How to Achieve Your Business Goals Using Splunk Workload Management

Shalabh Goyal
Product Manager | Splunk

Hongxun Liu
Principal Engineer | Splunk

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Shalabh Goyal

Product Manager | Splunk

Hongxun Liu

Principal Engineer | Splunk

splunk> .conf20

Agenda

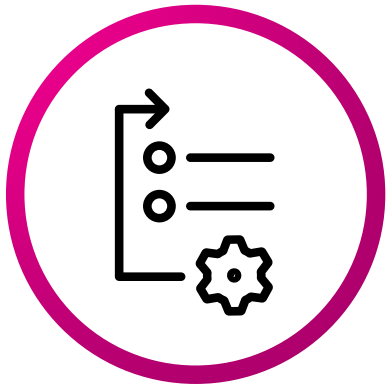
Review workload management, learn latest enhancements and use them to achieve your business goals

1. **Workload Management Review**
   Let's catchup
2. **Recent Enhancements**
   Good things are happening
3. **Solving Business Use Cases**
   Make it work!
4. **Best Practices**
   Watch out
5. **Resources**
   Get help

Important Splunk Admin Tasks

Broad categorization

Prioritize



Service business use cases in order of priority

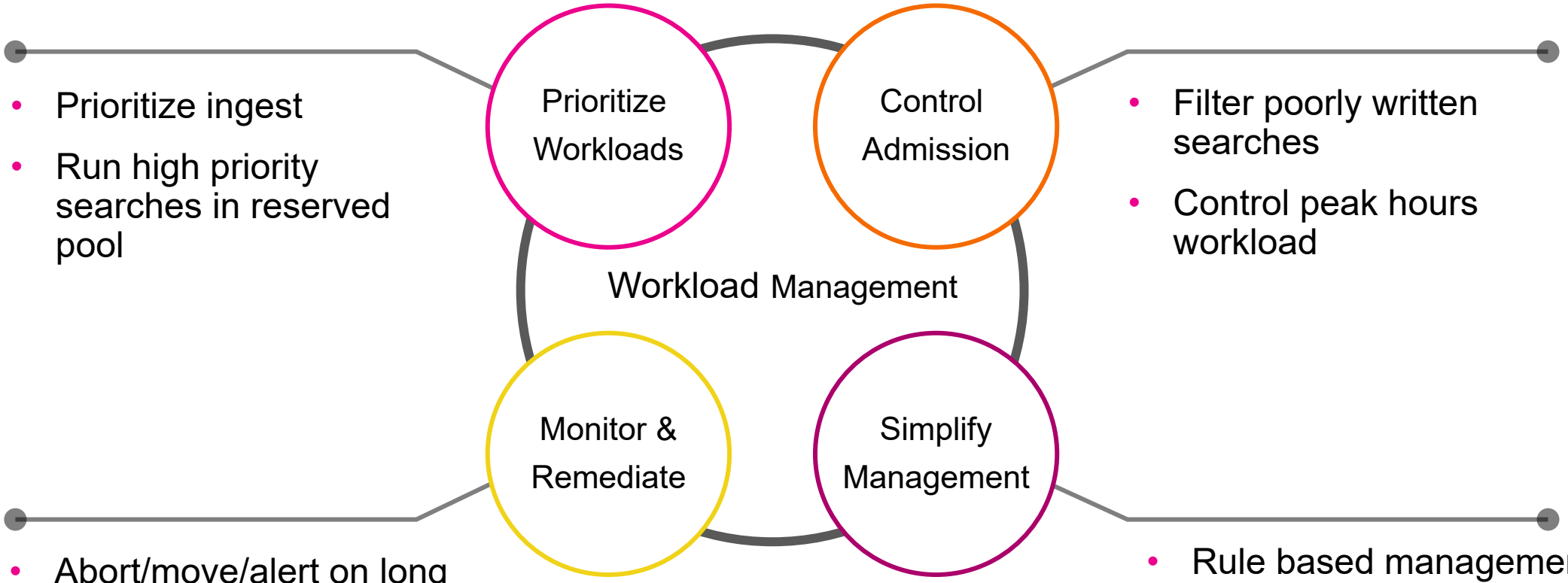
Manage at Scale

Manage apps, users, capacity…

Remediate

Take remediation actions to resolve issues

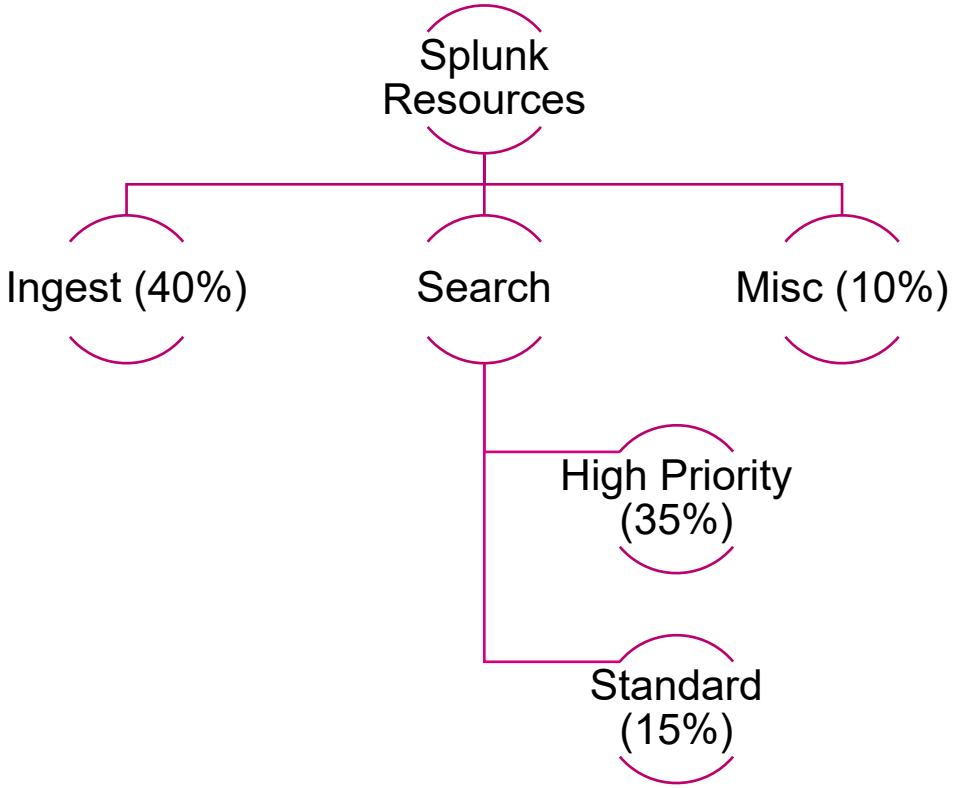
Splunk Workload Management



Workload Management (review)

Using workload management rules to prioritize business critical searches during execution

Workload Categories/Pools



Workload Rules

Name	Condition	Action
abort	`(NOT role=admin) AND runtime>15m`	Abort
throttle	`(NOT role=admin) AND runtime>10m`	Move to: Standard Pool
high_priority	`search_type=adhoc AND role=security`	Place in High Priority Pool

Enhancements to Workload Management

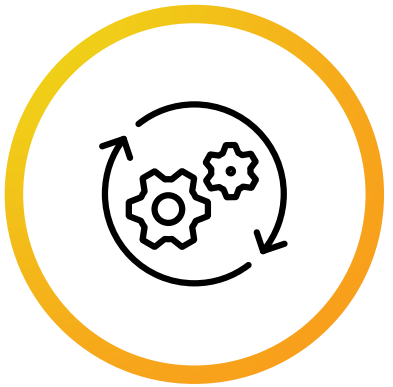
Admission Rules

Filter out wildcard searches

Custom User Messages

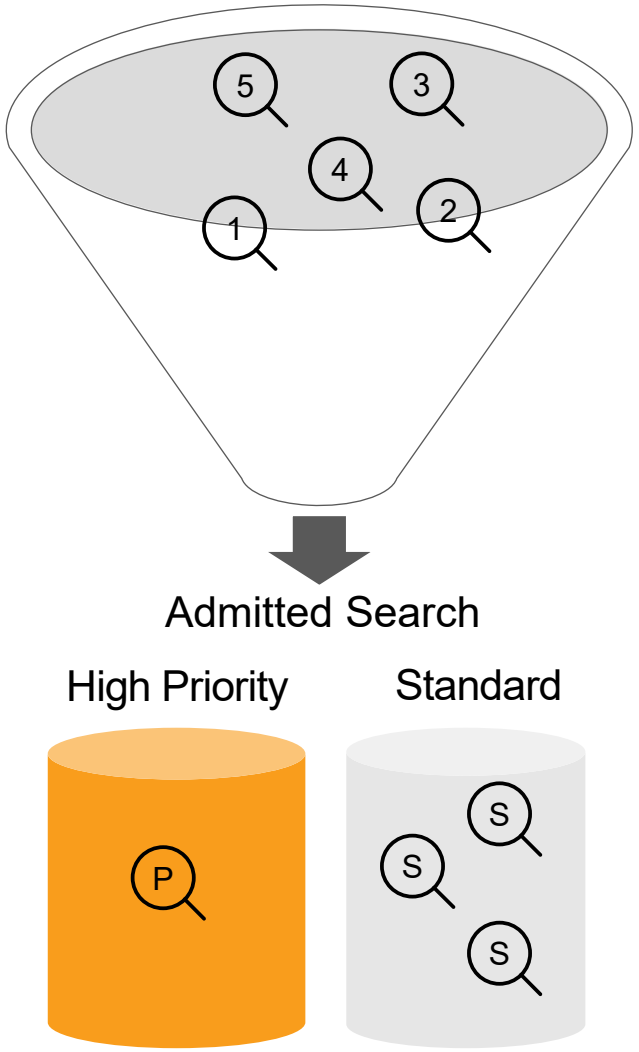
Educate users that trigger workload rules

Simplified Management



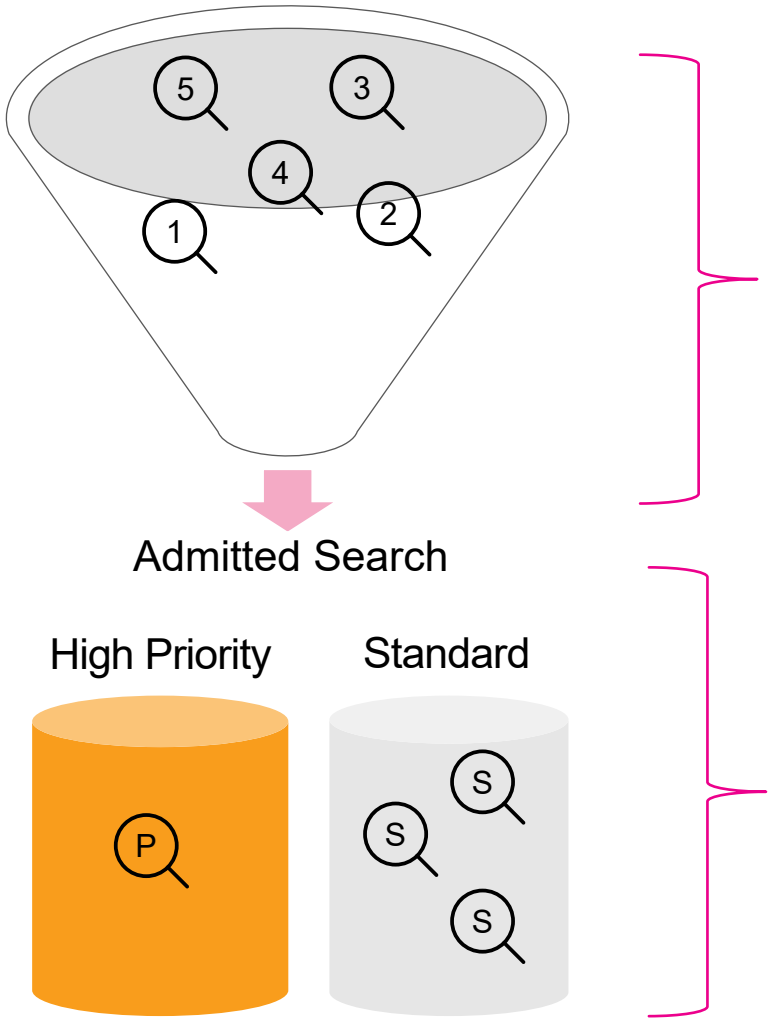
Monitor impact of workload rules

Search Lifecycle



1. Searches in pipeline
2. Searches admitted
3. Searches in execution

Admin Controls



Admission Control

- Quota controls
  - Role/user quotas
- Maximum concurrency
  - Scheduled, total concurrency
- [New] Admission rules

Search Execution

- Place in Workload Pools
  - Prioritize workloads
- Monitor during execution
  - Remediate long running searches

Admission Rules (New)

Filter rogue searches that may impact other users

Admission Rules | Workload Pools | Workload Rules

Admission Rules Enabled

Add Admission Rule

Admission Rules

	Admission Rule	Predicate (Condition)	Rule Action	User Message	Schedule	Actions
1	Alltime	(NOT app=splunk_monitoring_console) AND (NOT role=admin) AND search_time_range=alltime	Filter search	Please specify a shorter time duration.	Always On	Edit Delete
2	no_new_user	role=new_user	Filter search	Please run your search outside of peak hours	Every Day (9:00) - (12:00)	Edit Delete
3	nowildcard	index=* AND (search_type=adhoc OR search_type=scheduled)	Filter search	Please specify an index	Always On	Edit Delete

1. Filter ‘alltime’ range searches except from monitoring console or admin

2. Disallow ‘new users’ to run searches in peak hours

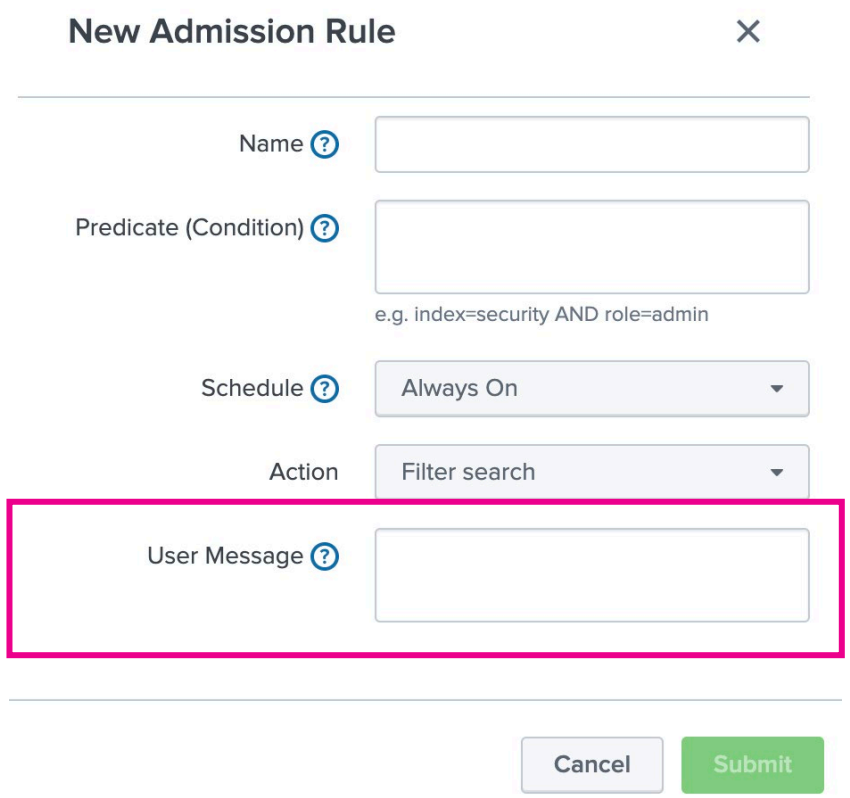
3. Filter any wildcard searches that are adhoc or scheduled (DMA searches excluded)

splunk> .conf20

Custom User Messages (New)

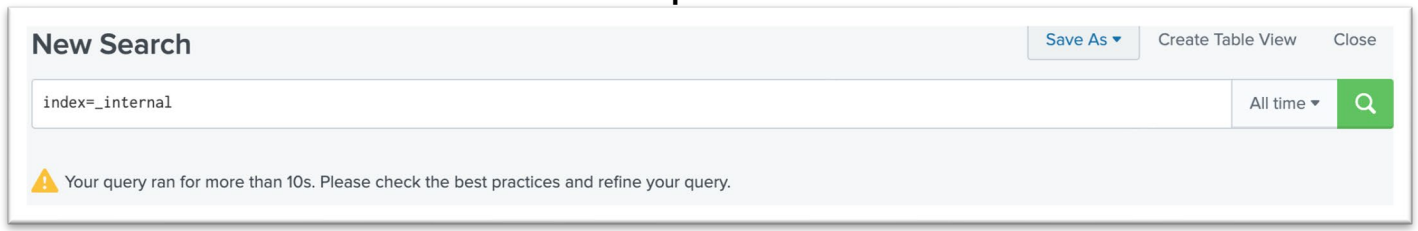
Using workload management rules to prioritize business critical searches

Define User Message

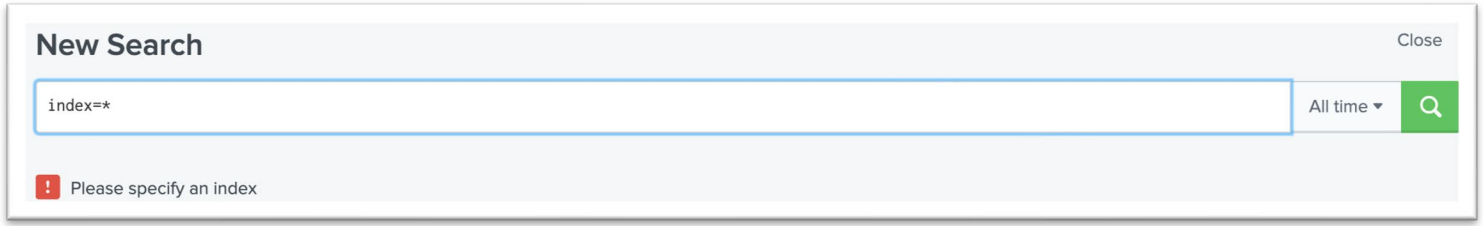


User Message

Search aborted after pre-defined runtime

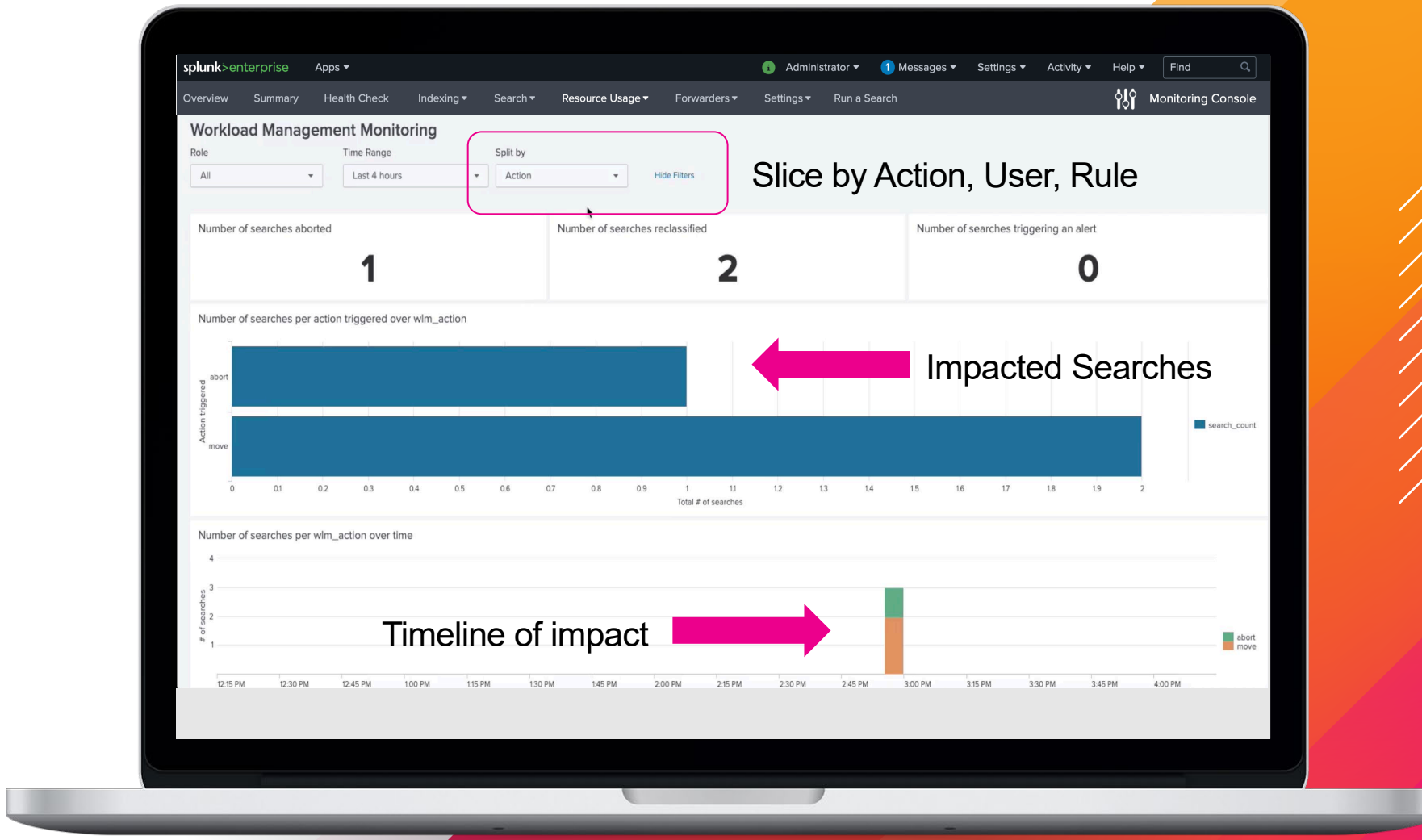


Search filtered due to admission rules



splunk> .conf20

Simplified Management (New)



.conf20

splunk>

Transition Slide for New Speaker

Use Case 1: Splunk Cloud

Uses a single SHC with core workload and ITSI

Key Use Cases

- High priority for ITSI searches
- Put searches from novice Splunk users in low priority pool
- Limit realtime searches to 5m
- No user searches with index=*
- No user searches with all time range

- Pre-provisioned Search Pools
- High Priority
- Standard
- Low Priority

Use Case 2: Splunk On-prem

Multiple SH deployment

Deployment

- SH for Corporate Teams – Finance, HR, Legal
- SH for Dev Team – R&D
- Single shared indexer cluster

Key Use Cases

- Ingest protection
- High priority for Executives on Corporate team SH
- High priority for Security on Dev team SH

.conf20

splunk>

Transition Slide for New Speaker

Best Practices

- **Allocate resource appropriately**
  - Think through memory allocation well
  - SH and IDX may have different resource allocations
- **Don’t overcrowd the high priority pool**
  - Allocate majority of CPU resources and minority number of searches
- **Think through mixed deployment well (SH, SHC, IDXC)**
- **Onboard a single use case at a time — crawl, walk, run**
- **Remember the corner cases**
  - Workload rules have top down precedence
  - Roles inheritance needs to be accounted
  - Some DMA searches may be using index=*
  - View indexes feature and monitoring app may use alltime searches

Resources

Blogs

https://www.splunk.com/en_us/blog/tips-and-tricks.html

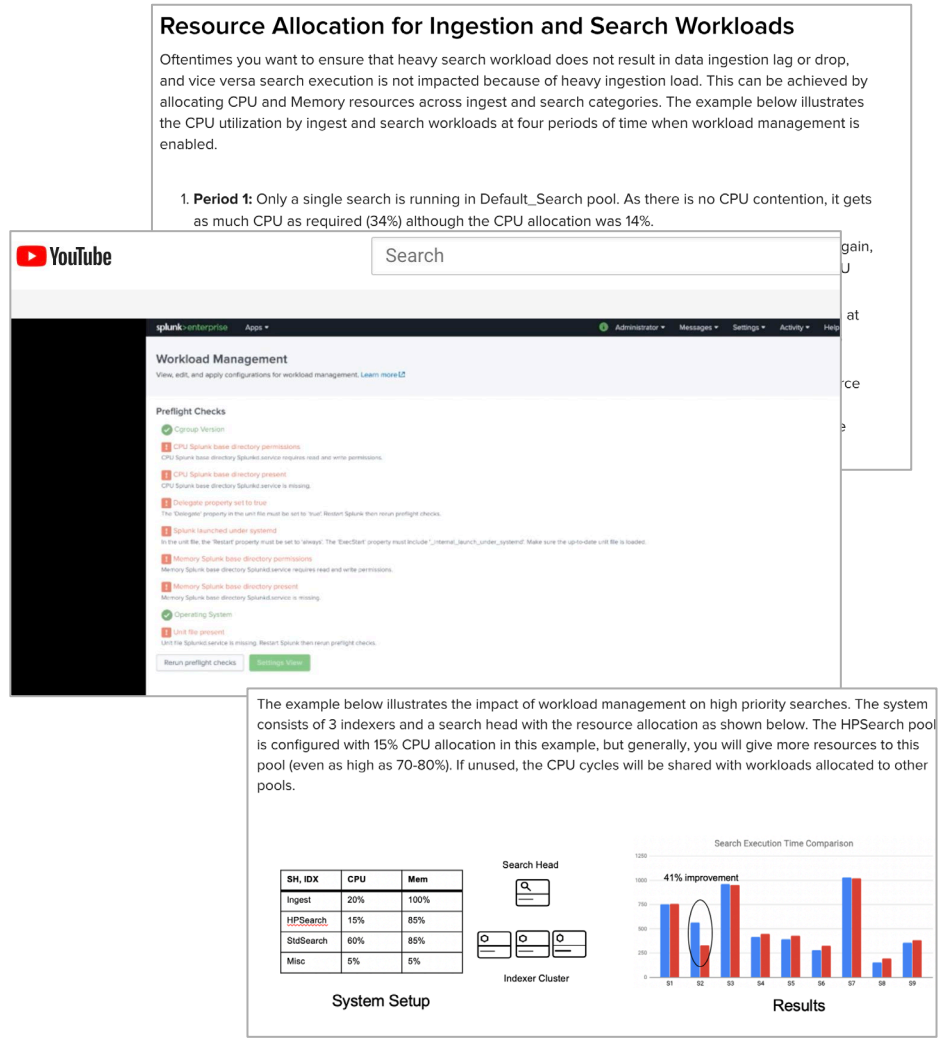
- Best practices for using admission rules in Splunk workload management
- Best practices for using Splunk workload management
- Get in command of Splunk resources with workload management (part 1, 2, 3)

Splunk User Group Slack Channel

#workload_management

Splunk Education

https://www.splunk.com/en_us/training/courses/splunk-workload-management.html



splunk> .conf20

Key Takeaways

Splunk Workload Management provides powerful controls that help you prioritize, manage, scale and remediate

1. Workload Management now allows more controls, better user messaging and simplified management
2. Workload Management is pre-configured for Splunk Cloud
3. Follow the best practices to get most value

Thank You

Please provide feedback via the

SESSION SURVEY