Splunk4Admins

Indexer Performance

splunk>
a CISCO company

© 2024 SPLUNK INC.

Forward-looking statements

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

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

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

© 2025 Splunk LLC. All rights reserved.

splunk>
a CISCO company

Enroll in Today's Workshop

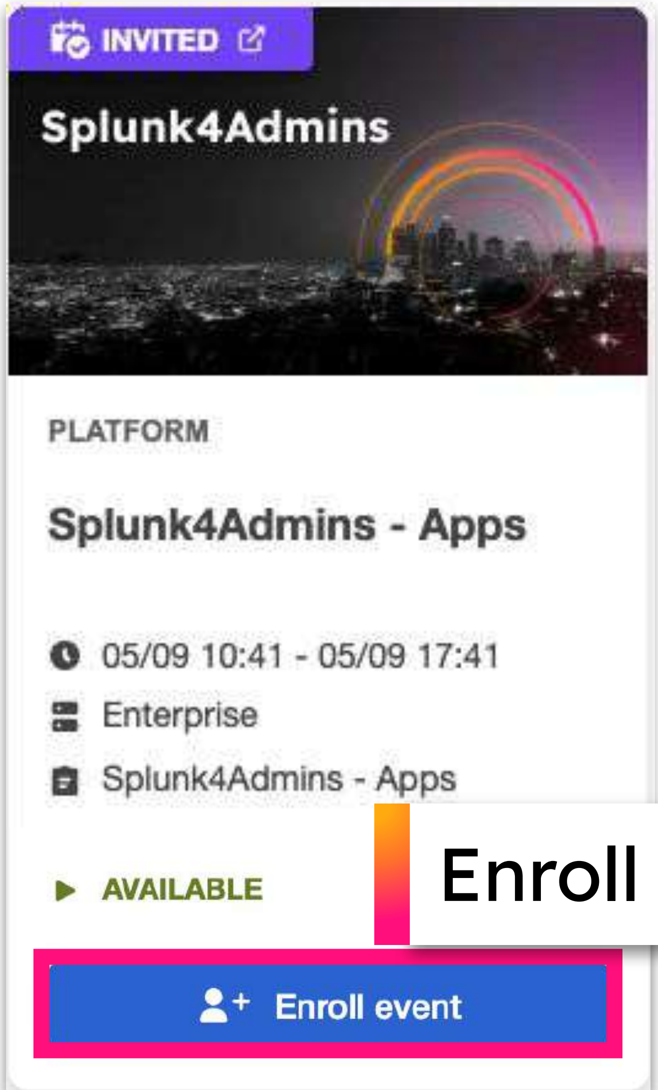
Tasks

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-IDX-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-IDX-Attendee

Goal



INVITED

Splunk4Admins

PLATFORM

Splunk4Admins - Apps

05/09 10:41 - 05/09 17:41

Enterprise

Splunk4Admins - Apps

AVAILABLE

Enroll event

Enroll in today's event

© 2025 SPLUNK LLC

Please introduce yourself!

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

© 2025 SPLUNK LLC

Workshop Agenda

- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
  - Lab^1
  - Lab^2
  - Lab^3
  - Lab^{4} - Lab^{6}
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

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
  - “Required”: Splunk Admin enabled
  - “Required”: Splunk Admin Certified preferred

© 2025 SPLUNK LLC

Expectations for Workshop

Indexer Performance

- Last roughly 90 - 120 minutes
- Understand what affects Splunk indexer performance
- Understand how Splunk Architecture affects performance
- Understand how Splunk Search load affects indexer performance
- Guidelines for when to “scale-out” vs when to “scale-up”
- Tools to use for performance issue detection
- Some solutions to common performance issues
- Many, many resources

© 2025 SPLUNK LLC

What is Splunk “performance”

- What constitutes Splunk indexer performance diagnosis and remediation?
- Understand Architecture
  - Indexers vs Search head
  - Utility systems)
- Slow search
- Slow and delayed ingest

Maximizing performance with the latest Splunk platform capabilities	https://lantern.splunk.com/Splunk_Platform/UCE/Observability/Maximizing_performance_with_the_latest_Splunk_platform_capabilities

© 2025 SPLUNK LLC

Workshop Agenda

- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
    - Lab^1
    - Lab^2
    - Lab^3
    - Lab^4 - Lab^6
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

Aspects of Splunk “performance”

- OS vs. Splunk
- Understanding how the two pieces interact is essential
- Understanding where the most likely bottlenecks exist helps accelerate diagnosis
- Using the correct tools helps ensure quick responses
  - Splunk tools first, then OS tools
  - Third party tools are available, but diagnosing Splunk should start with Splunk

Maximizing performance with the latest Splunk platform capabilities	https://lantern.splunk.com/Splunk_Platform/UCE/Observability/Maximizing_performance_with_the_latest_Splunk_platform_capabilities

© 2025 SPLUNK LLC

Workshop Agenda

- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
  - Lab^1
  - Lab^2
  - Lab^3
  - Lab^4 - Lab^6
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

Splunk Specifications

- How important is “minimum specifications”?
- How important is using SVA?
  - Where to get SVA?
- How to use SVA?
- Minimum architecture? C1 or C11
- Prefer actual hardware to VM infrastructure

Planning for infrastructure and resource scalability	https://lantern.splunk.com/Splunk_Platform/Splunk_Outcome_Paths/Improve_Performance/Planning_for_infrastructure_and_resource_scalability
Splunk Validated Architectures	https://docs.splunk.com/Documentation/SVA/current/Architectures/About
Reference hardware	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware

© 2025 SPLUNK LLC

System Architecture

Tiering

- Search
  - Clustered or otherwise
- Indexing
  - Cluster Manager (CM) plus however many indexers, min: 3
- Utility
  - CM, License Manager (LM), Deployment Server (DS), and Deployer (search head cluster manager)
- Forwarding
  - Actual work environment for enterprise
  - May include Heavy Forwarder tier

Planning for infrastructure and resource scalability	https://lantern.splunk.com/Splunk_Platform/Splunk_Outcome_Paths/Improve_Performance/Planning_for_infrastructure_and_resource_scalability
Splunk Validated Architectures	https://docs.splunk.com/Documentation/SVA/current/Architectures/About
Reference hardware	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware
Summary of performance recommendations	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Summaryofperformancerecommendations

© 2025 SPLUNK LLC

Splunk Parallelism

- Map/Reduce is the key
- Parallelism scales much more easily than single-machine parallelism (SMP)
- Distributing workload reduces response time significantly
- Plenty of reasons to scale-up
  - Large memory footprint of KV Store or lookups
    - Every search sends a package of information related to the Knowledge Objects. The larger the package, the higher the latency as the search startup is delayed
  - Large results set returns

Configure parallel reduce search processing	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Setupparallelreduce
Capacity Planning Manual	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Performancechecklist
Summary of performance recommendations	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Summaryofperformancerecommendations

© 2025 SPLUNK LLC

System Architecture

Storage

- Shared vs. direct attached storage devices (DASD)
  - Types - Recommendation
    - Hot-warm - NVME/SSD
    - Cold/Frozen - Large SSD, but can be spinning disk or network storage. Must be carefully tuned
  - Shared infrastructure should be dedicated to Splunk with Quality of Service (QoS) to tune performance needs (throughput and IOPs)
- Primary issues
  - Latency
    - < 20ms, but faster will always be better
  - IOPs
    - Dependent on Premium Apps
    - Minimum 800, but more for indexers
  - Throughput
    - More is better, but there are no recommendations

Sizing your Splunk architecture	Link to Splunk Lantern
What storage type should I use for a role?	Link to Splunk Docs

© 2025 SPLUNK LLC

System Architecture

Memory

- More is better
- Competing requirements:
  - OS Write cache
  - OS Read cache
  - Search KV Store and lookups and then results loaded and returned
  - Splunkd
  - OS requirements
- Architecture for different tiers
  - For indexers - (sm: 12GB, mid: 64GB, high: 128GB)
  - Search heads - rough recommendation start at 32GB (MC can use more)
  - Utilities - start at the minimum, but have separate hardware/VM for the various services
  - Premium Apps - always require more

Sizing your Splunk architecture	Link to Splunk Lantern
Indexer Memory Specification	Link to Splunk Docs

© 2025 SPLUNK LLC

System Architecture

CPU

- As with RAM, more is better
- Competing requirements:
  - OS activities
  - Splunk search (1 (v)cpu per search drives available concurrency)
  - Splunk indexing (also 1 (v)cpu per search drives available resources)
- For indexers - (sm: 12p/24vpcu, mid: 24p/48vcpu, high: 48p/96vcpu)
- Search heads - 16p/32vcpu
- Utilities - start at the minimum, but have separate hardware/VM for the various services
- Premium Apps - always require more

Sizing your Splunk architecture	Link to Splunk Lantern
Indexer CPU Specification	Link to Splunk Docs

© 2025 SPLUNK LLC

System Architecture

Network

- Minimum recommendation is : 1Gbit, idx < 100ms, sh < 200ms
- More is better
- Among the Splunk infrastructure, 10Gbit is likely a reasonable minimum
- Competing aspects
  - Indexers
    - Ingest can be extremely high
    - Bucket replication among indexers leaches bandwidth
    - Search results returns
  - Search heads
    - Interactive workload is low
    - Copying search bundles with large KV/lookups can be significant
    - Search results returns

Sizing your Splunk architecture	Link to Splunk Lantern
Network latency limits for clustered deployments	Link to Splunk Docs

© 2025 SPLUNK LLC

Workshop Agenda

- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
  - Lab^1
  - Lab^2
  - Lab^3
  - Lab^4 - Lab^6
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

Search Workload

Affects

- Bigger search workload = the bigger indexers required
- Competition between search and ingest is a balancing act
- Understanding where search workload comes from is essential
  - Savedsearches (Premium app and user-generated)
  - Poor SPL hygeine (especially if in a frequently run savedsearch)
  - Skipped searches can indicate insufficient resources at either the search head or the indexer - can also be slow networking …
- In summary, understanding the search workload can help troubleshoot whether the issue is search- or indexer-related

Reducing search load	https://lantern.splunk.com/Splunk_Platform/Splunk_Outcome_Paths/Reduce_Costs/Reducing_search_load
How search types affect Splunk Enterprise performance	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/HowsearchtypesaffectSplunkEnterpriseperformance
How concurrent users and searches impact performance	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Accommodatemanysimultaneoussearches

© 2025 SPLUNK LLC

Scale-up or Scale-out

That is the question …

- Appropriate sizing
  - Based on predicted ingest and search workload
  - Can be affected by new requirements, beyond what was initially envisioned for Splunk
- Watch the indexer CPU and RAM usage
  - If RAM is hitting the maximum on the system, scale-up
  - If CPU is hitting the maximum on the system, scale-out
  - If network traffic is tied, upgrade network
  - If storage is tied, upgrade storage, adjust workload (slow Cold/Frozen)
- Reasonable suggestions to start with, but there are more subtle variations, not in scope

Determine when to scale your Splunk Enterprise deployment	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Performancechecklist
Scalability in IT: The Complete Guide To Scaling	https://www.splunk.com/en_us/blog/learn/scalability.html
Determine when to scale your Splunk Enterprise deployment	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Performancechecklist
Indexing and search architecture	Link to Lantern

© 2025 SPLUNK LLC

Workshop Agenda

- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
    - Lab^1
    - Lab^2
    - Lab^3
    - Lab^4 - Lab^6
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

Detect Performance issues

Tools

- Splunk monitors (Monitoring Console, custom dashboards)
  - MC: Indexing:Performance:[Instance|Advanced|Deployment]
  - MC:Indexing:Indexer Clustering:[Status|Service Activity]
  - MC:Indexing:Indexes and Volumes:*
  - MC:Indexing:Inputs:*
- OS tools - on system
  - Top/glances/iostat/iftop/mtr
- OS tools - performance monitoring with agent off-host

Monitoring Splunk Enterprise	https://docs.splunk.com/Documentation/Splunk/9.3.2/DMC/DMCoverview
NixCraft System Monitoring Tools	https://www.cyberciti.biz/tips/top-linux-monitoring-tools.html
Glances	https://github.com/nicolargo/glances
Linux interface analytics on-demand with iftop	https://www.redhat.com/en/blog/linux-interface-iftop

© 2025 SPLUNK LLC

Access the lab

Tools

- ‘ssh’ to the ‘jumphost’ as per the command in the lab guide/SHOW spreadsheet
  - ssh -p 2222 attendee@<your_assigned_IP>, password ‘5p1unk.conf’ or Windows App (putty)
- Access to the GUI on the MC and the Cluster Manager
  - Cluster Manager - http://<your_assigned_IP>:4501
  - Monitoring Console - http://<your_assigned_IP>:4505
  - For both - username = ‘admin’, password = ‘5p1unk.conf’

DO NOT USE THIS ANYWHERE ELSE - LAB ONLY

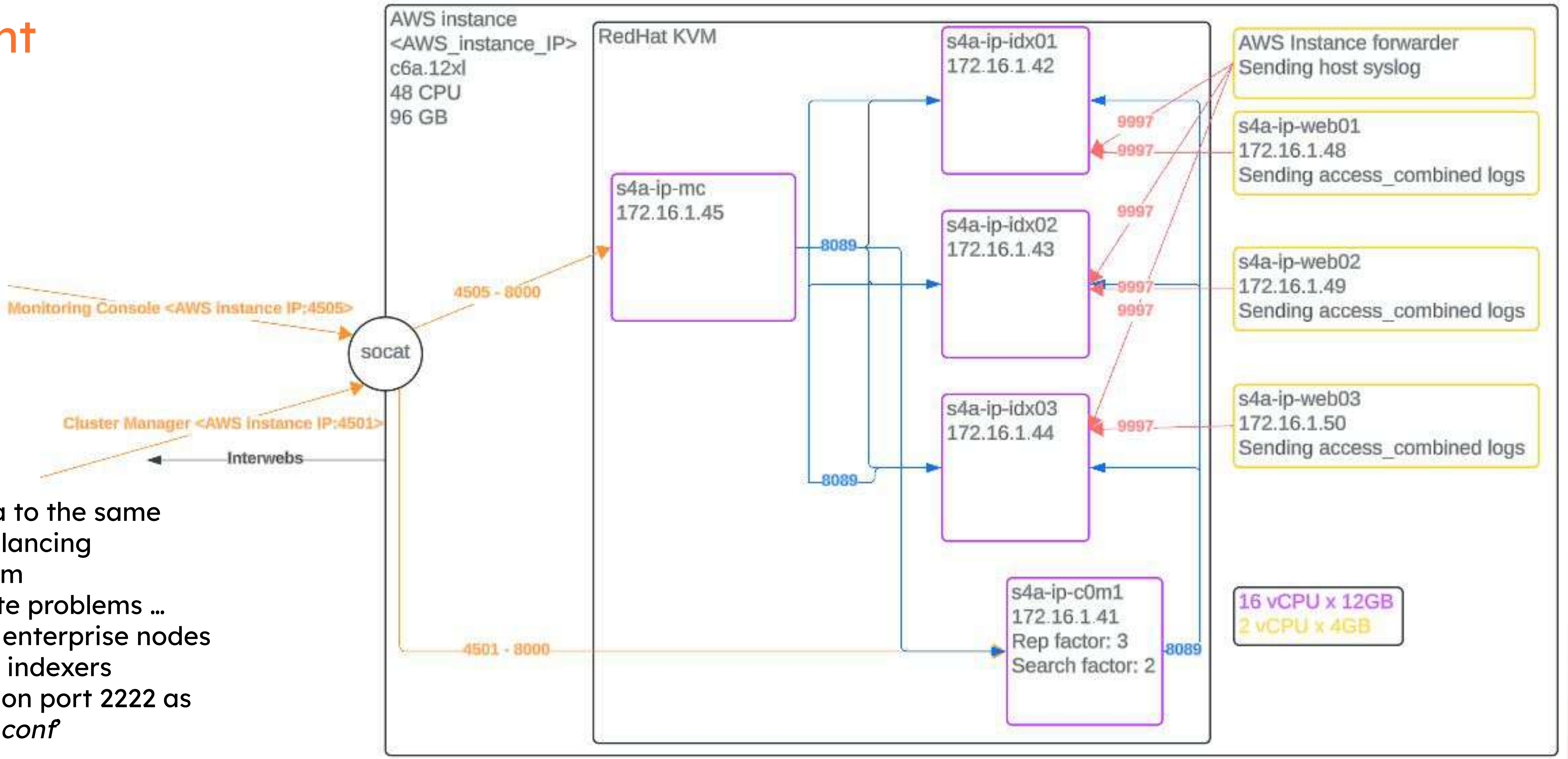
- Once on the jumphost, ssh to the hostname as necessary

Cluster Manager	s4a-ip-c0m1 (172.16.1.41)	Indexer 03	s4a-ip-idx01 (172.16.1.44)
Indexer 01	s4a-ip-idx01 (172.16.1.42)	Monitoring Console	s4a-ip-idx01 (172.16.1.45)
Indexer 02	s4a-ip-idx02 (172.16.1.43)	Load generators web01,2,3	s4a-ip-web0[1,2,3] (172.16.1.48,49,50)

© 2025 SPLUNK LLC

Detect Performance issues

Lab environment



Note:

- Each “web” server sends data to the same numbered indexer. No loadbalancing
- Ensures consistent data stream
- Permits manipulation to create problems …
- Syslog and perf metrics from enterprise nodes loadbalanced across all three indexers
- ssh to the <AWS instance IP> on port 2222 as *‘attendee’*, password ‘*5p1unk.conf*’
- Web GUI
  - Cluster Manager <AWS instance IP>:4501
  - Monitoring Console <AWS instance IP>:4501

© 2025 SPLUNK LLC

Workshop Agenda

- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
    - Lab^1
    - Lab^2
    - Lab^3
    - Lab^{4} - Lab^{6}
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

Access the lab

Lab1

Tools

- Likely be useful to have multiple open ssh sessions (one each) into each of the indexers (1, 2, and 3) as well as the cluster manager (c0m1)
- A GUI login into the Monitoring Console (MC)
- Explore the different instances in the CLI with the different commands
- The MC will be used to explore both Splunk performance and machine performance

© 2025 SPLUNK LLC

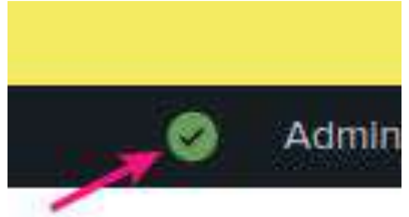
Detect Performance issues

Lab1

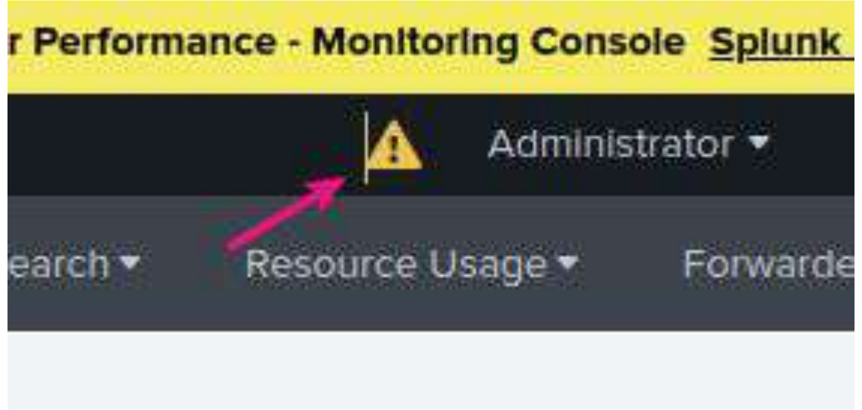
Tools: Splunk

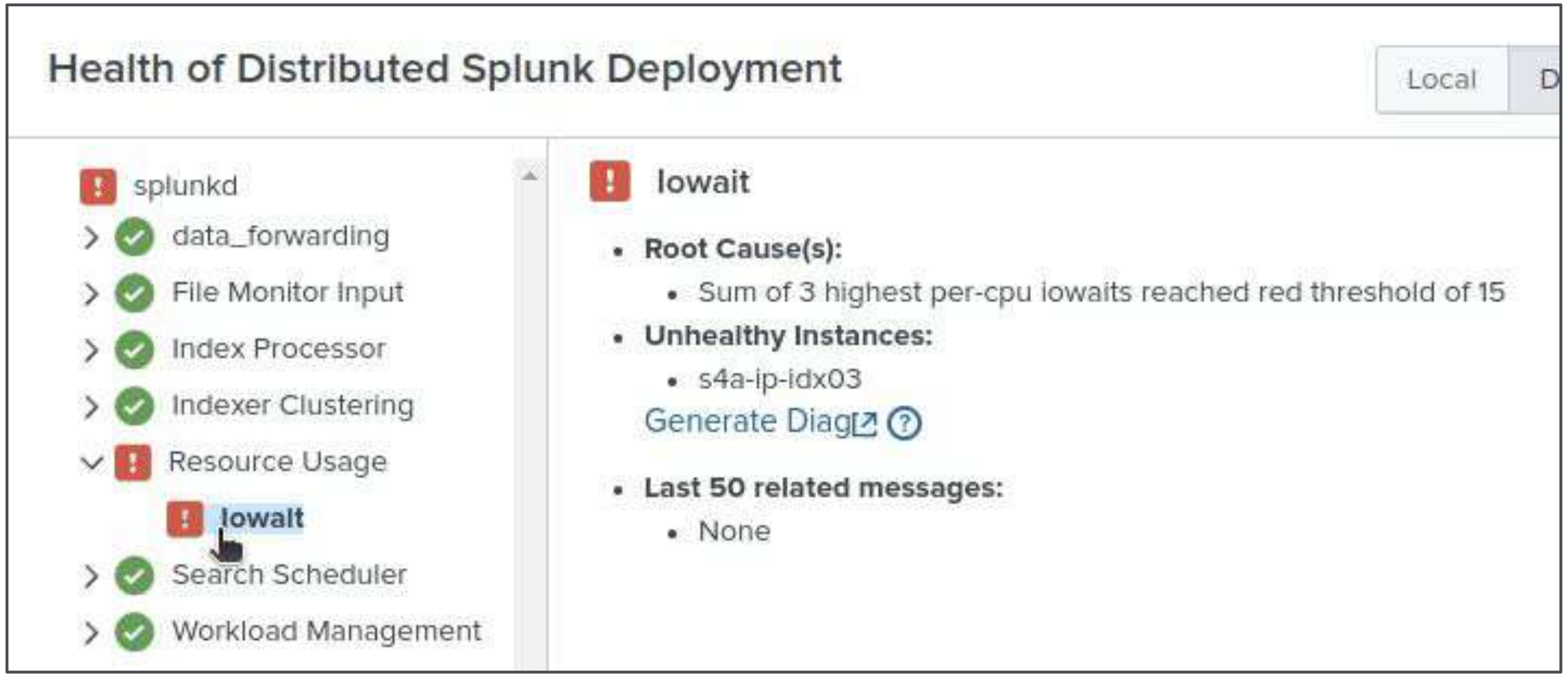
- Alert Dropdown

Healthy



Un-Healthy





Health of Distributed Splunk Deployment

Iowait

- **Root Cause(s):**
  - Sum of 3 highest per-cpu iowaits reached red threshold of 15
- **Unhealthy Instances:**
  - s4a-ip-idx03

  Generate Diag
- **Last 50 related messages:**
  - None

Monitoring Splunk Enterprise with MC	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
MC Summary/Overview	https://docs.splunk.com/Documentation/Splunk/latest/DMC/HowtheDMCworks

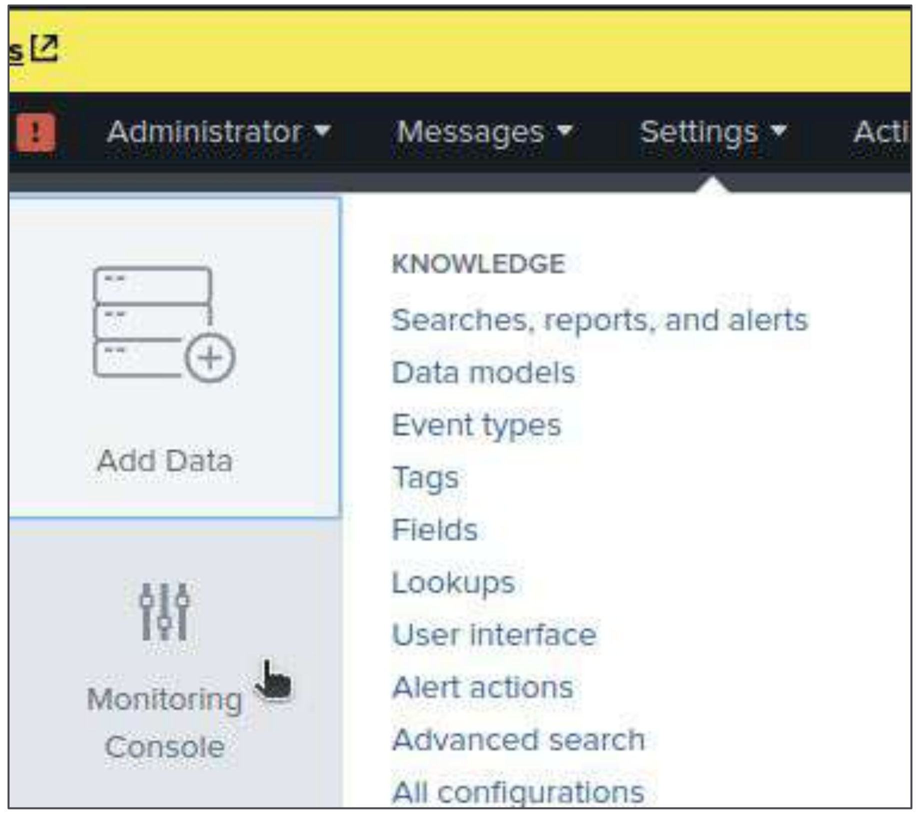
© 2025 SPLUNK LLC

Detect Performance issues

Lab1

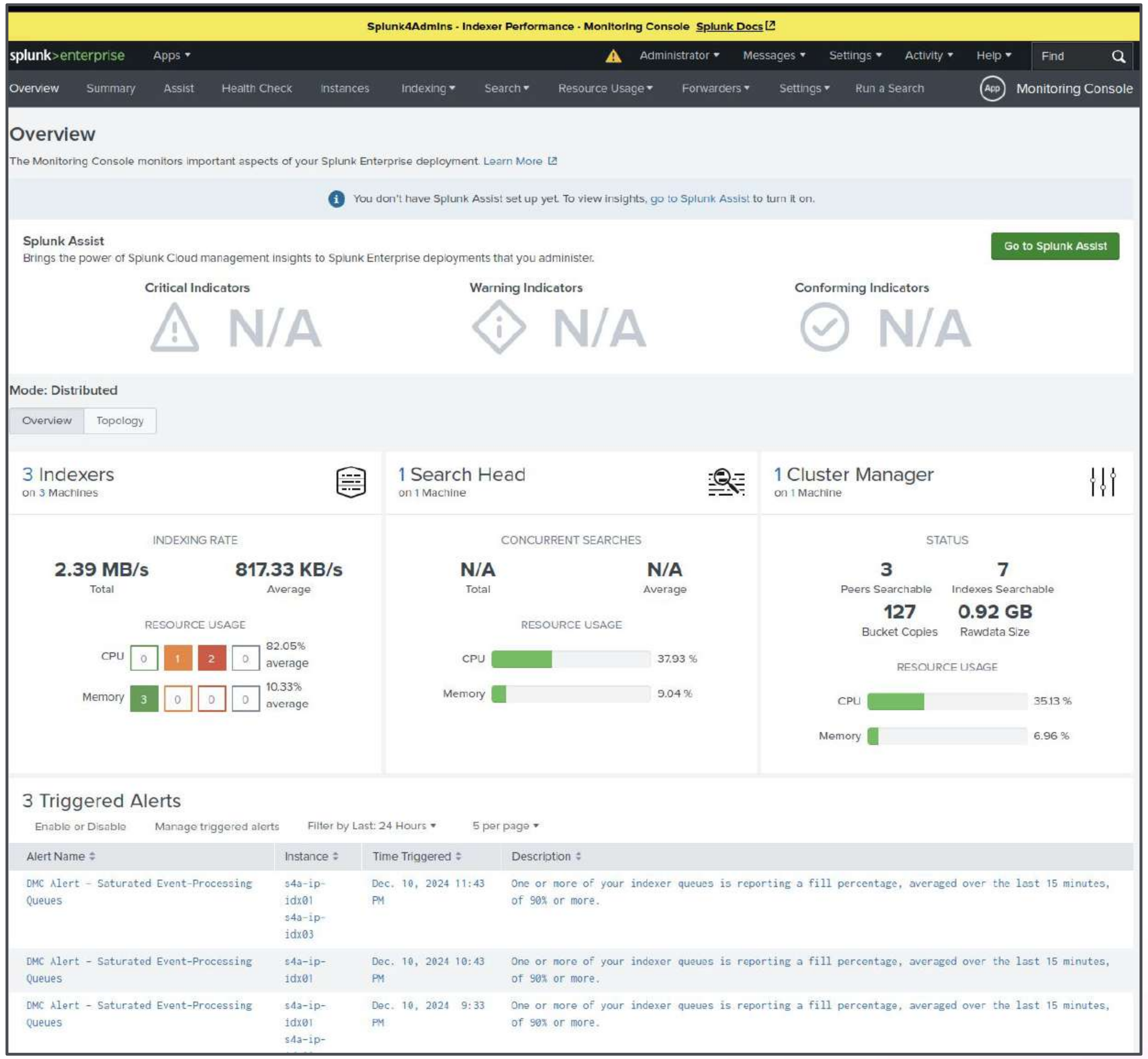
Tools: Splunk

- MC: Overview



KNOWLEDGE

Searches, reports, and alerts
Data models
Event types
Tags
Fields
Lookups
User interface
Alert actions
Advanced search
All configurations



Overview

The Monitoring Console monitors important aspects of your Splunk Enterprise deployment. Learn More

You don't have Splunk Assist set up yet. To view insights, go to Splunk Assist to turn it on.

Splunk Assist

Brings the power of Splunk Cloud management insights to Splunk Enterprise deployments that you administer.

Critical Indicators N/A

Warning Indicators N/A

Conforming Indicators N/A

Mode: Distributed

3 Indexers on 3 Machines

INDEXING RATE: 2.39 MB/s Total; 817.33 KB/s Average

RESOURCE USAGE

CPU 0 1 2 0 82.05% average

Memory 3 0 0 0 10.33% average

1 Search Head on 1 Machine

CONCURRENT SEARCHES: N/A Total; N/A Average

RESOURCE USAGE

CPU 37.93 %

Memory 9.04 %

1 Cluster Manager on 1 Machine

STATUS: 3 Peers Searchable; 7 Indexes Searchable; 127 Bucket Copies; 0.92 GB Rawdata Size

RESOURCE USAGE

CPU 35.13 %

Memory 6.96 %

3 Triggered Alerts

Alert Name	Instance	Time Triggered	Description
DMC Alert - Saturated Event-Processing Queues	s4a-ip-idx01 s4a-ip-idx03	Dec. 10, 2024 11:43 PM	One or more of your indexer queues is reporting a fill percentage, averaged over the last 15 minutes, of 90% or more.
DMC Alert - Saturated Event-Processing Queues	s4a-ip-idx01	Dec. 10, 2024 10:43 PM	One or more of your indexer queues is reporting a fill percentage, averaged over the last 15 minutes, of 90% or more.
DMC Alert - Saturated Event-Processing Queues	s4a-ip-idx01 s4a-ip-	Dec. 10, 2024 9:33 PM	One or more of your indexer queues is reporting a fill percentage, averaged over the last 15 minutes, of 90% or more.

Monitoring Splunk Enterprise with MC	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
MC Summary/Overview	https://docs.splunk.com/Documentation/Splunk/latest/DMC/HowtheDMCwork

© 2025 SPLUNK LLC

Detect Performance issues

Tools: Splunk

- When addressing Indexing Performance …
- MC Indexing Performance Dashboards
  - Instance - specific to each Splunk indexer instance
  - Advanced - deeper dive into each indexer, including increased resolution CPU analysis, thread, pipeline, sourcetype performance
  - Deployment - Overview to provide both configuration and high-level knowledge leading to where the actual performance issue may be
- MC Indexer Clustering dashboards
  - Status - Much of the same information as from the Cluster Manager, just not accessing the CM directly
  - Service Activity - detect errors and administrative activities such as Fixup Tasks
- Resource Usage
  - Instance and Machine

Monitoring Splunk Enterprise with MCc	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
MC Summary/Overview	https://docs.splunk.com/Documentation/Splunk/latest/DMC/Summary
Indexing: Performance	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexingDeployment

© 2025 SPLUNK LLC

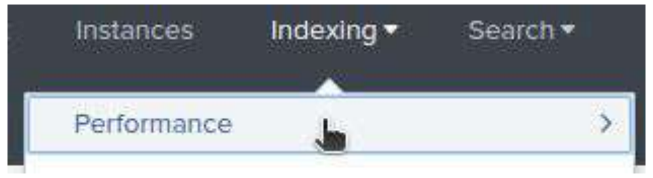
Workshop Agenda

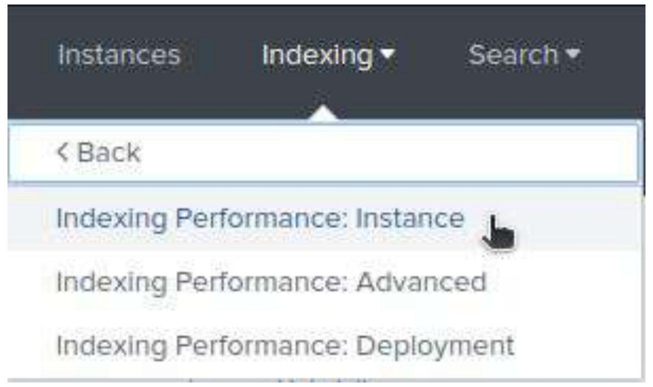
- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
  - Lab^1
  - Lab^2
  - Lab^3
  - Lab^{4} $^{-}$ Lab^6
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

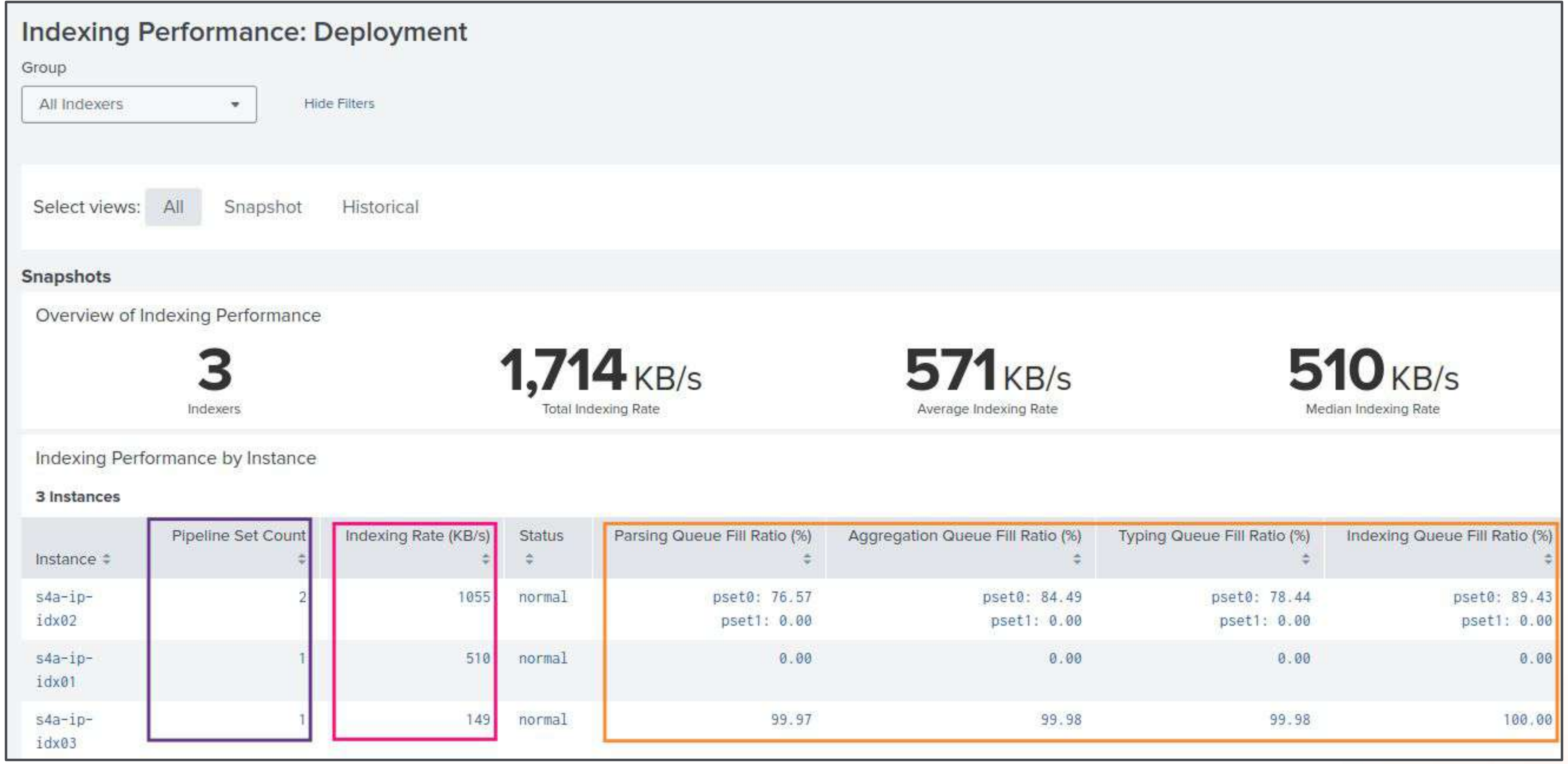
Detect Performance issues

Tools: SplunkMC:IP:Deployment




Instances
Indexing ▾
Search ▾
‹ Back
Indexing Performance: Instance
Indexing Performance: Advanced
Indexing Performance: Deployment

- Dashboards on IP:Deployment
- Get a direction on where issues exist
- Understand where outliers exist
- Purple - base configuration of indexers
- Pink - ingest rate of each indexers
- Orange - Queue fill percentages


Indexing Performance: Deployment
Group
All Indexers ▾
Hide Filters
Select views: All Snapshot Historical

Snapshots

Overview of Indexing Performance

3 Indexers

1,714 KB/s Total Indexing Rate

571 KB/s Average Indexing Rate

510 KB/s Median Indexing Rate

Indexing Performance by Instance

3 Instances

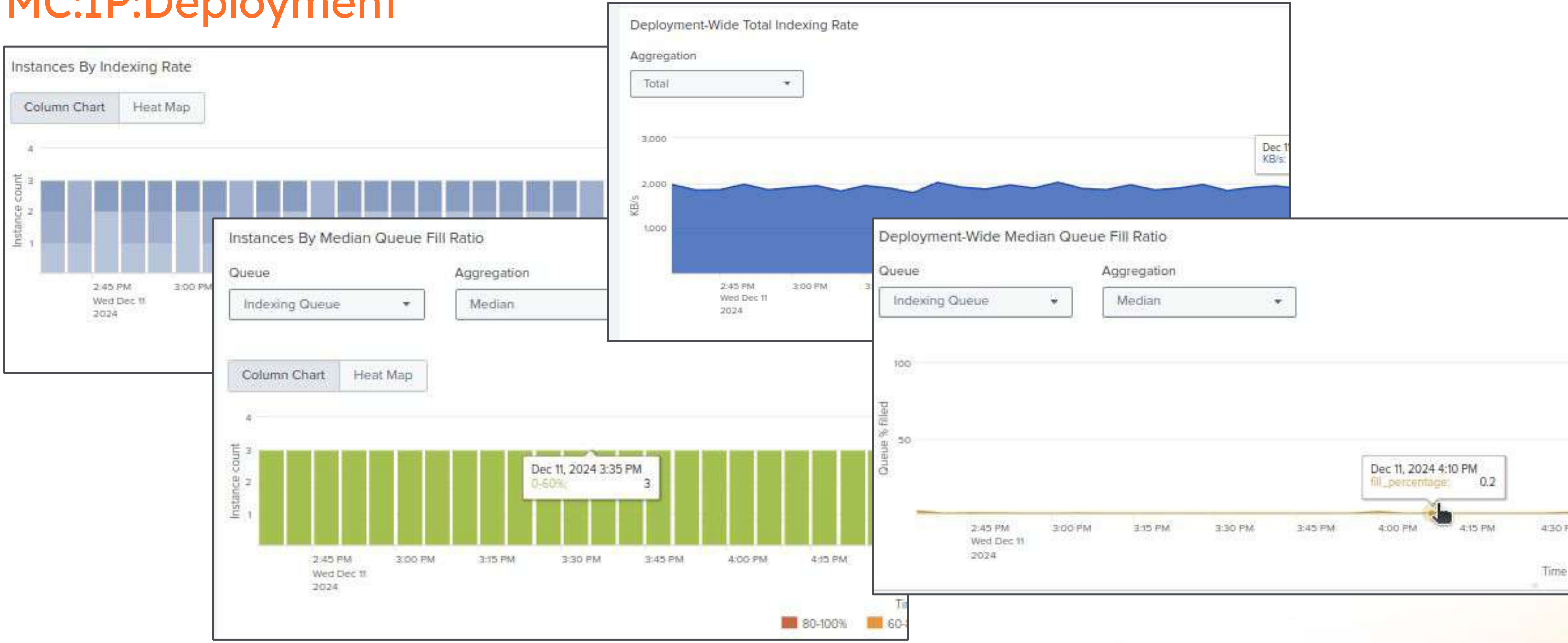
Instance	Pipeline Set Count	Indexing Rate (KB/s)	Status	Parsing Queue Fill Ratio (%)	Aggregation Queue Fill Ratio (%)	Typing Queue Fill Ratio (%)	Indexing Queue Fill Ratio (%)
s4a-ip-idx02	2	1055	normal	pset0: 76.57 pset1: 0.00	pset0: 84.49 pset1: 0.00	pset0: 78.44 pset1: 0.00	pset0: 89.43 pset1: 0.00
s4a-ip-idx01	1	510	normal	0.00	0.00	0.00	0.00
s4a-ip-idx03	1	149	normal	99.97	99.98	99.98	100.00

Monitoring Splunk Enterprise with MC	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Indexing: Performance	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexingDeployment

© 2025 SPLUNK LLC

Detect Performance issues

Tools: Splunk: MC:IP:Deployment



Instances By Indexing Rate

Column Chart | Heat Map

Deployment-Wide Total Indexing Rate

Aggregation: Total

Instances By Median Queue Fill Ratio

Queue: Indexing Queue

Aggregation: Median

Column Chart | Heat Map

Dec 11, 2024 3:35 PM
0-60%: 3

Deployment-Wide Median Queue Fill Ratio

Queue: Indexing Queue

Aggregation: Median

Dec 11, 2024 4:10 PM
fill_percentage: 0.2

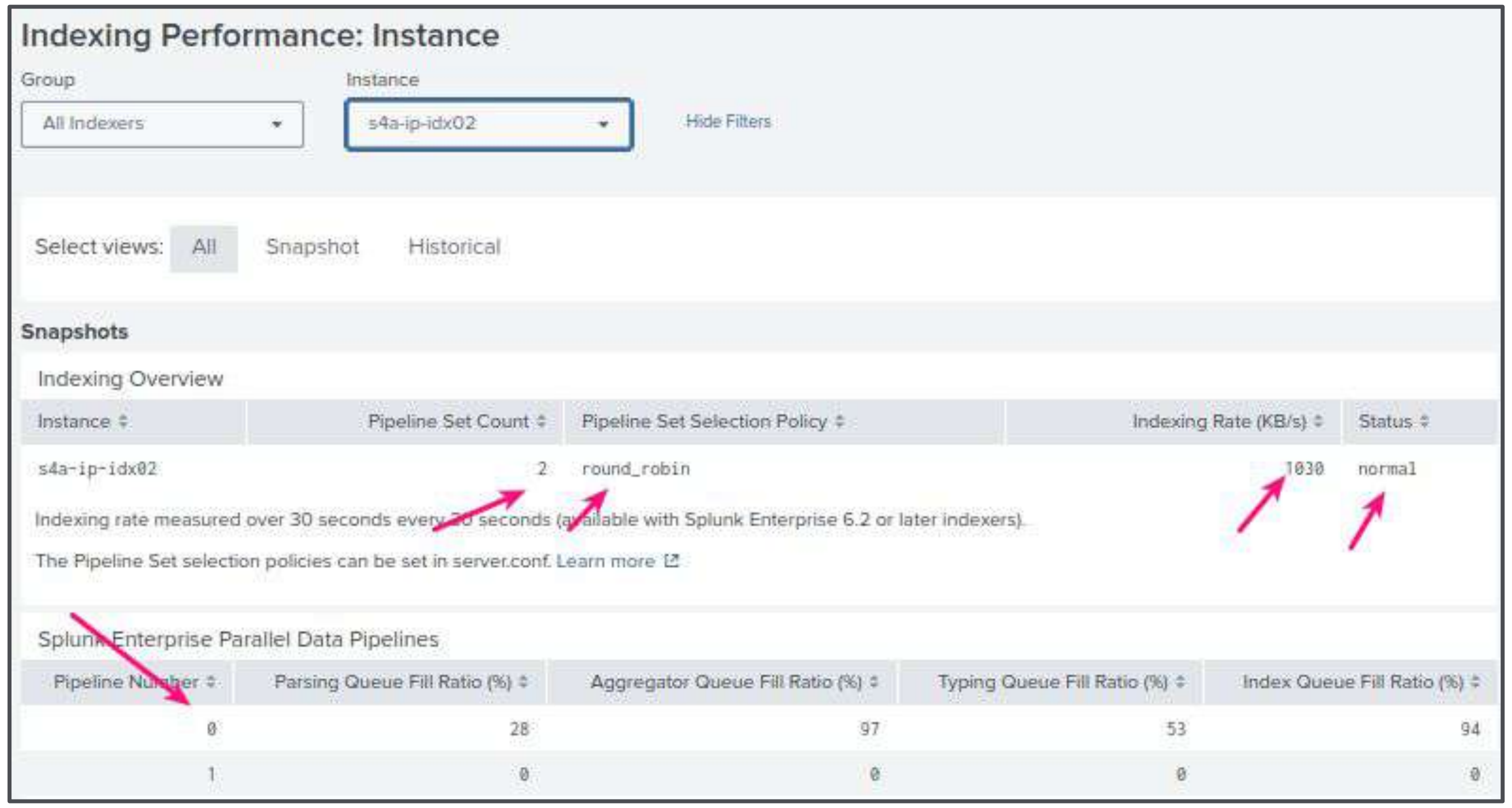
- Get a feel for overall performance
- Find outliers in the environment, especially over time
- Discover point-source events that have caused changes in performance

Monitoring Splunk Enterprise with MCc	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Indexing: Performance	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexingDeployment

© 2025 SPLUNK LLC

Detect Performance issues

Tools: Splunk: MC:IP:Instance



Indexing Performance: Instance

Group: All Indexers
Instance: s4a-ip-idx02

Select views: All Snapshot Historical

Snapshots

Indexing Overview

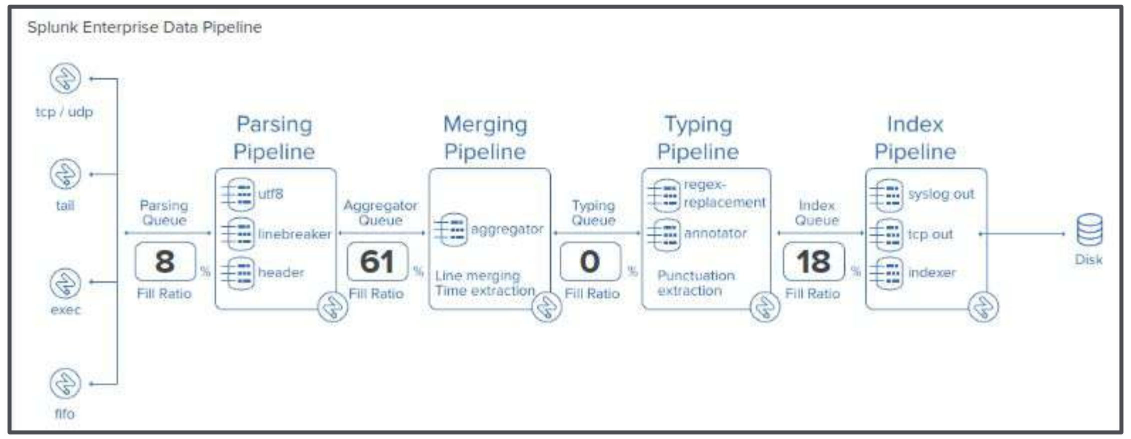
Instance	Pipeline Set Count	Pipeline Set Selection Policy	Indexing Rate (KB/s)	Status
s4a-ip-idx02	2	round_robin	1030	normal

Indexing rate measured over 30 seconds every 30 seconds (available with Splunk Enterprise 6.2 or later indexers).

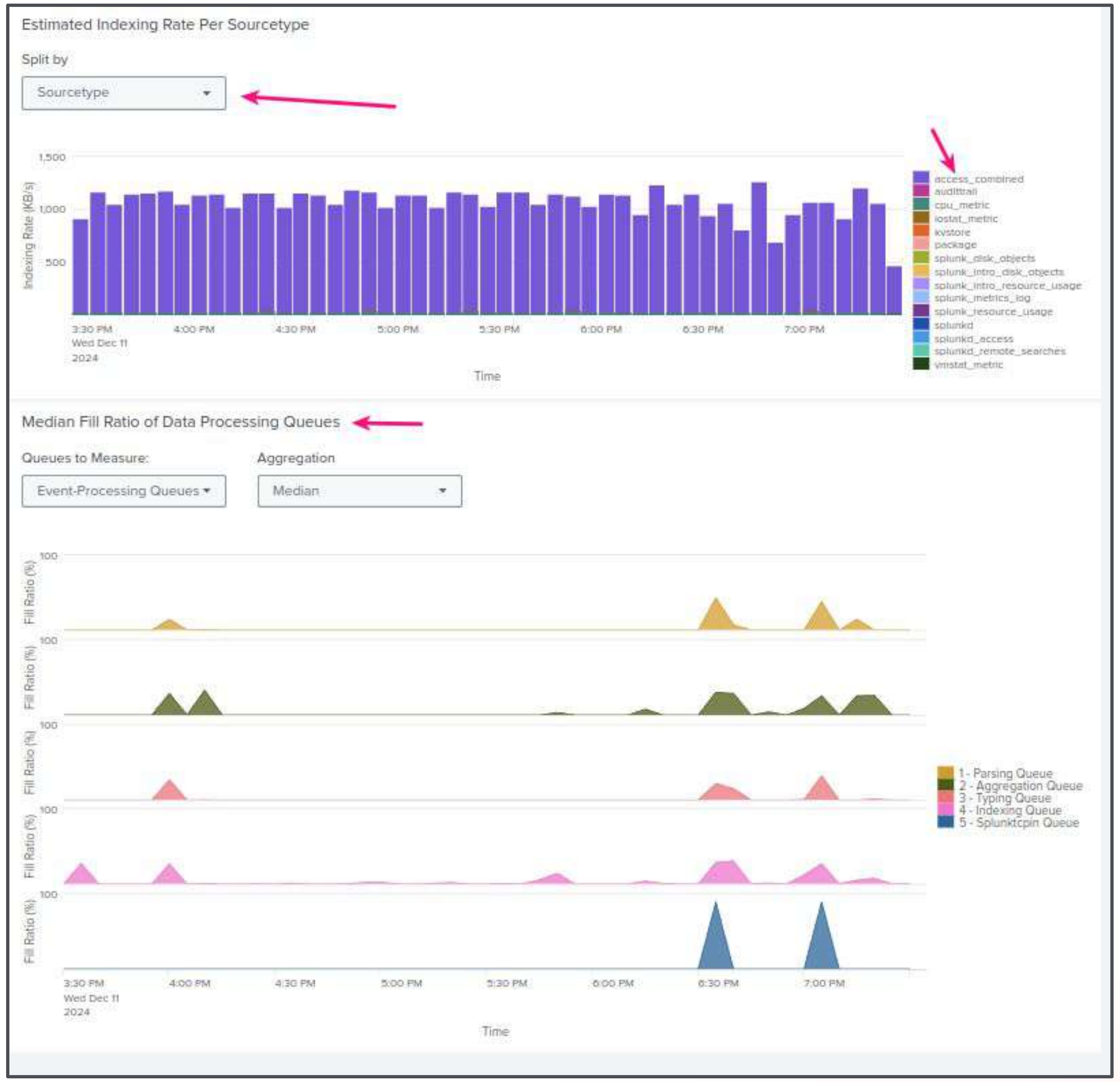
The Pipeline Set selection policies can be set in server.conf. Learn more

Splunk Enterprise Parallel Data Pipelines

Pipeline Number	Parsing Queue Fill Ratio (%)	Aggregator Queue Fill Ratio (%)	Typing Queue Fill Ratio (%)	Index Queue Fill Ratio (%)
0	28	97	53	94
1	0	0	0	0



Splunk Enterprise Data Pipeline



Estimated Indexing Rate Per Sourcetype

Split by: Sourcetype

Median Fill Ratio of Data Processing Queues

Queues to Measure: Event-Processing Queues
Aggregation: Median

Monitoring Splunk Enterprise with MCc	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Indexing: Performance	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexingDeployment

© 2025 SPLUNK LLC

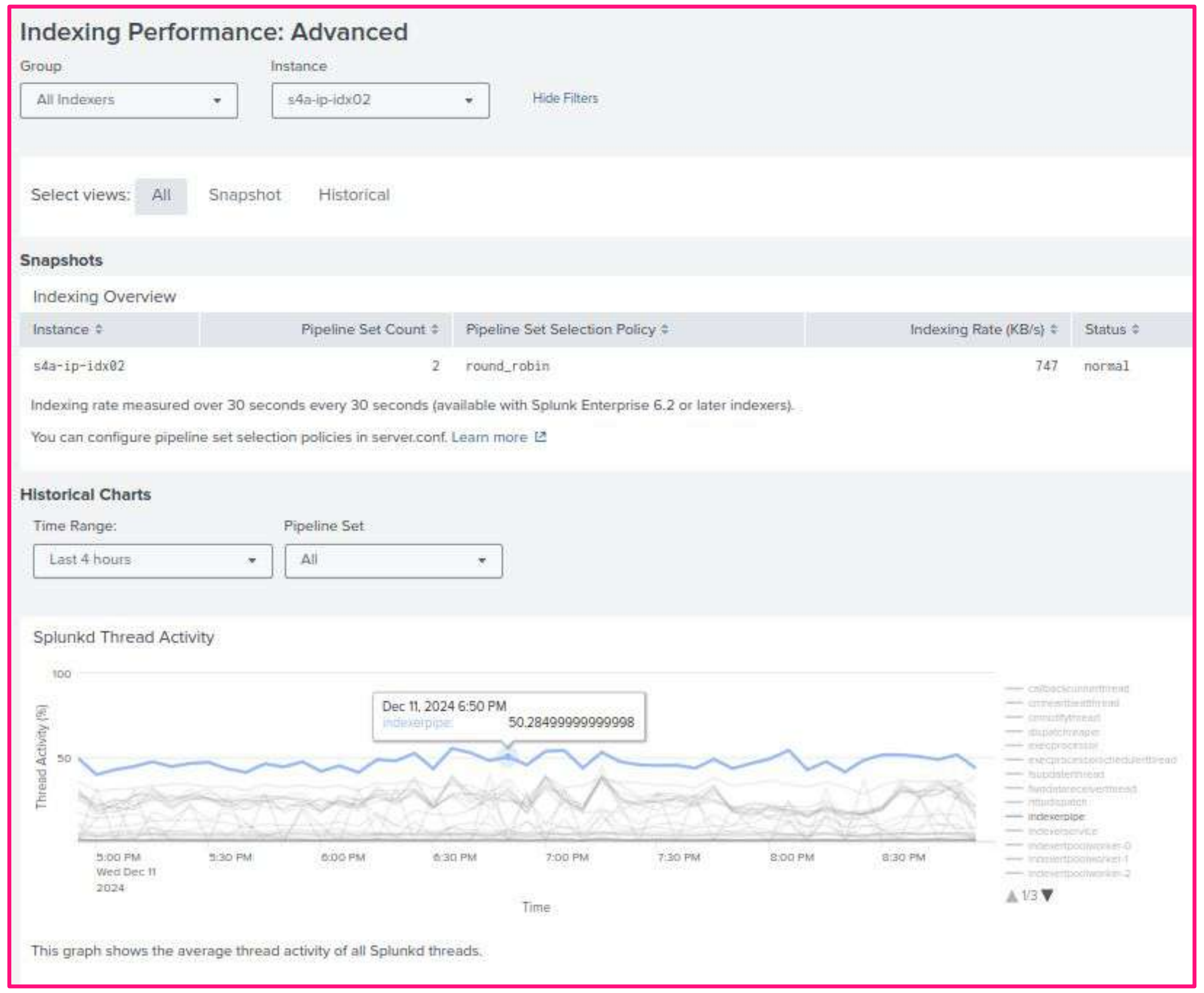
Workshop Agenda

- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
  - Lab^1
  - Lab^2
  - Lab^3
  - Lab^{4} - Lab^6
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

Detect Performance issues

Tools: Splunk: MC:IP:Advanced



Indexing Performance: Advanced

Group: All Indexers

Instance: s4a-ip-idx02

Hide Filters

Select views: All Snapshot Historical

Snapshots

Indexing Overview

Instance	Pipeline Set Count	Pipeline Set Selection Policy	Indexing Rate (KB/s)	Status
s4a-ip-idx02	2	round_robin	747	normal

Indexing rate measured over 30 seconds every 30 seconds (available with Splunk Enterprise 6.2 or later indexers).

You can configure pipeline set selection policies in server.conf. Learn more

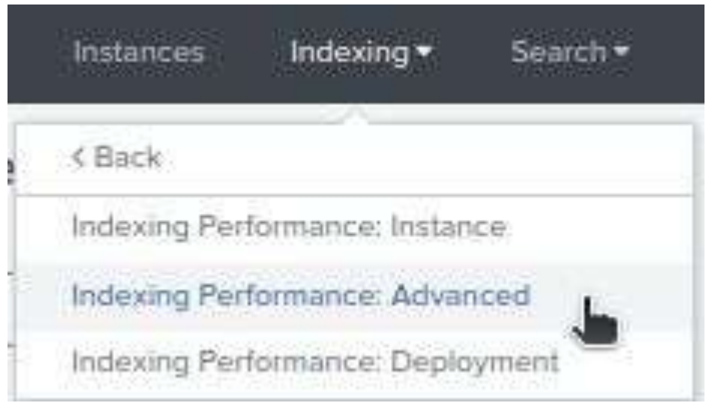
Historical Charts

Time Range: Last 4 hours

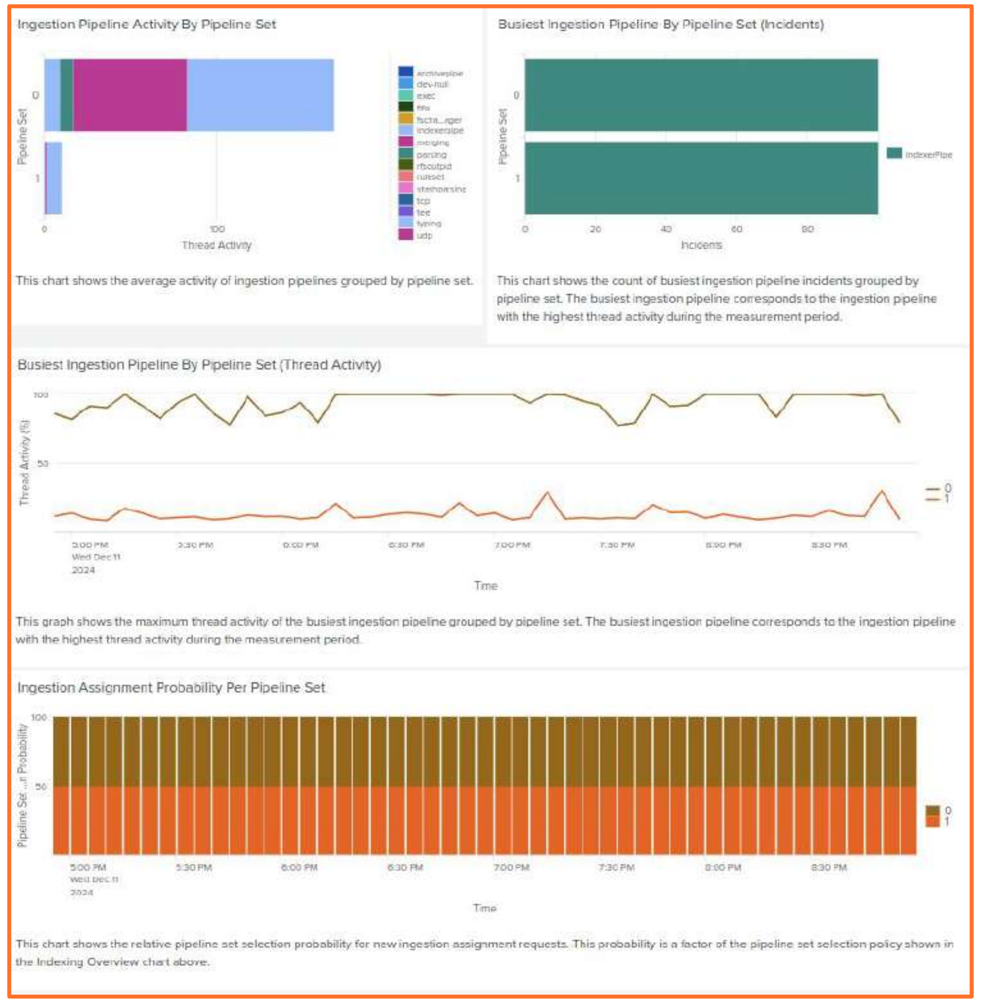
Pipeline Set: All

Splunkd Thread Activity

This graph shows the average thread activity of all Splunkd threads.



Instances
Indexing ▾
Search ▾
‹ Back
Indexing Performance: Instance
Indexing Performance: Advanced
Indexing Performance: Deployment



Ingestion Pipeline Activity By Pipeline Set

This chart shows the average activity of ingestion pipelines grouped by pipeline set.

Busiest Ingestion Pipeline By Pipeline Set (Incidents)

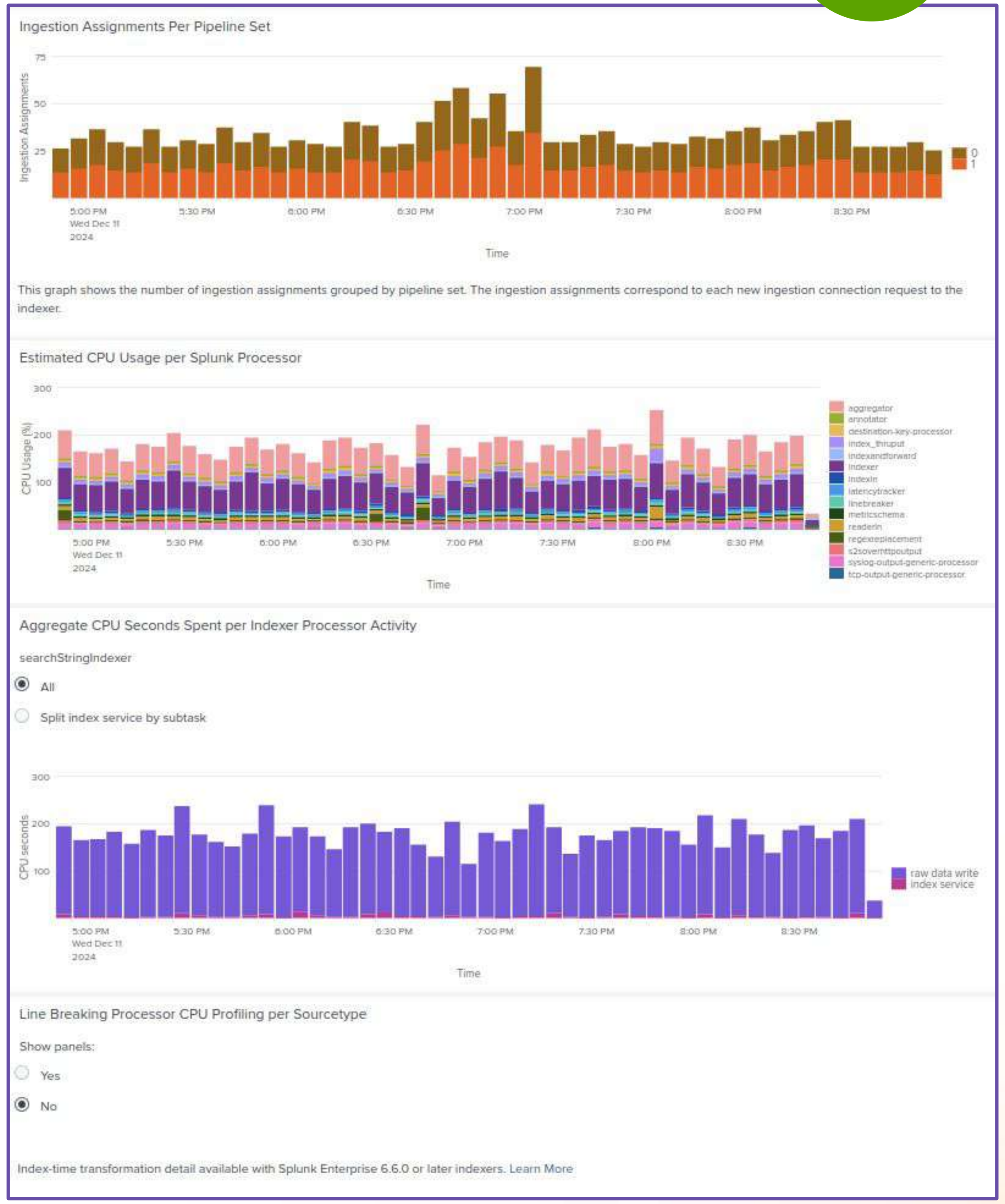
This chart shows the count of busiest ingestion pipeline incidents grouped by pipeline set. The busiest ingestion pipeline corresponds to the ingestion pipeline with the highest thread activity during the measurement period.

Busiest Ingestion Pipeline By Pipeline Set (Thread Activity)

This graph shows the maximum thread activity of the busiest ingestion pipeline grouped by pipeline set. The busiest ingestion pipeline corresponds to the ingestion pipeline with the highest thread activity during the measurement period.

Ingestion Assignment Probability Per Pipeline Set

This chart shows the relative pipeline set selection probability for new ingestion assignment requests. This probability is a factor of the pipeline set selection policy shown in the Indexing Overview chart above.



Ingestion Assignments Per Pipeline Set

This graph shows the number of ingestion assignments grouped by pipeline set. The ingestion assignments correspond to each new ingestion connection request to the indexer.

Estimated CPU Usage per Splunk Processor

Aggregate CPU Seconds Spent per Indexer Processor Activity

searchStringIndexer

● All

○ Split index service by subtask

Line Breaking Processor CPU Profiling per Sourcetype

Show panels:

○ Yes

● No

Index-time transformation detail available with Splunk Enterprise 6.6.0 or later indexers. Learn More

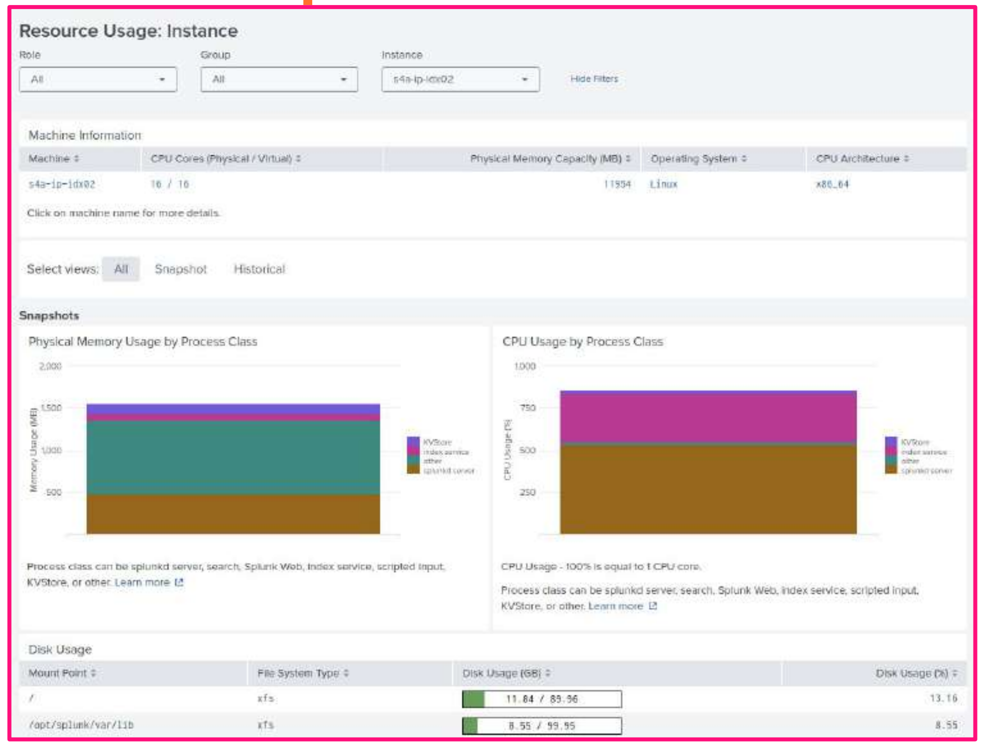
Monitoring Splunk Enterprise with MCc	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Indexing: Performance	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexingDeployment

© 2025 SPLUNK LLC

Detect Performance issues

Lab³

Tools: Splunk: MC:Resource Usage:Instance



Resource Usage: Instance

Role: All | Group: All | Instance: s4a-ip-idx02 | Hide Filters

Machine Information

Machine	CPU Cores (Physical / Virtual)	Physical Memory Capacity (MB)	Operating System	CPU Architecture
s4a-ip-idx02	16 / 16	11954	Linux	x86_64

Click on machine name for more details.

Select views: All Snapshot Historical

Snapshots

Physical Memory Usage by Process Class

Process class can be splunkd server, search, Splunk Web, index service, scripted input, KVStore, or other. Learn more

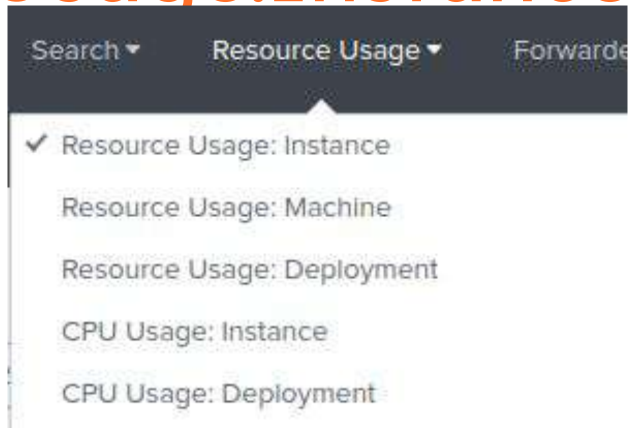
CPU Usage by Process Class

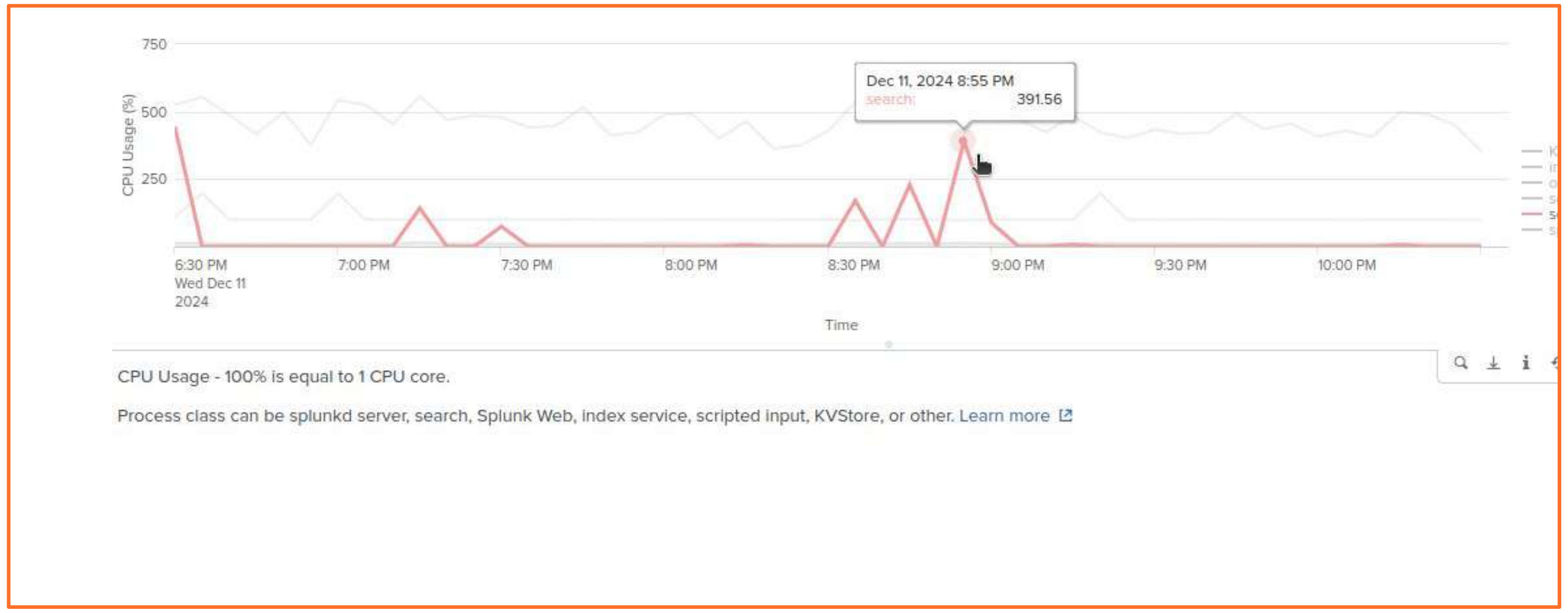
CPU Usage - 100% is equal to 1 CPU core.

Process class can be splunkd server, search, Splunk Web, index service, scripted input, KVStore, or other. Learn more

Disk Usage

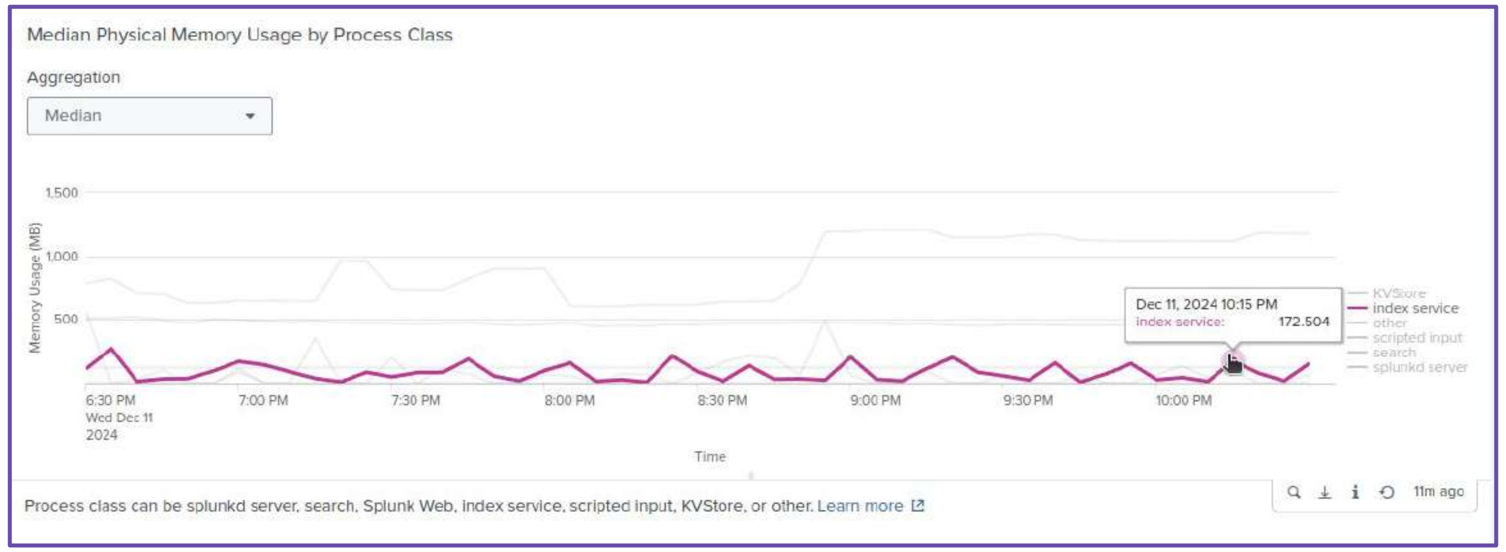
Mount Point	File System Type	Disk Usage (GB)	Disk Usage (%)
/	xfs	11.84 / 89.96	13.16
/opt/splunk/var/lib	xfs	8.55 / 99.95	8.55





CPU Usage - 100% is equal to 1 CPU core.

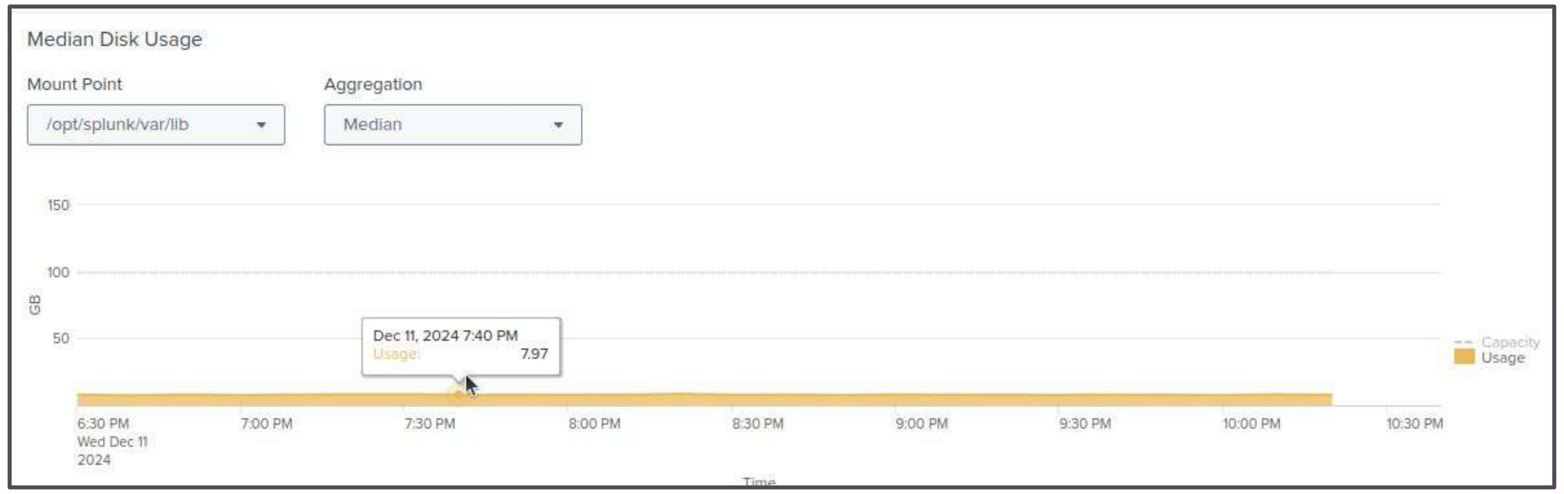
Process class can be splunkd server, search, Splunk Web, index service, scripted input, KVStore, or other. Learn more



Median Physical Memory Usage by Process Class

Aggregation: Median

Process class can be splunkd server, search, Splunk Web, index service, scripted input, KVStore, or other. Learn more



Median Disk Usage

Mount Point: /opt/splunk/var/lib

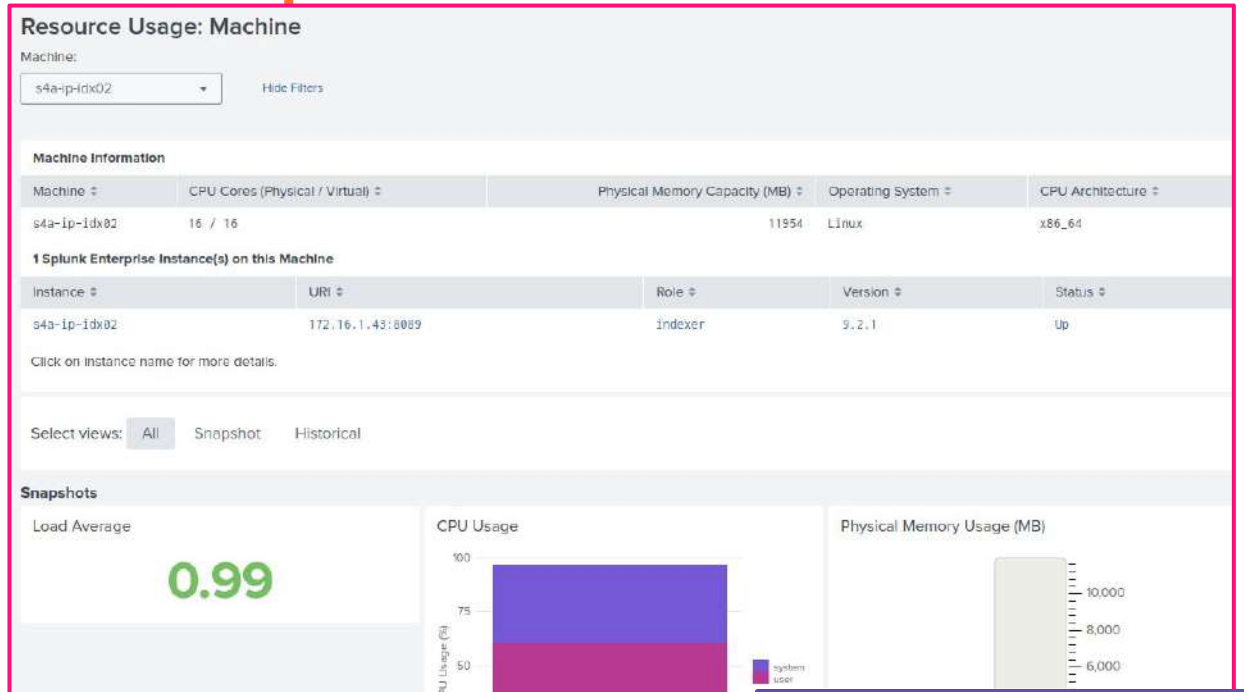
Aggregation: Median

Monitoring Splunk Enterprise with MC	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Resource Usage	https://docs.splunk.com/Documentation/Splunk/latest/DMC/ResourceusageDeployment

© 2025 SPLUNK LLC

Detect Performance issues

Tools: Splunk: MC:Resource Usage:Machine



Resource Usage: Machine

Machine: s4a-ip-idx02

Machine Information

Machine ⇕	CPU Cores (Physical / Virtual) ⇕	Physical Memory Capacity (MB) ⇕	Operating System ⇕	CPU Architecture ⇕
s4a-ip-idx02	16 / 16	11954	Linux	x86_64

1 Splunk Enterprise Instance(s) on this Machine

Instance ⇕	URI ⇕	Role ⇕	Version ⇕	Status ⇕
s4a-ip-idx02	172.16.1.43:8089	indexer	9.2.1	Up

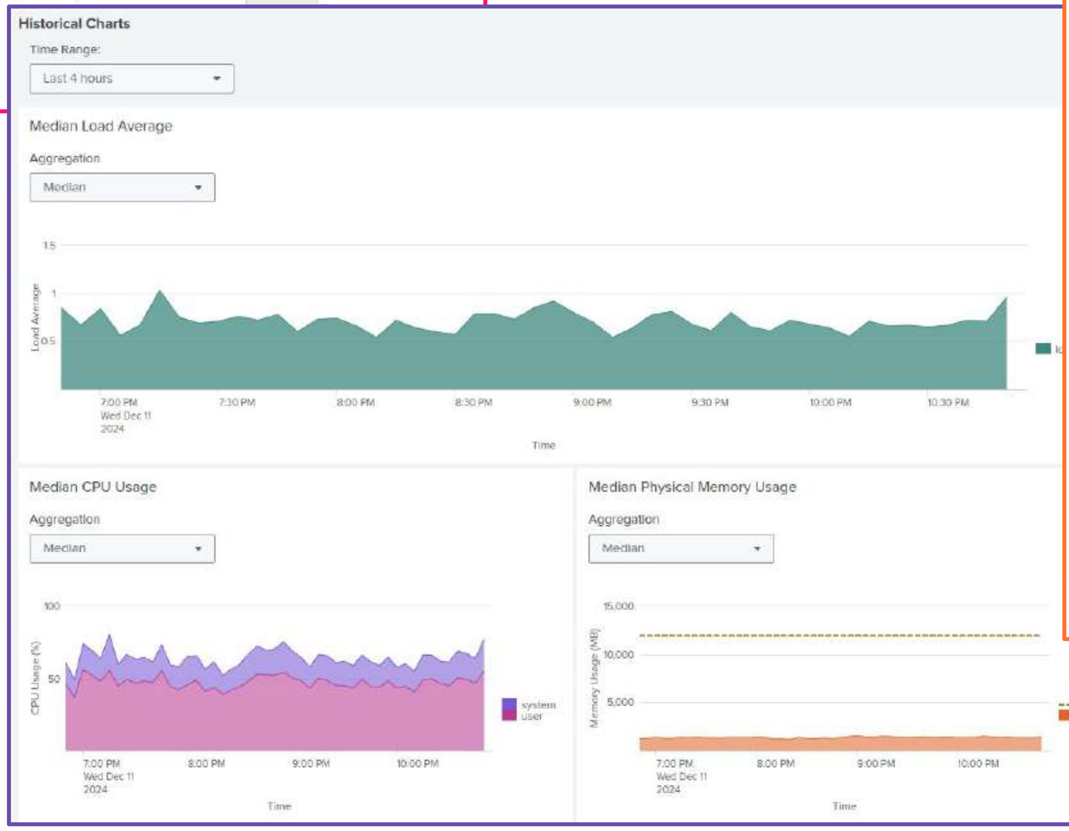
Click on instance name for more details.

Select views: All Snapshot Historical

Snapshots

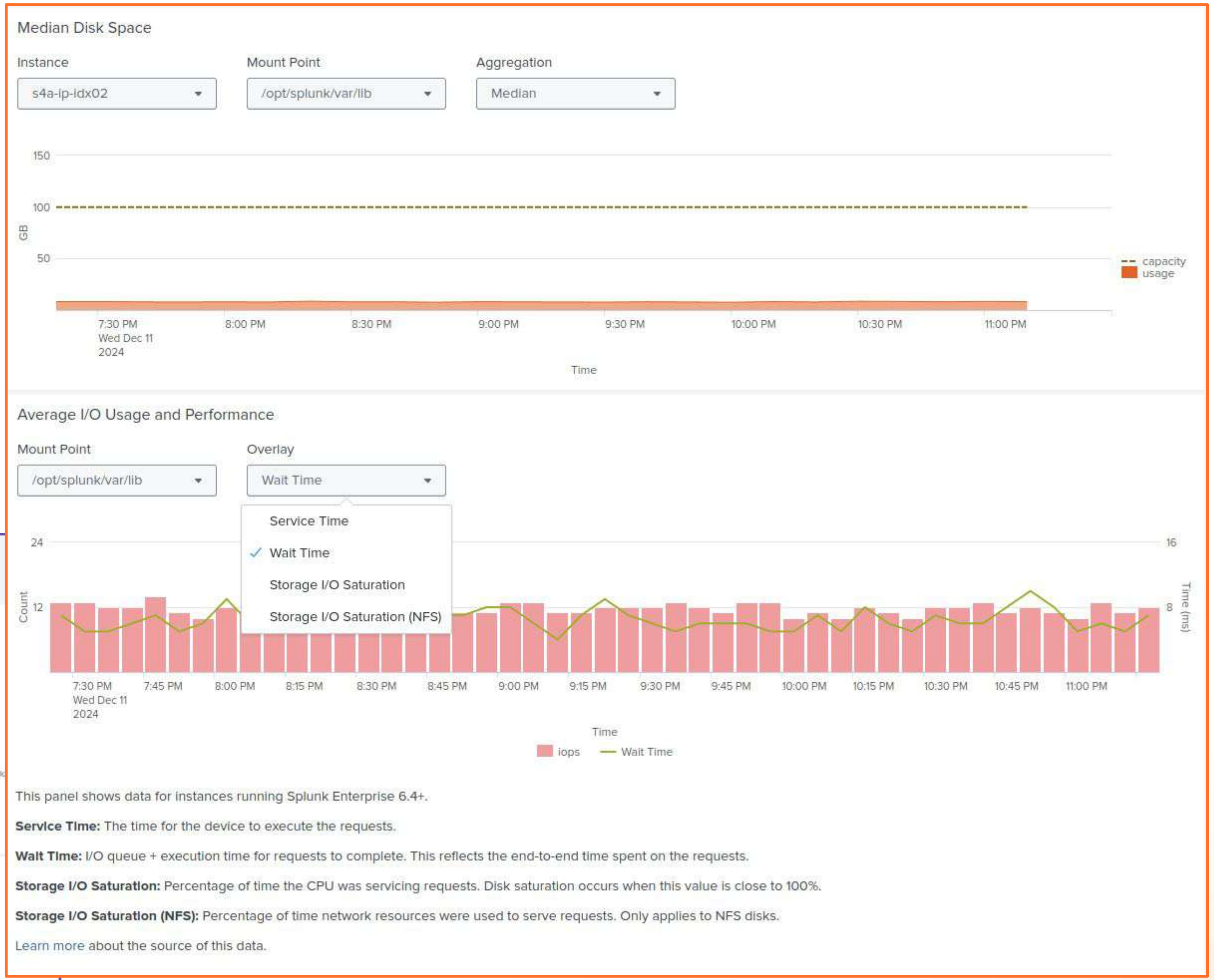
Load Average

0.99



Historical Charts

Time Range: Last 4 hours



Median Disk Space

Instance: s4a-ip-idx02 — Mount Point: /opt/splunk/var/lib — Aggregation: Median

Average I/O Usage and Performance

Mount Point: /opt/splunk/var/lib — Overlay: Wait Time

This panel shows data for instances running Splunk Enterprise 6.4+.

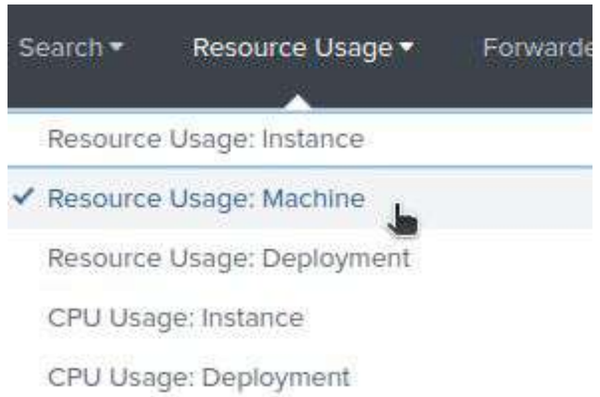
Service Time: The time for the device to execute the requests.

Wait Time: I/O queue + execution time for requests to complete. This reflects the end-to-end time spent on the requests.

Storage I/O Saturation: Percentage of time the CPU was servicing requests. Disk saturation occurs when this value is close to 100%.

Storage I/O Saturation (NFS): Percentage of time network resources were used to serve requests. Only applies to NFS disks.

Learn more about the source of this data.



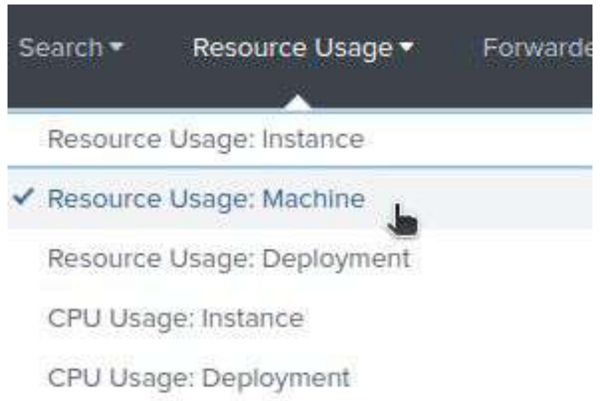
Monitoring Splunk Enterprise with MC	Link to Splunk Docs
Resource Usage	Link to Splunk Docs

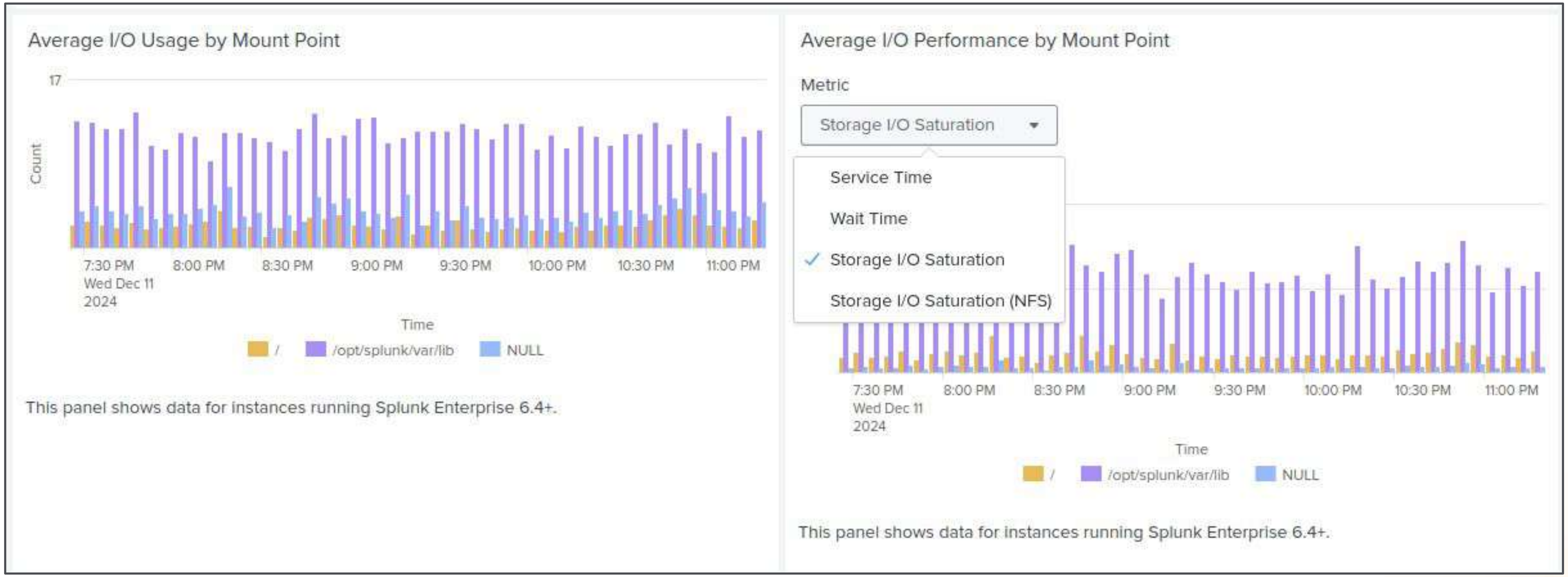
© 2025 SPLUNK LLC

Detect Performance issues

Lab3

Tools: Splunk: MC:Resource Usage:Machine





This panel shows data for instances running Splunk Enterprise 6.4+.

Metric: Storage I/O Saturation ▾

This panel shows data for instances running Splunk Enterprise 6.4+.

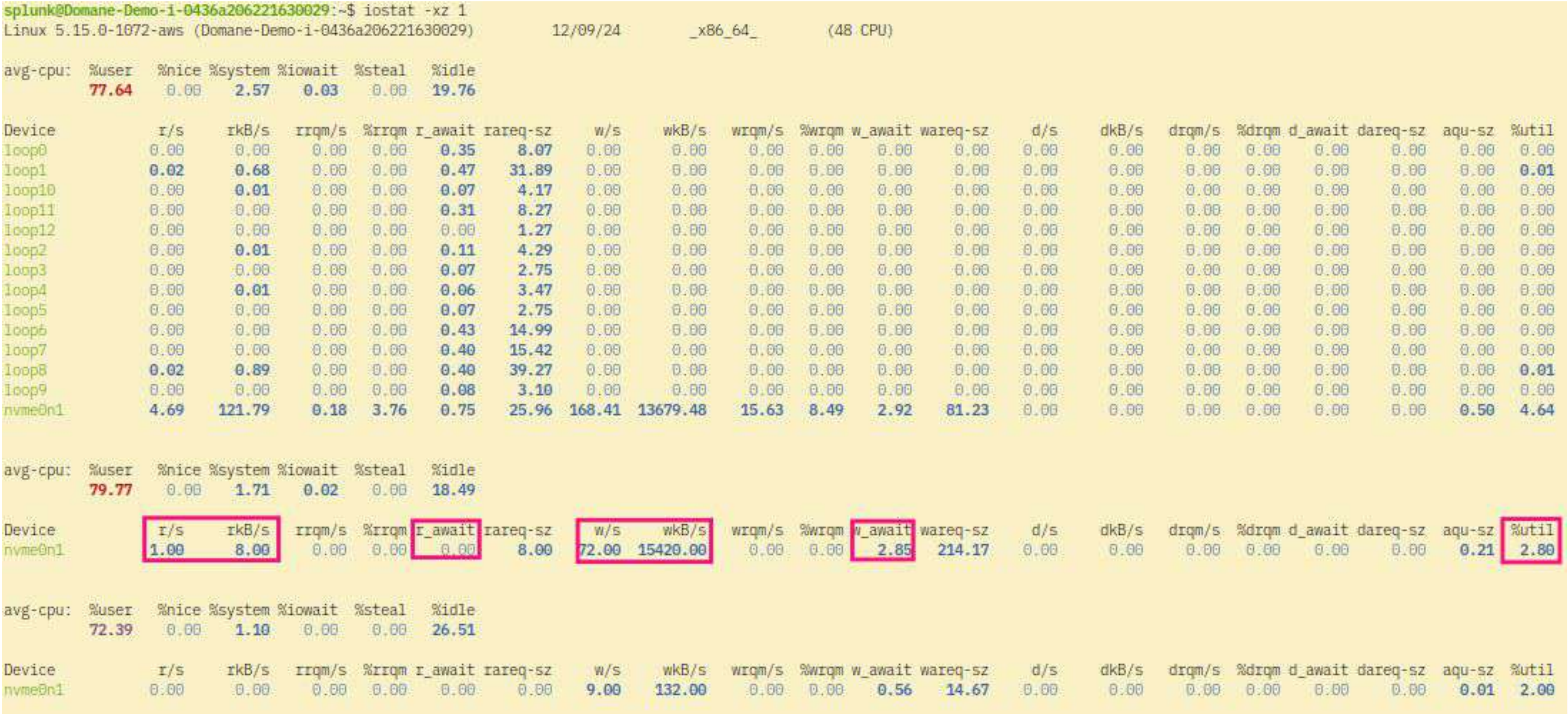
Monitoring Splunk Enterprise with MC	Link to Splunk Docs
Resource Usage	Link to Splunk Docs

© 2025 SPLUNK LLC

Detect Performance issues

Tools: OS

- iostat



```
splunk@Domane-Demo-i-0436a206221630029:~$ iostat -xz 1
Linux 5.15.0-1072-aws (Domane-Demo-i-0436a206221630029)         12/09/24        _x86_64_        (48 CPU)

avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          77.64    0.00    2.57    0.03    0.00   19.76

Device            r/s     rkB/s   rrqm/s  %rrqm r_await rareq-sz     w/s     wkB/s   wrqm/s  %wrqm w_await wareq-sz     d/s     dkB/s   drqm/s  %drqm d_await dareq-sz  aqu-sz  %util
loop0            0.00      0.00     0.00   0.00    0.35     8.07    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop1            0.02      0.68     0.00   0.00    0.47    31.89    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.01
loop10           0.00      0.01     0.00   0.00    0.07     4.17    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop11           0.00      0.00     0.00   0.00    0.31     8.27    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop12           0.00      0.00     0.00   0.00    0.00     1.27    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop2            0.00      0.01     0.00   0.00    0.11     4.29    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop3            0.00      0.00     0.00   0.00    0.07     2.75    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop4            0.00      0.01     0.00   0.00    0.06     3.47    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop5            0.00      0.00     0.00   0.00    0.07     2.75    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop6            0.00      0.00     0.00   0.00    0.43    14.99    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop7            0.00      0.00     0.00   0.00    0.40    15.42    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
loop8            0.02      0.89     0.00   0.00    0.40    39.27    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.01
loop9            0.00      0.00     0.00   0.00    0.08     3.10    0.00      0.00     0.00   0.00    0.00     0.00    0.00      0.00     0.00   0.00    0.00     0.00    0.00   0.00
nvme0n1          4.69    121.79     0.18   3.76    0.75    25.96  168.41  13679.48    15.63   8.49    2.92    81.23    0.00      0.00     0.00   0.00    0.00     0.00    0.50   4.64


avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          79.77    0.00    1.71    0.02    0.00   18.49

Device            r/s     rkB/s   rrqm/s  %rrqm r_await rareq-sz     w/s     wkB/s   wrqm/s  %wrqm w_await wareq-sz     d/s     dkB/s   drqm/s  %drqm d_await dareq-sz  aqu-sz  %util
nvme0n1          1.00      8.00     0.00   0.00    0.00     8.00   72.00  15420.00     0.00   0.00    2.85   214.17    0.00      0.00     0.00   0.00    0.00     0.00    0.21   2.80


avg-cpu:  %user   %nice %system %iowait  %steal   %idle
          72.39    0.00    1.10    0.00    0.00   26.51

Device            r/s     rkB/s   rrqm/s  %rrqm r_await rareq-sz     w/s     wkB/s   wrqm/s  %wrqm w_await wareq-sz     d/s     dkB/s   drqm/s  %drqm d_await dareq-sz  aqu-sz  %util
nvme0n1          0.00      0.00     0.00   0.00    0.00     0.00    9.00    132.00     0.00   0.00    0.56    14.67    0.00      0.00     0.00   0.00    0.00     0.00    0.01   2.00
```

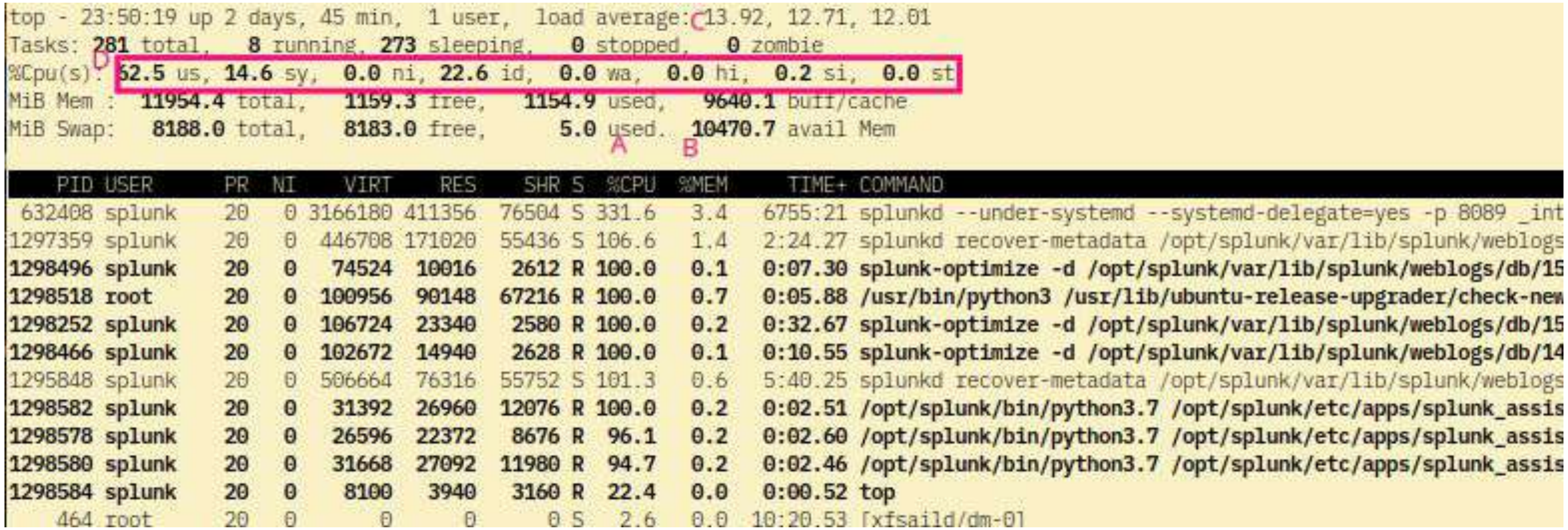
Linux troubleshooting 101: System performance	https://www.redhat.com/en/blog/troubleshooting-system-performance
Brendan Gregg: Linux Performance	https://www.brendangregg.com/linuxperf.html
iostat – Montor Linux disk activity	https://www.cyberciti.biz/tips/top-linux-monitoring-tools.html#:~:text=7.-,iostat,-%E2%80%93%20Montor%20Linux%20average

© 2025 SPLUNK LLC

Detect Performance issues

Tools: OS

- Top



```
top - 23:50:19 up 2 days, 45 min,  1 user,  load average: 13.92, 12.71, 12.01
Tasks: 281 total,   8 running, 273 sleeping,   0 stopped,   0 zombie
%Cpu(s): 62.5 us, 14.6 sy,  0.0 ni, 22.6 id,  0.0 wa,  0.0 hi,  0.2 si,  0.0 st
MiB Mem :  11954.4 total,   1159.3 free,   1154.9 used,   9640.1 buff/cache
MiB Swap:   8188.0 total,   8183.0 free,      5.0 used.  10470.7 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
 632408 splunk    20   0 3166180 411356  76504 S 331.6   3.4   6755:21 splunkd --under-systemd --systemd-delegate=yes -p 8089 _int
1297359 splunk    20   0  446708 171020  55436 S 106.6   1.4   2:24.27 splunkd recover-metadata /opt/splunk/var/lib/splunk/weblogs
1298496 splunk    20   0   74524  10016   2612 R 100.0   0.1   0:07.30 splunk-optimize -d /opt/splunk/var/lib/splunk/weblogs/db/15
1298518 root      20   0  100956  90148  67216 R 100.0   0.7   0:05.88 /usr/bin/python3 /usr/lib/ubuntu-release-upgrader/check-new
1298252 splunk    20   0  106724  23340   2580 R 100.0   0.2   0:32.67 splunk-optimize -d /opt/splunk/var/lib/splunk/weblogs/db/15
1298466 splunk    20   0  102672  14940   2628 R 100.0   0.1   0:10.55 splunk-optimize -d /opt/splunk/var/lib/splunk/weblogs/db/14
1295848 splunk    20   0  506664  76316  55752 S 101.3   0.6   5:40.25 splunkd recover-metadata /opt/splunk/var/lib/splunk/weblogs
1298582 splunk    20   0   31392  26960  12076 R 100.0   0.2   0:02.51 /opt/splunk/bin/python3.7 /opt/splunk/etc/apps/splunk_assis
1298578 splunk    20   0   26596  22372   8676 R  96.1   0.2   0:02.60 /opt/splunk/bin/python3.7 /opt/splunk/etc/apps/splunk_assis
1298580 splunk    20   0   31668  27092  11980 R  94.7   0.2   0:02.46 /opt/splunk/bin/python3.7 /opt/splunk/etc/apps/splunk_assis
1298584 splunk    20   0    8100   3940   3160 R  22.4   0.0   0:00.52 top
    464 root      20   0       0      0      0 S   2.6   0.0  10:20.53 [xfsaild/dm-0]
```

Linux troubleshooting 101: System performance	https://www.redhat.com/en/blog/troubleshooting-system-performance
Brendan Gregg: Linux Performance	https://www.brendangregg.com/linuxperf.html
top – Process activity monitoring command	https://www.cyberciti.biz/tips/top-linux-monitoring-tools.html#:~:text=top%20%E2%80%93%20Process%20activity%20monitoring%20command

© 2025 SPLUNK LLC

Workshop Agenda

- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
  - Lab^1
  - Lab^2
  - Lab^3
  - Lab^{4} - Lab^{6}
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

Detect Performance issues

Lab4

Exercise 4 - Full memory usage

- The tools to use have been presented, now more exercises
- Work on detecting Full memory usage

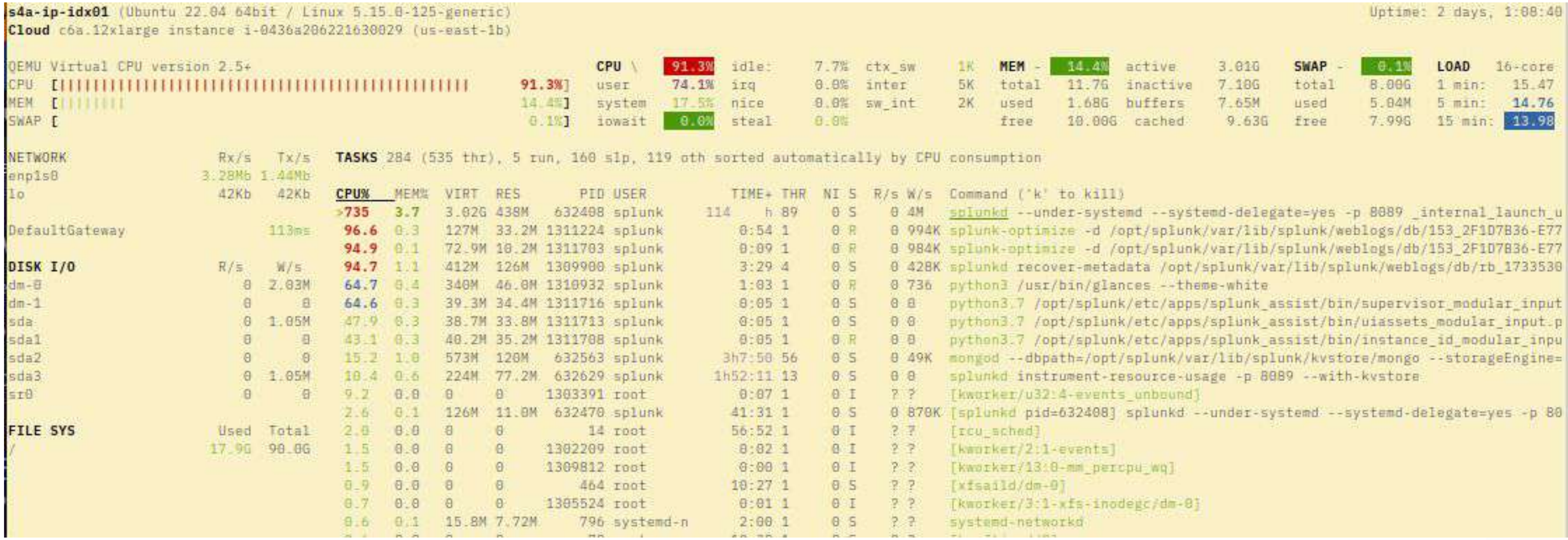
Monitoring Splunk Enterprise with MC	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Resource Usage	https://docs.splunk.com/Documentation/Splunk/latest/DMC/ResourceusageDeployment

© 2025 SPLUNK LLC

Detect Performance issues

Tools: OS

- Glances



```
s4a-ip-idx01 (Ubuntu 22.04 64bit / Linux 5.15.0-125-generic)                                                                          Uptime: 2 days, 1:08:40
Cloud c6a.12xlarge instance i-0436a206221630029 (us-east-1b)

QEMU Virtual CPU version 2.5+                                         CPU \   91.3%  idle:      7.7%  ctx_sw    1K  MEM -  14.4%  active     3.01G  SWAP -  0.1%  LOAD  16-core
CPU  [|||||||||||||||||||||||||||||||||||||||||||||||||||    91.3%]  user    74.1%  irq       0.0%  inter     5K  total  11.7G  inactive   7.10G  total  8.00G  1 min:   15.47
MEM  [||||||||                                               14.4%]  system  17.5%  nice      0.0%  sw_int    2K  used   1.68G  buffers    7.65M  used   5.04M  5 min:   14.76
SWAP [                                                        0.1%]  iowait   0.0%  steal     0.0%                free  10.00G   cached    9.63G  free   7.99G  15 min:  13.98

NETWORK              Rx/s   Tx/s   TASKS 284 (535 thr), 5 run, 160 slp, 119 oth sorted automatically by CPU consumption
enp1s0             3.28Mb 1.44Mb
lo                   42Kb   42Kb   CPU%   MEM%  VIRT  RES        PID USER          TIME+ THR  NI S  R/s W/s  Command ('k' to kill)
                                   >735   3.7   3.02G 438M    632408 splunk     114     h 89    0 S    0 4M    splunkd --under-systemd --systemd-delegate=yes -p 8089 _internal_launch_u
DefaultGateway              113ms  96.6   0.3   127M  33.2M  1311224 splunk         0:54 1      0 R    0 994K  splunk-optimize -d /opt/splunk/var/lib/splunk/weblogs/db/153_2F1D7B36-E77
                                   94.9   0.1   72.9M 10.2M  1311703 splunk         0:09 1      0 R    0 984K  splunk-optimize -d /opt/splunk/var/lib/splunk/weblogs/db/153_2F1D7B36-E77
DISK I/O             R/s    W/s    94.7   1.1   412M  126M   1309900 splunk         3:29 4      0 S    0 428K  splunkd recover-metadata /opt/splunk/var/lib/splunk/weblogs/db/rb_1733530
dm-0                   0  2.03M    64.7   0.4   340M  46.0M  1310932 splunk         1:03 1      0 R    0 736   python3 /usr/bin/glances --theme-white
dm-1                   0      0    64.6   0.3   39.3M 34.4M  1311716 splunk         0:05 1      0 S    0 0     python3.7 /opt/splunk/etc/apps/splunk_assist/bin/supervisor_modular_input
sda                    0  1.05M    47.9   0.3   38.7M 33.8M  1311713 splunk         0:05 1      0 S    0 0     python3.7 /opt/splunk/etc/apps/splunk_assist/bin/uiassets_modular_input.p
sda1                   0      0    43.1   0.3   40.2M 35.2M  1311708 splunk         0:05 1      0 R    0 0     python3.7 /opt/splunk/etc/apps/splunk_assist/bin/instance_id_modular_inpu
sda2                   0      0    15.2   1.0   573M  120M    632563 splunk      3h7:50 56     0 S    0 49K   mongod --dbpath=/opt/splunk/var/lib/splunk/kvstore/mongo --storageEngine=
sda3                   0  1.05M    10.4   0.6   224M  77.2M   632629 splunk     1h52:11 13     0 S    0 0     splunkd instrument-resource-usage -p 8089 --with-kvstore
sr0                    0      0    9.2    0.0   0     0      1303391 root           0:07 1      0 I    ? ?     [kworker/u32:4-events_unbound]
                                   2.6    0.1   126M  11.0M   632470 splunk        41:31 1      0 S    0 870K  [splunkd pid=632408] splunkd --under-systemd --systemd-delegate=yes -p 80
FILE SYS             Used  Total   2.0    0.0   0     0           14 root          56:52 1      0 I    ? ?     [rcu_sched]
/                   17.9G  90.0G   1.5    0.0   0     0      1302209 root           0:02 1      0 I    ? ?     [kworker/2:1-events]
                                   1.5    0.0   0     0      1309812 root           0:00 1      0 I    ? ?     [kworker/13:0-mm_percpu_wq]
                                   0.9    0.0   0     0          464 root          10:27 1      0 S    ? ?     [xfsaild/dm-0]
                                   0.7    0.0   0     0      1305524 root           0:01 1      0 I    ? ?     [kworker/3:1-xfs-inodegc/dm-0]
                                   0.6    0.1   15.8M 7.72M      796 systemd-n      2:00 1      0 S    ? ?     systemd-networkd
```

Linux troubleshooting 101: System performance	https://www.redhat.com/en/blog/troubleshooting-system-performance
Brendan Gregg: Linux Performance	https://www.brendangregg.com/linuxperf.html
Glances	https://github.com/nicolargo/glances

© 2025 SPLUNK LLC

Detect Performance issues

Exercise 5 - Undersized node

- The tools to use have been presented, now more exercises
- Work on detecting an undersized node

Monitoring Splunk Enterprise with MC	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Capacity Planning Manual	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Performancechecklist
Scalability in IT: The Complete Guide To Scaling	https://www.splunk.com/en_us/blog/learn/scalability.html
Reference hardware	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware

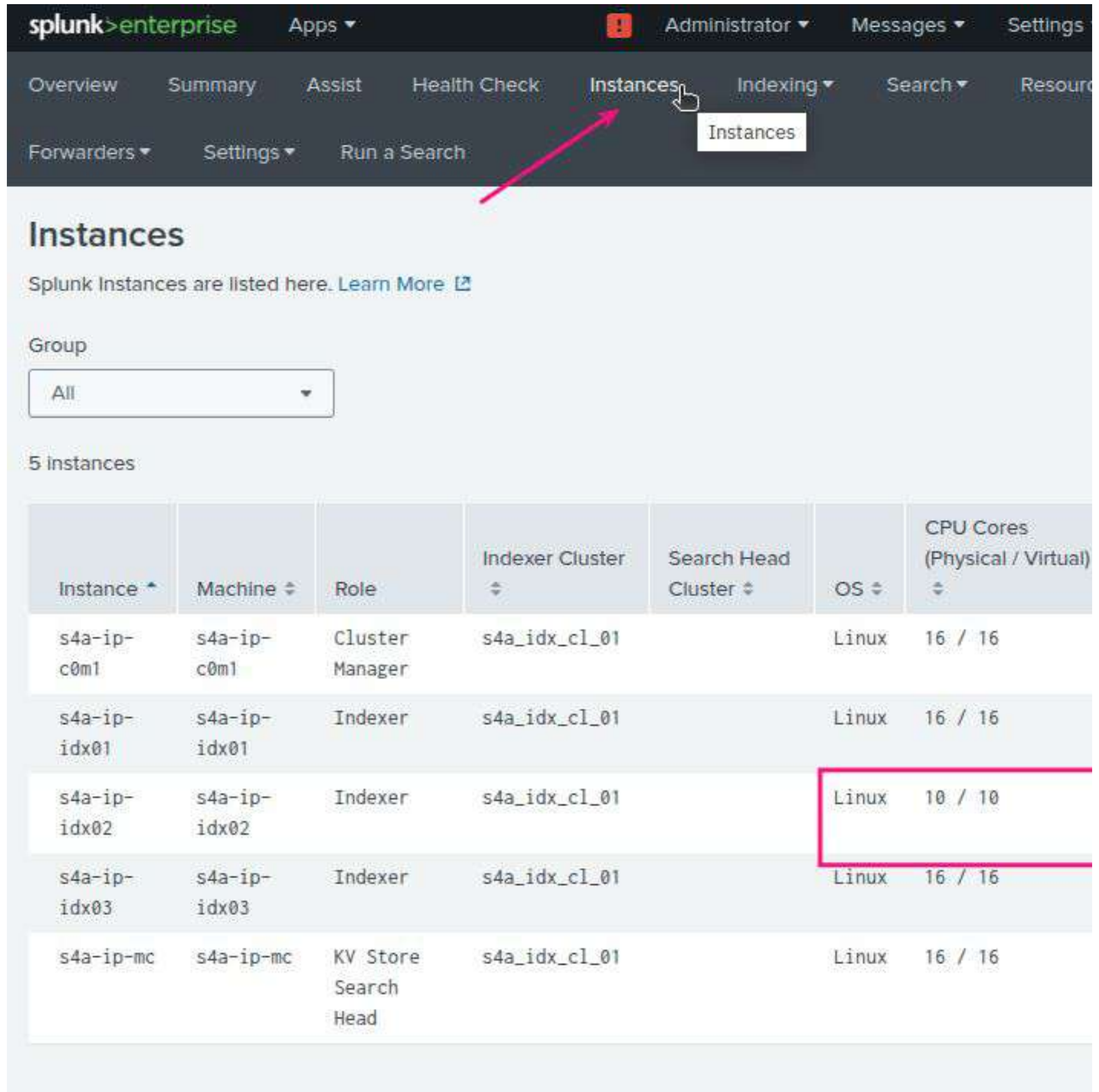
© 2025 SPLUNK LLC

Detect Performance issues

Lab5

Exercise 5 - Undersized node

- The ‘Instances’ dashboard helps discover specification issues



Instances

Splunk Instances are listed here. Learn More

Group

All

5 instances

Instance	Machine	Role	Indexer Cluster	Search Head Cluster	OS	CPU Cores (Physical / Virtual)
s4a-ip-c0m1	s4a-ip-c0m1	Cluster Manager	s4a_idx_cl_01		Linux	16 / 16
s4a-ip-idx01	s4a-ip-idx01	Indexer	s4a_idx_cl_01		Linux	16 / 16
s4a-ip-idx02	s4a-ip-idx02	Indexer	s4a_idx_cl_01		Linux	10 / 10
s4a-ip-idx03	s4a-ip-idx03	Indexer	s4a_idx_cl_01		Linux	16 / 16
s4a-ip-mc	s4a-ip-mc	KV Store Search Head	s4a_idx_cl_01		Linux	16 / 16

Monitoring Splunk Enterprise with MC	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Capacity Planning Manual	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Performancechecklist
Scalability in IT: The Complete Guide To Scaling	https://www.splunk.com/en_us/blog/learn/scalability.html
Reference hardware	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware

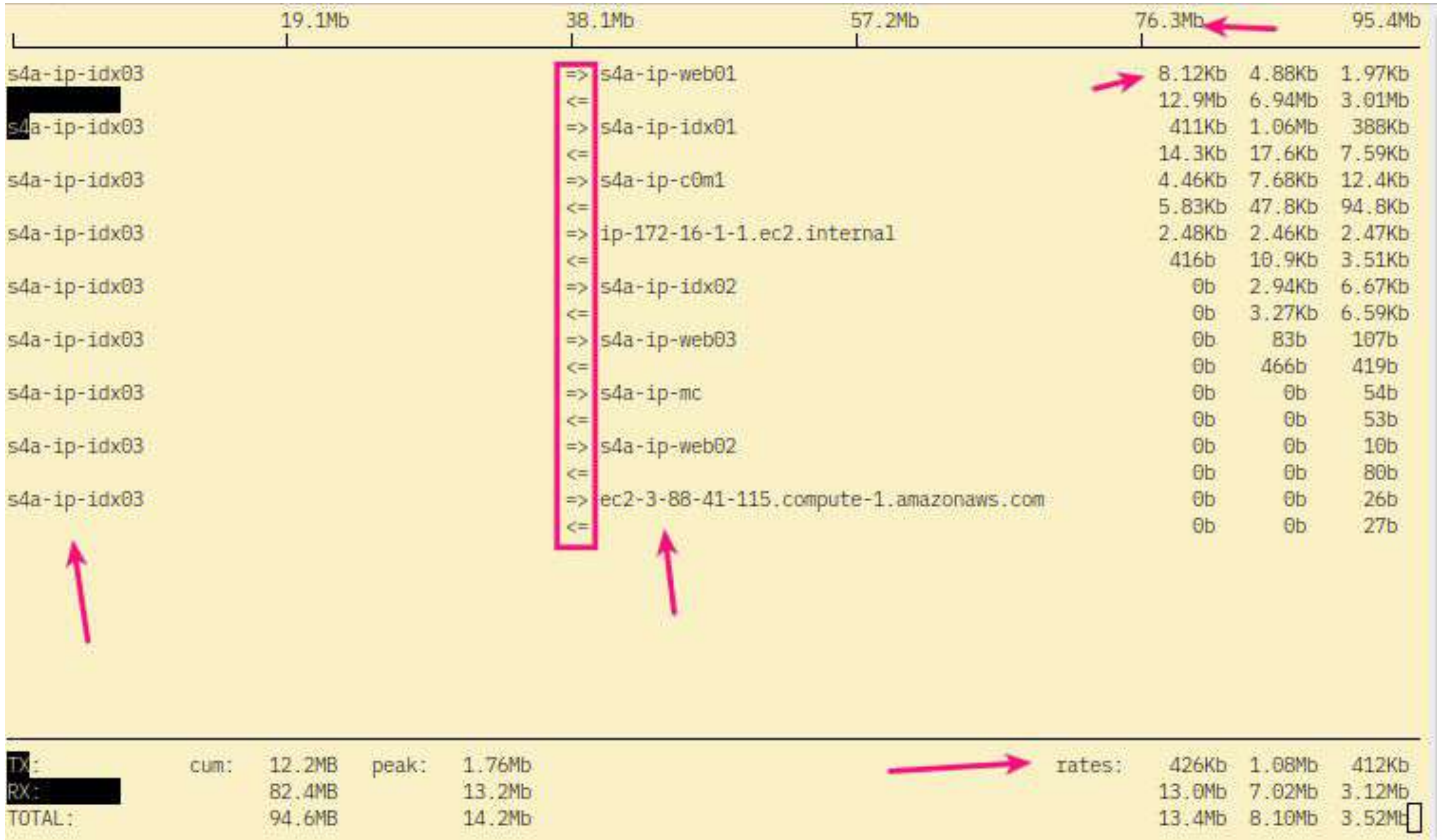
© 2025 SPLUNK LLC

Detect Performance issues

Lab⁶

Tools: OS

- iftop



```
              19.1Mb        38.1Mb        57.2Mb        76.3Mb        95.4Mb
└─────────────┴─────────────┴─────────────┴─────────────┴─────────────
s4a-ip-idx03                 => s4a-ip-web01                          8.12Kb  4.88Kb  1.97Kb
[redacted]                   <=                                       12.9Mb  6.94Mb  3.01Mb
s4a-ip-idx03                 => s4a-ip-idx01                           411Kb  1.06Mb   388Kb
                             <=                                       14.3Kb  17.6Kb  7.59Kb
s4a-ip-idx03                 => s4a-ip-c0m1                           4.46Kb  7.68Kb  12.4Kb
                             <=                                       5.83Kb  47.8Kb  94.8Kb
s4a-ip-idx03                 => ip-172-16-1-1.ec2.internal            2.48Kb  2.46Kb  2.47Kb
                             <=                                        416b   10.9Kb  3.51Kb
s4a-ip-idx03                 => s4a-ip-idx02                             0b   2.94Kb  6.67Kb
                             <=                                          0b   3.27Kb  6.59Kb
s4a-ip-idx03                 => s4a-ip-web03                             0b     83b    107b
                             <=                                          0b    466b    419b
s4a-ip-idx03                 => s4a-ip-mc                                0b      0b     54b
                             <=                                          0b      0b     53b
s4a-ip-idx03                 => s4a-ip-web02                             0b      0b     10b
                             <=                                          0b      0b     80b
s4a-ip-idx03                 => ec2-3-88-41-115.compute-1.amazonaws.com  0b      0b     26b
                             <=                                          0b      0b     27b



──────────────────────────────────────────────────────────────────────────────────────────
TX:           cum:   12.2MB   peak:   1.76Mb                      rates:   426Kb  1.08Mb   412Kb
RX:[redacted]        82.4MB           13.2Mb                              13.0Mb  7.02Mb  3.12Mb
TOTAL:               94.6MB           14.2Mb                              13.4Mb  8.10Mb  3.52Mb
```

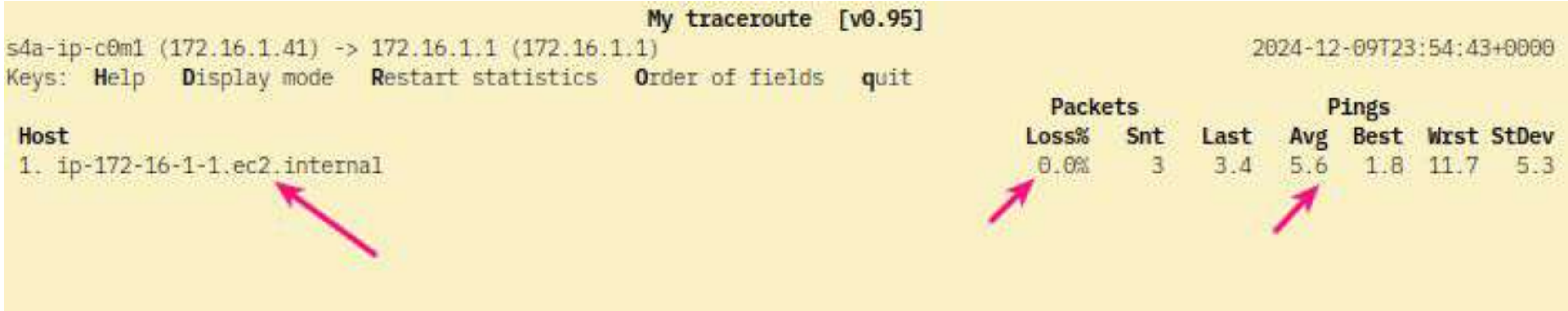
Linux troubleshooting 101: System performance	https://www.redhat.com/en/blog/troubleshooting-system-performance
Brendan Gregg: Linux Performance	https://www.brendangregg.com/linuxperf.html
Linux interface analytics on-demand with iftop	https://www.redhat.com/en/blog/linux-interface-iftop

© 2025 SPLUNK LLC

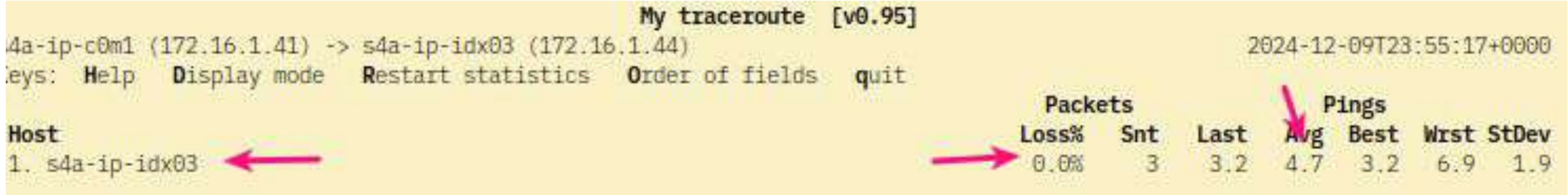
Detect Performance issues

Tools: OS

- MTR



```
                                   My traceroute  [v0.95]
s4a-ip-c0m1 (172.16.1.41) -> 172.16.1.1 (172.16.1.1)                 2024-12-09T23:54:43+0000
Keys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                        Packets               Pings
 Host                                                 Loss%   Snt   Last   Avg  Best  Wrst StDev
 1. ip-172-16-1-1.ec2.internal                         0.0%     3    3.4   5.6   1.8  11.7   5.3
```



```
                                   My traceroute  [v0.95]
4a-ip-c0m1 (172.16.1.41) -> s4a-ip-idx03 (172.16.1.44)                2024-12-09T23:55:17+0000
eys:  Help   Display mode   Restart statistics   Order of fields   quit
                                                        Packets               Pings
Host                                                  Loss%   Snt   Last   Avg  Best  Wrst StDev
1. s4a-ip-idx03                                        0.0%     3    3.2   4.7   3.2   6.9   1.9
```

Linux troubleshooting 101: System performance	https://www.redhat.com/en/blog/troubleshooting-system-performance
Brendan Gregg: Linux Performance	https://www.brendangregg.com/linuxperf.html
mtr - monitor network connections and latency	https://www.cyberciti.biz/tips/finding-out-a-bad-or-simply-overloaded-network-link-with-linuxunix-oses.html

© 2025 SPLUNK LLC

Detect Performance issues

Tools: Splunk:MC:Inputs and Indexes and Volumes

- When addressing Indexing Performance …
- Five MC Inputs dashboards
  - HEC:Instance and Deployment - information related to HEC ingest and performance
  - Splunk TCP Input Performance:Instance and Deployment - information related to S2S TCP ingest performance
  - Data Quality - related to how well the ingest data is configured
    - Detects pooly defined event ingest, by sourcetype, especially time/date, event record size, line-breaking, line aggregation, and metrics issues
- Six MC Indexes and Volumes
  - Indexes and Volumes:Instance and Deployment - sizes, discover full volumes here
  - Index Detail:Instance and Deployment - specifics about each index
  - Volume Detail: Instance and Deployment - specifics about each volume

Monitoring Splunk Enterprise with MC	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Indexing: Performance	https://docs.splunk.com/Documentation/Splunk/latest/DMC/IndexingDeployment
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

© 2025 SPLUNK LLC

Workshop Agenda

- Who?|What?|Why?
- Expectations
- Aspects of Splunk Performance
- Effects of Indexer Performance on Splunk
- Splunk Architecture and Specifications
- Effects of Search Workload on Splunk
- Scale-up or Scale-out?
- Performance Detection Tools
  - Lab^1
  - Lab^2
  - Lab^3
  - Lab^{4} - Lab^{6}
- Performance Problem Mitigation
- Summary

© 2025 SPLUNK LLC

Mitigate Performance issues

- CPU at 100%, blocked running jobs >= core count
  - Queue management, IO constraints, spread parallel
- Memory at 100%
  - Smaller, more tightly managed searches (restraint in bundle size,smaller event returns), search concurrency reduction (fewer searches run at once), scale-up opportunity
- IO constraints
  - Reduce search load (see above), reduce ingest amount (spread workload over more indexers), ensure on NVME SSD, not shared
- Network constraints
  - See Memory and IO, but ensure that the highest performance networks are available. 10G/s likely a minimum in enterprise
- Data Quality issues
  - Ensure the most efficient props/transforms/regexes - again, see this in high CPU in Parsing Queue

Summary of performance recommendations	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Summaryofperformancerecommendations
Sizing your Splunk architecture	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Sizing_your_Splunk_architecture
Splunk Validated Architectures	https://docs.splunk.com/Documentation/SVA/current/Architectures/About
Scalability in IT: The Complete Guide To Scaling	https://www.splunk.com/en_us/blog/learn/scalability.html
Lantern: Splunk Validated Architecture	https://lantern.splunk.com/Splunk_Success_Framework/Platform_Management/Indexing_and_search_architecture
Summary of performance recommendations	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Summaryofperformancerecommendations

© 2025 SPLUNK LLC

Summary
Splunk Performance

- A fine dance between system and application configuration
- Pay attention to the Splunk requirements
- Scale-out first, but be ready to adjust due to memory requirements
- Storage and/or networking are the underpinning of everything
- Use the MC heavily, but do not modify the in-app MC dashboards. Copy those that are of most interest and modify in a private app
- Use MC to diagnose, if OS-related, use the OS tools as well

© 2025 SPLUNK LLC

Links

Maximizing performance with the latest Splunk platform capabilities	https://lantern.splunk.com/Splunk_Platform/UCE/Observability/Maximizing_performance_with_the_latest_Splunk_platform_capabilities
Planning for infrastructure and resource scalability	https://lantern.splunk.com/Splunk_Platform/Splunk_Outcome_Paths/Improve_Performance/Planning_for_infrastructure_and_resource_scalability
Splunk Validated Architectures	https://docs.splunk.com/Documentation/SVA/current/Architectures/About
Reference hardware	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware
Indexing and search architecture	https://lantern.splunk.com/Splunk_Success_Framework/Platform_Management/Indexing_and_search_architecture
Configure parallel reduce search processing	https://docs.splunk.com/Documentation/Splunk/latest/DistSearch/Setupparallelreduce
Capacity Planning Manual	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Performancechecklist
Summary of performance recommendations	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Summaryofperformancerecommendations
Sizing your Splunk architecture	https://lantern.splunk.com/Splunk_Platform/Product_Tips/Administration/Sizing_your_Splunk_architecture
What storage type should I use for a role?	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware
Indexer Memory Specification	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware#:~:text=search%20performance.-,Indexer,-When%20you%20distribute
Network latency limits for clustered deployments	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Referencehardware#:~:text=performance%20recommendations.-,Network%20latency%20limits%20for%20clustered%20deployments,-A%20Splunk%20environment
How search types affect Splunk Enterprise performance	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/HowsearchtypesaffectSplunkEnterpriseperformance
How concurrent users and searches impact performance	https://docs.splunk.com/Documentation/Splunk/latest/Capacity/Accommodatemanysimultaneoussearches

Reducing search load	https://lantern.splunk.com/Splunk_Platform/Splunk_Outcome_Paths/Reduce_Costs/Reducing_search_load
Scalability in IT: The Complete Guide To Scaling	https://www.splunk.com/en_us/blog/learn/scalability.html
NixCraft System Monitoring Tools	https://www.cyberciti.biz/tips/top-linux-monitoring-tools.html
Monitoring Splunk Enterprise	https://docs.splunk.com/Documentation/Splunk/latest/DMC/DMCoverview
Glances	https://github.com/nicolargo/glances
Linux interface analytics on-demand with iftop	https://www.redhat.com/en/blog/linux-interface-iftop
Resource Usage	https://docs.splunk.com/Documentation/Splunk/latest/DMC/ResourceusageDeployment
top – Process activity monitoring command	https://www.cyberciti.biz/tips/top-linux-monitoring-tools.html#:~:text=top%20%E2%80%93%20Process%20activity%20monitoring%20command
Brendan Gregg: Linux Performance	https://www.brendangregg.com/linuxperf.html
Linux troubleshooting 101: System performance	https://www.redhat.com/en/blog/troubleshooting-system-performance
iostat – Monitor Linux disk activity	https://www.cyberciti.biz/tips/top-linux-monitoring-tools.html#:~:text=7.-,iostat,-%E2%80%93%20Montor%20Linux%20average
mtr - monitor network connections and latency	https://www.cyberciti.biz/tips/finding-out-a-bad-or-simply-overloaded-network-link-with-linuxunix-oses.html
Indexing: Inputs: HTTP Event Collector	https://docs.splunk.com/Documentation/Splunk/9.3.2/DMC/Inputdashboards
Indexing: Inputs: Data Quality	https://docs.splunk.com/Documentation/Splunk/9.3.2/DMC/Dataquality
What is SSH (Secure Shell)?	https://www.ssh.com/academy/ssh
Download PuTTY: latest release	https://putty.org/

© 2025 SPLUNK LLC

Thank you

splunk> a CISCO company

© 2025 SPLUNK LLC