Splunk4Admins - Monitoring Console

Lab Guide

Overview

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

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

Prerequisites

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

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

⚠️ Troubleshooting Connectivity

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

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

Table of Contents

Exercise 1 – Setup Monitoring Console in Distributed Mode

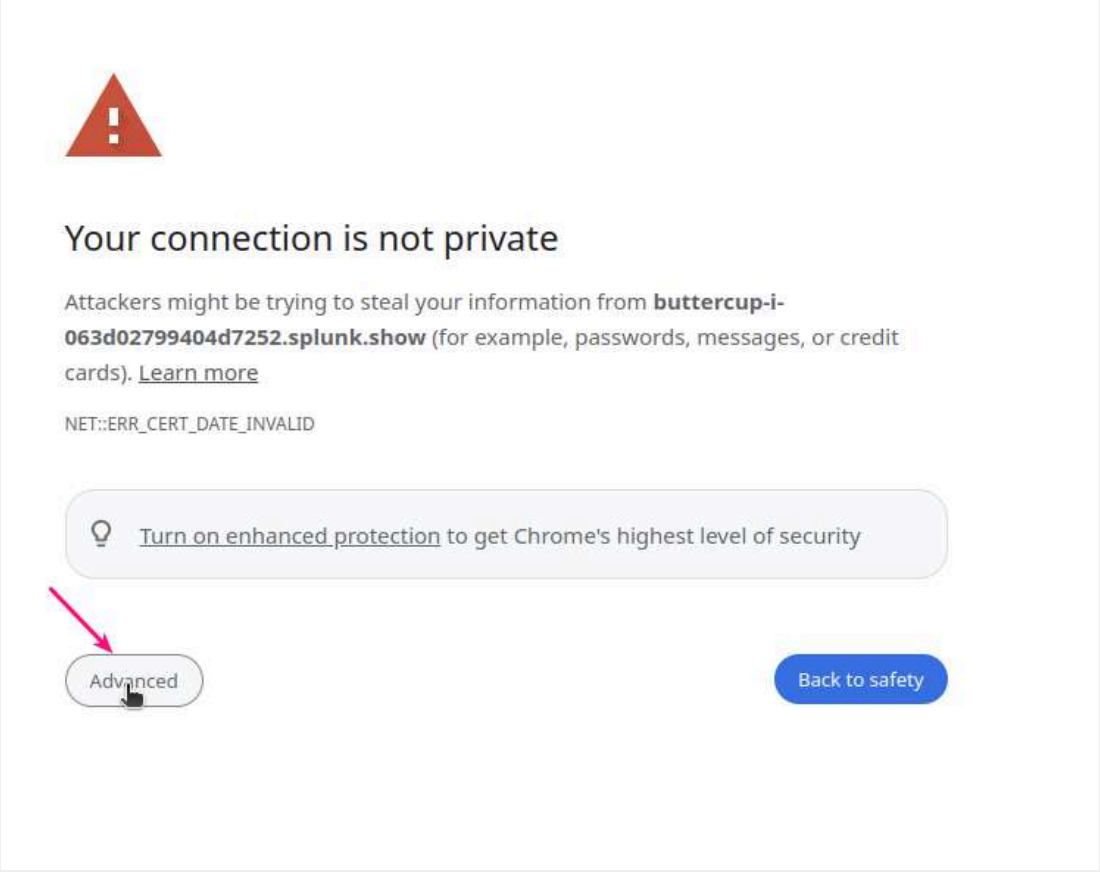
Description

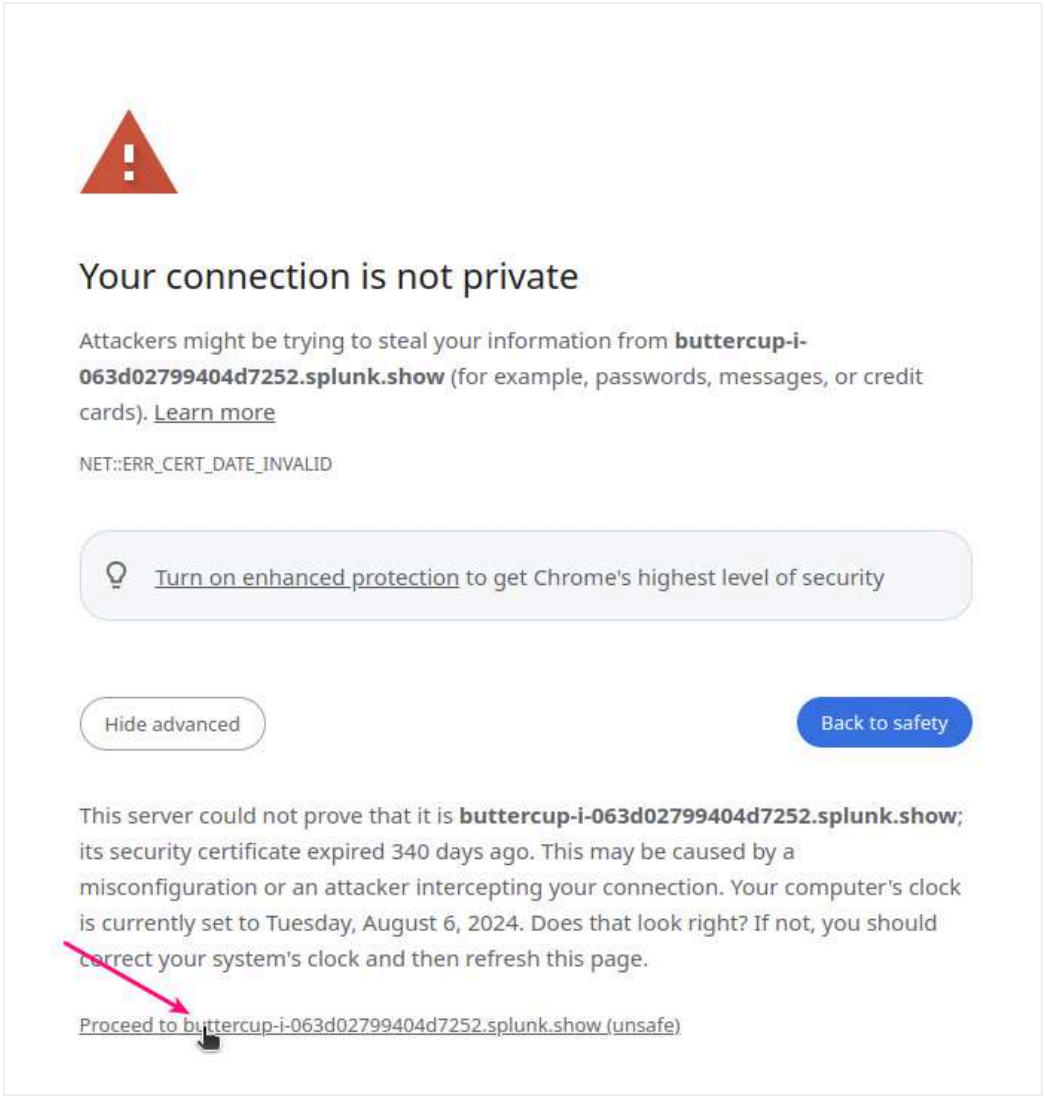
Configure the Monitoring Console (MC) in Distributed Mode. Connect the MC to all of the resources in the Splunk environment to allow effective monitoring. Each of the members of the Splunk environment (search heads, cluster manager, indexers) must be configured as peers to allow information to flow back to the MC node.

Steps

Access the Monitoring Console node

1. At https://<your_assigned_IP:4500" <- the port matters
2. Due to constraints within the lab environment, the connections will be unencrypted and unvalidated. This is not an issue, as nothing of value is passed, but you will see the following screen. Click on the "Advanced" button and then "Proceed" at the bottom of the prompt …

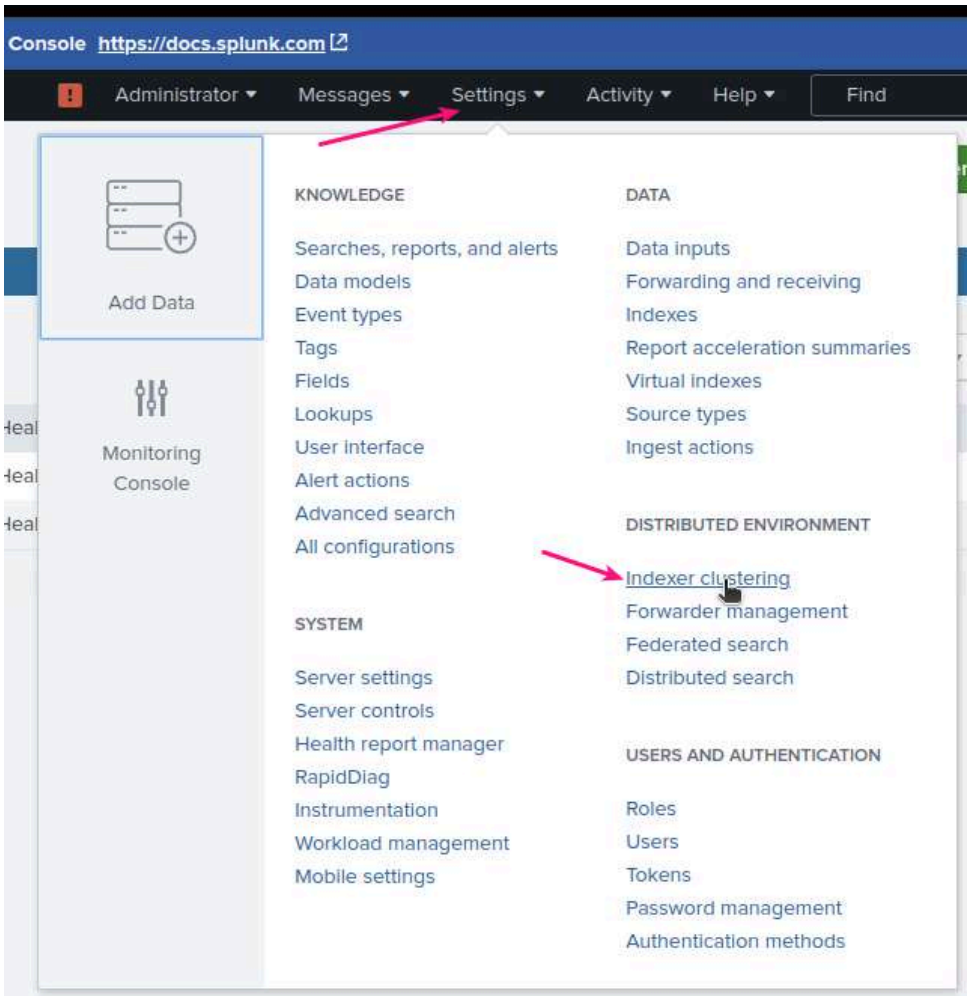




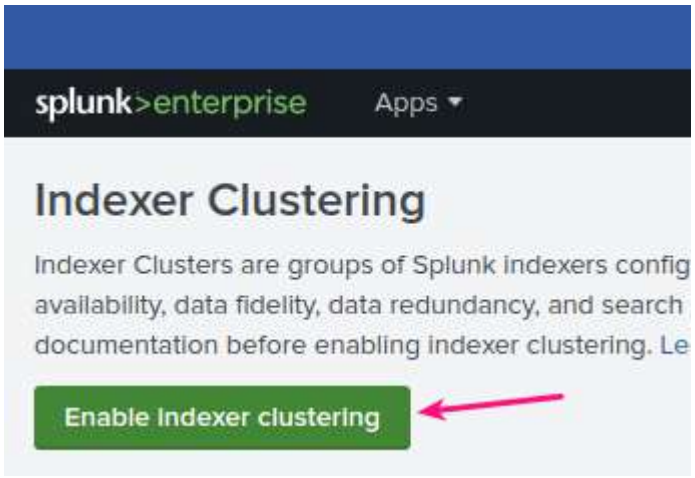
3. Type “admin” in the username field and the “5p1unk.conf” in the password field

4. Click on “Sign In”

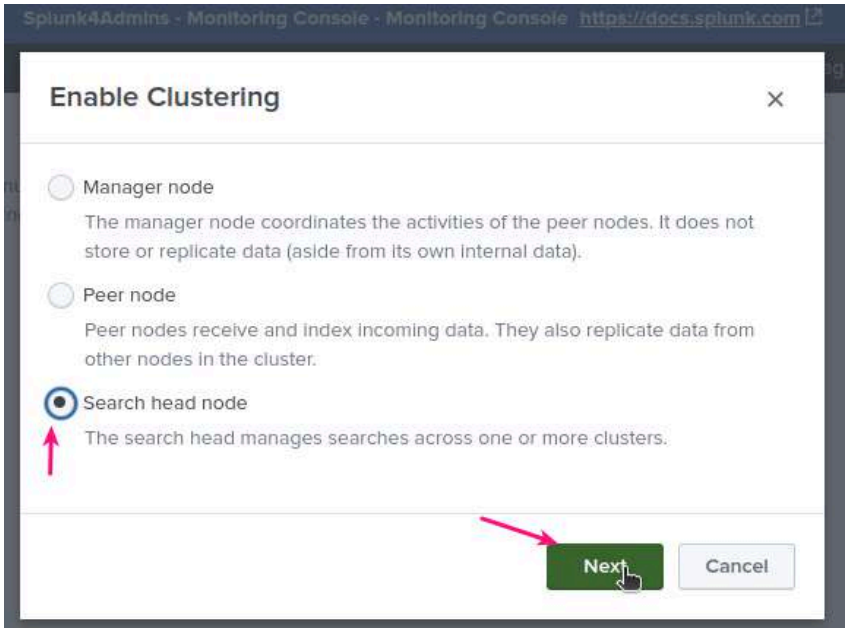
5. Click on “Settings” in the black bar, and then “Indexer Clustering”



6. Click on “Enable indexer clustering”

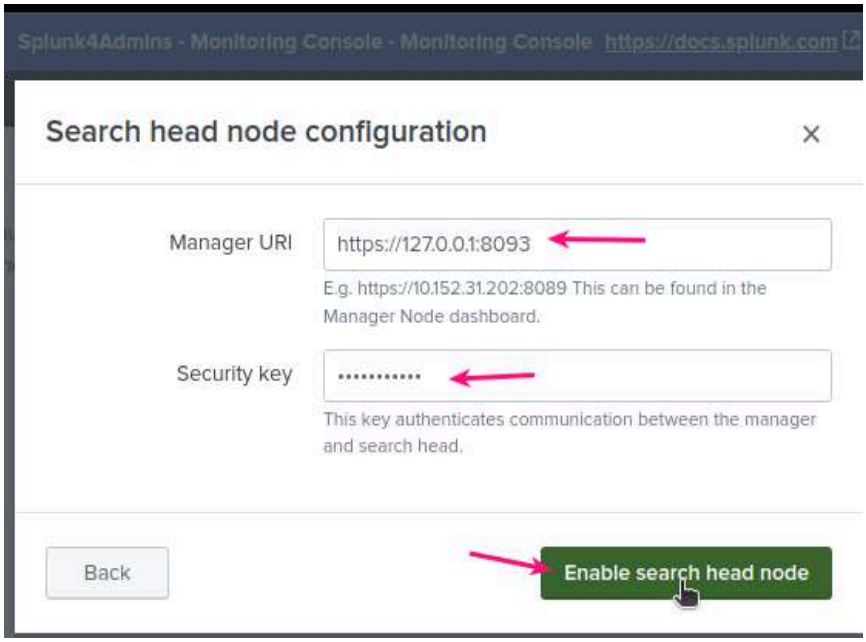


7. Select “Search head node” and click on “Next”

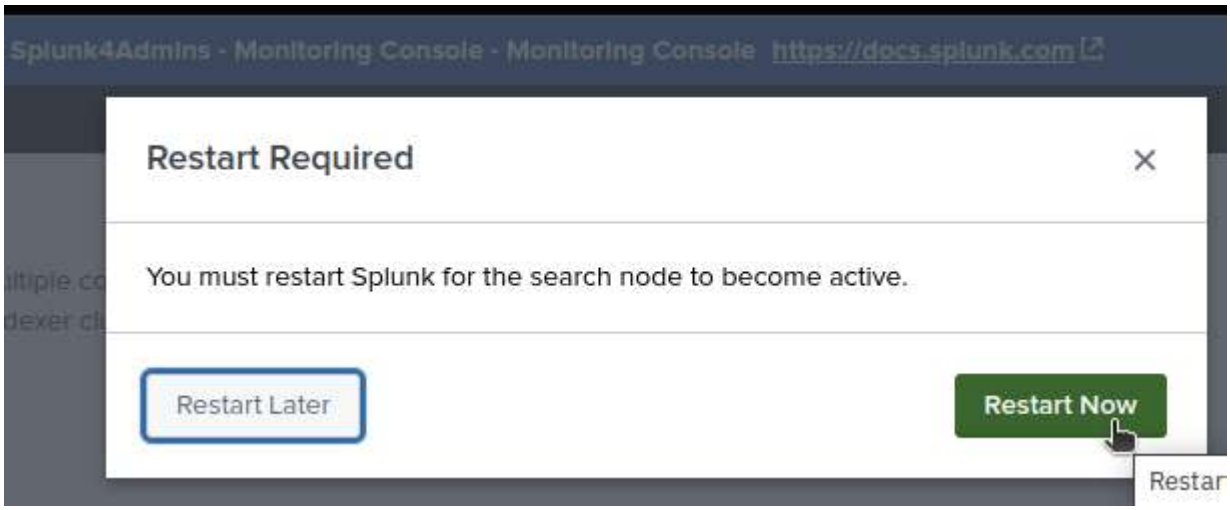


8. Configure the Cluster Manager node interface on 8093 and the security key “5p1unk.conf”

```
https://127.0.0.1:8093
```



9. Click on “Restart Now”

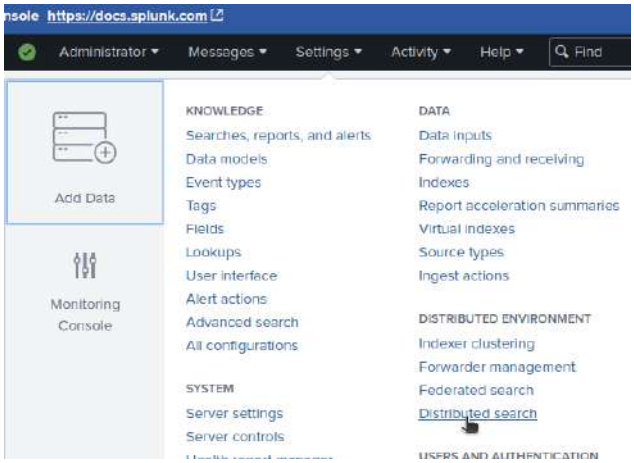


10. Log back in to the Monitoring Console node

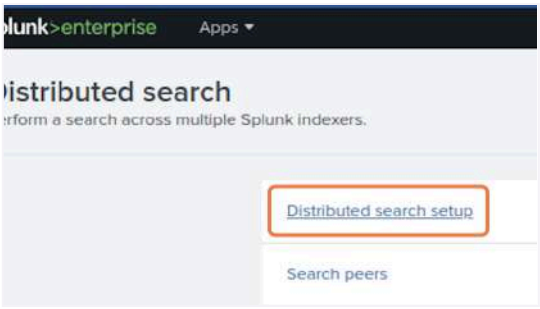
    Username “admin” || password “5p1unk.conf”

11. Click on “Distributed search”

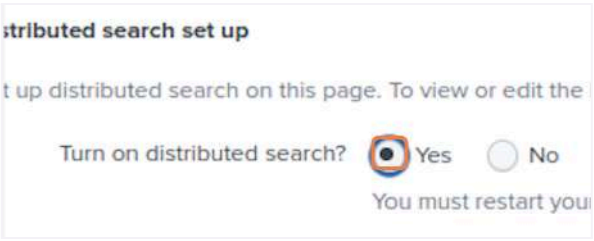
12. On the black-bar “Settings” dropdown click on “Distributed search setup”



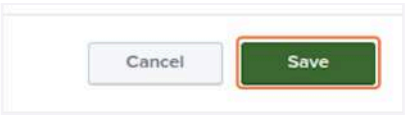
13. Select “Distribute search setup”



14. Ensure “Yes” is selected

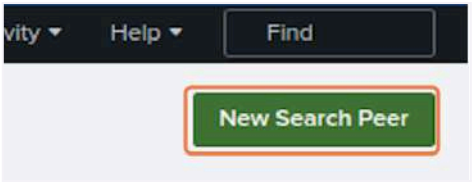


15. Click on “Save”



16. Click on “Search peers”

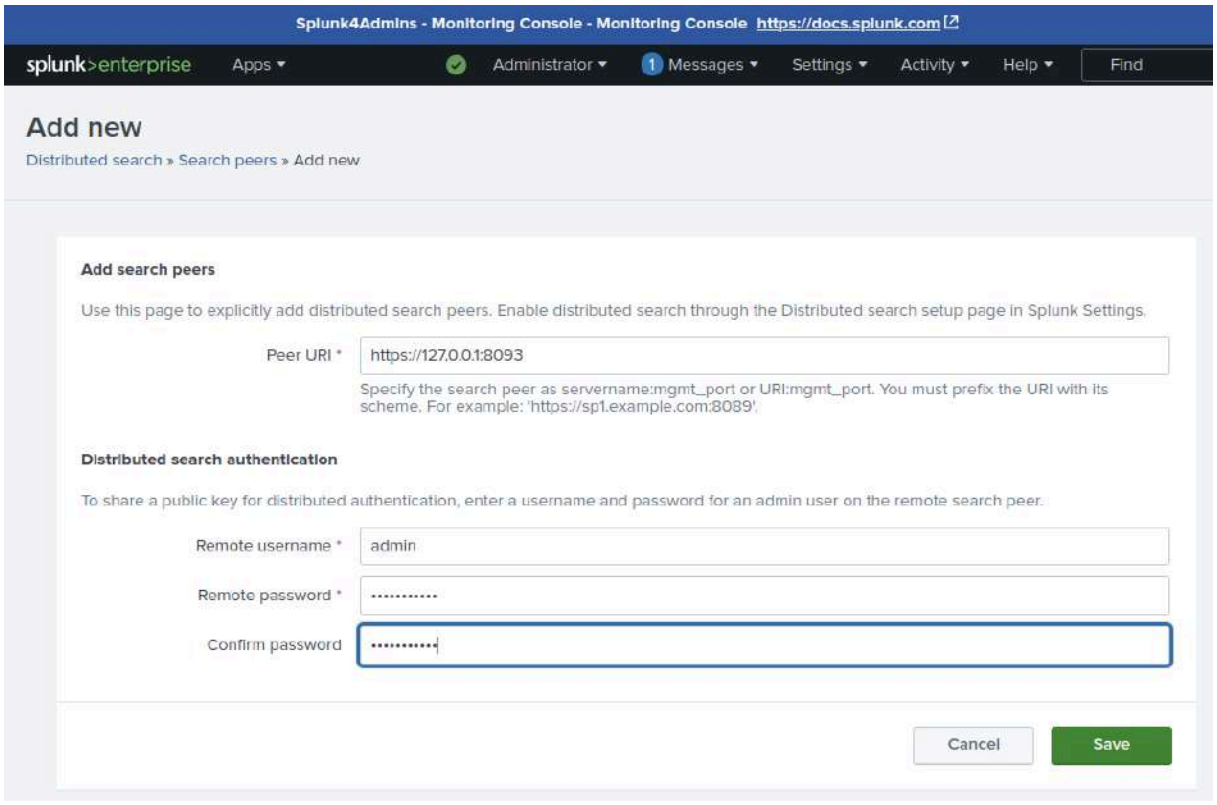
17. Click on “New Search Peer”



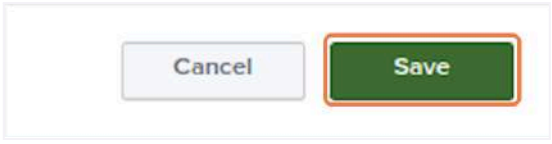
18. Add the Cluster Manager to the Monitoring Console

```
https://127.0.0.1:8093
```

In “Remote username” type “`admin`”
In “Remote password” type “`5p1unk.conf`”
In “Confirm password type “`5p1unk.conf`”



19. Click on “Save”

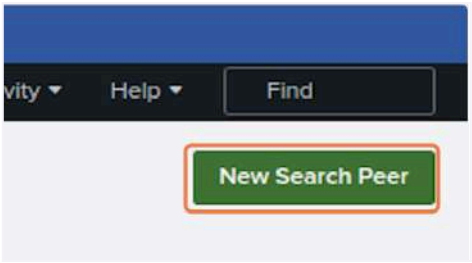


20. Add the other node (s4a-mc-sh)

    With the Monitoring Console search head integrated as a search head to the indexer cluster, and the Cluster Manager added as a distributed search head peer (accomplished above), the only other node to add is the other example search head. Clicking on “New Search Peer” and following the process until all are complete. Do NOT re-add c0m1 … but use the web.conf:mgmtHostPort as shown

    The table of nodes is:

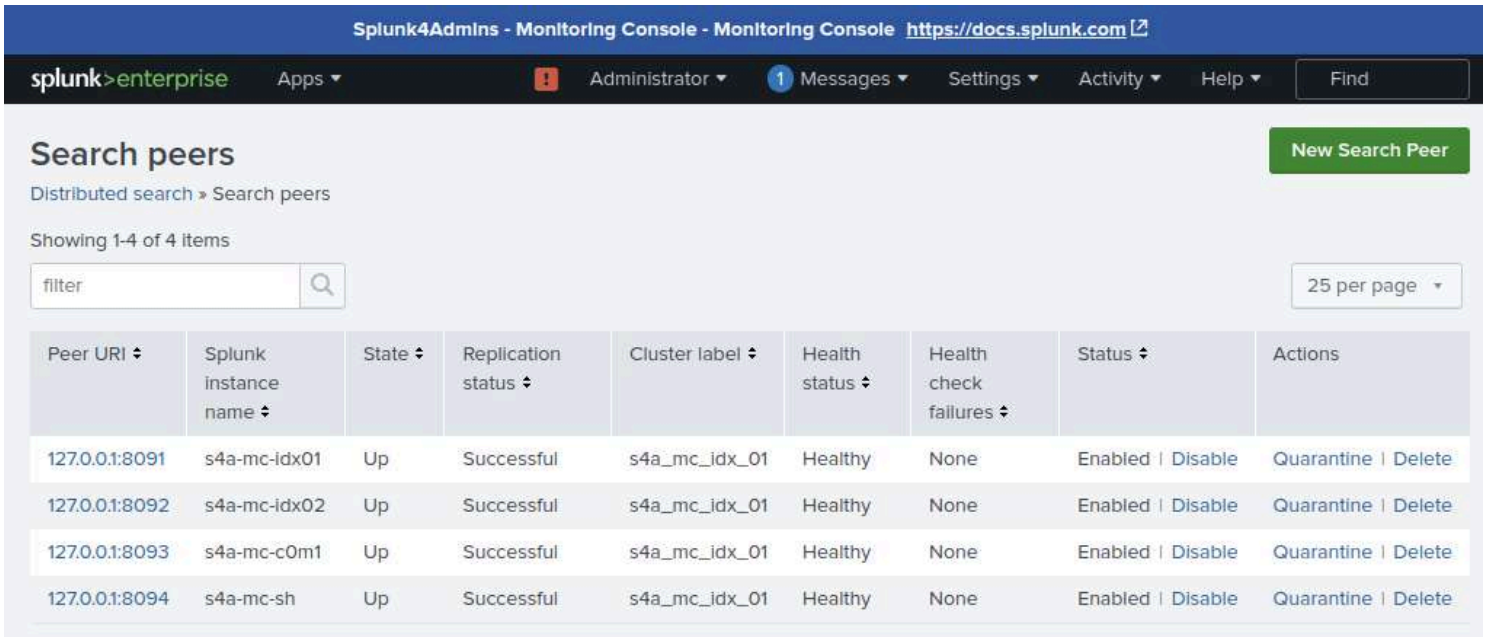
Host	web.conf:mgmtHostPort	web.conf:httpport	web.conf:appServerPorts	server.confkvstore	server.conf:splunktcp
s4a-mc-c0m1	8093	4501	8068	9194	
s4a-mc-idx01	8091	4502	8066	8192	9999
s4a-mc-idx02	8092	4504	8067	8193	9998
s4a-mc-sh	8094	4503	8069	8195	
s4a-mc-mc	8095	4500	8070	8196	
s4a-mc-forwarder		N/A			



Therefore, the two nodes to be assigned are the Cluster Manager (com1 on port 8093 - already done, and s4a-mc-sh on port 8094): (copy and paste into the “Peer URI” field and then provide the Username (admin) and Password (twice - 5p1unk.conf) and hit save …

```
https://127.0.0.1:8094
```

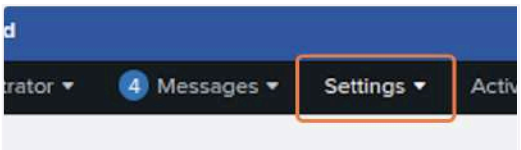
21. Observe the configured nodes in the “Search Peers” configuration



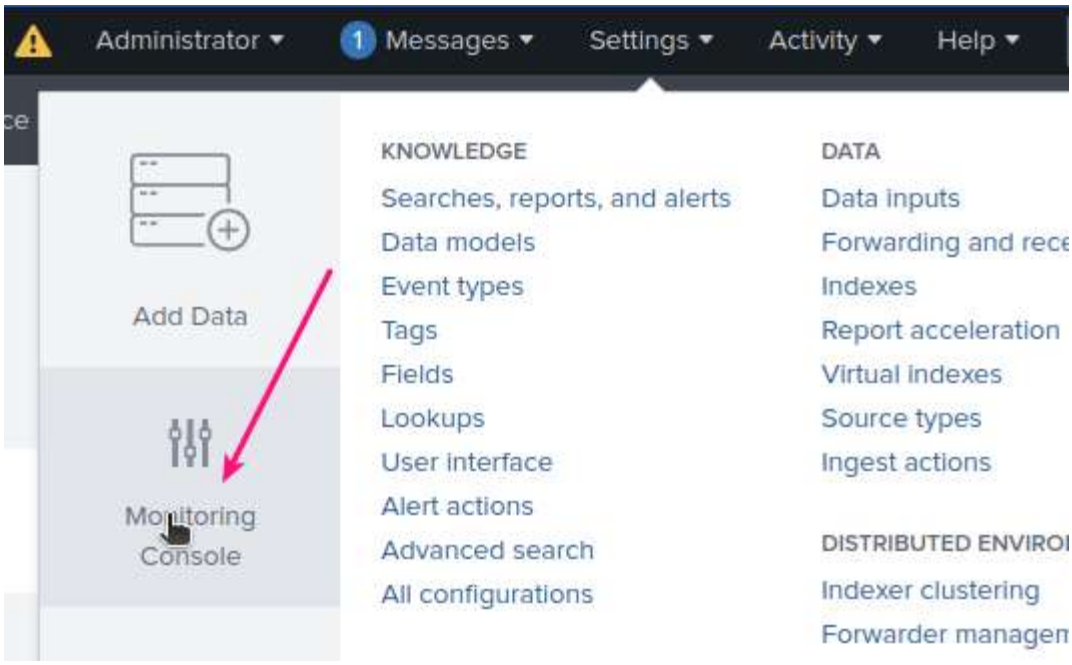
Sometimes the “Peer URI” will have a node name “s4a-c-c0m1:8091” and sometimes it will carry “127.0.0.1:8093”. In a real environment, these should each be a separate node talking to each other on port 8089.

22. Set the MC to “Distributed” mode

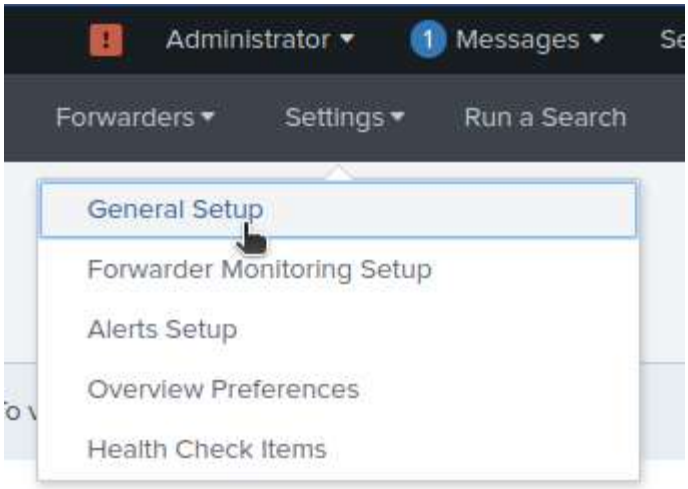
Now that the other nodes in the environment are set as part of the distributed search space for the MC, Click on “Settings” in the black bar



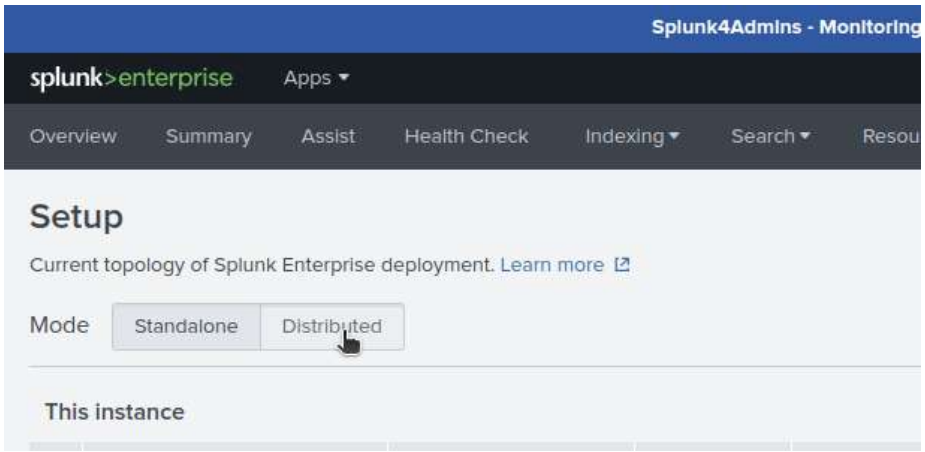
… and select “Monitoring Console” to access the MC app itself.



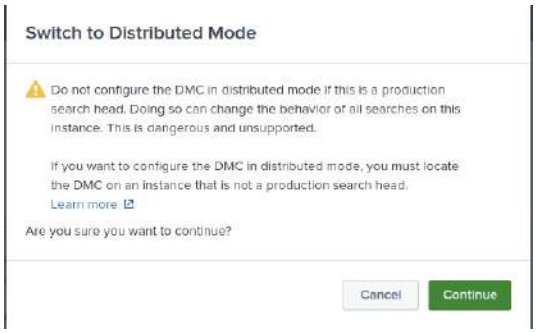
23. Click on the gray-bar “Settings” - “General Setup”



24. Set the Click on “Distributed”

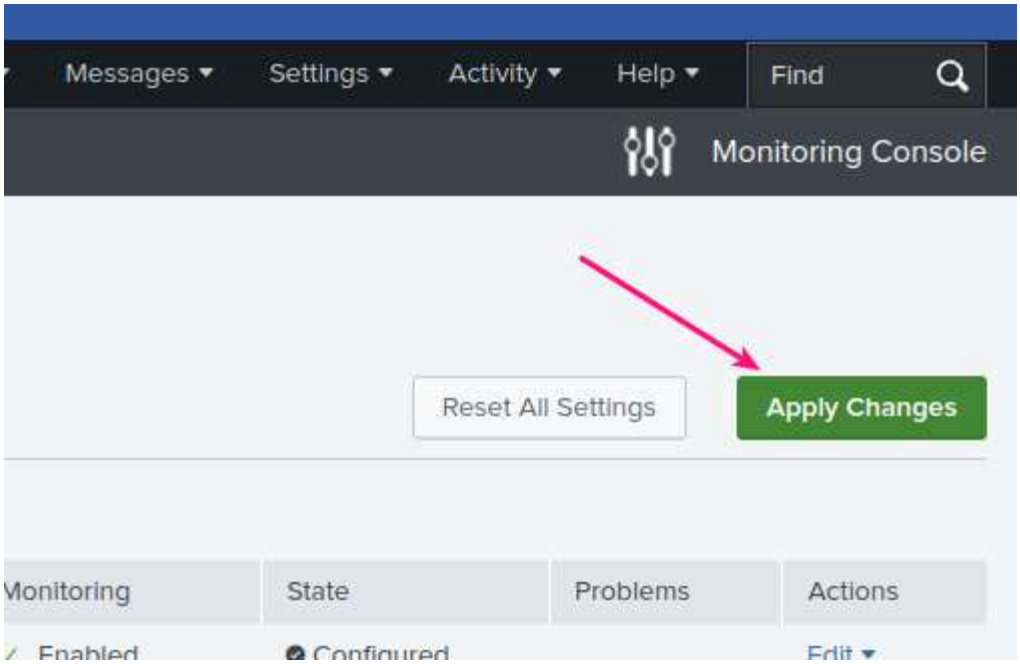


25. Click on “Continue”



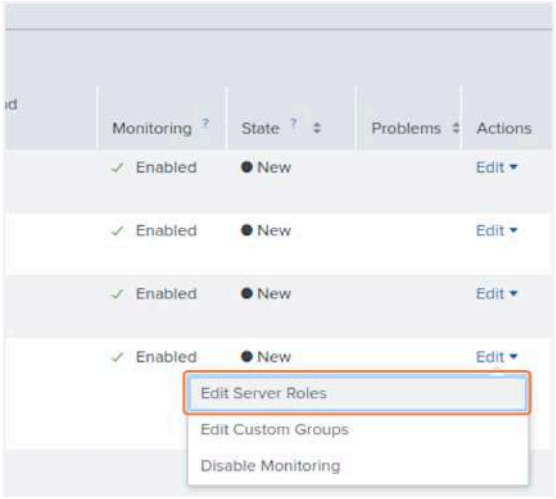
26. Click on “Apply Changes”

This is extremely important as the change from “Standalone” to “Distributed” is NOT engaged until “Apply Changes” is clicked … this is true for any modifications on this page.

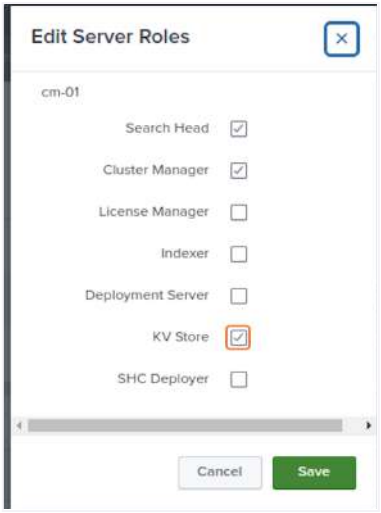


27. Configure Server Roles on Cluster Manager

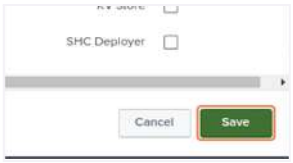
Once the MC is configured to work with all of the nodes in the environment, the server roles must be configured. Splunk assigns different roles to different systems. Having these configured correctly helps in both display, but also in the monitoring aspect. Click “Edit” for the Cluster Manager, then click “Edit Server Roles”. Frequently the Monitoring Console will select correctly, but sometimes it won’t, so edit the settings to reflect the correct Server Roles for each of the nodes … step 31 actually provides the way this screen should look. If any of the Server roles don’t match, reconfigure them. Changes made here are NOT reflected fully until the “Apply Changes” button is pressed. Cannot be stressed enough, hit “Apply Changes” …



28. Ensure “KV Store” and “Search Head” are deselected, frequently they are accidentally enabled for the Cluster Manager.



29. Click on Save



30. Click on “Done” in the subsequent dialogue

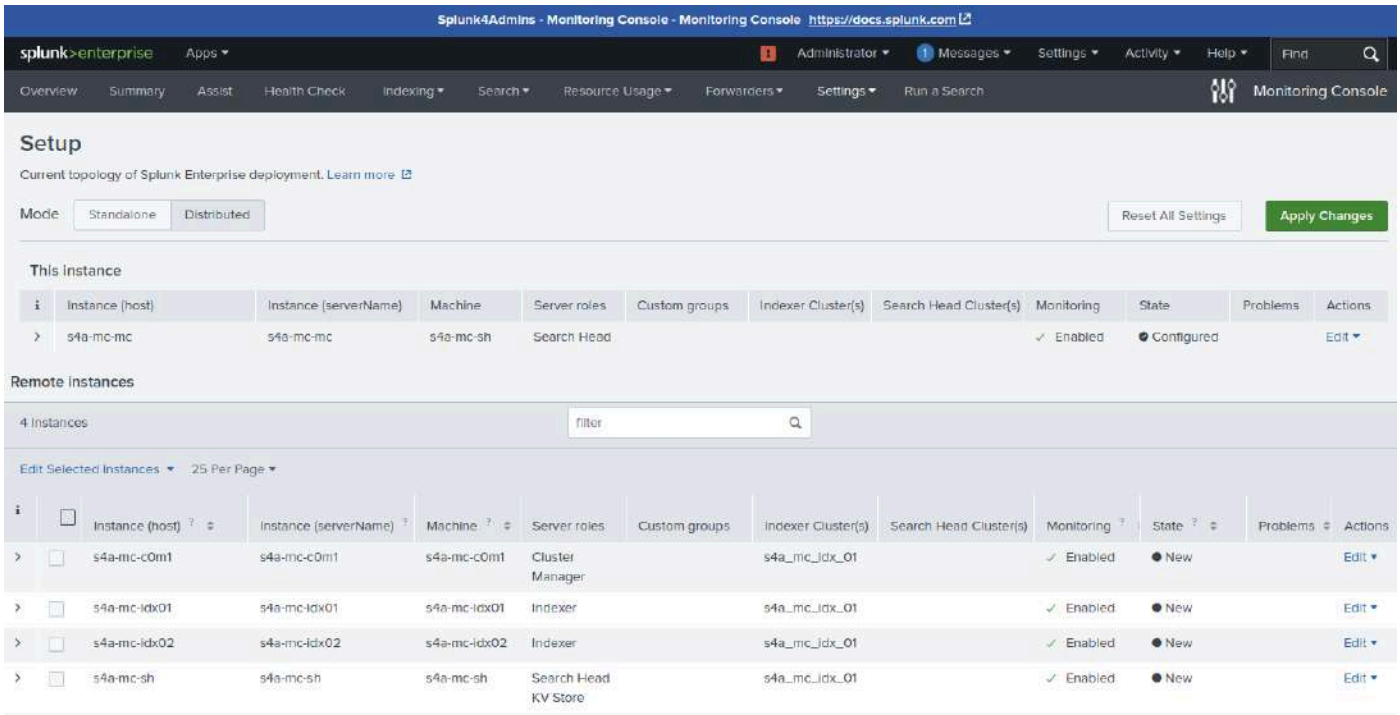
31. Configure Server Roles for the remainder of the nodes …

    License Manager should have “License Manager” - because this is a lab, the LM is managed outside of the lab and is inaccessible by the MC. **This lab environment is an exception due to the unique configuration.** It is best practice to associate the License Manager role to the instance that is the License Manager in the attendee’s environment.

Search heads should have “Search Head” and “KV Store”

Indexers should be only “Indexer”

Cluster Manager should be “Cluster Manager”

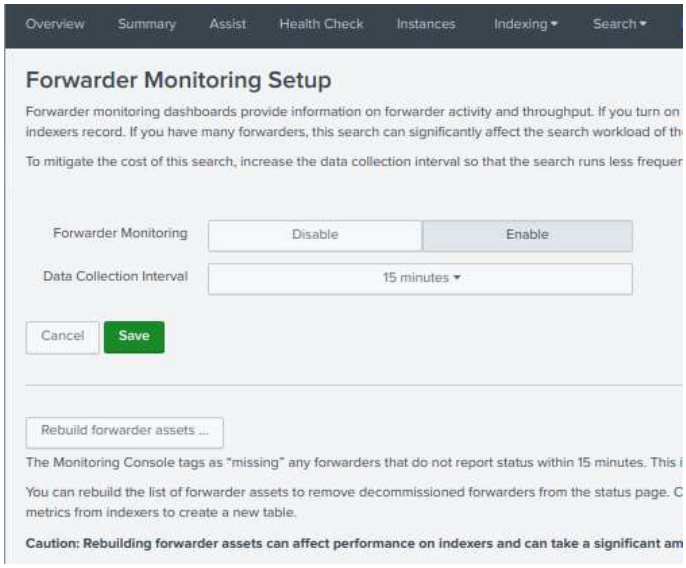


32. Apply Changes

Nothing is complete until all modifications have been done for the individual nodes and the changes have been applied. Click on “Apply Changes”

33. Click on “Refresh” to see the changes reflected on the Setup page

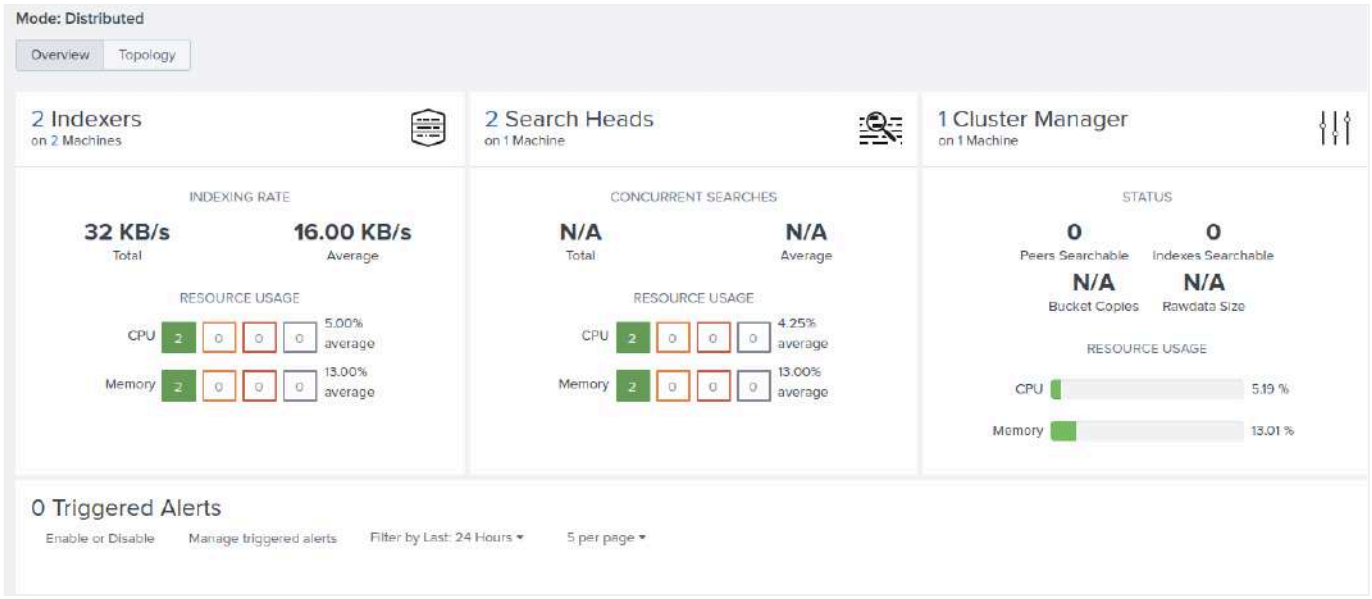
34. Setup Forwarder Monitoring - Click on “Settings” and then “Forwarder Monitoring Setup”



Select “Enable”, and leave the “Data Collection Interval” at 15 minutes

Click on “Save”

35. Overview of configured MC



splunk>

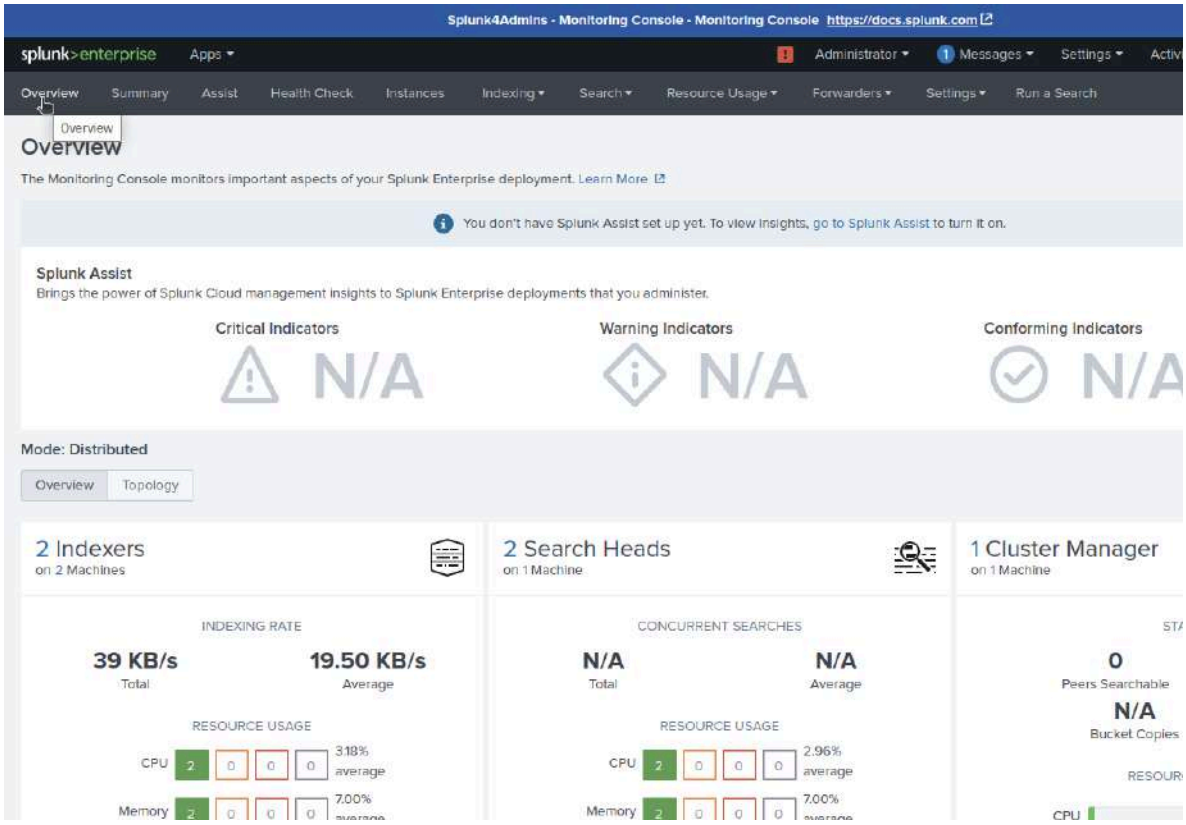
Exercise 2 – Explore Overview|Summary|Health Check|Instances

Description

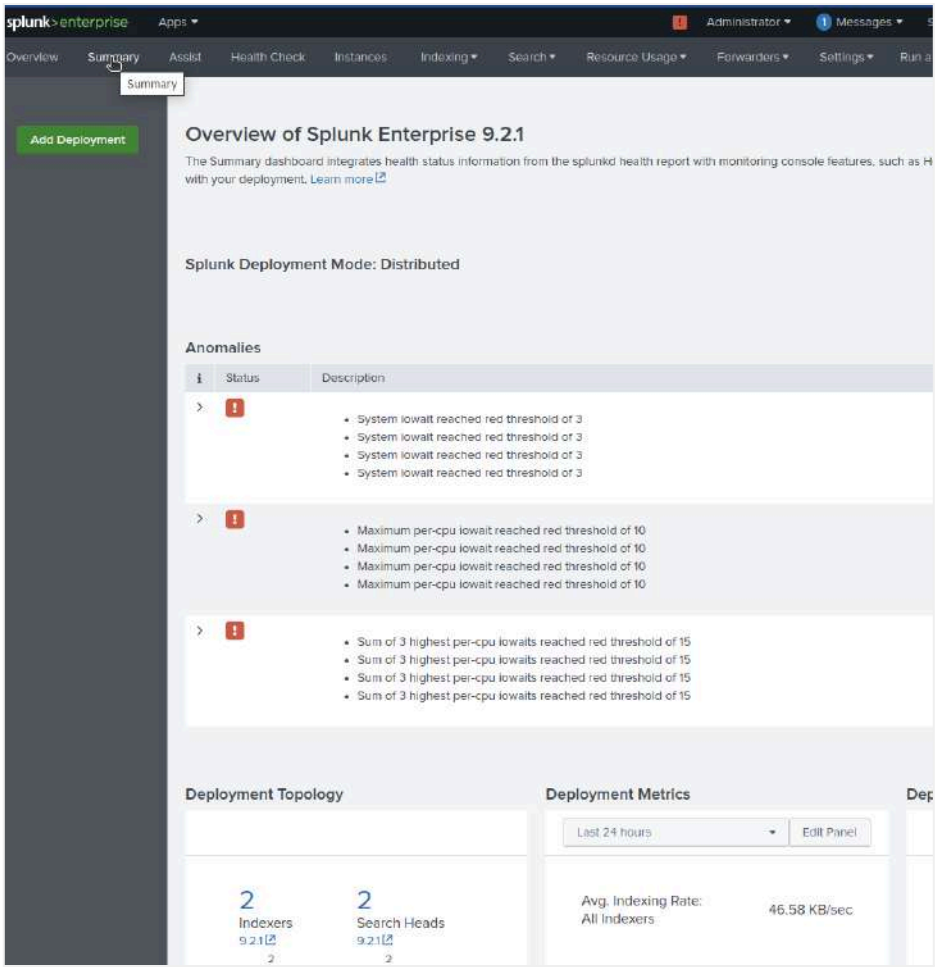
[Description]

Steps

1. Click on “Overview”



2. Click on “Summary”

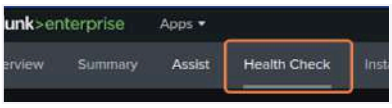


There are things “wrong” with this environment, mostly due to the fact that it exists on a single node. Later, there will be some exploration of some of these things “wrong”.

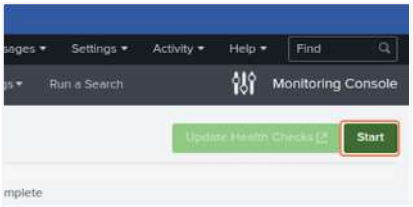
IO Wait and other machine performance issues are related to the AWS instance type and –here– not an issue. If you see them in your environment, be sure to research what is going on.

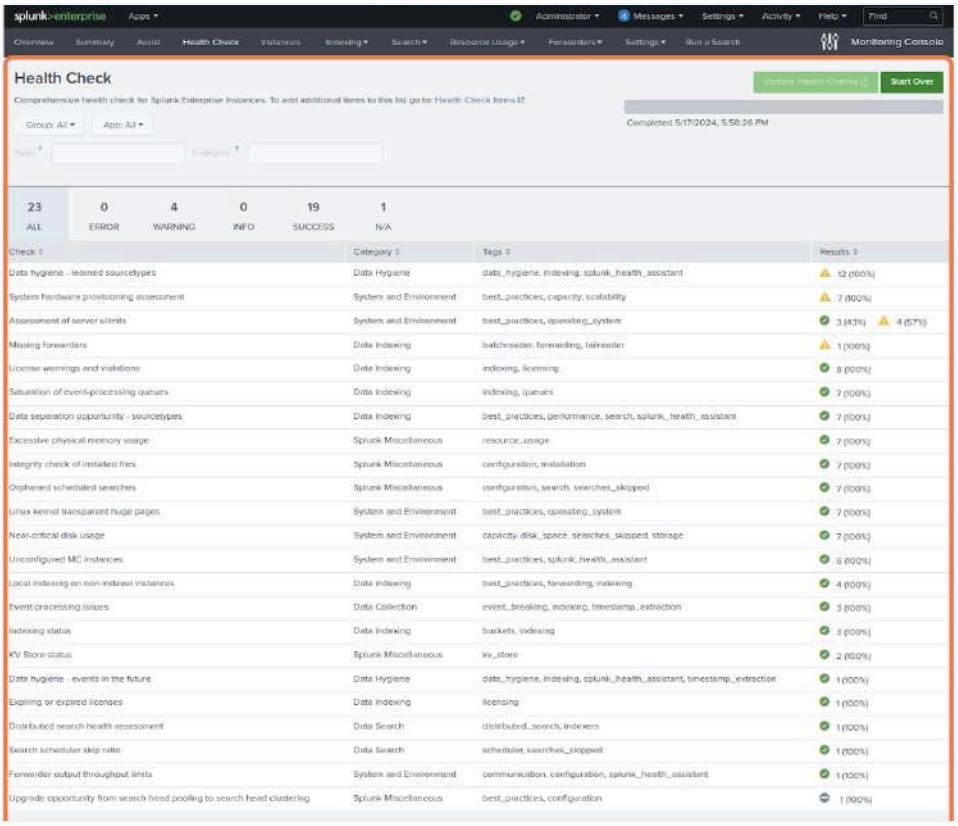
Forwarding destination issues also are due to this being a lab environment that “springs into being” from a prior configuration. Research and exploration about what is occurring in a real environment would begin in these first two Monitoring Console dashboards …

3. Click on “Health Check”

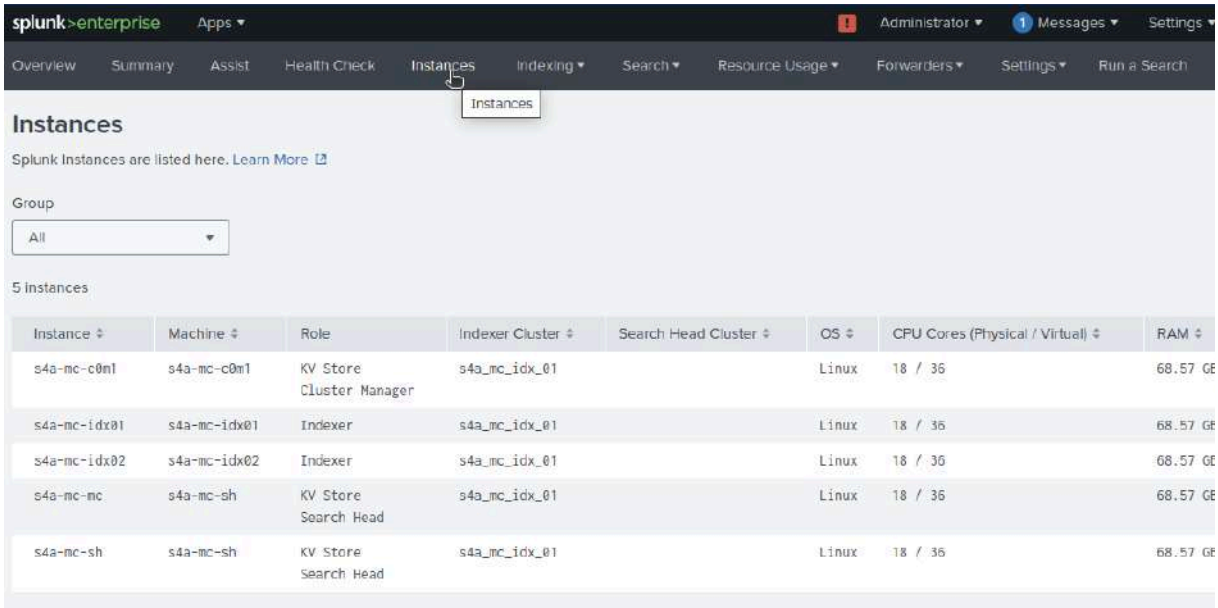


4. Click on “Start”





5. Click on “Instances”



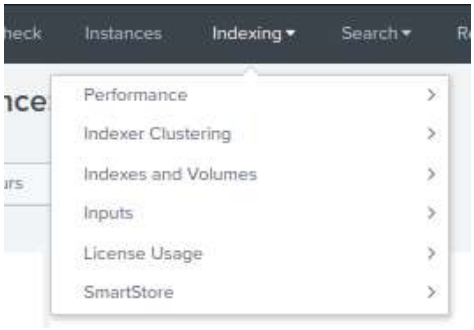
Exercise 3 – Explore the Indexing Dashboards

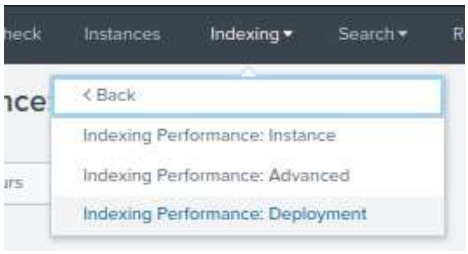
Description

Explore the various Indexing Performance dashboards to understand what information is made available.

Steps

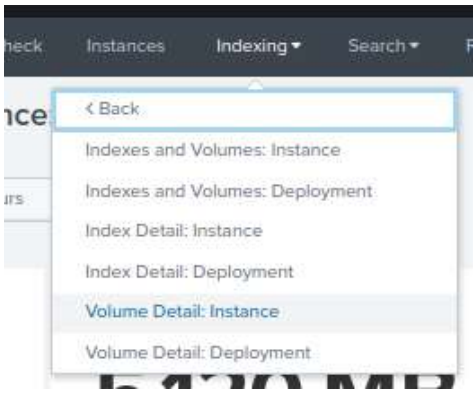
1. Click on “Indexing” and then “Performance”



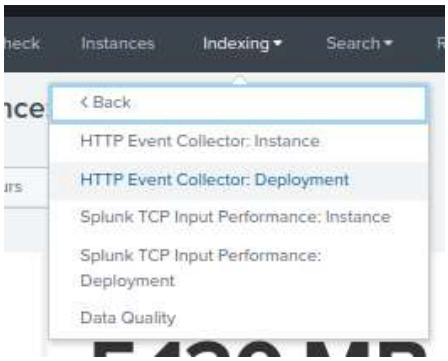


2. Click on “Indexing Performance: Instance”
3. Click on “Indexing Performance: Deployment”
4. On each of the dashboards, similar information is presented, but the “Deployment” dashboard permits better discovery of issues as the information is “as-a-whole” rather than “per-instance”
5. Important panels:
    a. Pipelines
    b. Indexing rate per X
    c. Median Fill Rate of Queues
    d. Advanced: Aggregate CPU Seconds per Indexer Processing Activity
6. Click on “Indexing” then “Clustering”

7. Then “Indexing Clustering:Status”
    a. Useful information
8. Back to “Clustering”, click on “Indexing Clustering: Service Activity”
    a. Most useful
        i. “Warning and Errors”
        ii. Fixup Tasks
9. Click on “Indexing and Volumes”



    a. Excellent statistics on the size and configuration of indexes, both at high-level and individual index levels
10. Click on Indexing” then “Inputs”



a. Most Useful

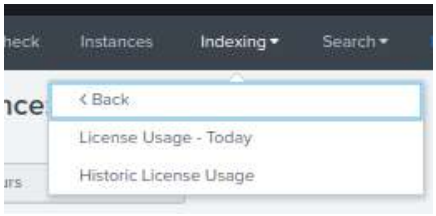
   i. HEC:Instance - Events and Valid Requests Count

   ii. HEC:Deployment - Data Received and Indexed

   iii. Splunk TCP Input Performance:Instance - TCP Input Queue Fill Ratio

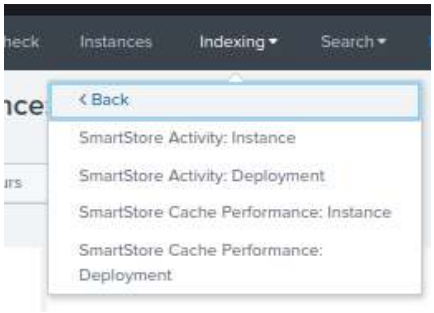
   iv. Data Quality - Event Processing Issues by Source Type

11. Click on “Indexing” then “Licensing”



   a. Useful daily and historical statistics for license management without accessing the License Manager

12. Click on “Indexing” then “SmartStore”



13. Most Useful
   a. Cache Performance:Instance/Deployment - Buckets Evicted
   b. Cache Performance:Instance/Deployment - Cache Hits/Missed
   c. Cache Performance:Instance/Deployment - Cache Thrash by Index

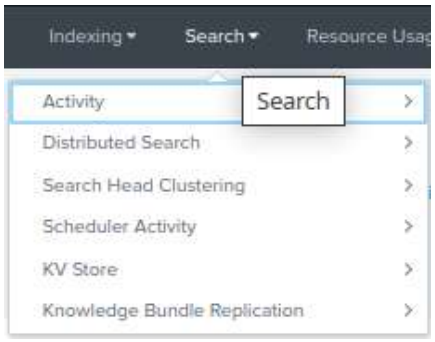
Exercise 4 – Explore the Search Dashboards

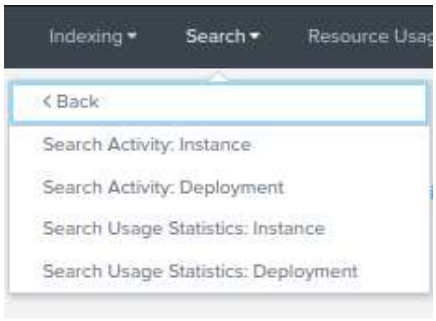
Description

Explore the various Search Performance dashboards to understand what information is made available.

Steps

1. Click on “Search” and then “Activity”





   a. Most Useful

      i. Activity:Instance/Deployment - Concurrency | Median Search Concurrency

      ii. Activity:Instance/Deployment - Top 20 Memory Consuming Searches

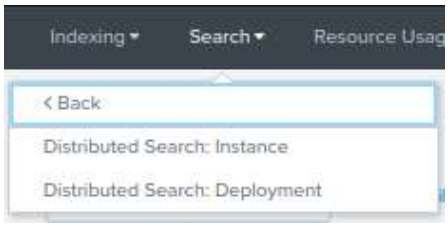
      iii. Activity:Instance/Deployment - Frequently run searches

      iv. Activity:Instance/Deployment - Long-running searches

      v. Usage Statistics:Instance/Deployment - Frequently run searches

      vi. Usage Statistics:Instance/Deployment - Long-running searches

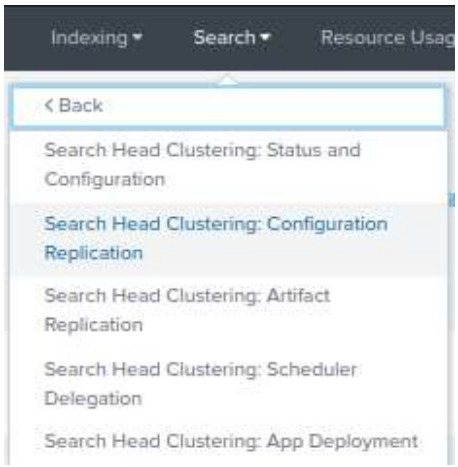
2. Click on “Search” and then “Distributed Search”



a. Most Useful

i. Distributed Search:Instance/Deployment - Peer Heartbeat

3. Click on “Search” and then “Search Head Clustering”

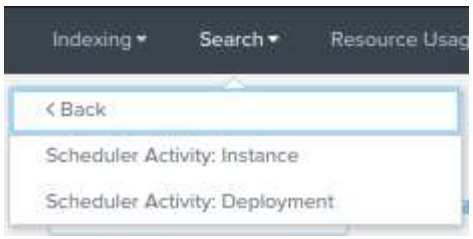


a. Most Useful

i. Status and Configuration

ii. Configuration Replication: Warnings and Errors

4. Click on “Search” and then “Scheduler Activity”



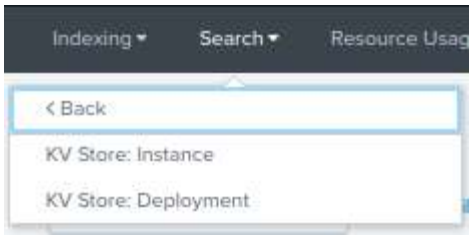
a. Most Useful

i. Instance/Deployment - Count of Skipped Scheduled Reports

ii. Instance/Deployment - Count of Skipped Reports by Name Reason

iii. Instance/Deployment - Count of Skipped Reports over Time

5. Click on “Search” and then “KV Store”

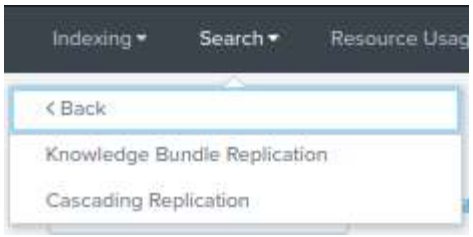


a. Most Useful

i. Instance/Deployment - Warnings and Error Patterns

ii. Instance/Deployment - Instances by Average Replication Latency

6. Knowledge Bundle Replication



a. Most Useful

i. Knowledge Bundle Replication - Average Full Bundle Replication Time

ii. Knowledge Bundle Replication - Average Delta Bundle Replication Time

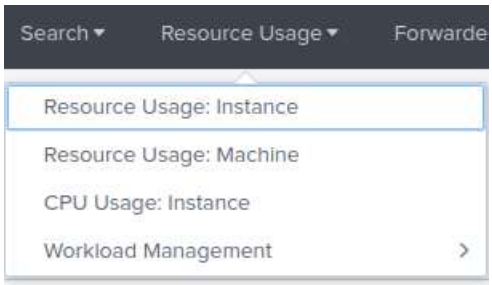
Exercise 5 – Explore the Resources Dashboards

Description

Explore the various Resources dashboards to understand what information is made available.

Steps

1. Click on “Resource Usage”

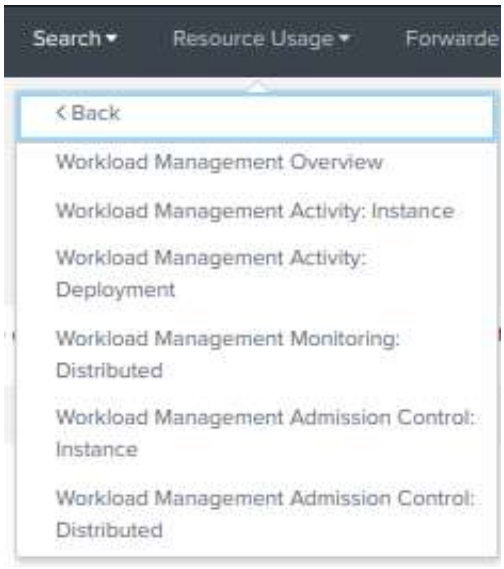


   a. Most Useful

      i. Resource Usage:Instance/Machine/Deployment

         1. Disk Space Usage
         2. IO Usage and Performance
         3. CPU usage and Saturation
         4. Instance - IO Usage by Mount Point

2. Click on “Workload Management”



   a. Useful for when using the Workload Management features of Splunk

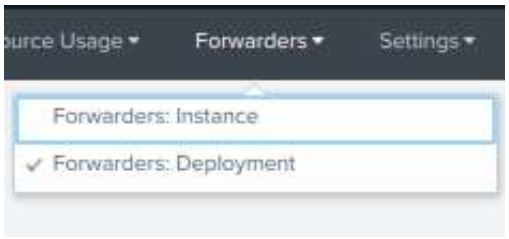
Exercise 6 – Explore - Detect: Forwarders

Description

Discover which forwarders are out-of-support.

Steps

1. Click on “Forwarders” then “Forwarders:Deployment”



Process

2. Look for the “Version” column to detect versions of the forwarders reporting into the Deployment Server
3. Click on the column header (“Version”) to reconfigure the table sort order
4. Compare the versions presented with the chart and decide which forwarders may be out-of-support (or nearly so). Click here for the Splunk Supported Versions page at docs.splunk.com.

Exercise 7 – Explore - Detect: Skipped Searches

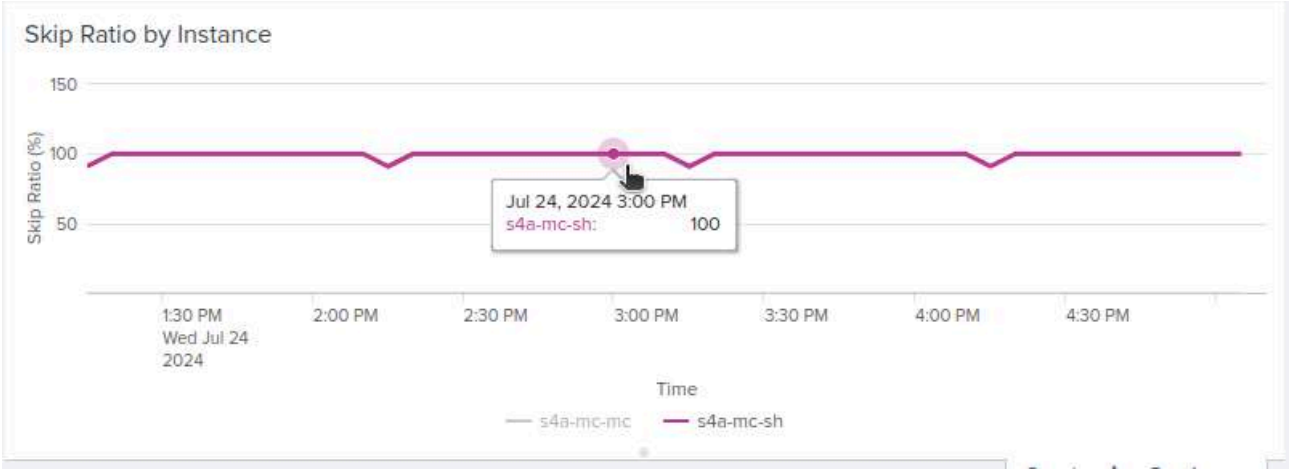
Description

Find searches that are being skipped. Skipped searches mean that information is not being captured correctly, and may indicate over-saturation of resources. Frequently this means that searches that do not need to be executed are running, but it can also mean that the architecture needs to be tuned to support the workload required.

Steps

Find which searches are being skipped

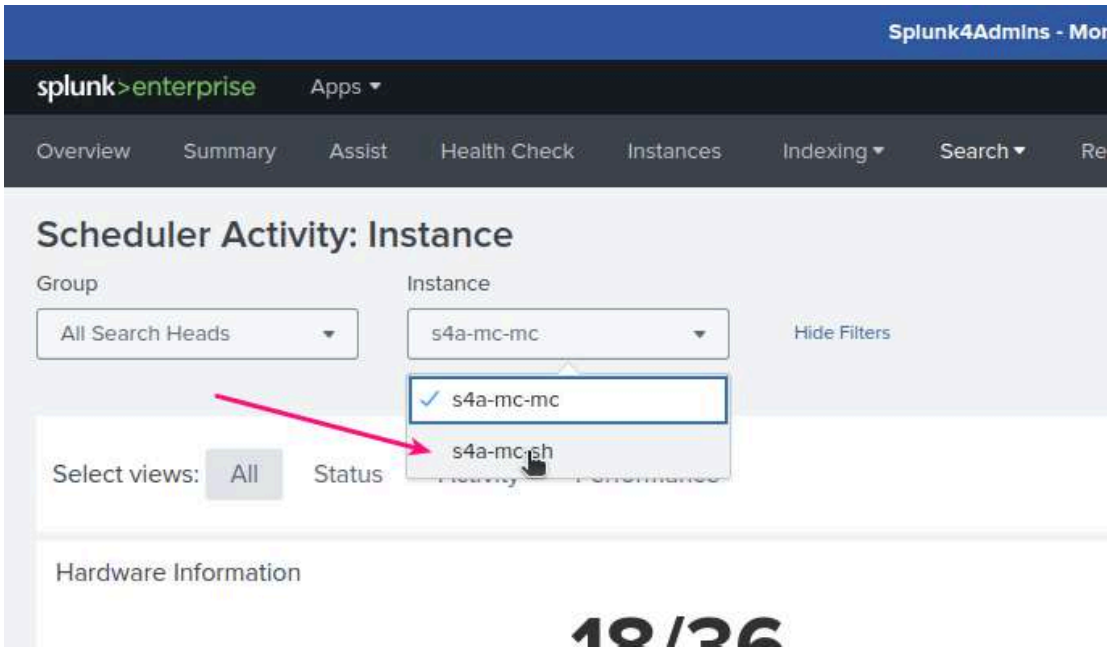
1. Click on “Search”, “Scheduler Activity”, then “Scheduler Activity:Deployment”
2. Part way down the dashboard, look for higher “Skip Ratio by Instance” and “Skip Ratio Across All Instances” panels and hover over the line in “Skip Ratio by Instance” that seems high.



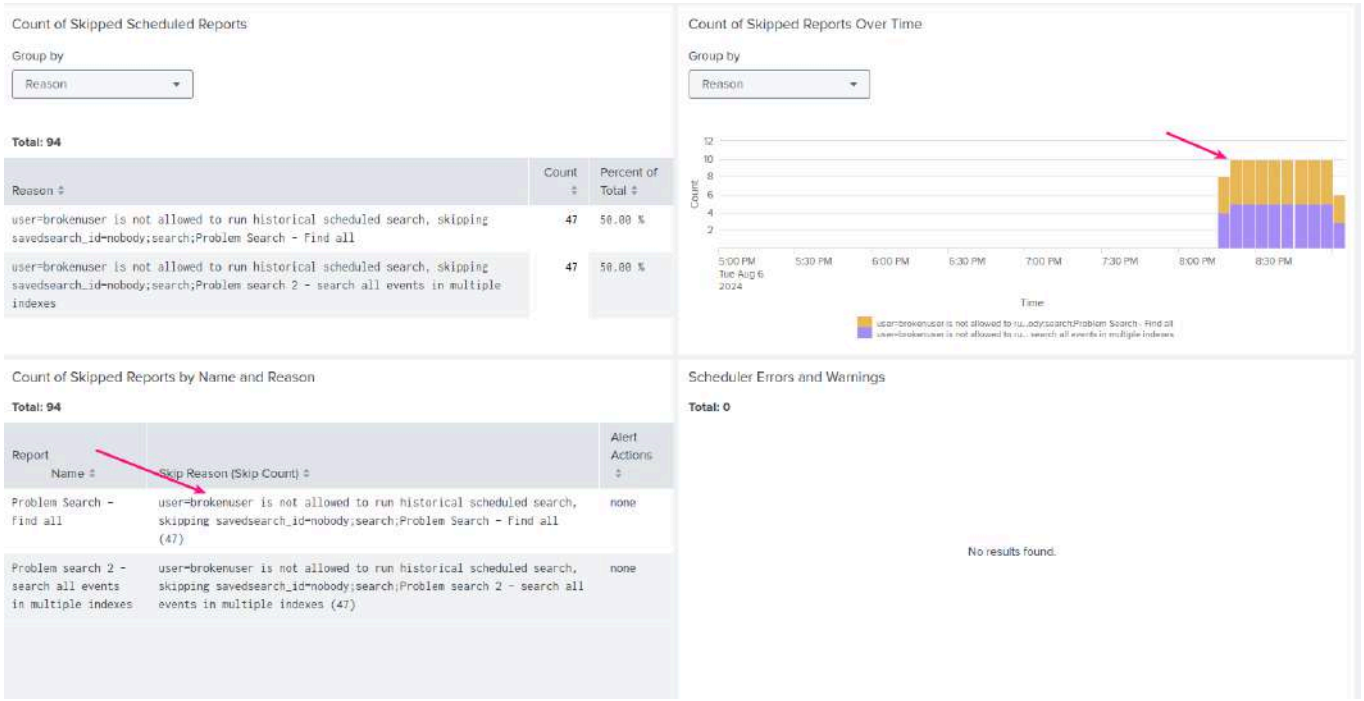
3. These two panels provide insight as to whether searches are being skipped and where
4. Non-zero indicates investigation may be required, but the “Ratio Across All Instances” indicates if there are endemic issues in the environment

Discover specifics

5. Once the location of skipped searches is identified, use the “Scheduler Activity:Instance” dashboard to determine more facts regarding the specifics of what is skipping. Select the search head that the prior panel indicated was showing skipped searches



6. Review the panels “Count of Skipped Reports by Name and Reason” and “Scheduler Errors and Warnings” to continue the investigation



7. Depending on what is discovered, explore the reasons behind the skips, whether over-saturation of resources, enabling unnecessary scheduled reports (searches), or potential resource failures.

8. This lab will not dig any deeper into resolving these issues, just discovery.

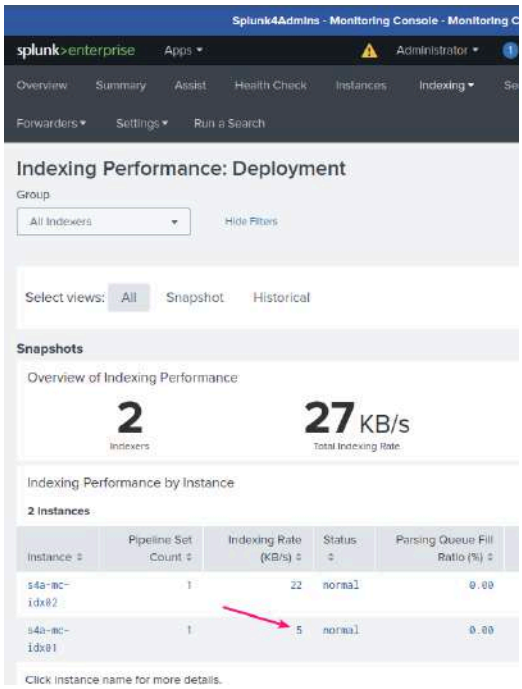
Exercise 9 – Explore - Detect:Disabled Ingest Port

Description

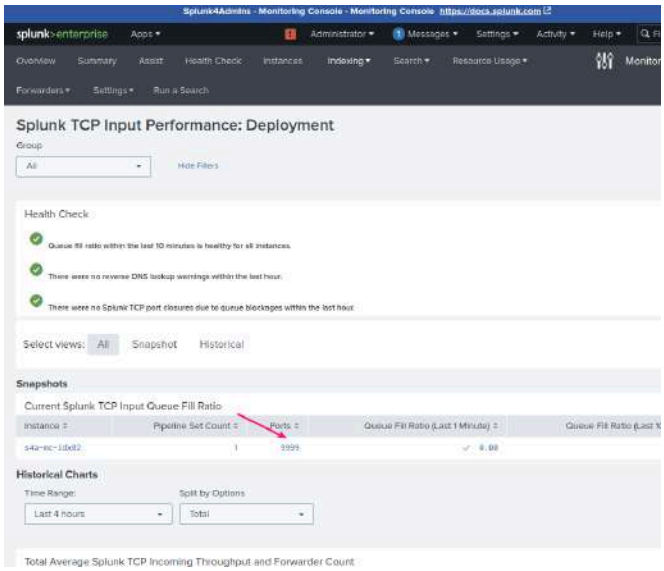
The MC can be used to detect issues in configuring the specifics of the Splunk environment due to inadvertent changes or poor architectural decisions. Finding a port that has been removed or ingest disabled can be difficult, but the MC can help.

Steps

1. Notice an issue in the “Indexing Performance:Deployment” dashboard



2. Review the “Indexing Performance by Instance” Panel
    a. Unbalanced ingest is an indicator that, for whatever reason, an indexer is not performing correctly. This is cause for an investigation. Given that the system is explicitly referenced, the discovery and diagnosis is straightforward.
3. Review other indexing performance dashboards
    a. After reviewing the “Indexing Performance:Instance” and “...:Advanced” dashboards and not discovering anything specific.
4. Explore other possible issues
    a. Validate the networking setup on the indexer via “Indexing -> Inputs -> Splunk TCP Input Performance:Instance”



b. This indicates that there is zero ingest on idx02, which corresponds to what is shown in the “Deployment” from step 1.

5. Check other configuration settings

   a. ssh out to the instance and check the receiving port

   b. `ssh -p 2222 splunk@<your_up_address|instance_DNS_name>` (password “5p1unk.conf”)

   c. See the command line output -

   d. `ss -anlp | grep -E LISTEN | grep -E '2222|9998|9999'` - see that there are no listeners on the 9998 ingest port as there should be.

   e. Check on the inputs as configured for both “indexer” instances

```
more /opt/splunk-idx0*/splunk/etc/apps/s4a-mc-indexer_receive_idx0*/local/inputs.conf
```

```
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
```

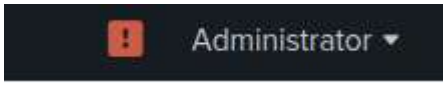
Exercise 10 – Explore - Detect: Misconfigured File Descriptors

Description

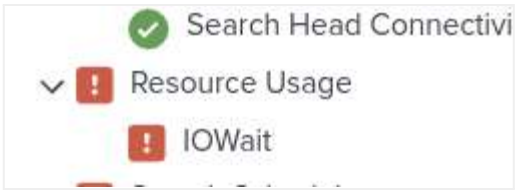
Due to Splunk's requirements for many open files, the operating system default for Open File Descriptors is too low. Splunk recommends that the maximum value for what is available, and the Health Check validates these settings. This sort of issue is frequently detected as high IO Wait (but IO Wait can be many other things).

Steps

1. Notice issue on the black "Status" bar

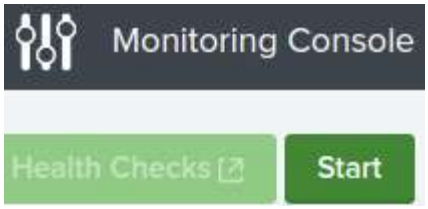


   a. Click on the red "exclamation point", scroll down to find the red "exclamation point"

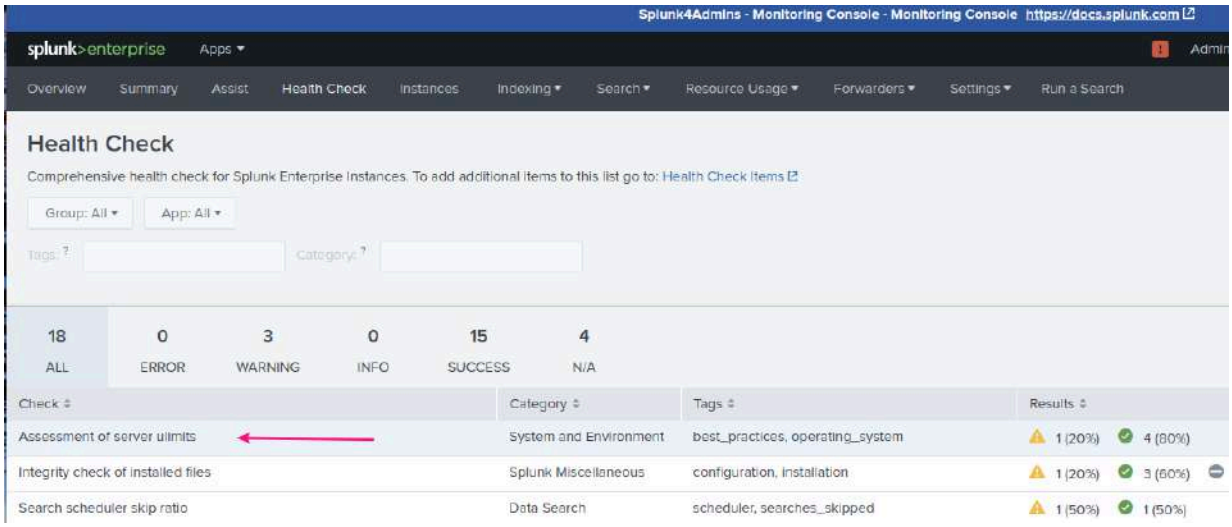


2. Go to the "Health Check", click "Start"

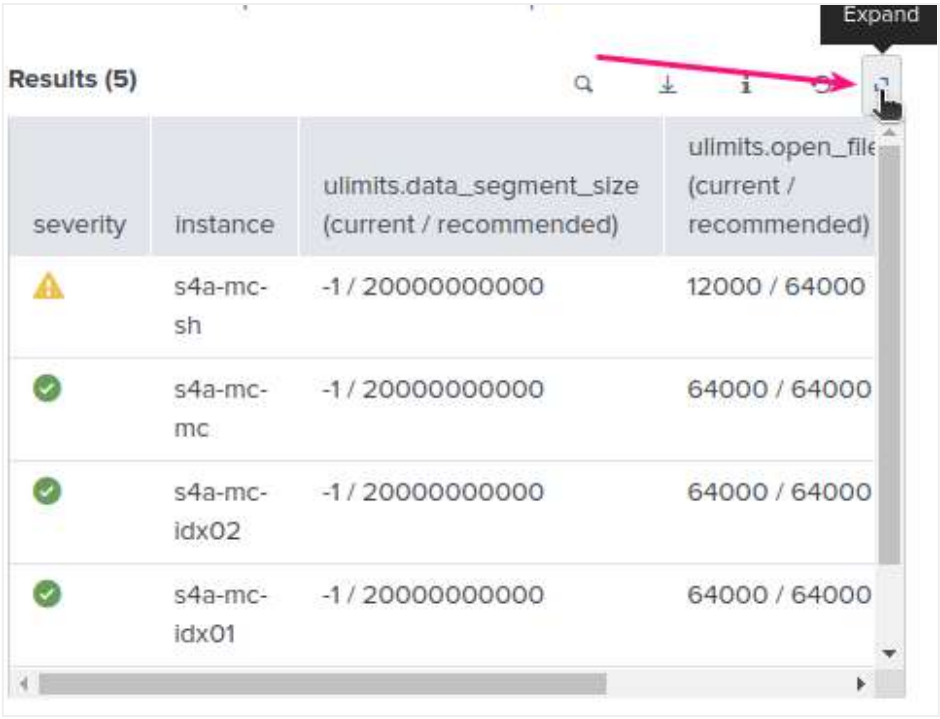
   Let the Health Check run to completion.



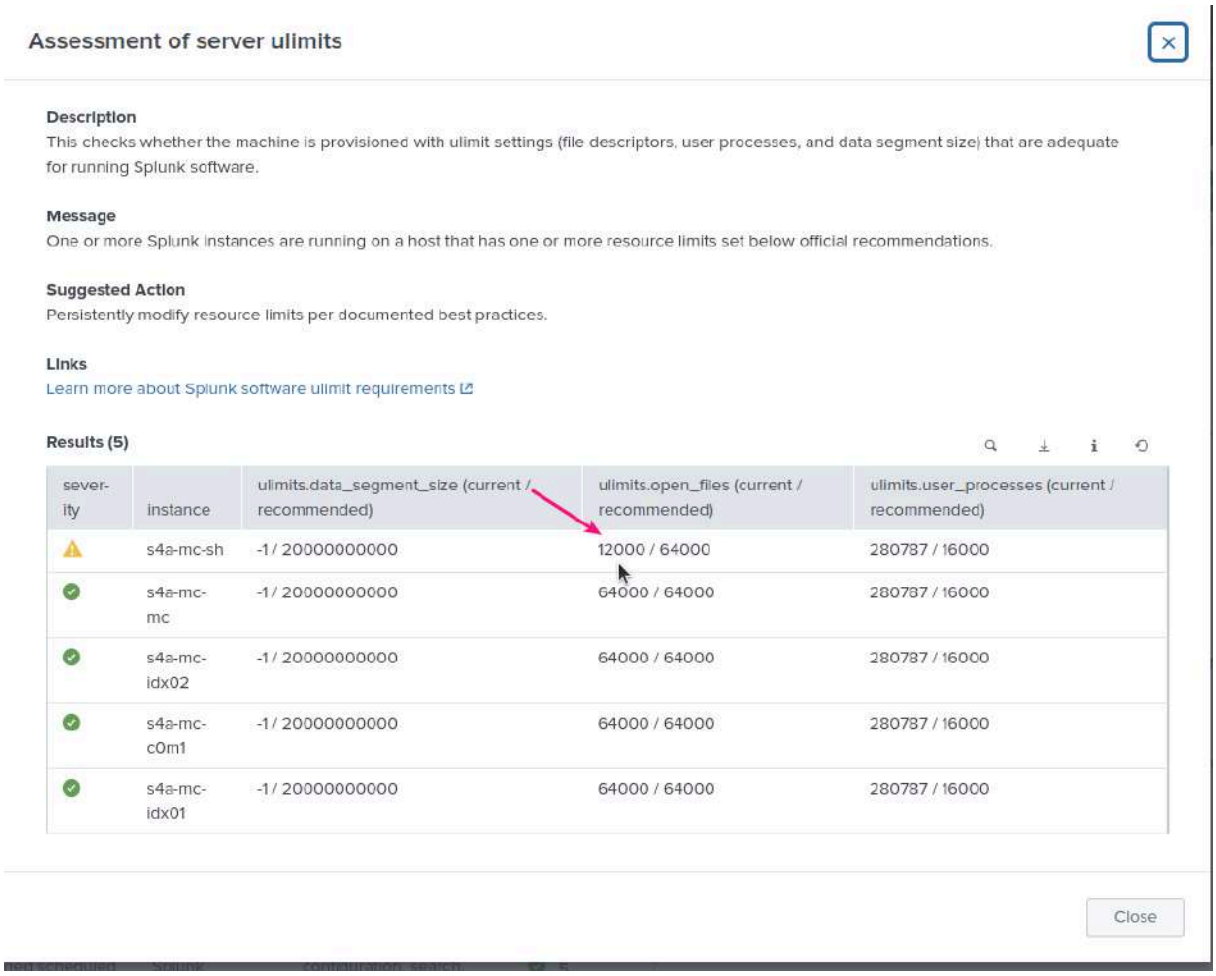
3. Scan down for "Assessment of server ulimits"



4. See the side bar, click on the expanding “<>”



5. Discover the misconfigured ulimits



For linux, the number of available file descriptors is essential, ensuring splunkd is started with the highest number of available file descriptors ensures optimal performance. If splunk is started via systemd, this is automatically configured correctly.

Summary of All Dashboards

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

Overview

- High level, collects from each of the different systems (with Server Roles)

Summary

- Similar to Overview, with a different viewpoint, can connect to other MCs with "Add Deployment"

Assist (Cloud management to Enterprise ...)

- <Needs description>

Health Check

- Many basics validated and reported - can build your own and add as needed

Instances

- Which instances exist on which "machine" with which roles ...
- Including version identification
- Depending on role, Action→Views has differing endpoints

Indexing

Performance

- Instance - Overview / Pipelines | Indexing rate per [sourcetype|index|host|source] / Median Fill rate of Queues
- Advanced - Overview / Thread Activity / Ingest pipeline Activity By Pipeline Set (incidents) / Busiest Pipeline / Assignment Probability / Assignments per pipeline set
- Deployment - Overview of all instances / Instances by indexing rate / Deployment-wide Total Indexing Rate / Instances by Median Queue Fill Ratio / Deployment-Wide Median Queue Fill Ratio

Clustering

- Status - Similar to Settings/Indexer Clustering - Node status / Index status, replication, size / Search head status
- Service Activity - Warning and Error Patterns / Fixup Tasks - In Progress / Fixup Tasks - Pending (select index) / Excess Buckets / Historical: Bucket Fixup, Service Job Activity, Service Jobs Executed, REST Endpoint Activity, Count of Hits on REST endpoints

Indexes and Volumes

- Instance - By instance, Total index size, event count, bucket count, individual index information, Volume information, Volume usage, Historical charts: Size of indexes over time, Volume Size over time,
- Deployment - Overview, Number of indexes, non-empty indexes, instances, total index size, index size by instances, data age, median and oldest, per index size statistics, per volume size statistics
- Index Detail: Instance - per index size and usage information
- Index Detail:Deployment - Overall index size, age, usage, event count (by N). Historical: Maximum Index size, average index usage, median data age
- Volume Detail: Instance - Overview of volume information, event count, earliest event, latest event, usage (size), capacity, indexes on volume, data age by index. Historical:Volumes size over time
- Volume Detail: Deployment - Overview of all instances, volume usage, capacity, path. Historical: maximum, average volume usage

Inputs

- HTTP Event Collector:Instance - By instance, throughput, current and last 30 minutes. Historical: request overview, data overview, events and valid requests count, errors, data received and indexed, list of tokens
- HTTP Event Collector: Deployment - Overall, throughput, current and last 30 minutes, list of instances with performance statistics. Historical: Historical: request overview, data overview, events and valid requests count, errors, data received and indexed, instances overview
- Splunk TCP Input Performance: Instance - Health Check, TCP input queue fill ratio. Historical:TCP incoming throughput and forwarder count
- Splunk TCP Input Performance: Deployment - Health Check, TCP Input queue fill ratio. Historical: Average TCP incoming throughput and forwarder count, indexer count by tcp input queue fill ratio, deployment-wide TCP input queue fill ratio
- Data Quality - Event Processing Issues by Source Type

License Usage

- Today - Usage today, usage per pool percentage by pool, pool warnings, license peer usage warnings
- Historic License Usage - usage by day, percentage license used by day, average and peak license usage

Smartstore

- Activity:Instance - individual instance connectivity, bucket activity, bucket upload/download failure count
- Activity:Deployment - overall connectivity, bucket activity, bucket upload/download failure count
- Cache Performance: Instance - individual instance minimum free space, eviction padding, max cache size, hotlist recency seconds, hotlist bloom filter recency hours, buckets evicted by time, remote storage search overhead, cache hits/misses, cache thrash by index
- Cache Performance: Deployment - overall instance minimum free space, eviction padding, max cache size, hotlist recency seconds, hotlist bloom filter recency hours, buckets evicted by time, remote storage search overhead, cache hits/misses, cache thrash by index

Search

Activity

- Instance - Concurrency / Count of Ad hoc and Scheduled searches / Search Activity. Historical: Median Search Concurrency, Median Resource Usage of Searches, Top 20 Memory-consuming searches, Searches started per minute by dispatcher, Aggregate search runtime
- Deployment - Search activity by instance. Historical: Instances by median search concurrency, deployment-wide Median Search Concurrency per instance over time, Instances by media search CPU usage, Top 20 memory-consuming searches
- Usage Statistics:Instance - Search activity by user, Frequently run searches, Long-running searches, Common search commands
- Usage Statistics:Deployment - Search activity by user, Frequently run searches, Long-running searches

Distributed Search

- Instance - Peers, Knowledge bundle replication. Historical: Peer heartbeat, Knowledge bundle upload activity, Time to reap
- Deployment - Search peers. Historical: Peer heartbeat, Knowledge bundle upload activity, Time to reap

Search Head Clustering

- Status and Configuration - Search Concurrency, Status. HIstorical: Search Concurrency, Captain election activity, Captain election details

- Configuration Replication - Warning and Error Patterns. Historical: Configuration Replication Activity, Configuration Replication Performance, Count of actions over time, Time spent on actions over time
- Artifact Replication - Warning and error patterns, Count of artifacts. Historical: Median count of artifacts to replication, artifact replication job activity
- Scheduler Delegation - Delegation count, Delegation activity. Historical: Scheduler activity, scheduler status
- App Deployment - App status. Historical: App deployment requests, count of app deployment actions on deployer

Scheduler Activity

- Instance - Hardware information, concurrency of scheduled reports, unique scheduled reports, Count of reports scheduled, Skip ratio, Average execution latency. Historical: Count of scheduler executions, Count of scheduler executions over time, Scheduled report completions, Median concurrency of scheduled reports, Aggregate scheduled search runtime, Runtime statistics, Execution latency over time, Count of skipped scheduled reports, Count of skipped reports by name and reason, Count of skipped reports over time
- Deployment - <Needs description>

KV Store

- Instance - Collection metrics, Memory Usage, Flush Time, Page Fault per Operation, Count of Operations, Status (Active Connections, Total Queues, Total Asserts). Historical: Memory Usage, Operations per minute, Asserts, Page Faults per Operation, Network Traffic, Size of Queues, Connections over Time, Percent of Each Minute Spent Flushing to Disk, Slowest Operations
- Deployment - Warning and error patterns, KV Store status. Historical: Instances by median page faults per operation, Deployment-wide KV Store network traffic, Instances by virtual to mapped memory ratio, instances by average replication latency, operations log window of KV Store captain, Instances by percent of each minute spent flushing to disk, Slowest operations

Knowledge Bundle Replication

- Knowledge Bundle Replication - Replication policy, Replication threads, Average full bundle replication time, average delta bundle replication time, average full bundle size, average delta bundle size, latest common bundle across all peers. Historical: Replication cycle count, replication cycle count by peer success ratio, average bundle replication time by bundle type, average bundle size by bundle type, Bundle replication activity, Average bundle replication time and size
- Cascading Replication

Resource Usage

- Instance - Machine information, Physical memory usage by process class, CPU usage by process class, Disk usage. Historical: Median physical memory usage by process class, Median CPU usage by process class, Median disk usage

- Machine - Machine information, Load average, CPU usage, Physical memory usage, Disk usage. Historical: Median load average, Median CPU usage, Median physical memory usage, Median disk space, Average IO usage and performance, Average IO Usage by mount point
- Deployment - Resource usage by instance. Historical: Median load average, Deployment-wide Median load average, Median CPU usage, Deployment-wide median CPU usage, Median physical memory usage, deployment-wide median physical memory usage, Median storage IO saturation, Deployment-wide median storage IO saturation, Median disk usage, Deployment-wide median disk usage
- CPU Usage:Instance - CPU usage, CPU usage over Splunk process type. Historical: Median CPU usage by process class, Median CPU usage of searches, Median historical CPU usage
- CPU Usage:Deployment - Effective CPU, CPU per primary server role, search heads CPU usage, indexers CPU usage, CPU usage by instances, CPU usage by primary server role over Splukn process type. Historical: Deployment-wide median CPU usage, Median CPU usage, Median CPU usage by process class, Median CPU usage of searches, Median historical CPU usage
- Workload Management
    - Overview - Status, Configuration. Historical:Deployment-wide CPU usage by workload pool, Deployment-wide median physical memory usage by workload pool
    - Activity:Instance - Pool limits
    - Activity:Deployment - Pool limits
    - Monitoring:Distributed - Historical: Number of searches aborted, Number of search moved to alternate pool, Number of searches triggering an alert, Number of searches per action triggered, Number of searches per action triggered over time, Overview of scheduled searches triggering rules
    - Admission Control:Instance - Total searches prefiltered, Adhoc searches prefiltered, Scheduled searches prefiltered. Historical: Count of prefiltered searches, Count of prefiltered searches over time, Scheduled searches prefiltered
    - Admission Control:Distributed - Total searches prefiltered, Adhoc searches prefiltered, Scheduled searches prefiltered. Historical: Count of prefiltered searches, Count of prefiltered searches over time, Scheduled searches prefiltered

Forwarders

- Instance - Status and configuration, Outgoing data rate
- Deployment - Forwarders by status, Status and configuration, Total count of forwarders and receivers, Forwarder connection count over time

Links

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

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
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
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/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