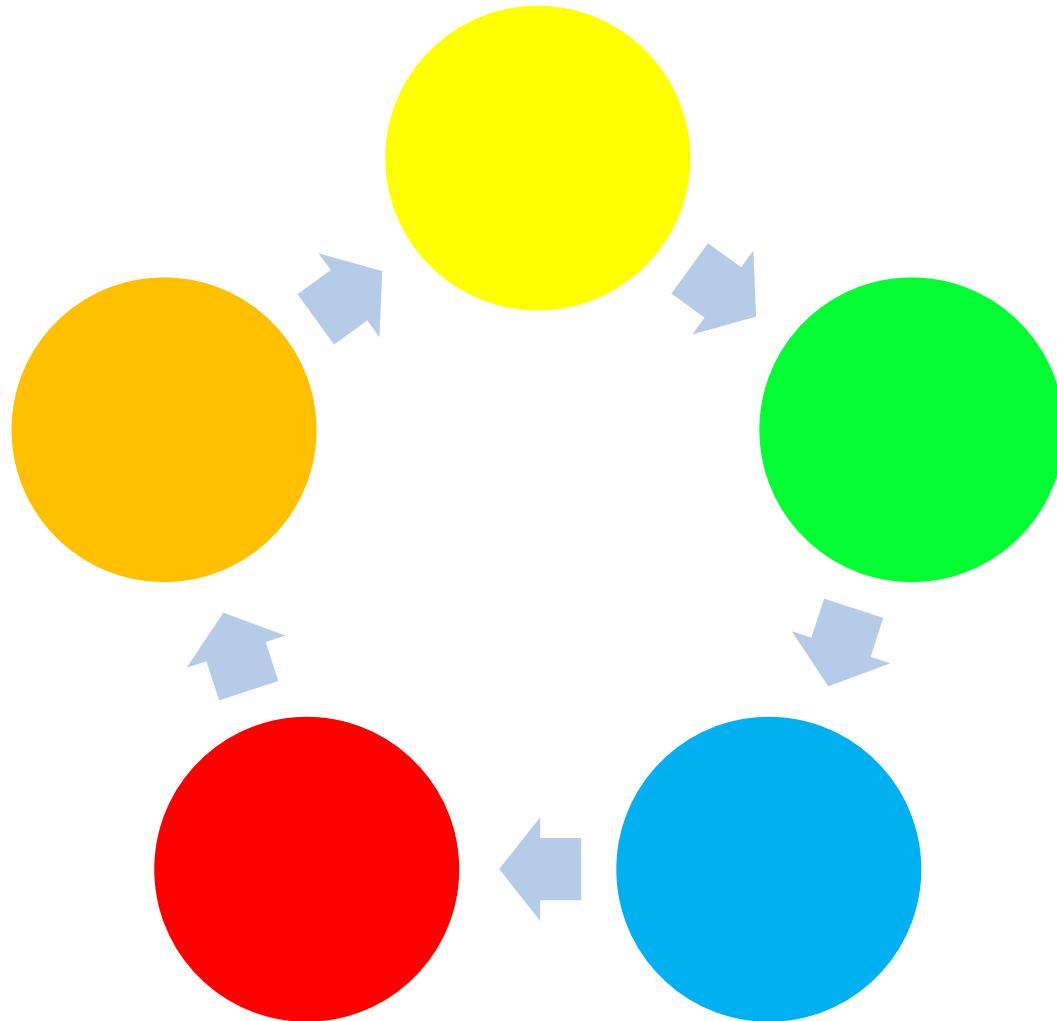


Voorstelrondje



Doel van de cursus

Het leren van basisvaardigheden in het gebruik van Splunk

Opzet van de cursus

Module 1: Kennismaking met Splunk

Module 2: Opstellen van een basis Search

Module 3: Aanvullen van een basis Search met commando's

Module 4: Genereren van Tabellen en Grafieken

Module 5: Genereren van een Dashboard

Cursus Fundamentals I (gratis; e-learning)

In de officiële Splunk cursus Fundamentals I worden in een notendop de functionaliteiten van Splunk besproken.

Informatie over de inhoud van de cursus:

<https://www.splunk.com/pdfs/training/splunk-fundamentals-1.pdf>

Het volgen van de cursus kan via:

https://www.splunk.com/en_us/training/courses/splunk-fundamentals-1.html

Men kan zich na het volgen van deze cursus gratis laten certificeren tot officieel Splunk-user.

Cursus Fundamentals II (niet gratis)

In de officiële Splunk cursus Fundamentals II worden Splunk functionaliteiten zoals o.a. scheduling, alerting en embedding van Reports behandeld.

Voor meer informatie zie:

<https://www.splunk.com/pdfs/training/splunk-fundamentals-2.pdf>

Een superuser is een persoon binnen een team/unit welke geautoriseerd is tot de Splunk rol job. De eis die er ligt tot het verkrijgen van deze rol is het volgen van de officiële Splunk cursus Fundamentals II.

De superuser kan dan op zijn naam de overgedragen Searches/Dashboards schedulen. Per team/unit zijn dit twee personen.

In de online documentatie van Splunk wordt uitgebreid ingegaan op commando's, functies van Splunk:

<http://docs.splunk.com/Documentation>

Een quick reference card voor deze documentatie kun je hier vinden:

<https://www.splunk.com/pdfs/solution-guides/splunk-quick-reference-guide.pdf>

Er is een online forum beschikbaar, waarin Splunk gebruikers wereldwijd elkaar vragen stellen en antwoorden geven:

<https://answers.splunk.com/index.html>

Binnen de Belastingdienst is er een connectpeople community voor Splunk. Ook hier wordt informatie verschaft en kunnen gebruiker vragen stellen:

2/2

<https://connectpeople.belastingdienst.nl/communities/service/html/communitystart?communityUuid=3b406640-b971-41b9-aa05-f2ebb67dfffc>

Cursus Splunk

Module 1:
Kennismaking met Splunk

Over Splunk



Is een commercieel software pakket voor:

- Het snel doorzoeken van opgeslagen data
- Het genereren van statistieken, tabellen en grafieken uit de data
- Het genereren van dashboards
- En nog veel meer ...

Data binnen de Belastingdienst

1/2

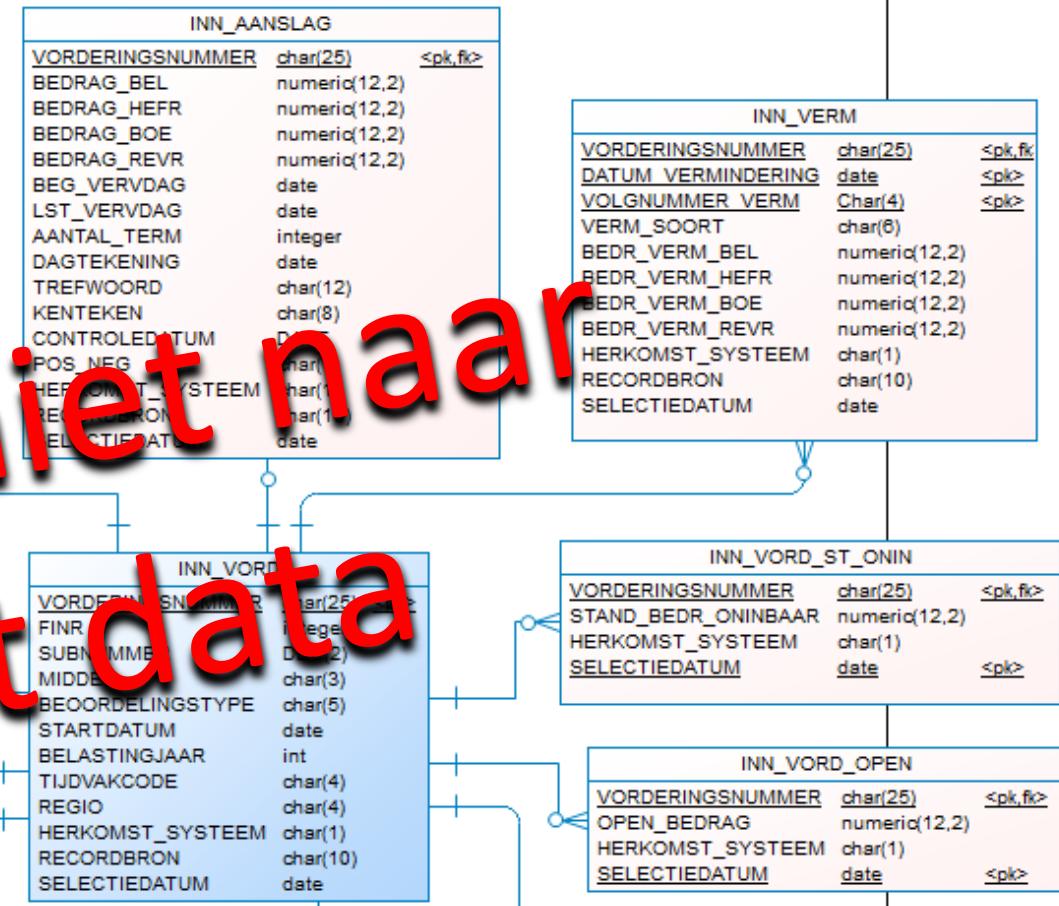
Data in tabelvorm

- Gegevens van burgers en bedrijven
- Gegevens van processen

	Id	Onderneming	Adres	Postcode	Plaats
1	00031	Tankstation De Bever	Wateman 108	6510 LC	Nijmegen
2	07365	Viskraam De Antenne	Antenneweg 62	3411 KJ	Lopik
3	10291	Actually	Reeshof 89a	1455 DL	Nijmegen
4	12198	Kwekerij De Anjer	Koningsberg 22	2181 RB	Hillegom
5	12733	Kantoorboekhandel Gembit	Duyspelaan 6	8221 DH	Zutphen
6	15621	Floppy Computers	Veldhof 22	5731 VL	Oudenbosch
7	21213	Zwembad West	Oostweg 78	8911 DD	Leeuwarden
8	22779	Café De Eerste Ronde	Plein 10	6531 XX	Nijmegen
9	23765	Midgetgolfsbaan Hole In One	Boslaan 2	8899 TD	Vlieland
10	33254	Slagerij Leo	Krijtlaan 5	8620 LH	Aalsmeer
11	49003	Het Radiohuis	Beekhorst 3	7118 TH	Aalsmeer
12	54323	SMP Automaterialen	Rooslaan 2	5614 SW	Bergen op Zoom
13	67234	Stomerij Brink	Aarweg 21	8600 CE	Sneek
14	67832	Koffie Tango Bravo	Baristaweg 5	1008 ST	Amsterdam
15	78342	Slijterij Minter	Narcisplein 34	2545 FB	Den Haag
16	90026	Oliebollenkraam De Krent	De Keeten 10	4712 TT	Roosendaal

fictieve data

We kijken niet naar
dit soort data



Data in de vorm van logregels (=tekstregels) in een logbestand

2/2

- Gegevens over gebeurtenissen (= Events)

Een klant logt in

Een bericht gaat van A naar B

Een foutsituatie treedt op

...

9/25/17 12:48:31.387 event_type="BUSINESS" gebr_id_srt="BSN" gebr_id=██████████ reg_moment="2017-09-25 12:48:31.00387" hulpmid=██████████ del_naam="OLDV_OLA_IH" hulpmiddel_versienr="1" meetpunt="BSS010A01E" soort="Start" app_comp="GOS" ip_adres=██████████ actie="0 ondertekenen" result="Succes" berichtsoort="Aangifte" regeling="Inkomstenbelasting" gemach_id_srt="BSN" gemach_id=██████████ belan gh_id_srt="BSN" belangh_id=██████████ tijdvak_begin="2015-01-01" tijdvak_einde="2015-12-31" kanaal="Internet"
host = JHOP-OTS_201731-on02p025 | source = /var/log/was/applogs/ots/businessevents/GOS-str14.log | sourcetype = OTS:GOS

9/25/17 12:48:31.387 PM 2017-09-25 12:48:31.387000, naam="Eduard", handeling="Handeling", category=GOS, Ondertekenen, result="Succes", disc="Onderstelbelasting:Aangift e: 2015-01-01", begin="2015-01-01", user_id=██████████, src_ip=██████████, time=2017-09-25 12:48:31.387000, die_st燵ode=IBAangifte2015, belan ghe_bende=██████████ machineprofile=██████████
host = JHOP-OTS_201731-on02p025 | source = /var/log/was/applogs/ots/businessevents/GOS-str14.log | sourcetype = OTS:GOS

9/25/17 12:48:31.223 event_type="PHSINFO" for_id_srt="BSN" gebr_id=██████████ reg_moment="2017-09-25 12:48:31.00223" hulpmid=██████████ del_naam="OLDV_OLA_IH" hulpmiddel_versienr="1" meetpunt="BSS010A005" soort="Start" app_comp="GOS" ip_adres=██████████ actie="0 ondertekenen" berichtsoort="Printfile" regeling="Inkomstenbelasting" gemach_id_srt="BSN" gemach_id=██████████ belangh_id_srt="BSN" belangh_id=██████████ tijdvak_begin="2015-01-01" tijdvak_einde="2015-12-31" kanaal="Internet"
host = JHOP-OTS_201731-on02p025 | source = /var/log/was/applogs/ots/businessevents/GOS-str14.log | sourcetype = OTS:GOS

Dit is het soort data waarmee we werken in Splunk

Meetpunten, Logfiles en Events

De data waarmee we werken in Splunk wordt gegenereerd door meetpunten

Meetpunt:

Een print statement in de programmacode van een systeem, neergezet op een positie waar een relevante gebeurtenis (= Event) kan optreden.

Als dit gebeurt, dan zal het meetpunt een tekstregel (= logregel) met data over het Event afdrukken naar een bestand (= logfile).

De Logfiles van verschillende systemen zijn input voor Splunk

Doel van een meetpunt

- Performance meting
Hoeveel berichten gaan bij meetpunt A naar buiten per minuut?
- Controleren volledigheid
Komen de berichten die bij meetpunt A verstuurd worden wel bij meetpunt B aan?
- Controleren tijdigheid
Is een bericht wel binnen 10 sec na versturen bij meetpunt A bij meetpunt B aangekomen?
- Signaleren foutsituaties
Als het groene systeem een fout signaleert, dan genereert meetpunt C een logregel.



Index, sourcetype en source

Source

Een logbestand met data gegenereerd door één of meer meetpunten in een systeem. **Voorbeeld:** mhs_mp03_mp04_20180725.log

Sourcetype

Verschillende logbestanden (sources) kunnen van hetzelfde type (sourcetype) zijn. Bijvoorbeeld omdat een systeem ieder uur een nieuw logbestand aanmaakt. **Voorbeeld:** mhs:keten

Index

De (fysieke of virtuele) locatie waar Splunk de logbestanden (sources) van een bepaald sourcetype opslaat. **Voorbeeld:** mhs-bem

Splunk productie omgevingen

Splunk

<https://splunk.belastingdienst.nl>

- Dit is de reguliere Splunk omgeving
- Je hebt een IMS autorisatie nodig voor toegang tot Splunk productie. Hierbij krijg je ook toegang tot een klein gedeelte van alle data in Splunk.
- Additioneel zijn er IMS autorisaties voor toegang tot verschillende datagebieden in Splunk

Splunk OTA

<https://otaspunk.belastingdienst.nl>

- Dit is de Splunk omgeving voor Ontwikkelen, Test en Acceptatie
- Je hebt een IMS autorisatie nodig voor toegang tot Splunk OTA. Hierbij krijg je meteen ook toegang tot alle beschikbare data in Splunk OTA.

Welke mogelijkheden heeft de gebruiker?

1/5

- Het doen van een Search (= zoekopdracht) over alle Events die zijn opgeslagen in Splunk*

Dit resulteert in een verzameling Events ...

9/25/17 12:48:31.387 PM	2017-09-25 12:48:31.387 event_type="BUSINESS" gebr_id_srt="BSN" gebr_id=██████████ reg_moment="2017-09-25-12:48:31.00387" hulpmid del_naam="OLDV_OLA_IH" hulpmiddel_versienr="1" meetpunt="BSS010A01E" soort="Einde" app_comp="GOS" ip_adres=██████████ actie="Ondertekenen" result="Sukses" berichtsoort="Aangifte" regeling="Inkomstenbelasting" gemach_id_srt="BSN" gemach_id=██████████ belangh_id_srt="BSN" belangh_id=██████████ tijdvak_begin="2015-01-01" tijdvak_einde="2015-12-31" kanaal="Internet" host = JHOP-OTS_201731-on02p025 source = /var/log/was/applogs/ots/businessevents/GOS-str14.log sourcetype = OTS:GOS
9/25/17 12:48:31.387 PM	2017-09-25-12:48:31.387000, name=Succesvolle handeling, category=GOS Ondertekenen, result=success, desc=Inkomstenbelasting:Aangifte:2015-01-01:2015-12-31, user_id=██████████, src_ip=██████████, time=2017-09-25-12:48:31.387000, dienstcode=IBAangifte2015, belanghebbende=██████████, machineprofiel= host = JHOP-OTS_201731-on02p025 source = /var/log/was/applogs/ots/businessevents/GOS-str14.log sourcetype = OTS:GOS
9/25/17 12:48:31.223 PM	2017-09-25 12:48:31.223 event_type="BUSINESS" gebr_id_srt="BSN" gebr_id=██████████ reg_moment="2017-09-25-12:48:31.00223" hulpmid del_naam="OLDV_OLA_IH" hulpmiddel_versienr="1" meetpunt="BSS010A00S" soort="Start" app_comp="GOS" ip_adres=██████████ actie="Ondertekenen" berichtsoort="Aangifte" regeling="Inkomstenbelasting" gemach_id_srt="BSN" gemach_id=██████████ belangh_id_srt="BSN" belangh_id=██████████ tijdvak_begin="2015-01-01" tijdvak_einde="2015-12-31" kanaal="Internet" host = JHOP-OTS_201731-on02p025 source = /var/log/was/applogs/ots/businessevents/GOS-str14.log sourcetype = OTS:GOS

* Je kunt alleen zoeken over Events van datagebieden waarvoor je geautoriseerd bent

... en in een verzameling Fields (= variabelen)

2/5

< Hide Fields All Fields

Selected Fields

a actie 10 

a app_comp 1

a belangh_id_srt 1

a belangh_id_srt2 1

date_hour 2

date_mday 1

date_minute 60

a date_month 1

date_second 60

a date_wday 1

date_year 1

a date_zone 1

a gebr_id_srt 2

a host 6

a index 1

actie

10 Values, 82.375% of events

Selected Yes No

Reports

Top values Top values by time Rare values

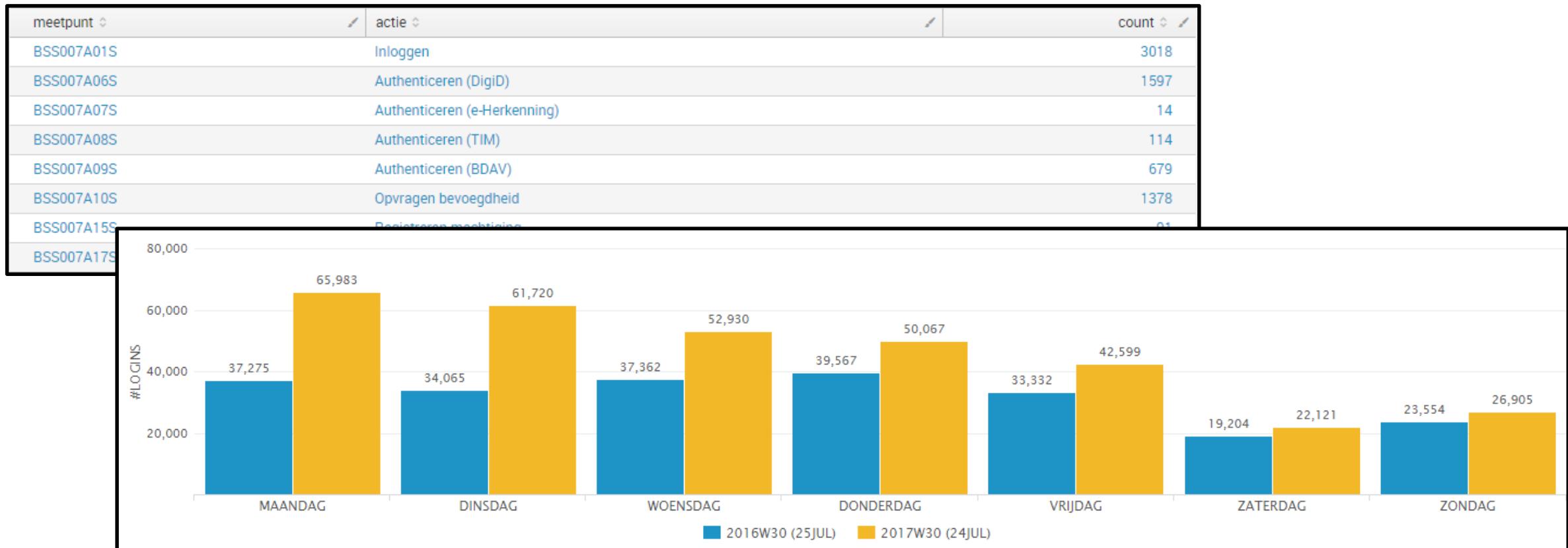
Events with this field

Top 10 Values	Count	%
Inloggen	2,215	26.761%
Authenticeren (DigiD)	2,030	24.526%
Opvragen bevoegdheid	1,864	22.52%
Verkrijgen Toegang generiek	1,117	13.495%
Authenticeren (BDAV)	807	9.75%
Authenticeren (TIM)	136	1.643%
Registreren machtiging	70	0.846%
Authenticeren (e-Herkenning)	18	0.217%
Activeren machtiging	14	0.169%
Authenticeren (eID)	6	0.072%

- Op basis van Events en Fields:

3/5

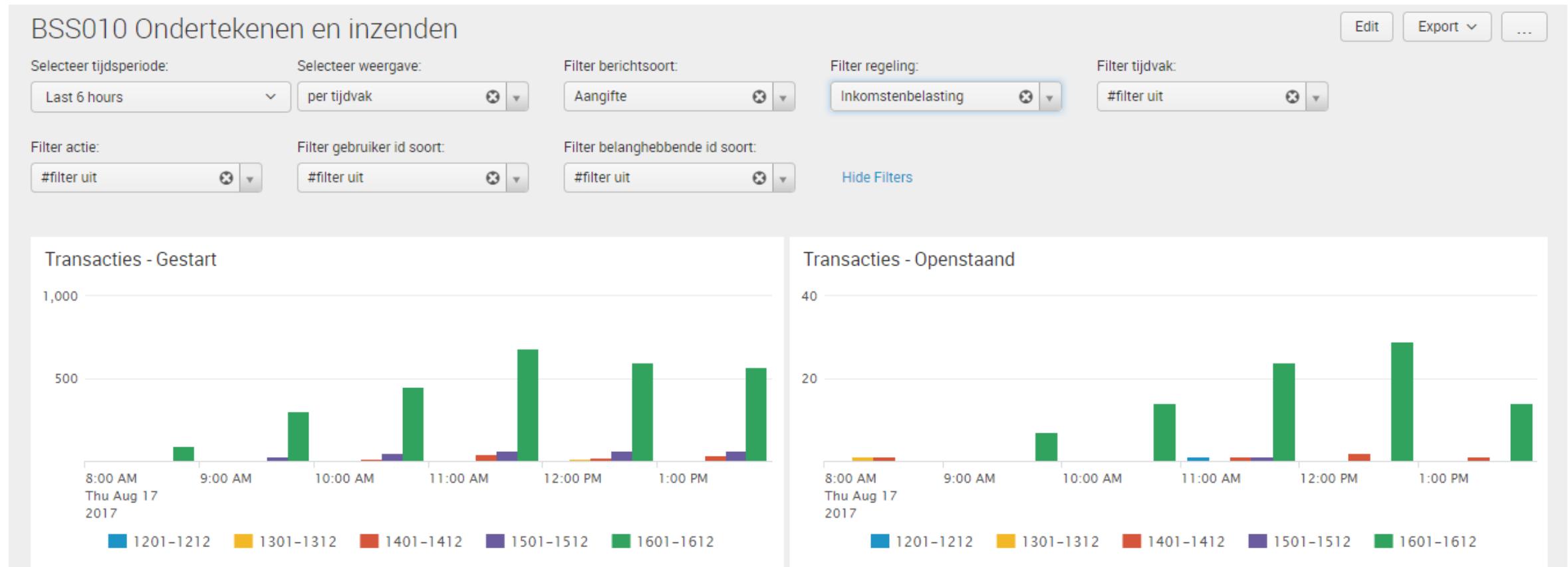
Het genereren van Reports (= losse tabellen en grafieken)



- Op basis van Reports:

4/5

Het genereren van een Dashboard (= pagina met tabellen, grafieken en controls)



- Het delen van Searches, Reports en Dashboards met andere Splunk gebruikers **5/5**

Basishandelingen in Splunk

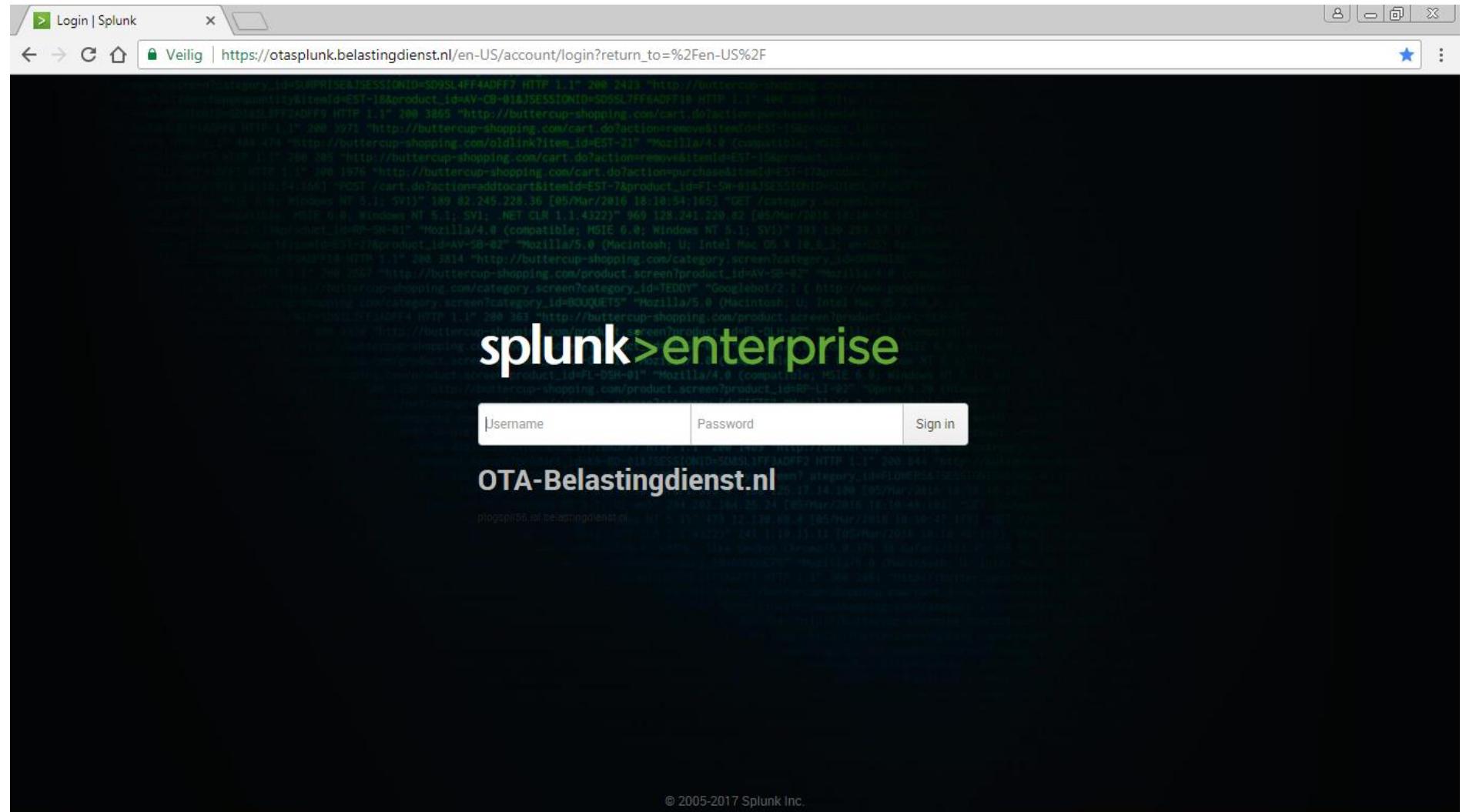
Opstarten van Splunk

Start een browser

Ga naar
[https://otasplunk.
belastingdienst.nl](https://otasplunk.belastingdienst.nl)

Tip: Maak een
snelkoppeling aan!

Log in met je DWB
username en
wachtwoord

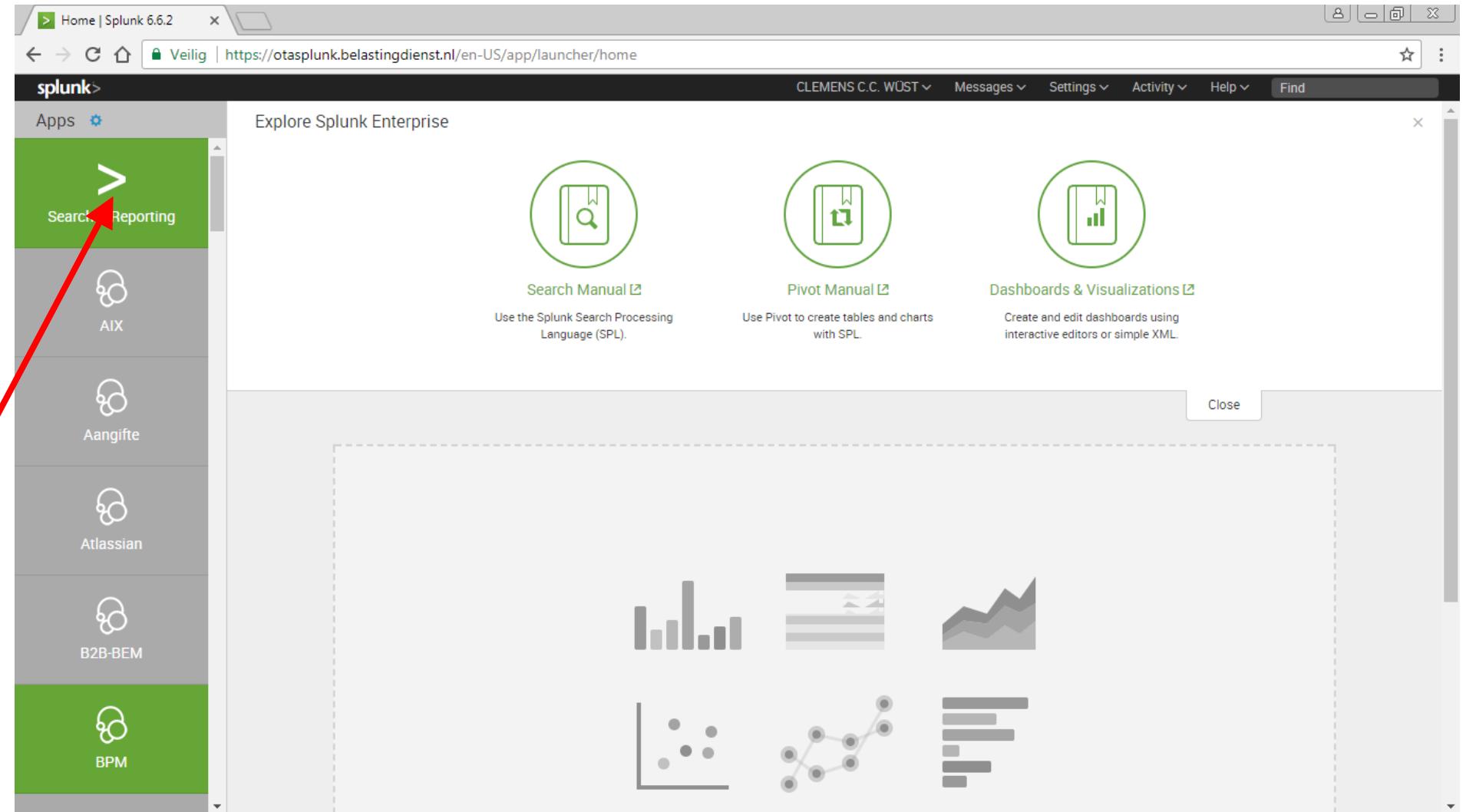


Welkom in Splunk

In Splunk werk je altijd onder een bepaalde App (= werkruimte)

De meest generieke App is **Search & Reporting**

Klik linksboven op het groene vlak om deze App te openen



Hoofdscherm (van de App Search & Reporting)

Splunk Bar (zwart):

Generiek menu
(App onafhankelijk)

App Bar (gekleurd):

Menu van de App die
actief is

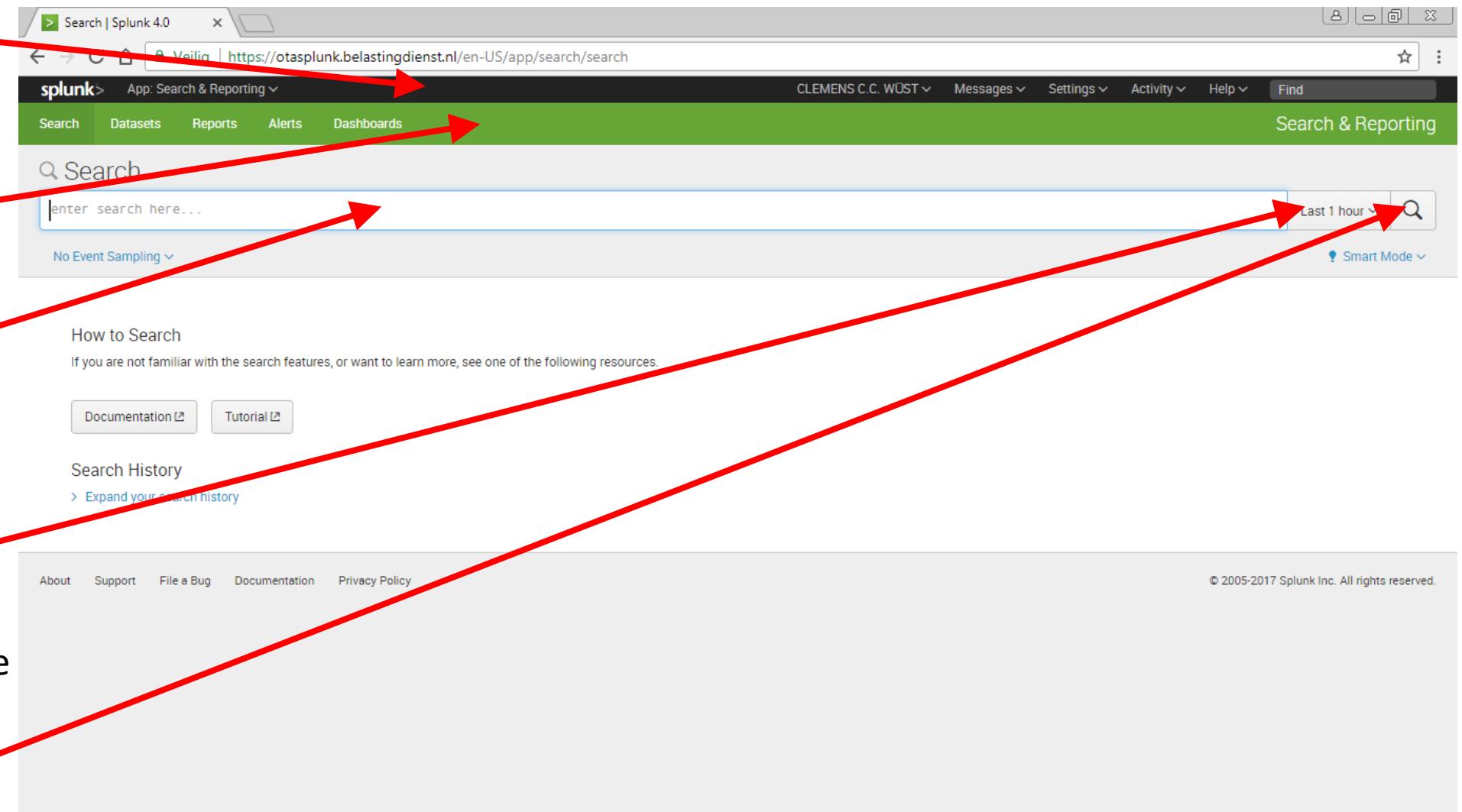
Search Bar:

Hier kun je een
zoekopdracht invoeren

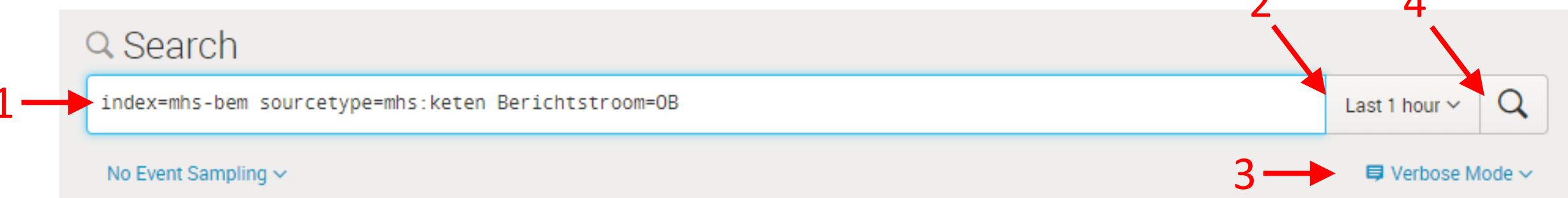
Time Range Picker:

Hier kun je invoeren
over welke tijdsperiode
gezocht moet worden

Start zoekopdracht



Uitvoeren van een Search (=zoekopdracht)



- 1 Typ een Search in de Search Bar *
- 2 Gebruik de Time Range Picker om de tijdsperiode te kiezen waarover gezocht moet worden (= de zoekperiode)
- 3 Kies een Search Mode
- 4 Klik op het vergrootglas of druk op ENTER om de Search te starten

* Gebruik SHIFT-ENTER om verder te typen op een nieuwe regel

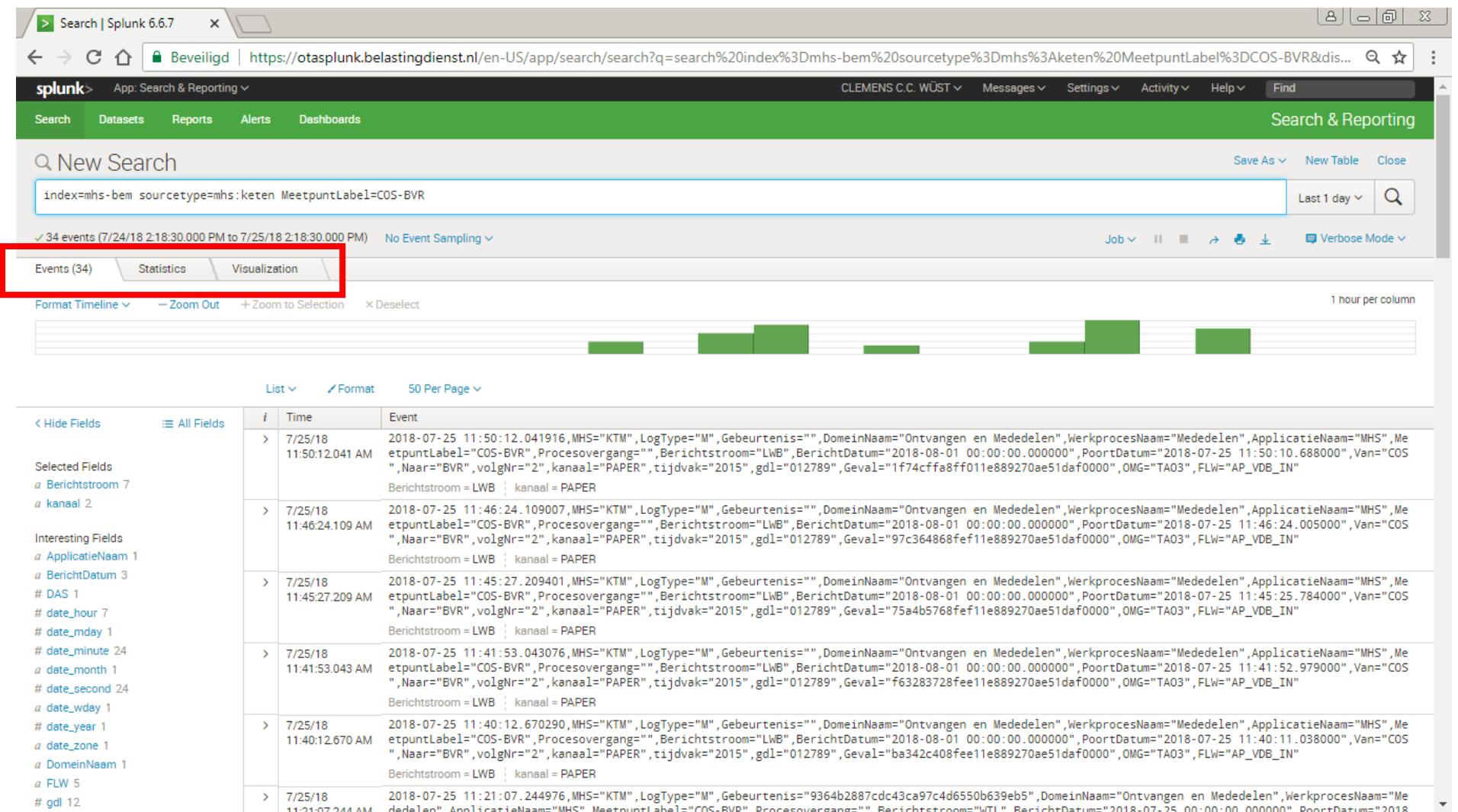
Resultaten van een Search

De zoekresultaten zijn verdeeld over drie tabbladen:

Events

Statistics

Visualization



Tabblad Events

1/10

The screenshot shows the Splunk 6.6.7 interface with the following components highlighted:

- Aantal Events**: Points to the "Events (34)" button in the top navigation bar.
- Timeline**: Points to the timeline visualization showing event distribution over time.
- Events**: Points to the list of events table.
- Fields**: Points to the "Fields" sidebar.

Search Bar: index=mhs-bem sourcetype=mhs:keten MeetpunktLabel=COS-BVR

Event Count: 34 events (7/24/18 2:18:30.000 PM to 7/25/18 2:18:30.000 PM) No Event Sampling

Timeline: 1 hour per column

i	Time	Event
>	7/25/18 11:50:12.041 AM	2018-07-25 11:50:12.041916, MHS="KTM", LogType="M", Gebeurtenis="", DomeinNaam="Ontvangen en Mededelen", WerkprocesNaam="Mededelen", ApplicatieNaam="MHS", MeetpunktLabel="COS-BVR", Procesovergang="", Berichtstroomb="LWB", BerichtDatum="2018-08-01 00:00:00.000000", PoortDatum="2018-07-25 11:50:10.688000", Van="COS ", Naar="BVR", volgNr="2", kanaal="PAPER", tijdvak="2015", gdl="012789", Geval="1f74cffa8ff011e889270ae51daf0000", OMG="TA03", FLW="AP_VDB_IN" Berichtstroomb = LWB kanaal = PAPER
>	7/25/18 11:46:24.109 AM	2018-07-25 11:46:24.109007, MHS="KTM", LogType="M", Gebeurtenis="", DomeinNaam="Ontvangen en Mededelen", WerkprocesNaam="Mededelen", ApplicatieNaam="MHS", MeetpunktLabel="COS-BVR", Procesovergang="", Berichtstroomb="LWB", BerichtDatum="2018-08-01 00:00:00.000000", PoortDatum="2018-07-25 11:46:24.005000", Van="COS ", Naar="BVR", volgNr="2", kanaal="PAPER", tijdvak="2015", gdl="012789", Geval="97c364868fef11e889270ae51daf0000", OMG="TA03", FLW="AP_VDB_IN" Berichtstroomb = LWB kanaal = PAPER
>	7/25/18 11:45:27.209401	2018-07-25 11:45:27.209401, MHS="KTM", LogType="M", Gebeurtenis="", DomeinNaam="Ontvangen en Mededelen", WerkprocesNaam="Mededelen", ApplicatieNaam="MHS", MeetpunktLabel="COS-BVR", Procesovergang="", Berichtstroomb="LWB", BerichtDatum="2018-08-01 00:00:00.000000", PoortDatum="2018-07-25 11:45:25.784000", Van="COS ", Naar="BVR", volgNr="2", kanaal="PAPER", tijdvak="2015", gdl="012789", Geval="75a4b5768fef11e889270ae51daf0000", OMG="TA03", FLW="AP_VDB_IN" Berichtstroomb = LWB kanaal = PAPER
>	7/25/18 11:41:53.043043	2018-07-25 11:41:53.043076, MHS="KTM", LogType="M", Gebeurtenis="", DomeinNaam="Ontvangen en Mededelen", WerkprocesNaam="Mededelen", ApplicatieNaam="MHS", MeetpunktLabel="COS-BVR", Procesovergang="", Berichtstroomb="LWB", BerichtDatum="2018-08-01 00:00:00.000000", PoortDatum="2018-07-25 11:41:52.979000", Van="COS ", Naar="BVR", volgNr="2", kanaal="PAPER", tijdvak="2015", gdl="012789", Geval="f63283728fee11e889270ae51daf0000", OMG="TA03", FLW="AP_VDB_IN" Berichtstroomb = LWB kanaal = PAPER
>	7/25/18 11:40:12.670 AM	2018-07-25 11:40:12.670290, MHS="KTM", LogType="M", Gebeurtenis="", DomeinNaam="Ontvangen en Mededelen", WerkprocesNaam="Mededelen", ApplicatieNaam="MHS", MeetpunktLabel="COS-BVR", Procesovergang="", Berichtstroomb="LWB", BerichtDatum="2018-08-01 00:00:00.000000", PoortDatum="2018-07-25 11:40:11.038000", Van="COS ", Naar="BVR", volgNr="2", kanaal="PAPER", tijdvak="2015", gdl="012789", Geval="ba342c408fee11e889270ae51daf0000", OMG="TA03", FLW="AP_VDB_IN" Berichtstroomb = LWB kanaal = PAPER
>	7/25/18 11:21:07.244976	2018-07-25 11:21:07.244976, MHS="KTM", LogType="M", Gebeurtenis="9364b2887cdc43ca97c4d6550b639eb5", DomeinNaam="Ontvangen en Mededelen", WerkprocesNaam="Mededelen", ApplicatieNaam="MHS", MeetpunktLabel="COS-BVR", Procesovergang="", Berichtstroomb="LWB", BerichtDatum="2018-08-01 00:00:00.000000", PoortDatum="2018-07-25 11:21:07.244976", Van="COS ", Naar="BVR", volgNr="2", kanaal="PAPER", tijdvak="2015", gdl="012789", Geval="9364b2887cdc43ca97c4d6550b639eb5", OMG="TA03", FLW="AP_VDB_IN" Berichtstroomb = LWB kanaal = PAPER

De gevonden Events zijn verdeeld over meerdere pagina's.
Splunk zoekt altijd achteruit in de tijd, daarom:

2/10

Het Event met de jongste datum/tijd op pagina 1 bovenaan.

Het Event met de oudste datum/tijd op de laatste pagina onderaan.

List <input checked="" type="checkbox"/> Format 20 Per Page <input type="button" value="▼"/>		
i	Time	Event
>	10/5/17 2:24:28.451 PM	2017-10-05 14:24:28.451146,Gebeurtenis="",DomeinNaam="Ontvangen en Mededelen",WerkprocesNaam="Mededelen",ApplicatieNaam="MHS",MeetpuntLabel="COS-BVR",Geval="21d1aa02a9c811e782b50ae41c800000",Procesovergang="21ba42b8a9c811e7a0730ae41c800000",BerichtstroombewerktDatum="2016-03-24 00:00:00.000000",PoortDatum="2017-10-05 14:24:28.259000",QMMsgId="414d51205154414d425355313449312059b7402f215ca44",MsgLen="946",LenMQ="946",Van="COS",Naar="BVR",Flow="AP_XDB_START",FlowUit="2017-10-05 14:24:29.120915",FlowDL="669769",FlowStart="mhs-mhs",FlowEinde="service-request",VorigDL="48146",volgNr="2",gd1="012686",tijdvak="2016",kanaal="EBMS",LogType="M",LogSeq="1" host = tambsu14 source = /var/mqsi/log/mhs/T01MHS3QMHSGENERIEK2/mhs-splunk.log sourcetype = mhs:keten
>	10/5/17 2:24:28.354 PM	2017-10-05 14:24:28.354663,Gebeurtenis="",DomeinNaam="Ontvangen en Mededelen",WerkprocesNaam="Mededelen",ApplicatieNaam="MHS",MeetpuntLabel="COS-BVR",Geval="21c76358a9c811e782b50ae41c800000",Procesovergang="",BerichtstroombewerktDatum="2016-10-26 00:00:00.000000",PoortDatum="2017-12-17 11:30:47.000000",QMMsgId="414d51205154414d425355313449312059b7402f2115ca2f",MsgLen="855",LenMQ="855",Van="COS",Naar="BVR",Flow="AP_VDB_IN",FlowUit="2017-10-05 14:24:29.112041",FlowDL="757378",FlowStart="mhs-mhs",FlowEinde="service-request",VorigDL="19663",volgNr="2",kanaal="PAPER",gd1="012493",tijdvak="2016",LogType="M",LogSeq="1" host = tambsu14 source = /var/mqsi/log/mhs/T01MHS3QMHSGENERIEK2/mhs-splunk.log sourcetype = mhs:keten
>	10/5/17 2:24:27.953 PM	2017-10-05 14:24:27.953757,Gebeurtenis="",DomeinNaam="Ontvangen en Mededelen",WerkprocesNaam="Mededelen",ApplicatieNaam="MHS",MeetpuntLabel="COS-BVR",Geval="20ba43fea9c811e79c980ae41c800000",Procesovergang="",BerichtstroombewerktDatum="2015-01-01 00:00:00.000000",PoortDatum="2017-10-05 14:24:26.571763",QMMsgId="414d51205154414d425355313449312059b7402f2115b5de",MsgLen="1229",LenMQ="1229",Van="COS",Naar="BVR",Flow="ANBI_MEDD_T1",FlowUit="2017-10-05 14:24:28.304150",FlowDL="350393",FlowStart="mhs-mhs",FlowEinde="service-request",VorigDL="10656",volgNr="3",kanaal="PAPER",gd1="001160",tijdvak="2015",LogType="M",LogSeq="1" host = tambsu14 source = /var/mqsi/log/mhs/T01MHS3QMHSGENERIEK2/mhs-splunk.log sourcetype = mhs:keten

Als je met de muiscursor over een Event beweegt,
dan gaat een gedeelte ervan oplichten:

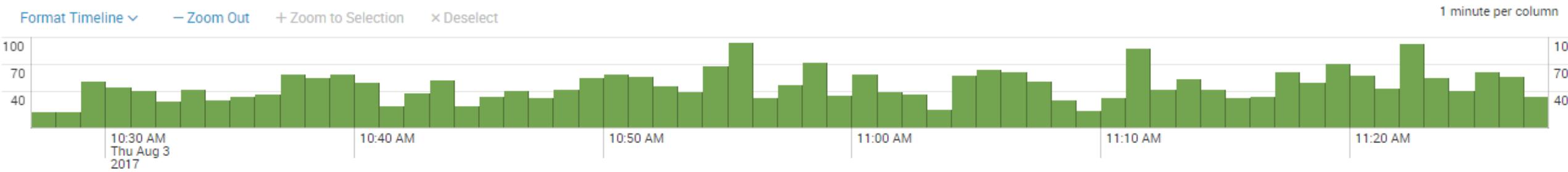
> 10/5/17 2017-10-05 14:24:28.451146,Gebeurtenis="",DomeinNaam="Ontvangen en Mededelen",WerkprocesNaam="Mededelen",ApplicatieNaam="MHS",MeetpuntLabel="COS-BVR",Geval="21d1aa02a9c811e782b50ae41c800000",Procesovergang="21ba42b8a9c811e7a0730ae41c800000",Berichtstroom="CVU",BerichtDatum="2016-03-24 00:00:00.000000",PoortDatum="2017-10-05 14:24:28.259000",QMsgId="414d51205154414d425355313449312059b7402f215ca44",MsgLen="946",LenMQ="946",Van="COS",Naar="BVR",Flow="AP_XDB_START",FlowUit="2017-10-05 14:24:29.120915",FlowDL="669769",FlowStart="mhs-mhs",FlowEinde="service-request",VorigDL="48146",volgNr="2",gd1="012686",tijdvak="2016",kanaal="EBMS",LogType="M",LogSeq="1"
host = tamsbu14 source = /var/mqsi/log/mhs/T01MHS3QMHSGENERIEK2/mhs-splunk.log sourcetype = mhs:keten
> 10/5/17 2017-10-05 14:24:28.354663,Gebeurtenis="",DomeinNaam="Ontvangen en Mededelen",WerkprocesNaam="Mededelen",ApplicatieNaam="MHS",MeetpuntLabel="COS-BVR",Geval="21c76358a9c811e782b50ae41c800000",Procesovergang="",Berichtstroom="BHD",BerichtDatum="2016-10-26 00:00:00.000000",PoortDatum="2017-12-17 11:30:47.000000",QMsgId="414d51205154414d425355313449312059b7402f2115ca2f",MsgLen="855",LenMQ="855",Van="COS",Naar="mhs",FlowEinde="service-r
Add to search
Exclude from search
New search
host = tamsbu14 source = /var/mqsi/log/mhs/T01MHS3QMHSGENERIEK2/mhs-splunk.log sourcetype = mhs:keten
> 10/5/17 2017-10-05 14:24:27.95375,Gebeurtenis="",DomeinNaam="Ontvangen en Mededelen",WerkprocesNaam="Mededelen",ApplicatieNaam="MHS",MeetpuntLabel="COS-BVR",Geval="20ba43fea9c811e79c980ae41c800000",Procesovergang="",Berichtstroom="ANB",BerichtDatum="2015-01-01 00:00:00.000000",PoortDatum="2017-10-05 14:24:26.571763",QMsgId="414d51205154414d425355313449312059b7402f2115b5de",MsgLen="1229",LenMQ="1229",Van="COS",Naar="BVR",Flow="ANBI_MEDD_T1",FlowUit="2017-10-05 14:24:28.304150",FlowDL="350393",FlowStart="mhs-mhs",FlowEinde="service-request",VorigDL="10656",volgNr="3",kanaal="PAPER",gd1="001160",tijdvak="2015",LogType="M",LogSeq="1"
host = tamsbu14 source = /var/mqsi/log/mhs/T01MHS3QMHSGENERIEK2/mhs-splunk.log sourcetype = mhs:keten

Door nu op de linker muisknop te drukken krijg je de mogelijkheid om:

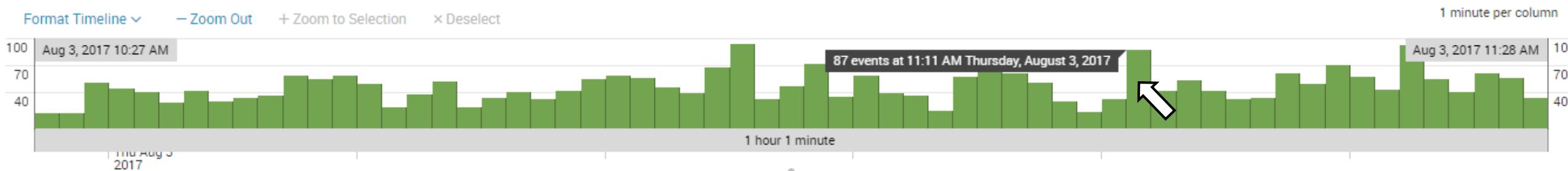
- De Search aan te passen zodat alleen Events met het geselecteerde overblijven
- De Search aan te passen zodat alleen Events zonder het geselecteerde overblijven
- Een geheel nieuwe Search te starten, waarbij je alleen zoekt op het geselecteerde

De Timeline toont een verdeling van de gevonden Events over de zoekperiode:

4/10



Beweeg met de muiscursor over de Timeline voor meer informatie:

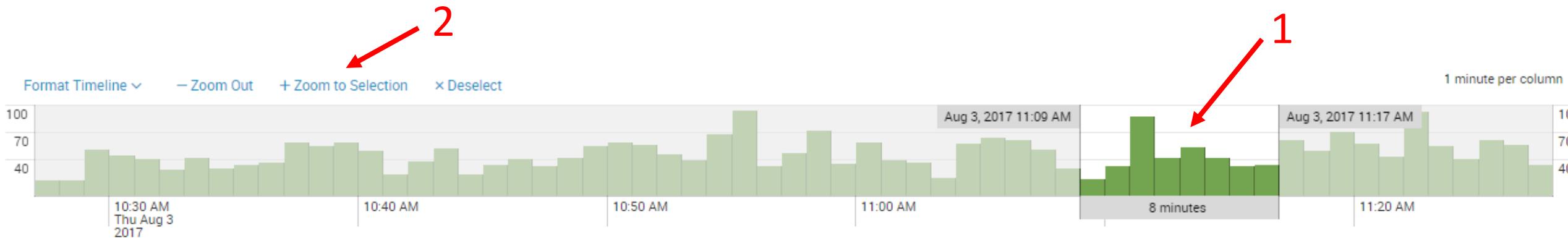


Je kunt de Search beperken tot een kleiner deel van de Timeline.

5/10

Ga hiervoor met de muiscursor in de Timeline staan. Druk op de linkermuisknop, houd deze knop ingedrukt en verplaats de muiscursor om een aaneengesloten gedeelte van de Timeline te selecteren. Laat vervolgens de muisknop los (1).

Klik hierna op *Zoom to Selection* om alleen de Events van het geselecteerde gebied over te houden (2)



Fields zijn variabelen:

6/10

Een Field heeft een naam en, per Event, een bepaalde waarde (of is leeg).

Fields worden door Splunk afgeleid door te zoek naar key-value pairs in de gevonden Events.

Fields →

Events

> 11/9/17 2:45:54.495 PM	2017-11-09 14:45:54.495, Gebeurtenis="RB0000000000000000000000781107441", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP3", Geval="", Procesovergang="", BERICHTSOORTCODE="RB024"
> 11/9/17 2:45:54.492 PM	2017-11-09 14:45:54.492, Gebeurtenis="RB0000000000000000000000781107441", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP10", Geval="", Procesovergang=""
> 11/9/17 2:45:54.488 PM	2017-11-09 14:45:54.488, Gebeurtenis="RB0000000000000000000000781107441", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP12", Geval="", Procesovergang="", MededelingId="496306430AE50B37153D4FFAEE491D7A", SoortMededeling="DNI02", Referentie="496306430AE50B37153D4FFAEE491D7A"
> 11/9/17 2:45:54.210 PM	2017-11-09 14:45:54.21, Gebeurtenis="RB0000000000000000000000781107441", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP1", Geval="", Procesovergang="", BERICHTSOORTCODE="RB024"
> 11/9/17 2:45:30.240 PM	2017-11-09 14:45:30.240, Gebeurtenis="8c8a42f6a011415685d36d8d78103b5a", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP13", Geval="", Procesovergang="", Berichtsoortcode="DNI03", Referentie="3ED194ED0AE50FB3B188537A42ACDE9F"
> 11/9/17 2:45:20.281 PM	2017-11-09 14:45:20.281, Gebeurtenis="RB0000000000000000000000781107428", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP3", Geval="", Procesovergang="", BERICHTSOORTCODE="RB024"
> 11/9/17 2:45:20.277 PM	2017-11-09 14:45:20.277, Gebeurtenis="RB0000000000000000000000781107428", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP10", Geval="", Procesovergang=""

Selected Fields

= Lijstje met favoriete Fields
(geselecteerd door Splunk of gebruiker)

Interesting Fields

= Fields waarvan Splunk denkt dat ze ook interessant kunnen zijn voor de gebruiker

All Fields

Druk op deze knop om een overzicht te krijgen van alle beschikbare Fields

	< Hide Fields	All Fields
Selected Fields		
a host	7	
a index	1	
a source	8	
a sourcetype	1	
Interesting Fields		
a Adapter	4	
a ApplicatieNaam	1	
# BBA	1	
a BerichtDatum	8	
a Berichtstroomb	9	
# date_hour	2	
# date_mday	1	
# date_minute	41	
a date_month	1	

Een *a* voor een Field betekent dat het Field alfanumerieke waarden bevat

Een # voor een Field betekent dat het Field numerieke waarden bevat

Het getal achter een Field geeft aan hoeveel verschillende waarden er in het Field voorkomen (in de verzameling gevonden Events)

100+ betekent meer dan 100

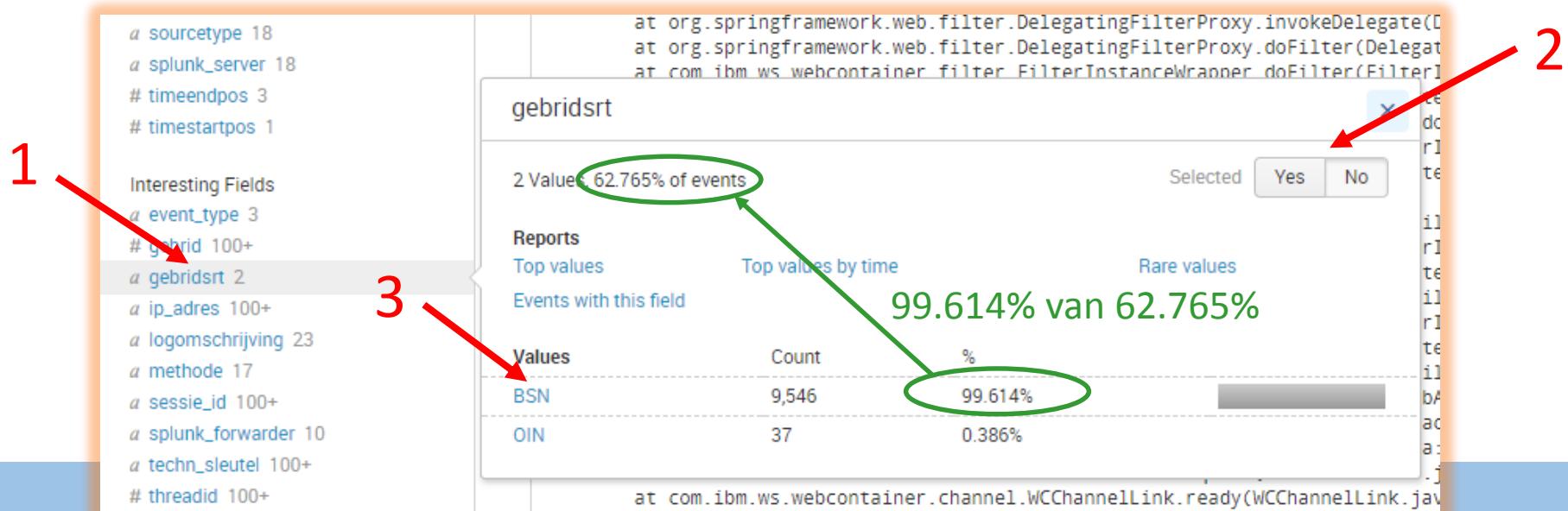
```
# belangh_id 100+
a event_type 2
# gebr_id 100+
a hulpmiddel_versienr 49
a ip_adres 100+
a kanaal 1
a result 6
```

Bij de lijstjes Selected Fields en Interesting Fields geldt:

9/10

Klik op een Field om het Field window te openen (1). Dit window geeft informatie over de voorkomende Field waarden en hun frequenties. Ook kun je een Field selected of juist niet-selected maken (2).

Door in het Field window op een Field waarde te klikken, kun je de zoekopdracht hiermee uitbreiden (3).



- Als je op **All Fields** klikt, dan opent het Select Fields window. Dit window bevat een overzicht van ALLE beschikbare Fields.

10/10

The screenshot shows the 'Select Fields' window from Splunk. The title bar says 'varieer de coverage!' and has a close button 'x'. At the top left are buttons for 'Select All Within Filter' and 'Deselect All'. In the center is a dropdown labeled 'Coverage: 100%' with a green oval around it. To its right is a search bar with the placeholder 'filter'. On the far right is a blue link '+ Extract New Fields'. The main area is a table with the following data:

	Field	# of Values	Event Coverage	Type
>	date_hour	24	100%	Number
>	date_mday	2	100%	Number
>	date_minute	60	100%	Number
>	date_month	1	100%	String
>	date_second	60	100%	Number
>	date_wday	2	100%	String
>	date_year	1	100%	Number
>	date_zone	1	100%	String
>	host	12	100%	String
>	index	1	100%	String
>	linecount	5	100%	Number

Met de vinkjes kun je Fields aan het lijstje Selected Fields toevoegen of uit dit lijstje verwijderen.

Tabblad Statistics

Als de Search een commando heeft die een tabel oplevert, dan verschijnt deze tabel op dit tabblad

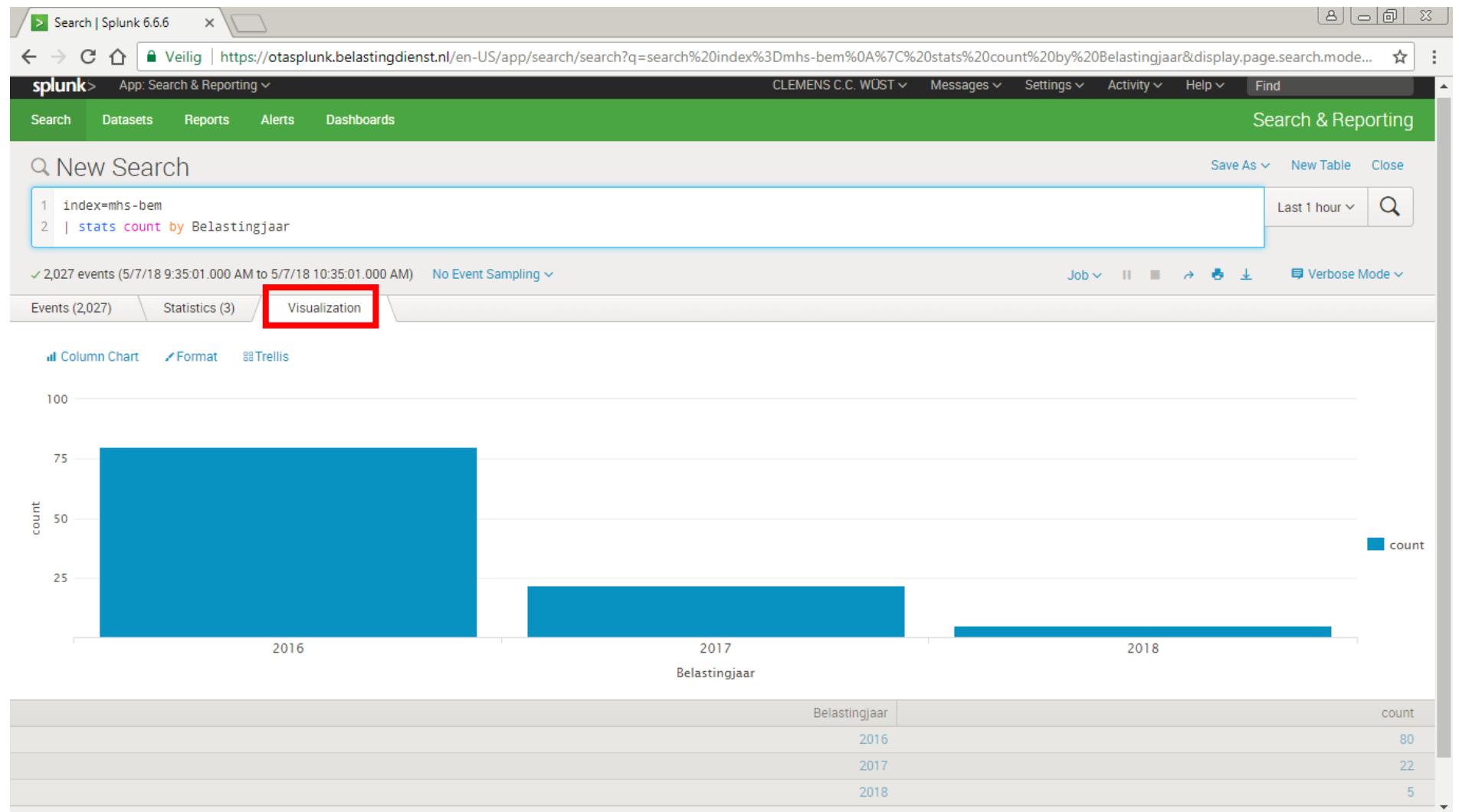
The screenshot shows the Splunk web interface with the title "Search | Splunk 6.6.6". The URL in the address bar is <https://otaspunk.belastingdienst.nl/en-US/app/search/search?q=search%20index%3Dmhs-bem%0A%7C%20stats%20count%20by%20Belastingjaar&display.page.search.mode...>. The top navigation bar includes links for User Profile, Logout, Home, App: Search & Reporting, CLEMENS C.C. WÜST, Messages, Settings, Activity, Help, and Find. Below the navigation is a green header bar with tabs for Search, Datasets, Reports, Alerts, and Dashboards, and a "Search & Reporting" label. A search bar contains the query: 1 index=mhs-bem 2 | stats count by Belastingjaar. To the right of the search bar are buttons for Save As, New Table, Close, and Last 1 hour. The main content area shows a search summary: 2,027 events (5/7/18 9:35:01.000 AM to 5/7/18 10:35:01.000 AM) with No Event Sampling. Below this are three tabs: Events (2,027), Statistics (3) (which is highlighted with a red box), and Visualization. Under the Statistics tab, there are buttons for 100 Per Page, Format, and Preview. A table displays the results:

Belastingjaar	count
2016	80
2017	22
2018	5

At the bottom of the page are links for About, Support, File a Bug, Documentation, and Privacy Policy, along with a copyright notice: © 2005-2018 Splunk Inc. All rights reserved.

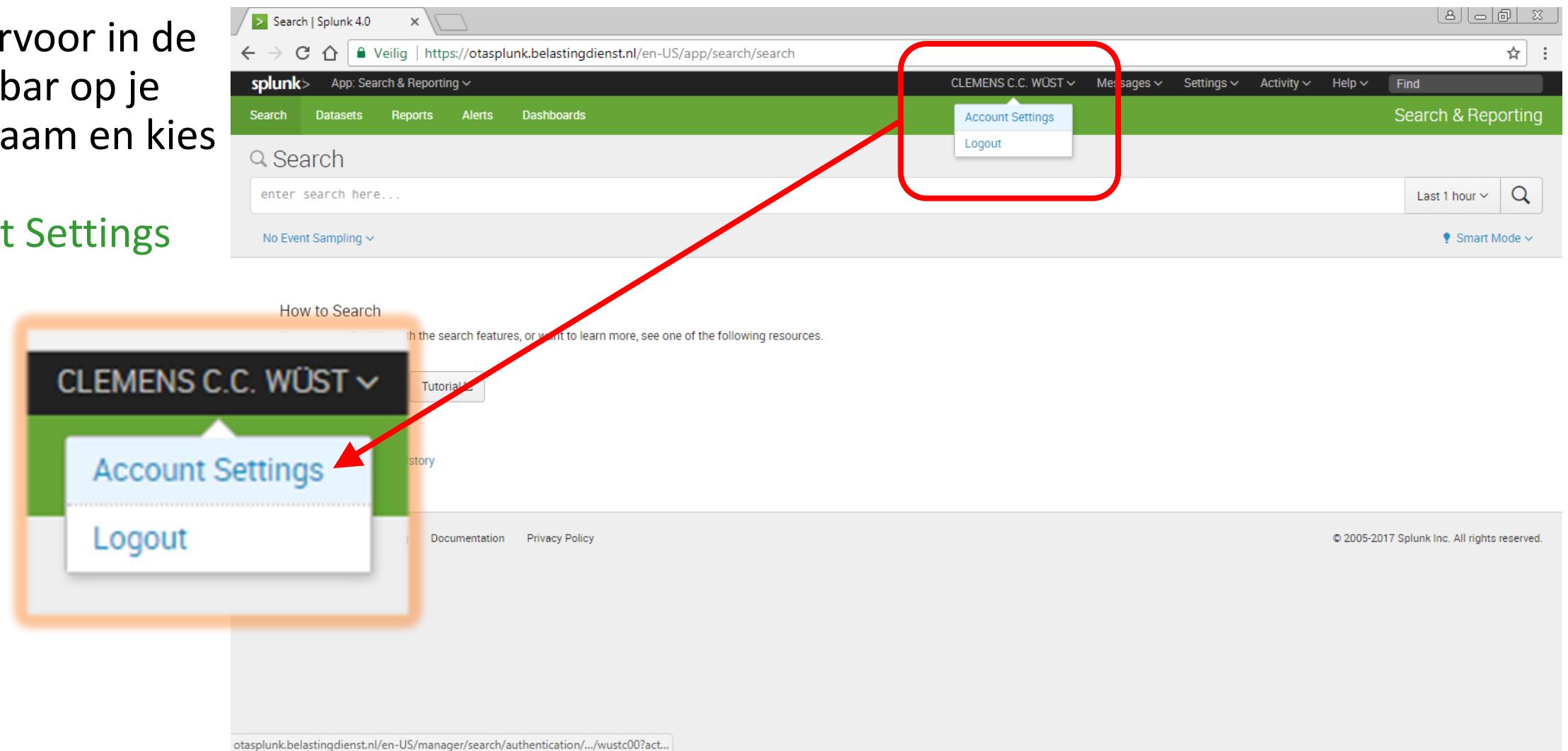
Tabblad Visualization

Als de Search een commando heeft die een grafiek oplevert, dan verschijnt deze tabel op dit tabblad



Aanpassen van gebruikersinstellingen

Klik hiervoor in de Splunk bar op je eigen naam en kies voor
Account Settings



Wat kun als gebruiker instellen?

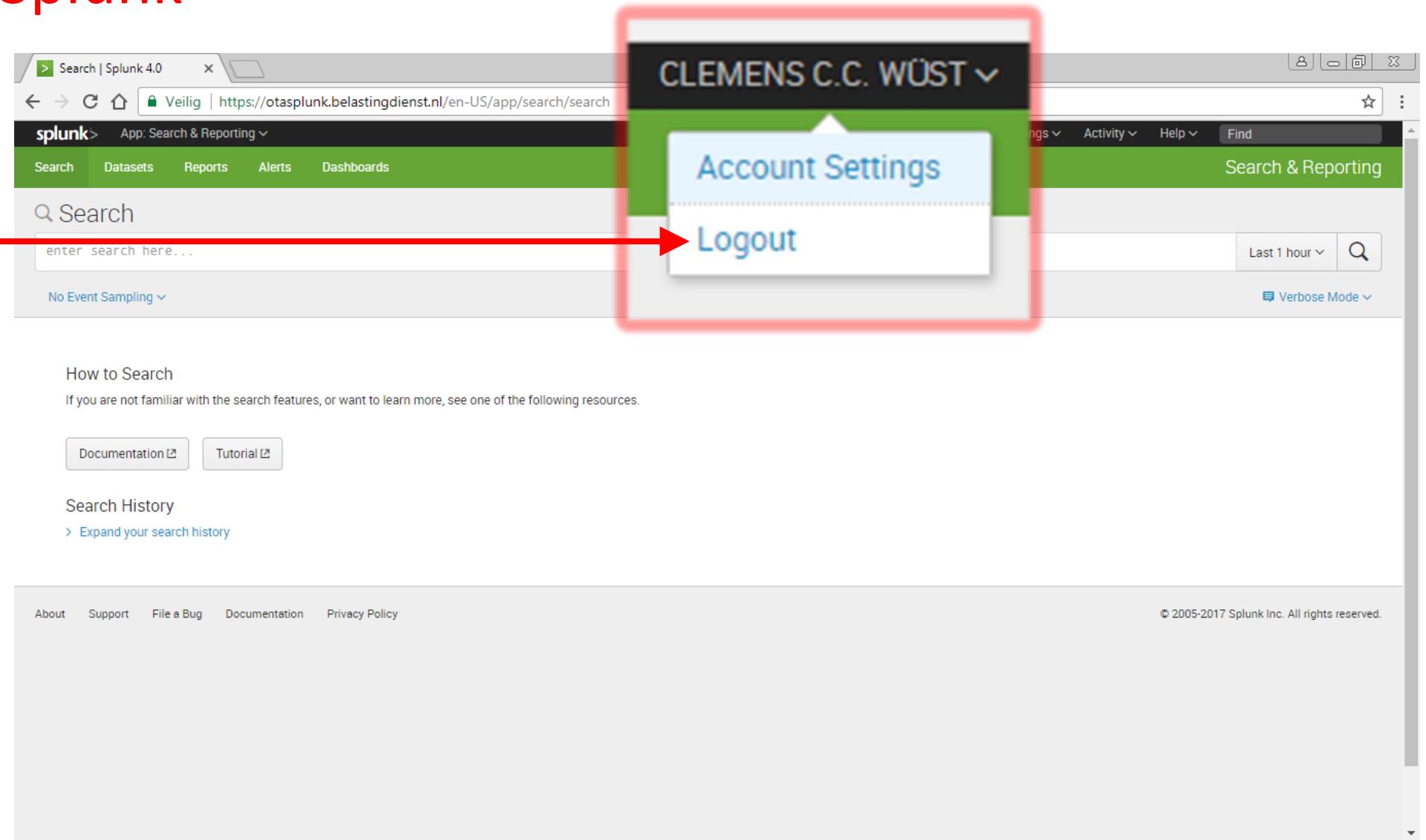
- Tijdzone
- De keuze voor een default App
- Search Bar instellingen, zoals syntax highlighting en regelnummers
- ...

The screenshot shows the 'Settings | Splunk' interface for a user named 'wustc00'. The URL is https://otaspunk.belastingdienst.nl/en-US/manager/search/authentication/changepassword/wustc00?action=edit. The page includes a navigation bar with 'splunk', 'Apps', and user information 'CLEMENS C.C. WÜST'. Below the navigation is a breadcrumb trail 'Users » wustc00'. The main content area contains several sections:

- Personal**: Fields for 'Full name' (CLEMENS C.C. WÜST) and 'Email address' (cc.wust@belastingdienst.nl).
- Set password**: Fields for 'Password' and 'Confirm password'.
- Global**: A dropdown for 'Time zone' set to '-- Default System Timezone --'. A note says 'Set a time zone for this user.' Below it is a dropdown for 'Default application'.
- On restart**: A checked checkbox for 'Restart backgrounded jobs' with the note 'Restart background jobs when the Splunk software is restarted.'
- Search**: A note: 'Use these properties for assistance with command syntax including examples, autocomplete syntax, or to turn off search assistant. Syntax highlighting displays search string components.'

Afsluiten van Splunk

Klik hiervoor in de Splunk bar op je eigen naam en kies voor Logout



Cursus Splunk

Module 2:
Opstellen van een basis Search

De structuur van een Search

Structuur van een Search (= zoekopdracht)

1/7

Een Search bestaat uit een **basis** en nul of meer **commando's**:

<basis> | <commando> ... | <commando>

<basis> is de basis van de Search

Hiermee wordt gericht naar bepaalde Events in de logdata gezocht.

Voor de gevonden Events worden door Splunk Fields afgeleid.

Resultaat: een verzameling Events en een verzameling Fields.

Dit commando wordt uitgevoerd voor ieder Event in de verzameling

Als gevolg van een commando kan de verzameling Events en/of de verzameling Fields worden aangepast. Er is een commando om Events te sorteren, om Events uit te filteren, om een nieuw Field te introduceren, etc.

Een commando begint altijd met een pipe-teken |

Splunk werkt alle opgegeven commando's in een Search sequentieel af, van pipe teken naar pipe teken.

Een gewenste bewerking kan vaak op verschillende manieren worden geprogrammeerd. Denk altijd na over de efficiëntie van je Search.

Voorbeeld:

niet efficiënt:

```
index=oldv-business sourcetype=OTS:GOS
```

```
| sort 0 belastingjaar
```

```
| where belastingjaar>2016
```

wel efficiënt:

```
index=oldv-business sourcetype=OTS:GOS belastingjaar>2016
```

```
| sort 0 belastingjaar
```

Voorbeeld: Een verzameling Events gevonden in een Basis Search

4/7

>	11/9/17 2:45:54.495 PM	2017-11-09 14:45:54.495, Gebeurtenis="RB0000000000000000000000781107441", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP3", Geval="", Procesovergang="", BERICHTSOORTCODE="RB024"
>	11/9/17 2:45:54.492 PM	2017-11-09 14:45:54.492, Gebeurtenis="RB0000000000000000000000781107441", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP10", Geval="", Procesovergang=""
>	11/9/17 2:45:54.488 PM	2017-11-09 14:45:54.488, Gebeurtenis="RB0000000000000000000000781107441", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP12", Geval="", Procesovergang="", MededelingId="496306430AE50B37153D4FFAEE491D7A", SoortMededeling="DNI02", Referentie="496306430AE50B37153D4FFAEE491D7A"
>	11/9/17 2:45:54.210 PM	2017-11-09 14:45:54.21, Gebeurtenis="RB0000000000000000000000781107441", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP1", Geval="", Procesovergang="", BERICHTSOORTCODE="RB024"
>	11/9/17 2:45:30.240 PM	2017-11-09 14:45:30.240, Gebeurtenis="8c8a42f6a011415685d36d8d78103b5a", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP13", Geval="", Procesovergang="", Berichtsoortcode="DNI03", Referentie="3ED194ED0AE50FB3B188537A42ACDE9F"
>	11/9/17 2:45:20.281 PM	2017-11-09 14:45:20.281, Gebeurtenis="RB0000000000000000000000781107428", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP3", Geval="", Procesovergang="", BERICHTSOORTCODE="RB024"
>	11/9/17 2:45:20.277 PM	2017-11-09 14:45:20.277, Gebeurtenis="RB0000000000000000000000781107428", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP10", Geval="", Procesovergang=""

Voorbeeld: De verzameling Fields die uit deze Events is afgeleid

5/7

Events



Fields (enkele geselecteerd) →

DomeinNaam	WerkprocesNaam	MeetpuntLabel	BERICHTSOORTCODE
Aanslag	Uitnodigen	MP3	RB024
Aanslag	Uitnodigen	MP10	
Aanslag	Uitnodigen	MP12	
Aanslag	Uitnodigen	MP1	RB024
Aanslag	Uitnodigen	MP13	DNI03
Aanslag	Uitnodigen	MP3	RB024
Aanslag	Uitnodigen	MP10	

Voorbeeld: Aanvullende commando's

6/7

| head 4

| eval MeetpuntLabel2 = MeetpuntLabel + "_" + BERICHTSOORTCODE

Fields (enkele geselecteerd) →

Events ↓

DomeinNaam	WerkprocesNaam	MeetpuntLabel	BERICHTSOORTCODE	MeetpuntLabel2
Aanslag	Uitnodigen	MP3	RB024	MP3_RB024
Aanslag	Uitnodigen	MP10		MP10_
Aanslag	Uitnodigen	MP12		MP12_
Aanslag	Uitnodigen	MP1	RB024	MP1_RB024
Aanslag	Uitnodigen	MP13	DNI03	
Aanslag	Uitnodigen	MP3	RB024	
Aanslag	Uitnodigen	MP10		

Om een Search uit te voeren is het verder noodzakelijk:

7/7

- Om de zoekperiode op te geven
- Om een Search Mode op te geven

In deze module behandelen we

- Het opstellen van een basis Search
- Het invoeren van de zoekperiode
- Het kiezen van een Search Mode

Pas in Module 3 gaan we een basis Search aanvullen met commando's

Opstellen van een basis Search

Een basis Search (= zoekopdracht) levert het volgende op:

- Een verzameling Events
- Een verzameling Fields

Fields zijn variabelen:

Een Field heeft een naam en per Event een bepaalde waarde (of is leeg)

Voorbeeld:

Field naam	Field waarde voor Event x	Field waarde voor Event y
sourcetype	OTS:verkrijgen_toegang	OTS:GOS
gebr_id_srt	BSN	leeg

- 1 Standaard Fields. Deze Fields ontstaan bij iedere basis Search, onafhankelijk van welke Events worden gevonden.

`_raw , _time, host, index, linecount, punct, source, sourcetype, splunk_server, timestamp, date_hour, date_mday, date_minute, date_month, date_second, date_wday, date_year, date_zone`

- 2 Aanvullend worden Fields afgeleid uit de gevonden Events.
Ieder key-value pair x=y leidt tot een Field met naam x.

```
11/1/17      2017-11-01 17:05:24.504556,Gebeurtenis="",DomeinNaam="Ontvangen en Mededelen",WerkprocesNaam="Ontvangen",ApplicatieNaam="MHS",MeetpunktLabel="BSM-END",Geval="",Procesovergang="",MsgLen="183165",Van="BSM",Naar="END",LogType="S",LogSeq="1",Flow="BVR_Stub",FlowDL="473962",QM="QOLMBSU0801",MQid="414d5120514f4c4d42535530384f31205973058a2ba82390"
```

Er ontstaan dus Fields: **Gebeurtenis**, **DomeinNaam**, **WerkprocesNaam**, ...

Een basis Search bestaat uit één of meer zoektermen.

Er zijn twee soorten zoektermen:

1 In de vorm van een **Field naam = Field waarde** paar

Voorbeeld: `actie=verzenden, bedrag=23, limiet=5923`

Voorbeeld: `actie!=verzenden, bedrag>23`

2 In de vorm van een losse waarde

Voorbeeld: `actie, "IH 2016", 517`

- Field namen zijn case-sensitive.
Losse waarden en Field waardes zijn NIET case-sensitive.
- Als een Field naam of Field waarde een spatie bevat, dan moeten er in de zoekterm dubbele aanhalingstekens omheen gezet worden
Dit mag je ook doen als de Field naam of Field waarde geen spaties bevat
- Een joker (symbool: *) staat voor 0 of meer willekeurige karakters (geen spaties!). **Vermijd het gebruik van * in het midden van een zoekterm (dit kan overwachte resultaten geven)!**

Voorbeeld: Zoektermen van type Field naam = Field waarde

3/4

Zoekterm	Splunk zoekt naar Events waar een Field berichtsoort in voorkomt met een gehele waarde als bijvoorbeeld:
berichtsoort>=86	780, 1191, 25336 (maar bijv. niet 86AHA)
berichtsoort=aaNGIfte	aangifte, Aangifte, AANGIFTE
Berichtsoort="Aangifte 2016"	Splunk zoekt niet naar Field berichtsoort , maar naar Field Berichtsoort . Dat Field moet een waarde hebben als bijvoorbeeld aangifte 2016, AANGIFTE 2016, aAnGiFtE 2016.
berichtsoort="Aangifte 20*"	Aangifte 2014, AANGIFTE 20Koala
berichtsoort=*20*	3220, abc20, 20DEF, Miner2049er

Voorbeeld: Zoektermen van type losse waarde

4/4

Zoekterm	Splunk zoekt naar Events waar een gehele waarde in voorkomt als bijvoorbeeld:
86*	86, 860, 86AHA (maar bijv. niet 89)
ActiE	actie, Actie, ACTIE, ActiE
"speciale actie"	speciale actie, Speciale Actie, SPECIALE ACTIE
act*	act, Actie, Action, ACTIEPRIJS
ACT	act, Actie, Action, ACTIEPRIJS, pact, React, REACTOR
"Aangifte 20*"	aangifte 2015, Aangifte 2016, AANGIFTE 20LR

Verschil tussen != en NOT

- Een zoekterm field != waarde levert Events op waarvoor field èn gevuld is èn niet de opgegeven waarde heeft.
- Een zoekterm NOT field = waarde levert Events op waarvoor field òf leeg is òf niet de opgegeven waarde heeft.
- Het gebruik van != en NOT is niet efficiënt. Doe dit zo min mogelijk.

Een basis Search bestaat uit één of meer zoektermen

- Begin met een zoekterm voor Field **index**.
- Voeg een zoekterm toe voor Field **sourcetype**.
- Voeg verder zoektermen toe om in te zoomen op de Events die je wilt hebben.

Voorbeeld:

**index=oldv-business sourcetype=OTS:GOS actie=verzenden
belastingjaar=2016**

- Zoektermen kunnen worden gecombineerd d.m.v. de logische operatoren OR en NOT en haakjes ()

2/3

Voorbeeld:

zoekterm1 zoekterm2 ((NOT zoekterm3) OR zoekterm4)

- De logische operator AND is impliciet

Voorbeeld:

zoekterm1 zoekterm2 *is equivalent met* zoekterm1 AND zoekterm2

- `index=oldv-business sourcetype=OTS:verkrijgen_toegang dienstcode=IBAangifte2015 bedrag>6502`
- `index=oldv-business sourcetype=OTS:verkrijgen_toegang (dienstcode=IBAangifte2015 OR dienstcode=IBAangifte2016)`
- `(index=oldv-business OR index=oldv-appl) aangifte`
- `index=oldv-business (NOT dienstcode=*)`

Invoeren van de zoekperiode

Soorten tijd

Absolute Time

Een hardcoded tijdwaarde. Bijv. 1 mei 2018 12:00.

Relative Time

Een tijdwaarde in relatieve termen, zoals *15 minuten geleden*. Bij het starten van een Search wordt de tijdwaarde geëvalueerd. Bijv. als een Search wordt gestart op 1 mei 2018 om 15:10, dan levert *15 minuten geleden* de tijdwaarde 1 mei 2018 14:55.

Soorten Searches

Absolute Search

Het begin en het einde van de zoekperiode zijn beide Absolute times

Relative Search

Het begin en einde van de zoekperiode zijn beide Relative Times, of de een is een Relative Time en de ander een Absolute Time

Time Range Picker

The screenshot shows the Splunk Time Range Picker interface. On the left, there's a sidebar with a tree view:

- Presets (selected)
- Real-time
- 30 second window
- 1 minute window
- 5 minute window
- 30 minute window
- 1 hour window
- All time (real-time)

In the main area, there are three tabs at the top:

- Relative (selected)
- Today
- Last 15 minutes

The Relative tab has a dropdown menu:

- Earliest: 1 Hour
- No Snap-to
- Beginning of 7/26/17 3:18:34.000

The Date & Time Range section at the bottom contains:

- Between ▾
- 07/26/2017 15:18:34.000 HH:MM:SS.SSS
- and
- 07/26/2017 16:18:34.000 HH:MM:SS.SSS
- Apply

Kiezen van een Search Mode

Kiezen van een Search Mode

Een Search kan op drie verschillende manieren worden uitgevoerd:



A screenshot of the Splunk search interface is shown at the top. It features a search bar with the query "index=mhs-bem sourcetype=mhs:keten Berichtstroomb=OB", a time range selector set to "Last 1 hour", and a search button. Below the search bar are two mode selection buttons: "No Event Sampling" and "Verbose Mode". A red arrow points from the "Search Mode" column header in the table below to the "No Event Sampling" button.

Search Mode	Tijdens de basis Search worden Fields afgeleid uit de gevonden Events	Bij een Search die een tabel oplevert (tabblad Statistics) of een grafiek oplevert (tabblad Visualization), is tabblad Events ook beschikbaar
Verbose Mode	JA	JA
Smart Mode	JA	NEE
Fast Mode	NEE	NEE

Cursus Splunk

Module 3:
Aanvullen van een basis Search met commando's

Expressies

Commando's maken vaak gebruik van **expressies**

Een **numerieke expressie** levert een numerieke waarde op

Voorbeeld: `(Kosten + 10) * 0.21`

Bij concateneren of tekstfuncties, gebruik altijd dubbele aanhalingstekens om hardcoded tekst heen!

Een **alfanumerieke expressie** levert een alfanumerieke waarde op

Voorbeeld: `"Meetpunt " + substr(MeetpuntLabel, 3, 2)`

Een **logische expressie** levert een logische waarde op (True of False)

Voorbeeld: `MeetpuntLabel2 != MP09`

Componenten waaruit expressies kunnen worden opgebouwd:
hardcoded waarden, Fields, operatoren, functies, haakjes

Gegeven een Event met de volgende Fields en Field waarden:

a = 7.52, b = 8, c = "basta", d = 1, e = 3, f = 2

Dan leveren de volgende expressies de volgende resultaten op:

- $(\text{round}(a) * 10) + b \rightarrow 88$ numerieke expressie
- "De eerste de " + replace(c,"a","e") + "!"
 \rightarrow "De eerste de beste!" alfanumerieke expressie
- NOT ((d < e) OR (e > f)) \rightarrow False logische expressie

Commando's

Categorie: Het beïnvloeden van Events

Sorteren van Events: commando sort

1/4

Met het commando **sort** kunnen Events worden gesorteerd op (de waarden van) één of meer Fields:

| sort <één of meer Fields gescheiden door spaties of komma's>

- De Events worden gesorteerd op (de waarden van) het eerste Field
- Als een tweede Field is genoemd, dan worden (binnen de sortering op het eerste Field) alle Events waarvoor (de waarde van) het eerste Field hetzelfde is, gesorteerd op (de waarden van) het tweede Field
- Etcetera

- Plak een + / - voor een Field om oplopend / aflopend op de waarden van dat Field te sorteren. De + is optioneel.

2/4

Voorbeeld: | sort +actie *is equivalent aan:* | sort actie

Voorbeeld: | sort -tijdvak

- Default levert het sort commando nà sortering maximaal 10,000 Events op. Om nà sortering maximaal n Events over te houden, zet de waarde n tussen het sort commando en het eerste Field. Gebruik $n=0$ voor alle Events.

Voorbeeld: | sort 5 -actie +tijdvak

Equivalent: | sort limit=5 -actie +tijdvak

- Als een Field waarop je sorteert leeg is voor één of meer Events, dan komen deze Events in de sorteervolgorde helemaal achteraan. Hierbij maakt het niet uit of je oplopend of aflopend sorteert!

Voorbeeld: Basis Search

3/4

New Search

Save As ▾ New Table Close

index=douane-bem sourcetype=douane-process WerkprocesId!=MDD01 Last 1 hour

✓ 5 events (7/2/18 4:00:00.000 PM to 7/2/18 4:15:00.000 PM) No Event Sampling Job ▾ More Options Verbose Mode ▾

7/2/18 4:10:01.430 PM	Registratiemoment="20180702 16:10:01.430", BedrijfsprocesId="COPISA", WerkprocesId="OVD01", MeetpuntId="od4", ITservice="DBA", ITcomponent="UC100", Gevalstype="bericht", DouaneberichtId="760d03417b744feab38f7c4648be656f", Berichtstatus="1", Berichttype="DATA-COPIS-MSG", DouanecorrelatieId=""
7/2/18 4:10:01.285 PM	Registratiemoment="2018-07-02T14:10:01.285939Z", MeetpuntId="od2", ITService="HTD", Gevalstype="Bericht", WerkprocesId="Ontvangen digitaal", BedrijfsprocesId="ZGRA", DouaneberichtId="760d03417b744feab38f7c4648be656f", Stroom="COPISA"
7/2/18 4:09:06.518 PM	Registratiemoment="20180702 16:09:06.518", BedrijfsprocesId="SEED", WerkprocesId="OVD01", MeetpuntId="od4", ITservice="DBA", ITcomponent="UC100", Gevalstype="bericht", DouaneberichtId="aa010288410c4aac8ad79c6bb103d15d", Berichtstatus="1", Berichttype="IE713-MSG", DouanecorrelatieId=""
7/2/18 4:00:02.447 PM	Registratiemoment="20180702 16:00:02.447", BedrijfsprocesId="COPISA", WerkprocesId="OVD01", MeetpuntId="od4", ITservice="DBA", ITcomponent="UC100", Gevalstype="bericht", DouaneberichtId="6beb0ddce8e7449e8e8f4b9707a9c094", Berichtstatus="1", Berichttype="DATA-COPIS-MSG", DouanecorrelatieId=""
7/2/18 4:00:02.193 PM	Registratiemoment="2018-07-02T14:00:02.193333Z", MeetpuntId="od2", ITService="HTD", Gevalstype="Bericht", WerkprocesId="Ontvangen digitaal", BedrijfsprocesId="ZGRA", DouaneberichtId="6beb0ddce8e7449e8e8f4b9707a9c094", Stroom="COPISA"

Voorbeeld: Dezelfde basis Search + sort commando

4/4

New Search

Save As ▾ New Table Close

```
index=douane-bem sourcetype=douane-process WerkprocesId!=MDD01  
| sort 4 BedrijfsprocesId DouaneberichtId
```

Last 1 hour ▾

4 events (7/2/18 4:00:00.000 PM to 7/2/18 4:15:00.000 PM) No Event Sampling ▾ Job ▾ II ■ ▶ ↴ ↓ Verbose Mode ▾

7/2/18 4:00:02.447 PM	Registratiemoment="20180702 16:00:02.447", BedrijfsprocesId="COPISA", WerkprocesId="OVD01", MeetpuntId="od4", ITservice="DBA", ITcomponent="UC100", Gevalstype="bericht", DouaneberichtId="6beb0ddce8e7449e8e8f4b9707a9c094", Berichtstatus="1", Berichttype="DATA-COPIS-MSG", DouanecorrelatieId=""	
7/2/18 4:10:01.430 PM	Registratiemoment="20180702 16:10:01.430", BedrijfsprocesId="COPISA", WerkprocesId="OVD01", MeetpuntId="od4", ITservice="DBA", ITcomponent="UC100", Gevalstype="bericht", DouaneberichtId="760d03417b744feab38f7c4648be656f", Berichtstatus="1", Berichttype="DATA-COPIS-MSG", DouanecorrelatieId=""	
7/2/18 4:09:06.518 PM	Registratiemoment="20180702 16:09:06.518", BedrijfsprocesId="SEED", WerkprocesId="OVD01", MeetpuntId="od4", ITservice="DBA", ITcomponent="UC100", Gevalstype="bericht", DouaneberichtId="aa010288410c4aac8ad79c6bb103d15d", Berichtstatus="1", Berichttype="IE713-MSG", DouanecorrelatieId=""	
7/2/18 4:00:02.193 PM	Registratiemoment="2018-07-02T14:00:02.193333Z", MeetpuntId="od2", ITService="HTD", Gevalstype="Bericht", WerkprocesId="Ontvangen digitaal", BedrijfsprocesId="ZGRA", DouaneberichtId="6beb0ddce8e7449e8e8f4b9707a9c094", Stroom="COPISA"	

Met het commando **where** kunnen Events worden gefilterd:

| where <logische expressie>

- Als de expressie voor een Event de waarde True oplevert, dan wordt dat Event verder meegenomen (blijft in de verzameling)
- Als de expressie voor een Event de waarde False oplevert, dan wordt dat Event niet verder meegenomen (verdwijnt uit de verzameling)

Gebruik dit commando alleen als het echt nodig is. Probeer (vanuit efficiëntie oogpunt) zoveel mogelijk om Events in de basis Search te filteren met een extra zoekterm.

Voorbeeld: Basis Search

2/3

New Search

Save As ▾ New Table Close

index=mhs-bem sourcetype=mhs:keten

Last 1 hour ▾

✓ 7 events (7/25/18 12:10:00.000 PM to 7/25/18 12:15:00.000 PM) No Event Sampling ▾ Job ▾ More Options Download Print Copy Verbose Mode ▾

7/25/18 12:11:55.537 PM	2018-07-25 12:11:55.537092, MHS="IIB", DL="276817", BRK="BTAMBSU64A1", SRV="AMHS1048", APP="Beheer", QM="QTAMBSU64A1", LEN="0", TYP="OTH", IIB="GSF", OMG="TA01", FLW="Scheduler"
7/25/18 12:11:28.308 PM	2018-07-25 12:11:28.308127, MHS="IIB", DL="265989", BRK="BTAMBSU56I1", SRV="TMHS5048", APP="Beheer", QM="QTAMBSU56I1", LEN="0", TYP="OTH", IIB="GSF", END="normal", OMG="TST5", FLW="Scheduler", EventID="185899b08ff311e8b9020ae41c3b0000", EventVolgNr="1"
7/25/18 12:11:25.861 PM	2018-07-25 12:11:25.861757, MHS="IIB", DL="290588", BRK="BTAMBSU58I1", SRV="TMHS3048", APP="Beheer", QM="QTAMBSU58I1", LEN="0", TYP="OTH", IIB="GSF", END="normal", OMG="TST3", FLW="Scheduler", EventID="16e350848ff311e8bd510ae41c450000", EventVolgNr="1"
7/25/18 12:11:22.846 PM	2018-07-25 12:11:22.846531, MHS="IIB", DL="279298", BRK="BTAMBSU58I1", SRV="TMHS6048", APP="Beheer", QM="QTAMBSU58I1", LEN="0", TYP="OTH", IIB="GSF", END="normal", OMG="TST6", FLW="Scheduler", EventID="15173d2e8ff311e895fc0ae41c450000", EventVolgNr="1"
7/25/18 12:10:58.599 PM	2018-07-25 12:10:58.599414, MHS="IIB", DL="312809", BRK="BTAMBSU54I1", SRV="TMHS4048", APP="Beheer", QM="QTAMBSU54I1", LEN="0", TYP="OTH", IIB="GSF", OMG="TST4", FLW="Scheduler"
7/25/18 12:10:45.673 PM	2018-07-25 12:10:45.673708, MHS="IIB", DL="275386", BRK="BTAMBSU56I1", SRV="TMHS2048", APP="Beheer", QM="QTAMBSU56I1", LEN="0", TYP="OTH", IIB="GSF", OMG="TST2", FLW="Scheduler"
7/25/18 12:10:20.751 PM	2018-07-25 12:10:20.751395, MHS="IIB", DL="311632", BRK="BOLMBSU5401", SRV="OMHS1048", APP="Beheer", QM="QOLMBSU5401", LEN="0", TYP="OTH", IIB="GSF", END="normal", OMG="ONT5", FLW="Scheduler", EventID="f014431e8ff211e8b3b50ae21c300000", EventVolgNr="1"

Voorbeeld: Dezelfde basis Search + where commando

3/3

New Search

Save As ▾ New Table Close

```
index=mhs-bem sourcetype=mhs:keten  
| where DL>300000
```

Last 1 hour ▾

✓ 2 events (7/25/18 12:10:00.000 PM to 7/25/18 12:15:00.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

7/25/18 12:10:58.599 PM	2018-07-25 12:10:58.599414, MHS="IIB", DL="312809", BRK="BTAMBSU54I1", SRV="TMHS4048", APP="Beheer", QM="QTAMBSU54I1", LEN="0", TYP="OTH", IIB="GSF", OMG="TST4", FLW="Scheduler"
7/25/18 12:10:20.751 PM	2018-07-25 12:10:20.751395, MHS="IIB", DL="311632", BRK="BOLMBSU5401", SRV="OMHS1048", APP="Beheer", QM="QOLMBSU5401", LEN="0", TYP="OTH", IIB="GSF", END="normal", OMG="ONT5", FLW="Scheduler", EventID="f014431e8ff211e8b3b50ae21c300000", EventVolgNr="1"

Selecteren van de eerste of laatste Events: Commando's head en tail

1/2

Met het commando **head** / **tail** kunnen de eerste / laatste n Events worden geselecteerd:

| head n | tail n

Met eerste / laatste wordt bedoeld: bovenaan / onderaan in de lijst van Events. En dus niet: eerste / laatste in tijd!

- De eerste / laatste (maximaal) n Events blijven behouden. Alle andere Events worden verwijderd.
- Als n niet wordt gespecificeerd, dan geldt een default waarde van 10

Voorbeeld: Basis Search aangevuld met head comando

2/2

New Search

Save As ▾ New Table Close

```
index=mhs-bem sourcetype=mhs:keten | tail 4
```

Last 1 hour ▾

4 events (7/25/18 9:00:00.000 AM to 7/25/18 1:00:00.000 PM) No Event Sampling ▾ Job ▾ II ■ → + ↓ Verbose Mode ▾

7/25/18 9:00:56.132 AM	2018-07-25 09:00:56.132980, MHS="KTM", LogType="M", Gebeurtenis="aef142d875b54cd49775e5cd8b2a6995", DomeinNaam="Ontvangen en Mededelen", WerkprocesNaam="Ontvangen", ApplicatieNaam="MHS", MeetpuntLabel="B2A-C05", Procesovergang="", Berichtstroom="GGI", BerichtDatum="2018-07-25 00:00:00.000000", PoortDatum="2018-07-25 09:00:56.134630", Van="B2A", Naar="COS", volgNr="1", kanaal="EBMS", tijdvak="2018", in="1", Adapter="OntvB2B", Lenght="3005", gd1="012746", Geval="aef142d875b54cd49775e5cd8b2a6995", OMG="TA03", FLW="GF_B2bAdapter" Berichtstroom = GGI Lenght = 3005 kanaal = EBMS
7/25/18 9:00:56.132 AM	2018-07-25 09:00:56.132980, MHS="IIB", DL="657762", BRK="BTAMBSU66A1", SRV="AMHS3048", APP="ONTV_Adapters", QM="QTAMBSU66A1", LEN="3005", TYP="MQ", IIB="GSF", SRC="QABMWB2BL02A1", QUE="MHS.AI.TA03.ONTV_ADAPTER_B2B", ID="414d51205141424d574232424c30324186753b5b2151e823", gd1="012746", Geval="aef142d875b54cd49775e5cd8b2a6995", OMG="TA03", FLW="GF_B2bAdapter"
7/25/18 9:00:56.804 AM	2018-07-25 09:00:56.804885, MHS="KTM", LogType="M", Gebeurtenis="aef142d875b54cd49775e5cd8b2a6995", DomeinNaam="Ontvangen en Mededelen", WerkprocesNaam="Ontvangen", ApplicatieNaam="MHS", MeetpuntLabel="COS-END", Procesovergang="", Berichtstroom="GGI", BerichtDatum="2018-07-25 00:00:00.000000", PoortDatum="2018-07-25 09:00:56.134630", Van="COS", Naar="END", volgNr="2", kanaal="EBMS", tijdvak="2018", BBA="1", DAS="1", MID="1", OVB="1", gd1="012746", Geval="aef142d875b54cd49775e5cd8b2a6995", OMG="TA03", FLW="B2B_ONTV_T1" Berichtstroom = GGI kanaal = EBMS
7/25/18 9:00:56.804 AM	2018-07-25 09:00:56.804885, MHS="IIB", DL="851476", BRK="BTAMBSU66A1", SRV="AMHS3011", APP="B2B", QM="QTAMBSU66A1", LEN="1164", TYP="MQ", IIB="GSF", SRC="QTAMBSU66A1", QUE="MHS.AI.TA03.B2B_ONTV_START", ID="414d51205154414d42535536364131205a2fb69e21d49664", gd1="012746", Geval="aef142d875b54cd49775e5cd8b2a6995", OMG="TA03", FLW="B2B_ONTV_T1"

Commando's

Categorie: Het beïnvloeden van Fields

Toevoegen of inhoudelijk aanpassen van Fields: commando eval

1/2

Met het commando **eval** kan een nieuw Field worden toegevoegd, of kan een bestaand Field inhoudelijk worden aangepast:

| eval <Field>=<numerieke of alfanumerieke expressie>

- <Field> is een nieuw of al bestaand Field
 - Als <Field> nog niet bestaat, dan wordt het nieuw toegevoegd
 - Als <Field> al bestaat, dan wordt het inhoudelijk overschreven
- Een nieuw toegevoegd Field kan door een volgend commando meteen worden gebruikt

Voorbeeld: Basis Search aangevuld met eval commando's

2/2

New Search

```
index=mhs-bem sourcetype=mhs:keten
| eval DLX=(DL-10000)*20
| eval SRV2=lower(SRV)+"_"+DLX
| table DL DLX SRV SRV2
```

Last 1 hour

✓ 5 events (7/25/18 1:08:00.000 PM to 7/25/18 1:09:00.000 PM) No Event Sampling Job

Het commando table wordt later besproken!

DL	DLX	SRV	SRV2
31389	427780	AMHS3011	amhs3011_427780
12237	44740	AMHS3046	amhs3046_44740
17046	140920	AMHS3046	amhs3046_140920
39060	581200	AMHS3011	amhs3011_581200
13752	75040	AMHS3048	amhs3048_75040

Hernoemen van Fields: Commando rename

1/2

Met het commando **rename** kan een Field worden hernoemd:

| rename <Field1> as <Field2>

- Hierbij wordt <Field1> hernoemd naar <Field2>
- Als <Field2> al bestaat, dan wordt dat Field overschreven
- Er mogen meerdere rijtjes <Field1> as <Field2> achter elkaar staan, telkens gescheiden door een spatie of een komma

Voorbeeld: | rename actie as action bericht as message taak as task

Voorbeeld: Basis Search aangevuld met rename commando

2/2

The image shows two Splunk search interfaces. The top interface displays a search for 'index=sea-bem sourcetype=sea_meetpunten' resulting in 16,369 events from June 25, 2018, to July 25, 2018. The 'Selected Fields' pane (highlighted with a green border) lists fields: '# Belastingjaar 3', '@ KanaalCode 4', '@ MededelingID 100+', and '@ SoortMededeling 7'. The bottom interface shows the same search with an added 'rename' command: 'index=sea-bem sourcetype=sea_meetpunten | rename Belastingjaar as jaar KanaalCode as Code SoortMededeling as TypeMededeling'. This results in the same 16,369 events and the same 'Selected Fields' list. A large green arrow points from the top search results down to the bottom search results.

New Search

```
index=sea-bem sourcetype=sea_meetpunten
```

✓ 16,369 events (6/25/18 4:53:30.000 PM to 7/25/18 4:53:30.000 PM) No Event Sampling

Selected Fields

- # Belastingjaar 3
- @ KanaalCode 4
- @ MededelingID 100+
- @ SoortMededeling 7

New Search

```
index=sea-bem sourcetype=sea_meetpunten  
| rename Belastingjaar as jaar KanaalCode as Code SoortMededeling as TypeMededeling
```

✓ 16,369 events (6/25/18 4:55:47.000 PM to 7/25/18 4:55:47.000 PM) No Event Sampling

Selected Fields

- @ Code 4
- # jaar 3
- @ MededelingID 100+
- @ TypeMededeling 7

Verwijderen van Fields: Commando fields

1/2

Met het commando **fields** kunnen Fields worden verwijderd:

| fields + <één of meer Fields gescheiden door spaties of komma's> (var. 1)

| fields - <één of meer Fields gescheiden door spaties of komma's> (var. 2)

- Variant 1: Behoud de genoemde Fields en verwijder alle andere Fields (behalve `_raw` en `_time`). Het plusteken is optioneel.
- Variant 2: Verwijder de genoemde Fields en behoud alle andere Fields
- Let op! Achter het plus- en minteken moet een spatie staan!

| fields actie meetpunt

Hierna zijn alleen de Fields **actie**, **meetpunt**, **_raw** en **_time** nog beschikbaar.

| fields - actie meetpunt

Hierna zijn alle Fields, behalve **actie** en **meetpunt** nog beschikbaar.

| fields - actie meetpunt **_raw** **_time**

Hierna zijn alle Fields, behalve **actie**, **meetpunt**, **_raw** en **_time** nog beschikbaar.

Vullen van lege Field waarden: Commando fillnull

1/3

Een Field kan, voor sommige Events, geen waarde hebben (leeg zijn).

Met het commando **fillnull** kunnen lege Field waarden worden gevuld met een hardcoded waarde:

| **fillnull value=<hardcoded waarde> <Field>**

- Als <Field> voor een Event geen waarde heeft, dan wordt de waarde <hardcoded waarde> ingevuld
- De hardcoded waarde kan numeriek of alfanumeriek zijn

Voorbeeld: Basis Search zonder fillnull commando

The screenshot shows the Splunk 6.6.7 search interface. The search bar contains the query `index=sea-bem sourcetype=sea_meetpunten`. The results section shows 16,369 events from July 25, 2018. A histogram for the field `KanaalCode` is displayed, with four bars representing different values. A tooltip for the first bar (DFE) shows the following data:

Values	Count	%
DFE	820	78.17%
SEA_VERTOESEN_PAPIER_LAANGIFTE	118	11.249%
SEA_VERTOESEN_PAPIER_VERZOEKVA	110	10.486%
string	1	0.095%

The tooltip also lists other values: "C9C5094", Dom "", MeetpuntLa AE40F3050D651 and "C9C5094", Dom "", MeetpuntLa 623ERF1800000.

Voorbeeld: Dezelfde basis Search met fillnull commando

3/3

The screenshot shows the Splunk 6.6.7 search interface. The search bar contains the following command:

```
index=sea-bem sourcetype=sea_meetpunten  
| fillnull value=onbekend KanaalCode
```

The results section indicates 16,369 events from June 25, 2018, to July 25, 2018. A histogram visualization titled "KanaalCode" is displayed, showing the distribution of values. The table below provides the top values and their counts:

Values	Count	%
onbekend	15,320	93.592%
DFE	820	5.009%
SEA_VERTOESEN_PAPIER_AANGIFTE	118	0.721%
SEA_VERTOESEN_PAPIER_VERZOEKVA	110	0.672%
string	1	0.006%

Reports: Het opslaan van een Search

Reports

Als je een goed werkende Search hebt geschreven, dan kun je deze opslaan en op een later moment weer inlezen

Een opgeslagen Search wordt een Report genoemd

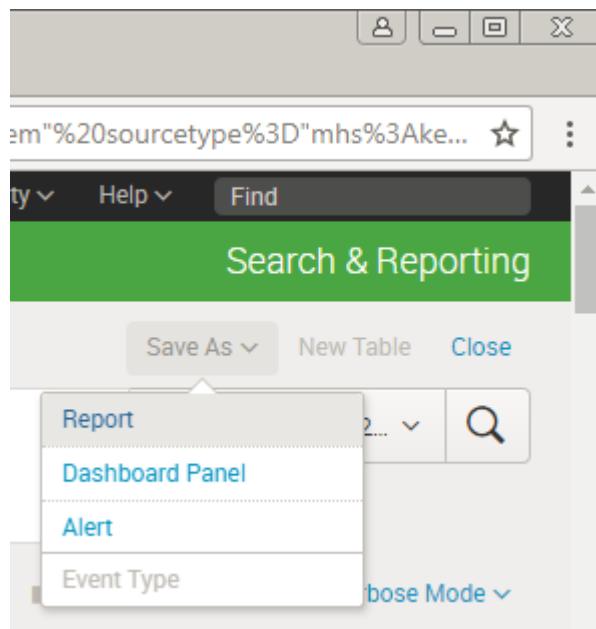
Hierbij wordt tevens opgeslagen welk type resultaat uit de Search moet komen. Ook de geselecteerde tijdsperiode wordt opgeslagen.

Het resultaat zelf wordt niet opgeslagen (dit wordt opnieuw gegenereerd)

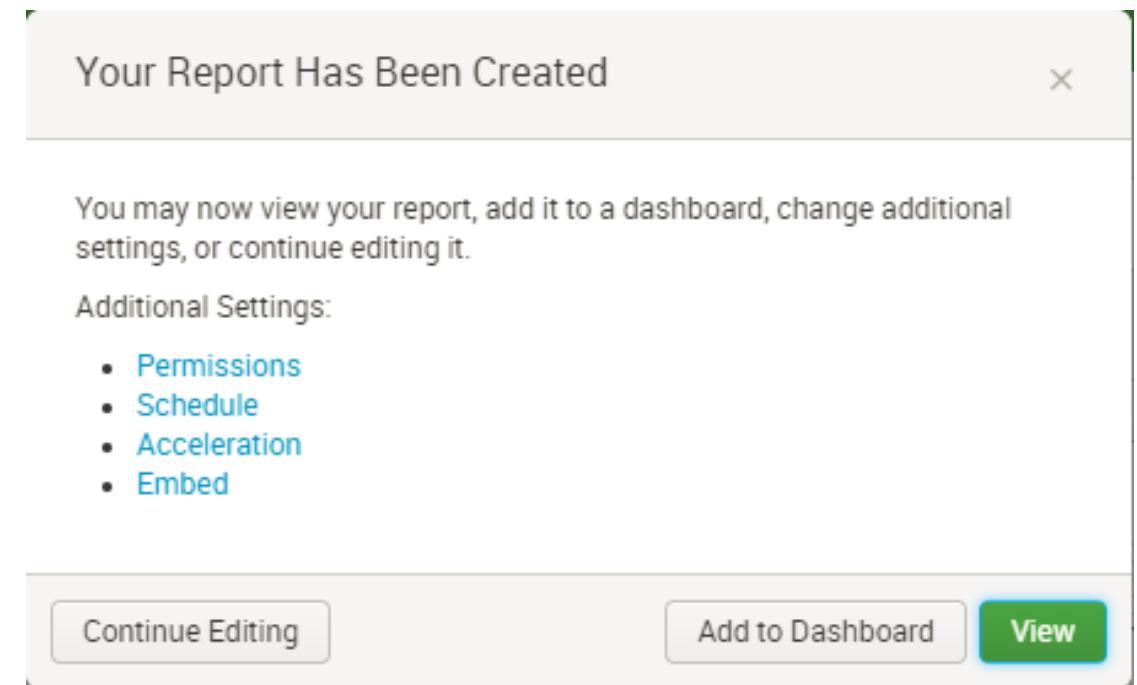
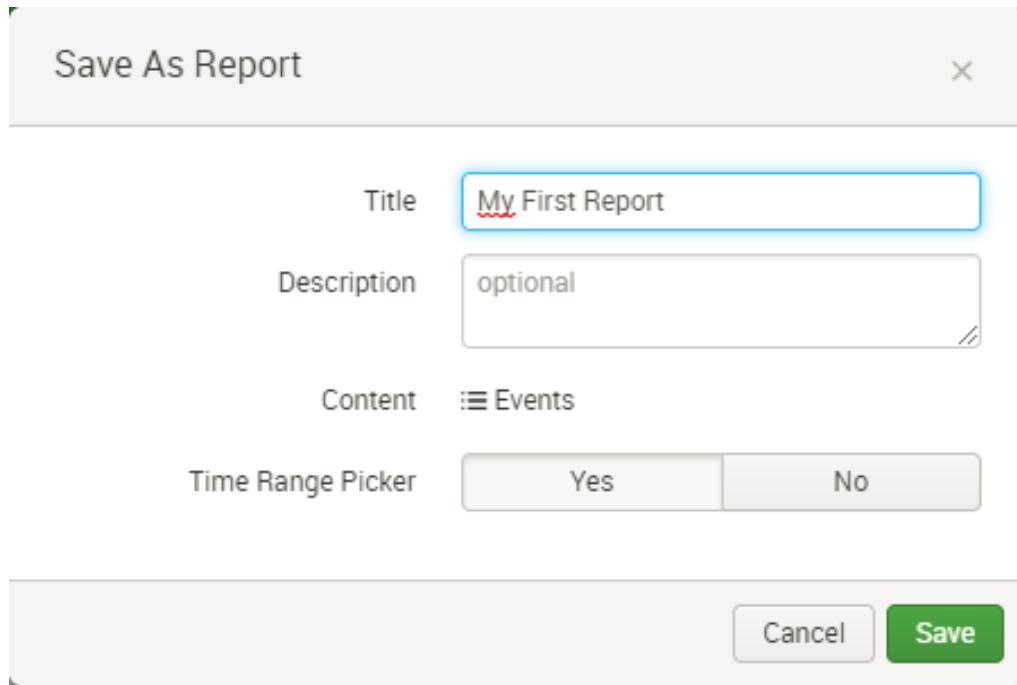
Reports zijn de bouwstenen waaruit dashboards worden opgebouwd

Opslaan van een Report

- Schrijf een Search en voer deze uit
- Ga naar het tabblad met het gewenste type resultaat (tabblad Events, tabblad Statistics, of tabblad Visualization)
- Kies rechtsbovenaan in het scherm voor **Save As → Report**



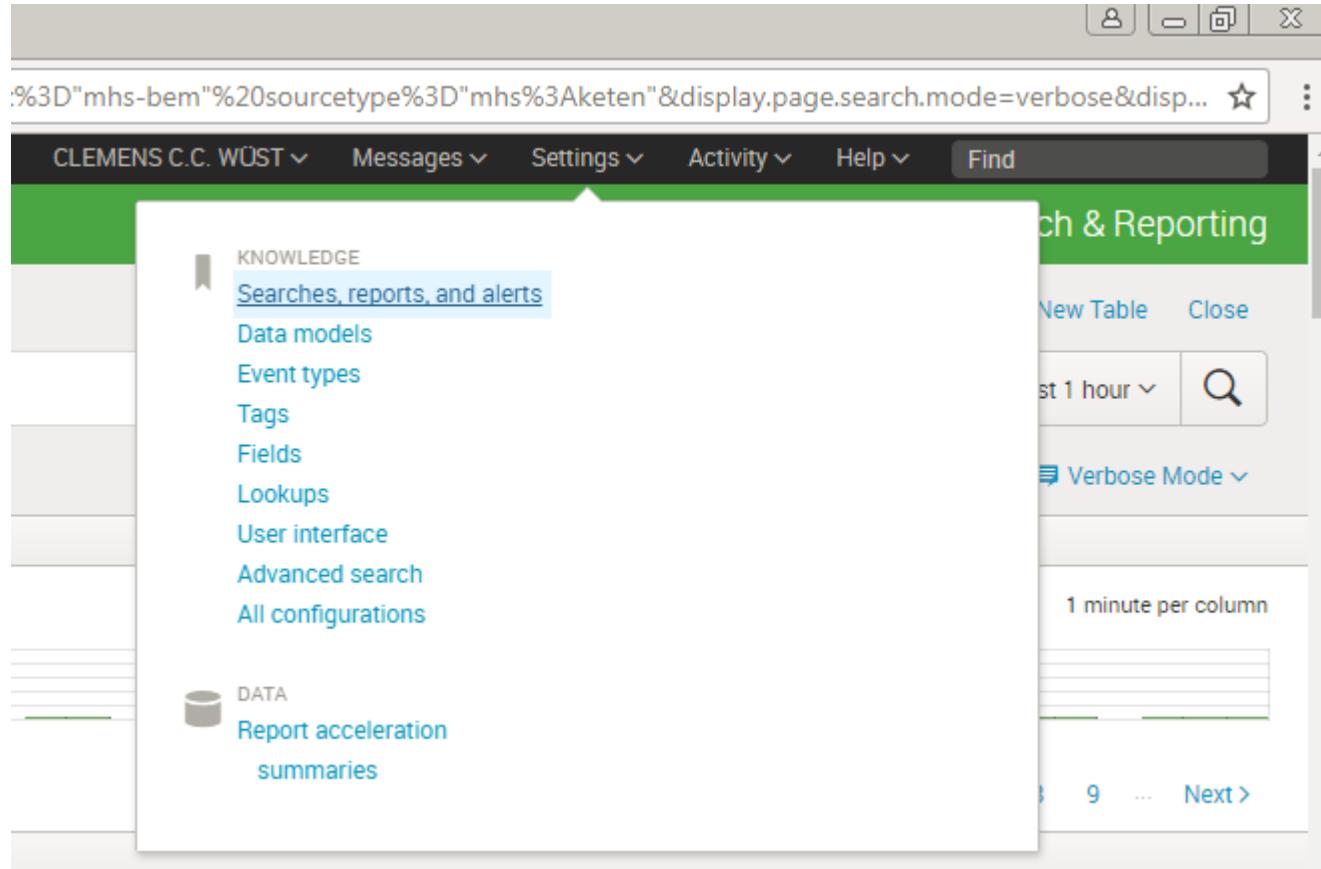
- Er verschijnt nu een window **Save As Report**. Vul bij het veld **Title** een geschikte naam in. Druk daarna op de knop **Save**. 2/2
- Hierna verschijnt het window **Your Report Has Been Created**. Klik op **Continue Editing** om verder te gaan waar je was gebleven was



Inlezen van een Report

1/4

- Kies bovenin het scherm voor **Settings → Searches, reports and alerts**



- In het scherm dat volgt, kies voor Filter by Owner → je eigen naam

2/4

The screenshot shows the Splunk interface for managing saved searches, reports, and alerts. A modal window titled 'Filter by Owner' is open over the main list of items. The modal contains a dropdown menu with options: 'All', 'Nobody', and 'CLEMENS C.C. WÜST (wustc00)'. The 'CLEMENS C.C. WÜST (wustc00)' option is highlighted. Below the dropdown is a table listing various search and reporting configurations. The columns include Name, Actions, App, Owner, Alerts, Sharing, and Status. One entry is highlighted: 'BRM_SEA_ACCT_alert error on GRM last 20m' (App: Search & Reporting). The 'Owner' column for this entry shows 'verwd02'. The 'Status' column indicates it is 'Enabled'.

Name	Actions	App	Owner	Alerts	Sharing	Status
ACCT-WEB-FAILED	Edit Run	search	verwd02	0	App	Enabled
ASBL-FOUTEN	Edit Run	search	verwd02	0	App	Enabled
BRM_SEA_ACCT_alert error on GRM last 20m Alert welke afgaat op het moment dat er een fout optreedt naar / in GRM	Edit Run View Recent 2017-11-27 12:00:00 CET	doddd00	doddd00	0	App	Enabled
BRM_SEA_TEST_alert error on GRM last 20m Alert wanneer in de SEA testomgeving een error ontstaat naar de aanroep	Edit Run View Recent 2017-11-27 12:00:00 CET	doddd00	doddd00	0	App	Enabled
CICS RACF	Edit Run	search	hoekb03	0	App	Enabled
DZU-NCTS	Edit Run	search	verwd02	0	App	Enabled
DZU-NCTS-V02	Edit Run	search	verwd02	0	App	Enabled
Deploy vs zIIP RCQ1	Edit Run	search	hoekb03	0	App	Enabled
Deploy vs zIIP RCT1	Edit Run	search	hoekb03	0	App	Enabled
Ding zIIP RCQ1	Edit Run	search	hoekb03	0	App	Enabled

- Je ziet nu alle Reports die je zelf hebt opgeslagen

3/4

The screenshot shows the Splunk interface for managing saved searches, reports, and alerts. The title bar indicates the user is on the 'splunk' instance at the URL <https://otasplunk.belastingdienst.nl/en-US/manager/search/saved/searches?app=search&count=10&offset=0&itemType=&owner=wustc00>. The main title is 'Searches, Reports, and Alerts'. Below it, a sub-header states: 'Searches, reports, and alerts are saved searches created from pivot or the search page. [Learn more](#)'. The search results table has the following columns: Name, Actions, Next Scheduled Time, Display View, Owner, App, Alerts, Sharing, and Status. There is one entry: 'My First Report' with 'Edit' and 'Run' actions, no scheduled time, 'none' display view, owner 'wustc00', app 'search', 0 alerts, private sharing, and enabled status.

Name	Actions	Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
My First Report	Edit Run	none	none	wustc00	search	0	Private	Enabled

- Klik bij een Report op **Edit** om het Report verder te bewerken
- Klik bij een Report op **Run** om het Report uit te voeren

4/4

The screenshot shows the Splunk web interface for managing saved searches, reports, and alerts. The title bar reads 'Searches, reports, and ale'. The URL in the address bar is 'https://otasplunk.belastingdienst.nl/en-US/manager/search/saved/se'. The top navigation bar includes links for 'splunk', 'Apps', and 'User: CLEMENS C.C. WÜST'. The main content area is titled 'Searches, Reports, and Alerts' and contains the message 'Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more'. Below this, there is a summary row with the count '1 Searches, Reports, and Alerts', the type 'All', the app 'Search & Reporting (search)', and the owner 'CLEMENS C.C.'. A table lists the single report entry:

Name	Actions	Next Scheduled Time	Display View
My First Report	Edit Run	none	none

Cursus Splunk

Module 4:
Genereren van Tabellen en Grafieken

Het concept van een tabel in Splunk

Het concept van een tabel in Splunk

1/2

- Een tabel heeft rijen (horizontaal), kolommen (verticaal), en cellen
- Betreft de rijen:
Ieder Event* draagt bij aan precies één rij van de tabel.
Aan iedere rij van de tabel wordt bijgedragen door één of meer Events.
Een tabel is dus een indikking (= aggregatie) van Events:
 x Events worden omgezet in y rijen, waarbij $x \geq y$
- Betreft de kolommen:
Iedere kolom van de tabel is een Field

*Ieder Event dat nog over is op het moment dat de tabel gegenereerd wordt

Voorbeeld:

2/2

We aggregeren de Events op Field **Meetpunt**.

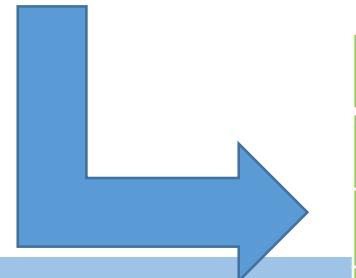
Voor de kolommen kiezen we de Fields **Meetpunt**, **Tegoed** en **Schuld**.

Zelf voegen we kolom **Verschil** toe, welke is afgeleid als **Tegoed** minus **Schuld**.

Events:

	_time	Meetpunt	Naam	Tegoed	Schuld
Event 1	2017-11-13 11:00:03.960	MP3	Bert	€ 2000	€ 100
Event 2	2017-11-13 11:00:02.636	MP5	Igor	€ 300	€ 800
Event 3	2017-11-13 10:55:38.651	MP4	Peter	€ 500	€ 0
Event 4	2017-11-13 10:55:37.272	MP4	Robbert	€ 0	€ 200
Event 5	2017-11-13 10:55:37.102	MP5	Edgar	€ 900	€ 300

Tabel:



	Meetpunt	Tegoed	Schuld	Verschil
Rij 1	MP3	€ 2000	€ 100	€ 1900
Rij 2	MP4	€ 500	€ 200	€ 300
Rij 3	MP5	€ 1200	€ 1100	€ 100

Commando's

Categorie: Het genereren van een tabel

Tabel met Event data: Commando table

1/2

Met het commando **table** kan een tabel worden gemaakt met daarin, per Event, de waarden van één of meer Fields:

| table <één of meer Fields gescheiden door spaties of komma's>

- De tabel heeft een rij voor ieder Event en een kolom voor ieder genoemd Field. De aggregatie is dus 1:1 (geen indikking).
- Je mag een joker (symbool *) gebruiken om één of meer Fields tegelijk aan te duiden
- Gebruik dit commando alleen als de verzameling Events niet al te groot is

Voorbeeld: Basis Search + tail comando + table comando

2/2

The screenshot shows the Splunk 6.6.7 search interface. The search bar contains the following command:

```
index=oldv-business sourcetype=OTS:GOS actie=*  
| tail 5  
| table _time actie *_srt
```

The search results show 5 events from July 1, 2018, to July 8, 2018. The table has five columns: _time, actie, belangh_id_srt, gebr_id_srt, and gemach_id_srt. All entries show the same values: 2018-07-03 17:14:39.649, Ondertekenen, BSN, BSN, and BSN respectively.

_time	actie	belangh_id_srt	gebr_id_srt	gemach_id_srt
2018-07-03 17:14:39.649	Ondertekenen	BSN	BSN	BSN
2018-07-03 17:14:39.649	Ondertekenen	BSN	BSN	BSN
2018-07-03 17:14:39.744	Ondertekenen	BSN	BSN	BSN
2018-07-03 17:14:40.555	Ondertekenen	BSN	BSN	BSN
2018-07-03 17:14:40.808	Ondertekenen	BSN	BSN	BSN

Tabel met statistieken: Commando stats

1/10

Met het commando **stats** kan een tabel worden gemaakt met daarin statistieken afgeleid voor Events.

Voor het berekenen van een statistiek moet je aggregeren.

Oftewel, het berekenen van een waarde (bijv. het gemiddelde) voor een Field (bijv. een bedragveld) over een verzameling van Events (alle Events uit je basis Search, of subsets hiervan).

Het commando maakt gebruik van **aggregatie functies**. Zo geeft bijv. de functie **avg(x)** de gemiddelde waarde van Field **x**.

Belangrijkste aggregatie functies:

2/10

- sum(**x**): berekent de som van Field **x** (**x** is numeriek)
- avg(**x**): berekent de gemiddelde waarde van Field **x** (**x** is numeriek)
- max(**x**): geeft de maximum waarde van Field **x** (**x** is numeriek)
- min(**x**): geeft de minimum waarde van Field **x** (**x** is numeriek)

- count: telt het aantal Events (let op: geen argument!)
- count(**x**): telt het aantal Events waarvoor Field **x** niet leeg is
- dc(**x**): telt het aantal uniek voorkomende waarden van Field **x**

Zonder by-clausule aggregeer je over alle Events.
Het resultaat is een tabel met één rij.

3/10

Voorbeeld: | stats avg(bedrag) as gemiddelde

Met een by-clausule kun je groepen van Events definiëren.
Je aggregert dan over de gedefinieerde groepen van Events.
Het resultaat is een tabel met één rij per groep.

Voorbeeld: | stats avg(bedrag) as gemiddelde by type

Voorbeeld: | stats avg(bedrag) as gemiddelde by kanaal,type

Het is mogelijk om in één tabel meerdere statistieken tegelijk af te leiden

4/10

Voorbeeld: | stats avg(bedrag) as gembed min(bedrag) as minbed

Voorbeeld: | stats avg(bedrag) as gembed min(bedrag) as minbed by type

Omdat het stats commando erg uitgebreid is, laten we aan de hand van voorbeelden zien wat er zoal mogelijk is

Voorbeeld: | stats count as aantal

5/10

The screenshot shows the Splunk search interface. The search bar contains the command: `index=mhs-bem sourcetype=mhs:keten | stats count as aantal`. A green callout box highlights this command with the text: "Dit stats commando geeft een tabel met het aantal Events". Below the search bar, it says "27,547 events (7/2/18 4:00:00.000 PM to 7/2/18 6:00:00.000 PM)". The results pane shows a single row with the value "27547" under the column "aantal". The interface includes tabs for "Events (27,547)", "Statistics (1)", and "Visualization", along with various search and visualization controls.

New Search

Save As ▾ New Table Close

Last 1 day ▾ Search

index=mhs-bem sourcetype=mhs:keten
| stats count as aantal

✓ 27,547 events (7/2/18 4:00:00.000 PM to 7/2/18 6:00:00.000 PM)

Dit stats commando geeft een tabel met het aantal Events

Events (27,547) Statistics (1) Visualization

100 Per Page ▾ Format Preview ▾

aantal
27547

Voorbeeld: | stats count(kanaal) as aantal

6/10

The screenshot shows the Splunk search interface. The search bar contains the command: `index=mhs-bem sourcetype=mhs:keten | stats count(kanaal) as aantal`. A green box highlights this command. To the right, there are buttons for 'Save As', 'New Table', and 'Close'. Below the search bar, it says 'Last 1 day' and has a search icon. The results section shows '27,547 events (7/2/18 4:00:00.000 PM to 7/2/18 6:0:00.000 PM)'. Below this, there are tabs for 'Events (27,547)', 'Statistics (1)', and 'Visualizations'. The 'Statistics (1)' tab is selected. A green callout box points to the 'aantal' field in the table below, containing the value '9951'. The table also has a header 'aantal' with a dropdown arrow.

Dit stats commando geeft een tabel met het aantal Events waarvoor Field kanaal niet leeg is

aantal
9951

Voorbeeld: | stats count as aantal by kanaal

7/10

The screenshot shows a Splunk search interface. The search bar contains the command: `index=mhs-bem sourcetype=mhs:keten | stats count as aantal by kanaal`. Below the search bar, it says `✓ 27,547 events (7/2/18 4:00:00.000 PM to 7/2/18`. The results table has two columns: `kanaal` and `aantal`. The data is as follows:

kanaal	aantal
EBMS	9918
MSG	1
ONP	1
PAPER	16
WEB	15

A green callout box highlights the command in the search bar and points to the results table, containing the text: "Dit stats commando geeft een tabel met het aantal Events, per voorkomende waarde van Field kanaal".

Voorbeeld: | stats count as aantal by kanaal,LogType

8/10

New Search

Save As ▾ New Table Close

Last 1 day ▾

index=mhs-bem sourcetype=mhs:keten
| stats count as aantal by kanaal,LogType

✓ 27,547 events (7/2/18 4:00:00.000 PM to 7/2/18 6:00:00.000 PM)

Events (27,547) Statistics (6) Visualization

100 Per Page ▾ Format Preview ▾

Dit stats commando geeft een tabel met het aantal Events, per voorkomende combinatie van waarden van Fields kanaal en Logtype

kanaal	LogType	aantal
EBMS	M	9918
MSG	M	1
ONP	M	1
PAPER	M	10
WEB	E	3
WEB	M	12

Voorbeeld: | stats sum(Lenght) as som by kanaal

9/10

New Search

Save As ▾ New Table Close

```
index=mhs-bem sourcetype=mhs:keten  
| stats sum(Lenght) as som by kanaal
```

Last 1 day ▾

✓ 27,547 events (7/2/18 4:00:00.000 PM to 7/2/18 6:00:00.)

Events (27,547) Statistics (5) Visualization

100 Per Page ▾ Format Preview ▾

Dit stats commando geeft een tabel met de som van Field Lenght, per voorkomende waarde van Field kanaal

kanaal	som
EBMS	27142808
MSG	
ONP	
PAPER	253341
WEB	33784

Voorbeeld: | stats max(Lengt) as maxlen min(Lengt) as minlen
avg(Lengt) as avglen by LogType

10/10

New Search

Save As ▾ New Table Close

```
index=mhs-bem sourcetype=mhs:keten
| stats max(Lengt) as maxlen min(Lengt) as minlen avg(Lengt) as avglen by kanaal
```

Last 1 day ▾

✓ 27,547 events (7/2/18 4:00:00.000 PM to 7/2/18 6:00:00.000 PM) No Event Sampling ▾ Job ▾ Verbose Mode ▾

Events (27,547) Statistics (5)

100 Per Page ▾ Format Preview ▾

Dit stats commando geeft de maximale, minimale en gemiddelde waarde van Field Lengt, alle drie per voorkomende waarde van Field kanaal

kanaal	maxlen	minlen	avglen
EBMS	85192	2662	5486.720840913685
MSG			
ONP			
PAPER	84447	84447	84447
WEB	14556	6706	11261.333333333334

Sorteren van rijen: commando sort

1/2

In Module 3 hebben we het commando `sort` besproken, voor de sortering van Events op basis van één of meer Fields

Het commando `sort` kan op precies dezelfde manier gebruikt worden voor de sortering van de rijen van een tabel

Voorbeeld: | sort 0 aantal

2/2

New Search

```
index=mhs-bem sourcetype=mhs:keten  
| stats count as aantal by kanaal  
| sort 0 aantal
```

Last 1 day

27,547 events (7/2/18 4:00:00.000 PM to 7/2/18 4:00:00.000 PM)

Events (27,547) Statistics (5) Visualization

100 Per Page Format Preview

kanaal	aantal
MSG	1
ONP	1
WEB	15
PAPER	16
EBMS	9918

Dit sort commando sorteert de rijen van de tabel (gegenererd door het commando stats) op de waarden van kolom aantal.

Weergave van Field waarden aanpassen: Commando fieldformat

1/4

Een Field kun je een zogenaamd *format* meegeven.

Een format is een expressie die bepaalt hoe de Field waarden in een tabel of grafiek worden afgedrukt. De waarden zelf veranderen echter NIET.

Voorbeeld:

Door gebruik te maken van een format kun je de waarde 3000 in een tabel afdrukken als \$3000.00. De waarde blijft echter 3000.

Het Field _time heeft als enige Field standaard al een format.

Voor een Field kan een format worden gedefinieerd met het commando **fieldformat**: 2/4

| fieldformat <Field>=<alfanumerieke of numerieke expressie>

- <Field> is een bestaand Field
- De expressie bepaalt hoe de Field waarden worden afgedrukt.
De Field waarden zelf veranderen niet!

De expressie zal in het algemeen gebruikmaken van <Field>
(maar dit is niet strikt noodzakelijk!)

Voorbeeld: Search die een tabel oplevert (zonder fieldformat commando) 3/4

New Search

Save As ▾ New Table Close

```
index=oldv-business sourcetype=OTS:GOS result=Success
| head 6
| table _time actie poortbericht_id
```

Last 1 day ▾

✓ 6 events (7/15/18 2:15:00.000 PM to 7/20/18 2:16:00.000 PM) No Event Sampling ▾ Job ▾ II ■ ↗ + ↓ Verbose Mode ▾

Events (6) Statistics (6) Visualization

100 Per Page ▾ Format Preview ▾

_time	actie	poortbericht_id
2018-07-20 14:15:59.978	Ondertekenen	
2018-07-20 14:15:59.964	Verzenden	6E15511FD4EF4C57BEFFC04E4704C94A
2018-07-20 14:15:59.934	Verzenden	64A8A7036E374007A37A56DA8B19EC71
2018-07-20 14:15:59.903	Verzenden	A1908416DA504F0998B117604B8293A2
2018-07-20 14:15:59.875	Verzenden	AF240A261FDD4CD893A15D46DBA19EF4
2018-07-20 14:15:59.829	Ondertekenen	

Voorbeeld: Dezelfde Search, maar nu met fieldformat commando

4/4

New Search

```
index=oldv-business sourcetype=OTS:GOS result=Success  
| head 6  
| table _time actie poortbericht_id  
| fieldformat actie="jawel: "+lower(actie)
```

Last 1 day

✓ 6 events (7/15/18 2:15:00.000 PM to 7/20/18 2:16:00.000 PM) No Event Sampling Job More Options Print Download Verbose Mode

Events (6) Statistics (6) Visualization

100 Per Page Format Preview

_time	actie	poortbericht_id
2018-07-20 14:15:59.978	jawel: ondertekenen	
2018-07-20 14:15:59.964	jawel: verzenden	6E15511FD4EF4C57BEFFC04E4704C94A
2018-07-20 14:15:59.934	jawel: verzenden	64A8A7036E374007A37A56DA8B19EC71
2018-07-20 14:15:59.903	jawel: verzenden	A1908416DA504F0998B117604B8293A2
2018-07-20 14:15:59.875	jawel: verzenden	AF240A261FDD4CD893A15D46DBA19EF4
2018-07-20 14:15:59.829	jawel: ondertekenen	

Commando's

Categorie: Het genereren van een grafiek

Commando's stats, chart en timechart

Met de commando's **stats**, **chart** en **timechart** kan een grafiek worden gemaakt

- Afhankelijk van het gewenste type grafiek, moet een van deze drie commando's worden gebruikt

Commando **stats** wordt gebruikt voor een grafiek met een enkele waarde

Commando **chart** wordt gebruikt voor x-y grafieken

Commando **timechart** wordt gebruikt voor x-y grafieken waarbij de x-as de tijd is

- De grafiek verschijnt op tabblad Visualization 2/19
- Cadeautje:
De bijpassende grafiek data verschijnt in een tabel op tabblad Statistics
- De commando's maken gebruik van aggregatie functies
(zie de slides voor commando **stats**)

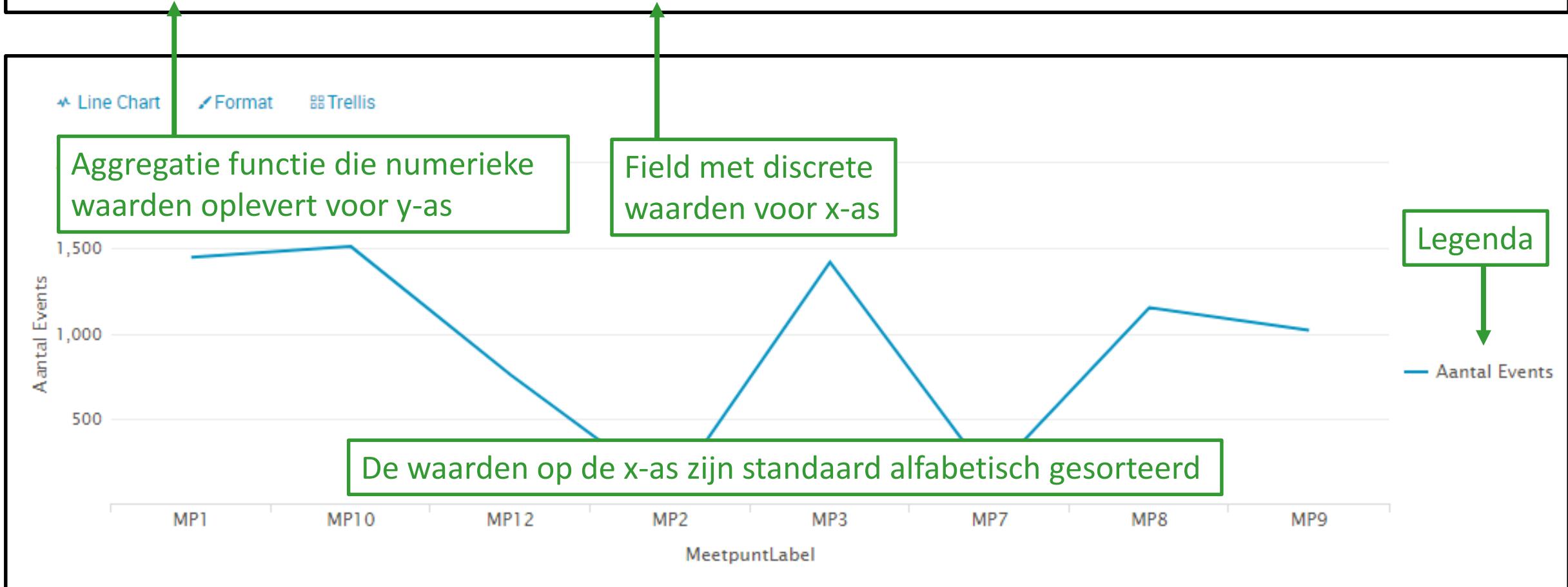
We laten we aan de hand van voorbeelden zien hoe de commando's gebruikt moeten worden:

Type grafiek: Line Chart

3/19

```
index=sea-bem sourcetype=sea_meetpunten-2
```

```
| chart count as "Aantal Events" by MeetpuntLabel
```



De bijbehorende grafiek data staat op tabblad Statistics

4/19

```
index=sea-bem sourcetype=sea_meetpunten-2  
| chart count as "Aantal Events" by MeetpuntLabel
```

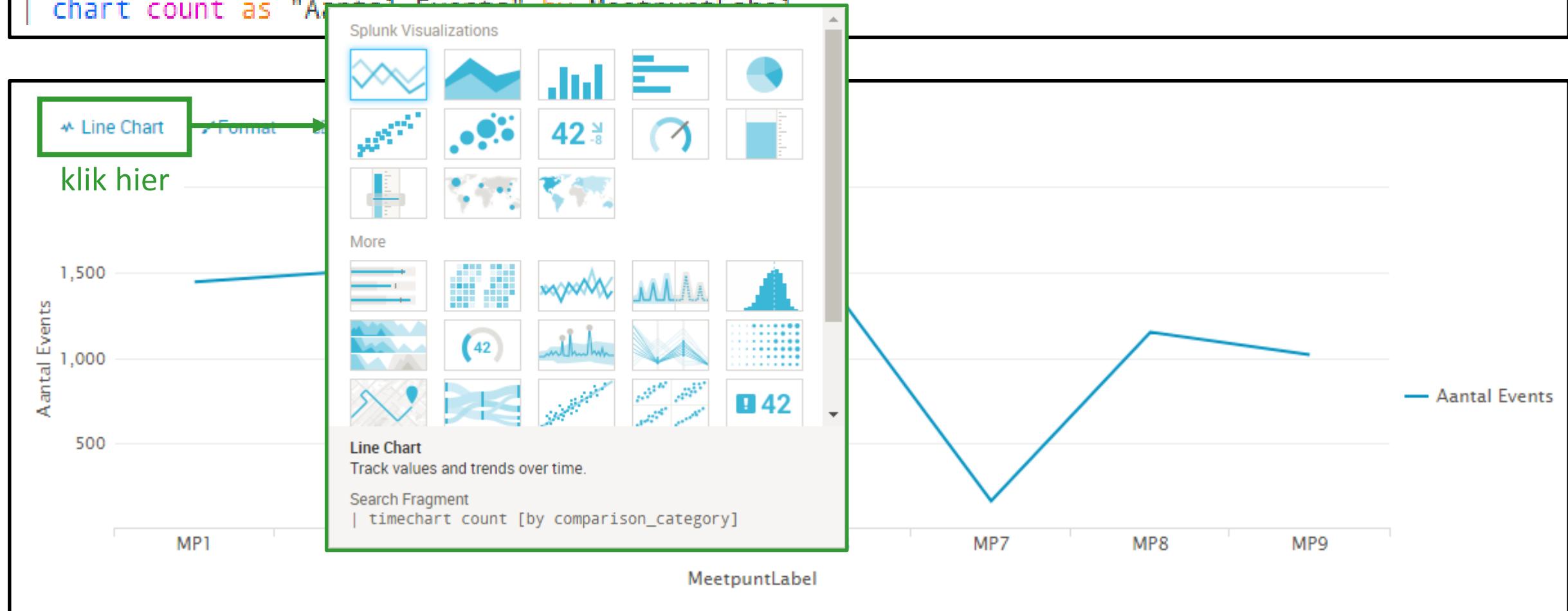
MeetpuntLabel	Aantal Events
MP1	1447
MP10	1510
MP12	756
MP2	63
MP3	1418
MP7	157
MP8	1150
MP9	1018

Kiezen van een ander type grafiek

5/19

```
index=sea-bem sourcetype=sea_meetpunten-2
```

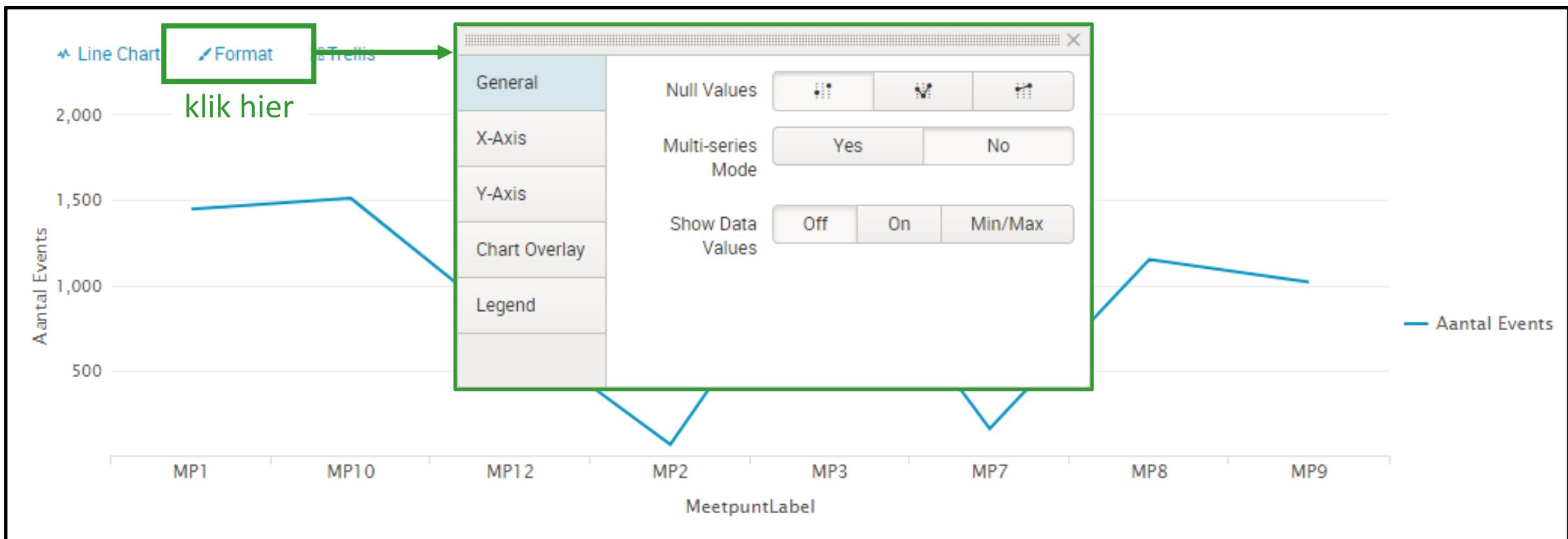
```
| chart count as "Aantal Events"
```



Aanpassen van instellingen voor de x-as, y-as en legenda

6/19

```
index=sea-bem sourcetype=sea_meetpunten-2  
| chart count as "Aantal Events" by MeetpunktLabel
```

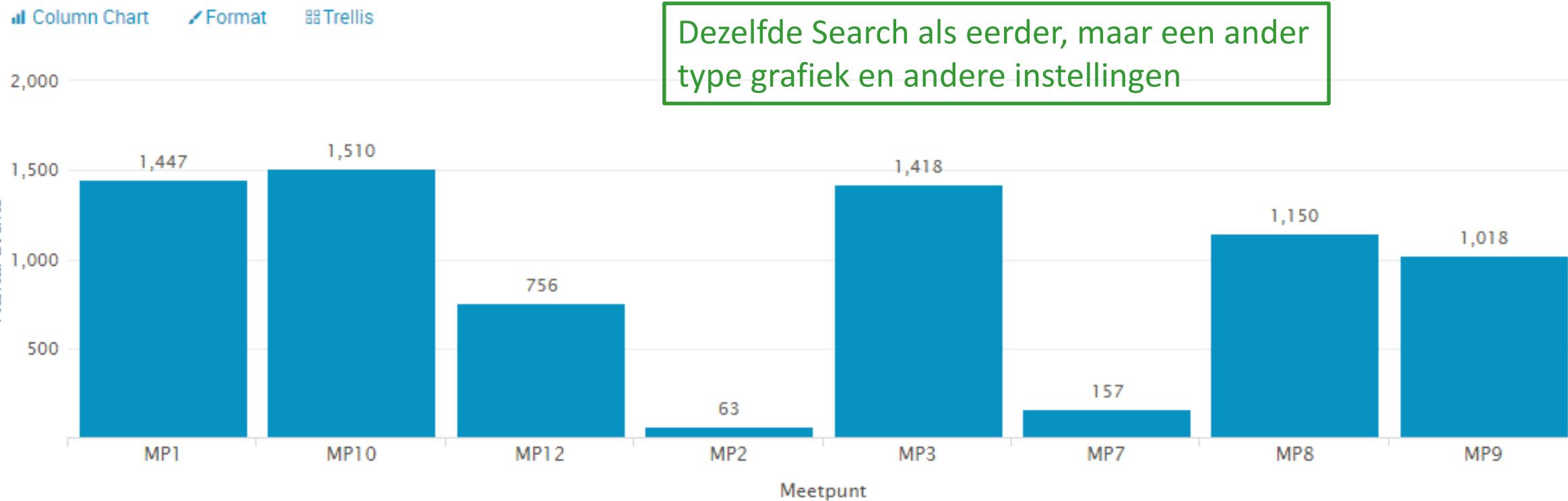


Type grafiek: Column Chart

7/19

```
index=sea-bem sourcetype=sea_meetpunten-2
```

```
| chart count as "Aantal Events" by MeetpuntLabel
```

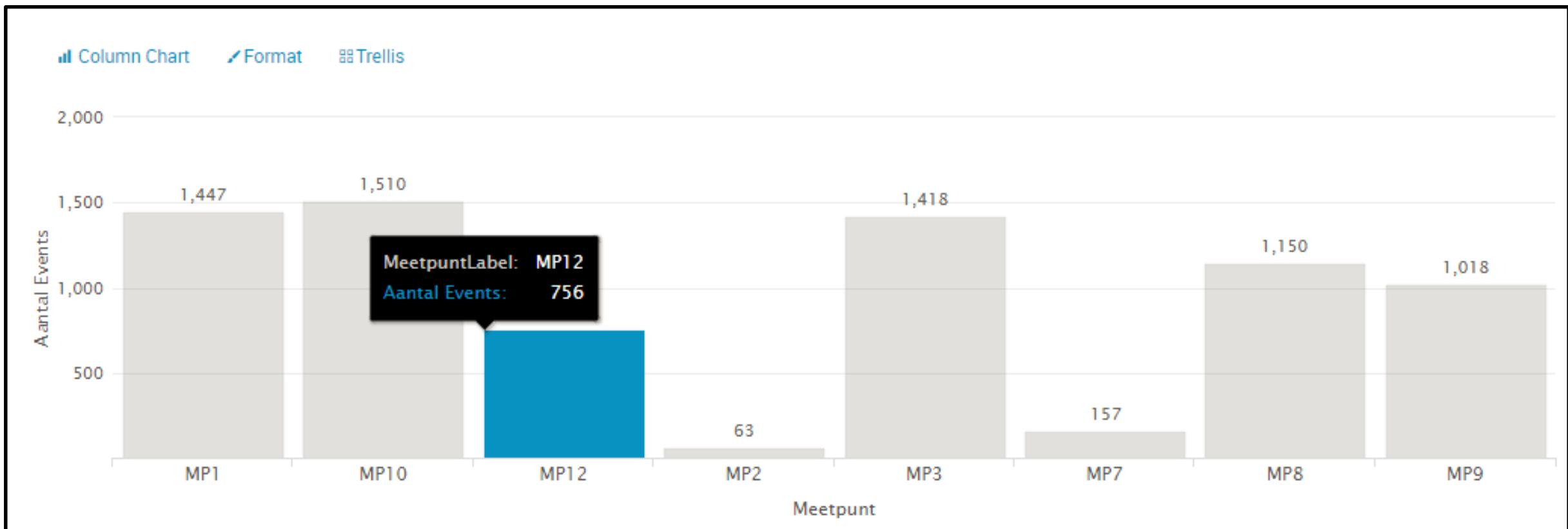


Beweeg met de muiscursor over de data voor meer informatie

8/19

```
index=sea-bem sourcetype=sea_meetpunten-2
```

```
| chart count as "Aantal Events" by MeetpuntLabel
```

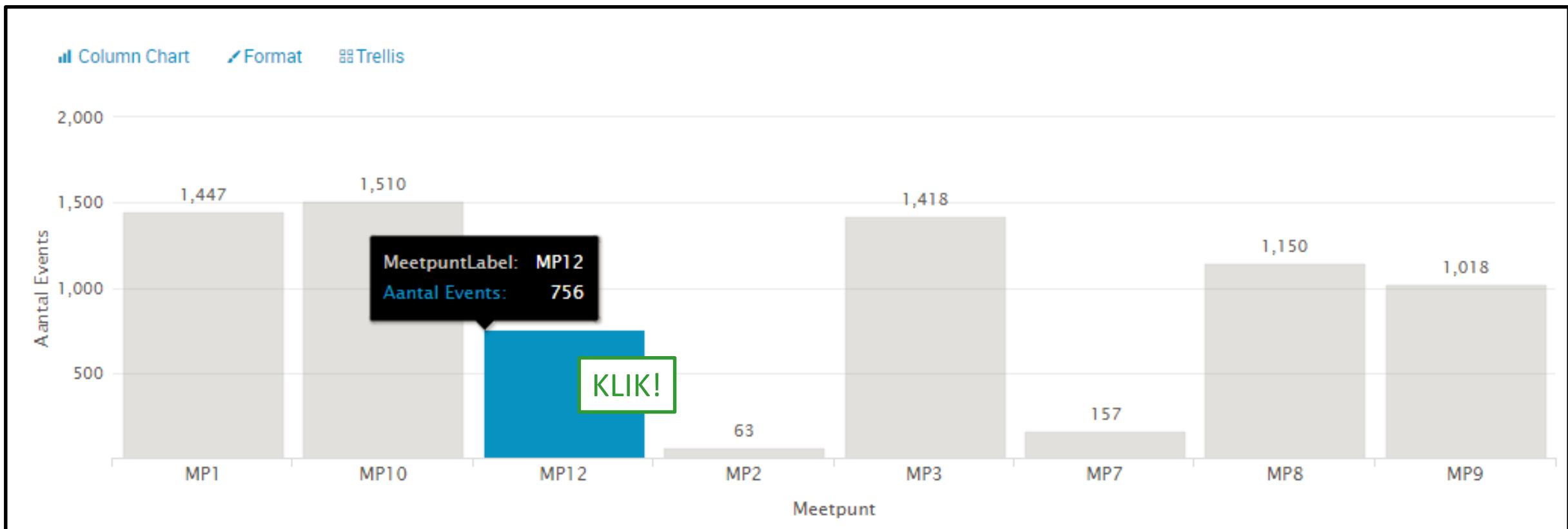


Klik op een gedeelte van de grafiek ... →

9/19

```
index=sea-bem sourcetype=sea_meetpunten-2
```

```
| chart count as "Aantal Events" by MeetpuntLabel
```



→ ... om de bijbehorende Events te bekijken

10/19

Splunk 6.6.3

Veilig | https://otaspplunk.belastingdienst.nl/en-US/app/search/search?q=search%20index%3D"sea-bem"%20sourcetype%3D"sea_meetpunten-2"%20earliest%3D"08%2F01%2F2017... ☆

splunk > App: Search & Reporting

CLEMENS C.C. WÜST > Messages > Settings > Activity > Help > Find

Search Datasets Reports Alerts Dashboards Search & Reporting

New Search

index=sea-bem sourcetype=sea_meetpunten-2

Last 1 hour

756 events (8/1/17 12:00:00.000 AM to 11/1/17 12:00:00.000 AM) No Event Sampling

Job Verbose Mode

Events (756) Statistics Visualization

Format Timeline - Zoom Out + Zoom to Selection × Deselect 1 day per column

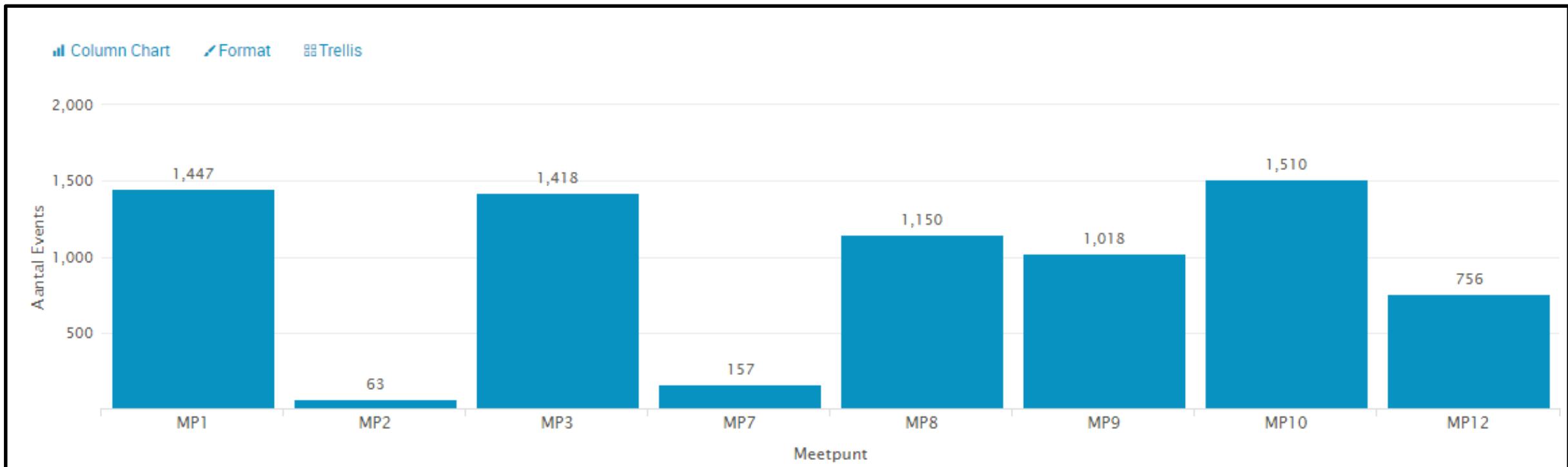
List Format 20 Per Page < Prev 1 2 3 4 5 6 7 8 9 ... Next >

< Hide Fields	All Fields	i	Time	Event
Selected Fields	a MededelingId 100+	>	10/31/17 4:40:23.977 PM	2017-10-31 16:40:23.977, Gebeurtenis="RB000000000000000000000000000000781107398", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP12", Geval="", Procesovergang="", MededelingId="7A44BCAA0AE50FB3B515E63245C1D19A", SoortMededeling="DNI02", Referentie="7A44BCAA0AE50FB3B515E63245C1D19A" MededelingId = 7A44BCAA0AE50FB3B515E63245C1D19A
Interesting Fields	a ApplicatieNaam 1	>	10/31/17 4:29:53.800 PM	2017-10-31 16:29:53.80, Gebeurtenis="RB000000000000000000000000000000781098129", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP12", Geval="", Procesovergang="", MededelingId="7779BFA70AE50B370C79B46EACAA6CCF", SoortMededeling="DNI02", Referentie="7779BFA70AE50B370C79B46EACAA6CCF" MededelingId = 7779BFA70AE50B370C79B46EACAA6CCF
	# date_hour 13	>	10/31/17 4:28:51.384 PM	2017-10-31 16:28:51.384, Gebeurtenis="RB000000000000000000000000000000781098142", DomeinNaam="Aanslag", WerkprocesNaam="Uitnodigen", ApplicatieNaam="SEA", MeetpuntLabel="MP12", Geval="", Procesovergang="", MededelingId="45CCE81D0AE50FB3AA7D5EB690706B68", SoortMededeling="DNI02", Referentie="45CCE81D0AE50FB3AA7D5EB690706B68" MededelingId = 45CCE81D0AE50FB3AA7D5EB690706B68

Een truc om de sortering van de x-as goed te krijgen

11/19

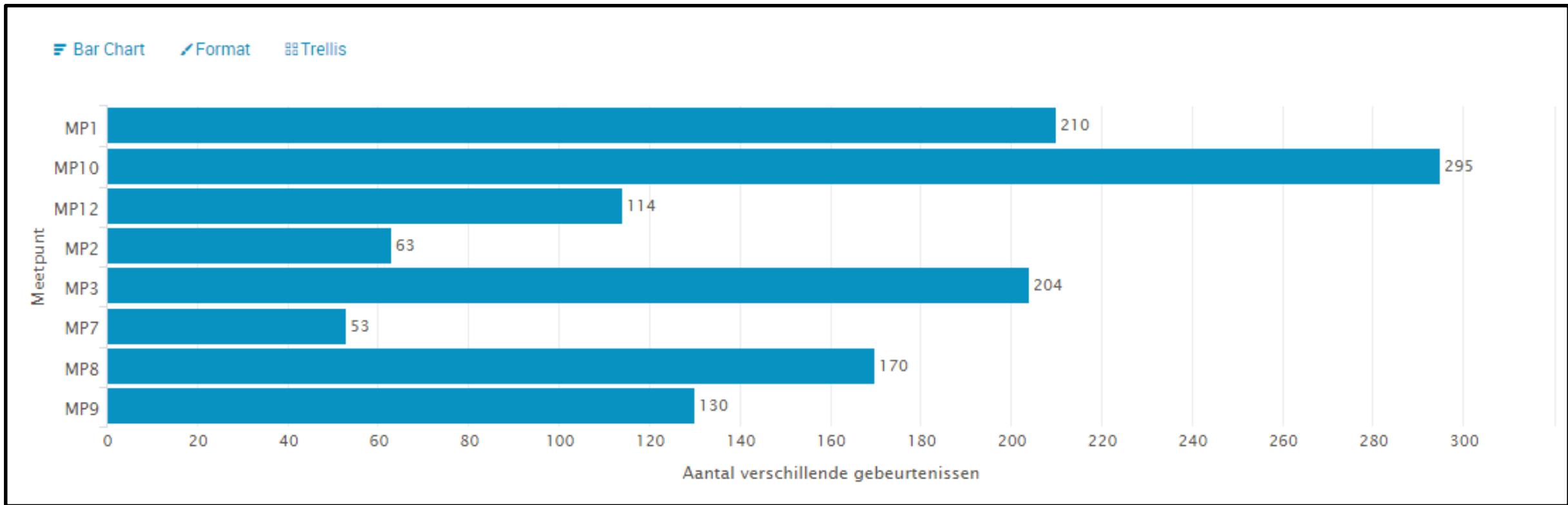
```
index=sea-bem sourcetype=sea_meetpunten-2  
| chart count as "Aantal Events" by MeetpuntLabel  
| eval NewMeetpuntLabel=if(len(MeetpuntLabel)=3,"MPO"+substr(MeetpuntLabel,3,1),MeetpuntLabel)  
| sort NewMeetpuntLabel  
| fields - NewMeetpuntLabel
```



Andere aggregatie functie, ander type grafiek (Bar Chart)

12/19

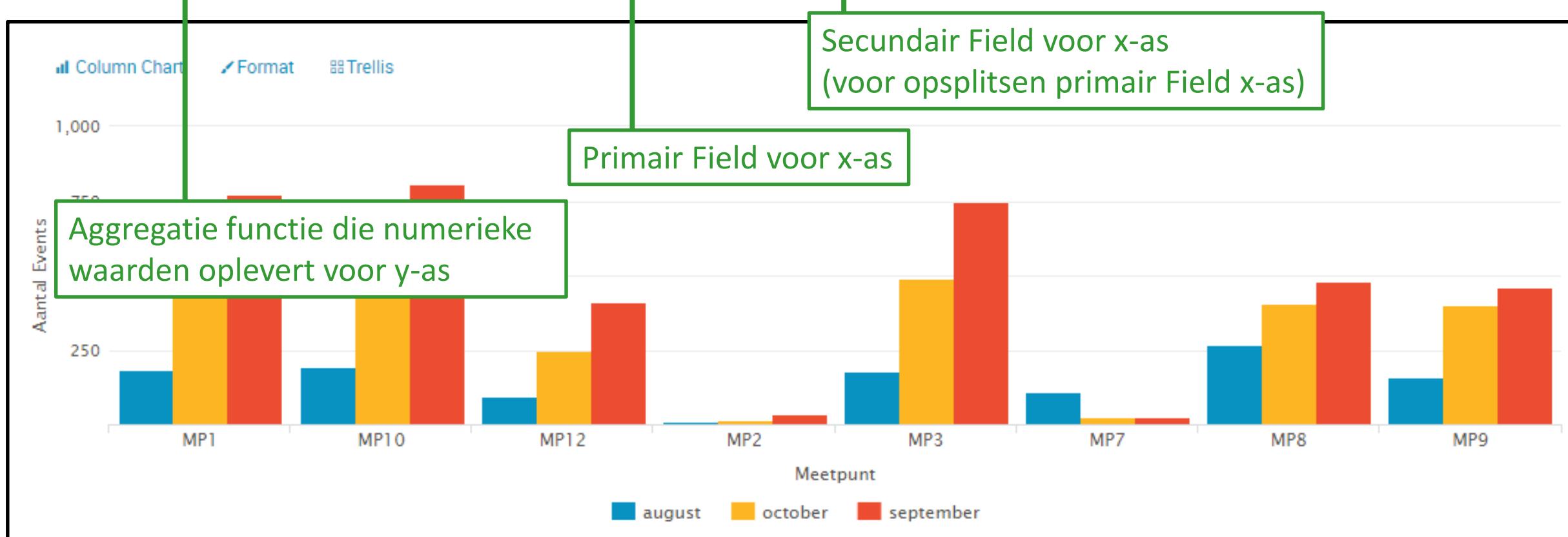
```
index=sea-bem sourcetype=sea_meetpunten-2  
| chart dc(Gebeurtenis) as "Aantal verschillende gebeurtenissen" by MeetpuntLabel
```



De x-as kan opgesplitst worden door een tweede Field

13/19

```
index=sea-bem sourcetype=sea_meetpunten-2  
| chart count as "Aantal Events" by MeetpuntLabel,date_month
```

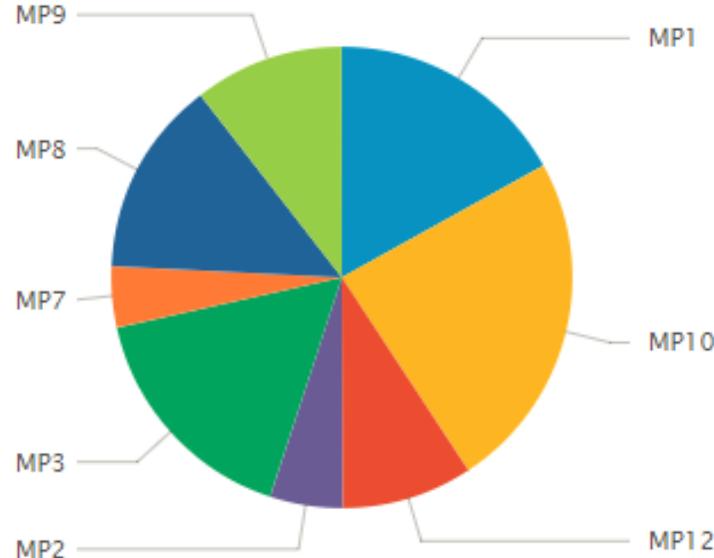


Type grafiek: Pie Chart

14/19

```
index=sea-bem sourcetype=sea_meetpunten-2  
| chart dc(Gebeurtenis) as "Aantal verschillende gebeurtenissen" by MeetpuntLabel
```

Pie Chart Format Trellis



Type grafiek: Single Value

15/19

```
index=sea-bem sourcetype=sea_meetpunten-2  
| stats dc(Gebeurtenis) as "Aantal verschillende gebeurtenissen"
```

Single Value Format Trellis

334

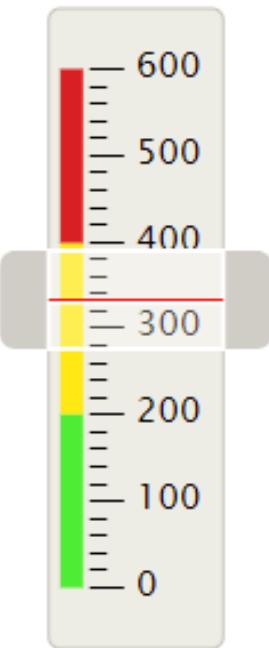
Type grafiek: Marker Gauge

16/19

```
index=sea-bem sourcetype=sea_meetpunten-2  
| stats dc(Gebeurtenis) as "Aantal verschillende gebeurtenissen"  
| gauge "Aantal verschillende gebeurtenissen" 0 200 400 600
```

Marker Gauge Format Trellis

Commando gauge wordt gebruikt om het resultaat Field te classificeren. Dit is nodig bij de type grafieken Marker Gauge en Radial Gauge.

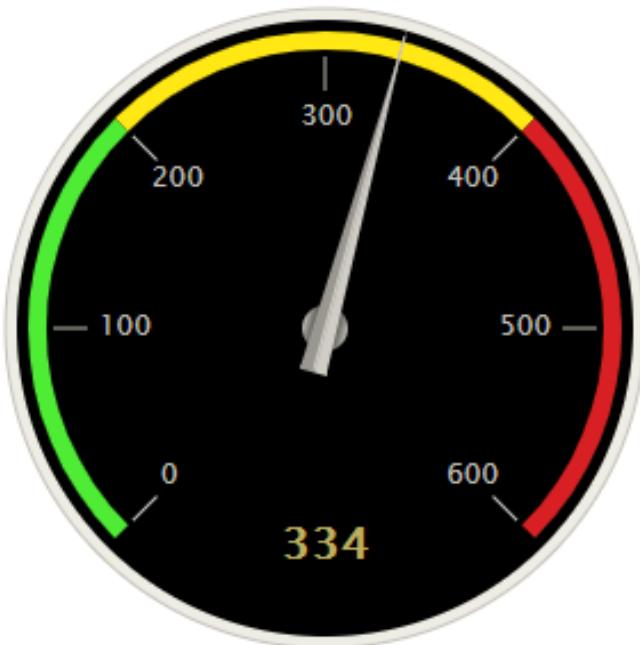


Type grafiek: Radial Gauge

17/19

```
index=sea-bem sourcetype=sea_meetpunten-2  
| stats dc(Gebeurtenis) as "Aantal verschillende gebeurtenissen"  
| gauge "Aantal verschillende gebeurtenissen" 0 200 400 600
```

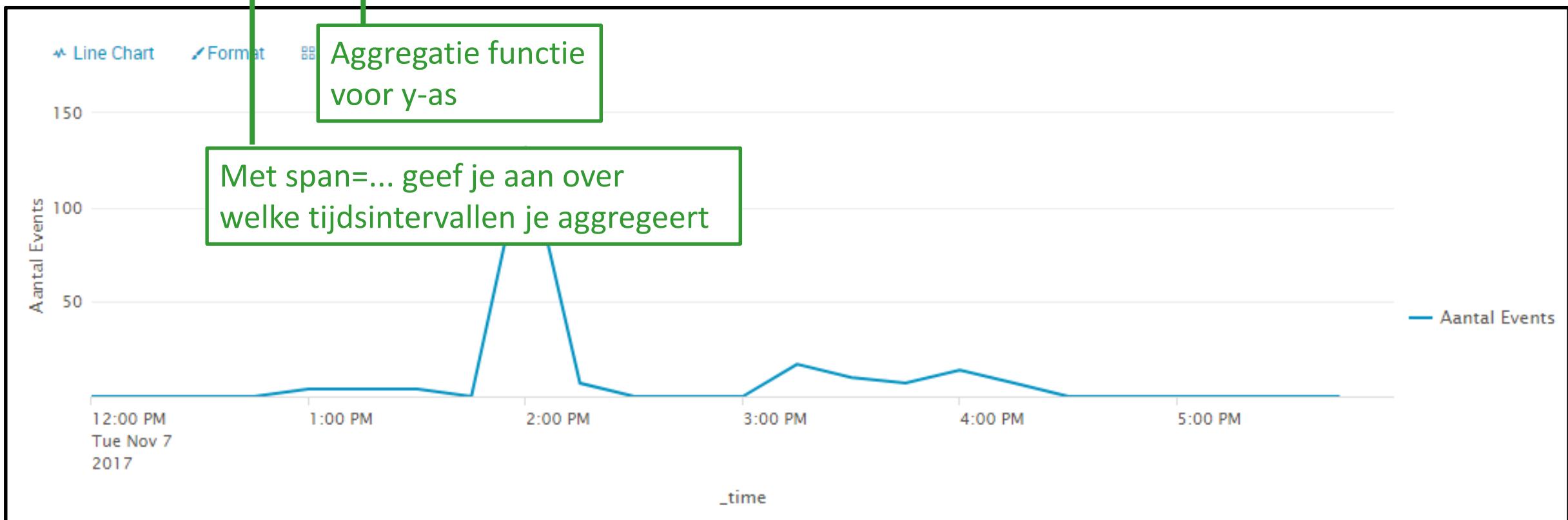
Radial Gauge Format Trellis



Type grafiek: timechart

18/19

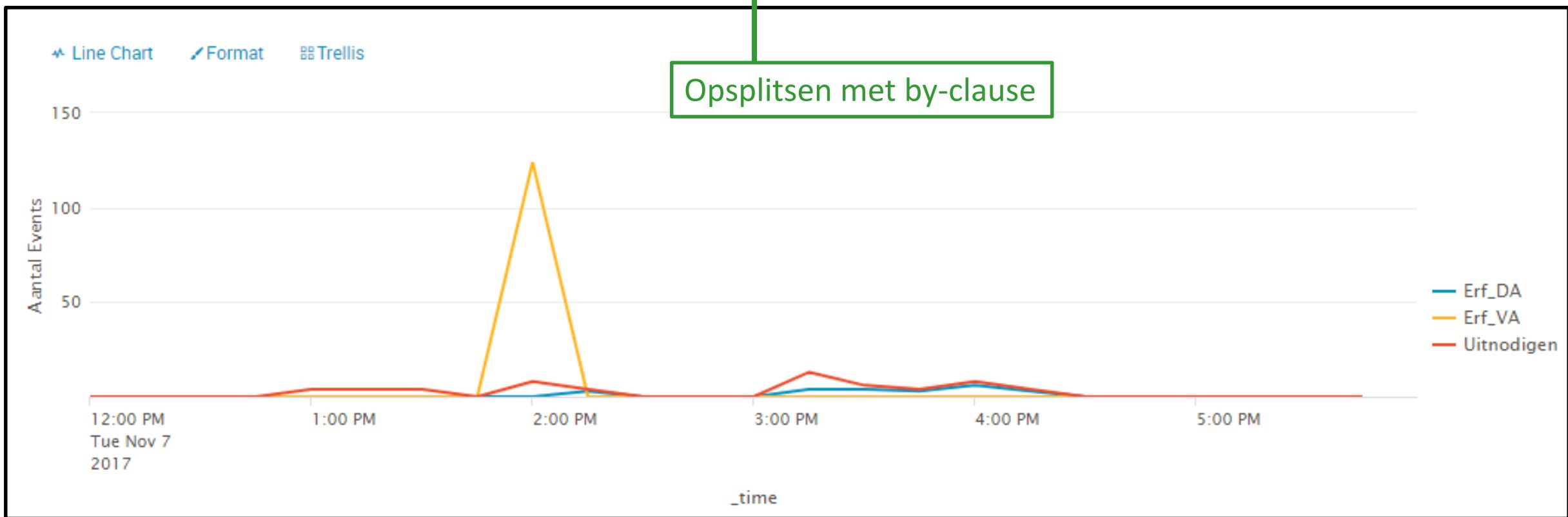
```
index=sea-bem sourcetype=sea_meetpunten-2  
| timechart span=15m count as "Aantal Events"
```



De x-as (tijd) kan opgesplitst worden door een Field

19/19

```
index=sea-bem sourcetype=sea_meetpunten-2  
| timechart span=15m count as "Aantal Events" by WerkprocesNaam
```



Cursus Splunk

Module 5: Genereren van een Dashboard

- Een Dashboard is een pagina waarop Reports zijn geplaatst (dus: tabellen, grafieken, en/of lijsten met Events). Hierbij staan de Reports naast elkaar en/of onder elkaar.
- Aan het Dashboard kan een titel worden gegeven
- Aan ieder Report op het Dashboard kan een titel worden gegeven
- In een Dashboard kunnen Controls (knoppen) worden toegevoegd die invloed hebben op de Reports

In deze cursus leren we NIET hoe Controls toegevoegd kunnen worden

Voorbeeld Dashboard:

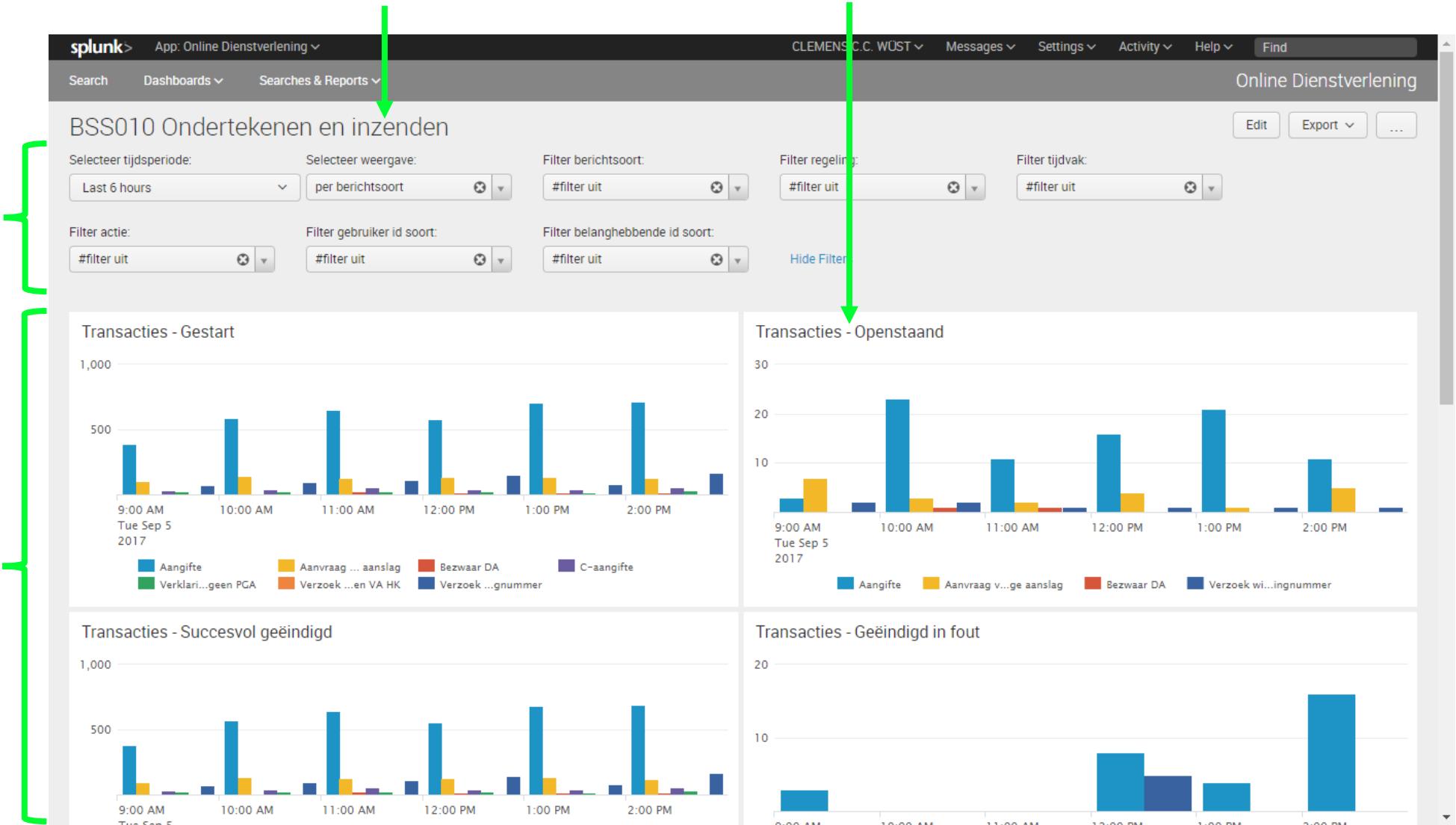
Titel van het Dashboard

2/2

Titel van een Report

Controls

Reports



Stap 1: Genereer de Reports die in het Dashboard moeten komen

Stap 2: Open de Reports één voor één

- Bij het eerste Report: Voeg toe aan een nieuw Dashboard
- Bij de andere Reports: Voeg toe aan het zojuist aangemaakte Dashboard

Stap 3: Wijzig de opmaak van het Dashboard, o.a.

- Plaatsing van de Reports
- Toevoegen titels

In een Report wordt o.a. opgeslagen:

- De Search query
- De zoekperiode
- Het type resultaat (tabel, grafiek, of lijst met Events)
- Opmaak van het resultaat

In Module 3 is uitgelegd hoe je Reports kunt genereren

- In een Dashboard kan de opmaak van een Report niet worden aangepast. Het enige dat in het Dashboard nog mogelijk is, is het toevoegen van een titel.

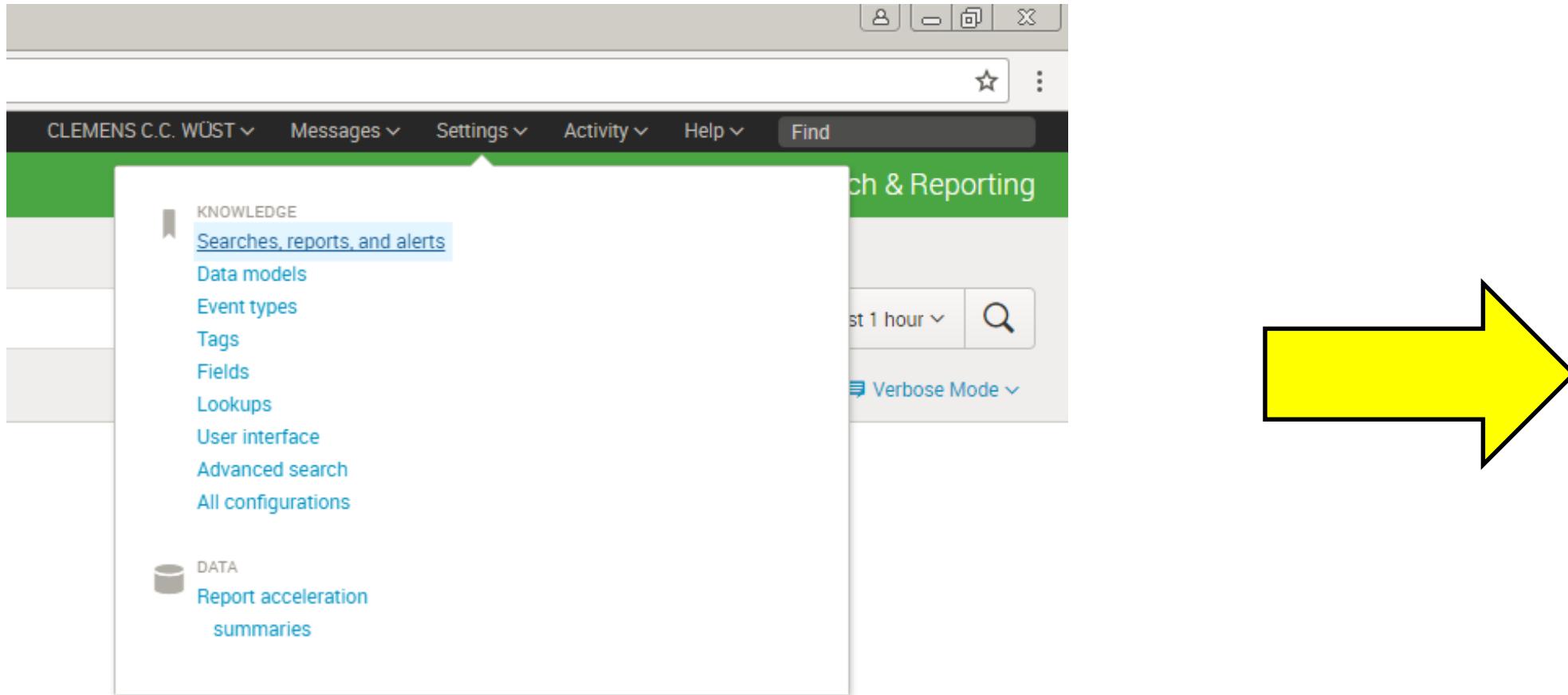
Je moet de opmaak dus al geregeld hebben bij het opslaan van het Report!

- Om ervoor te zorgen dat een Dashboard zichzelf kan vernieuwen over tijd, moet je in de Reports gebruikmaken van een Relative Search

Stap 2: Voor ieder Report dat in het Dashboard moet komen:

4/19

Ga naar **Settings** → **Searches, reports and alerts**.



Kies voor Filter by Owner → Je eigen naam

5/19

The screenshot shows a Splunk interface with a search results page. A modal dialog box is open in the center, titled "Lookup an owner". Inside the dialog, there are two options: "All" and "Nobody". Below these options, the name "CLEMENS C.C. WÜST (wustc00)" is displayed in blue text. At the bottom of the dialog, there are "Edit" and "Home" buttons. The background of the main interface shows a list of search results, with the first result being "3 hosts voor Andre le Noble". A red rectangular box highlights the "Filter by Owner" dropdown menu and the modal dialog. To the right of the main interface, a large yellow arrow points to the right.

Searches, reports, and alerts are saved searches created from runs on the search page. Learn more [?]

94 Searches, Reports, and Alerts Type: All

Filter by Owner filter

Lookup an owner

All

Nobody

CLEMENS C.C. WÜST (wustc00)

BRM CBD: Aantal ERRORS CBD vandaag, vergeleken met 24 uur eerder

BRM CBD: Aantal aanroepen CBD-RIH laatste 12 uur

BRM CBD: Aantal aanroepen CBD-RIH laatste 12 uur

BRM CBD: Aantal aanroepen CBD-RIH laatste 12 uur

BRM RSE: Aantal aanroepen RSE laatste week

BRM SBB: Aantal aanroepen SBB laatste 1 week

BRM SBB: Aantal aanroepen SBB laatste week

BRM SEA: Aantal ERRORS SEA (RSE & SBB) vandaag, vergeleken met 24 uur eerder

BRM TDI: Aantal ERRORS TDI vandaag, vergeleken met 24 uur eerder

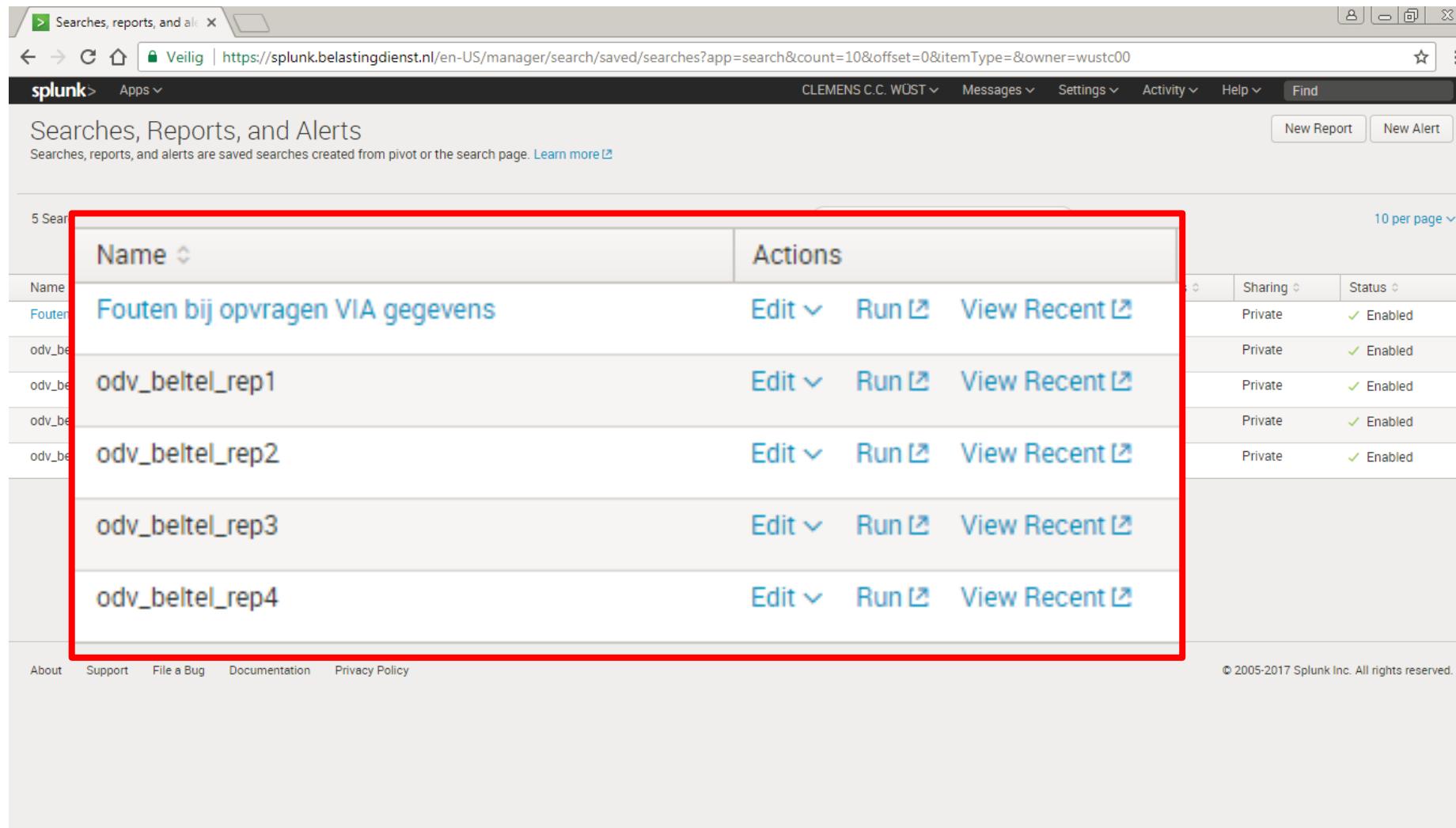
2017-11-29 23:00:00 CET none doddd00 search 0 App ✓ Enabled

2017-11-29 23:00:00 CET none doddd00 search 0 App ✓ Enabled

About Support File a Bug Documentation Privacy Policy © 2005-2017 Splunk Inc. All rights reserved.

Klik bij het betreffende Report op Run om het Report te draaien

6/19



The screenshot shows the Splunk 'Searches, Reports, and Alerts' interface. The page title is 'Searches, Reports, and Alerts'. The URL is <https://splunk.belastingdienst.nl/en-US/manager/search/saved/searches?app=search&count=10&offset=0&itemType=&owner=wustc00>. The top navigation bar includes links for 'splunk', 'Apps', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the navigation is a search bar with 'New Report' and 'New Alert' buttons. The main content area displays a table of saved searches:

Name	Actions
Fouten bij opvragen VIA gegevens	Edit ▾ Run View Recent
odv_beltel_rep1	Edit ▾ Run View Recent
odv_beltel_rep2	Edit ▾ Run View Recent
odv_beltel_rep3	Edit ▾ Run View Recent
odv_beltel_rep4	Edit ▾ Run View Recent

A red box highlights the first search entry, 'Fouten bij opvragen VIA gegevens'. To the right of the highlighted row is a yellow arrow pointing to the right.

Kies na het draaien van het Report voor Save As → Dashboard Panel

7/19

The screenshot shows a Splunk search results page. At the top, there's a search bar and a navigation bar with tabs for Search, Datasets, Reports, Alerts, and Dashboards. Below the search bar, a search string is displayed: `| multisearch [search index=oldv-business sourcetype="OTS:GOS" name="Succesvolle handeling" category="GOS Verzenden" earliest=-1d | eval eval | eval eval | xyseries weekdag jaarweek count`. The results section shows 86,472 events from November 29, 2017, to November 29, 2017. A bar chart visualizes the data by day of the week, comparing the number of transactions in 2016W47 (21NOV) and 2017W47 (20NOV). The chart shows the highest transaction volume on Monday (11,551) and the lowest on Saturday (2,407). A red box highlights the 'Save As' dropdown menu, which is open to show options: Report, Dashboard Panel, Alert, and Event Type. A large yellow arrow points to the right from the bottom right of the interface.

Weekday	2016W47 (21NOV)	2017W47 (20NOV)
MAANDAG	6,746	11,551
DINSDAG	6,076	9,984
WOENSDAG	5,649	8,629
DONDERDAG	4,915	7,415
VRIJDAG	3,965	5,868
ZATERDAG	2,407	4,192
ZONDAG	3,263	5,812

Bij het eerste Report, kies voor **New**, vul een naam in voor het Dashboard (bij **Dashboard Title**) en kies voor **Save**

Save As Dashboard Panel

Dashboard

Dashboard Title

Dashboard ID?
Can only contain letters, numbers and underscores.

Dashboard Description

Dashboard Permissions

Panel Title

Panel Powered By

Drilldown?

Panel Content

Bij de andere Reports, kies voor **Existing**, selecteer de naam van het Dashboard en kies voor **Save**

Save As Dashboard Panel

Dashboard

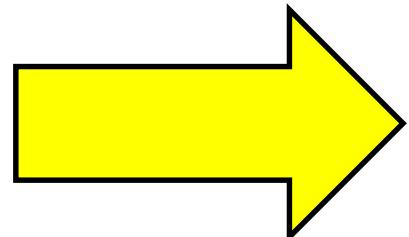
My First Dashboard

Panel Title

Panel Powered By

Drilldown?

Panel Content



Kies voor View Dashboard om het Dashboard tot dusver in te zien

9/19

Your Dashboard Panel Has Been Created

The panel has been created and added to my_first_dashboard. You may now view the dashboard.

[View Dashboard](#)

first Dashboard | Splunk

http://search/my_first_dashboard

CLEMENS C.C. WÜST Messages Settings Activity Help Find

Search & Reporting

Edit Export ...

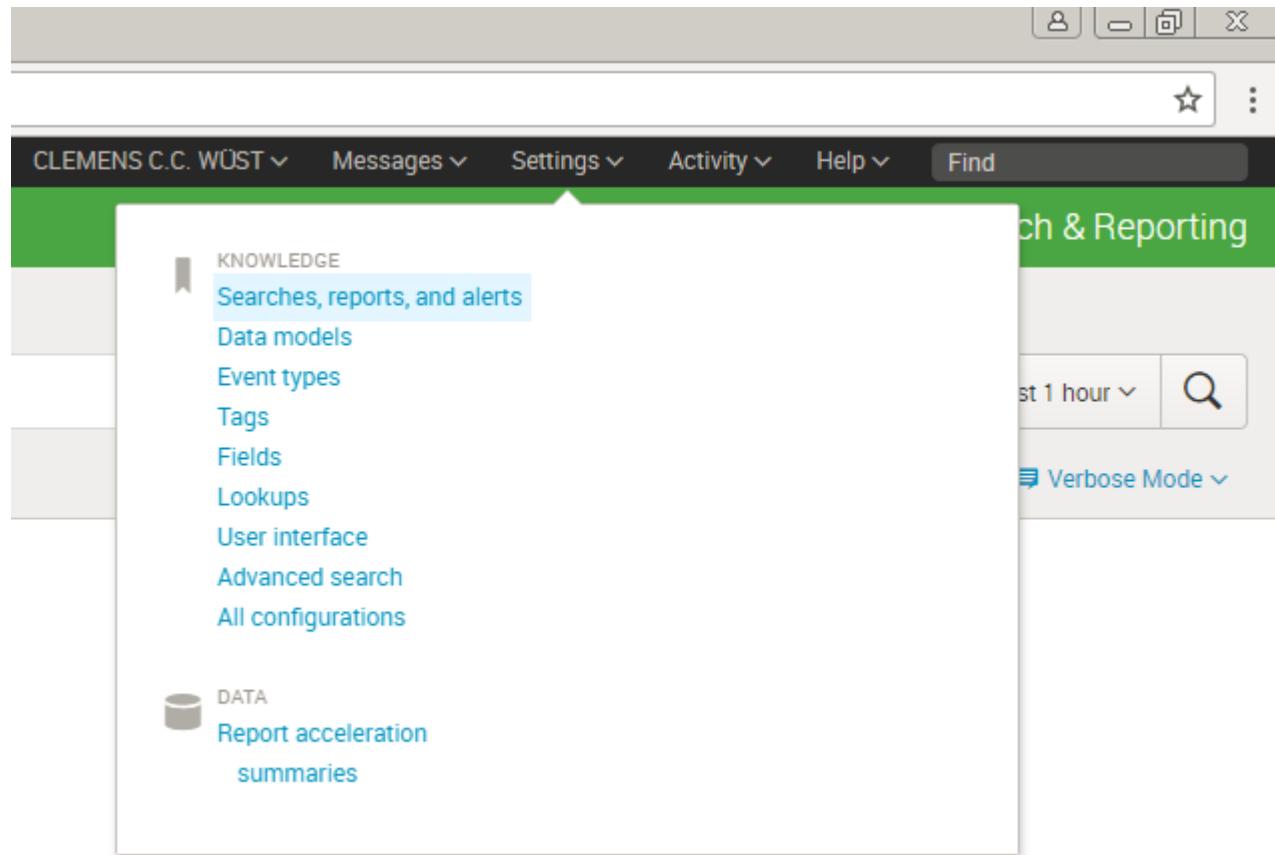
Dag	2016W47 (21NOV)	2017W47 (20NOV)
MAANDAG	6,746	6,076
DINSDAG	5,649	8,629
WOENSDAG	4,915	7,415
VRIJDAG	3,965	5,868
ZATERDAG	2,407	4,192
ZONDAG	3,263	5,812

Week	Waarde
2017W07 (13FEB)	~100,000
2017W08 (20FEB)	~100,000
2017W09 (03MRT)	~300,000
2017W10 (10MRT)	~400,000
2017W11 (17MRT)	~800,000
2017W12 (24MRT)	~900,000
2017W13 (03APR)	~500,000
2017W14 (10APR)	~500,000
2017W15 (17APR)	~600,000
2017W16 (24APR)	~100,000
2017W17 (01MEI)	~1,100,000
2017W18 (08MEI)	~100,000
2017W19 (15MEI)	~100,000
2017W20 (22MEI)	~100,000
2017W21 (29MEI)	~100,000
2017W22 (05JUN)	~100,000
2017W23 (12JUN)	~100,000
2017W24 (19JUN)	~100,000
2017W25 (03JUL)	~100,000
2017W26 (10JUL)	~100,000
2017W27 (17JUL)	~100,000
2017W28 (03AUG)	~100,000
2017W29 (10AUG)	~100,000
2017W30 (17AUG)	~100,000
2017W31 (31AUG)	~100,000
2017W32 (07AUG)	~100,000
2017W33 (14AUG)	~100,000
2017W34 (21AUG)	~100,000
2017W35 (28AUG)	~100,000
2017W36 (04SEP)	~100,000
2017W37 (11SEP)	~100,000
2017W38 (18SEP)	~100,000
2017W39 (25SEP)	~100,000
2017W40 (02OKT)	~100,000
2017W41 (09OKT)	~100,000
2017W42 (16OKT)	~100,000
2017W43 (23OKT)	~100,000
2017W44 (30OKT)	~100,000
2017W45 (06NOV)	~100,000
2017W46 (13NOV)	~100,000

Stap 3: Wijzig de opmaak van het Dashboard

10/19

Ga naar **Settings** → **User interface**



The screenshot shows the Splunk User interface with the title 'User interface'. On the left, there is a sidebar with the following links:

- Time ranges (highlighted with a red box)
- Views
- View PDF scheduling
- Navigation menus
- Prebuilt panels
- Bulletin messages

The main content area displays these same links under the heading 'Actions' with the sub-option 'Add new' next to each:

- Actions
Add new
- Actions
Add new
- Actions
Add new

At the bottom of the page, there are links for 'About', 'Support', 'File a Bug', and 'Documentation', along with a copyright notice: '© 2005-2017 Splunk Inc. All rights reserved.'

Kies voor Owner → Je eigen naam

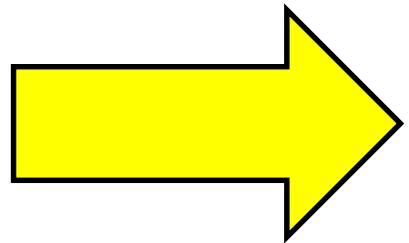
12/19

The screenshot shows the Splunk UI for managing views. The URL is https://splunk.belastingdienst.nl/en-US/manager/search/data/ui/views. The top navigation bar includes 'splunk', 'Apps', 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. The current user is CLEMENS C.C. WÜST. The main area is titled 'Views' under 'User interface'.

On the left, there's a sidebar with a 'New' button and a list of view names: 4hr_msu_areachart, _admin, agsperformance, alert, alerts, analytics_dashboard, app_analytics, b, batch, brm_cbd_dashboard, brm_dashboard, brm.osa.dashboard, brm_sea_dashboard, capture_ip_addresses, charting, cics, and nice_transaction_drilldown.

The main content area shows a table of views. A red box highlights the 'Owner' dropdown menu in the top-left corner of the table header. The dropdown menu has four options: 'Any', 'Any', 'CLEMENS C.C. WÜST (wustc00)', and 'No owner'. The 'CLEMENS C.C. WÜST (wustc00)' option is selected and highlighted in blue.

View name	Type	Owner	Actions
4hr_msu_areachart	search	App Permissions	Enabled Open Clone Move Delete
_admin	search	App Permissions	Enabled Open Clone Move Delete
agsperformance	search	App Permissions	Enabled Open Clone Move Delete
alert	search	App Permissions	Enabled Open Clone Move Delete
alerts	search	App Permissions	Enabled Open Clone Move Delete
analytics_dashboard	search	App Permissions	Enabled Open Clone Move Delete
app_analytics	search	App Permissions	Enabled Open Clone Move Delete
b	search	App Permissions	Enabled Open Clone Move Delete
batch	search	App Permissions	Enabled Open Clone Move Delete
brm_cbd_dashboard	search	App Permissions	Enabled Open Clone Move Delete
brm_dashboard	search	App Permissions	Enabled Open Clone Move Delete
brm.osa.dashboard	search	App Permissions	Enabled Open Clone Move Delete
brm_sea_dashboard	search	App Permissions	Enabled Open Clone Move Delete
capture_ip_addresses	search	splunk_app_stream	Global Permissions
charting	search	Global Permissions	Enabled Open Clone
cics	search	App Permissions	Enabled Open Clone Move Delete
nice_transaction_drilldown	search	App Permissions	Enabled Open Clone Move Delete



Kies bij het betreffende Dashboard voor Open

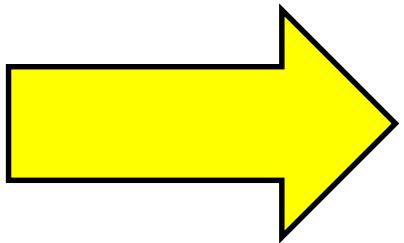
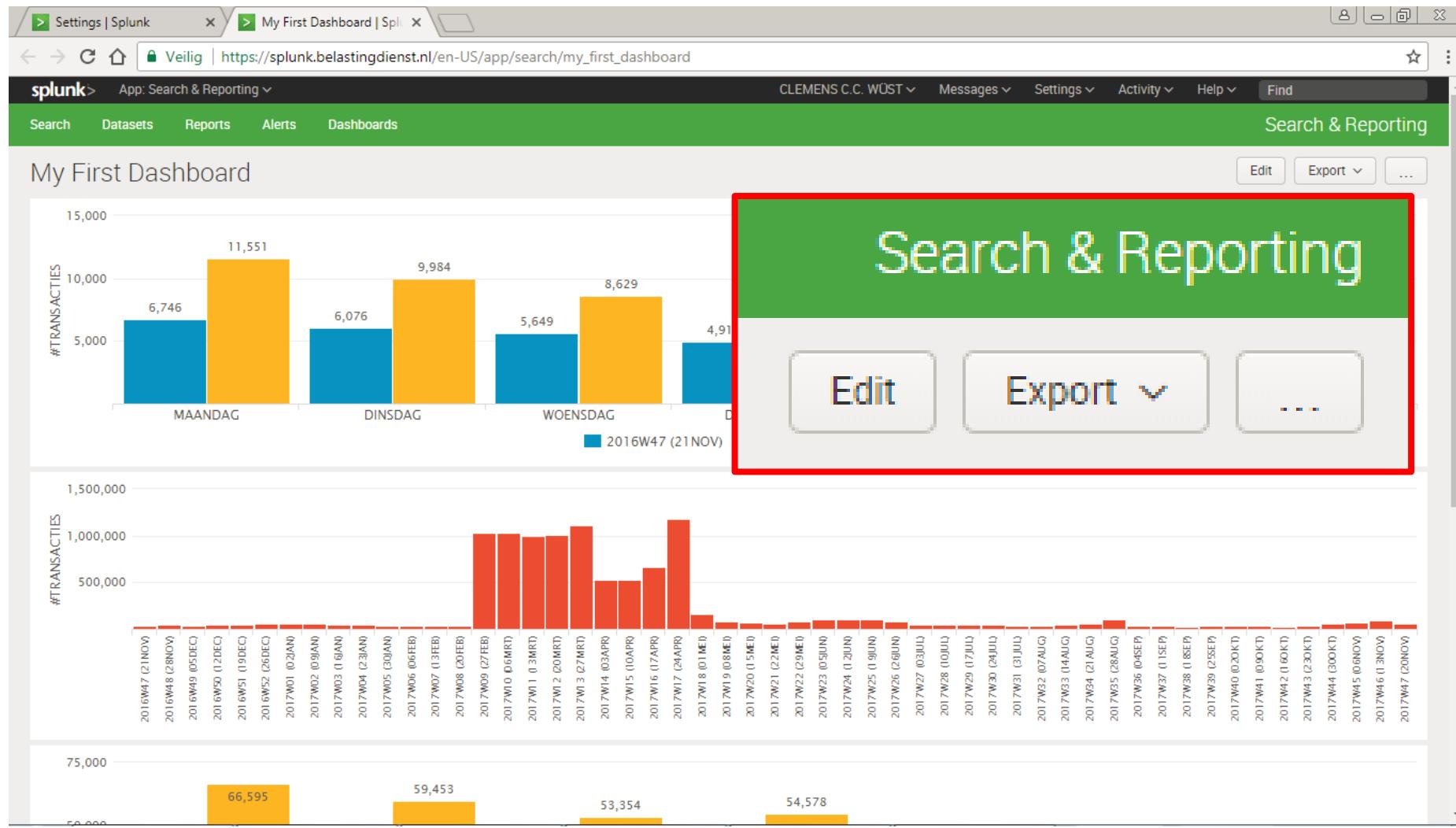
13/19

The screenshot shows the Splunk UI for managing views. The URL in the browser is <https://splunk.belastingdienst.nl/en-US/manager/search/data/ui/views?ns=search&pwnr=wustc00&search=&count=25>. The top navigation bar includes links for Settings, Apps, CLEMENS C.C. WÜST, Messages, Settings, Activity, Help, and Find. The main title is "Views" under "User interface > Views". Below the title, there are filters for App context (Search & Reporting (search)), Owner (CLEMENS C.C. WÜST (wustc)), and a search bar. A checkbox for "Show only objects created in this app context" is checked. A large green "New" button is visible. The table below shows one item: "my_first_dashboard" owned by "wustc00" in the "search" app, with "Private | Permissions" sharing, "Enabled" status, and actions "Open | Clone | Move | Delete". A red box highlights the "Actions" column. A yellow arrow points to the right side of the page.

View name	Owner	App	Sharing	Status	Actions
my_first_dashboard	wustc00	search	Private Permissions	Enabled	Open Clone Move Delete

Kies voor **Edit** om het Dashboard te bewerken

14/19



Klik met de muis om het Dashboard een nieuwe titel te geven

15/19

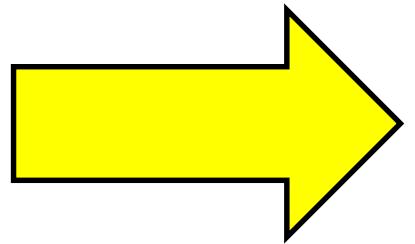
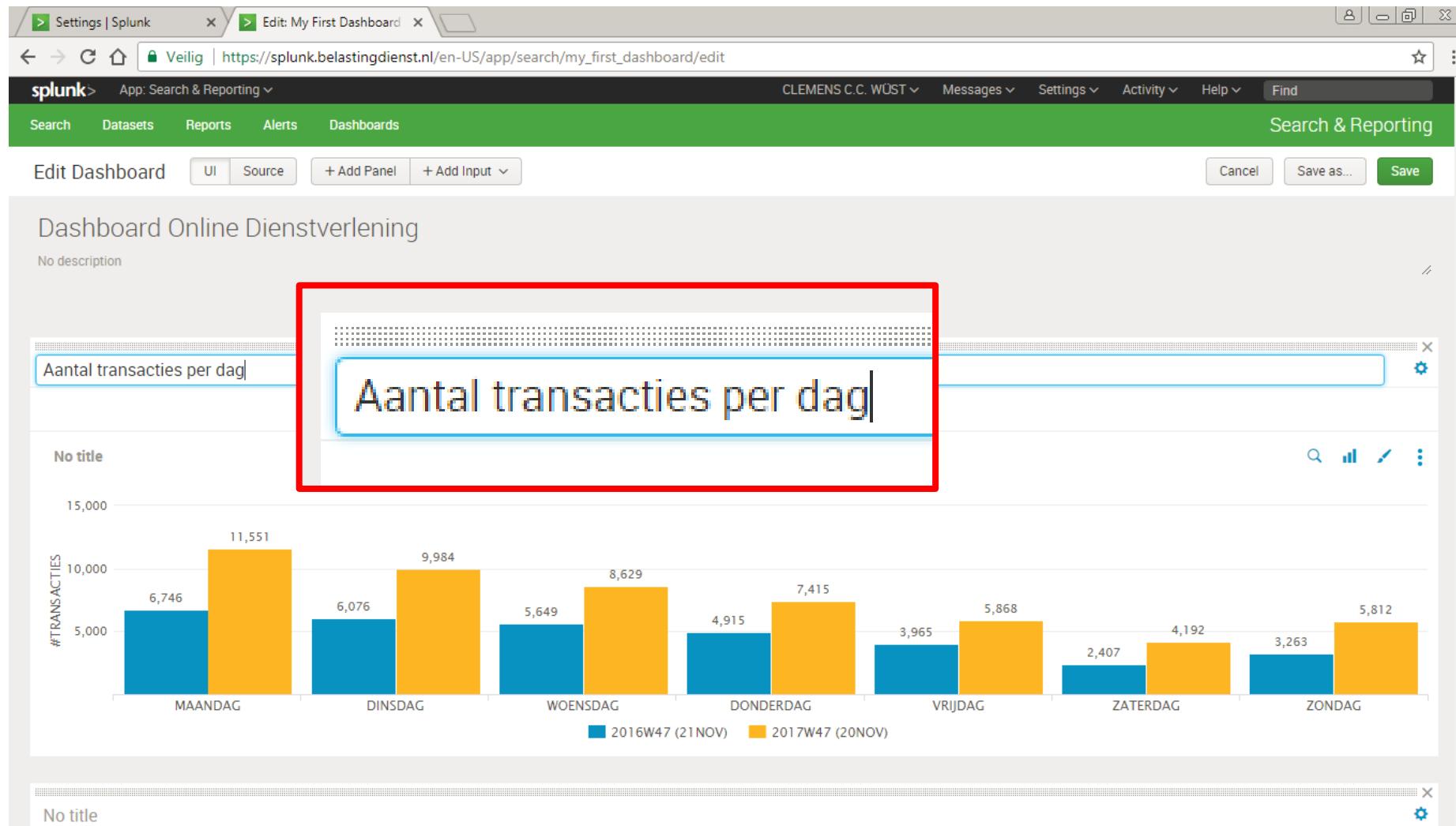
Screenshot of the Splunk interface showing the 'Edit Dashboard' screen. A red box highlights the title input field, which contains the text 'Dashboard Online Dienstverlening'. Below it is a placeholder 'No description'. To the right of the title input is a large yellow arrow pointing to the right.

The dashboard itself displays a bar chart comparing transaction volumes between two time periods: 2016W47 (21NOV) and 2017W47 (20NOV). The Y-axis represents the number of transactions (#TRANSACTIES), ranging from 0 to 15,000. The X-axis lists the days of the week: MAANDAG, DINSDAG, WOENSDAG, DONDERDAG, VRIJDAG, ZATERDAG, and ZONDAG. The chart shows the following data:

Dag	2016W47 (21NOV)	2017W47 (20NOV)
MAANDAG	6,746	11,551
DINSDAG	6,076	9,984
WOENSDAG	5,649	8,629
DONDERDAG	4,915	7,415
VRIJDAG	3,965	5,868
ZATERDAG	2,407	4,192
ZONDAG	3,263	5,812

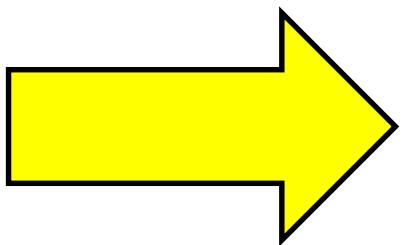
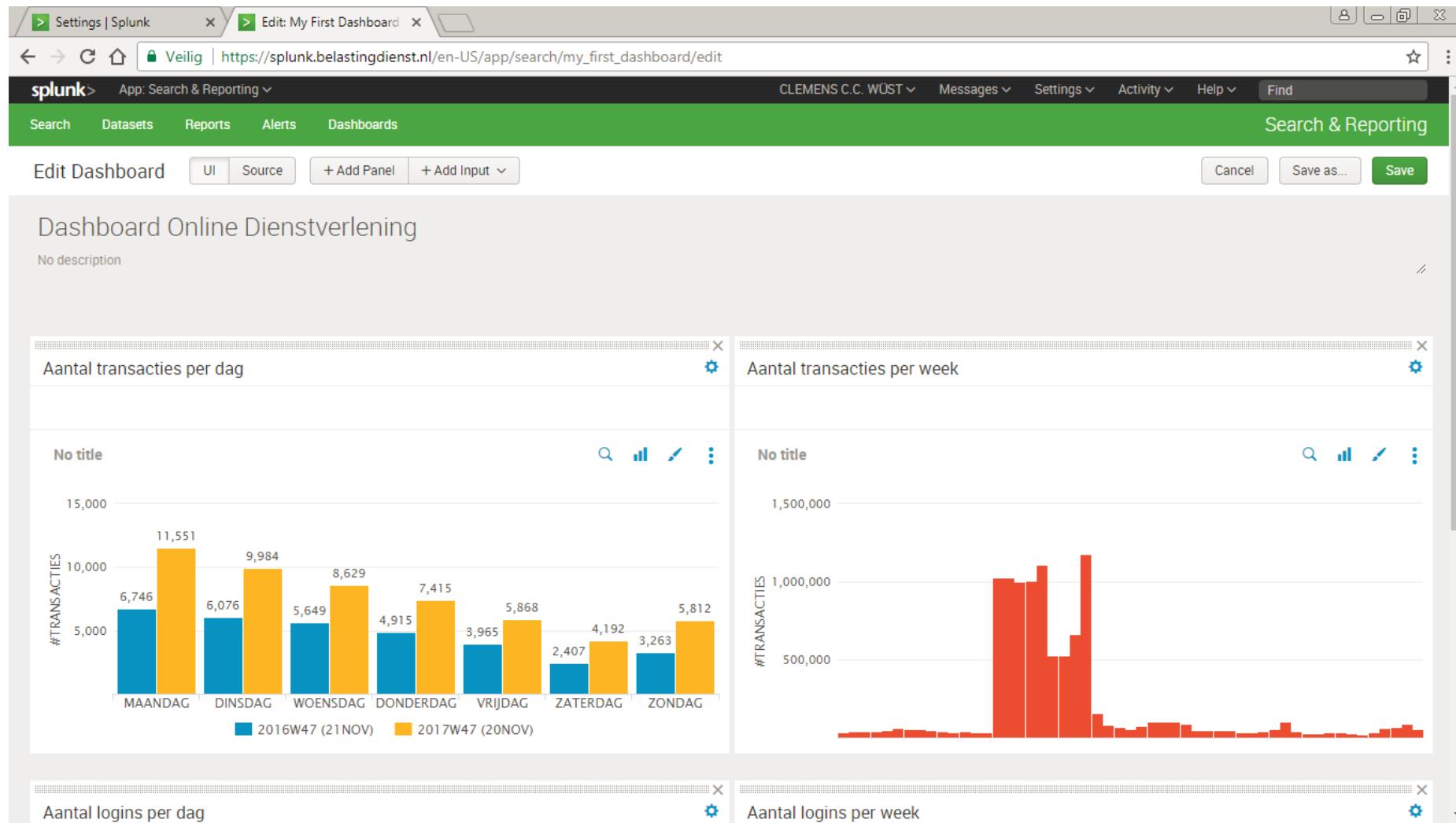
Klik met de muis om een Report een titel te geven

16/19



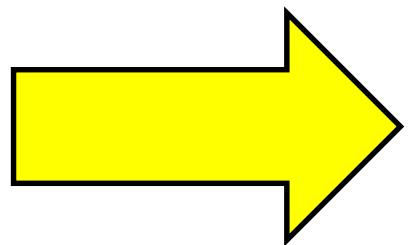
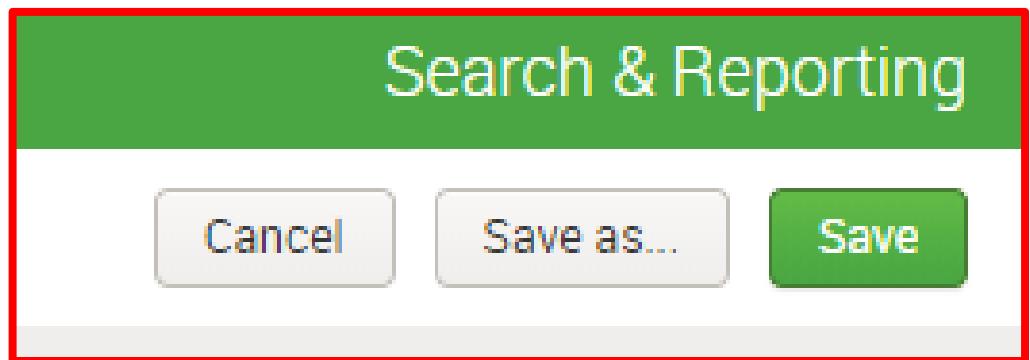
Gebruik de muis om de Reports te herpositioneren t.o.v. elkaar

17/19



Als je klaar bent, druk rechtsbovenin op Save

18/19



Gefeliciteerd met je nieuwe Dashboard!

19/19

