Nagios & Squared up (SCOM)

SECURITY – LOGS ANALYSEREN / FILTEREN / DASHBOARDS

Realisatie

3ITF – Realisatie stage @ Essers

Timo Goossens 3CSS

Academiejaar 2023-2024

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

INHOUDSTAFEL

1 INLEIDING

Een stage is een belangrijk moment in het studietraject, je leert er veel dingen bij die je op school niet snel tegenkomt. Je leert omgaan met collega's en de sfeer op de werkvloer. In dit document ga ik het hebben over mijn stage bij Essers.

1.1 Het stagebedrijf

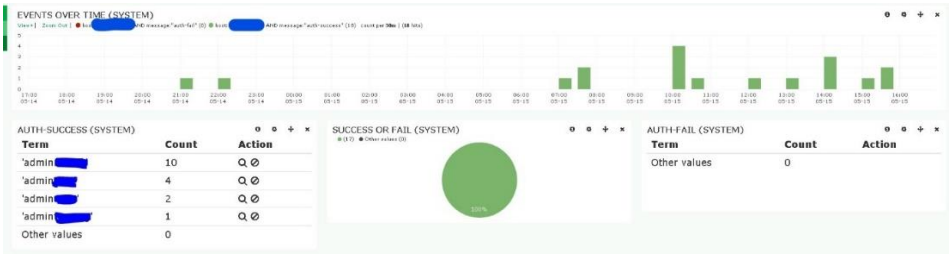
De vorige 13 weken heb ik gewerkt aan mijn stageopdrachten, dit heb ik gedaan bij Essers een bedrijf met het hoofdkantoor van de IT gelegen in Genk.

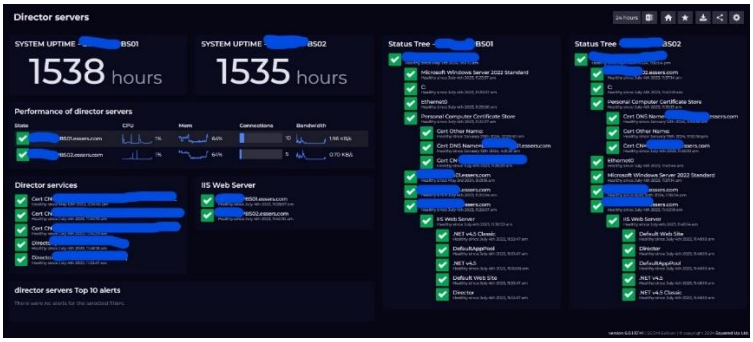
Essers is een bedrijf gelegen in Genk, ze bieden gepersonaliseerde en geïntegreerde oplossingen voor duurzaam transport en logistiek in heel Europa. Al deze infrastructuur heeft natuurlijk ook een grote IT-afdeling nodig om alles vlot te laten verlopen. In Genk zorgen ze dat dit in goede banen loopt voor heel Essers maar Essers heeft ook zusterbedrijven en zij krijgen natuurlijk ook IT-support van Essers.

H.ESSERS
IT'S TRANSPOSSIBLE.

1.2 De opdracht

13 weken geleden heb ik de opdracht gekregen om ervoor te zorgen dat de hele IT-afdeling een beter overzicht kreeg over de IT-infrastructuur. Dit was een hele opgave want ik had geen idee wat er allemaal bij kwam kijken, Essers heeft dan ook onnoemelijk veel IT-systemen en een eigen datacenter met veel systemen. Het doel van de opdracht verschillende kritische componenten monitoren en centraliseren door middel van query's, filters en alerts in monitoring/logging tools zoals Nagios Log Server en Squared up (SCOM).





2 HET PLAN

Squared Up (6 weken)

Dashboards (core components) (health states – geen ping, vooral services!)

- **Citrix infrastructure ([redacted]) (1)**
- **Exchange (on prem + M365)**
- **Domain controllers (1) ([redacted])**
- **Remote sites (1) ([redacted])**
- **Firewall – Palo alto (2) ([redacted])**
- **SQL ([redacted]) (1) X**
- **ClearPass ([redacted])**
- **Top 10 authentication error logs (1)**
- **Datacenter (3)**
- **Server / network components uptime ([redacted])**
- **Anti-Virus (XDR) status ([redacted]) (2)**
- **Privileged accounts activity (1)**
- **Health checks van buitenaf (3rd party)**

Nagios (6 weken)

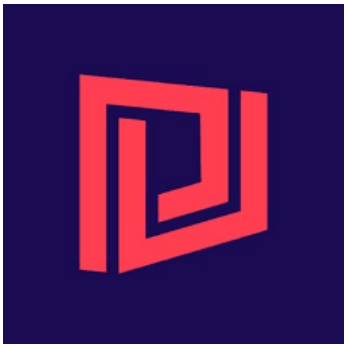
- **Query's bouwen**
- **Sources toevoegen (indien mogelijk)**
- **Bestaande sources filteren**
- **Notificaties sturen**
- **Upgraden en Certificaat in orde brengen (samen met [redacted])**

3 KENNIS OPDOEN

De eerste stap voor het maken van dit project was het opnemen van kennis. Alle tools die ik gebruikt heb in dit project zijn dan ook nieuw voor mij dus het was heel belangrijk dat ik voldoende kennis opdeed om te kunnen beginnen.

3.1 Squared up

Zoals ik al zei had ik geen kennis van Squared up maar heb veel informatie opgezocht en hulp gevraagd aan de SCOM (Squared up) expert, hij heeft mij uitgelegd hoe de Squared up in elkaar zit en dat SCOM een grote factor speelt in de werking van Squared up. Als ik iets nodig had kon ik het ook altijd aan hem vragen. Tenslotte heb ik ook veel YouTube video's gekeken zodat ik nog meer kennis kon opdoen.



3.2 Nagios Log Server

Ook bij deze tool was ik een nieuwkomer en moest dus ook nog veel leren. Dit heb ik gedaan door zo veel mogelijk opzoek werk maar de documentatie van Nagios is aan de magere kant.

Nagios®

Bij deze tool heb ik het principe van al doende leert men toegepast om zo veel mogelijk progressie te boeken en kennis op te doen. Ik begon dus ook al snel uit te zoeken hoe de basics van deze tool werkte. Later in de stage heb ik dit tot een ander niveau getild.

4 DE PRAKTIJK

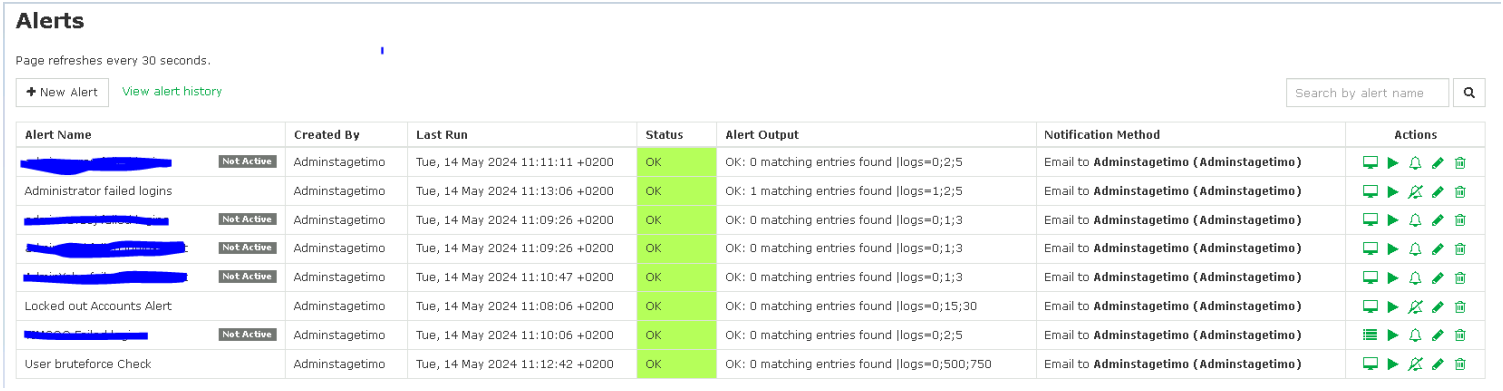
Natuurlijk heb ik ook iets gerealiseerd. In dit deel laat ik zien wat ik gerealiseerd heb.

4.1 Nagios Log Server

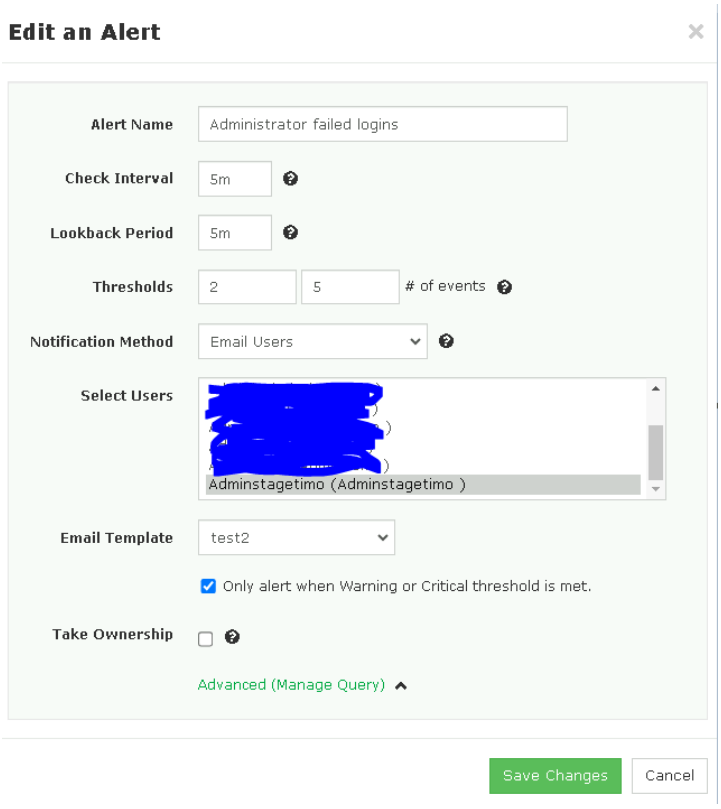
In dit gedeelte vindt u het bewijs voor de realisatie in Nagios.

4.1.1 Alerts

De eerste weken heb ik mij verdiept in alerts en alles wat erbij hoort.



In de screenshot zie je dat er maar enkele alerts actief zijn. Dit komt omdat dit de meest voor de hand liggende en nuttige alerts zijn en ik anders een overvolle mailbox had.

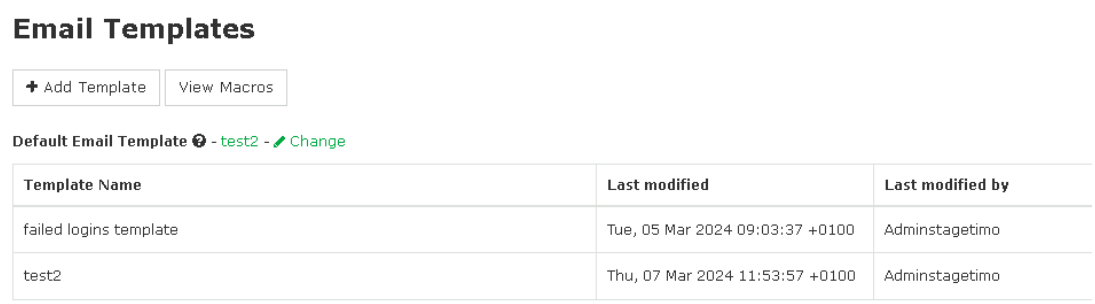


Hier een close-up op hoe een alert in Nagios in elkaar zit.

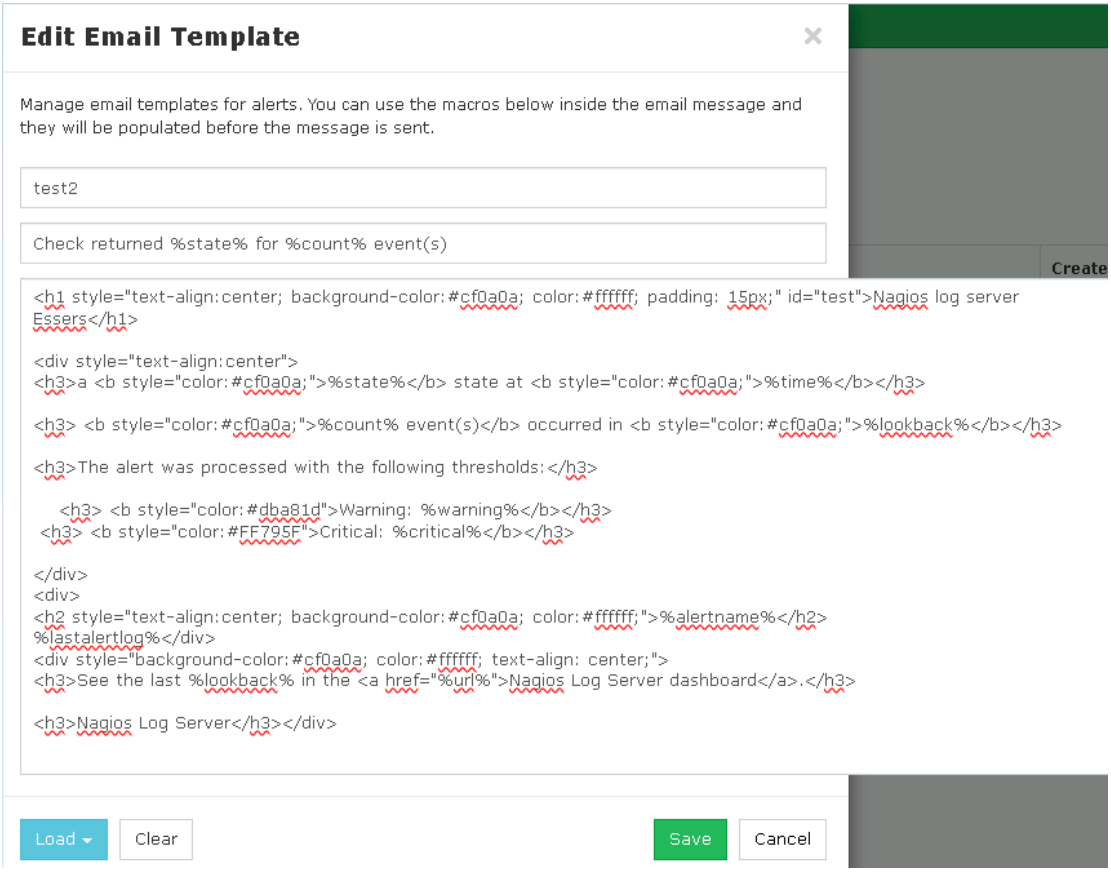
Zoals je in bovenstaande screenshot ziet kunnen we van alles instellen zoals:

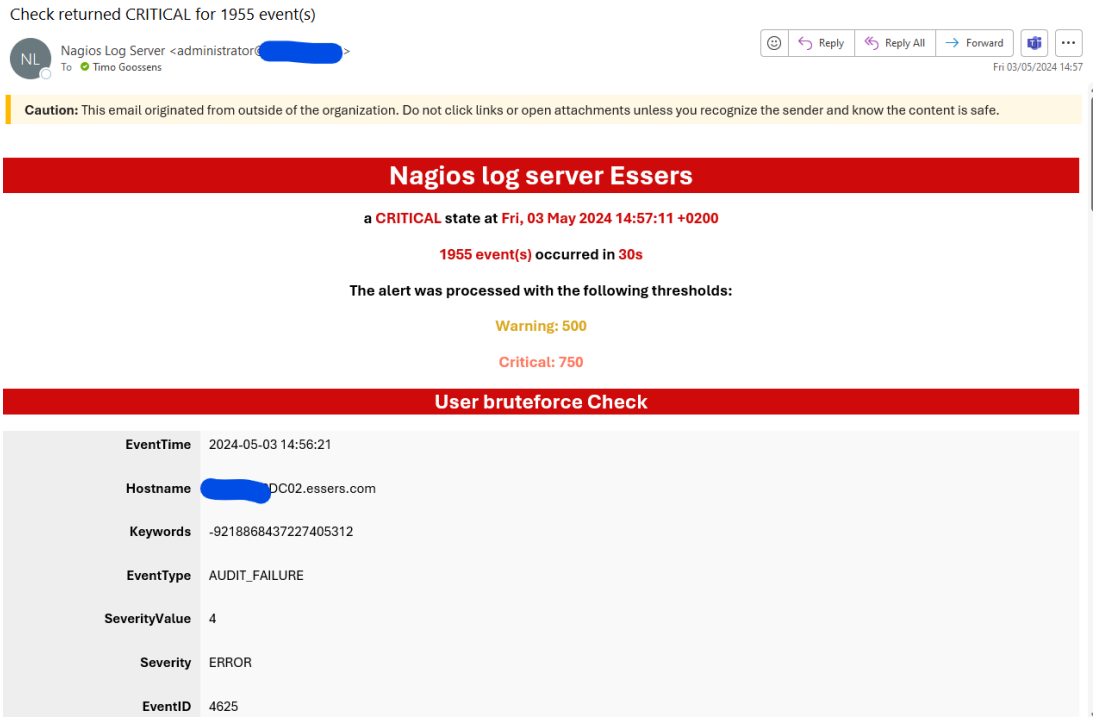
- *Intervallen*
- De *thresholds* voor *warning* en *critical*
- Hoe er een notificatie gestuurd wordt (via mail)
- Welke users een melding krijgen
- Welke template we willen gebruiken (zie screenshot hieronder)

Dit waren de belangrijkste delen van een alert in Nagios aangezien de overige delen voor zichzelf spreken en ik het zo kort mogelijk wil houden gaan we verder naar het volgende gedeelte.



Dit zijn 2 templates waarvan test2 als default gezet is omdat deze de laatste en nieuwst gemaakte template was. In de onderstaande screenshots zie je de code en het resultaat.




Check returned CRITICAL for 1955 event(s)

NL Nagios Log Server <administrator@[redacted]>
To Timo Goossens

Reply | Reply All | Forward

Fri 03/05/2024 14:57

Caution: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Nagios log server Essers

a CRITICAL state at Fri, 03 May 2024 14:57:11 +0200

1955 event(s) occurred in 30s

The alert was processed with the following thresholds:

Warning: 500

Critical: 750

User bruteforce Check

EventTime	2024-05-03 14:56:21
Hostname	[redacted]DC02.essers.com
Keywords	-9218868437227405312
EventType	AUDIT_FAILURE
SeverityValue	4
Severity	ERROR
EventID	4625

Ikzelf vind het er niet slecht uit zien maar nu wat meer uitleg hierover.

Info in mail *template*:

- De *state*
- Tijdstip
- Aantal events en in welke tijdsspanne
- De waarde v/d *thresholds*
- Naam v/d alert
- Laatste alert met betrekking tot de melding (is niet volledig zichtbaar in screenshot 5)

Ik heb dus een mail gekregen van de Nagios log server die buiten het Essers domain zit voor security redenen, daarom krijg ik de "*Caution"* melding. Het leuke aan deze alerts is dat ik er weldegelijk iets mee bereikt heb want zoals je ziet zijn er wel heel veel *failed logins* op met het account 'user'. Ik heb dit dan ook aan mijn mentor laten weten en hij is hier mee verder gegaan. Dit was niet het enige want dit gebeurden ook met het Administrator account. (Zie dashboards in Nagios gedeelte)

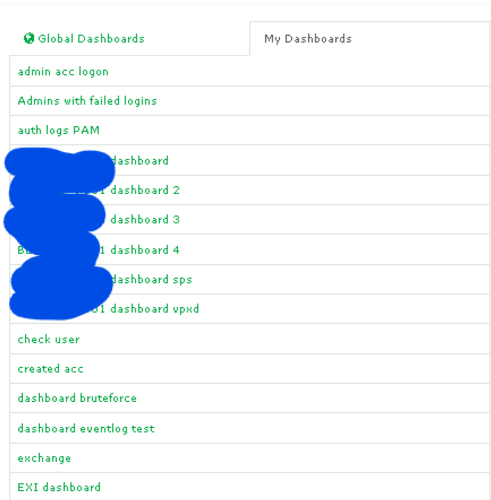
Host Freshness Alerts

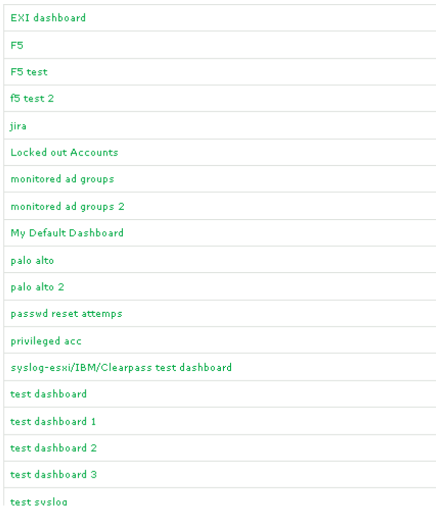
Alert Name		Created By	Last Run	Status	Alert Output	Notification Method	Actions
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:06:06 +0200	CRITICAL	CRITICAL: 1 non-sending hosts found |hosts=1;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Tue, 26 Mar 2024 08:33:46 +0100	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Tue, 26 Mar 2024 08:34:06 +0100	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Tue, 26 Mar 2024 08:34:06 +0100	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Tue, 26 Mar 2024 08:34:06 +0100	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:06:27 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:09:43 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:06 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:06 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:06 +0200	CRITICAL	CRITICAL: 1 non-sending hosts found |hosts=1;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
[redacted]	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	
localhost	Not Active	Adminstagetimo	Wed, 15 May 2024 15:10:07 +0200	OK	OK: 0 non-sending hosts found |hosts=0;0;0	Email to **Adminstagetimo (Adminstagetimo)**	

Om het alert gedeelte af te sluiten is er ook nog een “*host freshness alert*”. Deze alert kan ingesteld worden om te testen of *hosts* bereikbaar zijn via ping. Zoals je ziet in de screenshot werkte het niet altijd even goed op dat moment dus heb ik besloten deze te deactiveren aangezien ik nog volop aan het uitzoeken was hoe ik Nagios moest gebruiken.

4.1.2 Dashboards in Nagios

In Nagios heb je ook dashboards en daar heb ik ook gebruik van gemaakt. Deze kunnen handig zijn in het opsporen van logs aangezien Nagios bedoeld is om logs te centraliseren op 1 punt.



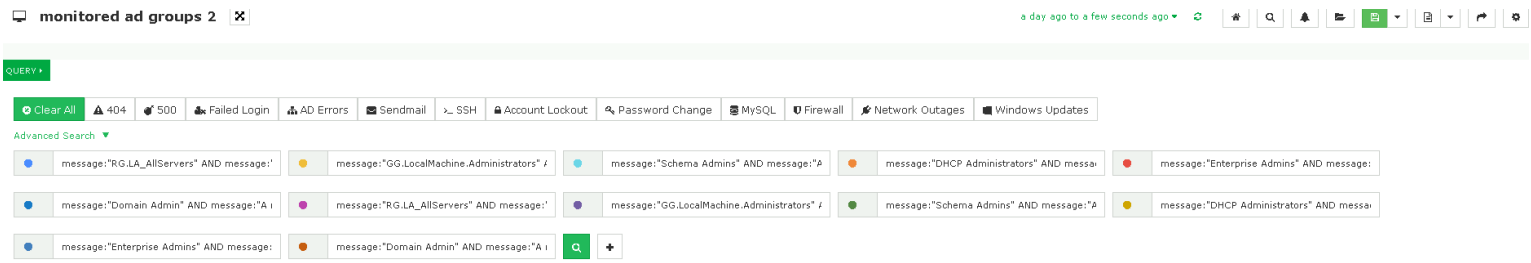


In deze screenshot zie je al de dashboards die ik tot nu toe gemaakt heb maar ze zijn zeker niet allemaal perfect. Ik heb veel moeten proberen om uiteindelijk een goed resultaat te bekomen. In de volgende screenshots gaan we de meest relevante dashboards bekijken. De volgende punten heb ik gerealiseerd in Nagios:

1. Monitored AD groups membership changes.
2. Palo alto logins
3. F5 logins en errors
4. Locked users
5. Privileged accounts logins
6. Bekijken welke event ID’s overbodig zijn

Nummer 1:

Dit is het dashboard "monitored AD groups 2"



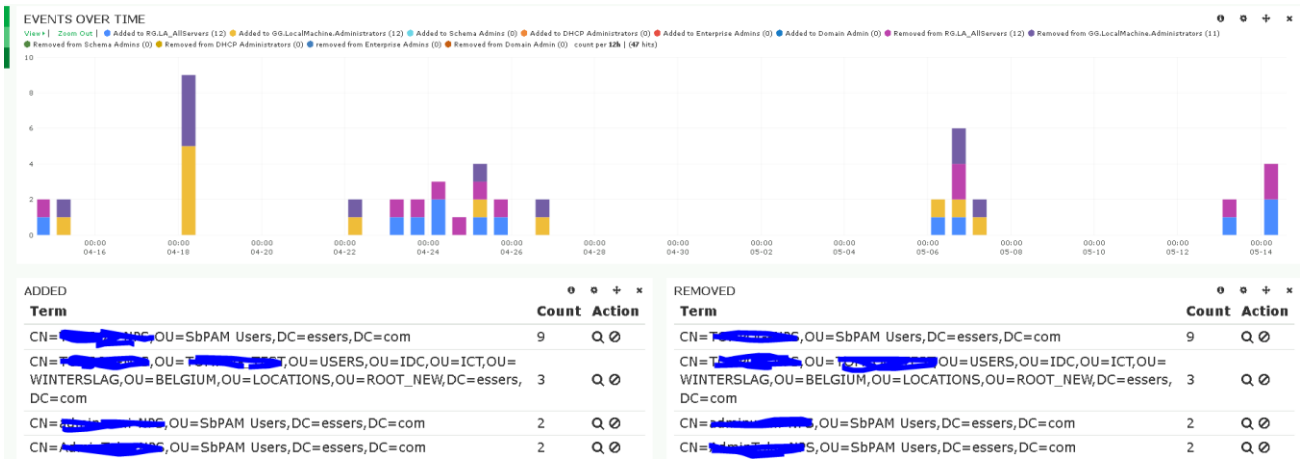
Hier zie je de query's voor membership changes. In dit dashboard wordt dus getoond of er iemand wordt toegevoegd aan een bepaalde groep of dat er iemand wordt verwijderd uit een bepaalde groep.

Query voor toegevoegde members:

message:" [placeholder v/d AD groep naar keuze]" AND message: "A member was added to a security enabled global group."

Query voor verwijderde members:

message:" [placeholder v/d AD groep naar keuze]" AND message: "A member was removed from a security enabled global group."



In deze screenshot zie je het dashboard met Events over time waar je ziet welke events wanneer gebeurd zijn en daaronder een tabel met toegevoegde members en een tabel met verwijderde members. Normaal gezien zouden deze 2 gelijk moeten staan aan elkaar want binnen Essers wordt gebruikgemaakt van bepaalde securitymaatregelingen die ervoor zorgen dat je niet voor altijd de rechten hebt die je aangevraagd hebt. Hier komt in de loop van de documentatie over stage nog informatie over. Ook kun je in de dashboards bepalen op welke tijdstippen je wilt gaan monitoren, deze screenshot speelt zich af in een periode van 30 dagen.

ALL EVENTS

Show Fields

0 to 47 of 47 available for paging

@timestamp	host	type	message
2024-05-14T12:04:18.616+02:00	[redacted]	eventlog	A member was removed from
2024-05-14T10:55:35.381+02:00	[redacted]	eventlog	A member was removed from
2024-05-14T10:03:34.070+02:00	[redacted]	eventlog	A member was added to
2024-05-14T08:56:24.978+02:00	[redacted]	eventlog	A member was added to
2024-05-13T11:41:47.415+02:00	[redacted]	eventlog	A member was removed from
2024-05-13T09:42:46.631+02:00	[redacted]	eventlog	A member was added to
2024-05-07T13:02:42.974+02:00	[redacted]	eventlog	A member was removed from
2024-05-07T11:57:51.095+02:00	[redacted]	eventlog	A member was added to
2024-05-06T17:40:35.966+02:00	[redacted]	eventlog	A member was removed from
2024-05-06T17:14:53.257+02:00	[redacted]	eventlog	A member was removed from
2024-05-06T16:54:47.748+02:00	[redacted]	eventlog	A member was added to
2024-05-06T15:40:57.586+02:00	[redacted]	eventlog	A member was added to
2024-05-06T15:17:21.547+02:00	[redacted]	eventlog	A member was removed from
2024-05-06T15:11:51.167+02:00	[redacted]	eventlog	A member was removed from
2024-05-06T13:17:47.893+02:00	[redacted]	eventlog	A member was added to
2024-05-06T11:52:49.173+02:00	[redacted]	eventlog	A member was added to
2024-04-26T16:00:08.706+02:00	[redacted]	eventlog	A member was removed from

Onderaan de vorige visualisaties vindt u ook nog alle logs terug van de waargenomen events. Als je op deze klikt zal u nog meer informatie kunnen krijgen over de log waar je op klikt.

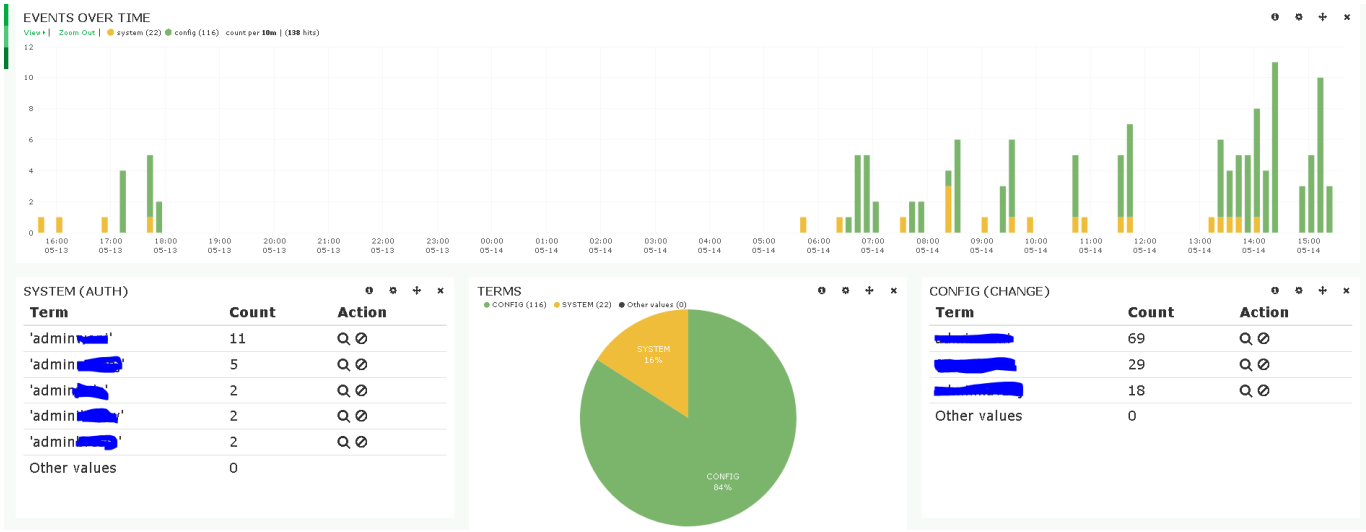
Nummer 2:

Palo alto dashboard:

Query's:

Host: [placeholder van Ip palo alto] AND sysorconf: SYSTEM

Host: [placeholder van Ip palo alto] AND sysorconf:CONFIG



Dit zijn de events over time. Hier zie je welke events wanneer zijn gebeurd. Er zijn ook tabellen met de users die inloggen of uitloggen en een tabel met users die aan het configureren zijn. De *pie chart* is om een overzicht te krijgen van de authenticatie logs en de configuratie logs.

Er zijn ook nog 2 tabellen, 1 voor SYSTEM en 1 voor CONFIG. In deze tabellen kun je per soort zien welke logs erbinnen komen met de belangrijkste filters direct zichtbaar en als je klikt op een log dan krijg je een *extended* versie van die log.

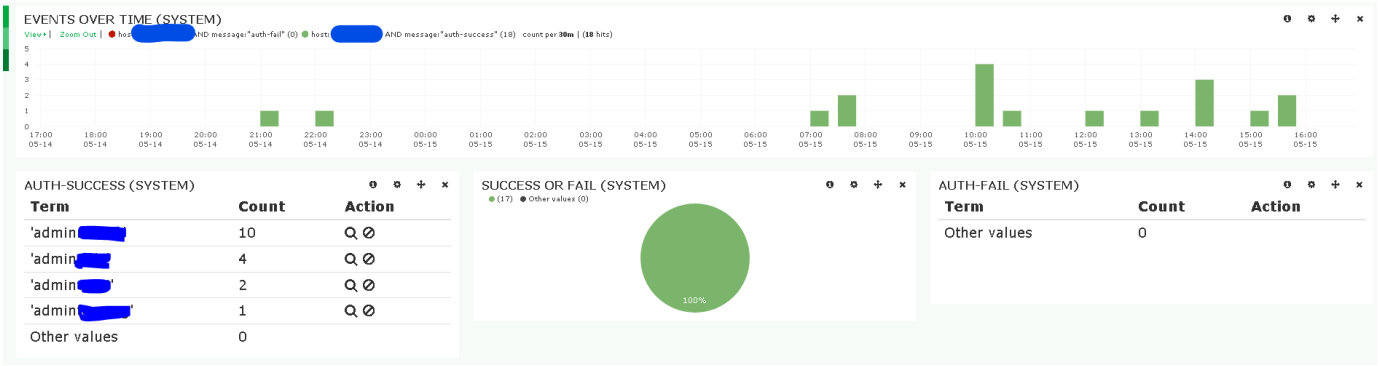
Onderaan in het dashboard vind je zoals in het vorig dashboard nog een tabel met alle logs over de Palo alto.

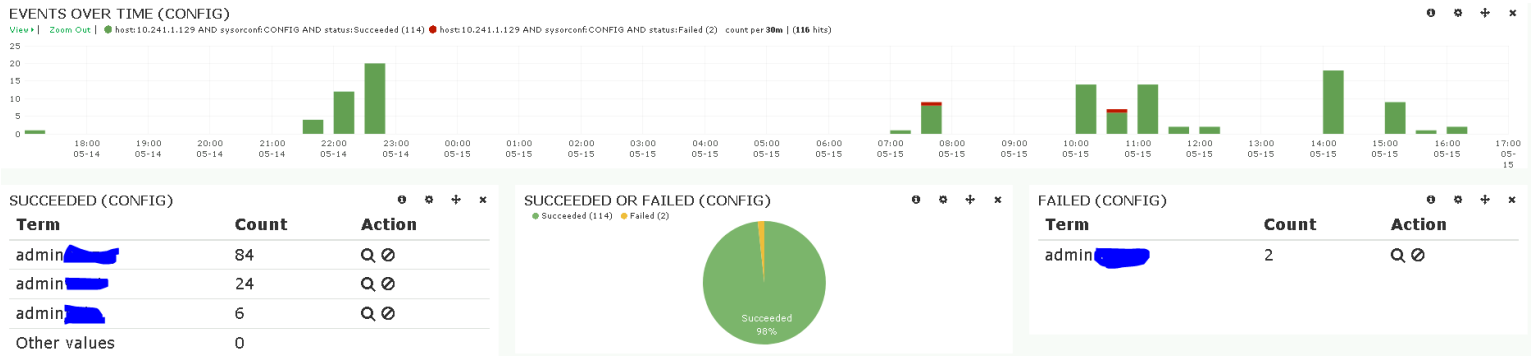
Palo alto 2 dashboard:

Query's:

Host: [placeholder van Ip palo alto] AND message:" auth-success"

Host: [placeholder van Ip palo alto] AND message:" auth-fail"





Hier ligt de focus op het kijken of de user met succes of met geen succes heeft ingelogd. Dit weer aan de hand van een events over time en 2 tabellen voor beide query's met in het midden een overzicht van de hoeveelheid door middel van een pie chart. Voor zover de dashboards van palo alto.

Nummer 3:

Dit zijn de dashboards van de F5 (loadbalancer)

F5 dashboard:

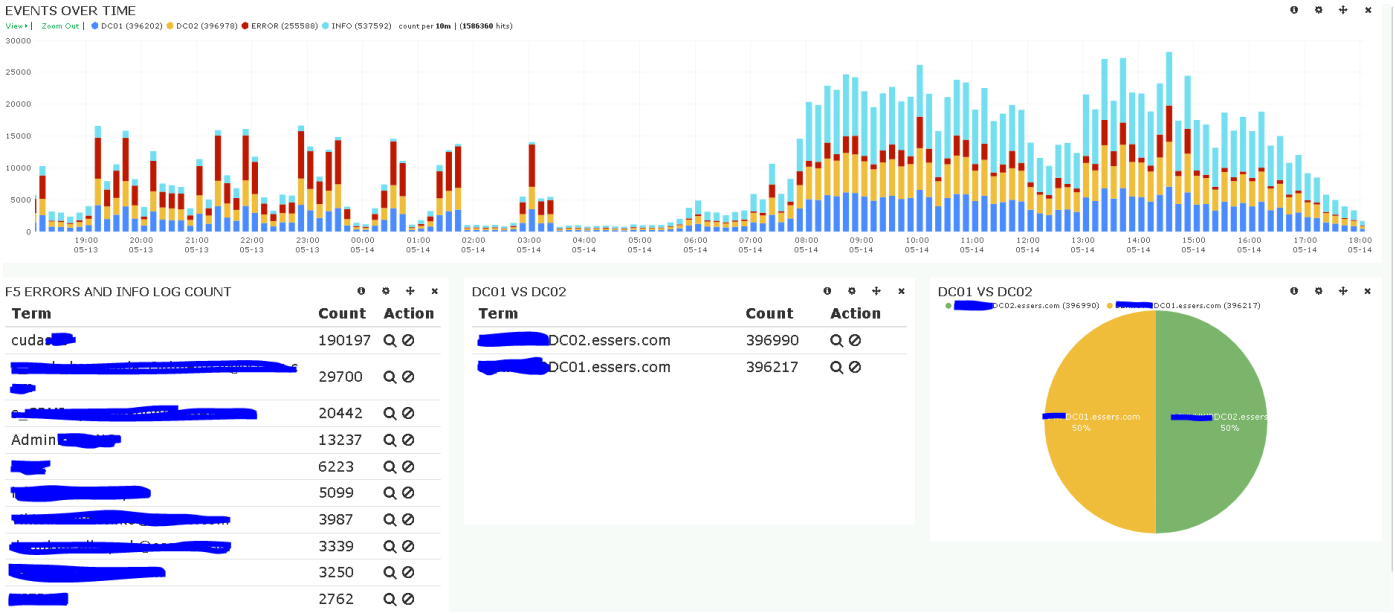
Query's:

Workstation:" [placeholder voor F5 auth server]" AND EventID:4776 AND Hostname:"[placeholder naam van Domain controller 1]"

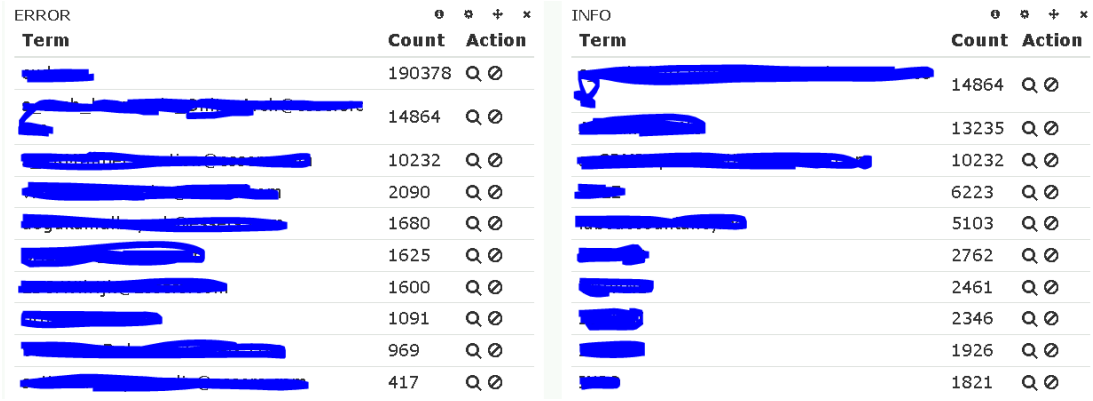
Workstation:" [placeholder voor F5 auth server]" AND EventID:4776 AND Hostname:"[placeholder naam van Domain controller 2]"

Workstation:" [placeholder voor F5 auth server]" AND Severity: ERROR

Workstation:" [placeholder voor F5 auth server]" AND Severity: INFO



Op dit dashboard zie je weer de events in time met daaronder de gebruikers/services met de meeste error and info logs achter hun naam. Daarnaast een overzicht van de verdeling van de logs onder de 2 domain controllers via een tabel en een pie chart.



Daaronder hebben we dan de Error en info log count apart in een tabel. Zodat je ziet welke gebruiker of service een error krijgt of gewoon een info log. Onder deze tabellen is er ook nog een tabel met alle logs van de query's.

In dit dashboard heb ik ook wat bellen laten rinkelen omdat er services bij stonden die normaal niet gebruikt worden of niet bekend voorkomen. Dit is leuk want je weet dat je het op die manier niet voor niks die.

Dit dashboard is gebaseerd op meldingen van F5authserver in de domain controllers in tegenstelling tot de volgende dashboards van F5

<u>Dashboard F5 test:</u>

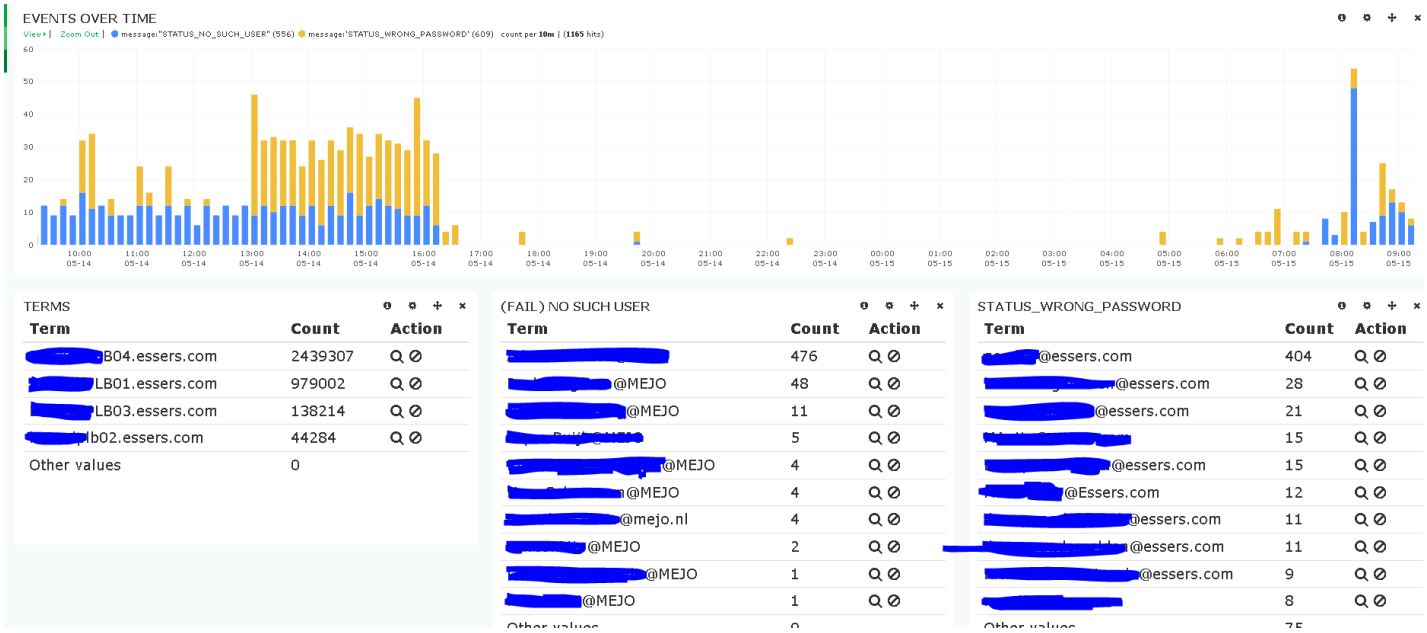
Query's:

message:"STATUS_NO_SUCH_USER"

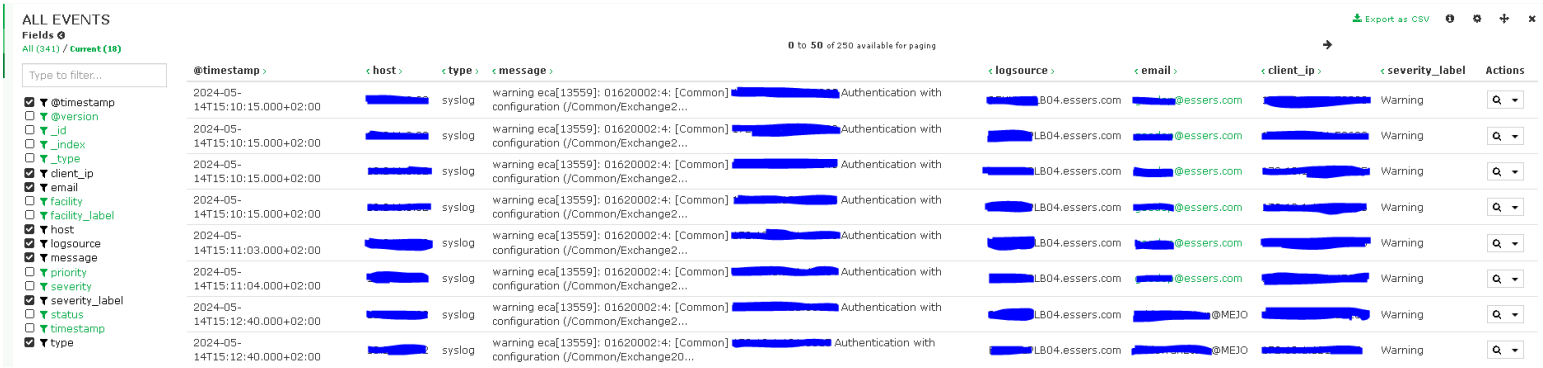
message:"STATUS_WRONG_PASSWORD"

Filters:

Logsource:"[naam van een F5 server]" OR logsource:"[naam van een F5 server]" OR logsource:"[naam van een F5 server]" OR logsource:"[naam van een F5 server]"



Hier zie je weer een events over time van de query's hierboven en daaronder hebben we een lijst met alle 5F servers (lb4 is voor authenticatie), een lijst met users die niet bestaan maar toch hebben proberen inloggen en een lijst met gebruikers die hun paswoord verkeerd hebben ingegeven.



Dit is weer een tabel met alle logs gerelateerd tot de query's en filters bovenaan maar ook de filters gemaakt in de nagios configuratie. Dit wordt later in het document behandeld.

<u>Dashboard F5 test 2:</u>

Query's:

message:"SSL Handshake failed"

status:[13814]

Filters:

Logsource:"[naam van een F5 server]" OR logsource:"[naam van een F5 server]" OR logsource:"[naam van een F5 server]" OR logsource:"[naam van een F5 server]" → must

message:"STATUS_NO_SUCH_USER" message:"STATUS_WRONG_PASSWORD" → must not

Hier hebben we weer een events over time dit geeft een makkelijk overzicht over hoeveel van elke soort log er is. Daarnaast heb ik daaronder 3 tabellen met als eerste de hoeveelheid "*failed SSL handshakes*" per server zoals je ziet is het alleen maar op de LB04 omdat dit de authenticatie server is. Vervolgens hebben we het IP dat voor de "*handshake*" vraagt en daarnaast het IP met dat wordt gecontacteerd.

AUTHENTICATION FAILED

Term	Count	Action
[redacted]LB04.essers.com	3625	
Other values	0	

USERS WHERE AUTHENTICATION FAILED

Term	Count	Action
[redacted]	2047	
[redacted]	1408	
[redacted]	26	
[redacted]	16	
[redacted]	13	
[redacted]	11	
[redacted]	11	
[redacted]	8	
[redacted]	8	
[redacted]	6	
Other values	71	

Daaronder hebben we dan de volgende query waarbij we 2 tabellen zien met in de eerste de hoeveelheid en in de andere de gebruikers met de “failed authentication”.

AUTHENTICATION FAILED

Export as CSV

0 to 10 of 50 available for paging

timestamp	logsource	message	user	Actions
May 15 10:23:10	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd62f7fe700> client[11]: DC[10.2...	[redacted]	
May 15 10:23:07	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd6454007 00> client[11]: DC[10.2...	[redacted]	
May 15 10:23:07	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd637fff700> client[11]: DC[10.2...	[redacted]	
May 15 10:21:26	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd6454007 00> client[11]: DC[10.2...	[redacted]	
May 15 10:21:26	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd62f7fe700> client[11]: DC[10.2...	[redacted]	
May 15 10:21:26	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd637fff700> client[11]: DC[10.2...	[redacted]	
May 15 10:16:41	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd62f7fe700> client[11]: DC[10.2...	[redacted]	
May 15 10:16:41	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd6454007 00> client[11]: DC[10.2...	[redacted]	
May 15 10:16:41	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd645c01700> client[11]: DC[10.2...	[redacted]	
May 15 10:16:08	[redacted]LB04.essers.com	warning nlad[13814]: 01620000:4: <0x7fd644bff700> client[11]: DC[10.2...	[redacted]	

0 to 10 of 50 available for paging

FAILED SSL HANDSHAKES

Export as CSV

0 to 10 of 50 available for paging

timestamp	type	host	logsource	message	protocol	FROM	TO	Actions
May 15 10:24:30	syslog	[redacted]	[redacted]LB04.essers.com	warning tmm2[18805]: 01260013:4: SSL Handshake failed for TCP [redacted] -> [redacted]	TCP	[redacted]	[redacted]	
May 15 10:24:06	syslog	[redacted]	[redacted]LB04.essers.com	warning tmm2[18805]: 01260013:4: SSL Handshake failed for TCP [redacted] -> [redacted]	TCP	[redacted]	[redacted]	
May 15 10:23:55	syslog	[redacted]	[redacted]LB04.essers.com	warning tmm3[18805]: 01260013:4: SSL Handshake failed for TCP [redacted]	TCP	[redacted]	[redacted]	
May 15 10:23:55	syslog	[redacted]	[redacted]LB04.essers.com	warning tmm2[18805]: 01260013:4: SSL Handshake failed for TCP [redacted]	TCP	[redacted]	[redacted]	
May 15 10:23:20	syslog	[redacted]	[redacted]LB04.essers.com	warning tmm[18805]: 01260013:4: SSL Handshake failed for TCP [redacted]	TCP	[redacted]	[redacted]	
May 15 10:23:16	syslog	[redacted]	[redacted]LB04.essers.com	warning tmm3[18805]: 01260013:4: SSL Handshake failed for TCP [redacted]	TCP	[redacted]	[redacted]	
May 15 10:23:09	syslog	[redacted]	[redacted]	warning tmm1[18805]: 01260013:4: SSL Handshake failed for TCP [redacted]	TCP	[redacted]	[redacted]	
May 15 10:23:09	syslog	[redacted]	[redacted]LB04.essers.com	warning tmm2[18805]: 01260013:4: SSL Handshake failed for TCP [redacted]	TCP	[redacted]	[redacted]	

Dit zijn de 2 lijsten onderaan waar je de logs van de 2 query’s tot in detail kan bekijken.

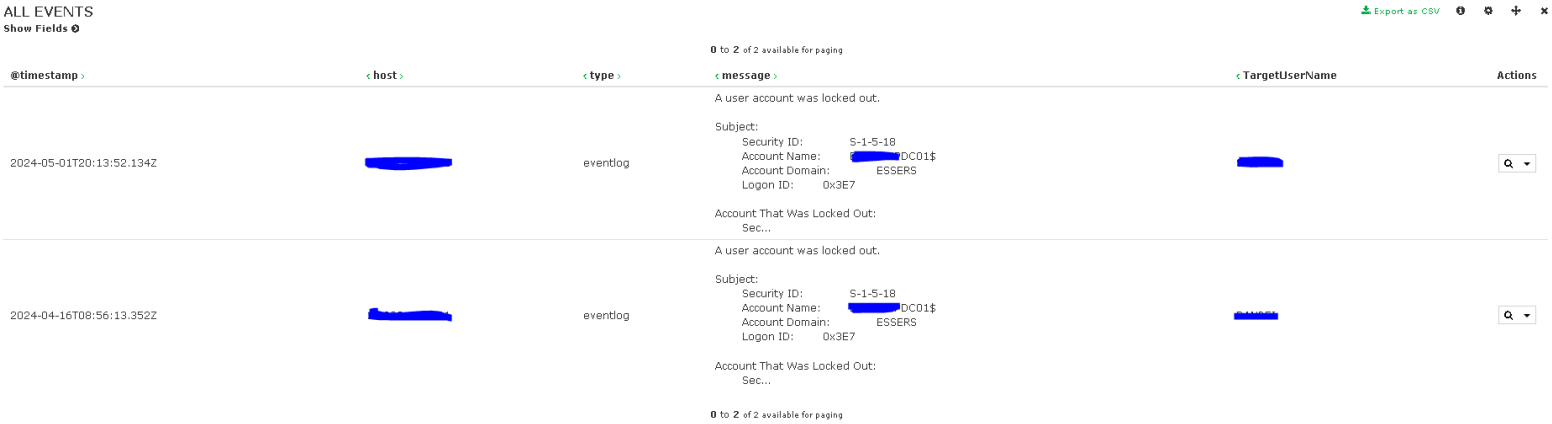
Dashboard locked out accounts:

Query's:

EventID:644

EventID:4740

Hier zie je een tabel met balken om de top 10 users te laten zien en zoals je ziet op de events over time histogram zijn er 2 events met event ID 4740. Dit wil dus zeggen dat er 2 mensen gelocked zijn. Daarnaast zie je de users die locked out zijn.



Dit is weer een lijst met alle logs met betrekking tot lock-outs zodat je ze in detail kan bekijken als dat nodig is.

Dashboards privileged accounts:

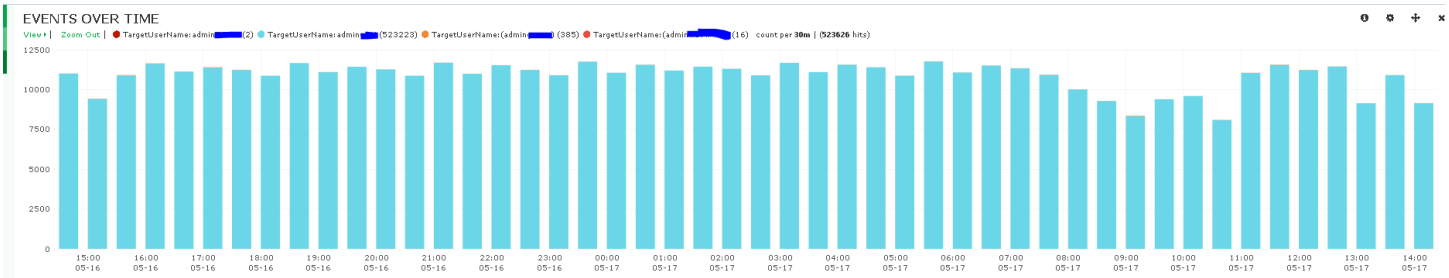
Query's:

TargetUserName:admin+naam v/d privileged user

TargetUserName:admin+naam v/d privileged user

TargetUserName:admin+naam v/d privileged user

TargetUserName:admin+naam v/d privileged user



ACTIVITY PER PRIVILEGED ADMIN

Term	Count	Action
admin[redacted]	523213	
Admin[redacted]	268	
Admin[redacted]-NPS	117	
Admin[redacted]	14	
admin[redacted]-NPS	10	
Admin[redacted]-NPS	2	
Admin[redacted]-NPS	2	
Other values	0	

MOST USED EVENTID'S BY PRIVILEGED ADMINS

Term	Count	Action
4771	523433	
4634	67	
4624	67	
4768	21	
4776	14	
4648	13	
4738	5	
4725	2	
4724	2	
4722	1	
Other values	1	

MOST USED LOG CATEGORY

Term	Count	Action
Kerberos Authentication Service	523454	
Logon	81	
Logoff	67	
Credential Validation	14	
User Account Management	10	
Other values	0	

Hier zien we weer een histogram met events over time en daaronder 3 tabellen met activiteit per gebruiker, meest gebruikte event ID's door privileged users, meest gebruikte log categorieën

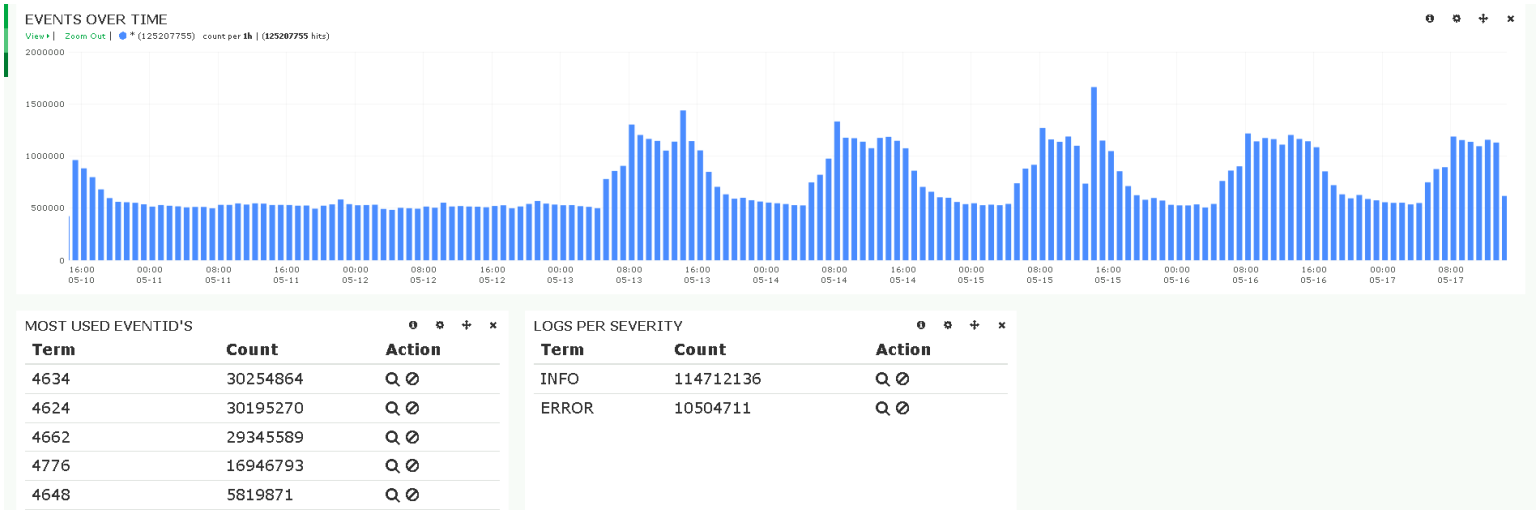
Dashboard eventlog test:

Query:

* → omdat ik alle eventlogs wil hebben

Filters:

Type: eventlog → omdat ik alleen maar eventlog wil zien.



MOST USED EVENTID'S

Term	Count	Action
4634	30254864	
4624	30195270	
4662	29345589	
4776	16946793	
4648	5819871	

LOGS PER SEVERITY

Term	Count	Action
INFO	114712136	
ERROR	10504711	

We beginnen weer met een event over time histogram en daarna een lijst met alle event ID's die verzameld worden in Nagios en vervolgens ook nog een tabel met de severity's om snel te wisselen tussen info logs in error logs.

Onderaan hebben we weer een lijst met alle logs om specifieke informatie te bekijken.

4.1.3 Extra dashboards

Admin acc logon:

Query's:

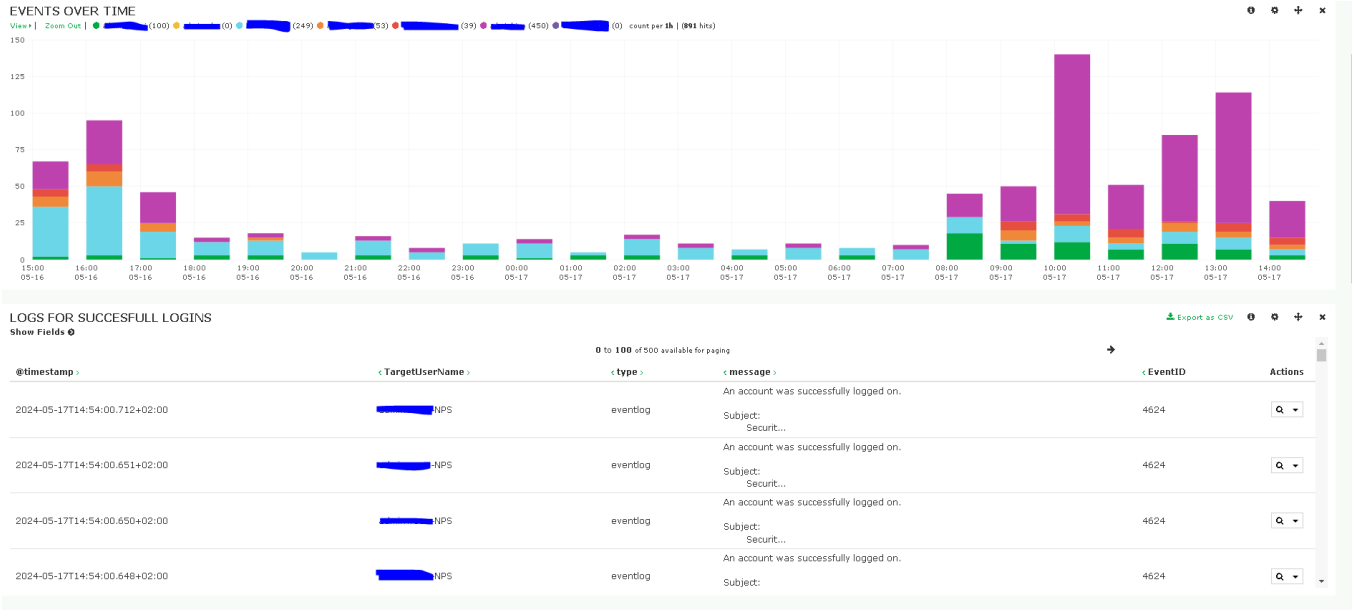
TargetUserName:admin+naam v/d admin

TargetUserName:admin+naam v/d admin

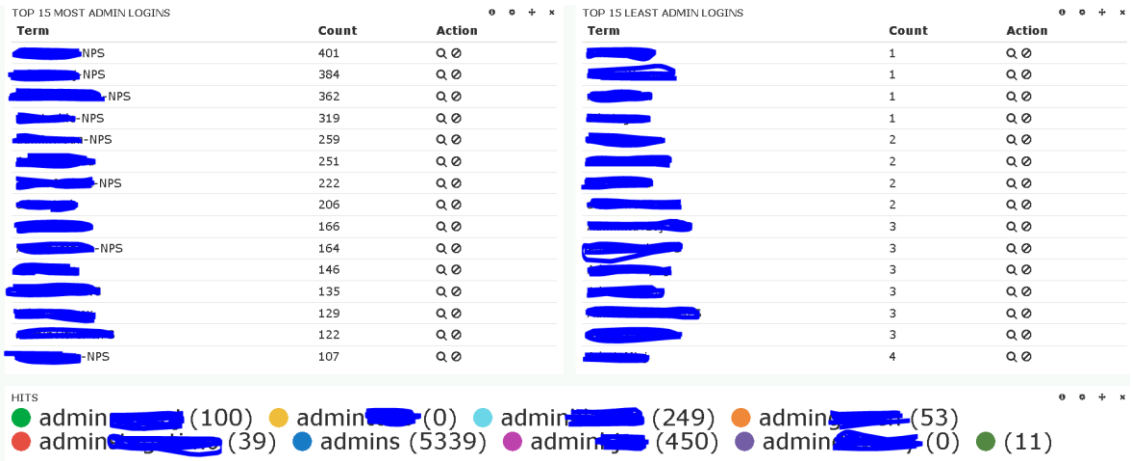
…

Filters:

EventID:4624



Met de events over time zien we de users die in de query's en daaronder een mooie tabel met meer informatie over de logs die ze getriggerd hebben.



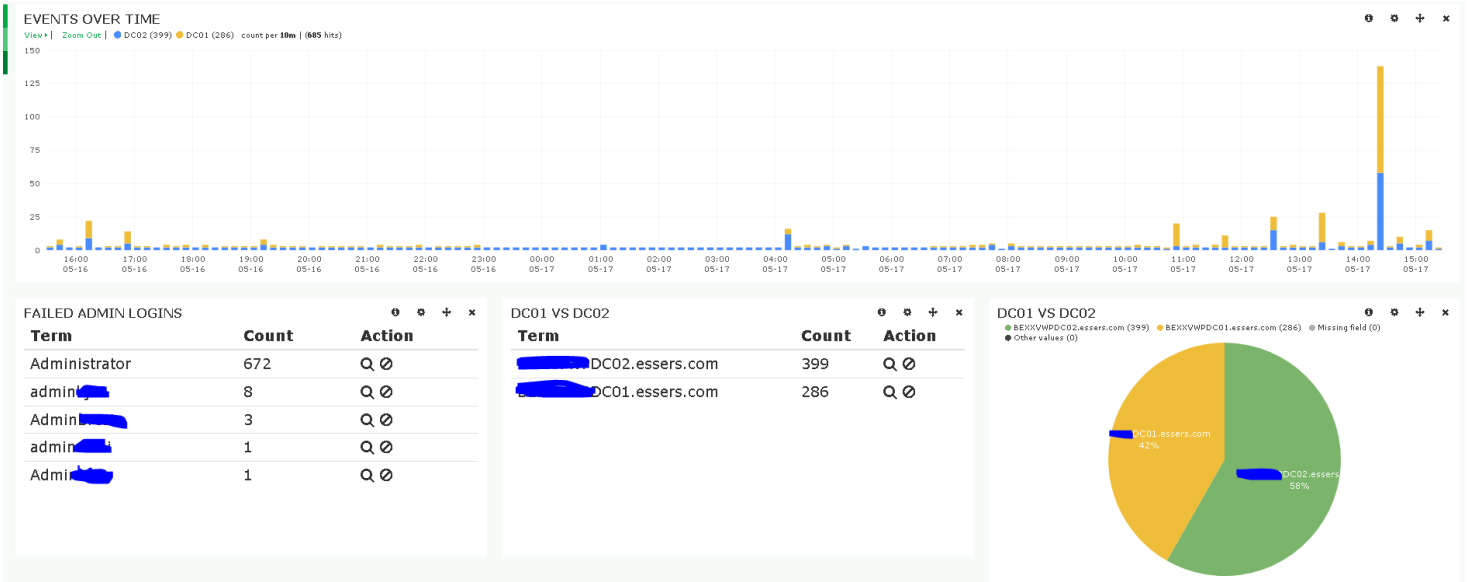
Daaronder heb je 2 tabellen met in de eerste tabel een lijst met de top 15 meest ingelogde admins en daarnaast een lijst met minst ingelogde admins.
Vervolgens nog een legende met de kleuren van die bij de users met de query horen.

Dashboard Admins with failed logins:

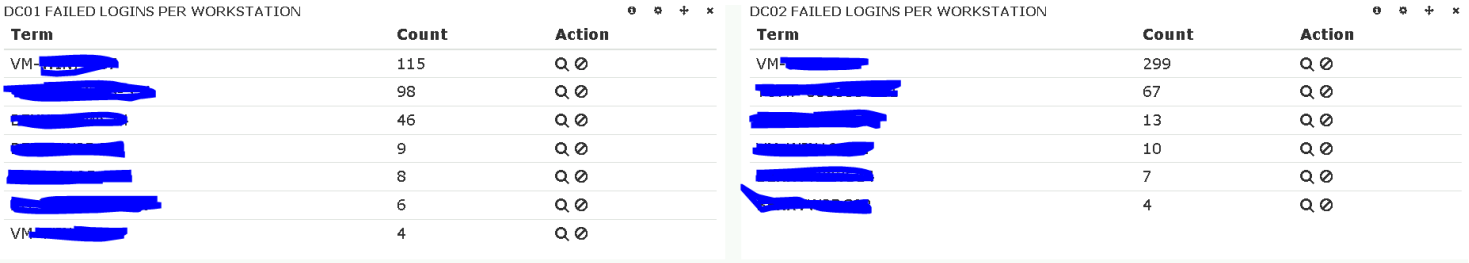
Query's

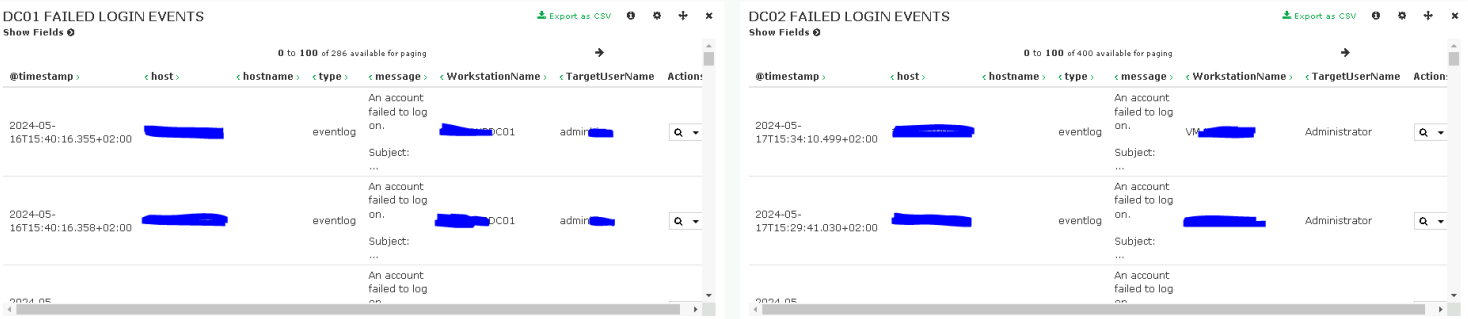
TargetUserName:admin* AND EventID:4625 AND Hostname: naam van DC01

TargetUserName:admin* AND EventID:4625 AND Hostname: naam van DC02



Events over time om op een snelle manier de verschillende query's van elkaar te onderscheiden. Vervolgens 2 tabellen en een pie chart met in de eerste tabel de admins met failed logins en daarnaast kun je de verdeling tussen de domain controllers zien in een tabel en pie chart.





Daaronder zien we 2 tabellen met mislukte logins per workstation, een tabel per domain controller en daaronder nog een lijst met de failed login events om extra informatie te krijgen over de failed logins.

Met dit dashboard hebben we ook gevonden dat er werd ingelogd met Administrator, terwijl die naam normaal niet gebruikt wordt.

Dashboard auth logs PAM:

Query’s

message:”An account was logged off.”

message:”An account was successfully logged on.”

message:”Special privileges assigned to new logon.”

message:”An attempt was made to reset an account’s password.”

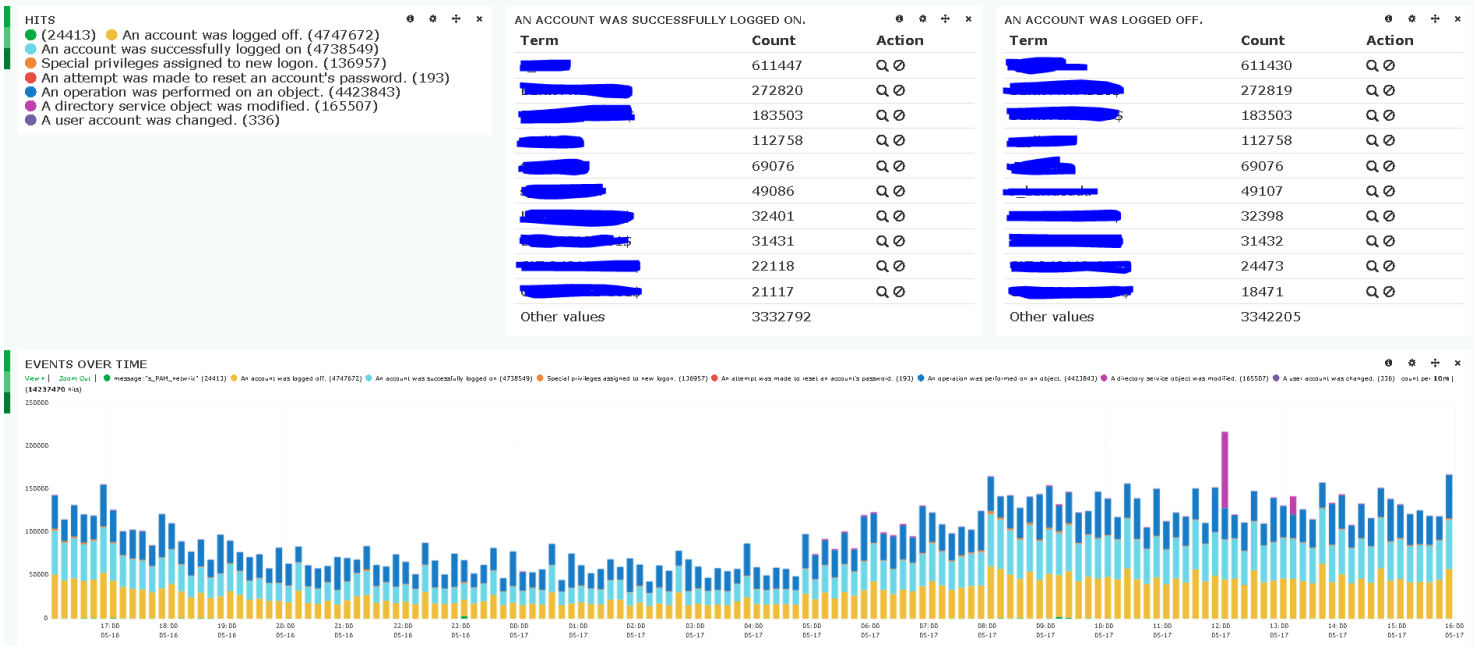
message:”An operation was performed on an object.”

message:”A directory service object was modified.”

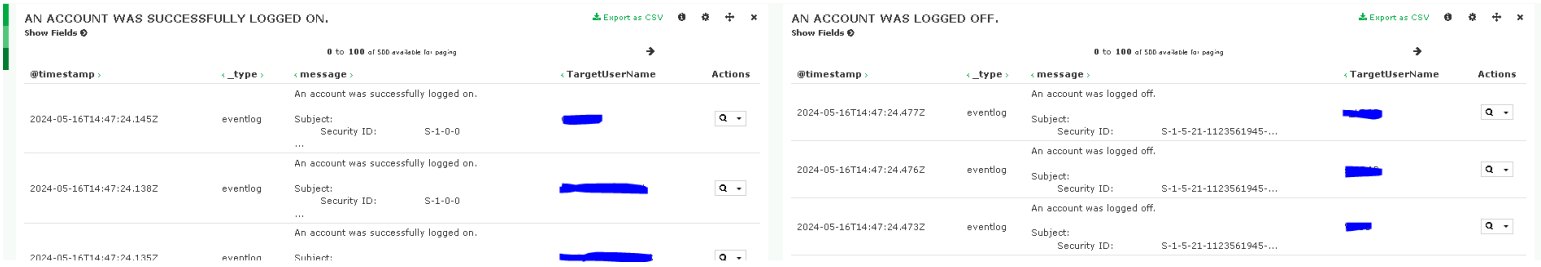
message:”A user account was changed.”

Pinned query:

message:”s_PAM_netwrix”

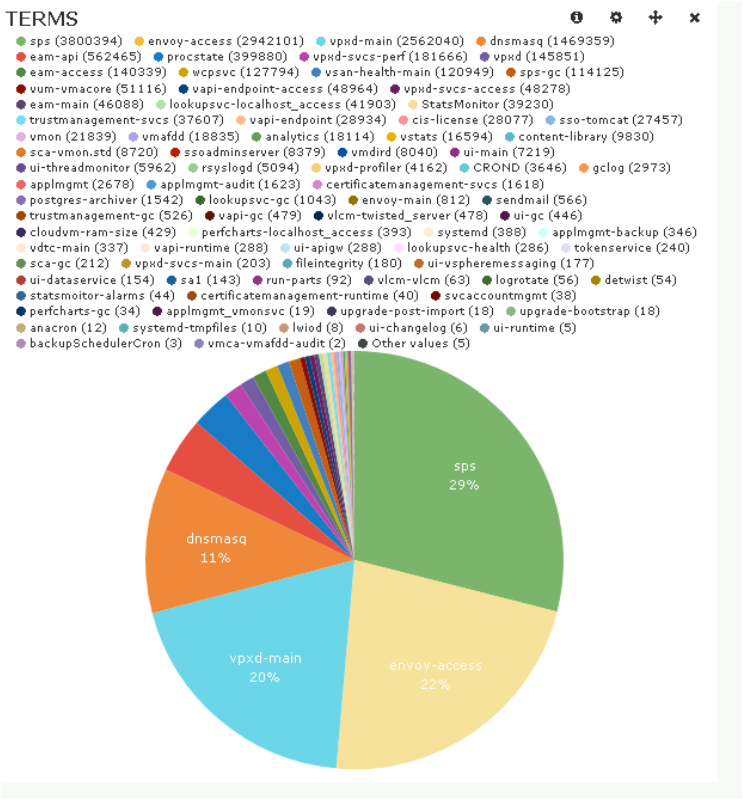


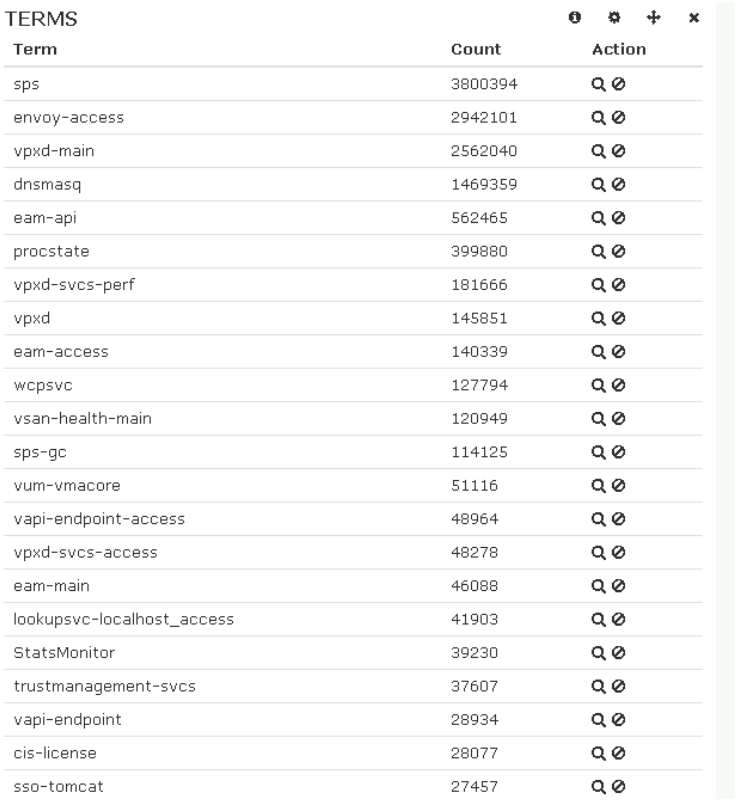
Eerst hebben we een overzicht van de verschillende query’s en daarnaast 2 tabellen met de logins en logoffs. Vervolgens een event over time histogram zodat je makkelijk het verschil tussen de hoeveelheid van de verschillende query’s kan zien.



Daaronder hebben we 2 lijsten waar je die log in en log uit events gemakkelijk kan bekijken voor meer informatie.

Dashboard VMWare vcenter server:





Term	Count	Action
sps	3800394	
envoy-access	2942101	
vpxd-main	2562040	
dnsmasq	1469359	
eam-api	562465	
procstate	399880	
vpxd-svcs-perf	181666	
vpxd	145851	
eam-access	140339	
wcpsvc	127794	
vsan-health-main	120949	
sps-gc	114125	
vum-vmacore	51116	
vapi-endpoint-access	48964	
vpxd-svcs-access	48278	
eam-main	46088	
lookupsvc-localhost_access	41903	
StatsMonitor	39230	
trustmanagement-svcs	37607	
vapi-endpoint	28934	
cis-license	28077	
sso-tomcat	27457	

Dit dashboard was meer een overzicht voor mij zodat ik na het filteren kon zien welke verschillende type van logs er allemaal gestuurd werden. In de volgende dashboards ga je zien dat ik een paar van de meest voorkomende log types ga verwerken in een dashboard.

Dasboard 2 VMWare vcenter:

Query's:

host: "Ip van vcenter" AND type_of_log:"vpxd-main"

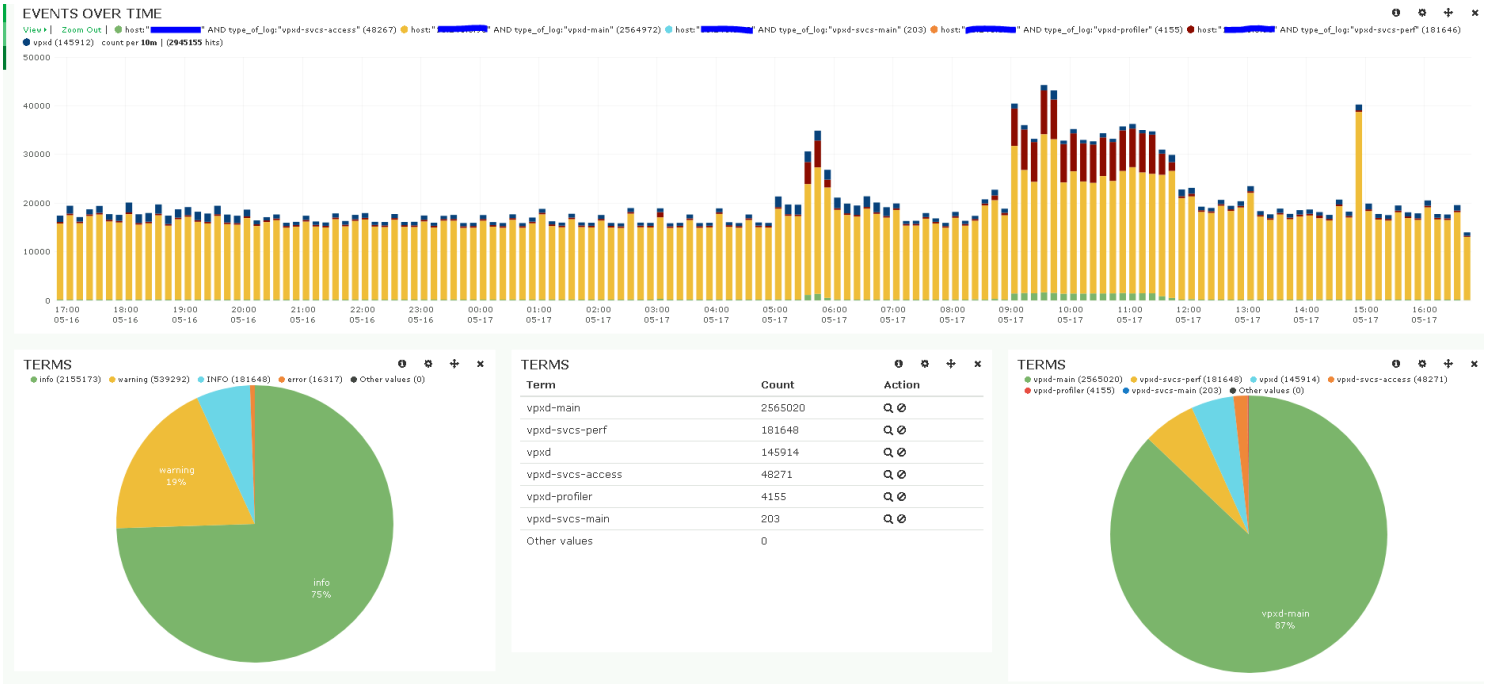
host:"Ip van vcenter" AND type_of_log:"vpxd-svcs-perf"

host:"ip van vcenter" AND type_of_log:"vpxd"

host: "Ip van vcenter" AND type_of_log:"vpxd-svcs-access"

host:"ip van vcenter" AND type_of_log:"vpxd-profiler"

host:"ip van vcenter" AND type_of_log:"vpxd-svcs-main"



Hier een overzicht van al de "vpxd" soorten logs, verschillende severity's, hoeveelheid per type en pie chart.

VPXD-SVCS-ACCESS

Show Fields

Export as CSV

0 to 10 of 50 available for paging

@timestamp	status_code	http_method	tomcat-exec-id	topic	Actions
2024-05-17T16:47:37.988+02:00	200	POST	tomcat-exec-54	"VMware-client/6.5.0"	
2024-05-17T16:47:37.988+02:00	200	POST	tomcat-exec-84	"VMware-client/6.5.0"	
2024-05-17T16:47:37.988+02:00	400	GET	tomcat-exec-30	"VMware-client/6.5.0"	
2024-05-17T16:47:37.987+02:00	200	POST	tomcat-exec-47	"VMware-client/6.5.0"	
2024-05-17T16:47:27.987+02:00	200	POST	tomcat-exec-17	"VMware vim-java 1.0"	
2024-05-17T16:47:07.987+02:00	200	POST	tomcat-exec-4	"VMware vim-java 1.0"	
2024-05-17T16:46:47.986+02:00	200	POST	tomcat-exec-241	"VMware vim-java 1.0"	
2024-05-17T16:46:47.986+02:00	200	POST	tomcat-exec-285	"VMware vim-java 1.0"	
2024-05-17T16:46:27.986+02:00	200	POST	tomcat-exec-21	"VMware vim-java 1.0"	
2024-05-17T16:46:07.986+02:00	200	POST	tomcat-exec-289	"VMware vim-java 1.0"	

0 to 10 of 50 available for paging

VPXD-SVCS-PERF

Show Fields

Export as CSV

0 to 10 of 50 available for paging

message	severity_label2	stats	Actions
<134>1 2024-05-17T16:47:19.507016+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:19.5...	INFO	Requesting LDAP connection	
<134>1 2024-05-17T16:47:19.507032+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:19.5...	INFO	Connection type: LDAP, Max allowed connections: 24, Number of active connections: 1, Number of idle ...	
<134>1 2024-05-17T16:47:18.535989+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:18.5...	INFO	Connection type: LDAP, Max allowed connections: 24, Number of active connections: 1, Number of idle ...	
<134>1 2024-05-17T16:47:18.535983+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:18.5...	INFO	Requesting LDAP connection	
<134>1 2024-05-17T16:47:18.535747+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:18.5...	INFO	Connection type: LDAP, Max allowed connections: 24, Number of active connections: 1, Number of idle ...	
<134>1 2024-05-17T16:47:18.536144+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:18.5...	INFO	Connection type: LDAP, Max allowed connections: 24, Number of active connections: 1, Number of idle ...	
<134>1 2024-05-17T16:47:18.536138+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:18.5...	INFO	Requesting LDAP connection	
<134>1 2024-05-17T16:47:18.535368+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:18.5...	INFO	Requesting LDAP connection	
<134>1 2024-05-17T16:47:18.535741+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:18.5...	INFO	Requesting LDAP connection	
<134>1 2024-05-17T16:47:18.535380+02:00 BEXXVLPVC01 vpxd-svcs-perf - - - 2024-05-17T16:47:18.5...	INFO	Connection type: LDAP, Max allowed connections: 24, Number of active connections: 1, Number of idle ...	

VPXD

Show Fields

Export as CSV

0 to 10 of 50 available for paging

@timestamp	shortermessage	severity_label2	user	location	type_of_log	Actions
2024-05-17T16:47:33.868+02:00	User [redacted] logged out (login time: Friday...	info	root	Genk - HQ Datacenter PRODUCTION	vpxd	
2024-05-17T16:47:33.868+02:00	User [redacted] logged in as [redacted]agent/7.0.3-1...	info	root	Genk - HQ Datacenter PRODUCTION	vpxd	
2024-05-17T16:47:33.573+02:00	Virtual machine [redacted] in cluster Cluster...	info		Genk - HQ Datacenter CITRIX	vpxd	
2024-05-17T16:47:33.571+02:00	Virtual machine [redacted] in cluster Cluster...	info		Genk - HQ Datacenter CITRIX	vpxd	
2024-05-17T16:47:33.569+02:00	Virtual machine [redacted] in cluster Cluster...	info		Genk - HQ Datacenter CITRIX	vpxd	
2024-05-17T16:47:31.757+02:00	Alarm 'Virtual machine CPU usage' on XD-V0...	info		Genk - HQ Datacenter CITRIX	vpxd	
2024-05-17T16:47:31.757+02:00	Alarm 'Virtual machine memory usage' on XD...	info		Genk - HQ Datacenter CITRIX	vpxd	
2024-05-17T16:47:29.964+02:00	User root@127.0.0.1 logged in as hbr-agent/7.0.3-1...	info	root	Genk - HQ Datacenter PRODUCTION	vpxd	
2024-05-17T16:47:29.964+02:00	User root@127.0.0.1 logged out (login time: Friday...	info	root	Genk - HQ Datacenter PRODUCTION	vpxd	
2024-05-17T16:47:28.812+02:00	Alarm 'Virtual machine memory usage' on XD...	info		Genk - HQ Datacenter CITRIX	vpxd	

0 to 10 of 50 available for paging

Verschillende types met hun eigen tabel en eigen filters.

Die types die niet gefilterd zijn en waar dus geen dashboard voor is zijn onnuttig en kunnen geen waardes uitgehaald worden.

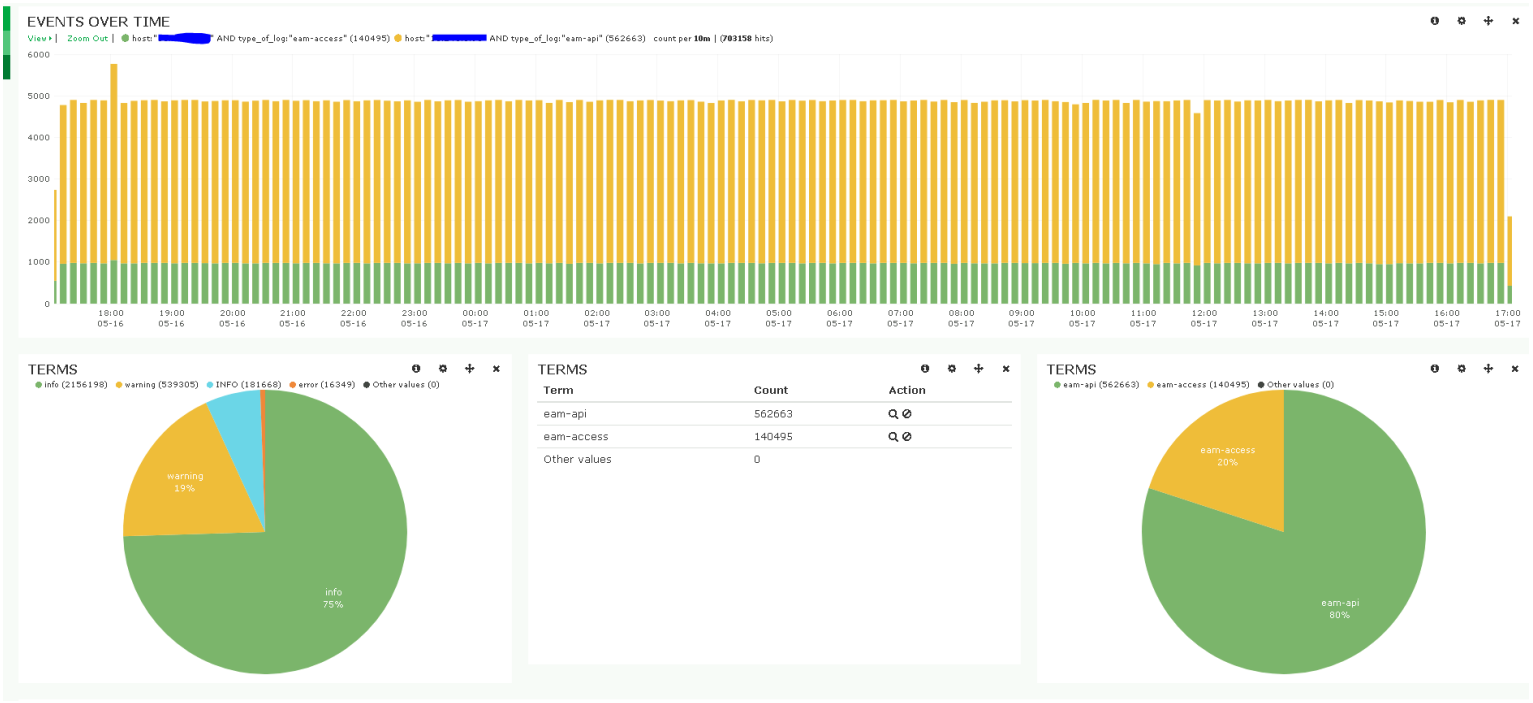
Onderaan het dashboard nog een tabel met alle logs van elke query in dit dashboard.

Dashboard 3 VMWare vcenter:

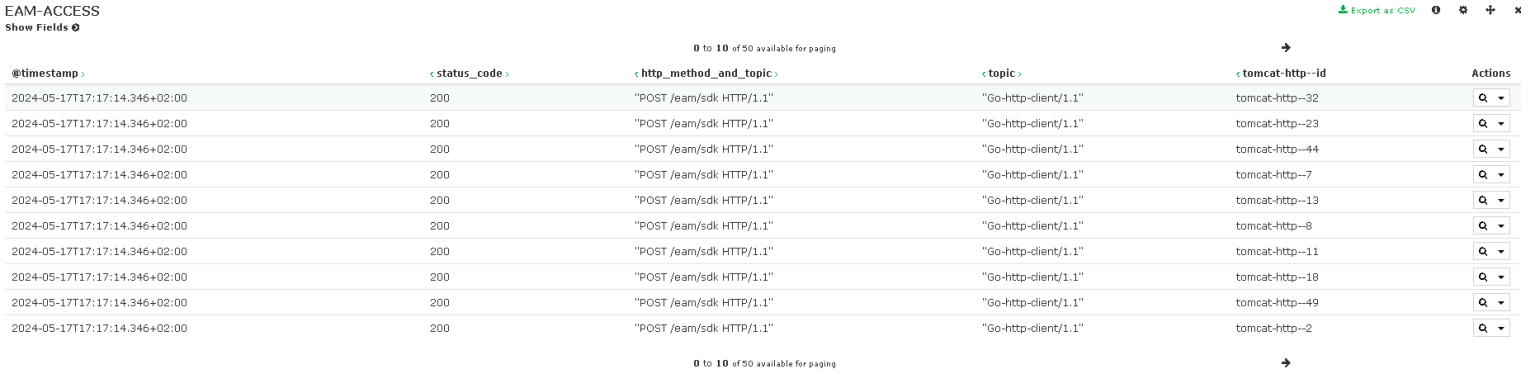
Query's:

host:"ip van vcenter" AND type_of_log:"eam-access"

host:"ip van vcenter" AND type_of_log:"eam-api"



Events over time histogram om de verschillen aan te tonen met de 2 pie charts de eerste voor de severity's en de andere voor de verdeling tussen de verschillende types. Vervolgens daar tussen een tabel met de hoeveelheid van logs bij de verschillende types.



Verschillende types met hun eigen tabel en eigen filters.

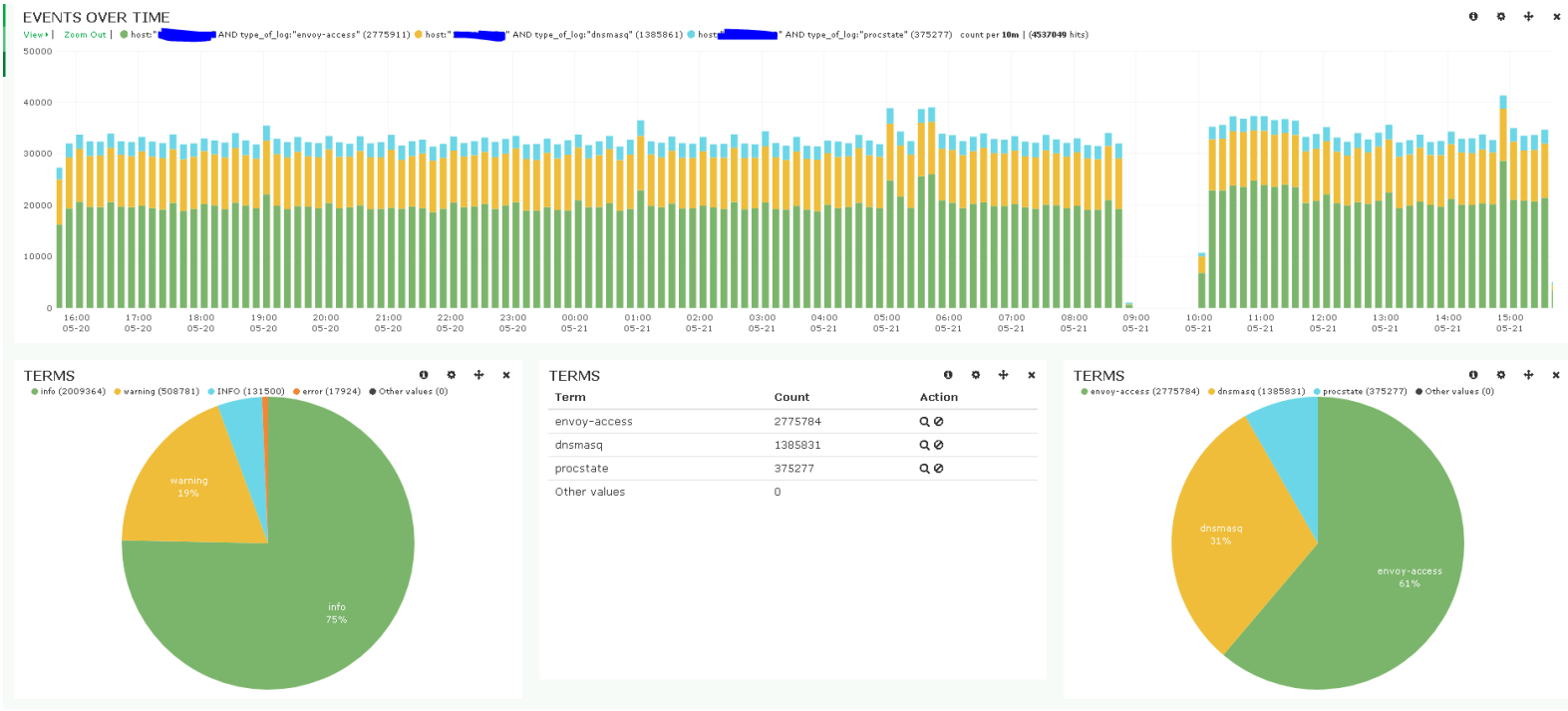
Dashboard 4 VMWare vcenter:

Query's:

host:"ip van vcenter" AND type_of_log:"envoy-access"

host:"ip van vcenter" AND type_of_log:"dnsmasq"

host:"ip van vcenter" AND type_of_log:"procstate"



Dit is een dashboard voor vcenter log types envoy-acces, dnsmasq en procstate. In dit dashboard zie je een events over time, 2 pie charts voor severity en de percentages van de verschillende types maar ook een tabel met de hoeveelheid logs per type log uit VMWare vcenter. Tenslotte onderaan het dashboard ook nog een lijst met al de logs die in verband staan met de query's hierboven.

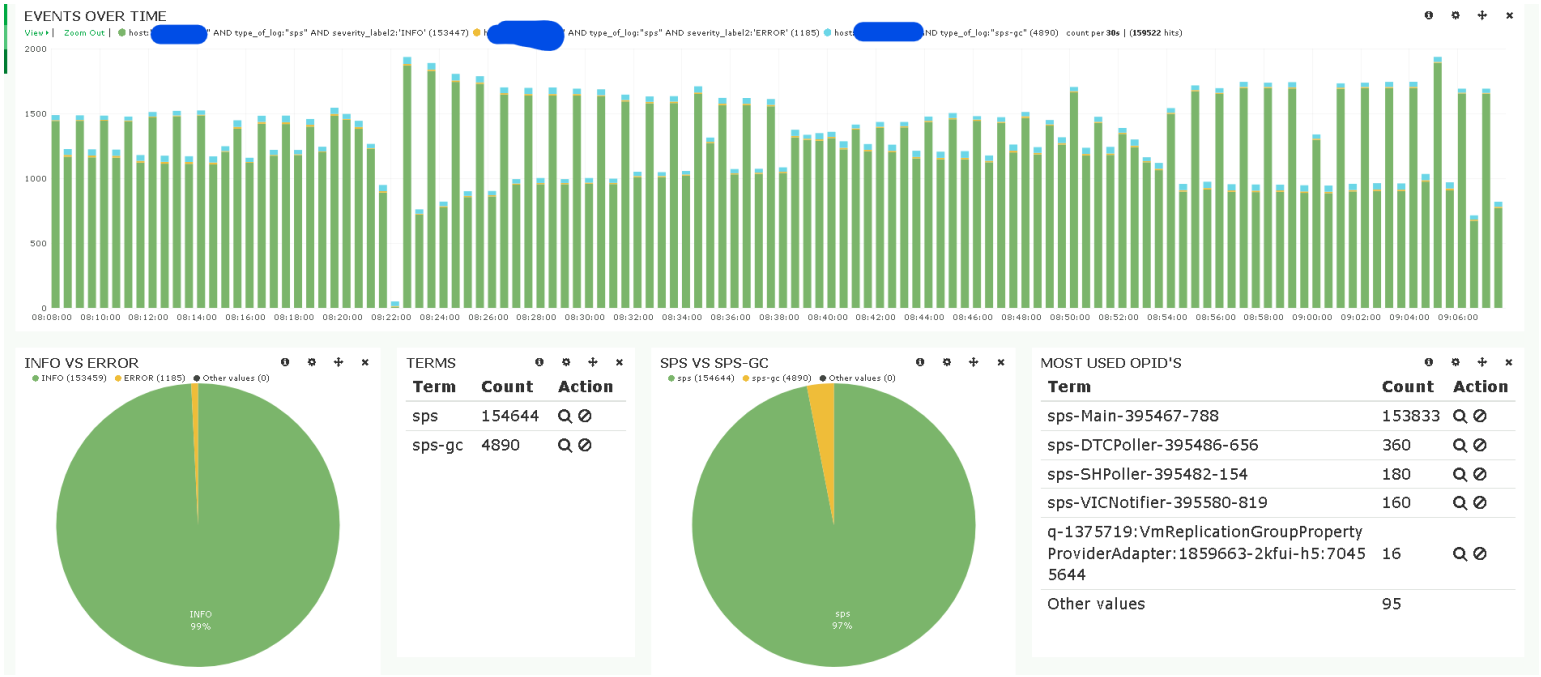
Aangezien deze types veel logs geven heb ik hier een apart dashboard van gemaakt. Deze types moesten ook nog gefilterd worden maar daar ben ik niet aangekomen.

Dashboard sps (Storage management service) VMware vcenter:

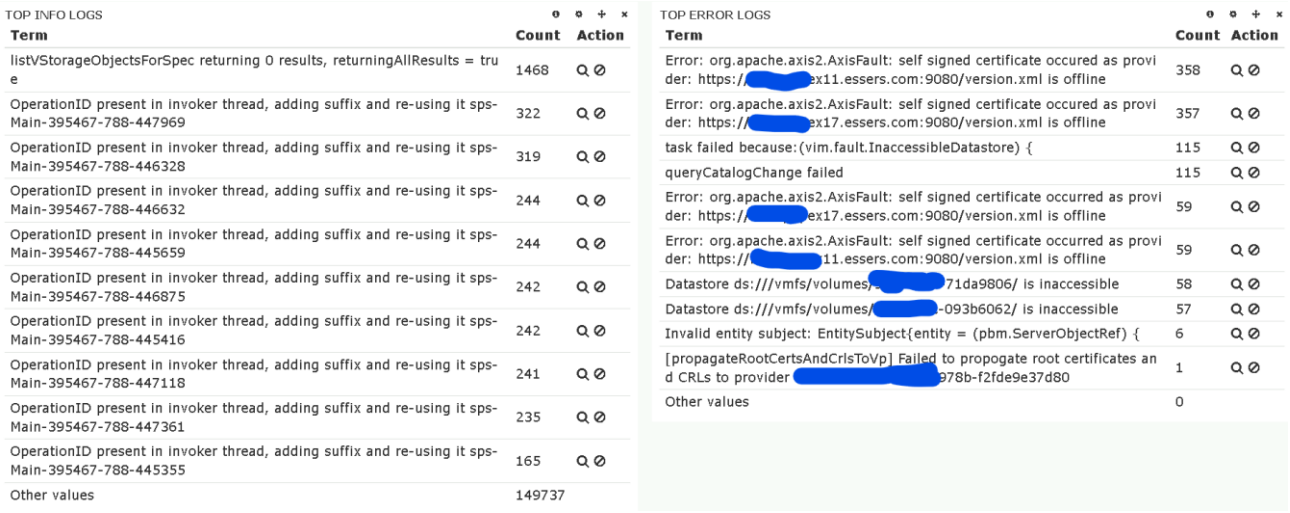
Query's:

host:"ip van vcenter" AND type_of_log:"sps"

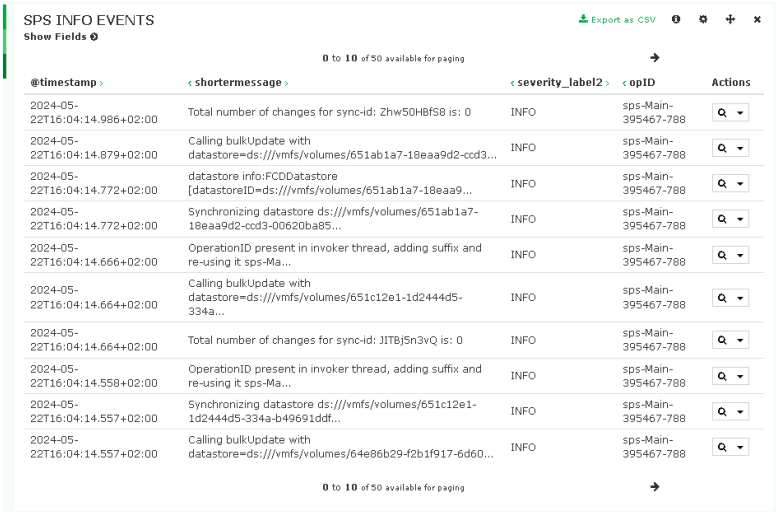
host:"ip van vcenter" AND type_of_log:"sps-gc"

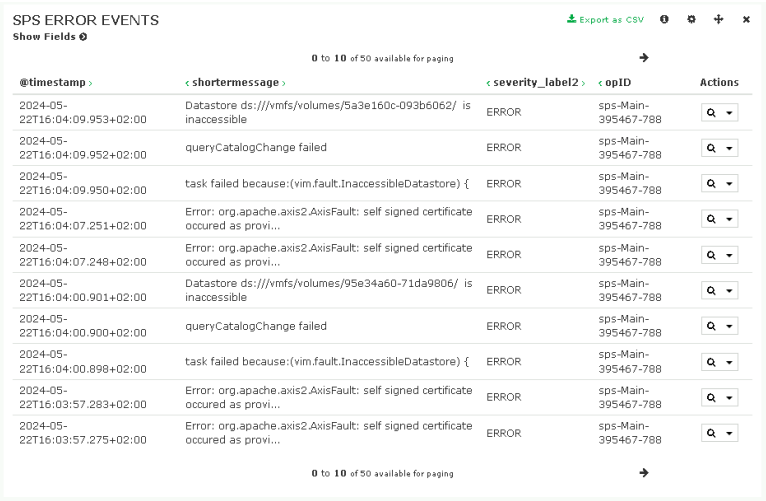


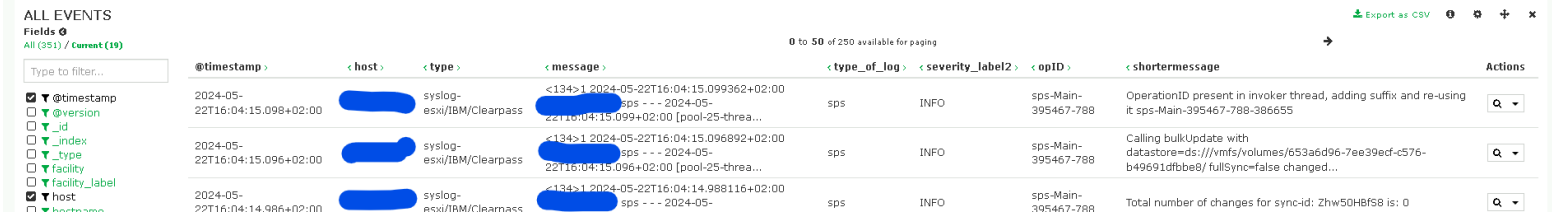
In dit dashboard zie je een events over time histogram met daaronder een pie chart waar de info logs tegenover de error logs in percentages wordt weergegeven, daarnaast de verschillende log types van SPS, vervolgens weer een pie chart maar nu het verschil in percentage van de verschillende types, tenslotte hebben we aan de rechter kant een tabel met de meest gebruikte opID's.



Daaronder zie je nog 2 tabellen. De eerste is voor info logs en de tweede voor error logs die te maken hebben met SPS.







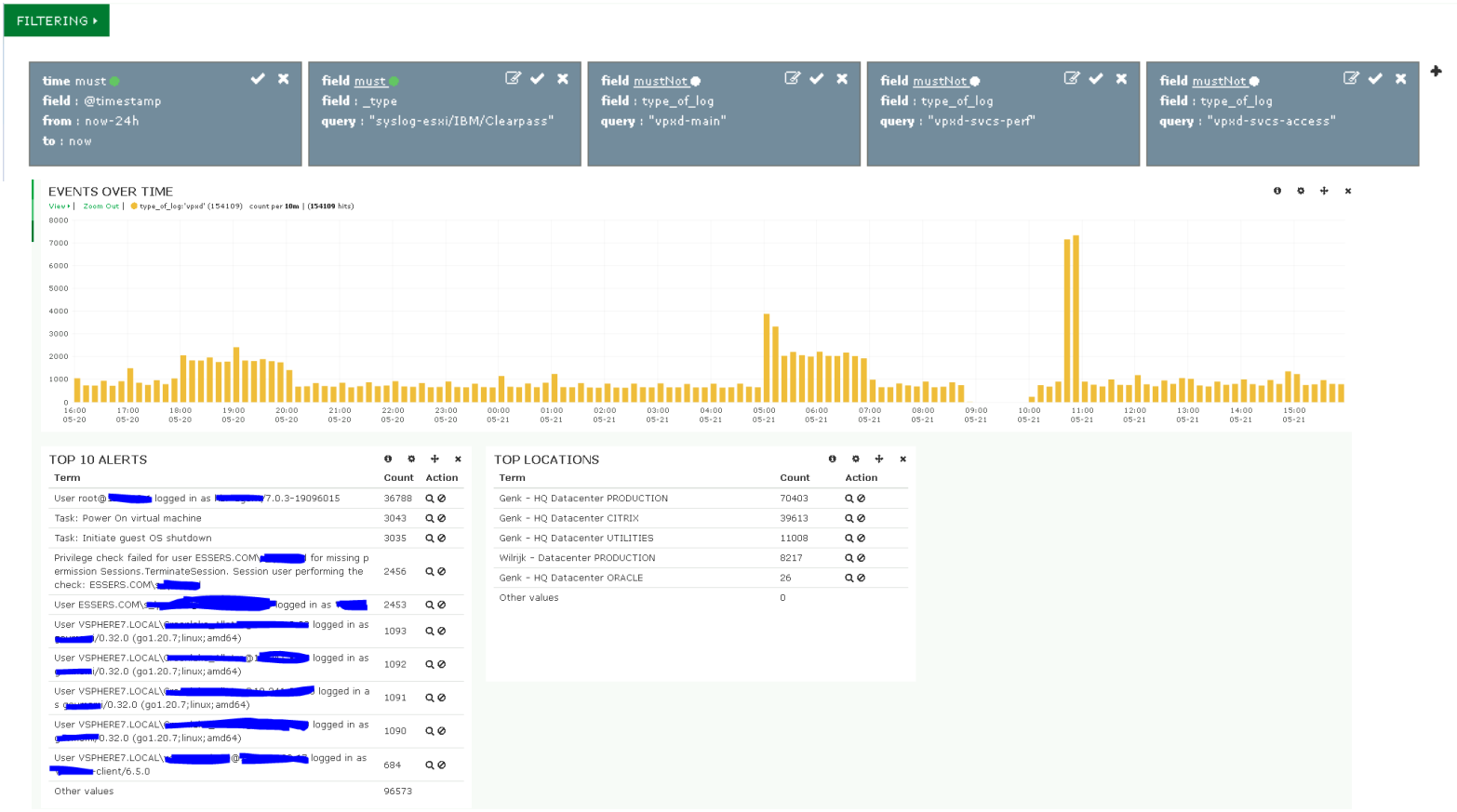
Onderaan dit dashboard heb je dan weer verschillende lijsten van de events met INFO, ERROR en een lijst met alle events over SPS.

Dashboard vpxd VMware vcenter:

Query's :

type_of_log:'vpxd'

filters :



Dit dashboard bestaat uit een events over time met daaronder gefilterde messages zodat een top 10 alerts gemaakt kon worden. (Met gefilterde messages bedoel ik niet de filters hierboven.) (Zie later)

Hier zie je ook al de logs met de filters zodat je meer tot in detail de logs kunt gaan bekijken met aangepaste filters voor een beter overzicht.

Dashboard check user:

Context: Ik werd gevraagd om bepaalde users te checken op activiteit omdat er sprake was van mogelijke spookusers.

Query's:

"Email/naam v/d user"

"Email/naam v/d user"

"Email/naam v/d user"

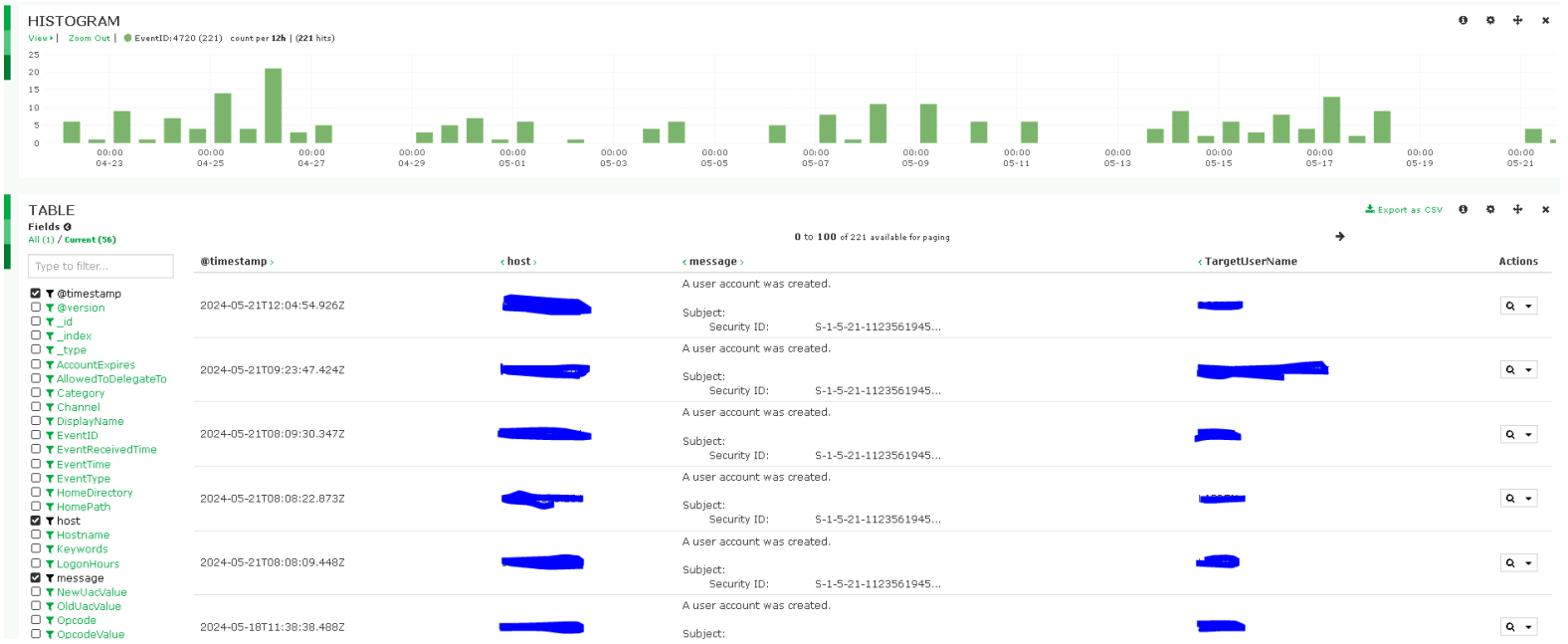
"Email/naam v/d user"

Geen screenshots voor dit dashboard omdat er nu niks meer op te zien valt aangezien dit probleem opgelost is.

Dashboard created accounts:

Query:

EventID:4720



In dit dashboard zie je alle users die aangemaakt worden in de domain controllers. Doormiddel van de events over time krijg je een makkelijk overzicht van wanneer accounts gemaakt zien en daar onder kun je meer in detail de logs bekijken.

Dasboard bruteforce check:

Context: Dit dashboard is gemaakt omdat er veel inlog pogingen waren met het account User terwijl dit account normaal niet gebruikt wordt.

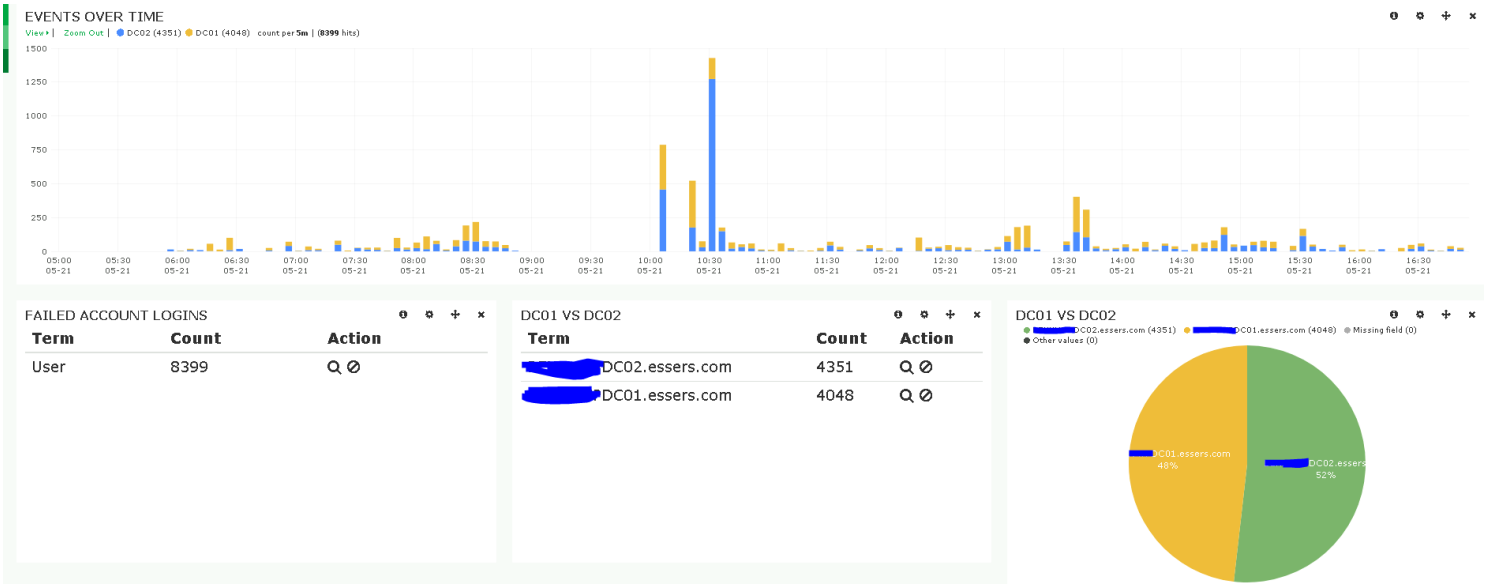
Query's:

TargetUserName:* AND EventID:4625 AND Hostname:"naam van dc01"

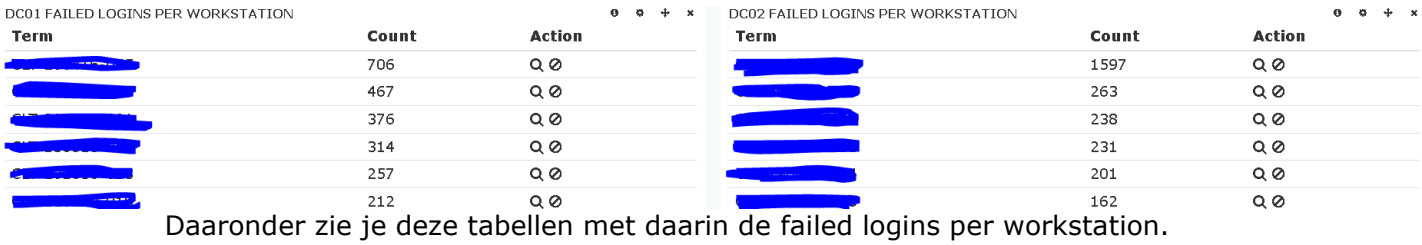
TargetUserName:* AND EventID:4625 AND Hostname:"naam van dc02"

Filters:

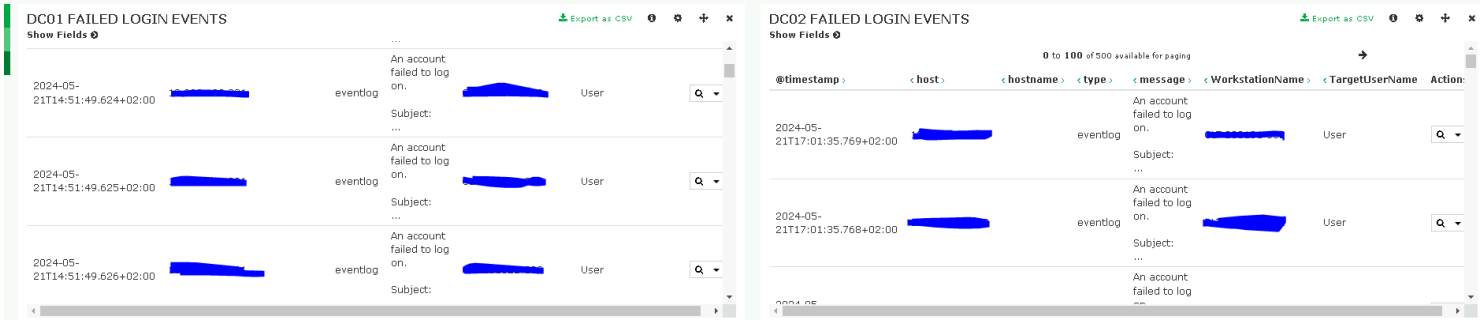
Field: TargetUserName
value: User → dit kun je aanpassen naar de user die je wilt checken ofwel laat je de filter weg en dan zie je alle users met het aantal verkeerde inlog pogingen.



Dit is het dashboard voor het checken voor een "bruteforce"



Daaronder zie je deze tabellen met daarin de failed logins per workstation.



Tenslotte is er ook nog per DC een lijst met de logs zodat je ze tot in detail kan bekijken.

Exchange dashboard:

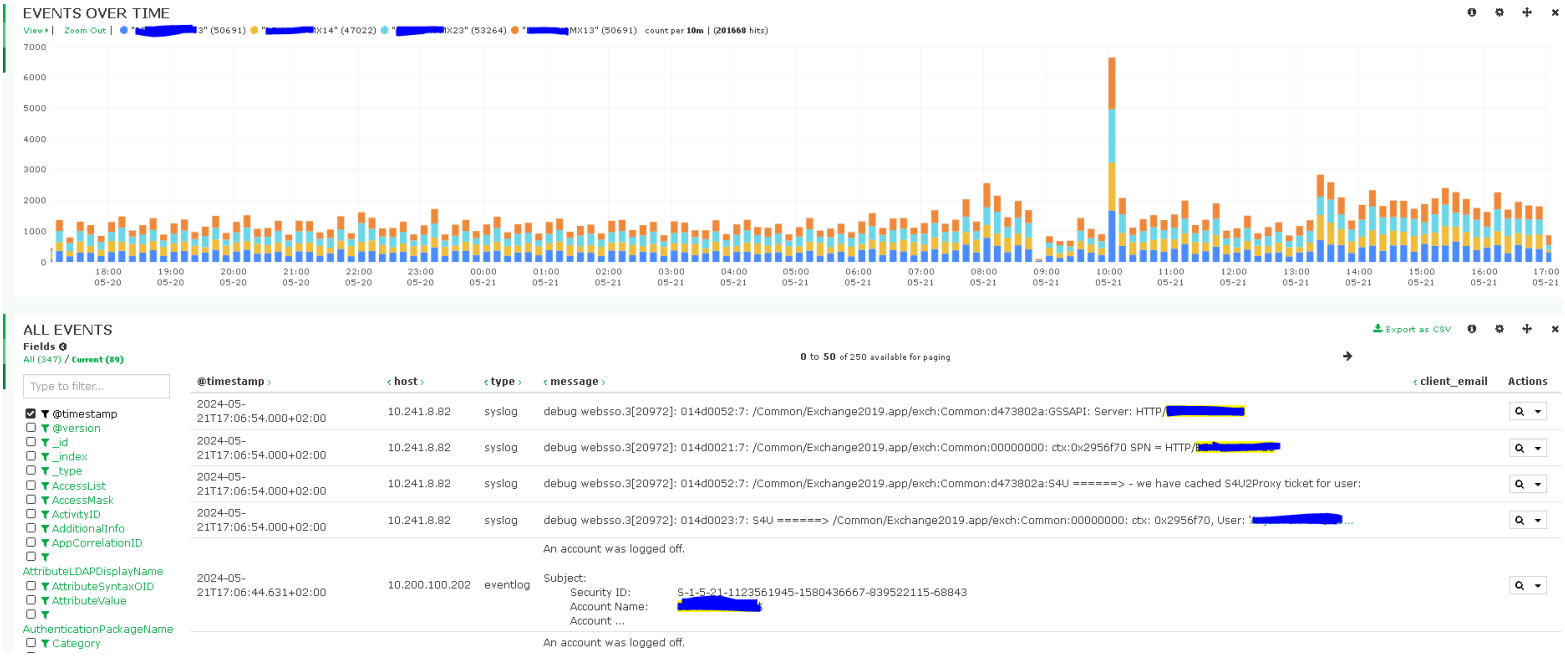
Query's:

"…mx13"

"…mx14"

"…mx23"

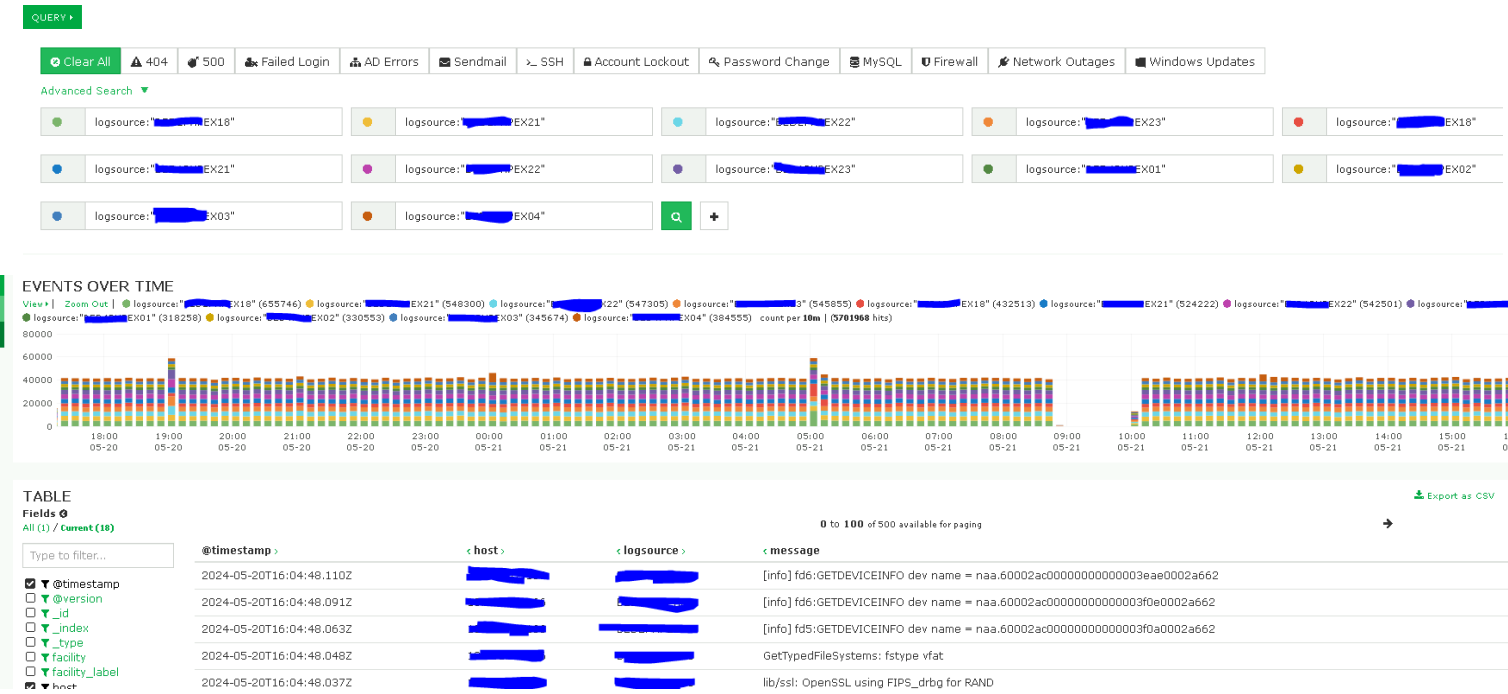
"…mx24" → naam v/d exchange servers



Omdat er veel meer over exchange was te visualiseren in Squared up heb ik hier in Nagios niet veel aandacht aan gegeven.

Ex dashboard:

Query's:



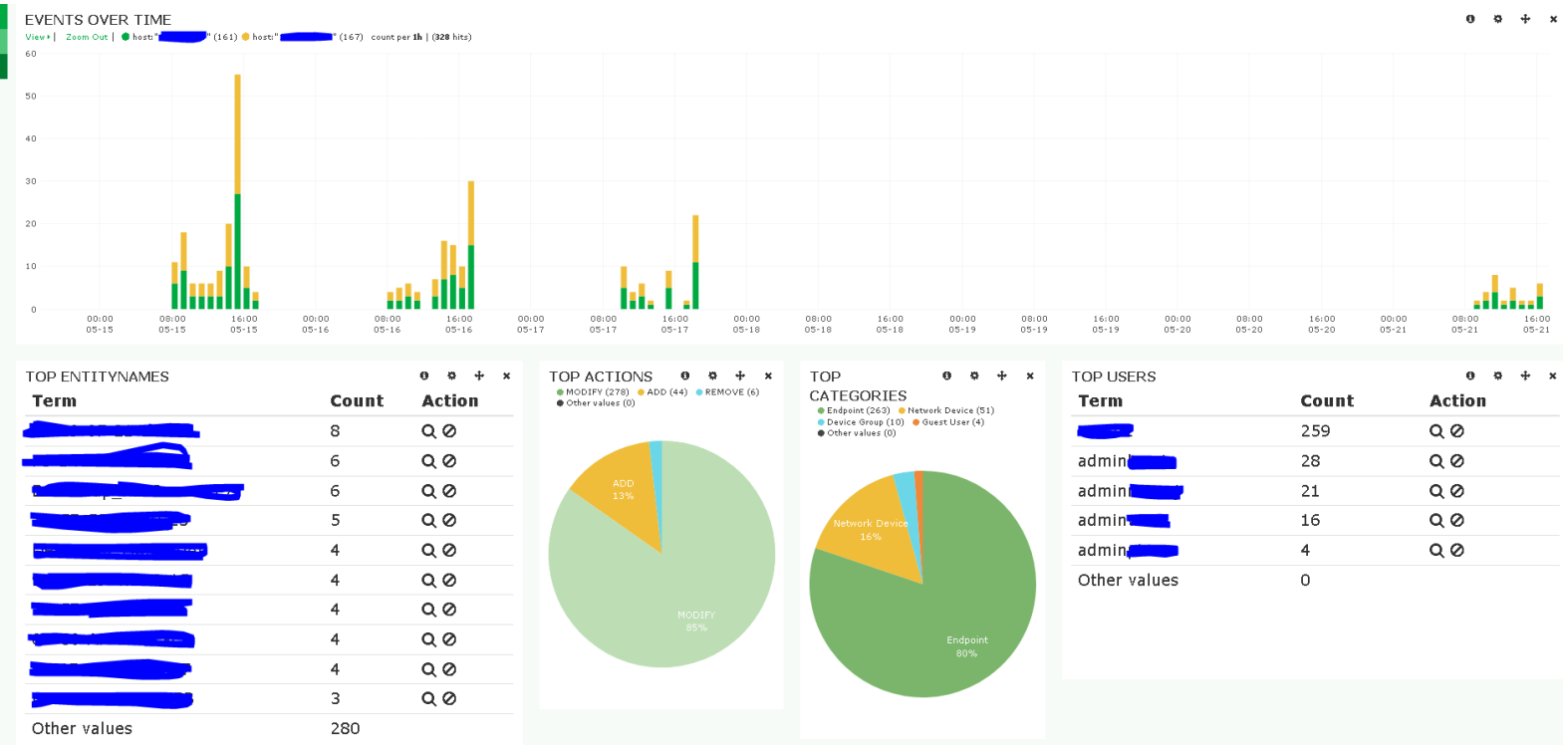
Dit dashboard en het vorig dashboard zijn heel basic en niet veel aandacht aanbesteed.

Dashboard Jira:

Query's:

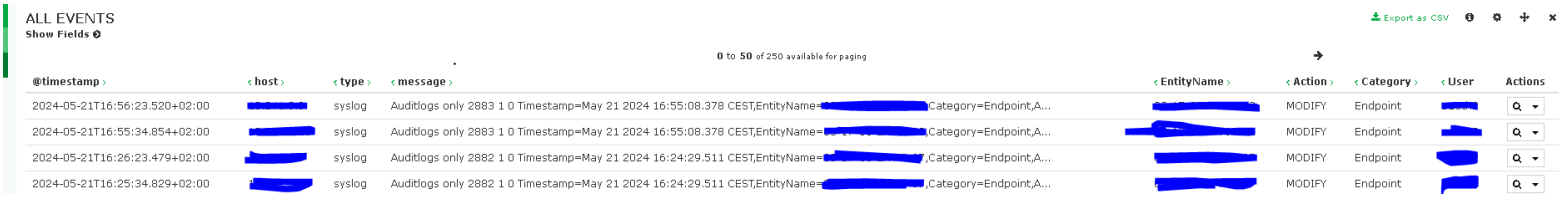
Host:"IP"

Host: "IP"



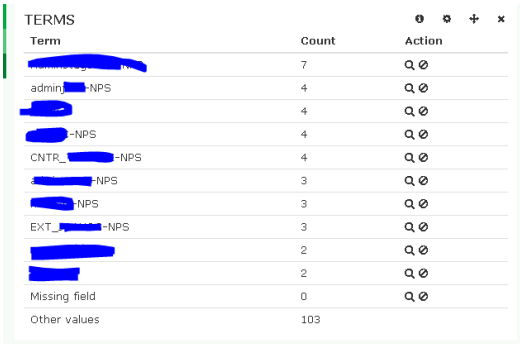
In dit dashboard zie je de gebruikte actions categorieën users en entity namen op Jira.

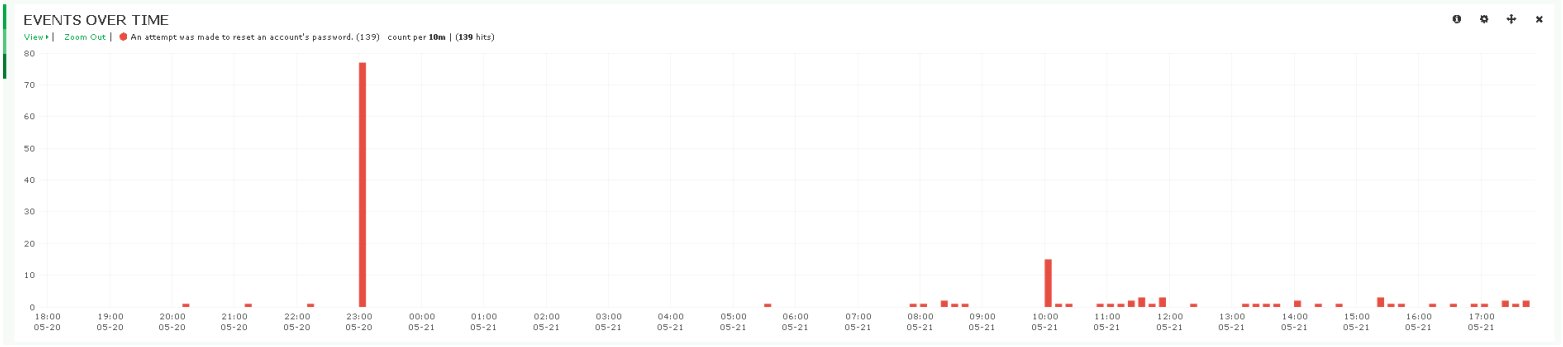
Dit in tabellen en pie charts met daaronder alle logs met de filters om zo tot in detail de logs te kunnen zien indien nodig.



Dashboard attempt password reset:

Gebruikte query: message:”An attempt was made to reset an account’s password.”





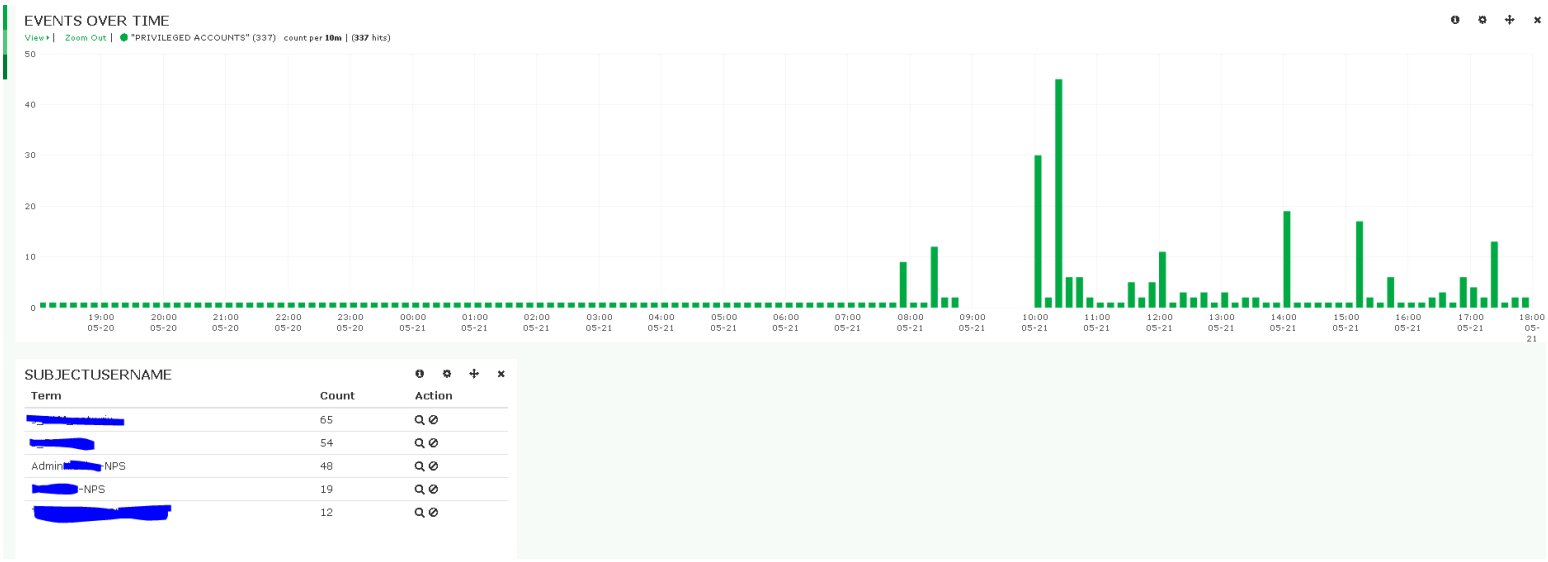
In dit dashboard zie je de Top 10 users voor de gebruikte query met daaronder een events over time histogram.

Daaronder staan al de logs in een tabel zodat je ze in detail kan bekijken.

Test dashboard:

Query's:

"PRIVILEGED ACCOUNTS"



Dit dashboard laat alle logs zien die iets te maken hebben met "privileged accounts". Op de screenshot zie je een tabel met users die te maken hebben met privileged accounts. Daaronder is een ALL-events lijst met alle logs met betrekking tot "privileged accounts".

Test dashboard 1:

Context: Dit dashboard is om een overzicht te krijgen over de succesvolle logins en de gefaalde logins.

Query's:

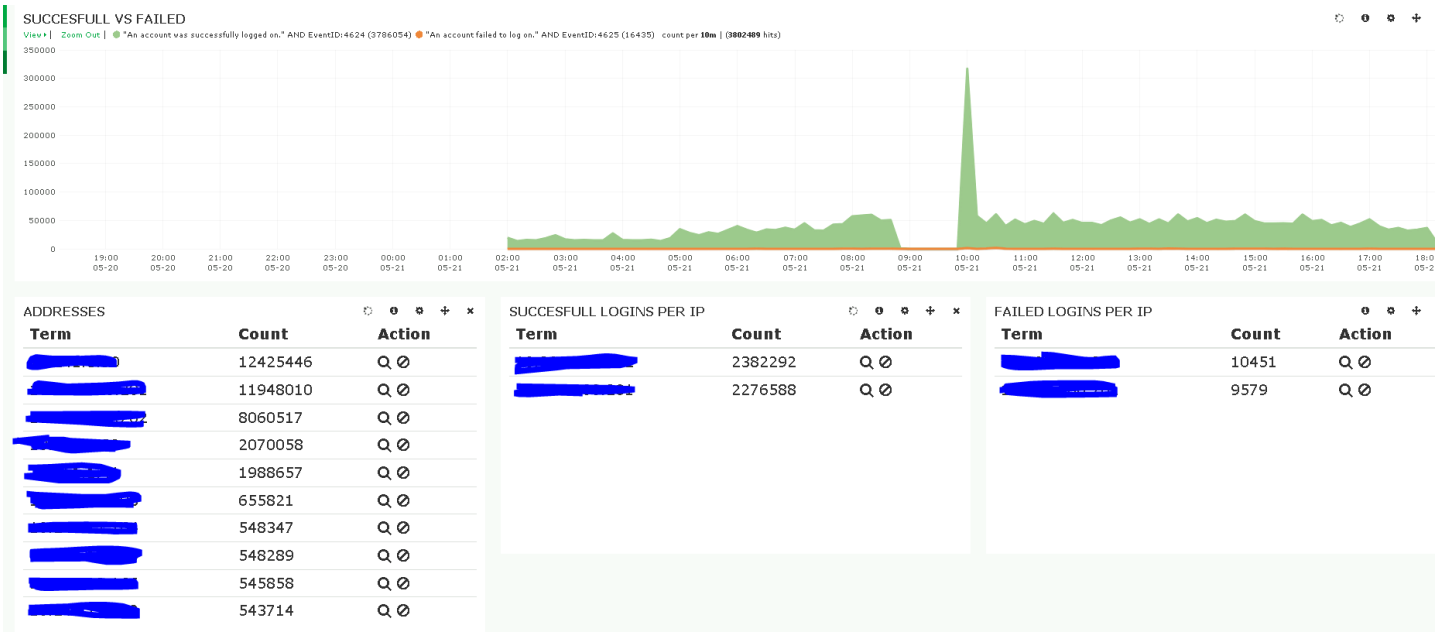
*

"An account was successfully logged on." AND EventID:4624

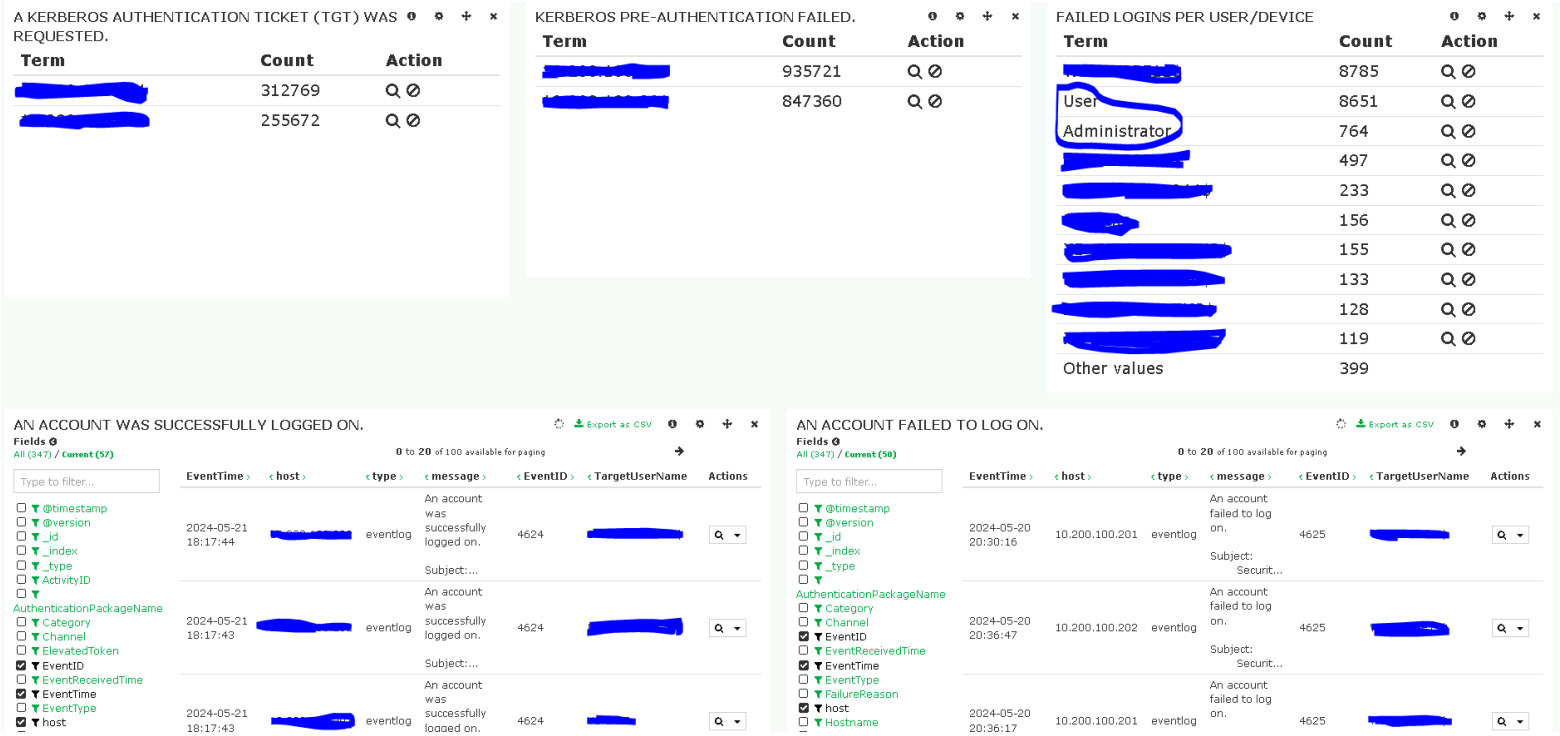
"An account failed to log on." AND EventID:4625

"Kerberos pre-authentication failed." AND EventID:4771

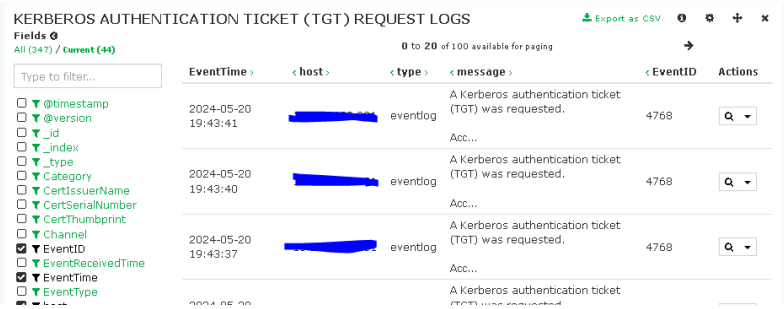
"A Kerberos authentication ticket (TGT) was requested." AND EventID:4768

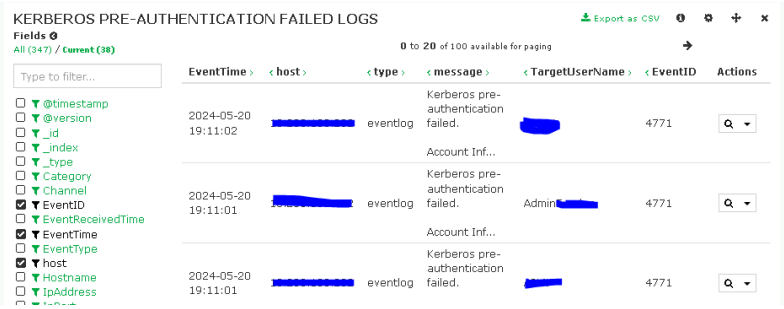


Hier zie je een event over time om het verschil aan te tonen tussen succesvolle en gefaalde logins. Daaronder zijn 3 tabellen met als eerste tabel alle adressen, daarna succesvolle logins per IP en de gefaalde logins per IP.



Hier zie je 3 andere tabellen waar bij de eerste 2 over de verdeling tussen dc01 en dc02 gaat en de laatste tabel over welke users/devices het meeste gefaalde logins heeft. Daaronder zie je 2 lijsten met daarin alle logs met betrekking tot de query's van succesvolle logins en gefaalde logins.





Dit zijn alle logs van de laatste 2 query's van hierboven zodat je deze in detail kan bekijken indien nodig. Helemaal onderaan is er ook nog een ALL-events lijst met alle logs.

Test dashboard 2:

Context: Deze test dashboards heb ik in het begin van mijn stage gemaakt en zijn heel simpel omdat ik toen nog niet voldoende kennis had van Nagios

Query's:

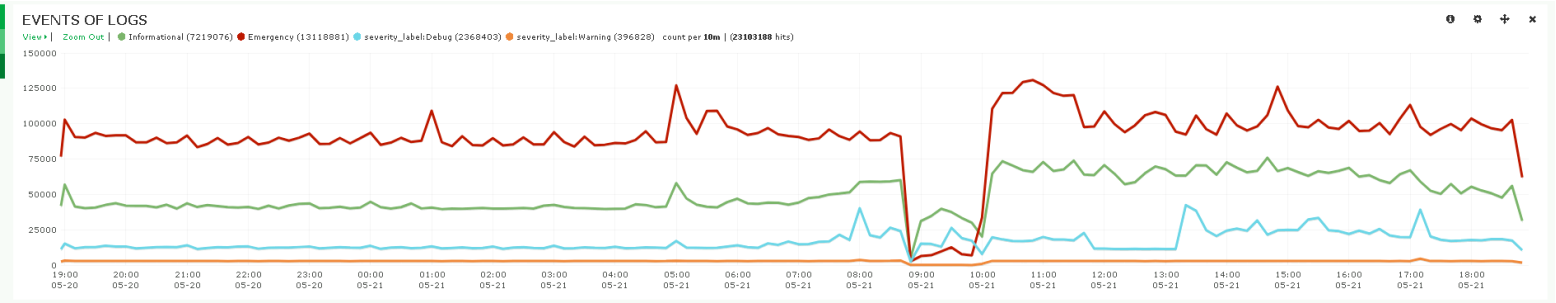
Severity_label:Informational

Severity_label:Emergency

Severity_label:Debug

Severity_label:Warning

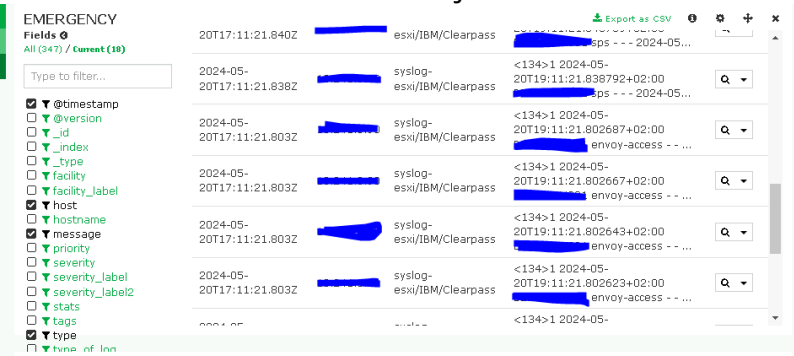
*

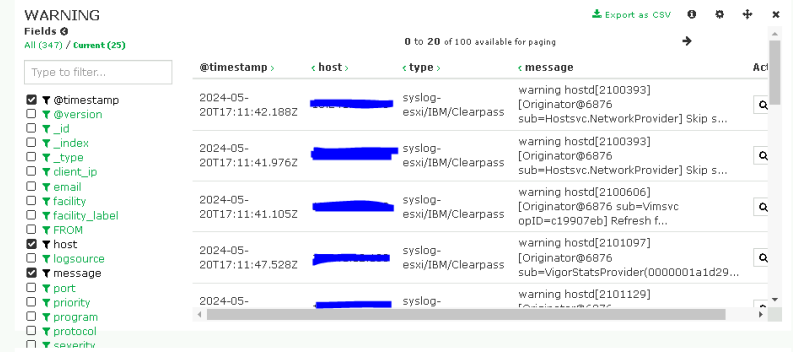


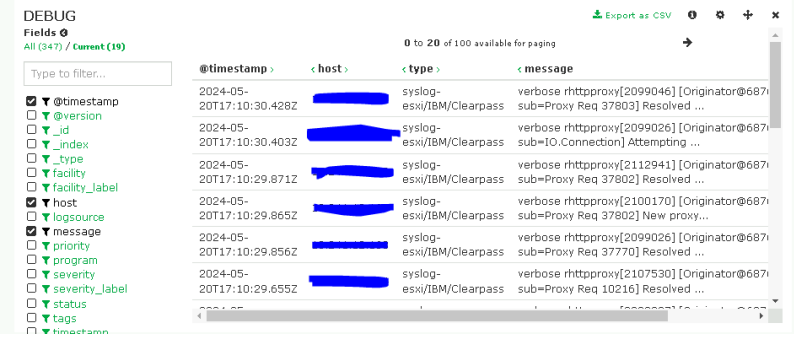
TOP TERMS IN FIELD SEVERITY_LABEL

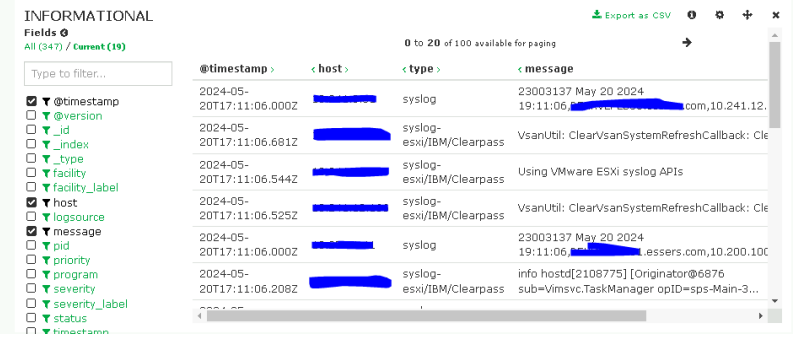
Term	Count	Action
Emergency	13119159	
Informational	7219476	
Debug	2368442	
Warning	396840	

Hier zie je een events over time van alle logs gesorteerd op severity label en daaronder kun je in de tabel zien welke severity het meest voorkomt.







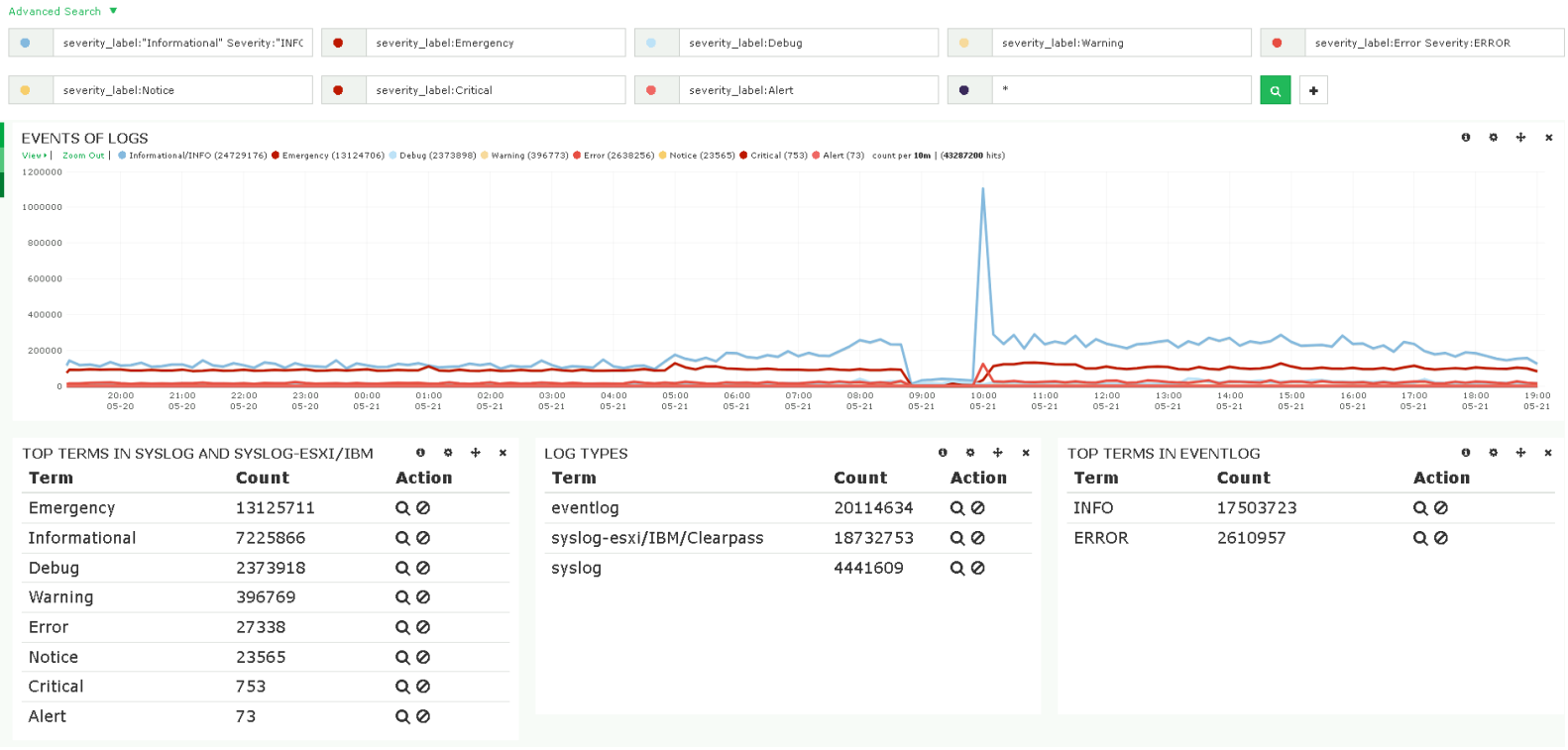


Onderaan het dashboard heb je dan de 4 verschillende severities logs in een lijst om deze verder te bekijken. Dit dashboard was meer om te kijken hoe nagios werkte.

Test dashboard 3:

Context: Dit is eigenlijk een vervolg op test dashboard 2

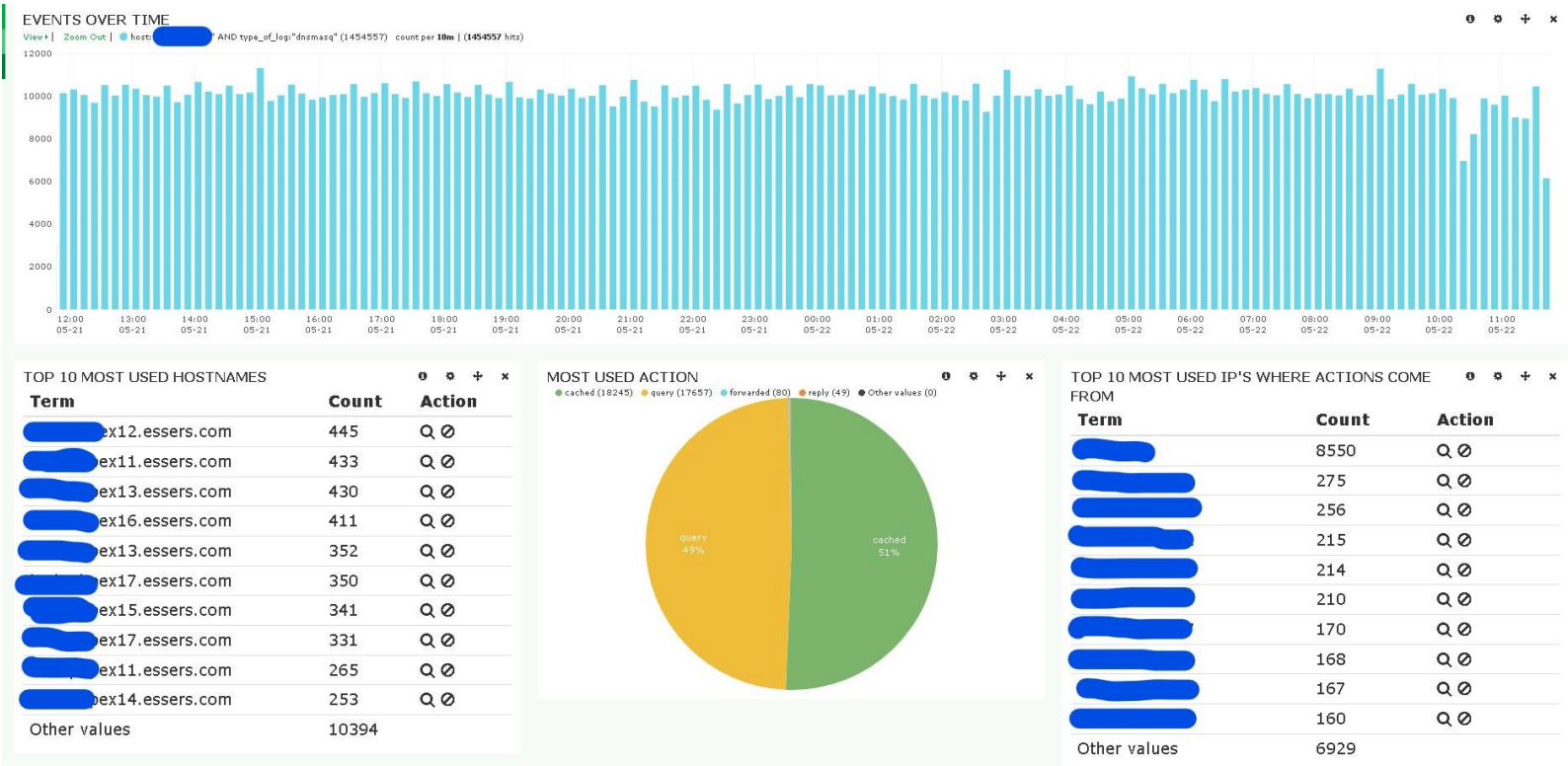
Query's:



In dit dashboard zie je ook de severities maar dan beter met een event over time histogram en 3 tabellen met de TOP severities in Syslog en Syslog esxi /IBM, vervolgens een tabel met de verschillende log types en tenslotte een tabel voor de severities van eventlog. Onderaan dit dashboard bevindt zich een ALL-events lijst zodat je alle logs kan bekijken indien nodig.

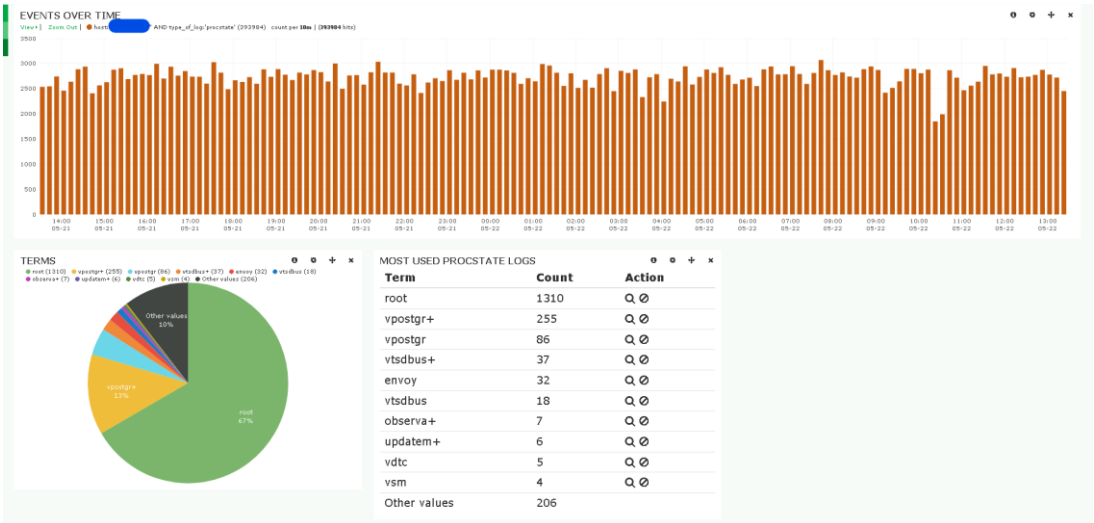
Vcenter dnsmasq dashboard:

Dit waren alle dashboards waarover ik iets kan documenteren.



Hier zie je weer een events over time histogram met daaronder 2 tabellen, de linkse voor de meest voorkomende *Hostnames* waar de acties op worden uitgevoerd en de rechtse voor de IP's waar de acties vandaan komen. In het midden hebben we dan weer een pie chart om te zien welke verschillende types er gestuurd worden en welke daarvan het meest of het minste percentage aanwezig is.

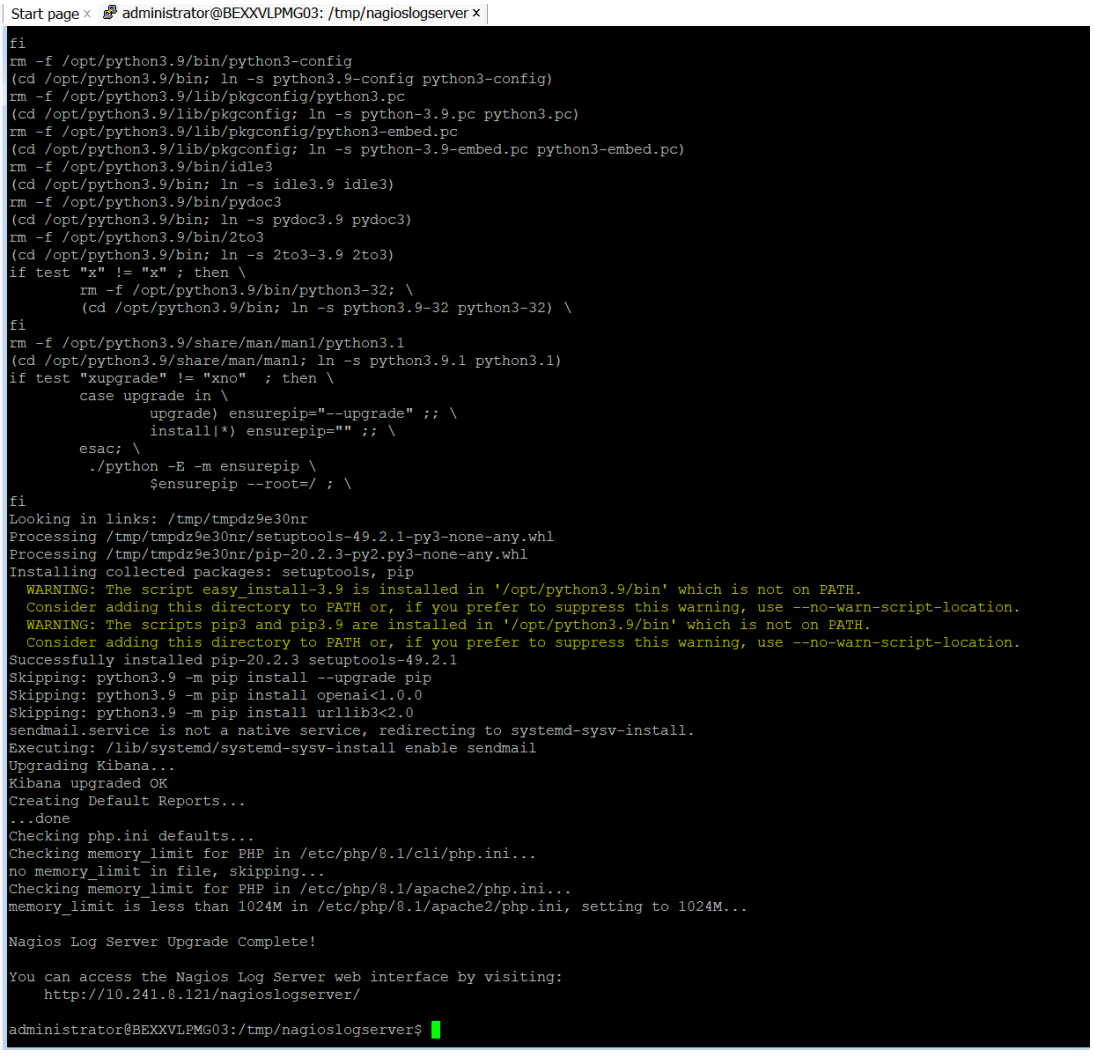
Vcenter Procstate dashboard:



Op dit dashboard heb ik niet veel geconfigureerd met de reden dat de logs die hier gegeven worden niet goed gefilterd kunnen worden maar ik heb wel een filter gemaakt die mij de verschillende soorten Procstate logs laat zien.

4.1.4 Upgrade

Als extraatje heb ik de Nagios server mogen upgraden samen met de persoon wie er verantwoordelijk voor was maar ik mocht alle handelingen doen en was verantwoordelijk voor de voorbereiden. Het was eigenlijk de bedoeling dat ik de Nagios server ging upgraden zonder op de Nagios server zelf internet connectie te moeten voorzien want op de Nagios server zelf is geen connectie naar het internet. Later bleek dat de documentatie van Nagios niet zo up-to-date is als het aankomt op upgraden zonder internet connectie, dus hebben we uiteindelijk aan het netwerkteam gevraagd om even internet connectie te voorzien voor de Nagios server. Daarna hebben we het succesvol kunnen upgraden.



Stappen bij het upgraden:

--> downloaden van de nieuwe versie

--> snapshot maken van de server voor de upgrade op VMWare (voor als er iets misgaat)

--> zorgen dan vcenter specialist eraan kon --> bestand zetten in een temp folder

--> via winscp het bestand naar de nagios log server sturen

--> als het bestand op de server was heb ik deze naar de temp folder gemoved

--> daar heb ik het uitgepakt

--> vervolgens het script upgrade gerund

--> nagios is geüpgraded

De struggles bij het upgraden:

--> verloopt niet zo vlot als gehoopt --> nagios slechte documentatie

--> eerst gaan we proberen om een paar commando's weg te laten --> niet gelukt

--> daarna proberen om met internet acces op de server nagios te upgraden

--> nagios is geüpgraded naar de nieuwste versie

De offline upgrade documentatie was niet up to date (van 2020), dus hebben een tijdelijke internet connectie laten opzetten door iemand van het netwerkteam.

4.1.5 Nagios Global Config

Dit zijn de configuraties voor filters inputs etc. zodat de nagios server logs kan ontvangen en indien nodig deze gefilterd worden.

Inputs:

Default inputs:

Active Syslog (Default)

```
syslog {
    type => 'syslog'
    port => 5544
}
```

Active Windows Event Log (Default)

```
tcp {
    type => 'eventlog'
    port => 3515
    codec => json
}
```

Active Import Files - Raw (Default)

```
tcp {
    type => 'import_raw'
    tags => 'import_raw'
    port => 2056
}
```

Active Import Files - JSON (Default)

```
tcp {
    type => 'import_json'
    tags => 'import_json'
    port => 2057
    codec => json
}
```

Inputs voor esxi:

Active Syslog 514 (ESXi)

```
syslog {
type => 'syslog-esxi/IBM/Clearpass'
port => 514
}
```

Active Syslog 1514 (ESXi)

```
syslog {
type => 'syslog-esxi'
port => 1514
}
```

Filters:

Default filters:

Active **Apache (Default)**

```
if [program] == 'apache_access' {
    grok {
        match => [ 'message', '%{COMBINEDAPACHELOG}']
    }
    date {
        match => [ 'timestamp', 'dd/MMM/yyyy:HH:mm:ss Z', 'MMM  d HH:mm:ss', 'MMM dd HH:mm:ss', 'ISO8601' ]
    }
    mutate {
        replace => [ 'type', 'apache_access' ]
         convert => [ 'bytes', 'integer' ]
         convert => [ 'response', 'integer' ]
    }
}

if [program] == 'apache_error' {
    grok {
        match => [ 'message', '\[(?<timestamp>%{DAY:day} %{MONTH:month} %{MONTHDAY} %{TIME} %{YEAR})\] \[%{WORD:class}\]
\[%{WORD:originator} %{IP:clientip}\] %{GREEDYDATA:errmsg}']
    }
    mutate {
        replace => [ 'type', 'apache_error' ]
    }
}
```

Gemaakte filters (niet actief):

Inactive **syslog client email filter**

```
if [type] == 'syslog' {
grok {
match => [ 'message', '%{EMAILADDRESS:client_email}' ]
}
}
```

Inactive **syslog-esxi/IBM/Clearpass email filter**

```
if [type] == 'syslog-esxi/IBM/Clearpass' {
grok {
match => [ 'message', '%{EMAILADDRESS:client_email}' ]
}
}
```

Inactive **syslog client email filter test2**

```
if [type] == 'syslog' {
grok {
match => [ 'message', '%{NOSPACE} %{GREEDYDATA:errormessage}' ]
}
}
```

Inactive **syslog client email filter testtest**

```
if [type] == 'syslog' {
grok {
match => [ 'message', '%{IP:ip} %{GREEDYDATA:message}']
overwrite => ["message"]
}
}
```

Inactive **eventlog filter**

```
if [type] == 'eventlog' {
grok {
match => [ 'message', '%{GREEDYDATA:errormessage}' ]
}
}
```

Inactive **syslog-esxi/IBM/Clearpass email filter**

```
if [type] == 'syslog-esxi/IBM/Clearpass' {
grok {
match => [ 'message', '%{LOGLEVEL:loglevel} %{GREEDYDATA:errormessage}' ]
}
}
```

Inactive **syslog-esxi/IBM/Clearpass email filter**

```
if [type] == 'syslog-esxi/IBM/Clearpass' {
grok {
match => [ 'message', '%{NOSPACE} %{GREEDYDATA:errormessage}' ]
}
}
```

Inactive **syslog-esxi/IBM/Clearpass email filter**

```
if [type] == 'syslog-esxi/IBM/Clearpass' {
grok {
match => [ 'message', '%{GREEDYDATA:errormessage}' ]
}
}
```

Inactive **ESXi**

```
if [host] == '[redacted] or [host] == '[redacted]' or [host] == '[redacted] or [host] == '[redacted] or
[host] == '[redacted] or [host] == '[redacted] or [host] == '[redacted]or [host] == '[redacted]' or
[host] == '[redacted]' or [host] == '[redacted] or [host] == '[redacted] or [host] == '[redacted]' or
[host] == '[redacted]' or [host] == '[redacted] or [host] == '[redacted] {
mutate {
replace => { 'type' => 'syslog-esxi' }
}
}
```

Inactive **test PA**

```
if [host] == '[redacted] {

   grok {
    match => {
          "message" => [
            "Ip: %{IP:test}",
            "Speed: %{NUMBER:speed}"
          ]
        }

  }
}
```

Gemaakte filters (actief):

Active **test JIRA**

```
if [host] == '[redacted]' or [host] == '[redacted]' {

   grok {
    match => { "message" => "EntityName=%{DATA:EntityName},Category=%{DATA:Category},Action=%{DATA:Action},User=%
{WORD:User}" }
  }
}
```

Active **test PA**

```
if [host] == '[redacted]' {

   grok {
    match => { "message" => "000702489883,%{WORD:sysorconf}" }

  }
}


if [host] == '[redacted]' and [sysorconf] == 'SYSTEM' {

   grok {
    match => { "message" => "000702489883,%{WORD},%{WORD},%{INT},%{DATA},,%{DATA:failorsuccess}," }

  }
}
if [host] == '[redacted]' and [sysorconf] == 'SYSTEM' and [failorsuccess] == 'auth-success' {
     grok {
    match => { "message" => "user %{QS:user}. %{DATA:data} auth profile %{QS:auth_profile}, vsys %{QS:vsys_status},
server profile %{QS:server_profile}, server address %{QS:server_address}, auth protocol %{QS:auth_protocol}, admin role %
{QS:admin_role}, From: %{IP:client_ip}." }

  }
}
if [host] == '[redacted]' and [sysorconf] == 'SYSTEM' and [failorsuccess] == 'auth-fail' {
     grok {
    match => { "message" => "user %{QS:user}. %{DATA:data}." }

  }
}
if [host] == '[redacted]' and [sysorconf] == 'CONFIG' {

   grok {
    match => { "message" => "%{IP:client_ip},,%{DATA:action},%{WORD:user},%{WORD:WeborCLI},%{WORD:status},%{DATA:data}," }

  }
}
```

Active test F5

```
if [host] == '[redacted]' {

   grok {
    match => { "message" => "%{WORD} %{WORD}%{DATA:status}:" }
  }
}

if [host] == '[redacted]' and [status] == '[13559]' {

   grok {
    match => { "message" => "%{HOSTPORT:client_ip} Authentication%{DATA}%{EMAILADDRESS:email}" }
  }
}

if [host] == '[redacted]' and [status] == '[18805]' {

   grok {
    match => { "message" => "SSL Handshake failed for %{WORD:protocol} %{IP:FROM}:%{INT:port} -> %{HOSTPORT:TO}" }
  }
}
if [host] == '[redacted]' and [status] == '[13814]' {

   grok {
    match => { "message" => "user %{QS:user}" }
  }
}
```

Active [redacted]CO1 test

```
if [host] == [redacted] {

   grok {
    match => { "message" => "%{TIMESTAMP_ISO8601} %{WORD:hostname} %{EMAILLOCALPART:type_of_log}" }
  }

}

if [host] == '[redacted]' and [type_of_log] == 'vpxd-main' {

   grok {
    match => { "message" => "%{TIMESTAMP_ISO8601} %{WORD} %{EMAILLOCALPART} %{DATA} %{TIMESTAMP_ISO8601} %
{WORD:severity_label2}" }
  }

}
if [host] == '[redacted]' and [type_of_log] == 'vpxd-svcs-perf' {

   grok {
    match => { "message" => "%{TIMESTAMP_ISO8601} %{WORD} %{EMAILLOCALPART} %{DATA} %{TIMESTAMP_ISO8601} %{DATA} %
{LOGLEVEL:severity_label2} %{DATA}\] %{GREEDYDATA:stats}" }
  }

}
if [host] == '[redacted]' and [type_of_log] == 'vpxd-svcs-access' {

   grok {
    match => { "message" => "%{TIMESTAMP_ISO8601} %{WORD} %{EMAILLOCALPART} %{DATA} %{TIMESTAMP_ISO8601} %{INT} %{INT}
%{EMAILLOCALPART:tomcat-exec-id} %{INT:status_code} %{QS:topic} %{EMAILLOCALPART:http_method}" }
  }

}
if [host] == '[redacted]' and [type_of_log] == 'eam-access' {

   grok {
    match => { "message" => "%{TIMESTAMP_ISO8601} %{WORD} %{EMAILLOCALPART} %{DATA} \[%{EMAILLOCALPART:tomcat-http--
id}\] %{QS:http_method_and_topic} %{INT:status_code} %{INT} %{DATA} %{QS:topic}" }
  }

}

if [host] == '[redacted]' and [type_of_log] == 'vpxd' {

   grok {
    match => { "message" => "%{TIMESTAMP_ISO8601} %{WORD} %{EMAILLOCALPART} %{DATA} \[%{TIMESTAMP_ISO8601}\] %{DATA} \
[%{LOGLEVEL:severity_label2}\] (\[%{DATA:user}\]|\[\]) (\[%{DATA:location}\]|\[\]) \[%{INT}\] \[%
{DATA:shortermessage}\]" }
  }
```

Active test monitored ad groups (short message)

```
if [Category] == 'Security Group Management' {

   grok {
    match => { "message" => "%{DATA:messageTitle}\n" }
  }
}
```

Active **dnsmasq en procstate en sps vcenter filter**

```
if [type_of_log] == 'dnsmasq' {

   grok {
    match => { "message" => "dnsmasq - - - %{MONTH} %{MONTHDAY} %{TIME} %{DATA} %{WORD:action}%{DATA} %
{HOSTNAME:target_hostname} %{WORD} %{IP:client_ip}" }
  }
}

if [type_of_log] == 'procstate' {

   grok {
    match => { "message" => "procstate - - - %{DATA:type_of_procstate} %{SPACE}" }
  }
}

if [type_of_log] == 'sps' {

   grok {
    match => { "message" => "sps - - - %{TIMESTAMP_ISO8601} \[%{DATA}\] %{LOGLEVEL:severity_label2} %{SPACE}opId=%
{EMAILLOCALPART:opID} %{DATA} - %{GREEDYDATA:shortermessage}" }
  }
}
```

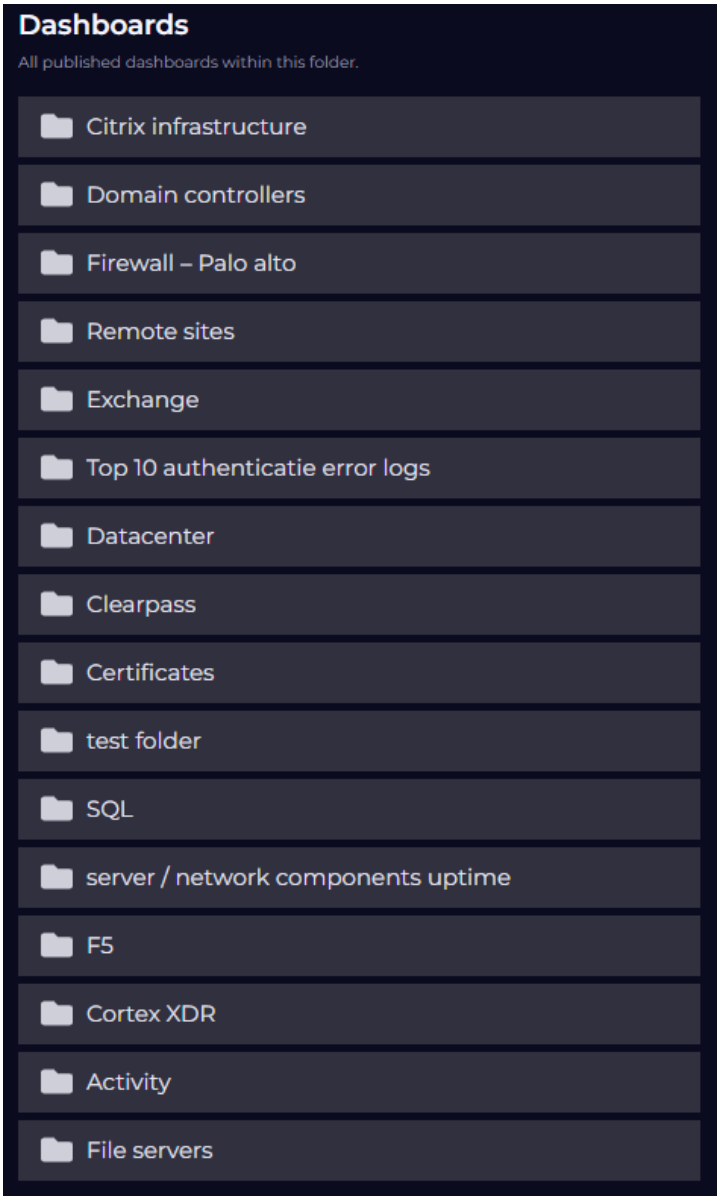
4.1.6 Configuration

In Configure had je de mogelijkheid om de Elasticsearch Database Service en Logstash Collector Service opnieuw op te starten of eventueel stoppen. Dit is namelijk niet altijd genoeg geweest om problemen op te lossen en heb regelmatig aan de persoon die verantwoordelijk is voor deze server moeten vragen om de server te herstarten omdat ik zelf niet aan deze server mocht komen.

4.2 Squared up

In dit deel zie je de realisaties in Squared up.

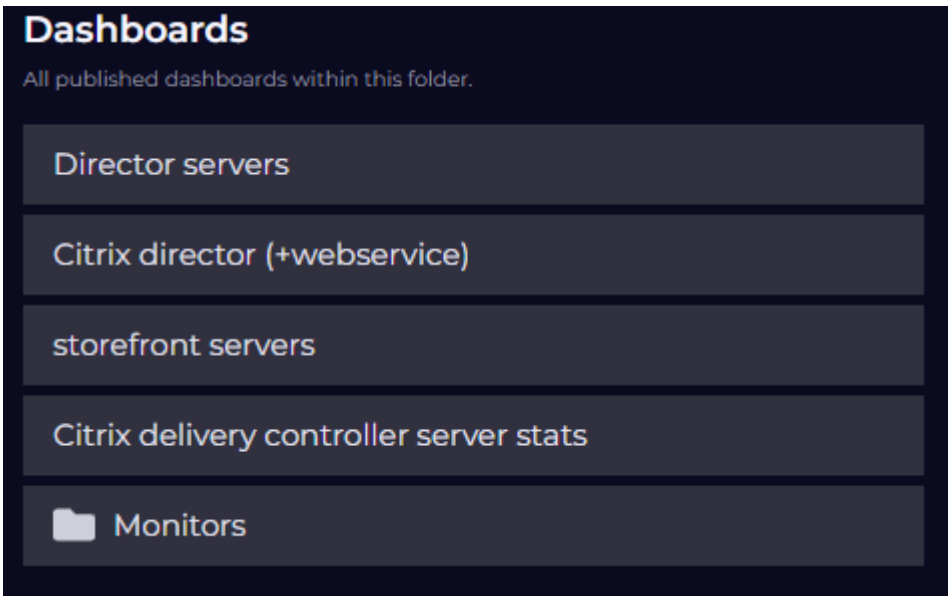
4.2.1 Dashboards



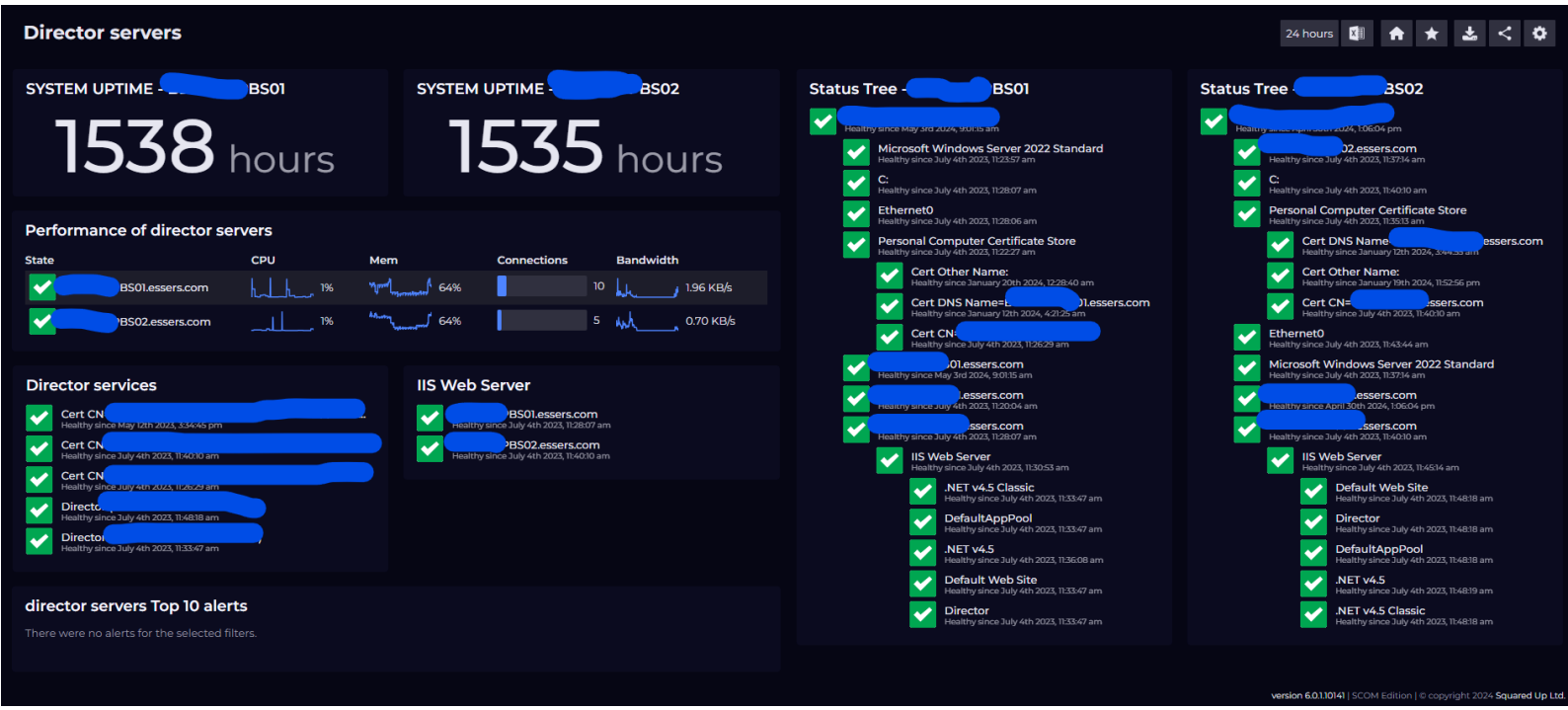
Dit zijn alle onderdelen die ik heb behandeld in Squared up.

Citrix:

We starten met de Citrix dashboards.

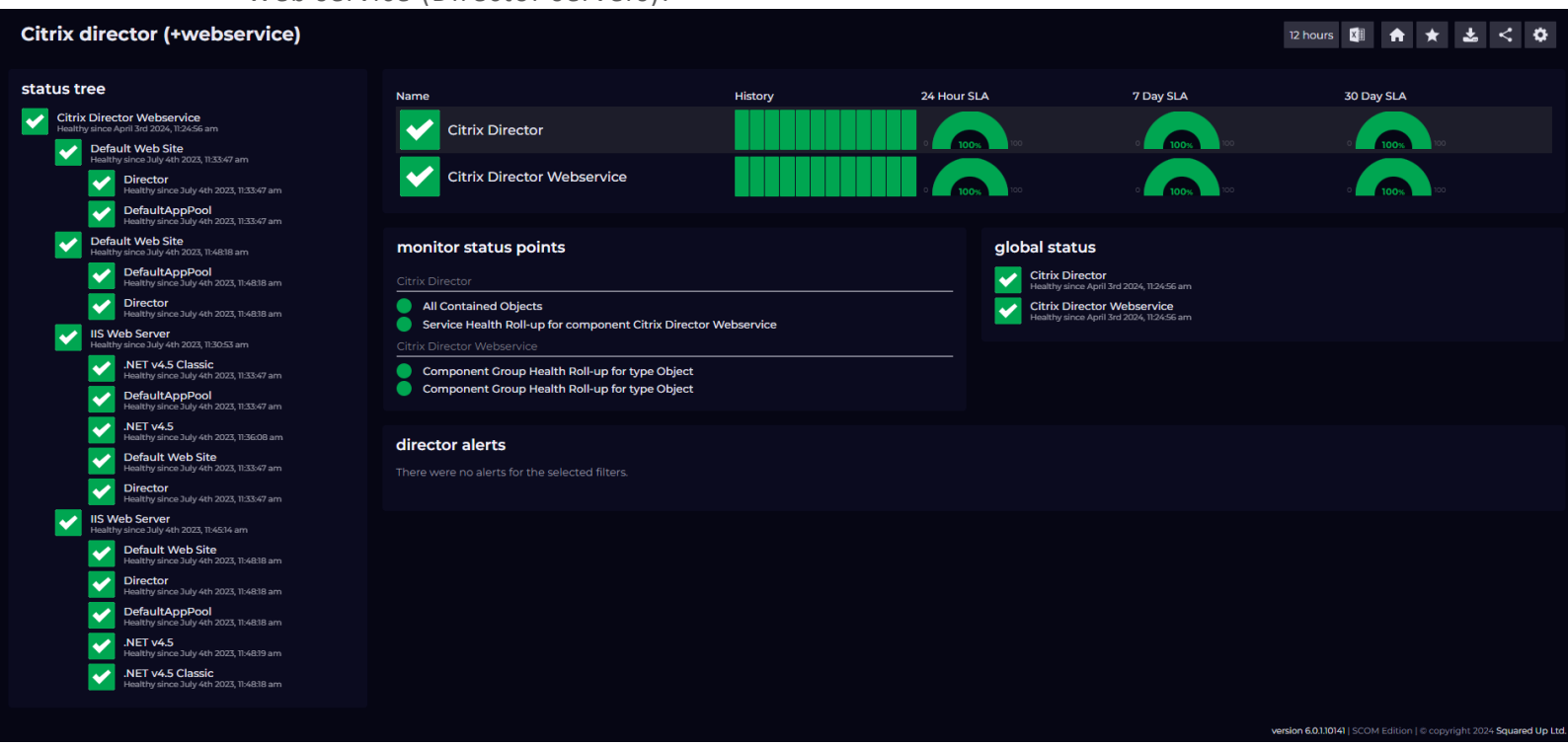


Director servers dashboard:



In dit dashboard zie je de uptime van de 2 director servers, een status tree per server en ook de Director services en certificaten gelinkt aan de director servers. De IIS Web Server service was een belangrijke service die ik moest monitoren. Tenslotte ook nog de TOP 10 alerts van de 2 servers.

Web service (Director servers):



Het volgende dashboard is meer gefocust op de web service met een status tree alleen voor Citrix Director Web service met daarnaast een *matrix* waar je de *health*, *health history* en de SLA in 24h/7d/30d ziet. Daaronder een paar monitors die gekoppeld zijn aan de servers en tenslotte ook nog alerts die bij de Director servers horen.

Storefront servers:

Dit is het dashboard voor de storefront servers, hierbij hebben we ook de Uptime van de servers aan de zijkant staan met daarnaast een status tree per storefront server. Vervolgens ook nog matrix waar je de health, CPU gebruik, memory gebruik, aantal connecties en de bandbreedte op kan zien. Daaronder hebben we ook nog status checks voor de certificaten, Delivery services authentication, IIS-web server en de receiver for web service met tenslotte daaronder nog de TOP 10 alerts van de storefront servers.

Delivery controller servers:

Dit is het dashboard van de delivery controllers met alweer de uptime v/d servers met daaronder de status van de Citrix Delivery Services Resources en De IIS Web Servers services. Aan de rechterkant hebben we een matrix waar je health status, CPU gebruik, memory gebruik, aantal connecties en de bandbreedte die gebruikt wordt kan zien. Daaronder vind je de alerts van de servers en tenslotte ook nog de status trees van de 2 delivery controllers.

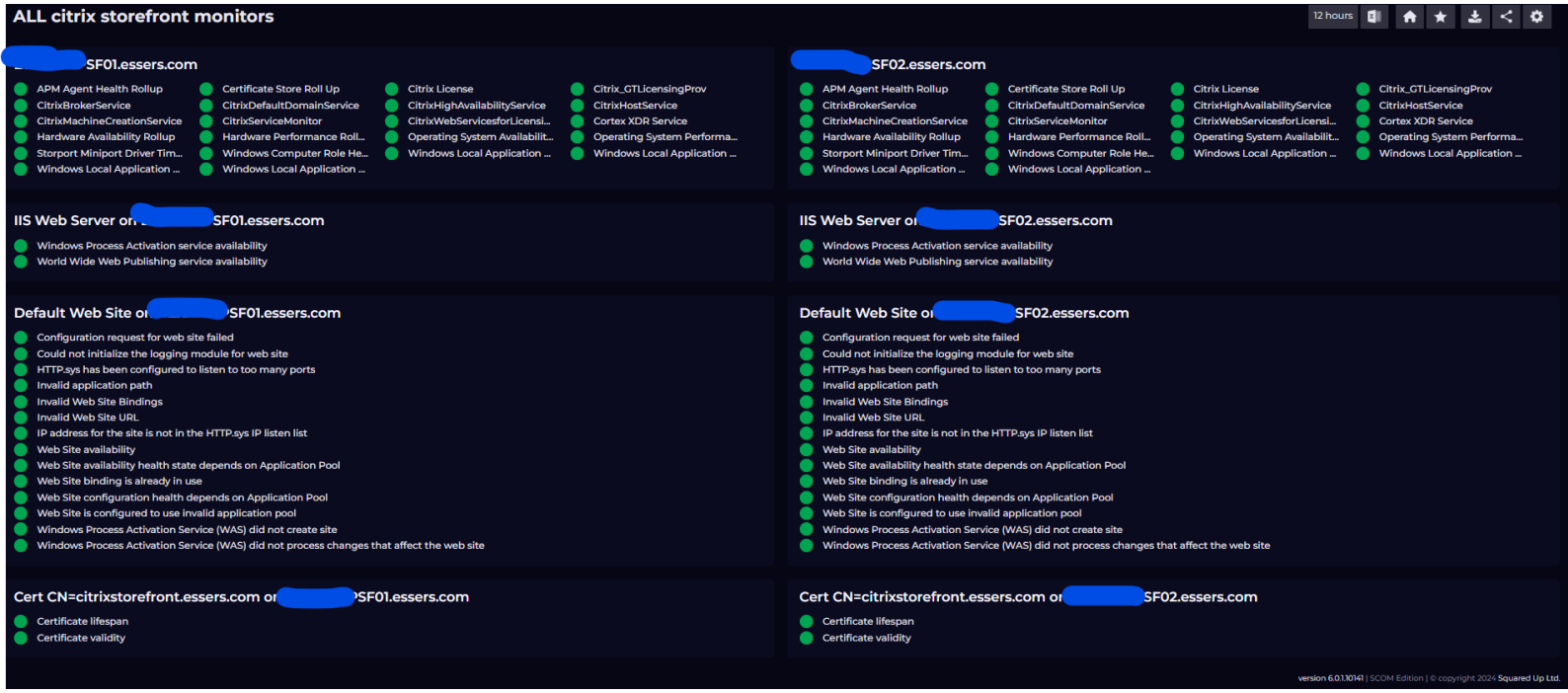
ALL Citrix director monitor:

Volgende dashboards gaan ongeveer hetzelfde zijn als deze die je hier ziet. Het is de bedoeling dat je een snel overzicht krijgt over alle monitors zodat je snel kan zien welke delen van de servers problemen hebben.

De verschillende monitors zijn:

- De server monitors
- IIS Web Server monitors
- Default Web Site monitors
- Director monitors

ALL Citrix Storefront monitors:



Zoals al aangehaald is dit dashboard hetzelfde opgebouwd als het vorige dashboard en zijn dit de verschillende monitors:

- De server monitors
- IIS Web Server monitors
- Default Web Site monitors
- Storefront certificaat monitors

ALL Citrix Delivery server monitors:

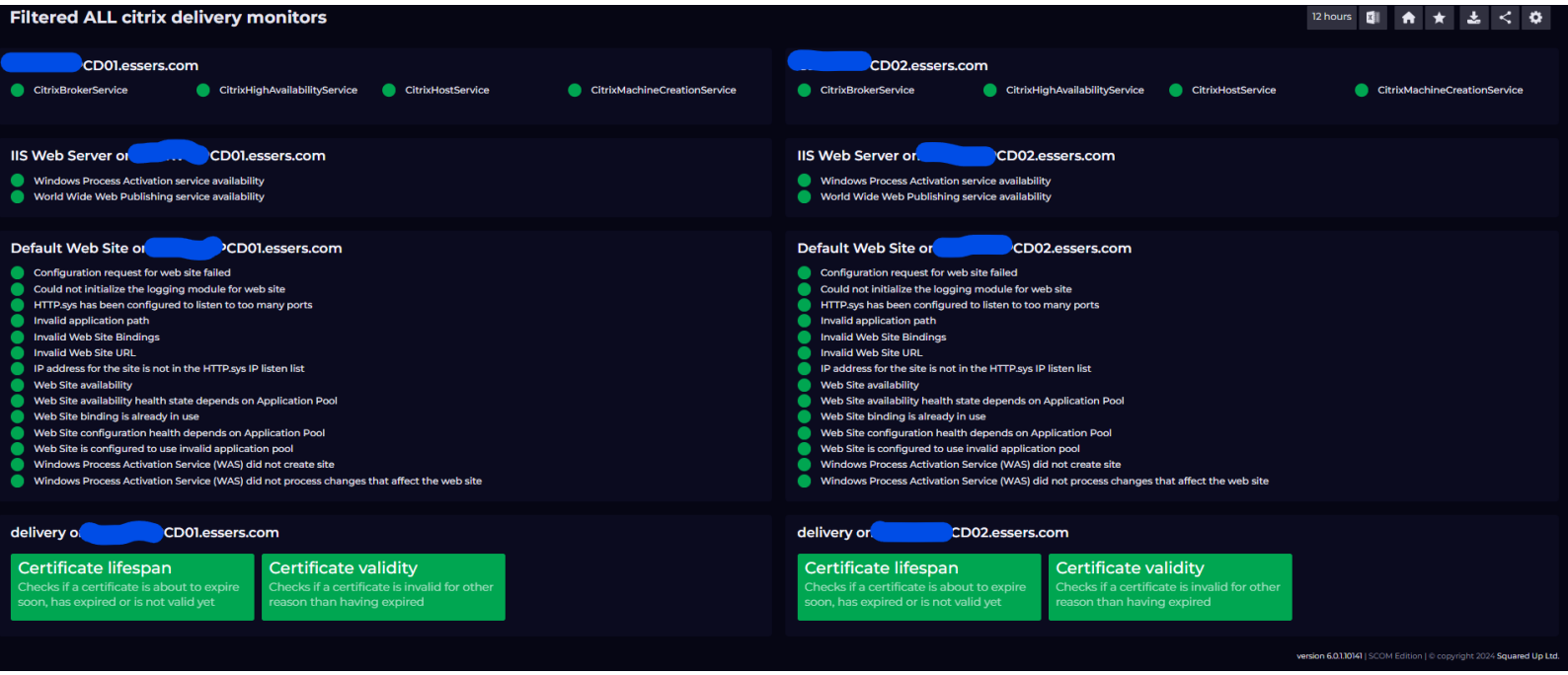
Tenslotte het laatste monitor dashboard van de Citrix servers dat ik wil documenteren is de Citrix Delivery monitor dasboard.

De verschillende monitors zijn:

- De server monitors
- IIS Web Server monitors
- Default Web Site monitors
- Delivery certificaat monitors

De volgende screenshots zijn de gefilterde versies van de bovenstaande dashboards. Dit wil zeggen dat er bepaalde monitors uitgelaten zijn zodat de meest belangrijke er meer uit springen.

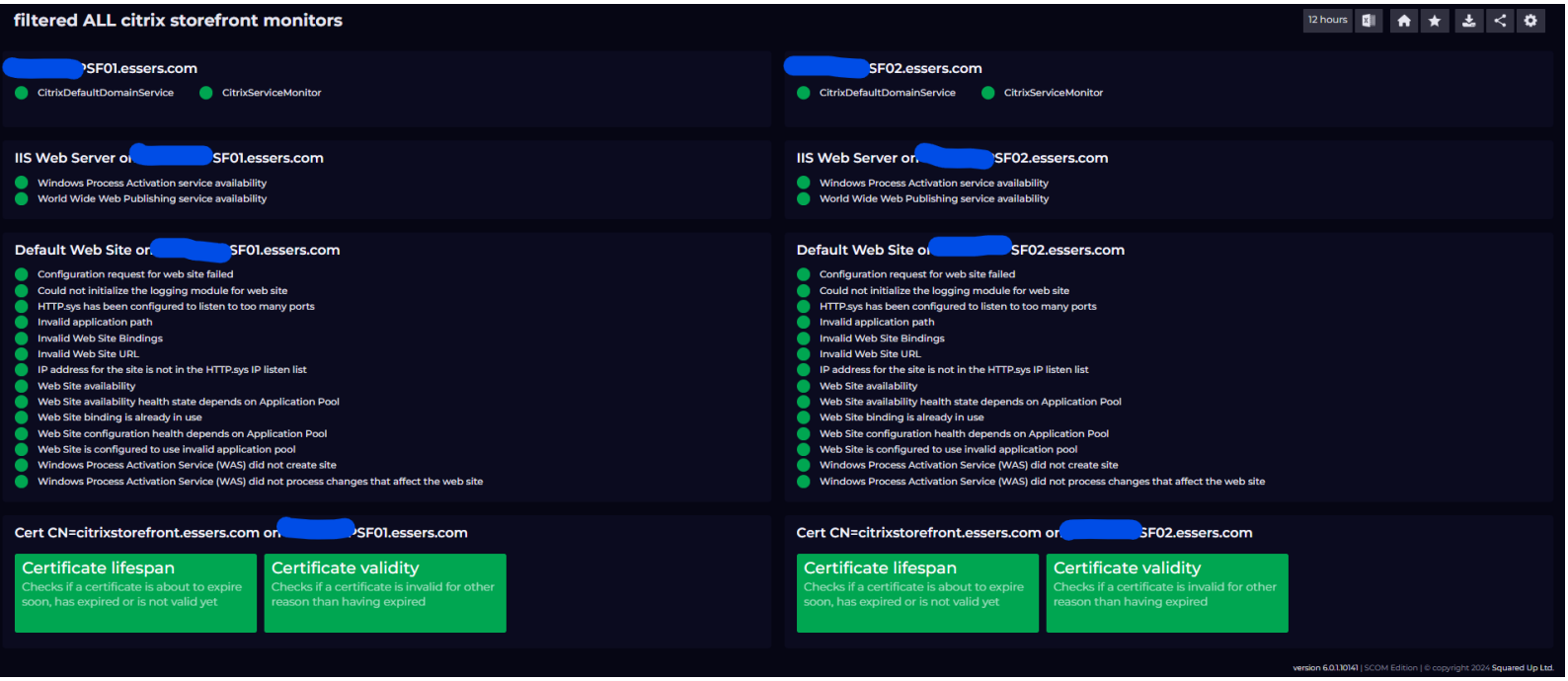
Filtered ALL Citrix Delivery server monitors:



Voor de Delivery controllers waren de volgende services belangrijk:

- CitrixBrokerService
- CitrixMachineCreationService
- CitrixHostService
- CitrixHighAvailabilityService

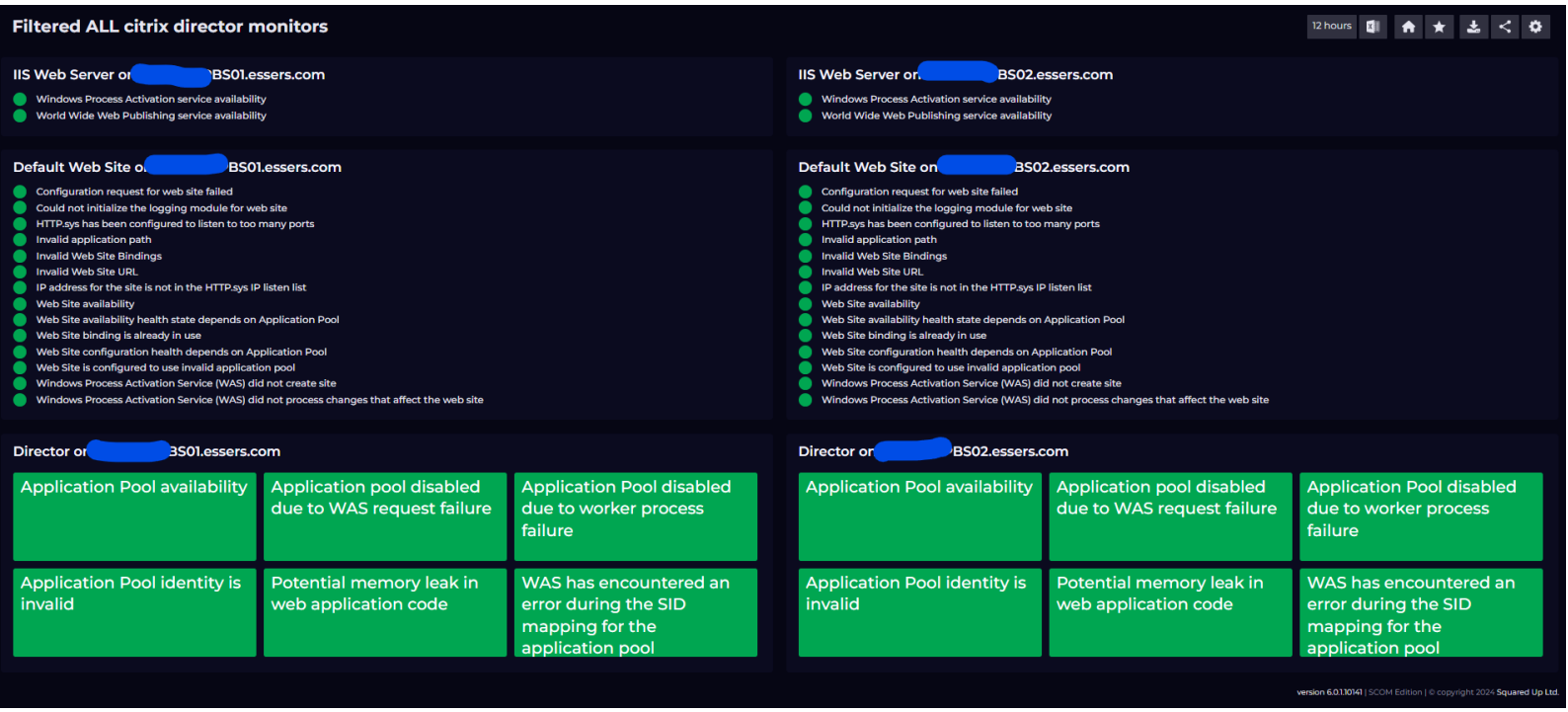
Filtered ALL Citrix Storefront monitors:



Voor de Storefront servers waren de volgende services belangrijk:

- CitrixDefaultDomainService
- CitrixServiceMonitor
- W3SVC of IIS

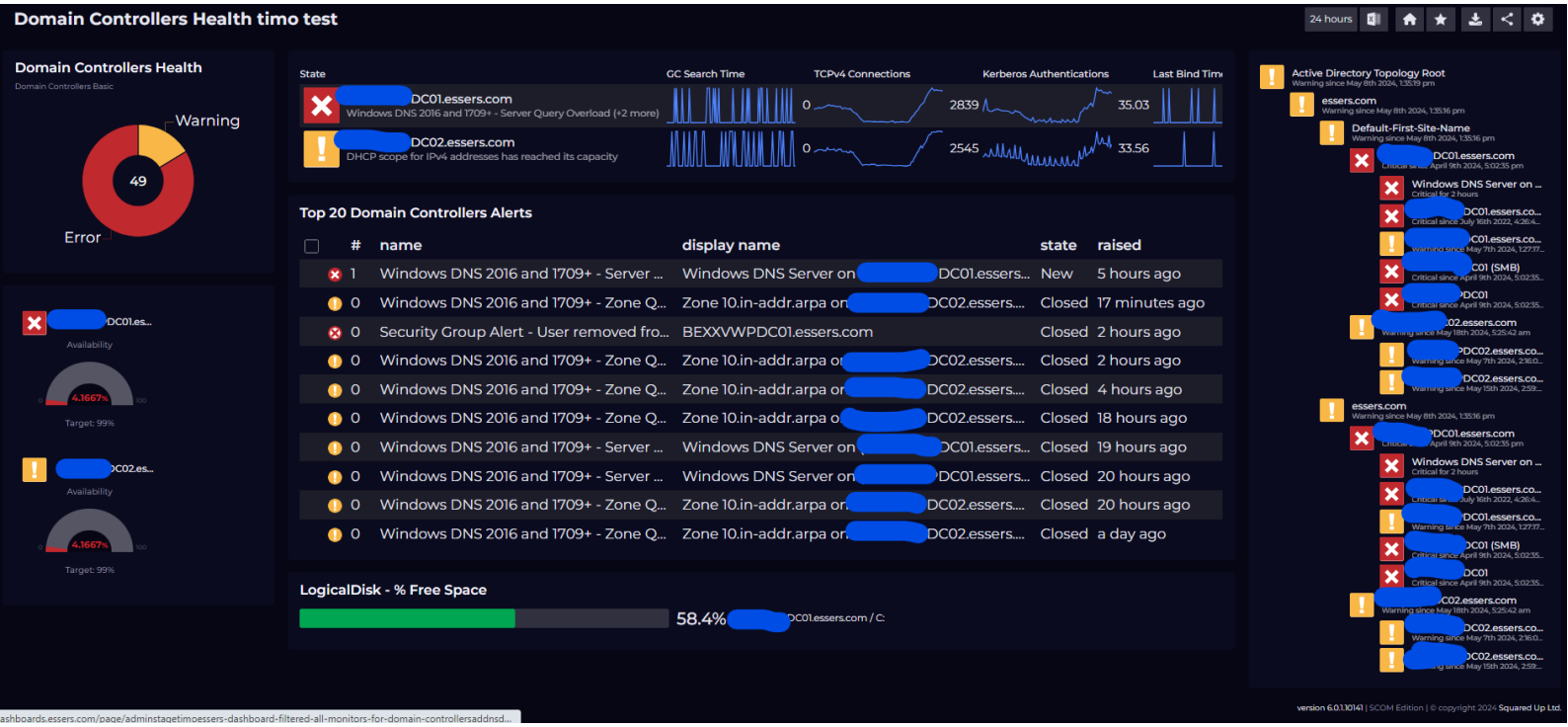
Filtered ALL Citrix Director monitors:



Voor de Director servers was er maar 1 die heel belangrijk is en dat is de W3SVC service.

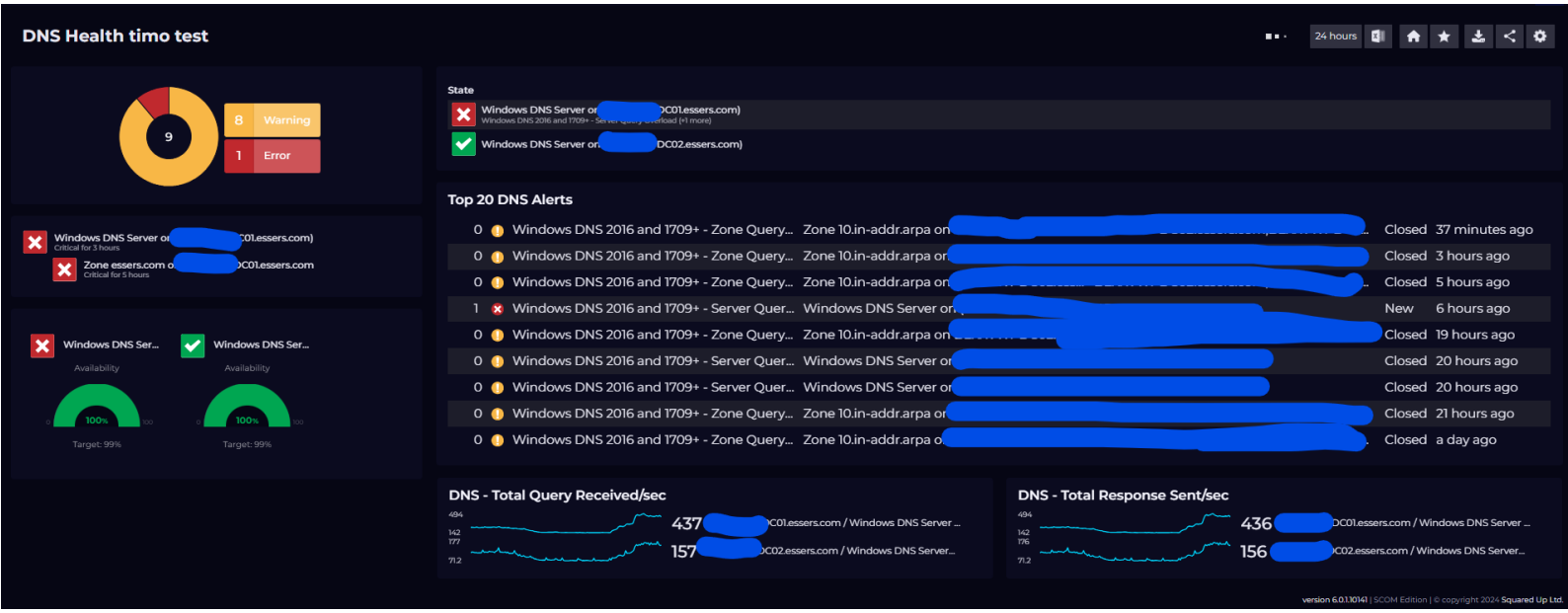
Domain controllers:

Domain Controllers Health:



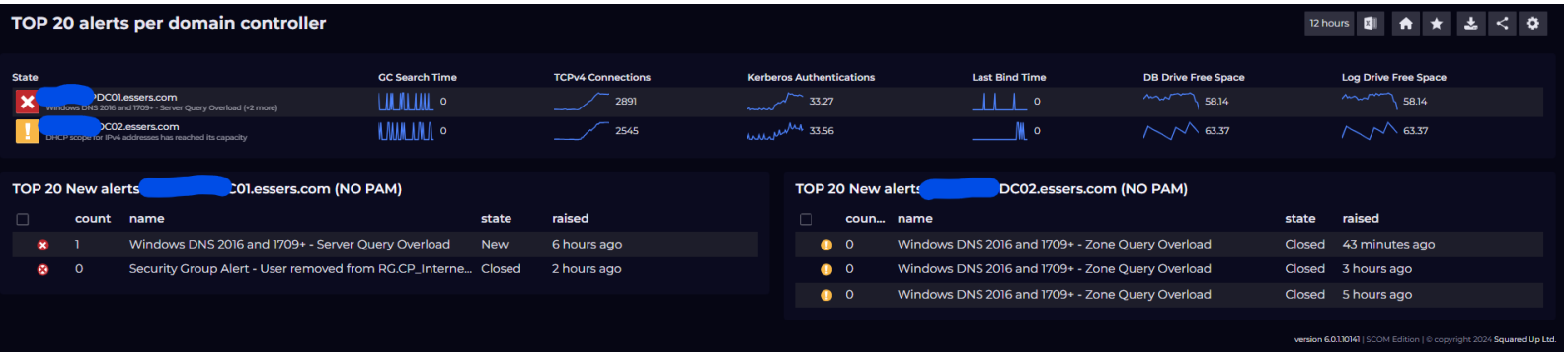
Dit dashboard draait rond de 2 domain controllers waar we weer verschillende dingen terugzien die we in de vorige dashboards al gezien hebben maar er zijn ook een paar andere monitors zoals de *SLA's* voor de 2 domain controllers en de vrije disk ruimte onderaan het dashboard.

DNS Health:



Dit dashboard is voor de DNS van Essers dit wordt gemanaged in de Domain controllers, zoals je kan zien komen er weer veel dingen terug die we al eerder gezien hebben maar een nieuwigheid is de performance grafieken onderaan het dashboard die weergeven hoeveel query's per seconden er aankomen en weg worden gestuurd.

Top 20 alerts per domain controller:

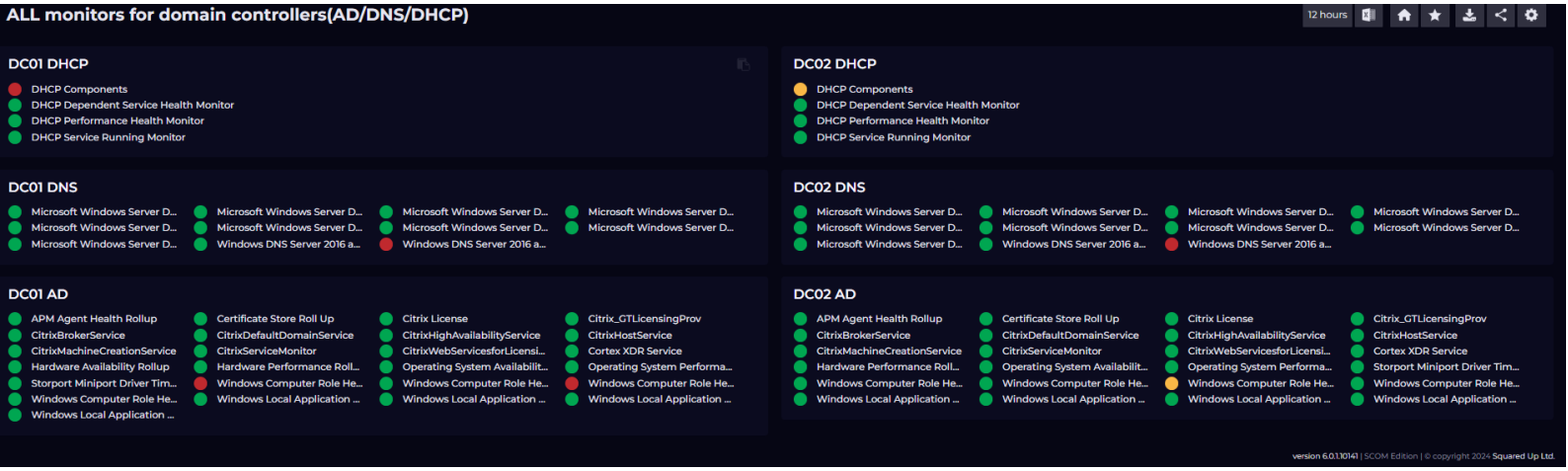


Dit dashboard is gemaakt omdat ze een dashboard wouden met de TOP 20 domain controller alerts. Aangezien het maar saai was om alleen de alerts te laten zien heb ik besloten om ook een matrix toe te voegen met verschillende waardes op die handig kunnen zijn. De alerts zijn ook onderverdeeld per domain controller waardoor het overzichtelijker wordt.

DHCP-health:

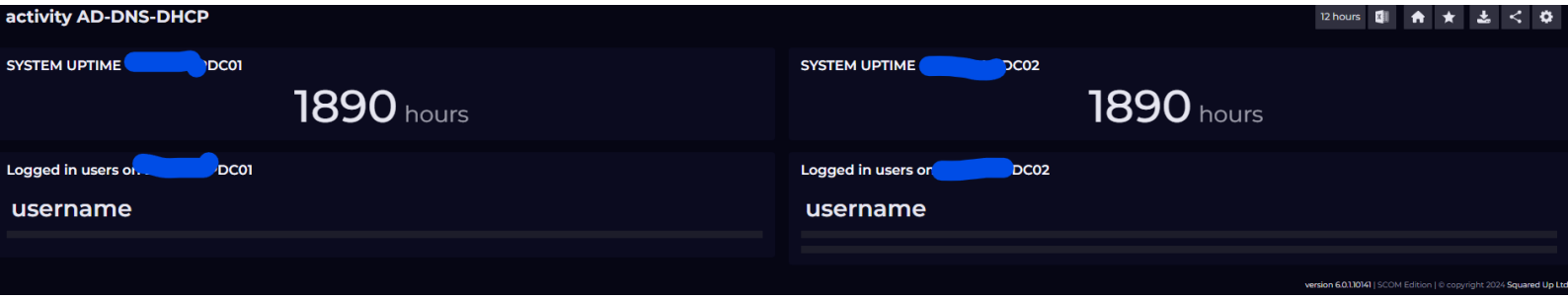
Dit dashboard is special voor de DHCP dat ook gemanaged wordt via de domain controllers en zoals je kan zien zijn er weer veel terugkomende elementen. De performance grafieken zijn er ook weer in verwerkt omdat je altijd wel wilt weten hoe je DHCP het daadwerkelijk doet.

ALL monitors for domain controllers:



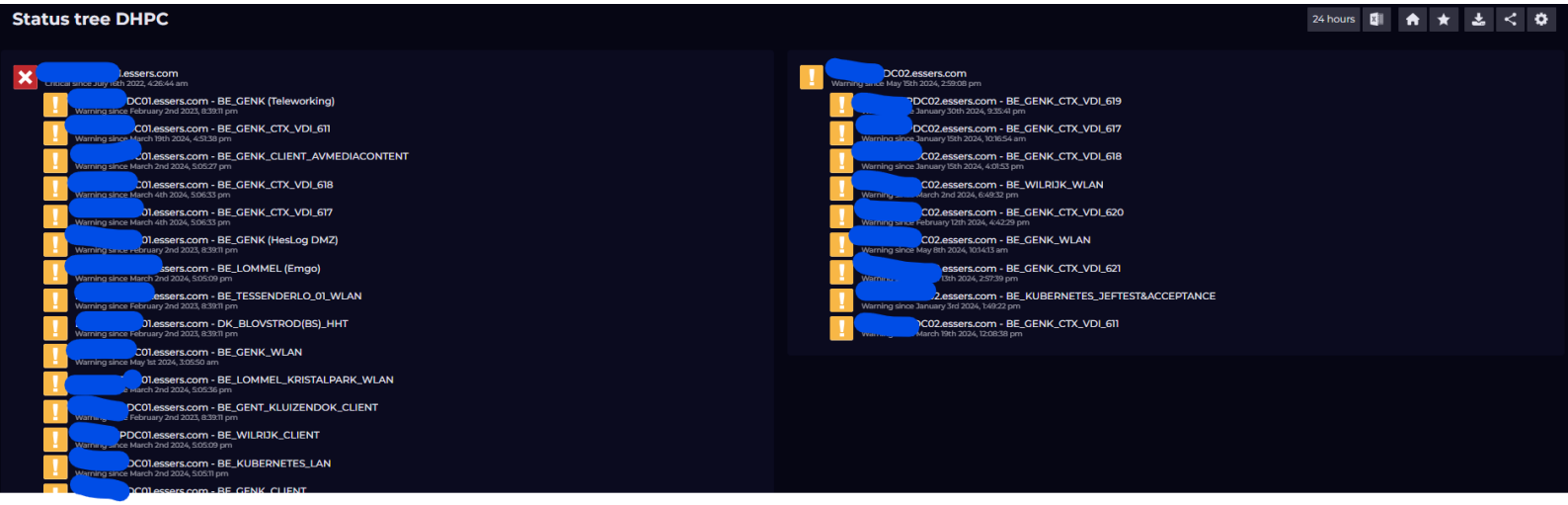
Dit dashboard is voor AD/DHCP/DNS en laat heel overzichtelijk zien welk deel van AD, DHCP of DNS moeilijkheden heeft.

AD-DNS-DHCP activity:



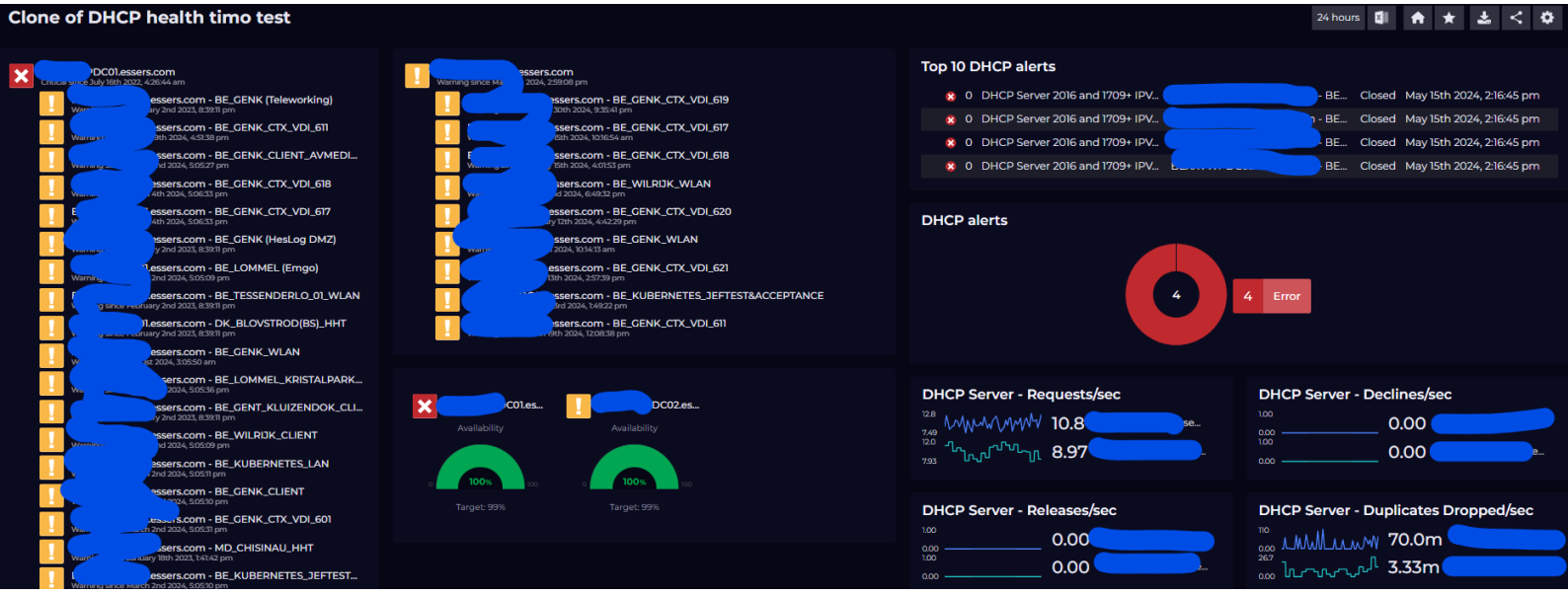
Dit dashboard laat de activiteit op de server zien, dus de naam van de users die aangemeld zijn op de Domain controllers worden hier weergegeven.

Status tree DHCP:



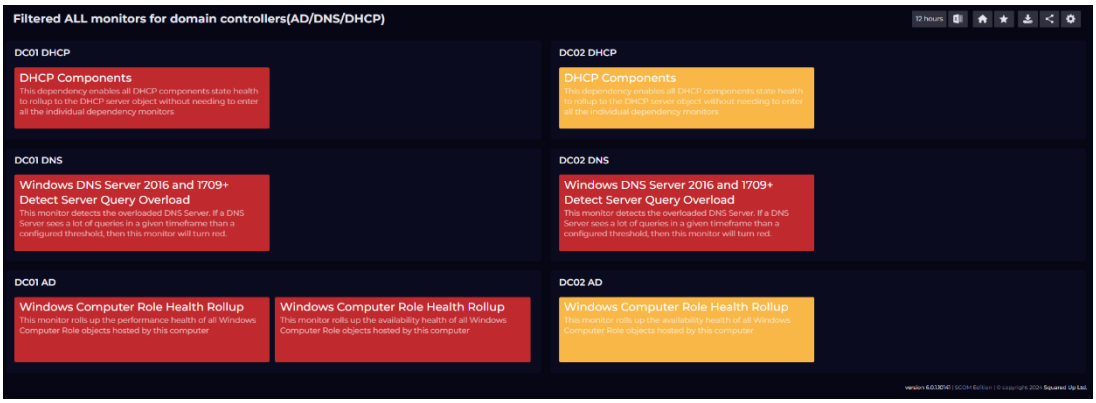
Dit dashboard is meer voor te bekijken op een laptop als je snel iets wil bekijken wat er allemaal mis is met de DHCP want de lijst in deze status tree gaat nog even door.

Clone of DHCP-health:



Dit dashboard is een geëxperimenteerd dashboard voor DHCP.

Filtered ALL monitors for domain controllers:

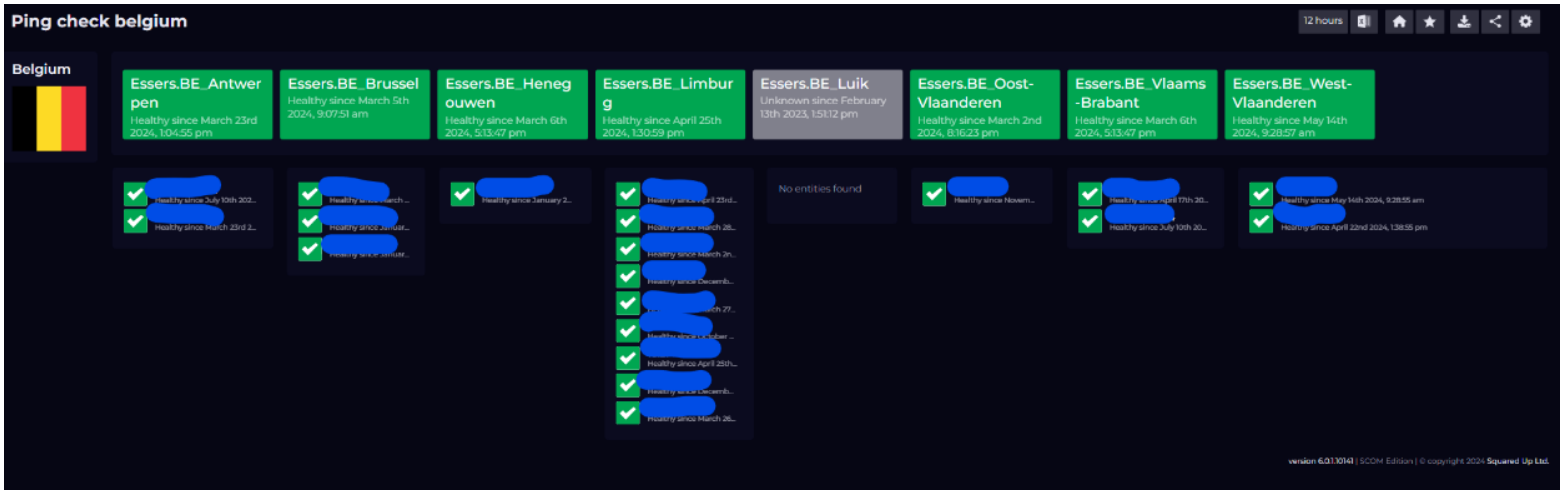


Dit dashboard is hetzelfde als het andere monitor dashboard voor AD/DHCP/DNS maar hier is het gefilterd en heeft het een groter beeld op wat er fout gaat.

Remote sites:

De remote sites in deze dashboards zijn nog niet alle remote site. De andere remote sites moeten nog toegevoegd worden in SCOM.

Ping check Belgium:

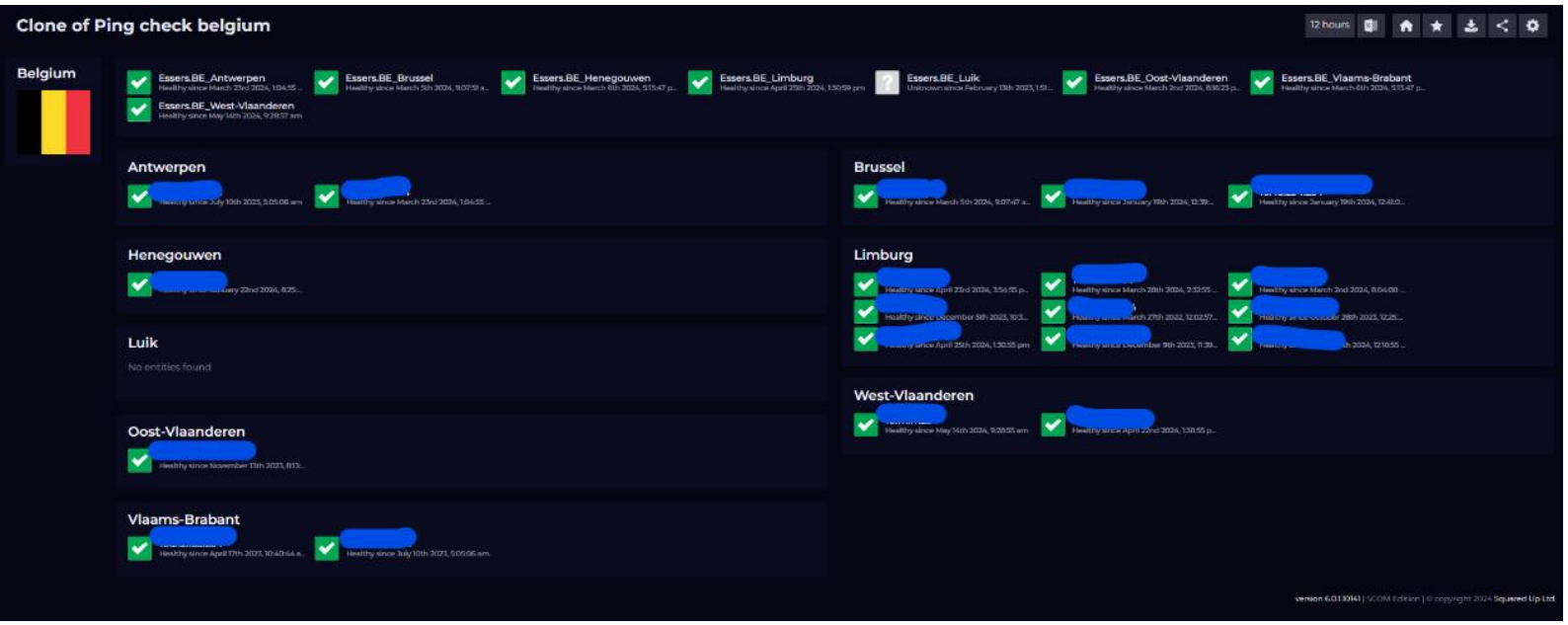


Dit dashboard is het dashboard voor alle sites in België. De IP's zijn verborgen maar onder elke site zie je de IP's met de health check status ervoor.

Ping check per country #1 & #2:

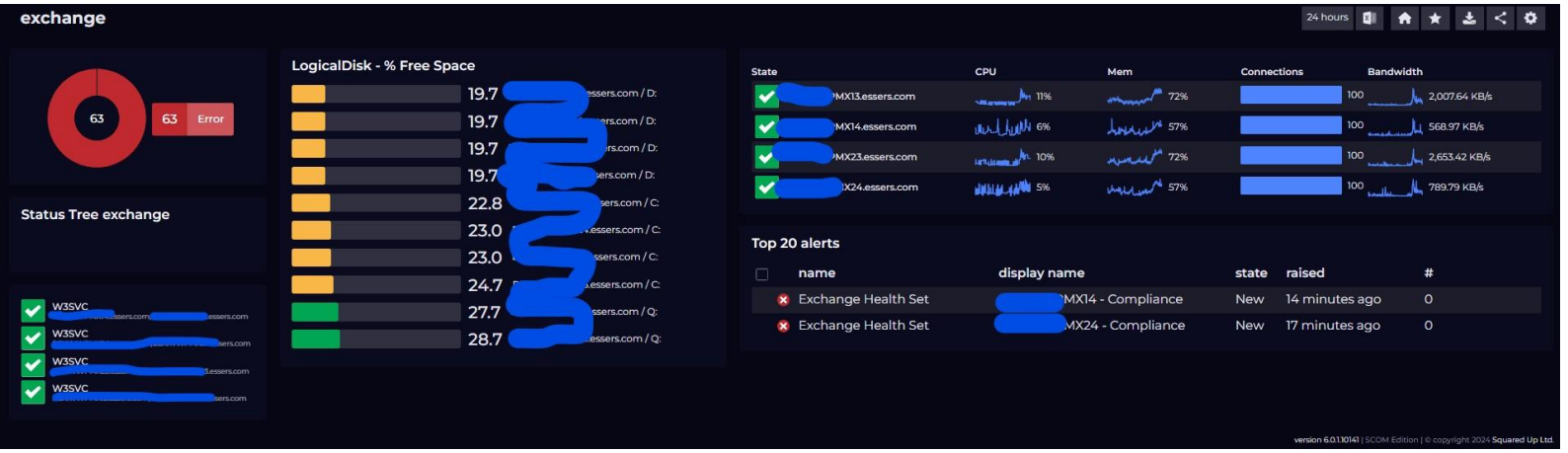
In deze dashboards zie je alleen de IP's waar er problemen zijn zodat het overzichtelijk blijft en we alles op zo weinig mogelijk dashboards kunnen krijgen.

Clone of Ping check Belgium:



Een andere versie van de ping check Belgium dashboard.

Exchange:

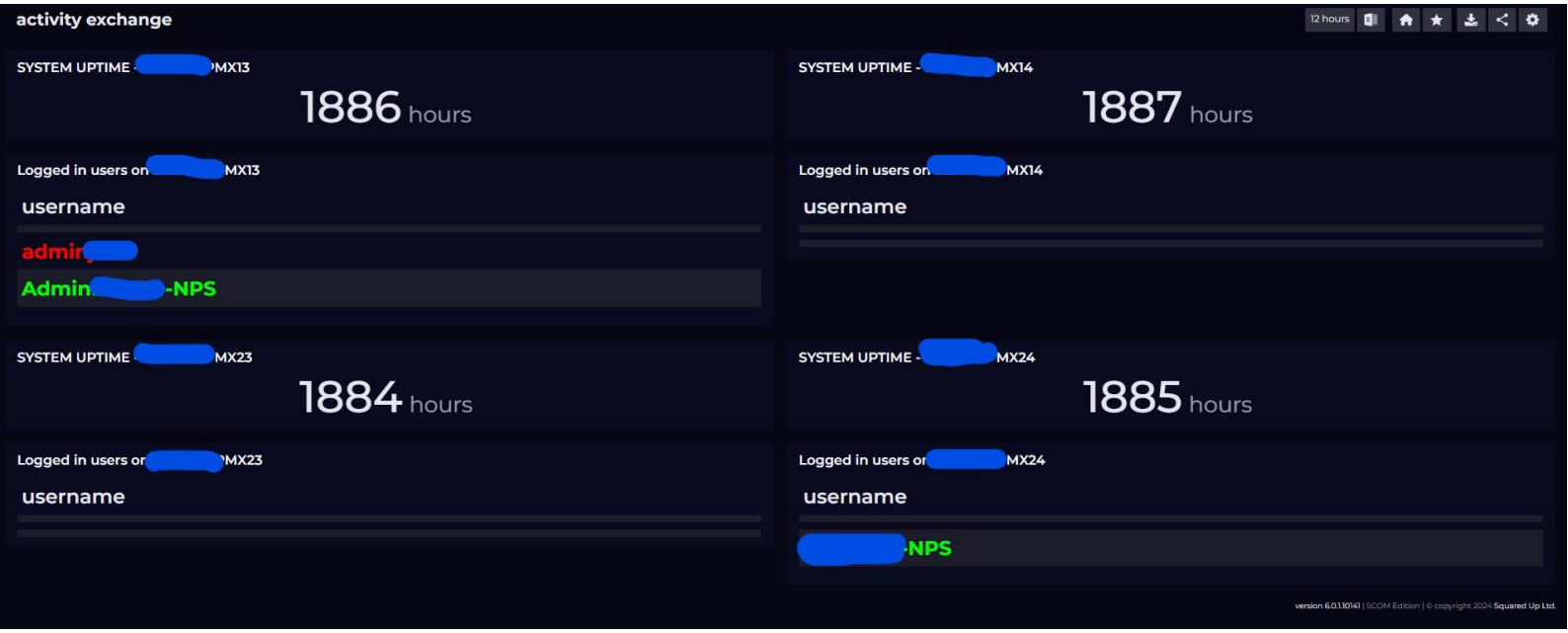


Dashboard voor de exchange servers met aan de linkerkant het aantal error messages, de status tree errors/warnings en de w3svc service status daaronder. Vervolgens hebben we de disk ruimtes in het midden en een matrix met verschillende waardes over de servers. Tenslotte daaronder een lijst met alerts in verband met exchange.

ALL-monitors for exchange:

Dit dashboard is voor alle monitors v/d exchange servers verdeelt per server.

Activity exchange:



In dit dashboard zie je de activiteit op de exchange servers doormiddel van de namen die je ziet. Als de naam groen is wil dit zeggen dat ze correct ingelogd hebben, dit doormiddel van in te loggen met NPS en als de naam rood is, hebben ze ingelogd zonder NPS. Dit dashboard is daar een mooi voorbeeld van.

PAM top 10 alerts:

Dit dashboard zijn de Top 10 PAM alerts.

AD top 10 alerts:

Dit dashboard zijn de top 10 AD alerts

Er zijn nog een paar andere dashboards maar die zijn ongeveer gelijk aan deze dashboards en meer om te testen.

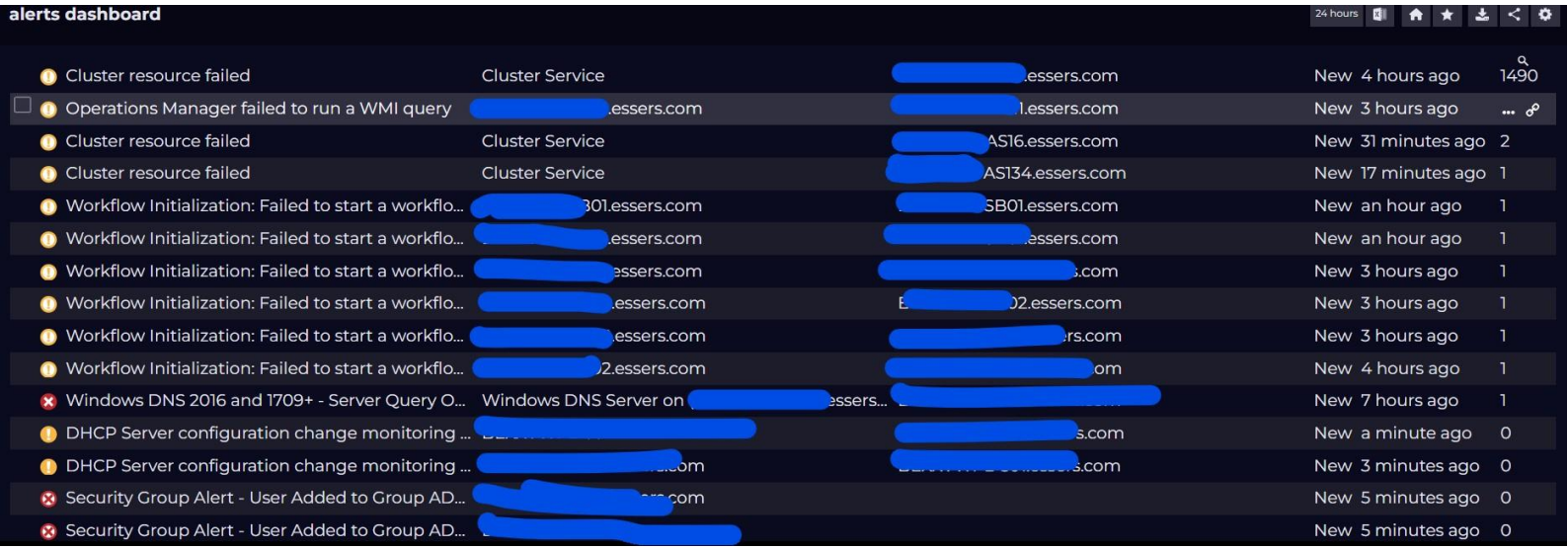
Datacenters:

Dit dashboard is voor de datacenters. Hier zien we monitors voor de vochtigheid, temperatuur en SNMP Ping maar ook UPS oplaadt status, ICMP-ping en UPS batterij status. Dit is niet volledig omdat ik hier niet op gefocust heb tijdens mijn stage. In de datacenter folder hebben we nog een ander dashboard maar zijn niet specifiek gerelateerd tot datacenters.

Datacenter monitors:

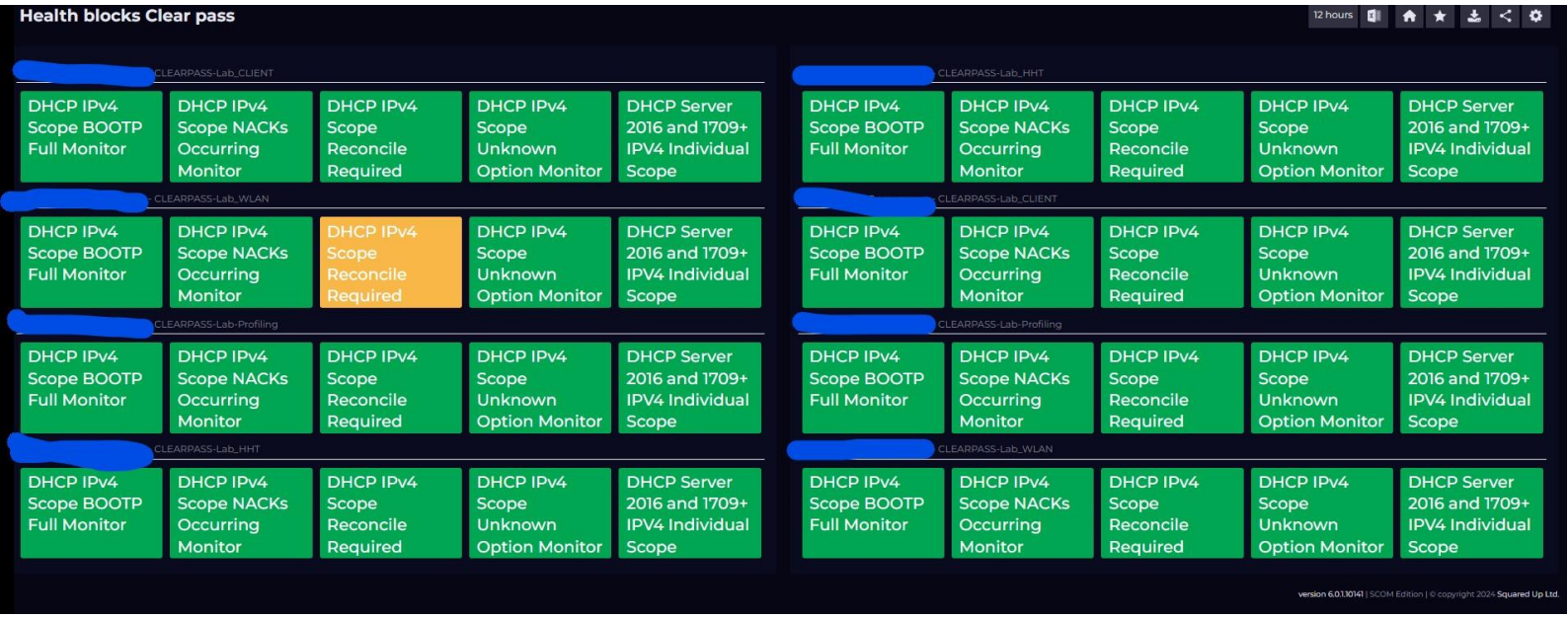
Andere versie van het bovenstaande dashboard.

Alerts dashboard voor alle alerts van alle servers in SCOM:



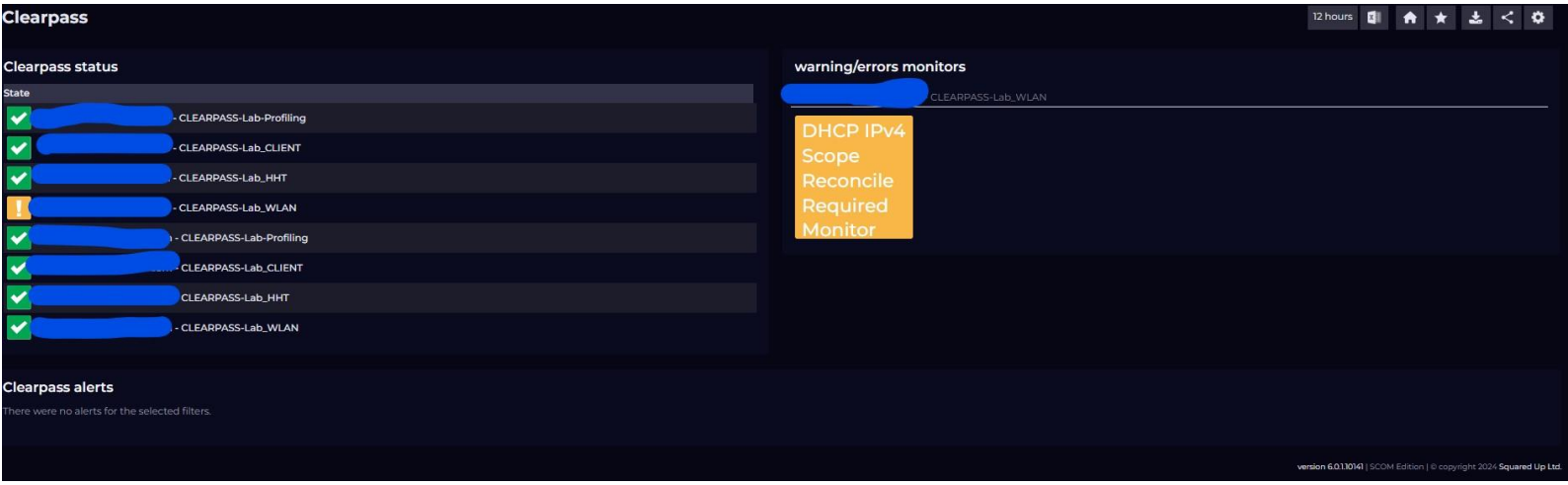
Top alerts over heel Squared up/SCOM.

Health blocks voor ClearPass:



Dit dashboard is voor de monitors van Clearpass.

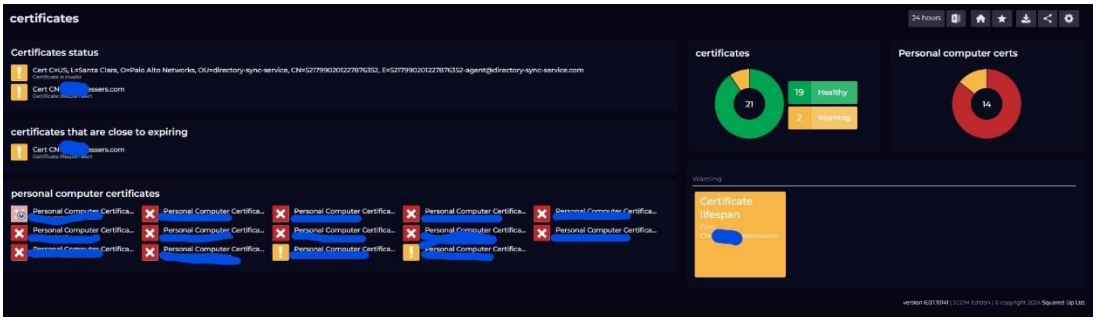
Extra Clearpass:



Dit dashboard is voor de status van de Clearpass instanties en error/warning monitors daarvan. Onderaan is ook nog een lijst met alerts moesten die er eventueel zijn.

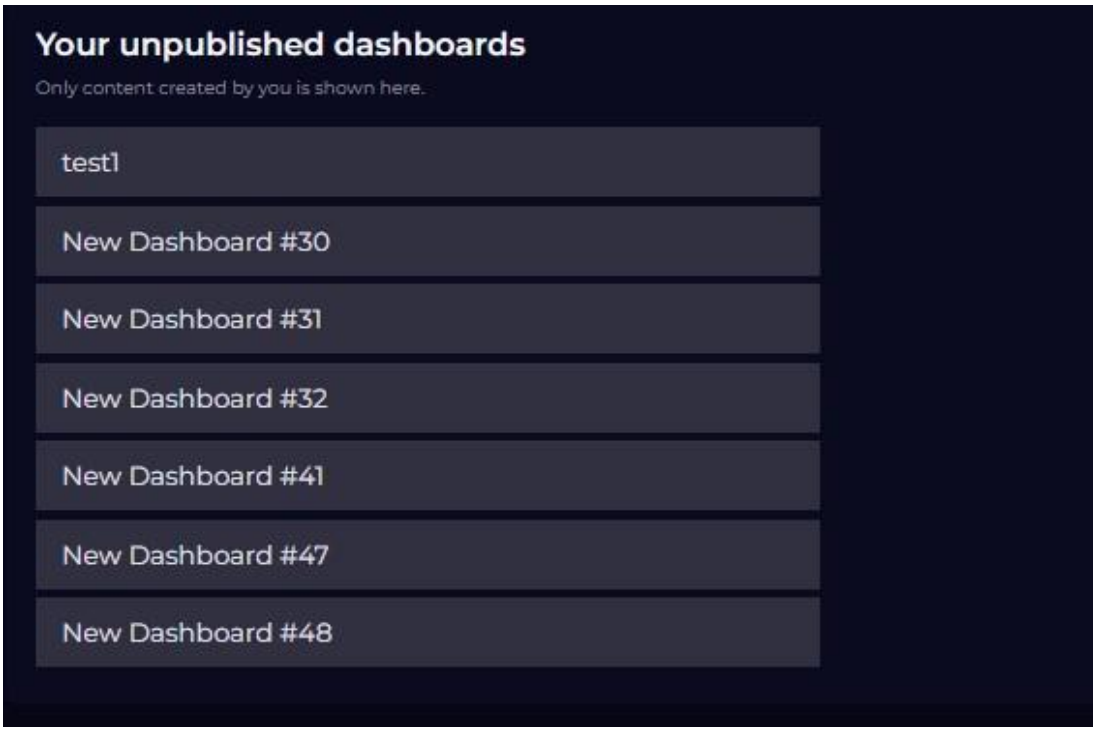
Andere variant van Health status Clearpass:

Certificaten:



Dit is een dashboard met de status van de certificaten waarvan warning/error status wordt weergegeven.

Niet gepubliceerde dashboards:



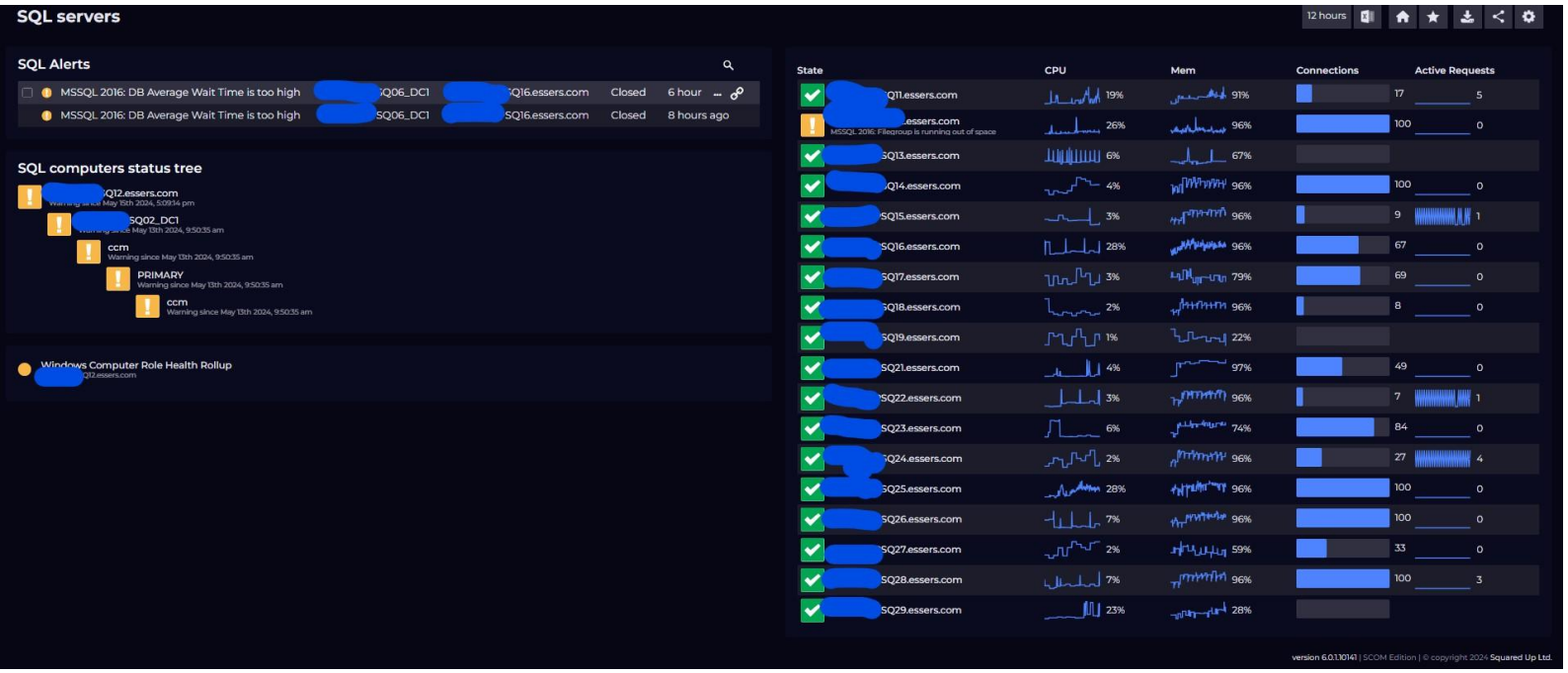
Dit zijn allemaal dashboards die ik gebruikt heb om dashboards te testen en ga deze dus niet overlopen.

SQL-server activity:

Dit is een dashboard voor de activiteit op de SQL-servers. Je ziet hierop de

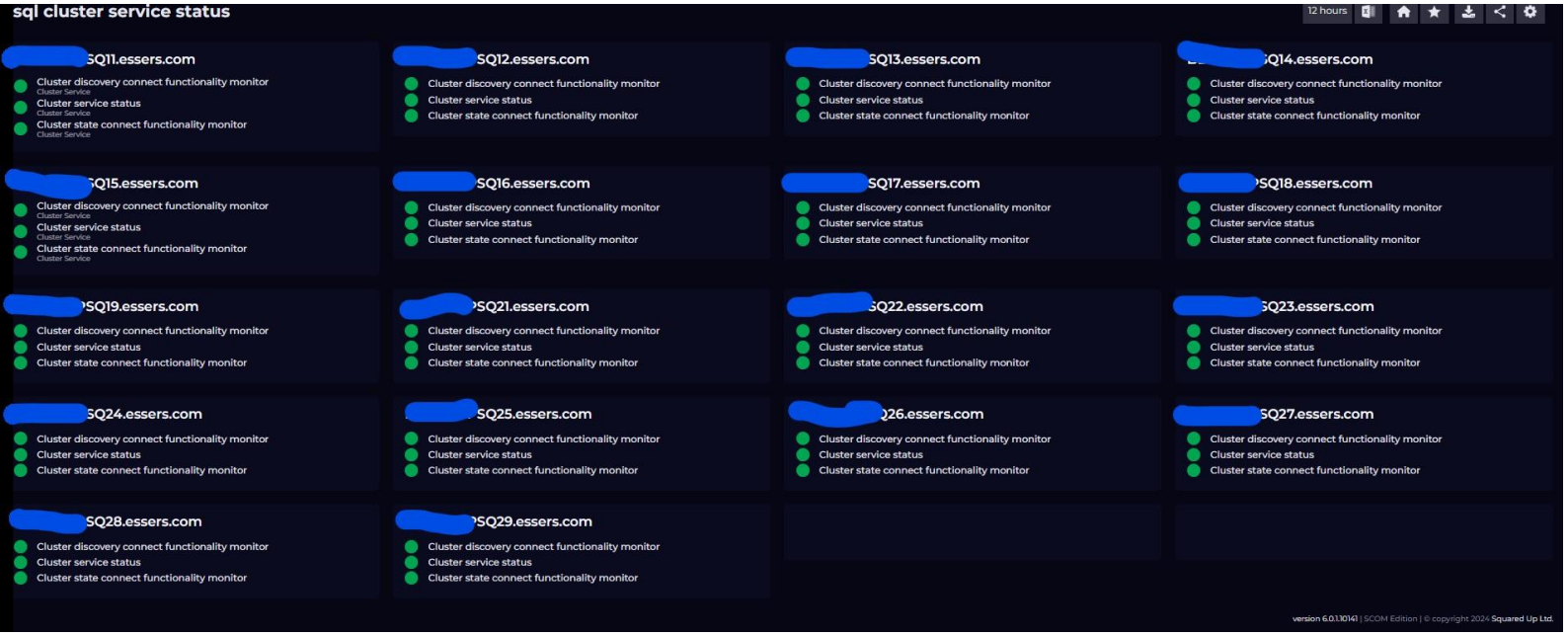
uptime van de server en de namen van de ingelogde user op elke server.

SQL-servers:



Hierop zie je de status v/d SQL-servers, de alerts, status tree en de monitors als warning of error.

SQL-cluster services status:



Dit is een dashboard voor de SQL-cluster services per SQL-server.

Diskspace dashboard #1:

Diskspace dashboard #2:

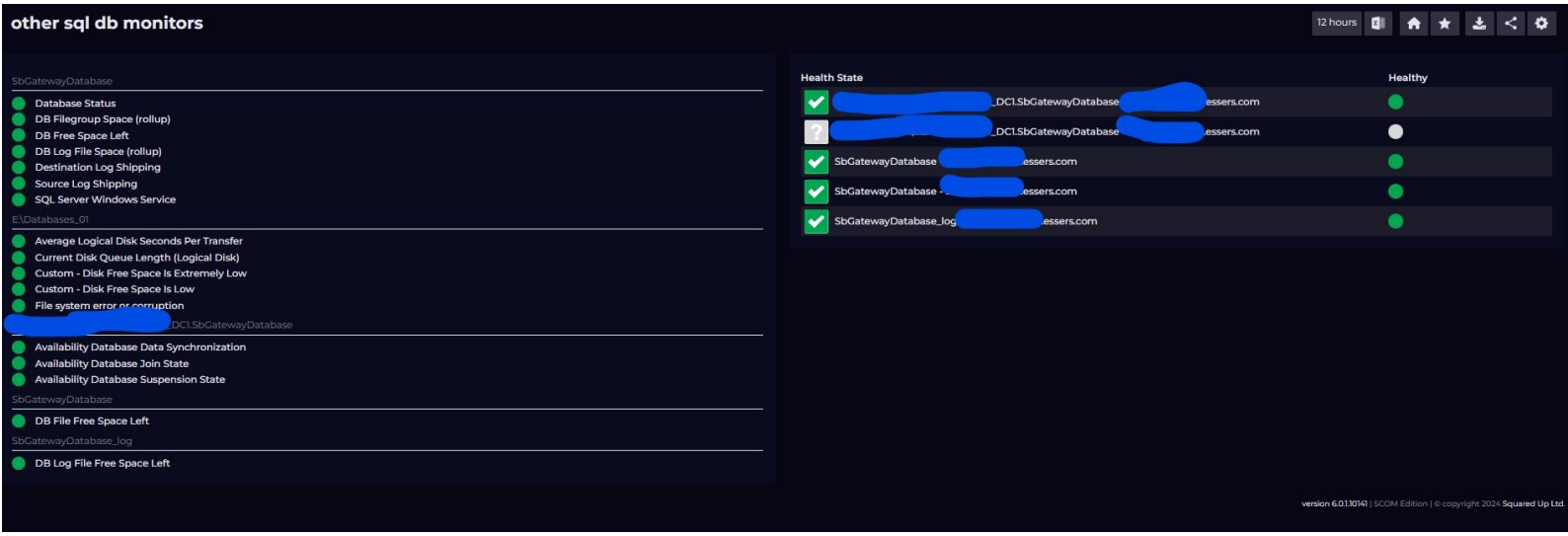
Diskspace dashboard #2:

Deze drie dashboards zijn bedoeld om de disk ruimte van elke server te laten zien en aan te tonen dat er disks zijn waar ze mee moeten opletten.

Database availability on SQL servers:

Dit dashboard is voor de availability van de SQL-databases aan de hand van een matrix met verschillende waardes die meer vertellen over de toegankelijkheid van de server.

Andere monitors voor SQL DB's:

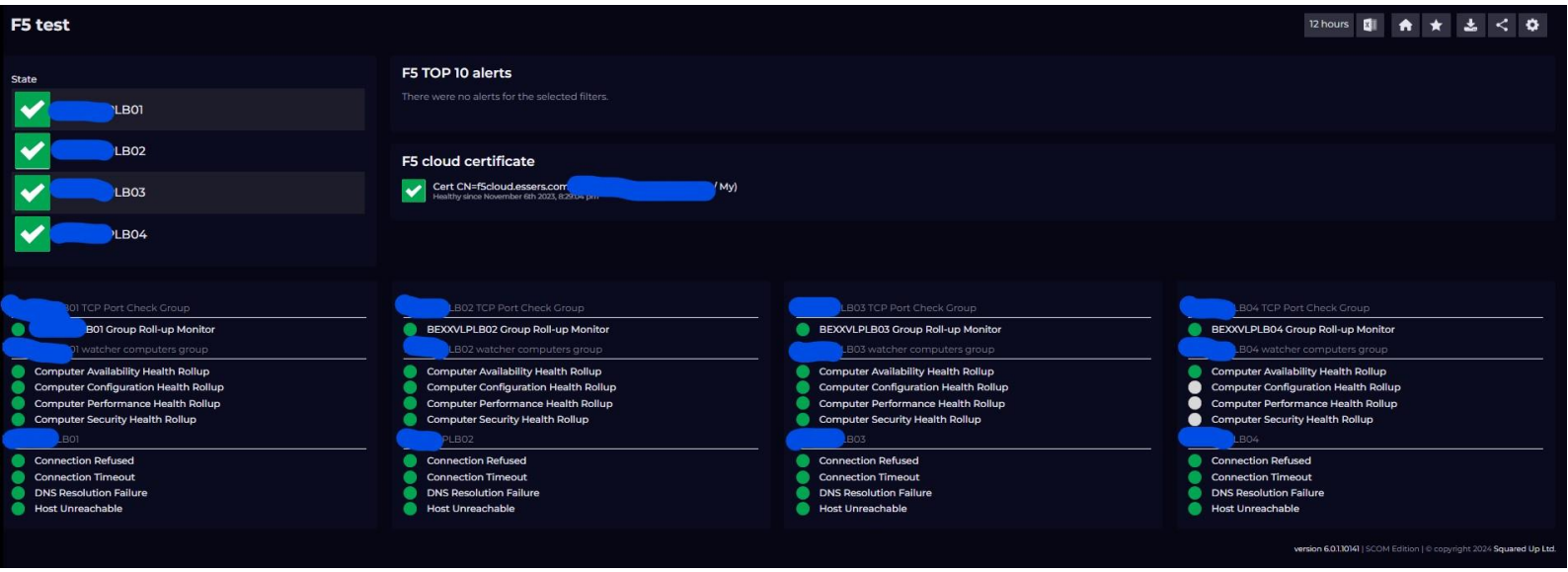


Dit dashboard zijn nog een paar andere monitors met betrekking tot SQL-databases.

Uptime dashboard van een paar servers:

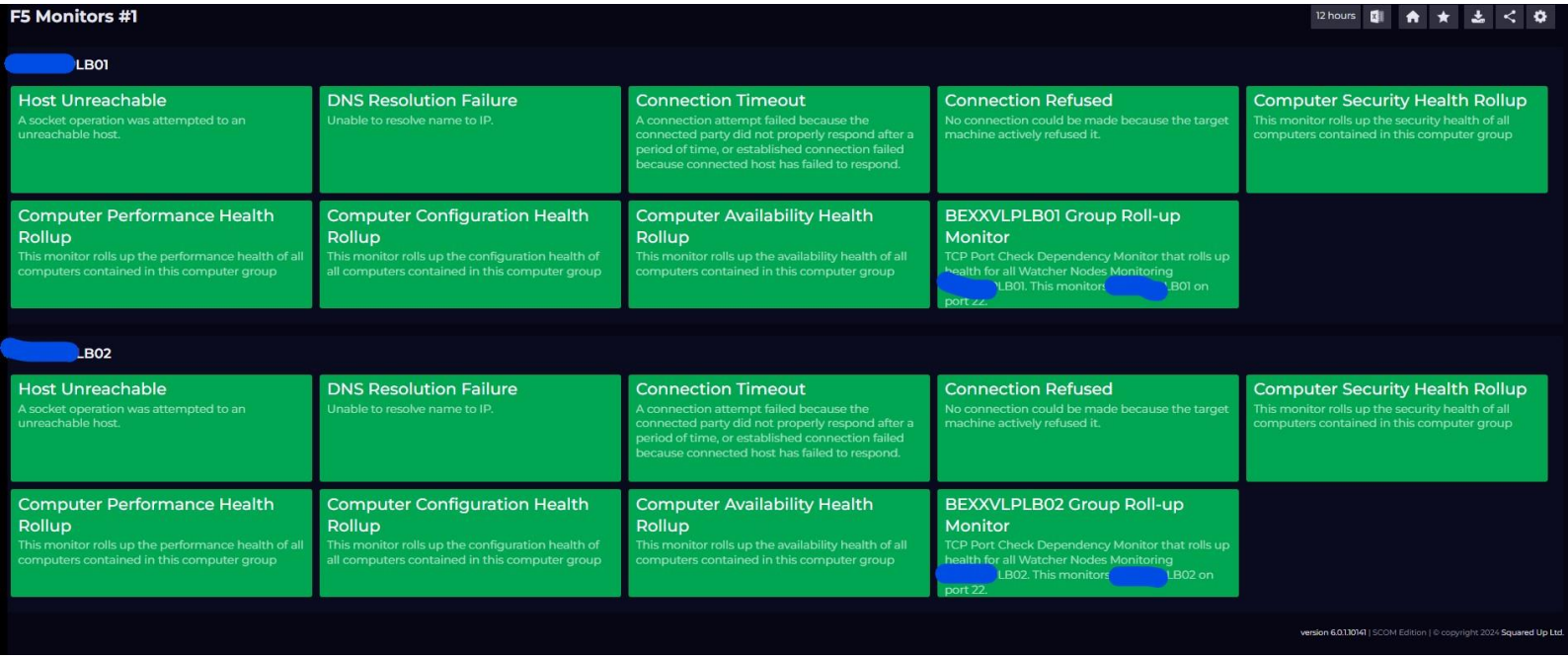
Dit dashboard was bedoeld om de uptime te tonen van alle kritische servers, dit heb ik niet als mijn prioriteit genomen aangezien er verschillende servers waren dit niet toegankelijk zijn via SCOM → alleen via een ping of monitor.

F5 dashboard:



Dit dashboard is een algemeen dashboard voor F5 met de status checks, alerts, certificaten en een paar monitors.

F5 Monitors:



F5 monitors:

Deze dashboards zijn enkel en alleen voor de monitors zodat je er een specifieker overzicht van krijgt.

Cortex service dashboard:

Dit dashboard is voor te checken of er een probleem is met de Cortex XDR service op elke server in System Center Managed Windows Computer of SCOM. Hier worden alleen warning en/of alerts getoond omdat het anders niet overzichtelijk blijft. Onderaan heb je ook nog Cortex XDR alerts als die er zijn.

Managementserver status dashboard:

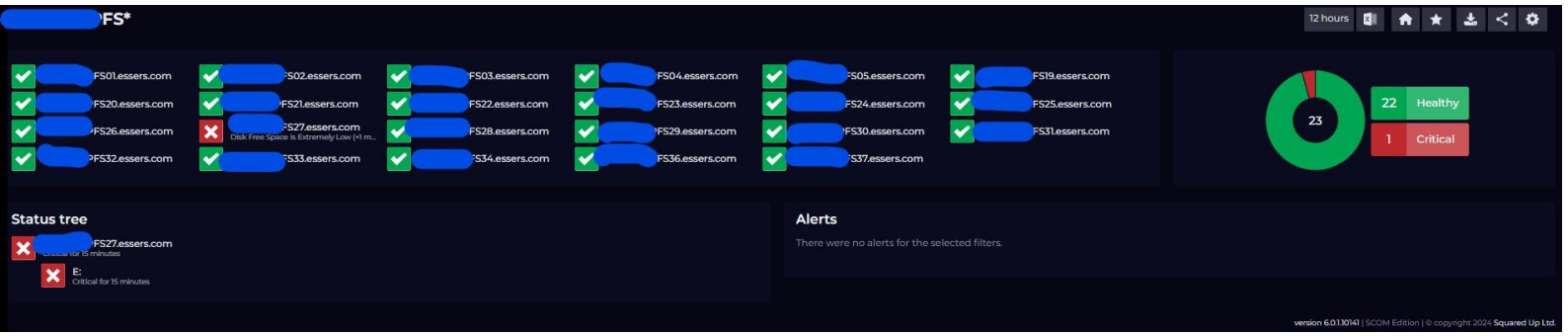
Dit is een algemeen dashboard van de managementservers.

Activity on management server's dashboard:

Dit is het activity dashboard van de managementservers.

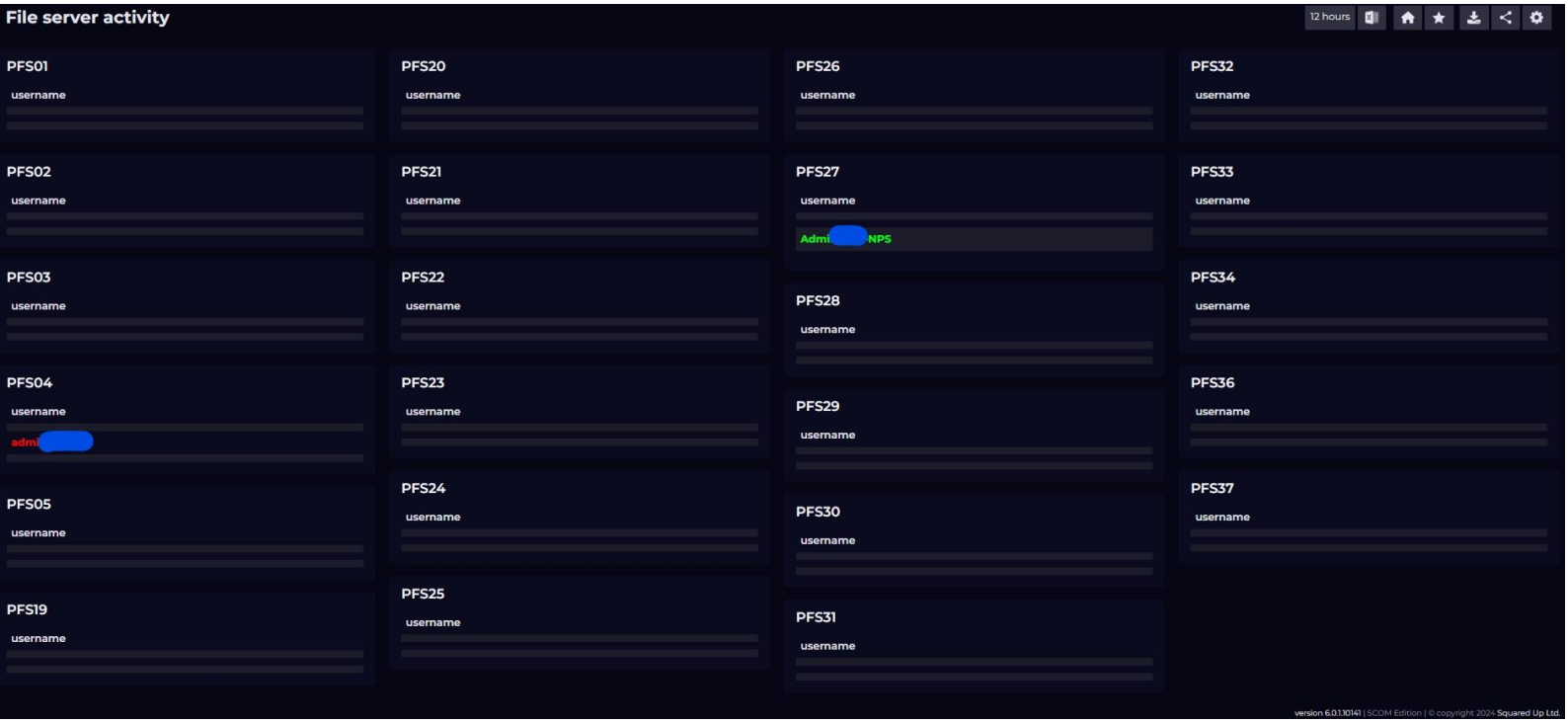
Hier zie je ook nog de manier waarop ik dit gerealiseerd heb. Dit is aan de hand van een custom template die ik gemaakt heb aan de hand van de Squared up GitHub. Daar heb ik dus informatie gehaald om uiteindelijk op dit te komen.

Fileservers status dashboard:



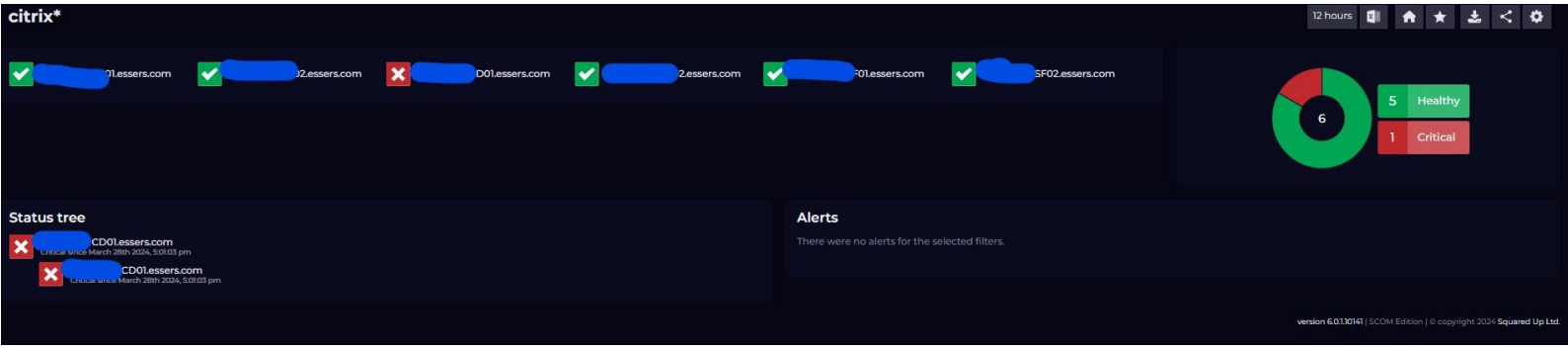
Dit is het algemene dashboard van de file servers.

Activity on fileservers dashboard:



Dit is het activity dashboard van de file servers.

Citrix status dashboard:

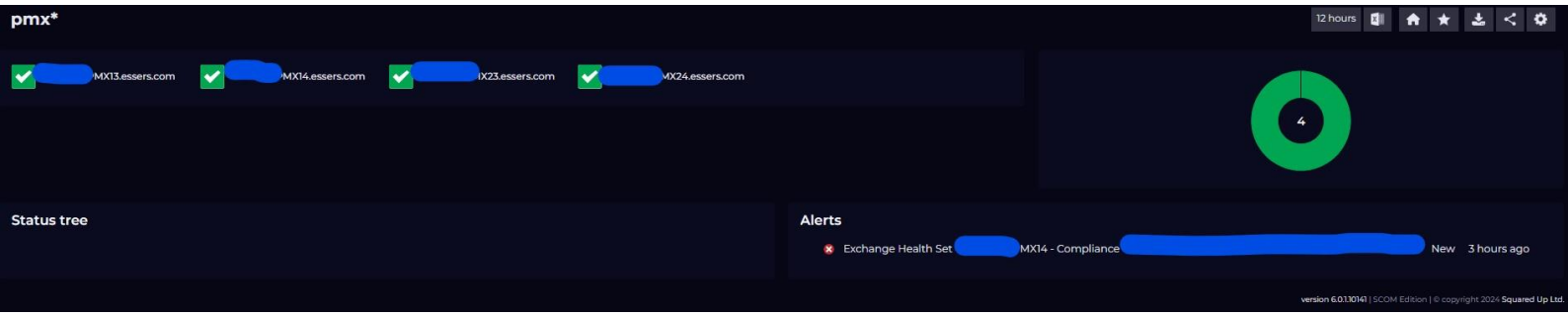


Dit is het algemene dashboard van de Citrix servers.

Activity on Citrix servers:

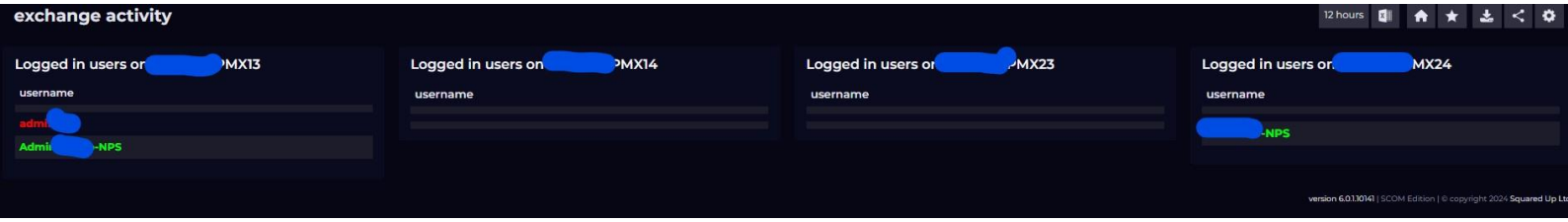
Dit is het activity dashboard van de Citrix servers.

Exchange status dashboard:



Dit is het algemene dashboard van de exchange servers.

Activity on exchange server:



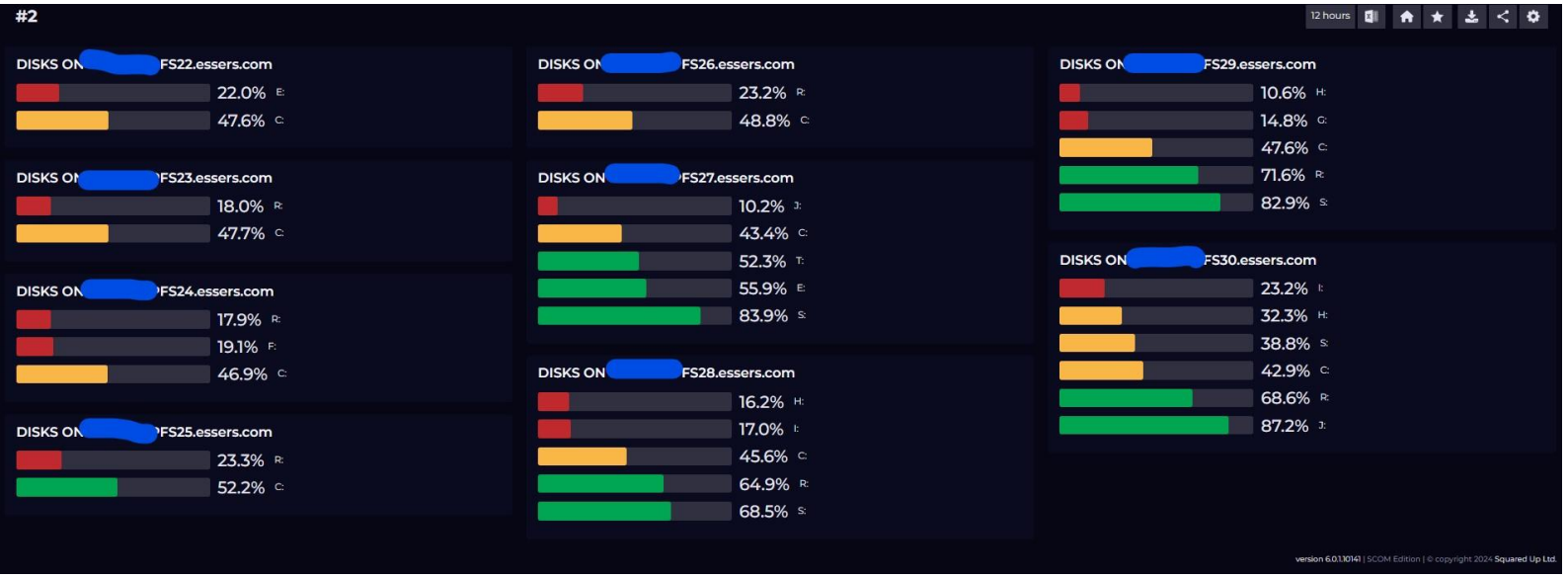
Dit is het activity dashboard van de exchange servers.

Fileserver:

Voor de file servers heb ik 2 varianten voor disk space dasboards eentje voor percentages en eentje in gigabytes.

Diskspace on fileservers in % dashboard #1:

Diskspace on fileservers in % dashboard #2:



Diskspace on fileservers in % dashboard #3:

Dit zijn de dashboards voor de visualisatie van de disk ruimtes in percentage.

Diskspace on fileservers in GB dashboard #1:

Diskspace on fileservers in GB dashboard #2:

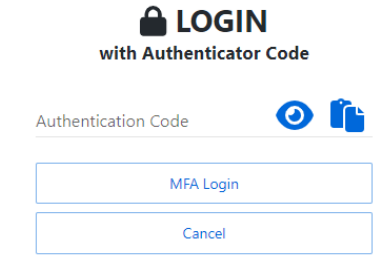
Diskspace on fileservers in GB dashboard #2:

Dit zijn de dashboards voor de visualisatie van de disk spaces in GB. Hiermee stuitte ik op enkele problemen zoals de balk komt niet overeen met de effectieve waarde maar de kleur wel. Tweede probleem was dat ik in het eerste dashboard schijf E: niet kreeg lijk ik het wilde.

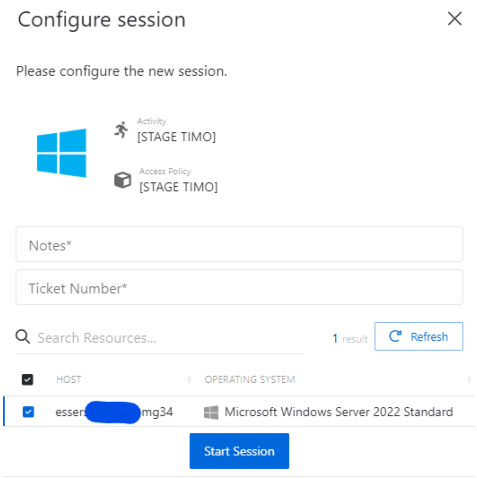
5 NETWRIX

Dit is een heel belangrijk deel binnen Essers en ook de manier waarop ik kon aanloggen om de managementserver om connectie te kunnen maken met de Nagios server.

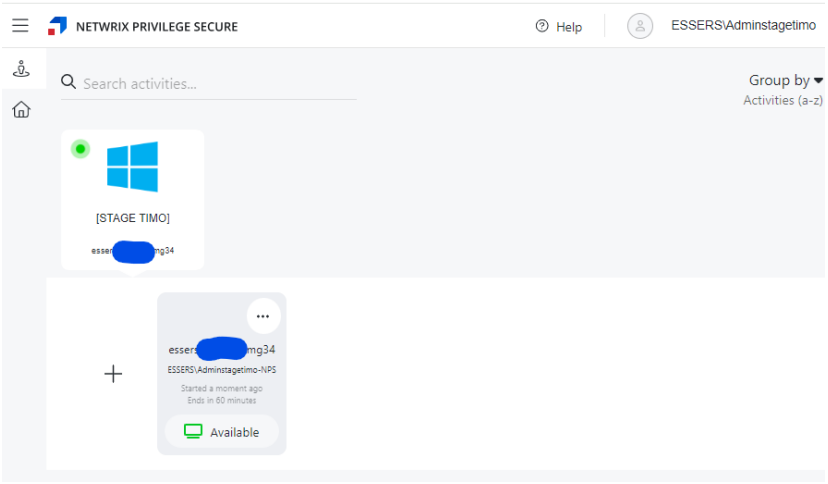
Om binnen te komen moet je natuurlijk eerst inloggen maar daarna krijg je een MFA.



Dan kon ik beginnen met het aanmaken van een sessie die we vooraf voor mij hebben ingesteld.



Als we de sessie een naam en ticket nummer hebben gegeven kunnen we het starten en krijg je het volgende beeld. Als we op de “Available” knop drukken krijgen we een RDP om te connecteren naar de managementserver via Netrwix met een tijdelijke user. Die tijdelijke gebruiker kreeg meestal gewoon de naam met er NPS achter.



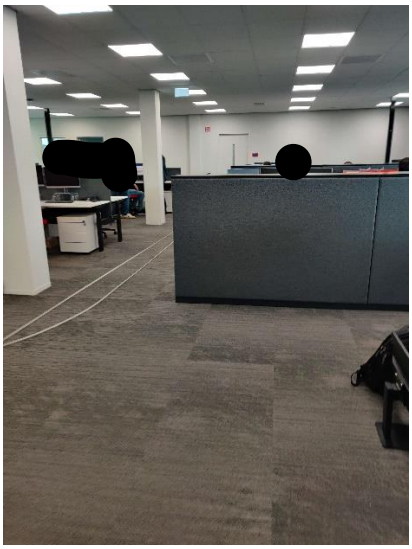
6 SLOT

Ik vond het een interessante stage met veel nieuwe kennis die ik heb opgedaan van Nagios, SCOM en Squared up maar ook van hoe het gaat in de IT van een groot bedrijf als Essers.

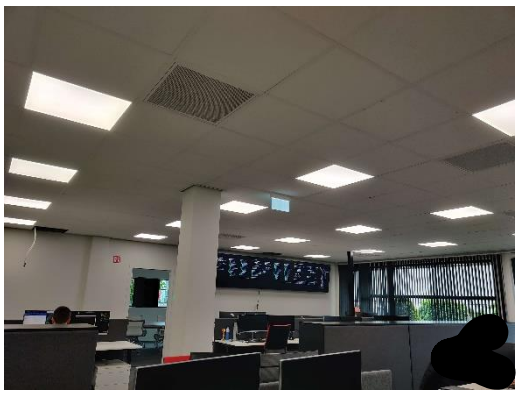
Ik heb zo veel mogelijk van de gevraagde doelstellingen behaald met af en toe een extraatje.

In de tussentijd heb hier veel aangename mensen leren kennen en veel kennis opgedaan van de werking hier. Ik ben heel blij dat ik de kans heb gekregen om stage te doen bij Essers.

Before:



After:



Het begin van een ruimte met een heleboel monitor schermen om zo het overzicht over hun infrastructuur te vergroten en ik ben heel blij dat ik daar de basis voor heb mogen leggen.