# Lees meer over Log Analytics-ELK Stack op ISE

## Inhoud



## Inleiding

Dit document beschrijft de elk Stack-componenten die zijn ingebouwd in Cisco Identity Services Engine (ISE) 3.3 via System 360 Log Analytics.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Identity Service Engine
- ELK Stack

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ISE-lijnkaart 3.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

## Achtergrondinformatie

System 360 omvat bewaking en loganalyses.

Met de **bewakingsfunctie** kunt u een brede reeks toepassings- en systeemstatistieken en de belangrijkste

prestatie-indicatoren (KPI) van alle knooppunten in een implementatie vanuit een gecentraliseerde console bewaken. KPIâ€™s zijn nuttig om inzicht te krijgen in de algehele gezondheid van de knoopomgeving. Statistieken bieden een vereenvoudigde weergave van de systeemconfiguraties en gebruiksspecifieke gegevens.

**Log Analytics** biedt een flexibel analysesysteem voor diepgaande analyse van endpointverificatie, autorisatie en accounting (AAA) en profilering van syslog-gegevens. U kunt ook de gezondheidssamenvatting en de processtatus van Cisco ISE analyseren. U kunt rapporten genereren die vergelijkbaar zijn met het Cisco ISE-tellers en het rapport met gezondheidsoverzichten.

# ELK Stack

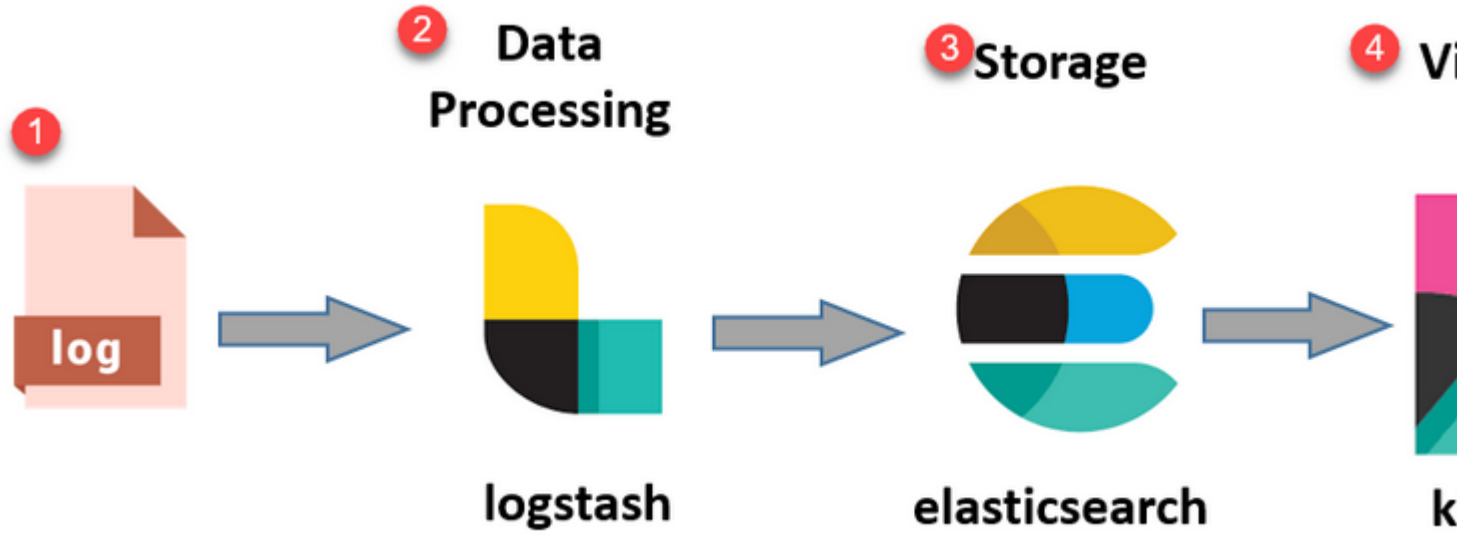
De ELK Stack is een populaire opensourcesoftware die wordt gebruikt voor het verzamelen, verwerken en visualiseren van grote hoeveelheden gegevens. Het staat voor Elasticsearch, Logstash en Kibana.

- **Elasticsearch**: Elasticsearch is een gedistribueerde zoek- en analytics-engine. Het is ontworpen om grote hoeveelheden gegevens snel en in bijna real-time op te slaan, te zoeken en te analyseren. Het maakt gebruik van een op JSON gebaseerde query taal en is zeer schaalbaar.

- **Logstash**: Logstash is een dataverwerkingspijplijn die gegevens uit meerdere bronnen opneemt, verwerkt en transformeert. Het kan gegevens ontleden en verrijken, waardoor het meer gestructureerd en geschikt voor analyse. Logstash ondersteunt een breed scala aan invoerbronnen en uitvoerbestemmingen.

- **Kibana**: Kibana is een datavisualisatieplatform dat werkt met Elasticsearch. Het stelt gebruikers in staat om interactieve dashboards, grafieken, grafieken en visualisaties te maken om gegevens te verkennen en te begrijpen die zijn opgeslagen in Elasticsearch. De interface van Kibana maakt het gemakkelijk om gegevens te vragen en te visualiseren.

In combinatie vormen deze componenten een krachtige stack voor het beheer en de analyse van verschillende soorten gegevens, van logbestanden tot metriek en meer, terwijl ze visualisatiemogelijkheden bieden om de informatie te begrijpen.

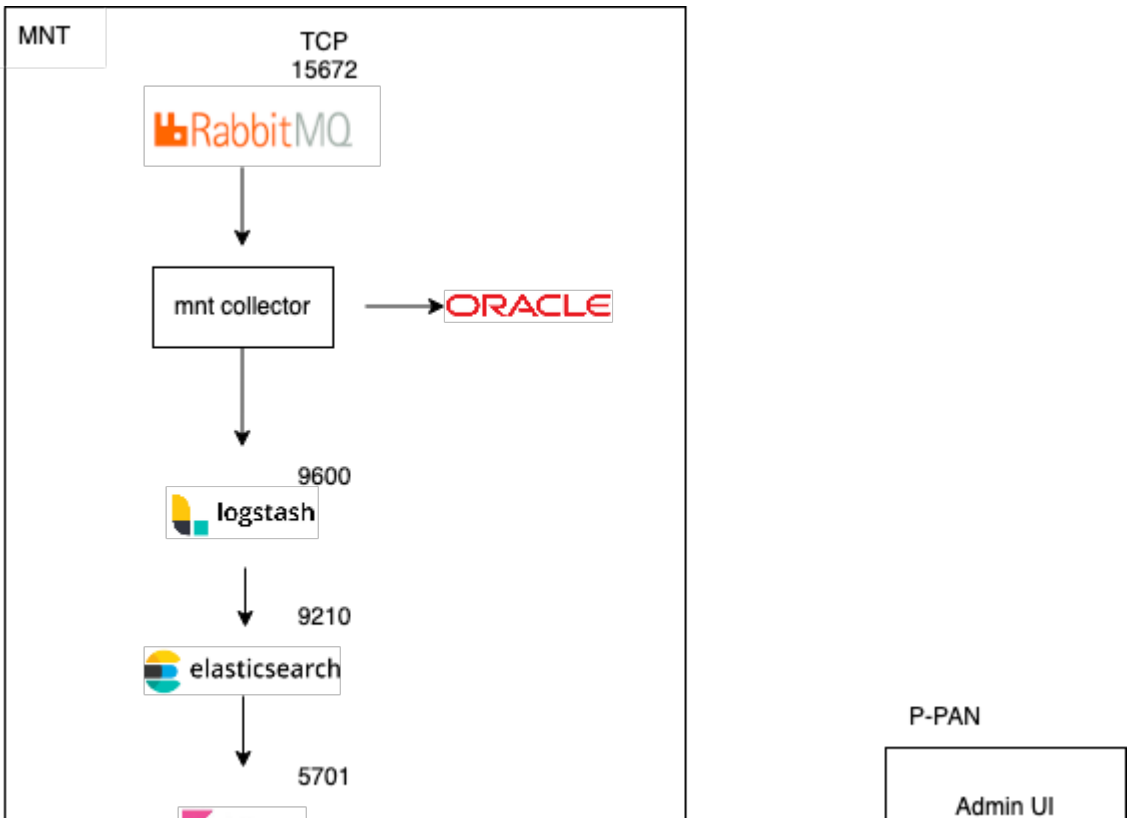



*ELK Stack flow*

# ELK Stack als log analyse

- Een afzonderlijk geval van ElasticSearch+LogStash+Kibana stack wordt uitgevoerd op alleen MnT knooppunten.
  - Dit heeft geen correlatie met de Elasticsearch of Context-Visibility.
  - Operatie ELK 7,17

- Primaire en secundaire MNT's hebben hun eigen afzonderlijke voorbeelden van ELK.
  - Kibana is alleen ingeschakeld op secundaire MNT indien deze beschikbaar is, waarbij alleen gegevens van dit knooppunt worden weergegeven.
- Log Analytics is standaard uitgeschakeld.
- Verbruikt Oracle-bronnen.
- Slaat maximaal 7 dagen gegevens op.
- De totale grootte van de door Log Analytics verbruikte gegevens is beperkt tot 10GB.
  - Zodra een van de limieten is bereikt, worden de gegevens door ElasticSearch verwijderd.



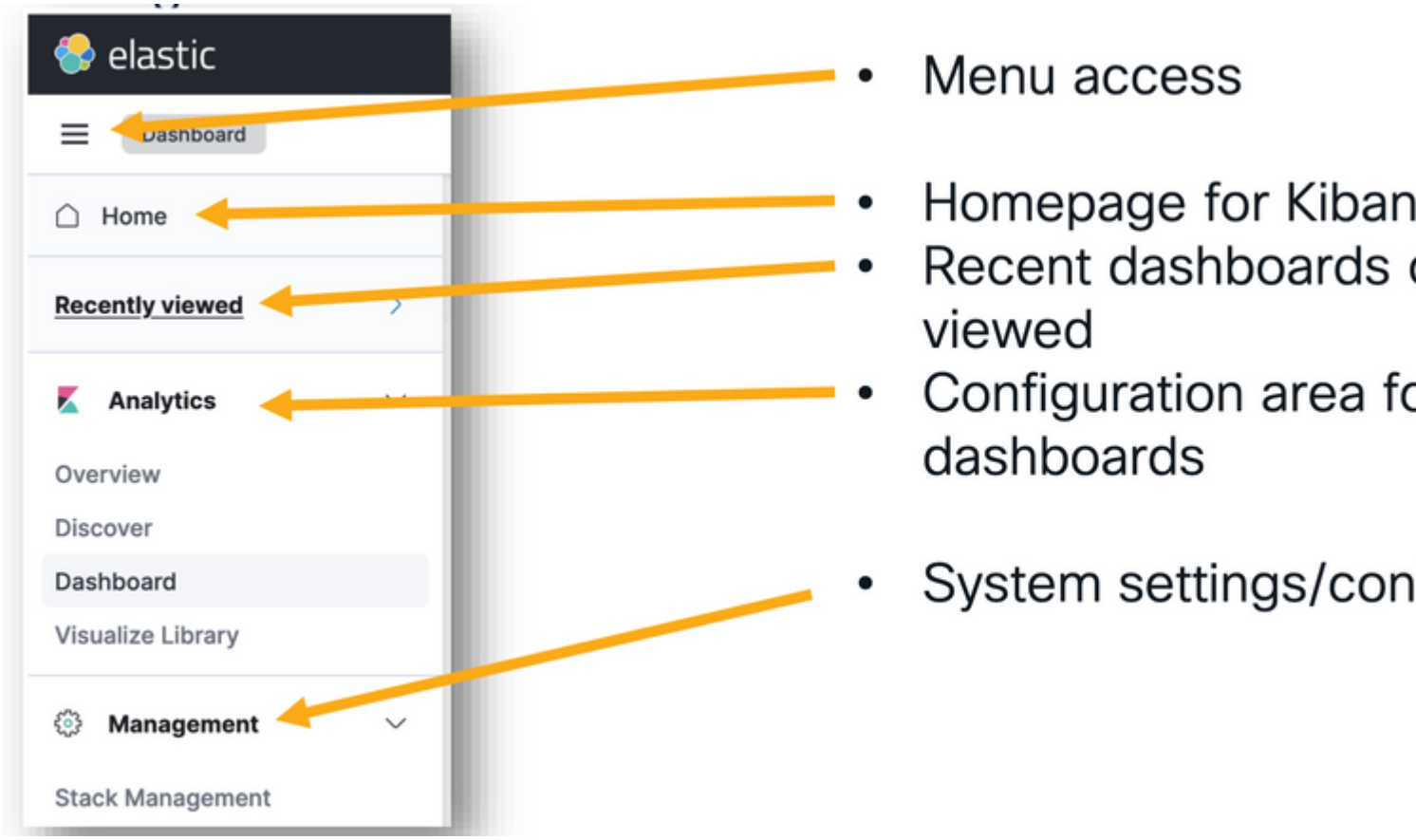
**ISE Logstash Service running 614339**

**ISE Kibana Service running 616064**

ISE Native IPSec Service running 75883
MFC Profiler running 651910

## Navigation menu

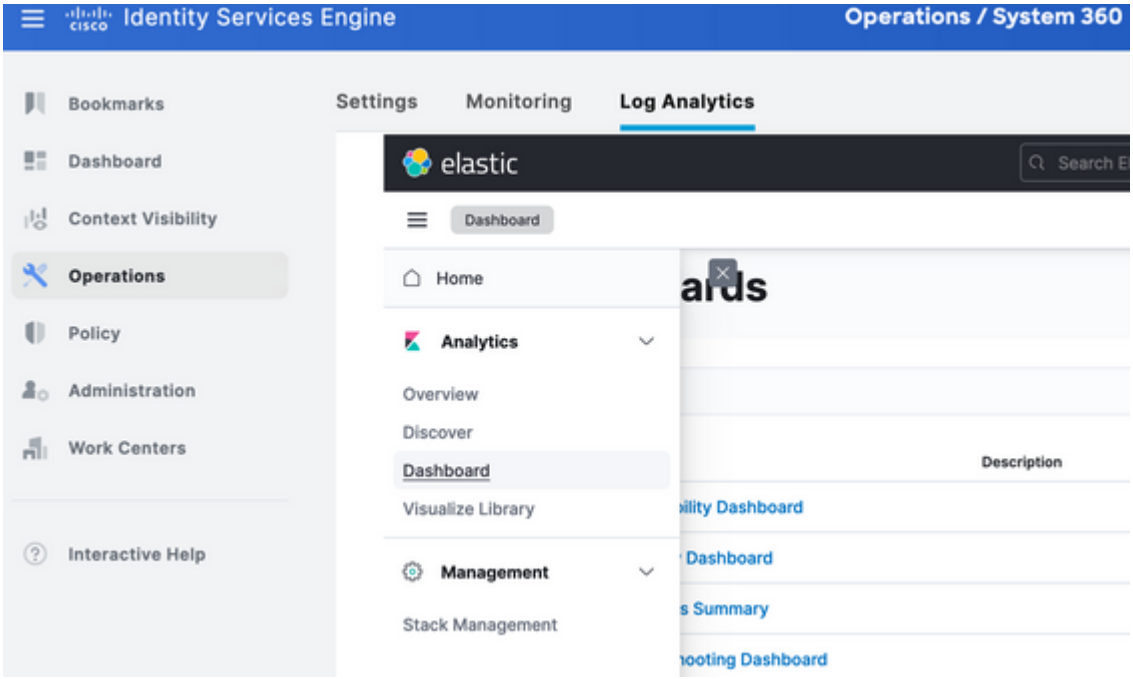
Zodra ELK services beginnen, hebt u nu toegang tot het Elastic navigatie menu.




*Navigation menu*

# Ingebouwde Dashboards

- ISE heeft standaard ingebouwde dashboards met gegevens van Radius, TACACâ€™s, systeemprestaties en ISE-waarneembaarheid.
- Deze dashboards zijn toegankelijk via navigatie naar Operations>Log Analytics.
    - Klik na het openen van de elastische gebruikersinterface op sandwichmenu >Analytics>Dashboards.



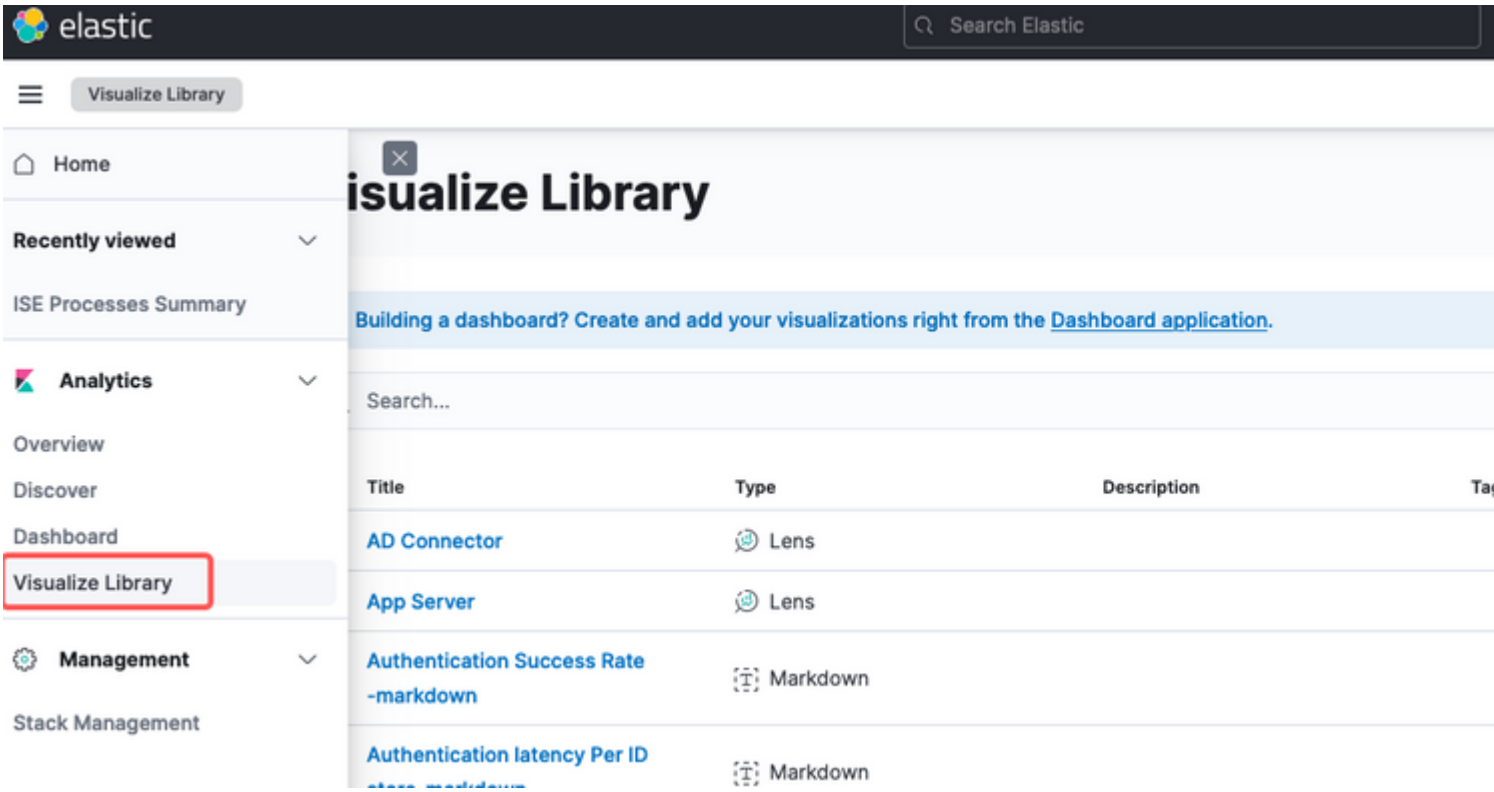

*Ingebouwde dashboards*

- Beschikbare dashboards op ISE 3.3

: Deze tonen gegevens in verticale balken, waardoor het gemakkelijk is om waarden over categorieën of tijdintervallen te vergelijken.

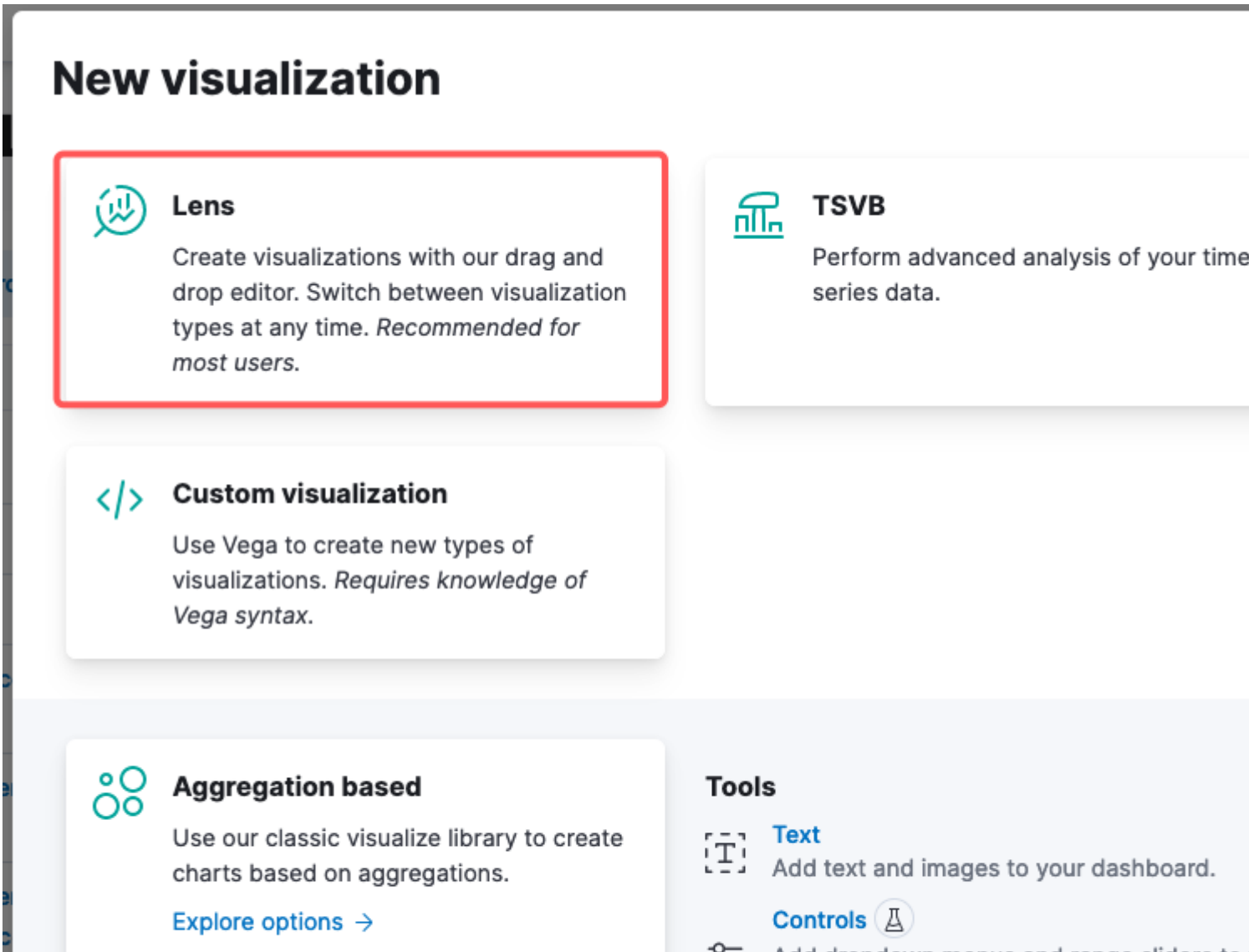
- **Lijnkaarten**: Lijnkaarten geven gegevens weer als een reeks gegevenspunten verbonden door lijnen. Ze zijn handig om trends door de tijd heen te visualiseren.
- **Taartgrafieken**: Taartgrafieken vertegenwoordigen gegevens in een cirkelvormige grafiek, waarbij elk segment van de taart een categorie en de grootte van het segment vertegenwoordigt en de verhouding aangeeft.
- **Gebiedskaarten**: Net als lijnkaarten, tonen gebiedskaarten ook trends in de tijd, maar ze vullen het gebied onder de lijnen, waardoor het gemakkelijker wordt om de omvang van veranderingen te zien.
- **Warmtekaarten**: Warmtekaarten gebruiken kleuren om gegevenswaarden in een matrix of raster weer te geven. Zij zijn nuttig om concentraties of variaties in gegevens te tonen.
- **Metrische visualisaties**: Deze geven enkele numerieke waarden weer, zoals tellingen of gemiddelden. Zij worden vaak gebruikt om essentiële prestatie-indicatoren (KPI's) te tonen.
- **Datatabellen**: Datatabellen presenteren ruwe gegevens in tabelvorm, zodat u gedetailleerde informatie kunt zien en de gegevens kunt sorteren of filteren.
- **Histogrammen**: Histogrammen verdelen gegevens in bins of intervallen en tonen de frequentie of de telling van gegevenspunten in elke bak. Zij zijn nuttig om gegevensdistributies te begrijpen.
- **Coördinaat Kaarten**: Deze visualiseren georuimtelijke gegevens, zodat u gegevens op een kaart kunt weergeven en verschillende markeringen, kleuren of groottes kunt gebruiken om datakenmerken weer te geven.
- **Tag Clouds**: Tag clouds tonen woordfrequenties, waarbij de grootte van elk woord het belang of de frequentie van elk woord aangeeft in een dataset.

Navigeer naar Analytics>Visaulize Library en klik op "Creëer visualisatie".




*Creëer visualisatie*

Selecteer de visualisatie van uw voorkeur, op dit voorbeeld Lens is de voorkeur voor praktische uitvoerbaarheid.



: In het linker paneel kunt u de gegevensbron of het indexpatroon van Elasticsearch selecteren dat u voor uw visualisatie wilt gebruiken.

- **Visualisatiekantoor**: Het centrale gebied is waar u uw visualisatie opbouwt door velden te slepen en te laten vallen, grafiektypes te selecteren en grafiekinstellingen te configureren.
- **Visualization Toolbar**: Boven het canvas vindt u mogelijk een werkbalk waarmee u uw visualisatie kunt aanpassen, inclusief opties voor het wijzigen van grafiektypes, het toevoegen van filters en het configureren van grafiekinstellingen.

- **Datapaneel**: Aan de rechterkant hebt u toegang tot het 'Data'-paneel, waarmee u uw gegevenstransformatie, aggregatie en veldinstellingen kunt beheren.

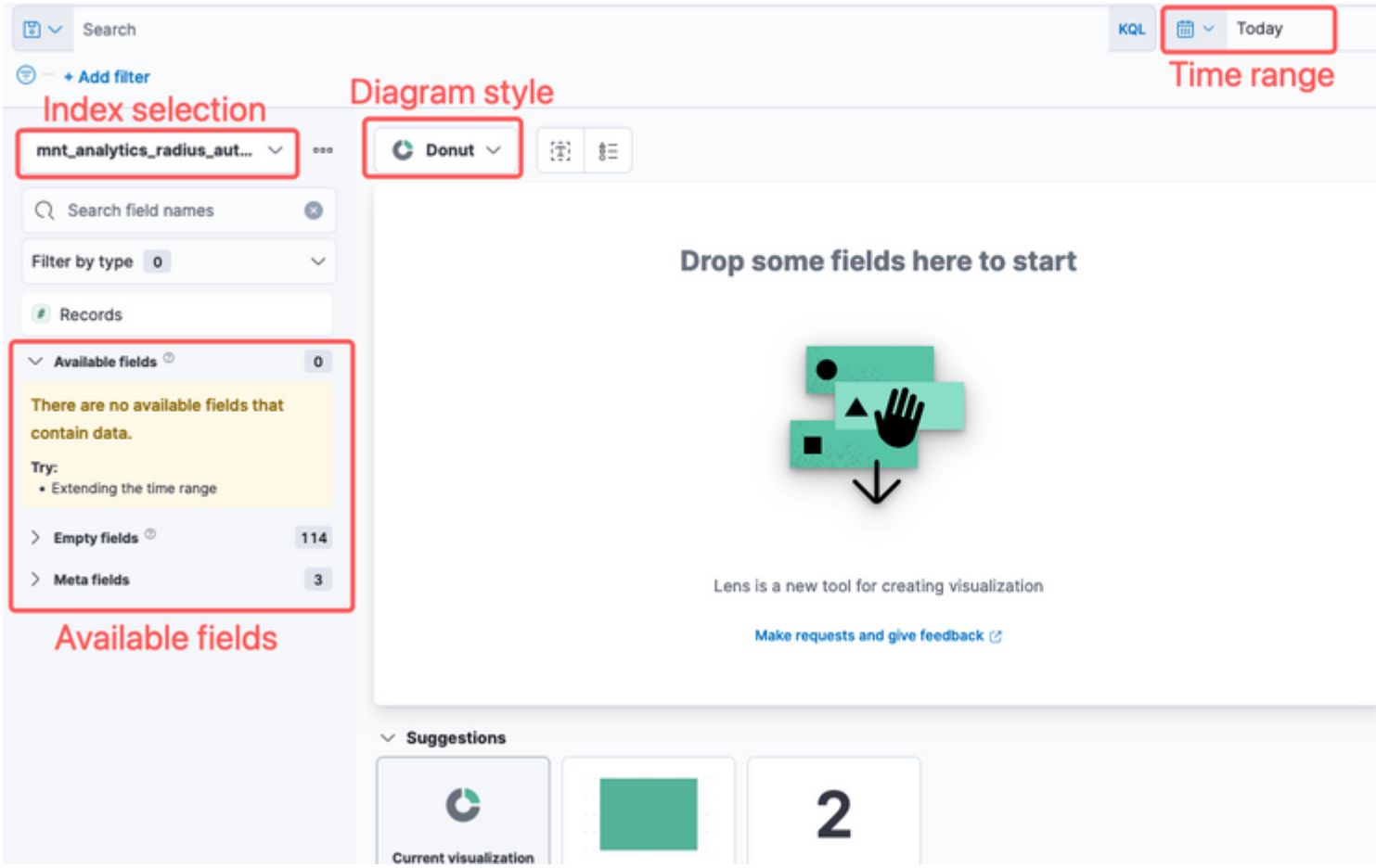
- **Layer Management**: Afhankelijk van het type visualisatie dat u maakt (bijvoorbeeld gelaagde diagrammen), kunt u een Layer Management Area hebben voor het configureren van meerdere lagen in uw visualisatie.

- **Voorbeeld:** als u wijzigingen in uw visualisatie aanbrengt, wordt er meestal een realtime voorbeeld gegeven, zodat u kunt zien hoe uw tabel er uitziet met de huidige instellingen**.**

- **Visualisatie-instellingen**: Afhankelijk van het geselecteerde kaarttype kunt u specifieke instellingen voor dat visualisatietype openen, zoals asconfiguratie, kleurenschema's en labels.

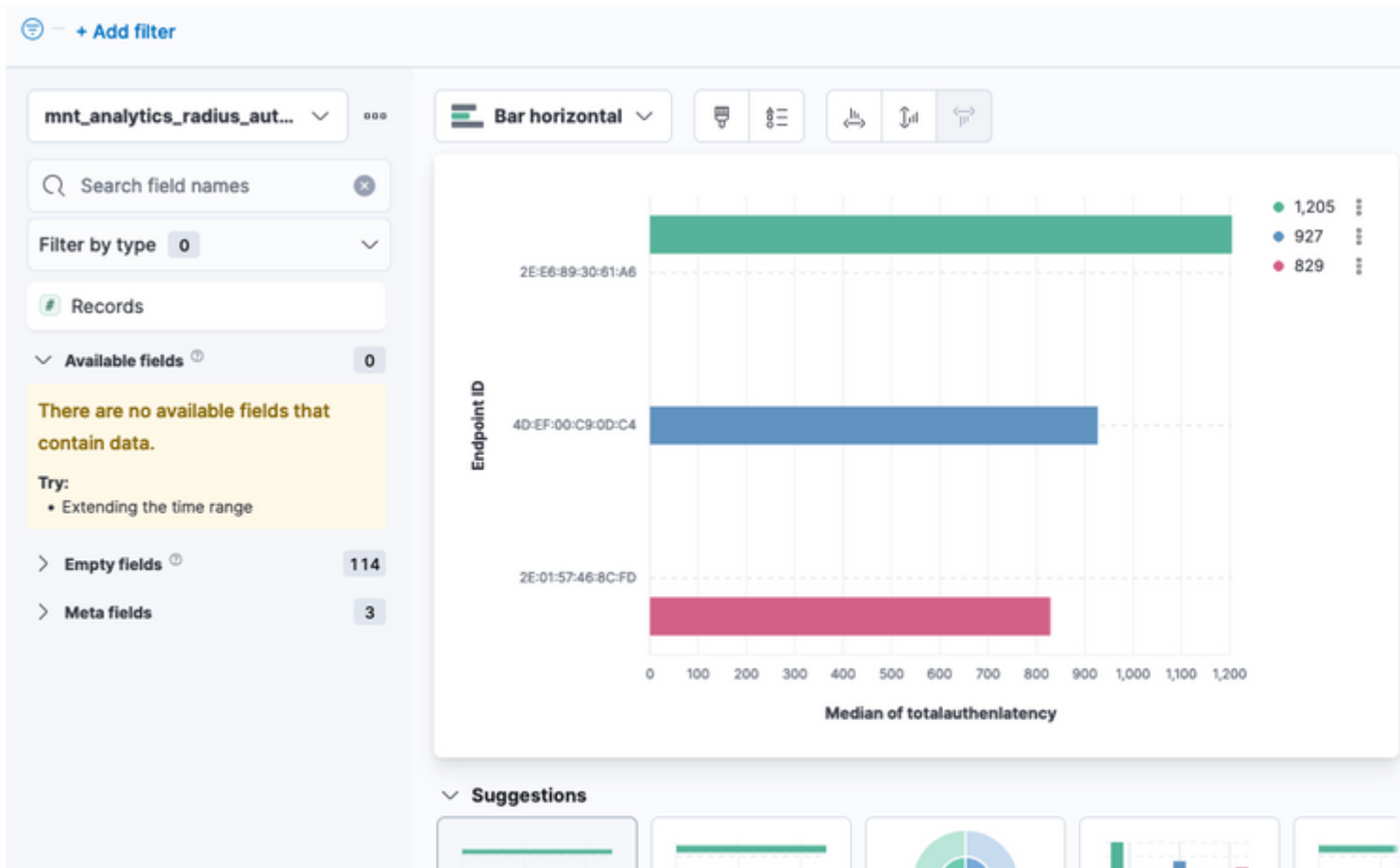
- **Interactiviteit-instellingen**: U kunt interacties en acties toevoegen aan uw visualisatie, zodat gebruikers gegevens kunnen filteren of naar andere delen van uw Kibana-dashboards kunnen navigeren.

- **Opslaan en delen**: Bovenaan de Lens-interface staan meestal opties om uw visualisatie op te slaan, toe te voegen aan een dashboard of het met anderen te delen.




*Lensvisualisatie*

Vanwege Cisco-bug-id CSCwh48057 worden in het linkerpaneel geen beschikbare velden voor gebruik weergegeven. Aan de rechterkant kunt u echter de gewenste velden en diagramstijl selecteren. Op dit voorbeeld, aangezien auth latency een onderwerp van gemeenschappelijk belang is wordt de grafiek gebouwd om authentificatie latentie versus endpoint id te visualiseren.



```
admin#show logging application ise-logstash/logstash.log
admin#show logging application mnt-la-elasticsearch/mnt-la-elasticsearch.log
```

## Gerelateerde informatie

ISE 3.3 beheerdershandleiding

Kibana-documentatie

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.