Aansluitvoorwaarden

Eindgebruiker

Om aan te sluiten op en gebruik te maken van Splunk, raden we aan om een aantal Splunk cursussen te volgen. Om gebruik te kunnen maken van scheduling en alerting in Splunk is extra autorisatie (JOB-rechten) benodigd. Hiervoor is het verplicht om de Splunk cursussen te hebben afgerond. Het betreft de volgende cursussen:

- What is Splunk?
- Intro to Splunk
- Using Fields
- Scheduling Reports and Alerts
- Visualizations
- Search Under the Hood
- Introduction to Knowledge Objects
- Introduction to Dashboards

Deze trainingen zijn te vinden middels de Splunk website.

Gebruiker dient kennis te hebben genomen van het feit dat er niet zelf aan de Splunk-configuratie mag worden gesleuteld. Een wijziging in de configuratie moet **altijd** worden aangevraagd via de reguliere procedure.

Data

Naast voorwaarden voor de eindgebruiker gelden ook aansluitvoorwaarden op de aan te leveren gegevens, namelijk:

- Data dient in ASCII formaat (oftewel, platte leesbare tekst) aangeleverd te worden.
- Data dient te zijn voorzien van een timestamp (het liefst inclusief timezone notatie).
- Data dient geen persoonlijke, of tot een persoon herleidbare, gegevens te bevatten (AVG).
- Data dient te voldoen aan de Standaard Technische Beveiligingslogging IV wanneer het om gegevens ten behoeve van beveiligingslogging gaat.
- Data dient een dataeigenaar te hebben. De dataeigenaar is verantwoordelijk voor de data die naar Splunk gestuurd wordt en fungeert als het aanspreekpunt voor team Splunk.
- De datahoeveelheid dient de aangevraagde datalimiet niet te overschrijden.

Externe databronnen

Voor het aansluiten van databronnen vanuit externe locaties of externe netwerken, denk aan Azure cloud omgevingen, gelden additionele voorwaarden. Binnen het Belastingdienst domein zorgt de Operations Intelligence dienst voor componenten binnen koppelvlakken. Om dit koppelvlak te bereiken dient de klant van de externe databron te zorgen voor connectiviteit naar het interne Belastingdienst domein waar een IaaS dienst wordt geleverd. Dit dient te gebeuren in afstemming met het Netwerken team om een zodanig veilige, stabiele en conform geldende richtlijnen connectie op te zetten tussen beide omgevingen. Wanneer connectiviteit is gerealiseerd draagt de Operations Intelligence dienst zorg voor een component dat als koppelvlak dient richting het centrale Splunk platform. De benodigde Splunk Universal Forwarders (agents) binnen het externe domein vallen onder de verantwoordelijkheid van de klant waarbij de klant de Universal Forwarder volledig beheert.

- Er worden alleen Splunk functionaliteiten aangeboden.
- Netwerkconnectiviteit tussen de Splunk oplossing en de externe partij wordt niet door het Splunk team verzorgd.
- Deze netwerkconnectiviteit dient alleen gebruikt te worden voor het verzenden van data richting Splunk.
- Data eigenaar van de verzonden data is altijd een interne afnemer, nooit een externe partij.
- Data eigenaar is in deze zin verantwoordelijk voor de verzonden data en de configuratie van de externe databronnen.
- Operations Intelligence is nooit verantwoordelijk voor de configuratie van de externe databronnen, behalve configuratie die middels een Deployment Server in beheer is bij Operations Intelligence.

Gevoelige data in OTA

Het is ons opgevallen dat er regelmatig gevoelige data in de OTA omgeving terecht komt. In tegenstelling tot de productieomgeving, is de data in de OTA niet afgeschermd per index d.m.v. een IMS permissie, maar toegankelijk voor iedereen met één algemene IMS rol. Mocht het werkelijk noodzakelijk zijn om met gevoelige data te werken in de OTA, bieden we de mogelijkheid OTA data naar de Splunk Productieomgeving te sturen. Mocht dit voor jullie team/aanvraag relevant zijn, neem dan contact op met de Operations Intelligence Postbus.

Datalimiet

Om onze dienst te kunnen blijven leveren en service te kunnen garanderen, is een nauwkeurige inschatting van de hoeveelheid te loggen data noodzakelijk. Overschrijding van de aangevraagde datalimiet leidt tot het overschrijden van de licentie van het platform, met uitval van functionaliteit tot gevolg. De dataeigenaar en aanvrager gaan akkoord met de volgende aansluitvoorwaarde met betrekking tot het overschrijden van de aangevraagde datalimiet:

> ***Bij overschrijding van de aangevraagde datalimiet met een gemiddelde van 20% per dag, gedurende een periode van langer dan 10 werkdagen, zal - bij het uitblijven van communicatie of goedkeuring vooraf - worden overgegaan tot het afsluiten van de aanvraag en/of index.***

Het monitoren en het handelen naar deze voorwaarden gebeurt vanuit Functioneel Beheer Operations Intelligence (FBOI) en verloopt aan de hand van de volgende stappen:

1. Wanneer er wordt geconstateerd dat een index langer dan 3 werkdagen gemiddeld 20% boven de aangevraagde datalimiet zit, of wanneer er een piek is van meer dan 100% bovenop de aangevraagde datalimiet, dan stuurt FBOI een email ter attentie richting de dataeigenaar van de index. Deze email is bedoeld om met de gebruiker in contact te komen. Op basis van de reactie op de email gaat FBOI in overleg met de afnemer richting een passende oplossing.
2. Wanneer er na 5 werkdagen na het versturen van de email uit stap 1 geen passende oplossing is overeengekomen, of er geen reactie is geweest en de situatie aanhoudt, stuurt FBOI een tweede email richting de dataeigenaar van de index. Daarnaast zal er getracht worden om op een andere manier in contact te komen met desbetreffend persoon of team. In deze tweede poging tot contact worden de mogelijke consequenties gecommuniceerd voor in het geval dat contact en/of een oplossing uitblijft.
3. Wanneer er na 5 werkdagen na het zoeken van contact uit stap 2 nog steeds geen passende oplossing is overeengekomen, of er nog steeds geen reactie is geweest en de situatie aanhoudt, gaat team Splunk over tot uitvoer van de eerder in stap 2 genoemde consequenties. Dit houdt in: het afsluiten van de betreffende aanvraag en/of index. Hierover ontvangt de dataeigenaar een email.