

Forward-Looking Statements



This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. 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.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. 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 us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no 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.

Splunk, Splunk> and Turn Data Into Doing 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. © 2023 Splunk Inc. All rights reserved.

Administrators Anonymous

Interactive Splunk Therapy Session
With Splunk Trust Experts
PLA1347C

Tom Kopchak

Director of Technical Operations, Splunk
Implementation Lead | Hurricane Labs



splunk> .conf23

<https://splk.it/pla1347c>





Tom Kopchak

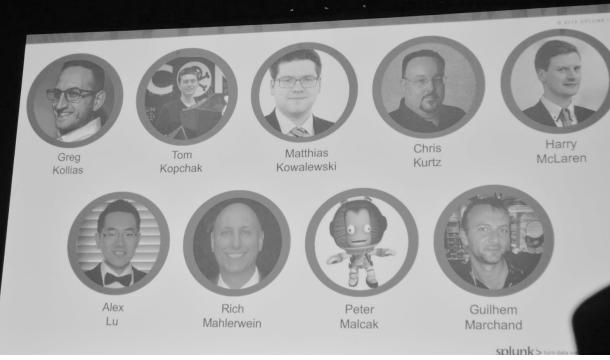
Director of Technical Operations, Splunk
Implementation Lead | Hurricane Labs

Hurricane Labs

My goal: You learn something new



Why Are We Here?



To Learn to be Better Splunk Admins!



Tools for Today

Your Splunk Environment

Lab Splunk
Environment

Help From
a Fez

Workshop
Materials

Audience
Participation

🔗 Check This Out:

[github.com/HurricaneLabs
/conf23_PLA1347C](https://github.com/HurricaneLabs/conf23_PLA1347C)



Tools for Today

Your Splunk Environment

Lab Splunk
Environment



🔗 Check This Out:

[github.com/HurricaneLabs
/conf23_PLA1347C](https://github.com/HurricaneLabs/conf23_PLA1347C)

Tools for Today

Your Splunk Environment

Lab Splunk
Environment



🔗 Check This Out:

[github.com/HurricaneLabs
/conf23_PLA1347C](https://github.com/HurricaneLabs/conf23_PLA1347C)

Tools for Today

Your Splunk Environment

Lab Splunk
Environment



🔗 Check This Out:

[github.com/HurricaneLabs
/conf23_PLA1347C](https://github.com/HurricaneLabs/conf23_PLA1347C)

Tools for Today

Your Splunk Environment

Lab Splunk
Environment



🔗 Check This Out:

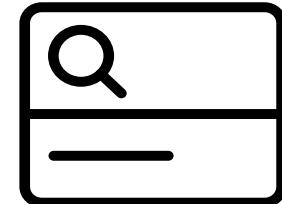
[github.com/HurricaneLabs
/conf23_PLA1347C](https://github.com/HurricaneLabs/conf23_PLA1347C)

Hands-On Training

Whenever possible, use your own environment for examples!

Your Splunk

Results tailored to
your environment

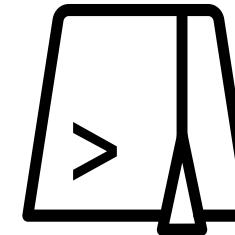
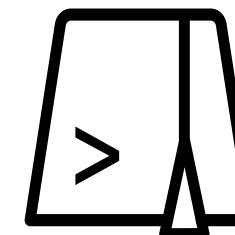
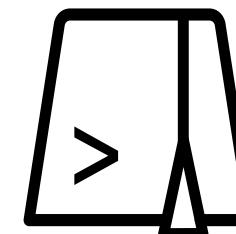
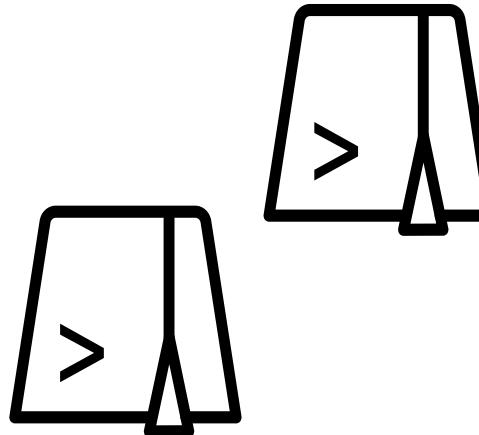
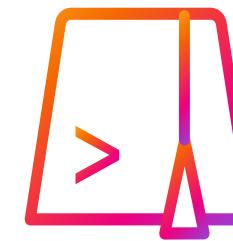
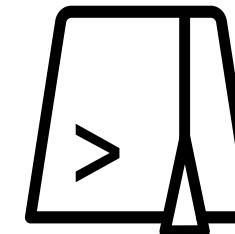
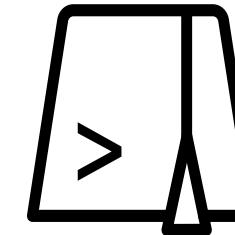
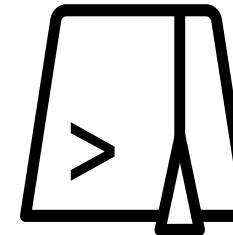
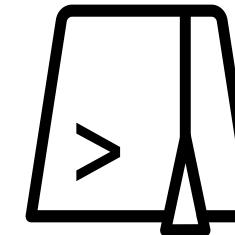
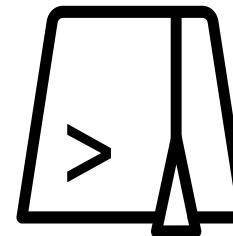
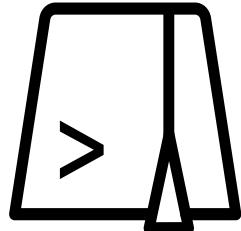


Demo Splunk

May work better for
some examples

If You Need Help?

Find a fez!



Today's Goals

What we're going to cover



Today's Goals

What we're going to cover



+ Keep your **auditors** happy

Not having data from 6 months ago when they expect it is *not* a recommendation for increased job security

Today's Goals

What we're going to cover



- + Keep your **auditors** happy
Not having data from 6 months ago when they expect it is *not* a recommendation for increased job security

- + Keep your **users** happy
You want everyone to get the same search results, right?

Today's Goals

What we're going to cover



- + Keep your **auditors** happy
Not having data from 6 months ago when they expect it is *not* a recommendation for increased job security
- + Keep your **users** happy
You want everyone to get the same search results, right?
- + Keep your **Splunk instance** happy
Everyone's search doesn't need to run at 9am

Today's Goals

What we're going to cover



- + Keep your **auditors** happy
Not having data from 6 months ago when they expect it is *not* a recommendation for increased job security
- + Keep your **users** happy
You want everyone to get the same search results, right?
- + Keep your **Splunk instance** happy
Everyone's search doesn't need to run at 9am
- + Keep your **SOC team** happy
Alerts work best when they run against the right data

Today's Goals

What we're going to cover



- + Keep your **auditors** happy
Not having data from 6 months ago when they expect it is *not* a recommendation for increased job security
- + Keep your **users** happy
You want everyone to get the same search results, right?
- + Keep your **Splunk instance** happy
Everyone's search doesn't need to run at 9am
- + Keep your **SOC team** happy
Alerts work best when they run against the right data
- + Keep **YOU** happy!
Why they let me stand here and say things

Let's get started!





Let's Talk About Auditors





Data Retention and Splunk

Data Retention and Splunk

Default settings can cause data loss!

By default: Splunk indexes store 500gb of data

Data Retention and Splunk

Default settings can cause data loss!

By default: Splunk indexes store 500gb of data

- + With default settings (in Splunk® Enterprise), once you have 500gb of data in an index, that data is **deleted!**
 - This is independent of any other time-based retention settings (unless they are reached first)
 - maxTotalDataSizeMB = 500000
 - Data actually rolls to frozen, but will be deleted if you don't have frozen storage defined

Data Retention and Splunk

Default settings can cause data loss!

By default: Splunk indexes store 500gb of data

- + With default settings (in Splunk® Enterprise), once you have 500gb of data in an index, that data is **deleted!**
 - This is independent of any other time-based retention settings (unless they are reached first)
 - maxTotalDataSizeMB = 500000
 - Data actually rolls to frozen, but will be deleted if you don't have frozen storage defined
- + This may result in having less data in Splunk than required for compliance!
 - If you're using volume definitions, check out maxVolumeDataSizeMB for the same issue

Data Retention and Splunk

Default settings can cause data loss!

By default: Splunk indexes store 500gb of data

- + With default settings (in Splunk® Enterprise), once you have 500gb of data in an index, that data is **deleted!**
 - This is independent of any other time-based retention settings (unless they are reached first)
 - maxTotalDataSizeMB = 500000
 - Data actually rolls to frozen, but will be deleted if you don't have frozen storage defined
- + This may result in having less data in Splunk than required for compliance!
 - If you're using volume definitions, check out maxVolumeDataSizeMB for the same issue
- + Less of an issue for Splunk® Cloud Platform, due to how retention is set in the UI

Data Retention and Splunk

Default settings can cause data loss!

By default: Splunk indexes store 500gb of data

- + With default settings (in Splunk® Enterprise), once you have 500gb of data in an index, that data is **deleted!**
 - This is independent of any other time-based retention settings (unless they are reached first)
 - maxTotalDataSizeMB = 500000
 - Data actually rolls to frozen, but will be deleted if you don't have frozen storage defined
- + This may result in having less data in Splunk than required for compliance!
 - If you're using volume definitions, check out maxVolumeDataSizeMB for the same issue
- + Less of an issue for Splunk® Cloud Platform, due to how retention is set in the UI

Best Practice:

Set maxTotalDataSizeMB to the largest legal value (4294967295 on-prem, 0 in Splunk Cloud) to force time-based data retention

Your Turn!



Data Retention Lab Instructions

Try it yourself!

- + Run the Lab 1 search from  GitHub on your search head

- + Review the **Archive Time** column
 - This is your configured retention period

- + Review the **Max Total Data Size (MB)** column
 - This is the max index size

- + Review the **Cold To Frozen** column
 - This is what happens when your data expires

Index	Indexer	Disabled	homeVolume	coldVolume	Max Bucket Time	Max Bucket Size (MB)	Max Hot Buckets	Max Warm Buckets	Archive Time	Max Total Data Size (MB)	Cold To Frozen	count
audit_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
ba_test	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
botsv3	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	1609014
botsv4	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	533389
bro	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
cim_modactions	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	420
endpoint_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	1
firealerts	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
gia_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years.	750	auto	300	3 years.	500000	Delete	10

Data Retention Lab Instructions

Try it yourself!

+ Run the Lab 1 search from  GitHub on your search head

+ Review the **Archive Time** column
— This is your configured retention period

+ Review the **Max Total Data Size (MB)** column
— This is the max index size

+ Review the **Cold To Frozen** column
— This is what happens when your data expires

Index	Indexer	Disabled	homeVolume	coldVolume	Max Bucket Time	Max Bucket Size (MB)	Max Hot Buckets	Max Warm Buckets	Archive Time	Max Total Data Size (MB)	Cold To Frozen	count
audit_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
ba_test	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
botsv3	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	1609014
botsv4	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	533389
bro	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
cim_modactions	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	420
endpoint_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	1
firedalerts	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
gia_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years.	750	auto	300	3 years	500000	Delete	10

Data Retention Lab Instructions

Try it yourself!

+ Run the Lab 1 search from  GitHub on your search head

+ Review the **Archive Time** column
– This is your configured retention period

+ Review the **Max Total Data Size (MB)** column
– This is the max index size

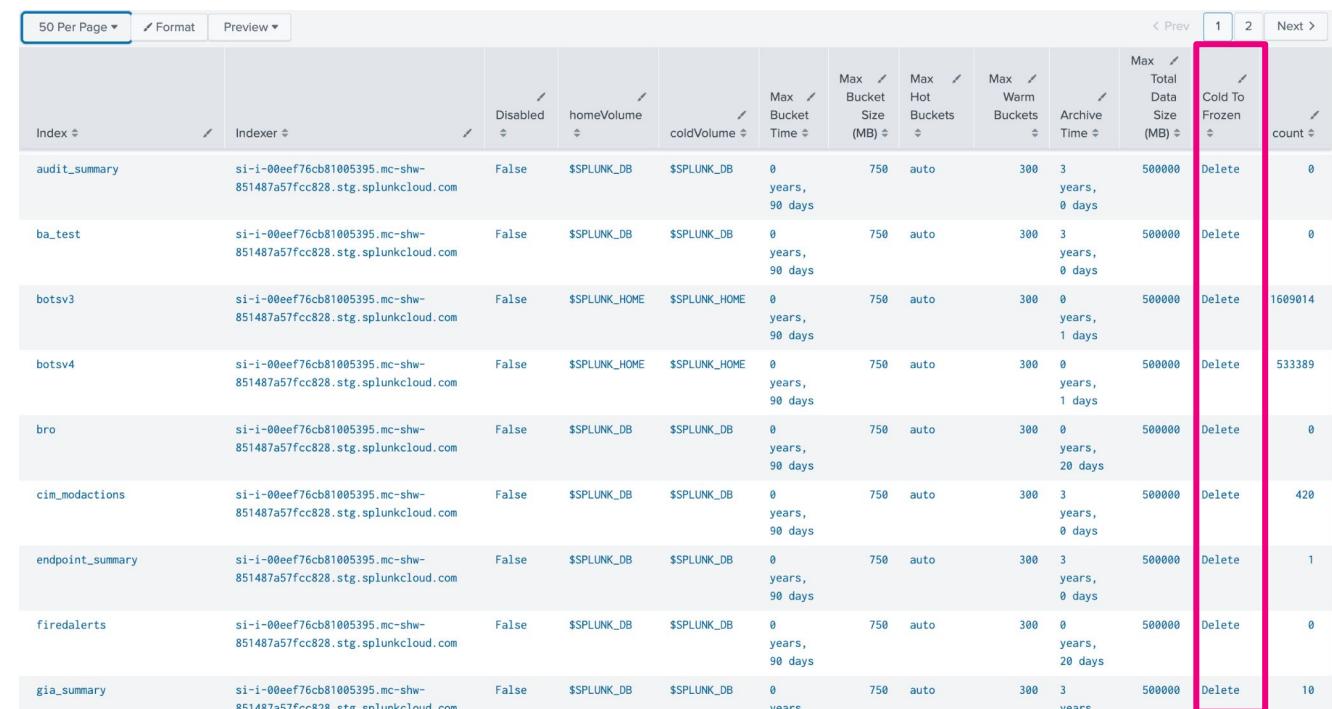
+ Review the **Cold To Frozen** column
– This is what happens when your data expires

Index	Indexer	Disabled	homeVolume	coldVolume	Max Bucket Time	Max Bucket Size (MB)	Max Hot Buckets	Max Warm Buckets	Archive Time	Max Total Data Size (MB)	Cold To Frozen	count
audit_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
ba_test	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
botsv3	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	1609014
botsv4	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	533389
bro	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
cim_modactions	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	420
endpoint_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	1
firedalerts	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
gia_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years.	750	auto	300	3 years.	500000	Delete	10

Data Retention Lab Instructions

Try it yourself!

- + Run the Lab 1 search from  GitHub on your search head
- + Review the **Archive Time** column
 - This is your configured retention period
- + Review the **Max Total Data Size (MB)** column
 - This is the max index size
- + Review the **Cold To Frozen** column
 - This is what happens when your data expires



Index	Indexer	Disabled	homeVolume	coldVolume	Max Bucket Time	Max Bucket Size (MB)	Max Hot Buckets	Max Warm Buckets	Archive Time	Max Total Data Size (MB)	Cold To Frozen	count
audit_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
ba_test	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
botsv3	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	1609014
botsv4	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	533389
bro	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
cim_modactions	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	420
endpoint_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	1
firealerts	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
gia_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years.	750	auto	300	3 years.	500000	Delete	10

Data Retention Lab Instructions

Try it yourself!

Index	Indexer	Disabled	homeVolume	coldVolume	Max Bucket Time	Max Bucket Size (MB)	Max Hot Buckets	Max Warm Buckets	Archive Time	Max Total Data Size (MB)	Cold To Frozen	count
audit_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
ba_test	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
botsv3	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	1609014
botsv4	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	533389
bro	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
cim_modactions	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	420
endpoint_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	1
firedalerts	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
gia_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years.	750	auto	300	3 years.	500000	Delete	10

Data Retention Lab Instructions

Try it yourself!

Index	Indexer	Disabled	homeVolume	coldVolume	Max Bucket Time	Max Bucket Size (MB)	Max Hot Buckets	Max Warm Buckets	Archive Time	Max Total Data Size (MB)	Cold To Frozen count
audit_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete 0
ba_test	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete 0
botsv3	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete 1609014
botsv4	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete 533389
bro	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete 0
cim_modactions	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete 420
endpoint_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete 1
firealerts	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete 0
gia_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years.	750	auto	300	3 years	500000	Delete 10

Data Retention Lab Instructions

Try it yourself!

Index	Indexer	Disabled	homeVolume	coldVolume	Max Bucket Time	Max Bucket Size (MB)	Max Hot Buckets	Max Warm Buckets	Archive Time	Max Total Data Size (MB)	Cold To Frozen	count
audit_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
ba_test	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
botsv3	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	1609014
botsv4	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	533389
bro	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
cim_modactions	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	420
endpoint_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	1
firedalerts	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
gia_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years.	750	auto	300	3 years.	500000	Delete	10

Data Retention Lab Instructions

Try it yourself!

Index	Indexer	Disabled	homeVolume	coldVolume	Max Bucket Time	Max Bucket Size (MB)	Max Hot Buckets	Max Warm Buckets	Archive Time	Max Total Data Size (MB)	Cold To Frozen	count
audit_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
ba_test	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	0
botsv3	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	1609014
botsv4	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_HOME	\$SPLUNK_HOME	0 years, 90 days	750	auto	300	0 years, 1 days	500000	Delete	533389
bro	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
cim_modactions	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	420
endpoint_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	3 years, 0 days	500000	Delete	1
firedalerts	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years, 90 days	750	auto	300	0 years, 20 days	500000	Delete	0
gia_summary	si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	False	\$SPLUNK_DB	\$SPLUNK_DB	0 years.	750	auto	300	3 years.	500000	Delete	10

Data Retention Recap

What we just learned



Data Retention Recap

What we just learned

- + Remember the **500gb default index size**



Data Retention Recap

What we just learned



- + Remember the **500gb default index size**
- + Use the **lab search** to confirm your indexes are not losing data early

Data Retention Recap

What we just learned



- + Remember the **500gb default index size**
- + Use the **lab search** to confirm your indexes are not losing data early
- + Having **frozen storage** can help protect you from data loss due to a misconfiguration

BONUS MATERIAL

But wait, there's more!



BONUS MATERIAL

But wait, there's more!

- + maxVolumeContentSizeMB
 - This does not typically account for DMA



BONUS MATERIAL

But wait, there's more!



+ maxVolumeDataSizeMB

- This does not typically account for DMA

+ maxWarmDBCount

- Can be adjusted if you want data in an index to roll to cold storage sooner

BONUS MATERIAL

But wait, there's more!



+ maxVolumeDataSizeMB

- This does not typically account for DMA

+ maxWarmDBCount

- Can be adjusted if you want data in an index to roll to cold storage sooner

+ maxDataSize

- This is a per bucket setting, not index/disk setting
- `auto_high_volume` - OK for on-prem, not for indexes you intend to migrate to SmartStore

What About Splunk Users?

They exist and you should like them



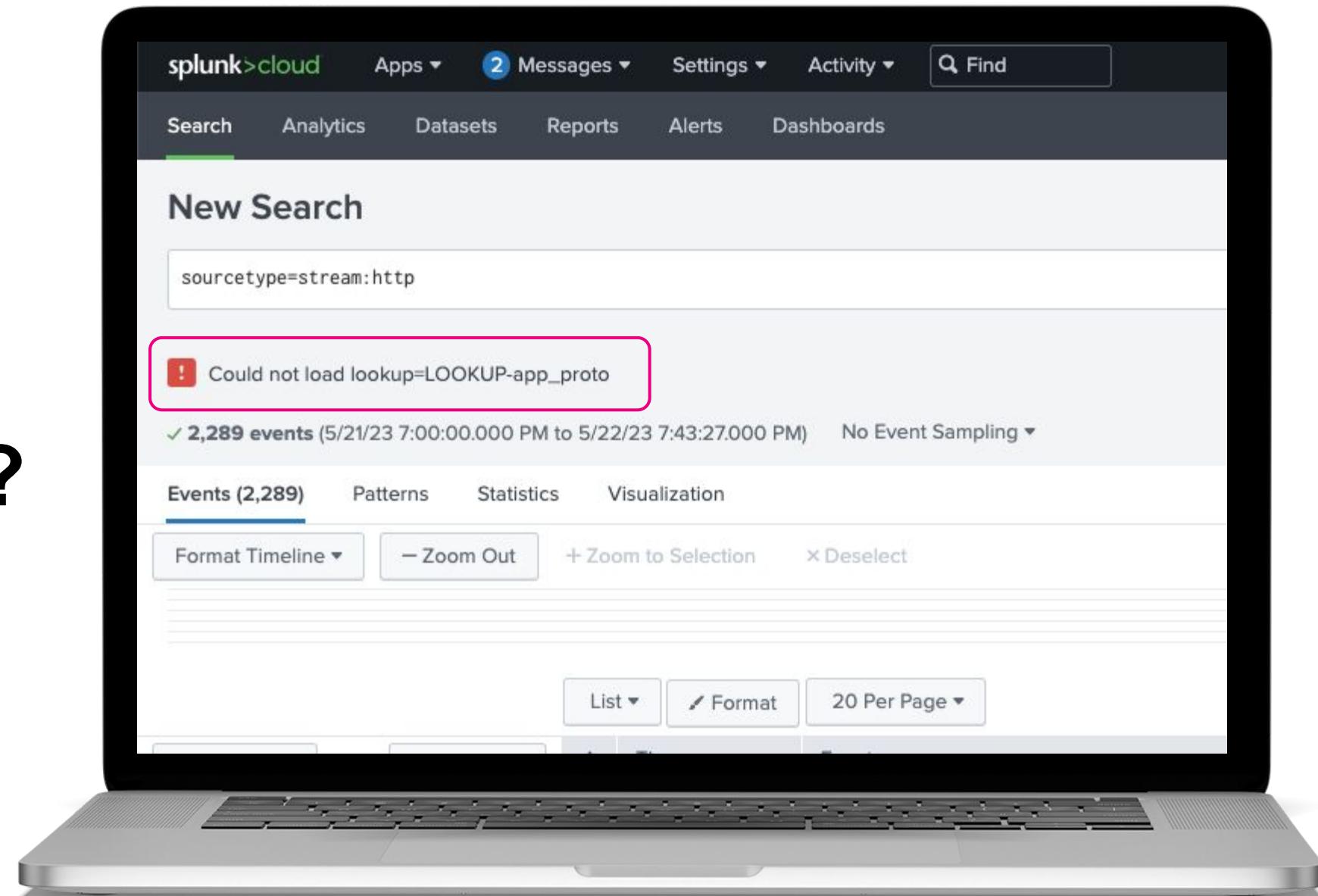


A Tale of Two Splunk Users

It's Best When Everyone Gets the Same Search Results



Have You Seen *This* Error Before?



Sharing Content in Splunk



Sharing Content in Splunk

Knowledge (objects) work best when they're not private to you

Knowledge object permissions matter!

Sharing Content in Splunk

Knowledge (objects) work best when they're not private to you

Knowledge object permissions matter!

+ What happens when permissions are wrong?

- Missing knowledge objects
- Errors in searches, such as a lookup not found

Sharing Content in Splunk

Knowledge (objects) work best when they're not private to you

Knowledge object permissions matter!

+ What happens when permissions are wrong?

- Missing knowledge objects
- Errors in searches, such as a lookup not found

+ App context matters!

- Shared to user: you only (private)
- Shared to app: only searches within that app
- Global/system: every user/search in the environment

Sharing Content in Splunk

Knowledge (objects) work best when they're not private to you

Knowledge object permissions matter!

+ What happens when permissions are wrong?

- Missing knowledge objects
- Errors in searches, such as a lookup not found

+ App context matters!

- Shared to user: you only (private)
- Shared to app: only searches within that app
- Global/system: every user/search in the environment

+ Where is this a problem?

- Knowledge objects shared to an app (only) won't work in the search/reporting app
- Users expect to see the same fields regardless of how they run a search

Sharing Content in Splunk

Knowledge (objects) work best when they're not private to you

Knowledge object permissions matter!

+ What happens when permissions are wrong?

- Missing knowledge objects
- Errors in searches, such as a lookup not found

+ App context matters!

- Shared to user: you only (private)
- Shared to app: only searches within that app
- Global/system: every user/search in the environment

+ Where is this a problem?

- Knowledge objects shared to an app (only) won't work in the search/reporting app
- Users expect to see the same fields regardless of how they run a search

Best Practice:

Develop a process for sharing content with others (once it's tested)

Sharing Content in Splunk

Knowledge (objects) work best when they're not private to you

Sharing Content in Splunk

Knowledge (objects) work best when they're not private to you

Field extractions use resources at search time

Sharing Content in Splunk

Knowledge (objects) work best when they're not private to you

Field extractions use resources at search time

- + Inefficient/too many extractions + millions of events = poor performance
 - You don't want everyone to share everything globally
 - Example: client with 7 different extractions for the same data

Your Turn!



Permissions Lab Instructions

Your turn!

+ Create a second user in your instance

- You can go with “tom” or anything else
- User role is fine

+ Log into Splunk in a different browser/incognito window with your new user

- Confirm you can run a search, such as sourcetype=stream:http

The screenshot shows the Splunk Cloud interface. The top navigation bar includes links for 'splunk>cloud', 'Apps', 'Messages', 'Settings', 'Activity', 'Find', 'Splunk Administrator', 'Support & Services', and a search bar. Below the navigation is a secondary header with 'Search & Reporting' and buttons for 'Save As', 'Create Table View', and 'Close'. The main area is titled 'New Search' and contains a search bar with the query 'sourcetype=stream:http', a time range selector 'Last 24 hours', and a search button. Below the search bar, it displays '6,664 events (5/18/23 8:00:00.000 PM to 5/19/23 8:19:19.000 PM)' and 'No Event Sampling'. A timeline visualization shows green bars representing event data over a 24-hour period. At the bottom, there are buttons for 'Events (6,664)', 'Patterns', 'Statistics', 'Visualization', and 'Format Timeline'. The 'Events' tab is selected. Navigation controls at the bottom include 'List', 'Format', '20 Per Page', 'Prev', a page number selector (1), and 'Next'.

Permissions Lab Instructions

Your turn!

- + From your admin window, find an app/TA associated with the data you are searching, and change the permissions to app only
 - Manage apps -> locate app > sharing -> app

Apply selected role permissions to:

[Learn more](#)

This app only (Splunk Stream Knowledge Objects for Wire Data) All apps (system)

- + Re-run the same search in the Searching & Reporting app
 - Note the change in field extractions

New Search

Save As ▾ Create Table View Close

Last 24 hours ▾



sourcetype=stream:http

✓ 6,664 events (5/18/23 8:00:00.000 PM to 5/19/23 8:19:19.000 PM) No Event Sampling ▾

Job ▾



standard_perf (search default) ▾

Smart Mode ▾



Events (6,664) Patterns Statistics Visualization

Format Timeline ▾

- Zoom Out

+ Zoom to Selection

x Deselect

1 hour per column

List ▾ Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

< Hide Fields

All Fields



Time



Event

SELECTED FIELDS

a host 3
a source 5
a sourcetype 1

INTERESTING FIELDS

a action 2
a app 1
count 81
a dest 7
a dest_ip 7
a dest_is_expected 1
a dest_pcl_domain 1
a dest_requires_av 1
a dest_should_timesync 1
a dest_should_update 1
a endtime 100+
a eventtype 2
a index 2
linecount 1
a protocol 1
a punct 9
a site 13
a splunk_server 1
status 12
sum(bytes_in) 100+
sum(bytes_out) 100+
sum(time_taken) 100+
a tag 3
a tag:eventtype 3
a timestamp 100+

```
> 5/19/23 { [-]
  bytes: 11855
  bytes_in: 965
  bytes_out: 10890
  cookie: mybb[lastvisit]=1534770578; mybb[lastactive]=1534770616; sid=b046d548ebac8b52d127e271020d9eff
  dest_ip: 172.16.0.178
  dest_mac: 02:A0:38:1B:B3:70
  dest_port: 80
  endtime: 2023-05-19T20:19:11.972897Z
  flow_id: d7121bdb-5a96-4b69-a55c-47911ff019a7
  form_data: action=do_login&url=http://www.brewertalk.com/forumdisplay.php?fid=5&quick_login=1&quick_username=fyodor&quick_password=&quick_remember=yes&submit=Login
  http_comment: HTTP/1.1 200 OK
  http_content_type: text/html; charset=UTF-8
  http_method: POST
  http_referrer: http://www.brewertalk.com/forumdisplay.php?fid=5
  http_user_agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.17134
  protocol_stack: ip:tcp:http
  server: Apache/2.2.34 (Amazon)
  site: www.brewertalk.com
  src_ip: 107.77.75.123
  src_mac: 02:4F:D7:61:53:04
  src_port: 16014
  status: 200
  time_taken: 64019
  timestamp: 2023-05-19T20:19:11.909303Z
  transport: tcp
  uri_path: /member.php
}
```

Show as raw text

host = matar | source = stream:http | sourcetype = stream:http

5/19/23

5/19/23

Splunk > cloud Apps ▾ 3 Messages ▾ Settings ▾ Activity ▾ Q Find Splunk Administrator ▾ ? Support & Services ▾

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search

sourcetype=stream:http Last 24 hours ▾

6,783 events (5/18/23 8:00:00.000 PM to 5/19/23 8:24:32.000 PM) No Event Sampling ▾ Job ▾

Events (6,783) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect 1 hour per column

List ▾ Format 20 Per Page ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

SELECTED FIELDS

a host 3
a source 5
a sourcetype 1

INTERESTING FIELDS

count 81
a dest_ip 7
a endtime 100+
a index 2
linecount 1
a punct 9
a site 13
a splunk_server 1
status 12
sum(bytes_in) 100+
sum(bytes_out) 100+
sum(time_taken) 100+
a timestamp 100+
a uri_path 100+
vxlan_id 1

23 more fields + Extract New Fields

Event

> 5/19/23 8:24:26.000 PM { [-]
count: 4
dest_ip: 169.254.169.254
endtime: 2023-05-19T20:24:26.116481Z
site: 169.254.169.254
status: 200
sum(bytes_in): 652
sum(bytes_out): 2140
sum(time_taken): 1359
timestamp: 2023-05-19T20:24:26.116481Z
uri_path: /latest/meta-data/
vxlan_id: 0
}
Show as raw text
host = ip-172-31-82-109.ec2.internal | source = stream:Splunk_HTTPURI | sourcetype = stream:http

> 5/19/23 8:24:26.000 PM { [-]
count: 5
dest_ip: 169.254.169.254
endtime: 2023-05-19T20:24:26.116481Z
site: 169.254.169.254
status: 200
sum(bytes_in): 970
sum(bytes_out): 1280
sum(time_taken): 2061
timestamp: 2023-05-19T20:24:26.116481Z
uri_path: /latest/meta-data/iam/security-credentials/
vxlan_id: 0
}
Show as raw text
host = ip-172-31-82-109.ec2.internal | source = stream:Splunk_HTTPURI | sourcetype = stream:http

> 5/19/23 { [-]

Permissions Lab Instructions

Your turn!

- + Try changing the permissions to Global, but only give administrators read access
 - Manage apps -> locate app > sharing -> app

The screenshot shows the 'App permissions' configuration page. On the left, there's a table titled 'App permissions' showing roles and their Read and Write permissions. The table includes rows for 'Everyone', 'admin', 'apps', 'can_delete', and 'cmon_role'. The 'admin' row has the 'Read' checkbox checked. A red box highlights this row. On the right, under 'Apply selected role permissions to:', there are two options: 'This app only (Splunk Stream Knowledge Objects for Wire Data)' and 'All apps (system)'. The 'All apps (system)' option is selected and highlighted with a red box. There's also a 'Learn more' link.

Roles	Read	Write
Everyone	<input type="checkbox"/>	<input type="checkbox"/>
admin	<input checked="" type="checkbox"/>	<input type="checkbox"/>
apps	<input type="checkbox"/>	<input type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
cmon_role	<input type="checkbox"/>	<input type="checkbox"/>

Apply selected role permissions to:

[Learn more](#)

This app only (Splunk Stream Knowledge Objects for Wire Data)

All apps (system)

- + Re-run the same search in the Searching & Reporting app
 - Note the change in field extractions
- + Re-run the same search as your other user

Permissions Lab Instructions

Your turn!

- + Click the share link in your admin window, and share the search with your limited permissions user
 - What fields do you see?

- + Re-run the same search as the user with limited permissions
 - Note the change in field extractions

Permissions Recap

What we just learned



Permissions Recap

What we just learned



- + Remember that incorrect permissions can result in **different users having different fields available** (and potentially different search results)

Permissions Recap

What we just learned



- + Remember that incorrect permissions can result in **different users having different fields available** (and potentially different search results)
- + Export useful knowledge objects **globally**

Permissions Recap

What we just learned



- + Remember that incorrect permissions can result in **different users having different fields available** (and potentially different search results)
- + Export useful knowledge objects **globally**
- + **Regularly review knowledge objects** for best performance

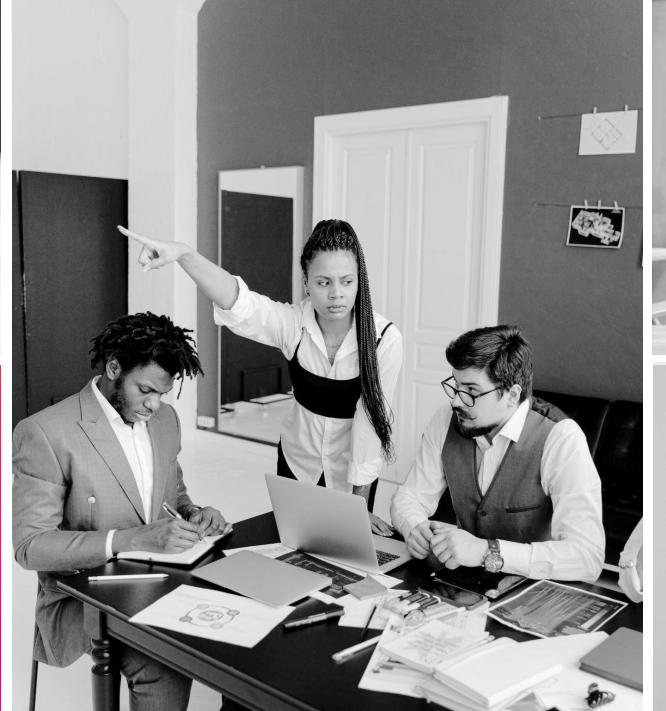
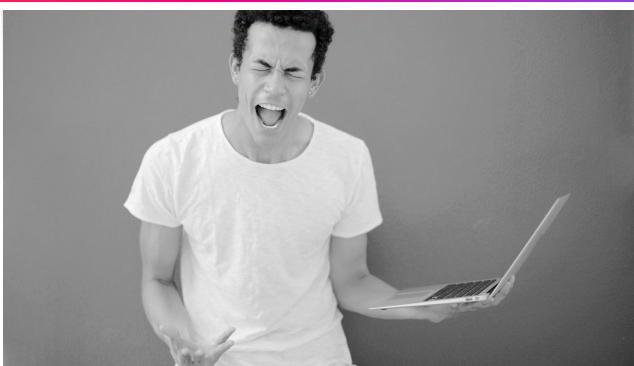
Search Performance

Getting results when you need them





The Boss From Hell



How We Look When Scheduled Searches Are *Working Properly*



How We Look When They *Do Not...*



Scheduler Flexibility



Scheduler Flexibility

Computers get stressed out sometimes too

Scheduler Flexibility

Computers get stressed out sometimes too

- + What happens: humans are predictable when it comes to picking times
 - Everyone will choose to have their scheduled search run at 9am
 - Some of these searches won't work because of limited resources at the same time

Scheduler Flexibility

Computers get stressed out sometimes too

+ What happens: humans are predictable when it comes to picking times

- Everyone will choose to have their scheduled search run at 9am
- Some of these searches won't work because of limited resources at the same time

+ Solution - enable search skewing!

- Best to do this globally for all searches with allow_skew = 5m
- Can also be configured in the GUI on a per-search basis
- Some searches can benefit from a large skew value, such as a daily search with a long runtime (Splunk will schedule the search in a slot where there's less resource contention)
- Settings -> Searches, reports, alerts -> locate search -> Edit -> Advanced Edit

Scheduler Flexibility

Computers get stressed out sometimes too

+ What happens: humans are predictable when it comes to picking times

- Everyone will choose to have their scheduled search run at 9am
- Some of these searches won't work because of limited resources at the same time

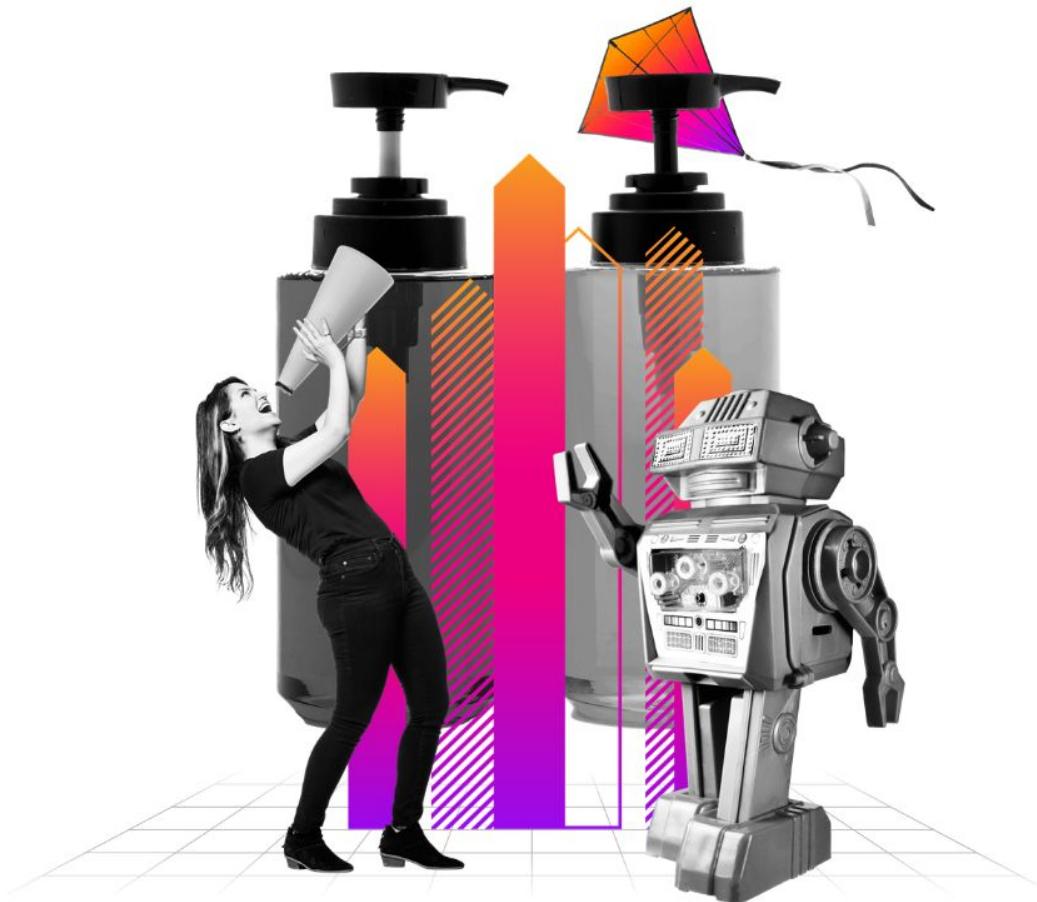
+ Solution - enable search skewing!

- Best to do this globally for all searches with `allow_skew = 5m`
- Can also be configured in the GUI on a per-search basis
- Some searches can benefit from a large skew value, such as a daily search with a long runtime (Splunk will schedule the search in a slot where there's less resource contention)
- Settings -> Searches, reports, alerts -> locate search -> Edit -> Advanced Edit

Best Practice:

Enable a default skew of 5 minutes for all searches. Use larger skew values for searches that are not time-sensitive with a long runtime.

Extended Search Reporting



Extended Search Reporting

Deep-dive into search statistics

- + This is the go-to dashboard for deep-dives into search performance
 - Identifying search issues and optimizations
 - https://github.com/dpaper-splunk/public/blob/master/dashboards/extended_search_reporting.xml

Best Practice:

Keep this dashboard handy for troubleshooting issues with search performance

Your Turn!



Search Performance Lab Instructions

Your turn!

+ Two exercises:

- Skewing search
- Extended Search Reporting

+ ✨ Bonus ✨

- Savedsearch audit

New Search

Save As ▾ Create Table View Close

Last 24 hours ▾



| rest /servicesNS/-/-/saved/searches splunk_server=local | table title, author, allow_skew, is_scheduled, search

✓ 2,136 results (5/18/23 8:00:00.000 PM to 5/19/23 8:40:43.000 PM) No Event Sampling ▾

Job ▾ II ⌂ ⌃ ⌄ standard_perf (search default) ▾ Smart Mode ▾

Events Patterns Statistics (2,136) Visualization

50 Per Page ▾ Format Preview ▾

< Prev 1 2 3 4 5 6 7 8 ... Next >

			author	allow_skew	is_scheduled	search
360 by Account	nobody	5m				1 `infosec-indexes` (tag=security OR tag=attack) bucket span=1h@h _time eval tag=mvfilter(match(tag, "failure") OR match(tag, "success") OR match(tag, "access") OR match(tag, "add") OR match(tag, "change") OR match(tag, "delete") OR match(tag, "error") OR match(tag, "misconfiguration") OR stats count, dc(user) AS dc by tag, _time eval hours=tostring(-floor((now() - _time)/3600))."h" eval hours;if(hours=="0h","now",hours) sort _time fields hours, tag, count, dc
360 by Host	nobody	5m				1 `infosec-indexes` (tag=security OR tag=attack) bucket span=1h@h _time eval tag=mvfilter(match(tag, "failure") OR match(tag, "success") OR match(tag, "access") OR match(tag, "add") OR match(tag, "change") OR match(tag, "delete") OR match(tag, "error") OR match(tag, "misconfiguration") OR stats count, dc(host) AS dc by tag, _time eval hours=tostring(-floor((now() - _time)/3600))."h" eval hours;if(hours=="0h","now",hours) sort _time fields hours, tag, count, dc
Access - Access App Tracker - Lookup Gen	admin	5m				1 tstats summariesonly=true min("_time") as "firstTime",max("_time") as "lastTime" from datamodel="Authentication"."Authentication" where "Authentication.app"!="unknown" by "Authentication.app" rename "Authentication.app" as "lastTime" by "app" outputlookup override_if_empty=false "access_app_tracker" stats count
Access - Access Over Time	admin	5m				0 'tstats' count from datamodel=Authentication.Authentication by _time span=10m timechart minspan=10m count
Access - Access Over Time By Action	admin	5m				0 'tstats' count from datamodel=Authentication.Authentication by _time,Authentication.action span=10m timechart minspan=10m useother='useother' count by Authentication.action 'drop_dm_object_name("Authentication")'
Access - Access Over Time By App	admin	5m				0 'tstats' count from datamodel=Authentication.Authentication by _time,Authentication.app span=10m timechart minspan=10m useother='useother' count by Authentication.app

Extended Search Reporting

Create New Dashboard

Dashboard Title extended_search_reporting

Description

Permissions

How do you want to build your dashboard? What's this?

Classic Dashboards
 The traditional Splunk dashboard builder

Dashboard Studio NEW
 A new builder to create visually-rich, customizable dashboards

```

1 <form version="1.1">
2   <label>Extended Search Reporting, v1.6</label>
3   <!-- Author: David Paper, dpaper@splunk.com -->
4   <fieldset submitButton="false"></fieldset>
5   <row>
6     <panel>
7       <html>
8         The Extended Search Reporting dashboard is here to augment your Splunk management efforts with information and views not o
           indexes are necessary for this view to render properly. Latest version can be found at <a href="https://github.com/dpaper
9       <p/>
10      Feedback is welcome via GitHub or directly to David Paper at dpaper@splunk.com or @cerby on Splunk usergroups Slack.
11
12      </p>
13    </panel>
14  </row>
15  <row>
16    <panel>
17      <html>
18        <h3>Search Efficiency Ratings</h3>
19        <p/>
20        Description: The efficiency panel is a ranking of searches based on how efficient the searches are. The value represents a fu
          efficiency value. Searches that run in less time have higher efficiency values.
21        <p/>
22        Higher efficiency values, relative to each other, are better. Anything below 10 should be considered for improvement in SPL, t
23        <p/>
24        Actions to take: Review how often the search is scheduled to run, and if it is a frequently scheduled search, optimize SPL to

```

Extended Search Reporting

Create New Dashboard

Dashboard Title: Extended Search Reporting

Description: Optional

Permissions: Private

How do you want to build your dashboard? [What's this?](#)

Classic Dashboards: The traditional Splunk dashboard builder

Dashboard Studio: NEW A new builder to create visually-rich, customizable dashboards

[Cancel](#) [Create](#)

```
1 <form version="1.1">
2   <label>Extended Search Reporting, v1.6</label>
3   <!-- Author: David Paper, dpaper@splunk.com -->
4   <fieldset submitButton="false"></fieldset>
5   <row>
6     <panel>
7       <html>
8         The Extended Search Reporting dashboard is here to augment your Splunk management efforts with information and views not o
      indexes are necessary for this view to render properly. Latest version can be found at <a href="https://github.com/dpaper
9
10
11
12
13
14
15
16
17
18   <h3>Search Efficiency Ratings</h3>
19
20   Description: The efficiency panel is a ranking of searches based on how efficient the searches are. The value represents a fu
      efficiency value. Searches that run in less time raise efficiency value.
21
22   Higher efficiency values, relative to each other, are better. Anything below 10 should be considered for improvement in SPL, t
23
24   Actions to take: Review how often the search is scheduled to run, and if it is a frequently scheduled search, optimize SPL to
```

Search Scheduling Distribution

Description: The distribution of scheduled searches is a way to visualize the scheduled search load for each minute of the last hour from the Splunk scheduler perspective. This view only encompasses scheduled and enabled searches on the local server.

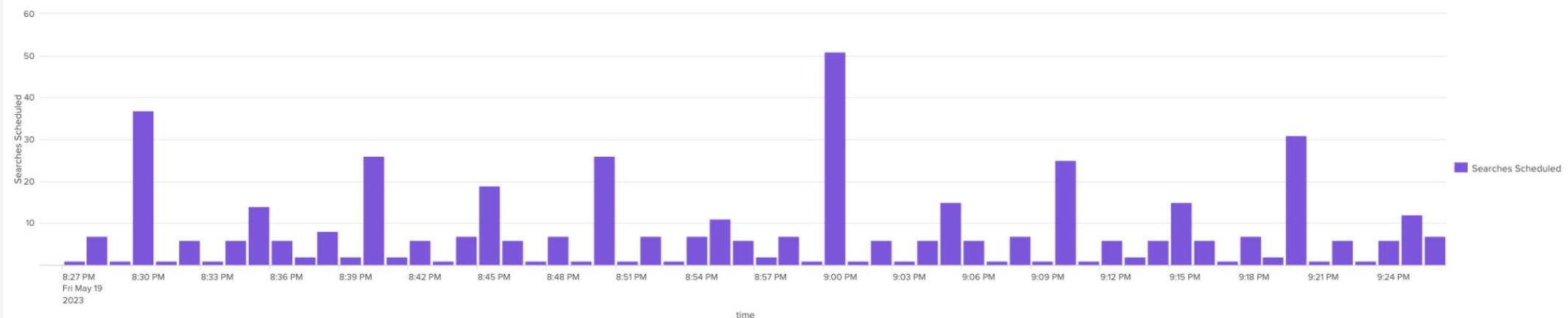
Actions to take: Review how often searches are scheduled to run and which minutes of the clock to run on - do all the searches running frequently need to run at the default 5, 10, 15, et al minute boundaries? Spread searches out to lesser utilized minutes each hour. Assistance can be found on <http://docs.splunk.com/Documentation/Splunk/latest/Alert/CronExpressions>.

Time frame: Trending over the past 60 minutes by default.

Search Scheduling Distribution

Search Scheduling Distribution Select timechart span

Custom time 1 minute
 5 minutes
 60 minutes



Panel Execution Duration

00:00:10.470

Search Scheduling Distribution by App

Bonus: Savedsearch Audit

Find searches behaving badly

Events	Patterns	Statistics (66)	Visualization									
		Format	Preview	< Prev	1	2	Next >					
splunk_server	savedsearch_name	user	average_run_time	max_run_time	min_run_time	cron_schedule	schedule_window	is_realtime	max_mem_used	avg_mem_used	App Name	search
si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	Network - Policy Or Configuration Change - Rule	admin	174.37992213465657	348.58555	1.0113	*5 * * * *	auto	yes	928.65	507.93414155906254	SA-NetworkProtection	from datamodel:"Change"
si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	Audit - Dataset Relation	admin	1.9666307692307694	2.04795	1.89867	*/30 * * * *	auto	no	115.70	112.25032051282054	SA-Utils	rest /servicesNS/nobody
si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	Audit - Anomalous Audit Trail Activity Detected - Rule	admin	0.4819075757575756	0.64027	0.1362	*/54 * * * *	auto	no	565.93	498.94225806451624	SA-AuditAndDataProtection	from datamodel:"Change"
si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	Threat - Correlation Searches - Lookup Gen	admin	0.2220379734848485	0.55832	0.1351	* * * * *	auto	no	213.68	128.04382882882885	SA-ThreatIntelligence	rest splunk_server=local "@@" eval annotations=security_domain;if(security_domain!="") security_domain appendpipe [where _key
si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	Threat - Watchlisted Events - Rule	admin	0.2157729166666667	0.32927	0.1494	*/19 * * * *	auto	no	740.36	353.36138888888889	SA-ThreatIntelligence	tag=watchlist NOT sourcet
si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	Identity - Activity from Expired User Identity - Rule	admin	0.2040361111111114	0.26805	0.1648	*/37 * * * *	auto	no	231.40	184.14263157894734	SA-IdentityManagement	from datamodel:"Identit
si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	Threats - Disable Suppressions - Administrative	admin	0.1271833333333334	0.19953	0.03472	0 3 * * *	auto	no	116.25	109.54666666666667	SA-ThreatIntelligence	rest splunk_server=local "@@" eval annotations=security_domain;if(security_domain!="") security_domain appendpipe [where _key
si-i-00eef76cb81005395.mc-shw-851487a57fcc828.stg.splunkcloud.com	Network - Traffic Source Count Per 30m - Model Gen	admin	0.1238111111111112	0.1427	0.1094	35 * * * *	5	no	117.48	117.08166666666666	SA-NetworkProtection	tstats `summariesonly`

Search Performance Recap

What we just learned



Search Performance Recap

What we just learned

- + **Search skewing** can have a massive impact on success of searches



Search Performance Recap

What we just learned



- + **Search skewing** can have a massive impact on success of searches
- + Set a global skew of **5 minutes** for all searches (more for others if appropriate)

Search Performance Recap

What we just learned



- + **Search skewing** can have a massive impact on success of searches
- + Set a global skew of **5 minutes** for all searches (more for others if appropriate)
- + Leverage the **extended search** reporting dashboard for a deep dive into performance concerns and search metrics

Reliable SOC Alerting

Ensuring that your Enterprise Security correlation searches work properly





Stories from the soc





Auditing Data Model Acceleration (DMA)

Auditing Data Model Acceleration (DMA)

A critical step for proper correlation search behavior

Auditing Data Model Acceleration (DMA)

A critical step for proper correlation search behavior

Data model searches can take a ton of time to run

Auditing Data Model Acceleration (DMA)

A critical step for proper correlation search behavior

Data model searches can take a ton of time to run

- + By default, all indexes are included
 - May result in searches taking significantly longer to run
 - Increased search time = longer data model build times = increased likelihood of missed alerts

Auditing Data Model Acceleration (DMA)

A critical step for proper correlation search behavior

Data model searches can take a ton of time to run

- + By default, all indexes are included
 - May result in searches taking significantly longer to run
 - Increased search time = longer data model build times = increased likelihood of missed alerts

Audit your data models!

Auditing Data Model Acceleration (DMA)

A critical step for proper correlation search behavior

Data model searches can take a ton of time to run

- + By default, all indexes are included
 - May result in searches taking significantly longer to run
 - Increased search time = longer data model build times = increased likelihood of missed alerts

Audit your data models!

- + Only enable acceleration for indexes that contain relevant data
- + Ensure data is Common Information Model (CIM) compliant before enabling acceleration or the data models won't work properly

Auditing Data Model Acceleration (DMA)

A critical step for proper correlation search behavior

Data model searches can take a ton of time to run

- + By default, all indexes are included
 - May result in searches taking significantly longer to run
 - Increased search time = longer data model build times = increased likelihood of missed alerts

Audit your data models!

- + Only enable acceleration for indexes that contain relevant data
- + Ensure data is Common Information Model (CIM) compliant before enabling acceleration or the data models won't work properly

Best Practice:

Have a process for adding new data which includes updating relevant data models

Your Turn!



Data Model Audit Dashboard

Your turn!

datamodel	acceleration_enabled	acceleration_earliest	macro	definition	complete(%)	size(MB)	correlation_searches_enabled	access_time
Certificates	true	-1y			100.0	0.0		01/01/1970 00:00:00
Email	true	-1y			100.0	0.0		1 05/19/2023 21:30:11
Incident_Management	true	0			100.0	0.0		01/01/1970 00:00:00
Malware	true	-1y			100.0	0.0		6 05/19/2023 21:20:57
Network_Resolution	true	-3mon			100.0	0.0		01/01/1970 00:00:00
Network_Sessions	true	-3mon			100.0	0.0		01/01/1970 00:00:00
UEBA	true	0			100.0	0.0		3 01/01/1970 00:00:00
Vulnerabilities	true	-1y			100.0	0.0		05/19/2023 21:20:47
Authentication	true	-1y			100.0	0.1		9 05/19/2023 21:30:07
Intrusion_Detection	true	-1y			100.0	0.2		05/19/2023 21:31:04

Data Model Audit Dashboard

Your turn!



datamodel	acceleration_enabled	acceleration_earliest	macro	definition	complete(%)	size(MB)	correlation_searches_enabled	access_time
Certificates	true	-1y			100.0	0.0		01/01/1970 00:00:00
Email	true	-1y			100.0	0.0	1	05/19/2023 21:30:11
Incident_Management	true	0			100.0	0.0		01/01/1970 00:00:00
Malware	true	-1y			100.0	0.0	6	05/19/2023 21:20:57
Network_Resolution	true	-3mon			100.0	0.0		01/01/1970 00:00:00
Network_Sessions	true	-3mon			100.0	0.0		01/01/1970 00:00:00
UEBA	true	0			100.0	0.0	3	01/01/1970 00:00:00
Vulnerabilities	true	-1y			100.0	0.0		05/19/2023 21:20:47
Authentication	true	-1y			100.0	0.1	9	05/19/2023 21:30:07
Intrusion_Detection	true	-1y			100.0	0.2		05/19/2023 21:31:04

Data Model Audit Dashboard

Your turn!



datamodel	acceleration_enabled	acceleration_earliest	macro	definition	complete(%)	size(MB)	correlation_searches_enabled	access_time
Certificates	true	-1y			100.0	0.0		01/01/1970 00:00:00
Email	true	-1y			100.0	0.0	1	05/19/2023 21:30:11
Incident_Management	true	0			100.0	0.0		01/01/1970 00:00:00
Malware	true	-1y			100.0	0.0	6	05/19/2023 21:20:57
Network_Resolution	true	-3mon			100.0	0.0		01/01/1970 00:00:00
Network_Sessions	true	-3mon			100.0	0.0		01/01/1970 00:00:00
UEBA	true	0			100.0	0.0	3	01/01/1970 00:00:00
Vulnerabilities	true	-1y			100.0	0.0		05/19/2023 21:20:47
Authentication	true	-1y			100.0	0.1	9	05/19/2023 21:30:07
Intrusion_Detection	true	-1y			100.0	0.2		05/19/2023 21:31:04

Data Model Audit Dashboard

Your turn!



datamodel	acceleration_enabled	acceleration_earliest	macro	definition	complete(%)	size(MB)	correlation_searches_enabled	access_time
Certificates	true	-1y			100.0	0.0		01/01/1970 00:00:00
Email	true	-1y			100.0	0.0	1	05/19/2023 21:30:11
Incident_Management	true	0			100.0	0.0		01/01/1970 00:00:00
Malware	true	-1y			100.0	0.0	6	05/19/2023 21:20:57
Network_Resolution	true	-3mon			100.0	0.0		01/01/1970 00:00:00
Network_Sessions	true	-3mon			100.0	0.0		01/01/1970 00:00:00
UEBA	true	0			100.0	0.0	3	01/01/1970 00:00:00
Vulnerabilities	true	-1y			100.0	0.0		05/19/2023 21:20:47
Authentication	true	-1y			100.0	0.1	9	05/19/2023 21:30:07
Intrusion_Detection	true	-1y			100.0	0.2		05/19/2023 21:31:04

Data Model Audit Dashboard

Your turn!



datamodel	acceleration_enabled	acceleration_earliest	macro	definition	complete(%)	size(MB)	correlation_searches_enabled	access_time
Certificates	true	-1y			100.0	0.0		01/01/1970 00:00:00
Email	true	-1y			100.0	0.0	1	05/19/2023 21:30:11
Incident_Management	true	0			100.0	0.0		01/01/1970 00:00:00
Malware	true	-1y			100.0	0.0	6	05/19/2023 21:20:57
Network_Resolution	true	-3mon			100.0	0.0		01/01/1970 00:00:00
Network_Sessions	true	-3mon			100.0	0.0		01/01/1970 00:00:00
UEBA	true	0			100.0	0.0	3	01/01/1970 00:00:00
Vulnerabilities	true	-1y			100.0	0.0		05/19/2023 21:20:47
Authentication	true	-1y			100.0	0.1	9	05/19/2023 21:30:07
Intrusion_Detection	true	-1y			100.0	0.2		05/19/2023 21:31:04

Data Model Acceleration Audit Recap

What we just learned



Data Model Acceleration Audit Recap

What we just learned

- + Ensure data model acceleration searches are set to **only use indexes with data**



Data Model Acceleration Audit Recap

What we just learned



- + Ensure data model acceleration searches are set to **only use indexes with data**
- + Data needs to be **CIM compliant** to be used in correlation searches in Splunk Enterprise Security (ES)

Data Model Acceleration Audit Recap

What we just learned

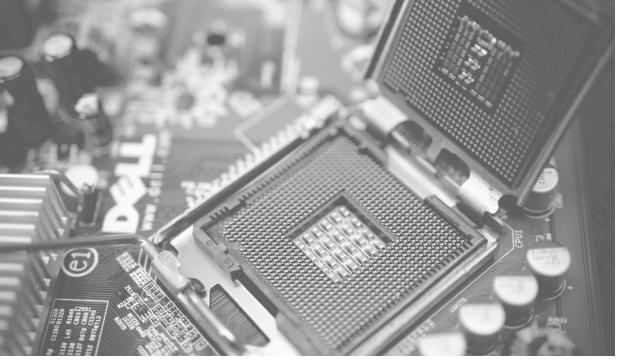


- + Ensure data model acceleration searches are set to **only use indexes with data**
- + Data needs to be **CIM compliant** to be used in correlation searches in Splunk Enterprise Security (ES)
- + Make sure you add **new indexes** to the data models as part of your data onboarding process

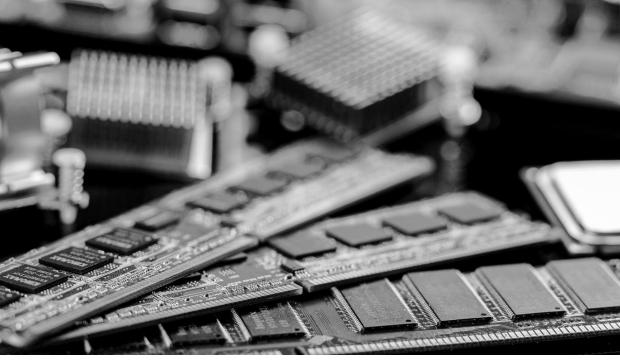
Don't Waste Resources

Finding and fixing unneeded acceleration





Using Resources Responsibly



Auditing Acceleration Summaries



Auditing Acceleration Summaries

A quick and easy way to reduce resource consumption

Auditing Acceleration Summaries

A quick and easy way to reduce resource consumption

Identify report accelerations that are not used

Auditing Acceleration Summaries

A quick and easy way to reduce resource consumption

Identify report accelerations that are not used

- + Some apps will enable these by default

Auditing Acceleration Summaries

A quick and easy way to reduce resource consumption

Identify report accelerations that are not used

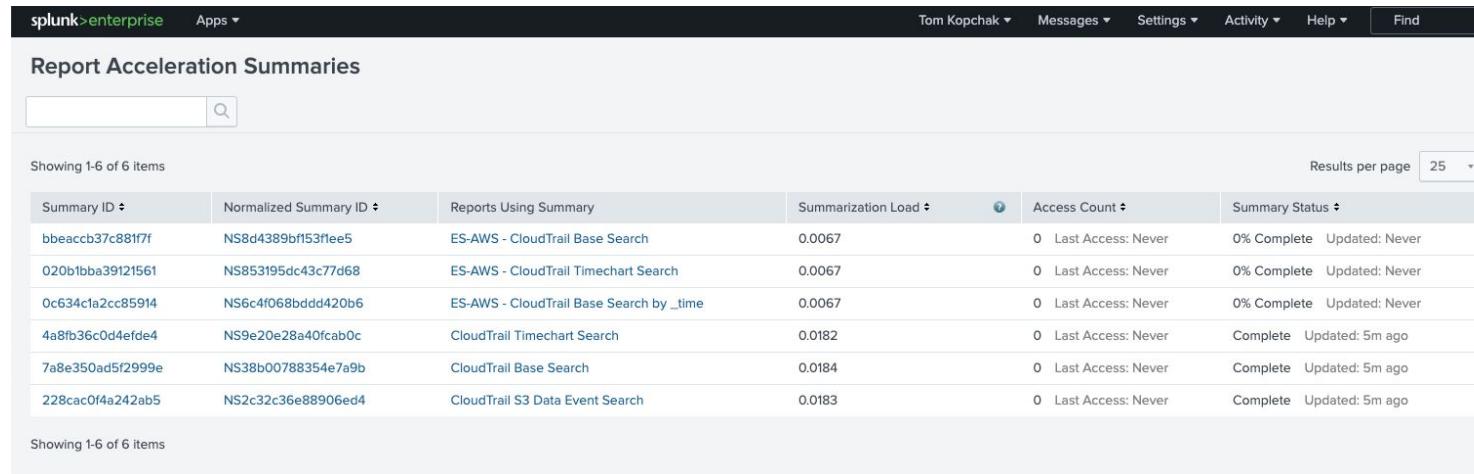
- + Some apps will enable these by default
- + Disabling these will reduce resource usage

Auditing Acceleration Summaries

A quick and easy way to reduce resource consumption

Identify report accelerations that are not used

- + Some apps will enable these by default
- + Disabling these will reduce resource usage



The screenshot shows the Splunk enterprise interface with the title "Report Acceleration Summaries". The page displays a table of 6 items, each representing a summary configuration. The columns include Summary ID, Normalized Summary ID, Reports Using Summary, Summarization Load, Access Count, and Summary Status. All summaries listed have a summarization load of 0.0067, access count of 0, and summary status of 0% Complete, Updated: Never.

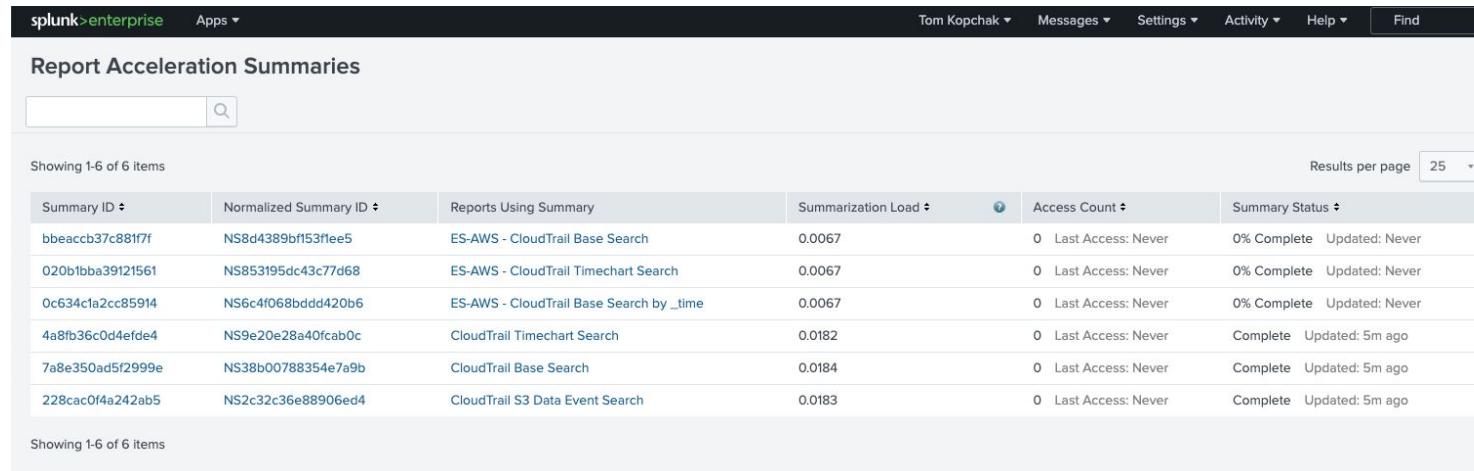
Summary ID	Normalized Summary ID	Reports Using Summary	Summarization Load	Access Count	Summary Status
bbeaccb37c881f7f	NS8d4389bf153flee5	ES-AWS - CloudTrail Base Search	0.0067	0	Last Access: Never 0% Complete Updated: Never
020b1bba39121561	NS853195dc43c77d68	ES-AWS - CloudTrail Timechart Search	0.0067	0	Last Access: Never 0% Complete Updated: Never
0c634c1a2cc85914	NS6c4f068bdd420b6	ES-AWS - CloudTrail Base Search by _time	0.0067	0	Last Access: Never 0% Complete Updated: Never
4a8fb36c0d4efde4	NS9e20e28a40fcab0c	CloudTrail Timechart Search	0.0182	0	Last Access: Never Complete Updated: 5m ago
7a8e350ad5f2999e	NS38b00788354e7a9b	CloudTrail Base Search	0.0184	0	Last Access: Never Complete Updated: 5m ago
228cac0f4a242ab5	NS2c32c36e88906ed4	CloudTrail S3 Data Event Search	0.0183	0	Last Access: Never Complete Updated: 5m ago

Auditing Acceleration Summaries

A quick and easy way to reduce resource consumption

Identify report accelerations that are not used

- + Some apps will enable these by default
- + Disabling these will reduce resource usage



The screenshot shows the Splunk interface with the title "Report Acceleration Summaries". The page displays a table of 6 items, each representing a report acceleration summary. The columns include Summary ID, Normalized Summary ID, Reports Using Summary, Summarization Load, Access Count, and Summary Status. The data is as follows:

Summary ID	Normalized Summary ID	Reports Using Summary	Summarization Load	Access Count	Summary Status
bbeaccb37c881f7f	NS8d4389bf153flee5	ES-AWS - CloudTrail Base Search	0.0067	0	Last Access: Never 0% Complete Updated: Never
020b1bbba39121561	NS853195dc43c77d68	ES-AWS - CloudTrail Timechart Search	0.0067	0	Last Access: Never 0% Complete Updated: Never
0c634c1a2cc85914	NS6c4f068bdd420b6	ES-AWS - CloudTrail Base Search by _time	0.0067	0	Last Access: Never 0% Complete Updated: Never
4a8fb36c0d4efde4	NS9e20e28a40fcab0c	CloudTrail Timechart Search	0.0182	0	Last Access: Never Complete Updated: 5m ago
7a8e350ad5f2999e	NS38b00788354e7a9b	CloudTrail Base Search	0.0184	0	Last Access: Never Complete Updated: 5m ago
228cac0f4a242ab5	NS2c32c36e88906ed4	CloudTrail S3 Data Event Search	0.0183	0	Last Access: Never Complete Updated: 5m ago

Best Practice:

Disable report acceleration summaries that are unused/not accessed



Identifying Unused Apps

splunk> .conf23

Identifying Unused Apps

Check for user activity

Identifying Unused Apps

Check for user activity

Identify apps that are potentially good candidates for removal

Identifying Unused Apps

Check for user activity

Identify apps that are potentially good candidates for removal

- + This should only be used on apps with UI elements
- + Removing unused/unconfigured apps can save resources on your search head

Identifying Unused Apps

Check for user activity

Identify apps that are potentially good candidates for removal

- + This should only be used on apps with UI elements
- + Removing unused/unconfigured apps can save resources on your search head

Premium apps on dedicated search heads

Identifying Unused Apps

Check for user activity

Identify apps that are potentially good candidates for removal

- + This should only be used on apps with UI elements
- + Removing unused/unconfigured apps can save resources on your search head

Premium apps on dedicated search heads

- + Splunk Enterprise Security (ES) & IT Service Intelligence (ITSI) should be on dedicated search heads
- + Other apps should be on the ad-hoc search head

Identifying Unused Apps

Check for user activity

Identify apps that are potentially good candidates for removal

- + This should only be used on apps with UI elements
- + Removing unused/unconfigured apps can save resources on your search head

Premium apps on dedicated search heads

- + Splunk Enterprise Security (ES) & IT Service Intelligence (ITSI) should be on dedicated search heads
- + Other apps should be on the ad-hoc search head

Best Practice:

Remove apps associated with products you are no longer using in your environment (once the data has rolled off)

Your Turn!



Auditing Acceleration Summaries

This is a quick and easy one!

Auditing Acceleration Summaries

This is a quick and easy one!

- + On your search head, navigate to manager/system/summarization
 - For example: <https://splunksearch.yourdomain.com/en-US/manager/system/summarization>

Auditing Acceleration Summaries

This is a quick and easy one!

- + On your search head, navigate to manager/system/summarization
 - For example: <https://splunksearch.yourdomain.com/en-US/manager/system/summarization>
- + Review the list of acceleration summaries
 - Summaries with an access count of 0 are good candidates for disabling

Auditing Acceleration Summaries

This is a quick and easy one!

- + On your search head, navigate to manager/system/summarization
 - For example: <https://splunksearch.yourdomain.com/en-US/manager/system/summarization>
- + Review the list of acceleration summaries
 - Summaries with an access count of 0 are good candidates for disabling

Best Practice:

Remove apps associated with products you are no longer using in your environment (once the data has rolled off)

Auditing Acceleration Summaries

The image shows a laptop screen displaying the Splunk Cloud interface. The title bar reads "splunk>cloud". The main content is a table titled "Report Acceleration Summaries" showing 8 items. The columns are: Summary ID, Normalized Summary ID, Reports Using Summary, Summarization Load, Access Count, and Summary Status. The data is as follows:

Summary ID	Normalized Summary ID	Reports Using Summary	Summarization Load	Access Count	Summary Status
d52c556c4bf06a37	NSf91a6616cde1858c	ES-AWS - CloudTrail Base Search by _time	0.0045	0	Last Access: Never 0% Complete Updated: Never
c07bfd5d5f179d6c	NS7823abb6569c7fb7	ES-AWS - CloudTrail Timechart Search	0.0044	0	Last Access: Never 0% Complete Updated: Never
1c30edf62e134275	NS566d5e105b348678	ES-AWS - CloudTrail Base Search	0.0044	0	Last Access: Never 0% Complete Updated: Never
0fb0b0f7d8ed83b0	NSa44393704f79ed7e	AWS Security CloudTrail Base Search	0.0042	0	Last Access: Never 0% Complete Updated: Never
80b5f7b4e0fb0633	NS90dte5a9153cd83d	AWS Security CloudTrail Timechart Search	0.0043	0	Last Access: Never 0% Complete Updated: Never
5d508af4df53bafe	NS7c7c796e2fa8e573	AWS Security CloudTrail S3 Data Event Search	0.0048	0	Last Access: Never 0% Complete Updated: Never
c509e9dbdbb6f256	NSd3c8734ff059a3be	360 by Host	0.0165	6	Last Access: 5m ago Complete Updated: 6m ago
7282ee5dd9cce0b3	NS9035acbbb2d5e42d	360 by Account	0.0194	6	Last Access: 21m ago Complete Updated: 6m ago

Checking for Unused Apps

This one requires a bit more input

On your search head, identify some apps names you think may not be used

- + Choose a product you've removed from your environment
- + Run the unused_apps search with the app name specified



The screenshot shows the Splunk search interface. The top navigation bar includes tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Search' tab is currently selected. Below the navigation bar, the title 'New Search' is displayed. The search bar contains the following SPL command:

```
index=_internal sourcetype=splunkd_ui_access appLogo.png earliest=-30d@d latest=now  
| rex field=uri "/en-US/splunkd/_raw/servicesNS/[^/]+/(?<app>[^/]+)/static/appLogo.png"  
| search app=<candidate_app_for_removal>  
| stats values values(user) as users by app
```

The search command is highlighted with a red rectangular box around the first three lines. The variable placeholder <candidate_app_for_removal> is also highlighted with a red box.

Auditing Acceleration Summaries Recap

What we just learned



Auditing Acceleration Summaries Recap

What we just learned

- + Accelerating reports that no one is using **wastes resources**



Auditing Acceleration Summaries Recap

What we just learned



- + Accelerating reports that no one is using **wastes resources**
- + Disabling acceleration reports that aren't accessed can **save resources**

Auditing Acceleration Summaries Recap

What we just learned



- + Accelerating reports that no one is using **wastes resources**
- + Disabling acceleration reports that aren't accessed can **save resources**
- + Use the **summarization settings** page to identify potential searches

Auditing Acceleration Summaries Recap

What we just learned



- + Accelerating reports that no one is using **wastes resources**
- + Disabling acceleration reports that aren't accessed can **save resources**
- + Use the **summarization settings** page to identify potential searches
- + Consider **removing unused apps** to reduce overhead

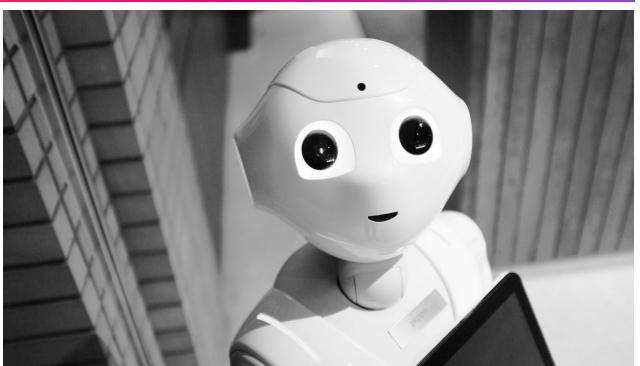
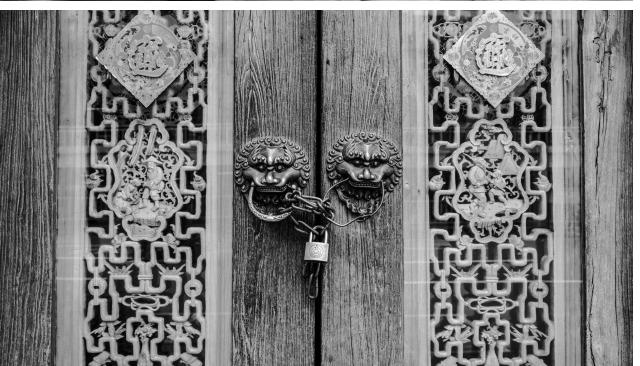
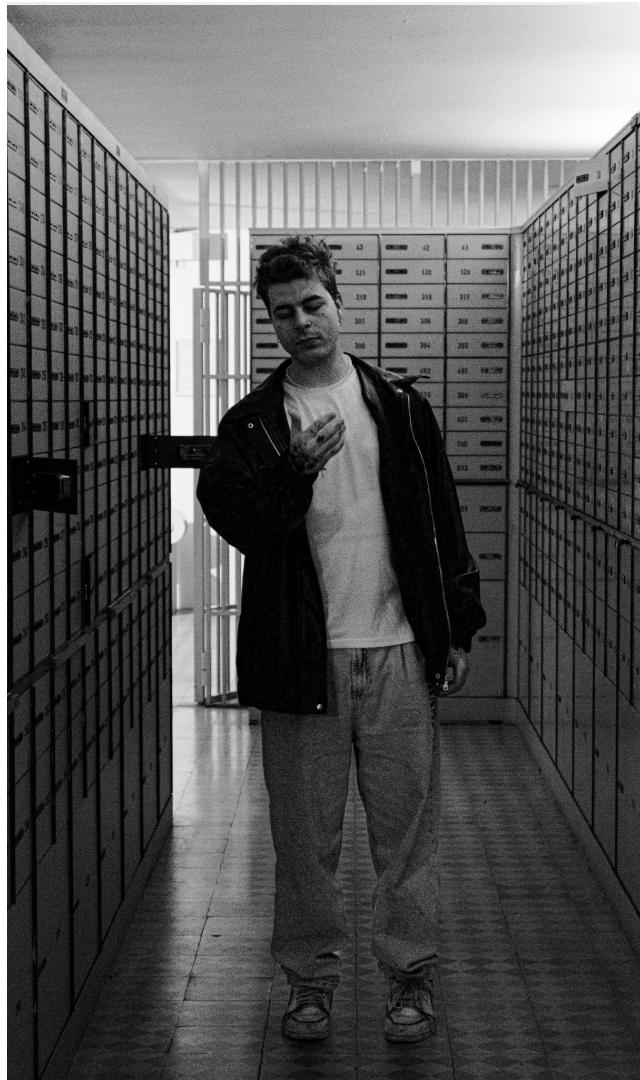
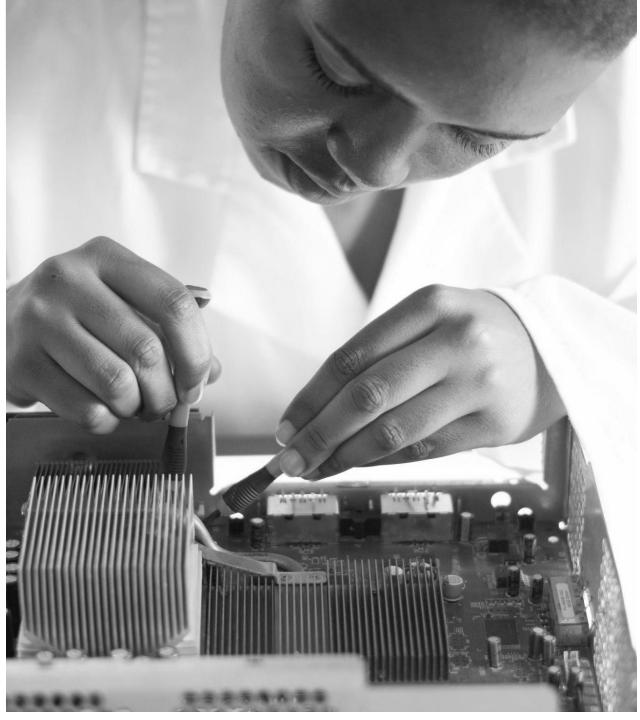
Recovering Credentials

Accessing Splunk's Password Store





API Secret Management Story



Managing & Recovering API Keys



Managing/Recovering API Keys

Using Splunk to recover credentials

Managing/Recovering API Keys

Using Splunk to recover credentials

- + You may need to recover API keys for an input
 - Splunk needs to be able to decode these keys to use them
 - You can use the same mechanism to show the decoded passwords

Managing/Recovering API Keys

Using Splunk to recover credentials

+ You may need to recover API keys for an input

- Splunk needs to be able to decode these keys to use them

- You can use the same mechanism to show the decoded passwords

+ Syntax - REST search

- | rest splunk_server=local "/servicesNS/-/SA-ldapsearch/storage/passwords"
| table username,clear_password,title

- Replace SA-ldapsearch with the appropriate app

Managing/Recovering API Keys

Using Splunk to recover credentials

+ You may need to recover API keys for an input

- Splunk needs to be able to decode these keys to use them

- You can use the same mechanism to show the decoded passwords

+ Syntax - REST search

- | rest splunk_server=local "/servicesNS/-/SA-ldapsearch/storage/passwords"
| table username,clear_password,title
- Replace SA-ldapsearch with the appropriate app

Best Practice:

Run this search on the system (heavy forwarder, etc.) where the input is configured

Your Turn!



Recovering API Keys/Credentials

This is a quick and easy one!

- + Head to the search app on a system where you have an app with stored credentials
 - For example: a heavy forwarder running the O365 app
- + Syntax - REST search
 - | rest splunk_server=local "/servicesNS/-/<app name>/storage/passwords"
| table username,clear_password,title
 - Specify the appropriate app in your search
 - The results table will show credentials

Troubleshooting: this is only available to admins with appropriate permissions

Recovering API Keys/Credentials

This is a quick and easy one!

The screenshot shows the Splunk Cloud search interface with the following details:

- Search Bar:** Contains the search command: `| rest splunk_server=local "/servicesNS/-/search/storage/passwords"
| table username,clear_password,title`.
- Results Panel:** Shows 10 results from the search, spanning from 5/18/23 10:00:00.000 PM to 5/19/23 10:06:04.000 PM. The results are listed in a table with columns: `username`, `clear_password`, and `title`. The results are heavily redacted with pink boxes.
- Statistics Tab:** The `Statistics (10)` tab is selected, showing 10 results.
- Visualizations:** Buttons for `Events`, `Patterns`, `Visualization`, `50 Per Page`, `Format`, and `Preview`.
- Toolbar:** Includes buttons for `Save As`, `Create Table View`, `Close`, `Last 24 hours`, and a search icon.
- Header:** Shows the user is a `Splunk Administrator` and includes links for `Support & Services`, `Search & Reporting`, and navigation links for `Search`, `Analytics`, `Datasets`, `Reports`, `Alerts`, and `Dashboards`.

Recovering API Keys & Credentials Recap

What we just learned



Recovering API Keys & Credentials Recap

What we just learned

- + Sometimes you may need to **recover credentials** as a Splunk admin



Recovering API Keys & Credentials Recap

What we just learned



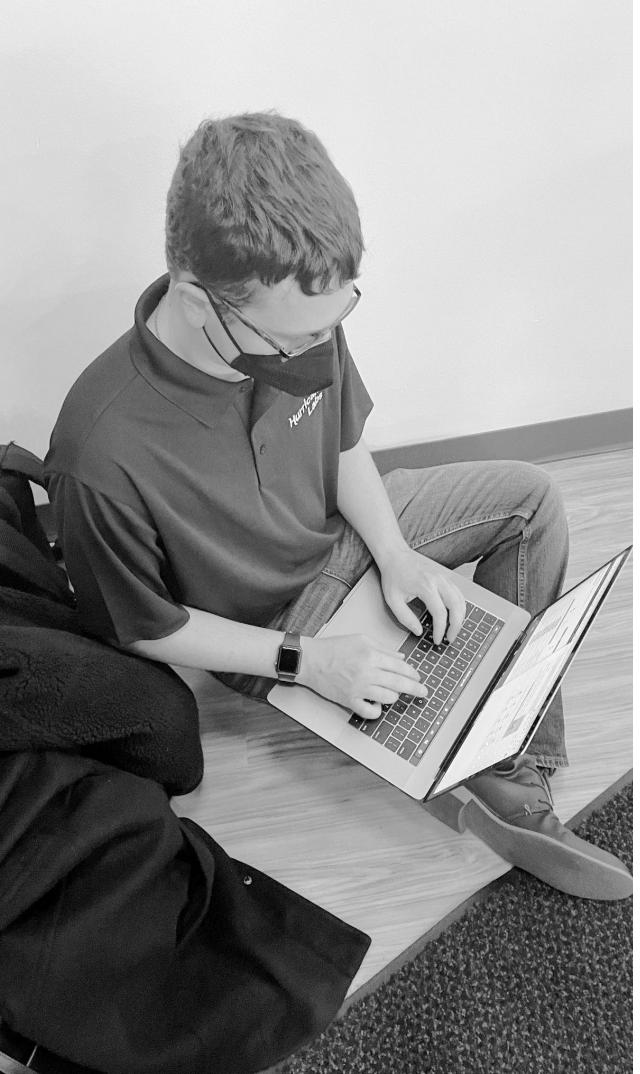
- + Sometimes you may need to **recover credentials** as a Splunk admin
- + Using the **Splunk interface** to do so is one of the simplest ways to get this information

Recovering API Keys & Credentials Recap

What we just learned



- + Sometimes you may need to **recover credentials** as a Splunk admin
- + Using the **Splunk interface** to do so is one of the simplest ways to get this information
- + It's helpful when doing **migrations** between systems (or to Splunk Cloud!)



Recap of Today's Goals

What we covered



Recap of Today's Goals

What we covered

- + Keep your **auditors** happy
Data retention audit



Recap of Today's Goals

What we covered

- + Keep your **auditors** happy
Data retention audit
- + Keep your **users** happy
Knowledge object permissions



Recap of Today's Goals

What we covered



- + Keep your **auditors** happy
Data retention audit
- + Keep your **users** happy
Knowledge object permissions
- + Keep your **Splunk instance** happy
Scheduler health and skewing

Recap of Today's Goals

What we covered



- + Keep your **auditors** happy
Data retention audit
- + Keep your **users** happy
Knowledge object permissions
- + Keep your **Splunk instance** happy
Scheduler health and skewing
- + Keep your **SOC team** happy
Datamodel and report acceleration audits

Recap of Today's Goals

What we covered



- + Keep your **auditors** happy
Data retention audit
- + Keep your **users** happy
Knowledge object permissions
- + Keep your **Splunk instance** happy
Scheduler health and skewing
- + Keep your **SOC team** happy
Datamodel and report acceleration audits
- + Keep **YOU** happy!
Recovering credentials

Let's Keep This Going!

How we can continue learning

Submit your own helpful searches/tips for Splunk administration, and I'll publish the best ones for everyone to share!

splunk> .conf23





Have More Questions?

Talk to me at the Hurricane Labs booth!

M122

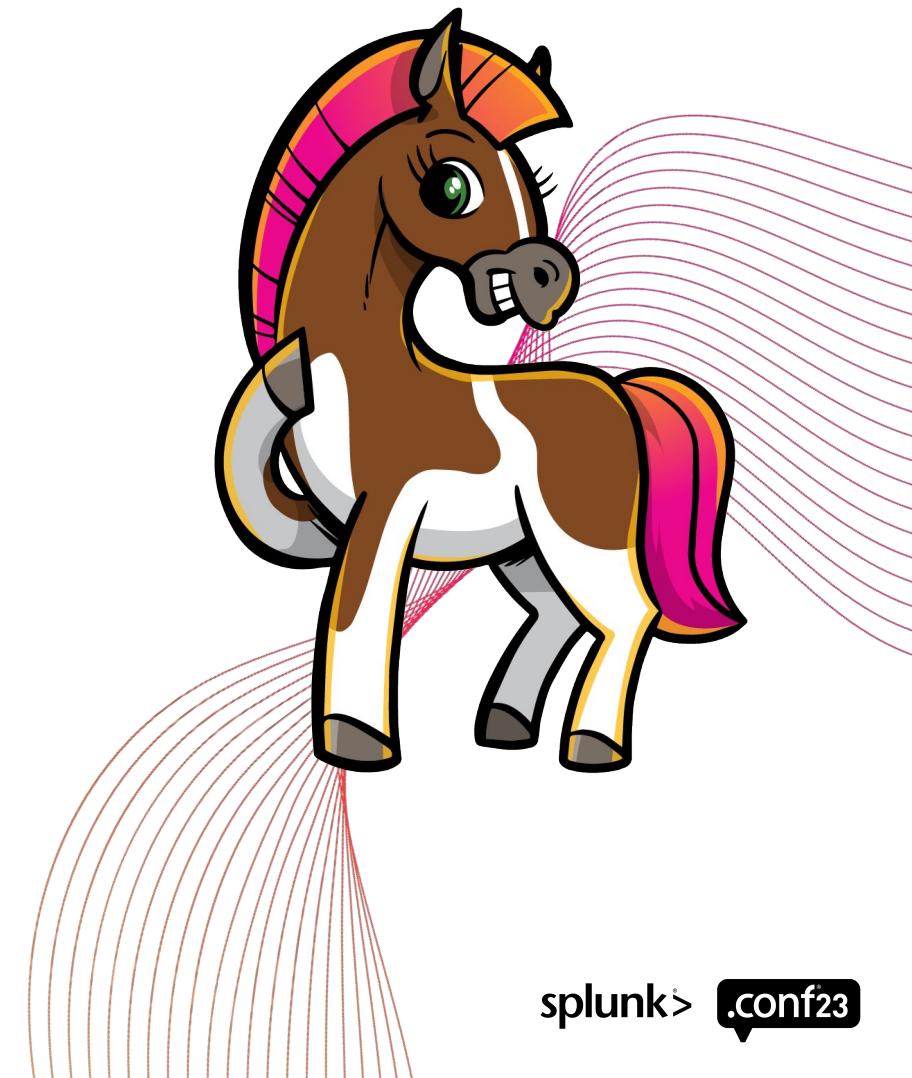
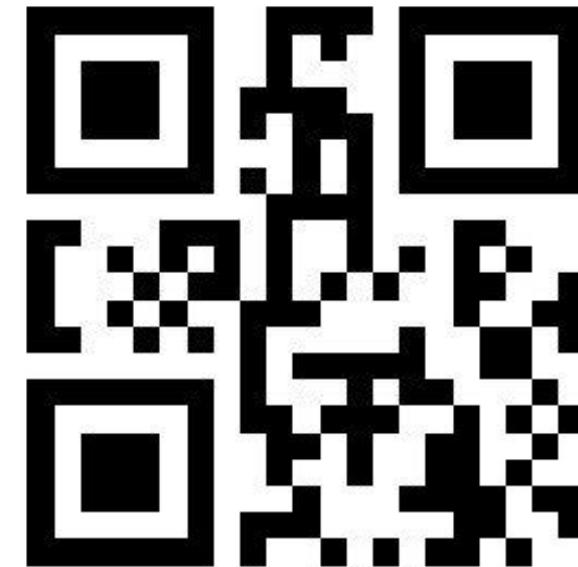
Hurricane Labs

.conf23 Learning Quest

Explore all .conf23
has to offer!



SCAN ME in the
.conf23 mobile
app game



Thank You





Bonus Content

Extra stuff

Splunk Search Optimization:

+ <https://hurricanelabs.com/splunk-tutorials/splunk-search-optimization-a-paleo-diet-for-spl/>

Splunk 9.0 Configuration Change Tracking:

+ <https://hurricanelabs.com/splunk-tutorials/first-look-splunk-9-0-configuration-change-logging/>

Splunk Indexer Clustering:

+ <https://hurricanelabs.com/splunk-tutorials/splunk-indexer-clustering-your-hero-in-the-fight-against-data-loss/>