



Workload Management

To Achieve Efficient Resource Utilization

Bharath Aleti

Product Management, Splunk

Anish Shrigondekar

Principal Software Engineer, Splunk

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2018 Splunk Inc. All rights reserved.

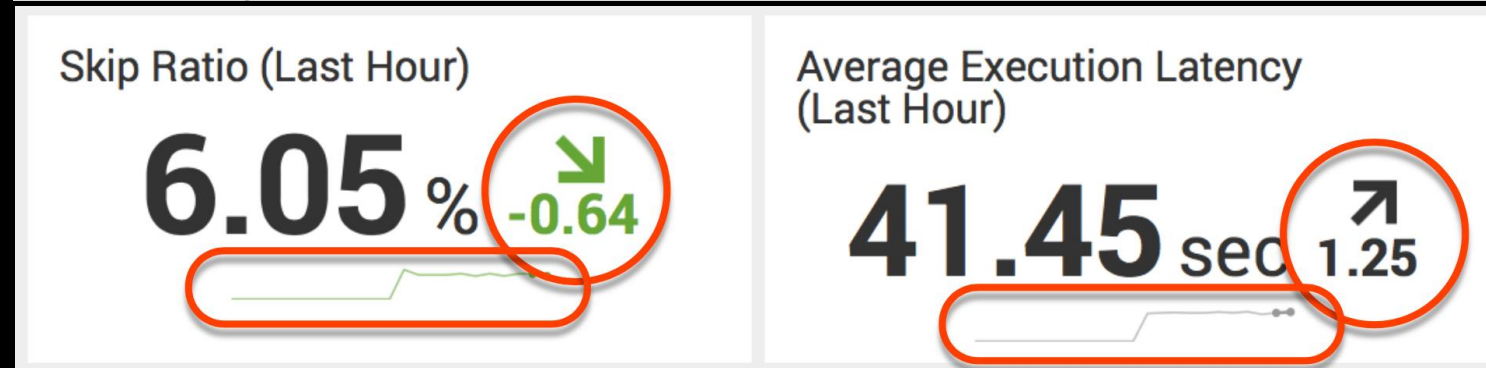
Workload Management

How does it help ?

Challenges

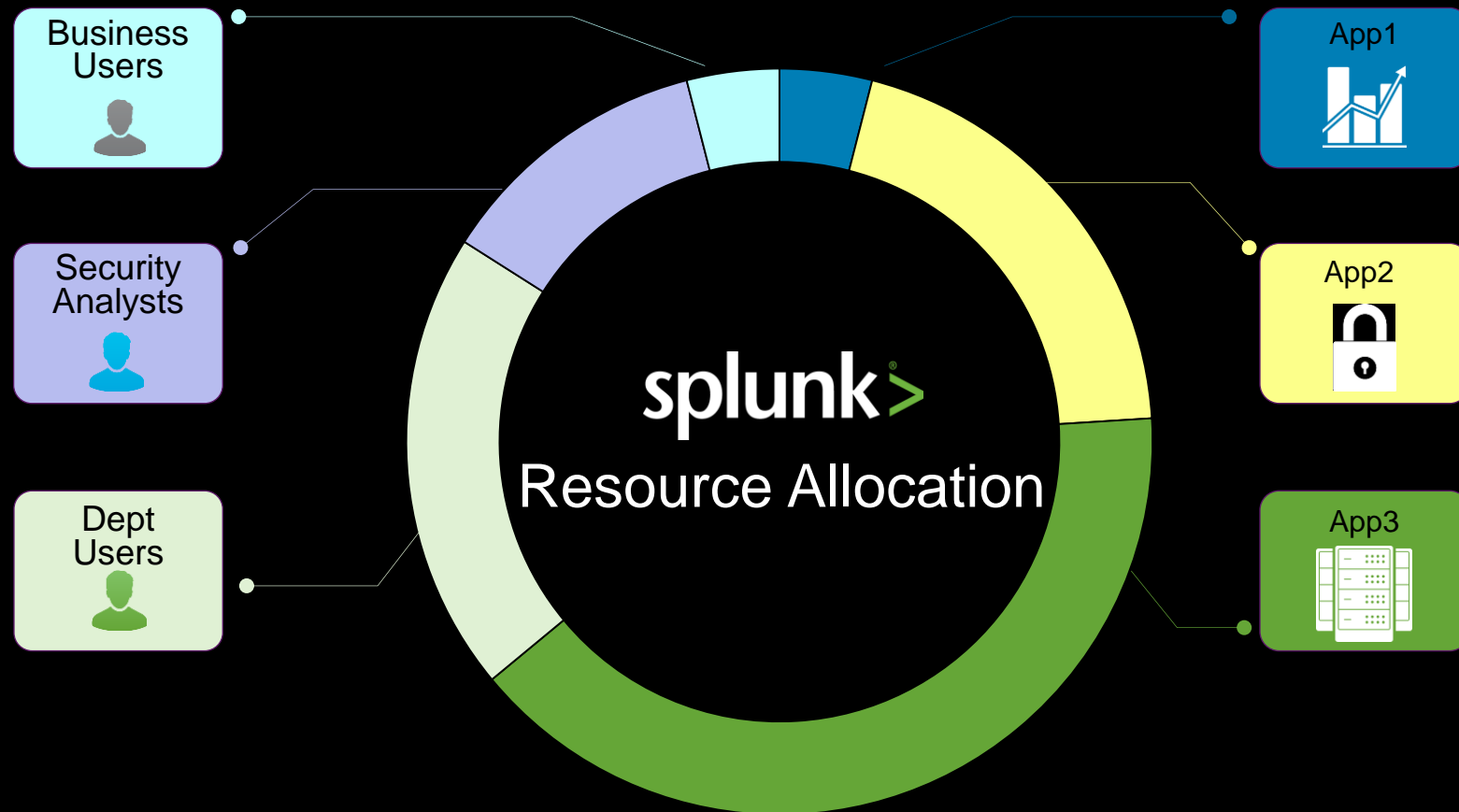
Unpredictability in search execution

Monitoring Console Scheduler Activity



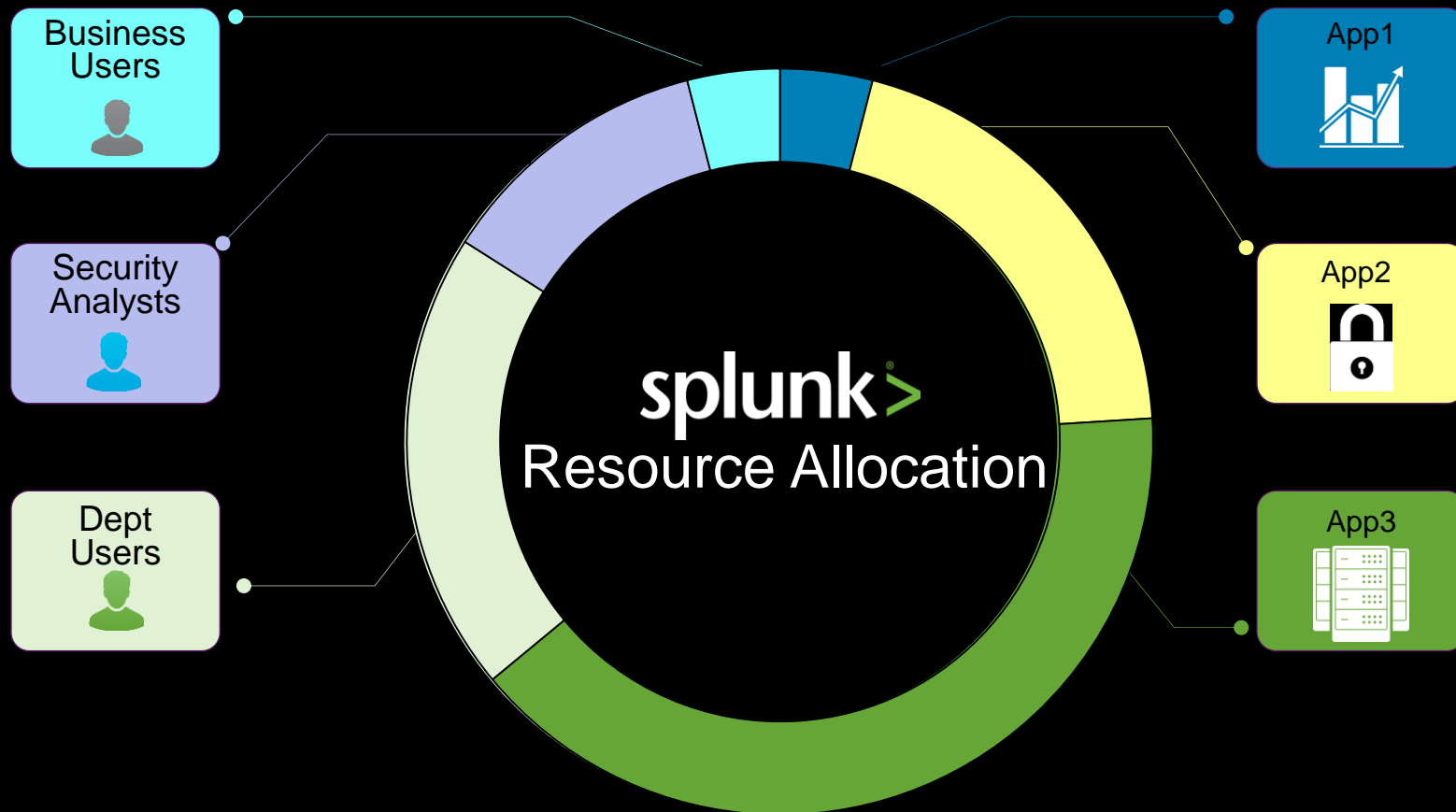
- ▶ New users run wildcard searches, all-time searches, real time searches
- ▶ Users/apps running wildcard or expensive searches
- ▶ Resource utilization goes through the roof and impacts other users
- ▶ High search load impacts data ingestion lag and fails to fire alerts in time

Lack of control to align resource allocation with business priorities



| App Priority | User Priority |
|--------------|-------------------|
| App1 | Business users |
| App2 | Security Analysts |
| App3 | Dept Users |

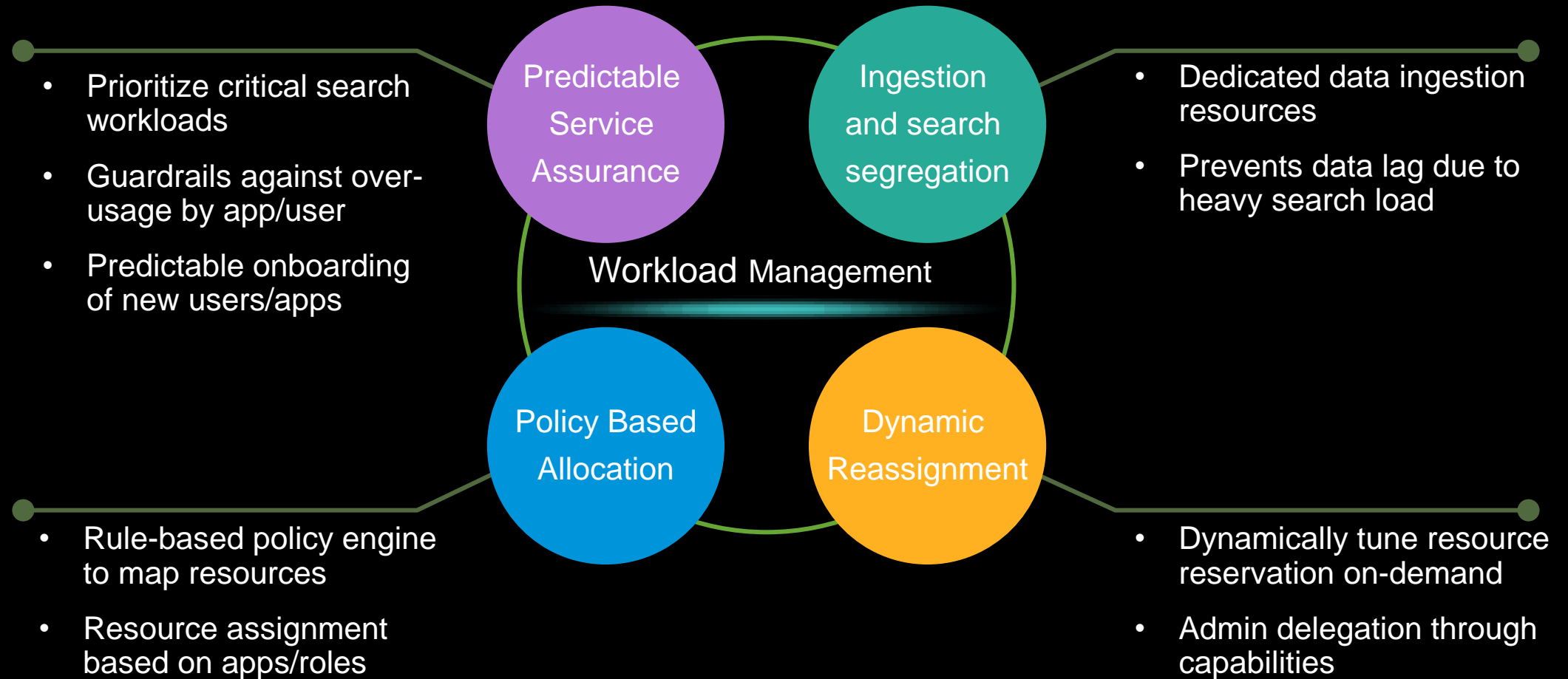
No guardrails over excessive resource usage



| App Priority | User Priority |
|--------------|-------------------|
| App1 | Business users |
| App2 | Security Analysts |
| App3 | Dept Users |

Workload Management

Aligns resource allocation with business priorities



Workload Pools and Rules

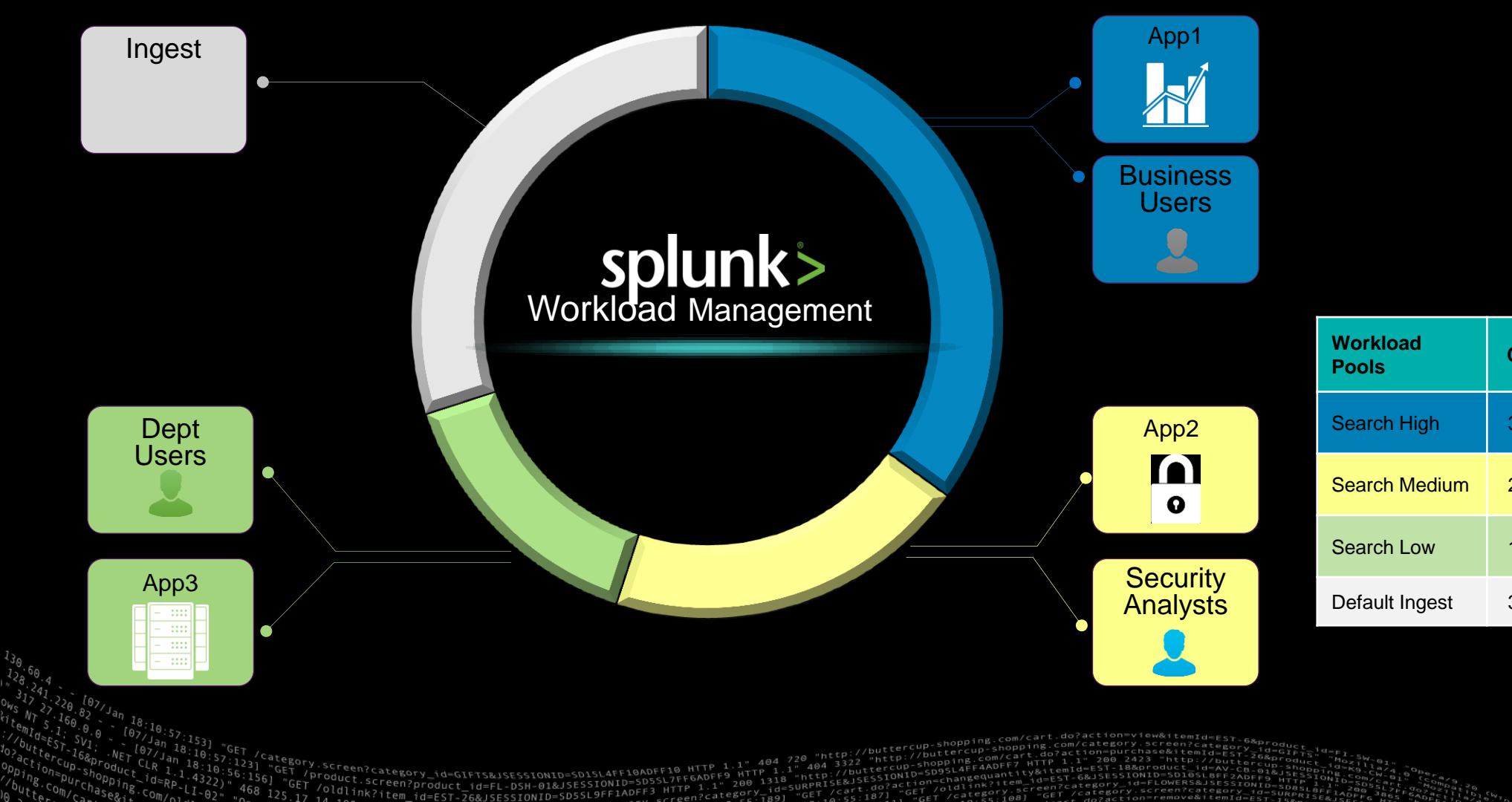
Policy Based Assignment of Resources

| Workload Pools | CPU | Memory | Workload Rules/Policy |
|----------------|-----|--------|-------------------------------|
| Search High | 35% | 35% | App=App1 Role=BusinessUser |
| Search Medium | 20% | 20% | App=App2 Role=SecAnalyst |
| Search Low | 15% | 15% | App=App3 Role=DeptUsers |
| Default Ingest | 30% | 30% | |

| App Priority | User Priority |
|--------------|-------------------|
| App1 | Business users |
| App2 | Security Analysts |
| App3 | Dept Users |

Workload Management

Control over resource allocation and enforced guardrails



| App Priority | User Priority |
|--------------|-------------------|
| App1 | Business users |
| App2 | Security Analysts |
| App3 | Dept Users |

| Workload Pools | CPU | Memory | Workload Rules/Policy |
|----------------|-----|--------|-------------------------------|
| Search High | 35% | 35% | App=App1 Role=BusinessUser |
| Search Medium | 20% | 20% | App=App2 Role=SecAnalyst |
| Search Low | 15% | 15% | App=App3 Role=DeptUsers |
| Default Ingest | 30% | 30% | |

Workload Management (Admin)

The screenshot shows the Splunk Enterprise Admin interface. The top navigation bar includes the Splunk logo, 'App: Search & Reporting', and a dropdown menu with 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. A search bar is on the right. Below the navigation bar, there are tabs for 'Search', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active, showing a search bar with the placeholder 'enter search here...', a 'No Event Sampling' dropdown, and a 'How to Search' section with links to 'Documentation' and 'Tutorial'. A 'Search History' link is also visible. A dropdown menu is open from the 'Administrator' link, showing a list of administrative tasks. The 'Workload Management' option is highlighted with a green circle. The background of the interface shows a log of network traffic.

splunk>enterprise App: Search & Reporting ▾

Administrator ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find 🔍

Search Datasets Reports Alerts Dashboards

Search

enter search here...

No Event Sampling ▾

How to Search

If you are not familiar with the search features, or want to learn more, see one of the following resources.

[Documentation](#) [Tutorial](#)

> Search History

Knowledge

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

Data

- Data inputs
- Forwarding and receiving
- Indexes
- Report acceleration summaries
- Virtual indexes
- Source types

DISTRIBUTED ENVIRONMENT

- Indexer clustering
- Forwarder management
- Distributed search

SYSTEM

- Server settings
- Server controls
- Instrumentation
- Licensing
- Workload Management**

USERS AND AUTHENTICATION

- Access controls

Monitoring Console

Explore Data

Add Data

Workload Management (Admin)

splunk>enterprise

Apps ▾



Administrator ▾

Messages ▾

Settings ▾

Activity ▾

Help ▾

Find



Workload Management

Enabled

Add Workload Pool

Add Workload Rule

Apply Changes

View, edit and apply configurations of workload management. [Learn more](#)

| Workload Pool | CPU (%) | Memory (%) | Default Search Pool | Default Ingest Pool | Actions | |
|---------------|---------|------------|---------------------|---------------------|----------------------|------------------------|
| pool_1 | 35 | 35 | | | Edit | Delete |
| pool_2 | 20 | 20 | | | Edit | Delete |
| pool_4 | 15 | 15 | | | Edit | Delete |
| pool_5 | 30 | 30 | | | Edit | Delete |

| Order | Workload Rule | Predicate | Workload Pool | Actions | |
|-------|---------------|----------------------------|---------------|----------------------|------------------------|
| 1 | rule_1 | app=search | pool_1 | Edit | Delete |
| 2 | rule_2 | role=admin | pool_2 | Edit | Delete |
| 3 | rule_3 | role=analyst | pool_2 | Edit | Delete |
| 4 | rule_5 | app=splunk_instrumentation | pool_4 | Edit | Delete |

Configuration Files

workload_pools.conf

```
[workload_pool:pool_1]
cpu_weight = 25
mem_weight = 25

[workload_pool:pool_2]
cpu_weight = 20
mem_weight = 20

[workload_pool:pool_4]
cpu_weight = 15
mem_weight = 15

[workload_pool:pool_5]
cpu_weight = 30
mem_weight = 30

[general]
default_pool = pool_4
enabled = 1
ingest_pool = pool_5
```

workload_rules.conf

```
[workload_rule:rule_1]
predicate = app=search
workload_pool = pool_1

[workload_rule:rule_2]
predicate = role=admin
workload_pool = pool_2

[workload_rule:rule_3]
predicate = role=analyst
workload_pool = pool_2

[workload_rules_order]
rules = workload_rule:rule_1,workload_rule:rule_2,workload_rule:rule_3,workload_rule:rule_5
rules_number = 4

[workload_rule:rule_5]
predicate = app=splunk_instrumentation
workload_pool = pool_4
```

Workload Management: Pool Creation

Workload Pools

- ▶ CPU/Memory resource pools
- ▶ Specify allocation of CPU and memory resources
- ▶ Indicate ingest or search pool

Workload Management
View, edit and apply configurations for workload management

There are no workload rules. Use the Add Workload Rule button to create a new rule.

| Workload Pool | CPU % | Memory % | Default Search Pool | Default Ingest Pool | Actions |
|---------------|-------|----------|---------------------|---------------------|-------------|
| IngestPool | 30 | | | | Edit Delete |
| SearchPool1 | 35 | | | | Edit Delete |
| SearchPool2 | 20 | | | | Edit Delete |
| SearchPool3 | 15 | | | | Edit Delete |

New Workload Pool

Name: SearchPool4

CPU %: 10

Memory %: 10

Default Search Pool: ☐

Default Ingest Pool: ☐

Cancel Submit

First Version

- ▶ One ingest pool
- ▶ Multiple Search Pools

```
130.60.4 - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SL4FF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20
128.241.220.82 - - [07/Jun 18:10:57:123] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MOX-11W-0" "Compa
ows NT 5.1; SV1: - - [07/Jun 18:10:57:153] "GET /category.screen?category_id=GIFTS&JSESSIONID=SD5SL4FF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemId=EST-6&product_id=FL-SW-01" "Opera/9.80.20
317 27.160.0.0 - - [07/Jun 18:10:57:153] "GET /product.screen?product_id=FL-DSH-01&JSESSIONID=SD5SL7FF6ADFF9 HTTP/1.1" 404 3322 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MOX-11W-0" "Compa
item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL4FF10ADFF10 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MOX-11W-0" "Compa
do?action=shopping-product_id=RP-LI-02" 468 125.17 14.10.189 "GET /oldlink?item_id=EST-26&JSESSIONID=SD5SL9FF1ADFF3 HTTP/1.1" 200 1316 "http://buttercup-shopping.com/cart.do?action=changequantity&itemId=EST-18&product_id=AV-CB-01&JSESSIONID=SD5SL4FF10ADFF10 HTTP/1.1" 200 2423 "http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MOX-11W-0" "Compa
http://buttercup-shopping.com/cart.do?action=purchase&itemId=EST-26&product_id=MOX-11W-0" "Compa
```

Workload Management: Rule Creation

Workload Rules:

- Determines assignment of pools based on custom rules
- Rules can be specified on an app, role or user basis
- Rules order determines rule precedence
- Provision to provide more complex rules going forward

Workload Management
View, edit and apply configurations for workload management

There are no workload rules. Use the Add Workload Rule button to create a new rule.

| Workload Pool | CPU % |
|---------------|-------|
| IngestPool | 30 |
| SearchPool1 | 35 |
| SearchPool2 | 20 |
| SearchPool3 | 15 |

New Workload Rule

Name

Predicate

Workload Pool

Cancel Submit

| Pool | Actions |
|------|-------------|
| | Edit Delete |
| | Edit Delete |
| | Edit Delete |
| | Edit Delete |

Workload Management
View, edit and apply configurations for workload management

There are no workload rules. Use the Add Workload Rule button to create a new rule.

| Workload Pool | CPU % |
|---------------|-------|
| IngestPool | 30 |
| SearchPool1 | 35 |
| SearchPool2 | 20 |
| SearchPool3 | 15 |

Edit Workload Rule: rule1

Order

Predicate

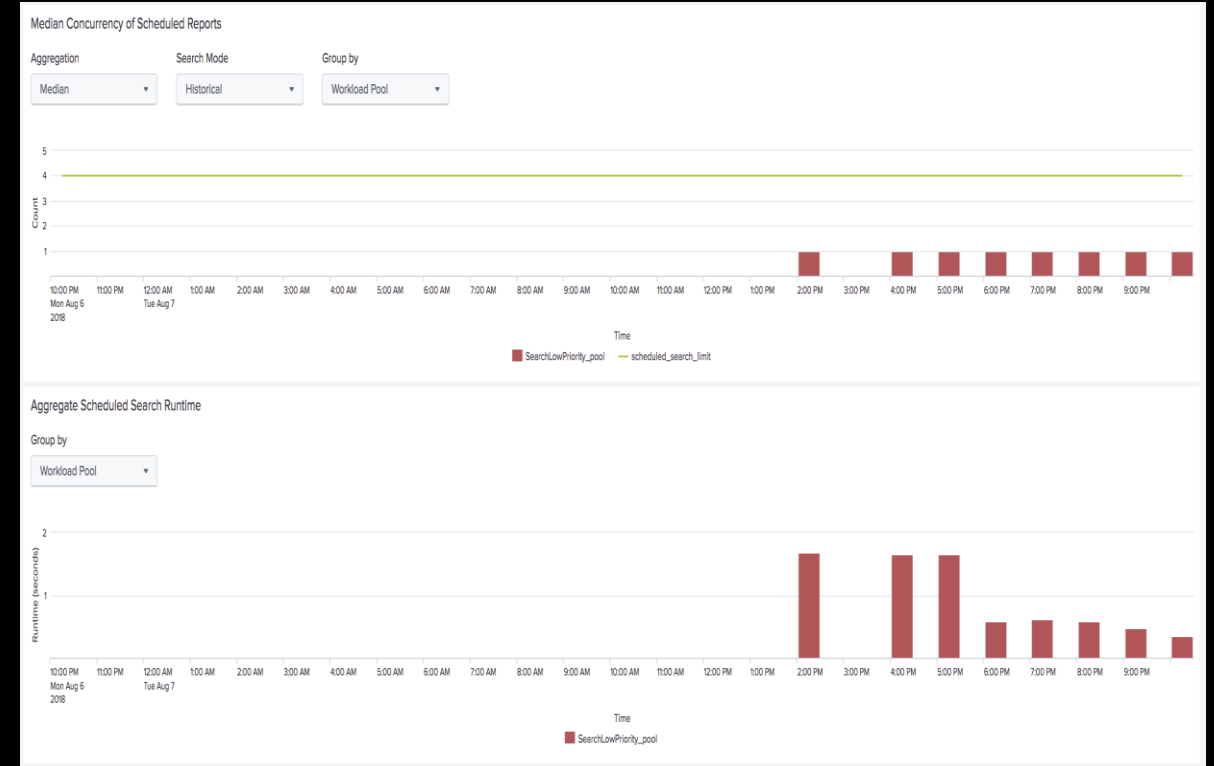
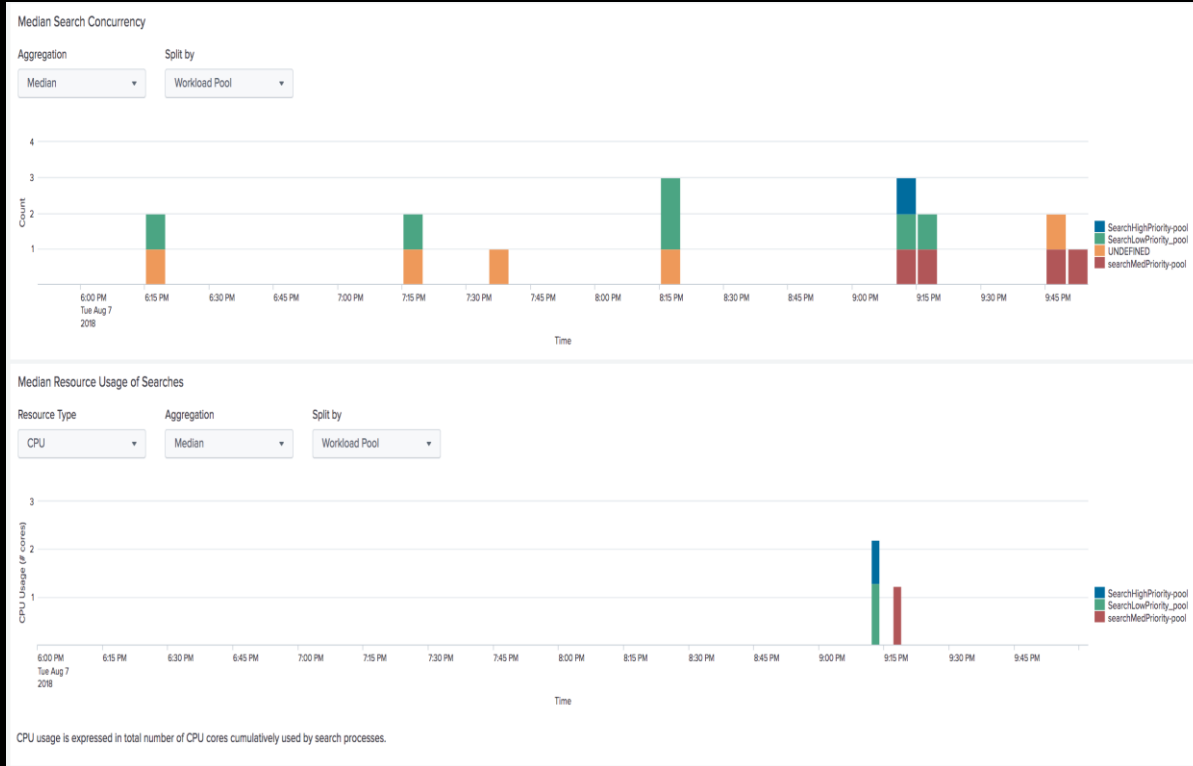
Workload Pool

Cancel Submit

| Pool | Actions |
|------|-------------|
| | Edit Delete |
| | Edit Delete |
| | Edit Delete |
| | Edit Delete |

Monitor Search and Scheduler Activity

Using New Workload Pools Filter



Dynamic Reassignment

On-demand Reassignment of workload pool

- ▶ Available through capabilities
- ▶ Allows power users to use higher/lower priority workload pools on-demand
- ▶ Available to ad-hoc and scheduled searches

| Capability | Actions |
|-----------------------|------------------------------|
| edit_workload_pools | Create/Modify Workload Pools |
| list_workload_pools | List Workload Pools |
| select_workload_pools | Select Workload Pools |
| edit_workload_rules | Create/Modify Workload Rules |
| list_workload_rules | List Workload Rules |

Dynamic Pool Selection: Ad-hoc Searches

New Search Save As ▾ New Table Close

index="access_combined" | eventstats first(bytes) as FirstBytes, last(_time) as mostRecentTestTime BY clientip | stats first(date_second) AS seconds, first(status) AS status BY clientip | sort -seconds Last 4 hours ▾ 🔍

✓ 0 events (8/8/18 7:33:00.000 AM to 8/8/18 11:33:13.000 AM) No Event Sampling ▾ Job ▾ ⏸ ■ ↶ 🖨 ⬇ SearchPool3 (default) ▾ 💡 Smart Mode ▾

Events Patterns **Statistics (0)** Visualization

20 Per Page ▾ ✎ Format Preview ▾

No results found. Try expanding the time range.

- Policy-Based Pool
Based on assigned policy
- SearchPool1
CPU: 35%, Memory: 35%
- SearchPool2
CPU: 20%, Memory: 20%
- ✓ SearchPool3 (default)
CPU: 15%, Memory: 15%

Dynamic Pool Selection: Scheduled Searches

Jobs

Manage your jobs. [Learn More](#)

3 Jobs App: Search & Reporting (search) Filter by owner Status: All filter 10 Per Page

Edit Selected

| | <input type="checkbox"/> | Owner | Application | Events | Size | Created at | Expires | Runtime | Status | Workload Pool | Actions |
|---|--------------------------|------------|-------------|--------|--------|----------------------------|----------------------------|----------|--------|---------------|----------------|
| > | <input type="checkbox"/> | whisper-qa | search | 0 | 92 KB | Aug 8, 2018 11:33:14 AM | Aug 8, 2018 11:46:46 AM | 00:00:01 | Done | SearchPool3 | Job ▾ ■ ↗ ⬇ |
| index="access_combined" eventstats first(bytes) as FirstBytes, last(_time) as mostRecentTestTime BY clientip stats first(date_second) AS seconds, first(status) AS status BY clientip sort -se... | | | | | | | | | | | |
| > | <input type="checkbox"/> | whisper-qa | search | 0 | 84 KB | Aug 8, 2018 11:33:09 AM | Aug 8, 2018 11:43:09 AM | 00:00:01 | Done | SearchPool3 | Job ▾ ■ ↗ ⬇ |
| index="access_combined" eventstats first(bytes) as FirstBytes, last(_time) as mostRecentTestTime BY clientip stats first(date_second) AS seconds, first(status) AS status BY clientip sort -se... | | | | | | | | | | | |
| > | <input type="checkbox"/> | whisper-qa | search | 0 | 488 KB | Aug 8, 2018 11:22:36 AM | Aug 8, 2018 11:44:01 AM | 00:11:24 | Failed | SearchPool3 | Job ▾ ■ ↗ ⬇ |
| metadata type=sourcetypes search totalCount > 0 [real-time] | | | | | | | | | | | |

Job Settings

×

Owner whisper-qa

App search

Read Permissions

Private

Everyone

Lifetime ?

10 minutes

7 days

Link To Job

<https://sh1.wlm-beta-qualcomm.splunkcloud.com>

Copy or bookmark the link by right-clicking the icon, or drag the icon into your bookmarks bar.

Workload Pool

SearchPool3 (default) ▾

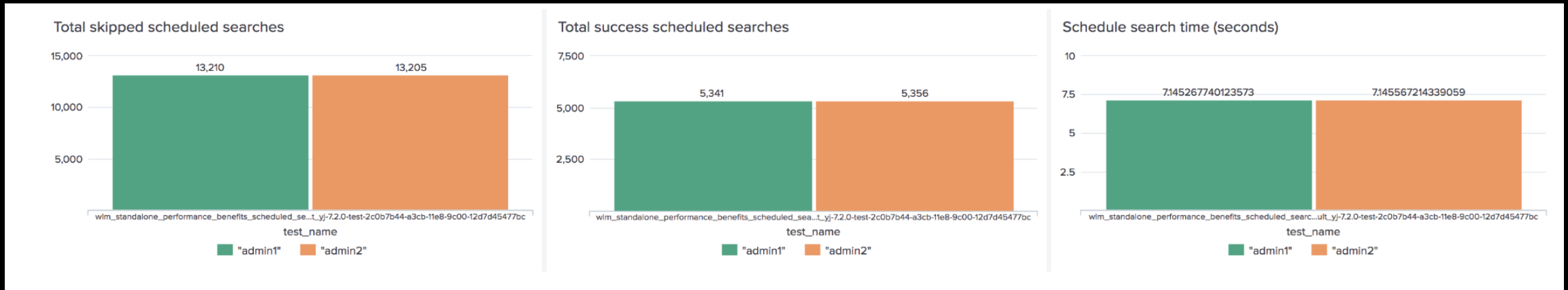
Workload pool can only be selected for running search jobs.

Cancel

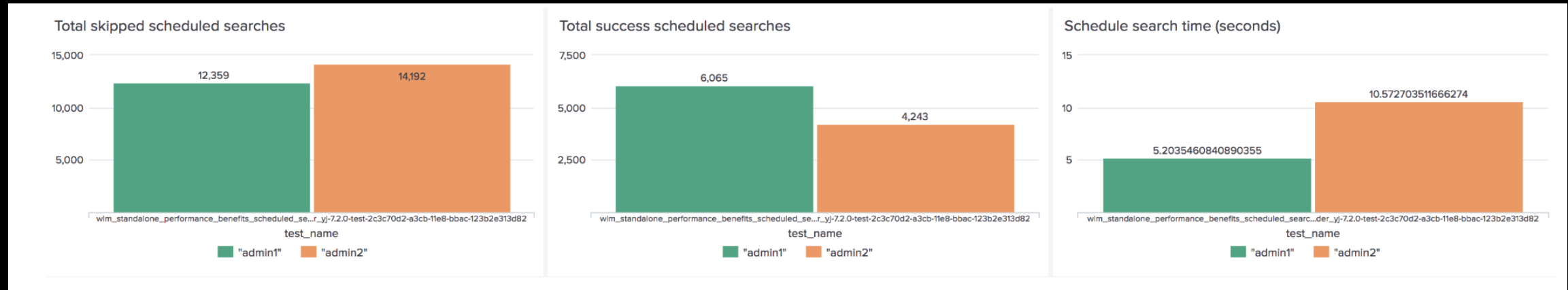
Save

Scheduled Search Behavior across Workload Pools

◆ WLM Disabled



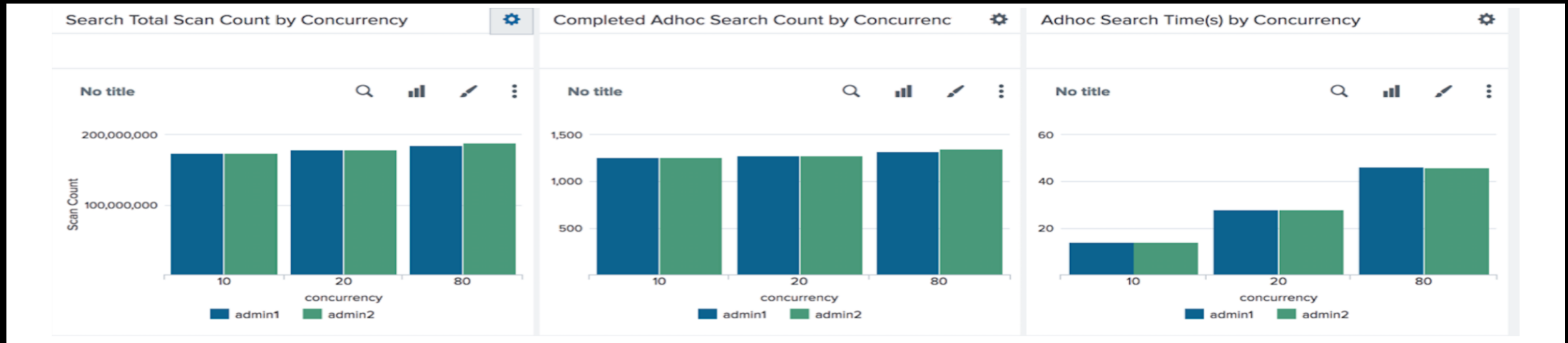
◆ WLM Enabled



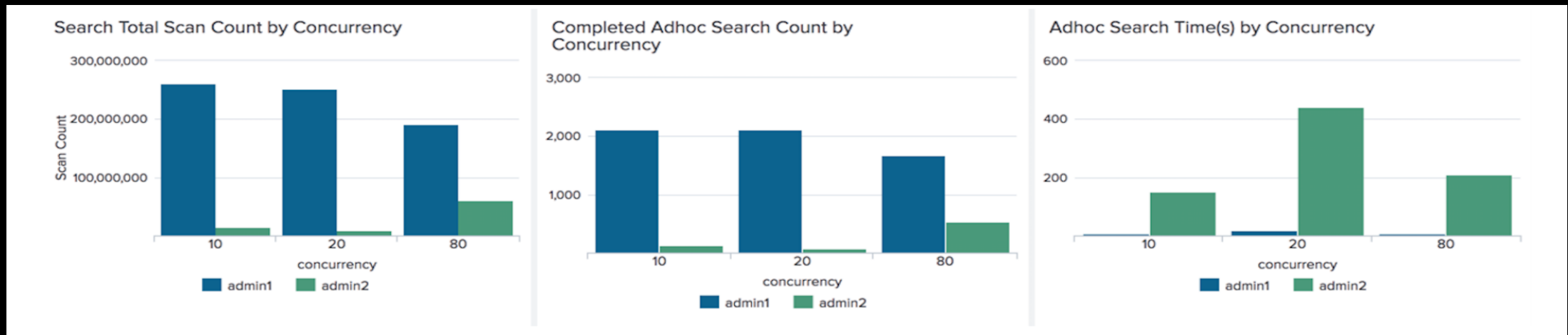
- ▶ Scheduled searches run faster in higher resource workload pool
- ▶ Fewer skipped searches in higher resource workload pool
- ▶ Higher number of successfully scheduled searches in higher resource workload pool

Ad-hoc Search Behavior across Workload Pools

◆ WLM Disabled

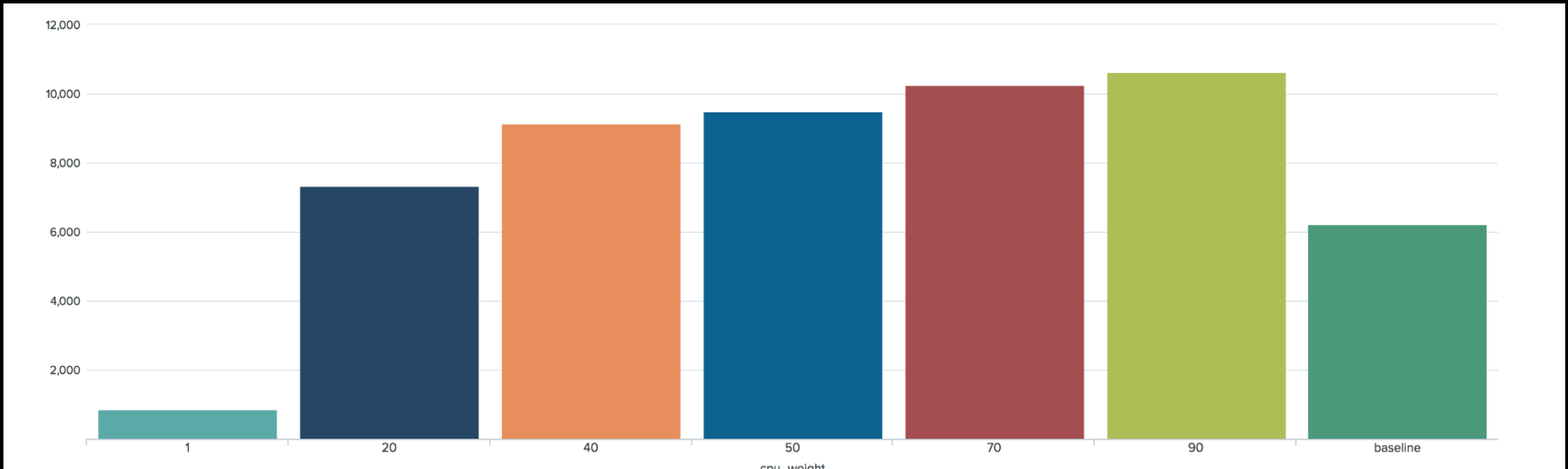


◆ WLM Enabled



- Ad-hoc searches run faster in higher resource workload pool
- Higher number of successfully completed ad-hoc searches by concurrency in higher resource workload pool

Ingest Behavior across Workload Pools



- ▶ Increased ingest throughput under CPU load for higher resource workload pool
- ▶ Throughput will be affected if resources are under-provisioned for Ingest pool
- ▶ Parallel ingestion pipeline sets can help achieve better performance with sufficient resource allocation for Ingest workload pool

Deep Dive

Setup, Configuration and Diagnostics

Setup

Systemd

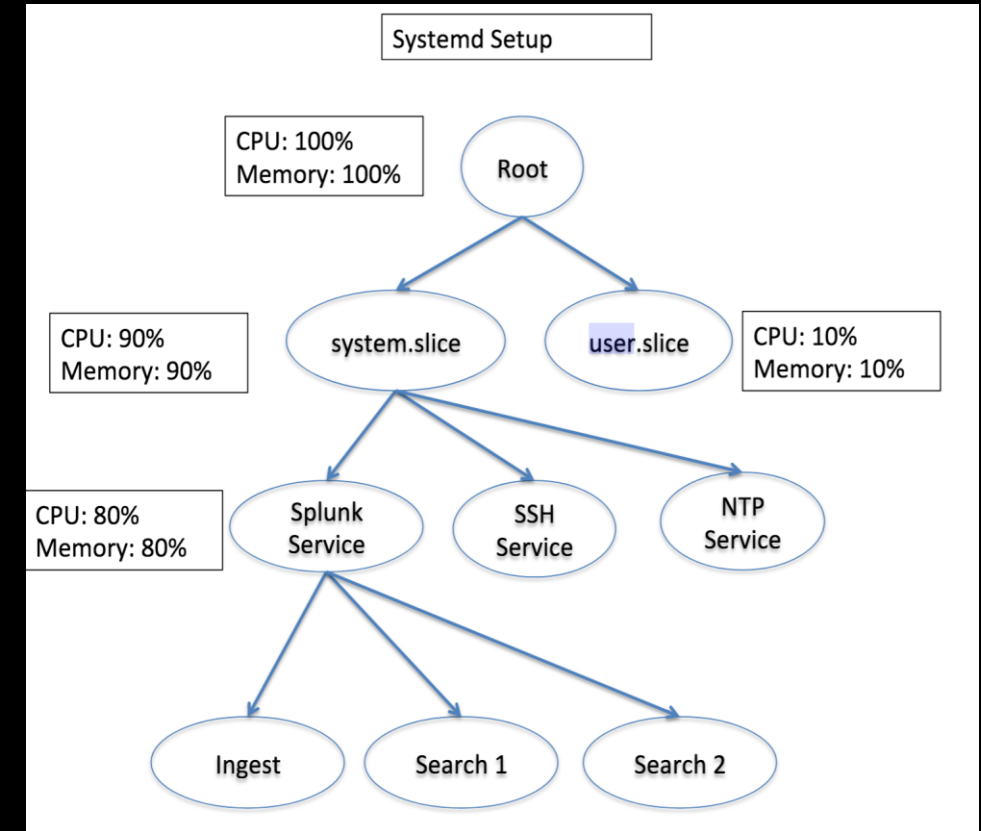
- Create a systemd unit file in /etc/systemd/system/systemd.service
 - Sample unit file available in the [docs](#)
- Run "systemctl daemon-reload" to reload the unit file
- Run splunk start. This starts splunkd as a systemd service.
- Verify that splunkd is running as a systemd service
systemctl status SPLUNK_SERVER_NAME.service

Assign CPU for "splunk" cgroup

- Total system CPU shares in /sys/fs/cgroup/cpu/cpu.shares
- Set CPU in
 - /sys/fs/cgroup/cpu/system.slice to 9126
 - /sys/fs/cgroup/cpu/system.slice/splunkd.service /cpu.shares to 9126

Assign physical memory for "splunk" cgroup

- Total system physical memory from /proc/meminfo
- Set Memory in
 - /sys/fs/cgroup/memory/memory.limit_in_bytes to 100% of total physical memory
 - /sys/fs/cgroup/memory/system.slice/memory.limit_in_bytes to 90% of total physical memory
 - /sys/fs/cgroup/memory/system.slice/splunkd.service/memory.limit_in_bytes to 80% of physical memory



Sample Unit File

[Service]

Restart=always

Type=simple

ExecStart=/root/rdimri/splunk/bin/splunk _internal_launch_under_systemd --accept-license --no-prompt --answer-yes --seed-passwd changeme

Delegate=true

#Splunk defines successful exit codes other than 0 to indicate special exit scenarios which are

#used by splunk operations like rolling-restart, offline etc.

SuccessExitStatus=51 52

RestartPreventExitStatus=51

RestartForceExitStatus=52

#On some systemd installations, systemd does not create cgroups for memory and cpu controller under system.slice

#rather it runs process under root cgroups, we can force systemd to create cgroups under system.slice by specifying

#MemoryLimit and CPUShares, please look at description below.

MemoryLimit=100G

CPUShares=1024

#If you want to run splunk as non-root user uncomment the following four lines.

PermissionsStartOnly=true

User=splunk

Group=splunk

ExecStartPost=/bin/bash -c "chown -R <USER Specified above>:<GROUP of User> /sys/fs/cgroup/cpu/system.slice/%n"

ExecStartPost=/bin/bash -c "chown -R <USER Specified above>:<GROUP of User> /sys/fs/cgroup/memory/system.slice/%n"

Setup

▶ Non-Systemd (Initd)

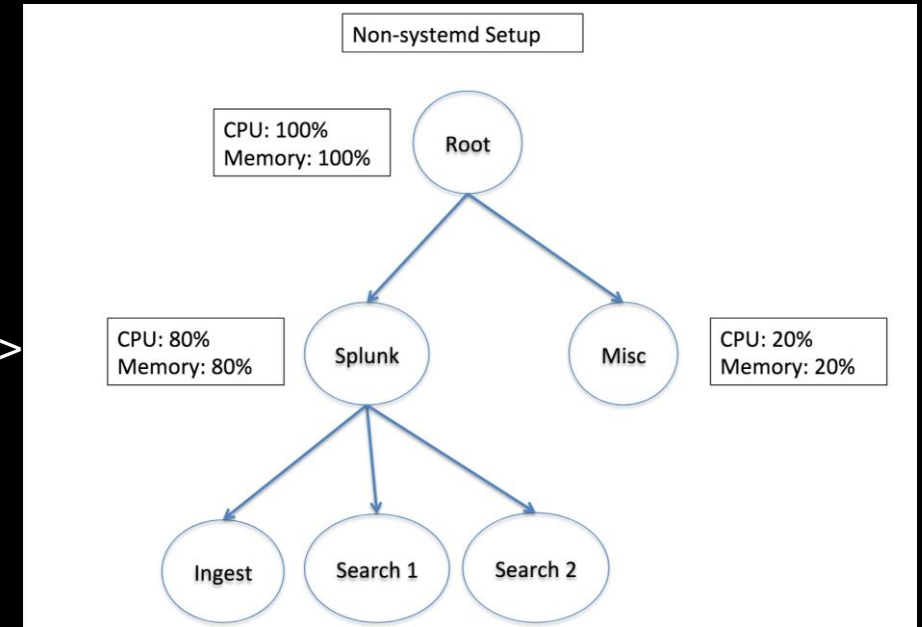
- Set splunk root cgroup in workload_pools.conf
[general]
`workload_pool_base_dir_name = splunk`
- Create cpu and memory cgroups
 - `sudo mkdir /sys/fs/cgroup/cpu/<workload_pool_base_dir_name>`
 - `sudo mkdir /sys/fs/cgroup/memory/<workload_pool_base_dir_name>`
 - `sudo chown -R ${USER} /sys/fs/cgroup/cpu/<workload_pool_base_dir_name>`
 - `sudo chown -R ${USER} /sys/fs/cgroup/memory/<workload_pool_base_dir_name>`

▶ Assign CPU for “splunk” cgroup

- Total system CPU shares in `/sys/fs/cgroup/cpu/cpu.shares`
- Set CPU in `/sys/fs/cgroup/cpu/splunk/cpu.shares` (80% of total cpu)

▶ Assign physical memory for “splunk” cgroup

- Total system physical memory from `/proc/meminfo`
- Set Memory in `/sys/fs/cgroup/memory/splunk/memory.limit_in_bytes` (80% of physical memory)



Configuration

- ▶ On a search head, perform the below steps through UI/CLI/REST
 - Create workload groups
 - Create workload rules
 - Enable workload Management
 - Check workload management status
 - splunk show workload-management-status
 - If search head is part of a search head cluster, changes are propagated to the other cluster members
- ▶ Indexer Cluster Configuration
 - Copy workload_pools.conf from search head to the CM
 - CM location: \$SPLUNK_HOME/etc/master-apps/_cluster/local directory
 - Execute CM bundle push from the CM

Interaction with Existing Search Quota Settings

- Existing search quota and scheduler priority changes continue to be applied along with Splunk Workload Management.
- Workload management does not attempt to override the settings described below.

| Setting Name | Configuration File | Description | Default Value |
|-------------------------|--------------------|--|---------------|
| srchJobsQuota | authorize.conf | Max number of concurrent historical searches by role | 3 |
| cumulativeSrchJobsQuota | authorize.conf | Max number of concurrent historical searches for all members of role | N/A |
| base_max_searches | limits.conf | Constant to add to max no of searches as a factor of CPUs | 6 |
| max_searches_per_cpu | limits.conf | Max number of concurrent historical searches per CPU | 1 |
| schedule_priority | savedsearches.conf | Raises scheduling priority of a search. Can have value: default, higher, highest. | default |

Key Takeaways

1. First level bullets should be sentence case, 28pt
2. First level bullets should be sentence case, 28pt
3. First level bullets should be sentence case, 28pt



Q&A

Thank You

Don't forget to **rate this session**
in the **.conf18** mobile app

.conf18

splunk>