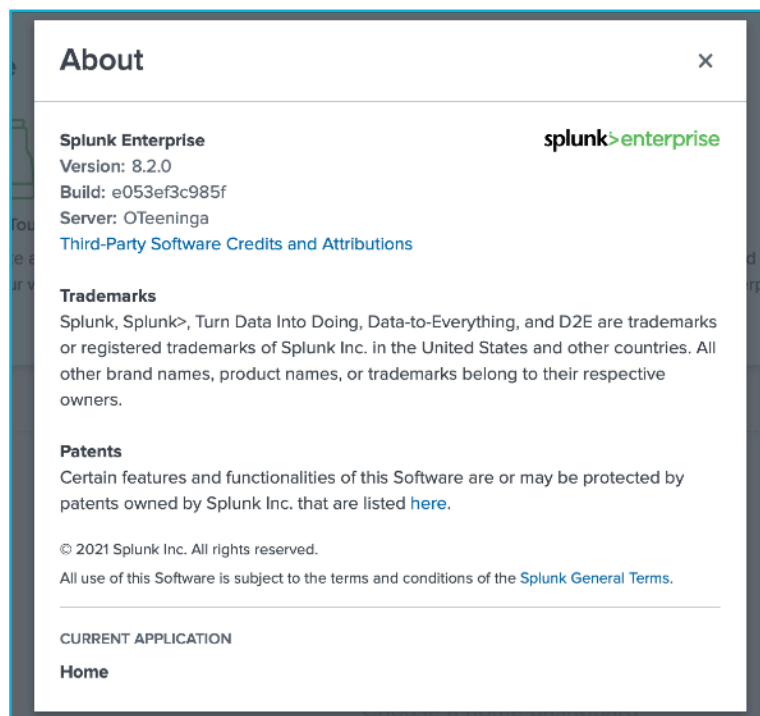


Splunk

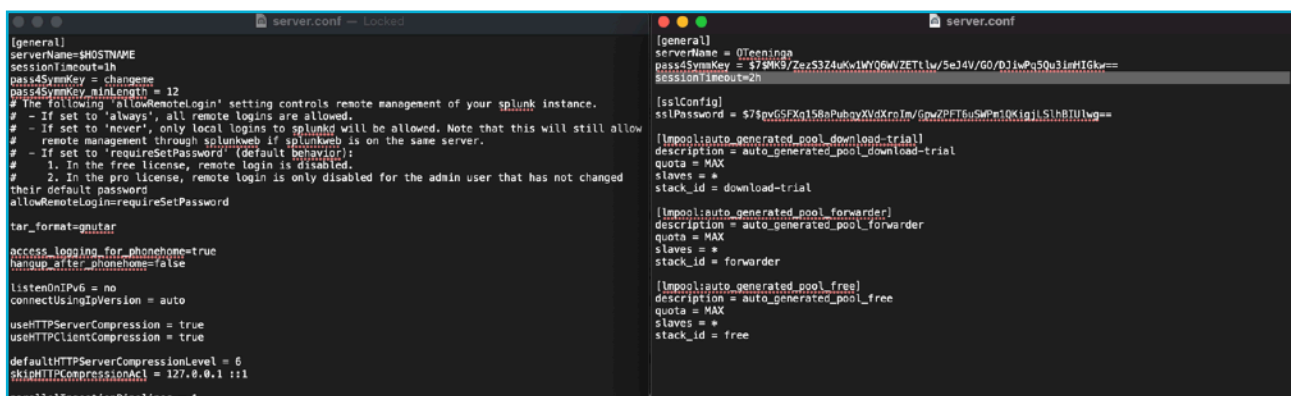
Oscar Teeninga
OSZBD

1. Instalacja i uruchomienie instancji

- Rozpakowanie przygotowanego archiwum
Korzystałem z wersji na MacOS. Wszystko dalej odbywa się normalnie jak na laboratoriach.
- Problemy z uruchomieniem
Nie napotkałem na jakiegokolwiek problemy.
- Modyfikacja nazwy serwera
Zmieniłem nazwę serwera zgodnie z instrukcją.



- Polecenie bttool
Zmieniłem parametr Timeoutu.



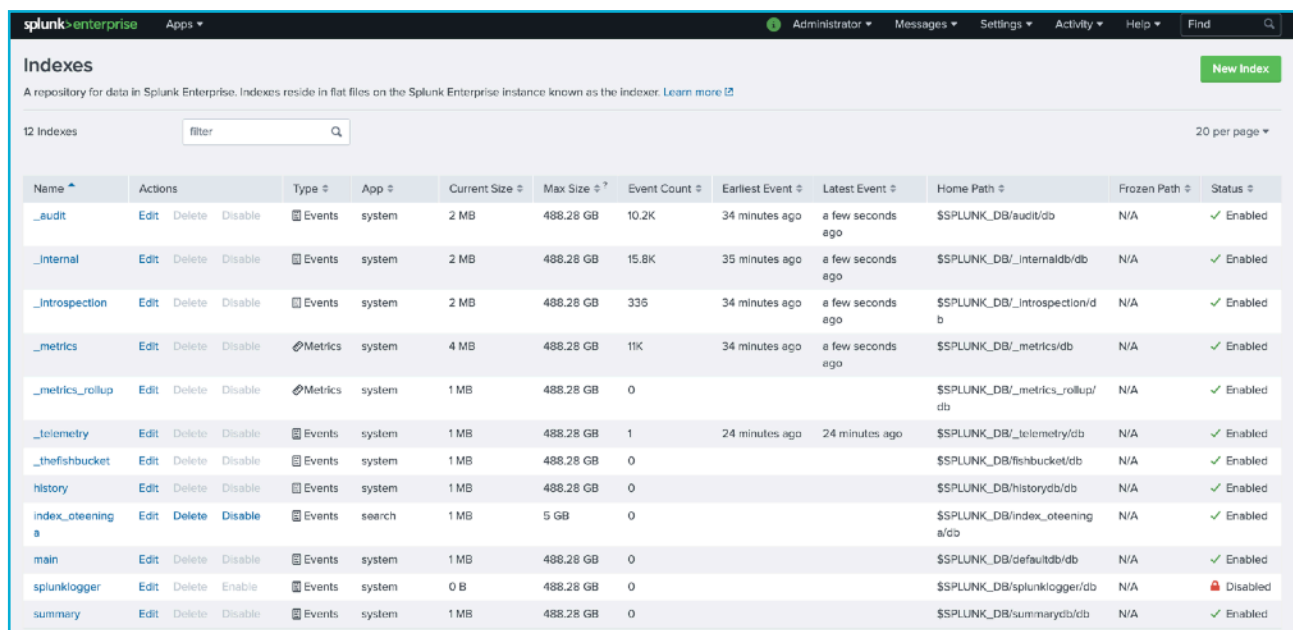
Następnie za pomocą polecenia `./splunk cmd btool server list | grep Timeout` sprawdziłem jaki jest ustawiony `sessionTimeout`.

```
oscarteeninga@MacBook-Pro-16-Oscar bin % ./splunk cmd btool server list | grep Timeout
updateTimeout = 24h
s2sHeartbeatTimeout = 600
sessionTimeout = 2h
busyKeepAliveIdleTimeout = 12
keepAliveIdleTimeout = 7200
streamInWriteTimeout = 5
clientConnectionTimeout = 10
clientSocketTimeout = 300
replicationWriteTimeout = 1800
shutdownTimeout = 100
s2sHeartbeatTimeout = 600
responseTimeout = 8
```

Zgodnie z oczekiwaniami, wyższy priorytet ma konfiguracja z podkatalogu `local`.

2. Indeksowanie danych

- a) Stworzenie indeksu `index_oteeninga`
Indeks stworzyłem poprzez GUI o nazwie `index_oteeninga`.



Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen Path	Status
._audit	Edit Delete Disable	Events	system	2 MB	488.28 GB	10.2K	34 minutes ago	a few seconds ago	\$SPLUNK_DB/audit/db	N/A	Enabled
._internal	Edit Delete Disable	Events	system	2 MB	488.28 GB	15.8K	35 minutes ago	a few seconds ago	\$SPLUNK_DB/_internaldb/db	N/A	Enabled
._introspection	Edit Delete Disable	Events	system	2 MB	488.28 GB	336	34 minutes ago	a few seconds ago	\$SPLUNK_DB/_introspection/db	N/A	Enabled
._metrics	Edit Delete Disable	Metrics	system	4 MB	488.28 GB	11K	34 minutes ago	a few seconds ago	\$SPLUNK_DB/_metrics/db	N/A	Enabled
._metrics_rollup	Edit Delete Disable	Metrics	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_metrics_rollup/db	N/A	Enabled
._telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	1	24 minutes ago	24 minutes ago	\$SPLUNK_DB/_telemetry/db	N/A	Enabled
._thefishbucket	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_thefishbucket/db	N/A	Enabled
history	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/historydb/db	N/A	Enabled
index_oteeninga	Edit Delete Disable	Events	search	1 MB	5 GB	0			\$SPLUNK_DB/index_oteeninga/db	N/A	Enabled
main	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/defaultdb/db	N/A	Enabled
splunklogger	Edit Delete Enable	Events	system	0 B	488.28 GB	0			\$SPLUNK_DB/splunklogger/db	N/A	Disabled
summary	Edit Delete Disable	Events	system	1 MB	488.28 GB	0			\$SPLUNK_DB/summarydb/db	N/A	Enabled

- b) Zaindeksowanie danych
Dane, które importowałem to `tutorialdata.zip`. Zrobiłem to przez GUI, poprzez `Settings` -> `Add Data`, ustawiając index na `index_oteeninga`.
- c) Powtórzenie czynności 2a-2c z monitorowaniem
Skorzystałem z logów na systemie MacOS.

File or Directory ?

`/var/log/system.log`

Browse

On Windows: `c:\apache\apache.error.log` or
`\\hostname\apache\apache.error.log`. On Unix: `/var/log` or `/mnt/www01/var/log`.

Następnie odtworzyłem wcześniejsze kroki.

Add Data

< Back

Review >

Select Source

Set Source Type

Input Settings

Review

Done

Input Settings

Optionally set additional input parameters for this data input as follows:

App context

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context

Monitoring Console (splunk_monitoring_console) ▾

Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value

Regular expression on path

Segment in path

Host field value

OTeeninga

Index

The Splunk platform stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index

Index_oteeninga ▾

Create a new index

FAQ

> How do indexes work?

> How do I know when to create or use multiple indexes?

3. Wyszukiwanie zaindeksowanych danych

- Zapoznanie się z składnią SPL
Zapoznałem się :)
- Stworzenie zapytań korzystając z indeksów z punktu 2
 - Wszystkie zdarzenia w przykładowym logu dotyczą uwierzytelniania

New Search Save As Create Table View Close

index="index_oteeninga" authentication All time

✓ 2 events (before 19/05/2021 20:42:13.000) No Event Sampling Job

Events (2) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 millisecond per column

List Format 50 Per Page

	i	Time	Event
	>	19/05/2021 11:31:04.000	May 19 11:31:04 MacBook-Pro-16-Oscar accountsd[424]: objc[424]: Class AMSyncAccountFlagsTask is implemented in both /System/Library/Accounts/Notification/AMSAccountNotificationPlugin.bundle/Contents/MacOS/AMSAccountNotificationPlugin (0x7fff84c89c38) and /System/Library/Accounts/Authentication/AMSAccountAuthenticationPlugin.bundle/Contents/MacOS/AMSAccountAuthenticationPlugin (0x10e03bd58). One of the two will be used. Which one is undefined. host = OTeeninga source = /var/log/system.log sourcetype = macoslogs
	>	19/05/2021 11:31:04.000	May 19 11:31:04 MacBook-Pro-16-Oscar accountsd[424]: objc[424]: Class AMSyncAccountFlagsResult is implemented in both /System/Library/Accounts/Notification/AMSAccountNotificationPlugin.bundle/Contents/MacOS/AMSAccountNotificationPlugin (0x7fff84c89c38) and /System/Library/Accounts/Authentication/AMSAccountAuthenticationPlugin.bundle/Contents/MacOS/AMSAccountAuthenticationPlugin (0x10e03bd58). One of the two will be used. Which one is undefined. host = OTeeninga source = /var/log/system.log sourcetype = macoslogs

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 1
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
a Index 1
linecount 1
a punct 1
a splunk_server 1
timeendpos 1
timestartpos 1

+ Extract New Fields

- Wszystkie zdarzenia dotyczą serwera http

New Search Save As Create Table View Close

index="index_oteeninga" http All time

✓ 39,532 events (before 19/05/2021 20:43:21.000) No Event Sampling Job

Events (39,532) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 50 Per Page < Prev 1 2 3 4 5 6 7 8 ... Next >

	i	Time	Event
	>	07/04/2021 18:22:16.000	91.205.189.15 - - [07/Apr/2021:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159 host = OTeeninga source = tutorialdata.zip:/www2/access.log sourcetype = access_combined_wcookie
	>	07/04/2021 18:22:15.000	91.205.189.15 - - [07/Apr/2021:18:22:15] "GET /category.screen?categoryId=SHOOTER&JSESSIONID=SD6SL7FF7ADF53113 HTTP 1.1" 200 1369 "http://www.google.com" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 779 host = OTeeninga source = tutorialdata.zip:/www2/access.log sourcetype = access_combined_wcookie
	>	07/04/2021 18:20:56.000	182.236.164.11 - - [07/Apr/2021:18:20:56] "GET /cart.do?action=addtocart&itemId=EST-15&productId=BS-AG-G09&JSESSIONID=SD6SL8FF10ADF53101 HTTP 1.1" 200 2252 "http://www.buttercupgames.com/oldlink?itemId=EST-15" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 506 host = OTeeninga source = tutorialdata.zip:/www2/access.log sourcetype = access_combined_wcookie
	>	07/04/2021 18:20:55.000	182.236.164.11 - - [07/Apr/2021:18:20:55] "POST /oldlink?itemId=EST-18&JSESSIONID=SD6SL8FF10ADF53101 HTTP 1.1" 400 893 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 134 host = OTeeninga source = tutorialdata.zip:/www2/access.log sourcetype = access_combined_wcookie
	>	07/04/2021 18:20:54.000	182.236.164.11 - - [07/Apr/2021:18:20:54] "GET /category.screen?categoryId=ACCESSORIES&JSESSIONID=SD6SL8FF10ADF53101 HTTP 1.1" 200 3920 "http://www.buttercupgames.com/oldlink?itemId=EST-17" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 648 host = OTeeninga source = tutorialdata.zip:/www2/access.log sourcetype = access_combined_wcookie
	>	07/04/2021 18:20:54.000	182.236.164.11 - - [07/Apr/2021:18:20:54] "POST /cart.success.do?JSESSIONID=SD6SL8FF10ADF53101 HTTP 1.1" 200 356 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-6" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 228 host = OTeeninga source = tutorialdata.zip:/www2/access.log sourcetype = access_combined_wcookie

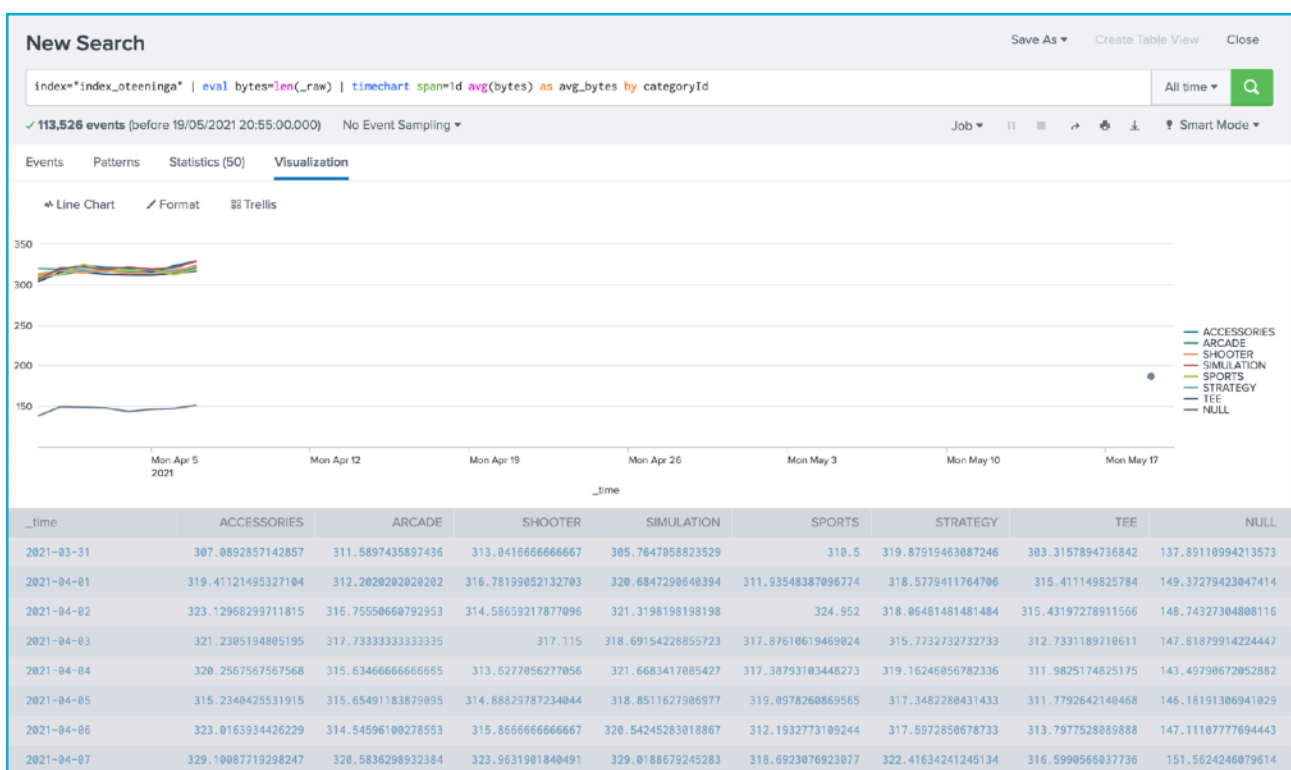
SELECTED FIELDS
a host 1
a source 3
a sourcetype 1

INTERESTING FIELDS
a action 5
bytes 100+
a categoryid 8
a clientip 100+
date_hour 24
date_mday 8
date_minute 60
date_month 2
date_second 60
date_wday 7
date_year 1
date_zone 1
a file 14
a ident 1
a index 1
a itemid 14
a JSESSIONID 100+
linecount 1
a method 2
other 100+
a productid 16
a punct 98

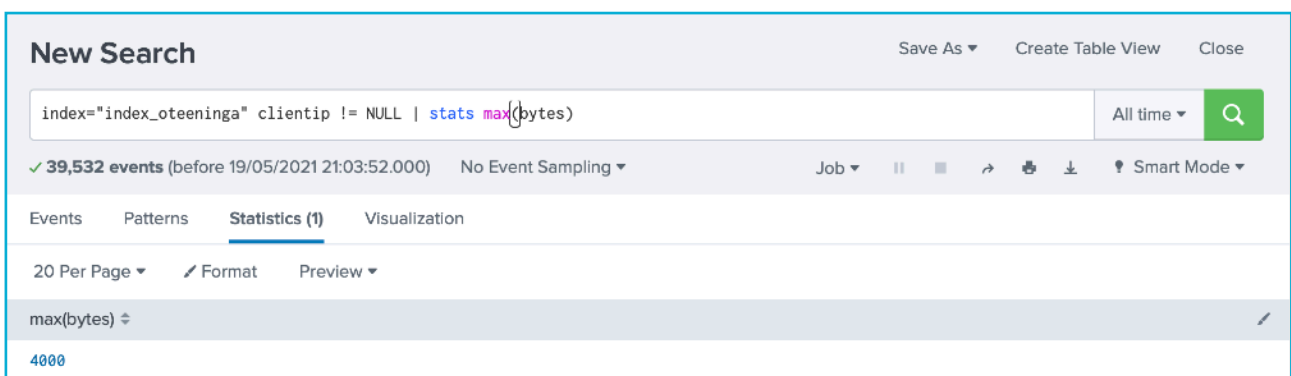
iii. Średni rozmiar danych zwrócony przez zapytanie w ostatnim miesiącu



iv. Wizualizację średniego rozmiaru danych dla każdego klienta z agregacją dobową



v. Maksymalny rozmiar transferu danych dla każdego klienta (id przez IP)




- vi. Listę user agentów dla każdego adresu IP

New Search

Save As ▾ Create Table View Close

index="index_oteeninga" | stats distinct_count(useragent) by clientip

All time ▾ 

✓ 113,845 events (before 19/05/2021 21:36:30.000) No Event Sampling ▾

Job ▾ || ▮ ➔ ⚙ ⬇ ⚡ Smart Mode ▾

Events Patterns Statistics (182) Visualization

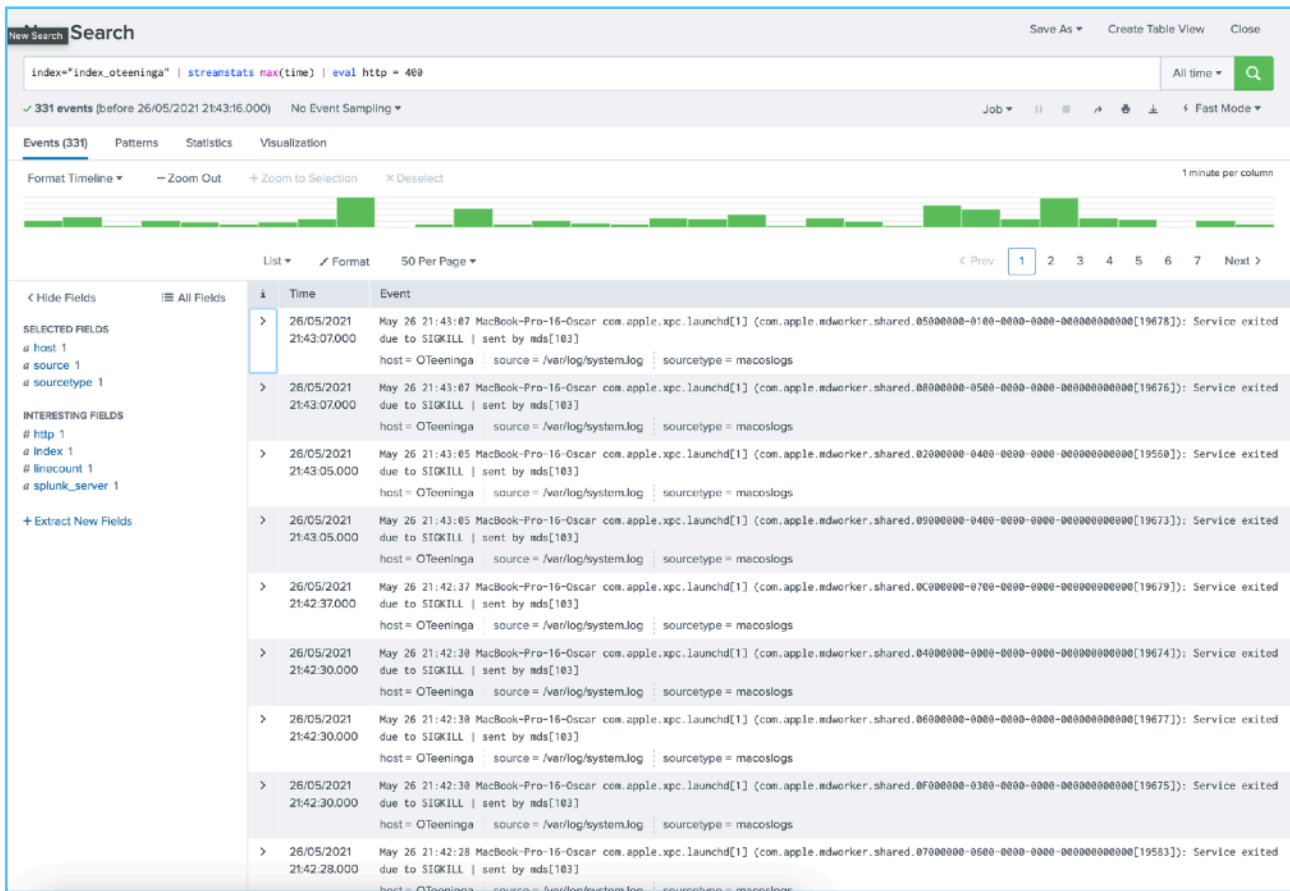
20 Per Page ▾ ↗ Format Preview ▾

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

clientip ⓘ	distinct_count(useragent) ⚙
107.3.146.207	16
109.65.113.83	17
109.169.32.135	14
110.138.30.229	13
110.159.208.78	15
111.161.27.20	15
112.111.162.4	13
117.21.246.164	15
118.142.68.222	12
12.130.60.4	13
12.130.60.5	14
121.254.179.199	13
121.9.245.177	13
123.118.73.155	13
123.196.113.11	12
123.30.106.208	10
124.168.192.241	12
125.17.14.100	14
125.7.55.100	14
125.89.78.6	15

[illegible]

vii. Dla każdej podstrony - ostatni kod http jaki wystąpił oraz poprzedni kod http jaki wystąpił wraz z czasami ich wystąpienia



c) Przygotuj zapytanie oraz wizualizację do niego



d) Zbadaj co najbardziej wpływa na czas wykonania zapytania

Najwięcej czasu zajmuje zapytanie search oraz dispatch. Całość zajęła 0.637s.

Duration (seconds)		Component	Invocations	Input count	Output count
	0.00	command.addinfo	37	39,532	39,532
	0.01	command.bin	37	39,532	39,532
	0.00	command.convert	37	39,532	39,532
	0.00	command.fields	37	39,532	39,532
	0.00	command.fillnull	37	39,532	39,532
■	0.06	command.prestats	37	39,532	3,611
■	0.38	command.search	37	-	39,532
■	0.03	command.timechart	39	3,611	169
■	0.02	command.timechart.execute_output	1	-	169
	0.01	command.timechart.execute_input	38	3,611	-
	0.00	command.timechart.execute_output.getIntermediateResults()	1	-	-
	0.01	command.timechart.execute_output.reduce_and_emit	1	-	2,346
	0.01	command.timechart.execute_output.series_filter	1	-	-
	0.00	dispatch.createdSearchResultInfrastructure	1	-	-
■	0.05	dispatch.evaluate.search	2	-	-
	0.01	dispatch.evaluate.timechart	2	-	-
■	0.48	dispatch.fetch.rcp.phase_0	38	-	-
	0.00	dispatch.finalWriteToDisk	1	-	-
■	0.46	dispatch.localSearch	1	-	-
■	0.46	dispatch.stream.local	37	-	-
	0.00	dispatch.writeStatus	3	-	-
■	0.05	startup.configuration	2	-	-
■	0.16	startup.handoff	2	-	-

4. Modele danych

a) Przygotuj model danych

MyDataModel

MyDataModel

[All Data Models](#)

Datasets

SEARCHES

MyDataSet

MyDataSet

MyDataSet

BASE SEARCH

index="*_audit"

Search

Edit

Bulk Edit

EXTRACTED

	_time	Time	Required
<input type="checkbox"/>	action	String	Edit
<input type="checkbox"/>	info	String	Edit
<input type="checkbox"/>	timestamp	String	Edit
<input type="checkbox"/>	user	String	Edit

Calculated fields are processed in the order above, so ensure any dependent fields are defined first. Drag to rearrange.

Edit

Download

Pivot

Documentation

Rename

Delete

Add Dataset

Add Field

b) Policz statystyki z ostatniego tygodnia dotyczące

i. Ilość wystąpień poszczególnych akcji per użytkownik

New Search

Save As

Create Table View

Close

testate count from dataset1-mydatamodel1 by mydataset.user,mydataset.action

Last 7 days

10,161 events (19/05/2021 16:00:00:000 to 26/05/2021 16:53:50:000)

No Event Sampling

Jobs

Smart Mode

Events

Patterns

Statistics (64)

Visualization

20 Per Page

Format

Preview

MyDataSet.user	MyDataSet.action	count
admin	accelerate_search	437
admin	change_authentication	186
admin	edit_deployment_client	53
admin	edit_deployment_server	371
admin	edit_dist_peer	186
admin	edit_forwarders	132
admin	edit_global_banner	53
admin	edit_health	53
admin	edit_indexer_cluster	132
admin	edit_metrics_rollup	3
admin	edit_modinput_admon	53
admin	edit_modinput_perfaon	53
admin	edit_modinput_winhostan	53
admin	edit_modinput_winmetan	53
admin	edit_modinput_winprintan	53
admin	edit_monitor	148
admin	edit_roles	112
admin	edit_roles_granttable	3
admin	edit_scripted	53
admin	edit_search_schedule_priority	119

This search has completed and has returned 64 results by scanning 10,165 events in 0.212 seconds

New Search

Save As

Create Table View

Close

index="*_audit" | stats count by user,action

Last 7 days

10,031 events (19/05/2021 17:00:00:000 to 26/05/2021 17:18:05:000)

No Event Sampling

Jobs

Smart Mode

Events

Patterns

Statistics (64)

Visualization

20 Per Page

Format

Preview

user	action	count
admin	accelerate_search	374
admin	change_authentication	88
admin	edit_deployment_client	44
admin	edit_deployment_server	368
admin	edit_dist_peer	88
admin	edit_forwarders	132
admin	edit_global_banner	44
admin	edit_health	44
admin	edit_indexer_cluster	132
admin	edit_metrics_rollup	2
admin	edit_modinput_admon	44
admin	edit_modinput_perfaon	44
admin	edit_modinput_winhostan	44
admin	edit_modinput_winmetan	44
admin	edit_modinput_winprintan	44
admin	edit_monitor	88
admin	edit_roles	54
admin	edit_roles_granttable	3
admin	edit_scripted	44
admin	edit_search_schedule_priority	115

This search has completed and has returned 64 results by scanning 10,031 events in 0.149 seconds

Normalne wyszukiwania okazało się szybsze. Nie jest to jedna znacząca różnica.

ii. Najczęściej pojawiające się akcje per użytkownik

New Search Save As Create Table View Close

`| tstats count(MyDataSet.action) as action_count from datamodel=MyDataSet by MyDataSet.user, MyDataSet.action | stats max(action_count) by MyDataSet.user` Last 7 days Q

✓ 11,733 events (19/05/2021 17:00:00.000 to 26/05/2021 17:44:00.000) No Event Sampling Job || → ⬇ Smart Mode

Events Patterns **Statistics (3)** Visualization

20 Per Page Format Preview

MyDataSet.user	max(action_count)
admin	3024
n/a	163
splunk-system-user	165

This search has completed and has returned **3** results by scanning **11,733** events in **0.225** seconds

New Search Save As Create Table View Close

`index="_audit" | stats count(action) as action_count by user, action | stats max(action_count) by user` Last 7 days Q

✓ 11,889 events (19/05/2021 17:00:00.000 to 26/05/2021 17:45:08.000) No Event Sampling Job || → ⬇ Smart Mode

Events Patterns **Statistics (3)** Visualization

20 Per Page Format Preview

user	max(action_count)
admin	3060
n/a	163
splunk-system-user	165

This search has completed and has returned **3** results by scanning **11,889** events in **0.161** seconds

Analogiczna sytuacja do poprzedniej. Znów szybsza okazało się zapytane stats.

Następnie odpaliłem akcelerację, po kilku minutach było gotowe. Po raz kolejny wykonałem testy szybkości.

▼

MyDataModel

MODEL

Datasets 1 Search Event [Edit](#)

Permissions Shared in App. Owned by admin. [Edit](#)

ACCELERATION

[Rebuild](#) [Update](#) [Edit](#)

Status 100.00% Completed

Access Count 0. Last Access: -

Size on Disk 636 KB

Summary Range 604800 second(s)

Buckets 2

Updated 26/05/2021 18:00:00.000

> Detailed Acceleration Information

> Configuration Settings

Dla zapytania tstats

This search has completed and has returned **63** results by scanning **8,227** events in **0.177** seconds

This search has completed and has returned **3** results by scanning **8,606** events in **0.177** seconds

Dla zapytania stats

This search has completed and has returned **63** results by scanning **8,346** events in **0.156** seconds

This search has completed and has returned **3** results by scanning **8,489** events in **0.189** seconds

Widzimy znaczną poprawę szybkości w przypadku zapytania tstats. Ciekawy jest brak wpływu max() na zapytanie w przypadku tstats, dzięki czemu wyprzedza w drugim zapytaniu standardowego stats.

5. Polityka retencji

- a) Zapoznaj się z etapami życia bucketów. Zmodyfikuj indexes.conf zgodnie z poleceniem.
Korzystałem z systemu MacOS, więc dane wykorzystywane przez splunk przechowywane są w dedykowanym folderze, do której ostatecznie postanowiłem zapisywać kubelki.

```
indexes.conf

[index_oteeninga]
enableDataIntegrityControl = 0
enableTsidxReduction = 0
homePath = $SPLUNK_DB/index_oteeninga/db
maxTotalDataSizeMB = 5120
thawedPath = $SPLUNK_DB/index_oteeninga/thaweddb
maxDataSizeMB = 2
maxWarmDBCount = 3
frozenTimePeriodInSecs = 900
coldPath = $SPLUNK_DB/0Teeninga/cold
archiver.enableDataArchive = 0
bucketMerging = 0
bucketRebuildMemoryHint = 0
coldToFrozenDir = $SPLUNK_DB/0Teeninga/frozen
```

Edit Index: index_oteeninga

General Settings

Home Path:
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).

Cold Path:
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/cold).

Thawed Path:
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).

Data Integrity Check:
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.

Max Size of Entire Index: GB
Maximum target size of entire index.

Max Size of Hot/Warm/Cold Bucket: MB
Maximum target size of buckets. Enter 'auto_high_volume' for high volume indexes.

Frozen Path:
Frozen bucket archive path. Set this if you want Splunk to automatically archive frozen buckets.

App:

> _introspection	19 May 2021 at 14:51	--	Folder
> _metrics	19 May 2021 at 14:51	--	Folder
> _metrics_rollup	19 May 2021 at 14:51	--	Folder
> _telemetry	19 May 2021 at 14:51	--	Folder
> audit	19 May 2021 at 14:51	--	Folder
> authDb	19 May 2021 at 14:50	--	Folder
> defaultdb	Today at 21:14	--	Folder
> fishbucket	Today at 21:22	--	Folder
> hashDb	19 May 2021 at 14:50	--	Folder
> historydb	19 May 2021 at 14:51	--	Folder
> index_oteeninga	Today at 18:57	--	Folder
> kvstore	19 May 2021 at 14:51	--	Folder
> modinputs	19 May 2021 at 14:51	--	Folder
> 0Teeninga	Today at 19:33	--	Folder
> cold	Today at 21:15	--	Folder
> frozen	Today at 19:59	--	Folder
> db_1622050331_1622049231_3	Today at 20:00	--	Folder
> db_1622050801_1622050341_4	Today at 20:51	--	Folder
> db_1622050808_1622050808_5	Today at 19:59	--	Folder
> persistentstorage	Today at 21:08	--	Folder
> summarydb	19 May 2021 at 14:51	--	Folder
> _audit.dat	Today at 21:15	1 byte	Document
> _internal.dat	Today at 21:15	1 byte	Document
> _introspection.dat	Today at 21:15	1 byte	Document
> _metrics.dat	Today at 21:15	2 bytes	Document
> _telemetry.dat	Today at 19:43	1 byte	Document

- b) Dokonaj pomiaru wydajności wyszukiwania w poszczególnych bucketach
Czas najprostszego zapytania to 0.15 s, natomiast liczba wyszukanych elementów jest bardzo mała. Właściwie znajduje jedynie najnowsze informacje. Oznacza to, że kubelki jest bardzo mały.
- c) Czy w sytuacji posiadania znacznych zasobów dyskowych uzasadnione jest trzymanie wszystkich danych w bucketach hot?
Jest uzasadnione w momencie jeżeli posiadamy znaczne zasoby pamięci operacyjnej, ponieważ jest ona znacznie szybsza. Natomiast rzadko zdarza się taka sytuacja, dlatego znacznie efektywniej przechowywać dane w innych kubelkach.
- d) Korzystając z komendy splunk rebuild oraz instrukcji przywróć do wyszukiwania dowolny zamrożony bucket.
- i. Ile trwa operacja przywracania?
Trwało tylko 70 ms, zdaje się jednak, że mógł wystąpić błąd.

```
oscarteeninga@MacBook-Pro-16-Oscar bin % ./splunk rebuild /Applications/Splunk/var/lib/splunk/defaultdb/thaweddb/db_1622050808_1622050808_5
USAGE: splunk rebuild <bucketPath> [<indexName>] [--ignore-read-error] [--no-log]
Please see 'splunk fsck' for more options. This command is just a wrapper for 'splunk fsck'.

Redirecting to 'splunkd fsck' with args:
repair --one-bucket --include-hot --bucket-path=/Applications/Splunk/var/lib/splunk/defaultdb/thaweddb/db_1622050808_1622050808_5 --log-to--splunkd-log
ERROR ProcessTracker - (subchild_43_RollFixMetadata) IndexConfig - Asked to check if idx= is an index with a remote storage, but that index does not exist on the sys
tem or is disabled
INFO Fsck - (entire bucket) Rebuild for bucket='/Applications/Splunk/var/lib/splunk/defaultdb/thaweddb/db_1622050808_1622050808_5' took 69.23 milliseconds
```

- ii. Jaka jest różnica w rozmiarze między bucketem frozen, a przywróconym?
Przywrócony waży 139 KB, natomiast bazowo było to 12 KB.
- iii. Jak wydajne jest wyszukiwanie w przywróconym bucketcie?
Porównywalnie jak wszystko inne ~ 0.2 s