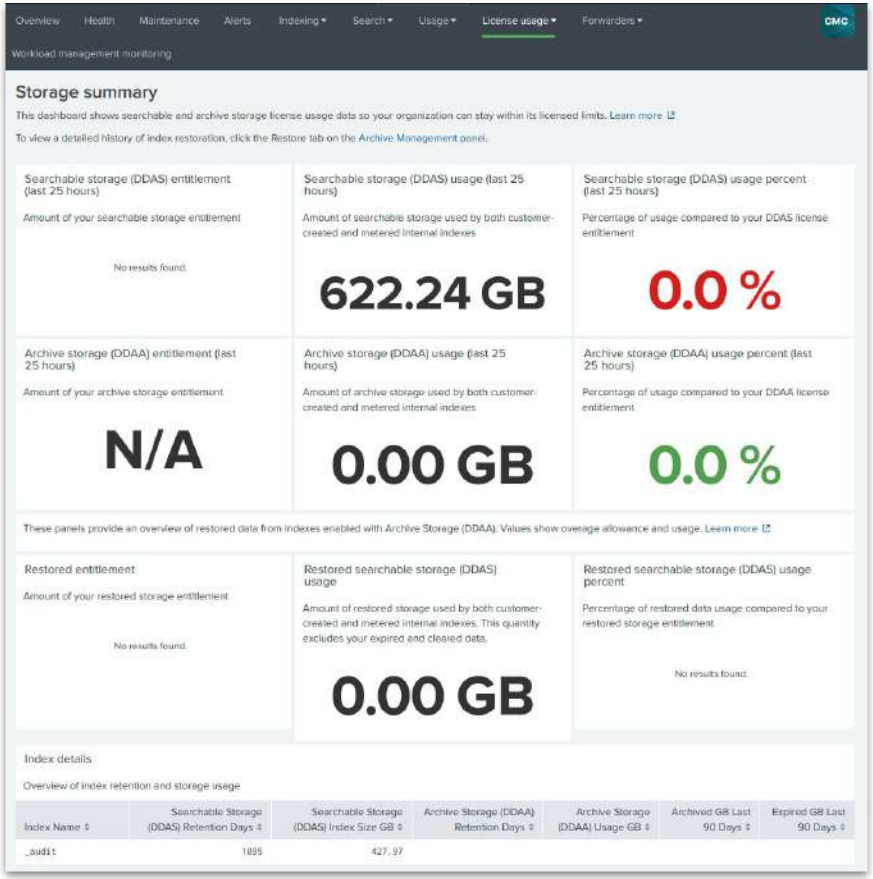
Use the Workload (preview) dashboard	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/Workload
How is SVC Utilization Measured	What is Splunk Virtual Compute (SVC)?

Explore Dashboards

Lab5

License Usage - Storage summary





Storage summary

This dashboard shows searchable and archive storage 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.

Searchable storage (DDAS) entitlement (last 25 hours)

Amount of your searchable storage entitlement

No results found.

Searchable storage (DDAS) usage (last 25 hours)

Amount of searchable storage used by both customer-created and metered internal indexes

622.24 GB

Searchable storage (DDAS) usage percent (last 25 hours)

Percentage of usage compared to your DDAS license entitlement

0.0 %

Archive storage (DDAA) entitlement (last 25 hours)

Amount of your archive storage entitlement

N/A

Archive storage (DDAA) usage (last 25 hours)

Amount of archive storage used by both customer-created and metered internal indexes

0.00 GB

Archive storage (DDAA) usage percent (last 25 hours)

Percentage of usage compared to your DDAA license entitlement

0.0 %

These panels provide an overview of restored data from indexes enabled with Archive Storage (DDAA). Values show overage allowance and usage. Learn more

Restored entitlement

Amount of your restored storage entitlement

No results found.

Restored searchable storage (DDAS) usage

Amount of restored storage used by both customer-created and metered internal indexes. This quantity excludes your expired and cleared data.

0.00 GB

Restored searchable storage (DDAS) usage percent

Percentage of restored data usage compared to your restored storage entitlement

No results found.

Index details

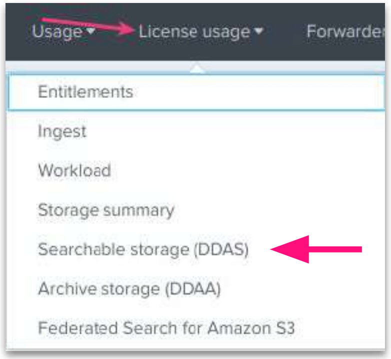
Overview of index retention and storage usage

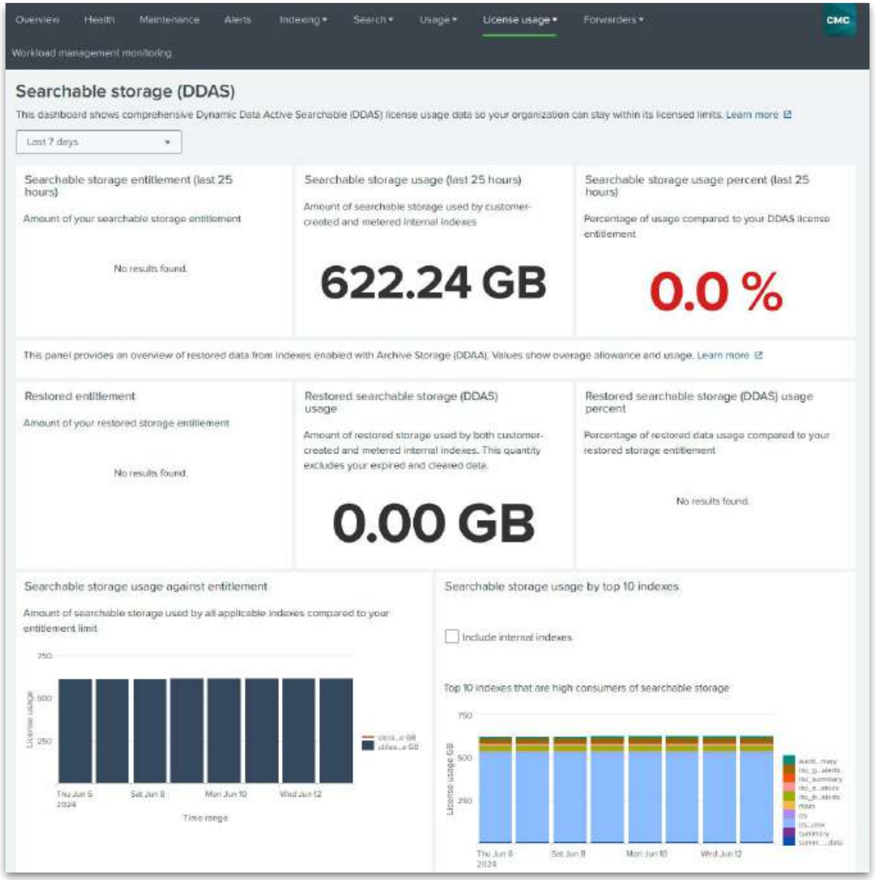
Index Name ⇕	Searchable Storage (DDAS) Retention Days ⇕	Searchable Storage (DDAS) Index Size GB ⇕	Archive Storage (DDAA) Retention Days ⇕	Archive Storage (DDAA) Usage GB ⇕	Archived GB Last 90 Days ⇕	Expired GB Last 90 Days ⇕
_audit	1895	427.97				

Use the License Usage dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage
How is SVC Utilization Measured	What is Splunk Virtual Compute (SVC)?

Explore Dashboards

License Usage - Archive 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. Learn more

Last 7 days ▾

Searchable storage entitlement (last 25 hours)

Amount of your searchable storage entitlement

No results found.

Searchable storage usage (last 25 hours)

Amount of searchable storage used by customer-created and metered internal indexes

622.24 GB

Searchable storage usage percent (last 25 hours)

Percentage of usage compared to your DDAS license entitlement

0.0 %

This panel provides an overview of restored data from indexes enabled with Archive Storage (DDAA). Values show overage allowance and usage. Learn more

Restored entitlement

Amount of your restored storage entitlement

No results found.

Restored searchable storage (DDAS) usage

Amount of restored storage used by both customer-created and metered internal indexes. This quantity excludes your expired and cleared data.

0.00 GB

Restored searchable storage (DDAS) usage percent

Percentage of restored data usage compared to your restored storage entitlement

No results found.

Searchable storage usage against entitlement

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

Searchable storage usage by top 10 indexes

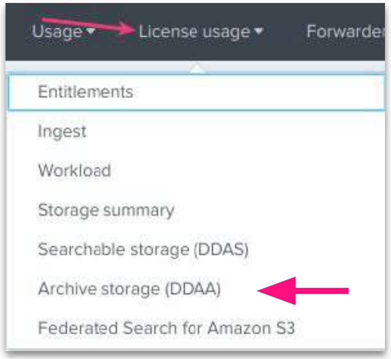
□ Include internal indexes

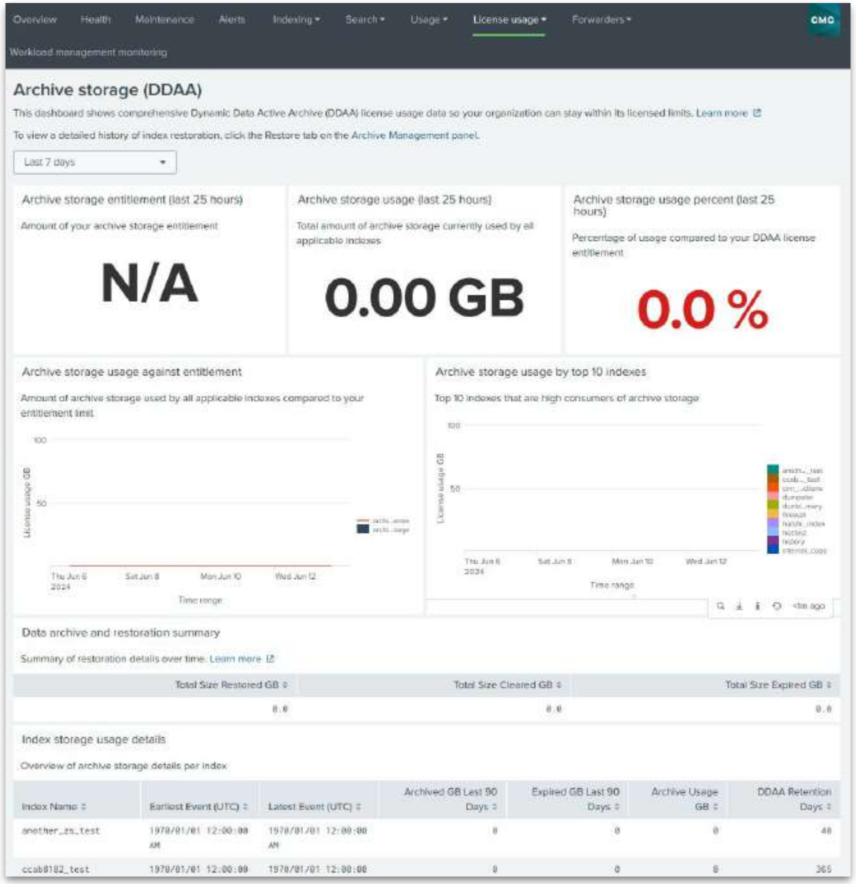
Top 10 indexes that are high consumers of searchable storage

Use the License Usage dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage
How is SVC Utilization Measured	What is Splunk Virtual Compute (SVC)?

Explore Dashboards

License Usage - Searchable 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.

Last 7 days ▾

Archive storage entitlement (last 25 hours)	Archive storage usage (last 25 hours)	Archive storage usage percent (last 25 hours)
Amount of your archive storage entitlement	Total amount of archive storage currently used by all applicable indexes	Percentage of usage compared to your DDAA license entitlement
N/A	0.00 GB	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

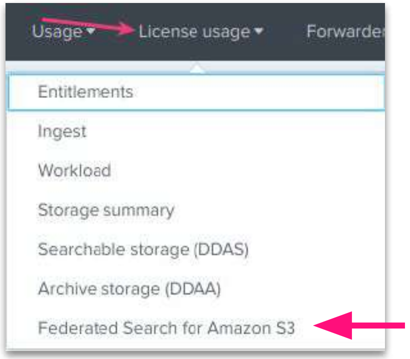
Index Name ⇕	Earliest Event (UTC) ⇕	Latest Event (UTC) ⇕	Archived GB Last 90 Days ⇕	Expired GB Last 90 Days ⇕	Archive Usage GB ⇕	DDAA Retention Days ⇕
another_zs_test	1970/01/01 12:00:00 AM	1970/01/01 12:00:00 AM	0	0	0	40
ccab8182_test	1970/01/01 12:00:00	1970/01/01 12:00:00	0	0	0	365

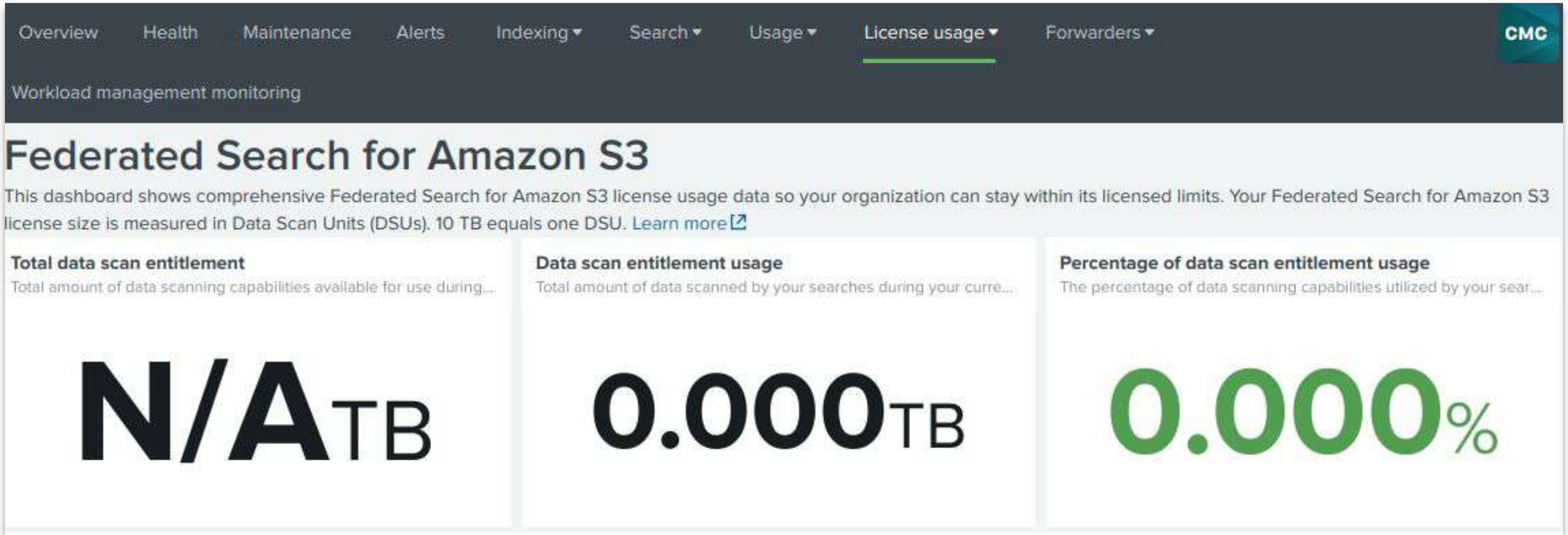
Use the License Usage dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage
How is SVC Utilization Measured	What is Splunk Virtual Compute (SVC)?

Explore Dashboards

Lab5

License Usage - Federated Search for Amazon S3





Federated Search for Amazon S3

This dashboard shows comprehensive Federated Search for Amazon S3 license usage data so your organization can stay within its licensed limits. Your Federated Search for Amazon S3 license size is measured in Data Scan Units (DSUs). 10 TB equals one DSU. Learn more

Total data scan entitlement
Total amount of data scanning capabilities available for use during...
N/ATB

Data scan entitlement usage
Total amount of data scanned by your searches during your curre...
0.000TB

Percentage of data scan entitlement usage
The percentage of data scanning capabilities utilized by your sear...
0.000%

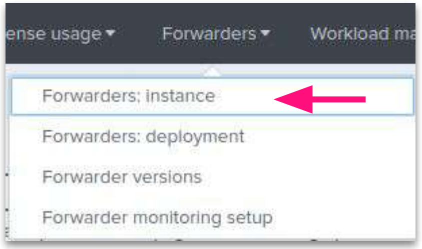
Use the License Usage dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringLicenseUsage
How is SVC Utilization Measured	What is Splunk Virtual Compute (SVC)?

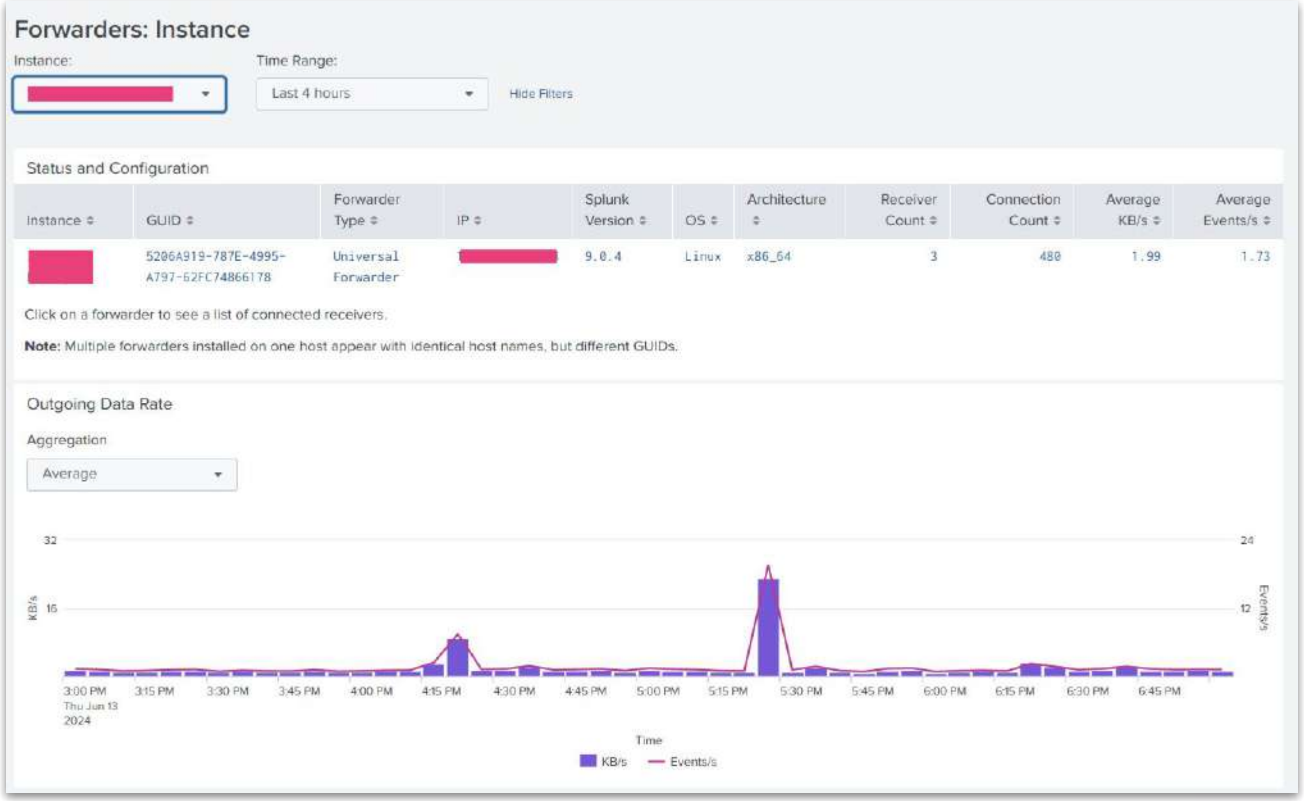
Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Dashboard Modification
- Summary

Explore Dashboards

Forwarders: Instance





Forwarders: Instance

Instance: [redacted]

Time Range: Last 4 hours

Hide Filters

Status and Configuration

Instance ⇕	GUID ⇕	Forwarder Type ⇕	IP ⇕	Splunk Version ⇕	OS ⇕	Architecture ⇕	Receiver Count ⇕	Connection Count ⇕	Average KB/s ⇕	Average Events/s ⇕
[redacted]	5206A919-787E-4995-A797-62FC74866178	Universal Forwarder	[redacted]	9.0.4	Linux	x86_64	3	480	1.99	1.73

Click on a forwarder to see a list of connected receivers.

Note: Multiple forwarders installed on one host appear with identical host names, but different GUIDs.

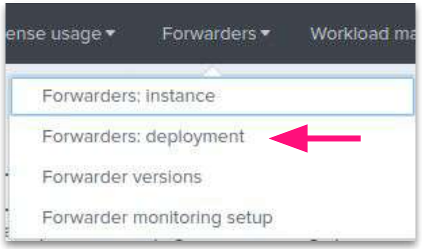
Outgoing Data Rate

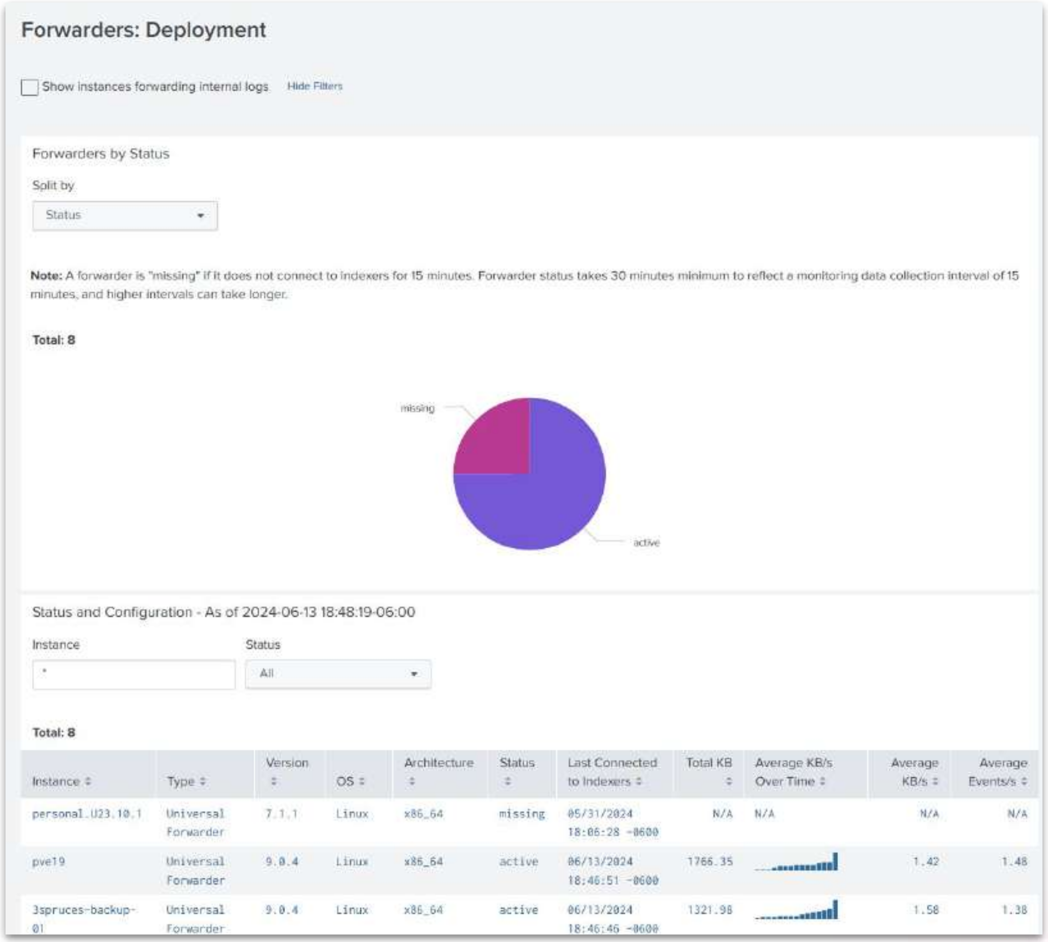
Aggregation: Average

Use the Forwarder dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringForwarders

Explore Dashboards

Forwarders: Deployment





Forwarders: Deployment

☐ Show instances forwarding internal logs   Hide Filters

Forwarders by Status

Split by: Status ▾

Note: A forwarder is "missing" if it does not connect to indexers for 15 minutes. Forwarder status takes 30 minutes minimum to reflect a monitoring data collection interval of 15 minutes, and higher intervals can take longer.

Total: 8

Status and Configuration - As of 2024-06-13 18:48:19-06:00

Instance: *   Status: All ▾

Total: 8

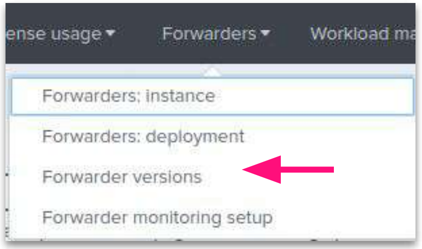
Instance ⇕	Type ⇕	Version ⇕	OS ⇕	Architecture ⇕	Status ⇕	Last Connected to Indexers ⇕	Total KB ⇕	Average KB/s Over Time ⇕	Average KB/s ⇕	Average Events/s ⇕
personal_U23.10.1	Universal Forwarder	7.1.1	Linux	x86_64	missing	05/31/2024 18:06:28 -0600	N/A	N/A	N/A	N/A
pve19	Universal Forwarder	9.0.4	Linux	x86_64	active	06/13/2024 18:46:51 -0600	1766.35		1.42	1.48
3spruces-backup-01	Universal Forwarder	9.0.4	Linux	x86_64	active	06/13/2024 18:46:46 -0600	1321.98		1.58	1.38

Use the Forwarder dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringForwarders

Explore Dashboards

Lab6

Forwarder versions



ense usage ▾ Forwarders ▾ Workload ma

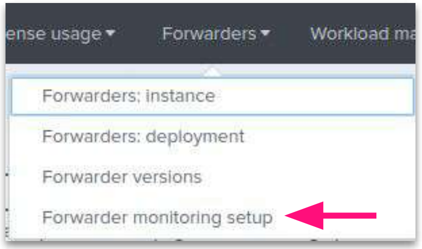
Forwarders: instance
Forwarders: deployment
Forwarder versions
Forwarder monitoring setup

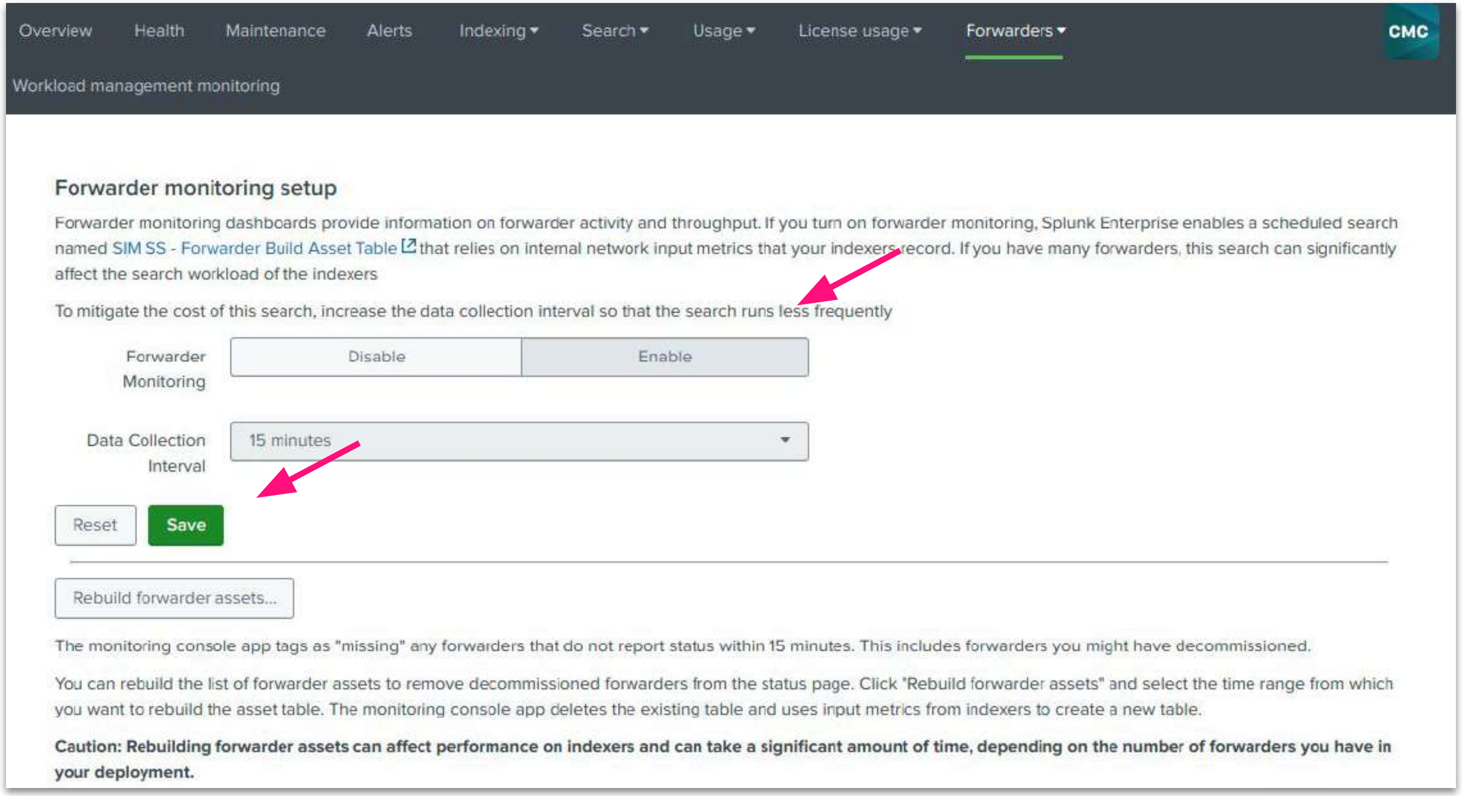
NEED WORKING LAB FOR THIS, TEST SYSTEM DIDN'T HAVE ANYTHING

Use the Forwarder dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringForwarders

Explore Dashboards

Forwarder versions





Forwarder monitoring setup

Forwarder monitoring dashboards provide information on forwarder activity and throughput. If you turn on forwarder monitoring, Splunk Enterprise enables a scheduled search named SIM SS - Forwarder Build Asset Table that relies on internal network input metrics that your indexers record. If you have many forwarders, this search can significantly affect the search workload of the indexers

To mitigate the cost of this search, increase the data collection interval so that the search runs less frequently

Forwarder Monitoring: Disable | Enable

Data Collection Interval: 15 minutes

Reset | Save

Rebuild forwarder assets...

The monitoring console app tags as "missing" any forwarders that do not report status within 15 minutes. This includes forwarders you might have decommissioned.

You can rebuild the list of forwarder assets to remove decommissioned forwarders from the status page. Click "Rebuild forwarder assets" and select the time range from which you want to rebuild the asset table. The monitoring console app deletes the existing table and uses input metrics from indexers to create a new table.

Caution: Rebuilding forwarder assets can affect performance on indexers and can take a significant amount of time, depending on the number of forwarders you have in your deployment.

Use the Forwarder dashboards	https://docs.splunk.com/Documentation/SplunkCloud/latest/Admin/MonitoringForwarders

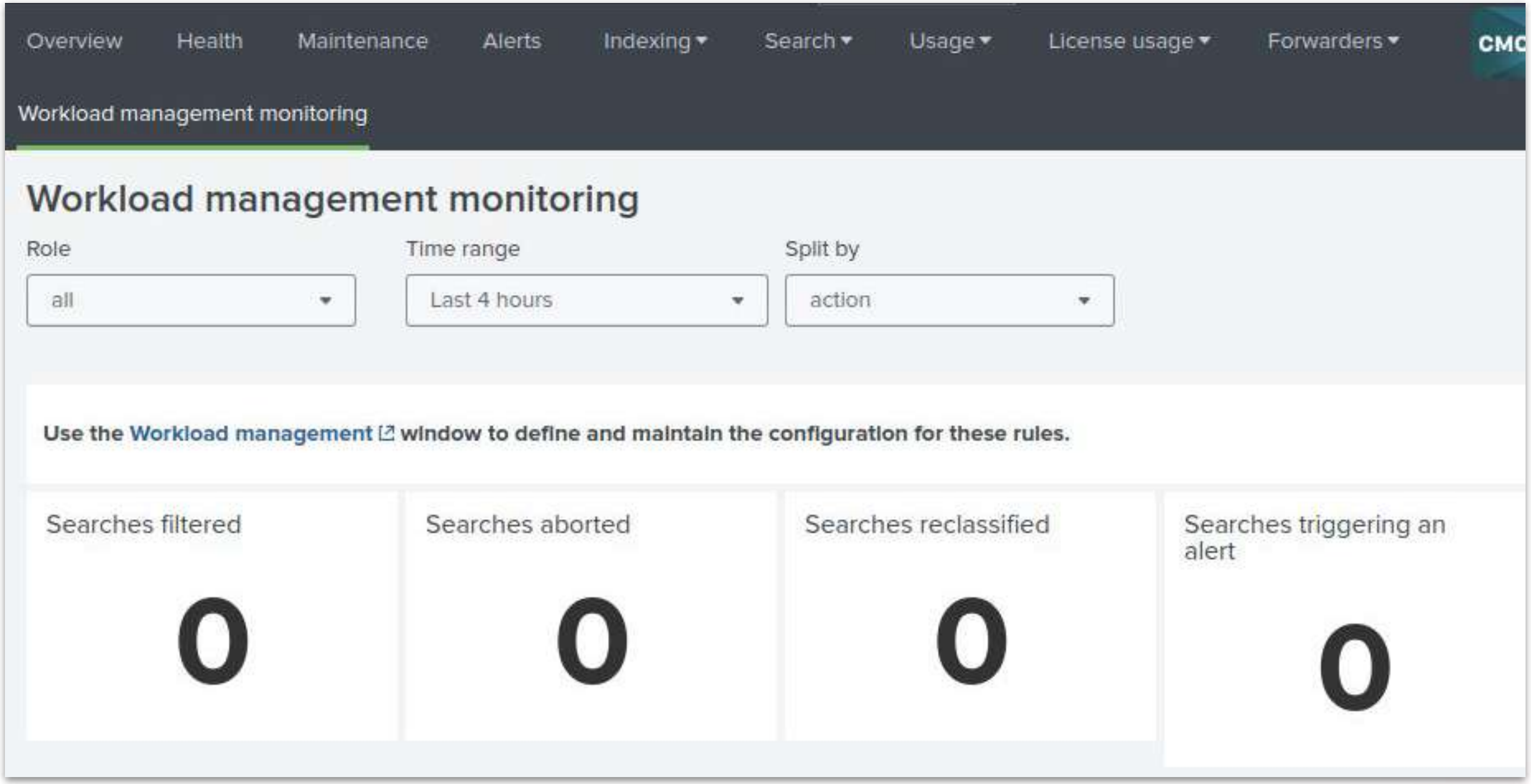
Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Explore Workload management monitoring - Lab 7
- Dashboard Modification
- Summary

Explore Dashboards

Workload management monitoring

Lab7



Workload management monitoring

Role: all

Time range: Last 4 hours

Split by: action

Use the Workload management window to define and maintain the configuration for these rules.

Searches filtered	Searches aborted	Searches reclassified	Searches triggering an alert
0	0	0	0

Use the Workload Management Monitoring dashboard	https://docs.splunk.com/Documentation/SplunkCloud/9.2.2403/Admin/MonitoringWrkldMgmt

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Explore Workload management monitoring - Lab 7
- Dashboard Modification
- Summary

Dashboard Modification

Localization

- Optimize a master CMC for your needs
  - Each dashboard/panel is cloneable (do not modify the existing in CMC)
    - Build a MC that is specific to your environment requirements
    - The app that hosts the MC is called “Cloud Monitoring Console (splunk_instance_monitoring)”
    - All dashboards, panels, and searches are in that app
    - Copy and modify as necessary
- Reiterate - **Do not modify any dashboards in the “Cloud Monitoring Console (splunk_instance_monitoring)” app**

MC/CMC Overview	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
How the Monitoring Console works	https://docs.splunk.com/Documentation/Splunk/latest/DMC/HowtheDMCworks
Clone and manage dashboards	https://docs.splunk.com/Documentation/Splunk/latest/Viz/DashboardCloneHome

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Cloud Monitoring Console (CMC)?
- Explore Overview/Health/Maintenance/Alerts - Lab 1
- Explore Indexing - Lab 2
- Explore Search - Lab 3
- Explore Usage - Lab 4
- Explore License Usage - Lab 5
- Explore Forwarders - Lab 6
- Dashboard Modification
- Summary

Summary

Covered a great deal …

- Learn CMC to understand your environment
  - Overview
  - Health Check
  - Indexing Performance
  - Search - Activity
  - Forwarders
- Difference between “deployment” and “instance”
  - Deployment provides overall - detect where potential issues are
  - Instance - determine specifically what is causing issue
- Clone and customize as necessary

Links

Also in the Lab Guide

Title	Link
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
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

Thank you

splunk>
a CISCO company