Splunk Enterprise Security™

ES @ 100TB

Jesse Chen
Principal Performance Engineer | Splunk

Devendra Badhani
Sr Engineering Manager | 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.

Splunk, Splunk>, Turn Data Into Doing, 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. © 2019 Splunk Inc. All rights reserved.

ES @ 100TB

Jesse Chen

Jesse Chen

Principal Performance Engineer | Splunk

Devendra Badhani

Senior Engineering Manager | Splunk

What this talk is about

1. Scale tests in lab environment
2. Simulated workload
3. Confidence vote

What this talk is “NOT” about

1. Deployment architecture guidance
2. Sizing guide
3. Use case optimization

In This Session

1. Why the 100TB test?
2. Workload considerations
3. Tests and results
4. Best practices for scaling

Why the 100TB Test?

Incidents and Asks

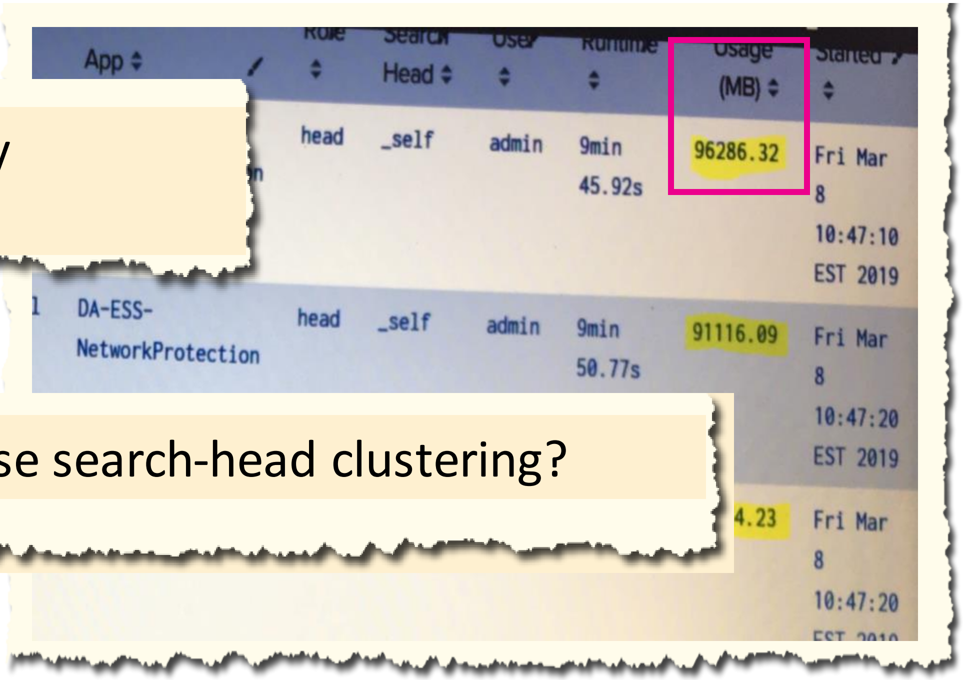
* Problem Statement: Continuous memory spikes on ES causing search head causing Splunk to go down - a total of 6 times today

Doing great at 15TB, can we get to 30?

eality (at the moment and trending towards healthier in most
many buckets in those indexes.

An expensiv
Some get
Some getting
Some returning after 500+ secs
Bundle errors were seen (unable to distribute)
ES warning on memory, but is up. Slowed

Expanding a 35TB to 60TB, getting ready to buy hardware (millions$), will it work?



App		Role	Search Head	User	Runtime	Usage (MB)	Started
n		head	_self	admin	9min 45.92s	96286.32	Fri Mar 8 10:47:10 EST 2019
DA-ESS-NetworkProtection		head	_self	admin	9min 50.77s	91116.09	Fri Mar 8 10:47:20 EST 2019
						4.23	Fri Mar 8 10:47:20 EST 2019

Can Enterprise Security use search-head clustering?

Cluster peer status is flapping Up and Down.

LISTEN, LINDA, LISTEN...
memegenerator.net

Workload Considerations

Key test parameters

Representative Workload

Search Head Cluster - Multi-Site	20-node search head cluster with ES	✓
Indexer Cluster – Multi-Site	3 sites; replication factor: 2; search factor: 2	✓
SmartStore	Enabled, with AWS S3 object store	✓
Top Technology Add-Ons (TAs)	TAs in ES, F5 bigip, palo-alto, checkpoint-opseclea, bluecoat-proxysg,akamai	✓
Top source types	Pan:traffic, wineventlog, syslog, f5:bigip:apm:syslog, akamai:cm:json, opsec, bro_dns, and more	✓
Scheduled searches	Correlation, tracker, generating	✓
Data Model Acceleration	All built-in CIM data models accelerated	✓
ES UI pages	Top 10 pages: security_posture, incident_review, etc.	✓
Ad-hoc searches in Splunk Web	160K searches per day, e.g., “search index=_internal INFO sourcetype=splunkd”	✓
Many buckets	13M	✓
Knowledge Bundles	1.4M assets, 300K identities; total 1.2GB in size	✓
Notable events per day	2000+	✓
Splunk version	7.3.0	✓
Enterprise Security	5.3.0	✓

By the Numbers

100TB

Daily ingestion

1000

Indexers

500

Indexes

500

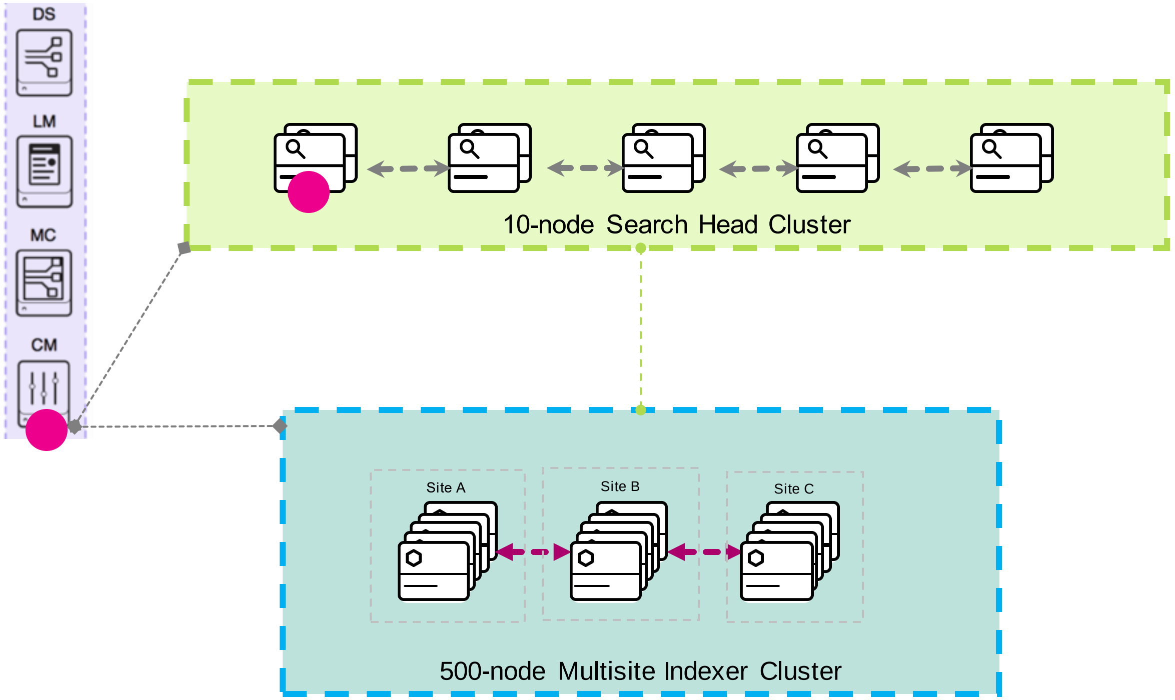
Saved searches

1GB

Knowledge bundle

Default Topology

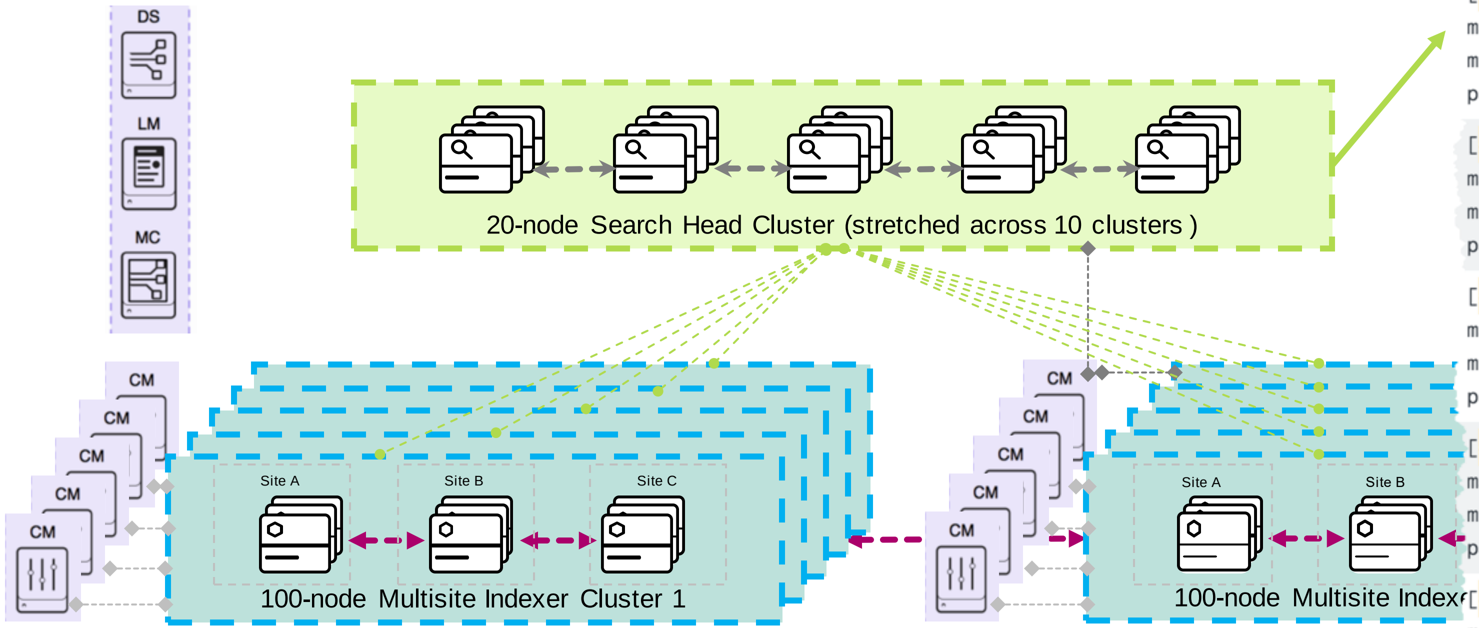
Search Head Cluster + 1 large indexer cluster

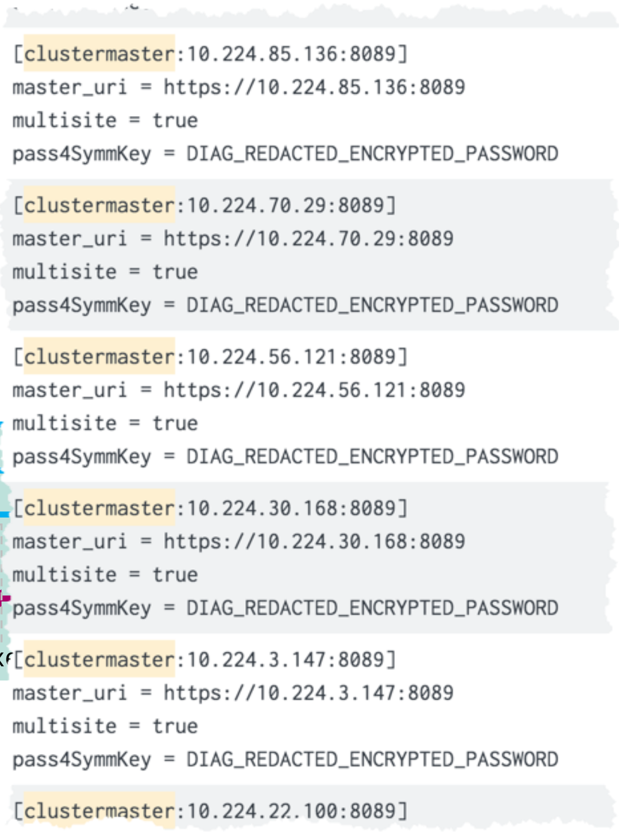

DS
LM
MC
CM
10-node Search Head Cluster
Site A
Site B
Site C
500-node Multisite Indexer Cluster

Signs of stress
Search head captain: Knowledge bundle replication times increase; CPU 100%
Cluster Master: SmartStore bootstrap, rolling restart, fixup times increase

Better: Distributed Clustered Deployment

Stretched Search Head Cluster + Indexer Clusters


DS
LM
MC
20-node Search Head Cluster (stretched across 10 clusters)
CM
CM
CM
CM
CM
Site A
Site B
Site C
100-node Multisite Indexer Cluster 1
CM
CM
CM
CM
CM
Site A
Site B
100-node Multisite Indexe



```
[clustermaster:10.224.85.136:8089]
master_uri = https://10.224.85.136:8089
multisite = true
pass4SymmKey = DIAG_REDACTED_ENCRYPTED_PASSWORD
[clustermaster:10.224.70.29:8089]
master_uri = https://10.224.70.29:8089
multisite = true
pass4SymmKey = DIAG_REDACTED_ENCRYPTED_PASSWORD
[clustermaster:10.224.56.121:8089]
master_uri = https://10.224.56.121:8089
multisite = true
pass4SymmKey = DIAG_REDACTED_ENCRYPTED_PASSWORD
[clustermaster:10.224.30.168:8089]
master_uri = https://10.224.30.168:8089
multisite = true
pass4SymmKey = DIAG_REDACTED_ENCRYPTED_PASSWORD
[clustermaster:10.224.3.147:8089]
master_uri = https://10.224.3.147:8089
multisite = true
pass4SymmKey = DIAG_REDACTED_ENCRYPTED_PASSWORD
[clustermaster:10.224.22.100:8089]
```

Size: This environment has **16,688** CPU cores, **262** TB of RAM (~20 full data center racks!)
AWS Instance types: c5.9xlarge (search head), **i3.8xlarge** (indexer), **x1.16xlarge** (cluster master),
10 Gigabit network, 4X1.9 NVMe SSD as local storage
How to: Google "Splunk configure multi cluster search"

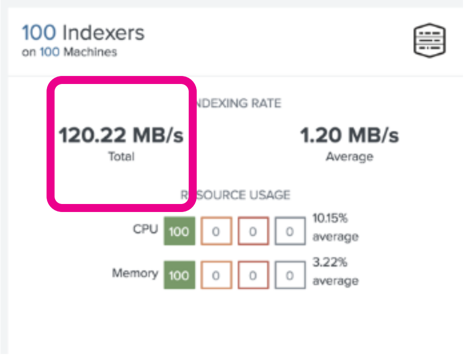
Tests & Results

How does ES perform on SHC at 100TB?

ES Results

Per day

Ingestion: 100GB / indexer / day
Searches: 160,000 / day
Concurrency: 70 at peak



100 Indexers
on 100 Machines

NDEXING RATE

120.22 MB/s
Total

1.20 MB/s
Average

R SOURCE USAGE

CPU	100	0	0	0	10.15% average
Memory	100	0	0	0	3.22% average

Tip: You can find cluster ingestion rate in the Monitor Console. Example shows one of our clusters during level load.

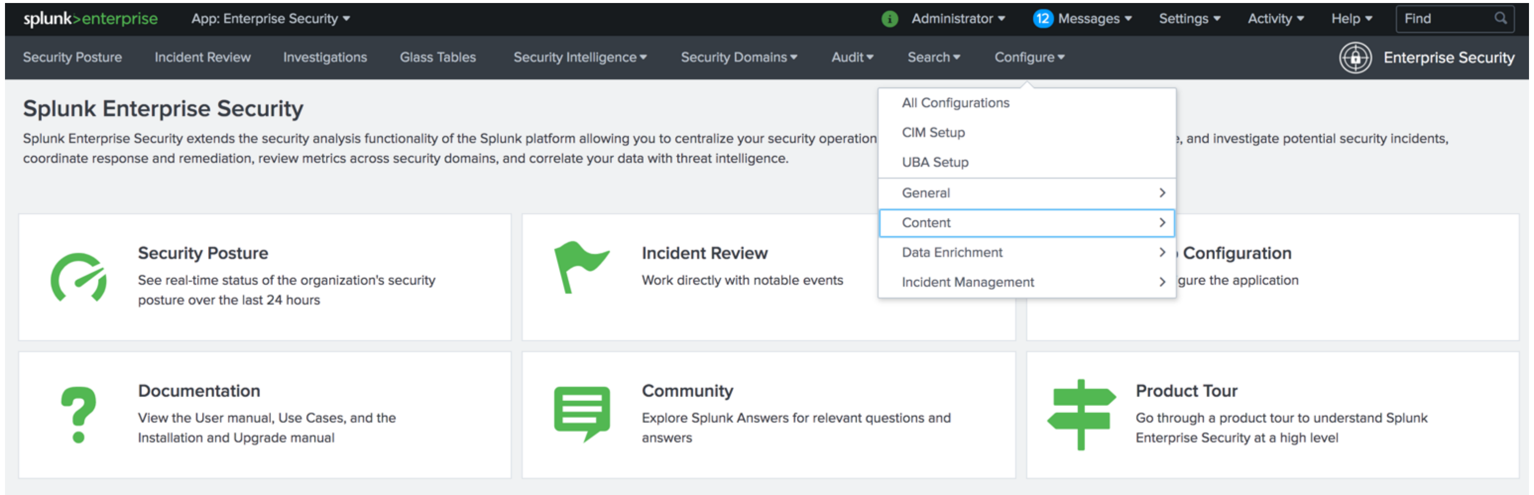
Search performance

- DMA <= 300 seconds
- Correlation < 100 seconds
- Ad-hoc 8~50 seconds
- ES UI page load times: avg. 50 seconds
- Skip rates < 1%
- Rolling restart time: a few minutes

Resource utilization

- Both search head & indexer
  - CPU% < 15%
  - Memory < 20GB
  - IOPS < 74K
  - Network < 40 MB/s
- Low resource usage
  - 300~400TB/day possible on this stack
  - Over-provisioned

ES UI Performance



Splunk Enterprise Security

Splunk Enterprise Security extends the security analysis functionality of the Splunk platform allowing you to centralize your security operation , and investigate potential security incidents, coordinate response and remediation, review metrics across security domains, and correlate your data with threat intelligence.

Security Posture
See real-time status of the organization's security posture over the last 24 hours

Incident Review
Work directly with notable events

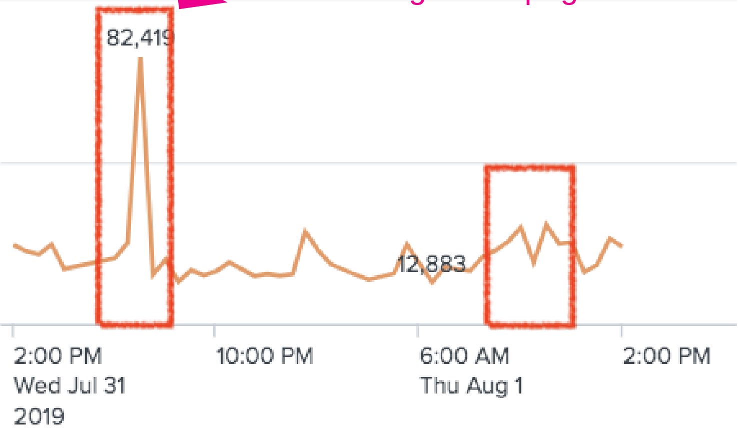
Configuration
gure the application

Documentation
View the User manual, Use Cases, and the Installation and Upgrade manual

Community
Explore Splunk Answers for relevant questions and answers

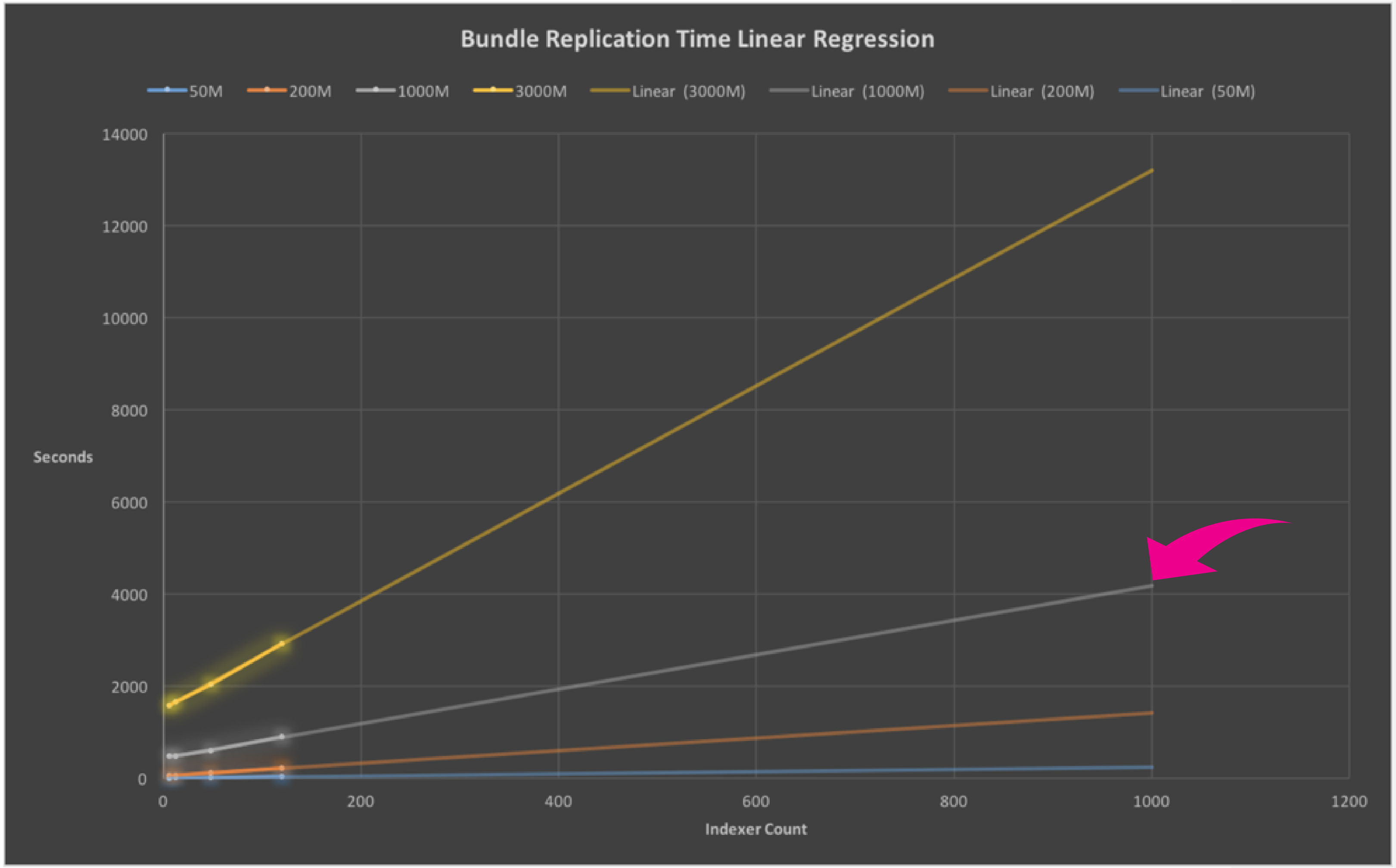
Product Tour
Go through a product tour to understand Splunk Enterprise Security at a high level

Big impact: Bundle replication slows down UI. Ex. Content Management page.



Bundle Replication

Linear and predictable



Measured: Bundle replication time of 1GB assets and identities onto 1000 nodes is close to predicted.

Scaling Recommendations

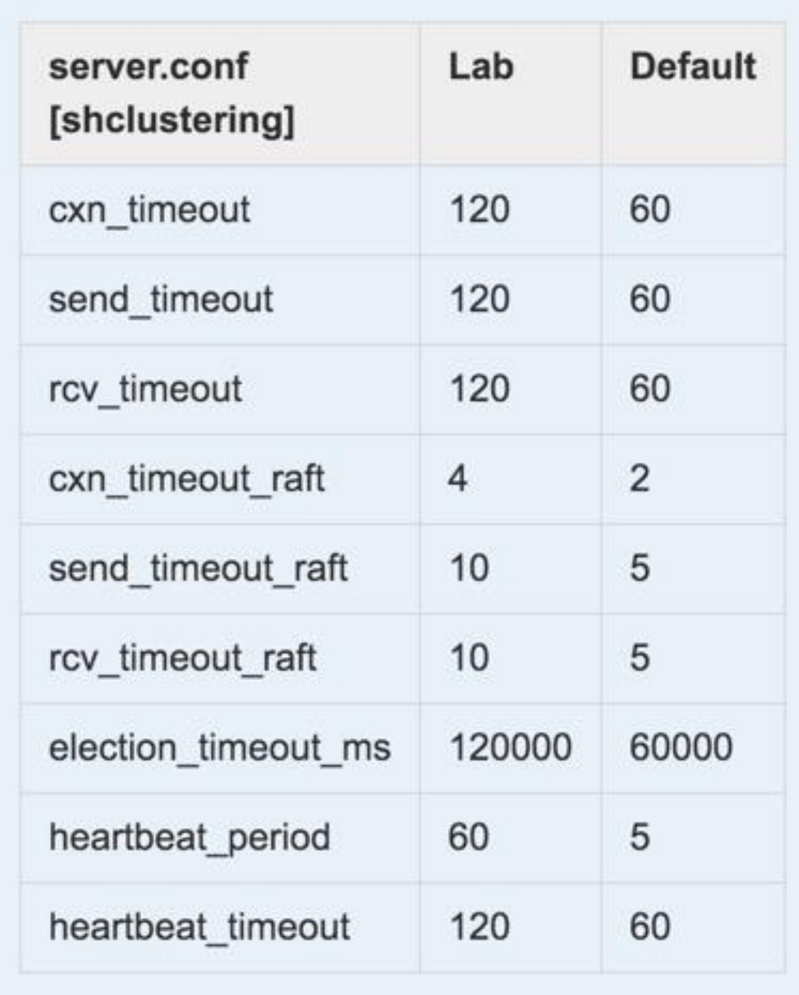
Splunk/ES Tuning

Category	Tune this	Outcome
Indexing	`parallelIngestionPipelines=2`	Can leverage addition CPU cores for higher indexing throughput

Data Model Acceleration	`[cim_Web_indexes]`
	`definition = (index=web OR index=bluct001)`
		Data model acceleration does not have to look at index=*, reducing lag

Search Scheduling	`allow_skew = 50%`	Distribute your saved searches more evenly; avoid search “waves”
	`max_searches_per_cpu = 5`	Help reduce “Max concurrent searches reached" errors; experiment with your load
	`acceleration.max_concurrent = 5`	For data models that are slower to accelerate
Bundle Replication	`replication_period_sec = 3600`	Time between two successive bundle replications. If the default 1 minute is too frequent, increase to a longer period to reduce stress on search head

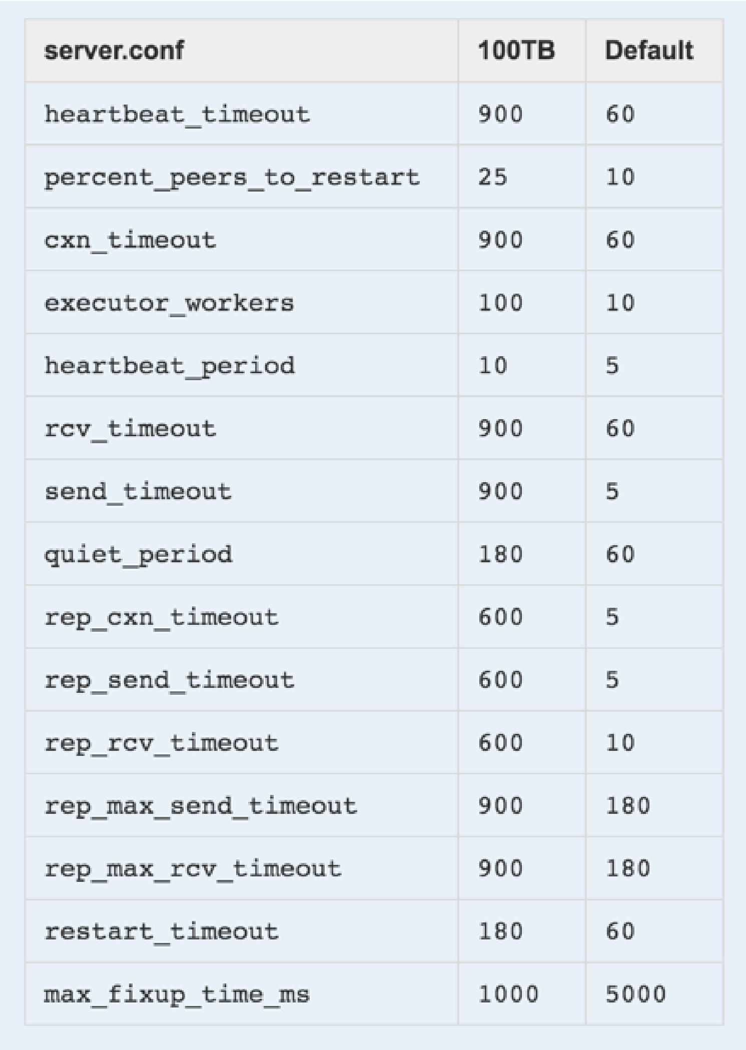
Search Head Cluster Settings



server.conf [shclustering]	Lab	Default
cxn_timeout	120	60
send_timeout	120	60
rcv_timeout	120	60
cxn_timeout_raft	4	2
send_timeout_raft	10	5
rcv_timeout_raft	10	5
election_timeout_ms	120000	60000
heartbeat_period	60	5
heartbeat_timeout	120	60

election_timeout_ms: The amount of time, in milliseconds, that a member waits before trying to become the captain. Make them wait longer with more members.

Cluster Settings



server.conf	100TB	Default
heartbeat_timeout	900	60
percent_peers_to_restart	25	10
cxn_timeout	900	60
executor_workers	100	10
heartbeat_period	10	5
rcv_timeout	900	60
send_timeout	900	5
quiet_period	180	60
rep_cxn_timeout	600	5
rep_send_timeout	600	5
rep_rcv_timeout	600	10
rep_max_send_timeout	900	180
rep_max_rcv_timeout	900	180
restart_timeout	180	60
max_fixup_time_ms	1000	5000

Increase timeouts for large Splunk deployments

Improve Cluster Master response times

Improve remote bucket bootstrapping (SmartStore)

More in depth –
Attend session **FN1635** *“What’s On Your Bucket List?”*
Thursday, October 24, 11:45 AM - 12:30 PM

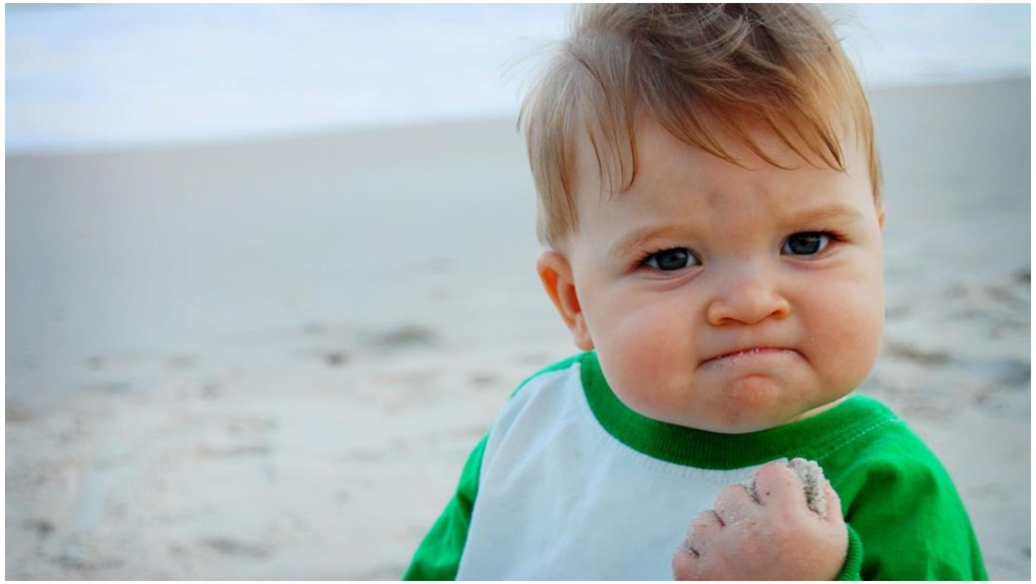
In Conclusion

Yes, 100TB ES is doable!

Yes, you can run ES on SHC!

Proven topology for large scale

Tuning to help improve response times



Security, Compliance and Fraud Intermediate

SEC2120 - Scaling Splunk Enterprise Security

SCHEDULE Wednesday, October 23, 04:15 PM - 05:00 PM

Marquis Montgomery, Principal Security Architect, Splunk

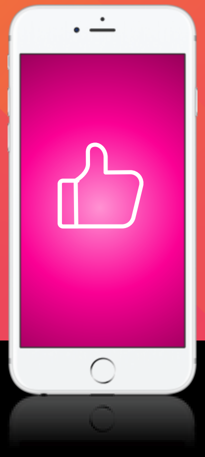
More from the real world!

Email us:
Jesse Chen jessec@splunk.com
Devendra Badhani dbadhani@splunk.com

.conf19

splunk>

Thank You!



Go to the .conf19 mobile app to

RATE THIS SESSION