

Splunk4Admins

Monitoring Console



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.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2024 Splunk Inc. All rights reserved.





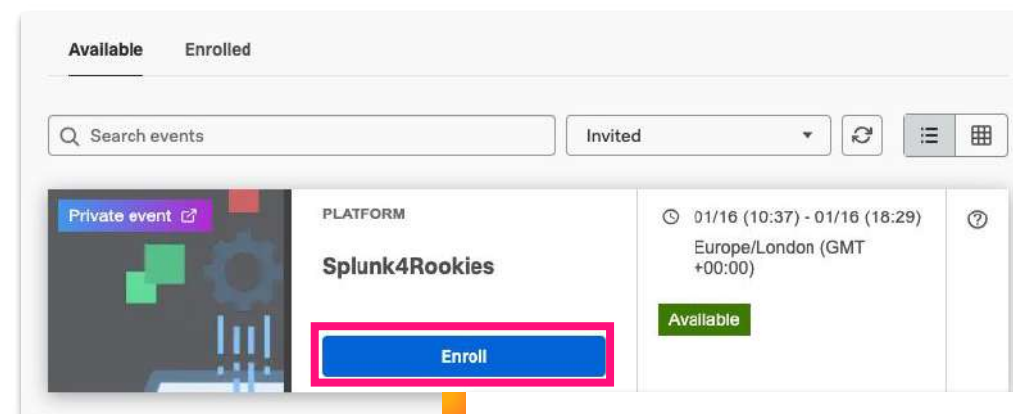
Enroll in Today's Workshop

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-MC-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-MC-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 Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Assist|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- 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 “MC” ...

- Last roughly 90 - 120 minutes
- Experience setup and configuration of MC
- Understand the dashboards in MC
 - Indexing
 - Search
 - Resource Usage
 - Forwarders
- Understand how to use MC to adhere more closely to Best Practices
- Experience discovery of common issues from MC

What is the MC?

- MC - Enterprise, customer-managed cloud
 - Set of dashboards providing information about OnPremise resources
- CMC - Splunk Cloud
 - Set of dashboards providing information about customer-influenceable resources - more limited than the MC for OnPremise Enterprise
- Understanding what the MC/CMC has available can help Admins diagnose and remediate more quickly
- Should be separate from all other production activities
- Architecture - size appropriately
 - Scale up the MC or run separate MCs for different tiers
 - Not part of standard user-accessible architecture

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 an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- Dashboard Modification
- Summary

Configure and setup MC



- Requirements

- Splunk Enterprise
- Each instance has unique `serverName` & `inputs.conf` `host` value
- Forwarding logs
- Setup user has `admin_all_objects` capability
- MC platform is separate from all other instances

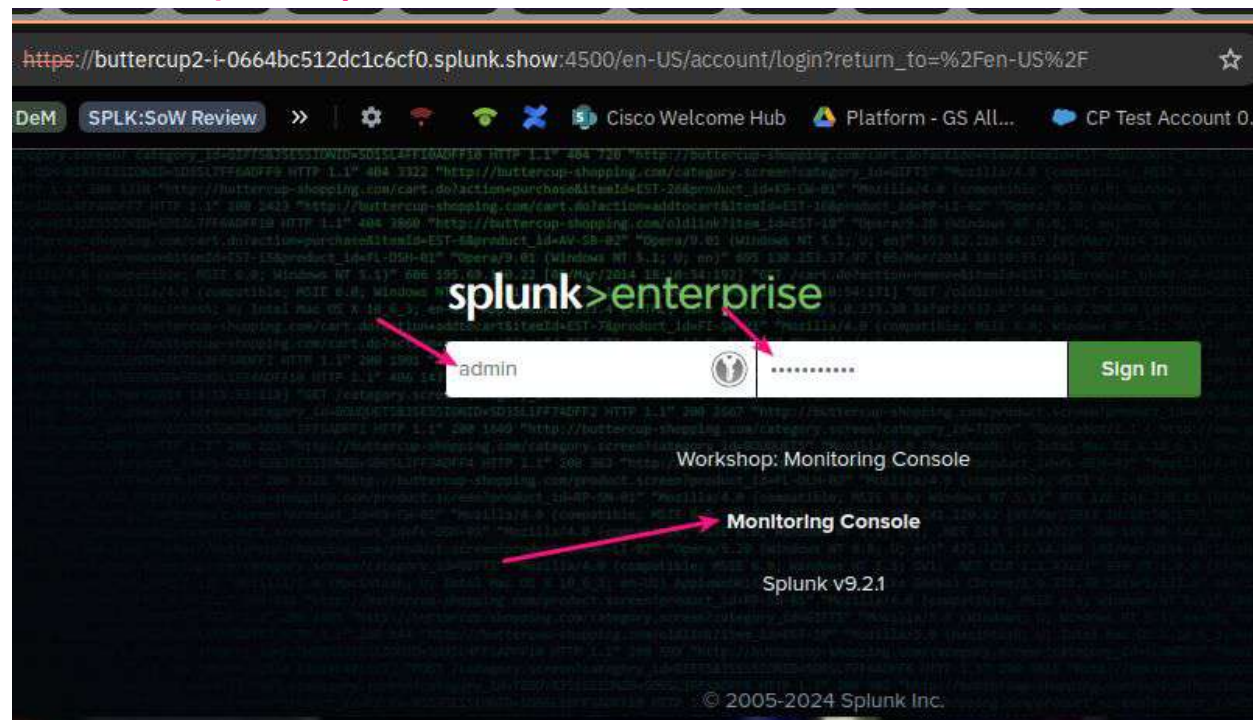
MC/CMC Overview	About the Monitoring Console - Splunk Documentation
Which should host?	https://docs.splunk.com/Documentation/Splunk/latest/DMC/WheretohostDMC
Single-instance Monitoring Console setup steps	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Singleinstancesetup

Configure and setup MC



Setup “Indexer Clustering” as a search head member

Access your MC https://<your_IP>:4500

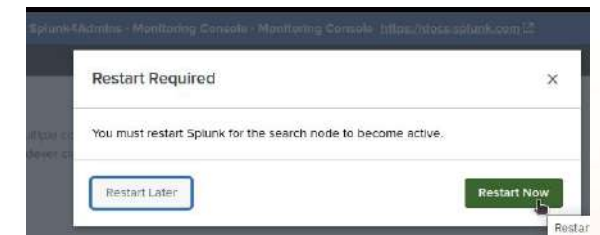
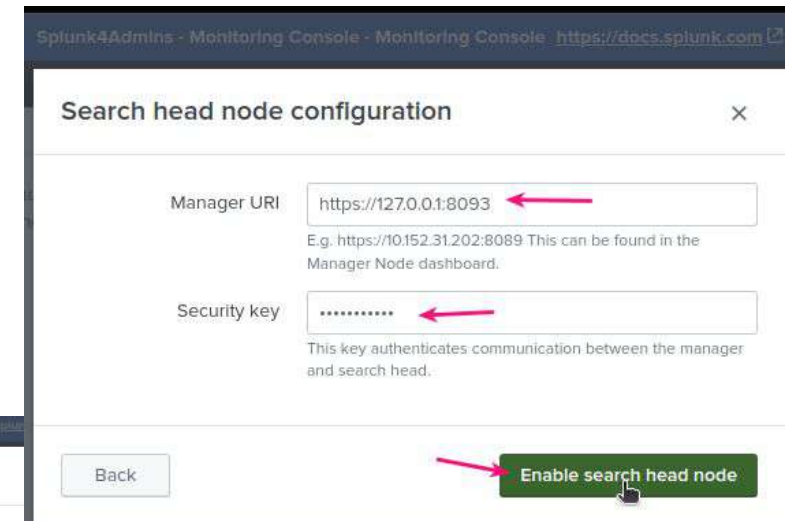
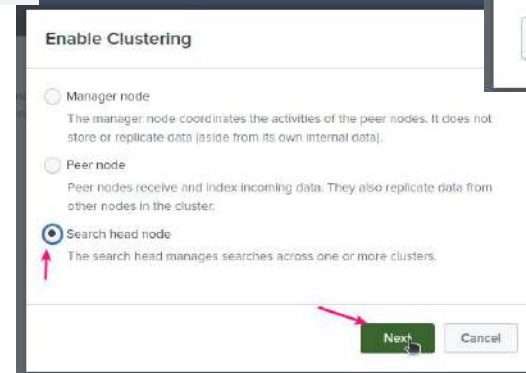
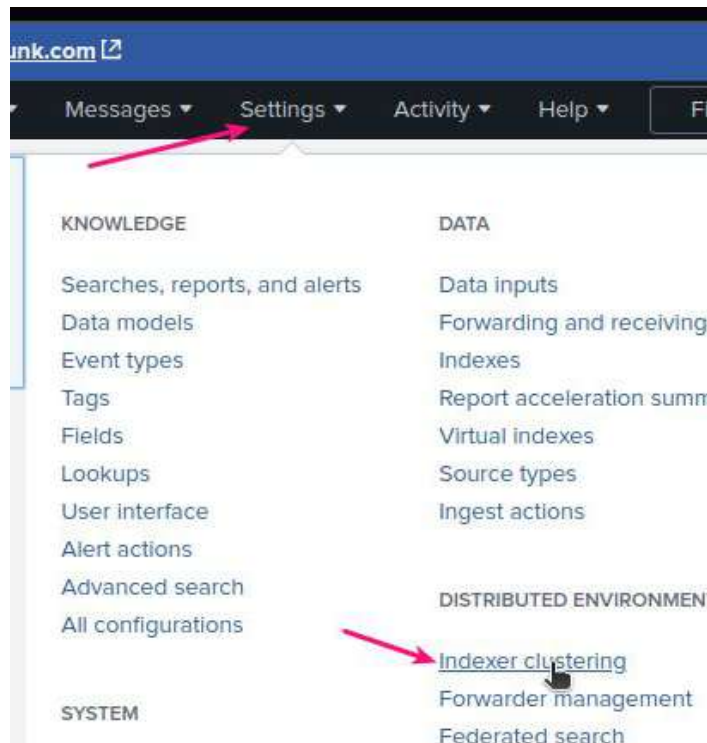


MC/CMC Overview	About the Monitoring Console - Splunk Documentation
Which should host?	https://docs.splunk.com/Documentation/Splunk/latest/DMC/WheretohostDMC
Single-instance Monitoring Console setup steps	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Singleinstancesetup

Configure and setup MC



Setup “Indexer Clustering” as a search head member



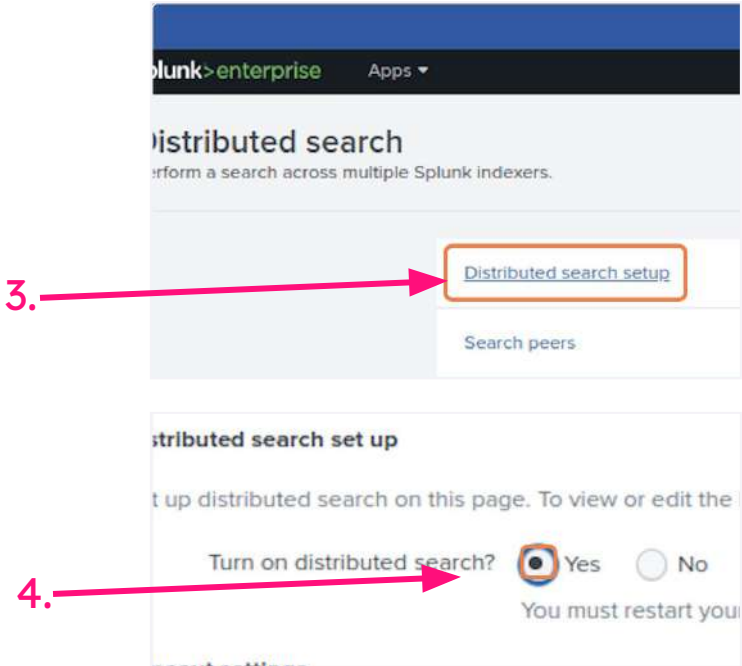
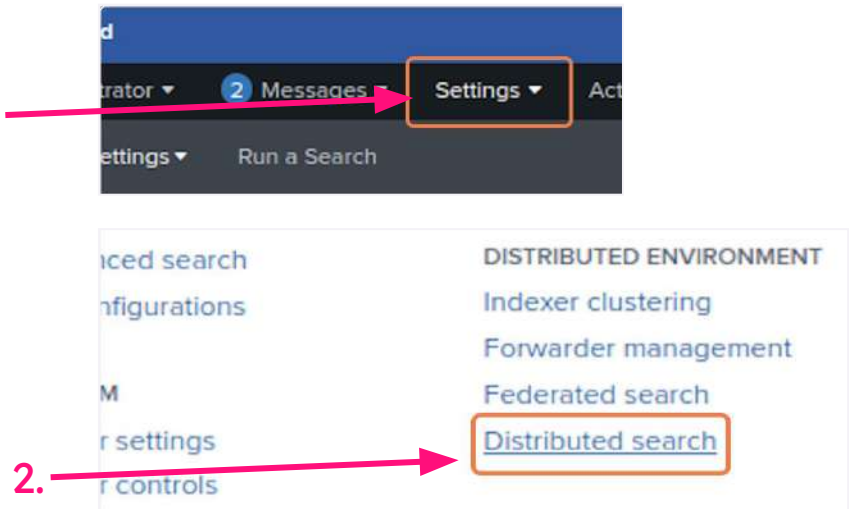
MC/CMC Overview	About the Monitoring Console - Splunk Documentation
Which should host?	https://docs.splunk.com/Documentation/Splunk/latest/DMC/WheretohostDMC
Single-instance Monitoring Console setup steps	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Singleinstancesetup

Configure and setup MC



Setup “Distributed Search”

1. Access your MC `https://<your_IP>:4500`



MC/CMC Overview	About the Monitoring Console - Splunk Documentation
Which should host?	https://docs.splunk.com/Documentation/Splunk/latest/DMC/WheretohostDMC
Single-instance Monitoring Console setup steps	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Singleinstancesetup

Configure and setup MC



Setup “Distributed Search” Peers

1.

2.

3.

4.

5.

6.

7.

MC/CMC Overview	About the Monitoring Console - Splunk Documentation
Which should host?	https://docs.splunk.com/Documentation/Splunk/latest/DMC/WheretohostDMC
Single-instance Monitoring Console setup steps	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Singleinstancesetup

Configure and setup MC



Setup “Distributed Search” - configure to “Distributed” Mode

1.

2.

3.

4.

Switch to Distributed Mode

⚠ Do not configure the DMC in distributed mode if this is a production search head. Doing so can change the behavior of all searches on this instance. This is dangerous and unsupported.

If you want to configure the DMC in distributed mode, you must locate the DMC on an instance that is not a production search head.

[Learn more](#)

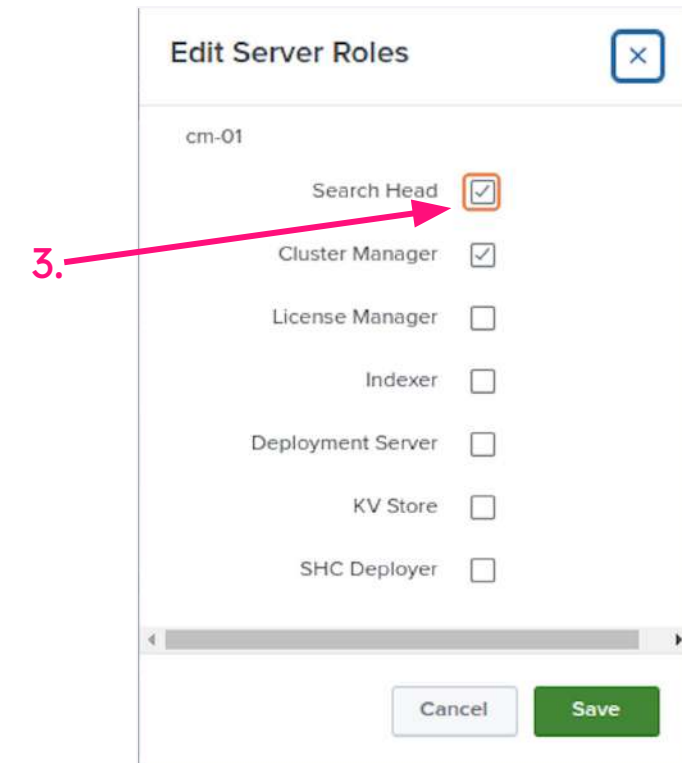
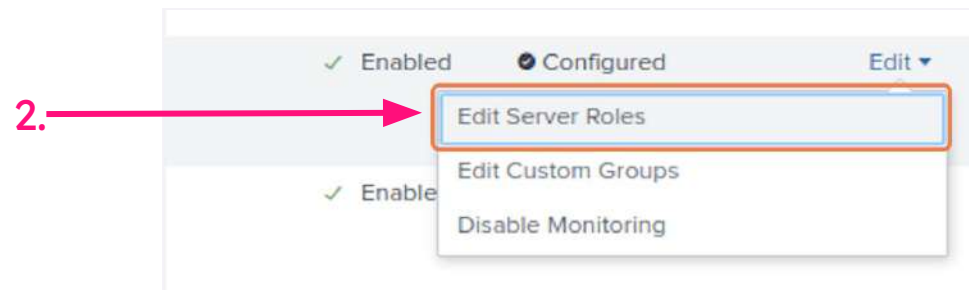
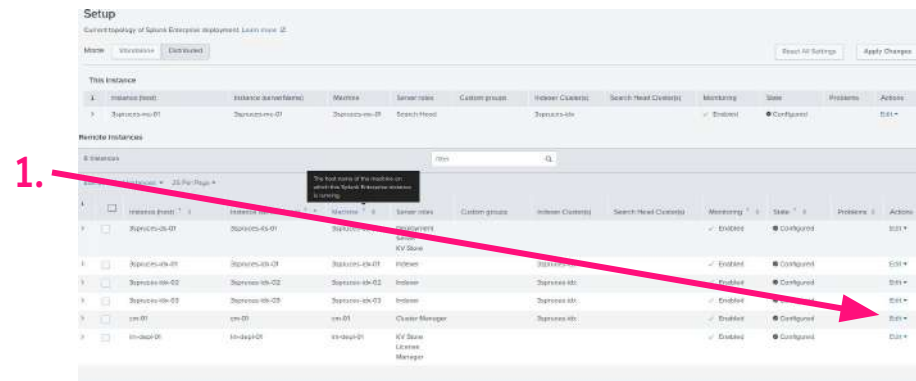
Are you sure you want to continue?

MC/CMC Overview	About the Monitoring Console - Splunk Documentation
Which should host?	https://docs.splunk.com/Documentation/Splunk/latest/DMC/WheretohostDMC
Single-instance Monitoring Console setup steps	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Singleinstancesetup

Configure and setup MC



Set the individual node "Role"



MC/CMC Overview	About the Monitoring Console - Splunk Documentation
Which should host?	https://docs.splunk.com/Documentation/Splunk/latest/DMC/WheretohostDMC
Single-instance Monitoring Console setup steps	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Singleinstancesetup

Configure and setup MC



Configure forwarder tracking

1.

Forwarders

Settings

Run a Search

General Setup

Forwarder Monitoring Setup

Alerts Setup

Overview Preferences

Health Check Items

Overview

Summary

Assist

Health Check

Instances

Indexing

Search

Forwarder Monitoring Setup

Forwarder monitoring dashboards provide information on forwarder activity and throughput. If you turn on 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

Cancel

Save

Overview

Summary

Assist

Health Check

Instances

Indexing

Search

Forwarder Monitoring Setup

Forwarder monitoring dashboards provide information on forwarder activity and throughput. If you turn on 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

Cancel

Save

Rebuild forwarder assets ...

The Monitoring Console tags as "missing" any forwarders that do not report status within 15 minutes. This information is used to identify forwarders that are not running or have stopped reporting status. You can rebuild the list of forwarder assets to remove decommissioned forwarders from the status page. This will create a new table of 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.

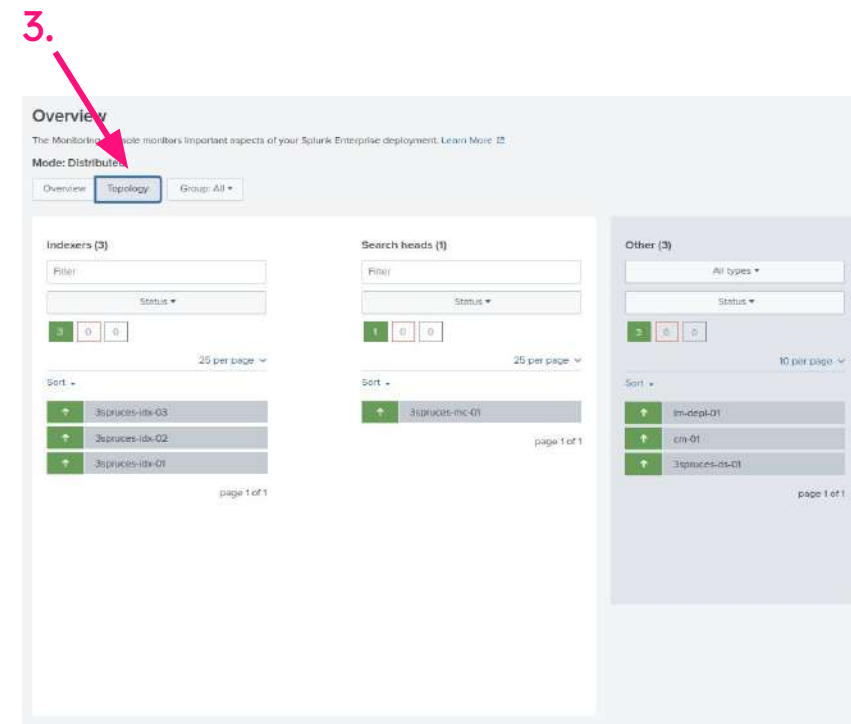
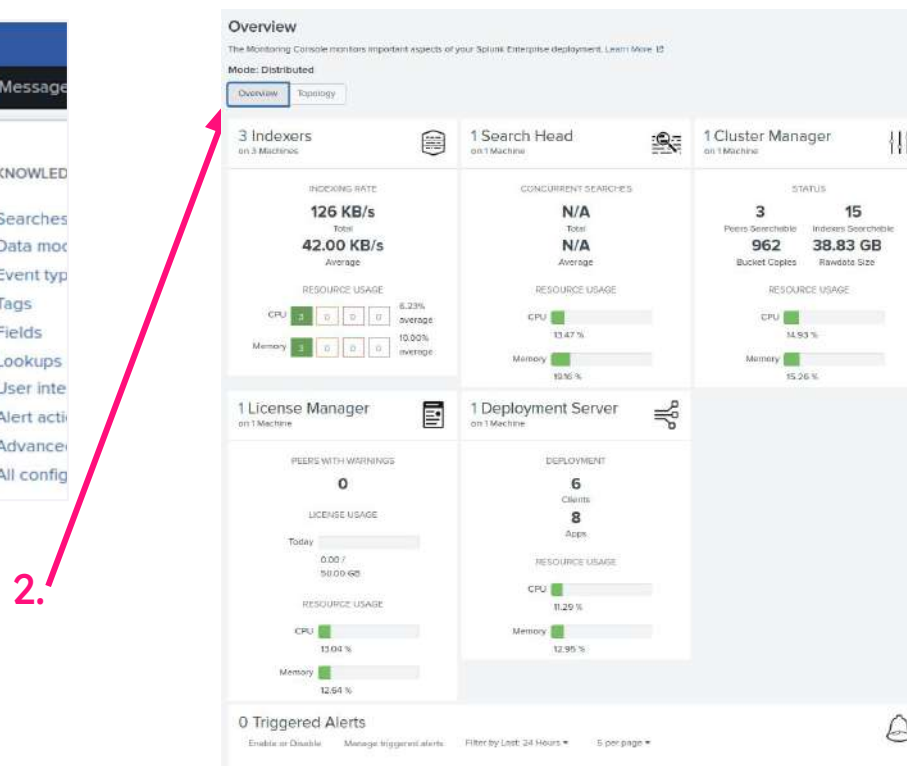
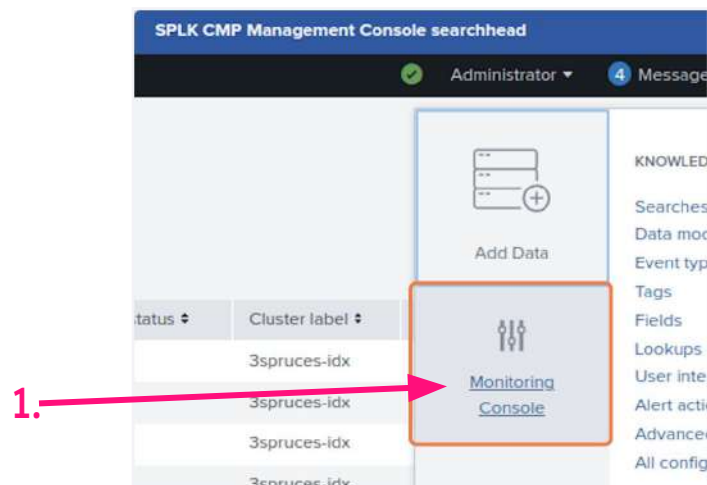
MC/CMC Overview	About the Monitoring Console - Splunk Documentation
Which should host?	https://docs.splunk.com/Documentation/Splunk/latest/DMC/WheretohostDMC
Single-instance Monitoring Console setup steps	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Singleinstancesetup

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- Dashboard Modification
- Summary

Explore Dashboards

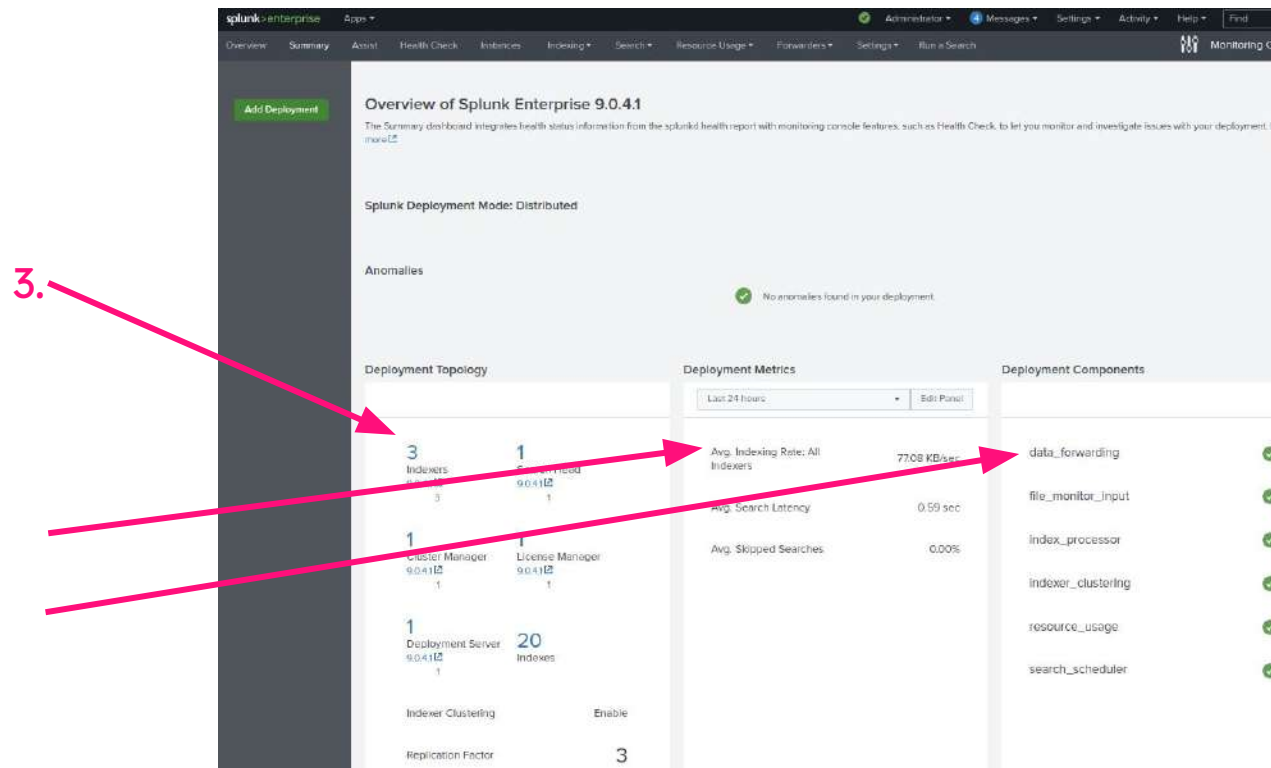
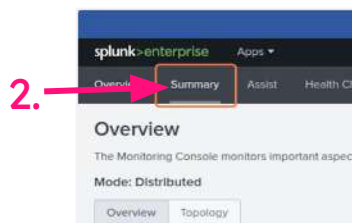
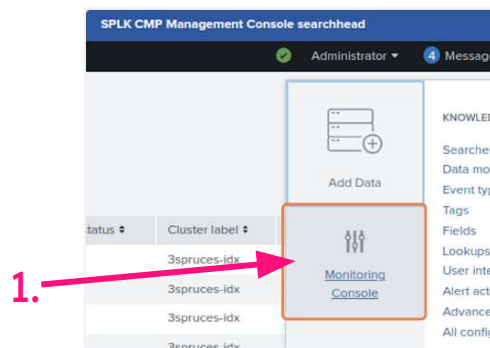
Overview & Summary



Explore Dashboards



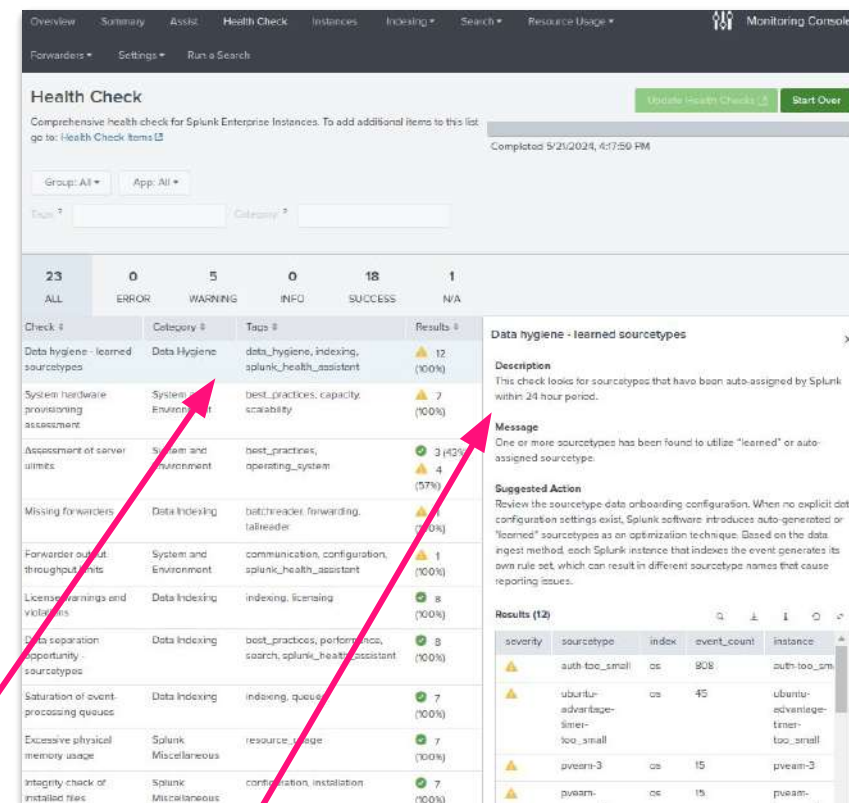
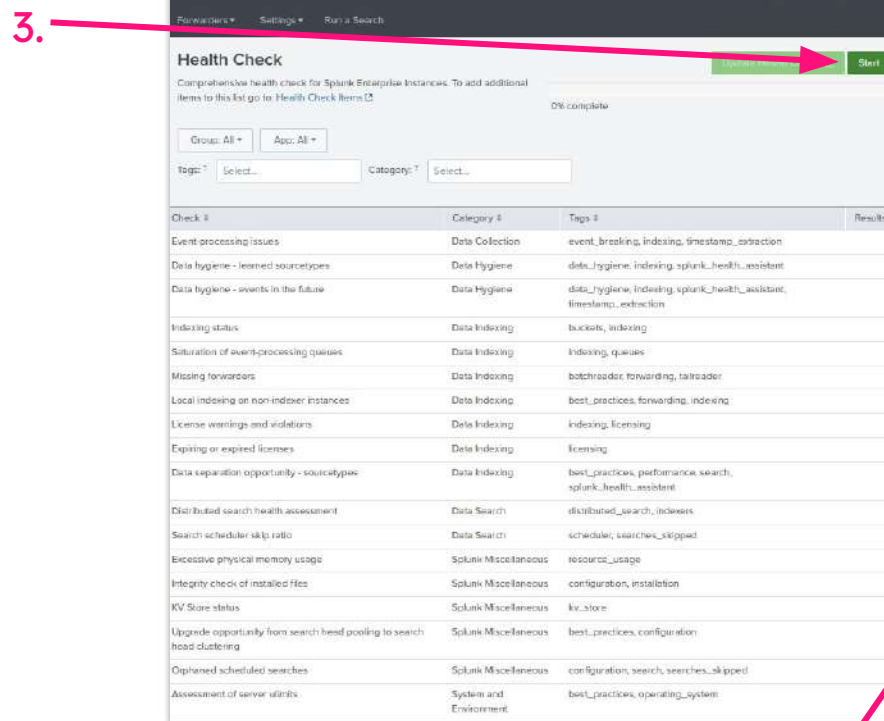
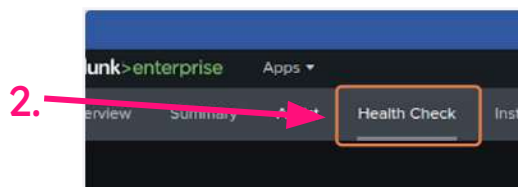
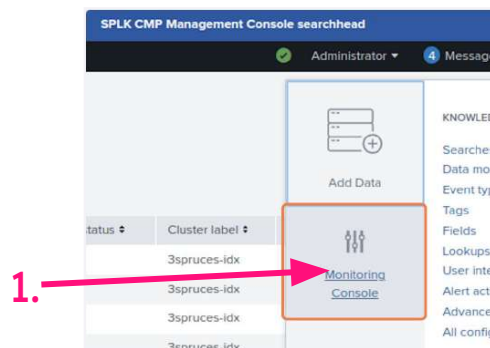
Overview & Summary



Explore Dashboards



Health Check



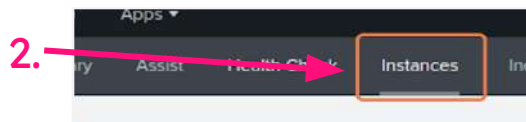
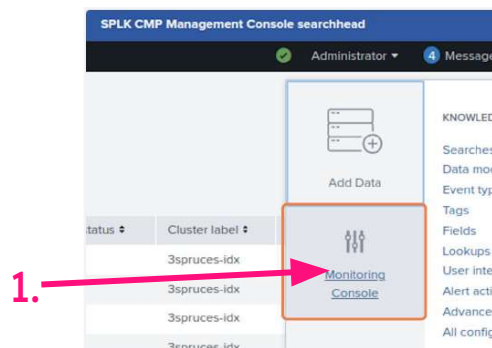
4.

5.

Explore Dashboards



Instances



Instances

Splunk Instances are listed here. [Learn More](#)

Group: All

7 instances

Instance	Machine	Role	Indexer Cluster	Search Head Cluster	OS	CPU Cores (Physical / Virtual)	RAM	Version	Status	Action
3spruces-ds-01	3spruces-ds-01	Deployment Server KV Store			Linux	2 / 2	3.83 GB	9.0.4.1	✓ Up	Views
3spruces-idx-01	3spruces-idx-01	Indexer	3spruces-idx		Linux	4 / 4	7.76 GB	9.0.4.1	✓ Up	Views
3spruces-idx-02	3spruces-idx-02	Indexer	3spruces-idx		Linux	4 / 4	7.76 GB	9.0.4.1	✓ Up	Views
3spruces-idx-03	3spruces-idx-03	Indexer	3spruces-idx		Linux	4 / 4	7.76 GB	9.0.4.1	✓ Up	Views
3spruces-mc-01	3spruces-mc-01	Search Head	3spruces-idx		Linux	4 / 4	3.83 GB	9.0.4.1	✓ Up	Views
cm-01	cm-01	Cluster Manager	3spruces-idx		Linux	2 / 2	3.83 GB	9.0.4.1	✓ Up	Views
lm-depl-01	lm-depl-01	KV Store License Manager			Linux	2 / 2	3.83 GB	9.0.4.1	✓ Up	Views

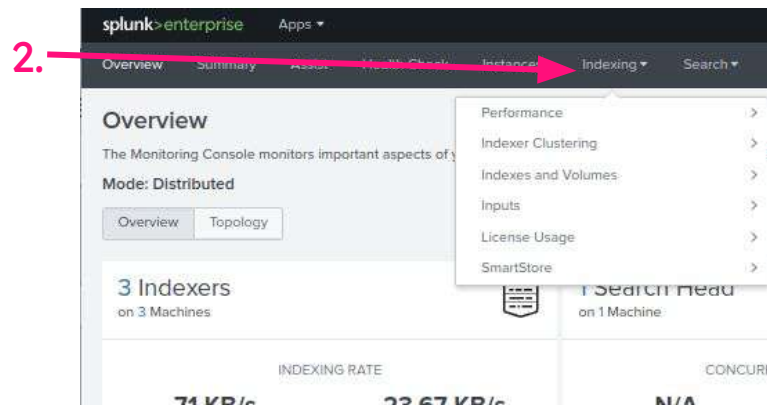
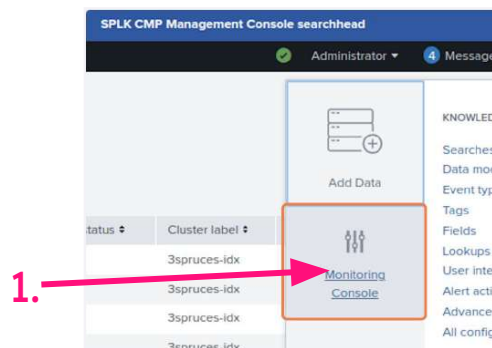
Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- **Explore Indexing - Lab 3**
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- Dashboard Modification
- Summary

Explore Dashboards



Indexing



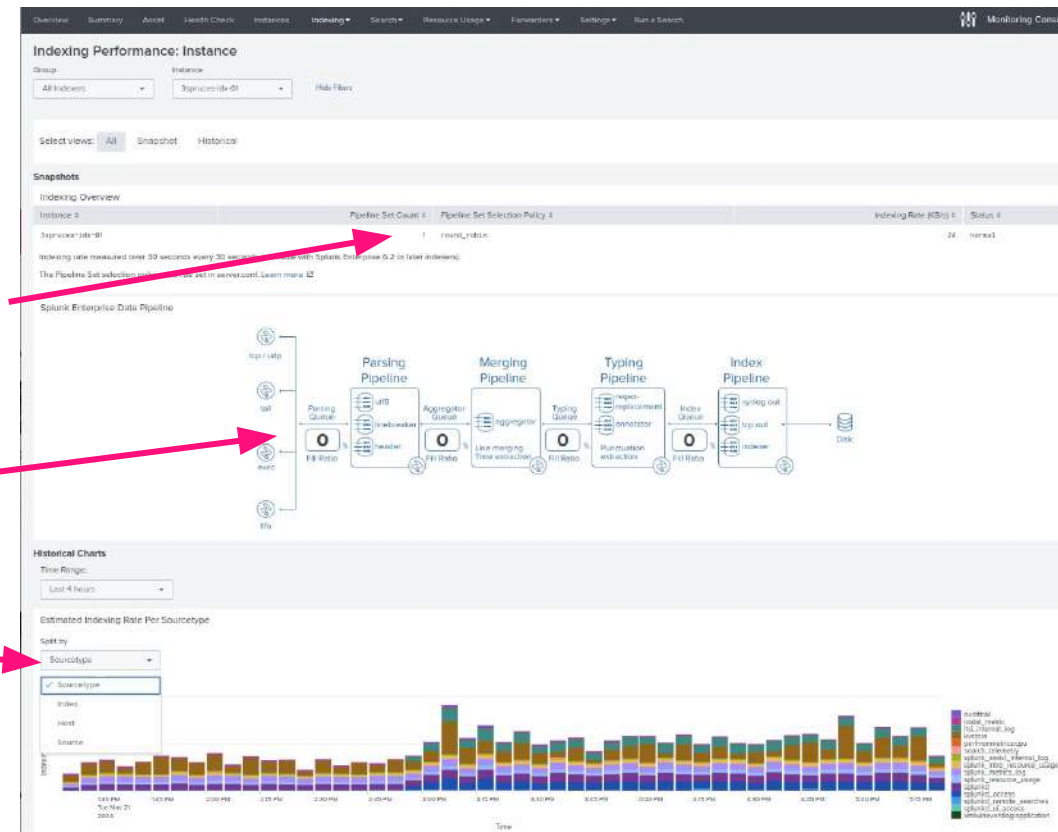
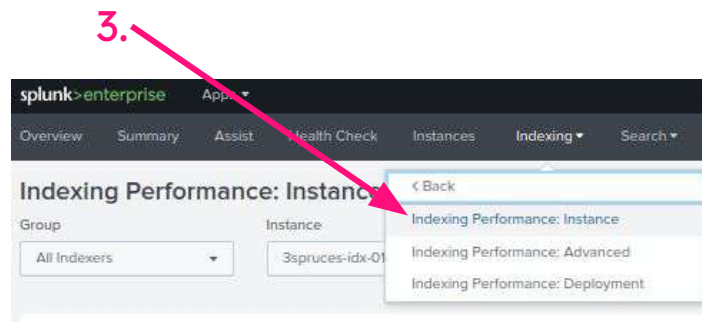
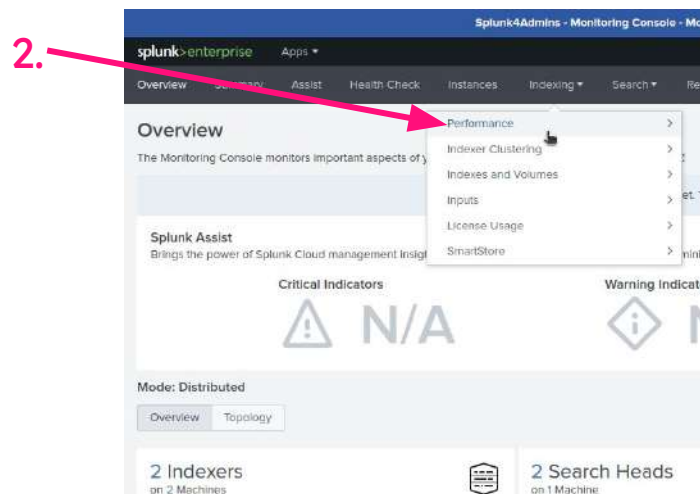
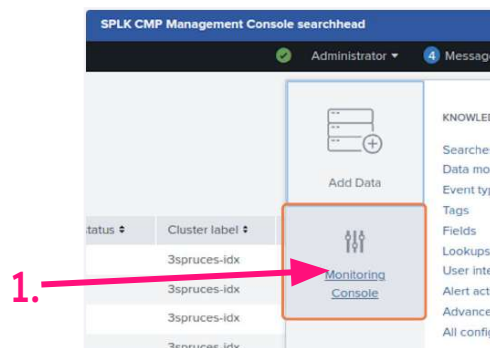
- Performance
 - Instance
 - Advanced
- Indexer Clustering
 - Status
 - Service Activity
- Indexes and Volumes
 - Instance
 - Deployment
 - Index Detail:Instance
 - Index Detail:Deployment
 - Volume Detail:Instance
 - Volume Detail:Deployment

- Inputs
 - HTTP Event Collector:Instance
 - HTTP Event Collector:Deployment
 - Splunk TCP Input
 - Performance:Instance
 - Performance:Deployment
 - Data Quality
- License Usage
 - Today
 - Historic License Usage
- SmartStore
 - Activity:Instance
 - Activity:Deployment
 - Cache Performance:Instance
 - Cache Performance:Deployment

Explore Dashboards



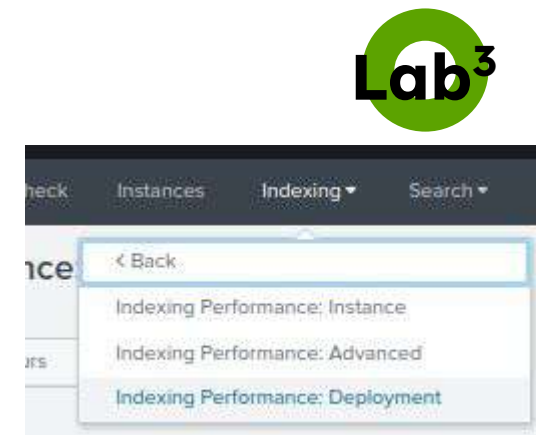
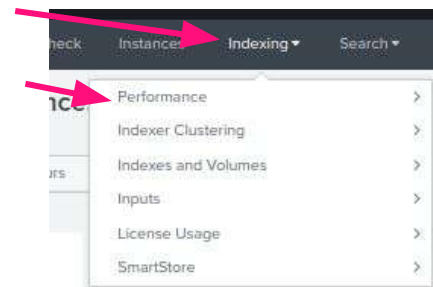
Indexing - Performance:Instance



Explore Dashboards

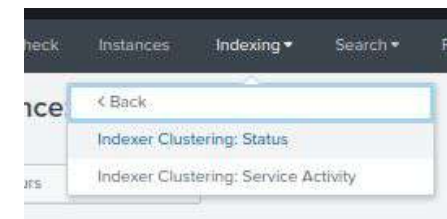
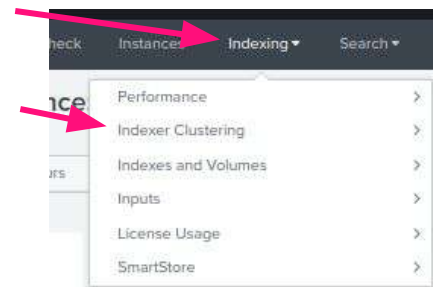
Indexing - Performance

- One of the most significant issue detection tools available
- Valuable dashboards
 - Indexing:Performance:Instance
 - Pipelines - which are above 0% full
 - Indexing rate per X - are any of the split-bys being bullies
 - Median fill rate of queues - are any showing an imbalance
 - Indexing:Performance:Deployment
 - Overview:Average/Median indexing rate - compare to individuals for imbalance
 - Indexing:Performance:Advanced
 - Aggregate CPU Seconds per Indexer Processing Activity - can be used to find where in the queue excessive workload is occurring



Explore Dashboards

Indexing - Clustering

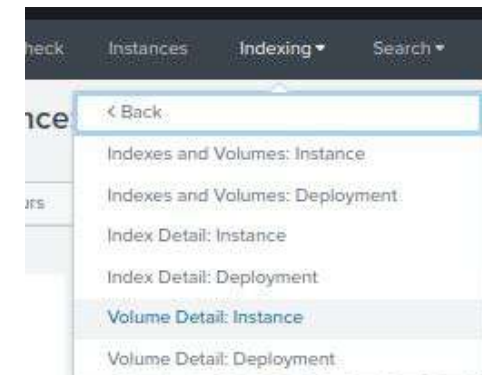
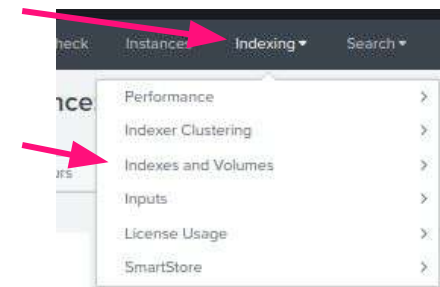


- Also important, both for understanding configuration, but also for detecting issues
- Status
 - Same as on the Cluster Manager (CM), Settings->Indexer Clustering, but there is no need to actually access the CM directly
- Service Activity
 - Most useful of the dashboards - “Warning and Error Patterns” - used to detect problems such as replication or search issues and how quickest to resolve them
 - The “Fixup Tasks” panel can be used to determine if there is additional workload due to replication issues

Indexing: Indexer Clustering: Status	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Indexerclusteringhistory
Indexing: Indexer Clustering: Service Activity	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexerclusteringServiceactivity

Explore Dashboards

Indexing - Indexes and Volumes



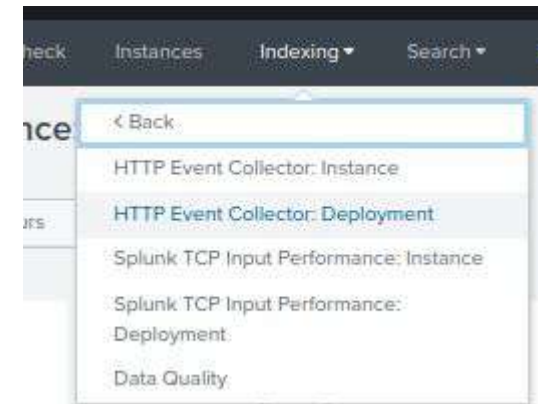
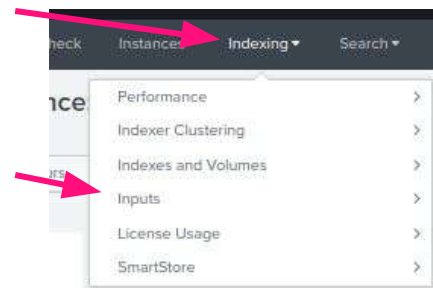
- Status and statistics related to specific instance and overall deployment size and distribution of indexes
- Detecting oversize or unbalanced indexes can help ensure fewer problems due to too few buckets hosting too much workload (split the index)
- Volume specifics - instance and deployment can help understand underlying OS volume issues (IO overload on a specific space)

Explore Dashboards

Indexing - Inputs

- Ingest monitoring

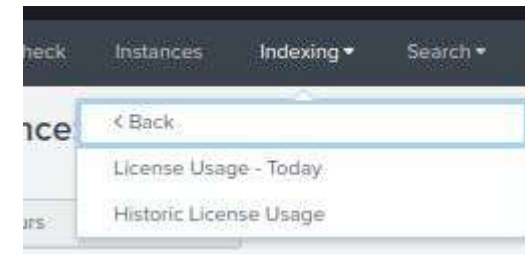
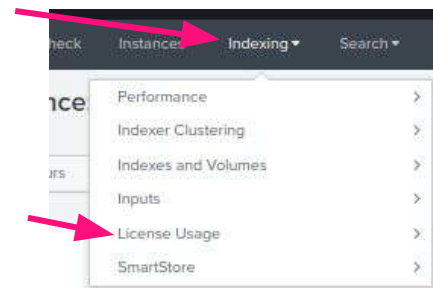
- HEC:Instance - **Events and Valid Requests Count** - load and HEC errors
- HEC:Deployment - **Data received and indexed** - load and imbalances
- Splunk TCP Input Performance:Instance - **TCP Input Queue Fill Ratio** - load and imbalances
- Data Quality - **Event Processing Issues by Source Type** - Detect misconfiguration and bullies



Indexing: Inputs: HTTP Event Collector	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Inputdashboards
Indexing: Inputs: Data Quality	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Dataquality

Explore Dashboards

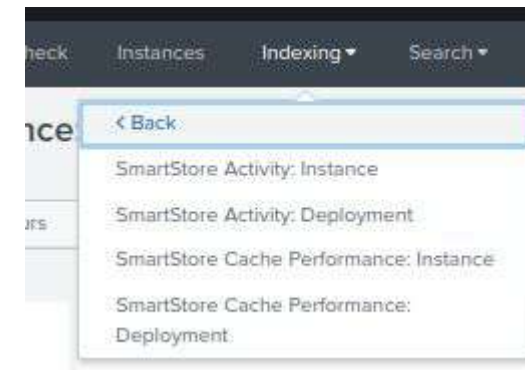
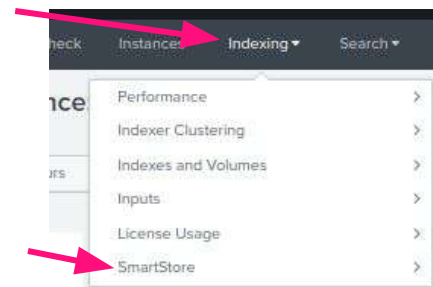
Indexing - Licensing



- Identical to the License Manager (LM) “Settings->License”
- Status and statistics related to Licensing
 - “Today” provides insight about the current licensing load
 - “Historical License Usage” allows exploration regarding trends in license load

Explore Dashboards

Indexing - SmartStore



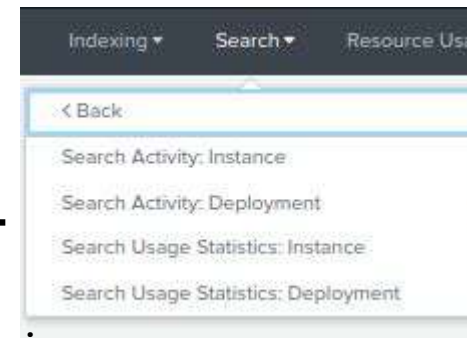
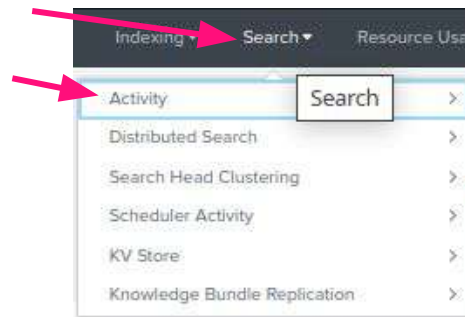
- Status and statistics related to SmartStore
- Activity and functional status for both individual indexers (instance) and the overall deployment
- Cache Performance:Instance/Deployment
 - Buckets Evicted (over time) - detects IO workload
 - Cache Hits/Missed - provides insight into how well-sized the local disk cache is
 - Cache Thrash by Index - provides insight into whether the local cache is size appropriately based on search load

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- **Explore Search - Lab 4**
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- Dashboard Modification
- Summary

Explore Dashboards

Search - Activity

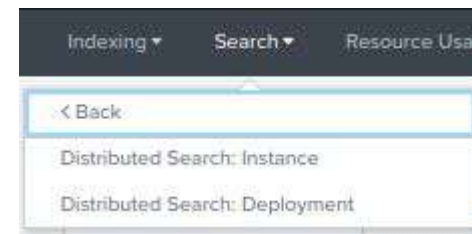
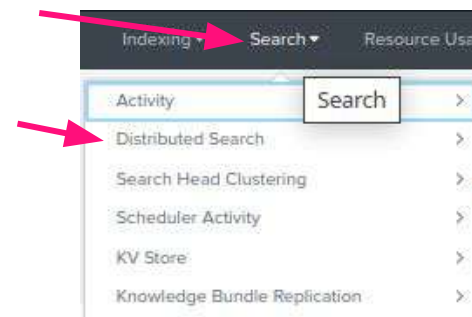


- Statistics related to search, both instance and deployment
 - Activity:Instance and Deployment
 - **Concurrency | Median Search Concurrency** - useful to determine how many searches are running and using too many slots (bullies)
 - **Top 20 Memory Consuming Searches** - inefficient searches degrade all performance
 - **Frequently run searches** - find heavily used searches, cross-reference with “Top 20 Memory” or CPU usage to determine efficiency and bullying
 - **Long-running searches** - find searches that run for an extended time and cross reference for “Top 20 Memory” or CPU usage to determine efficiency and bullying
 - Usage Statistics:Instance and Deployment
 - **Frequently run searches** - find heavily used searches, cross-reference with “Top 20 Memory” or CPU usage to determine efficiency and bullying
 - **Long-running searches** - find searches that run for an extended time and cross reference for “Top 20 Memory” or CPU usage to determine efficiency and bullying

Search: Search Activity	https://docs.splunk.com/Documentation/Splunk/latest/DMC/SearchactivityDeploymentwide
Search: Search Usage Statistics	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Searchusagestatistics
Optimizing 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-optimize-a-long-running-search/m-p/551040

Explore Dashboards

Search - Distributed Search

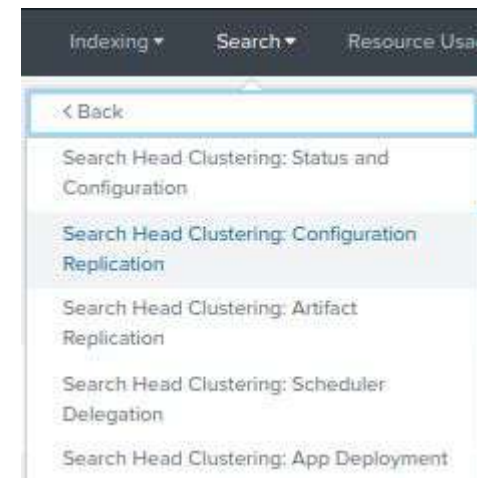
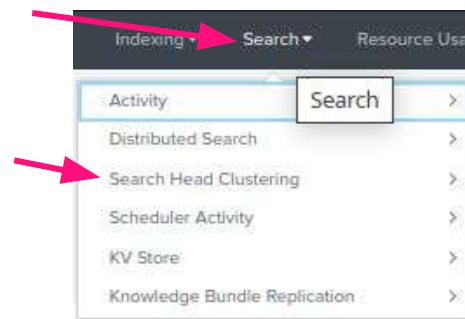


- Statistics related to Distributed Search against the indexers, both instance and across the fleet
 - Distributed Search:Instance and Deployment
 - Summary and statistics of Distributed Search configuration
 - **Peer Heartbeat** - discover if there are communication issues between the search head and the search peers. This will slow down all searches
 - Knowledge Bundle Replication statistics and Upload activity

Explore Dashboards

Search - Search Head Clustering

- Status and Configuration
 - Configuration summaries and Historical information for determining trends in status
- Configuration Replication
 - Warning and Error Patterns allow discovery of issues over time
- Search Artifact Replication
 - Statistics and “Warnings and Errors” - information about possible issues or problems
- Search Scheduler Delegation and Activity
 - Insights about delegating savedsearches by the Captain
- App Deployment
 - Status, issues, and requests related to deploying Splunk Apps from the deployer out to the members of the cluster



Search: Search Head Clustering	https://docs.splunk.com/Documentation/Splunk/latest/DMC/SHCdashboards
Search Head Clustering	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/SHCarchitecture

Explore Dashboards

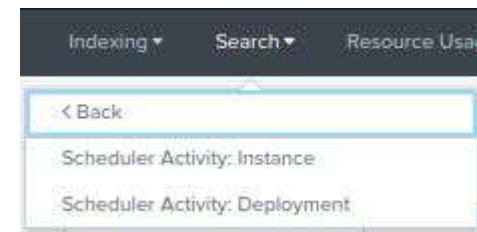
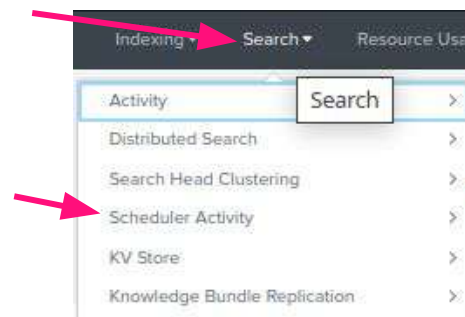
Search - Scheduler Activity

○ Instance

- Many pieces of useful and important information regarding scheduled searches, including concurrency, number of scheduled searches, aggregate search time, runtime statistics ...
- Most useful
 - **Count of Skipped Scheduled Reports** - highly relevant as skipped reports mean that summaries or other aggregation searches are not running, can be indicative of different types of problem
 - **Count of Skipped Reports by Name Reason** - more definition of which searches are being skipped
 - **Count of Skipped Reports over Time** - discover time-based trending “Did something change at a point in time and cause more skips?”

○ Deployment

- The same information, but related to the deployment (Search Head Cluster as a whole)



Search: Scheduler Activity	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Scheduleractivity
Reducing skipped searches	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Searching_and_Reporting/Reducing_skipped_searches
Are You Skipping? Please Read!	https://www.splunk.com/en_us/blog/tips-and-tricks/are-you-skipping-please-read.html

Explore Dashboards

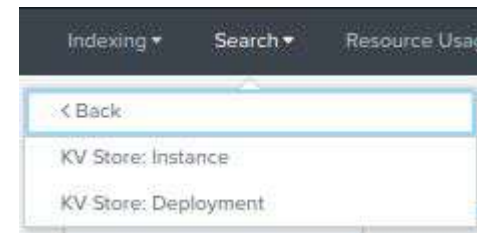
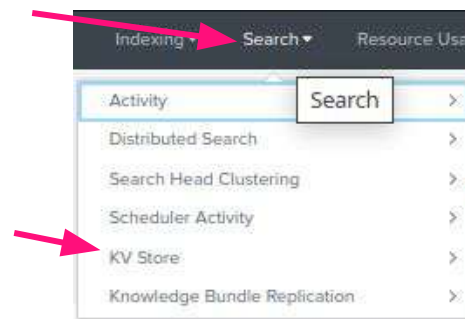
Search - KV Store

○ Instance

- Status and statistics related to KV Store operations
 - Warnings and Error Patterns, Page Faults/operation, Network Traffic, Size of Queue, many more.
 - **Instances by Average Replication Latency** - KV Stores are replicated among the members of a cluster. Latency can cause searches to return different values, and therefore is an indicator of potential issues. Note this value and compare the over-time trend to determine if the replication is slowing. Can be due to size of package or network issues.

○ Deployment

- The same information, but related to the deployment (Search Head Cluster as a whole)



Explore Dashboards

Search - Knowledge Bundle Replication

Knowledge Bundle Replication

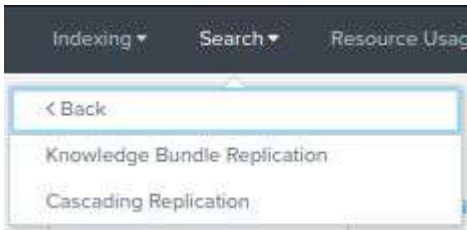
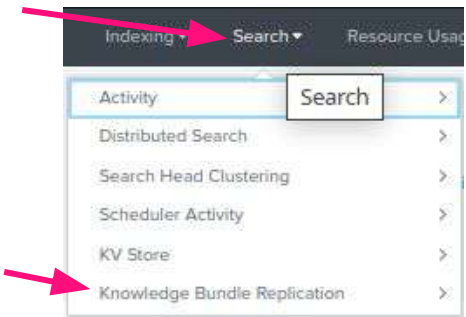
Status and statistics

- Replication Policy, threads, Latest Common Bundle, Bundle size statistics
- **Average Full Bundle Replication Time** - Similar to KV Store, search moves all of the relevant Knowledge Objects to the indexer to ensure accurate searches. This can be time consuming. Initially, a full bundle is replicated to the indexer
- **Average Delta Bundle Replication Time** - Once a full bundle has been replicated, the search head tracks what has been changed, and will only send deltas from then on.
- For both Full and Delta Replication, time is an excellent indicator. If the sizes haven't changed, but time does, this is an indicator
- Historical section - Use this to understand prior replication behavior (time, latency, bundle size) to determine what cause change in replication

Deployment

- The same information, but related to the deployment (Search Head Cluster as a whole)

Search: Knowledge Bundle Replication	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Knowledgebundlereplication
Knowledge bundle replication overview	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Knowledgebundlereplication
Optimizing Splunk knowledge bundles	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Searching_and_Reporting/Optimizing_Splunk_knowledge_bundles



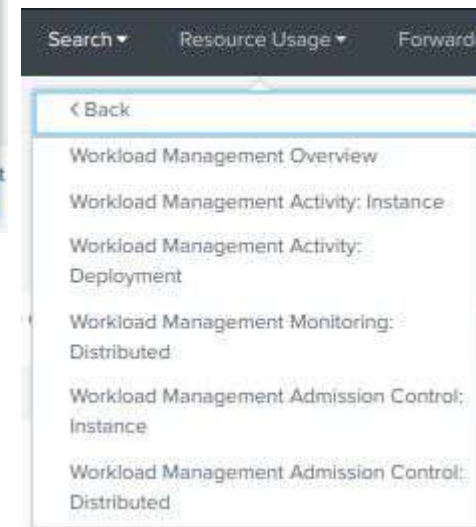
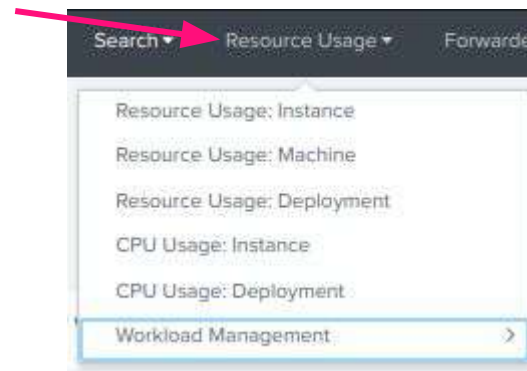
Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Resource Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- Dashboard Modification
- Summary

Explore Dashboards

Resource Usage

- Instance - Machine information
- Machine/Deployment - Performance statistics
 - Disk Space Usage
 - IO Usage and Performance
 - CPU usage and saturation
 - IO Usage by Mount Point (instance)
- CPU Usage:Instance/Deployment
 - In-depth CPU statistics, relevant when other insights lead to over subscription of CPUs
- Workload Management
 - A group of dashboards with configuration and statistics for the use of the Workload Management function



Resource Usage	https://docs.splunk.com/Documentation/Splunk/latest/DMC/ResourceusageDeployment
Resource Usage: CPU Usage	https://docs.splunk.com/Documentation/Splunk/latest/DMC/ResourceusageCPU

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- **Explore Forwarders - Lab 6**
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- Dashboard Modification
- Summary

Explore



Detect:Forwarders

- One of the forwarders is out of date ... where to discover information as to why?

Explore



Detect:Forwarders

- One of the forwarders is out of date ... where to discover information as to why?

Forwarders: Instance
✓ Forwarders: Deployment

Total: 2

Instance	Type	Version	OS	Architecture	Status	Last Connected to Indexers	Total KB	Average KB/s Over Time	Average KB/s	Average Events/s
s4a-mc-OutOfDate-splunkforwarder	Universal Forwarder	7.1.1	Linux	x86_64	active	08/07/2024 16:29:42 +0000	953.78		2.44	0.58
s4a-mc-forwarder	Universal Forwarder	9.2.2	Linux	x86_64	active	08/07/2024 16:29:42 +0000	251.67		0.28	0.49

Forwarders in the Monitoring Console	https://docs.splunk.com/Documentation/Splunk/latest/DMC/ForwardersDeployment
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

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- **Discover: Detect “Skipped searches” - Lab 7**
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- Dashboard Modification
- Summary

Detect



Skipped Searches

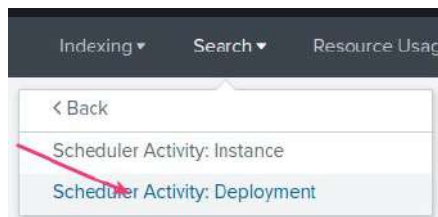
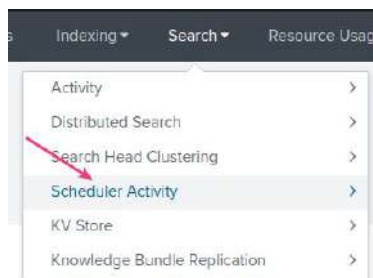
- Users are reporting that alerts are not firing, apparently due to missing search results ...

Detect



Skipped Searches

- Users are reporting that some alerts are not firing, apparently due to missing search results ...



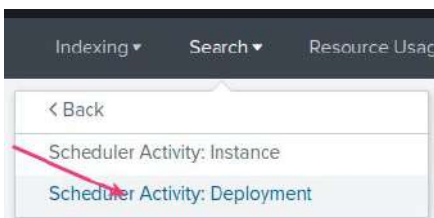
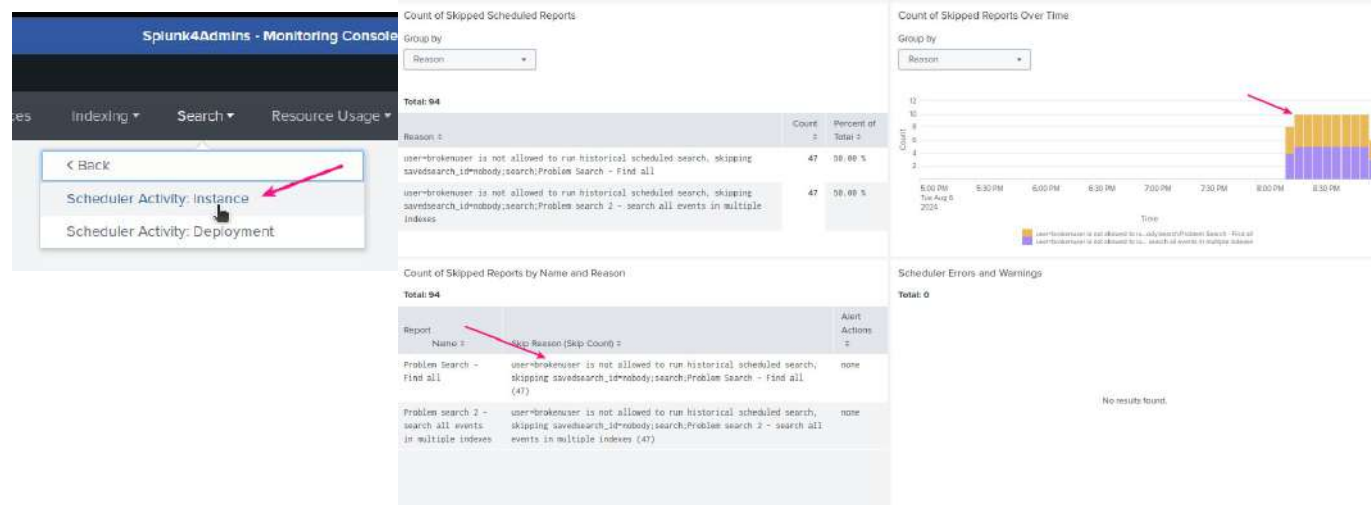
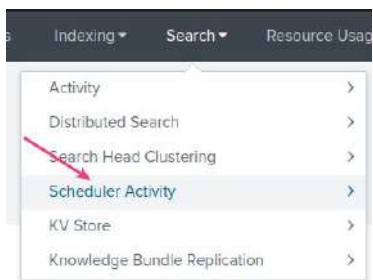
Search: Scheduler Activity	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Scheduleractivity
Reducing skipped searches	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Searching_and_Reporting/Reducing_skipped_searches
Are You Skipping? Please Read!	https://www.splunk.com/en_us/blog/tips-and-tricks/are-you-skipping-please-read.html

Detect

Skipped Searches



- Users are reporting that some data is missing from certain dashboards ... Search - Scheduler Activity:Deployment and then :Instance



Search: Scheduler Activity

<https://docs.splunk.com/Documentation/Splunk/latest/DMC/Scheduleractivity>

Reducing skipped searches

https://lantern.splunk.com/Splunk_Platform/Product_Tips/Searching_and_Reporting/Reducing_skipped_searches

Are You Skipping? Please Read!

https://www.splunk.com/en_us/blog/tips-and-tricks/are-you-skipping-please-read.html

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- **Discover: Detect “Indexer is not indexing data” - Lab 8**
- Discover: Detect “Best Practices misconfiguration” - Lab 9
- Dashboard Modification
- Summary

Detect



Indexer is not indexing data

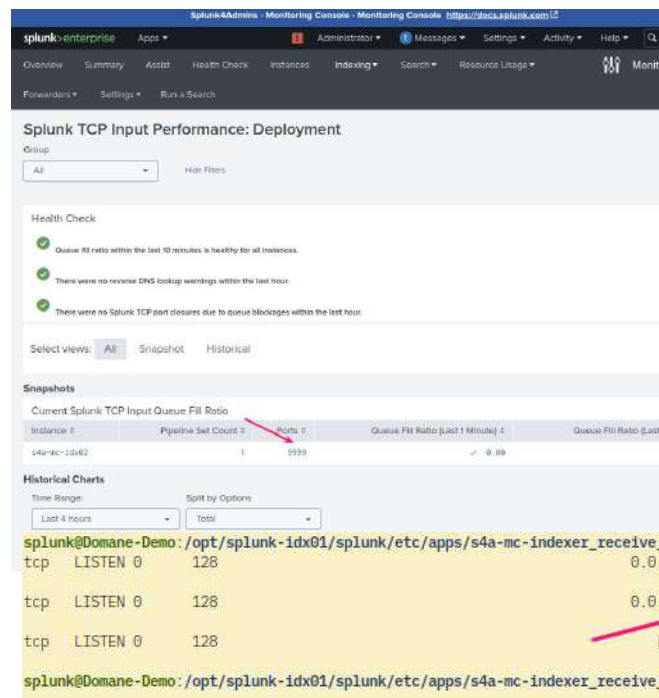
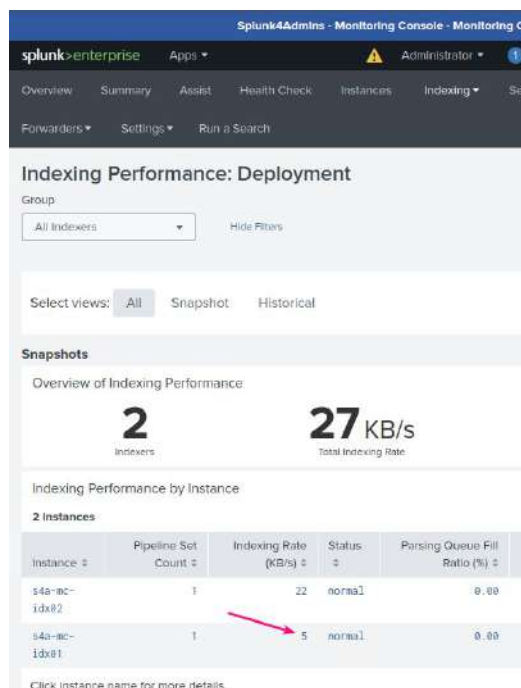
- It appears that one indexer is NOT ingesting data. Why?

Detect



Indexer is not indexing data

- It appears that one indexer is NOT ingesting data. Why?



```
splunk@Domane-Demo:/opt$ more /opt/splunk-idx0*/splunk/etc/apps/s4a-mc-indexer_receive_idx0*/local/inputs.conf
.....
/opt/splunk-idx01/splunk/etc/apps/s4a-mc-indexer_receive_idx01/local/inputs.conf
.....
#[splunktcp://9998]
#disabled = 0
.....
/opt/splunk-idx02/splunk/etc/apps/s4a-mc-indexer_receive_idx02/local/inputs.conf
.....
[splunktcp://9999]
disabled = 0
```

```
splunk@Domane-Demo:/opt/splunk-idx01/splunk/etc/apps/s4a-mc-indexer_receive_idx01/local$ ss -anlpo | grep LISTEN | grep -E '2222|9998|9999'
tcp LISTEN 0 128 0.0.0.0:9999 0.0.0.0:* users:((("splunkd",pid=11524,fd=74))
tcp LISTEN 0 128 0.0.0.0:2222 0.0.0.0:*
tcp LISTEN 0 128 [::]:2222 [::]:*
```

Workshop Agenda

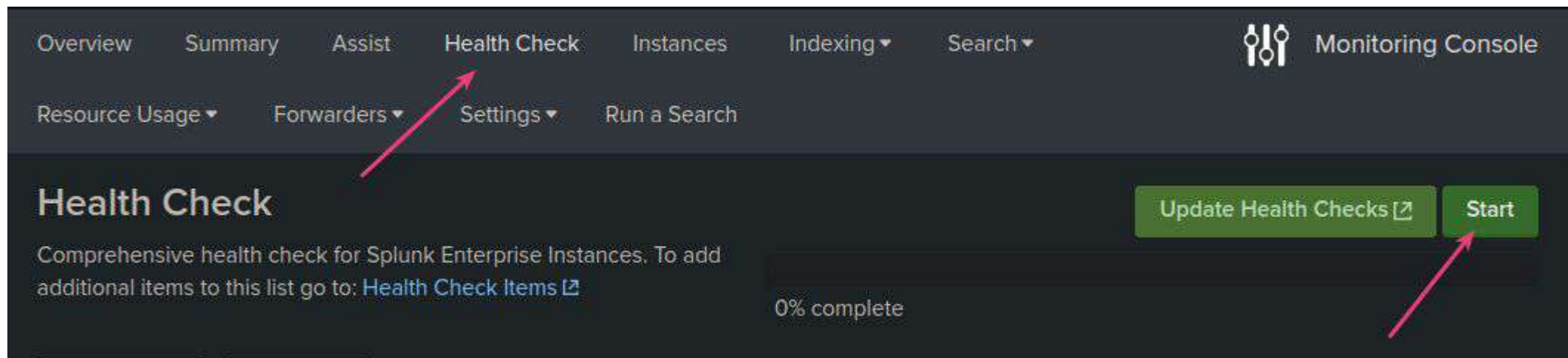
- Discuss Who? What? Why?
- Expectations
- What is an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- **Discover: Detect “Misconfigured file descriptors” - Lab 9**
- Dashboard Modification
- Summary

Detect



Health Check misconfiguration discovered

- Running the Health Check has discovered an issue.



Detect



Health Check misconfiguration discovered

- Best Practices
 - Splunk requires certain OS limits
 - Open file descriptors, number of possible user processes, data segment size
 - Several others ...

Splunk4Admins - Monitoring Console - Monitoring Console <https://docs.splunk.com>

splunk>enterprise Apps

Overview Summary Assist Health Check Instances Indexing Search Resource Usage Forwarders Settings Run a Search

Health Check

Comprehensive health check for Splunk Enterprise Instances. To add additional items to this list go to: [Health Check Items](#)

Group: All App: All

Tags: Category:

18	0	3	0	15	4
ALL	ERROR	WARNING	INFO	SUCCESS	N/A
Check	Category		Tags		Results
Assessment of server ulimits	System and Environment		best_practices, operating_system		1 (20%) 4 (80%)
Integrity check of installed files	Splunk Miscellaneous		configuration, installation		1 (20%) 3 (60%)
Search scheduler skip ratio	Data Search		scheduler, searches_skipped		1 (50%) 1 (50%)

Detect



Health Check misconfiguration discovered

- Discovering these sorts of issues is easy with Monitoring Console

Health Check

Comprehensive health check for Splunk Enterprise instances. To add additional items to this list go to: Health Check Items

Group: All App: All

Tags: Category:

18 ALL 0 ERROR 3 WARNING 0 INFO 15 SUCCESS 3 N/A

Check	Category	Tags	Results
Integrity check of installed files	Miscellaneous	configuration, installation	1 (20%) (80%)
Assessment of server ulimits	System and Environment	best_practices, operating_system	1 (20%) (80%)
Search scheduler skip ratio	Data Search	scheduler, searches_skipped	1 (50%) (50%)
Saturation of event-processing queues	Data Indexing	indexing, queues	5 (100%)
Excessive physical memory usage	Miscellaneous	resource_usage	5 (100%)
Orphaned scheduled searches	Splunk	configuration, search, searches_skipped	5 (100%)
System hardware provisioning assessment	System and Environment	best_practices, capacity, scalability	5 (100%)
Linux kernel transparent huge pages	System and Environment	best_practices, operating_system	5 (100%)
Near-critical disk usage	System and Environment	capacity, disk_space, searches_skipped, storage	4 (100%)
Local indexing on non-indexer instances	Data Indexing	best_practices, forwarding, indexing	3 (100%)
Distributed search health assessment	Data Search	distributed_search, indexes	3 (100%)
KV Store status	Splunk	kv_store	3 (100%)

Assessment of server ulimits

Description: This checks whether the machine is provisioned with ulimit settings (file descriptors, user processes, and data segment size) that are adequate for running Splunk software.

Message: One or more Splunk instances are running on a host that has one or more resource limits set below official recommendations.

Suggested Action: Persistently modify resource limits per documented best practices.

Links: Learn more about Splunk software ulimit requirements.

severity	instance	ulimits.data_segment_size (current / recommended)	ulimits.open_file (current / recommended)
Warning	s4a-mc-sh	-1 / 20000000000	12000 / 64000
Success	s4a-mc-mc	-1 / 20000000000	64000 / 64000
Success	s4a-mc-idx02	-1 / 20000000000	64000 / 64000
Success	s4a-mc-idx01	-1 / 20000000000	64000 / 64000

Results (5)




severity	instance	ulimits.data_segment_size (current / recommended)	ulimits.open_file (current / recommended)
Warning	s4a-mc-sh	-1 / 20000000000	12000 / 64000
Success	s4a-mc-mc	-1 / 20000000000	64000 / 64000
Success	s4a-mc-idx02	-1 / 20000000000	64000 / 64000
Success	s4a-mc-idx01	-1 / 20000000000	64000 / 64000

Detect



Health Check misconfiguration discovered

- Monitoring Console makes it easy to detect
- Many Best Practice settings are configured in Health Check
- These should be set in systemd unit-files
- More can be configured

severity	instance	ulimits.data_segment_size (current / recommended)	ulimits.open_files (current / recommended)	ulimits.user_processes (current / recommended)
	3spruces-mc-01	-1 / 1073741824	65536 / 64000	15315 / 16000
	cm-01	-1 / 1073741824	65536 / 64000	15317 / 16000
	lm-depl-01	-1 / 1073741824	65536 / 64000	15317 / 16000

Workshop Agenda

- Discuss Who? What? Why?
- Expectations
- What is an Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- **Dashboard Modification**
- Summary

Dashboard Modification

Localization

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

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 Enterprise Monitoring Console?
- Set up Monitoring Console in Distributed Mode|Settings tab - Lab 1
- Explore Overview|Summary|Health Check|Instances - Lab 2
- Explore Indexing - Lab 3
- Explore Search - Lab 4
- Explore Research Usage - Lab 5
- Explore Forwarders - Lab 6
- Discover: Detect “Skipped searches” - Lab 7
- Discover: Detect “Indexer is not indexing data” - Lab 8
- Discover: Detect “Misconfigured file descriptors” - Lab 9
- Dashboard Modification
- Summary

Summary

Covered a great deal ...

- Learn MC 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
- Be sure to monitor performance on the MC
 - Architecture matters

Links

Also in Lab Guide

Title	Link
MC/CMC Overview	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Which should host?	https://docs.splunk.com/Documentation/Splunk/latest/DMC/WheretohostDMC
Splunk Assist	https://docs.splunk.com/Documentation/Splunk/latest/DMC/AssistIntro
Splunk Monitoring Console Health Check	https://docs.splunk.com/Documentation/Splunk/latest/InheritedDeployment/Systemhealth
How the Monitoring Console works	https://docs.splunk.com/Documentation/Splunk/latest/DMC/HowtheDMCworks
Summary	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Summary
Indexing: Performance	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexingDeployment
Indexing: Indexes and Volumes	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexingIndexesandvolumes
Indexing: Inputs: HTTP Event Collector	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Inputdashboards
Indexing: Inputs: Data Quality	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Dataquality
Indexing: License Usage	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCLicensing
Indexing: SmartStore	https://docs.splunk.com/Documentation/Splunk/latest/DMC/SmartStore
Indexing: Indexer Clustering: Status	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Indexerclusteringhistory
Indexing: Indexer Clustering: Service Activity	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexerclusteringServiceactivity
Search: Search Activity	https://docs.splunk.com/Documentation/Splunk/latest/DMC/SearchactivityDeploymentwide
Search: Search Usage Statistics	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Searchusagestatistics
Search: KV Store	https://docs.splunk.com/Documentation/Splunk/latest/DMC/KVStoreDeployment
Search: Scheduler Activity	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Scheduleractivity
Search: Distributed Search	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Distributedsearchdashboards
Search: Knowledge Bundle Replication	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Knowledgebundlereplication
Search: Search Head Clustering	https://docs.splunk.com/Documentation/Splunk/latest/DMC/SHCdashboards

Title	Link
Resource Usage	https://docs.splunk.com/Documentation/Splunk/latest/DMC/ResourceusageDeployment
Resource Usage: CPU Usage	https://docs.splunk.com/Documentation/Splunk/latest/DMC/ResourceusageCPU
Forwarders in the Monitoring Console	https://docs.splunk.com/Documentation/Splunk/latest/DMC/ForwardersDeployment
Optimizing 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-optimize-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
Knowledge bundle replication overview	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Knowledgebundlereplication
Optimizing Splunk knowledge bundles	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Searching_and_Reporting/Optimizing_Splunk_knowledge_bundles
Forwarder Management Overview	https://docs.splunk.com/Documentation/Splunk/latest/Updating/Forwardermanagementoverview
How to manage a lot of forwarder agents	https://community.splunk.com/t5/Monitoring-Splunk/How-to-manage-a-lot-of-forwarder-agents/m-p/549800
Single-instance Monitoring Console setup steps	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Singleinstancesetup
Identify and triage indexing performance problems	https://docs.splunk.com/Documentation/Splunk/latest/Troubleshooting/Troubleshootingindexingperformance
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