Tableau Server bedrijfsbreed Implementatiegids

Laatst bijgewerkt 13-2-2025

Inhoud

Gids voor bedrijfsbrede implementatie van Tableau Server

De GBI (Gids voor bedrijfsbrede implementatie van Tableau Server) is ontwikkeld om prescriptieve richtlijnen te bieden voor de implementatie van Tableau Server (on-premises of in de cloud). De gids biedt implementatierichtlijnen voor bedrijfsscenario's in de context van een referentiearchitectuur. We hebben de referentiearchitectuur getest om de naleving van beveiligings-, schaal- en prestatiebenchmarks te verifiëren, die voldoen aan de best practices uit de branche.

Op een hoog niveau bestaan de kernfuncties van een normconforme implementatie voor ondernemingen uit een gelaagde topologie waarbij elke laag van servertoepassingsfunctionaliteit (webgatewaylaag, toepassingslaag en datalaag) is gebonden en beveiligd door subnetten met toegangsbeheer. Gebruikers die via internet toegang hebben tot de servertoepassing worden op de weblaag geverifieerd. Na verificatie wordt de aanvraag via een proxy verzonden naar een beveiligd subnet, waar de toepassingslaag de bedrijfslogica afhandelt. Data met een hoge waarde worden beschermd door het derde subnet: de datalaag. Services op de toepassingslaag communiceren via het beveiligde netwerk met de datalaag om dataverzoeken aan de back-enddatabronnen te verwerken.

Bij deze implementatie staat beveiliging voorop bij alle ontwerpbeslissingen en de uitvoering. Betrouwbaarheid, prestaties en schaalbaarheid zijn echter ook belangrijke vereisten. Gezien het gedistribueerde en modulaire ontwerp van de referentiearchitectuur worden betrouwbaarheid en prestaties op een lineair voorspelbare manier geschaald door compatibele services strategisch samen te plaatsen bij elk knooppunt en door services toe te voegen op knelpunten.

Voor wie is deze informatie bedoeld?

De GBI is ontwikkeld voor IT-beheerders van ondernemingen die mogelijk het volgende nodig hebben:

- Een door IT beheerde Tableau-implementatie
- Handhaving van naleving van industrienormen
- Best practices voor industriële implementatie
- Standaard beveiligde implementatie

De GBI is een gids voor het implementeren van de referentiearchitectuur voor de onderneming. Hoewel deze versie van de GBI een voorbeeld van een AWS/Linux-implementatie bevat, kan de gids door ervaren IT-beheerders in ondernemingen worden gebruikt als hulpmiddel om de voorgeschreven referentiearchitectuur te implementeren in elke standaarddatacenteromgeving.

Versie

Deze versie van GBI is ontwikkeld voor versie 2021.2.3 (of later) van Tableau Server. Hoewel u de GBI kunt gebruiken als algemeen naslagwerk voor de implementatie van oudere versies van Tableau Server, raden wij u aan de referentiearchitectuur te implementeren met Tableau Server 2021.2.3 of hoger. Sommige functies en opties zijn niet beschikbaar in oudere versies van Tableau Server.

Voor de meest recente functies en verbeteringen raden wij u aan GBI te implementeren met Tableau Server 2022.1.7 en hoger.

De referentiearchitectuur die in deze gids wordt beschreven, ondersteunt de volgende Tableau-clients: webauthoring met compatibele browsers, Tableau Mobile en Tableau Desktop versie 2021.2.1 of hoger. Andere Tableau-clients (Tableau Prep, Bridge enz.) zijn nog niet gevalideerd met de referentiearchitectuur.

Belangrijke functies

De eerste versie van de Tableau Server-referentiearchitectuur introduceert de volgende scenario's en functies:

- Voorafgaande clientverificatie: Tableau-clients (Desktop, Mobile, Web Authoring) worden geverifieerd via de zakelijke verificatieprovider in de weblaag voordat ze toegang krijgen tot de interne Tableau Server. Dit proces wordt geregeld door het configureren van een authN-plug-in op de onafhankelijke gateway in Tableau Server, die fungeert als reverse-proxyserver. Zie Deel 5 - Weblaag configureren.
- Zero-trust-implementatie: omdat al het verkeer naar Tableau-servers vooraf wordt geverifieerd, werkt de volledige Tableau-implementatie in een privésubnet waarvoor geen vertrouwde verbinding nodig is.
- Externe opslagplaats: de referentiearchitectuur specificeert dat de Tableau-opslagplaats in een externe PostgreSQL-database moet worden geïnstalleerd. Hierdoor kunnen DBA's bij het beheren, optimaliseren, schalen en maken van een back-up van de opslagplaats op dezelfde manier te werk gaan als bij een generieke database.
- Herstel van eerste knooppunt: de GBI introduceert een script dat het herstel van het eerste knooppunt automatiseert in geval van een storing.
- Op TAR gebaseerde back-up en herstel: gebruik vertrouwde TAR-back-ups bij strategische mijlpalen van de Tableau-implementatie. In het geval van een storing of een verkeerde implementatieconfiguratie kunt u snel herstellen naar de vorige implementatiefase door de bijbehorende TAR-back-up terug te zetten.
- Prestatieverbetering: klant- en laboratoriumvalidatie tonen een prestatieverbetering van 15-20% bij het uitvoeren van GBI in vergelijking met standaardimplementatie.

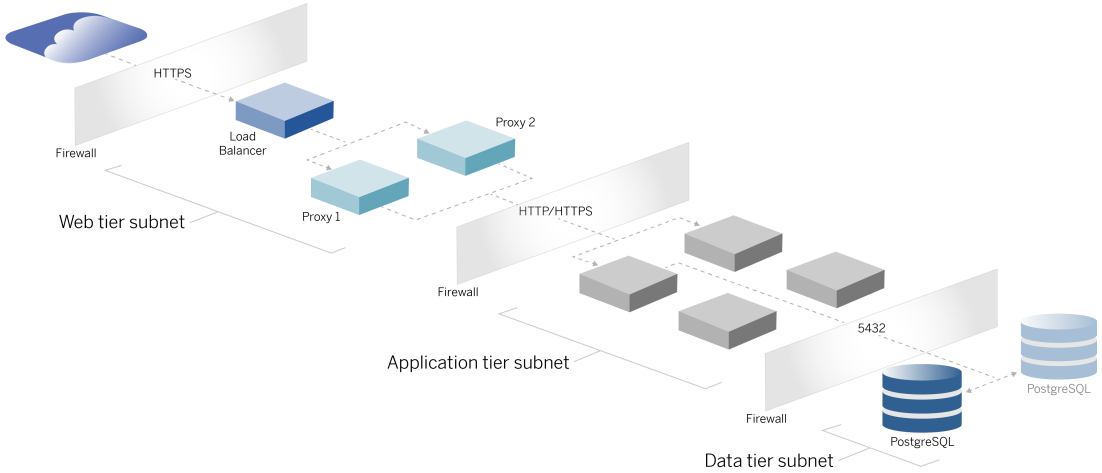
Licenties

Voor de Tableau Server-referentiearchitectuur die in deze gids wordt voorgeschreven, is een Tableau Advanced Management-licentie vereist om de externe opslagplaats van Tableau Server in te schakelen. U kunt desgewenst Extern bestandsarchief van Tableau Server implementeren. Hiervoor is ook de Tableau Advanced Management-licentie vereist. Zie *Tableau Advanced Management op Tableau Server* (Linux).

Deel 1 - De basisprincipes van implementatie in bedrijven

In deel 1 worden de functies en vereisten van de industriestandaard implementatie in bedrijven nader beschreven. Hiervoor is de Gids voor bedrijfsbrede implementatie van Tableau Server ontworpen.

Het onderstaande netwerkdiagram toont een generieke gelaagde implementatie voor een datacenter met Tableau Server-referentiearchitectuur.



Industriestandaard en implementatievereisten

Hieronder staan de kenmerken van implementaties die voldoen aan de industriestandaard. Dit zijn de vereisten waarvoor de referentiearchitectuur is ontworpen:

- Een netwerkontwerp met meerdere lagen: het netwerk is verbonden door beveiligde subnetten om de toegang te beperken per laag: web-, toepassings- en datalaag. Enkele communicatie kan niet door meerdere subnetten heen gaan, omdat alle communicatie bij het volgende subnet wordt beëindigd.
- Standaard geblokkeerde poorten en protocollen: elk subnet en elke beveiligingsgroep blokkeert standaard alle inkomende en uitgaande poorten en protocollen.

Communicatie wordt deels mogelijk gemaakt door excepties te openen in de poort- of protocolconfiguratie.

- 'Off-box' webverificatie: gebruikersverzoeken vanaf internet worden geverifieerd door een verificatiemodule op de reverse-proxy in de weblaag. Daarom worden alle verzoeken aan de toepassingslaag al in de weblaag geverifieerd voordat ze naar de beveiligde toepassingslaag worden doorgestuurd.
- Platformonafhankelijk: de oplossing kan worden geïmplementeerd met on-premises servertoepassingen of in de cloud.
- Technologie-agnostisch: de oplossing kan worden geïmplementeerd in een virtuele machine-omgeving of in containers. Kan ook op Windows of Linux worden geïmplementeerd. Deze eerste versie van de referentiearchitectuur en ondersteunende documentatie is echter ontwikkeld voor Linux die draait op AWS.
- Hoge beschikbaarheid: alle componenten in het systeem worden als cluster geïmplementeerd en zijn ontworpen om te werken in een actieve/actieve- of actieve/passieve-implementatie.
- Geïsoleerde rollen: elke server vervult een discrete rol. Dit ontwerp verdeelt alle servers zodanig dat de toegang beperkt blijft tot service-specifieke beheerders. DBA's beheren bijvoorbeeld PostgreSQL voor Tableau, identiteitsbeheerders beheren de verificatiemodule op de weblaag, en netwerk- en cloudbeheerders maken verkeer en connectiviteit mogelijk.
- Lineair schaalbaar: u kunt elke laag onafhankelijk schalen op basis van het belastingprofiel, omdat het discrete rollen zijn.
- Clientondersteuning: de referentiearchitectuur ondersteunt alle Tableau-clients: Tableau Desktop (versie 2021.2 of later), Tableau Mobile en Tableau Web Authoring.

Veiligheidsmaatregelen

Zoals gezegd is beveiliging een van de belangrijkste kenmerken van de industriestandaard voor ontwerpen voor datacenters.

- Toegang: elke laag is gebonden aan een subnet dat toegangscontrole op netwerklaag afdwingt met behulp van poortfiltering. Communicatietoegang tussen subnetten kan ook worden afgedwongen door de toepassingslaag met geverifieerde services tussen processen.

- Integratie: de architectuur is ontworpen om te worden aangesloten op een identiteitsprovider (IdP) op de reverse-proxy in de weblaag.
- Privacy: verkeer naar de weblaag wordt vanaf de client versleuteld met SSL. Optioneel kan het verkeer naar de interne subnetten ook worden versleuteld.

Webproxy-laag

De weblaag is een subnet in de DMZ (ook wel perimeterzone genoemd) die fungeert als beveiligingsbuffer tussen het internet en de interne subnetten waar toepassingen worden geïmplementeerd. De weblaag host reverse-proxyservers die geen gevoelige informatie opslaan. De reverse-proxyservers zijn geconfigureerd met een AuthN-plug-in om clientsessies vooraf te verifiëren met een vertrouwde IdP, voordat de clientaanvraag wordt omgeleid naar Tableau Server. Zie Pre-verificatie met een AuthN-module voor meer informatie.

Loadbalancers

Het implementatieontwerp omvat een zakelijke loadbalancing-oplossing vóór de reverse-proxyservers.

Loadbalancers bieden belangrijke verbeteringen op het gebied van beveiliging en prestaties, dankzij de volgende functies:

- Virtualisatie van de front-end URL voor de services van de toepassingslaag
- Het afdwingen van SSL-versleuteling
- Het ontlasten van SSL
- Afgedwongen compressie tussen de client en de weblaagservices
- Bescherming tegen DOS-aanvallen
- Het bieden van hoge beschikbaarheid

Opmerking: Tableau Server versie 2022.1 bevat de onafhankelijke gateway van Tableau Server. De onafhankelijke gateway is een zelfstandige instantie van het Tableau Gateway-proces dat fungeert als een Tableau-bewuste reverse-proxy. Bij de release is de onafhankelijke gateway gevalideerd, maar nog niet volledig getest in de EDG-

referentiearchitectuur. Nadat de tests volledig zijn voltooid, wordt de EDG bijgewerkt met de aanbevolen richtlijnen voor de onafhankelijke gateway van Tableau Server.

Toepassingslaag

De toepassingslaag bevindt zich in een subnet waarop de belangrijkste bedrijfslogica van de servertoepassing wordt uitgevoerd. De toepassingslaag bestaat uit services en processen die zijn geconfigureerd op gedistribueerde knooppunten in een cluster. De toepassingslaag is alleen toegankelijk via de weblaag en is niet rechtstreeks toegankelijk voor gebruikers.

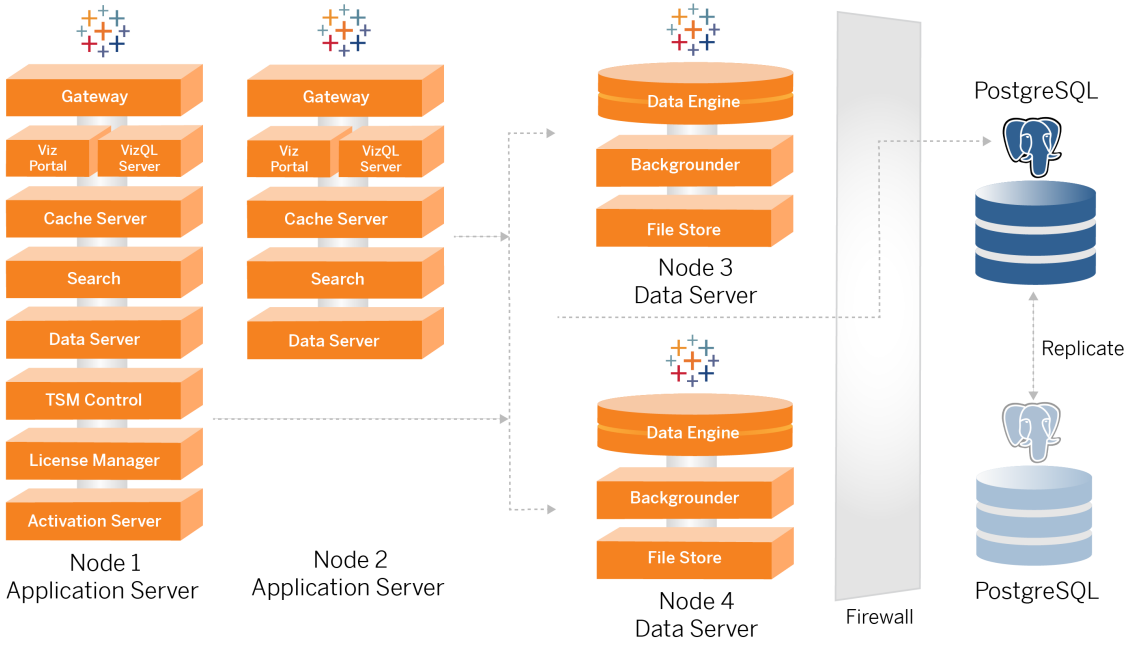
Prestaties en betrouwbaarheid worden verbeterd door de toepassingsprocessen zo te configureren dat processen die verschillende resources gebruiken (oftewel CPU-intensief versus geheugenintensief profiel) op dezelfde locatie worden uitgevoerd.

Datalaag

De datalaag is een subnet dat waardevolle data bevat. Al het verkeer naar deze laag is afkomstig van de toepassingslaag en is daarom al geverifieerd. Naast de toegangsvereisten op de netwerklaag met poortconfiguratie, moet deze laag ook geverifieerde toegang en optioneel versleuteld verkeer met de toepassingslaag omvatten.

Deel 2 - De basisprincipes van de referentiearchitectuur voor de implementatie van Tableau Server

De afbeelding hieronder toont de relevante Tableau Server-processen en hoe deze in de referentiearchitectuur zijn geïmplementeerd. Deze implementatie wordt beschouwd als de minimale Tableau Server-implementatie die geschikt is voor bedrijven.



De procesdiagrammen in dit onderwerp zijn bedoeld om de belangrijkste, bepalende processen van elk knooppunt weer te geven. Er zijn veel ondersteunende processen die ook op de knooppunten draaien, maar die niet in de diagrammen zijn weergegeven. Zie de configuratiesectie van deze gids, Deel 4 – Tableau Server installeren en configureren voor een lijst met alle processen.

Tableau Server-processen

De Tableau Server-referentiearchitectuur is een Tableau Server-clusterimplementatie met vier knooppunten en een externe opslagplaats op PostgreSQL:

- Het eerste knooppunt van Tableau Server (Knooppunt 1): voert de vereiste TSM-beheer- en licentieservices uit die alleen op één knooppunt in het cluster kunnen worden uitgevoerd. In de zakelijke context is het eerste knooppunt van Tableau Server het primaire knooppunt in het cluster. Dit knooppunt voert ook redundante toepassingservices uit met Knooppunt 2.
- De toepassingsknooppunten van Tableau Server (Knooppunt 1 en Knooppunt 2): de twee knooppunten verwerken clientverzoeken, maken verbinding met en voeren query's uit op databronnen en op de dataknooppunten.
- De dataknooppunten van Tableau Server (Knooppunt 3 en Knooppunt 4): twee knooppunten die speciaal zijn bedoeld voor het beheer van data.
- Externe PostgreSQL: deze host voert het proces voor de Tableau Server-opslagplaats uit. Voor implementatie van hoge beschikbaarheid moet u een extra PostgreSQL-host gebruiken voor actieve/passieve redundantie.

  U kunt PostgreSQL ook op Amazon RDS laten draaien. Zie *Externe opslagplaats Tableau Server* (Linux) voor meer informatie over de verschillen tussen het uitvoeren van de opslagplaats op RDS en een EC2-instantie.

  Voor het implementeren van Tableau Server met een externe opslagplaats is een Tableau Advanced Management-licentie vereist.

  Als uw organisatie niet over interne DBA-expertise beschikt, hebt u de optie om het proces voor de Tableau Server-opslagplaats uit te voeren in de standaard, interne PostgreSQL-configuratie. In het standaardscenario draait de opslagplaats op een Tableau-knooppunt met ingesloten PostgreSQL. In dit geval raden we aan om de opslagplaats op een speciaal Tableau-knooppunt te laten draaien en een passieve opslagplaats op een extra, speciaal hiervoor bestemd knooppunt, ter ondersteuning van de Failover voor opslagplaats. Zie *Failover voor opslagplaats* (Linux).

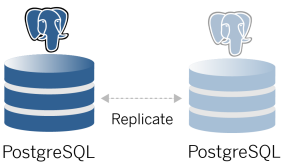
Ter illustratie legt de AWS-implementatie die in deze gids wordt beschreven uit hoe u de externe opslagplaats implementeert op PostgreSQL die draait op een EC2-instantie.

- Optioneel: Als uw organisatie externe opslag gebruikt, kunt u Tableau Bestandsarchief implementeren als een externe service. In deze gids is het externe bestandsarchief niet in het kernimplementatiescenario opgenomen. Zie *Tableau Server installeren met extern bestandsarchief* (Linux).

  Voor het implementeren van Tableau Server met een extern bestandsarchief is een Tableau Advanced Management-licentie vereist.

PostgresSQL-opslagplaats

Tableau Server-opslagplaats is een PostgresSQL-database die serverdata opslaat. Deze data bevatten informatie over Tableau Server met betrekking tot de gebruikers, groepen en groepstoewijzingen, machtigingen, projecten, databronnen en metadata en vernieuwingsinformatie van extracten.



De standaard PostgresSQL-implementatie verbruikt bijna 50% van de resources voor systeemgeheugen. Afhankelijk van het gebruik (voor productie en grootschalige productie-implementaties) kan het gebruik van de resources nog toenemen. Om deze reden raden wij aan om het opslagplaatsproces uit te voeren op een computer waarop geen andere resource-intensieve servercomponenten zoals VizQL, Backgrounder of Data-engine worden uitgevoerd. Wanneer u het opslagplaatsproces samen met een van deze componenten uitvoert, ontstaan er I/O-conflicten, resource-beperkingen en worden de algehele prestaties van de implementatie slechter.

Knooppunt 1: eerste knooppunt

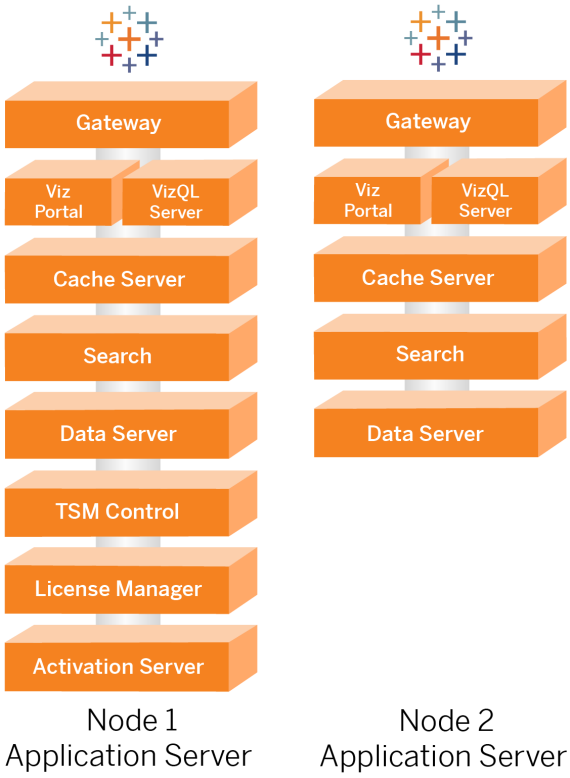
Het eerste knooppunt voert een klein aantal belangrijke processen uit en deelt de toepassingsbelasting met Knooppunt 2.

De eerste computer waarop u Tableau installeert, het 'eerste knooppunt', heeft een aantal unieke kenmerken. Drie processen worden alleen op het eerste knooppunt uitgevoerd en kunnen niet naar een ander knooppunt worden verplaatst, behalve in geval van een storing: de Licentieservice (Licentiebeheer), de Activeringsservice en de TSM-controller (Beheercontroller).

Knooppunt 1 failover en geautomatiseerd herstel

De services Licentie, Activering en TSM-controller zijn van cruciaal belang voor de status van een Tableau Server-implementatie. Als Knooppunt 1 uitvalt, kunnen gebruikers nog steeds verbinding maken met de Tableau Server-implementatie, omdat een correct geconfigureerde referentiearchitectuur de verzoeken naar Knooppunt 2 routeert. Zonder deze kernservices zal de implementatie een kritieke status krijgen en waarschijnlijk mislukken. Zie Automatisch herstel van eerste knooppunt.

Knooppunten 1 en 2: toepassingsservers



Knooppunten 1 en 2 voeren de Tableau Server-processen uit die clientverzoeken verwerken, databronnen bevragen, visualisaties genereren, inhoud en beheer hanteren en andere belangrijke bedrijfslogica van Tableau uitvoeren. De toepassingsservers slaan geen gebruikersdata op.

Opmerking:Toepassingsserver is een term die ook verwijst naar een Tableau Server-proces dat in TSM wordt vermeld. Het onderliggende proces voor Toepassingsserver is VizPortal.

Wanneer Knooppunt 1 en Knooppunt 2 parallel worden uitgevoerd, schalen ze om verzoeken te verwerken van de loadbalancing-logica die op de reverse-proxyservers wordt uitgevoerd.

Wanneer een van deze knooppunten uitvalt, worden de clientverzoeken en -diensten door het resterende knooppunt afgehandeld, aangezien het redundante knooppunten zijn.

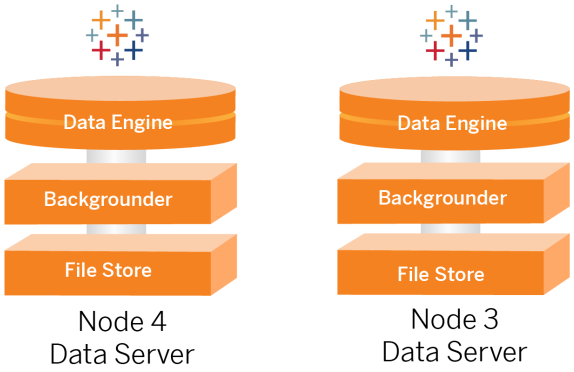
De referentiearchitectuur is zo ontworpen dat complementaire toepassingsprocessen op dezelfde computer worden uitgevoerd. Dit betekent dat de processen niet met elkaar concurreren om resources en zo conflicten veroorzaken.

Zo is bijvoorbeeld VizQL, een kernverwerkingsservice op toepassingsservers, sterk CPU- en geheugengebonden. VizQL gebruikt bijna 60-70% van de CPU en het geheugen op de computer. Om deze reden is de referentiearchitectuur zo ontworpen dat er zich geen andere geheugen- of CPU-gebonden processen op hetzelfde knooppunt bevinden als VizQL. Uit tests blijkt dat de hoeveelheid belasting of het aantal gebruikers geen invloed heeft op het geheugen- of CPU-gebruik op VizQL-knooppunten. Het verlagen van het aantal gelijktijdige gebruikers in onze belastingstest had alleen invloed op de prestaties van het dashboard of het laadproces van de visualisatie, maar het gebruik van resources werd niet verminderd. Afhankelijk van het beschikbare geheugen en de CPU tijdens piekgebruik, kunt u overwegen om meer VizQL-processen toe te voegen. Als startpunt voor typische werkmappen wijst u 4 kernen per VizQL-proces toe.

Toepassingsservers schalen

De referentiearchitectuur is ontworpen voor schaalbaarheid op basis van een gebruiksgebaseerd model. Als algemeen uitgangspunt adviseren wij minimaal twee toepassingsservers, die elk maximaal 1000 gebruikers ondersteunen. Naarmate het aantal gebruikers groeit, kunt u voor elke 1000 extra gebruikers een toepassingsserver toevoegen. Monitor het gebruik en de prestaties om het aantal gebruikers per host voor uw organisatie af te stemmen.

Knooppunten 3 en 4: dataservers



De processen Bestandsarchief, Data-engine (Hyper) en Backgrounder zijn om de volgende redenen op Knooppunt 3 en 4 samengebracht:

- Optimalisatie van extract: als u Backgrounder, Hyper en Bestandsarchief op hetzelfde knooppunt uitvoert, worden de prestaties en betrouwbaarheid geoptimaliseerd. Tijdens het extractieproces zal Backgrounder de doeldatabase bevragen, het Hyperbestand aanmaken op hetzelfde knooppunt en het vervolgens uploaden naar Bestandsarchief. Door deze processen op hetzelfde knooppunt te plaatsen, hoeven er voor de workflow voor het maken van extracties geen grote hoeveelheden data over het netwerk of de knooppunten te worden gekopieerd.
- Complementaire resourcebalancering: Backgrounder is voornamelijk CPU-intensief. Data-engine is een proces dat veel geheugen vergt. Door deze processen te koppelen, wordt het gebruik van de resources op elk knooppunt maximaal benut.
- Consolidatie van dataprocessen: omdat elk van deze processen back-end-dataprocessen zijn, is het zinvol om ze in de veiligste datalaag uit te voeren. In toekomstige versies van de referentiearchitectuur zullen de toepassings- en dataservers in afzonderlijke lagen draaien. Vanwege toepassingsafhankelijkheden in de Tableau-architectuur moeten toepassings- en dataservers op dit moment echter in dezelfde laag draaien.

Dataservers schalen

Net als bij toepassingsservers is voor het plannen van de resources die nodig zijn voor Tableau-dataservers gebruiksgebaseerd modelleren vereist. Over het algemeen kunt u

verwachten dat elke dataserver maximaal 2000 extractvernieuwingsjobs per dag kan ondersteunen. Naarmate het aantal extractjobs toeneemt, voegt u extra dataservers toe zonder de service Bestandsarchief. De implementatie van een dataserver met twee knooppunten is over het algemeen geschikt voor implementaties die het lokale bestandssysteem gebruiken voor de service Bestandsarchief. Houd er rekening mee dat het toevoegen van meer toepassingsservers geen lineaire invloed heeft op de prestaties of schaalbaarheid van dataservers. Afgezien van wat overhead door extra gebruikersquery's is de impact van het toevoegen van meer toepassingshosts en gebruikers minimaal.

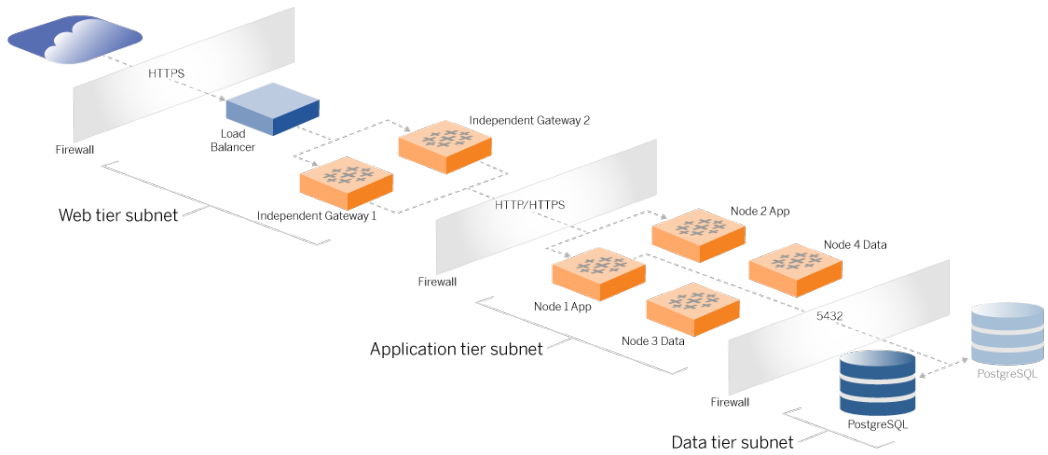
Deel 3 – De implementatie van Tableau Server Enterprise voor-bereiden

In deel 3 worden de vereisten beschreven voor het voorbereiden van uw infrastructuur voor de implementatie van de Tableau Server-referentiearchitectuur. Voordat u begint, raden wij u aan om Deel 2 – De basisprincipes van de referentiearchitectuur voor de implementatie van Tableau Server nogmaals door te nemen.

Naast beschrijvingen van vereisten biedt dit onderwerp een implementatievoorbeeld van de referentiearchitectuur in een AWS-omgeving. De rest van deze gids bouwt voort op het voor-beeld van een AWS-referentiearchitectuur dat in dit onderwerp is gestart.

Een kernprincipe van de referentiearchitectuur is standaardisatie met best practices voor datacenterbeveiliging. De architectuur is specifiek ontworpen om services te scheiden in beveiligde netwerksubnetten. Communicatie tussen subnetten is beperkt tot specifiek pro-tocol- en poortverkeer.

Het onderstaande diagram illustreert het subnetontwerp voor de referentiearchitectuur voor een on-premises implementatie of een door de klant beheerde cloud-implementatie. In de sectie Voorbeeld: subnetten en beveiligingsgroepen configureren in AWS hieronder, vindt u een voorbeeld van een cloud-implementatie.



Subnetten

Maak drie subnetten:

- een weblaag
- een toepassingslaag
- een datasubnet

Regels voor firewall-/beveiligingsgroep

De tabbladen hieronder beschrijven de firewallregels voor elke laag van het datacenter. Zie de sectie verderop in dit onderwerp voor AWS-specifieke beveiligingsgroepsregels.

Weblaag

De weblaag is een openbaar DMZ-subnet dat inkomende HTTPS-verzoeken verwerkt en doorstuurt naar de toepassingslaag. Dit ontwerp biedt een verdedigingslaag tegen malware waarmee een mogelijke aanval op uw organisatie gericht zou kunnen worden. De weblaag blokkeert de toegang tot de toepassings-/datalaag.

Verkeer	Type	Protocol	Poortbereik	Bron

Inkomend	SSH	TCP	22	Bastion-subnet (voor cloud-implementaties)
Inkomend	HTTP	TCP	80	Internet (0.0.0.0/0)
Inkomend	HTTPS	TCP	443	Internet (0.0.0.0/0)
Uitgaand	Alle verkeer	Alle	Alle	

Toepassingslaag

Het toepassingssubnet is de locatie waar de Tableau Server-implementatie zich bevindt. Het toepassingssubnet omvat de Tableau-toepassingsservers (Knooppunt 1 en Knooppunt 2). De Tableau-toepassingsservers verwerken gebruikersverzoeken aan de dataservers en voeren de belangrijkste bedrijfslogica uit.

Het toepassingssubnet omvat ook de Tableau-dataservers (Knooppunt 3 en Knooppunt 4).

Al het clientverkeer naar de toepassingslaag wordt geverifieerd op de weblaag. Beheerderstoegang tot het subnet van de toepassing wordt geverifieerd en gerouteerd via de bastionhost.

Verkeer	**Type**	**Protocol**	**Poortbereik**	**Bron**
Inkomend	SSH	TCP	22	Bastion-subnet (voor cloud-implementaties)
Inkomend	HTTPS	TCP	443	Subnet van weblaag
Uitgaand	Alle verkeer	Alle	Alle	

Datalaag

Het datasubnet is de plek waar de externe PostgreSQL-databaseserver zich bevindt.

Verkeer	Type	Protocol	Poortbereik	Bron
Inkomend	SSH	TCP	22	Bastion-subnet (voor cloud-implementaties)
Inkomend	PostgreSQL	TCP	5432	Subnet van toepassingslaag
Uitgaand	Alle verkeer	Alle	Alle	

Bastion

De meeste beveiligingsteams in bedrijven staan geen directe communicatie toe van het on-premises beheersysteem naar de knooppunten die in de cloud zijn geïmplementeerd. In plaats daarvan wordt al het beheerde SSH-verkeer naar de cloudknooppunten doorgestuurd via een bastionhost (ook wel een 'jumpserver' genoemd). Voor cloud-implementaties adviseren wij een bastionhostproxyverbinding met alle resources in de referentiearchitectuur. Dit is een optionele configuratie voor on-premises omgevingen.

De bastionhost verifieert beheerderstoegang en staat alleen verkeer toe via het SSH-protocol.

Verkeer	Type	Protocol	Poortbereik	Bron	Bestemming
Inkomend	SSH	TCP	22	IP-adres van de beheerderscomputer	
Uitgaand	SSH	TCP	22		Subnet van weblaag
Uitgaand	SSH	TCP	22		Subnet van toe-

					passingslaag

Voorbeeld: subnetten en beveiligingsgroepen configureren in AWS

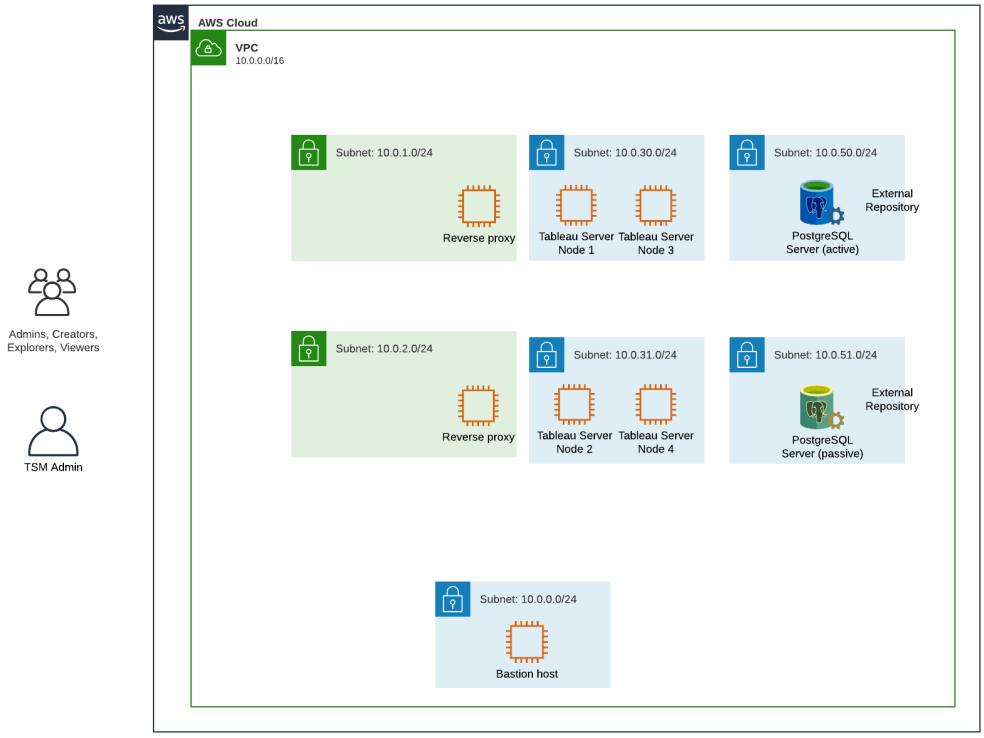
In deze sectie vindt u stapsgewijze procedures voor het maken en configureren van de VPC- en netwerkomgeving voor de implementatie van de Tableau Server-referentiearchitectuur in AWS.

De onderstaande afbeeldingen tonen de referentiearchitectuur in vier lagen. De afbeeldingen laten zien hoe de componentelementen op de topologiekaart worden gelaagd:

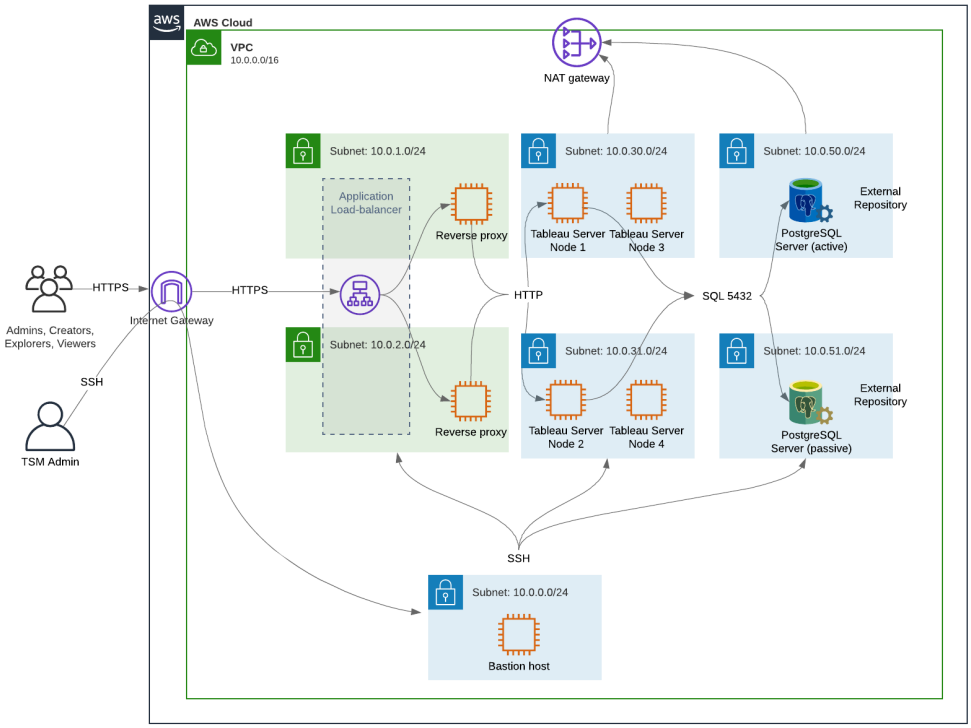
1. VPC-subnettopologie en EC2-instanties: één bastionhost, twee reverse-proxyservers, vier Tableau-servers en ten minste één PostgreSQL-server.
2. Protocolflow en internetconnectiviteit. Al het inkomende verkeer wordt beheerd via de AWS-internetgateway. Verkeer naar het internet wordt via de NAT gerouteerd.
3. Beschikbaarheidszones. De proxy-, Tableau Server- en PostgreSQL-hosts zijn gelijkmatig verdeeld over twee beschikbaarheidszones.
4. Beveiligingsgroepen. Vier beveiligingsgroepen (Openbaar, Privé, Data en Bastion) beschermen elke laag op protocolniveau.

AWS-referentiearchitectuur

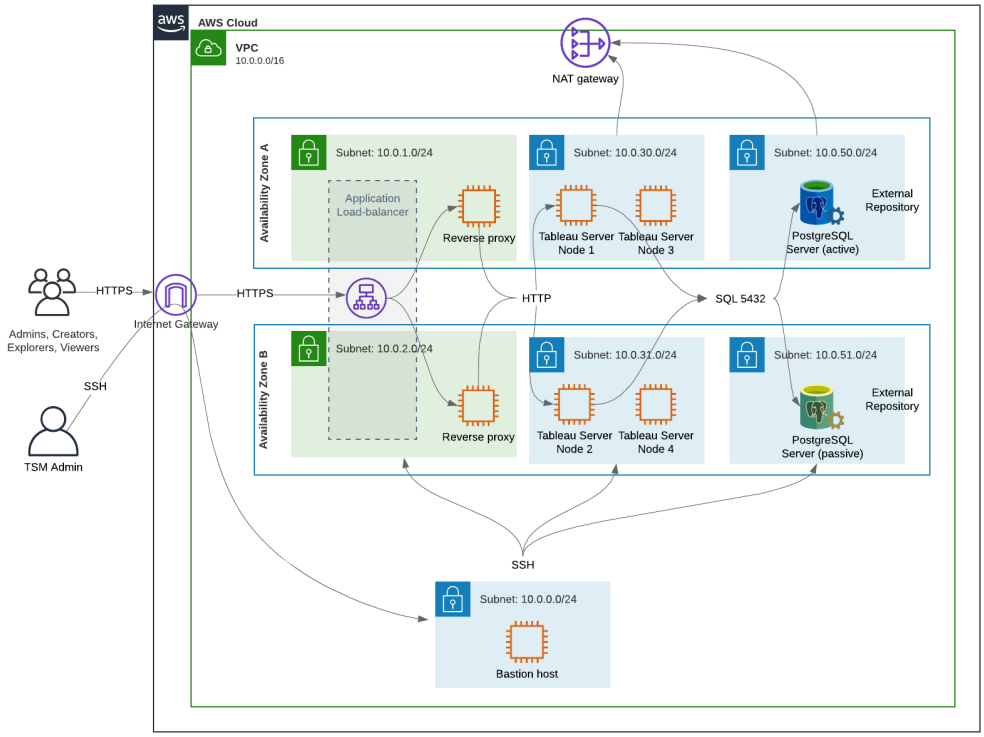
Afbeelding 1: VPC-subnettopologie en EC2-instanties



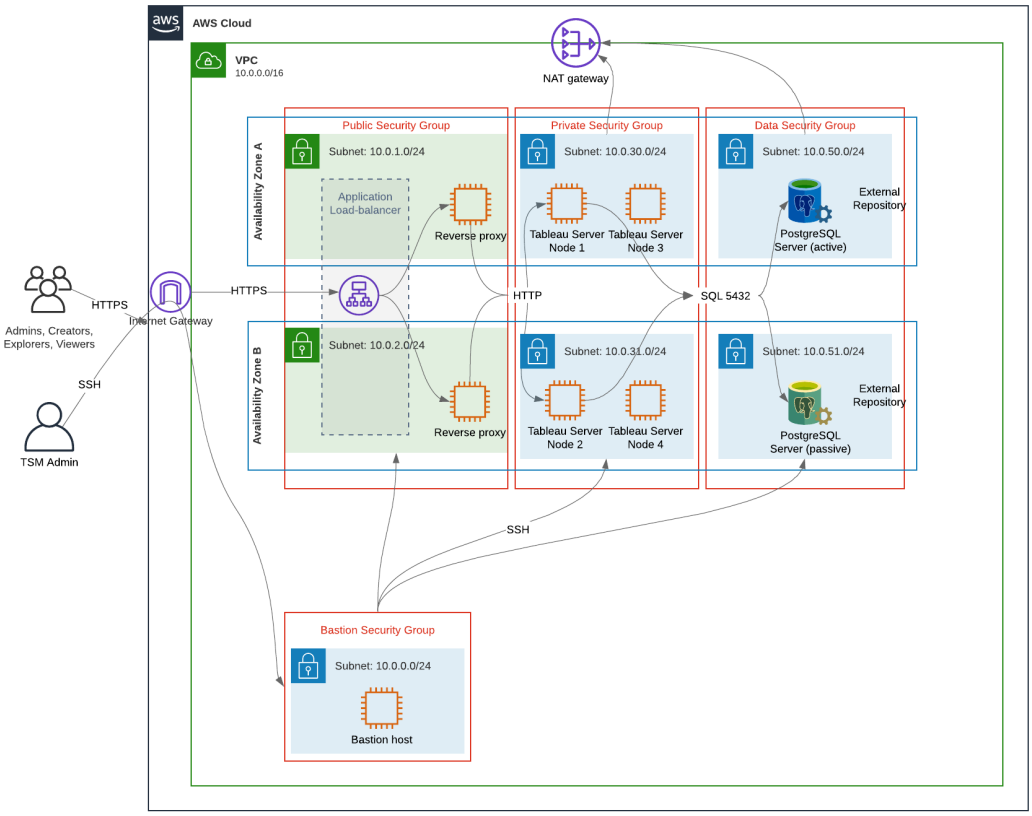
Afbeelding 2: Protocolflow en connectiviteit



Afbeelding 3: Beschikbaarheidszones



Afbeelding 4: Beveiligingsgroepen



AWS-beschikbaarheidszones en hoge beschikbaarheid

De referentiearchitectuur zoals gepresenteerd in deze gids specificeert een implementatie die beschikbaarheid biedt via redundantie wanneer een van de hosts uitvalt. In het geval van AWS, waarbij de referentiearchitectuur is geïmplementeerd in twee beschikbaarheidszones, komt de beschikbaarheid echter in gevaar in het zeldzame geval dat een beschik-baarheidszone uitvalt.

VPC-configuratie

In deze sectie wordt het volgende beschreven:

- De VPC installeren en configureren
- Internetconnectiviteit configureren
- Subnetten configureren
- Beveiligingsgroepen maken en configureren

VPC configureren

De procedure in deze sectie komt overeen met de gebruikersinterface in de klassieke VPC-ervaring. U kunt de gebruikersinterface omschakelen naar de klassieke weergave door de optie Nieuwe VPC-ervaring in de linkerbovenhoek van het AWS VPC-dashboard uit te schakelen.

Voer de VPC-wizard uit om de standaard subnetten Privé en Openbaar, de standaardroutering en het netwerk-ACL te maken.

1. Voordat u een VPC configureert, moet u een elastisch IP-adres maken. Maak een toewijzing met behulp van alle standaardwaarden.
2. VPC-wizard uitvoeren > VPC met subnetten Openbaar en Privé
3. Accepteer de meeste standaardinstellingen. Met uitzondering van het volgende:
    - Voer een VPC-naam in.
    - Geef de Elastische IP-toewijzings-ID op.
    - Geef de volgende CIDR-maskers op:
        - IPv4 CIDR van Openbaar subnet: 10.0.1.0/24, hernoem dit subnet `Public-a`.
        - IPv4 CIDR van Privé subnet: 10.0.30.0/24, hernoem dit subnet `Private-a`.
    - Beschikbaarheidszone: selecteer voor beide subnetten de optie **a** voor de regio waarin u zich bevindt.

      Opmerking: In dit voorbeeld gebruiken we **a** en **b** om onderscheid te maken tussen beschikbaarheidszones in een bepaald AWS-datacenter. In AWS komen de namen van beschikbaarheidszones mogelijk niet overeen met de

hier getoonde voorbeelden. Sommige beschikbaarheidszones omvatten bijvoorbeeld zones **c** en **d** binnen een datacenter.

4. Klik op **VPC maken**.
5. Nadat de VPC is gemaakt, maakt u de subnetten `Public-b`, `Private-b`, `Data` en `Bastion`. Om een subnet te maken, klikt u op **Subnetten** > **Subnet maken**.
    - `Public-b`: selecteer bij Beschikbaarheidszone optie **b** voor de regio waarin u zich bevindt. CIDR-blok: 10.0.2.0/24
    - `Private-b`: selecteer bij Beschikbaarheidszone optie **b** voor de regio waarin u zich bevindt. CIDR-blok: 10.0.31.0/24
    - `Data`: selecteer bij Beschikbaarheidszone optie **a** voor de regio waarin u zich bevindt. CIDR-blok: 10.0.50.0/24. Optioneel: als u van plan bent de externe database te repliceren over een PostgreSQL-cluster, maak dan een Data-b-subnet in Beschikbaarheidszone b met een CIDR-blok van 10.0.51.0/24.
    - `Bastion`: selecteer een van beide zones voor Beschikbaarheidszone. CIDR-blok: 10.0.0.0/24
6. Nadat de subnetten zijn gemaakt, bewerkt u de routetabellen in de subnetten Openbaar en Bastion, zodat de routetabel wordt gebruikt die is geconfigureerd voor de bijbehorende internetgateway (IGW). Bewerk ook de subnetten Privé en Data, zodat de routetabel wordt gebruikt die is geconfigureerd voor de network address translator (NAT).
    - Om te bepalen welke routetabel is geconfigureerd met de IGW of de NAT, klikt u op **Routetabellen** in het AWS-dashboard. Selecteer een van de twee routetabelkoppelingen om de eigenschappenpagina te openen. Kijk naar de Doelwaarde bij **Routes** > **Bestemming**> **0.0.0.0/0**. De Doelwaarde onderscheidt het type route en zal ofwel beginnen met de tekenreeks `igw-` of `nat-`.
    - Om routetabellen bij te werken, gaat u naar **VPC** > **Subnetten** > [subnet_naam] > **Routetabel** > **Routetabelkoppeling bewerken**.

Beveiligingsgroepen configureren

De VPC-wizard maakt één beveiligingsgroep die u niet zult gebruiken. Maak de volgende beveiligingsgroepen (**Beveiligingsgroepen** > **Beveiligingsgroep maken**). De EC2-hosts

worden in deze groepen geïnstalleerd in twee beschikbaarheidszones, zoals weergegeven in het bovenstaande diagram met afbeeldingen.

- Maak een nieuwe beveiligingsgroep: **Privé**. Hier worden alle vier de knooppunten van Tableau Server geïnstalleerd. Later in het installatieproces wordt de beveiligingsgroep Privé gekoppeld aan de subnetten 10.0.30.0/24 en 10.0.31.0/24.
- Maak een nieuwe beveiligingsgroep: **Openbaar**. Hier worden proxyservers geïnstalleerd. Later in het installatieproces wordt de beveiligingsgroep Openbaar gekoppeld aan de subnetten 10.0.1.0/24 en 10.0.2.0/24.
- Maak een nieuwe beveiligingsgroep: **Data**. Hier wordt de externe Tableau-opslagplaats van PostgreSQL geïnstalleerd. Later in het installatieproces wordt de beveiligingsgroep Data gekoppeld aan het subnet 10.0.50.0/24 (en optioneel 10.0.51.0/24).
- Maak een nieuwe beveiligingsgroep: **Bastion**. Hier installeert u de bastionhost. Later in het installatieproces wordt de beveiligingsgroep Bastion gekoppeld aan het subnet 10.0.0.0/24.

Geef inkomende en uitgaande regels op

In AWS zijn beveiligingsgroepen te vergelijken met firewalls in een on-premises omgeving. U moet het type verkeer (bijv. http, https, enz.), het protocol (TCP of UDP) en de poorten of het poortbereik (bijv. 80, 443, enz.) opgeven die de beveiligingsgroep mogen in- en/of uitgaan. Voor elk protocol moet u ook het bestemmings- of bronverkeer opgeven.

Regels voor beveiligingsgroep Openbaar

Inkomende regels			
Type	**Protocol**	**Poortbereik**	**Bron**
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	Beveiligingsgroep Bastion

Uitgaande regels

Type	Protocol	Poortbereik	Bestemming
Alle verkeer	Alle	Alle	0.0.0.0/0

Regels voor beveiligingsgroep Privé

De beveiligingsgroep Privé bevat een inkomende regel om HTTP-verkeer van de beveiligingsgroep Openbaar toe te staan. Sta HTTP-verkeer alleen toe tijdens het implementatieproces om de connectiviteit te verifiëren. Wij raden u aan de regel voor inkomend HTTP-verkeer te verwijderen nadat u de reverse-proxy hebt geïmplementeerd en SSL voor Tableau hebt geconfigureerd.

Inkomende regels			
Type	**Protocol**	**Poortbereik**	**Bron**
HTTP	TCP	80	Beveiligingsgroep Openbaar
HTTPS	TCP	443	Beveiligingsgroep Openbaar
PostgreSQL	TCP	5432	Beveiligingsgroep Data
SSH	TCP	22	Beveiligingsgroep Bastion
Alle verkeer	Alle	Alle	Beveiligingsgroep Privé

Uitgaande regel			
Type	**Protocol**	**Poortbereik**	**Bestemming**
Alle verkeer	Alle	Alle	0.0.0.0/0
PostgreSQL	TCP	5432	Beveiligingsgroep Data
SSH	TCP	22	Beveiligingsgroep Bastion

Regels voor beveiligingsgroep Data

Inkomende regels			
Type	**Protocol**	**Poortbereik**	**Bron**
PostgreSQL	TCP	5432	Beveiligingsgroep Privé
SSH	TCP	22	Beveiligingsgroep Bastion

Uitgaande regels			
Type	**Protocol**	**Poortbereik**	**Bestemming**
Alle verkeer	Alle	Alle	0.0.0.0/0
PostgreSQL	TCP	5432	Beveiligingsgroep Privé
SSH	TCP	22	Beveiligingsgroep Bastion

Regels voor beveiligingsgroep Bastion

Inkomende regels			
Type	**Protocol**	**Poortbereik**	**Bron**
SSH	TCP	22	Het IP-adres en netmasker van de computer waarmee u zich aanmeldt bij AWS (beheerderscomputer).
SSH	TCP	22	Beveiligingsgroep Privé
SSH	TCP	22	Beveiligingsgroep Openbaar

Uitgaande regels

Type	Protocol	Poortbereik	Bestemming
SSH	TCP	22	Het IP-adres en netmasker van de computer waarmee u zich aanmeldt bij AWS (beheerderscomputer).
SSH	TCP	22	Beveiligingsgroep Privé
SSH	TCP	22	Beveiligingsgroep Openbaar
SSH	TCP	22	Beveiligingsgroep Data
HTTPS	TCP	443	0.0.0.0/0 (Optioneel: maak deze regel als u toegang tot internet nodig hebt om ondersteunende software op de bastionhost te downloaden)

Automatisch toewijzen van openbare IP-adressen inschakelen

Hiermee krijgt u een IP-adres waarmee u verbinding kunt maken met de proxyservers en de bastionhost.

Voor subnetten Openbaar en Bastion:

1. Selecteer het subnet.
2. Selecteer onder het menu **Acties** Instellingen voor automatisch toewijzen van IP-adressen wijzigen.
3. Klik op Automatisch toewijzen van openbare IPv4-adressen inschakelen.
4. Klik op **Opslaan**.

Loadbalancer

Opmerking: Als u in AWS installeert en de voorbeeldimplementatie in deze gids volgt, moet u de AWS-loadbalancer later in het implementatieproces installeren en configureren, zoals beschreven in Deel 5 - Weblaag configureren.

Voor on-premises implementaties werkt u samen met uw netwerkbeheerders om loadbalancers te implementeren ter ondersteuning van de weblaag van de referentiearchitectuur:

- Een webgerichte toepassings-loadbalancer die HTTPS-verzoeken van Tableau-clients accepteert en communiceert met de reverse-proxyservers.
- Reverse-proxy:
  - Wij adviseren minimaal twee proxyservers voor redundantie en om de belasting van de client te verwerken.
  - Ontvangt HTTPS-verkeer van loadbalancer.
  - Ondersteunt sticky session naar Tableau-host.
  - Configureert een proxy voor round robin loadbalancing voor elke Tableau Server waarop het Gateway-proces wordt uitgevoerd.
  - Verwerkt verificatieverzoeken van externe IdP.
- Forward-proxy: Tableau Server vereist toegang tot internet voor licenties en kaartfunctionaliteit. Afhankelijk van uw forward-proxy-omgeving moet u mogelijk forward-proxy-toelatingslijsten configureren voor Tableau-service-URL's. Zie *Communiceren met internet* (Linux).

Hostcomputers configureren

Minimaal aanbevolen hardware

De volgende aanbevelingen zijn gebaseerd op onze tests van echte data in de referentiearchitectuur.

Toepassingsservers:

- CPU: 8 fysieke kernen (16vCPU's)
- RAM: 128 GB (16 GB/fysieke kern)
- Schijfruimte: 100 GB

Dataservers

- CPU: 8 fysieke kernen (16vCPU's)
- RAM: 128 GB (16 GB/fysieke kern)
- Schijfruimte: 1 TB. Als uw implementatie gebruikmaakt van externe opslag voor het Tableau Bestandsarchief, moet u de juiste schijfruimte berekenen. Zie *Tableau Server installeren met extern bestandsarchief* (Linux).

Proxyservers

- CPU: 2 fysieke kernen (4vCPU's)
- RAM: 8 GB (4 GB/fysieke kern)
- Schijfruimte: 100 GB

Externe opslagplaats-database

- CPU: 8 fysieke kernen (16vCPU's)
- RAM: 128 GB (16 GB/fysieke kern)
- De benodigde schijfruimte is afhankelijk van de hoeveelheid data die u verzamelt en de gevolgen hiervan voor de back-up. Zie de sectie *Back-up- en herstelprocessen* in het onderwerp *Vereisten voor schijfruimte* (Linux).

Directorystructuur

De referentiearchitectuur beveelt aan om het Tableau Server-pakket en de data te installeren op niet-standaardlocaties:

- Pakket installeren op: `/app/tableau_server`. Maak dit directorypad voordat u het Tableau Server-pakket installeert en geef dit pad vervolgens op tijdens de installatie.
- Installeer Tableau-data op: `/data/tableau_data`. Maak deze directory niet aan voordat u Tableau Server installeert. In plaats daarvan moet u het pad opgeven tijdens de installatie. Tableau Setup zal vervolgens het pad maken en de juiste machtigingen toekennen.

Zie Het installatiepakket uitvoeren en TSM initialiseren voor implementatiedetails.

Voorbeeld: hostcomputers installeren en voorbereiden in AWS

In deze sectie wordt uitgelegd hoe u EC2-hosts installeert voor elk servertype in de Tableau Server-referentiearchitectuur.

De referentiearchitectuur vereist acht hosts:

- Vier instanties voor Tableau Server
- Twee instanties voor proxyservers (Apache)
- Eén instantie voor bastionhost
- Eén of twee EC2 PostgreSQL-database-instanties

Details voor host-instantie

Installeer de hostcomputers volgens de onderstaande details.

Tableau Server

- Amazon Linux 2
- Instantietype: m5a.8xlarge
- Beveiligingsgroep-ID: Privé
- Opslag: EBS, 150 GiB, gp2-volumetype. Als uw implementatie gebruikmaakt van externe opslag voor het Tableau Bestandsarchief, moet u de juiste schijfruimte berekenen. Zie *Tableau Server installeren met extern bestandsarchief* (Linux).
- Netwerk: installeer twee EC2-hosts in elk privé-subnet (10.0.30.0/24 en 10.0.31.0/24).
- Kopieer de nieuwste onderhoudsverklaring van het rpm-pakket van Tableau Server 2021.2 (of later) van Tableau-downloadpagina naar elke Tableau-host.

Bastionhost

- Amazon Linux 2
- Instantietype: t3.micro
- Beveiligingsgroep-ID: Bastion

- Opslag: EBS, 50 GiB, gp2-volumetype
- Netwerk: subnet Bastion 10.0.0.0/24

Onafhankelijke gateway van Tableau Server

- Amazon Linux 2
- Instantietype: t3.xlarge
- Beveiligingsgroep-ID: Openbaar
- Opslag: EBS, 100 GiB, gp2-volumetype
- Netwerk: installeer één EC2-instantie in elk openbaar subnet (10.0.1.0/24 en 10.0.2.0/24)

PostgreSQL EC2-host

- Amazon Linux 2
- Instantietype: r5.4xlarge
- Beveiligingsgroep-ID: Data
- Opslag: De benodigde schijfruimte is afhankelijk van de hoeveelheid data die u verzamelt en de gevolgen hiervan voor de back-up. Zie de sectie *Back-up- en herstelprocessen* in het onderwerp *Vereisten voor schijfruimte* (Linux).
- Netwerk: subnet Data 10.0.50.0/24. (Als u PostgreSQL in een hoge beschikbaarheidscluster repliceert, installeert u de tweede host in het subnet 10.0.51.0/24.)

Verificatie: VPC-connectiviteit

Nadat u de hostcomputers hebt geïnstalleerd, controleert u de netwerkconfiguratie. Controleer de connectiviteit tussen de hosts door verbinding te maken via SSH vanaf de host in de beveiligingsgroep Bastion naar de hosts in elk subnet.

Voorbeeld: verbinding maken met bastionhost in AWS

1. Stel uw beheerderscomputer in voor ssh-agent. Hierdoor kunt u verbinding maken met hosts in AWS zonder dat u uw privésleutelbestand op EC2-instanties hoeft te plaatsen.

   Om ssh-agent op een Mac te configureren, voert u de volgende opdracht uit:

`ssh-add -K myPrivateKey.pem` of, voor het nieuwste Mac OS, `ssh-add --apple-use-keychain myPrivateKey.pem`

Voor Windows, zie het onderwerp Veilig verbinding maken met Linux-instanties die in een privé Amazon VPC worden uitgevoerd.

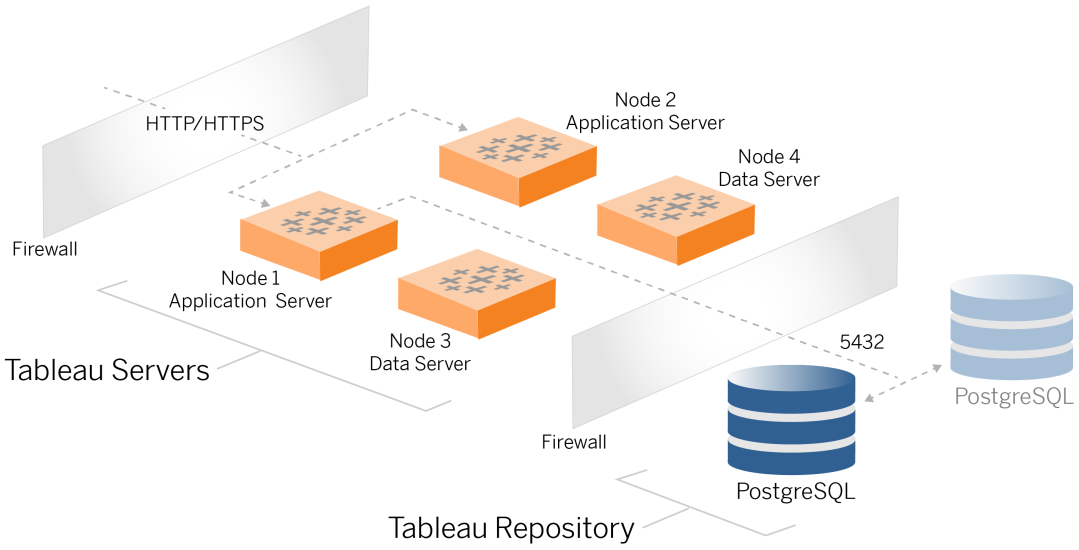
2. Maak verbinding met de bastionhost door de volgende opdracht uit te voeren:

   ```
   ssh -A ec2-user@<public-IP>
   ```

3. U kunt vervolgens verbinding maken met andere hosts in de VPC vanaf de bastionhost, met behulp van het privé-IP-adres, bijvoorbeeld:

   ```
   ssh -A ec2-user@10.0.1.93
   ```

Deel 4 - Tableau Server installeren en configureren



In dit onderwerp wordt beschreven hoe u de installatie en configuratie van de basis-implementatie van Tableau Server voltooit. De procedure wordt uiteengezet aan de hand van het voorbeeld voor de AWS- en Linux-referentiearchitectuur.

De Linux-voorbeelden in deze installatieprocedures tonen opdrachten voor RHEL-achtige distributies. De hier gebruikte opdrachten zijn specifiek ontwikkeld met de Amazon Linux 2-distributie. Als u de Ubuntu-distributie gebruikt, moet u de opdrachten dienovereenkomstig bewerken.

Voordat u begint

U moet uw omgeving voorbereiden en valideren zoals beschreven in Deel 3 – De implementatie van Tableau Server Enterprise voorbereiden.

PostgreSQL installeren, configureren en tarren

Deze PostgreSQL-instantie host de externe opslagplaats voor de Tableau Server-implementatie. U moet PostgreSQL installeren en configureren voordat u Tableau installeert.

U kunt PostgreSQL uitvoeren op Amazon RDS of op een EC2-instantie. Zie *Externe opslagplaats Tableau Server* (Linux) voor meer informatie over de verschillen tussen het uitvoeren van de opslagplaats op RDS en een EC2-instantie.

De onderstaande procedure laat zien hoe u Postgres op een Amazon EC2-instantie installeert en configureert. Het hier getoonde voorbeeld is een algemene installatie en configuratie voor PostgreSQL in de referentiearchitectuur. Uw DBA moet de PostgreSQL-implementatie optimaliseren op basis van de omvang van de data en prestatiebehoeften.

Vereisten: houd er rekening mee dat u PostgreSQL 1.6 moet gebruiken en dat u de module uuid-ossp moet installeren.

PostgreSQL-revisiegeschiedenis

U moet compatibele hoofdversies van PostgreSQL installeren voor de externe opslagplaats van Tableau Server. Daarnaast moeten ook kleinere versies aan minimumvereisten voldoen.

Tableau Server-versies	**Minimaal compatibele versies van PostgreSQL**
2021.2.3 - 2021.2.8 2021.3.0 - 2021.3.7 2021.4.0 - 2021.4.3	12.6
2021.2.10 - 2021.2.14 2021.3.8 - 2021.3.13 2021.4.4 - 2021.4.8	12.8
2021.2.15 - 2021.2.16	12.10

2021.3.14 - 2021.3.15 2021.4.9 - 2021.4.10	
2021.2.17 - 2021.2.18 2021.3.16 - 2021.3.17 2021.4.11 - 2021.4.12	12.11
2021.3.26 2021.4.23	12.15
2022.1.0	13.3
2022.1.1 - 2022.1.3	13.4
2022.1.4 - 2022.1.6	13.6
2022.1.7 - 2022.1.16 2022.3.0 - 2022.3.7 2023.1.0 - 2023.1.4	13.7
2022.1.17 - 2022.1.19 2022.3.8 - 2022.3.19 2023.1.5 - 2023.1.15 2023.3.0 - 2023.3.8	13.11
2022.3.20 - 2022.3.x 2023.1.16 - 2023.1.x 2023.3.9 - 2023.3.x	13.14
2024,0: 2024.x	15.6

PostgreSQL installeren

Deze voorbeeldinstallatieprocedure beschrijft hoe u PostgreSQL versie 13.6 installeert.

Meld u aan bij de EC2-host die u in het vorige deel hebt gemaakt.

1. Voer een update uit om de nieuwste oplossingen voor het Linux-besturingssysteem toe te passen:

   ```
   sudo yum update
   ```

2. Maak en bewerk het bestand pgdg.repo. in het pad `/etc/yum.repos.d/`. Vul het bestand met de volgende configuratiedata:

   ```
   [pgdg13]
   name=PostgreSQL 13 for RHEL/CentOS 7 - x86_64
   baseur-
   l=https://download.postgresql.org/pub/repos/yum/13/redhat/rhel-
   7-x86_64
   enabled=1
   gpgcheck=0
   ```

3. Installeer Postgres 13.6:

   ```
   sudo yum install postgresql13-server-13.6-1PGDG.rhel7.x86_64
   ```

4. Installeer de uuid-ossp module:

   ```
   sudo yum install postgresql13-contrib-13.6-1PGDG.rhel7.x86_64
   ```

5. Initialiseer Postgres:

   ```
   sudo /usr/pgsql-13/bin/postgresql-13-setup initdb
   ```

Postgres configureren

Rond de basisinstallatie af door Postgres te configureren:

1. Werk het configuratiebestand pg_hba `/var/lib/pgsql/13/data/pg_hba.conf` bij met de volgende twee zinnen. Elke zin moet het masker bevatten van de subnetten waarop uw Tableau-servers worden uitgevoerd:

   ```
   host all all 10.0.30.0/24 password

   host all all 10.0.31.0/24 password
   ```

2. Werk het PostgreSQL-bestand `/var/lib/pgsql/13/data/postgresql.conf` bij door deze zin toe te voegen:

   ```
   listen_addresses = '*'
   ```

3. Configureer om Postgres te starten bij opnieuw opstarten:

   ```
   sudo systemctl enable --now postgresql-13
   ```

4. Stel het wachtwoord voor de supergebruiker in:

   ```
   sudo su - postgres

   psql -c "alter user postgres with password 'StrongPassword'"
   ```

   > **Opmerking**: Stel een sterk wachtwoord in. Gebruik dus niet `'StrongPassword'` zoals in het voorbeeld hierboven.

   ```
   exit
   ```

5. Postgres opnieuw starten:

   ```
   sudo systemctl restart postgresql-13
   ```

Tar-back-up van PostgreSQL Stap 1 maken

Maak een tar-back-up van de PostgreSQL-configuratie. Door een tar-momentopname van de huidige configuratie te maken, bespaart u tijd als u tijdens de implementatie fouten

tegenkomt.

We noemen dit de back-up van Stap 1.

Op de PostgreSQL-host:

1. Zet de Postgres-database-instantie stop:

   ```
   sudo systemctl stop postgresql-13
   ```

2. Voer de volgende opdrachten uit om de tar-back-up te maken:

   ```
   sudo su
   cd /var/lib/pgsql
   tar -cvf step1.13.bkp.tar 13
   exit
   ```

3. Start de Postgres-database:

   ```
   sudo systemctl start postgresql-13
   ```

Herstel Stap 1

Ga terug naar stap 1 als het eerste knooppunt van Tableau Server tijdens de installatie uitvalt.

1. Voer op de computer waarop Tableau draait het vernietigingsscript uit om Tableau Server volledig van de host te verwijderen:

   ```
   sudo /app/tableau_server/packages/scripts.<version_code>/./-
   tableau-server-obliterate -a -y -y -y -l
   ```

2. Herstel de tar van PostgreSQL Stap 1. Voer de volgende opdrachten uit op de computer waarop Postgres draait:

   ```
   sudo su
   systemctl stop postgresql-13
   ```

```
cd /var/lib/pgsql

tar  -xvf step1.13.bkp.tar

systemctl start postgresql-13

exit
```

Hervat het installatieproces van het eerste knooppunt van Tableau Server.

Voor de installatie

Als u Tableau implementeert volgens de voorbeeldimplementatie van AWS/Linux die in deze gids wordt beschreven, kunt u mogelijk het geautomatiseerde installatiescript TabDeploy4EDG uitvoeren. Met het script TabDeploy4EDG wordt de voorbeeldinstallatie van de Tableau-implementatie met vier knooppunten geautomatiseerd. Deze implementatie wordt beschreven in de volgende procedures. Zie Bijlage – AWS Deployment Toolbox.

Het eerste knooppunt van Tableau Server installeren

Deze procedure beschrijft hoe u het eerste knooppunt van Tableau Server installeert zoals gedefinieerd door de referentiearchitectuur. Met uitzondering van de pakketinstallatie en de initialisatie van TSM, maakt de hier weergegeven procedure waar mogelijk gebruik van de TSM-opdrachtregel. Naast het feit dat TSM CLI platformonafhankelijk is, zorgt het gebruik ervan voor een naadloze installatie in gevirtualiseerde en headless omgevingen.

Het installatiepakket uitvoeren en TSM initialiseren

Meld u aan bij de hostserver van Knooppunt 1.

1. Voer een update uit om de nieuwste oplossingen voor het Linux-besturingssysteem toe te passen:

   ```
   sudo yum update
   ```

2. Kopieer het installatiepakket van Tableau-downloadpagina naar de hostcomputer waarop Tableau Server wordt uitgevoerd.

   Voer bijvoorbeeld op een computer met een Linux RHEL-achtig besturingssysteem het volgende uit:

   ```
   wget htt-
   ps://downloads.tableau.com/esdalt/2022<version>/tableau-server-
   <version>.rpm
   ```

   waarbij `<version>` het releasenummer is.

3. Download en installeer afhankelijkheden:

   ```
   sudo yum deplist tableau-server-<version>.rpm | awk '/pro-
   vider:/ {print $2}' | sort -u | xargs sudo yum -y install
   ```

4. Maak het pad `/app/tableau_server` aan in de hoofddirectory:

   ```
   sudo mkdir -p /app/tableau_server
   ```

5. Voer het installatieprogramma uit en geef het installatiepad `/app/tableau_server` op. Voer bijvoorbeeld op een Linux RHEL-achtig besturingssysteem het volgende uit:

   ```
   sudo rpm -i --prefix /app/tableau_server tableau-server-<ver-
   sion>.x86_64.rpm
   ```

6. Wijzig naar de directory `/app/tableau_server/packages/scripts.<version_code>/` en voer het `initialize-tsm`-script dat zich daar bevindt uit:

   ```
   sudo ./initialize-tsm -d /data/tableau_data --accepteula
   ```

7. Nadat de initialisatie is voltooid, verlaat u de shell:

   ```
   exit
   ```

Tableau Server activeren en registreren

1. Meld u aan bij de hostserver van Knooppunt 1.
2. Geef in deze stap de productcode(s) van Tableau Server op. Voer de volgende opdracht uit voor elke licentiesleutel die u hebt gekocht:

   ```
   tsm licenses activate -k <product key>
   ```

3. Maak een json-registratiebestand met de notatie zoals hier getoond:

   ```
   {
   "zip" : "97403",
   "country" : "USA",
   "city" : "Springfield",
   "last_name" : "Simpson",
   "industry" : "Energy",
   "eula" : "yes",
   "title" : "Safety Inspection Engineer",
   "company_employees" : "100",
   "phone" : "5558675309",
   "company" : "Example",
   "state" : "OR",
   "opt_in" : "true",
   "department" : "Engineering",
   "first_name" : "Homer",
   "email" : "homer@example.com"
   }
   ```

4. Nadat u de wijzigingen in het bestand hebt opgeslagen, geeft u dit door met de optie `--file` om Tableau Server te registreren:

   ```
   tsm register --file path_to_registration_file.json
   ```

Het identiteitenarchief configureren

Opmerking: Als uw implementatie gebruikmaakt van externe opslag voor het Tableau Bestandsarchief, moet u het Externe bestandsarchief inschakelen voordat u het identiteitenarchief configureert. Zie *Tableau Server installeren met extern bestandsarchief* (Linux).

De standaard referentiearchitectuur maakt gebruik van een lokaal identiteitenarchief. Configureer de initiële host met een lokaal identiteitenarchief door middel van het bestand `config.json` met de opdracht `tsm settings import`.

Importeer het bestand `config.json` volgens uw besturingssysteem:

Het bestand `config.json` is opgenomen in het directorypad scripts.<versie> (bijvoorbeeld `scripts.20204.21.0217.1203`), en is geformatteerd om het identiteitenarchief te configureren.

Om het bestand `config.json` te importeren, voert u de volgende opdracht uit:

```
tsm settings import -f /app/tableau_ser-
ver/packages/scripts.<version_code>/config.json
```

Externe Postgres configureren

1. Maak een extern database-json-bestand met de volgende configuratie-instellingen:

```
{
"flavor":"generic",
"masterUsername":"postgres",
"host":"<instance ip address>",
"port":5432
}
```

2. Nadat u de wijzigingen in het bestand hebt opgeslagen, zet u het bestand door met de volgende opdracht:

   ```
   tsm topology external-services repository enable -f <file-name>.json --no-ssl
   ```

   U wordt gevraagd om het wachtwoord van de primaire Postgres-gebruikersnaam.

   Met de optie `--no-ssl` configureert u Tableau om SSL/TLS alleen te gebruiken wanneer de Postgres-server is geconfigureerd voor SSL/TLS. Als Postgres niet is geconfigureerd voor SSL/TLS, is de verbinding niet versleuteld. Deel 6 - Configuratie na de installatie beschrijft hoe u SSL/TLS voor de Postgres-verbinding kunt inschakelen nadat u de eerste fase van de implementatie hebt voltooid.

3. Pas de wijzigingen toe.

   Voer deze opdracht uit om de wijzigingen toe te passen en Tableau Server opnieuw te starten:

   ```
   tsm pending-changes apply
   ```

4. Verwijder het configuratiebestand dat u in stap 1 hebt gebruikt.

De installatie van Knooppunt 1 afronden

1. Nadat u Tableau Server hebt geïnstalleerd, moet u de server initialiseren.

   Voer de volgende opdracht uit:

   ```
   tsm initialize --start-server --request-timeout 1800
   ```

2. Wanneer de initialisatie is voltooid, moet u een Tableau Server-beheerdersaccount maken.

   In tegenstelling tot het computeraccount dat u gebruikt om TSM-besturingssysteemcomponenten te installeren en beheren, is het Tableau Server-beheerdersaccount een toepassingsaccount dat wordt gebruikt voor het maken van Tableau

Server-gebruikers, -projecten en -sites. De Tableau Server-beheerder past ook machtigingen toe op Tableau-resources. Voer de volgende opdracht uit om het initiële beheerdersaccount aan te maken. In het volgende voorbeeld wordt de gebruiker `tableau-admin` genoemd:

```
tabcmd initialuser --server http://localhost --
username "tableau-admin"
```

Tabcmd vraagt u om een wachtwoord voor deze gebruiker in te stellen.

Verificatie: configuratie van Knooppunt 1

1. Voer de volgende opdracht uit om te controleren of de TSM-services actief zijn:

   ```
   tsm status -v
   ```

   Tableau zou het volgende moeten retourneren:

   ```
   external:
   Status: RUNNING
   'Tableau Server Repository 0' is running (Active Repository).
   node1: localhost
   Status: RUNNING
   'Tableau Server Gateway 0' is running.
   'Tableau Server Application Server 0' is running.
   'Tableau Server Interactive Microservice Container 0' is run-
   ning.
   'MessageBus Microservice 0' is running.
   'Relationship Query Microservice 0' is running.
   'Tableau Server VizQL Server 0' is running.
   ...
   ```

   Alle services worden vermeld.

2. Voer de volgende opdracht uit om te controleren of de beheerderssite van Tableau actief is:

   ```
   curl localhost
   ```

De eerste paar regels zouden Vizportal-html moeten weergeven, vergelijkbaar met:

```
<!DOCTYPE html>
<html xmlns:ng="" xmlns:tb="">
<head ng-csp>
<meta charset="UTF-8">
<meta http-equiv="X-UA-Compatible" content="IE=edge">
<meta name="viewport" content="initial-scale=1, maximum-sca-
le=2, width=device-width, height=device-height, viewport-fit-
t=cover">
<meta name="format-detection" content="telephone=no">
<meta name="vizportal-config ...
```

Tar-back-ups van Stap 2 maken

Nadat u de eerste installatie hebt geverifieerd, maakt u twee tar-back-ups:

- PostgreSQL
- Tableau eerste knooppunt (Knooppunt 1)

In de meeste gevallen kunt u de installatie van het eerste knooppunt terugzetten door deze tar-bestanden te herstellen. Het herstellen van de tar-bestanden gaat veel sneller dan het opnieuw installeren en initialiseren van het eerste knooppunt.

Tar-bestanden van Stap 2 maken

1. Stop Tableau op het eerste knooppunt van Tableau:

   ```
   tsm stop
   ```

   Wacht tot Tableau stopt voordat u doorgaat naar de volgende stap.

2. Stop de PostgreSQL-database-instantie op de PostgreSQL-host:

```
sudo systemctl stop postgresql-13
```

3. Voer de volgende opdrachten uit om de tar-back-up te maken:

   ```
   sudo su

   cd /var/lib/pgsql

   tar -cvf step2.13.bkp.tar 13

   exit
   ```

4. Controleer of het Postgres-tar-bestand is gemaakt met root-machtigingen:

   ```
   sudo ls -al /var/lib/pgsql
   ```

5. Stop de Tableau-beheerservices op de Tableau-host:

   ```
   sudo /app/tableau_server/packages/scripts.<version_
   code>/./stop-administrative-services
   ```

6. Voer de volgende opdrachten uit om de tar-back-up te maken:

   ```
   cd /data

   sudo tar -cvf step2.tableau_data.bkp.tar tableau_data
   ```

7. Start de Postgres-database op de Postgres-host:

   ```
   sudo systemctl start postgresql-13
   ```

8. Start Tableau-beheerservices:

   ```
   sudo /app/tableau_server/packages/scripts.<version_
   code>/./start-administrative-services
   ```

9. Voer de opdracht `tsm status` uit om de TSM-status te controleren voordat u opnieuw opstart.

   In de meeste gevallen retourneert de opdracht eerst de status GEDEGRADEERD of FOUT. Wacht een paar minuten en voer de opdracht dan opnieuw uit. Als de status

FOUT of GEDEGRADEERD wordt geretourneerd, wacht u nog wat langer. Probeer TSM niet te starten voordat de status GESTOPT wordt geretourneerd. Voer vervolgens de volgende opdracht uit:

```
tsm start
```

Herstel Stap 2

Met dit proces worden Tableau Knooppunt 1 en de Postgres-instantie teruggezet naar Stap 2. Nadat u deze stap hebt hersteld, kunt u de resterende Tableau Knooppunten opnieuw implementeren.

1. Stop de tsm-services op de eerste Tableau-host (Knooppunt 1):

   ```
   tsm stop
   ```

2. Stop de beheerservices van Tableau op alle knooppunten van de Tableau Server-implementatie. Voer de volgende opdracht uit op elk knooppunt, in de juiste volgorde (Knooppunt 1, Knooppunt 2 en vervolgens Knooppunt 3):

   ```
   sudo /app/tableau_server/packages/scripts.<version_
   code>/./stop-administrative-services
   ```

3. Nadat de Tableau-services zijn gestopt, herstelt u de PostgreSQL-tar van Stap 2. Voer de volgende opdrachten uit op de computer waarop Postgres draait:

   - ```
     sudo su

     systemctl stop postgresql-13

     cd /var/lib/pgsql

     tar  -xvf step2.13.bkp.tar

     systemctl start postgresql-13

     exit
     ```
     ```

4. Herstel de Tableau-tar van Stap 2. Voer de volgende opdrachten uit op de initiële Tableau-host:

   ```
   cd /data

   sudo rm -rf tableau_data

   sudo tar  -xvf step2.tableau_data.bkp.tar
   ```

5. Verwijder de volgende bestanden op de Tableau Knooppunt 1-computer:

   - `sudo rm /data/tableau_data/-data/tabsvc/appzookeeper/0/version-2/currentEpoch`
   - `sudo rm /data/tableau_data/-data/tabsvc/appzookeeper/0/version-2/acceptedEpoch`
   - `sudo rm /data/tableau_data/-data/tabsvc/tabadminagent/0/servicestate.json`

6. Start de Tableau-beheerservices:

   ```
   sudo /app/tableau_server/packages/scripts.<version_
   code>/./start-administrative-services
   ```

7. Laad de Tableau systmctl-bestanden opnieuw en voer vervolgens `start-administrative-services` opnieuw uit:

   ```
   sudo su -l tableau -c "systemctl --user daemon-reload"

   sudo /app/tableau_server/packages/scripts.<version_
   code>/./start-administrative-services
   ```

8. Voer op Knooppunt 1 de opdracht `tsm status` uit om de TSM-status te controleren voordat u opnieuw opstart.

   In sommige gevallen krijgt u een foutmelding `Cannot connect to server...` Deze fout treedt op omdat de tabadmincontroller-service niet opnieuw is opgestart. Blijf

`tsm status` met tussenpozen uitvoeren. Als deze fout na 10 minuten niet verdwijnt, voer dan de opdracht `start-administrative-services` opnieuw uit.

U moet even wachten en dan retourneert de opdracht `tsm status` de status GEDEGRADEERD en vervolgens FOUT. Start TSM pas als de status GESTOPT wordt geretourneerd. Voer vervolgens de volgende opdracht uit:

```
tsm start
```

Hervat het installatieproces om Tableau Server op de resterende knooppunten te installeren.

Tableau Server op de resterende knooppunten installeren

Kopieer het Tableau-installatieprogramma naar elk knooppunt om de implementatie voort te zetten.

Overzicht van knooppuntconfiguratie

In deze sectie wordt het proces voor het configureren van Knooppunten 2 tot 4 beschreven. In de volgende secties vindt u gedetailleerde configuratie- en validatieprocedures voor elke stap.

Voor de installatie van Tableau Server Knooppunten 2 tot 4 moet u tijdens de installatie van het knooppunt een bootstrap-bestand genereren, kopiëren en eraan refereren.

Om het bootstrap-bestand te genereren, voert u een TSM-opdracht uit op het eerste knooppunt. Vervolgens kopieert u het bootstrap-bestand naar het doelknooppunt, waar u het uitvoert als onderdeel van de knooppuntinitialisatie.

De volgende json-inhoud toont een voorbeeld van een bootstrap-bestand. (De certificaat- en cryptogerelateerde waarden zijn afgekapt om het voorbeeldbestand beter leesbaar te maken.)

```
{
"initialBootstrapSettings" : {
       "certificate" : "-----BEGIN CERTIFICATE-----\r\...=\r\n-----END
CERTIFICATE-----",
       "port" : 8850,
       "configurationName" : "tabsvc",
       "clusterId" : "tabsvc-clusterid",
       "cryptoKeyStore" : "zs7OzgAAAAIAAAABAAAAA...w==",
       "toksCryptoKeystore" : "LS0tLS1CRUdJTiBUT00tLS0tCjM5MDBh...L",
       "sessionCookieMaxAge" : 7200,
       "nodeId" : "node1",
       "machineAddress" : "ip-10-0-1-93.us-west-1.compute.internal",
       "cryptoEnabled" : true,
       "sessionCookieUser" : "tsm-bootstrap-user",
       "sessionCookieValue" : "eyJjdH-
kiOiJKV1QiLCJlbmMiOiJBMTI4Q0JDLUhQ...",
       "sessionCookieName" : "AUTH_COOKIE"
       }
}
```

Het bootstrap-bestand bevat verbindingsgebaseerde validatie om Knooppunt 1 te verifiëren en creëert een versleuteld kanaal voor het bootstrap-proces. De bootstrap-sessie is tijdsgebonden en het configureren en valideren van knooppunten kost veel tijd. Houd er rekening mee dat u nieuwe bootstraps moet maken en kopiëren terwijl u de knooppunten configureert.

Nadat u het bootstrap-bestand hebt uitgevoerd, meldt u zich aan bij het eerste Tableau Server-knooppunt en configureert u de processen voor het nieuwe knooppunt. Wanneer u klaar bent met het configureren van de knooppunten, moet u de wijzigingen toepassen en het eerste knooppunt opnieuw opstarten. Het nieuwe knooppunt is geconfigureerd en gestart. Naarmate u meer knooppunten toevoegt, duurt het langer om de configuratie en het opnieuw opstarten van de implementatie te voltooien.

De Linux-voorbeelden in deze installatieprocedures tonen opdrachten voor RHEL-achtige distributies. Als u de Ubuntu-distributie gebruikt, moet u de opdrachten dienovereenkomstig bewerken.

1. Voer een update uit om de nieuwste oplossingen voor het Linux-besturingssysteem toe te passen:

   ```
   sudo yum update
   ```

2. Download en installeer afhankelijkheden:

   ```
   sudo yum deplist tableau-server-<version>.rpm | awk '/pro-
   vider:/ {print $2}' | sort -u | xargs sudo yum -y install
   ```

3. Maak het pad `/app/tableau_server` aan in de hoofddirectory:

   ```
   sudo mkdir -p /app/tableau_server
   ```

4. Voer het installatieprogramma uit en geef het installatiepad `/app/tableau_server` op. Voer bijvoorbeeld op een Linux RHEL-achtig besturingssysteem het volgende uit:

   ```
   sudo rpm -i --prefix /app/tableau_server tableau-server-<ver-
   sion>.x86_64.rpm
   ```

Het bootstrap-bestand genereren, kopiëren en gebruiken om TSM te initialiseren

De volgende procedure laat zien hoe u een bootstrap-bestand genereert, kopieert en gebruikt bij het initialiseren van TSM op een ander knooppunt. In dit voorbeeld heet het bootstrap-bestand `boot.json`.

In dit voorbeeld draaien de hostcomputers op AWS, terwijl de EC2-hosts op Amazon Linux 2 draaien.

1. Maak verbinding met het eerste knooppunt (Knooppunt 1) en voer de volgende opdracht uit:

   ```
   tsm topology nodes get-bootstrap-file --file boot.json
   ```

2. Kopieer het bootstrap-bestand naar Knooppunt 2.

   ```
   scp boot.json ec2-user@10.0.31.83:/home/ec2-user/
   ```

3. Maak verbinding met Knooppunt 2 en schakel over naar de scriptsdirectory van Tableau Server:

   ```
   cd /app/tableau_server/packages/scripts.<version_number>
   ```

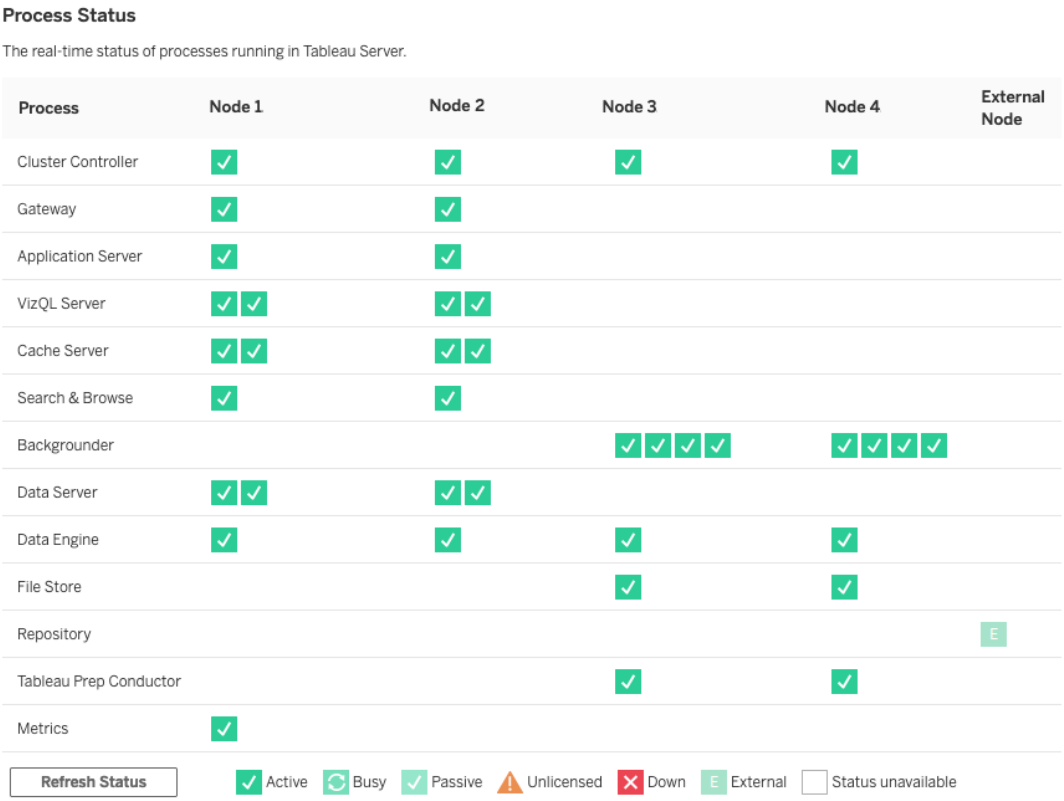
4. Voer de opdracht `initialize-tsm` uit en refereer aan het bootstrap-bestand:

   ```
   sudo ./initialize-tsm -d /data/tableau_data -b /home/ec2-user/-
   boot.json --accepteula
   ```

5. Nadat `initialize-tsm` is voltooid, verwijdert u `boot.json` en sluit vervolgens de sessie af of log uit.

Processen configureren

U moet het Tableau Server-cluster configureren op het knooppunt waarop de Tableau Server - Beheercontroller (TSM-controller) draait. De TSM-controller draait op het eerste knooppunt.



Knooppunt 2 configureren

1. Nadat u TSM hebt geïnitialiseerd met behulp van het bootstrap-bestand op Knooppunt 2, meldt u zich aan bij het eerste knooppunt.

2. Op het eerste knooppunt (`node1`) voert u de volgende opdrachten uit om processen op Knooppunt 2 te configureren:

```
tsm topology set-process -n node2 -pr clustercontroller -c 1
tsm topology set-process -n node2 -pr gateway -c 1
tsm topology set-process -n node2 -pr vizportal -c 1
tsm topology set-process -n node2 -pr vizqlserver -c 2
tsm topology set-process -n node2 -pr cacheserver -c 2
tsm topology set-process -n node2 -pr searchserver -c 1
tsm topology set-process -n node2 -pr dataserver -c 2
```

```
tsm topology set-process -n node2 -pr clientfileservice -c 1
tsm topology set-process -n node2 -pr tdsservice -c 1
tsm topology set-process -n node2 -pr collections -c 1
tsm topology set-process -n node2 -pr contentexploration -c 1
```

Als u versie 2022.1 of hoger installeert, voegt u ook de Indexerings- en zoekserver toe:

```
tsm topology set-process -n node2 -pr indexandsearchserver -c 1
```

Als u versie 2023.3 of hoger installeert, voegt u alleen de Indexerings- en zoekserver toe. Voeg de service Zoeken en bladeren (zoekserver) niet toe.

3. Controleer de configuratie voordat u deze toepast. Voer de volgende opdracht uit:

   ```
   tsm pending-changes list
   ```

4. Nadat u hebt gecontroleerd of uw wijzigingen in de lijst met in behandeling zijnde services staan (er staan ook andere services in de lijst met in behandeling zijnde services), past u de wijzigingen toe:

   ```
   tsm pending-changes apply
   ```

   De wijzigingen vereisen een herstart. Het configureren en opnieuw opstarten kan enige tijd duren.

5. Controleer de configuratie van Knooppunt 2. Voer de volgende opdracht uit:

   ```
   tsm status -v
   ```

Knooppunt 3 configureren

Initialiseer TSM met behulp van het bootstrap-proces op Knooppunt 3 en voer vervolgens de `tsm topology set-process`-opdrachten hieronder uit.

Elke keer dat u een proces instelt, wordt er een Coördinatieservicewaarschuwing weergegeven. U kunt deze waarschuwing negeren terwijl u de processen instelt.

1. Nadat u TSM hebt geïnitialiseerd met behulp van het bootstrap-bestand op Knooppunt 3, meldt u zich aan bij het eerste knooppunt (`node1`) en voert u de volgende opdrachten uit om de processen te configureren:

   ```
   tsm topology set-process -n node3 -pr clustercontroller -c 1
   tsm topology set-process -n node3 -pr clientfileservice -c 1
   tsm topology set-process -n node3 -pr backgrounder -c 4
   tsm topology set-process -n node3 -pr filestore -c 1
   ```

   Als u versie 2022.1 of hoger installeert, voegt u ook de Indexerings- en zoekserver toe:

   ```
   tsm topology set-process -n node3 -pr indexandsearchserver -c 1
   ```

2. Controleer de configuratie voordat u deze toepast. Voer de volgende opdracht uit:

   ```
   tsm pending-changes list
   ```

3. Nadat u hebt gecontroleerd of uw wijzigingen in de lijst met in behandeling zijnde services staan (er staan ook andere services in de lijst die automatisch worden geconfigureerd), past u de wijzigingen toe:

   ```
   tsm pending-changes apply --ignore-warnings
   ```

   De wijzigingen vereisen een herstart. Het configureren en opnieuw opstarten kan enige tijd duren.

4. Verifieer de configuratie door de volgende opdracht uit te voeren:

   ```
   tsm status -v
   ```

Coördinatieservice-ensemble implementeren op Knooppunten 1 tot 3

Voor een standaard referentiearchitectuur-implementatie met vier knooppunten voert u de volgende procedure uit:

1. Voer de volgende opdrachten uit op Knooppunt 1:

   ```
   tsm stop
   tsm topology deploy-coordination-service -n node1,node2,node3
   ```

   Het proces omvat een herstart van TSM, wat enige tijd in beslag zal nemen.

2. Nadat de coördinatieservice is geïmplementeerd, start u TSM:

   ```
   tsm start
   ```

Tar-back-ups van Stap 3 maken

Nadat u de installatie hebt geverifieerd, maakt u vier tar-back-ups:

- PostgreSQL
- Tableau eerste knooppunt (Knooppunt 1)
- Tableau-knooppunt 2
- Tableau-knooppunt 3

Tar-bestanden van Stap 3 maken

1. Stop Tableau op het eerste knooppunt van Tableau:

   ```
   tsm stop
   ```

2. Nadat TSM is gestopt, stopt u de beheerservices van Tableau op elk knooppunt. Voer de volgende opdracht uit op elk knooppunt, in de juiste volgorde (Knooppunt 1, Knooppunt 2 en vervolgens Knooppunt 3):

   ```
   sudo /app/tableau_server/packages/scripts.<version_
   code>/./stop-administrative-services
   ```

3. Stop de PostgreSQL-database-instantie op de PostgreSQL-host:

```
sudo systemctl stop postgresql-12
```

4. Voer de volgende opdrachten uit om de tar-back-up te maken:

   ```
   sudo su

   cd /var/lib/pgsql

   tar -cvf step3.12.bkp.tar 12

   exit
   ```

5. Controleer of het Postgres-tar-bestand is gemaakt met root-machtigingen:

   ```
   sudo ls -al /var/lib/pgsql
   ```

6. Start de Postgres-database op de Postgres-host:

   ```
   sudo systemctl start postgresql-12
   ```

7. Maak de tar-back-up op Knooppunt 1, Knooppunt 2 en Knooppunt 3. Voer de volgende opdrachten uit op elk knooppunt:

   - `cd /data`

     ```
     sudo tar -cvf step3.tableau_data.bkp.tar tableau_data
     ```

   - Controleer of het Tableau-tar-bestand is gemaakt met root-machtigingen:

     ```
     ls -al
     ```

8. Start Tableau-beheerservices op elk knooppunt, in de juiste volgorde (Knooppunt 1, Knooppunt 2 en vervolgens Knooppunt 3):

   ```
   sudo /app/tableau_server/packages/scripts.<version_
   code>/./start-administrative-services
   ```

9. Voer de opdracht `tsm status` uit om de TSM-status te controleren voordat u opnieuw opstart.

In de meeste gevallen retourneert de opdracht de status GEDEGRADEERD en daarna FOUT. Wacht even en voer de opdracht dan opnieuw uit. Als de status FOUT of GEDEGRADEERD wordt geretourneerd, wacht u nog wat langer. Probeer TSM niet te starten voordat de status GESTOPT wordt geretourneerd. Voer vervolgens de volgende opdracht uit:

```
tsm start
```

Herstel Stap 3

Dit proces herstelt Tableau Knooppunt 1, Knooppunt 2 en Knooppunt 3. Het herstelt ook het Postgres-exemplaar naar Stap 3. Nadat u deze stap hebt hersteld, kunt u de coördinatieservice, Knooppunt 4 en de definitieve knooppuntconfiguraties implementeren.

1. Stop de tsm-service op de eerste Tableau-host (Knooppunt 1):

   ```
   tsm stop
   ```

2. Nadat TSM is gestopt, stopt u de beheerservices van Tableau op Knooppunt 1, Knooppunt 2 en Knooppunt 3. Voer de volgende opdracht uit op elk knooppunt:

   ```
   sudo /app/tableau_server/packages/scripts.<version_
   code>/./stop-administrative-services
   ```

3. Herstel de PostgreSQL-tar van Stap 3. Voer de volgende opdrachten uit op de computer waarop Postgres draait:

   ```
   sudo su

   systemctl stop postgresql-12

   cd /var/lib/pgsql

   tar -xvf step3.12.bkp.tar

   systemctl start postgresql-12
   ```

```
exit
```

4. Herstel de Tableau-tar van Stap 3 op Knooppunt 1, Knooppunt 2 en Knooppunt 3. Voer de volgende opdrachten uit op elk Tableau-knooppunt:

   ```
   cd /data
   ```

   ```
   sudo rm -rf tableau_data
   ```

   ```
   sudo tar  -xvf step3.tableau_data.bkp.tar
   ```

5. Verwijder de volgende bestanden op de Tableau Knooppunt 1-computer:

   - `sudo rm /data/tableau_data/-data/tabsvc/appzookeeper/1/version-2/currentEpoch`
   - `sudo rm /data/tableau_data/-data/tabsvc/appzookeeper/1/version-2/acceptedEpoch`
   - `sudo rm /data/tableau_data/-data/tabsvc/tabadminagent/0/servicestate.json`

   Als de shell de foutmelding Bestand niet gevonden retourneert, moet u mogelijk de naam van het pad wijzigen om het nummer `<n>` te verhogen in deze sectie van het pad: `.../appzookeeper/<n>/version-2/....`

6. Start de beheerservices op Knooppunt 1, Knooppunt 2 en Knooppunt 3 opnieuw. Voer de volgende opdrachten uit op elk knooppunt:

   ```
   sudo /app/tableau_server/packages/scripts.<version_
   code>/./start-administrative-services
   ```

   ```
   sudo su -l tableau -c "systemctl --user daemon-reload"
   ```

   ```
   sudo /app/tableau_server/packages/scripts.<version_
   code>/./start-administrative-services
   ```

7. Voer op Knooppunt 1 de opdracht `tsm status` uit om de TSM-status te controleren voordat u opnieuw opstart.

In sommige gevallen krijgt u een foutmelding `Cannot connect to server...`. Deze fout treedt op omdat de tabadmincontroller-service niet opnieuw is opgestart. Blijf `tsm status` met tussenpozen uitvoeren. Als deze fout na 10 minuten niet verdwijnt, voer dan de opdracht `start-administrative-services` opnieuw uit.

U moet even wachten en dan retourneert de opdracht `tsm status` de status GEDEGRADEERD en vervolgens FOUT. Start TSM pas als de status GESTOPT is geretourneerd. Voer vervolgens de volgende opdracht uit:

```
tsm start
```

Hervat het installatieproces om de coördinatieservice op Knooppunten 1 tot 3 te implementeren.

Knooppunt 4 configureren

Het proces voor het configureren van Knooppunt 4 is hetzelfde als voor Knooppunt 3.

Stel dezelfde processen in als die u voor Knooppunt 3 hebt ingesteld, voer dezelfde reeks opdrachten uit als hierboven, maar geef `node4` op in de opdrachten in plaats van `node3`.

Net als bij de verificatie van Knooppunt 3, verifieert u de configuratie van Knooppunt 4 door `tsm status -v` uit te voeren.

Voordat u verdergaat, wacht u tot het Bestandsarchief-proces op Knooppunt 4 klaar is met synchroniseren. De status van de Bestandsarchief-service zal `is synchronizing` retourneren totdat het proces klaar is. Wanneer de status van de Bestandsarchief-service `is running` retourneert, kunt u doorgaan.

Definitieve procesconfiguratie en -verificatie

De laatste stap in het procesconfiguratieproces is het verwijderen van redundante processen uit Knooppunt 1.

1. Maak verbinding met het eerste knooppunt (`node1`).

2. Schakel het bestandsarchief op Knooppunt 1 uit. Dit zal een waarschuwing veroorzaken over het verwijderen van het bestandsarchief van een controller die zich op dezelfde locatie bevindt. U kunt de waarschuwing negeren. Voer de volgende opdracht uit:

   ```
   tsm topology filestore decommission -n node1
   ```

3. Wanneer het bestandsarchief buiten gebruik is, voert u de volgende opdracht uit om het achtergrondproces van Knooppunt 1 te verwijderen:

   ```
   tsm topology set-process -n node1 -pr backgrounder -c 0
   ```

4. Controleer de configuratie voordat u deze toepast. Voer de volgende opdracht uit:

   ```
   tsm pending-changes list
   ```

5. Nadat u hebt gecontroleerd of uw wijzigingen in de lijst met in behandeling zijnde wijzigingen staan, past u de wijzigingen toe:

   ```
   tsm pending-changes apply
   ```

   De wijzigingen vereisen een herstart. Het configureren en opnieuw opstarten kan enige tijd duren.

6. Controleer de configuratie:

   ```
   tsm status -v.
   ```

   Voordat u verdergaat, wacht u tot het Bestandsarchief-proces op Knooppunt 4 klaar is met synchroniseren. De status van de Bestandsarchief-service zal `is synchronizing` retourneren totdat het proces klaar is. Wanneer de status van de Bestandsarchief-service `is running` retourneert, kunt u doorgaan.

Back-up uitvoeren

Voor een volledig herstel van Tableau Server is een back-upportfolio nodig dat uit drie componenten bestaat:

- Een back-upbestand van de opslagplaats en de data van het bestandsarchief. Dit bestand wordt gegenereerd door de opdracht `tsm maintenance backup`.
- Een exportbestand met topologie en configuratie. Dit bestand wordt gegenereerd door de opdracht `tsm settings export`.
- Verificatiecertificaat, sleutel en keytab-bestanden.

Zie het Tableau Server-onderwerp *Een volledige back-up maken van Tableau Server en Tableau Server herstellen* (Linux) voor een volledige beschrijving van het back-up- en herstelproces.

In deze fase van uw implementatie worden alle relevante bestanden en assets die nodig zijn voor een volledig herstel opgenomen door de opdrachten `tsm maintenance backup` en `tsm settings export` uit te voeren.

1. Voer de volgende opdracht uit om de configuratie- en topologie-instellingen te exporteren naar een bestand met de naam `ts_settings_backup.json`.

   ```
   tsm settings export -f ts_settings_backup.json
   ```

2. Voer de volgende opdracht uit om een back-up te maken van de opslagplaats en de data van het bestandsarchief in een bestand met de naam `ts_backup-<yyyy-mm-dd>.tsbak`. Negeer de waarschuwing dat het bestandsarchief zich niet op het controller-knooppunt bevindt.

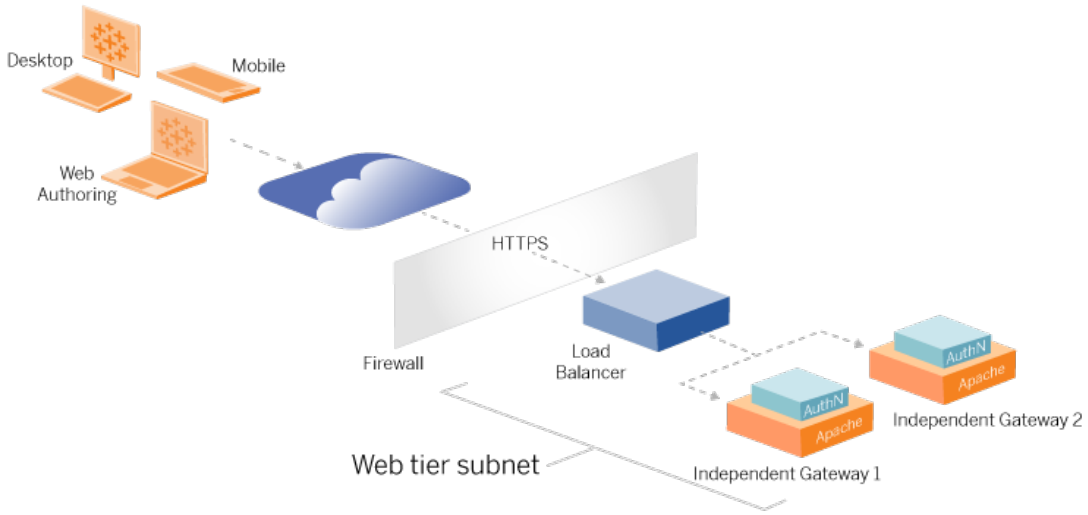
   ```
   tsm maintenance backup -f ts_backup -d --skip-compression
   ```

   Locatie van back-upbestand:

   ```
   /data/tableau_data/data/tabsvc/files/backups/
   ```

3. Kopieer beide bestanden en sla ze op een ander opslagmiddel op dat niet wordt gedeeld met uw Tableau Server-implementatie.

Deel 5 - Weblaag configureren



De weblaag van de referentiearchitectuur moet de volgende componenten bevatten:

- Een webgerichte Load Balancer voor de toepassing die HTTPS-verzoeken van Tableau-clients accepteert en communiceert met de reverse proxyservers.
- Reverse proxy:
  - Wij raden aan om de onafhankelijke gateway van Tableau Server te implementeren.
  - Wij adviseren minimaal twee proxyservers voor redundantie en om de belasting van de client te verwerken.
  - Ontvangt HTTPS-verkeer van Load Balancer.
  - Ondersteunt sticky sessie naar Tableau-host.
  - Configureer een proxy voor Round Robin Load Balancing voor elke Tableau Server waarop het gatewayproces wordt uitgevoerd.
  - Verwerkt verificatieverzoeken van externe IdP.
- Forward proxy: Tableau Server vereist toegang tot internet voor licenties en kaartfunctionaliteit. U moet veilige lijsten voor forward proxy's configureren voor URL's van Tableau-services. Zien *Communiceren met internet* (Linux).

- Al het clientgerelateerde verkeer kan worden gecodeerd via HTTPS:
  - Client-naar-toepassing Load Balancer
  - Toepassings-Load Balancer voor reverse proxyservers
  - Proxyserver naar Tableau Server
  - Verificatiehandler die op een reverse proxy naar IdP draait
  - Tableau Server naar IdP

De onafhankelijke gateway van Tableau Server

Tableau Server versie 2022.1 introduceerde de onafhankelijke gateway van Tableau Server. De onafhankelijke gateway is een zelfstandige instantie van het Tableau-gatewayproces dat fungeert als een Tableau-bewuste reverse proxy.

De onafhankelijke gateway ondersteunt eenvoudige Round Robin Load Balancing naar de backend Tableau Servers. De onafhankelijke gateway is echter niet bedoeld om te fungeren als Load Balancer voor Enterprise-toepassingen. Wij adviseren om de onafhankelijke gateway achter een Load Balancer voor toepassingen van Enterprise-klasse te gebruiken.

Voor de onafhankelijke gateway is een Advanced Management-licentie nodig.

Verificatie en autorisatie

De standaardreferentiearchitectuur specificeert dat Tableau Server wordt geïnstalleerd met geconfigureerde lokale verificatie. In dit model moeten clients verbinding maken met Tableau Server om te worden geverifieerd via het lokale verificatieproces van Tableau Server. Wij raden af om deze verificatiemethode te gebruiken in de referentiearchitectuur, omdat het scenario vereist dat niet-geverifieerde clients communiceren met de toepassingslaag, wat een beveiligingsrisico vormt.

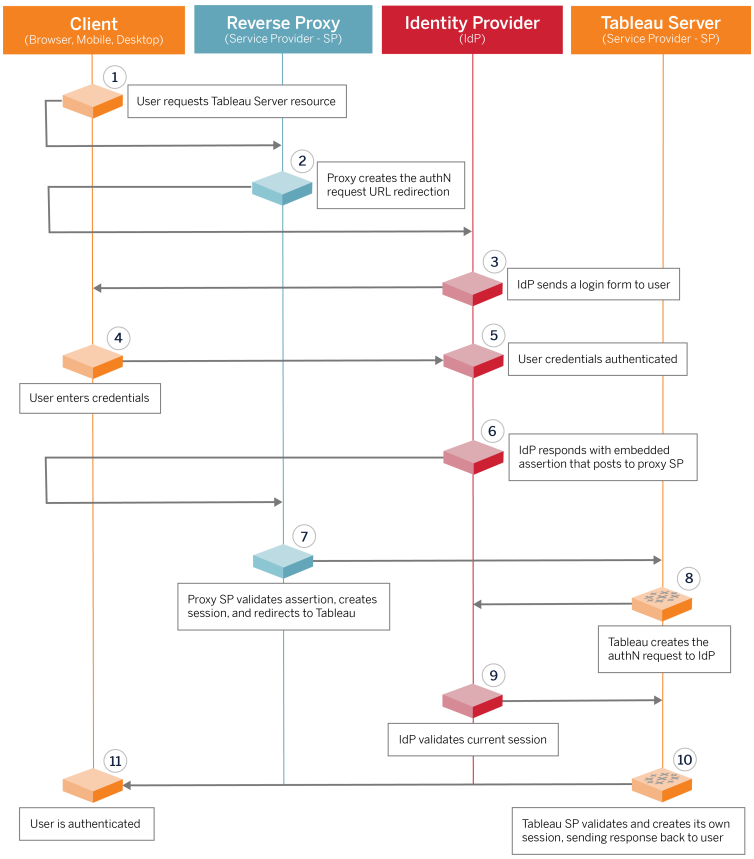
In plaats daarvan raden we aan om een externe identiteitsprovider op Enterprise-niveau te configureren in combinatie met een AuthN-module om al het verkeer naar de toepassingslaag vooraf te verifiëren. Wanneer geconfigureerd met een externe IdP, wordt het native lokale verificatieproces van Tableau Server niet gebruikt. Tableau Server autoriseert toegang tot bronnen in de implementatie nadat de IdP de gebruikers heeft geverifieerd.

Pre-verificatie met een AuthN-module

In het voorbeeld in deze handleiding is SAML SSO geconfigureerd, maar het pre-verificatieproces kan worden geconfigureerd met de meeste externe identiteitsproviders en een AuthN-module.

In de referentiearchitectuur is de reverse proxy geconfigureerd om een clientverificatiesessie met de IdP te maken voordat de aanvragen via een proxy naar Tableau Server worden verzonden. Wij noemen dit proces de *pre-auth*-fase. De reverse proxy leidt alleen geverifieerde clientsessies om naar Tableau Server. Tableau Server maakt vervolgens een sessie aan, verifieert de verificatie van de sessie bij de IdP en retourneert vervolgens de clientaanvraag.

In het onderstaande diagram staan de stappens van het pre-auth- en verificatieproces met een geconfigureerde AuthN-module. De reverse proxy kan een generieke oplossing van derden zijn of de onafhankelijke gateway van Tableau Server:



Configuratieoverzicht

Dit is een overzicht van het proces voor het configureren van de weblaag. Controleer de connectiviteit na elke stap:

1. Configureer twee reverse proxy's om HTTP-toegang tot Tableau Server te bieden.
2. Configureer logica voor Load Balancing met sticky sessies op proxyservers om verbinding te maken met elke Tableau Server-instantie waarop het gatewayproces wordt uitgevoerd.
3. Configureer Load Balancing voor de toepassing met sticky-sessies bij de internetgateway om verzoeken door te sturen naar de reverse proxyservers.
4. Configureer verificatie met een externe IdP. U kunt SSO of SAML configureren door een verificatiehandler te installeren op de reverse proxyservers. De AuthN-module beheert de verificatiehandshake tussen de externe IdP en uw Tableau-implementatie. Tableau fungeert ook als een IdP-serviceprovider en verifieert gebruikers bij de IdP.
5. Om in deze implementatie te kunnen verifiëren met Tableau Desktop, moeten uw clients Tableau Desktop 2021.2.1 of hoger gebruiken.

Voorbeeld van weblaagconfiguratie met de onafhankelijke gateway van Tableau Server

In de rest van dit onderwerp vindt u een end-to-endprocedure waarin wordt beschreven hoe u een weblaag implementeert in de voorbeeld-AWS-referentiearchitectuur met behulp van de onafhankelijke gateway van Tableau Server. Voor een voorbeeldconfiguratie met Apache als reverse proxy, zie Bijlage - Voorbeeldimplementatie van weblaag met Apache.

De voorbeeldconfiguratie bestaat uit de volgende componenten:

- AWS-toepassing Load Balancer
- De onafhankelijke gateway van Tableau Server
- Mellon-verificatiemodule
- Okta IdP
- SAML-verificatie

> **Opmerking**: het voorbeeld van de weblaagconfiguratie dat in deze sectie wordt gepresenteerd, bevat gedetailleerde procedures voor het implementeren van software en services van derden. We hebben ons uiterste best gedaan om de procedures voor het weblaagscenario te verifiëren en te documenteren. De software van derden kan echter veranderen of uw scenario kan afwijken van de hier beschreven referentiearchitectuur. Raadpleeg de documentatie van derden voor betrouwbare configuratiegegevens en ondersteuning.

De Linux-voorbeelden in deze sectie tonen opdrachten voor RHEL-achtige distributies. De opdrachten hier zijn specifiek ontwikkeld met de Amazon Linux 2-distributie. Als u de Ubuntu-distributie gebruikt, moet u de opdrachten dienovereenkomstig bewerken.

Het implementeren van de weblaag in dit voorbeeld verloopt volgens een stapsgewijze configuratie- en verificatieprocedure. De kernconfiguratie van de weblaag bestaat uit de volgende stappen om HTTP tussen Tableau en internet in te schakelen. De onafhankelijke gateway wordt uitgevoerd en geconfigureerd voor reverse proxy/Load Balancing achter de AWS-toepassing Load Balancer:

1. Omgeving voorbereiden
2. Installeer de onafhankelijke gateway
3. Configureer de onafhankelijke gatewayserver
4. Configureer de AWS-toepassing Load Balancer

Nadat de weblaag is ingesteld en de connectiviteit met Tableau is geverifieerd, configureert u de verificatie met een externe provider.

Omgeving voorbereiden

Voer de volgende taken uit voordat u de onafhankelijke gateway implementeert.

1. Wijzigingen in de AWS-beveiligingsgroep. Configureer de beveiligingsgroep Public (Openbaar) om binnenkomend de onafhankelijke gateway housekeeping-verkeer (TCP

21319) van de beveiligingsgroep Private (Privé) toe te staan.

2. Installeer versie 22.1.1 (of later) op een Tableau Server-cluster met vier knooppunten zoals beschreven in Deel 4 – Tableau Server installeren en configureren.

3. Configureer de twee proxy EC2-instanties in de openbare beveiligingsgroep zoals beschreven in Hostcomputers configureren.

Installeer de onafhankelijke gateway

Voor de onafhankelijke gateway van Tableau Server is een Advanced Management-licentie vereist.

De implementatie van de onafhankelijke gateway van Tableau Server bestaat uit het installeren en uitvoeren van het .rpm-pakket en vervolgens het configureren van de initiële status. In deze handleiding staat een procedure met richtlijnen voor implementatie in de referentiearchitectuur.

Wijkt uw implementatie af van de referentiearchitectuur? Raadpleeg de kerndocumentatie van Tableau Server, *Tableau Server installeren met onafhankelijke gateway* (Linux).

Belangrijk: de configuratie van de onafhankelijke gateway kan een foutgevoelig proces zijn. Het is erg lastig om configuratieproblemen op te lossen tussen twee instanties van onafhankelijke gateway-servers. Om deze reden raden wij aan om slechts één de onafhankelijke gateway-server tegelijk te configureren. Nadat u de eerste server hebt geconfigureerd en de functionaliteit hebt gecontroleerd, moet u de tweede onafhankelijke gateway-server configureren.

Hoewel u elke onafhankelijke gateway-server afzonderlijk configureert, moet u deze installatieprocedure uitvoeren op beide EC2-instanties die u in de openbare beveiligingsgroep hebt geïnstalleerd:

1. Voer een update uit om de nieuwste oplossingen voor het Linux-besturingssysteem toe te passen:

   ```
   sudo yum update
   ```

2. Hebt u Apache geïnstalleerd? Verwijder die dan:

   ```
   sudo yum remove httpd
   ```

3. Kopieer het installatiepakket van versie 2022.1.1 (of later) van de onafhankelijke gateway van Tableau Downloads-pagina naar de hostcomputer waarop Tableau Server wordt uitgevoerd.

   Voer bijvoorbeeld op een computer met een Linux RHEL-achtig besturingssysteem het volgende uit:

   ```
   wget https://downloads.tableau.com/esdalt/2022<version>/tableau-server-tsig-<version>.x86_64.rpm
   ```

4. Voer het installatieprogramma uit. Voer bijvoorbeeld op een Linux RHEL-achtig besturingssysteem het volgende uit:

   ```
   sudo yum install <tableau-tsig-version>.x86_64.rpm
   ```

5. Ga naar de `/opt/tableau/tableau_tsig/packages/scripts.<version_code>/` directory en voer het script `initialize-tsig` uit dat zich daar bevindt. Naast de `--accepteula`-vlag, moet u het IP-bereik opgeven van de subnetten waar de Tableau Server-implementatie wordt uitgevoerd. Gebruik de `-c`-optie om het IP-bereik op te geven. Zie onderstaande voorbeeldopdracht met de opgegeven voorbeeld-AWS-subnetten:

   ```
   sudo ./initialize-tsig --accepteula -c "ip 10.0.30.0/24 10.0.31.0/24"
   ```

6. Nadat de initialisatie is voltooid, opent u het bestand `tsighk-auth.conf` en kopieert u het verificatiegeheim in het bestand. U moet deze code voor elk van de onafhankelijke gateway-instanties indienen als onderdeel van de backend Tableau Server-configuratie:

   ```
   sudo less /var/opt/tableau/tableau_tsig/config/tsighk-auth.conf
   ```

7. Nadat u de voorgaande stappen op beide instanties van de onafhankelijke gateway hebt uitgevoerd, bereidt u het configuratiebestand `tsig.json` voor. Het configuratiebestand bestaat uit een independentGateways-array. In de matrix staan configuratieobjecten. Elk van de objecten definieert verbindingsdetails voor een onafhankelijke gateway-instantie.

   Kopieer de volgende JSON en pas deze aan op basis van uw implementatieomgeving. Zie hier een voorbeeld van een bestand voor een voorbeeld van een AWS-referentiearchitectuur.

   Het onderstaande JSON-voorbeeldbestand bevat alleen verbindingsgegevens voor één onafhankelijke gateway. Later in het proces voegt u de verbindingsgegevens voor de tweede onafhankelijke gateway-server toe.

   Sla het bestand op als `tsig.json` voor de procedures die volgen.

   ```
   {
   "independentGateways": [
    {
          "id": "ip-10-0-1-169.ec2.internal",
          "host": "ip-10-0-1-169.ec2.internal",
          "port": "21319",
          "protocol" : "http",
          "authsecret": "13660-27118-29070-25482-9518-22453"
          }]
    }
   ```

- `"id"` - De privé-DNS-naam van het AWS EC2-instantie waarop de onafhankelijke gateway wordt uitgevoerd.
- `"host"` - Hetzelfde als `"id"`.
- `"port"` - De housekeeping-poort is standaard `"21319"`.
- `"protocol"` - Het protocol voor clientverkeer. Laat dit op `http` staan voor de initiële configuratie.
- `"authsecret"` - Het geheim dat u in de vorige stap hebt gekopieerd.

Onafhankelijke gateway: directe vs. relayverbinding

Voordat u verdergaat, moet u beslissen welk verbindingsschema u in uw implementatie wilt configureren: een directe verbinding of een relayverbinding. Elke optie wordt hier kort beschreven, naast informatie die relevant is voor uw besluitvorming.

Relayverbinding: u kunt de onafhankelijke gateway configureren om clientcommunicatie via één poort door te geven aan het gatewayproces op Tableau Server. Wij noemen dit een *relayverbinding*:

- Het relayproces resulteert in een extra hop van de onafhankelijke gateway naar het backend Tableau Server-gatewayproces. Door de extra hop zijn de prestaties slechter in vergelijking met die bij de configuratie met directe verbinding.
- TLS wordt ondersteund in de relaymodus. Alle communicatie in de relaymodus is beperkt tot één enkel protocol (HTTP of HTTPS) en kan daarom worden gecodeerd en geverifieerd met TLS.

Directe verbinding: de onafhankelijke gateway kan rechtstreeks communiceren met de backendprocessen van Tableau Server via meerdere poorten. Wij verwijzen naar deze communicatie als *directe* verbinding:

- Omdat de verbinding rechtstreeks met de backend van Tableau Server verloopt, zijn de prestaties van de client aanzienlijk beter in vergelijking met die van bij de relayverbindingsoptie.
- Vereist het openen van 16 poorten van openbare naar privésubnetten voor directe procescommunicatie van de onafhankelijke gateway naar Tableau Server-computers.
- TLS wordt nog niet ondersteund voor de processen van de onafhankelijke gateway naar Tableau Server.

Relayverbinding configureren

Om TLS tussen Tableau Server en de onafhankelijke gateway uit te voeren, moet u een relay-verbinding configureren. De voorbeeldscenario's in de EDG zijn geconfigureerd met een relayverbinding.

1. Kopieer `tsig.json` naar knooppunt 1 van uw Tableau Server-implementatie.
2. Voer op knooppunt 1 de volgende opdrachten uit om de onafhankelijke gateway in te schakelen.

```
tsm stop
tsm configuration set -k gateway.tsig.proxy_tls_optional -v
none
tsm pending-changes apply
tsm topology external-services gateway enable -c tsig.json
tsm start
```

Directe verbinding configureren

Omdat directe verbindingen geen TLS ondersteunen, raden wij u aan om een directe verbinding alleen te configureren als u al het netwerkverkeer op andere manieren kunt beveiligen. Om TLS tussen Tableau Server en de onafhankelijke gateway uit te voeren, moet u een relayverbinding configureren. De voorbeeldscenario's in de EDG zijn geconfigureerd met een relayverbinding.

Als u de onafhankelijke gateway configureert voor directe verbinding met Tableau Server, moet u de configuratie inschakelen om communicatie te activeren. Nadat Tableau Server met de onafhankelijke gateway communiceert, worden de protocoldoelen vastgesteld. U moet dan de `proxy_targets.csv` van de onafhankelijke gateway-computer halen en de overeenkomstige poorten van de openbare naar de privébeveiligingsgroepen in AWS openen.

1. Kopieer `tsig.json` naar knooppunt 1 van uw Tableau Server-implementatie.

2. Voer op knooppunt 1 de volgende opdrachten uit om de onafhankelijke gateway in te schakelen.

   ```
   tsm stop
   tsm topology external-services gateway enable -c tsig.json
   tsm start
   ```

3. Voer op de onafhankelijke gateway-computer de volgende opdracht uit om de poorten te bekijken die de Tableau Server-cluster gebruikt:

   ```
   less /var/opt/tableau/tableau_tsig/config/httpd/proxy_targets.csv
   ```

4. Configureer AWS-beveiligingsgroepen. Voeg de TCP-poorten toe die in `proxy_targets.csv` staan om communicatie van de openbare beveiligingsgroep naar de privébeveiligingsgroep mogelijk te maken.

   Wij raden aan de poortingangsconfiguratie te automatiseren, omdat de poorten kunnen veranderen als de Tableau Server-implementatie verandert. Als u knooppunten toevoegt of processen opnieuw configureert in de Tableau Server-implementatie, leidt dit tot wijzigingen in de poorttoegang die de onafhankelijke gateway vereist.

Verificatie: basistopologieconfiguratie

U zou toegang moeten kunnen krijgen tot de beheerpagina van Tableau Server door te surfen naar `http://<gateway-public-IP-address>`.

Wordt de aanmeldingspagina van Tableau Server niet geladen of start Tableau Server niet? Volg deze stappen voor probleemoplossing:

Netwerk:

- Controleer de connectiviteit tussen de Tableau-implementatie en de onafhankelijke gateway-instantie door de volgende `wget`- opdracht vanaf Tableau Server-knooppunt 1 uit te voeren: wget http://<intern IP-adres of de onafhankelijke gateway>:21319,

bijvoorbeeld:

```
wget http://ip-10-0-1-38:21319
```

Als de verbinding wordt geweigerd of mislukt, controleer dan of de openbare beveiligingsgroep is geconfigureerd om onafhankelijke gateway housekeeping-verkeer (TCP 21319) van de privébeveiligingsgroep toe te staan.

Als de beveiligingsgroep correct is geconfigureerd, controleer dan of u de juiste IP-adressen of IP-bereiken hebt opgegeven tijdens de initialisatie van de onafhankelijke gateway. U kunt deze configuratie bekijken en wijzigen in het bestand `environment.bash` in `/etc/opt/tableau/tableau_tsig/environment.bash`. Als u een wijziging aanbrengt in dit bestand, start dan de tsig-http-service opnieuw op zoals hieronder beschreven wordt.

Op de Proxy 1-host:

1. Overschrijf het httpd.conf-bestand met het onafhankelijke gateway-stubbestand:

   ```
   cp /var/opt/tableau/tableau_tsig/config/httpd.conf.stub /var/opt/tableau/tableau_tsig/config/httpd.conf
   ```

2. Start tsig-httpd opnieuw op als eerste stap voor probleemoplossing:

   ```
   sudo su - tableau-tsig
   systemctl --user restart tsig-httpd
   exit
   ```

Op Tableau-knooppunt 1

- Controleer het `tsig.json`-bestand. Los eventuele fouten die u vindt op en voer vervolgens het programma `tsm topology external-services gateway update -c tsig.json` uit.
- Als u een directe verbinding gebruikt, controleer dan de TCP-poorten die in `proxy_targets.csv` zijn geconfigureerd als ingangspoorten van openbare naar privébeveiligingsgroepen.

Configureer de AWS-toepassing Load Balancer

Configureer de loadbalancer als een HTTP-listener. De procedure hier beschrijft hoe u een loadbalancer toevoegt in AWS.

Stap 1: Doelgroep maken

Een doelgroep is een AWS-configuratie die de EC2-instanties definieert waarop uw proxy-servers draaien. Dit zijn de doelen voor het verkeer van de LBS.

1. EC2 >**Target groups** (Doelgroepen) > **Create target group** (Doelgroep)
2. Doe het volgende op de pagina Create (Maken):
   - Voer een doelgroepnaam in, bijvoorbeeld `TG-internal-HTTP`.
   - Doeltype: instanties
   - Protocol: HTTP
   - Poort: 80
   - VPC: selecteer uw VPC.
   - Voeg de te lezen codelijst toe via **Health checks** (Statuscontroles) > **Advanced health checks settings** (Geavanceerde instellingen voor statuscontroles) > **Success codes** (Succescodes): `200,303`.
   - Klik op **Maken**.
3. Selecteer de doelgroep die u zojuist hebt gemaakt en klik vervolgens op het tabblad **Targets** (Doelen):
   - Klik op **Edit** (Bewerken).
   - Selecteer de EC2-instanties (of één instantie als u er één tegelijk configureert) waarop de proxytoepassing wordt uitgevoerd en klik vervolgens op **Toevoegen aan geregistreerd**.
   - Klik op **Opslaan**.

Stap 2: De loadbalancer-wizard starten

1. EC2> **Load Balancers** (Loadbalancers) > **Create Load Balancer** (Loadbalancer maken)
2. Maak op de pagina 'Select load balancer type' (Type loadbalancer selecteren) een toepassings-loadbalancer.

Opmerking: de gebruikersinterface die wordt weergegeven om de loadbalancer te configureren, is niet consistent in alle AWS-datacenters. De onderstaande procedure, 'Wizardconfiguratie', geeft aan welke instellingen moeten worden toegewezen in de AWS-configuratiewizard die begint met **Step 1 Configure Load Balancer** (Stap 1 Loadbalancer configureren).

Als uw datacenter alle configuraties weergeeft op één pagina met onderaan de knop **Create load balancer** (Loadbalancer maken), volgt u de onderstaande procedure 'Configuratie op één pagina'.

Wizardconfiguratie

1. Pagina **Configure load balancer** (Loadbalancer configureren):
    - Geef naam op.
    - Schema: internetgericht (standaard)
    - IP-adrestype: ipv4 (standaard)
    - Listeners (listeners en routering):
        a. Laat de standaard-HTTP-listener staan.
        b. Klik op **Add listener** (Luisteraar toevoegen) en voeg `HTTPS:443` toe.
    - VPC: selecteer de VPC waar u alles hebt geïnstalleerd.
    - Beschikbaarheidszones:
        - Selecteer **a** en **b** voor uw datacenterregio's.
        - Selecteer in elke corresponderende vervolgkeuzelijst het openbare subnet (waar uw proxyservers zich bevinden).

- Klik op **Configure Security Settings** (Beveiligingsinstellingen configureren).

2. Pagina **Configure Security Settings** (Beveiligingsinstellingen configureren)
   - Upload uw openbare SSL-certificaat.
   - Klik op **Next: Configure Security Groups** (Volgende stap: Beveiligingsgroepen configureren).
3. Pagina **Configure Security Groepen** (Beveiligingsinstellingen configureren):
   - Selecteer de openbare beveiligingsgroep (Public). Als de standaardbeveiligingsgroep (Default) is geselecteerd, wist u deze selectie.
   - Klik op **Next: Configure Routing** (Volgende stap: Routering configureren).
4. Pagina **Configure Routing** (Routering configureren)
   - Doelgroep: bestaande doelgroep.
   - Naam: selecteer de doelgroep die u eerder hebt gemaakt.
   - Klik op **Next: Register Targets** (Volgende stap: Doelen registreren).
5. Pagina **Register Targets** (Doelen registreren)
   - De twee proxyserverinstanties die u eerder hebt geconfigureerd, worden weergegeven.
   - Klik op **Next: Review** (Volgende stap: Controleren).
6. Pagina **Review** (Controleren)

   Klik op **Maken**.

Configuratie op één pagina

Basisconfiguratie

- Geef naam op.
- Schema: internetgericht (standaard)
- IP-adrestype: ipv4 (standaard)

Netwerktoewijzing

- VPC: selecteer de VPC waar u alles hebt geïnstalleerd.
- Toewijzingen:
  - Selecteer de beschikbaarheidszones **a** en **b** (of vergelijkbare beschikbaarheidszones) voor uw datacenterregio's.
  - Selecteer in elke corresponderende vervolgkeuzelijst het openbare subnet (waar uw proxyservers zich bevinden).

Beveiligingsgroepen

Selecteer de openbare beveiligingsgroep (Public). Als de standaardbeveiligingsgroep (Default) is geselecteerd, wist u deze selectie.

Listeners en routering

- Laat de standaard-HTTP-listener staan. Geef voor **Default action** (Standaardactie) de doelgroep op die u eerder hebt ingesteld.
- Klik op **Add listener** (Luisteraar toevoegen) en voeg `HTTPS:443` toe. Geef voor **Default action** (Standaardactie) de doelgroep op die u eerder hebt ingesteld.

Veilige listenerinstellingen

- Upload uw openbare SSL-certificaat.

Klik op **Create Load balancer** (Loadbalancer maken).

Stap 3: Stickiness inschakelen

1. Nadat u de loadbalancer hebt gemaakt, moet u 'stickiness' (sessieaffiniteit) inschakelen voor de doelgroep.
   - Open de AWS-pagina voor de doelgroep (**EC2**> **Load Balancing** (Taakverdeling) > **Target Groups** (Doelgroepen)) en selecteer de doelgroepinstantie die u zojuist hebt ingesteld. Selecteer in het menu **Action** (Actie) de optie **Edit attributes** (Attributen bewerken).
   - Selecteer op de pagina **Edit attributes** (Attributen bewerken) de optie **Stickiness** (sessieaffiniteit), geef een duur van `1 day` (1 dag) op en klik vervolgens op **Save changes** (Wijzigingen opslaan).

2. Schakel stickiness in voor de loadbalancer op de HTTP-listener. Selecteer de load-balancer die u zojuist hebt geconfigureerd en klik vervolgens op het tabblad **Listeners**:

    - Klik voor **HTTP:80** op **View/edit rules** (Regels weergeven/bewerken). Klik op de resulterende pagina **Rules** (Regels) op het bewerkingspictogram (eenmaal bovenaan de pagina en vervolgens nogmaals naast de regel) om de regel te bewerken. Verwijder de bestaande THEN-regel en vervang deze door op **Add action** (Actie toevoegen) > **Forward to...** (Doorsturen naar) te klikken. Specificeer in de hieruit voortvloeiende THEN-configuratie de doelgroep die u hebt gemaakt. Schakel Stickiness in onder Group-level stickiness (Sessieaffiniteit op groepsniveau) en stel de duur in op 1 dag. Sla de instelling op en klik vervolgens op **Update** (Bijwerken).

Stap 4: De time-out voor inactiviteit op de loadbalancer instellen

Werk de inactiviteitstime-out voor de loadbalancer bij naar 400 seconden.

Selecteer de loadbalancer die u voor deze implementatie hebt geconfigureerd en klik vervolgens op **Actions** (Acties) > **Edit attributes** (Kenmerken bewerken). Stel **Idle timeout** (Time-out inactiviteit) in op `400` seconden en klik op **Save** (Opslaan).

Stap 5: LBS-connectiviteit controleren

Open de AWS-pagina voor de doelgroep (**EC2**> **Load Balancers**) en selecteer de load-balancer-instantie die u zojuist hebt ingesteld.

Kopieer de DNS-naam onder **Description** (Beschrijving) en plak deze in een browser om toegang te krijgen tot de aanmeldingspagina van Tableau Server.

Als u een 500-niveaufout krijgt, moet u uw proxyservers mogelijk opnieuw opstarten.

DNS bijwerken met openbare Tableau-URL

Gebruik de DNS-zonenaam van uw domein uit de AWS Load Balancer-beschrijving om een CNAME-waarde in uw DNS te maken. Verkeer naar uw URL (tableau.example.com) moet naar de openbare DNS-naam van AWS worden verzonden.

Controleer de connectiviteit

Nadat uw DNS-updates zijn voltooid, zou u naar de aanmeldingspagina van Tableau Server moeten kunnen navigeren door uw openbare URL in te voeren, bijvoorbeeld: `https://tableau.example.com`.

Voorbeeld van verificatieconfiguratie: SAML met externe IdP

In het volgende voorbeeld wordt beschreven hoe u SAML instelt en configureert met Okta IdP en de Mellon-verificatiemodule voor een Tableau-implementatie die wordt uitgevoerd in de AWS-referentiearchitectuur.

In dit voorbeeld wordt voortgeborduurd op het vorige gedeelte. Er wordt ervan uitgegaan dat u één onafhankelijke gateway tegelijk configureert.

In het voorbeeld wordt beschreven hoe u Tableau Server en de onafhankelijke gateway via HTTP configureert. Okta stuurt een verzoek naar de AWS-Load Balancer via HTTPS, maar al het interne verkeer gaat via HTTP. Houd bij het configureren voor dit scenario rekening met de HTTP- en HTTPS-protocollen bij het instellen van URL-reeksen.

In dit voorbeeld wordt Mellon gebruikt als een serviceprovidermodule voor pre-verificatie op de onafhankelijke gateway-servers. Met deze configuratie kan alleen geverifieerd verkeer verbinding maken met Tableau Server, waarbij die ook fungeert als serviceprovider met de Okta IdP. Daarom moet u twee IdP-toepassingen configureren: één voor de Mellon-serviceprovider en één voor de Tableau-serviceprovider.

Een Tableau-beheerdersaccount maken

Een veelgemaakte fout bij het configureren van SAML is dat vóór inschakeling van SSO geen beheerdersaccount wordt gemaakt op Tableau Server.

De eerste stap is het maken van een account op Tableau Server met de rol van Serverbeheerder. Voor het Okta-voorbeeldscenario moet de gebruikersnaam een geldige e-mailadresnotatie hebben, bijvoorbeeld gebruiker@voorbeeld.com. U moet een wachtwoord voor deze gebruiker instellen, maar het wachtwoord wordt niet gebruikt nadat SAML is geconfigureerd.

Okta-toepassing voor voorafgaande verificatie configureren

Voor het end-to-end-scenario dat in deze sectie wordt beschreven, zijn twee Okta-toepassingen nodig:

- Okta-toepassing voor voorafgaande verificatie
- Tableau Server-toepassing van Okta

Elk van deze toepassingen is gekoppeld aan verschillende metadata die u respectievelijk op de reverse proxy en Tableau Server moet configureren.

In deze procedure wordt beschreven hoe u de Okta-toepassing voor voorafgaande verificatie maakt en configureert. Verderop in dit onderwerp gaat u de Tableau Server-toepassing van Okta maken. Zie de Okta Developer-webpagina (in het Engels) voor informatie over een gratis Okta-proefaccount met een beperkt aantal gebruikers.

Maak een SAML-app-integratie voor de Mellon-serviceprovider voor voorafgaande verificatie.

1. Open het Okta-beheerdashboard > **Applications** > **Create App Integration** (Toepassingen > App-integratie maken).
2. Selecteer op de pagina **Create a new app integration** (Nieuwe app-integratie maken) de optie **SAML 2.0** en klik dan op **Next** (Volgende).
3. Voer op het tabblad **General Settings** (Algemene instellingen) een app-naam in, bijvoorbeeld `Tableau Pre-Auth` en klik op **Next** (Volgende).
4. Doe het volgende op het tabblad **Configure SAML** (SAML configureren):

- URL voor eenmalige aanmelding (SSO). Het laatste element van het pad in de URL voor eenmalige aanmelding wordt aangeduid als `MellonEndpointPath` in het configuratiebestand `mellon.conf` dat verderop in deze procedure volgt. U kunt elk gewenst eindpunt opgeven. In dit voorbeeld is `sso` het eindpunt. Het laatste element, `postResponse`, is vereist: `https://tableau.example.com/sso/postResponse`.
- Schakel het selectievakje **Use this for Recipient URL and Destination URL** (Dit gebruiken voor ontvangers-URL en bestemmings-URL) uit.
- Recipient URL (Ontvangers-URL): Hetzelfde als de SSO-URL, maar met HTTP. Bijvoorbeeld `http://tableau.example.com/sso/postResponse`.
- Destination URL (Bestemmings-URL): hetzelfde als de SSO-URL, maar met HTTP. Bijvoorbeeld `http://tableau.example.com/sso/postResponse`.
- Audience URI (SP Entity ID) (Doelgroep-URI (SP-entiteits-ID). Bijvoorbeeld `https://tableau.example.com`.
- Name ID Format (Notatie van naam-ID): `EmailAddress`
- Application username (Toepassingsgebruikersnaam): `Email`
- Attributes Statements (Kenmerkinstructies): Name = `mail`; Name format (Naam-notatie)= `Unspecified`; Value (Waarde) = `user.email`.

Klik op **Next** (Volgende).

5. Selecteer op het tabblad **Feedback** het volgende:
   - **I'm an Okta customer adding an internal app (Ik ben een Okta-klant die een interne app toevoegt)**
   - **This is an internal app that we have created (Dit is een interne app die we hebben gemaakt)**
   - Klik op **Finish** (Voltooien).

6. Maak het IdP-metadatabestand voor voorafgaande verificatie:
   - In Okta: **Applications** > (Toepassingen) **Applications** > Uw nieuwe toepassing (bijv. `Tableau Pre-Auth`) > **Sign On** (Aanmelden)
   - Klik bij **SAML Signing Certificates** (SAML-ondertekeningscertificaten) op **View SAML setup instructions** (SAML-installatie-instructies weergeven).
   - Scroll op de pagina **How to Configure SAML 2.0 for <pre-auth> Application** (SAML 2.0 configureren voor<pre-auth>-toepassing) omlaag naar de sectie

Optional (Optioneel), **Provide the following IDP metadata to your SP provider** (de volgende IDP-metadata doorgeven aan uw SP-provider).
- Kopieer de inhoud van het XML-veld en sla deze op in een bestand met de naam `pre-auth_idp_metadata.xml`.

7. (Optioneel) Configureer meervoudige verificatie:
    - In Okta: **Applications** > (Toepassingen) **Applications** > Uw nieuwe toepassing (bijv. `Tableau Pre-Auth`) > **Sign On** (Aanmelden)
    - Klik onder **Sign On Policy** (Aanmeldingsbeleid) op **Add Rule** (Regel toevoegen).
    - Geef bij **App Sign On Rule** (App-aanmeldingsregel) een naam en de verschillende MFA-opties op. Om de functionaliteit te testen, kunt u alle opties op de standaardinstellingen laten staan. Onder **Actions** (Acties) moet u echter **Prompt for factor** (Om factor vragen) selecteren en vervolgens opgeven hoe vaak gebruikers zich moeten aanmelden. Klik op **Save** (Opslaan).

Okta-gebruiker maken en toewijzen

1. Maak in Okta een gebruiker aan met de gebruikersnaam die u in Tableau hebt gemaakt (gebruiker@voorbeeld.com): **Directory** > **People** (Mensen) > **Add person** (Persoon toevoegen).
2. Nadat de gebruiker is aangemaakt, wijst u de nieuwe Okta-app toe aan die persoon: klik op de gebruikersnaam en wijs de toepassing toe in **Assign Application** (Toepassing toewijzen).

Mellon installeren voor pre-auth

In dit voorbeeld wordt mod_auth_mellon gebruikt, een populaire opensource-module. Sommige Linux-distributies bevatten verouderde versies van mod_auth_mellon uit een oudere opslagplaats. Deze verouderde versies kunnen onbekende beveiligingsproblemen of functionele problemen bevatten. Als u mod_auth_mellon gebruikt, controleer dan of u de nieuwste versie gebruikt.

De mod_auth_mellon-module is software van derden. We hebben ons uiterste best gedaan om de procedures te verifiëren en te documenteren om dit scenario mogelijk te maken. Software van derden kan echter veranderen of uw scenario kan afwijken van de hier beschreven

referentiearchitectuur. Raadpleeg de documentatie van derden voor betrouwbare configuratiegegevens en ondersteuning.

1. Installeer een actuele versie van de Mellon-verificatiemodule op de actieve EC2-instantie waarop de onafhankelijke gateway wordt uitgevoerd.
2. Maak de directory `/etc/mellon`:

   ```
   sudo mkdir /etc/mellon
   ```

Mellon configureren als pre-auth-module

Voer deze procedure uit op de eerste instantie van de onafhankelijke gateway.

U moet een kopie hebben van het bestand `pre-auth_idp_metadata.xml` dat u hebt gemaakt vanuit de Okta-configuratie.

1. Ga naar de directory:

   ```
   cd /etc/mellon
   ```

2. Maak de metadata van de serviceprovider. Voer het script `mellon_create_metadata.sh` uit. U moet de entiteits-ID en de retour-URL voor uw organisatie in de opdracht opnemen.

   De retour-URL wordt de *URL voor eenmalige aanmelding* in Okta. Het laatste element van het pad in de retour-URL wordt de `MellonEndpointPath` in het `mellon.conf`-configuratiebestand dat later in deze procedure volgt. In dit voorbeeld specificeren we `sso` als eindpuntpad.

   Bijvoorbeeld:

   ```
   sudo /usr/libexec/mod_auth_mellon/mellon_create_metadata.sh https://tableau.example.com "https://tableau.example.com/sso"
   ```

Het script retourneert het certificaat, de sleutel en de metadatabestanden van de serviceprovider.

3. Hernoem de serviceproviderbestanden in de `mellon`-directory voor een betere leesbaarheid. In de documentatie verwijzen we naar deze bestanden met de volgende namen:

   ```
   sudo mv *.key mellon.key
   sudo mv *.cert mellon.cert
   sudo mv *.xml sp_metadata.xml
   ```

4. Kopieer het bestand`pre-auth_idp_metadata.xml` naar dezelfde map.

5. Wijzig eigendom en machtigingen voor alle bestanden in de `/etc/mellon`-directory:

   ```
   sudo chown tableau-tsig mellon.key
   sudo chown tableau-tsig mellon.cert
   sudo chown tableau-tsig sp_metadata.xml
   sudo chown tableau-tsig pre-auth_idp_metadata.xml
   sudo chmod +r * mellon.key
   sudo chmod +r * mellon.cert
   sudo chmod +r * sp_metadata.xml
   sudo chmod +r * pre-auth_idp_metadata.xml
   ```

6. Maak de directory `/etc/mellon/conf.d`:

   ```
   sudo mkdir /etc/mellon/conf.d
   ```

7. Maak het `global.conf`-bestand in de `/etc/mellon/conf.d`-directory.

   Kopieer de inhoud van het bestand zoals hieronder weergegeven, maar werk`MellonCookieDomain` bij met uw root-domeinnaam. Als de domeinnaam voor Tableau bijvoorbeeld `tableau.example.com` is, voer dan `example.com` in als rootdomein.

```
<Location "/">
AuthType Mellon
MellonEnable auth
Require valid-user
MellonCookieDomain <root domain>
MellonSPPrivateKeyFile /etc/mellon/mellon.key
MellonSPCertFile /etc/mellon/mellon.cert
MellonSPMetadataFile /etc/mellon/sp_metadata.xml
MellonIdPMetadataFile /etc/mellon/pre-auth_idp_metadata.xml
MellonEndpointPath /sso
</Location>

<Location "/tsighk">
MellonEnable Off
</Location>
```

8. Maak het `mellonmod.conf`-bestand in de `/etc/mellon/conf.d`-directory.

   Dit bestand bevat één enkele richtlijn die de locatie van het bestand `mod_auth_mellon.so` aangeeft. De locatie in het voorbeeld hier is de standaardlocatie van het bestand. Controleer of het bestand zich op deze locatie bevindt, of wijzig het pad in deze richtlijn zodat het overeenkomt met de werkelijke locatie van `mod_auth_mellon.so`:

   ```
   LoadModule auth_mellon_module /usr/lib64/httpd/modules/mod_
   auth_mellon.so
   ```

Maak een Tableau Server-toepassing in Okta

1. In het Okta-dashboard: **Applications** (Toepassingen) > **Applications** > **Browse App Catalog** (App-catalogus doorzoeken)
2. Zoek in **Browse App Integration Catalog** (App-integratiecatalogus doorzoeken) naar `Tableau`, selecteer de Tableau Server-tegel en klik vervolgens op **Add** (Toevoegen).
3. Voer bij **Add Tableau Server** (Tableau Server toevoegen) > **Algemene instellingen** (Algemene instellingen) een label in en klik vervolgens op **Next** (Volgende).
4. Selecteer in ‘Sign-On Options’ (Aanmeldingsopties) de optie **SAML 2.0** en scroll vervolgens omlaag naar 'Advanced Sign-on Settings' (Geavanceerde

aanmeldingsinstellingen):
    - **SAML Entity ID** (SAML-entiteits-ID): voer de openbare URL in, bijvoorbeeld https://tableau.example.com.
    - **Application user name format** (Notatie toepassingsgebruikersnaam): Email (E-mail)
5. Klik op de link **Identity Provider metadata** (Identiteitsprovider-metadata) om een browser te starten. Kopieer de browserlink. Dit is de link die u gebruikt wanneer u Tableau configureert in de volgende procedure.
6. Klik op **Done** (Gereed).
7. Wijs de nieuwe Tableau Server-toepassing van Okta toe aan uw gebruiker (gebruiker@voorbeeld.com): Klik op de gebruikersnaam en wijs de toepassing toe in **Assign Application** (Toepassing toewijzen).

Configuratie van verificatiemodule instellen op Tableau Server

Voer de volgende opdrachten uit op Tableau Server-knooppunt 1. Met deze opdrachten worden de bestandslocaties voor de Mellon-configuratiebestanden op de externe onafhankelijke gateway-computer opgegeven. Controleer nogmaals of de bestandspaden die in deze opdrachten worden opgegeven, overeenkomen met de paden en bestandslocaties op de externe onafhankelijke gateway-computer.

```
tsm configuration set -k gateway.tsig.authn_module_block -v "/etc/mellon/conf.d/mellonmod.conf" --force-keys
tsm configuration set -k gateway.tsig.authn_global_block -v "/etc/mellon/conf.d/global.conf" --force-keys
```

Om de downtime te beperken, mag u geen wijzigingen doorvoeren voordat u SAML hebt ingeschakeld zoals beschreven in de volgende sectie.

SAML inschakelen op Tableau Server voor IdP

Voer deze procedure uit op Tableau Server-knooppunt 1

1. Download de Tableau Server-toepassingsmetadata van Okta. Gebruik de link die u bij de vorige procedure hebt opgeslagen:

```
wget https://dev-66144217.ok-
ta.com/app/exk1egxgt1fhjkSeS5d7/sso/saml/metadata -O idp_met-
adata.xml
```

2. Kopieer een TLS-certificaat en bijbehorend sleutelbestand naar de Tableau Server. Het sleutelbestand moet een RSA-sleutel zijn. Zie *SAML-vereisten* (Linux) voor meer informatie over SAML-certificaat- en IdP-vereisten.

   Om het beheer en de implementatie van certificaten te vereenvoudigen en als best practice voor de beveiliging raden wij aan om certificaten te gebruiken die zijn gegenereerd door een grote, vertrouwde externe CA (certificeringsinstantie). U kunt er ook voor kiezen om zelfondertekende certificaten te genereren of certificaten van een PKI voor TLS te gebruiken.

   Als u geen TLS-certificaat hebt, kunt u een zelfondertekend certificaat genereren met behulp van de onderstaande ingesloten procedure.

Een zelfondertekend certificaat genereren

Voer deze procedure uit op Tableau Server-knooppunt 1.

a. Genereer een root-CA-sleutel:

   ```
   openssl genrsa -out rootCAKey-saml.pem 2048
   ```

b. Maak het root-CA-certificaat:

   ```
   openssl req -x509 -sha256 -new -nodes -key rootCAKey-
   saml.pem -days 3650 -out rootCACert-saml.pem
   ```

   U wordt gevraagd waarden in te voeren voor de certificaatvelden. Bijvoorbeeld:

```
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Washington
Locality Name (eg, city) [Default City]:Seattle
Organization Name (eg, company) [Default Company Ltd]:Ta-
bleau
Organizational Unit Name (eg, section) []:Operations
Common Name (eg, your name or your server's hostname) []:ta-
bleau.example.com
Email Address []:example@tableau.com
```

c. Maak het certificaat en de bijbehorende sleutel (`server-saml.csr` en `server-saml.key` in het onderstaande voorbeeld). De onderwerpnaam voor het certificaat moet overeenkomen met de openbare hostnaam van de Tableau-host. De onderwerpnaam wordt ingesteld met de optie `-subj` in de notatie "`/CN=<host-name>`", bijvoorbeeld:

```
openssl req -new -nodes -text -out server-saml.csr -keyout
server-saml.key -subj "/CN=tableau.example.com"
```

d. Onderteken het nieuwe certificaat met het CA-certificaat dat u hierboven hebt gemaakt. De volgende opdracht geeft het certificaat ook weer in de `crt`-notatie:

```
openssl x509 -req -in server-saml.csr -days 3650 -CA
rootCACert-saml.pem -CAkey rootCAKey-saml.pem -CAcre-
ateserial -out server-saml.crt
```

e. Converteer het sleutelbestand naar RSA. Tableau vereist een RSA-sleutelbestand voor SAML. Voer de volgende opdracht uit om de sleutel te converteren:

```
openssl rsa -in server-saml.key -out server-saml-rsa.key
```

3. Configureer SAML. Voer de volgende opdracht uit en geef daarbij uw entiteits-ID en retour-URL op, evenals de paden naar het metadatabestand, certificaatbestand en sleutelbestand:

```
tsm authentication saml configure --idp-entity-id "htt-
ps://tableau.example.com" --idp-return-url "htt-
ps://tableau.example.com" --idp-metadata idp_metadata.xml --
cert-file "server-saml.crt" --key-file "server-saml-rsa.key"

tsm authentication saml enable
```

4. Als uw organisatie Tableau Desktop 2021.4 of hoger gebruikt, moet u de volgende opdracht uitvoeren om verificatie via de reverse-proxyservers in te schakelen.

   Versies van Tableau Desktop 2021.2.1 - 2021.3 werken zonder dat u deze opdracht uitvoert, op voorwaarde dat de module voor voorafgaande verificatie (bijvoorbeeld Mellon) is geconfigureerd om het bewaren van cookies in het topleveldomein toe te staan.

   ```
   tsm configuration set -k features.ExternalBrowserOAuth -v false
   ```

5. Pas configuratiewijzigingen toe:

   ```
   tsm pending-changes apply
   ```

Start de tsig-httpd-service opnieuw

Wanneer uw Tableau Server-implementatie wijzigingen doorvoert, meldt u zich opnieuw aan bij de onafhankelijke gateway-computer van Tableau Server en voert u de volgende opdrachten uit om de tsig-httpd-service opnieuw te starten:

```
sudo su - tableau-tsig
systemctl --user restart tsig-httpd
exit
```

SAML-functionaliteit valideren

Om de end-to-end SAML-functionaliteit te valideren, meldt u zich aan bij Tableau Server met de openbare URL (bijvoorbeeld https://tableau.example.com) met het Tableau-beheerdersaccount dat u aan het begin van deze procedure hebt gemaakt.

Start TSM niet (gatewayfout) of krijgt u browserfoutmeldingen wanneer u verbinding probeert te maken? Raadpleeg dan Problemen met de onafhankelijke gateway van Tableau Server oplossen.

Verificatiemodule configureren bij tweede instantie van de onafhankelijke gateway

Nadat u de eerste instantie van de onafhankelijke gateway succesvol hebt geconfigureerd, implementeert u de tweede instantie. Het volgende is een voorbeeld van het laatste proces voor het installeren van het AWS-/Mellon-/Okta-scenario dat in dit onderwerp wordt beschreven. Bij deze procedure wordt ervan uitgegaan dat u de onafhankelijke gateway al op de tweede instantie hebt geïnstalleerd, zoals eerder in dit onderwerp is beschreven (Onafhankelijke gateway installeren).

Voor het proces voor de implementatie van de tweede onafhankelijke gateway moet u de volgende stappen doorlopen:

1. Op de tweede instantie van de onafhankelijke gateway: installeer de auth-module van Mellon.

   Configureer de Mellon-verificatiemodule niet zoals eerder in dit onderwerp beschreven. Neem in plaats daarvan de configuratie over die beschreven staat in de volgende stappen.

2. Op de geconfigureerde (eerste) instantie van de onafhankelijke gateway:

   Maak een tar-kopie van de bestaande Mellon-configuratie. De tar-back-up behoudt alle directoryhiërarchie en machtigingen. Voer de volgende opdrachten uit:

   ```
   cd /etc
   ```

   ```
   sudo tar -cvf mellon.tar mellon
   ```

   Kopieer `mellon.tar` naar de tweede instantie van de onafhankelijke gateway.

3. Over de tweede instantie van de onafhankelijke gateway:

Pak het tar-bestand uit ('unzip') naar de tweede instantie in de `/etc`-directory. Voer de volgende opdrachten uit:

```
cd /etc

sudo tar -xvf mellon.tar
```

4. Op knooppunt 1 van de Tableau Server-implementatie: werk het verbindingsbestand (`tsig.json`) bij met de verbindingsgegevens van de tweede onafhankelijke gateway. U moet de verificatiesleutel ophalen zoals eerder in dit onderwerp beschreven (Onafhankelijke gateway installeren).

   Zie hier een voorbeeld van een verbindingsbestand (`tsig.json`):

```
{
"independentGateways": [
 {
   "id": "ip-10-0-1-169.ec2.internal",
   "host": "ip-10-0-1-169.ec2.internal",
   "port": "21319",
   "protocol" : "http",
   "authsecret": "13660-27118-29070-25482-9518-22453"
 },
 {
   "id": "ip-10-0-2-230.ec2.internal",
   "host": "ip-10-0-2-230.ec2.internal",
   "port": "21319",
   "protocol" : "http",
   "authsecret": "9055-27834-16487-27455-30409-7292"
 }]
 }
```

5. Op knooppunt 1 van de Tableau Server-implementatie: voer de volgende opdrachten uit om de configuratie bij te werken:

```
tsm stop
```

```
tsm topology external-services gateway update -c tsig.json

tsm start
```

6. Op beide instanties van de onafhankelijke gateway: terwijl Tableau Server wordt gestart, start u het `tsig-httpd`-proces:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

7. In AWS **EC2>Target groups (Doelgroepen)**: werk de doelgroep bij met de EC2-instantie waarop de tweede onafhankelijke gateway-instantie wordt uitgevoerd.

   Selecteer de doelgroep die u zojuist hebt gemaakt en klik op het tabblad Doelen:

   - Klik op **Bewerken**.
   - Selecteer de EC2-instantie van de tweede onafhankelijke gateway-computer en klik vervolgens op **Toevoegen aan geregistreerd**. Klik op **Opslaan**.

Deel 6 - Configuratie na de installatie

SSL/TLS configureren van Load Balancer naar Tableau Server

Sommige organisaties hebben een end-to-end-versleutelingskanaal nodig van de client naar de backendservice. In de standaardreferentiearchitectuur zoals die tot nu toe beschreven is, wordt SSL van de client naar de Load Balancer opgegeven die op de weblaag van uw organisatie wordt uitgevoerd.

In dit gedeelte wordt beschreven hoe u SSL/TLS configureert voor Tableau Server en de onafhankelijke gateway in de voorbeeld-AWS-referentiearchitectuur. Zie Voorbeeld: SSL/TLS configureren in AWS-referentiearchitectuur voor een configuratievoorbeeld waarin wordt beschreven hoe u SSL/TLS configureert op Apache in de AWS-referentiearchitectuur.

Op dit moment wordt TLS niet ondersteund op de backend Tableau Server-processen die in het bereik 8000-9000 worden uitgevoerd. Om TLS in te schakelen, moet u de onafhankelijke gateway configureren met een relayverbinding met de Tableau Server.

In deze procedure wordt beschreven hoe u TLS inschakelt en configureert op de onafhankelijke gateway naar Tableau Server en op Tableau Server naar de onafhankelijke gateway. De procedure versleutelt het relayverkeer via HTTPS/443 en het housekeepingverkeer via HTTPS/21319.

In de Linux-procedures in dit voorbeeld worden opdrachten voor RHEL-achtige distributies getoond. De opdrachten hier zijn specifiek ontwikkeld met de Amazon Linux 2-distributie. Als u de Ubuntu-distributie gebruikt, moet u de opdrachten dienovereenkomstig bewerken.

De richtlijnen hier zijn aanbevelingen voor de specifieke AWS-voorbeeldreferentiearchitectuur in deze gids. Daarom zijn optionele configuraties niet inbegrepen. Zie *TLS configureren op onafhankelijke gateway* (Linux) voor volledige referentiedocumentatie.

Voordat u TLS configureert

Voer de TLS-configuraties buiten kantooruren uit. Voor de configuratie is minimaal één herstart van Tableau Server vereist. Als u een volledige implementatie van een referentiearchitectuur met vier knooppunten uitvoert, kan het even duren voordat Tableau Server opnieuw is opgestart.

- Controleer of clients via HTTP verbinding kunnen maken met Tableau Server. Het configureren van TLS met de onafhankelijke gateway is een proces dat uit meerdere stappen bestaat en waarbij mogelijk wat probleemoplossing nodig is. Daarom raden wij aan om te beginnen met een volledig operationele Tableau Server-implementatie voordat u TLS configureert.

- Verzamel TLS/SSL-certificaten, sleutels en gerelateerde assets. U hebt SSL-certificaten nodig voor de onafhankelijke gateways en voor Tableau Server. Om certificaatbeheer en -implementatie te vereenvoudigen en als best practice voor de beveiliging, raden we aan om certificaten te gebruiken die zijn gegenereerd door een grote, vertrouwde externe certificeringsinstantie (CA). U kunt er ook voor kiezen om zelfondertekende certificaten te genereren of certificaten van een PKI voor TLS te gebruiken.

  In de voorbeeldconfiguratie in dit onderwerp worden de volgende assetnamen ter illustratie gebruikt:
  - `tsig-ssl.crt`: het TLS/SSL-certificaat voor de onafhankelijke gateway.
  - `tsig-ssl.key`: de privésleutel voor `tsig-ssl.crt` op de onafhankelijke gateway.
  - `ts-ssl.crt`: het TLS/SSL-certificaat voor Tableau Server.
  - `ts-ssl.key`: de privésleutel voor `tsig-ssl.crt` op Tableau Server.

  - `tableau-server-CA.pem`: het basiscertificaat voor de CA die de certificaten voor de Tableau Server-computers genereert. Dit certificaat is doorgaans niet vereist als u certificaten van grote, vertrouwde derde partijen gebruikt.
  - `rootTSIG-CACert.pem`: het basiscertificaat voor de CA die de certificaten genereert voor de onafhankelijke gateway-computers. Dit certificaat is doorgaans niet vereist als u certificaten van grote, vertrouwde derde partijen gebruikt.
  - Er zijn nog andere certificaten en belangrijke bestandsassets vereist voor SAML. Deze worden gedetailleerd beschreven in Deel 5 van deze handleiding.
  - Hebt u voor uw implementatie van een certificaatketenbestand nodig? Raadpleeg dan het Knowledge Base-artikel TLS configureren op onafhankelijke gateway bij gebruik van een certificaat met een certificaatketen.
- Controleer of u toegang hebt tot IdP. Als u een IdP gebruikt voor verificatie, moet u waarschijnlijk wijzigingen aanbrengen in de URL's van de ontvanger en de bestemming bij de IdP nadat u SSL/TLS hebt geconfigureerd.

De onafhankelijke gateway-computers voor TLS configureren

De configuratie van TLS kan een foutgevoelig proces zijn. Omdat het veel tijd kan kosten om problemen in twee instanties van de onafhankelijke gateway op te lossen, raden we aan om TLS in te schakelen en te configureren op de EDG-implementatie met slechts één onafhankelijke gateway. Nadat u hebt gecontroleerd of TLS in de hele implementatie werkt, configureert u de tweede onafhankelijke gateway-computer.

Stap 1: distribueer certificaten en sleutels naar de onafhankelijke gateway-computer

U kunt de bestanden naar elke willekeurige map distribueren, zolang de tsig-httpd-gebruiker leesrechten voor de bestanden heeft. De paden naar deze bestanden worden in andere procedures vermeld. We zullen in dit hele onderwerp de voorbeeldpaden onder `/etc/ssl` gebruiken zoals ze hieronder weergegeven zijn.

1. Maak een map voor de privésleutel:

   ```
   sudo mkdir -p /etc/ssl/private
   ```

2. Kopieer de certificaat- en sleutelbestanden naar de `/etc/ssl`-paden. Bijvoorbeeld,

   ```
   sudo cp tsig-ssl.crt /etc/ssl/certs/
   ```

   ```
   sudo cp tsig-ssl.key /etc/ssl/private/
   ```

3. (Optioneel) Als u een zelfondertekend certificaat of PKI-certificaat voor SSL/TLS op Tableau Server gebruikt, moet u het CA-rootcertificaatbestand ook naar de onafhankelijke gateway-computer kopiëren. Bijvoorbeeld,

   ```
   sudo cp tableau-server-CA.pem /etc/ssl/certs/
   ```

Stap 2: werk de omgevingsvariabelen voor TLS bij

U moet de poort- en protocolomgevingsvariabelen voor de configuratie van de onafhankelijke gateway bijwerken.

Wijzig deze waarden door het bestand `/etc/opt/tableau/tableau_tsig/environment.bash`, als volgt bij te werken:

```
TSIG_HK_PROTOCOL="https"
TSIG_PORT="443"
TSIG_PROTOCOL="https"
```

Stap 3: werk het stubconfiguratiebestand voor het HK-protocol bij

Bewerk handmatig het stubconfiguratiebestand (`/var/opt/tableau/tableau_tsig/config/httpd.conf.stub`) om TLS-gerelateerde Apache-httpd-richtlijnen in te stellen voor het housekeeping (HK)-protocol.

Het stubconfiguratiebestand bevat een blok met TLS-gerelateerde richtlijnen waar een opmerking met een `#TLS#`-markering bij staat. Verwijder de markeringen uit de richtlijnen zoals in het onderstaande voorbeeld. Houd er rekening mee dat er in het voorbeeld gebruik wordt

gemaakt van een root-CA-certificaat voor het SSL-certificaat dat wordt gebruikt op Tableau Server met de `SSLCACertificateFile`-optie.

```
#TLS# SSLPassPhraseDialog exec:/path/to/file
<VirtualHost *:${TSIG_HK_PORT}>
SSLEngine on
#TLS# SSLHonorCipherOrder on
#TLS# SSLCompression off
SSLCertificateFile /etc/ssl/certs/tsig-ssl.crt
SSLCertificateKeyFile /etc/ssl/private/tsig-ssl.key
SSLCACertificateFile /etc/ssl/certs/tableau-server-CA.pem
#TLS# SSLCARevocationFile /path/to/file
</VirtualHost>
```

Deze wijzigingen gaan verloren als u de onafhankelijke gateway opnieuw installeert. Wij raden aan om een reservekopie te maken.

Stap 4: kopieer het stubbestand en start de service opnieuw

1. Kopieer het bestand dat u in de laatste stap hebt bijgewerkt om httpd.conf bij te werken met de wijzigingen:

   ```
   cp /var/opt/tableau/tableau_tsig/config/httpd.conf.stub /var/op-
   t/tableau/tableau_tsig/config/httpd.conf
   ```

2. Start de onafhankelijke gateway-service opnieuw:

   ```
   sudo su - tableau-tsig
   systemctl --user restart tsig-httpd
   exit
   ```

Nadat u de service opnieuw hebt opgestart, is de onafhankelijke gateway niet operationeel totdat u de volgende stappen op Tableau Server uitvoert. Nadat u de stappen op Tableau Server hebt voltooid, zal de onafhankelijke gateway de wijzigingen oppikken en online gaan.

Tableau Server-knooppunt 1 voor TLS configureren

Voer deze stappen uit op knooppunt 1 van de Tableau Server-implementatie.

Stap 1: kopieer certificaten en sleutels en stop TSM

1. Controleer of u de externe SSL-certificaten en -sleutels van Tableau Server naar knooppunt 1 hebt gekopieerd.
2. Om de downtime tot een minimum te beperken, raden we u aan TSM te stoppen, de volgende stappen uit te voeren en TSM opnieuw te starten nadat de wijzigingen zijn toegepast:

   ```
   tsm stop
   ```

Stap 2: stel certificaatassets in en schakel de configuratie van de onafhankelijke gateway in

1. Geef de locatie van certificaat- en sleutelbestanden voor de onafhankelijke gateway op. Deze paden verwijzen naar de locatie op de onafhankelijke gateway-computers. Houd er rekening mee dat in dit voorbeeld wordt aangenomen dat hetzelfde certificaat en sleutelpaar worden gebruikt om HTTPS- en housekeeping-verkeer te beschermen:

   ```
   tsm configuration set -k gateway.tsig.ssl.cert.file_name -v /etc/ssl/certs/tsig-ssl.crt --force-keys
   tsm configuration set -k gateway.tsig.ssl.key.file_name -v /etc/ssl/private/tsig-ssl.key --force-keys
   ```

2. Schakel TLS in voor HTTPS- en HK-protocollen voor de onafhankelijke gateway:

   ```
   tsm configuration set -k gateway.tsig.ssl.enabled -v true --force-keys
   tsm configuration set -k gateway.tsig.hk.ssl.enabled -v true --force-keys
   ```

3. (Optioneel) Als u een zelfondertekend certificaat of PKI-certificaat gebruikt voor SSL/TLS op de onafhankelijke gateway, moet u het CA-rootcertificaatbestand uploaden. Het CA-rootcertificaatbestand is het rootcertificaat dat werd gebruikt om de certificaten voor de onafhankelijke gateway-computers te genereren. Bijvoorbeeld,

```
tsm security custom-cert add -c rootTSIG-CACert.pem
```

4. (Optioneel) Als u een zelfondertekend certificaat of PKI-certificaat voor SSL/TLS op Tableau Server gebruikt, moet u het CA-rootcertificaatbestand naar de onafhankelijke gateway-directory `/etc/ssl/certs` kopiëren. Het CA-rootcertificaatbestand is het rootcertificaat dat is gebruikt om de certificaten voor de Tableau Server-computers te genereren. Nadat u het certificaat naar de onafhankelijke gateway hebt gekopieerd, moet u de locatie van het certificaat op knooppunt 1 opgeven met de volgende tsm-opdracht. Bijvoorbeeld,

   ```
   tsm configuration set -k gateway.tsig.ssl.proxy.gateway_relay_
   cluster.cacertificatefile -v /etc/ssl/certs/tableau-server-
   CA.pem --force-keys
   ```

5. (Optioneel: alleen voor testdoeleinden) Als u zelfondertekende certificaten of PKI-certificaten tussen computers deelt en de onderwerpnamen op de certificaten daarom niet overeenkomen met de computernamen, moet u certificaatverificatie uitschakelen.

   ```
   tsm configuration set -k gateway.tsig.ssl.proxy.verify -v opti-
   onal_no_ca --force-keys
   ```

Stap 3: schakel 'externe SSL' in voor Tableau Server en pas de wijzigingen toe

1. Schakel 'Externe SSL' op Tableau Server in en configureer dit:

   ```
   tsm security external-ssl enable --cert-file ts-ssl.crt --key-
   file ts-ssl.key
   ```

2. Pas de wijzigingen toe.

   ```
   tsm pending-changes apply
   ```

Stap 4: werk het JSON-configuratiebestand van de gateway bij en start tsm

1. Werk het configuratiebestand van de onafhankelijke gateway bij (bijvoorbeeld `tsig.json`) aan de Tableau Server-zijde om het `https`-protocol voor de onafhankelijke gateway-objecten op te geven:

   ```
   "protocol" : "https",
   ```

2. Verwijder (of maak een opmerking) over de verbindingsgegevens voor de tweede instantie van de onafhankelijke gateway. Controleer de JSON in een externe editor voordat u deze opslaat.

   Nadat u TLS voor de ene instantie van de onafhankelijke gateway hebt geconfigureerd en gevalideerd, werkt u dit JSON-bestand bij met de verbindingsgegevens voor de tweede instantie van de onafhankelijke gateway.

3. Voer de volgende opdracht uit om de configuratie van de onafhankelijke gateway bij te werken:

   ```
   tsm topology external-services gateway update -c tsig.json
   ```

4. Start TSM.

   ```
   tsm start
   ```

5. Terwijl TSM start, meldt u zich aan bij de onafhankelijke gateway-instantie en start u de `tsig-httpd`-service opnieuw op:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

IdP-verificatiemodule-URL's bijwerken naar HTTPS

Als u een externe identiteitsprovider voor Tableau hebt geconfigureerd, moet u waarschijnlijk de retour-URL's bijwerken in het IdP-beheerdashboard.

Als u bijvoorbeeld een pre-auth-toepassing van Okta gebruikt, moet u de toepassing bijwerken zodat deze het HTTPS-protocol gebruikt voor de Ontvanger-URL en de Bestemmings-URL.

AWS-Load Balancer voor HTTPS configureren

Als u implementeert met AWS Load Balancer zoals uiteengezet in deze handleiding, configureert u de AWS Load Balancer opnieuw om HTTPS-verkeer te verzenden naar de computers waarop de onafhankelijke gateway wordt uitgevoerd:

1. Bestaande HTTP-doelgroep verwijderen:

   Ga naar **Target Groups (Doelgroepen)** en selecteer de HTTP-doelgroep die is geconfigureerd voor de Load Balancer. Klik op **Acties** en vervolgens op **Verwijderen**.

2. HTTPS-doelgroep aanmaken:

   Doelgroepen > **Doelgroep maken**

   - Selecteer Instances (Instanties)
   - Voer een doelgroepnaam in, bijvoorbeeld `TG-internal-HTTPS`
   - Selecteer uw VPC
   - Protocol: HTTPS 443
   - Onder **Health checks (Gezondheidscontroles)** > **Advanced health checks settings (Geavanceerde instellingen voor gezondheidscontroles)** > **Success codes (Succescodes)**, voegt u de volgende codelijst toe: `200,303`.
   - Klik op **Maken**.

3. Selecteer de doelgroep die u zojuist hebt gemaakt en klik op het tabblad **Doelen**:

- Klik op **Bewerken**
- Selecteer de EC2-instantie waarop de door u geconfigureerde onafhankelijke gateway van Tableau Server wordt uitgevoerd en klik dan op **Toevoegen aan geregistreerd**.
- Klik op **Opslaan**.

4. Nadat u de doelgroep hebt aangemaakt, moet u de sticky-functie inschakelen:
    - Open de AWS-doelgroeppagina (**EC2**> **Load Balancing**> **Doelgroepen**) en selecteer de doelgroepinstantie die u zojuist hebt ingesteld. Ga naar het menu **Actie** en selecteer **Edit attributes (Kenmerken bewerken)**.
    - Op de pagina **Kenmerken bewerken** selecteert u **Stickiness (Kleverigheid)**. Geef een duur op van `1 day` en klik op **Wijzigingen opslaan**.
5. Werk de listener-regels bij op de Load Balancer. Selecteer de Load Balancer die u voor deze implementatie hebt geconfigureerd en klik vervolgens op het tabblad **Listeners (Luisteraars)**.
    - Klik voor **HTTP:80** op **View/edit rules (Regels weergeven/bewerken)**. Op de resulterende **Regels**pagina, klikt u op het bewerkingspictogram (eerst bovenaan de pagina en vervolgens nogmaals naast de regel) om de regel te bewerken. Verwijder de bestaande THEN-regel en vervang deze door te klikken op **Actie toevoegen** > **Redirect to... (Omleiden naar...)**. Geef in de resulterende THEN-configuratie `HTTPS` op en poort `443` en laat de overige opties op de standaardinstellingen staan. Sla de instelling op en klik vervolgens op **Bijwerken**.
    - Klik voor **HTTPS:443** op **View/edit rules (Regels weergeven/bewerken)**. Op de resulterende **Regels**pagina, klikt u op het bewerkingspictogram (eerst bovenaan de pagina en vervolgens nogmaals naast de regel) om de regel te bewerken. Verwijder de bestaande THEN-regel en vervang deze door te klikken op **Actie toevoegen** > **Forward to... (Doorsturen naar...)**. Geef de Doelgroep op voor de HTTPS-groep die u zojuist hebt gemaakt. Schakel onder **Group-level stickiness (Kleverigheid op groepsniveau)** kleverigheid in en stel de duur in op 1 dag. Sla de instelling op en klik vervolgens op **Bijwerken**.
6. Werk de inactiviteits-time-out voor de Load Balancer bij naar 400 seconden. Selecteer de Load Balancer die u voor deze implementatie hebt geconfigureerd en klik vervolgens op **Acties** > **Kenmerken bewerken**. Stel **Idle timeout (Time-out bij inactiviteit)** in op

`400` seconden, en klik dan op **Opslaan**.

TLS valideren

Om de TLS-functionaliteit te valideren, meldt u zich aan bij Tableau Server met de openbare URL (bijvoorbeeld https://tableau.example.com) met het Tableau-beheerdersaccount dat u aan het begin van deze procedure hebt gemaakt.

Start TSM niet of krijgt u andere foutmeldingen? Raadpleeg dan Problemen met de onafhankelijke gateway van Tableau Server oplossen.

Tweede instantie van de onafhankelijke gateway voor SSL configureren

Nadat u de eerste instantie van de onafhankelijke gateway succesvol hebt geconfigureerd, implementeert u de tweede instantie.

Voor het proces voor de implementatie van de tweede onafhankelijke gateway moet u de volgende stappen doorlopen:

1. Op de geconfigureerde (eerste) instantie van de onafhankelijke gateway: kopieer de volgende bestanden naar de overeenkomstige locaties op de tweede instantie van de onafhankelijke gateway:
    - `/etc/ssl/certs/tsig-ssl.crt`
    - `/etc/ssl/private/tsig-ssl.key` (U moet de `private`-directory op de tweede instantie aanmaken).
    - `/var/opt/tableau/tableau_tsig/config/httpd.conf.stub`
    - `/etc/opt/tableau/tableau_tsig/environment.bash`
2. Op knooppunt 1 van de Tableau Server-implementatie: werk het verbindingsbestand (`tsig.json`) bij met de verbindingsgegevens van de tweede onafhankelijke gateway.

Zie hier een voorbeeld van een verbindingsbestand (`tsig.json`):

```
{
"independentGateways": [
 {
   "id": "ip-10-0-1-169.ec2.internal",
   "host": "ip-10-0-1-169.ec2.internal",
   "port": "21319",
   "protocol" : "https",
   "authsecret": "13660-27118-29070-25482-9518-22453"
 },
 {
   "id": "ip-10-0-2-230.ec2.internal",
   "host": "ip-10-0-2-230.ec2.internal",
   "port": "21319",
   "protocol" : "https",
   "authsecret": "9055-27834-16487-27455-30409-7292"
 }]
 }
```

3. Op knooppunt 1 van de Tableau Server-implementatie: voer de volgende opdrachten uit om de configuratie bij te werken:

   ```
   tsm stop

   tsm topology external-services gateway update -c tsig.json

   tsm start
   ```

4. Op beide instanties van de onafhankelijke gateway: terwijl Tableau Server wordt gestart, start u het `tsig-httpd`-proces op beide instanties van de onafhankelijke gateway:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

5. In AWS **EC2>Target groups (Doelgroepen)**: werk de doelgroep bij met de EC2-instantie waarop de tweede onafhankelijke gateway-instantie wordt uitgevoerd.

   Selecteer de doelgroep die u zojuist hebt gemaakt en klik op het tabblad Doelen:

   - Klik op **Bewerken**.
   - Selecteer de EC2-instantie van de tweede onafhankelijke gateway-computer en klik vervolgens op **Toevoegen aan geregistreerd**. Klik op **Opslaan**.

SSL configureren voor Postgres

U kunt optioneel SSL (TLS) configureren voor de Postgres-verbinding voor de externe opslagplaatsverbinding op Tableau Server.

Om certificaatbeheer en -implementatie te vereenvoudigen en als best practice voor de beveiliging, raden we aan om certificaten te gebruiken die zijn gegenereerd door een grote, vertrouwde externe certificeringsinstantie (CA). U kunt er ook voor kiezen om zelfondertekende certificaten te genereren of certificaten van een PKI voor TLS te gebruiken.

In deze procedure wordt beschreven hoe u OpenSSL kunt gebruiken om een zelfondertekend certificaat te genereren op de Postgres-host op een RHEL-achtige Linux-distributie in de voorbeeld-AWS-referentiearchitectuur.

Nadat u het SSL-certificaat hebt gegenereerd en ondertekend, moet u het CA-certificaat kopiëren naar de Tableau-host.

Op de host waarop Postgress draait:

1. Genereer een root-certificeringsverificatiesleutel ofwel CA-sleutel (certificate authority):

   ```
   openssl genrsa -out pgsql-rootCAKey.pem 2048
   ```

2. Maak het root-CA-certificaat:

```
openssl req -x509 -sha256 -new -nodes -key pgsql-rootCAKey.pem
-days 3650 -out pgsql-rootCACert.pem
```

U wordt gevraagd waarden in te voeren voor de certificaatvelden. Bijvoorbeeld:

```
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Washington
Locality Name (eg, city) [Default City]:Seattle
Organization Name (eg, company) [Default Company Ltd]:Tableau
Organizational Unit Name (eg, section) []:Operations
Common Name (eg, Postgres server's hostname) []:ip-10-0-1-
189.us-west-1.compute.internal
Email Address []:example@tableau.com
```

3. Maak het certificaat en de bijbehorende sleutel (`server.csr` en `server.key` in het onderstaande voorbeeld) voor de Postgres-computer. De onderwerpnaam voor het certificaat moet overeenkomen met de EC2-privé-DNS-naam van de Postgres-host. De onderwerpnaam wordt ingesteld met de `-subj`-optie met de notatie `"/CN=<private DNS name>"`, bijvoorbeeld:

   ```
   openssl req -new -nodes -text -out server.csr -keyout ser-
   ver.key -subj "/CN=ip-10-0-1-189.us-west-1.compute.internal"
   ```

4. Onderteken het nieuwe certificaat met het CA-certificaat dat u in stap 2 hebt gemaakt. Met de volgende opdracht wordt het certificaat ook weergegeven in `crt`-notatie:

   ```
   openssl x509 -req -in server.csr -days 3650 -CA pgsql-
   rootCACert.pem -CAkey pgsql-rootCAKey.pem -CAcreateserial -out
   server.crt
   ```

5. Kopieer de crt- en key-bestanden naar het Postgres `/var/lib/pgsql/13/data/`-pad:

   ```
   sudo cp server.crt /var/lib/pgsql/13/data/
   ```

   ```
   sudo cp server.key /var/lib/pgsql/13/data/
   ```

6. Schakel over op rootgebruiker:

```
sudo su
```

7. Stel machtigingen in voor de cer- en key-bestanden. Voer de volgende opdrachten uit:

```
cd /var/lib/pgsql/13/data
chown postgres.postgres server.crt
chown postgres.postgres server.key
chmod 0600 server.crt
chmod 0600 server.key
```

8. Werk het configuratiebestand pg_haba bij, `/var/lib/pgsql/13/data/pg_hba.conf` om md5-vertrouwen op te geven:

   Wijzig de bestaande verbindingsverklaringen van

   `host all all 10.0.30.0/24 password` en

   `host all all 10.0.31.0/24 password`

   naar

   `host all all 10.0.30.0/24 md5` en

   `host all all 10.0.31.0/24 md5`.

9. Werk het PostgreSQL-bestand bij, `/var/lib/pgsql/13/data/postgresql.conf`, door deze regel toe te voegen:

   `ssl = on`

10. Verlaat de root-gebruikermodus:

    `exit`

11. Start Postgres opnieuw:

    `sudo systemctl restart postgresql-13`

Optioneel: schakel certificaatvertrouwensvalidatie in op Tableau Server voor Postgres SSL

Als u de installatieprocedure in Deel 4 – Tableau Server installeren en configureren hebt gevolgd, wordt Tableau Server geconfigureerd met optionele SSL voor de Postgres-verbinding. Dit betekent dat de configuratie van SSL op Postgres (zoals hierboven beschreven) resulteert in een gecodeerde verbinding.

Als u certificaatvertrouwensvalidatie voor de verbinding wilt vereisen, moet u de volgende opdracht uitvoeren op Tableau Server om de Postgres-hostverbinding opnieuw te configureren:

```
tsm topology external-services repository replace-host -f <file-
name>.json -c CACert.pem
```

Waarbij `<filename>.json` het verbindingsbestand is dat beschreven wordt in Externe Postgres configureren en `CACert.pem` het CA-certificaatbestand voor het SSL/TLS-certificaat dat door Postgres wordt gebruikt.

Optioneel: SSL-connectiviteit verifiëren

Om de SSL-connectiviteit te verifiëren, moet u het volgende doen:

- Installeer de Postgres-client op Tableau Server-knooppunt 1.
- Kopieer het rootcertificaat dat u in de vorige procedure hebt gemaakt naar de Tableau-host.
- Maak verbinding met de Postgres-server vanaf knooppunt 1

Postgres-client op knooppunt 1 installeren

Dit is een voorbeeld van hoe u Postgres versie 13.4 installeert. Installeer dezelfde versie als die u voor de externe opslagplaats gebruikt.

1. Maak en bewerk op knooppunt 1 het bestand pgdg.repo in het pad `/etc/yum.repos.d`. Vul het bestand met de volgende configuratiegegevens.

   ```
   [pgdg13]
   name=PostgreSQL 13 for RHEL/CentOS 7 - x86_64
   baseurl=https://download.postgresql.org/pub/repos/yum/13/redhat/rhel-7-x86_64
   enabled=1
   gpgcheck=0
   ```

2. Installeer de Postgres-client:

   ```
   sudo yum install postgresql13-13.4-1PGDG.rhel7.x86_64
   ```

Rootcertificaat naar knooppunt 1 kopiëren

Kopieer het CA-certificaat (`pgsql-rootCACert.pem`) naar de Tableau-host:

```
scp ec2-user@<private-DNS-name-of-Postgress-host>:/home/ec2-user/pgsql-rootCACert.pem /home/ec2-user
```

Verbinding maken met Postgres-host via SSL vanaf knooppunt 1

Voer de volgende opdracht uit vanaf knooppunt 1 en geef daarbij het IP-adres van de Postgres-serverhost en het root-CA-certificaat op:

```
psql "postgresql://postgres@<IP-address>:5432/postgres?sslmode=verify-ca&sslrootcert=pgsql-rootCACert.pem"
```

Bijvoorbeeld:

```
 psql "postgresql://postgres@10.0.1.189:5432/postgres?sslmode=verify-ca&sslrootcert=pgsql-rootCACert.pem"
```

Postgres vraagt u om het wachtwoord. Als het gelukt is om u aan te melden, zal de shell het volgende retourneren:

```
psql (13.4)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-
SHA384, bits: 256, compression: off)
Type "help" for help.
postgres=#
```

SMTP- en gebeurtenismeldingen configureren

Tableau Server stuurt e-mailmeldingen naar beheerders en gebruikers. Om dit mogelijk te maken, moet u Tableau Server configureren om e-mail naar uw e-mailserver te sturen. U moet ook de gebeurtenistypen, drempelwaarden en abonnementsgegevens opgeven die u wilt verzenden.

Voor de initiële configuratie van SMTP en meldingen raden we u aan de onderstaande configuratiebestandsjabloon te gebruiken om een JSON-bestand te maken. U kunt ook een willekeurige configuratiesleutel instellen die hieronder wordt vermeld met de syntaxis die wordt beschreven in *tsm configuration set* (Linux).

Voer deze procedure uit op knooppunt 1 in uw Tableau Server-implementatie:

1. Kopieer de volgende JSON-sjabloon naar een bestand. Pas het bestand aan met uw SMTP-configuratieopties en de abonnements- en waarschuwingsmeldingen voor uw organisatie.
   - Zie *Referentie configuratie SMTP CLI* (Linux) voor een lijst en beschrijving van alle SMTP-opties.
   - Zie het CLI-gedeelte van *Server-gebeurtenismelding configureren* (Linux) voor een lijst en beschrijving van alle opties voor meldingsgebeurtenissen.

   ```
   {
   "configKeys": {
          "svcmonitor.notification.smtp.server": "SMTP server host
   name",
   ```

```
        "svcmonitor.notification.smtp.send_account": "SMTP user name",
        "svcmonitor.notification.smtp.port": 443,
        "svcmonitor.notification.smtp.password": "SMTP user account
password",
        "svcmonitor.notification.smtp.ssl_enabled": true,
        "svcmonitor.notification.smtp.from_address": "From email
address",
        "svcmonitor.notification.smtp.target_addresses": "To email
address1,address2",
        "svcmonitor.notification.smtp.canonical_url": "Tableau Server
URL",
        "backgrounder.notifications_enabled": true,
        "subscriptions.enabled": true,
        "subscriptions.attachments_enabled": true,
        "subscriptions.max_attachment_size_megabytes": 150,
        "svcmonitor.notification.smtp.enabled": true,
        "features.DesktopReporting": true,
        "storage.monitoring.email_enabled": true,
        "storage.monitoring.warning_percent": 20,
        "storage.monitoring.critical_percent": 15,
        "storage.monitoring.email_interval_min": 25,
        "storage.monitoring.record_history_enabled": true
        }
}
```

2. Voer `tsm settings import -f file.json` uit om het JSON-bestand door te geven aan Tableau Services Manager.
3. Voer de opdracht `tsm pending-changes apply` uit om de wijzigingen toe te passen.
4. Voer de opdracht `tsm email test-smtp-connection` uit om de verbindingsconfiguratie te bekijken en te verifiëren.

PostgreSQL-stuurprogramma installeren

Om beheerdersweergaven op Tableau Server te bekijken, moet de PostgreSQL-driver op knooppunt 1 van de Tableau Server-implementatie zijn geïnstalleerd.

1. Ga naar de pagina Tableau-stuurprogramma downloaden en kopieer de URL voor het PostgreSQL-jarbestand.
2. Voer de volgende procedure uit op elk knooppunt van de Tableau-implementatie:
   - Maak het volgende bestandspad:

     ```
     sudo mkdir -p /opt/tableau/tableau_driver/jdbc
     ```

   - Download de nieuwste versie van het PostgreSQL-jarbestand via het nieuwe pad. Bijvoorbeeld:

     ```
     sudo wget htt-
     ps://-
     downloads.tableau.com/drivers/linux/postgresql/postgresql-
     42.2.22.jar
     ```

3. Start Tableau Server opnieuw op het initiële knooppunt:

   ```
   tsm restart
   ```

Sterk wachtwoordbeleid configureren

Als u Tableau Server niet implementeert met een IdP-verificatieoplossing, raden wij u aan het standaardwachtwoordbeleid van Tableau aan te scherpen.

Als u Tableau Server implementeert met een IdP, moet u het wachtwoordbeleid beheren met de IdP.

De volgende procedure bevat JSON-configuratie voor het instellen van wachtwoordbeleid op Tableau Server. Zie *Lokale verificatie* (Linux) voor meer informatie over de onderstaande opties.

1. Kopieer de volgende JSON-sjabloon naar een bestand. Vul de sleutelwaarden in met de configuratie van uw wachtwoordbeleid.

```
{
 "configKeys": {
       "wgserver.localauth.policies.mustcontainletters.enabled":
true,
       "wgserver.localauth.policies.mustcontainuppercase.enabled":
true,
       "wgserver.localauth.policies.mustcontainnumbers.enabled":
true,
       "wgserver.localauth.policies.mustcontainsymbols.enabled":
true,
       "wgserver.localauth.policies.minimumpasswordlength.enabled":
true,
       "wgserver.localauth.policies.minimumpasswordlength.value": 12,
       "wgserver.localauth.policies.maximumpasswordlength.enabled":
false,
       "wgserver.localauth.policies.maximumpasswordlength.value":
255,
       "wgserver.localauth.passwordexpiration.enabled": true,
       "wgserver.localauth.passwordexpiration.days": 90,
       "wgserver.localauth.ratelimiting.maxbackoff.minutes": 60,
       "wgserver.localauth.ratelimiting.maxattempts.enabled": false,
       "wgserver.localauth.ratelimiting.maxattempts.value": 5,
       "vizportal.password_reset": true
 }
}
```

2. Voer `tsm settings import -f file.json` uit om het JSON-bestand door te geven aan Tableau Services Manager om Tableau Server te configureren.

3. Voer de opdracht `tsm pending-changes apply` uit om de wijzigingen toe te passen.

Deel 7 - Validatie, tools en problemen oplossen

In dit deel worden onder andere validatiestappen voor na de installatie en richtlijnen voor probleemoplossing besproken.

Validatie van failover-systemen

Nadat u uw implementatie hebt geconfigureerd, raden wij u aan eenvoudige failover-tests uit te voeren om de systeemredundantie te valideren.

Wij raden u aan de volgende stappen uit te voeren om de failover-functionaliteit te valideren:

1. Sluit de eerste instantie van de onafhankelijke gateway (TSIG1) af. Al het binnenkomende verkeer moet via de tweede instantie van de onafhankelijke gateway (TSIG2) worden gerouteerd.
2. Start TSIG1 opnieuw op en sluit vervolgens TSIG2 af. Al het binnenkomende verkeer moet via TSIG1 worden gerouteerd.
3. Start TSIG2 opnieuw.

4. Sluit Tableau Server-knooppunt 1 af. Al het Vizportal-/toepassingsserviceverkeer wordt overgezet naar knooppunt 2.

   Opmerking Vanaf september 2022 was de hoge beschikbaarheid van knooppunt 1 in gevaar op bepaalde versies van Tableau Server 2021.4 en hoger. Clientverbindingen mislukken als knooppunt 1 niet beschikbaar is. Dit probleem is opgelost in de volgende onderhoudsverklaringen:

   - 2021.4.15 en hoger
   - 2022.1.11 en hoger
   - 2023.1.3 en hoger

> Om ervoor te zorgen dat uw Tableau Server-installatie met ATR-activeringen een respijtperiode van 72 uur heeft na de initiële uitval van een knooppunt, installeert u een van deze versies of voert u een upgrade uit naar een van deze versies. Raadpleeg Tableau Server HA met ATR heeft geen respijtperiode na de initiële knooppuntstoring (in het Engels) in de Tableau Knowledgebase voor nadere informatie.

5. Start knooppunt 1 opnieuw en sluit knooppunt 2 af. Al het Vizportal-/toepassingsserviceverkeer wordt overgezet naar knooppunt 1.
6. Start knooppunt 2 opnieuw op.

In deze context betekent ‘afsluiten’ of ‘opnieuw opstarten’ dat u het besturingssysteem of de virtuele machine uitschakelt zonder dat er eerst een poging is gedaan om de toepassing op een correcte manier af te sluiten. Het doel is om een hardware- of virtuele machinestoring te simuleren.

De minimale validatiestap voor elke failovertest is om te verifiëren met een gebruiker en basisweergavebewerkingen uit te voeren.

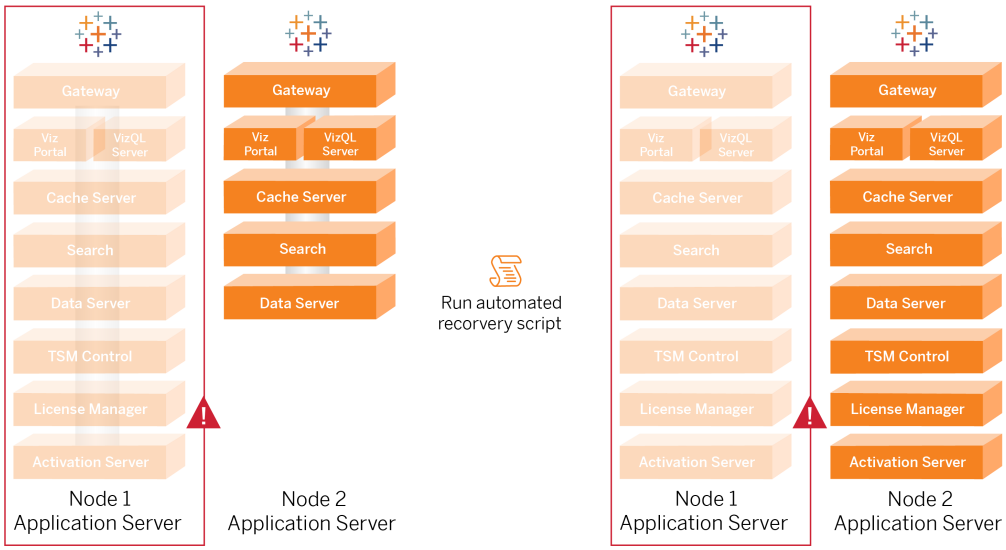
U krijgt mogelijk een browserfoutmelding 'Bad Request' wanneer u probeert in te loggen na een gesimuleerde mislukking. Het kan zijn dat u deze foutmelding zelfs krijgt als u de cache van uw browser wist. Dit probleem treedt vaak op wanneer de browser data van een eerdere IdP-sessie cachet. Als deze fout zich zelfs nadat u de lokale browsercache hebt gewist blijft voordoen, valideert u het Tableau-scenario door verbinding te maken met een andere browser.

Automatisch herstel van eerste knooppunt

Tableau Server versie 2021.2.4 en hoger bevatten een geautomatiseerd script voor initiële knooppuntherstel, `auto-node-recovery`, in de scriptdirectory (`/app/tableau_server/packages/scripts.<version>`).

Als er een probleem is met het eerste knooppunt en er redundante processen op knooppunt 2 zijn, is er geen garantie dat Tableau Server blijft werken. Tableau Server kan tot 72 uur na een initiële knooppuntstoring blijven draaien, voordat het uitvallen van de licentieservice gevolgen heeft voor andere processen. Als dat het geval is, kunnen uw gebruikers zich mogelijk nog steeds aanmelden en hun inhoud bekijken en gebruiken nadat het eerste knooppunt uitvalt. U kunt Tableau Server echter niet opnieuw configureren, omdat u geen toegang meer hebt tot de beheercontroller.

Zelfs als Tableau Server is geconfigureerd met redundante processen, is het mogelijk dat Tableau Server niet meer functioneert nadat het eerste knooppunt uitvalt.



Om een initiële knooppuntfout (knooppunt 1) te herstellen:

1. Meld u aan bij Tableau Server-knooppunt 2.
2. Navigeer naar de scriptdirectory:

   ```
   cd /app/tableau_server/packages/scripts.<version>
   ```

3. Voer de volgende opdracht uit om het script te starten:

```
sudo ./auto-node-recovery -p node1 -n node2 -k <license keys>
```

Waar `<license keys>` een door komma's gescheiden lijst (zonder spaties) is met de licentiesleutels voor uw implementatie. Als u geen toegang hebt tot uw licentiesleutels, ga dan naar de Tableau-klantenportaal om ze op te halen. Bijvoorbeeld:

```
sudo ./auto-node-recovery -p node1 -n node2 -k TSB4-8675-309F-TW50-9RUS,TSNM-559N-ULL6-22VE-SIEN
```

Het auto-node-recovery script voert ongeveer 20 stappen uit om services op knooppunt 2 te herstellen. Elke stap wordt in de terminal weergegeven terwijl het script vordert. Een meer gedetailleerde status wordt vastgelegd in `/data/tableau_data/logs/app-controller-move.log`. In de meeste omgevingen duurt het 35 tot 45 minuten om het script te voltooien.

Problemen met het herstel van het eerste knooppunt oplossen

Als het herstellen van een knooppunt mislukt, kan het handig zijn om het script interactief uit te voeren om bepaalde stappen in het proces toe te staan of te blokkeren. Als het script bijvoorbeeld halverwege het proces mislukt, kunt u het logbestand raadplegen, wijzigingen in de configuratie aanbrengen en het script vervolgens opnieuw uitvoeren. Als u de interactieve modus gebruikt, kunt u alle stappen overslaan totdat u bij de stap komt die is mislukt.

Om in de interactieve modus te werken, voegt u de `-i`-knop toe aan het scriptargument.

Het defecte knooppunt opnieuw opbouwen

Nadat u het script hebt uitgevoerd, voert knooppunt 2 alle services uit die zich voorheen op de uitgevallen knooppunt 1-host bevonden. Om het vierde knooppunt toe te voegen, moet u een nieuwe Tableau Server-host implementeren met het bootstrapbestand en deze configureren zoals u dat voor het oorspronkelijke knooppunt 2 hebt gedaan, zoals uiteengezet in Deel 4. Zie Knooppunt 2 configureren.

switchto

Switchto is een script van Tim waarmee u eenvoudig tussen Windows kunt schakelen.

1. Kopieer de volgende code in een bestand met de naam `switchto` in de home directory op uw bastionhost.

```
#!/bin/bash
#-------------------------------------------------------------
-----
# switchto
#
# Helper function to simplify SSH into the various AWS hosts
when
# following the Tableau Server Enterprise Deployment Guide
(EDG).
#
# Place this file on your bastion host and provide your AWS
hosts'
# internal ip addresses or machine names here.
# Example: readonly NODE1="10.0.3.187"
#
readonly NODE1=""
readonly NODE2=""
readonly NODE3=""
readonly NODE4=""
readonly PGSQL=""
readonly PROXY1=""
readonly PROXY2=""

usage() {
echo "Usage: switchto.sh [ node1 | node2 | node3 | node4 |
pgsql | proxy1 | proxy2 ]"
}
```

```
ip=""

case $1 in
        node1)
                ip="$NODE1"
                ;;
        node2)
                ip="$NODE2"
                ;;
        node3)
                ip="$NODE3"
                ;;
        node4)
                ip="$NODE4"
                ;;
        pgsql)
                ip="$PGSQL"
                ;;
        proxy1)
                ip="$PROXY1"
                ;;
        proxy2)
                ip="$PROXY2"
                ;;
        ?)
                usage
                exit 0
                ;;
        *)
                echo "Unkown option $1."
                usage
                exit 1
                ;;
esac
```

```
if [[ -z $ip ]]; then
echo "You must first edit this file to provide the ip addresses
of your AWS hosts."
exit 1
fi

ssh -A ec2-user@$ip
```

2. Werk de IP-adressen in het script bij, zodat ze worden toegewezen aan uw EC2-instanties en sla het bestand vervolgens op.
3. Pas machtigingen toe op het scriptbestand:

   ```
   sudo chmod +x switchto
   ```

Gebruik:

Als u naar een host wilt overstappen, voert u de volgende opdracht uit:

```
./switchto <target>
```

Om bijvoorbeeld over te schakelen naar knooppunt 1, voert u de volgende opdracht uit:

```
./switchto node1
```

Problemen met de onafhankelijke gateway van Tableau Server oplossen

Het configureren van de onafhankelijke gateway, Okta, Mellon en SAML op Tableau Server kan een foutgevoelig proces zijn. De meest voorkomende oorzaak van fouten is een tekenreeksfout. Een afsluitende slash (`/`) op de Okta-URL's die tijdens de configuratie zijn opgegeven, kan bijvoorbeeld een SAML-assertiegerelateerde mismatch-fout veroorzaken. Dit is slechts één voorbeeld. U kunt op veel punten tijdens de configuratie een onjuiste tekenreeks invoeren in een van de toepassingen.

Start de tableau-tsig-service opnieuw

Begin (en beëindig) het oplossen van problemen altijd door de tableau-tsig-service op de onafhankelijke gateway-computers opnieuw te starten. Deze service kan snel opnieuw gestart worden en vaak wordt dan het bijgewerkte config-bestand geladen vanaf de Tableau Server.

Voer de volgende opdrachten uit op de onafhankelijke gateway-computer:

```
sudo su - tableau-tsig

systemctl --user restart tsig-httpd

exit
```

Onjuiste tekenreeksen identificeren

Als u een tekenreeksfout hebt gemaakt (fout bij het kopiëren/plakken, afgebroken tekenreeks, enz.), neem dan de tijd om alle instellingen die u hebt geconfigureerd door te nemen:

- Okta-pre-verificatieconfiguratie. Controleer zorgvuldig de URL's die u hebt ingesteld. Let op de schuine strepen aan het einde. Controleer HTTP versus HTTPS.
- Shell-geschiedenis voor SAML-configuratie op knooppunt 1. Bekijk de `tsm authentication saml configure`-opdracht die u hebt uitgevoerd. Controleer of alle URL's overeenkomen met de URL's die u in Okta hebt geconfigureerd. Terwijl u de shell-geschiedenis van knooppunt 1 bekijkt, controleert u of de `tsm configuration set`-opdrachten die de paden van de Mellon-configuratiebestanden opgeven, exact zijn toegewezen aan de bestandspaden waarnaar u de bestanden op de onafhankelijke gateway hebt gekopieerd.
- Mellon-configuratie op onafhankelijke gateway. Controleer de shellgeschiedenis om te verifiëren of u de metadata hebt gemaakt met dezelfde URL-tekenreeks die u hebt geconfigureerd in Okta en Tableau SAML. Controleer of alle paden die zijn opgegeven in `/etc/mellon/conf.d/global.conf` kloppen en dat de `MellonCookieDomain` is ingesteld op uw hoofddomein, niet op uw Tableau-subdomein.

Relevante logboeken zoeken

Als alle tekenreeksen correct lijken te zijn ingesteld, moet u de logboeken controleren op fouten.

Tableau Server registreert fouten en gebeurtenissen in tientallen verschillende logbestanden. De onafhankelijke gateway registreert ook data in een aantal lokale bestanden. Wij adviseren u om deze logboeken in de volgende volgorde te controleren.

Logbestanden van de onafhankelijke gateway

De standaardlocatie van de logbestanden van de onafhankelijke gateway is `/var/opt/tableau/tableau_tsig/logs`.

- `access.log`: dit logboek is nuttig omdat het vermeldingen bevat die verbindingen van de Tableau Server-knooppunten weergeven. Als u gatewayfouten krijgt (start niet) wanneer u TSM probeert te starten en er geen vermeldingen in de `access.log` bestand, dan is er een kernprobleem met de connectiviteit. Controleer altijd als eerste stap de configuratie van de AWS-beveiligingsgroep. Een ander veelvoorkomend probleem is een typefout in `tsig.json`. Als u tsig.json bijwerkt, voer dan `tsm stop` uit voordat u `tsm topology external-services gateway update -c tsig.json` uitvoert. Nadat tsig.json is bijgewerkt, voert u `tsm start` uit.
- `error.log`: dit logboek bevat onder andere SAML- en Mellon-fouten.

Tableau Server tabadminagent-logbestand

De bestanden `tabadminagent` (niet `tabadmincontroller`) zijn de enige relevante logbestanden voor het oplossen van problemen met de onafhankelijke gateway.

U moet achterhalen waar de fouten van de onafhankelijke gateway zijn vastgelegd in `tabdminagent`. Deze fouten kunnen op elk knooppunt voorkomen, maar ze komen slechts op één knooppunt tegelijk voor. Voer de volgende stappen uit op elk knooppunt in het Tableau Server-cluster totdat u de tekenreeks 'onafhankelijk' vindt:

1. Zoek de locatie van het tabadminagent-logbestand op Tableau Server-knooppunten 1-4 in de EDG-installatie:

   ```
   cd /data/tableau_data/data/tabsvc/logs/tabadminagent
   ```

2. Open het laatste logboek om dit te lezen:

   ```
   less tabadminagent_nodeN.log
   ```

   (vervang N door knooppuntnummer)

3. Zoek naar alle instanties van 'Independent' en 'independent' door de volgende zoekreeks te gebruiken:

   ```
   /ndependent
   ```

   Zijn er geen overeenkomsten? Ga dan naar het volgende knooppunt en herhaal stappen 1-3.

4. Wanneer u een overeenkomst krijgt: `Shift + G` om naar beneden te gaan en de laatste foutmeldingen te zien.

httpd stub-bestand opnieuw laden

De onafhankelijke gateway beheert de configuratie van httpd voor Apache. Een algemene bewerking die vaak tijdelijke problemen oplost, is het opnieuw laden van het httpd-stub-bestand dat de onderliggende Apache-configuratie bevat. Voer de volgende opdrachten uit op beide instanties van de onafhankelijke gateway.

1. Kopieer het stub-bestand naar httpd.conf:

   ```
   cp /var/opt/tableau/tableau_tsig/config/httpd.conf.stub /var/opt/tableau/tableau_tsig/config/httpd.conf
   ```

2. Start de onafhankelijke gateway-service opnieuw:

```
sudo su - tableau-tsig
systemctl --user restart tsig-httpd
exit
```

Logbestanden verwijderen of verplaatsen

De onafhankelijke gateway registreert alle toegangsgebeurtenissen. U moet de opslag van logbestanden beheren om te voorkomen dat de schijfruimte vol raakt. Als uw schijf vol raakt, kan de onafhankelijke gateway geen toegangsgebeurtenissen meer schrijven en mislukt de service. Het volgende bericht wordt dan vastgelegd in error.log op de onafhankelijke gateway:

```
(28)No space left on device: [client 10.0.2.209:54332] AH00646:
Error writing to /var/opt/tableau/tableau_tsig/logs-
/access.%Y_%m_%d_%H_%M_%S.log
```

Deze mislukking zal resulteren in de status `DEGRADED` voor het`external` knooppunt wanneer u `tsm status -v` uitvoert op Tableau knooppunt 1. Het `external` knooppunt in de statusuitvoer verwijst naar de onafhankelijke gateway.

U kunt dit probleem oplossen door de access.log-bestanden van de schijf te verwijderen of te verplaatsen. Access.log-bestanden worden opgeslagen op `/var/opt/tableau/tableau_tsig/logs`. Nadat u de schijf hebt gewist, start u de tableau-tsig-service opnieuw.

Browserfouten

Bad Request (Ongeldige aanvraag): een veelvoorkomende fout in dit scenario is de foutmelding Bad Request (ongeldige aanvraag) van Okta. Dit probleem doet zich vaak voor wanneer de browser data van een eerdere Okta-sessie cachet. Als u bijvoorbeeld de Okta-toepassingen beheert als Okta-beheerder en vervolgens probeert toegang te krijgen tot Tableau met een ander Okta-account, kunnen sessiegegevens van de beheerdersgegevens de fout 'Bad Request' veroorzaken. Als deze fout zich zelfs nadat u de lokale browsercache

hebt gewist blijft voordoen, probeer dan het Tableau-scenario te valideren door verbinding te maken met een andere browser.

Een andere oorzaak van de fout 'Bad Request' is een typefout in een van de vele URL's die u invoert tijdens de configuratieprocessen van Okta, Mellon en SAML. Controleer of u al deze gegevens zonder fouten hebt ingevoerd.

Vaak staat in het `error.log`-bestand op de onafhankelijke gateway-server welke URL de fout veroorzaakt.

Not Found - The requested URL was not found on this server (Niet gevonden - De gevraagde URL is niet gevonden op deze server): deze fout geeft aan dat er sprake is van een van de vele configuratiefouten.

Als de gebruiker is geverifieerd met Okta en vervolgens deze foutmelding krijgt, is het waarschijnlijk dat u de Okta-toepassing vóór verificatie hebt geüpload naar Tableau Server toen u SAML configureerde. Controleer of u de Okta Tableau Server-toepassingsmetadata hebt geconfigureerd op Tableau Server, en niet de Okta pre-auth-toepassingsmetadata

Andere stappen voor probleemoplossing:

- Controleer de pre-auth-toepassingsinstellingen voor Okta. Zorg ervoor dat de HTTP- en HTTPS-protocollen zijn ingesteld zoals aangegeven in dit onderwerp.
- Start tsig-httpd opnieuw op beide onafhankelijke gateway-servers.
- Controleer of `sudo apachectl configtest` 'Syntax OK' retourneert op beide onafhankelijke gateways.
- Controleer of de testgebruiker aan beide toepassingen in Okta is toegewezen.
- Controleer of kleverigheid is ingesteld op de Load Balancer en de bijbehorende doelgroepen.

De TLS-verbinding van Tableau Server naar de onafhankelijke gateway verifiëren

Gebruik de `wget`-opdracht om de connectiviteit en toegang van Tableau Server naar de onafhankelijke gateway te verifiëren. Variaties op deze opdracht kunnen u helpen te achterhalen of

certificaatproblemen verbindingsproblemen veroorzaken.

Voer bijvoorbeeld deze `wget`-opdracht uit om het housekeeping (HK)-protocol van Tableau Server te verifiëren:

```
wget https://ip-10-0-1-38.us-west-1.compute.internal:21319
```

Maak de URL met hetzelfde hostadres dat u hebt opgegeven voor de hostoptie van het bestand tsig.json. Geef het `https`-protocol op en voeg de URL toe met de HK-poort `21319`.

Om de connectiviteit te controleren en certificaatverificatie te negeren:

```
wget https://ip-10-0-1-38.us-west-1.compute.internal:21319 --no-check-certificate
```

Om te verifiëren of het root-CA-certificaat voor TSIG geldig is:

```
wget https://ip-10-0-1-38.us-west-1.compute.internal:21319 --ca-certificate=tsigRootCA.pem
```

Als Tableau kan communiceren, kunt u nog steeds inhoudsgerelateerde fouten krijgen, maar u krijgt geen verbindingsgerelateerde fouten. Als Tableau helemaal geen verbinding kan maken, controleer dan eerst de protocolconfiguratie in de firewall/beveiligingsgroepen. De inkomende regels voor de beveiligingsgroep waarin de onafhankelijke gateway zich bevindt, moeten bijvoorbeeld TCP 21319 toestaan.

Bijlage - AWS Deployment Toolbox

Dit onderwerp bevat tools en alternatieve implementatieopties voor de referentiearchitectuur bij het implementeren in AWS. Dit onderwerp beschrijft specifiek hoe u de AWS-voorbeeldimplementatie kunt automatiseren die in de EDG wordt beschreven.

Geautomatiseerd installatiescript TabDeploy4EDG

Het TabDeploy4EDG-script automatiseert de Tableau-implementatie met vier knooppunten die wordt beschreven in Deel 4 – Tableau Server installeren en configureren. Als u de AWS-voorbeeldimplementatie volgt zoals beschreven in deze handleiding, kunt u mogelijk TabDeploy4EDG uitvoeren.

Vereisten. Om het script uit te voeren, moet u de AWS-omgeving voorbereiden en configureren volgens de voorbeeldimplementatie in Deel 3 – De implementatie van Tableau Server Enterprise voorbereiden:

- VPC, subnet en beveiligingsgroepen moeten zijn geconfigureerd zoals beschreven. IP-adressen hoeven niet overeen te komen met de adressen die in de voorbeeldimplementatie worden weergegeven.
- Vier EC2-instanties met de nieuwste, bijgewerkte builds van AWS Linux 2.
- PostgreSQL is geïnstalleerd en geconfigureerd zoals beschreven in PostgreSQL installeren, configureren en tarren.
- Een in Stap 1 gemaakt tar-back-upbestand bevindt zich op de EC2-instantie waar PostgreSQL is geïnstalleerd, zoals beschreven in Tar-back-up van PostgreSQL Stap 1 maken.
- De EC2-instantie die knooppunt 1 van de Tableau Server-implementatie zal uitvoeren, is geconfigureerd om te communiceren met PostgreSQL zoals beschreven in Deel 4 – Tableau Server installeren en configureren.
- U bent bij elke EC2-instantie ingelogd met een SSH-sessie vanaf de bastionhost.

Het script heeft ongeveer 1,5 tot 2 uur nodig om de vier Tableau-servers te installeren en configureren. Het script configureert Tableau volgens de voorgeschreven instellingen van de referentiearchitectuur. Het script voert de volgende acties uit:

- Herstelt de Stap 1-back-up van de PostgreSQL-host als u een pad naar het tar-bestand van de PostgreSQL-host opgeeft.
- Verwijdert bestaande Tableau-installaties voor alle knooppunten.
- Voert `sudo yum update` uit voor alle knooppunten.
- Downloadt en kopieert het Tableau rpm-pakket naar elk knooppunt.
- Downloadt en installeert afhankelijkheden voor elk knooppunt.
- Creëert `/app/tableau_server` en installeert het pakket voor alle knooppunten.
- Installeert Knooppunt 1 met een lokale identiteitenarchief en configureert een externe opslagplaats met PostgreSQL.
- Voert bootstrap-installatie en initiële configuratie van Knooppunt 2 tot Knooppunt 4 uit.
- Verwijdert het bootstrap-bestand en het configuratiebestand voor TabDeploy4EDG.
- Configureert services in het Tableau-cluster volgens de specificaties van de referentiearchitectuur.
- Valideert de installatie en retourneert de status voor elk knooppunt.

Het script downloaden en kopiëren naar de bastionhost

1. Kopieer het script van de TabDeploy4EDG-voorbeeldpagina en plak de code in een bestand met de naam: `TabDeploy4EDG`.
2. Sla het bestand op in de homedirectory van de EC2-host die als bastionhost fungeert.
3. Voer de volgende opdracht uit om de modus van het bestand te wijzigen, zodat het uitvoerbaar wordt:

```
sudo chmod +x TabDeploy4EDG
```

TabDeploy4EDG uitvoeren

TabDeploy4EDG moet worden uitgevoerd vanaf de bastionhost. Het script is geschreven met de veronderstelling dat u onder de context van ssh agent forwarding draait zoals beschreven in Voorbeeld: verbinding maken met bastionhost in AWS. Als u niet met ssh agent forwarding-context werkt, wordt u tijdens het installatieproces om wachtwoorden gevraagd.

1. Maak een registratiebestand (`registration.json`) aan, bewerk het en sla het op. Het bestand moet een correct geformatteerd JSON-bestand zijn. Kopieer de volgende sjabloon en pas die aan:

   ```
   {
          "zip" : "97403",
          "country" : "USA",
          "city" : "Springfield",
          "last_name" : "Simpson",
          "industry" : "Energy",
          "eula" : "yes",
          "title" : "Safety Inspection Engineer",
          "phone" : "5558675309",
          "company" : "Example",
          "state" : "OR",
          "department" : "Engineering",
          "first_name" : "Homer",
          "email" : "homer@example.com"
   }
   ```

2. Voer de volgende opdracht uit om een sjabloonconfiguratiebestand te genereren:

   ```
   ./TabDeploy4EDG -g edg.config
   ```

3. Open het configuratiebestand om te bewerken:

   ```
   sudo nano edg.config
   ```

   U moet minimaal de IP-adressen van elke EC2-host, een bestandspad naar het registratiebestand en een geldige licentiesleutel toevoegen.

4. Wanneer u klaar bent met het bewerken van het configuratiebestand, slaat u het op en sluit u het.

5. Om TabDeploy4EDG uit te voeren, gebruikt u de volgende opdracht:

   ```
   ./TabDeploy4EDG -f edg.config
   ```

Voorbeeld: de implementatie van AWS-infrastructuur automatiseren met Terraform

In deze sectie wordt beschreven hoe u Terraform configureert en uitvoert om de EDG-referentiearchitectuur in AWS te implementeren. De hier gepresenteerde Terraform-voorbeeldconfiguratie implementeert een AWS VPC met de subnetten, beveiligingsgroepen en EC2-instanties zoals beschreven in Deel 3 – De implementatie van Tableau Server Enterprise voorbereiden.

Voorbeelden van Terraform-sjablonen zijn beschikbaar op de website met Tableau-voorbeelden via https://help.tableau.com/samples/en-us/edg/edg-terraform.zip. Deze sjablonen moeten worden geconfigureerd en aangepast voor uw organisatie. De configuratie-inhoud in deze sectie beschrijft de minimale vereiste sjabloonwijzigingen die u moet aanbrengen alvorens te kunnen implementeren.

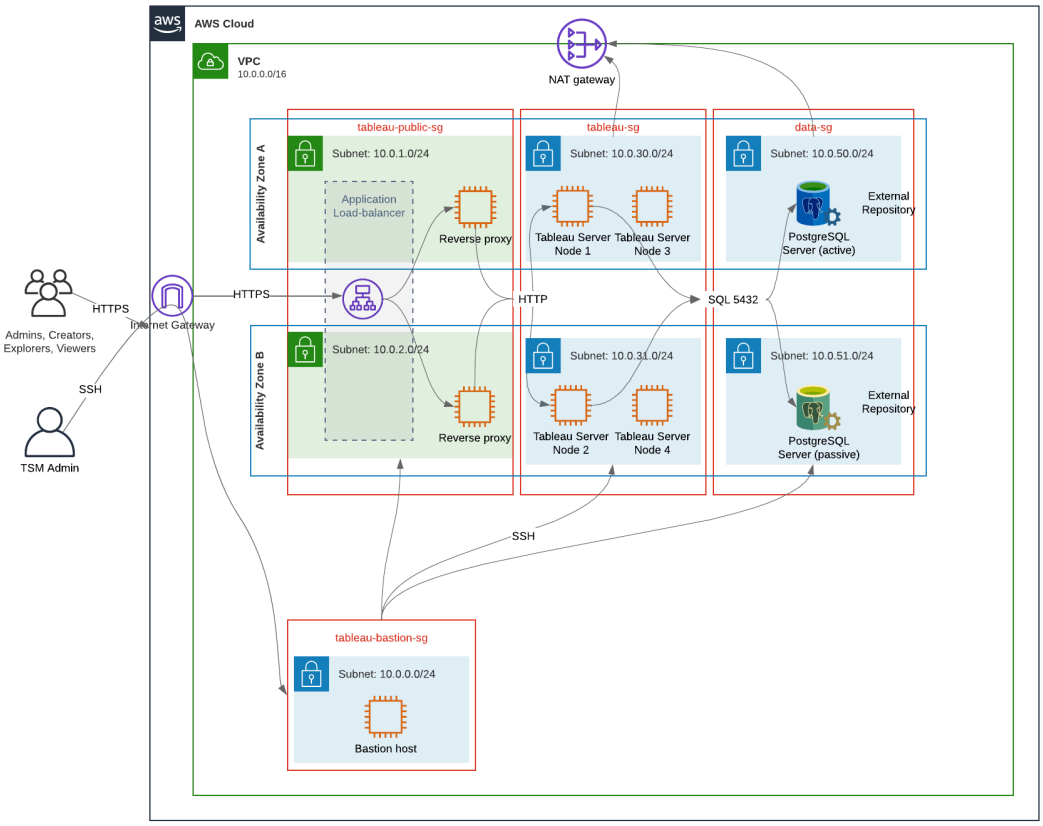
Doel

De Terraform-sjablonen en inhoud die hier worden aangeboden, zijn bedoeld om een werkend voorbeeld te bieden waarmee u EDG snel kunt implementeren in een ontwikkel-/testomgeving.

We hebben ons uiterste best gedaan om de Terraform-voorbeeldimplementatie te testen en te documenteren. Het gebruik van Terraform om EDG in een productieomgeving te implementeren en onderhouden, vereist echter Terraform-expertise die buiten het bereik van dit voorbeeld valt. Tableau biedt geen ondersteuning voor de hier beschreven Terraform-voorbeeldoplossing.

Eindstatus

Volg de procedure in deze sectie om een VPC in AWS in te stellen die functioneel gelijkwaardig is aan de VPC die is gespecificeerd in Deel 3 – De implementatie van Tableau Server Enterprise voorbereiden.



De voorbeeld Terraform-sjablonen en ondersteunende inhoud in deze sectie:

- Maken een VPC met een elastisch IP-adres, twee beschikbaarheidszones en een sub-netorganisatie zoals hierboven weergegeven (IP-adressen zijn verschillend).
- Maken de beveiligingsgroepen Bastion, Openbaar, Privé en Data aan.
- Stellen de meeste in- en uitgangsregels in voor de beveiligingsgroepen. U moet de beveiligingsgroepen bewerken nadat Terraform is uitgevoerd.
- Maken de volgende EC2-hosts aan (elk met AWS Linux2): bastion, proxy 1 proxy 2, Tableau-knooppunt 1, Tableau-knooppunt 2, Tableau-knooppunt 3, Tableau-knooppunt 4.
- EC2-hosts voor PostgreSQL worden niet aangemaakt. U moet EC2 handmatig aan-maken in de beveiligingsgroep Data en vervolgens PostgreSQL installeren en con-figureren zoals beschreven in PostgreSQL installeren, configureren en tarren.

Vereisten

- AWS-account: u moet toegang hebben tot een AWS-account waarmee u VPC's kunt maken.
- Als u Terraform vanaf een Windows-computer uitvoert, moet u AWS CLI installeren.
- Een beschikbaar elastisch IP-adres in uw AWS-account.
- Een domein dat geregistreerd is in AWS Route 53. Terraform creëert een DNS-zone en bijbehorende SSL-certificaten in Route 53. Daarom moet het profiel waaronder Terraform draait ook de juiste machtigingen hebben in Route 53.

Voordat u begint

- De voorbeelden van de opdrachtregels in deze procedure zijn voor het gebruik van een terminal met Apple OS. Als u Terraform op Windows gebruikt, moet u de opdrachten mogelijk aanpassen met de juiste bestandspaden.
- Een Terraform-project bestaat uit een groot aantal tekstconfiguratiebestanden (bestandsextensie .tf). U configureert Terraform door deze bestanden aan te passen. Als u niet over een krachtige teksteditor beschikt, installeer dan Atom of Text++.
- Als u het Terraform-project met anderen deelt, raden wij u aan het project in Git op te slaan voor wijzigingsbeheer.

Stap 1 – Omgeving voorbereiden

A. Terraform downloaden en installeren

https://www.terraform.io/downloads

B. Een sleutelpaar privé-openbaar genereren

Dit is de sleutel die u gebruikt om toegang te krijgen tot AWS en de resulterende VPC-omgeving. Wanneer u Terraform uitvoert, neemt u daarin de openbare sleutel op.

Open de terminal en voer de volgende opdrachten uit:

1. Maak een privésleutel. Bijvoorbeeld `my-key.pem`:

   ```
   openssl genrsa -out my-key.pem 1024
   ```

2. Maak een openbare sleutel. Deze sleutelindeling wordt niet gebruikt voor Terraform. Later in deze procedure converteert u deze naar een ssh-sleutel:

   ```
   openssl rsa -in my-key.pem -pubout > my-key.pub
   ```

3. Stel machtigingen in voor de privésleutel:

   ```
   sudo chmod 0600 my-key.pem
   ```

   Voor het instellen van machtigingen in Windows:

   - Vind het bestand in Windows Verkenner, klik er met de rechtermuisknop op en selecteer **Eigenschappen**. Navigeer naar het tabblad **Beveiliging** en klik vervolgens op **Geavanceerd**.
   - Wijzig de eigenaar naar uzelf, schakel overerving uit en verwijder alle machtigingen. Geef uzelf **Volledig beheer** en klik dan op **Opslaan**. Markeer het bestand als alleen-lezen.

4. Maak een openbare ssh-sleutel. Dit is de sleutel die u later in het proces naar Terraform kopieert.

   ```
   ssh-keygen -y -f my-key.pem >my-key-ssh.pub
   ```

C. Project downloaden en statusdirectory toevoegen

1. Download het EDG Terraform-project, pak het uit en sla het op uw lokale computer op. Nadat u de download hebt uitgepakt, hebt u een hoofddirectory, edg-terraform en een reeks subdirectory's.

2. Maak een directory met de naam `state`, op hetzelfde niveau als de hoofddirectory `edg-terraform`.

Stap 2 - De Terraform-sjablonen aanpassen

U moet de Terraform-sjablonen aanpassen aan uw AWS- en EDG-omgeving. Het onderstaande voorbeeld toont de minimale aanpassingen die de meeste organisaties in een sjabloon moeten doorvoeren. Het is mogelijk dat uw specifieke omgeving andere aanpassingen vereist.

Deze sectie is georganiseerd op sjabloonnaam.

Zorg ervoor dat u alle wijzigingen opslaat voordat u verdergaat naar *Stap 3 – Terraform uitvoeren*.

versies.tf

Er zijn drie instanties van de bestanden `versions.tf` waar het veld `required_version` overeen moet komen met de versie van terraform.exe die u gebruikt. Controleer de versie van Terraform (`terraform.exe -version`) en werk elk van de volgende instanties bij:

- `edg-terraform\versions.tf`
- `edg-terraform\modules\proxy\versions.tf`
- `edg-terraform\modules\tableau_instance\versions.tf`

sleutelpaar.tf

1. Open de openbare sleutel die u in stap 1B hebt gegenereerd en kopieer de sleutel:

   ```
   less my-key-ssh.pub
   ```

   Windows: kopieer de inhoud van uw openbare sleutel.

2. Kopieer de openbare sleutelreeks naar het public_key argument, bijvoorbeeld:

   ```
   resource "aws_key_pair" "tableau" {
   key_name = "my-key"
   public_key = "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgQ (truncated
   example) dZVHambOCw=="
   ```

Zorg ervoor dat de waarde `key_name` uniek is in het datacenter, anders zal `terraform apply` mislukken.

lokale.tf

Werk `user.owner` bij naar uw naam of alias. De waarde die u hier invoert, wordt gebruikt voor de tag 'Naam' in AWS voor de resources die Terraform maakt.

aanbieders.tf

1. Voeg tags toe volgens de vereisten van uw organisatie. Bijvoorbeeld:

```
default_tags {
  tags = {

   "Application" = "tableau",
   "Creator" = "alias@example.com",
   "DeptCode" = "8675309",
   "Description" = "EDG",
   "Environment" = "test",
   "Group" = "itcloud@example.com"
  }
}
```

2. Als u gebruik maakt van `provider`, voeg dan commentaar toe aan de lijnen `assume_role`:

```
/* assume_role {
role_arn     = "arn:aws:iam::310946706895:role/terraform-bac-
kend"
session_name = "terraform"
}*/
```

elb.tf

Kies onder `'resource "aws_lb" "tableau" {'` een unieke waarde om te gebruiken voor `name` en `tags.Name`.

Als een andere AWS-loadbalancer dezelfde naam heeft in het datacenter, dan zal `terraform apply` mislukken.

Voeg `idle_timeout` toe:

```
resource "aws_lb" "tableau" {
name                       = "edg-again-alb"
load_balancer_type         = "application"
```

```
subnets                    = [for subnet in aws_subnet.public : sub-
net.id]
security_groups            = [aws_security_group.public.id]
drop_invalid_header_fields = true
idle_timeout               = 400
tags = {
Name = "edg-again-alb"
}
                       }
```

variabelen.tf

Rootdomeinnaam bijwerken. Deze naam moet overeenkomen met het domein dat u bij Route 53 hebt geregistreerd.

```
variable "root_domain_name" {
 default = "example.com"
 }
```

Standaard is het subdomein, `tableau`, opgegeven als de VPC DNS-domeinnaam. Om dit te veranderen, werkt u `subdomain` bij:

```
variable "subdomain" {
 default = "tableau"
}
```

modules/tableau_instantie/ec2.tf

Het project bevat twee ec2.tf-bestanden. Deze aanpassing is voor de Tableau-instantie van ec2.tf in de directory: `modules/tableau_instance/ec2.tf`.

- Voeg indien nodig blobtags toe:

  ```
  tags = {
   "Name" : var.ec2_name,
   "user.owner" = "ALIAS",
   "Application" = "tableau",
   "Creator" = "ALIAS@example.com",
  ```

```
 "DeptCode" = "8675309",
 "Description" = "EDG",
 "Environment" = "test",
 "Group" = "itcloud@example.com"
 }
}
```

- Indien nodig kunt u uw opslag bijwerken om aan uw datavereisten te voldoen:

  Rootvolume:

  ```
  root_block_device {
   volume_size = 100
   volume_type = "gp3"
  }
  ```

  Toepassingsvolume:

  ```
  resource "aws_ebs_volume" "tableau" {
   availability_zone = data.aws_subnet.tableau.availability_zone
   size              = 500
   type              = "gp3"
  }
  ```

Stap 3 - Terraform uitvoeren

A. Terraform initialiseren

Ga op de terminal naar de directory `edg-terraform` en voer de volgende opdracht uit:

```
terraform init
```

Als de initialisatie succesvol is, gaat u verder met de volgende stap. Als de initialisatie mislukt, volgt u de instructies in de Terraform-uitvoer.

B. Terraform plannen

Voer vanuit dezelfde directory de opdracht 'plan' uit:

```
terraform plan
```

Deze opdracht kan meerdere keren worden uitgevoerd. Voer het zo vaak uit als nodig is om fouten te herstellen. Wanneer deze opdracht foutloos is uitgevoerd, gaat u verder met de volgende stap.

C. Terraform toepassen

Voer vanuit dezelfde directory de opdracht 'apply' uit:

```
terraform apply
```

Terraform zal u vragen om de implementatie te verifiëren. Typ `Yes`.

Optioneel: Terraform vernietigen

U kunt de volledige VPC vernietigen door de opdracht 'destroy' uit te voeren:

```
terraform destroy
```

De vernietigingsopdracht vernietigt alleen wat het zelf heeft gecreëerd. Als u handmatige wijzigingen hebt aangebracht in een aantal objecten in AWS (bijvoorbeeld beveiligingsgroepen, subnetten, enz.) zal `destroy` mislukken. Om een mislukte/vastgelopen vernietigingsbewerking te beëindigen, typt u `Control + C`. Vervolgens moet u de VPC handmatig opschonen en terugbrengen naar de staat waarin deze zich bevond toen Terraform deze oorspronkelijk aanmaakte. Dan kunt u de opdracht `destroy` uitvoeren.

Stap 4 - Verbinding maken met bastion

Alle opdrachtregelverbindingen verlopen via de bastionhost op TCP 22 (SSH-protocol).

1. Maak in AWS een inkomende regel in de beveiligingsgroep Bastion (**AWS** > **Beveiligingsgroepen** > **Bastion** > **Inkomende regels bewerken**) en maak een regel om SSH (TCP 22)-verbindingen toe te staan vanaf het IP-adres of subnetmasker waarop u terminal-opdrachten uitvoert.

Optioneel: het kan handig zijn om het kopiëren van bestanden tussen de EC2-instanties in de groepen Privé en Openbaar toe te staan tijdens de implementatie. Maak inkomende SSH-regels:

- Privé: maak een inkomende regel om SSH toe te staan vanaf Openbaar
- Openbaar: maak een inkomende regel om SSH toe te staan vanaf Privé en Openbaar

2. Gebruik de pem-sleutel die u in stap 1.B hebt gemaakt om verbinding te maken met de bastionhost:

   Op een Mac-terminal:

   Voer de volgende opdrachten uit vanuit de directory waar de pem-sleutel is opgeslagen:

   ```
   ssh-add —apple-use-keychain <keyName>.pem
   ```

   Als u een waarschuwing krijgt dat de privésleutel voor anderen toegankelijk is, voer dan de volgende opdracht uit: `chmod 600 <keyName.pem>` en voer daarna de opdracht `ssh-add` opnieuw uit.

   Maak verbinding met de bastionhost door middel van deze opdracht: `ssh -A ec2-user@IPaddress`

   Bijvoorbeeld: `ssh -A ec2-user@3.15.12.112.`

   Op Windows, gebruikmakend van PuTTY en Pageant:

   a. Maak een ppk van een pem-sleutel: gebruik PuTTY Key Generator. Laad de pem-sleutel die u in stap 1.B hebt gemaakt. Klik na het importeren van de sleutel op **Privésleutel opslaan**. Hiermee wordt een ppk-bestand gemaakt.

   b. Open in PuTTY de configuratie en breng de volgende wijzigingen aan:

      - Sessies>Hostnaam: voeg het IP-adres van de bastionhost toe.
      - Sessies>Poort: 22
      - Verbinding>Data>Automatisch inloggen gebruikersnaam: ec2-user

- Verbinding>SSH>Auth>Agent forwarding toestaan
- Verbinding>SSH>Auth> Voor de privésleutel klikt u op Bladeren en selecteert u het .ppk-bestand dat u zojuist hebt gemaakt.

c. Installeer Pageant en laad de ppk in de toepassing.

Stap 5 – PostgreSQL installeren

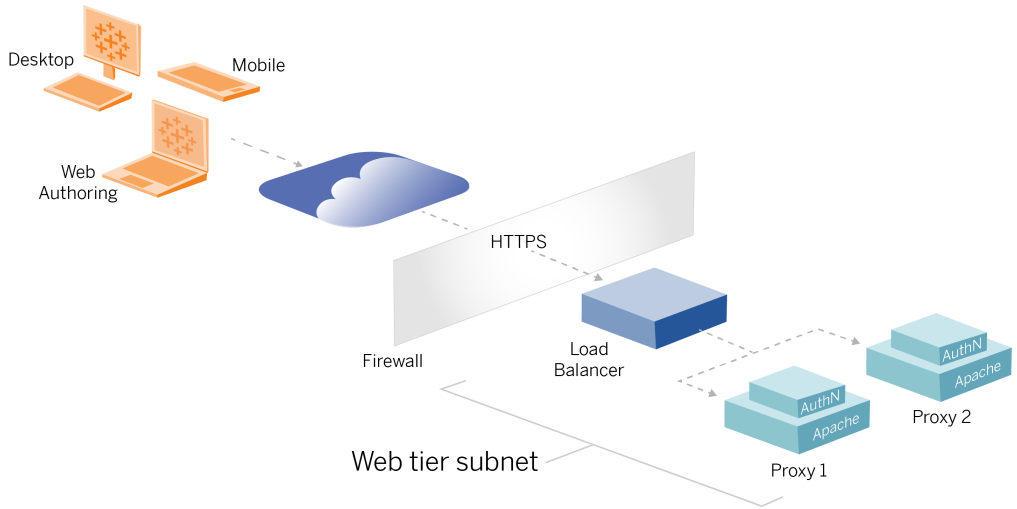
De Terraform-sjabloon installeert PostgreSQL niet voor gebruik als externe opslagplaats. De bijbehorende beveiligingsgroep en het bijbehorende subnet worden echter wel aangemaakt. Als u de externe opslagplaats op een EC2-instantie met PostgreSQL wilt installeren, moet u de EC2-instantie implementeren zoals beschreven in Deel 3 – De implementatie van Tableau Server Enterprise voorbereiden.

Vervolgens installeert en configureert u PostgreSQL en maakt u er een tar-back-up van, volgens de beschrijving in Deel 4 – Tableau Server installeren en configureren.

Stap 6 – (Optioneel) DeployTab4EDG uitvoeren

Het TabDeploy4EDG-script automatiseert de Tableau-implementatie met vier knooppunten die wordt beschreven in Deel 4. Zie Geautomatiseerd installatiescript TabDeploy4EDG.

Bijlage - Voorbeeldimplementatie van weblaag met Apache



Dit onderwerp bevat een end-to-end-procedure die beschrijft hoe u een weblaag implementeert in de voorbeeld-AWS-referentiearchitectuur. De voorbeeldconfiguratie bestaat uit de volgende componenten:

- Loadbalancer van AWS-toepassing
- Apache-proxyservers
- Mellon-verificatiemodule
- Okta IdP
- SAML-verificatie

Opmerking: de voorbeeldweblaagconfiguratie die in deze sectie wordt gepresenteerd, bevat gedetailleerde procedures voor het implementeren van software en services van derden. We hebben ons uiterste best gedaan om de procedures voor het realiseren van het weblaagscenario te verifiëren en te documenteren. De software van derden kan echter veranderen of uw scenario kan afwijken van de hier beschreven referentiearchitectuur.

Raadpleeg de documentatie van derden voor betrouwbare configuratiegegevens en ondersteuning.

De Linux-voorbeelden in deze sectie tonen opdrachten voor RHEL-achtige distributies. De opdrachten hier zijn specifiek ontwikkeld met de Amazon Linux 2-distributie. Als u de Ubuntu-distributie gebruikt, moet u de opdrachten dienovereenkomstig bewerken.

Het implementeren van de weblaag in dit voorbeeld verloopt volgens een stapsgewijze configuratie- en verificatieprocedure. De kernconfiguratie van de weblaag bestaat uit de volgende stappen om HTTP-verkeer tussen Tableau en internet mogelijk te maken. Apache wordt uitgevoerd en geconfigureerd voor reverse proxy/taakverdeling achter de loadbalancer van de AWS-toepassing:

1. Apache installeren
2. Reverse proxy configureren om de connectiviteit met Tableau Server te testen
3. Taakverdeling op proxy configureren
4. Loadbalancer van AWS-toepassing configureren

Nadat de weblaag is ingesteld en de connectiviteit met Tableau is geverifieerd, configureert u de verificatie met een externe provider.

Apache installeren

Voer de volgende procedure uit op beide EC2-hosts (Proxy 1 en Proxy 2). Als u in AWS implementeert volgens het referentiearchitectuurvoorbeeld, moet u over twee beschikbaarheidszones beschikken en in elke zone één proxyserver uitvoeren.

1. Apache installeren:

   ```
   sudo yum update -y
   sudo yum install -y httpd
   ```

2. Definieer de configuratie zodanig dat Apache wordt gestart bij opnieuw opstarten:

```
sudo systemctl enable --now httpd
```

3. Controleer of de door u geïnstalleerde versie van httpd `proxy_hcheck_module` bevat:

   ```
   sudo httpd -M
   ```

   De `proxy_hcheck_module` is vereist. Als uw versie van httpd deze module niet bevat, moet u een update uitvoeren naar een versie van httpd die deze module wel bevat.

Proxy configureren om de connectiviteit met Tableau Server te testen

Voer deze procedure uit op een van de proxyhosts (Proxy 1). Het doel van deze stap is om de connectiviteit tussen internet, uw proxyserver en de Tableau-server in de privébeveiligingsgroep te controleren.

1. Maak een bestand met de naam `tableau.conf` en voeg het toe aan de map `/etc/httpd/conf.d`.

   Kopieer de volgende code en geef de sleutels `ProxyPass` en `ProxyPassReverse` op met het privé-IP-adres van Tableau Server-knooppunt 1.

   > **Belangrijk**: de onderstaande configuratie is niet beveiligd en mag niet in productie worden gebruikt. Deze configuratie mag alleen tijdens het installatieproces worden gebruikt om de end-to-end-connectiviteit te verifiëren.

   Als het privé-IP-adres van knooppunt 1 bijvoorbeeld `10.0.30.32` is, is de inhoud van het bestand `tableau.conf` als volgt:

   ```
   <VirtualHost *:80>
   ProxyPreserveHost On
   ProxyPass "/" "http://10.0.30.32:80/"
   ```

```
ProxyPassReverse "/" "http://10.0.30.32:80/"
</VirtualHost>
```

2. Start httpd opnieuw:

   ```
   sudo systemctl restart httpd
   ```

Verificatie: configuratie van basistopologie

U kunt toegang krijgen tot de beheerpagina van Tableau Server door naar `http://<proxy-public-IP-address>` te bladeren.

Als de aanmeldingspagina van Tableau Server niet in uw browser wordt geladen, volgt u deze stappen voor probleemoplossing op de Proxy 1-host:

- Stop en start httpd als eerste stap bij het oplossen van problemen.
- Controleer het bestand `tableau.conf`. Controleer of het privé-IP-adres van knooppunt 1 correct is. Controleer dubbele aanhalingstekens en de syntaxis zorgvuldig.
- Voer de opdracht `curl` op de reverse-proxyserver uit met het privé-IP-adres van knooppunt 1, bijvoorbeeld, `curl 10.0.1.90`. Als de shell geen HTML retourneert of als HTML wordt geretourneerd voor de Apache-testwebpagina, controleer dan de protocol-/poortconfiguratie tussen de openbare en privébeveiligingsgroep.
- Voer de opdracht `curl` uit met het privé IP-adres van Proxy 1, bijvoorbeeld, `curl 10.0.0.163`. Als de shell de HTML-code voor de Apache-testwebpagina retourneert, is het proxybestand niet correct geconfigureerd.
- Start httpd altijd opnieuw op (`sudo systemctl restart httpd`) na configuratiewijzigingen in het proxybestand of in de beveiligingsgroepen.
- Zorg ervoor dat TSM op knooppunt 1 draait.

Taakverdeling op proxy configureren

1. Verwijder de bestaande Virtual Host-configuratie op dezelfde proxyhost (Proxy 1) als waar u het bestand `tableau.conf` hebt gemaakt en bewerk het bestand door er taakverdelingslogica aan toe te voegen.

   Bijvoorbeeld:

```
<VirtualHost *:80>
ServerAdmin admin@example.com
#Load balancing logic.
ProxyHCExpr ok234 {%{REQUEST_STATUS} =~ /^[234]/}
Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e;
path=/" env=BALANCER_ROUTE_CHANGED
<Proxy balancer://tableau>
#Replace IP addresses below with the IP addresses to the
Tableau Servers running the Gateway service.
BalancerMember http://10.0.3.40/ route=1 hcmethod=GET hcex-
pr=ok234 hcuri=/favicon.ico
BalancerMember http://10.0.4.151/ route=2 hcmethod=GET hcex-
pr=ok234 hcuri=/favicon.ico
ProxySet stickysession=ROUTEID
</Proxy>
ProxyPreserveHost On
ProxyPass / balancer://tableau/
ProxyPassReverse / balancer://tableau/
</VirtualHost>
```

2. Stop en start httpd:

```
sudo systemctl stop httpd
sudo systemctl start httpd
```

3. Controleer de configuratie door naar het openbare IP-adres van Proxy 1 te gaan.

Configuratie naar tweede proxyserver kopiëren

1. Kopieer het bestand `tableau.conf` van Proxy 1 en sla het op in de map `/etc/httpd/conf.d` op de host Proxy 2.

2. Stop en start httpd:

```
sudo systemctl stop httpd
sudo systemctl start httpd
```

3. Controleer de configuratie door naar het openbare IP-adres van Proxy 2 te gaan.

Loadbalancer van AWS-toepassing configureren

Configureer de loadbalancer als een HTTP-listener. De procedure hier beschrijft hoe u een loadbalancer toevoegt in AWS.

Stap 1: Doelgroep maken

Een doelgroep is een AWS-configuratie die de EC2-instanties definieert waarop uw proxy-servers draaien. Dit zijn de doelen voor het verkeer van de LBS.

1. EC2 >**Target groups** (Doelgroepen) > **Create target group** (Doelgroep)
2. Doe het volgende op de pagina Create (Maken):
   - Voer een doelgroepnaam in, bijvoorbeeld `TG-internal-HTTP`.
   - Doeltype: instanties
   - Protocol: HTTP
   - Poort: 80
   - VPC: selecteer uw VPC.
   - Voeg de te lezen codelijst toe via **Health checks** (Statuscontroles) > **Advanced health checks settings** (Geavanceerde instellingen voor statuscontroles) > **Success codes** (Succescodes): `200,303`.
   - Klik op **Maken**.
3. Selecteer de doelgroep die u zojuist hebt gemaakt en klik vervolgens op het tabblad **Targets** (Doelen):

- Klik op **Edit** (Bewerken).
- Selecteer de EC2-instanties (of één instantie als u er één tegelijk configureert) waarop de proxytoepassing wordt uitgevoerd en klik vervolgens op **Toevoegen aan geregistreerd**.
- Klik op **Opslaan**.

Stap 2: De loadbalancer-wizard starten

1. EC2> **Load Balancers** (Loadbalancers) > **Create Load Balancer** (Loadbalancer maken)
2. Maak op de pagina 'Select load balancer type' (Type loadbalancer selecteren) een toepassings-loadbalancer.

Opmerking: de gebruikersinterface die wordt weergegeven om de loadbalancer te configureren, is niet consistent in alle AWS-datacenters. De onderstaande procedure, 'Wizardconfiguratie', geeft aan welke instellingen moeten worden toegewezen in de AWS-configuratiewizard die begint met **Step 1 Configure Load Balancer** (Stap 1 Loadbalancer configureren).

Als uw datacenter alle configuraties weergeeft op één pagina met onderaan de knop **Create load balancer** (Loadbalancer maken), volgt u de onderstaande procedure 'Configuratie op één pagina'.

Wizardconfiguratie

1. Pagina **Configure load balancer** (Loadbalancer configureren):
   - Geef naam op.
   - Schema: internetgericht (standaard)
   - IP-adrestype: ipv4 (standaard)

- Listeners (listeners en routering):
  a. Laat de standaard-HTTP-listener staan.
  b. Klik op **Add listener** (Luisteraar toevoegen) en voeg `HTTPS:443` toe.
- VPC: selecteer de VPC waar u alles hebt geïnstalleerd.
- Beschikbaarheidszones:
  - Selecteer **a** en **b** voor uw datacenterregio's.
  - Selecteer in elke corresponderende vervolgkeuzelijst het openbare subnet (waar uw proxyservers zich bevinden).
- Klik op **Configure Security Settings** (Beveiligingsinstellingen configureren).

2. Pagina **Configure Security Settings** (Beveiligingsinstellingen configureren)

   - Upload uw openbare SSL-certificaat.
   - Klik op **Next: Configure Security Groups** (Volgende stap: Beveiligingsgroepen configureren).

3. Pagina **Configure Security Groepen** (Beveiligingsinstellingen configureren):

   - Selecteer de openbare beveiligingsgroep (Public). Als de standaardbeveiligingsgroep (Default) is geselecteerd, wist u deze selectie.
   - Klik op **Next: Configure Routing** (Volgende stap: Routering configureren).

4. Pagina **Configure Routing** (Routering configureren)

   - Doelgroep: bestaande doelgroep.
   - Naam: selecteer de doelgroep die u eerder hebt gemaakt.
   - Klik op **Next: Register Targets** (Volgende stap: Doelen registreren).

5. Pagina **Register Targets** (Doelen registreren)

   - De twee proxyserverinstanties die u eerder hebt geconfigureerd, worden weergegeven.
   - Klik op **Next: Review** (Volgende stap: Controleren).

6. Pagina **Review** (Controleren)

   Klik op **Maken**.

Configuratie op één pagina

Basisconfiguratie

- Geef naam op.
- Schema: internetgericht (standaard)
- IP-adrestype: ipv4 (standaard)

Netwerktoewijzing

- VPC: selecteer de VPC waar u alles hebt geïnstalleerd.
- Toewijzingen:
  - Selecteer de beschikbaarheidszones **a** en **b** (of vergelijkbare beschikbaarheidszones) voor uw datacenterregio's.
  - Selecteer in elke corresponderende vervolgkeuzelijst het openbare subnet (waar uw proxyservers zich bevinden).

Beveiligingsgroepen

Selecteer de openbare beveiligingsgroep (Public). Als de standaardbeveiligingsgroep (Default) is geselecteerd, wist u deze selectie.

Listeners en routering

- Laat de standaard-HTTP-listener staan. Geef voor **Default action** (Standaardactie) de doelgroep op die u eerder hebt ingesteld.
- Klik op **Add listener** (Luisteraar toevoegen) en voeg `HTTPS:443` toe. Geef voor **Default action** (Standaardactie) de doelgroep op die u eerder hebt ingesteld.

Veilige listenerinstellingen

- Upload uw openbare SSL-certificaat.

Klik op **Create Load balancer** (Loadbalancer maken).

Stap 3: Stickiness inschakelen

1. Nadat u de loadbalancer hebt gemaakt, moet u 'stickiness' (sessieaffiniteit) inschakelen voor de doelgroep.
    - Open de AWS-pagina voor de doelgroep (**EC2**> **Load Balancing** (Taakverdeling) > **Target Groups** (Doelgroepen)) en selecteer de doelgroepinstantie die u zojuist hebt ingesteld. Selecteer in het menu **Action** (Actie) de optie **Edit attributes** (Attributen bewerken).
    - Selecteer op de pagina **Edit attributes** (Attributen bewerken) de optie **Stickiness** (sessieaffiniteit), geef een duur van `1 day` (1 dag) op en klik vervolgens op **Save changes** (Wijzigingen opslaan).
2. Schakel stickiness in voor de loadbalancer op de HTTP-listener. Selecteer de loadbalancer die u zojuist hebt geconfigureerd en klik vervolgens op het tabblad **Listeners**:
    - Klik voor **HTTP:80** op **View/edit rules** (Regels weergeven/bewerken). Klik op de resulterende pagina **Rules** (Regels) op het bewerkingspictogram (eenmaal bovenaan de pagina en vervolgens nogmaals naast de regel) om de regel te bewerken. Verwijder de bestaande THEN-regel en vervang deze door op **Add action** (Actie toevoegen) > **Forward to...** (Doorsturen naar) te klikken. Specificeer in de hieruit voortvloeiende THEN-configuratie de doelgroep die u hebt gemaakt. Schakel Stickiness in onder Group-level stickiness (Sessieaffiniteit op groepsniveau) en stel de duur in op 1 dag. Sla de instelling op en klik vervolgens op **Update** (Bijwerken).

Stap 4: De time-out voor inactiviteit op de loadbalancer instellen

Werk de inactiviteitstime-out voor de loadbalancer bij naar 400 seconden.

Selecteer de loadbalancer die u voor deze implementatie hebt geconfigureerd en klik vervolgens op **Actions** (Acties) > **Edit attributes** (Kenmerken bewerken). Stel **Idle timeout** (Time-out inactiviteit) in op `400` seconden en klik op **Save** (Opslaan).

Stap 5: LBS-connectiviteit controleren

Open de AWS-pagina voor de doelgroep (**EC2**> **Load Balancers**) en selecteer de load-balancer-instantie die u zojuist hebt ingesteld.

Kopieer de DNS-naam onder **Description** (Beschrijving) en plak deze in een browser om toegang te krijgen tot de aanmeldingspagina van Tableau Server.

Als u een 500-niveaufout krijgt, moet u uw proxyservers mogelijk opnieuw opstarten.

DNS bijwerken met openbare Tableau-URL

Gebruik de DNS-zonenaam van uw domein uit de beschrijving van de AWS-loadbalancer om een CNAME-waarde in uw DNS te maken. Verkeer naar uw URL (tableau.example.com) moet naar de openbare DNS-naam van AWS worden verzonden.

Connectiviteit controleren

Nadat uw DNS-updates zijn voltooid, kunt u naar de aanmeldingspagina van Tableau Server navigeren door uw openbare URL in te voeren, bijvoorbeeld: `https://tableau.example.com`.

Voorbeeld van verificatieconfiguratie: SAML met externe IdP

In het volgende voorbeeld wordt beschreven hoe u SAML installeert en configureert met Okta als IdP, en de Mellon-verificatiemodule voor een Tableau-implementatie die wordt uitgevoerd in de AWS-referentiearchitectuur. In het voorbeeld wordt beschreven hoe u Tableau Server en de Apache-proxyservers configureert voor gebruik van HTTP. Okta stuurt via HTTPS een verzoek naar de AWS-loadbalancer, maar al het interne verkeer loopt via HTTP. Houd bij het configuratieproces voor dit scenario rekening met het HTTP- en HTTPS-protocol wanneer u URL-tekenreeksen instelt.

In dit voorbeeld wordt Mellon op de reverse-proxyservers gebruikt als serviceprovidermodule voor voorafgaande verificatie. Deze configuratie zorgt ervoor dat alleen geverifieerd verkeer verbinding maakt met Tableau Server, waarbij Tableau Server ook fungeert als serviceprovider met Okta als IdP. Daarom moet u twee IdP-toepassingen configureren: één voor de Mellon-serviceprovider en één voor de Tableau-serviceprovider.

Een Tableau-beheerdersaccount maken

Een veelgemaakte fout bij het configureren van SAML is dat vóór inschakeling van SSO geen beheerdersaccount wordt gemaakt op Tableau Server.

De eerste stap is het maken van een account op Tableau Server met de rol van Serverbeheerder. Voor het Okta-voorbeeldscenario moet de gebruikersnaam een geldige e-mailadresnotatie hebben, bijvoorbeeld gebruiker@voorbeeld.com. U moet een wachtwoord voor deze gebruiker instellen, maar het wachtwoord wordt niet gebruikt nadat SAML is geconfigureerd.

Okta-toepassing voor voorafgaande verificatie configureren

Voor het end-to-end-scenario dat in deze sectie wordt beschreven, zijn twee Okta-toepassingen nodig:

- Okta-toepassing voor voorafgaande verificatie
- Tableau Server-toepassing van Okta

Elk van deze toepassingen is gekoppeld aan verschillende metadata die u respectievelijk op de reverse proxy en Tableau Server moet configureren.

In deze procedure wordt beschreven hoe u de Okta-toepassing voor voorafgaande verificatie maakt en configureert. Verderop in dit onderwerp gaat u de Tableau Server-toepassing van Okta maken. Zie de Okta Developer-webpagina (in het Engels) voor informatie over een gratis Okta-proefaccount met een beperkt aantal gebruikers.

Maak een SAML-app-integratie voor de Mellon-serviceprovider voor voorafgaande verificatie.

1. Open het Okta-beheerdashboard > **Applications** > **Create App Integration** (Toepassingen > App-integratie maken).

2. Selecteer op de pagina **Create a new app integration** (Nieuwe app-integratie maken) de optie **SAML 2.0** en klik dan op **Next** (Volgende).

3. Voer op het tabblad **General Settings** (Algemene instellingen) een app-naam in, bijvoorbeeld `Tableau Pre-Auth` en klik op **Next** (Volgende).

4. Doe het volgende op het tabblad **Configure SAML** (SAML configureren):

    - URL voor eenmalige aanmelding (SSO). Het laatste element van het pad in de URL voor eenmalige aanmelding wordt aangeduid als `MellonEndpointPath` in het configuratiebestand `mellon.conf` dat verderop in deze procedure volgt. U kunt elk gewenst eindpunt opgeven. In dit voorbeeld is `sso` het eindpunt. Het laatste element, `postResponse`, is vereist: `https://tableau.example.com/sso/postResponse`.
    - Schakel het selectievakje **Use this for Recipient URL and Destination URL** (Dit gebruiken voor ontvangers-URL en bestemmings-URL) uit.
    - Recipient URL (Ontvangers-URL): Hetzelfde als de SSO-URL, maar met HTTP. Bijvoorbeeld `http://tableau.example.com/sso/postResponse`.
    - Destination URL (Bestemmings-URL): hetzelfde als de SSO-URL, maar met HTTP. Bijvoorbeeld `http://tableau.example.com/sso/postResponse`.
    - Audience URI (SP Entity ID) (Doelgroep-URI (SP-entiteits-ID). Bijvoorbeeld `https://tableau.example.com`.
    - Name ID Format (Notatie van naam-ID): `EmailAddress`
    - Application username (Toepassingsgebruikersnaam): `Email`
    - Attributes Statements (Kenmerkinstructies): Name = `mail`; Name format (Naamnotatie)= `Unspecified`; Value (Waarde) = `user.email`.

    Klik op **Next** (Volgende).

5. Selecteer op het tabblad **Feedback** het volgende:

    - **I'm an Okta customer adding an internal app (Ik ben een Okta-klant die een interne app toevoegt)**

- **This is an internal app that we have created (Dit is een interne app die we hebben gemaakt)**
- Klik op **Finish** (Voltooien).

6. Maak het IdP-metadatabestand voor voorafgaande verificatie:
    - In Okta: **Applications** > (Toepassingen) **Applications** > Uw nieuwe toepassing (bijv. `Tableau Pre-Auth`) > **Sign On** (Aanmelden)
    - Klik bij **SAML Signing Certificates** (SAML-ondertekeningscertificaten) op **View SAML setup instructions** (SAML-installatie-instructies weergeven).
    - Scroll op de pagina **How to Configure SAML 2.0 for <pre-auth> Application** (SAML 2.0 configureren voor<pre-auth>-toepassing) omlaag naar de sectie **Optional** (Optioneel), **Provide the following IDP metadata to your SP provider** (de volgende IDP-metadata doorgeven aan uw SP-provider).
    - Kopieer de inhoud van het XML-veld en sla deze op in een bestand met de naam `pre-auth_idp_metadata.xml`.
7. (Optioneel) Configureer meervoudige verificatie:
    - In Okta: **Applications** > (Toepassingen) **Applications** > Uw nieuwe toepassing (bijv. `Tableau Pre-Auth`) > **Sign On** (Aanmelden)
    - Klik onder **Sign On Policy** (Aanmeldingsbeleid) op **Add Rule** (Regel toevoegen).
    - Geef bij **App Sign On Rule** (App-aanmeldingsregel) een naam en de verschillende MFA-opties op. Om de functionaliteit te testen, kunt u alle opties op de standaardinstellingen laten staan. Onder **Actions** (Acties) moet u echter **Prompt for factor** (Om factor vragen) selecteren en vervolgens opgeven hoe vaak gebruikers zich moeten aanmelden. Klik op **Save** (Opslaan).

Okta-gebruiker maken en toewijzen

1. Maak in Okta een gebruiker aan met de gebruikersnaam die u in Tableau hebt gemaakt (gebruiker@voorbeeld.com): **Directory** > **People** (Mensen) > **Add person** (Persoon toevoegen).
2. Nadat de gebruiker is aangemaakt, wijst u de nieuwe Okta-app toe aan die persoon: klik op de gebruikersnaam en wijs de toepassing toe in **Assign Application** (Toepassing toewijzen).

Mellon installeren voor voorafgaande verificatie

1. Voer de volgende opdrachten uit op de EC2-instanties met de Apache-proxyserver om de PHP- en Mellon-module te installeren:

   ```
   sudo yum install httpd php mod_auth_mellon
   ```

2. Maak de map `/etc/httpd/mellon`.

Mellon configureren als module voor voorafgaande verificatie

Voer deze procedure uit op beide proxyservers.

U moet een kopie hebben van het bestand `pre-auth_idp_metadata.xml` dat u hebt gemaakt vanuit de Okta-configuratie.

1. Wissel van map:

   ```
   cd /etc/httpd/mellon
   ```

2. Maak de serviceprovider-metadata. Voer het script `mellon_create_metadata.sh` uit. U moet de entiteits-ID en de retour-URL (return-url) voor uw organisatie in de opdracht opnemen.

   De retour-URL wordt in Okta de *single sign on URL* genoemd. Het laatste element van het pad in de retour-URL wordt aangeduid als `MellonEndpointPath` in het configuratiebestand `mellon.conf` dat later in deze procedure volgt. In dit voorbeeld specificeren we `sso` als eindpuntpad.

   Bijvoorbeeld:

```
sudo /usr/libexec/mod_auth_mellon/mellon_create_metadata.sh htt-
ps://tableau.example.com "https://tableau.example.com/sso"
```

Het script retourneert het certificaat, de sleutel en de metadatabestanden van de serviceprovider.

3. Hernoem de serviceproviderbestanden in de map `mellon` voor betere leesbaarheid. In de documentatie verwijzen we naar deze bestanden met de volgende namen:

```
sudo mv *.key mellon.key
sudo mv *.cert mellon.cert
sudo mv *.xml sp_metadata.xml
```

4. Kopieer het bestand `pre-auth_idp_metadata.xml` naar dezelfde map.

5. Maak het bestand `mellon.conf` in de map `/etc/httpd/conf.d`:

```
sudo nano /etc/httpd/conf.d/mellon.conf
```

6. Kopieer de volgende inhoud naar `mellon.conf`.

```
<Location />
MellonSPPrivateKeyFile /etc/httpd/mellon/mellon.key
MellonSPCertFile /etc/httpd/mellon/mellon.cert
MellonSPMetadataFile /etc/httpd/mellon/sp_metadata.xml
MellonIdPMetadataFile /etc/httpd/mellon/pre-auth_idp_met-
adata.xml
MellonEndpointPath /sso
MellonEnable "info"
</Location>
```

7. Voeg de volgende inhoud toe aan het bestaande `tableau.conf`-bestand:

Voeg in het blok `<VirtualHost *:80>` de volgende inhoud toe. Werk `ServerName` bij met de openbare hostnaam in uw entiteits-ID:

```
DocumentRoot /var/www/html
ServerName tableau.example.com
ServerSignature Off
ErrorLog logs/error_sp.log
CustomLog logs/access_sp.log combined
LogLevel info
```

Voeg het Location-blok toe buiten het blok `<VirtualHost *:80>`. Werk `MellonCookieDomain` bij met het topleveldomein om cookie-informatie te bewaren, zoals hier weergegeven:

```
<Location />
AuthType Mellon
MellonEnable auth
Require valid-user
MellonCookieDomain example.com
</Location>
```

Het volledige `tableau.conf`-bestand ziet eruit zoals in het volgende voorbeeld:

```
<VirtualHost *:80>
ServerAdmin admin@example.com
ProxyHCExpr ok234 {%{REQUEST_STATUS} =~ /^[234]/}
Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e;
path=/" env=BALANCER_ROUTE_CHANGED
<Proxy balancer://tableau>
BalancerMember http://10.0.3.36/ route=1 hcmethod=GET hcex-
pr=ok234 hcuri=/favicon.ico
BalancerMember http://10.0.4.15/ route=2 hcmethod=GET hcex-
pr=ok234 hcuri=/favicon.ico
ProxySet stickysession=ROUTEID
</Proxy>
ProxyPreserveHost On
ProxyPass / balancer://tableau/
ProxyPassReverse / balancer://tableau/
DocumentRoot /var/www/html
```

```
ServerName tableau.example.com
ServerSignature Off
ErrorLog logs/error_sp.log
CustomLog logs/access_sp.log combined
LogLevel info
</VirtualHost>
<Location />
AuthType Mellon
MellonEnable auth
Require valid-user
MellonCookieDomain example.com
</Location>
```

8. Controleer de configuratie. Voer de volgende opdracht uit:

   ```
   sudo apachectl configtest
   ```

   Als de configuratietest een fout retourneert, herstelt u de fouten en voert u configtest opnieuw uit. Bij succesvolle configuratie wordt `Syntax OK` geretourneerd.

9. Start httpd opnieuw:

   ```
   sudo systemctl restart httpd
   ```

Een Tableau Server-applicatie maken in Okta

1. In het Okta-dashboard: **Applications** (Toepassingen) > **Applications** > **Browse App Catalog** (App-catalogus doorzoeken)
2. Zoek in **Browse App Integration Catalog** (App-integratiecatalogus doorzoeken) naar `Tableau`, selecteer de Tableau Server-tegel en klik vervolgens op **Add** (Toevoegen).
3. Voer bij **Add Tableau Server** (Tableau Server toevoegen) > **Algemene instellingen** (Algemene instellingen) een label in en klik vervolgens op **Next** (Volgende).
4. Selecteer in ‘Sign-On Options’ (Aanmeldingsopties) de optie **SAML 2.0** en scroll vervolgens omlaag naar 'Advanced Sign-on Settings' (Geavanceerde aanmeldingsinstellingen):

- **SAML Entity ID** (SAML-entiteits-ID): voer de openbare URL in, bijvoorbeeld https://tableau.example.com.
- **Application user name format** (Notatie toepassingsgebruikersnaam): Email (E-mail)

5. Klik op de link **Identity Provider metadata** (Identiteitsprovider-metadata) om een browser te starten. Kopieer de browserlink. Dit is de link die u gebruikt wanneer u Tableau configureert in de volgende procedure.
6. Klik op **Done** (Gereed).
7. Wijs de nieuwe Tableau Server-toepassing van Okta toe aan uw gebruiker (gebruiker@voorbeeld.com): Klik op de gebruikersnaam en wijs de toepassing toe in **Assign Application** (Toepassing toewijzen).

SAML inschakelen op Tableau Server voor IdP

Voer deze procedure uit op Tableau Server-knooppunt 1

1. Download de Tableau Server-toepassingsmetadata van Okta. Gebruik de link die u bij de vorige procedure hebt opgeslagen:

   ```
   wget https://dev-66144217.okta.com/app/exk1egxgt1fhjkSeS5d7/sso/saml/metadata -O idp_metadata.xml
   ```

2. Kopieer een TLS-certificaat en bijbehorend sleutelbestand naar de Tableau Server. Het sleutelbestand moet een RSA-sleutel zijn. Zie *SAML-vereisten* (Linux) voor meer informatie over SAML-certificaat- en IdP-vereisten.

   Om het beheer en de implementatie van certificaten te vereenvoudigen en als best practice voor de beveiliging raden wij aan om certificaten te gebruiken die zijn gegenereerd door een grote, vertrouwde externe CA (certificeringsinstantie). U kunt er ook voor kiezen om zelfondertekende certificaten te genereren of certificaten van een PKI voor TLS te gebruiken.

   Als u geen TLS-certificaat hebt, kunt u een zelfondertekend certificaat genereren met behulp van de onderstaande ingesloten procedure.

Een zelfondertekend certificaat genereren

Voer deze procedure uit op Tableau Server-knooppunt 1.

a. Genereer een root-CA-sleutel:

```
openssl genrsa -out rootCAKey-saml.pem 2048
```

b. Maak het root-CA-certificaat:

```
openssl req -x509 -sha256 -new -nodes -key rootCAKey-
saml.pem -days 3650 -out rootCACert-saml.pem
```

U wordt gevraagd waarden in te voeren voor de certificaatvelden. Bijvoorbeeld:

```
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Washington
Locality Name (eg, city) [Default City]:Seattle
Organization Name (eg, company) [Default Company Ltd]:Ta-
bleau
Organizational Unit Name (eg, section) []:Operations
Common Name (eg, your name or your server's hostname)
[]:tableau.example.com
Email Address []:example@tableau.com
```

c. Maak het certificaat en de bijbehorende sleutel (`server-saml.csr` en `server-saml.key` in het onderstaande voorbeeld). De onderwerpnaam voor het certificaat moet overeenkomen met de openbare hostnaam van de Tableau-host. De onderwerpnaam wordt ingesteld met de optie `-subj` in de notatie `"/CN=<host-name>"`, bijvoorbeeld:

```
openssl req -new -nodes -text -out server-saml.csr -keyout
server-saml.key -subj "/CN=tableau.example.com"
```

d. Onderteken het nieuwe certificaat met het CA-certificaat dat u hierboven hebt gemaakt. De volgende opdracht geeft het certificaat ook weer in de `crt`-notatie:

```
openssl x509 -req -in server-saml.csr -days 3650 -CA
rootCACert-saml.pem -CAkey rootCAKey-saml.pem -CAcre-
ateserial -out server-saml.crt
```

e. Converteer het sleutelbestand naar RSA. Tableau vereist een RSA-sleutelbestand voor SAML. Voer de volgende opdracht uit om de sleutel te converteren:

```
openssl rsa -in server-saml.key -out server-saml-rsa.key
```

3. Configureer SAML. Voer de volgende opdracht uit en geef daarbij uw entiteits-ID en retour-URL op, evenals de paden naar het metadatabestand, certificaatbestand en sleutelbestand:

```
tsm authentication saml configure --idp-entity-id "htt-
ps://tableau.example.com" --idp-return-url "htt-
ps://tableau.example.com" --idp-metadata idp_metadata.xml --
cert-file "server-saml.crt" --key-file "server-saml-rsa.key"

tsm authentication saml enable
```

4. Als uw organisatie Tableau Desktop 2021.4 of hoger gebruikt, moet u de volgende opdracht uitvoeren om verificatie via de reverse-proxyservers in te schakelen.

   Versies van Tableau Desktop 2021.2.1 - 2021.3 werken zonder dat u deze opdracht uitvoert, op voorwaarde dat de module voor voorafgaande verificatie (bijvoorbeeld Mellon) is geconfigureerd om het bewaren van cookies in het topleveldomein toe te staan.

```
tsm configuration set -k features.ExternalBrowserOAuth -v false
```

5. Pas configuratiewijzigingen toe:

```
tsm pending-changes apply
```

SAML-functionaliteit valideren

Om de end-to-end SAML-functionaliteit te valideren, meldt u zich aan bij Tableau Server met de openbare URL (bijvoorbeeld https://tableau.example.com) met het Tableau-beheerdersaccount dat u aan het begin van deze procedure hebt gemaakt.

Probleemoplossing bij validatie

Bad Request: een veelvoorkomende fout in dit scenario is de foutmelding 'Bad Request' (ongeldige aanvraag) van Okta. Dit probleem doet zich vaak voor wanneer de browser data van een eerdere Okta-sessie in de cache opslaat. Indien u bijvoorbeeld de Okta-toepassingen beheert als Okta-beheerder en vervolgens probeert toegang te krijgen tot Tableau met een ander Okta-account, kunnen sessiedata van de beheerdersdata de fout 'Bad Request' veroorzaken. Als deze fout zich blijft voordoen, zelfs nadat u de lokale browsercache hebt gewist, valideer het Tableau-scenario dan door verbinding te maken met een andere browser.

Een andere oorzaak van de fout 'Bad Request' is een typefout in een van de vele URL's die u invoert tijdens het configuratieproces voor Okta, Mellon en SAML. Controleer dit allemaal zorgvuldig.

Vaak geeft het httpd-bestand `error.log` op de Apache-server aan welke URL de fout veroorzaakt.

Not Found - The requested URL was not found on this server: (Niet gevonden - De gevraagde URL is niet gevonden op deze server) Deze fout duidt op een configuratiefout.

Als de gebruiker is geverifieerd met Okta en vervolgens deze foutmelding krijgt, hebt u de Okta-toepassing voor voorafgaande verificatie waarschijnlijk naar Tableau Server geüpload toen u SAML configureerde. Controleer of de metadata van de Okta Tableau Server-toepassing zijn geconfigureerd op Tableau Server, en niet de metadata van de Okta-toepassing voor voorafgaande verificatie.

Andere stappen voor probleemoplossing:

- Controleer `tableau.conf` zorgvuldig op typefouten of configuratiefouten.
- Controleer de instellingen van de Okta-toepassing voor voorafgaande verificatie. Zorg ervoor dat het HTTP- en het HTTPS-protocol zijn ingesteld zoals aangegeven in dit onderwerp.
- Start httpd opnieuw op beide proxyservers.
- Verifieer dat `sudo apachectl configtest` 'Syntax OK' retourneert op beide proxy-servers.
- Controleer of de testgebruiker aan beide toepassingen in Okta is toegewezen.
- Controleer of 'stickiness' (sessieaffiniteit) is ingesteld op de loadbalancer en de bij-behorende doelgroepen

SSL/TLS configureren van loadbalancer tot Tableau Server

Sommige organisaties hebben een end-to-end-encryptiekanaal nodig van de client naar de back-endservice. De standaardreferentiearchitectuur zoals tot dusver beschreven, specificeert SSL van de client tot de loadbalancer die op de weblaag van uw organisatie wordt uitgevoerd.

Om SSL van de loadbalancer tot Tableau Server te configureren, moet u het volgende doen:

- Een geldig SSL-certificaat installeren op zowel Tableau als de proxyservers.
- SSL van de loadbalancer tot de reverse-proxyservers configureren.
- SSL van de proxyservers tot Tableau Server configureren.
- U kunt SSL ook configureren van Tableau Server tot de PostgreSQL-instantie.

In de rest van dit onderwerp wordt deze implementatie beschreven in de context van de AWS-voorbeeldreferentiearchitectuur.

Voorbeeld: SSL/TLS configureren in AWS-referentiearchitectuur

In dit gedeelte wordt beschreven hoe u SSL respectievelijk op Tableau en op een Apache-proxyserver configureert in de voorbeeld-AWS-referentiearchitectuur.

De Linux-procedures in dit voorbeeld tonen opdrachten voor RHEL-achtige distributies. De opdrachten hier zijn specifiek ontwikkeld met de Amazon Linux 2-distributie. Als u de Ubuntu-distributie gebruikt, moet u de opdrachten dienovereenkomstig bewerken.

Stap 1: Certificaten en bijbehorende sleutels verzamelen

Om het beheer en de implementatie van certificaten te vereenvoudigen en als best practice voor de beveiliging raden wij aan om certificaten te gebruiken die zijn gegenereerd door een grote, vertrouwde externe CA (certificeringsinstantie).

U kunt er ook voor kiezen om zelfondertekende certificaten te genereren of certificaten van een PKI voor TLS te gebruiken.

De volgende procedure beschrijft hoe u zelfondertekende certificaten genereert. Als u certificaten van derden gebruikt, zoals wij aanbevelen, kunt u deze procedure overslaan.

Voer deze procedure uit op een van de proxyhosts. Nadat u het certificaat en de bijbehorende sleutel hebt gegenereerd, deelt u deze met de andere proxyhost en met Tableau Server-knooppunt 1.

1. Genereer een root-CA-sleutel:

   ```
   openssl genrsa -out rootCAKey.pem 2048
   ```

2. Maak het root-CA-certificaat:

```
openssl req -x509 -sha256 -new -nodes -key rootCAKey.pem -days
3650 -out rootCACert.pem
```

U wordt gevraagd waarden in te voeren voor de certificaatvelden. Bijvoorbeeld:

```
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Washington
Locality Name (eg, city) [Default City]:Seattle
Organization Name (eg, company) [Default Company Ltd]:Tableau
Organizational Unit Name (eg, section) []:Operations
Common Name (eg, your name or your server's hostname) []:ta-
bleau.example.com
Email Address []:example@tableau.com
```

3. Maak het certificaat en de bijbehorende sleutel (`serverssl.csr` en `serverssl.key` in het onderstaande voorbeeld). De onderwerpnaam voor het certificaat moet overeenkomen met de openbare hostnaam van de Tableau-host. De onderwerpnaam wordt ingesteld met de optie `-subj` in de notatie `"/CN=<host-name>"`, bijvoorbeeld:

   ```
   openssl req -new -nodes -text -out serverssl.csr -keyout ser-
   verssl.key -subj "/CN=tableau.example.com"
   ```

4. Onderteken het nieuwe certificaat met het CA-certificaat dat u in stap 2 hebt gemaakt. De volgende opdracht geeft het certificaat ook weer in de `crt`-notatie:

   ```
   openssl x509 -req -in serverssl.csr -days 3650 -CA
   rootCACert.pem -CAkey rootCAKey.pem -CAcreateserial -out ser-
   verssl.crt
   ```

Stap 2: Tableau Server voor SSL configureren

Voer deze procedure uit op beide proxyservers.

1. Installeer de Apache SSL-module:

   ```
   sudo yum install mod_ssl
   ```

2. Maak de map `/etc/ssl/private`:

   ```
   sudo mkdir -p /etc/ssl/private
   ```

3. Kopieer de crt- en sleutelbestanden naar de volgende `/etc/ssl/`-paden:

   ```
   sudo cp serverssl.crt /etc/ssl/certs/

   sudo cp serverssl.key /etc/ssl/private/
   ```

4. Werk het bestaande `tableau.conf`-bestand bij met de volgende updates:

   - Voeg het SSL-rewrite-blok toe:

     ```
     RewriteEngine on
     RewriteCond %{SERVER_NAME} =tableau.example.com
     RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI}
     [END,NE,R=permanent]
     ```

   - Werk in het SSL-rewrite-blok de `RewriteCond` servernaam bij: voeg uw openbare hostnaam toe, bijvoorbeeld `tableau.example.com`
   - Wijzig `<VirtualHost *:80>` in `<VirtualHost *:443>`.
   - Plaats het `<VirtualHost *:443>`-blok en het `<Location />`-blok in `<IfModule mod_ssl.c>` ... `</IfModule>`.
   - `BalancerMember`: verander het protocol van `http` in `https`.
   - Voeg `SSL*`-elementen toe in het `<VirtualHost *:443>`-blok:

     ```
     SSLEngine on
     SSLCertificateFile /etc/ssl/certs/serverssl.crt
     SSLCertificateKeyFile /etc/ssl/private/serverssl.key
     SSLProxyEngine on
     SSLProxyVerify none
     SSLProxyCheckPeerName off
     SSLProxyCheckPeerExpire off
     ```

   - In het `LogLevel`-element: voeg `ssl:warn` toe.
   - Optioneel: als u een verificatiemodule hebt geïnstalleerd en geconfigureerd, staan er mogelijk extra elementen in het bestand tableau.conf. Het blok `<Location /> </Location>` zal bijvoorbeeld elementen bevatten.

Hier ziet u een voorbeeld van een tableau.conf-bestand dat is geconfigureerd voor SSL:

```
RewriteEngine on
RewriteCond %{SERVER_NAME} =tableau.example.com
RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI} [END,NE,R-
R=permanent]

<IfModule mod_ssl.c>
<VirtualHost *:443>
ServerAdmin admin@example.com
ProxyHCExpr ok234 {%{REQUEST_STATUS} =~ /^[234]/}
Header add Set-Cookie "ROUTEID=.%{BALANCER_WORKER_ROUTE}e;
path=/" env=BALANCER_ROUTE_CHANGED
<Proxy balancer://tableau>
BalancerMember https://10.0.3.36/ route=1 hcmethod=GET hcex-
pr=ok234 hcuri=/favicon.ico
BalancerMember https://10.0.4.15/ route=2 hcmethod=GET hcex-
pr=ok234 hcuri=/favicon.ico
ProxySet stickysession=ROUTEID
</Proxy>
ProxyPreserveHost On
ProxyPass / balancer://tableau/
ProxyPassReverse / balancer://tableau/
DocumentRoot /var/www/html
ServerName tableau.example.com
ServerSignature Off
ErrorLog logs/error_sp.log
CustomLog logs/access_sp.log combined
LogLevel info ssl:warn
SSLEngine on
SSLCertificateFile /etc/ssl/certs/serverssl.crt
SSLCertificateKeyFile /etc/ssl/private/serverssl.key
SSLProxyEngine on
SSLProxyVerify none
SSLProxyCheckPeerName off
```

```
SSLProxyCheckPeerExpire off
</VirtualHost>
<Location />
#If you have configured a pre-auth module (e.g. Mellon) include
those elements here.
</Location>
</IfModule>
```

5. Voeg het bestand index.html toe om 403-fouten te onderdrukken:

   ```
   sudo touch /var/www/html/index.html
   ```

6. Start httpd opnieuw:

   ```
   sudo systemctl restart httpd
   ```

Stap 3: Tableau Server voor externe SSL configureren

Kopieer de bestanden serverssl.crt en serverssl.key van de host Proxy 1 naar de oorspronkelijke Tableau Server (knooppunt 1).

Voer de volgende opdrachten uit op knooppunt 1:

```
tsm security external-ssl enable --cert-file serverssl.crt --key-
file serverssl.key
tsm pending-changes apply
```

Stap 4: Optionele verificatieconfiguratie

Als u een externe identiteitsprovider voor Tableau hebt geconfigureerd, moet u de retour-URL's waarschijnlijk bijwerken in het IdP-beheerdashboard.

Als u bijvoorbeeld een Okta-toepassing voor voorafgaande verificatie gebruikt, moet u de toepassing zodanig bijwerken dat deze het HTTPS-protocol gebruikt voor de ontvangers-URL en de bestemmings-URL.

Stap 5: AWS-loadbalancer voor HTTPS configureren

Als u implementeert met AWS-loadbalancer zoals gedocumenteerd in deze gids, configureert u de AWS-loadbalancer opnieuw om HTTPS-verkeer naar de proxyservers te sturen:

1. Hef de registratie van de bestaande HTTP-doelgroep op:

   Selecteer in **Target Groups**, (Doelgroepen) de HTTP-doelgroep die is geconfigureerd voor de loadbalancer, klik op **Actions** (Acties) en klik vervolgens op **Register and deregister instance** (Instantie registreren en deregistreren).

   Selecteer op de pagina **Register and deregister targets** (Doelen registreren en deregistreren) de instanties die momenteel geconfigureerd zijn, klik op **Deregister** (Deregistreren) en klik vervolgens op **Save** (Opslaan).

2. Maak een HTTPS-doelgroep:

   Target groups > **Create target group** (Doelgroepen) > Doelgroep maken)

   - Selecteer 'Instances' (Instanties).
   - Voer een doelgroepnaam in, bijvoorbeeld `TG-internal-HTTPS`.
   - Selecteer uw VPC.
   - Protocol: HTTPS 443
   - Voeg de te lezen codelijst toe via **Health checks** (Statuscontroles) > **Advanced health checks settings** (Geavanceerde instellingen voor statuscontroles) > **Success codes** (Succescodes): `200,303`.
   - Klik op **Create** (Maken).

3. Selecteer de doelgroep die u zojuist hebt gemaakt en klik vervolgens op het tabblad **Targets** (Doelen):

   - Klik op **Edit** (Bewerken).
   - Selecteer de EC2-instanties waarop de proxytoepassing wordt uitgevoerd en klik vervolgens op **Toevoegen aan geregistreerd**.
   - Klik op **Opslaan**.

4. Nadat u de doelgroep hebt aangemaakt, moet u 'stickiness' (sessieaffiniteit) inschakelen:

    - Open de AWS-pagina voor de doelgroep (**EC2**> **Load Balancing** (Taakverdeling) > **Target Groups** (Doelgroepen)) en selecteer de doelgroepinstantie die u zojuist hebt ingesteld. Selecteer in het menu **Action** (Actie) de optie **Edit attributes** (Attributen bewerken).
    - Selecteer op de pagina **Edit attributes** (Attributen bewerken) de optie **Stickiness** (sessieaffiniteit), geef een duur van `1 day` (1 dag) op en klik vervolgens op **Save changes** (Wijzigingen opslaan).

5. Werk de listenerregels bij op de loadbalancer. Selecteer de loadbalancer die u voor deze implementatie hebt geconfigureerd en klik vervolgens op het tabblad **Listeners**.

    - Klik voor **HTTP:80** op **View/edit rules** (Regels weergeven/bewerken). Klik op de resulterende pagina **Rules** (Regels) op het bewerkingspictogram (eenmaal bovenaan de pagina en vervolgens nogmaals naast de regel) om de regel te bewerken. Verwijder de bestaande THEN-regel en vervang deze door op **Add action** (Actie toevoegen) > **Redirect to...** (Omleiden naar) te klikken. Geef in de resulterende THEN-configuratie `HTTPS` en poort `443` op en laat de overige opties op de standaardinstellingen staan. Sla de instelling op en klik vervolgens op **Update** (Bijwerken).
    - Klik voor **HTTP:443** op **View/edit rules** (Regels weergeven/bewerken). Klik op de resulterende pagina **Rules** (Regels) op het bewerkingspictogram (eenmaal bovenaan de pagina en vervolgens nogmaals naast de regel) om de regel te bewerken. Wijzig de doelgroep in de zojuist gemaakte HTTPS-groep onder **Forward to...** (Doorsturen naar) in de **THEN**-configuratie. Schakel Stickiness in onder **Group-level stickiness** (Sessieaffiniteit op groepsniveau) en stel de duur in op 1 dag. Sla de instelling op en klik vervolgens op **Update** (Bijwerken).

Stap 6: SSL controleren

Controleer de configuratie door naar https://tableau.example.com te gaan.