Tableau Server Enterprise Bereitstellungshandbuch

Letzte Aktualisierung 09.01.2025

Inhalt

Bereitstellungshandbuch zu Tableau Server Enterprise

Das Bereitstellungshandbuch "Tableau Server Enterprise" (Tableau Server Enterprise Deployment Guide, kurz: EDG) enthält eine Anleitung zur Bereitstellung von Tableau Server (lokal oder in der Cloud). Das Handbuch enthält Bereitstellungsanleitungen für Unternehmensszenarien im Kontext einer Referenzarchitektur. Wir haben die Referenzarchitektur getestet, um die Einhaltung von Sicherheits-, Skalierungs- und Leistungsbenchmarks zu überprüfen, die den branchenüblichen Best Practices entsprechen.

Ganz allgemein betrachtet, bestehen die Hauptmerkmale einer branchenüblichen Bereitstellung im Unternehmen aus einer mehrstufigen Topologie, bei der jede Ebene der Server-Anwendungsfunktionalität (Web-Gateway-Schicht, Anwendungsschicht und Datenschicht) durch zugriffsgesteuerte Subnetze gebunden und geschützt ist. Benutzer, die aus dem Internet auf die Serveranwendung zugreifen, werden in der Webschicht authentifiziert. Nach der Authentifizierung wird die Anfrage an ein geschütztes Subnetz weitergeleitet, wo die Anwendungsschicht die Geschäftslogik verarbeitet. Besonders wichtige Daten werden durch das dritte Subnetz geschützt: die Datenschicht. Dienste in der Anwendungsschicht kommunizieren über das geschützte Netzwerk mit der Datenschicht, um Datenanforderungen an die Backend-Datenquellen zu bedienen.

Bei dieser Bereitstellung steht die Sicherheit bei allen Design-Entscheidungen und der Implementierung im Vordergrund. Aber auch Zuverlässigkeit, Leistung und Skalierbarkeit sind vorrangige Anforderungen. Aufgrund des verteilten und modularen Designs der Referenzarchitektur skalieren Zuverlässigkeit und Leistung auf linear vorhersehbare Weise, indem kompatible Dienste an jedem Knoten strategisch nebeneinander platziert und Dienste an Engpässen hinzugefügt werden.

Zielgruppe

Das Bereitstellungshandbuch wurde für IT-Administratoren in Unternehmen entwickelt, die Folgendes benötigen:

- Eine IT-verwaltete Tableau-Bereitstellung
- Durchsetzung branchenüblicher Compliance
- Best Practices für branchenübliche Implementierungen
- Standardmäßig sichere Bereitstellung

Das Bereitstellungshandbuch ist ein Implementierungsleitfaden für die Bereitstellung der Referenzarchitektur für Unternehmen. Auch wenn diese Version des Bereitstellungshandbuchs eine AWS/Linux-Beispielimplementierung enthält, kann das Handbuch von erfahrenen IT-Unternehmensadministratoren als Ressource verwendet werden, um die vorgegebene Referenzarchitektur in beliebigen professionellen Rechenzentrumsumgebungen bereitzustellen.

Version

Diese Version des Bereitstellungshandbuchs wurde für die Tableau Server-Version 2021.2.3 (oder höher) entwickelt. Auch wenn Sie das Bereitstellungshandbuch als allgemeine Referenz für die Bereitstellung von älteren Versionen von Tableau Server verwenden können, empfehlen wir, die Referenzarchitektur mit Tableau Server 2021.2.3 (oder höher) bereitzustellen. Einige Funktionen und Optionen sind in älteren Versionen von Tableau Server nicht verfügbar.

Für die aktuellsten Funktionen und Verbesserungen empfehlen wir die Bereitstellung des Bereitstellungshandbuchs mit Tableau Server 2022.1.7 und höher.

Die in diesem Handbuch beschriebene Referenzarchitektur unterstützt die folgenden Tableau-Clients: Webdokumenterstellung mit kompatiblen Browsern, Tableau Mobile und Tableau Desktop ab der Version 2021.2.1. Andere Tableau-Clients (Tableau Prep, Bridge usw.) wurden noch nicht mit der Referenzarchitektur validiert.

Hervorhebungsfunktionen

Die erste Version der Tableau Server-Referenzarchitektur führt die folgenden Szenarien und Funktionen ein:

- Client-Vorauthentifizierung: Tableau-Clients (Desktop, Mobile, Web-dokumenterstellung) authentifizieren sich beim unternehmenseigenen Authen-tifizierungsanbieter in der Webschicht, bevor sie auf den internen Tableau Server zugreifen. Dieser Prozess wird durch die Konfiguration eines authN-Plug-ins auf dem Tableau Server Independent Gateway verwaltet, das als Reverse-Proxyserver fungiert. Siehe Teil 5 – Konfigurieren der Webschicht.
- Zero Trust-Bereitstellung: Da der gesamte Datenverkehr zu Tableau-Servern vor-authentifiziert wird, arbeitet die gesamte Tableau-Bereitstellung in einem privaten Sub-netz, das keine vertrauenswürdige Verbindung erfordert.
- Externes Repository: Die Referenzarchitektur sieht vor, das Tableau-Repository in einer externen PostgreSQL-Datenbank zu installieren, sodass DBAs das Repository wie eine generische Datenbank verwalten, optimieren, skalieren und sichern können.
- Anfangsknoten-Wiederherstellung: Das Bereitstellungshandbuch führt ein neues Skript ein, das die Anfangsknoten-Wiederherstellung im Falle eines Fehlers automatisiert.
- TAR-basierte Sicherung und Wiederherstellung: Verwenden Sie gewohnte TAR-Siche-rungen an strategischen Meilensteinen der Tableau-Bereitstellung. Im Falle eines Feh-lers oder einer Fehlkonfiguration der Bereitstellung können Sie die vorherige Bereitstellungsphase schnell wiederherstellen, indem Sie die zugehörige tar-Sicherung wiederherstellen.
- Leistungsverbesserung: Kundenbefragungen und Labortests zeigen eine Leis-tungsverbesserung von 15-20 % bei Ausführung nach dem Bereitstellungshandbuch im Vergleich zur Standardbereitstellung.

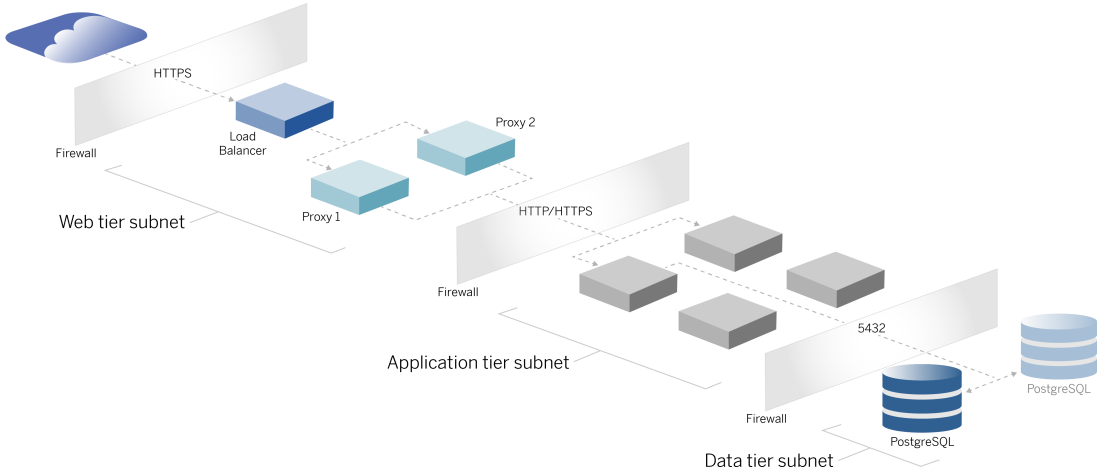
Lizenzierung

Die in diesem Handbuch beschriebene Tableau Sever-Referenzarchitektur erfordert eine Tableau Advanced Management-Lizenz, um das externe Repository von Tableau Server zu aktivieren. Optional können Sie auch den externen Dateispeicher von Tableau Server bereit-stellen, wofür ebenfalls die Tableau Advanced Management-Lizenz erforderlich ist. Siehe *Über Tableau Advanced Management-Add-on für Tableau Server* (Linux).

Teil 1 - Grundlegendes zur Unternehmensbereitstellung

In Teil 1 werden die Features und Anforderungen einer branchenüblichen Bereitstellung im Unternehmen ausführlicher beschrieben, für die das Tableau Server-Handbuch für die Bereitstellung im Unternehmen (Enterprise Deployment Guide, EDG) entwickelt wurde.

Das folgende Netzwerkdiagramm zeigt eine allgemeine, in Schichten gegliederte Bereitstellung im Rechenzentrum mit der Tableau Server-Referenzarchitektur.



Industriestandards und Bereitstellungsanforderungen

Im Folgenden finden Sie Funktionen für Bereitstellungen nach Industriestandard. Nachfolgend sind die Anforderungen aufgeführt, für die die Referenzarchitektur ausgelegt wurde:

- Ein mehrschichtiges Netzwerkdesign: Das Netzwerk ist durch geschützte Subnetze gebunden, um den Zugriff auf jeder Ebene zu beschränken: Webebene, Anwendungsebene und Datenebene. Kommunikation kann grundsätzlich nicht über Subnetze übertragen werden, da die gesamte Kommunikation im nächsten Subnetz

beendet wird.

- Standardmäßig blockierte Ports und Protokolle: Jedes Subnetz oder jede Sicherheitsgruppe blockiert standardmäßig alle eingehenden und ausgehenden Ports und Protokolle. Kommunikation wird durch Öffnen von Ausnahmen in der Portkonfiguration teilweise ermöglicht.
- Off-Box-Webauthentifizierung: Benutzeranforderungen aus dem Internet werden von einem Authentifizierungsmodul auf dem Reverseproxy in der Webschicht authentifiziert. Daher werden alle Anforderungen an die Anwendungsebene in der Webschicht authentifiziert, bevor sie an die geschützte Anwendungsebene weitergegeben werden.
- Plattformunabhängig: Die Lösung kann mit On-Premise-Serveranwendungen oder in der Cloud bereitgestellt werden.
- Technologieunabhängig: Die Lösung kann in einer Umgebung mit virtuellen Maschinen oder in Containern bereitgestellt werden. Eine Bereitstellung unter Windows oder Linux ist ebenfalls möglich. Diese erste Version der Referenzarchitektur und der unterstützenden Dokumentation wurde jedoch für Linux entwickelt, das in AWS ausgeführt wird.
- Hochverfügbar: Alle Komponenten des Systems werden als Cluster bereitgestellt und sind für eine aktive/aktive oder aktive/passive Bereitstellung ausgelegt.
- Isolierte Rollen: Jeder Server führt eine diskrete Rolle aus. Durch dieses Design werden alle Server so partitioniert, dass der Zugriff auf dienstspezifische Administratoren beschränkt werden kann. So wird zum Beispiel PostgreSQL für Tableau von Datenbankadministratoren verwaltet, das Authentifizierungsmodul in der Webschicht wird von Identitätsadministratoren verwaltet, und für den Datenverkehr und die Konnektivität sind Netzwerk- und Cloud-Administratoren verantwortlich.
- Linear skalierbar: Mit diskreten Rollen können Sie jeden Schichtendienst unabhängig gemäß dem Lastprofil skalieren.
- Client-Unterstützung: Die Referenzarchitektur unterstützt alle Tableau-Clients: Tableau Desktop (Version 2021.2 oder höher), Tableau Mobile und Tableau-Webdokumenterstellung.

Sicherheitsmaßnahmen

Wie bereits erwähnt, ist die Sicherheit ein Hauptmerkmal des branchenüblichen Rechenzentrumsdesigns.

- Zugriff: Jede Schicht ist von einem Subnetz gebunden, das die Zugriffskontrolle auf Netzwerkebene mittels Portfilterung erzwingt. Der Kommunikationszugriff zwischen Subnetzen kann auch von der Anwendungsebene mit authentifizierten Diensten zwischen Prozessen erzwungen werden.
- Integration: Die Architektur ist für die Verbindung mit dem Identitätsanbieter (IdP) auf dem Reverseproxy in der Webschicht konzipiert.
- Datenschutz: Datenverkehr in die Webschicht wird vom Client per SSL verschlüsselt. Der Datenverkehr in die internen Subnetze kann optional auch verschlüsselt werden.

Webproxy-Schicht

Die Webschicht ist ein Subnetz in der DMZ (Demilitarized Zone, entmilitarisierte Zone, wird auch als Umkreiszone bezeichnet), das als Sicherheitspuffer zwischen dem Internet und den internen Subnetzen dient, in denen die Anwendungen bereitgestellt sind. Die Webschicht hostet Reverseproxy-Server, die keine vertraulichen Informationen speichern. Die Reverseproxy-Server sind mit einem AuthN-Plugin so konfiguriert, dass sie Clientsitzungen mit einem vertrauenswürdigen Identitätsanbieter vorab authentifizieren, bevor er die Clientanfrage an Tableau Server umleitet. Weitere Informationen finden Sie unter Vor-Authentifizierung mit einem AuthN-Modul.

Lastenausgleich

Das Bereitstellungsdesign enthält vor den Reverseproxy-Servern eine Lastenausgleichslösung für den Unternehmenseinsatz.

Ein Lastenausgleich bietet wichtige Sicherheits- und Leistungsverbesserungen durch:

- Virtualisierung der Front-End-URL für die Anwendungsschicht-Dienste
- Erzwingen der SSL-Verschlüsselung
- SSL entladen
- Erzwingen der Komprimierung zwischen dem Client und den Webschichtdiensten
- Schutz vor DOS-Angriffen
- Bereitstellung von Hochverfügbarkeit

Hinweis: Tableau Server-Version 2022.1 enthält das Tableau Server Independent Gateway. Independent Gateway ist eine eigenständige Instanz des Tableau Gateway-Prozesses, die als Tableau-fähiger Reverse-Proxy dient. Zum Zeitpunkt der Veröffentlichung wurde das Independent Gateway zwar validiert, aber noch nicht vollständig in der Bereitstellungshandbuch-Referenzarchitektur getestet. Nach Abschluss der Tests wird das Bereitstellungshandbuch mit einer Anleitung für das Tableau Server Independent Gateway aktualisiert.

Anwendungsschicht

Die Anwendungsschicht ist ein Subnetz, in dem die zentrale Geschäftslogik der Serveranwendung ausgeführt wird. Die Anwendungsschicht besteht aus Diensten und Prozessen, die über verteilte Knoten in einem Cluster konfiguriert sind. Der Zugriff auf die Anwendungsschicht ist nur aus der Webschicht möglich. Benutzer können nicht direkt darauf zugreifen.

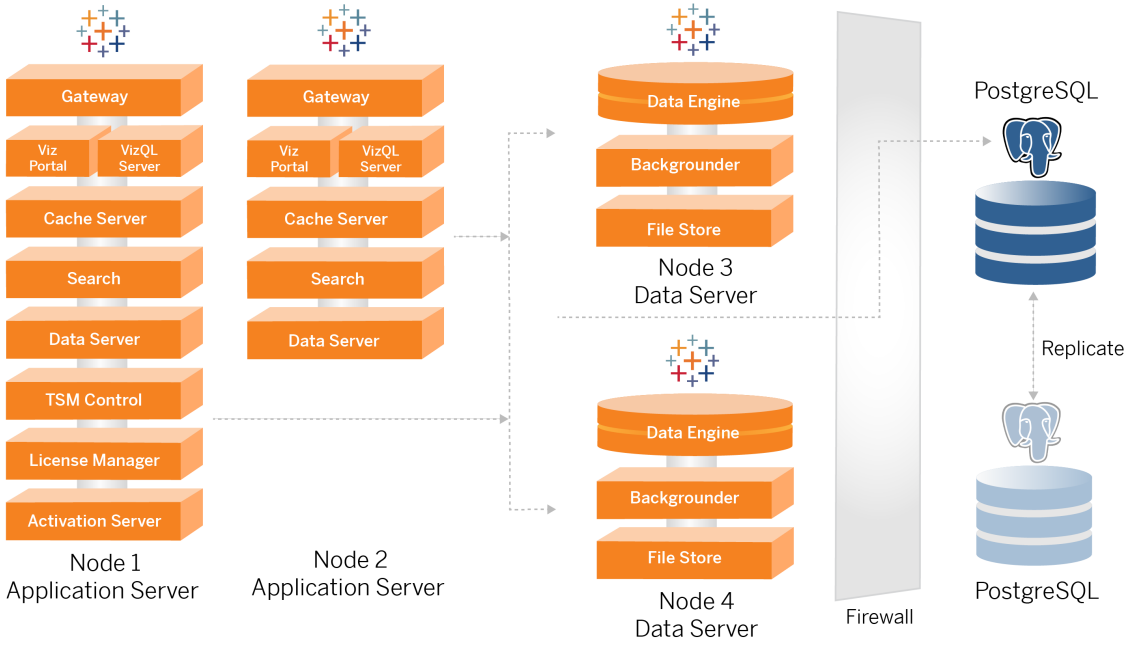
Leistung und Zuverlässigkeit werden verbessert, indem die Anwendungsprozesse so konfiguriert werden, dass Prozesse mit unterschiedlichen Ressourcennutzungsprofilen (d. h. CPU-intensiv oder speicherintensiv) gemeinsam platziert werden.

Datenschicht

Die Datenschicht ist ein Subnetz, das wertvolle Daten enthält. Sämtlicher Datenverkehr zu dieser Schicht stammt aus der Anwendungsschicht und ist daher bereits authentifiziert. Zusätzlich zu den Zugriffsanforderungen auf der Netzwerkebene mit Portkonfiguration sollte diese Ebene über authentifizierten Zugriff und optional verschlüsselten Datenverkehr mit der Anwendungsschicht verfügen.

Teil 2 - Einführung in die Referenzarchitektur für die Bereitstellung von Tableau Server

Die folgende Abbildung zeigt die relevanten Tableau Server-Prozesse und wie sie in der Referenzarchitektur bereitgestellt werden. Das ist die minimale für Unternehmen geeignete Bereitstellung von Tableau Server.



Die Prozessdiagramme in diesem Thema sollen die wichtigsten, bestimmenden Prozesse eines jeden Knotens zeigen. Es gibt viele unterstützende Prozesse, die ebenfalls auf den Knoten laufen und in den Diagrammen nicht dargestellt sind. Eine Liste aller Prozesse finden Sie im Konfigurationsabschnitt dieses Handbuchs: Teil 4 – Installieren und Konfigurieren von Tableau Server.

Tableau Server-Prozesse

Die Tableau Server-Referenzarchitektur ist eine Bereitstellung von Tableau Server in einem Cluster aus vier Knoten, mit einem externen Repository in PostgreSQL:

- Tableau Server-Anfangsknoten (Knoten 1): Auf diesem Knoten werden erforderliche TSM-Administrations- und Lizenzierungsdienste ausgeführt, die nur auf einem einzelnen Knoten im Cluster ausgeführt werden können. Im Unternehmenskontext ist der Tableau Server-Anfangsknoten der primäre Knoten im Cluster. Auf diesem Knoten werden auch redundante Anwendungsdienste mit Knoten 2 ausgeführt.
- Tableau Server-Anwendungsknoten (Knoten 1 und Knoten 2): Die beiden Knoten bedienen Clientanforderungen, stellen eine Verbindung zu Datenquellen und Datenknoten her und fragen diese ab.
- Tableau Server-Datenknoten (Knoten 3 und Knoten 4): Zwei Knoten, die für die Verwaltung von Daten vorgesehen sind.
- Externes PostgreSQL: Auf diesem Host wird der Tableau Server-Repository-Prozess ausgeführt. Für eine Hochverfügbarkeits-Bereitstellung müssen Sie einen zusätzlichen PostgreSQL-Host für aktive/passive Redundanz ausführen.

  Sie können PostgreSQL auch auf Amazon RDS ausführen. Weitere Informationen zu den Unterschieden zwischen der Ausführung des Repositorys auf RDS oder auf einer EC2-Instanz finden Sie unter *Externes Tableau Server-Repository* (Linux).

  Für die Bereitstellung von Tableau Server mit einem externen Repository ist eine Tableau Advanced Management-Lizenz erforderlich.

  Wenn es in Ihrem Unternehmen kein internes Datenbank-Know-How gibt, können Sie den Tableau Server-Repository-Prozess optional in der standardmäßigen, internen PostgreSQL-Konfiguration ausführen lassen. In dem Standardszenario wird das Repository auf einem Tableau-Knoten mit eingebettetem PostgreSQL ausgeführt. In diesem Fall empfehlen wir, dass das Repository auf einem dedizierten Tableau-Knoten und ein passives Repository auf einem zusätzlichen dedizierten Knoten ausgeführt werden, damit Repository-Failover unterstützt wird. Weitere Informationen dazu finden Sie unter *Repository-Failover* (Linux).

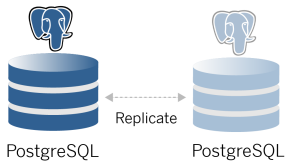
Die in diesem Leitfaden beschriebene AWS-Implementierung erläutert beispielsweise, wie das externe Repository auf PostgreSQL bereitgestellt wird, das auf einer EC2-Instanz ausgeführt wird.

- Optional: Wenn in Ihrem Unternehmen externer Speicher verwendet wird, können Sie den Tableau-Dateispeicher als externen Dienst bereitstellen. Der externe Dateispeicher im zentralen Bereitstellungsszenario ist in diesem Handbuch nicht enthalten. Informationen dazu finden Sie unter *Installieren von Tableau Server mit dem externen Dateispeicher* (Linux).

  Für die Bereitstellung von Tableau Server mit einem externen Dateispeicher ist eine Tableau Advanced Management-Lizenz erforderlich.

PostgresSQL-Repository

Das Tableau Server-Repository ist eine PostgresSQL-Datenbank, in der Serverdaten gespeichert werden. Zu diesen Daten zählen Informationen über Tableau Server-Benutzer, -Gruppen, -Gruppenzuweisungen, -Berechtigungen, -Projekte, -Datenquellen, -Extraktmetadaten und -Aktualisierungsinformationen.



Die standardmäßige PostgresSQL-Bereitstellung belegt fast 50 % der Systemspeicherressourcen. Abhängig von der Nutzung (für die Produktion und große Produktionsbereitstellungen) kann die Ressourcennutzung steigen. Daher empfehlen wir, den Repository-Prozess auf einem Computer auszuführen, auf dem keine anderen ressourcenintensiven Serverkomponenten wie VizQL, Hintergrundprozesskomponenten oder die Daten-Engine ausgeführt werden. Das Ausführen des Repository-Prozesses zusammen mit einer dieser Komponenten führt zu E/A-Konflikten, Ressourcenbeschränkungen und einer Verschlechterung der Gesamtleistung der Bereitstellung.

Knoten 1: Anfangsknoten

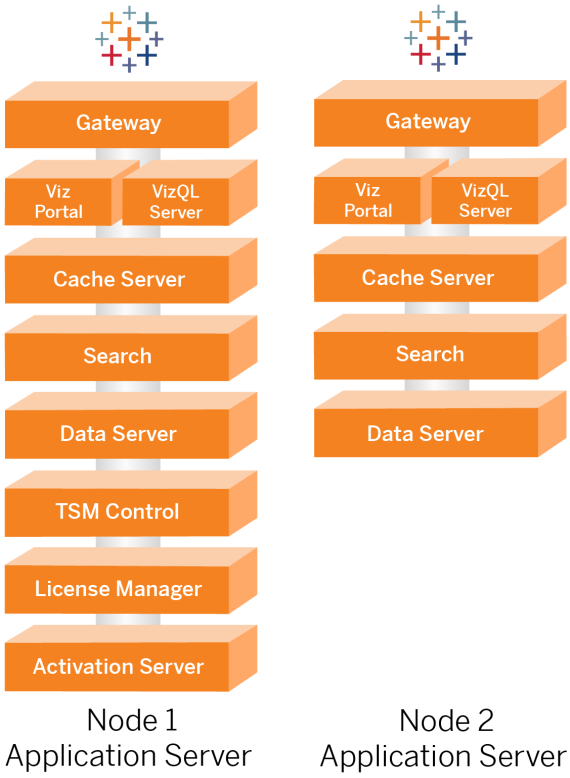
Auf dem Anfangsknoten wird eine kleine Anzahl wichtiger Prozesse ausgeführt und die Anwendungslast mit Knoten 2 geteilt.

Der erste Computer, auf dem Sie Tableau installieren (der "Anfangsknoten"), hat einige einzigartige Eigenschaften. Drei Prozesse werden nur auf dem Ausgangsknoten ausgeführt und können – außer bei einem Ausfall – nicht auf einen anderen Knoten verschoben werden. Dies sind der Lizenzdienst (Lizenzverwaltung), der Aktivierungsdienst und der TSM-Controller (Administration Controller).

Knoten-1-Failover und automatische Wiederherstellung

Die Lizenz-, Aktivierungs- und TSM-Controller-Dienste sind für die Funktionsfähigkeit einer Tableau Server-Bereitstellung entscheidend. Im Falle eines Ausfalls von Knoten 1 können Benutzer weiterhin eine Verbindung zu der Tableau Server-Bereitstellung herstellen, da eine ordnungsgemäß konfigurierte Referenzarchitektur Anfragen an Knoten 2 weiterleiten wird. Ohne diese zentralen Dienste befindet sich die Bereitstellung jedoch in einem kritischen Zustand und es besteht die Gefahr, dass sie jederzeit ausfallen kann. Informationen dazu finden Sie unter Automatische Wiederherstellung des Anfangsknotens.

Knoten 1 und 2: Anwendungsserver



Auf den Knoten 1 und 2 werden die Tableau Server-Prozesse ausgeführt, die Clientanforderungen bedienen, Datenquellen abfragen, Visualisierungen generieren, mit Inhalten umgehen, Verwaltungsaufgaben erledigen sowie andere zentrale Tableau-Geschäftslogik verwalten. Die Anwendungsserver speichern keine Benutzerdaten.

> **Hinweis**: "Anwendungsserver" ist ein Begriff, der sich auch auf einen Tableau Sever-Prozess bezieht, der in TSM aufgeführt ist. Der zugrunde liegende Prozess für "Anwendungsserver" ist VizPortal.

Parallel ausgeführt, skalieren Knoten 1 und Knoten 2, um Anforderungen von der Lastenausgleichslogik zu bedienen, die auf den Reverseproxy-Servern ausgeführt wird. Sollte

einer dieser redundanten Knoten ausfallen, werden Clientanfragen und -bearbeitung von dem verbleibenden Knoten verarbeitet.

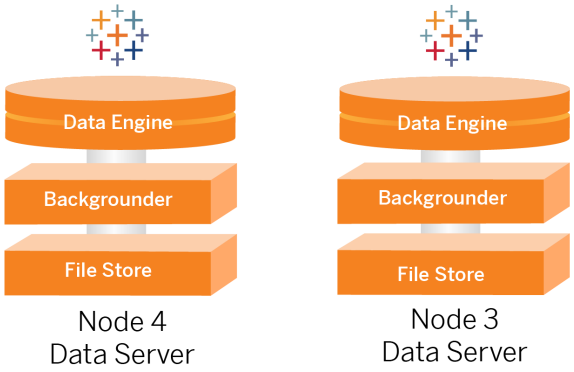
Die Referenzarchitektur wurde so konzipiert, dass komplementäre Anwendungsprozesse auf demselben Computer ausgeführt werden. Das bedeutet, dass die Prozesse nicht um Rechenressourcen konkurrieren und somit keine Konflikte verursachen.

So ist beispielsweise VizQL, ein zentraler Verarbeitungsdienst auf Anwendungsservern, in hohem Maße CPU- und speicherhungrig. VizQL beansprucht fast 60 bis 70 % der CPU und des Arbeitsspeichers des Computers. Daher ist die Referenzarchitektur so konzipiert, dass sich keine weiteren Prozesse auf demselben Knoten wie VizQL befinden, die Speicher oder CPU stark in Anspruch nehmen. Tests zeigen, dass die Last oder die Anzahl an Benutzern keinen Einfluss auf die Speicher- oder CPU-Auslastung auf VizQL-Knoten hat. In unserem Auslastungstest hat sich beispielsweise gezeigt, dass sich eine Verringerung der gleichzeitigen Benutzer nur auf die Leistung des Dashboards oder den Ladevorgang der Visualisierung auswirkt, während die Ressourcennutzung dadurch jedoch nicht verringert wird. Basierend auf dem verfügbaren Arbeitsspeicher und der CPU während der Spitzenauslastung können Sie daher das Hinzufügen weiterer VizQL-Prozesse in Betracht ziehen. Als Ausgangspunkt für typische Arbeitsmappen sollten Sie 4 Kerne pro VizQL-Prozess zuweisen.

Skalieren von Anwendungsservern

Die Referenzarchitektur ist so ausgelegt, dass es auf einem nutzungsbasierten Modell basierend skaliert wird. Als allgemeinen Ausgangspunkt empfehlen wir mindestens zwei Anwendungsserver, die jeweils bis zu 1.000 Benutzer unterstützen. Planen Sie bei steigender Benutzerbasis einen weiteren Anwendungsserver für jeweils weitere 1.000 Benutzer ein. Überwachen Sie Nutzung und Leistung, um die Benutzerbasis pro Host für Ihr Unternehmen zu optimieren.

Knoten 3 und 4: Datenserver



Die Dateispeicher-, Daten-Engine- (Hyper) und Hintergrundprozesskomponente-Prozesse befinden sich aus den folgenden Gründen auf den Knoten 3 und 4:

- Extraktoptimierung: Die Ausführung von Hintergrundprozesskomponente, Hyper und Dateispeicher auf demselben Knoten optimiert die Leistung und Zuverlässigkeit. Während des Extraktionsprozesses fragt die Hintergrundprozesskomponente die Zieldatenbank ab, erstellt die Hyper-Datei auf demselben Knoten und lädt sie dann in den Dateispeicher hoch. Wenn diese Prozesse auf demselben Knoten ablaufen, müssen bei der Extraktionserstellung keine großen Datenmengen über das Netz oder die Knoten kopiert werden.
- Ergänzender Ressourcenausgleich: Die Hintergrundprozesskomponente ist hauptsächlich CPU-intensiv. Die Daten-Engine ist ein speicherintensiver Prozess. Die Kopplung dieser Prozesse ermöglicht eine maximale Ressourcennutzung auf jedem Knoten.
- Konsolidierung von Datenprozessen: Da es sich bei jedem dieser Prozesse um Back-End-Datenprozesse handelt, ist es sinnvoll, sie in der sichersten Datenschicht auszuführen. In zukünftigen Versionen der Referenzarchitektur werden die Anwendungs- und Datenserver in getrennten Schichten ausgeführt. Aufgrund von Anwendungsabhängigkeiten in der Tableau-Architektur müssen Anwendungs- und Datenserver jedoch zu diesem Zeitpunkt in derselben Schicht ausgeführt werden.

Skalieren von Datenservern

Wie bei Anwendungsservern müssen die Ressourcen, die für Tableau-Datenserver erforderlich sind, auf Grundlage einer nutzungsbasierten Modellierung geplant werden. Gehen Sie im Allgemeinen davon aus, dass jeder Datenserver bis zu 2.000 Extraktaktualisierungsaufträge pro Tag unterstützen kann. Wenn Ihre Extraktaufträge zunehmen, fügen Sie zusätzliche Datenserver ohne den Dateispeicherdienst hinzu. Im Allgemeinen eignet sich die Datenserverbereitstellung mit zwei Knoten für Bereitstellungen, die das lokale Dateisystem für den Dateispeicherdienst verwenden. Beachten Sie, dass sich das Hinzufügen weiterer Anwendungsserver nicht linear auf die Leistung oder Skalierung auf Datenservern auswirkt. Abgesehen von einem gewissen Verwaltungsaufwand, den zusätzliche Benutzerabfragen mit sich bringen, sind die Auswirkungen weiterer Anwendungshosts und Benutzer minimal.

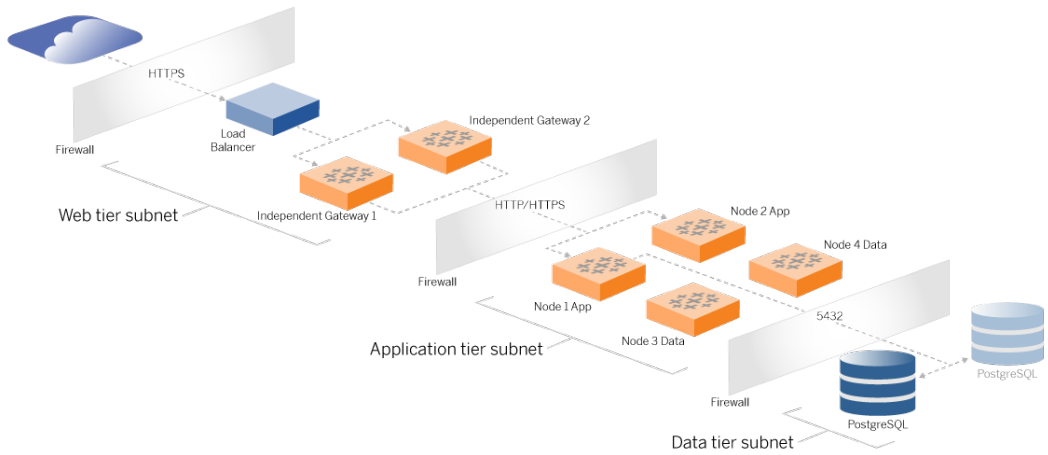
Teil 3 - Vorbereiten der Bereitstellung von Tableau Server Enterprise

Im 3. Teil werden die Anforderungen für die Vorbereitung Ihrer Infrastruktur auf die Bereitstellung der Tableau Server-Referenzarchitektur beschrieben. Bevor Sie beginnen sollten Sie sich Teil 2 – Einführung in die Referenzarchitektur für die Bereitstellung von Tableau Server ansehen.

Neben den Beschreibungen der Anforderungen enthält dieses Thema ein Implementierungsbeispiel der Referenzarchitektur in einer AWS-Umgebung. Der Rest dieses Handbuchs baut auf dem AWS-Referenzarchitekturbeispiel auf, das in diesem Thema begonnen wurde.

Ein Kernprinzip der Referenzarchitektur ist die Standardisierung mit Best Practices für die Sicherheit im Rechenzentrum. Die Architektur ist insbesondere darauf ausgelegt, Dienste in geschützte Netzwerk-Subnetze aufzuteilen. Die Kommunikation zwischen Subnetzen ist auf bestimmten Protokoll- und Portverkehr beschränkt.

Das folgende Diagramm veranschaulicht das Subnetzdesign der Referenzarchitektur für eine lokale Bereitstellung oder eine vom Kunden verwaltete Cloud-Bereitstellung. Ein Beispiel für eine Cloud-Bereitstellung finden Sie weiter unten im Abschnitt Beispiel: Konfigurieren von Subnetzen und Sicherheitsgruppen in AWS.



Subnetze

Erstellen Sie drei Subnetze:

- Eine Webschicht
- Eine Anwendungsschicht
- Eine Datenschicht

Firewall-/Sicherheitsgruppenregeln

Auf den folgenden Registerkarten werden die Firewallregeln für jede Schicht des Rechenzentrums beschrieben. Informationen zu Regeln AWS-spezifischer Sicherheitsgruppen finden Sie weiter unten in diesem Thema.

Webschicht

Die Webschicht ist ein öffentliches DMZ-Subnetz, das eingehende HTTPS-Anfragen verarbeitet und die Anfragen an die Anwendungsschicht weiterleitet. Dieses Design bietet eine Ebene zum Schutz vor Malware, die Ihr Unternehmen befallen könnte. Die Webschicht blockiert den Zugriff auf die Anwendungs-/Datenschicht.

Datenverkehr	Typ	Protokoll	Portbereich	Quelle
Eingehend	SSH	TCP	22	Bastion-Subnetz (für Cloud-Bereitstellungen)
Eingehend	HTTP	TCP	80	Internet (0.0.0.0/0)
Eingehend	HTTPS	TCP	443	Internet (0.0.0.0/0)
Ausgehend	Sämtlicher Datenverkehr	Alle	Alle	

Anwendungsschicht

Das Anwendungs-Subnetz ist die Stelle, an der sich die Tableau Server-Bereitstellung befindet. Das Anwendungs-Subnetz enthält die Tableau-Anwendungsserver (Knoten 1 und Knoten 2). Die Tableau-Anwendungsserver verarbeiten Benutzeranforderungen, die an die Datenserver gestellt werden, und führen die zentrale Geschäftslogik aus.

Das Anwendungs-Subnetz umfasst auch die Tableau-Datenserver (Knoten 3 und Knoten 4).

Sämtlicher Client-Datenverkehr zur Anwendungsschicht wird in der Webschicht authentifiziert. Der administrative Zugriff auf das Anwendungs-Subnetz wird authentifiziert und über den Bastion-Host geleitet.

Datenverkehr	Typ	Protokoll	Portbereich	Quelle
Eingehend	SSH	TCP	22	Bastion-Subnetz (für Cloud-Bereitstellungen)
Eingehend	HTTPS	TCP	443	Webschicht-Subnetz
Ausgehend	Sämtlicher	Alle	Alle	

	Datenverkehr			

Datenschicht

Das Daten-Subnetz ist die Stelle, an der sich der externe PostgreSQL-Datenbankserver befindet.

Datenverkehr	Typ	Protokoll	Portbereich	Quelle
Eingehend	SSH	TCP	22	Bastion-Subnetz (für Cloud-Bereitstellungen)
Eingehend	PostgreSQL	TCP	5432	Subnetz "Anwendungsschicht"
Ausgehend	Sämtlicher Datenverkehr	Alle	Alle	

Bastion

Die meisten Sicherheitsteams in Unternehmen erlauben keine direkte Kommunikation zwischen dem lokalen Verwaltungssystem und den in der Cloud bereitgestellten Knoten. Stattdessen wird der gesamte administrative SSH-Verkehr zu den Cloud-Knoten über einen Bastion-Host (auch als "Jump Server" bezeichnet) geleitet. Für Cloud-Bereitstellungen empfehlen wir eine Bastion-Host-Proxyverbindung zu allen Ressourcen in der Referenzarchitektur. Dies ist eine optionale Konfiguration für On-Premise-Umgebungen.

Der Bastion-Host authentifiziert den administrativen Zugriff und lässt nur Datenverkehr über das SSH-Protokoll zu.

Datenverkehr	Typ	Protokoll	Portbereich	Quelle	Ziel

Eingehend	SSH	TCP	22	IP-Adresse des Administratorcomputers	
Ausgehend	SSH	TCP	22		Webschicht-Subnetz
Ausgehend	SSH	TCP	22		Subnetz "Anwendungsschicht"

Beispiel: Konfigurieren von Subnetzen und Sicherheitsgruppen in AWS

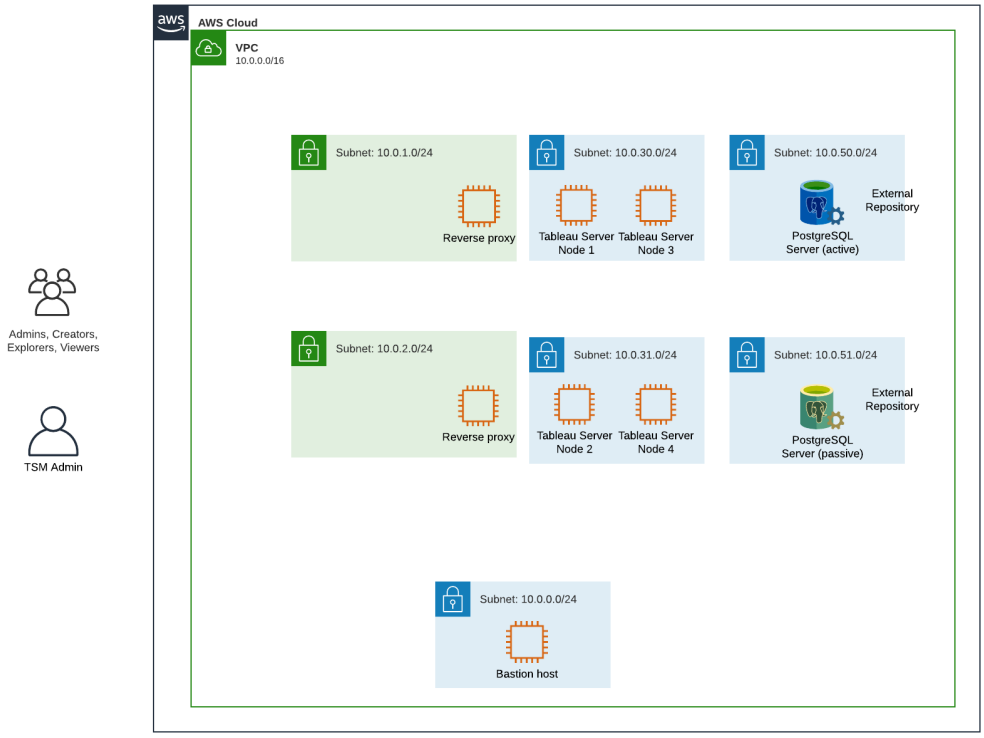
Dieses Thema enthält Schritt-für-Schritt-Anleitungen zum Erstellen und Konfigurieren der VPC und Netzwerkumgebung für die Bereitstellung der Tableau Server-Referenzarchitektur in AWS.

Die folgenden Folien zeigen die Referenzarchitektur in vier Ebenen. Während Sie die Folien durchgehen, werden Komponentenelemente auf die Topologiekarte geschichtet:

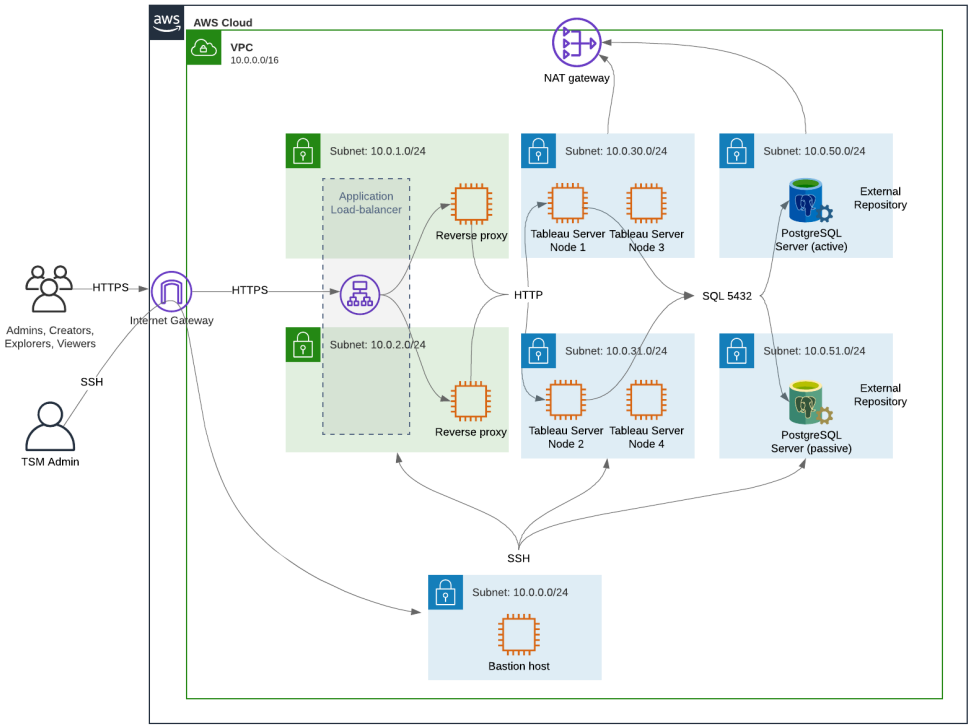
1. VPC-Subnetz-Topologie und EC2-Instanzen: ein Bastion-Host, zwei Reverseproxy-Server, vier Tableau Server und mindestens ein PostgreSQL-Server.
2. Protokollfluss und Internetverbindung: Sämtlicher eingehender Datenverkehr wird über das AWS-Internet-Gateway verwaltet. Datenverkehr in Richtung Internet wird über das NAT geroutet.
3. Verfügbarkeitszonen: Die Proxy-, Tableau Server- und PostgreSQL-Hosts sind gleichmäßig auf zwei Verfügbarkeitszonen verteilt.
4. Sicherheitsgruppen: Vier Sicherheitsgruppen (Öffentlich, Privat, Daten und Bastion) schützen jede Schicht auf der Protokollebene.

AWS-Referenzarchitektur

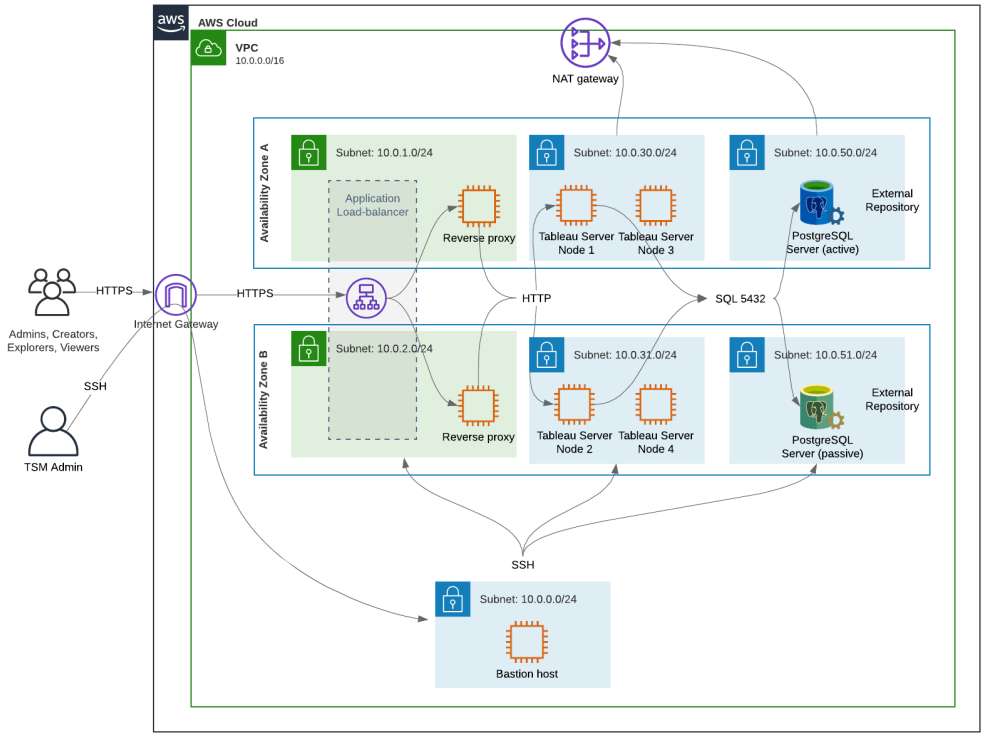
Folie 1: VPC-Subnetztopologie und EC2-Instanzen



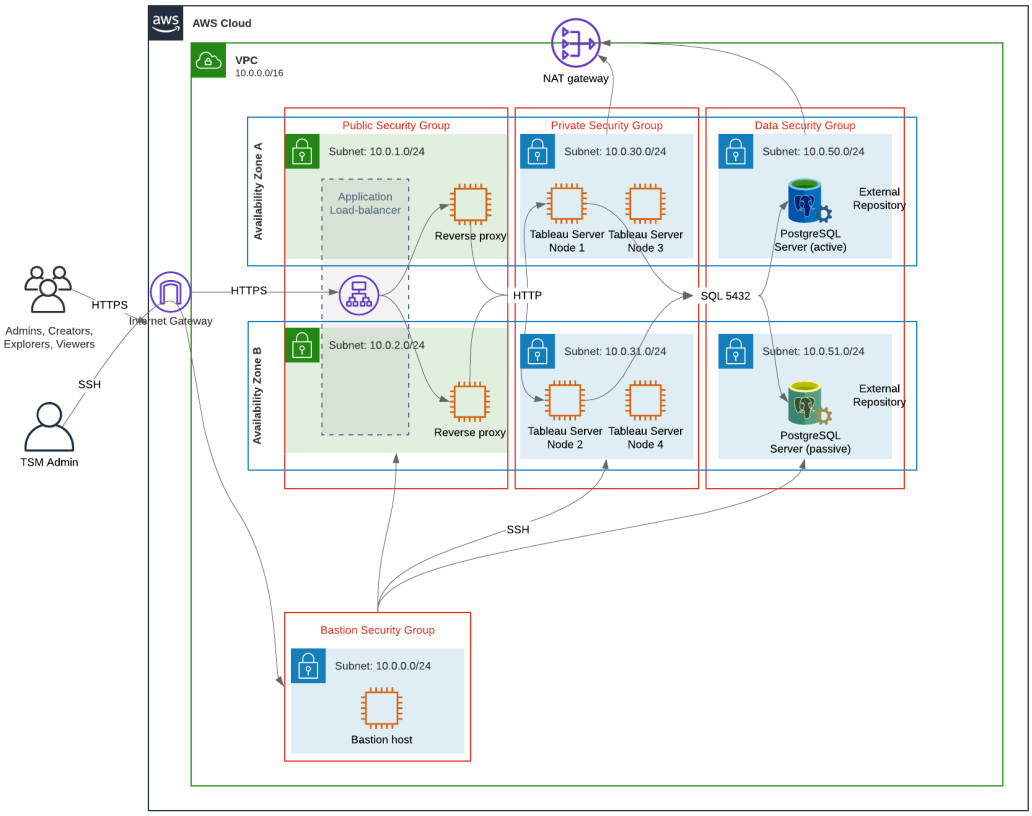
Folie 2: Protokollfluss und Konnektivität



Folie 3: Verfügbarkeitszonen



Folie 4: Sicherheitsgruppen



AWS-Verfügbarkeitszonen und hohe Verfügbarkeit

Die in diesem Handbuch vorgestellte Referenzarchitektur spezifiziert eine Bereitstellung, die Verfügbarkeit durch Redundanz bietet, wenn ein einzelner Host ausfällt. Im AWS-Fall, in dem die Referenzarchitektur in zwei Verfügbarkeitszonen bereitgestellt wird, ist die Verfügbarkeit jedoch in dem sehr seltenen Fall gefährdet, dass eine Verfügbarkeitszone ausfällt.

VPC-Konfiguration

In diesem Abschnitt wird Folgendes beschrieben:

- Installieren und Konfigurieren der VPC
- Konfigurieren der Internetkonnektivität

- Konfigurieren von Subnetzen
- Erstellen und Konfigurieren von Sicherheitsgruppen

Konfigurieren der VPC

Die Vorgehensweise in diesem Abschnitt entspricht der Benutzeroberfläche in der "klassischen" VPC-Umgebung. Sie können die Benutzeroberfläche zur Anzeige der klassischen Ansicht umschalten, indem Sie die neue VPC-Umgebung in der oberen linken Ecke des AWS VPC-Dashboards deaktivieren.

Führen Sie den VPC-Assistenten aus, um das standardmäßige private und öffentliche Subnetz sowie die Standard-Routing- und Standard-Netzwerk-Zugriffssteuerungsliste (ACL) zu erstellen.

1. Bevor Sie eine VPC konfigurieren, müssen Sie eine "Elastic IP" erstellen. Erstellen Sie eine Zuordnung unter Verwendung aller Standardeinstellungen.
2. Führen Sie den VPC-Assistenten aus, und wählen Sie die Option "VPC mit öffentlichen und privaten Subnetzen" aus.
3. Akzeptieren Sie die meisten Standardeinstellungen, außer den folgenden:
    - Geben Sie einen VPC-Namen ein.
    - Geben Sie die Zuordnungs-ID der "Elastic IP" an.
    - Geben Sie die folgenden CIDR-Masken an:
        - IPv4-CIDR des öffentlichen Subnetzes: 10.0.1.0/24 – benennen Sie dieses Subnetz in `Public-a` um.
        - IPv4-CIDR des privaten Subnetzes: 10.0.30.0/24 – benennen Sie dieses Subnetz in `Private-a` um.
    - Verfügbarkeitszone: Wählen Sie für beide Subnetze die Option **a** für die Region aus, in der Sie sich befinden.

        Hinweis: In diesem Beispiel verwenden wir **a** und **b**, um zwischen Verfügbarkeitszonen in einem bestimmten AWS-Rechenzentrum zu unterscheiden. In AWS stimmen die Namen der Verfügbarkeitszonen möglicherweise nicht mit den hier gezeigten Beispielen überein. So

> enthalten zum Beispiel einige Verfügbarkeitszonen **c-** und **d-**Zonen innerhalb eines Rechenzentrums.

4. Klicken Sie auf **VPC erstellen**.
5. Nachdem die VPC erstellt wurde, erstellen Sie die Subnetze `Public-b`,`Private-b`, `Data` und `Bastion`. Klicken Sie zum Erstellen eines Subnetzes auf **Subnetze** > **Subnetz erstellen**.
    - `Public-b`: Wählen Sie für "Verfügbarkeitszone" die Option **b** für die Region aus, in der Sie sich befinden. CIDR-Block: 10.0.2.0/24
    - `Private-b`: Wählen Sie für "Verfügbarkeitszone" die Option **b** für die Region aus, in der Sie sich befinden. CIDR-Block: 10.0.31.0/24
    - `Data`: Wählen Sie für "Verfügbarkeitszone" die Option **a** für die Region aus, in der Sie sich befinden. CIDR-Block: 10.0.50.0/24 Optional: Wenn Sie beabsichtigen, die externe Datenbank über einen PostgreSQL-Cluster zu replizieren, erstellen Sie ein Data-b-Subnetz in der Zone b mit einem CIDR-Block von 10.0.51.0/24.
    - `Bastion`: Wählen Sie für "Verfügbarkeitszone" eine der beiden Zonen aus. CIDR-Block: 10.0.0.0/24
6. Nachdem die Subnetze erstellt wurden, bearbeiten Sie die Routing-Tabellen für das öffentliche und das Bastion-Subnetz so, dass die Routing-Tabelle verwendet wird, die für das zugehörige Internet-Gateway (Internet Gateway, IGW) konfiguriert ist. Bearbeiten Sie das private Subnetz und das Daten-Subnetz so, dass die Routing-Tabelle verwendet, die für den Netzwerkadressübersetzer (Network Address Translator, NAT) konfiguriert ist.
    - Um festzustellen, welche Routing-Tabelle mit dem IGW oder dem NAT konfiguriert ist, klicken Sie im AWS-Dashboard auf **Routing-Tabellen**. Wählen Sie einen der beiden Routing-Tabellen-Links aus, um die Eigenschaftsseite zu öffnen. Achten Sie auf den Zielwert unter **Routen** > **Ziel** > **0.0.0.0/0**. Der Zielwert unterscheidet den Typ der Route. Er beginnt entweder mit der Zeichenfolge `igw-` oder mit `nat-`.
    - Zum Aktualisieren von Routing-Tabellen klicken Sie auf **VPC** > **Subnetze** > [Subnetzname] > **Routing-Tabelle** > **Routing-Tabellenzuordnung bearbeiten**.

Konfigurieren von Sicherheitsgruppen

Der VPC-Assistent erstellt eine einzelne Sicherheitsgruppe, die Sie nicht verwenden werden. Erstellen Sie die folgenden Sicherheitsgruppen (**Sicherheitsgruppen** > **Sicherheitsgruppe erstellen**). Die EC2-Hosts werden in diesen Gruppen über zwei Verfügbarkeitszonen hinweg installiert, wie in dem Foliendiagramm oben gezeigt.

- Erstellen Sie eine neue Sicherheitsgruppe: **Private** ("Privat"). Hier werden alle 4 Knoten von Tableau Server installiert. Die Sicherheitsgruppe "Private" wird den Subnetzen 10.0.30.0/24 und 10.0.31.0/24 zugeordnet.
- Erstellen Sie eine neue Sicherheitsgruppe: **Public** ("Öffentlich"). Hier werden Proxyserver installiert. Die Sicherheitsgruppe "Public" wird später in diesem Verfahren den Subnetzen 10.0.1.0/24 und 10.0.2.0/24 zugeordnet.
- Erstellen Sie eine neue Sicherheitsgruppe: **Data**. ("Daten"). Hier wird das externe PostgreSQL-Tableau-Repository installiert. Die Sicherheitsgruppe "Data" wird später in diesem Verfahren dem Subnetz 10.0.50.0/24 (und optional 10.0.51.0/24) zugeordnet.
- Erstellen Sie eine neue Sicherheitsgruppe: **Bastion**. Hier werden Sie den Bastion-Host installieren. Die Sicherheitsgruppe "Bastion" wird später in diesem Verfahren dem Subnetz und 10.0.0.0/24 zugeordnet.

Angeben von Regeln für eingehenden und ausgehenden Datenverkehr

In AWS sind Sicherheitsgruppen das Gegenstück zu Firewalls in einer On-Premise-Umgebung. Sie müssen den Typ von Datenverkehr (z. B. http, https usw.), das Protokoll (TCP oder UDP) und die Ports oder den Portbereich (z. B. 80, 443 usw.) angeben, über die Datenverkehr in die und aus der Sicherheitsgruppe geleitet werden darf. Für jedes Protokoll müssen Sie auch den Ziel- oder Quelldatenverkehr angeben.

Regeln für die öffentliche Sicherheitsgruppe

Regeln für eingehenden Datenverkehr			
Typ	**Protokoll**	**Portbereich**	**Quelle**
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0

SSH	TCP	22	Bastion-Sicherheitsgruppe ("Bastion")

Regeln für ausgehenden Datenverkehr			
Typ	**Protokoll**	**Portbereich**	**Ziel**
Sämtlicher Datenverkehr	Alle	Alle	0.0.0.0/0

Regeln für die Sicherheitsgruppe "Private"

Die Sicherheitsgruppe "Private" enthält eine Regel für eingehenden Datenverkehr, um HTTP-Datenverkehr von der Sicherheitsgruppe "Public" zuzulassen. Lassen Sie HTTP-Datenverkehr nur während des Bereitstellungsprozesses zu, um die Konnektivität zu überprüfen. Wir empfehlen, die Regel für über HTTP eingehenden Datenverkehr zu entfernen, nachdem Sie die Bereitstellung des Reverse-Proxys und die Konfiguration von SSL für Tableau abgeschlossen haben.

Regeln für eingehenden Datenverkehr			
Typ	**Protokoll**	**Portbereich**	**Quelle**
HTTP	TCP	80	Öffentliche Sicherheitsgruppe ("Public")
HTTPS	TCP	443	Öffentliche Sicherheitsgruppe ("Public")
PostgreSQL	TCP	5432	Daten-Sicherheitsgruppe ("Data")
SSH	TCP	22	Bastion-Sicherheitsgruppe ("Bastion")
Sämtlicher Datenverkehr	Alle	Alle	Private Sicherheitsgruppe ("Private")

Regel für ausgehenden Datenverkehr			
Typ	**Protokoll**	**Portbereich**	**Ziel**
Sämtlicher Datenverkehr	Alle	Alle	0.0.0.0/0
PostgreSQL	TCP	5432	Daten-Sicherheitsgruppe ("Data")
SSH	TCP	22	Bastion-Sicherheitsgruppe ("Bastion")

Regeln für die Daten-Sicherheitsgruppe ("Data")

Regeln für eingehenden Datenverkehr			
Typ	**Protokoll**	**Portbereich**	**Quelle**
PostgreSQL	TCP	5432	Private Sicherheitsgruppe ("Private")
SSH	TCP	22	Bastion-Sicherheitsgruppe ("Bastion")

Regeln für ausgehenden Datenverkehr			
Typ	**Protokoll**	**Portbereich**	**Ziel**
Sämtlicher Datenverkehr	Alle	Alle	0.0.0.0/0
PostgreSQL	TCP	5432	Private Sicherheitsgruppe ("Private")
SSH	TCP	22	Bastion-Sicherheitsgruppe ("Bastion")

Regeln für die Sicherheitsgruppe "Bastion-Host"

Regeln für eingehenden Datenverkehr			
Typ	**Protokoll**	**Portbereich**	**Quelle**
SSH	TCP	22	Die IP-Adresse und Netzmaske des Computers, mit dem Sie sich bei AWS anmelden werden (Admin-Computer).
SSH	TCP	22	Private Sicherheitsgruppe ("Private")
SSH	TCP	22	Öffentliche Sicherheitsgruppe ("Public")

Regeln für ausgehenden Datenverkehr			
Typ	**Protokoll**	**Portbereich**	**Ziel**
SSH	TCP	22	Die IP-Adresse und Netzmaske des Computers, mit dem Sie sich bei AWS anmelden werden (Admin-Computer).
SSH	TCP	22	Private Sicherheitsgruppe ("Private")
SSH	TCP	22	Öffentliche Sicherheitsgruppe ("Public")
SSH	TCP	22	Daten-Sicherheitsgruppe ("Data")
HTTPS	TCP	443	0.0.0.0/0 (Optional: Erstellen Sie diese Regel, wenn Sie Zugriff auf das Internet benötigen, um unterstützende Software auf dem Bas-

			tion-Host herunterzuladen.)

Aktivieren der automatischen Zuweisung öffentlicher IP-Adressen

Dadurch erhalten Sie eine IP-Adresse zum Herstellen einer Verbindung zu den Proxyservern und dem Bastion-Host.

Für das öffentliche Subnetz und das Bastion-Subnetz:

1. Wählen Sie das Subnetz aus.
2. Wählen Sie im Menü **Actions** (Aktionen) die Option "Modify auto-assign IP settings" (Einstellungen für automatische Zuweisung von IP-Adresse ändern) aus.
3. Klicken Sie auf "Enable auto-assign public IPv4 address" (Automatische Zuweisung von öffentlichen IPv4-Adressen aktivieren).
4. Klicken Sie auf **Save** (Speichern).

Lastenausgleich

Hinweis: Wenn Sie in AWS installieren und der Beispielbereitstellung in dieser Anleitung folgen, sollten Sie den AWS-Lastenausgleich später im Bereitstellungsprozess installieren und konfigurieren, wie in Teil 5 – Konfigurieren der Webschicht beschrieben.

Bei der lokalen Bereitstellung arbeiten Sie mit Ihren Netzwerkadministratoren zusammen, um einen Lastausgleich zur Unterstützung der Webschicht der Referenzarchitektur einzurichten:

- Ein webseitiger Anwendungs-Lastenausgleich, der HTTPS-Anforderungen von Tableau-Clients entgegen nimmt und mit den Reverse-Proxyservern kommuniziert.
- Reverse-Proxy:
  - Wir empfehlen mindestens zwei Proxyserver, um Redundanz zu erhalten und um die Client-Last zu bewältigen.
  - Er empfängt HTTPS-Datenverkehr vom Lastenausgleich.
  - Er unterstützt Sticky-Sitzung zum Tableau-Host.

    - Konfigurieren Sie den Proxy für Roundrobin-Lastenausgleich für jeden Tableau Server, auf dem der Gateway-Prozess ausgeführt wird.
    - Er verarbeitet Authentifizierungsanfragen von externem IdP.
- Forward-Proxy: Tableau Server benötigt für die Lizenzierung und die Kartenfunktionalität Zugriff auf das Internet. Je nach Ihrer Forward-Proxy-Umgebung müssen Sie möglicherweise Forward-Proxy-Safelists für Tableau-Service-URLs konfigurieren. Siehe *Kommunikation mit dem Internet* (Linux).

Konfigurieren der Hostcomputer

Empfohlene Mindesthardware

Die folgenden Empfehlungen stützen sich auf unsere Tests realer Daten in der Referenzarchitektur.

Anwendungsserver:

- CPU: 8 physische Kerne (16vCPUs),
- RAM: 128 GB (16 GB/physischer Kern)
- Festplattenplatz: 100 GB

Datenserver

- CPU: 8 physische Kerne (16vCPUs),
- RAM: 128 GB (16 GB/physischer Kern)
- Festplattenplatz: 1 TB Wenn Ihre Bereitstellung externen Speicher für den Tableau-Dateispeicher verwenden soll, müssen Sie den entsprechenden Speicherplatz berechnen. Informationen dazu finden Sie unter *Installieren von Tableau Server mit dem externen Dateispeicher* (Linux).

Proxyserver

- CPU: 2 physische Kerne (4vCPUs),
- RAM: 8 GB (4 GB/physischer Kern)
- Festplattenplatz: 100 GB

Externes Repository-Datenbank

- CPU: 8 physische Kerne (16vCPUs),
- RAM: 128 GB (16 GB/physischer Kern)
- Der Bedarf an Festplattenplatz hängt von Ihrer Datenlast und deren Auswirkungen auf Sicherungen ab. Weitere Informationen finden Sie im Abschnitt *Sicherungs- und Wiederherstellungsprozesse* im Thema *Festplattenspeicheranforderungen* (Linux).

Verzeichnisaufbau

DIn der Referenzarchitektur wird empfohlen, das Tableau Server-Paket und die Daten an nicht standardmäßigen Speicherorten zu installieren:

- Installieren Sie das Paket in: `/app/tableau_server`: Erstellen Sie diesen Verzeichnispfad, bevor Sie das Tableau Server-Paket installieren, und geben Sie diesen Pfad dann während der Installation an.
- Installieren Sie Tableau-Daten in: `/data/tableau_data`. Erstellen Sie dieses Verzeichnis erst, nachdem Sie Tableau Server installiert haben. Stattdessen müssen Sie den Pfad während der Installation angeben, und dann erstellt das Installationsprogramm von Tableau den Pfad und gibt ihn entsprechend frei.

Einzelheiten zur Implementierung finden Sie unter Ausführen des Installationspakets und Initialisieren von TSM.

Beispiel: Installieren und Vorbereiten von Hostcomputern in AWS

In diesem Abschnitt wird erläutert, wie Sie EC2-Hosts für jeden Servertyp in der Tableau Server-Referenzarchitektur installieren.

Die Referenzarchitektur erfordert acht Hosts:

- Vier Instanzen für Tableau Server
- Zwei Instanzen für Proxyserver (Apache)
- Eine Instanz für Bastion-Host
- Eine oder zwei EC2-PostgreSQL-Datenbankinstanzen

Details zur Hostinstanz

Installieren Sie die Hostcomputer gemäß den folgenden Angaben.

Tableau Server

- Amazon Linux 2
- Instanztyp: m5a.8xlarge
- Sicherheitsgruppen-ID: Privat
- Speicher: EBS, 150 GiB, gp2-Volume-Typ Wenn Ihre Bereitstellung externen Speicher für den Tableau-Dateispeicher verwenden soll, müssen Sie den entsprechenden Speicherplatz berechnen. Informationen dazu finden Sie unter *Installieren von Tableau Server mit dem externen Dateispeicher* (Linux).
- Netzwerk: Installieren Sie zwei EC2-Hosts in jedem privaten Subnetz (10.0.30.0/24 und 10.0.31.0/24).
- Kopieren Sie die neueste Wartungsversion von Tableau Server 2021.2 (oder höher) als rpm-Paket von der Tableau-Downloadseite auf jeden Tableau-Host.

Bastion-Host

- Amazon Linux 2
- Instanztyp: t3.micro
- Sicherheitsgruppen-ID: Bastion
- Speicher: EBS, 50 GiB, gp2-Volume-Typ
- Netzwerk: Bastion-Subnetz 10.0.0.0/24

Tableau Server Independent Gateway

- Amazon Linux 2
- Instanztyp: t3.xlarge
- Sicherheitsgruppen-ID: Öffentlich
- Speicher: EBS, 100 GiB, gp2-Volume-Typ
- Netzwerk: Installieren Sie eine EC2-Instanz in jedem öffentlichen Subnetz (10.0.1.0/24 und 10.0.2.0/24)

PostgreSQL-EC2-Host

- Amazon Linux 2
- Instanztyp: r5.4xlarge
- Sicherheitsgruppen-ID: Daten
- Speicher: Der Bedarf an Festplattenplatz hängt von Ihrer Datenlast und deren Auswirkungen auf Sicherungen ab. Weitere Informationen finden Sie im Abschnitt *Sicherungs- und Wiederherstellungsprozesse* im Thema *Festplattenspeicheranforderungen* (Linux).
- Netzwerk: Daten-Subnetz 10.0.50.0/24 (Wenn Sie PostgreSQL in einem Hochverfügbarkeits-Cluster replizieren, installieren Sie den zweiten Host im 10.0.51.0/24-Subnetz)

Überprüfung: VPC-Konnektivität

Überprüfen Sie nach der Installation der Hostcomputer die Netzwerkkonfiguration. Überprüfen Sie die Konnektivität zwischen den Hosts, indem Sie von dem Host in der Bastion-Sicherheitsgruppe eine SSH-Verbindung zu den Hosts in jedem Subnetz herstellen.

Beispiel: Herstellen einer Verbindung mit dem Bastion-Host in AWS

1. Richten Sie Ihren Administrationscomputer für ssh-agent ein. Auf diese Weise können Sie eine Verbindung zu Hosts in AWS herstellen, ohne Ihre private Schlüsseldatei auf EC2-Instanzen abzulegen.

   Führen Sie den folgenden Befehl aus, um ssh-agent auf einem Mac zu konfigurieren:

   `ssh-add -K myPrivateKey.pem` oder für das neueste macOS: `ssh-add --apple-use-keychain myPrivateKey.pem`

   Informationen zu Windows finden Sie im Thema Securely Connect to Linux Instances Running in a Private Amazon VPC (Sicheres Herstellen einer Verbindung zu Linux-Instanzen, die in einer Amazon-VPC ausgeführt werden).

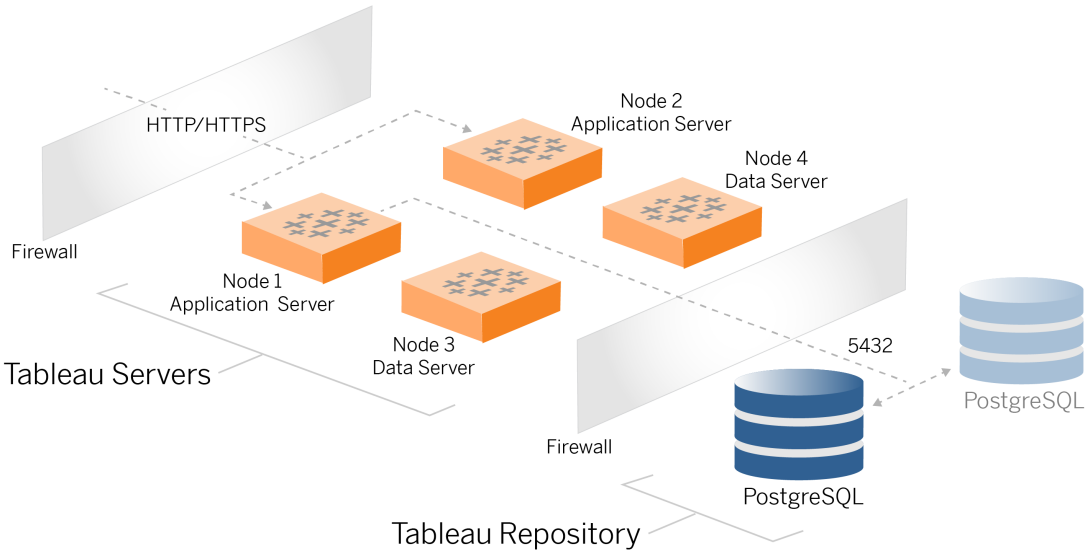
2. Stellen Sie eine Verbindung mit dem Bastion-Host her, indem Sie den folgenden Befehl ausführen:

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

3. Anschließend können Sie von dem Bastion-Host aus eine Verbindung mit anderen Hosts in der VPC herstellen, indem Sie die private IP-Adresse verwenden. Zum Beispiel:

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

Teil 4 - Installieren und Konfigurieren von Tableau Server



Dieses Thema beschreibt, wie Sie die Installation und Konfiguration der grundlegenden Tableau Server-Bereitstellung abschließen. Das Verfahren wird hier mit dem Beispiel der AWS- und Linux-Referenzarchitektur fortgesetzt.

Die Linux-Beispiele in sämtlichen Installationsverfahren zeigen Befehle für RHEL-ähnliche Distributionen. Die hier angegebenen spezifischen Befehle wurden mit der Amazon Linux 2-Distribution entwickelt. Wenn Sie die Ubuntu-Distribution ausführen, bearbeiten Sie die Befehle entsprechend.

Voraussetzungen

Sie müssen Ihre Umgebung wie in Teil 3 - Vorbereiten der Bereitstellung von Tableau Server Enterprise beschrieben vorbereiten und überprüfen.

Installieren, Konfigurieren und Anfertigen einer tar-Sicherung von PostgreSQL

Diese PostgreSQL-Instanz hostet das externe Repository für die Tableau Server-Bereitstellung. Sie müssen PostgreSQL installieren und konfigurieren, bevor Sie Tableau installieren.

Sie können PostgreSQL auf Amazon RDS oder auf einer EC2-Instanz ausführen. Weitere Informationen zu den Unterschieden zwischen der Ausführung des Repositorys auf RDS oder auf einer EC2-Instanz finden Sie unter *Externes Tableau Server-Repository* (Linux).

Im Folgenden wird beispielhaft gezeigt, wie Postgres auf einer Amazon EC2-Instanz installiert und konfiguriert wird. Das hier gezeigte Beispiel ist eine generische Installation und Konfiguration für PostgreSQL in der Referenzarchitektur. Ihr DBA sollte die Bereitstellung von PostgreSQL auf der Grundlage der Größe Ihrer Daten und der Leistungsanforderungen optimieren.

Voraussetzungen: Beachten Sie, dass Sie PostgreSQL 1.6 verwenden und das Modul "uuid-ossp" installieren müssen.

PostgreSQL-Versionskontrolle

Sie müssen kompatible Hauptversionen von PostgreSQL für das externe Repository von Tableau Server installieren.. Darüber hinaus müssen auch die Nebenversionen Mindestanforderungen erfüllen.

Tableau Server-Versionen	**Mindestens kompatible PostgreSQL-Versionen**
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	12.8

2021.3.8 – 2021.3.13 2021.4.4 – 2021.4.8	
2021.2.15 – 2021.2.16 2021.3.14 – 2021.3.15 2021.4.9 – 2021.4.10	12.10
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	13.14

2023.1.16 – 2023.1.x 2023.3.9 – 2023.3.x	
2024.0 – 2024.x	15.6

Installieren von PostgreSQL

Das Installationsverfahren in diesem Beispiel beschreibt die Installation von PostgreSQL, Version 13.6.

Melden Sie sich bei dem EC2-Host an, den Sie im vorherigen Teil erstellt haben.

1. Führen Sie das Update aus, um die neuesten Fixes für das Linux-Betriebssystem anzuwenden:

   ```
   sudo yum update
   ```

2. Erstellen und bearbeiten Sie die Datei "pgdg.repo" im Pfad `/etc/yum.repos.d/`. Fügen Sie folgende Konfigurationsinformationen in die Datei ein:

   ```
   [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. Installieren Sie PostgreSQL 13.6:

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

4. Installieren Sie das uuid-ossp-Modul:

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

5. Initialisieren Sie Postgres:

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

Konfigurieren von Postgres

Schließen Sie die Basisinstallation ab, indem Sie Postgres konfigurieren:

1. Aktualisieren Sie die pg_hba-Konfigurationsdatei (`/var/lib/pgsql/13/data/pg_hba.conf`) mit den folgenden beiden Einträgen. Jeder Eintrag muss die Maske der Subnetze enthalten, in denen Ihre Tableau Server ausgeführt werden:

   ```
   host all all 10.0.30.0/24 password

   host all all 10.0.31.0/24 password
   ```

2. Aktualisieren Sie die PostgreSQL-Datei `/var/-lib/pgsql/13/data/postgresql.conf`, indem Sie diese Zeile hinzufügen:

   ```
   listen_addresses = '*'
   ```

3. Konfigurieren Sie Postgres für den Start beim Neustart:

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

4. Legen Sie das Superuser-Kennwort fest:

   ```
   sudo su - postgres

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

   Hinweis: Legen Sie ein sicheres Kennwort fest. Verwenden Sie nicht `'StrongPassword'`, wie im Beispiel hier gezeigt.

   ```
   exit
   ```

5. Starten Sie Postgres neu:

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

Anfertigen einer "Schritt 1"-tar-Sicherung von PostgreSQL

Erstellen Sie eine tar-Sicherung der PostgreSQL-Konfiguration. Das Erstellen eines tar-Snapshots der aktuellen Konfiguration kann Zeit sparen, wenn beim Fortsetzen der Bereitstellung Fehler auftreten.

Wir bezeichnen dies als "Schritt 1"-Sicherung.

Auf dem PostgreSQL-Host:

1. Stoppen Sie die Postgres-Datenbankinstanz:

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

2. Führen Sie die folgenden Befehle zum Erstellen der tar-Sicherung aus:

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

3. Starten Sie die Postgres-Datenbank:

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

Wiederherstellen von Schritt 1

Sollte auf dem anfänglichen Knoten von Tableau Server während der Installation ein Fehler auftreten, stellen Sie die Sicherung von Schritt 1 wieder her.

1. Führen Sie auf dem Computer, auf dem Tableau ausgeführt wird, das Lösch-Skript aus, um Tableau Server vollständig vom Host zu entfernen:

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

2. Stellen Sie den Zustand von PostgreSQL-Schritt 1 aus dem tar-Backup wieder her. Führen Sie auf dem Computer, auf dem Postgres ausgeführt wird, die folgenden Befehle aus:

   ```
   sudo su

   systemctl stop postgresql-13

   cd /var/lib/pgsql

   tar  -xvf step1.13.bkp.tar

   systemctl start postgresql-13

   exit
   ```

Setzen Sie den Installationsvorgang mit dem Installieren des Anfangsknotens von Tableau Server fort.

Vor der Installation

Wenn Sie Tableau gemäß der in diesem Leitfaden beschriebenen AWS/Linux-Implementierung bereitstellen, können Sie möglicherweise das automatische Installationsskript "TabDeploy4EDG" ausführen. Das Skript "TabDeploy4EDG" automatisiert die Beispielinstallation der Tableau-Bereitstellung mit vier Knoten, die in den folgenden Verfahren beschrieben wird. Siehe Anhang – AWS Deployment Toolbox.

Installieren des ursprünglichen Knotens auf Tableau Server

In diesem Verfahren wird beschrieben, wie Sie den Ausgangsknoten von Tableau Server wie von der Referenzarchitektur definiert installieren. Mit Ausnahme der Paketinstallation und der Initialisierung von TSM verwendet das Verfahren hier nach Möglichkeit die TSM-Befehlszeile. Die Verwendung der TSM-Befehlszeile ist nicht nur plattformunabhängig, sondern ermöglicht auch eine nahtlose Installation in virtualisierten und Headless-Umgebungen.

Ausführen des Installationspakets und Initialisieren von TSM

Melden Sie sich beim Knoten-1-Hostserver an.

1. Führen Sie das Update aus, um die neuesten Fixes für das Linux-Betriebssystem anzuwenden:

   ```
   sudo yum update
   ```

2. Kopieren Sie das Installationspaket von der Tableau-Downloadseite auf den Hostcomputer, auf dem Tableau Server ausgeführt werden soll.

   Auf einem Linux-RHEL-ähnlichen Betriebssystem beispielsweise führen Sie den folgenden Befehl aus:

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

   wobei `<version>` die Versionsnummer ist.

3. Laden Sie Abhängigkeiten herunter und installieren Sie diese:

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

4. Erstellen Sie im Root-Verzeichnis den Pfad `/app/tableau_server`:

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

5. Führen Sie das Installationsprogramm aus und geben Sie den Installationspfad `/app/tableau_server` an. Auf einem Linux-RHEL-ähnlichen Betriebssystem beispielsweise führen Sie den folgenden Befehl aus:

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

6. Wechseln Sie in das Verzeichnis `/app/tableau_server/packages/scripts.<version_code>/` und führen Sie das Skript `initialize-tsm` aus, das sich dort befindet:

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

7. Beenden Sie nach Abschluss der Initialisierung die Shell:

   ```
   exit
   ```

Aktivieren und Registrieren von Tableau Server

1. Melden Sie sich beim Knoten-1-Hostserver an.

2. Geben Sie in diesem Schritt den bzw. die Tableau Server-Produktschlüssel an. Führen Sie den folgenden Befehl für jeden Lizenzschlüssel aus, den Sie erworben haben:

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

3. Erstellen Sie eine json-Registrierungsdatei mit dem hier gezeigten Format:

   ```
   {
   "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. Nachdem Sie die Änderungen gespeichert haben, übermitteln Sie die Datei mit der Option `--file`, um Tableau Server zu registrieren:

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

Konfigurieren des Identitätsspeichers

> **Hinweis**: Wenn Ihre Bereitstellung einen externen Speicher für den Tableau-Dateispeicher verwendet, müssen Sie den externen Dateispeicher aktivieren, bevor Sie den Identitätsspeicher konfigurieren. Informationen dazu finden Sie unter *Installieren von Tableau Server mit dem externen Dateispeicher* (Linux).

Die Standardreferenzarchitektur verwendet einen lokalen Identitätsspeicher. Konfigurieren Sie den Ausgangshost mit lokalem Identitätsspeicher, indem Sie die `config.json`-Datei mit dem Befehl `tsm settings import` übergeben.

Importieren Sie die Datei `config.json` entsprechend Ihrem Betriebssystem:

Die Datei `config.json` befindet sich in dem Verzeichnispfad "scripts.<version>" (z. B. `scripts.20204.21.0217.1203`) und ist zum Konfigurieren des Identitätsspeichers formatiert.

Führen Sie den folgenden Befehl aus, um die `config.json`-Datei zu importieren:

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

Konfigurieren von externem Postgres

1. Erstellen Sie eine JSON-Datei für eine externe Datenbank mit den folgenden Konfigurationseinstellungen:

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

2. Nachdem Sie die Änderungen gespeichert haben, übergeben Sie die Datei mit dem folgenden Befehl:

   ```
   tsm topology external-services repository enable -f <filen-
   ame>.json --no-ssl
   ```

   Sie werden aufgefordert, das Kennwort für den primären Postgres-Benutzernamen einzugeben.

   Mit der Option `--no-ssl` wird Tableau so konfiguriert, dass SSL/TLS nur verwendet werden soll, wenn der Postgres-Server für SSL/TLS konfiguriert ist. Wenn Postgres nicht für SSL/TLS konfiguriert ist, wird die Verbindung nicht verschlüsselt. Teil 6 – Konfiguration nach der Installation beschreibt, wie Sie SSL/TLS für die Postgres-Verbindung aktivieren, nachdem Sie die erste Phase der Bereitstellung abgeschlossen haben.

3. Wenden Sie die Änderungen an.

Führen Sie den folgenden Befehl aus, um die Änderungen zu übernehmen, und starten Sie Tableau Server neu:

```
tsm pending-changes apply
```

4. Löschen Sie die Konfigurationsdatei, die Sie in Schritt 1 verwendet haben.

Fertigstellen der Installation von Knoten 1

1. Nachdem Tableau Server installiert wurde, müssen Sie den Server initialisieren.

   Führen Sie den folgenden Befehl aus:

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

2. Nach Abschluss der Initialisierung müssen Sie ein Tableau Server-Administratorkonto erstellen.

   Im Gegensatz zu dem Computerkonto, das Sie zum Installieren und Verwalten von TSM-Betriebssystemkomponenten verwenden, ist das Tableau Server-Administratorkonto ein Anwendungskonto, das zum Erstellen von Tableau Server-Benutzern, -Projekten und -Sites dient. Der Tableau Server-Administrator wendet auch Berechtigungen auf Tableau-Ressourcen an. Führen Sie den folgenden Befehl zum Erstellen des ersten Administratorkontos aus: Im folgenden Beispiel heißt der Benutzer `tableau-admin`:

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

   Tabcmd fordert Sie auf, ein Kennwort für diesen Benutzer festzulegen.

Überprüfung: Konfiguration von Knoten 1

1. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die TSM-Dienste ausgeführt werden:

   ```
   tsm status -v
   ```

Tableau sollte Folgendes zurückgeben:

```
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 Dienste werden aufgelistet.

2. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die Administrator-Site von Tableau ausgeführt wird:

```
curl localhost
```

In den ersten Zeilen sollte VizPortal-HTML angezeigt werden, ähnlich wie hier:

```
<!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 ...
```

Anfertigen von tar-Sicherungen von Schritt 2

Nachdem Sie die Ausgangsinstallation überprüft haben, fertigen Sie zwei Tar-Sicherungen an:

- PostgreSQL
- Tableau-Ausgangsknoten (Knoten 1)

In den meisten Fällen können Sie Ihre Installation des Ausgangsknotens wiederherstellen, indem Sie diese tar-Dateien wiederherstellen. Das Wiederherstellen der tar-Dateien ist viel schneller als die Neuinstallation und Neuinitialisierung des Ausgangsknotens.

Erstellen von tar-Dateien für Schritt 2

1. Stoppen Sie Tableau auf dem Ausgangsknoten von Tableau:

   ```
   tsm stop
   ```

   Warten Sie, bis Tableau beendet wurde, bevor Sie mit dem nächsten Schritt fortfahren.

2. Stoppen Sie die Postgres-Datenbankinstanz auf dem PostgreSQL-Host:

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

3. Führen Sie die folgenden Befehle zum Erstellen der tar-Sicherung aus:

   ```
   sudo su
   cd /var/lib/pgsql
   tar -cvf step2.13.bkp.tar 13
   exit
   ```

4. Stellen Sie sicher, dass die Postgres-tar-Datei mit Root-Berechtigungen erstellt wurde:

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

5. Stoppen Sie die Tableau-Verwaltungsdienste auf dem Tableau-Host:

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

6. Führen Sie die folgenden Befehle zum Erstellen der tar-Sicherung aus:

   ```
   cd /data
   ```

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

7. Starten Sie die Postgres-Datenbank auf dem Postgres-Host:

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

8. Starten Sie Tableau-Verwaltungsdienste:

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

9. Führen Sie den Befehl `tsm status` zum Überwachen des TSM-Status vor dem Neustart aus.

   In den meisten Fällen gibt der Befehl zuerst den Status DEGRADED oder ERROR zurück. Warten Sie ein paar Minuten und führen Sie den Befehl erneut aus. Wenn immer noch ein ERROR- oder DEGRADED-Status zurückgegeben wird, warten Sie weiter. Versuchen Sie nicht, TSM zu starten, bis der Status STOPPED zurückgegeben wird. Führen Sie dann den folgenden Befehl aus:

   ```
   tsm start
   ```

Wiederherstellen von Schritt 2

Mit diesem Verfahren werden der Tableau-Knoten 1 und die Postgres-Instanz auf dem Stand von Schritt 2 wieder hergestellt. Nachdem Sie diesen Schritt wiederhergestellt haben, können Sie die verbleibenden Tableau-Knoten erneut bereitstellen.

1. Stoppen Sie die tsm-Dienste auf dem Tableau-Ausgangshost (Knoten 1):

   ```
   tsm stop
   ```

2. Stoppen Sie die Tableau-Verwaltungsdienste auf allen Knoten der Tableau Server-Bereitstellung. Führen Sie den folgenden Befehl auf jedem Knoten in der folgenden Reihenfolge aus: Knoten 1, Knoten 2 und dann Knoten 3:

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

3. Nachdem die Tableau-Dienste gestoppt wurden, stellen Sie die tar-Sicherung von PostgreSQL/Schritt 2 wieder her. Führen Sie auf dem Computer, auf dem Postgres ausgeführt wird, die folgenden Befehle aus:

   - ```
     sudo su

     systemctl stop postgresql-13

     cd /var/lib/pgsql

     tar  -xvf step2.13.bkp.tar

     systemctl start postgresql-13

     exit
     ```

4. Stellen Sie die tar-Sicherung von Tableau/Schritt 2 wieder her. Führen Sie auf dem Tableau-Ausgangshost die folgenden Befehle aus:

   ```
   cd /data

   sudo rm -rf tableau_data

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

5. Entfernen Sie auf dem Computer, der als Tableau-Knoten 1 dient, die folgenden Dateien:
   ```

- `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. Starten Sie die Tableau-Verwaltungsdienste:

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

7. Laden Sie die systmctl-Dateien von Tableau neu und führen Sie dann `start-administrative-services` erneut aus:

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

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

8. Führen Sie auf dem Knoten 1 den Befehl `tsm status` zum Überwachen des TSM-Status vor dem Neustart aus.

   In einigen Fällen erhalten Sie die Fehlermeldung `Cannot connect to server...` (Verbindung zum Server kann nicht hergestellt werden...). Dieser Fehler tritt auf, weil der Dienst "tabadmincontroller" nicht neu gestartet wurde. Führen Sie weiterhin `tsm status` in regelmäßigen Abständen aus. Wenn dieser Fehler nach 10 Minuten nicht verschwindet, führen Sie noch einmal den Befehl `start-administrative-services` aus.

   Nach einigen Augenblicken wird der Befehl `tsm status` den Status DEGRADED und dann ERROR zurückgeben. Starten Sie TSM erst, wenn der Status STOPPED zurückgegeben wird. Führen Sie dann den folgenden Befehl aus:

   ```
   tsm start
   ```

Setzen Sie den Installationsvorgang mit dem Installieren von Tableau Server auf den verbleibenden Knoten fort.

Installieren von Tableau Server auf weiteren Knoten

Um die Bereitstellung fortzusetzen, kopieren Sie das Tableau-Installationsprogramm auf jeden Knoten.

Übersicht über die Knoten-Konfiguration

In diesem Abschnitt wird der Vorgang zum Konfigurieren der Knoten 2-4 beschrieben. Die folgenden Abschnitte enthalten detaillierte Konfigurations- und Überprüfungsverfahren für jeden Schritt.

Für die Installation der Tableau Server-Knoten 2 bis 4 müssen Sie während der Knoteninstallation eine Bootstrap-Datei generieren, kopieren und darauf verweisen.

Zum Generieren der Bootstrap-Datei führen Sie einen TSM-Befehl auf dem Anfangsknoten aus. Anschließend kopieren Sie die Bootstrap-Datei auf den Zielknoten, wo Sie sie im Rahmen der Knoteninitialisierung ausführen.

Der folgende JSON-Inhalt zeigt ein Beispiel für eine bootstrap-Datei. (Die zertifikat- und kryptobezogenen Werte wurden abgeschnitten, damit das Beispiel nicht zu unübersichtlich wird.)

```
{
"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" : "eyJjdHkiOiJKV1QiLCJlb-
mMiOiJBMTI4Q0JDLUhQ...",
        "sessionCookieName" : "AUTH_COOKIE"
        }
}
```

Die Bootstrap-Datei enthält eine verbindungsbasierte Überprüfung zur Authentifizierung von Knoten 1 und erstellt einen verschlüsselten Kanal für den Bootstrap-Vorgang. Die Bootstrap-Sitzung ist zeitlich begrenzt und das Konfigurieren und Überprüfen von Knoten zeitaufwändig. Planen Sie das Erstellen und Kopieren neuer Bootstraps, während Sie die Knoten konfigurieren.

Nachdem Sie die Bootstrap-Datei ausgeführt haben, melden Sie sich beim ersten Tableau Server-Knoten an und konfigurieren die Vorgänge für den neuen Knoten. Wenn Sie die Konfiguration der Knoten abgeschlossen haben, müssen Sie die Änderungen übernehmen und den ursprünglichen Knoten neu starten. Der neue Knoten wird konfiguriert und gestartet. Beim Hinzufügen von Knoten dauert die Konfiguration und der Neustart der Bereitstellung nacheinander länger.

Die Linux-Beispiele in sämtlichen Installationsverfahren zeigen Befehle für RHEL-ähnliche Distributionen. Wenn Sie die Ubuntu-Distribution ausführen, bearbeiten Sie die Befehle entsprechend.

1. Führen Sie das Update aus, um die neuesten Fixes für das Linux-Betriebssystem anzuwenden:

   ```
   sudo yum update
   ```

2. Laden Sie Abhängigkeiten herunter und installieren Sie diese:

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

3. Erstellen Sie im Root-Verzeichnis den Pfad `/app/tableau_server`:

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

4. Führen Sie das Installationsprogramm aus und geben Sie den Installationspfad `/app/tableau_server` an. Auf einem Linux-RHEL-ähnlichen Betriebssystem beispielsweise führen Sie den folgenden Befehl aus:

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

Generieren, Kopieren und Verwenden der Bootstrap-Datei zum Initialisieren von TSM

Das folgende Verfahren zeigt, wie eine Bootstrap-Datei generiert, kopiert und zum Initialisieren von TSM auf einem anderen Knoten verwendet wird. In diesem Beispiel wird die Bootstrap-Datei `boot.json` benannt.

In diesem Beispiel werden die Hostcomputer in AWS ausgeführt, wobei auf EC2-Hosts Amazon Linux 2 läuft.

1. Stellen Sie eine Verbindung zum Ausgangsknoten (Knoten 1) her und führen Sie den folgenden Befehl aus:

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

2. Kopieren Sie die Bootstrap-Datei auf Knoten 2.

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

3. Stellen Sie eine Verbindung zu Knoten 2 her und wechseln Sie zum Skriptverzeichnis des Tableau Server:

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

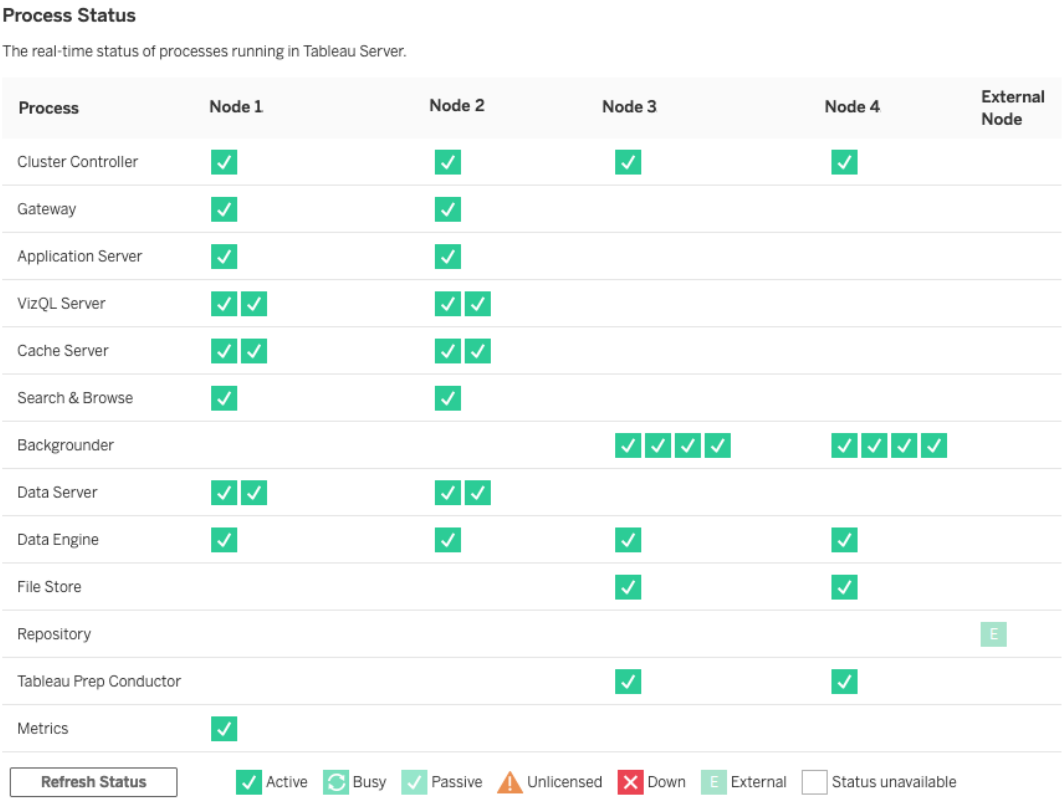
4. Führen Sie den Befehl `initialize-tsm` aus und verweisen Sie auf die Bootstrap-Datei:

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

5. Löschen Sie nach Abschluss von `initialize-tsm` die Datei `boot.json` und beenden Sie dann die Sitzung oder melden Sie sich ab.

Prozesse konfigurieren

Sie müssen den Tableau Server-Cluster auf dem Knoten konfigurieren, auf dem der Tableau Server Administration Controller (TSM-Controller) ausgeführt wird. Der TSM-Controller wird auf dem ursprünglichen Knoten ausgeführt.



Konfigurieren von Knoten 2

1. Nachdem Sie TSM mithilfe der Bootstrap-Datei auf dem Knoten 2 initialisiert haben, melden Sie sich beim Ausgangsknoten an.

2. Stellen Sie eine Verbindung zum Ausgangsknoten (`node1`) her und führen Sie die folgenden Befehle aus, um Prozesse auf Knoten 2 zu konfigurieren:

```
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
```

Wenn Sie die Version 2022.1 oder höher installieren, fügen Sie auch den Indizierungs- und Suchdienst hinzu:

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

Wenn Sie die Version 2023.3 oder höher installieren, schließen Sie nur den Indizierungs- und Suchdienst ein. Fügen Sie den Dienst „Suchen und Durchsuchen“ (searchserver) nicht hinzu

3. Überprüfen Sie die Konfiguration, bevor Sie sie anwenden. Führen Sie den folgenden Befehl aus:

   ```
   tsm pending-changes list
   ```

4. Nachdem Sie überprüft haben, dass sich Ihre Änderungen in der ausstehenden Liste befinden (dort werden auch andere Dienste aufgeführt sein), übernehmen Sie die Änderungen:

   ```
   tsm pending-changes apply
   ```

   Die Änderungen erfordern einen Neustart. Die Konfiguration und der Neustart nehmen einige Zeit in Anspruch.

5. Überprüfen Sie die Konfiguration von Knoten 2. Führen Sie den folgenden Befehl aus:

   ```
   tsm status -v
   ```

Konfigurieren von Knoten 3

Initialisieren Sie TSM mithilfe der Bootstrap-Methode auf dem Knoten 3 und führen Sie dann die unten aufgeführten `tsm topology set-process`-Befehle aus.

Eine Warnung des Koordinierungsdienstes wird jedes Mal angezeigt, wenn Sie einen Vorgang festlegen. Sie können diese Warnung ignorieren, wenn Sie die Vorgänge festlegen.

1. Nachdem Sie TSM mithilfe der Bootstrap-Datei auf dem Knoten 3 initialisiert haben, melden Sie sich bei dem Ausgangsknoten (`node1`) an und führen Sie die folgenden Befehle aus, um Prozesse zu konfigurieren:

   ```
   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
   ```

   Wenn Sie die Version 2022.1 oder höher installieren, fügen Sie auch den Indizierungs- und Suchdienst hinzu:

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

2. Überprüfen Sie die Konfiguration, bevor Sie sie anwenden. Führen Sie den folgenden Befehl aus:

   ```
   tsm pending-changes list
   ```

3. Nachdem Sie überprüft haben, dass sich Ihre Änderungen in der ausstehenden Liste befinden (die auch andere Dienste enthält, die automatisch konfiguriert werden), übernehmen Sie die Änderungen:

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

   Die Änderungen erfordern einen Neustart. Die Konfiguration und der Neustart nehmen einige Zeit in Anspruch.

4. Führen Sie die Konfiguration, indem Sie den folgenden Befehl ausführen:

   ```
   tsm status -v
   ```

Bereitstellen des Koordinationsdienstensembles auf den Knoten 1-3

Für eine Standardreferenzarchitektur mit vier Knoten führen Sie das folgende Verfahren aus:

1. Führen Sie die folgenden Befehle auf Knoten 1 aus:

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

   Dieser Vorgang beinhaltet auch einen Neustart von TSM, der einige Zeit in Anspruch nehmen wird.

2. Nachdem der Koordinationsdienst bereitgestellt wurde, starten Sie TSM:

   ```
   tsm start
   ```

Anfertigen von tar-Sicherungen von Schritt 3

Nachdem Sie die Installation überprüft haben, erstellen Sie vier Tar-Sicherungen:

- PostgreSQL
- Tableau-Ausgangsknoten (Knoten 1)
- Tableau-Knoten 2
- Tableau-Knoten 3

Erstellen von Schritt 3-tar-Dateien

1. Stoppen Sie Tableau auf dem Ausgangsknoten von Tableau:

   ```
   tsm stop
   ```

2. Nachdem TSM gestoppt wurde, stoppen Sie die Tableau-Verwaltungsdienste auf jedem Knoten. Führen Sie den folgenden Befehl auf jedem Knoten in der folgenden Reihenfolge aus: Knoten 1, Knoten 2 und dann Knoten 3:

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

3. Stoppen Sie die Postgres-Datenbankinstanz auf dem PostgreSQL-Host:

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

4. Führen Sie die folgenden Befehle zum Erstellen der tar-Sicherung aus:

   ```
   sudo su
   cd /var/lib/pgsql
   tar -cvf step3.12.bkp.tar 12
   exit
   ```

5. Vergewissern Sie sich, dass die Postgres-tar-Datei mit Root-Berechtigungen erstellt wird:

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

6. Starten Sie die Postgres-Datenbank auf dem Postgres-Host:

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

7. Erstellen Sie die tar-Sicherung auf Knoten 1, Knoten 2 und Knoten 3. Führen Sie auf jedem Knoten die folgenden Befehle aus:

   - ```
     cd /data
     sudo tar -cvf step3.tableau_data.bkp.tar tableau_data
     ```
     ```

- Stellen Sie sicher, dass die Tableau-tar-Datei mit Root-Berechtigungen erstellt wurde:

  ```
  ls -al
  ```

8. Starten Sie die Tableau-Verwaltungsdienste auf jedem Knoten der Reihe nach (Knoten 1, Knoten 2 und dann Knoten 3):

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

9. Führen Sie den Befehl `tsm status` zum Überwachen des TSM-Status vor dem Neustart aus.

   In den meisten Fällen gibt der Befehl den Status DEGRADED und dann ERROR zurück. Warten Sie einen Moment und führen Sie den Befehl erneut aus. Wenn immer noch ein ERROR- oder DEGRADED-Status zurückgegeben wird, warten Sie weiter. Versuchen Sie nicht, TSM zu starten, bis der Status STOPPED zurückgegeben wird. Führen Sie dann den folgenden Befehl aus:

   ```
   tsm start
   ```

Wiederherstellen von Schritt 3

Dieses Verfahren stellt die Tableau-Knoten 1, -Knoten 2 und -Knoten 3 wieder her. Es stellt auch die Postgres-Instanz auf Schritt 3 wieder her. Nachdem Sie diesen Schritt wiederhergestellt haben, können Sie den Koordinationsdienst, Knoten 4 und dann die endgültigen Knotenkonfigurationen bereitstellen.

1. Stoppen Sie den tsm-Dienst auf dem Tableau-Ausgangshost (Knoten 1):

   ```
   tsm stop
   ```

2. Nachdem TSM gestoppt wurde, stoppen Sie die Tableau-Verwaltungsdienste auf Knoten 1, Knoten 2 und Knoten 3. Führen Sie auf jedem Knoten den folgenden Befehl aus:

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

3. Stellen Sie die tar-Sicherung von PostgreSQL/Schritt 3 wieder her. Führen Sie auf dem Computer, auf dem Postgres ausgeführt wird, die folgenden Befehle aus:

   ```
   sudo su

   systemctl stop postgresql-12

   cd /var/lib/pgsql

   tar -xvf step3.12.bkp.tar

   systemctl start postgresql-12

   exit
   ```

4. Stellen Sie die tar-Sicherung von Tableau/Schritt 3 auf Knoten 1, Knoten 2 und Knoten 3 wieder her. Führen Sie auf jedem Tableau-Knoten die folgenden Befehle aus:

   ```
   cd /data

   sudo rm -rf tableau_data

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

5. Entfernen Sie auf dem Computer, der als Tableau-Knoten 1 dient, die folgenden Dateien:

   - `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`

Wenn die Shell den Fehler "file not found" (Datei nicht gefunden) zurück gibt, müssen Sie möglicherweise den Pfadnamen so ändern, dass sich die Zahl `<n>` im Pfadabschnitt `.../appzookeeper/<n>/version-2/...` um Eins erhöht.

6. Starten Sie die Verwaltungsdienste auf Knoten 1, Knoten 2 und Knoten 3 neu. Führen Sie auf jedem Knoten die folgenden Befehle aus:

```
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. Führen Sie auf dem Knoten 1 den Befehl `tsm status` zum Überwachen des TSM-Status vor dem Neustart aus.

   In einigen Fällen erhalten Sie die Fehlermeldung `Cannot connect to server...` (Verbindung zum Server kann nicht hergestellt werden...). Dieser Fehler tritt auf, weil der Dienst "tabadmincontroller" nicht neu gestartet wurde. Führen Sie weiterhin `tsm status` in regelmäßigen Abständen aus. Wenn dieser Fehler nach 10 Minuten nicht verschwindet, führen Sie noch einmal den Befehl `start-administrative-services` aus.

   Nach einigen Augenblicken wird der Befehl `tsm status` den Status DEGRADED und dann ERROR zurückgeben. Starten Sie TSM erst, wenn der Status STOPPED zurückgegeben wird. Führen Sie dann den folgenden Befehl aus:

```
tsm start
```

Setzen Sie den Installationsprozess mit dem Bereitstellen des Koordinierungsdienstes auf den Knoten 1-3 fort.

Konfigurieren von Knoten 4

Der Vorgang zum Konfigurieren von Knoten 4 ist derselbe wie bei Knoten 3.

Legen Sie dieselben Prozesse fest, die Sie für Knoten 3 festgelegt haben, und führen Sie dieselben Befehle wie oben aus, geben Sie jedoch `node4` in den Befehlen statt `node3` ein.

Überprüfen Sie die Konfiguration von Knoten 4 wie schon bei der Verifizierung von Knoten 3, indem Sie den Befehl `tsm status -v` ausführen.

Bevor Sie den Vorgang fortsetzen, müssen Sie warten, bis der Dateispeicherprozess auf Knoten 4 die Synchronisierung abgeschlossen hat. Der Status des Dateispeicherdienstes wird als `is synchronizing` zurückgegeben, bis der Vorgang abgeschlossen ist. Wenn der Status des Dateispeicherdienstes als `is running` zurückgegeben wird, können Sie den Vorgang fortsetzen.

Endgültige Prozesskonfiguration und Verifizierung

Der letzte Schritt zur Prozesskonfiguration besteht darin, redundante Prozesse aus Knoten 1 zu entfernen.

1. Stellen Sie eine Verbindung zum ursprünglichen Knoten her (`node1`).
2. Legen Sie den Dateispeicher auf Knoten 1 still. Dadurch wird eine Warnung verursacht, die besagt, dass der Dateispeicher von einem am gleichen Speicherort befindlichen Controller entfernt wird. Sie können diese Warnung ignorieren. Führen Sie den folgenden Befehl aus:

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

3. Wenn der Dateispeicher stillgelegt ist, führen Sie den folgenden Befehl aus, um den Hintergrundprozess von Knoten 1 zu entfernen:

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

4. Überprüfen Sie die Konfiguration, bevor Sie sie anwenden. Führen Sie den folgenden Befehl aus:

   ```
   tsm pending-changes list
   ```

5. Nachdem Sie überprüft haben, dass Ihre Änderungen in der Liste der ausstehenden Änderungen enthalten sind, wenden Sie die Änderungen an:

   ```
   tsm pending-changes apply
   ```

   Die Änderungen erfordern einen Neustart. Die Konfiguration und der Neustart nehmen einige Zeit in Anspruch.

6. Überprüfen Sie die Konfiguration:

   ```
   tsm status -v.
   ```

   Bevor Sie den Vorgang fortsetzen, müssen Sie warten, bis der Dateispeicherprozess auf Knoten 4 die Synchronisierung abgeschlossen hat. Der Status des Dateispeicherdienstes wird als `is synchronizing` zurückgegeben, bis der Vorgang abgeschlossen ist. Wenn der Status des Dateispeicherdienstes als `is running` zurückgegeben wird, können Sie den Vorgang fortsetzen.

Sicherung durchführen

Eine vollständige Wiederherstellung von Tableau Server erfordert eine Reihe von Sicherungen, die drei Komponenten beinhaltet:

- Eine Sicherungsdatei der Repository- und Dateispeicherdaten. Diese Datei wird mit dem Befehl `tsm maintenance backup` generiert.
- Eine Topologie- und Konfigurationsexportdatei. Diese Datei wird mit dem Befehl `tsm`

`settings export` generiert.
- Authentifizierungszertifikat, Schlüssel und Keytab-Dateien.

Eine vollständige Beschreibung des Sicherungs- und Wiederherstellungsvorgangs finden Sie im Tableau Server-Thema *Durchführen einer vollständigen Sicherung und Wiederherstellen von Tableau Server* (Linux).

In dieser Phase Ihrer Bereitstellung sind alle relevanten Dateien und Assets enthalten, die für eine vollständige Wiederherstellung erforderlich sind, indem Sie die Befehle `tsm maintenance backup` und `tsm settings export` ausführen.

1. Führen Sie den folgenden Befehl aus, um die Konfigurations- und Topologieeinstellungen in eine Datei namens `ts_settings_backup.json` zu exportieren.

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

2. Führen Sie den folgenden Befehl aus, um eine Sicherung der Repository- und Dateispeicherdaten in einer Datei namens `ts_backup-<yyyy-mm-dd>.tsbak` zu erstellen. Ignorieren Sie die Warnung, dass sich der Dateispeicher nicht auf dem Controller-Knoten befindet.

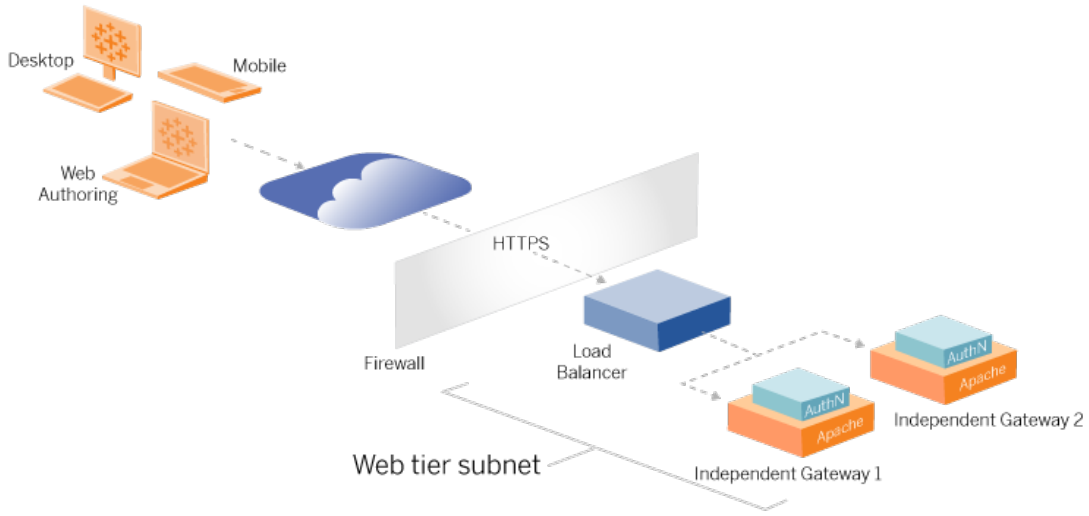
   ```
   tsm maintenance backup -f ts_backup -d --skip-compression
   ```

   Speicherort der Sicherungsdatei:

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

3. Kopieren Sie beide Dateien und speichern Sie sie auf einer anderen Speicherressource, die nicht von Ihrer Tableau Server-Bereitstellung gemeinsam genutzt wird.

Teil 5 - Konfigurieren der Web-schicht



Die Webschicht der Referenzarchitektur sollte die folgenden Komponenten umfassen:

- Ein webseitiger Anwendungs-Lastenausgleich, der HTTPS-Anforderungen von Tableau-Clients entgegen nimmt und mit den Reverse-Proxyservern kommuniziert.
- Reverse-Proxy:
  - Wir empfehlen die Bereitstellung des Tableau Server Independent Gateway.
  - Wir empfehlen mindestens zwei Proxyserver, um Redundanz zu erhalten und um die Client-Last zu bewältigen.
  - Er empfängt HTTPS-Datenverkehr vom Lastenausgleich.
  - Er unterstützt Sticky-Sitzung zum Tableau-Host.
  - Konfigurieren Sie den Proxy für Roundrobin-Lastenausgleich für jeden Tableau Server, auf dem der Gateway-Prozess ausgeführt wird.
  - Er verarbeitet Authentifizierungsanfragen von externem IdP.
- Forward-Proxy: Tableau Server benötigt für die Lizenzierung und die Kartenfunktionalität Zugriff auf das Internet. Für Tableau-Service-URLs müssen Sie Forward-Proxy-Safelists konfigurieren. Siehe *Kommunikation mit dem Internet* (Linux).

- Sämtlicher clientbezogene Datenverkehr kann über HTTPS verschlüsselt werden:
  - Client-zu-Anwendung-Lastenausgleich
  - Anwendungs-Lastenausgleich zu Reverse-Proxyserver
  - Proxyserver zu Tableau Server
  - Authentifizierungs-Handler, der auf Reverse-Proxy zu IdP ausgeführt wird
  - Tableau Server zu IdP

Tableau Server Independent Gateway

Ab Version 2022.1 enthält Tableau Server das Tableau Server Independent Gateway. Independent Gateway ist eine eigenständige Instanz des Tableau Gateway-Prozesses, die als Tableau-fähiger Reverse-Proxy dient.

Independent Gateway unterstützt einfachen Round-Robin-Lastenausgleich zu den Back-End-Tableau-Servern. Independent Gateway ist jedoch nicht als Lastenausgleich für Unternehmensanwendungen gedacht. Wir empfehlen, Independent Gateway hinter einem Lastenausgleich für Unternehmensanwendungen der Enterprise-Klasse auszuführen.

Für das Independent Gateway ist eine Lizenz vom Typ "Advanced Management" erforderlich.

Authentifizierung und Autorisierung

Die Standard-Referenzarchitektur sieht die Installation von Tableau Server mit konfigurierter lokaler Authentifizierung vor. In diesem Modell müssen die Clients eine Verbindung zu Tableau Server herstellen, um durch den nativen lokalen Authentifizierungsprozess von Tableau Server authentifiziert zu werden. Es wird nicht empfohlen, diese Authentifizierungsmethode in der Referenzarchitektur zu verwenden, da das Szenario erfordert, dass nicht authentifizierte Clients mit der Anwendungsebene kommunizieren, was ein Sicherheitsrisiko darstellt.

Stattdessen wird die Konfiguration eines externen Identitätsanbieters der Enterprise-Klasse in Verbindung mit einem AuthN-Modul zur Vor-Authentifizierung des gesamten Datenverkehrs zur Anwendungsebene empfohlen. Bei der Konfiguration mit einem externen IdP wird der native lokale Authentifizierungsprozess von Tableau Server nicht verwendet.

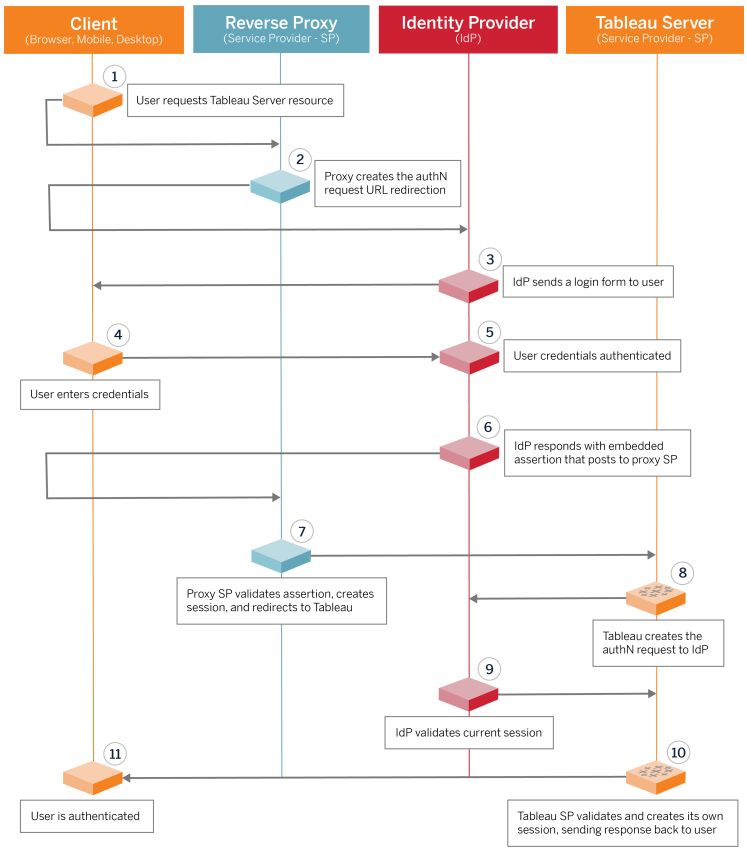
Tableau Server autorisiert den Zugriff auf Ressourcen in der Bereitstellung, nachdem der IdP die Benutzer authentifiziert hat.

Vor-Authentifizierung mit einem AuthN-Modul

IIn dem in diesem Leitfaden dokumentierten Beispiel ist SAML SSO konfiguriert, aber der Vorauthentifizierungsprozess kann mit den meisten externen Identitätsanbietern und einem AuthN-Modul konfiguriert werden.

In der Referenzarchitektur ist der Reverseproxy so konfiguriert, dass er eine Client-Authentifizierungssitzung mit dem IdP erstellt, bevor er die Anfragen an Tableau Server weiterleitet. Diesen Prozess bezeichnen wird als die *Vor-Authentifizierungs*-Phase. Der Reverseproxy wird nur authentifizierte Clientsitzungen an Tableau Server umleiten. Tableau Server erstellt dann eine Sitzung, überprüft die Authentifizierung der Sitzung bei dem Identitätsanbieter und gibt dann die Clientanforderung zurück.

Das folgende Diagramm zeigt den schrittweisen Ablauf des Vor-Authentifizierungs- und Authentifizierungsprozesses mit einem konfigurierten AuthN-Modul: Der Reverse-Proxy kann eine allgemeine Lösung von einem Drittanbieter oder das Tableau Server Independent Gateway sein:



Konfigurationsübersicht

Dies ist eine Übersicht über den Prozess zum Konfigurieren der Webschicht. Überprüfen Sie nach jedem Schritt die Konnektivität:

1. Konfigurieren Sie zwei Reverse-Proxys, um HTTP-Zugriff auf Tableau Server bereitzustellen.
2. Konfigurieren Sie die Lastenausgleichslogik mit Sticky-Sitzungen auf Proxyservern, um eine Verbindung zu jeder Tableau Server-Instanz herzustellen, auf der der Gateway-Prozess ausgeführt wird.
3. Konfigurieren Sie Anwendungslastenausgleich mit Sticky-Sitzungen bei dem Internet-Gateway, um Anforderungen an die Reverse-Proxyserver weiterzuleiten.
4. Konfigurieren Sie Authentifizierung mit einem externen IdP. Sie können SSO oder SAML konfigurieren, indem Sie einen Authentifizierungs-Handler auf den Reverse-

Proxyservern installieren. Das AuthN-Modul verwaltet den Authentifizierungs-Handshake zwischen dem externen IdP und Ihrer Tableau-Bereitstellung. Tableau wird auch als IdP-Dienstanbieter fungieren und Benutzer bei dem IdP authentifizieren.

5. Um sich bei Tableau Desktop in dieser Bereitstellung zu authentifizieren, müssen Ihre Clients Tableau Desktop 2021.2.1 (oder höher) ausführen.

Beispiel für eine Webschichtkonfiguration mit Tableau Server Independent Gateway

Der Rest dieses Themas enthält ein komplettes Verfahren, das beschreibt, wie die Webschicht in der AWS-Referenzarchitektur in dem Beispiel mit dem Tableau Server Independent Gateway implementiert wird. Eine Beispielkonfiguration mit Apache als Reverse-Proxy finden Sie in Anhang – Webschicht mit Apache-Beispielbereitstellung.

Die Beispielkonfiguration setzt sich aus folgenden Komponenten zusammen:

- AWS-Anwendungslastenausgleich
- Tableau Server Independent Gateway
- Mellon-Authentifizierungsmodul
- Okta-IdP
- SAML-Authentifizierung

Hinweis: Die in diesem Abschnitt vorgestellte Beispielkonfiguration für die Webschicht enthält detaillierte Verfahren zum Bereitstellen von Software und Diensten von Drittanbietern. Wir haben uns nach Kräften bemüht, die Verfahren zur Aktivierung des Webschicht-Szenarios zu überprüfen und zu dokumentieren. Die Software von Drittanbietern kann sich jedoch ändern oder Ihr Szenario kann von der hier beschriebenen Referenzarchitektur abweichen. Verbindliche Konfigurationsdetails und Support finden Sie in der Dokumentation der Drittanbieter.

Die Linux-Beispiele in diesem Abschnitt zeigen Befehle für RHEL-ähnliche Distributionen. Die hier angegebenen spezifischen Befehle wurden mit der Amazon Linux 2-Distribution

entwickelt. Wenn Sie die Ubuntu-Distribution ausführen, bearbeiten Sie die Befehle entsprechend.

Die Bereitstellung der Webschicht in diesem Beispiel erfolgt nach einem schrittweisen Konfigurations- und Überprüfungsverfahren. Die Konfiguration der zentralen Web-Ebene umfasst die folgenden Schritte, um HTTP zwischen Tableau und dem Internet zu aktivieren. Apache wird so konfiguriert, dass es als Reverse-Proxy bzw. als Lastenausgleich hinter dem AWS-Anwendungs-Lastenausgleich ausgeführt wird:

1. Vorbereiten der Umgebung
2. Installieren von Independent Gateway
3. Konfigurieren des Independent Gateway-Servers
4. Konfigurieren von AWS-Anwendungslastenausgleich

Nachdem die Web-Ebene eingerichtet und die Konnektivität zu Tableau überprüft wurde, konfigurieren Sie die Authentifizierung bei einem externen Anbieter.

Vorbereiten der Umgebung

Führen Sie die folgenden Aufgaben aus, bevor Sie Independent Gateway bereitstellen.

1. Änderungen der AWS-Sicherheitsgruppe. Konfigurieren Sie die öffentliche Sicherheitsgruppe so, dass aus der privaten Sicherheitsgruppe eingehender Housekeeping-Datenverkehr des Independent Gateways (TCP 21319) zugelassen wird.

2. Installieren Sie Version 22.1.1 (oder höher) auf einem Tableau Server-Cluster mit vier Knoten, wie in Teil 4 – Installieren und Konfigurieren von Tableau Server dokumentiert.

3. Konfigurieren Sie die beiden Proxy-EC2-Instanzen in der öffentlichen Sicherheitsgruppe, wie in Konfigurieren der Hostcomputer dokumentiert.

Installieren von Independent Gateway

Für Tableau Server Independent Gateway ist eine Lizenz vom Typ "Advanced Management" erforderlich.

Das Bereitstellen von Tableau Server Independent Gateway besteht aus der Installation und Ausführung des RPM-Pakets und der anschließenden Konfiguration des Ausgangszustands. Das in dieser Anleitung angegebene Verfahren gibt verbindliche Anweisungen für die Bereitstellung in der Referenzarchitektur ab.

Wenn Ihre Bereitstellung von der Referenzarchitektur abweicht, konsultieren Sie die Hauptdokumentation von Tableau Server, *Installieren von Tableau Server mit Independent Gateway* (Linux).

> **Wichtig**: Das Konfigurieren des Independent Gateways kann ein fehleranfälliger Prozess sein. Es ist sehr schwierig, Konfigurationsprobleme über zwei Instanzen von Independent Gateway-Servern hinweg zu beheben. Aus diesem Grund empfehlen wir, immer nur einen Independent Gateway-Server auf einmal zu konfigurieren. Nachdem Sie den ersten Server konfiguriert und die Funktionalität überprüft haben, sollten Sie den zweiten Independent Gateway-Server konfigurieren.

Auch wenn Sie jeden Independent Gateway-Server separat konfigurieren, führen Sie dieses Installationsverfahren auf beiden EC2-Instanzen aus, die Sie in der öffentlichen Sicherheitsgruppe installiert haben:

1. Führen Sie das Update aus, um die neuesten Fixes für das Linux-Betriebssystem anzuwenden:

   ```
   sudo yum update
   ```

2. Wenn Apache installiert ist, entfernen Sie es:

   ```
   sudo yum remove httpd
   ```

3. Kopieren Sie das Installationspaket für Independent Gateway 2022.1.1 (oder höher) von der Tableau-Downloadseite auf den Hostcomputer, auf dem Tableau Server ausgeführt werden soll.

Auf einem Linux-RHEL-ähnlichen Betriebssystem beispielsweise führen Sie den folgenden Befehl aus:

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

4. Führen Sie das Installationsprogramm aus. Auf einem Linux-RHEL-ähnlichen Betriebssystem beispielsweise führen Sie den folgenden Befehl aus:

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

5. Wechseln Sie in das Verzeichnis `/opt/tableau/tableau_tsig/packages/scripts.<version_code>/` und führen Sie das Skript `initialize-tsig` aus, das sich dort befindet. Außer dem `--accepteula`-Flag müssen Sie auch den IP-Bereich der Subnetze angeben, in denen die Tableau Server-Bereitstellung ausgeführt wird. Verwenden Sie die Option `-c`, um den IP-Bereich anzugeben. Das folgende Beispiel zeigt den Befehl mit den angegebenen Beispiel-AWS-Subnetzen:

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

6. Öffnen Sie nach Abschluss der Initialisierung die Datei `tsighk-auth.conf` und kopieren Sie das Authentifizierungsgeheimnis in der Datei. Sie müssen diesen Code für jede Independent Gateway-Instanz als Teil der Back-End-Konfiguration von Tableau Server übermitteln:

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

7. Nachdem Sie die vorherigen Schritte auf beiden Instanzen des Independent Gateway ausgeführt haben, bereiten Sie die `tsig.json`-Konfigurationsdatei vor. Die Konfigurationsdatei besteht aus einem Array von "independentGateways". Das Array enthält Konfigurationsobjekte, die jeweils Verbindungsdetails für eine Independent Gateway-Instanz definieren.

Kopieren Sie die folgende JSON und passen Sie sie entsprechend Ihrer Bereitstellungsumgebung an. Das Beispiel hier zeigt eine Datei für eine Beispiel-AWS-Referenzarchitektur.

Die folgende JSON-Beispieldatei enthält nur Verbindungsinformationen für ein Independent Gateway. Später im Prozess werden Sie die Verbindungsinformationen für den zweiten Independent Gateway-Server hinzufügen.

Speichern Sie die Datei unter dem Namen `tsig.json` für die folgenden Schritte.

```
{
"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"` – Der private DNS-Name der AWS EC2-Instanz, auf der Independent Gateway ausgeführt wird.
- `"host"` – ist identisch mit`"id"`.
- `"port"` – Der Housekeeping-Port (standardmäßig `"21319"`).
- `"protocol"` – Das Protokoll für Client-Datenverkehr. Lassen Sie hier `http` für die Ausgangskonfiguration stehen.
- `"authsecret"` – Das Geheimnis, das Sie im vorherigen Schritt kopiert haben.

Independent Gateway: Unterschied zwischen direkter Verbindung und Relay-Verbindung

Bevor Sie fortfahren, müssen Sie entscheiden, welches Verbindungsschema in Ihrer Bereitstellung konfiguriert werden soll: Direkte oder Relay-Verbindung. Jede Option wird hier

zusammen mit relevanten Entscheidungsdatenpunkten kurz beschrieben.

Relay-Verbindung: Sie können Independent Gateway konfigurieren, um die Client-Kommunikation über einen einzelnen Port an den Gateway-Prozess in Tableau Server weiterzuleiten. Dies bezeichnen wir als *Relay*-Verbindung:

- Der Relay-Prozess führt zu einem zusätzlichen Hop vom Independent Gateway zum Back-End-Tableau Server-Gateway-Prozess. Der zusätzliche Hop verschlechtert die Leistung im Vergleich zur direkten Verbindungskonfiguration.
- TLS wird für den Relay-Modus unterstützt. Die gesamte Kommunikation im Relay-Modus ist auf ein einziges Protokoll (HTTP oder HTTPS) beschränkt und kann daher mit TLS verschlüsselt und authentifiziert werden.

Direkte Verbindung: Das Independent Gateway kann über mehrere Ports direkt mit den Back-End-Prozessen von Tableau Server kommunizieren. Diese Kommunikation bezeichnen wir als *direkte* Verbindung:

- Da die Verbindung direkt zum Back-End-Tableau Server erfolgt, wird die Clientleistung im Vergleich zur Relay-Verbindungsoption deutlich verbessert.
- Dies erfordert das Öffnen von mehr als 16 Ports von öffentlichen zu privaten Subnetzen für die direkte Prozesskommunikation vom Independent Gateway zu Tableau Server-Computern.
- TLS wird für die Prozesse von Independent Gateway zu Tableau Server noch nicht unterstützt.

Konfigurieren von Relay-Verbindung

Zum Ausführen von TLS zwischen Tableau Server und Independent Gateway müssen Sie eine Relay-Verbindung konfigurieren. Die Beispielszenarien im EDG sind mit einer Relay-Verbindung konfiguriert.

1. Kopieren Sie `tsig.json` auf Knoten 1 Ihrer Tableau Server-Bereitstellung.

2. Führen Sie auf Knoten 1 die folgenden Befehle aus, um Independent Gateway zu aktivieren.

```
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
```

Konfigurieren von direkter Verbindung

Da direkte Verbindung TLS nicht unterstützt, empfehlen wir, direkte Verbindung nur zu konfigurieren, wenn Sie in der Lage sind, sämtlichen Netzwerkdatenverkehr auf andere Weise abzusichern. Zum Ausführen von TLS zwischen Tableau Server und Independent Gateway müssen Sie eine Relay-Verbindung konfigurieren. Die Beispielszenarien im EDG sind mit einer Relay-Verbindung konfiguriert.

Wenn Sie Independent Gateway für eine direkte Verbindung mit Tableau Server konfigurieren, müssen Sie die Konfiguration aktivieren, um die Kommunikation auszulösen. Nachdem Tableau Server mit dem Independent Gateway kommuniziert, werden die Protokollziele eingerichtet. Sie müssen dann die `proxy_targets.csv` vom Independent Gateway-Computer abrufen und die entsprechenden Ports von den öffentlichen zu den privaten Sicherheitsgruppen in AWS öffnen.

1. Kopieren Sie `tsig.json` auf Knoten 1 Ihrer Tableau Server-Bereitstellung.
2. Führen Sie auf Knoten 1 die folgenden Befehle aus, um Independent Gateway zu aktivieren.

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

3. Führen Sie auf dem Independent Gateway-Computer den folgenden Befehl aus, um die Ports anzuzeigen, die der Tableau Server-Cluster verwendet:

```
less /var/opt/tableau/tableau_tsig/config/httpd/proxy_tar-
gets.csv
```

4. Konfigurieren Sie AWS-Sicherheitsgruppen. Fügen Sie die in `proxy_targets.csv` aufgelisteten TCP-Ports hinzu, um die Kommunikation von der öffentlichen Sicherheitsgruppe zu der privaten Sicherheitsgruppe zu ermöglichen.

   Wir empfehlen, die Porteingangskonfiguration zu automatisieren, da sich die Ports ändern können, wenn sich die Topologie der Tableau Server-Bereitstellung ändert. Wenn in der Tableau Server-Bereitstellung Knoten hinzugefügt oder Prozesse neu konfiguriert werden, bringt dies Änderungen beim Portzugriff mit sich, der von Independent Gateway benötigt wird.

Überprüfung: Konfiguration der Basistopologie

Sie sollten auf die Tableau Server-Administrationsseite zugreifen können, indem Sie zu `http://<gateway-public-IP-address>` navigieren.

Wenn die Anmeldeseite von Tableau Server nicht geladen wird oder wenn Tableau Server nicht gestartet wird, führen Sie die folgenden Fehlerbehebungsschritte aus:

Netzwerk:

- Überprüfen Sie die Konnektivität zwischen der Tableau-Bereitstellung und der Independent Gateway-Instanz, indem Sie den folgenden `wget`-Befehl auf dem Tableau Server-Knoten 1 ausführen: wget http://<interne IP-Adresse von Independent Gateway>:21319. Zum Beispiel:

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

  Wenn die Verbindung verweigert wird oder fehlschlägt, überprüfen Sie, dass die öffentliche Sicherheitsgruppe so konfiguriert ist, dass sie Independent Gateway-Housekeeping-Datenverkehr (TCP 21319) aus der privaten Sicherheitsgruppe zulässt.

  Wenn die Sicherheitsgruppe korrekt konfiguriert ist, überprüfen Sie, dass Sie die richtigen IP-Adressen oder IP-Bereiche während der Initialisierung von Independent

Gateway angegeben haben. Sie können diese Konfiguration in der Datei `environment.bash` (unter `/etc/opt/tableau/tableau_tsig/environment.bash`) einsehen und ändern. Wenn Sie in dieser Datei Änderungen vornehmen, müssen Sie den tsig-http-Dienst wie nachfolgend beschrieben neu starten.

Führen Sie auf dem Proxy 1-Host Folgendes durch:

1. Überschreiben Sie die httpd.conf-Datei mit der Independent Gateway-Stub-Datei:

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

2. Starten Sie als ersten Schritt zur Fehlerbehebung "tsig-httpd" neu:

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

Führen Sie auf Tableau-Knoten 1 Folgendes durch:

- Überprüfen Sie die Datei `tsig.json` noch einmal. Wenn Sie Fehler finden, beheben Sie sie und führen Sie dann den folgenden Befehl aus: `tsm topology external-services gateway update -c tsig.json`.
- Wenn Sie eine direkte Verbindung ausführen, überprüfen Sie, dass die in `proxy_targets.csv` aufgelisteten TCP-Ports als Eingangsports von öffentlichen zu privaten Sicherheitsgruppen konfiguriert sind.

Konfigurieren von AWS-Anwendungslastenausgleich

Konfigurieren Sie den Lastenausgleich als HTTP-Listener. Im hier vorliegenden Verfahren wird beschrieben, wie Sie einen Lastenausgleich in AWS hinzufügen.

Schritt 1: Erstellen einer Zielgruppe

Eine Zielgruppe ist eine AWS-Konfiguration, welche die EC2-Instances definiert, auf denen Ihre Proxyserver ausgeführt werden. Dies sind die Ziele für den Datenverkehr von der LBS.

1. EC2 > **Target groups** > **Create target group** (EC2 > Zielgruppen > Zielgruppe erstellen)

2. Auf der Seite "Create" (Erstellen):

    - Geben Sie einen Zielgruppennamen ein, zum Beispiel `TG-internal-HTTP`.
    - Zieltyp: Instanzen
    - Protokoll: HTTP
    - Port: 80
    - VPC: Wählen Sie Ihre VPC aus.
    - Fügen Sie unter **Health checks** (Integritätsprüfungen) > **Advanced health checks settings** (Einstellungen für erweiterte Integritätsprüfungen) > **Success codes** (Erfolgscodes) die Codeliste zum Lesen hinzu: `200,303`.
    - Klicken Sie auf **Create** (Erstellen).

3. Wählen Sie die Zielgruppe aus, die Sie eben erstellt haben, und klicken Sie dann auf die Registerkarte **Targets** (Ziele):

    - Klicken Sie auf **Edit** (Bearbeiten).
    - Wählen Sie die EC2-Instanzen (oder eine einzelne Instanz, wenn Sie einzeln konfigurieren) aus, auf denen die Proxyanwendung ausgeführt wird. Klicken Sie dann auf **Zu registriert hinzufügen**.
    - Klicken Sie auf **Speichern**.

Schritt 2: Starten des Assistenten für Lastenausgleich

1. EC2 > **Load Balancers** > **Create Load Balancer** (EC2 > Lastenausgleichsmodule > Lastenausgleich erstellen)

2. Erstellen Sie auf der Seite "Select load balancer type" (Lastenausgleichstyp auswählen) einen Anwendungslastenausgleich.

Hinweis: Die Benutzeroberfläche, die zur Konfiguration des Lastenausgleichsmodulen angezeigt wird, ist in den AWS-Rechenzentren nicht einheitlich. Das folgende Verfahren

"Assistenten-Konfiguration" bezieht sich auf den AWS-Konfigurationsassistenten, der mit **Schritt 1 Lastenausgleichsmodul konfigurieren** beginnt.

Wenn Ihr Rechenzentrum alle Konfigurationen auf einer einzigen Seite anzeigt, die unten auf der Seite eine Schaltfläche **Create Load Balancer** enthält, befolgen Sie das nachstehende Verfahren "Konfiguration auf einer Seite".

Assistenten-Konfiguration

1. Die Seite **Configure load balancer** (Lastenausgleich konfigurieren):
    - Geben Sie den Namen an
    - Schema: Internetzugriff (Standard)
    - IP-Adresstyp: IPv4 (Standard)
    - Listener (Listener und Routing):
        a. Behalten Sie den Standard-HTTP-Listener bei.
        b. Klicken Sie auf **Listener hinzufügen** und fügen Sie `HTTPS:443` hinzu.
    - VPC: Wählen Sie die VPC aus, in der Sie alles installiert haben.
    - Verfügbarkeitszonen:
        - Wählen Sie **a** und **b** für Ihre Rechenzentrumsregionen aus.
        - Wählen Sie in der entsprechenden Dropdown-Liste das öffentliche Subnetz aus (in dem sich Ihre Proxyserver befinden).
    - Klicken Sie auf **Configure Security Settings** (Sicherheitseinstellungen konfigurieren)
2. Die Seite **Configure Security Settings** (Sicherheitseinstellungen konfigurieren)
    - Laden Sie Ihr öffentliches SSL-Zertifikat hoch.
    - Klicken Sie auf **Next: Configure Security Groups** (Weiter: Sicherheitsgruppen konfigurieren).
3. Die Seite **Configure Security Groups** (Sicherheitsgruppen konfigurieren):

- Wählen Sie die öffentliche Sicherheitsgruppe aus. Wenn die Standardsicherheitsgruppe ausgewählt ist, deaktivieren Sie diese Auswahl.
- Klicken Sie auf **Next: Configure Routing** (Weiter: Routing konfigurieren).

4. Die Seite **Configure Routing** (Routing konfigurieren)
    - Zielgruppe: Bestehende Zielgruppe.
    - Name: Wählen Sie eine Zielgruppe aus, die Sie zuvor erstellt haben.
    - Klicken Sie auf **Next: Register Targets** (Weiter: Ziele registrieren).

5. Die Seite **Register Targets** (Ziele registrieren)
    - Die beiden Proxyserver-Instanzen, die Sie zuvor konfiguriert haben, sollten angezeigt werden.
    - Klicken Sie auf **Next: Review** (Weiter: Überprüfung).

6. Die Seite **Review** (Überprüfen)

    Klicken Sie auf **Erstellen**.

Konfiguration auf einer Seite

Grundlegende Konfiguration

- Geben Sie den Namen an
- Schema: Internetzugriff (Standard)
- IP-Adresstyp: IPv4 (Standard)

Netzwerkzuordnung

- VPC: Wählen Sie die VPC aus, in der Sie alles installiert haben.
- Zuordnungen:
    - Wählen Sie die Verfügbarkeitszonen **a** und **b** (oder vergleichbare) für Ihre Rechenzentrumsregionen aus.
    - Wählen Sie in der entsprechenden Dropdown-Liste das öffentliche Subnetz aus (in dem sich Ihre Proxyserver befinden).

Sicherheitsgruppen

Wählen Sie die öffentliche Sicherheitsgruppe aus. Wenn die Standardsicherheitsgruppe ausgewählt ist, deaktivieren Sie diese Auswahl.

Listener und Routing

- Behalten Sie den Standard-HTTP-Listener bei. Geben Sie bei **Standardaktion** die zuvor eingerichtete Zielgruppe an.
- Klicken Sie auf **Listener hinzufügen** und fügen Sie `HTTPS:443` hinzu. Geben Sie bei **Standardaktion** die zuvor eingerichtete Zielgruppe an.

Sichere Listener-Einstellungen

- Laden Sie Ihr öffentliches SSL-Zertifikat hoch.

Klicken Sie auf **Create Load Balancer**.

Schritt 3: Stickiness aktivieren

1. Nachdem der Lastenausgleich erstellt wurde, müssen Sie Stickiness für die Zielgruppe aktivieren.
    - Öffnen Sie die AWS-Seite für die Zielgruppe (**EC2** > **Load Balancing** (Lastenausgleich) > **Target groups** (Zielgruppen)), und wählen Sie die Zielgruppeninstanz aus, die Sie gerade eingerichtet haben. Wählen Sie im Menü **Actions** (Aktionen) die Option **Edit attributes** (Attribute bearbeiten) aus.
    - Wählen Sie auf der Seite **Edit attributes** (Attribute bearbeiten) die Option **Stickiness** (Bindung) aus, geben Sie eine Zeitdauer von `1 day` (1 Tag) an, und klicken Sie dann auf **Save changes** (Änderungen speichern).
2. Aktivieren Sie beim Lastenausgleich Stickiness auf dem HTTP-Listener. Wählen Sie den Lastenausgleich aus, den Sie gerade konfiguriert haben, und klicken Sie dann auf die Registerkarte **Listeners**:
    - Klicken Sie für **HTTP:80** auf **View/edit rules** (Regeln anzeigen/bearbeiten). Klicken Sie auf der Seite **Rules** (Regeln), die daraufhin angezeigt wird, auf das Bearbeitungssymbol (zuerst oben auf der Seite und dann noch einmal für die Regel), um die Regel zu bearbeiten. Löschen Sie die vorhandene THEN-Regel ("DANN-Regel") und ersetzen Sie sie, indem Sie auf **Add action** (Aktion hinzufügen) > **Forward to...** (Weiterleiten an...) klicken. Geben Sie in der

resultierenden THEN-Konfiguration die gleiche Zielgruppe an, die Sie erstellt haben. Aktivieren Sie unter "Group-level stickiness" (Bindung auf Gruppenebene) den Punkt "Stickiness", und legen Sie "Duration" (Zeitdauer) auf "1 Day" (1 Tag) fest. Speichern Sie die Einstellung und klicken Sie dann auf **Update** (Aktualisieren).

Schritt 4: Festlegen des Leerlaufzeitlimits für den Lastenausgleich

Aktualisieren Sie für den Lastenausgleich das Leerlaufzeitlimit auf 400 Sekunden.

Wählen Sie den Lastenausgleich, den Sie für diese Bereitstellung konfiguriert haben, und klicken Sie dann auf **Aktionen** > **Attribute bearbeiten**. Stellen Sie das **Leerlaufzeitlimit** auf `400` Sekunden ein und klicken Sie dann auf **Speichern**.

Schritt 5: Überprüfen der LBS-Verbindung

Öffnen Sie die Seite "AWS Load Balancer" (AWS-Lastenausgleich) (**EC2**> **Load Balancers** (Lastenausgleich)), wählen Sie die Lastenausgleichsinstanz aus, die Sie gerade eingerichtet haben.

Kopieren Sie unter **Description** (Beschreibung) den DNS-Namen und fügen Sie ihn in einen Browser ein, um auf die Tableau Server-Anmeldeseite zuzugreifen.

Wenn ein Fehler auf 500-Niveau angezeigt wird, müssen Sie wahrscheinlich Ihre Proxyserver neu starten.

Aktualisieren des DNS mit der öffentlichen Tableau-URL

Verwenden Sie den DNS-Zonennamen Ihrer Domäne aus der AWS-Seite "Load Balancer" (Lastenausgleich) > "Description" (Beschreibung), um einen CNAME-Wert in Ihrem DNS zu erstellen. Datenverkehr zu Ihrer URL (tableau.example.com) sollte an den öffentlichen AWS-DNS-Namen gesendet werden.

Überprüfen der Konnektivität

Nachdem Ihre DNS-Updates abgeschlossen sind, sollten Sie zu der Tableau Server-Anmeldeseite navigieren können, indem Sie Ihre öffentliche URL eingeben, zum Beispiel:`https://tableau.example.com`.

Beispiel für eine Konfiguration für Authentifizierung: SAML mit externem IdP

Im folgenden Beispiel wird beschrieben, wie Sie SAML mit Okta-IdP und Mellon-Authentifizierungsmodul für eine Tableau-Bereitstellung einrichten und konfigurieren, die in der AWS-Referenzarchitektur ausgeführt wird.

Dieses Beispiel knüpft an den vorherigen Abschnitt an und geht davon aus, dass Sie immer nur ein Independent Gateway auf einmal konfigurieren.

In dem Beispiel wird beschrieben, wie Tableau Server und Independent Gateway über HTTP konfiguriert werden. Okta wird Anfragen an den AWS-Lastenausgleich über HTTPS senden, aber sämtlicher interner Datenverkehr wird über HTTP erfolgen. Beachten Sie bei der Konfiguration für dieses Szenario die Unterschiede von HTTP und HTTPS, wenn Sie URL-Zeichenfolgen festlegen.

In diesem Beispiel wird Mellon als Dienstanbietermodul für Vorauthentifizierung auf den Independent Gateway-Servern verwendet. Diese Konfiguration stellt sicher, dass nur authentifizierter Datenverkehr mit Tableau Server verbunden wird, der auch als Dienstanbieter mit dem Okta-IdP agiert. Daher müssen Sie zwei IdP-Anwendungen konfigurieren: eine für den Mellon-Dienstanbieter und eine für den Tableau-Dienstanbieter.

Erstellen des Tableau-Administratorkontos

Ein häufiger Fehler beim Konfigurieren von SAML ist, die Erstellung eines Administratorkontos in Tableau Server zu vergessen, bevor SSO aktiviert wird.

Der erste Schritt besteht darin, ein Konto in Tableau Server mit einer Serveradministratorrolle zu erstellen. Für das Okta-Beispielszenario muss der Benutzername in einem gültigen E-Mail-Adressformat angegeben werden (z. B. user@example.com). Sie müssen für diesen Benutzer ein Kennwort festlegen, das jedoch nach der Konfiguration von SAML nicht mehr verwendet wird.

Konfigurieren der Vor-Authentifizierungsanwendung von Okta

Das in diesem Abschnitt beschriebene End-to-End-Szenario erfordert zwei Okta-Anwendungen:

- Vor-Authentifizierungsanwendung von Okta
- Tableau Server-Anwendung von Okta

Jede dieser Anwendungen ist mit unterschiedlichen Metadaten verbunden, die Sie auf dem Reverse-Proxy bzw. Tableau Server konfigurieren müssen.

In diesem Verfahren wird beschrieben, wie Sie die Vor-Authentifizierungsanwendung von Okta erstellen und konfigurieren. Später in diesem Thema ist vorgesehen, dass Sie die Tableau Server-Anwendung von Okta erstellen. Ein kostenloses Okta-Testkonto mit eingeschränkten Benutzern finden Sie auf der Okta-Entwickler-Webseite.

Erstellen Sie eine SAML-App-Integration für den Mellon-Vorauthentifizierungs-Dienstanbieter.

1. Öffnen Sie das Okta-Administrations-Dashboard, und klicken Sie auf **Applications** > **Create App Integration** (Anwendungen > App-Integration erstellen).
2. Wählen Sie auf der Seite **Create a new app integration** (Neue App-Integration erstellen) die Option **SAML 2.0** aus, und klicken Sie dann auf **Next** (Weiter).
3. Geben Sie auf der Registerkarte **General Settings** (Allgemeine Einstellungen) einen App-Namen ein (z. B. `Tableau Pre-Auth`), und klicken Sie dann auf **Next** (Weiter).
4. Auf der Registerkarte **Configure SAML** (SAML konfigurieren):

- SSO-URL (Single Sign-On): Das letzte Element des Pfads in der Single Sign-On-URL wird als der `MellonEndpointPath` in der `mellon.conf` Konfigurationsdatei bezeichnet, die später in diesem Verfahren behandelt wird. Sie können einen beliebigen Endpunkt angeben. In diesem Beispiel ist `sso` der Endpunkt. Das letzte Element, `postResponse`, ist erforderlich: `https://tableau.example.com/sso/postResponse`.
- Deaktivieren Sie das Kontrollkästchen **Use this for Recipient URL and Destination URL** (Dieses für Empfänger-URL und Ziel-URL verwenden).
- Recipient URL (Empfänger-URL): Ist die gleiche wie die SSO-URL, jedoch mit HTTP. Zum Beispiel: `http://tableau.example.com/sso/postResponse`.
- Destination URL (Ziel-URL): Ist die gleiche wie die SSO-URL, jedoch mit HTTP. Zum Beispiel: `http://tableau.example.com/sso/postResponse`.
- Audience URI (SP Entity ID) (Zielgruppen-URI (SP-Entitäts-ID)). Zum Beispiel: `https://tableau.example.com`.
- Name ID Format (Format der Namens-ID): `EmailAddress`
- Application Username (Anwendungsbenutzername): `Email`
- Attributes Statements (Attributangaben): Name = `mail`; Name format (Namensformat) = `Unspecified`; Value (Wert) = `user.email`.

Klicken Sie auf **Next** (Weiter).

5. Wählen Sie auf der Registerkarte **Feedback** Folgendes aus:
   - **I'm an Okta customer adding an internal app (Ich bin ein Okta-Kunde und füge eine interne App hinzu)**
   - **This is an internal app that we have created (Dies ist eine interne App, die wir erstellt haben)**
   - Klicken Sie auf **Finish** (Fertigstellen).

6. Erstellen Sie die IdP-Metadatendatei vor der Authentifizierung:
   - In Okta: **Applications** (Anwendungen) > **Applications** (Anwendungen) > Ihre neue Anwendung (z. B. `Tableau Pre-Auth`) > **Sign On** (Anmelden)
   - Klicken Sie neben **SAML-Signaturzertifikate** auf **Anweisungen zur SAML-Einrichtung anzeigen**.
   - Führen Sie auf der Seite **Konfigurieren von SAML 2.0 für die Anwendung vor der Authentifizierung** einen Bildlauf nach unten zum Abschnitt **Optional** durch, **Stellen Sie die folgenden IDP-Metadaten für Ihren SP-Anbieter bereit**.

- Kopieren Sie den Inhalt des XML-Felds, und speichern Sie ihn in einer Datei mit dem Namen `pre-auth_idp_metadata.xml`.

7. (Optional) Konfigurieren Sie Multi-Faktor-Authentifizierung (MFA):

   - In Okta: **Applications** (Anwendungen) > **Applications** (Anwendungen) > Ihre neue Anwendung (z. B. `Tableau Pre-Auth`) > **Sign On** (Anmelden)
   - Klicken Sie unter **Sign On Policy** (Anmelderichtlinie) auf **Add Rule** (Regel hinzufügen).
   - Geben Sie in der **App Sign On Rule** (App-Anmelderegel) einen Namen und die verschiedenen MFA-Optionen an. Um die Funktionalität zu testen, können Sie alle Optionen in der jeweiligen Standardeinstellung belassen. Sie müssen jedoch unter **Actions** (Aktionen) den Punkt **Prompt for factor** (Zur Eingabe des Faktors auffordern) auswählen und dann angeben, wie oft sich Benutzer anmelden müssen. Klicken Sie auf **Save** (Speichern).

Erstellen und Zuweisen eines Okta-Benutzers

1. Erstellen Sie in Okta einen Benutzer mit dem gleichen Benutzernamen, den Sie in Tableau erstellt haben (user@example.com): **Directory** (Verzeichnis) > **People** (Personen) > **Add person** (Person hinzufügen).
2. Nachdem der Benutzer erstellt wurde, weisen Sie ihm die neue Okta-App zu: Klicken Sie auf den Benutzernamen und weisen Sie dann die Anwendung in **Assign Application** (Anwendung zuweisen) zu.

Installieren von Mellon für die Vor-Authentifizierung

Dieses Beispiel verwendet "mod_auth_mellon", ein beliebtes Open-Source-Modul. Einige Linux-Distributionen packen veraltete "mod_auth_mellon"-Versionen aus einem älteren Repository. Diese veralteten Versionen können unbekannte Sicherheitslücken enthalten oder Funktionsprobleme verursachen. Wenn Sie sich für "mod_auth_mellon" entscheiden, überprüfen Sie, ob Sie eine aktuelle Version verwenden.

Das Modul "mod_auth_mellon" ist eine Software von Drittanbietern. Wir haben uns nach Kräften bemüht, die Verfahren zur Aktivierung dieses Szenarios zu überprüfen und zu dokumentieren. Allerdings kann sich Software von Drittanbietern ändern oder Ihr Szenario kann

von der hier beschriebenen Referenzarchitektur abweichen. Verbindliche Konfigurationsdetails und Support finden Sie in der Dokumentation der Drittanbieter.

1. Installieren Sie auf der aktiven EC2-Instanz, auf der Independent Gateway ausgeführt wird, eine aktuelle Version des Mellon-Authentifizierungsmoduls.
2. Erstellen Sie das Verzeichnis `/etc/mellon`:

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

Konfigurieren von Mellon als Vor-Authentifizierungsmodul

Führen Sie dieses Verfahren auf der ersten Instanz von Independent Gateway durch.

Sie müssen eine Kopie der Datei `pre-auth_idp_metadata.xml` haben, die Sie aus der Okta-Konfiguration erstellt haben.

1. Wechseln Sie das Verzeichnis:

   ```
   cd /etc/mellon
   ```

2. Erstellen Sie die Dienstanbieter-Metadaten. Führen Sie das Skript `mellon_create_metadata.sh` aus. Sie müssen in dem Befehl die Entitäts-ID und die Rückgabe-URL für Ihre Organisation mit angeben.

   Die Rückgabe-URL wird in Okta als *Single Sign On URL* (SSO-URL) bezeichnet. Das letzte Element des Pfads in der Rückgabe-URL wird als `MellonEndpointPath` in der Konfigurationsdatei `mellon.conf` bezeichnet, die später in diesem Verfahren folgt. In diesem Beispiel geben wir `sso` als EndpointPath an.

   Beispiel:

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

Das Skript gibt das Dienstanbieterzertifikat, den Schlüssel und Metadatendateien zurück.

3. Benennen Sie die Dienstanbieterdateien im Verzeichnis `mellon` so um, dass sie leichter verständlich sind. Wir werden diese Dateien in der Dokumentation mit den folgenden Namen bezeichnen:

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

4. Kopieren Sie die Datei `pre-auth_idp_metadata.xml` in dasselbe Verzeichnis.

5. Ändern Sie die Eigentümerschaft und die Berechtigungen für alle Dateien in dem Verzeichnis `/etc/mellon`:

   ```
   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. Erstellen Sie das Verzeichnis `/etc/mellon/conf.d`:

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

7. Erstellen Sie die Datei `global.conf` im Verzeichnis `/etc/mellon/conf.d`.

   Kopieren Sie den Dateiinhalt, wie unten gezeigt, aber aktualisieren Sie `MellonCookieDomain` mit Ihrem Stammdomänennamen. Wenn beispielsweise der Domänenname für Tableau `tableau.example.com` lautet, geben Sie `example.com` für die Stammdomäne ein.

```
<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. Erstellen Sie die Datei `mellonmod.conf` im Verzeichnis `/etc/mellon/conf.d`.

   Diese Datei enthält eine einzige Direktive, die den Speicherort der Datei `mod_auth_mellon.so` angibt. Der Speicherort in diesem Beispiel ist der Standardspeicherort der Datei. Stellen Sie sicher, dass sich die Datei an diesem Speicherort befindet, oder ändern Sie den Pfad in dieser Direktive so, dass er mit dem tatsächlichen Speicherort von `mod_auth_mellon.so` übereinstimmt:

   ```
   LoadModule auth_mellon_module /usr/lib64/httpd/modules/mod_auth_mellon.so
   ```

Erstellen einer Tableau Server-Anwendung in Okta

1. Im Okta-Dashboard: **Applications** (Anwendungen) > **Applications** (Anwendungen) > **Browse App Catalog** (App-Katalog durchsuchen)
2. Suchen Sie in **Browse App Integration Catalog** (App-Integrationskatalog durchsuchen) nach `Tableau`, wählen Sie die Kachel "Tableau Server" aus und klicken Sie dann auf **Add** (Hinzufügen).

3. Geben Sie unter **Add Tableau Server** (Tableau Server hinzufügen) > **General Settings** (Allgemeine Einstellungen) ein "Label" (Beschriftung) ein, und klicken Sie dann auf **Next** (Weiter).
4. Wählen Sie in "Sign-On Options" (Anmeldeoptionen) die Option **SAML 2.0** aus und führen Sie dann einen Bildlauf nach unten durch, bis "Advanced Sign-on Settings" (Erweiterte Anmeldeeinstellungen) angezeigt wird:
    - **SAML Entity ID** (SAML-Entitäts-ID): Geben Sie die öffentliche URL ein (z. B. https://tableau.example.com).
    - **Application user name format** (Format des Anwendungsbenutzernamens): Email (E-Mail)
5. Klicken Sie auf den Link **Identity Provider metadata** (Identitätsanbieter-Metadaten), um einen Browser zu starten. Kopieren Sie den Browserlink. Das ist der Link, den Sie verwenden werden, wenn Sie Tableau im folgenden Verfahren konfigurieren.
6. Klicken Sie auf **Done** (Fertig).
7. Weisen Sie Ihrem Benutzer (user@example.com) die neue Tableau Server-Okta-App zu: Klicken Sie auf den Benutzernamen und weisen Sie dann die Anwendung in **Assign Application** (Anwendung zuweisen) zu.

Festlegen der Konfiguration des Authentifizierungsmoduls in Tableau Server

Führen Sie die folgenden Befehle auf dem Tableau Server-Knoten 1 aus. Diese Befehle geben die Dateispeicherorte für die Mellon-Konfigurationsdateien auf dem remoten Independent Gateway-Computer an. Überprüfen Sie noch einmal, dass die in diesen Befehlen angegebenen Dateipfade mit den Pfaden und Dateispeicherorten auf dem remoten Independent Gateway-Computer übereinstimmen.

```
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
```

Um Ausfallzeiten zu reduzieren, sollten Sie keine Änderungen anwenden, bevor Sie SAML – wie im nächsten Abschnitt beschrieben – aktiviert haben.

Aktivieren von SAML in Tableau Server für IdP

Führen Sie dieses Verfahren auf dem Tableau Server-Knoten 1 aus.

1. Laden Sie die Metadaten der Tableau Server-Anwendung von Okta herunter. Verwenden Sie den Link, den Sie im vorherigen Verfahren gespeichert haben:

   ```
   wget https://dev-66144217.okta.com/app/exk1egxgt1fhjkSeS5d7/sso/saml/metadata -O idp_metadata.xml
   ```

2. Kopieren Sie ein TLS-Zertifikat und die zugehörige Schlüsseldatei auf Tableau Server. Die Schlüsseldatei muss ein RSA-Schlüssel sein. Weitere Informationen zu SAML-Zertifikat- und Identitätsanbieteranforderungen finden Sie unter *SAML-Anforderungen* (Linux).

   Zur Vereinfachung der Zertifikatsverwaltung und -bereitstellung sowie als bewährte Sicherheitspraxis empfehlen wir die Verwendung von Zertifikaten, die von einer bedeutenden vertrauenswürdigen Zertifizierungsstelle (CA) eines Drittanbieters erstellt wurden. Alternativ dazu können Sie auch selbstsignierte Zertifikate generieren oder Zertifikate von einer PKI für TLS verwenden.

   Wenn Sie nicht über ein TLS-Zertifikat verfügen, können Sie nach der folgenden Vorgehensweise ein selbstsigniertes Zertifikat generieren.

Generieren eines selbstsignierten Zertifikats

Führen Sie dieses Verfahren auf dem Tableau Server-Knoten 1 aus.

a. Generieren Sie den Schlüssel der signierenden Stammzertifizierungsstelle (CA):

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

b. Erstellen Sie das Zertifikat der Stammzertifizierungsstelle:

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

Sie werden aufgefordert, Werte für die Zertifikatfelder einzugeben. Beispiel:

```
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. Erstellen Sie das Zertifikat und den zugehörigen Schlüssel (im Beispiel unten als `server-saml.csr` und `server-saml.key` bezeichnet). Der Antragstellername ("Subject Name") für das Zertifikat muss mit dem öffentlichen Hostnamen des Tableau-Hosts übereinstimmen. Der Antragstellername wird mit der Option `-subj` im Format `"/CN=<host-name>"` festgelegt, beispielsweise:

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

d. Signieren Sie das neue Zertifikat mit dem CA-Zertifikat, das Sie oben erstellt haben. Der folgende Befehl gibt das Zertifikat auch im `crt`-Format aus:

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

e. Konvertieren Sie die Schlüsseldatei in RSA. Tableau erfordert eine RSA-Schlüsseldatei für SAML. Führen Sie den folgenden Befehl aus, um den Schlüssel zu

konvertieren:

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

3. Konfigurieren Sie SAML. Führen Sie den folgenden Befehl aus und geben Sie Ihre Entitäts-ID und die Rückgabe-URL sowie die Pfade zur Metadatendatei, zur Zertifikatsdatei und zur Schlüsseldatei an:

   ```
   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. Wenn in Ihrer Organisation Tableau Desktop 2021.4 oder höher ausgeführt wird, müssen Sie den folgenden Befehl ausführen, um Authentifizierung über die Reverse-Proxyserver zu aktivieren.

   Die Tableau Desktop-Versionen 2021.2.1 bis 2021.3 funktionieren ohne Ausführung dieses Befehls, vorausgesetzt, Ihr Vorauthentifizierungsmodul (z. B. Mellon) ist so konfiguriert, dass es die Aufbewahrung von Cookies auf der Domäne der obersten Ebene erlaubt.

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

5. Übernehmen Sie die Konfigurationsänderungen:

   ```
   tsm pending-changes apply
   ```

Neustarten des tsig-httpd-Dienstes

Wenn Ihre Tableau Server-Bereitstellung Änderungen übernimmt, melden Sie sich wieder bei den Tableau Server Independent Gateway-Computern an und führen Sie die folgenden Befehle aus, um den tsig-httpd-Dienst neu zu starten:

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

Validierung der SAML-Funktionalität

Um die End-to-End-SAML-Funktionalität zu validieren, melden Sie sich bei Tableau Server mit der öffentlichen URL (z. B. https://tableau.example.com) mit dem Tableau-Administratorkonto an, das Sie zu Beginn dieses Verfahrens erstellt haben.

Wenn TSM nicht startet ("Gateway-Fehler") oder wenn Sie bei einem Verbindungsversuch Browserfehler erhalten, lesen Sie Fehlerbehebung beim Tableau Server Independent Gateway.

Konfigurieren des Authentifizierungsmoduls auf der zweiten Instanz von Independent Gateway

Nachdem Sie die erste Instanz von Independent Gateway erfolgreich konfiguriert haben, stellen Sie die zweite Instanz bereit. Das Beispiel hier ist der letzte Prozess zum Installieren des in diesem Thema beschriebenen AWS/Mellon/Okta-Szenarios. Bei diesem Verfahren wird davon ausgegangen, dass Sie Independent Gateway bereits auf der zweiten Instanz installiert haben, wie zuvor in diesem Thema beschrieben (Installieren von Independent Gateway).

Der Prozess zum Bereitstellen des zweiten Independent Gateways erfordert die folgenden Schritte:

1. Auf der zweiten Instanz von Independent Gateway: Installieren Sie das Mellon-Authentifizierungsmodul.

   Konfigurieren Sie das Mellon-Authentifizierungsmodul nicht wie weiter oben in diesem Thema beschrieben. Stattdessen müssen Sie die Konfiguration klonen, wie in den folgenden Schritten beschrieben.

2. Auf der konfigurierten (ersten) Instanz von Independent Gateway:

   Fertigen Sie eine tar-Kopie der vorhandenen Mellon-Konfiguration an. Die tar-Sicherung wird alle Verzeichnishierarchien und Berechtigungen enthalten. Führen Sie die folgenden Befehle aus:

   ```
   cd /etc

   sudo tar -cvf mellon.tar mellon
   ```

   Kopieren Sie `mellon.tar` auf die zweite Instanz von Independent Gateway.

3. Gehen Sie auf der zweiten Instanz von Independent Gateway wie folgt vor:

   Extrahieren ("entpacken") Sie die tar-Datei auf der zweiten Instanz in das Verzeichnis `/etc`. Führen Sie die folgenden Befehle aus:

   ```
   cd /etc

   sudo tar -xvf mellon.tar
   ```

4. Auf Knoten 1 der Tableau Server-Bereitstellung: Aktualisieren Sie die Verbindungsdatei (`tsig.json`) mit den Verbindungsinformationen vom zweiten Independent Gateway. Sie müssen den Authentifizierungsschlüssel abrufen, wie zuvor in diesem Thema beschrieben (Installieren von Independent Gateway).

   Ein Beispiel für eine Verbindungsdatei (`tsig.json`) wird hier gezeigt:

   ```
   {
   "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. Auf Knoten 1 der Tableau Server-Bereitstellung: Führen Sie die folgenden Befehle aus, um die Konfiguration zu aktualisieren:

   ```
   tsm stop

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

   tsm start
   ```

6. Auf beiden Instanzen von Independent Gateway: Wenn Tableau Server gestartet wird, starten Sie den `tsig-httpd`-Prozess neu:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

7. In AWS **EC2>Target groups** (EC2 > Zielgruppen): Aktualisieren Sie die Zielgruppe so, dass sie die EC2-Instanz enthält, auf der die zweite Independent Gateway-Instanz ausgeführt wird.

   Wählen Sie die Zielgruppe aus, die Sie eben erstellt haben, und klicken Sie dann auf die Registerkarte "Targets" (Ziele):

   - Klicken Sie auf **Edit** (Bearbeiten).
   - Wählen Sie die EC2-Instanz des zweiten Independent Gateway-Computers aus und klicken Sie dann auf **Add to registered** (Zur registrierten hinzufügen). Klicken Sie dann auf **Speichern**.

Teil 6 - Konfiguration nach der Installation

Konfigurieren von SSL/TLS vom Lastenausgleichsmodul zu Tableau Server

Einige Organisationen verlangen eine Ende-zu-Ende-Verschlüsselung vom Client zum Backend-Dienst. Die bis hierhin beschriebene Standardreferenzarchitektur sieht SSL vom Client zum Lastenausgleich vor, der in der Webschicht Ihrer Organisation ausgeführt wird.

In diesem Abschnitt wird beschrieben, wie Sie SSL/TLS für Tableau Server und das Independent Gateway in der AWS-Beispielreferenzarchitektur konfigurieren. Ein Konfigurationsbeispiel, das beschreibt, wie SSL/TLS auf Apache in der AWS-Referenzarchitektur konfiguriert wird, finden Sie unter Beispiel: Konfigurieren von SSL/TLS in der AWS-Referenzarchitektur.

Auf den Back-End-Tableau Server-Prozesse, die in dem Bereich 8000 – 9000 ausgeführt werden, wird TLS zum gegenwärtigen Zeitpunkt nicht unterstützt. Um TLS zu aktivieren, müssen Sie Independent Gateway mit einer Relay-Verbindung zu Tableau Server konfigurieren.

In diesem Verfahren wird beschrieben, wie TLS im Independent Gateway in Tableau Server und von Tableau Server zum Independent Gateway aktiviert und konfiguriert wird. Das Verfahren verschlüsselt den Relay-Datenverkehr über HTTPS/443 und den Housekeeping-Datenverkehr über HTTPS/21319.

Die Linux-Beispiele in diesem Abschnitt zeigen Befehle für RHEL-ähnliche Distributionen. Die hier angegebenen spezifischen Befehle wurden mit der Amazon Linux 2-Distribution entwickelt. Wenn Sie die Ubuntu-Distribution ausführen, bearbeiten Sie die Befehle entsprechend.

Die hier aufgeführte Anleitung ist für die in diesem Leitfaden gezeigte AWS-Beispiel-Referenzarchitektur verbindlich. Daher sind optionale Konfigurationen nicht enthalten. Eine vollständige Referenzdokumentation finden Sie unter *Konfigurieren von TLS im Independent Gateway* (Linux).

Bevor Sie TLS konfigurieren

Führen Sie die TLS-Konfigurationen außerhalb der Geschäftszeiten durch. Die Konfiguration erfordert mindestens einen Neustart von Tableau Server. Wenn Sie eine vollständige Bereitstellung auf allen vier Knoten in der Referenzarchitektur ausführen, kann der Neustartvorgang eine Weile dauern.

- Stellen Sie sicher, dass Clients eine Verbindung zu Tableau Server über HTTP herstellen können. Das Konfigurieren von TLS mit Independent Gateway ist ein mehrstufiger Prozess, der auch Maßnahmen zur Fehlerbehebung beinhalten kann. Daher empfehlen wir, mit einer voll funktionsfähigen Tableau Server-Bereitstellung zu beginnen, bevor Sie TLS konfigurieren.

- Stellen Sie alle erforderlichen TLS/SSL-Zertifikate, Schlüssel und zugehörige Assets zusammen. SSL-Zertifikate werden Sie für die Independent Gateways und für Tableau Server benötigen. Zur Vereinfachung der Zertifikatsverwaltung und -bereitstellung sowie als bewährte Sicherheitspraxis empfehlen wir die Verwendung von Zertifikaten, die von einer bedeutenden vertrauenswürdigen Zertifizierungsstelle (CA) eines Drittanbieters erstellt wurden. Alternativ dazu können Sie auch selbstsignierte Zertifikate generieren oder Zertifikate von einer PKI für TLS verwenden.

  Die Beispielkonfiguration in diesem Thema verwendet die folgenden Asset-Namen zur besseren Veranschaulichung:
  - `tsig-ssl.crt`: Das TLS/SSL-Zertifikat für Independent Gateway.
  - `tsig-ssl.key`: Der private Schlüssel für `tsig-ssl.crt` auf Independent Gateway.
  - `ts-ssl.crt`: Das TLS/SSL-Zertifikat für Tableau Server.
  - `ts-ssl.key`: Der private Schlüssel für `tsig-ssl.crt` auf Tableau Server.

  - `tableau-server-CA.pem`: Das Stammzertifikat für die Zertifizierungsstelle, die die Zertifikate für die Tableau Server-Computer generiert. Dieses Zertifikat ist im Allgemeinen nicht erforderlich, wenn Sie Zertifikate von namhaften vertrauenswürdigen Drittparteien verwenden
  - `rootTSIG-CACert.pem`: Das Stammzertifikat für die Zertifizierungsstelle, die die Zertifikate für die Independent Gateway-Computer generiert. Dieses Zertifikat ist im Allgemeinen nicht erforderlich, wenn Sie Zertifikate von namhaften vertrauenswürdigen Drittparteien verwenden
  - Es gibt noch weitere Zertifikate und Schlüsseldatei-Assets, die für SAML erforderlich sind. Nähere Details dazu finden Sie in Teil 5 dieser Anleitung.
  - Wenn für Ihre Implementierung die Verwendung einer Zertifikatskettendatei erforderlich ist, finden Sie weitere Informationen dazu in dem Knowledgebase-Artikel Configure TLS on Independent Gateway when using a certificate that has a certificate chain (Konfigurieren von TLS für das Independent Gateway bei Verwendung eines Zertifikates mit einer Zertifikatskette).

- Stellen Sie sicher, dass Sie über Zugriff zum IdP verfügen. Wenn Sie für Authentifizierungszwecke einen IdP nutzen, müssen Sie wahrscheinlich Änderungen an den Empfänger- und Ziel-URLs beim IdP vornehmen, nachdem Sie SSL/TLS konfiguriert haben.

Konfigurieren der Independent Gateway-Computer für TLS

Das Konfigurieren von TLS kann ein fehleranfälliger Prozess sein. Da die Fehlerbehebung über zwei Instanzen von Independent Gateway zeitaufwändig sein kann, empfehlen wir, TLS in der EDG-Bereitstellung mit nur einem Independent Gateway zu aktivieren und zu konfigurieren. Nachdem Sie überprüft haben, dass TLS in der gesamten Bereitstellung funktioniert, konfigurieren Sie den zweiten Independent Gateway-Computer.

Schritt 1: Verteilen von Zertifikaten und Schlüsseln an den Independent Gateway-Computer

Sie können die Assets in ein beliebiges Verzeichnis verteilen, solange der Benutzer "tsig-httpd" über Lesezugriff auf die Dateien verfügt. Auf die Pfade zu diesen Dateien wird in

anderen Verfahren verwiesen. Wir werden die Beispielpfade unter `/etc/ssl`, wie unten gezeigt, im gesamten Thema verwenden.

1. Erstellen Sie ein Verzeichnis für den privaten Schlüssel:

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

2. Kopieren Sie die Zertifikat- und die Schlüsseldatei in die `/etc/ssl`-Pfade: Beispiel:

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

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

3. (Optional) Wenn Sie ein selbstsigniertes oder PKI-Zertifikat für SSL/TLS in Tableau Server verwenden, müssen Sie die Zertifizierungstellen-Stammzertifikatsdatei auch auf den Independent Gateway-Computer kopieren. Beispiel:

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

Schritt 2: Aktualisieren der Umgebungsvariablen für TLS

Sie müssen Port- und Protokoll-Umgebungsvariablen für die Konfiguration des Independent Gateways aktualisieren.

Ändern Sie diese Werte, indem Sie die Datei `/etc/opt/tableau/tableau_tsig/environment.bash` wie folgt aktualisieren:

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

Schritt 3: Aktualisieren der Stub-Konfigurationsdatei für das HK-Protokoll

Bearbeiten Sie manuell die Stub-Konfigurationsdatei (`/var/opt/tableau/tableau_tsig/config/httpd.conf.stub`), um TLS-bezügliche Apache-httpd-Anweisungen für das Housekeeping-Protokoll (HK) festzulegen.

Die Stub-Konfigurationsdatei enthält einen Block von TLS-bezogenen Anweisungen, die mit einer `#TLS#`-Markierung auskommentiert sind. Entfernen Sie die Markierungen in den Anweisungen, wie im Beispiel unten gezeigt. Beachten Sie, dass das Beispiel die Verwendung eines Stammzertifizierungsstellen-Zertifikats für das in Tableau Server verwendete SSL-Zertifikat mit der Option `SSLCACertificateFile` zeigt.

```
#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>
```

Wenn Sie Independent Gateway neu installieren, gehen diese Änderungen verloren. Wir empfehlen, eine Sicherungskopie anzufertigen.

Schritt 4: Kopieren der Stub-Datei und Neustarten des Dienstes

1. Kopieren Sie die Datei, die Sie im letzten Schritt aktualisiert haben, um "httpd.conf" mit den Änderungen zu aktualisieren:

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

2. Starten Sie den Independent Gateway-Dienst neu:

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

Nach dem Neustart bleibt das Independent Gateway solange außer Betrieb, bis Sie die nächsten Schritte in Tableau Server ausführen. Nachdem Sie die Schritte in Tableau Server aus-

geführt haben, übernimmt das Independent Gateway die Änderungen und wird online geschaltet.

Konfigurieren des Tableau Server-Knotens 1 für TLS

Führen Sie die folgenden Schritte auf Knoten 1 der Tableau Server-Bereitstellung aus:

Schritt 1: Kopieren der Zertifikate und Schlüssel und Stoppen von TSM

1. Stellen Sie sicher, dass Sie die "externen SSL"-Zertifikate und -Schlüssel von Tableau Server auf Knoten 1 kopiert haben.
2. Um die Ausfallzeit zu minimieren, empfehlen wir, TSM zu stoppen, die folgenden Schritte auszuführen und TSM dann zu starten, nachdem die Änderungen übernommen wurden:

   ```
   tsm stop
   ```

Schritt 2: Festlegen der Zertifikat-Assets und Aktivieren der Independent Gateway-Konfiguration

1. Geben Sie den Speicherort der Zertifikats- und Schlüsseldateien für Independent Gateway an. Diese Pfade verweisen auf den Speicherort auf Independent Gateway-Computern. Hinweis: In diesem Beispiel wird davon ausgegangen, dass für den Schutz von HTTPS- und Housekeeping-Datenverkehr dasselbe Zertifikat- und Schlüsselpaar verwendet wird:

   ```
   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. Aktivieren Sie TLS für HTTPS- und HK-Protokolle für Independent 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. (Optional) Wenn Sie in dem Independent Gateway ein selbstsigniertes oder PKI-Zertifikat für SSL/TLS verwenden, müssen Sie die Zertifizierungstellen-Stammzertifikatsdatei hochladen. Die Stammzertifikatdatei der Zertifizierungsstelle ist das Stammzertifikat, das verwendet wurde, um die Zertifikate für die Independent Gateway-Computer zu generieren. Beispiel:

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

4. (Optional) Wenn Sie ein selbstsigniertes oder PKI-Zertifikat für SSL/TLS in Tableau Server verwenden, müssen Sie die Zertifizierungstellen-Stammzertifikatdatei in das Independent Gateway-Verzeichnis `/etc/ssl/certs` kopieren. Die Stammzertifikatdatei der Zertifizierungsstelle ist das Stammzertifikat, das verwendet wurde, um die Zertifikate für die Tableau Server-Computer zu generieren. Nachdem Sie das Zertifikat zum Independent Gateway kopiert haben, müssen Sie den Speicherort des Zertifikats auf Knoten 1 mit dem folgenden tsm-Befehl angeben. Beispiel:

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

5. (Optional, nur zu Testzwecken:) Wenn Sie selbstsignierte oder PKI-Zertifikate computerübergreifend freigeben und daher die Antragstellernamen in den Zertifikaten nicht mit den Computernamen übereinstimmen, müssen Sie die Zertifikatsüberprüfung deaktivieren.

   ```
   tsm configuration set -k gateway.tsig.ssl.proxy.verify -v optio-
   nal_no_ca --force-keys
   ```

Schritt 3: Aktivieren von "externem SSL" für Tableau Server und Anwenden der Änderungen

1. Aktivieren und konfigurieren Sie "externes SSL" in Tableau Server:

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

2. Übernehmen Sie die Änderungen.

   ```
   tsm pending-changes apply
   ```

Schritt 4: Aktualisieren der Gateway-Konfigurations-JSON-Datei und Starten von TSM

1. Aktualisieren Sie die Konfigurationsdatei des Independent Gateways (z. B. `tsig.json`) auf der Tableau Server-Seite, um das`https`-Protokoll für die Independent Gateway-Objekte anzugeben:

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

2. Entfernen Sie die Verbindungsinformationen für die zweite Instanz von Independent Gateway (oder kommentieren Sie sie aus). Vergessen Sie nicht, den JSON in einem externen Editor zu überprüfen, bevor Sie ihn speichern.

   Nachdem Sie TLS für die einzelne Instanz von Independent Gateway konfiguriert und validiert haben, aktualisieren Sie diese JSON-Datei mit den Verbindungsinformationen für die zweite Instanz von Independent Gateway.

3. Führen Sie den folgenden Befehl aus, um die Independent Gateway-Konfiguration zu aktualisieren:

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

4. Starten Sie TSM.

   ```
   tsm start
   ```

5. Melden Sie sich während des Starts von TSM bei der Independent Gateway-Instanz an und starten Sie den`tsig-httpd`-Dienst:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

Aktualisieren der URLs des IdP-Authentifizierungsmoduls auf HTTPS

Wenn Sie einen externen Identitätsanbieter für Tableau konfiguriert haben, müssen Sie wahrscheinlich die Rückgabe-URLs im IdP-Verwaltungsdashboard aktualisieren.

Wenn Sie beispielsweise eine Vor-Authentifizierungsanwendung von Okta verwenden, müssen Sie die Anwendung so aktualisieren, dass das HTTPS-Protokoll für die Empfänger-URL und die Ziel-URL verwendet wird.

Konfigurieren von AWS-Lastenausgleich für HTTPS

Wenn Sie – wie in dieser Anleitung beschrieben – mit AWS-Lastenausgleich bereitstellen, ändern Sie die Konfiguration des AWS-Lastenausgleichs so, dass HTTPS-Datenverkehr an die Computer gesendet wird, auf denen Independent Gateway ausgeführt wird:

1. Löschen Sie die vorhandene HTTP-Zielgruppe:

   Wählen Sie in **Target Groups** (Zielgruppen) die HTTP-Zielgruppe aus, die für den Lastenausgleich konfiguriert wurde, klicken Sie auf **Actions** (Aktionen), und klicken Sie dann auf **Delete** (Löschen).

2. Erstellen Sie die HTTPS-Zielgruppe:

   Zielgruppen (Zielgruppen) > **Create target group** (Zielgruppe erstellen)

- Wählen Sie "Instances" (Instanzen) aus.
- Geben Sie einen Zielgruppennamen ein, zum Beispiel `TG-internal-HTTPS`.
- Wählen Sie Ihre VPC aus.
- Protokoll: HTTPS 443
- Fügen Sie unter **Health checks** (Integritätsprüfungen) > **Advanced health checks settings** (Einstellungen für erweiterte Integritätsprüfungen) > **Success codes** (Erfolgscodes) die Codeliste zum Lesen hinzu: `200,303`.
- Klicken Sie auf **Create** (Erstellen).

3. Wählen Sie die Zielgruppe aus, die Sie eben erstellt haben, und klicken Sie dann auf die Registerkarte **Targets** (Ziele):
   - Klicken Sie auf **Edit** (Bearbeiten).
   - Wählen Sie die EC2-Instanz aus, auf der das Tableau Server Independent Gateway ausgeführt wird, das Sie konfiguriert haben, und klicken Sie dann auf **Add to registered** (Zu registriert hinzufügen).
   - Klicken Sie auf **Save** (Speichern).

4. Nachdem die Zielgruppe erstellt wurde, müssen Sie "Stickiness" aktivieren:
   - Öffnen Sie die AWS-Seite für die Zielgruppe (**EC2** > **Load Balancing** (Lastenausgleich) > **Target groups** (Zielgruppen)), und wählen Sie die Zielgruppeninstanz aus, die Sie gerade eingerichtet haben. Wählen Sie im Menü **Actions** (Aktionen) die Option **Edit attributes** (Attribute bearbeiten) aus.
   - Wählen Sie auf der Seite **Edit attributes** (Attribute bearbeiten) die Option **Stickiness** (Bindung) aus, geben Sie eine Zeitdauer von `1 day` (1 Tag) an, und klicken Sie dann auf **Save changes** (Änderungen speichern).

5. Aktualisieren Sie für den Lastenausgleich die Listener-Regeln. Wählen Sie den Lastenausgleich aus, den Sie für diese Bereitstellung konfiguriert haben, und klicken Sie dann auf die Registerkarte **Listeners**.
   - Klicken Sie für **HTTP:80** auf **View/edit rules** (Regeln anzeigen/bearbeiten). Klicken Sie auf der Seite **Rules** (Regeln), die daraufhin angezeigt wird, auf das Bearbeitungssymbol (zuerst oben auf der Seite und dann noch einmal für die Regel), um die Regel zu bearbeiten. Löschen Sie die vorhandene THEN-Regel ("DANN") und ersetzen Sie sie, indem Sie auf **Add action** (Aktion hinzufügen) >

Redirect to... (Umleiten an...) klicken. Geben Sie in der daraus resultierenden THEN-Konfiguration `HTTPS` und Port `443` an und belassen Sie die anderen Optionen auf den Standardeinstellungen. Speichern Sie die Einstellung und klicken Sie dann auf **Update** (Aktualisieren).

- Klicken Sie für **HTTP:443** auf **View/edit rules** (Regeln anzeigen/bearbeiten). Klicken Sie auf der Seite **Rules** (Regeln), die daraufhin angezeigt wird, auf das Bearbeitungssymbol (zuerst oben auf der Seite und dann noch einmal für die Regel), um die Regel zu bearbeiten. Löschen Sie die vorhandene THEN-Regel ("DANN-Regel") und ersetzen Sie sie, indem Sie auf **Add action** (Aktion hinzufügen) > **Forward to...** (Weiterleiten an...) klicken. Geben Sie die Zielgruppe für die HTTPS-Gruppe an, die Sie gerade erstellt haben. Aktivieren Sie unter **Group-level stickiness** (Bindung auf Gruppenebene) den Punkt "Stickiness", und legen Sie "Duration" (Zeitdauer) auf "1 Day" (1 Tag) fest. Speichern Sie die Einstellung und klicken Sie dann auf **Update** (Aktualisieren).

6. Aktualisieren Sie für den Lastenausgleich das Leerlaufzeitlimit auf 400 Sekunden. Wählen Sie den Lastenausgleich, den Sie für diese Bereitstellung konfiguriert haben, und klicken Sie dann auf **Aktionen** > **Attribute bearbeiten**. Stellen Sie das **Leerlaufzeitlimit** auf `400` Sekunden ein und klicken Sie dann auf **Speichern**.

Validieren von TLS

Um die TLS-Funktionalität zu validieren, melden Sie sich bei Tableau Server mit der öffentlichen URL (z. B. https://tableau.example.com) mit dem Tableau-Administratorkonto an, das Sie zu Beginn dieses Verfahrens erstellt haben.

Wenn TSM nicht startet oder wenn Sie andere Fehlermeldungen erhalten, lesen Sie Fehlerbehebung beim Tableau Server Independent Gateway.

Konfigurieren der zweiten Instanz von Independent Gateway für SSL

Nachdem Sie die erste Instanz von Independent Gateway erfolgreich konfiguriert haben, stellen Sie die zweite Instanz bereit.

Der Prozess zum Bereitstellen des zweiten Independent Gateways erfordert die folgenden Schritte:

1. Auf der konfigurierten (ersten) Instanz von Independent Gateway: Kopieren Sie die folgenden Dateien in die entsprechenden Speicherorte auf der zweiten Instanz von Independent Gateway:
   - `/etc/ssl/certs/tsig-ssl.crt`
   - `/etc/ssl/private/tsig-ssl.key` (Sie werden auf der zweiten Instanz das Verzeichnis `private` erstellen müssen).
   - `/var/opt/tableau/tableau_tsig/config/httpd.conf.stub`
   - `/etc/opt/tableau/tableau_tsig/environment.bash`
2. Auf Knoten 1 der Tableau Server-Bereitstellung: Aktualisieren Sie die Verbindungsdatei (`tsig.json`) mit den Verbindungsinformationen vom zweiten Independent Gateway.

   Ein Beispiel für eine Verbindungsdatei (`tsig.json`) wird hier gezeigt:

   ```
   {
   "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. Auf Knoten 1 der Tableau Server-Bereitstellung: Führen Sie die folgenden Befehle aus, um die Konfiguration zu aktualisieren:

   ```
   tsm stop

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

   tsm start
   ```

4. Auf beiden Instanzen von Independent Gateway: Wenn Tableau Server gestartet wird, starten Sie den `tsig-httpd`-Prozess auf beiden Instanzen von Independent Gateway neu:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

5. In AWS **EC2>Target groups** (EC2 > Zielgruppen): Aktualisieren Sie die Zielgruppe so, dass sie die EC2-Instanz enthält, auf der die zweite Independent Gateway-Instanz ausgeführt wird.

   Wählen Sie die Zielgruppe aus, die Sie eben erstellt haben, und klicken Sie dann auf die Registerkarte "Targets" (Ziele):

   - Klicken Sie auf **Edit** (Bearbeiten).
   - Wählen Sie die EC2-Instanz des zweiten Independent Gateway-Computers aus und klicken Sie dann auf **Add to registered** (Zur registrierten hinzufügen). Klicken Sie dann auf **Speichern**.

Konfigurieren von SSL für Postgres

Optional können Sie SSL (TSL) für die Postgres-Verbindung für die externe Repository-Verbindung in Tableau Server konfigurieren.

Zur Vereinfachung der Zertifikatsverwaltung und -bereitstellung sowie als bewährte Sicherheitspraxis empfehlen wir die Verwendung von Zertifikaten, die von einer bedeutenden vertrauenswürdigen Zertifizierungsstelle (CA) eines Drittanbieters erstellt wurden. Alternativ dazu können Sie auch selbstsignierte Zertifikate generieren oder Zertifikate von einer PKI für TLS verwenden.

In diesem Verfahren wird beschrieben, wie Sie OpenSSL verwenden, um ein selbstsigniertes Zertifikat auf dem Postgres-Host auf einer RHEL-ähnlichen Linux-Distribution in der AWS-Referenzarchitektur zu erstellen.

Nachdem Sie das SSL-Zertifikat erzeugt und signiert haben, müssen Sie das CA-Zertifikat auf den Tableau-Host kopieren.

Führen Sie auf dem Host, auf dem Postgres ausgeführt wird, Folgendes durch:

1. Generieren Sie den Schlüssel der signierenden Stammzertifizierungsstelle (CA):

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

2. Erstellen Sie das Zertifikat der Stammzertifizierungsstelle:

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

   Sie werden aufgefordert, Werte für die Zertifikatfelder einzugeben. Beispiel:

   ```
   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. Erstellen Sie das Zertifikat und den zugehörigen Schlüssel (`server.csr` und `server.key` im Beispiel unten) für den Postgres-Computer. Der Antragstellername für das Zertifikat muss mit dem privaten DNS-Namen des Postgres-Hosts auf EC2 übereinstimmen. Der Antragstellername wird mit der Option `-subj` im Format "`/CN=<private DNS name>`" festgelegt, beispielsweise:

   ```
   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. Signieren Sie das neue Zertifikat mit dem CA-Zertifikat, das Sie in Schritt 2 erstellt haben. Der folgende Befehl gibt das Zertifikat auch im `crt`-Format aus:

   ```
   openssl x509 -req -in server.csr -days 3650 -CA pgsql-rootCACer-
   t.pem -CAkey pgsql-rootCAKey.pem -CAcreateserial -out ser-
   ver.crt
   ```

5. Kopieren Sie die .crt- und die .key-Datei in den Postgres-Pfad `/var/-lib/pgsql/13/data/`:

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

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

6. Schalten Sie auf Root-Benutzer um:

   ```
   sudo su
   ```

7. Legen Sie Berechtigungen für die .cer- und.key-Dateien fest. Führen Sie die folgenden Befehle aus:

   ```
   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. Aktualisieren Sie die pg_haba-Konfigurationsdatei `/var/lib/pgsql/13/data/pg_hba.conf`, um MD5-Trust anzugeben:

   Ändern Sie die vorhandenen Verbindungsanweisungen von

   `host all all 10.0.30.0/24 password` und

   `host all all 10.0.31.0/24 password`

   zu

   `host all all 10.0.30.0/24 md5` und

   `host all all 10.0.31.0/24 md5`.

9. Aktualisieren Sie die postgresql-Datei `/var/-lib/pgsql/13/data/postgresql.conf`, indem Sie diese Zeile hinzufügen:

   ```
   ssl = on
   ```

10. Beenden Sie den Root-Benutzer-Modus:

    ```
    exit
    ```

11. Starten Sie Postgres neu:

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

Optional: Aktivieren der Überprüfung der Vertrauenswürdigkeit von Zertifikaten in Tableau Server für Postgres SSL

Wenn Sie nach dem in Teil 4 – Installieren und Konfigurieren von Tableau Server aufgeführten Installationsverfahren vorgegangen sind, ist Tableau Server mit optionalem SSL für

die Postgres-Verbindung konfiguriert. Das bedeutet, die Konfiguration von SSL für Postgres (wie oben beschrieben) führt zu einer verschlüsselten Verbindung.

Wenn Sie möchten, dass die Überprüfung der Zertifikatvertrauenswürdigkeit für die Verbindung erforderlich sein soll, müssen Sie den folgenden Befehl in Tableau Server ausführen, um die Postgres-Host-Verbindung neu zu konfigurieren:

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

Dabei steht `<filename>.json` für die Verbindungsdatei, die in Konfigurieren von externem Postgres beschrieben wird. Und `CACert.pem` ist die Zertifizierungstellen-Zertifikatdatei für das von Postgres verwendete SSL/TLS-Zertifikat.

Optional: Überprüfen der SSL-Konnektivität

Um die SSL-Konnektivität zu überprüfen, müssen Sie wie folgt vorgehen:

- Installieren Sie den Postgres-Client auf Tableau Server-Knoten 1.
- Kopieren Sie das Stammzertifikat, das Sie in dem vorherigen Verfahren erstellt haben, auf den Tableau-Host.
- Stellen Sie eine Verbindung zum Postgres-Server vom Knoten 1 aus her.

Installieren des Postgres-Clients auf Knoten 1

Dieses Beispiel zeigt, wie Postgres der Version 13.4 installiert wird. Installieren Sie die gleiche Version, die Sie für das externe Repository ausführen.

1. Auf Knoten 1: Erstellen und bearbeiten Sie die Datei "pgdg.repo" im Pfad `/etc/yum.repos.d`. Füllen Sie die Datei mit den folgenden Konfigurationsinformationen auf.

   ```
   [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
```

2. Installieren des Postgres-Clients:

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

Kopieren des Stammzertifikats auf Knoten 1

Kopieren Sie das Zertifizierungsstellen-Zertifikat (`pgsql-rootCACert.pem`) auf den Tableau-Host:

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

Herstellen einer SSL-Verbindung vom Knoten 1 aus zum Postgres-Host

Führen Sie den folgenden Befehl auf dem Knoten 1 aus, mit dem Sie die IP-Adresse des Postgres-Server-Hosts und das Stammzertifizierungsstellen-Zertifikat angeben:

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

Beispiel:

```
 psql "post-
gresql://postgres@10.0.1.189:5432/postgres?sslmode=verify-ca&ssl-
rootcert=pgsql-rootCACert.pem"
```

Postgres fordert Sie zur Eingabe des Kennworts auf. Nach erfolgreicher Anmeldung gibt die Shell Folgendes zurück:

```
psql (13.4)
SSL connection (protocol: TLSv1.2, cipher: ECDHE-RSA-AES256-GCM-
```

```
SHA384, bits: 256, compression: off)
Type "help" for help.
postgres=#
```

Konfigurieren von SMTP- und Ereignisbenachrichtigungen

Tableau Server sendet E-Mail-Benachrichtigungen an Administratoren und Benutzer. Um dies zu aktivieren, müssen Sie Tableau Server so konfigurieren, dass E-Mails an Ihren E-Mail-Server gesendet werden. Sie müssen auch die Ereignistypen, Schwellenwerte und die Subscription-Informationen angeben, die gesendet werden sollen.

Für die Ausgangskonfiguration von SMTP und Benachrichtigungen wird empfohlen, dass Sie die unten gezeigte Konfigurationsdatei als Vorlage zum Erstellen einer JSON-Datei verwenden. Sie können auch jeden einzelnen Konfigurationsschlüssel mit der in *tsm configuration set* (Linux) beschriebenen Syntax festlegen.

Führen Sie dieses Verfahren auf Knoten 1 in Ihrer Tableau Server-Bereitstellung aus:

1. Kopieren Sie folgende JSON-Vorlage in eine Datei. Passen Sie die Datei mit Ihren SMTP-Konfigurationsoptionen und den Subscription- und Warnbenachrichtigungen für Ihre Organisation an.
    - Eine Liste und Beschreibung aller SMTP-Optionen finden Sie in der *Referenz zur SMTP-CLI-Konfiguration* (Linux).
    - Eine Liste und Beschreibung aller Optionen für Benachrichtigungsereignisse finden Sie im CLI-Abschnitt von *Konfigurieren von Servereignisbenachrichtigungen* (Linux).

```
{
"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. Führen Sie den Befehl `tsm settings import -f file.json` aus, um die JSON-Datei an Tableau Services Manager zu übergeben.
3. Führen Sie den Befehl `tsm pending-changes apply` aus, um die Änderungen anzuwenden.
4. Führen Sie `tsm email test-smtp-connection` aus, um die Verbindungskonfiguration anzuzeigen und zu verifizieren.

Installieren des PostgreSQL-Treibers

Um Verwaltungsansichten in Tableau Server anzuzeigen, muss der PostgreSQL-Treiber auf dem Knoten 1 der Tableau Server-Bereitstellung installiert werden.

1. Rufen Sie die Tableau-Seite Treiber herunterladen auf und kopieren Sie die URL für die PostgreSQL-JAR-Datei.

2. Führen Sie das folgende Verfahren auf jedem Knoten der Tableau-Bereitstellung aus:

   - Erstellen Sie den folgenden Dateipfad:

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

   - Laden Sie die neueste Version der PostgreSQL-JAR-Datei in den neuen Pfad herunter: Beispiel:

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

3. Starten Sie Tableau Server auf dem Ausgangsknoten neu:

   ```
   tsm restart
   ```

Konfigurieren der Richtlinie für starke Kennwörter

Wenn Sie Tableau Server nicht mit einer IdP-Authentifizierungslösung bereitstellen, empfehlen wir, die Sicherheit der standardmäßigen Tableau-Kennwortrichtlinie zu erhöhen.

Wenn Sie Tableau Server mit einem IdP bereitstellen, müssen Sie Kennwortrichtlinien mit dem IdP verwalten.

Das folgende Verfahren umfasst die JSON-Konfiguration für die Einstellung der Kennwortrichtlinie auf Tableau Server. Weitere Informationen zu den folgenden Optionen finden Sie unter *Lokale Authentifizierung* (Linux).

1. Kopieren Sie folgende JSON-Vorlage in eine Datei. Geben Sie als Schlüsselwerte die Konfiguration Ihrer Kennwortrichtlinien ein.

```
{
 "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. Führen Sie den Befehl `tsm settings import -f file.json` aus, um die JSON-Datei an Tableau Services Manager zu übergeben, um Tableau Server zu konfigurieren.

3. Führen Sie den Befehl `tsm pending-changes apply` aus, um die Änderungen anzuwenden.

Teil 7 - Überprüfung, Tools und Fehlerbehebung

Dieser Teil enthält Schritte zur Überprüfung nach einer Installation sowie Anleitungen zur Fehlerbehebung.

Überprüfung der Failover-Funktionalität des Systems

Nachdem Sie Ihre Bereitstellung konfiguriert haben, empfiehlt es sich, einfache Failover-Tests durchzuführen, um die Systemredundanz zu überprüfen.

Wir empfehlen, die folgenden Schritte durchzuführen, um die Failover-Funktionalität zu überprüfen:

1. Fahren Sie die erste Instanz von Independent Gateway (TSIG1) herunter. Sämtlicher eingehender Datenverkehr sollte über die zweite Instanz von Independent Gateway (TSIG2) geleitet werden.
2. Starten Sie TSIG1 neu, und fahren Sie dann TSIG2 herunter. Sämtlicher eingehender Datenverkehr sollte über die TSIG1 geleitet werden.
3. Starten Sie TSIG2 neu.

4. Fahren Sie Tableau Server-Knoten 1 herunter. Sämtlicher Vizportal/Application Server-Datenverkehr wird auf den Knoten 2 verlegt ("Failover").

   Hinweis: Ab September 2022 gilt die Hochverfügbarkeit von Knoten 1 in bestimmten Versionen von Tableau Server 2021.4 (und höher) als kompromittiert. Client-Verbindungen schlagen fehl, wenn Knoten 1 heruntergefahren ist. Dieses Problem wurde in den folgenden Wartungsupdates behoben:

– 2021.4.15 (und höher)
– 2022.1.11 (und höher)
– 2023.1.3 (und höher)

Um sicherzustellen, dass Ihre Tableau Server-Installation mit ATR-Aktivierungen nach einem Ausfall des Primärknotens über eine Toleranzfrist von 72 Stunden verfügt, installieren Sie oder führen Sie ein Upgrade auf eine dieser Versionen durch. Weitere Einzelheiten finden Sie unter Tableau Server-Hochverfügbarkeits-Cluster mit ATR hat keine Toleranzfrist nach dem Ausfall des Anfangsknotens in der Tableau-Knowledgebase.

5. Starten Sie Knoten 1 neu, und fahren Sie Knoten 2 herunter. Sämtlicher Vizportal/Application Server-Datenverkehr wird auf den Knoten 1 verlegt ("Failover").
6. Starten Sie Knoten 2 neu.

In diesem Kontext erfolgt das "Herunterfahren" oder "Neustarten", indem das Betriebssystem oder der virtuelle Computer (VM) ausgeschaltet wird, ohne dass zuvor versucht wird, die Anwendung sauber herunterzufahren. Auf diese Weise soll ein Ausfall der Hardware oder des virtuellen Computers (VM) simuliert werden.

Der für jeden Failover-Test mindestens erforderliche Validierungsschritt besteht darin, sich als ein Benutzer zu authentifizieren und grundlegende Anzeigevorgänge durchzuführen.

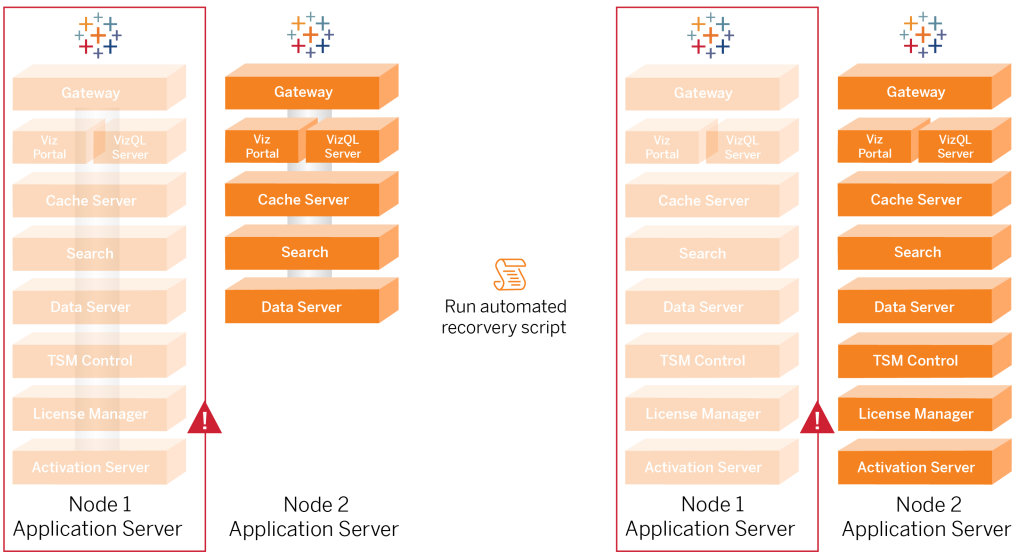
Es kann sein, dass Sie einen Browserfehler vom Typ "Bad Request" (Ungültige Anforderung) erhalten, wenn Sie versuchen, sich nach einem simulierten Ausfall anzumelden. Diese Fehlermeldung wird möglicherweise auch dann noch angezeigt, nachdem Sie den Cache in Ihrem Browser geleert haben. Dieses Problem tritt häufig auf, wenn der Browser Daten aus einer vorherigen IdP-Sitzung zwischenspeichert. Sollte dieser Fehler auch dann noch auftreten, nachdem Sie den lokalen Browser-Cache gelöscht haben, validieren Sie das Tableau-Szenario, indem Sie eine Verbindung mit einem anderen Browser herstellen.

Automatische Wiederherstellung des Anfangsknotens

Tableau Server 2021.2.4 (und höher) enthält ein Skript für die automatisierte Wiederherstellung des Anfangsknotens (`auto-node-recovery`), das sich im Skriptverzeichnis (`/app/tableau_server/packages/scripts.<version>`) befindet.

Wenn es ein Problem mit dem Anfangsknoten gibt und redundante Prozesse auf Knoten 2 vorhanden sind, gibt es keine Garantie, dass Tableau Server weiterhin ausgeführt wird. Tableau Server kann bis zu 72 Stunden nach einem Ausfall des Anfangsknotens weiter ausgeführt werden, bevor sich das Fehlen des Lizenzierungsdienstes auf andere Prozesse auswirkt. Wenn dies der Fall ist, können sich Ihre Benutzer nach dem Ausfall des Anfangsknotens zwar weiterhin anmelden und ihre Inhalte anzeigen und verwenden. Sie können Tableau Server jedoch nicht neu konfigurieren, da Sie keinen Zugriff auf den Administration Controller haben.

Auch bei Konfiguration mit redundanten Prozessen ist es möglich, dass Tableau Server nach dem Ausfall des Anfangsknotens nicht mehr funktioniert.



So stellen Sie den Anfangsknoten (Knoten 1) nach einem Ausfall wieder her:

1. Melden Sie sich auf dem Tableau Server-Knoten 2 an.
2. Wechseln Sie in das Skriptverzeichnis:

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

3. Führen Sie den folgenden Befehl aus, um das Skript zu starten:

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

   Dabei steht `<license keys>` für eine durch Kommas getrennte Liste (keine Leerzeichen) der Lizenzschlüssel für Ihre Bereitstellung. Wenn Sie keinen Zugriff auf Ihre Lizenzschlüssel haben, rufen Sie aus dem Tableau-Kundenportal ab. Beispiel:

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

Das Skript zur automatischen Knotenwiederherstellung (auto-node-recovery) führt dann rund 20 Schritte aus, um Dienste auf dem Knoten 2 wiederherzustellen. Jeder einzelne Schritt wird während der Ausführung des Skripts im Terminal angezeigt. Ausführlichere Statusinformationen werden in `/data/tableau_data/logs/app-controller-move.log` protokolliert. In den meisten Umgebungen benötigt das Skript zwischen 35 und 45 Minuten, bis es fertig ist.

Fehlerbehebung bei einer Wiederherstellung des Anfangsknotens

Wenn die Knotenwiederherstellung fehlschlägt, ist es möglicherweise hilfreich, das Skript interaktiv auszuführen, um einzelne Schritte im Prozess zuzulassen oder zu verbieten. Beispiel: Wenn das Skript während der Ausführung fehlschlägt, können Sie die Protokolldatei überprüfen, Änderungen an der Konfiguration vornehmen und das Skript dann erneut ausführen. Durch Ausführen im interaktiven Modus können Sie dann alle Schritte überspringen, bis Sie zu dem Schritt gelangen, in dem der Fehler aufgetreten ist.

Um das Skript im interaktiven Modus auszuführen, fügen Sie dem Skriptargument den Schalter `-i` hinzu.

Wiederherstellung des fehlgeschlagenen Knotens

Nachdem Sie das Skript ausgeführt haben, führt Knoten 2 alle Dienste aus, die zuvor auf dem ausgefallenen Host von Knoten 1 ausgeführt wurden. Um Knoten 4 hinzuzufügen, müssen Sie einen neuen Tableau Server-Host mit der Bootstrap-Datei bereitstellen und ihn so konfigurieren, wie Sie es für den ursprünglichen Knoten 2 getan haben, wie in Teil 4 beschrieben. Siehe Konfigurieren von Knoten 2.

Switchto

Switchto ist ein Shell-Skript von Tim, das den Wechsel zwischen Fenstern erleichtert.

1. Kopieren Sie den folgenden Code in eine Datei namens `switchto` im Basisverzeichnis auf Ihrem Bastion-Host.

```
#!/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. Ändern Sie die IP-Adressen im Skript so, dass sie mit Ihren EC2-Instanzen übereinstimmen, und speichern Sie dann die Datei.
3. Wenden Sie Berechtigungen auf die Skriptdatei an:

   ```
   sudo chmod +x switchto
   ```

Verwendung:

Um zu einem Host umzuschalten, führen Sie den folgenden Befehl aus:

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

Wenn Sie zum Beispiel zum Knoten 1 umschalten möchten, führen Sie den folgenden Befehl aus:

```
./switchto node1
```

Fehlerbehebung beim Tableau Server Independent Gateway

Das Konfigurieren von Independent Gateway, Okta, Mellon und SAML in Tableau Server kann ein fehleranfälliger Prozess sein. Die häufigste Fehlerursache sind Zeichenfolgenfehler. So kann zum Beispiel ein nachgestellter Schrägstrich (`/`) in den Okta-URLs, die während der Konfiguration angegeben wurden, einen Nichtübereinstimmungsfehler in Bezug auf SAML-Assertion verursachen. Dies ist nur ein Beispiel. Es gibt viele Möglichkeiten während der Konfiguration, bei einer der Anwendungen eine falsche Zeichenfolge einzugeben.

Neustarten des tableau-tsig-Dienstes

Beginnen (und beenden) Sie die Fehlerbehebung immer mit einem Neustart des tableau-tsig-Dienstes auf den Independent Gateway-Computern. Das Neustarten dieses Dienstes geht schnell und bewirkt meist, dass die aktualisierte Konfiguration von Tableau Server geladen wird.

Führen Sie die folgenden Befehle auf dem Independent Gateway-Computer aus:

```
sudo su - tableau-tsig

systemctl --user restart tsig-httpd

exit
```

Auffinden falscher Zeichenfolgen

Wenn Sie einen Zeichenfolgenfehler gemacht haben (Fehler beim Kopieren/Einfügen, Zeichenfolge abgeschnitten usw.), nehmen Sie sich die Zeit, alle von Ihnen konfigurierten Einstellungen durchzugehen:

- Die Konfiguration der Okta-Vorauthentifizierung. Überprüfen Sie sorgfältig die von Ihnen festgelegten URLs. Suchen Sie nach abschließenden Schrägstrichen. Prüfen Sie auf HTTP anstelle von HTTPS.

- Shell-Verlauf für die SAML-Konfiguration auf Knoten 1. Überprüfen Sie den Befehl `tsm authentication saml configure`, den Sie ausgeführt haben. Stellen Sie sicher, dass alle URLs mit denen übereinstimmen, die Sie in Okta konfiguriert haben. Vergewissern Sie sich beim Überprüfen des Shell-Verlaufs von Knoten 1, dass die `tsm configuration set`-Befehle, die die Mellon-Konfigurationsdateipfade angeben, exakt mit den Dateipfaden übereinstimmen, in die Sie die Dateien in Independent Gateway kopiert haben.
- Die Mellon-Konfiguration in Independent Gateway. Überprüfen Sie den Shell-Verlauf, um sicherzustellen, dass Sie die Metadaten mit der gleichen URL-Zeichenfolge erstellt haben, die Sie in Okta und Tableau-SAML konfiguriert haben. Stellen Sie sicher, dass alle Pfade, die in `/etc/mellon/conf.d/global.conf` angegeben sind, korrekt sind und dass die `MellonCookieDomain` auf Ihre Stammdomäne festgelegt ist, nicht auf Ihre Tableau-Unterdomäne.

Durchsuchen relevanter Protokolle

Wenn alle Zeichenfolgen korrekt zu sein scheinen, sollten Sie die Protokolle auf Fehler überprüfen.

Tableau Server protokolliert Fehler und Ereignisse in Dutzenden verschiedener Protokolldateien. Auch Independent Gateway protokolliert in einer Reihe lokaler Dateien. Wir empfehlen, diese Protokolle in der folgenden Reihenfolge zu überprüfen.

Independent Gateway-Protokolldateien

Der standardmäßige Speicherort der Protokolldateien des Independent Gateway lautet `/var/opt/tableau/tableau_tsig/logs`.

- `access.log`: Dieses Protokoll ist insofern nützlich, als es Einträge enthält, die Verbindungen von den Tableau Server-Knoten anzeigen. Wenn Sie bei dem Versuch, TSM zu starten, Gateway-Fehler erhalten ("...startet nicht"), und es keine Einträge in der Datei `access.log` gibt, liegt ein grundlegendes Konnektivitätsproblem vor. Überprüfen Sie als ersten Schritt immer die Konfiguration der AWS-Sicherheitsgruppe. Ein weiteres häufiges Problem ist ein Schreibfehler in `tsig.json`. Wenn Sie in tsig.json eine Änderung vornehmen, führen Sie `tsm stop` aus, bevor Sie `tsm topology external-services gateway update -c tsig.json` ausführen. Nachdem tsig.json

aktualisiert wurde, führen Sie `tsm start` aus.
- `error.log`: Neben anderen Einträgen werden in diesem Protokoll auch SAML- und Mellon-Fehler verzeichnet.

Protokolldatei von Tableau Server-tabadminagent

Die `tabadminagent`-Dateien (nicht `tabadmincontroller`) sind die einzigen relevanten Protokolldateien für die Behebung von Fehlern im Zusammenhang mit Independent Gateway.

Sie müssen herausfinden, wo Independent Gateway-Fehler in `tabdminagent` protokolliert wurden. Diese Fehler können auf jedem beliebigen Knoten, aber nur auf einem einzigen Knoten auftreten. Führen Sie die folgenden Schritte auf jedem Knoten im Tableau Server-Cluster durch, bis Sie die Zeichenfolge "independent" finden:

1. Suchen Sie den Speicherort der tabadminagent-Protokolldatei auf den Tableau Server-Knoten 1–4 im EDG-Setup:

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

2. Öffnen Sie das neueste Protokoll, in dem Folgendes steht:

   ```
   less tabadminagent_nodeN.log
   ```

   (Ersetzen Sie "N" durch die Knotennummer.)

3. Suchen Sie nach allen Stellen, an denen "Independent" oder "independent" steht, indem Sie die folgende Suchzeichenfolge verwenden:

   ```
   /ndependent
   ```

   Wenn es keine Treffer gibt, gehen Sie zum nächsten Knoten und wiederholen Sie die Schritte 1–3.

4. Wenn Sie einen Treffer erhalten: Drücken Sie die Tastenkombination `Shift + G`, um nach unten zu den letzten Fehlermeldungen zu gelangen.

Neuladen der httpd-Stub-Datei

Independent Gateway verwaltet die Konfiguration von httpd für Apache. Eine allgemeine Methode, mit der sich vorübergehende Probleme oftmals beheben lassen, ist die httpd-Stub-Datei neu zu laden, aus der die zugrunde liegende Apache-Konfiguration stammt. Führen Sie auf beiden Instanzen von Independent Gateway die folgenden Befehle aus.

1. Kopieren Sie die Stub-Datei herüber zu httpd.conf:

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

2. Starten Sie den Independent Gateway-Dienst neu:

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

Löschen oder Verschieben von Protokolldateien

Independent Gateway protokolliert sämtliche Zugriffsereignisse. Um zu verhindern, dass dabei der gesamte Festplattenplatz belegt wird, müssen Sie die Protokolldateispeicherung verwalten. Wenn Ihre Festplatte voll wird, kann Independent Gateway keine Zugriffsereignisse mehr protokollieren und stellt den Betrieb mit einem Fehler ein. Die folgende Meldung wird in "error.log" in Independent Gateway protokolliert:

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

Dieser Fehler führt zum Status `DEGRADED` für den `external` Knoten, wenn Sie `tsm status -v` auf Tableau-Knoten 1 ausführen. Der Knoten `external` in der Statusmeldung bezieht sich auf Independent Gateway.

Um dieses Problem zu beheben, müssen Sie die "access.log"-Dateien auf der Festplatte löschen. Die "access.log"-Dateien werden unter `/var/opt/tableau/tableau_`

`tsig/logs` gespeichert. Nachdem Sie Platz auf der Festplatte geschaffen haben, starten Sie den tableau-tsig-Dienst neu.

Browserfehler

Bad Request: Ein häufiger Fehler in diesem Szenario ist ein Fehler vom Typ "Bad Request" (Ungültige Anforderung) von Okta. Dieses Problem tritt häufig auf, wenn der Browser Daten aus einer früheren Okta-Sitzung zwischenspeichert. Wenn Sie beispielsweise die Okta-Anwendungen als Okta-Administrator verwalten und dann versuchen, mit einem anderen Okta-fähigen Konto auf Tableau zuzugreifen, können Sitzungsdaten aus den Administratordaten den Fehler "Bad Request" verursachen. Wenn dieser Fehler auch dann noch auftritt, wenn Sie den lokalen Browser-Cache löschen, versuchen Sie, das Tableau-Szenario zu validieren, indem Sie eine Verbindung mit einem anderen Browser herstellen.

Eine weitere Ursache für Fehler vom Typ "Bad Request" (ungültige Anforderung) sind Schreibfehler in einer der vielen URLs, die Sie während der Okta-, Mellon- und SAML-Konfigurationsprozesse eingeben. Überprüfen Sie, ob Sie diese alle fehlerfrei eingegeben haben.

Oftmals gibt die Datei `error.log` auf dem Independent Gateway-Server an, welche URL den Fehler verursacht.

Not Found – The requested URL was not found on this server: Diese Fehlermeldung weist auf einen von vielen Konfigurationsfehlern hin.

Wenn der Benutzer mit Okta authentifiziert ist und dann diese Fehlermeldung erhält, haben Sie wahrscheinlich die Vor-Authentifizierungsanwendung von Okta bei der Konfiguration von SAML auf Tableau Server hochgeladen. Stellen Sie sicher, dass Sie die Metadaten der Tableau Server-Anwendung von Okta auf Tableau Server konfiguriert haben und nicht die Metadaten der Vor-Authentifizierungsanwendung von Okta.

Weitere Fehlerbehebungsschritte

- Überprüfen Sie die Einstellungen der Vor-Authentifizierungsanwendung von Okta. Stellen Sie sicher, dass die Protokolle HTTP und HTTPS wie in diesem Thema beschrieben festgelegt sind.

- Starten Sie tsig-httpd auf beiden Independent Gateway-Servern neu.
- Überprüfen Sie, ob `sudo apachectl configtest` auf beiden Independent Gateways die Meldung "Syntax OK" zurückgibt.
- Stellen Sie sicher, dass der Testbenutzer in Okta beiden Anwendungen zugewiesen ist.
- Stellen Sie sicher, dass "Stickiness" für das Lastenausgleichsmodul und die zugehörigen Zielgruppen aktiviert ist.

Überprüfen der TLS-Verbindung von Tableau Server zu Independent Gateway

Verwenden Sie den `wget`-Befehl, um die Konnektivität und den Zugriff von Tableau Server zu Independent Gateway zu überprüfen. Variationen dieses Befehls können Ihnen helfen zu verstehen, ob Verbindungsprobleme aus Problemen mit Zertifikaten resultieren.

Führen Sie zum Beispiel diesen `wget`-Befehl aus, um das Housekeeping-Protokoll (HK) von Tableau Server zu überprüfen:

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

Erstellen Sie die URL mit derselben Hostadresse, die Sie für die Hostoption der Datei "tsig.json" angegeben haben. Geben Sie das `https`-Protokoll an und fügen Sie die URL mit dem HK-Port `21319` an.

So überprüfen Sie die Konnektivität und ignorieren die Zertifikatsüberprüfung:

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

So überprüfen Sie, ob das Stammzertifizierungsstellenzertifikat für TSIG gültig ist:

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

Wenn Tableau in der Lage ist, zu kommunizieren, werden Ihnen möglicherweise noch inhaltsbezogene Fehler gemeldet, aber keine verbindungsbezogenen Fehler. Wenn Tableau überhaupt keine Verbindung herstellen kann, überprüfen Sie zunächst die Protokollkonfiguration in

den Firewall-/Sicherheitsgruppen. So müssen zum Beispiel die Regeln für eingehenden Datenverkehr für die Sicherheitsgruppe, in der sich Independent Gateway befindet, TCP 21319 zulassen.

Anhang – AWS Deployment Toolbox

Dieses Thema umfasst Tools und alternative Bereitstellungsoptionen für die Referenzarchitektur, wenn diese in AWS bereitgestellt wird. In diesem Thema wird insbesondere beschrieben, wie die im Bereitstellungshandbuch beschriebene AWS-Bereitstellung automatisiert werden kann.

TabDeploy4EDG – Skript für automatisierte Installation

Das TabDeploy4EDG-Skript automatisiert die Implementierung der Tableau-Bereitstellung mit vier Knoten, die in Teil 4 – Installieren und Konfigurieren von Tableau Server beschrieben wird. Wenn Sie die in diesem Leitfaden beschriebene AWS-Beispielimplementierung verwenden, können Sie TabDeploy4EDG ausführen.

Anforderungen: Um das Skript auszuführen, müssen Sie die AWS-Umgebung gemäß der Beispielimplementierung in Teil 3 - Vorbereiten der Bereitstellung von Tableau Server Enterprise vorbereiten und konfigurieren:

- VPC, Subnetz und Sicherheitsgruppen wurden wie beschrieben konfiguriert. IP-Adressen müssen nicht mit den in der Beispielimplementierung angegebenen Adressen übereinstimmen.
- Vier EC2-Instanzen, auf denen die neuesten, aktualisierten Builds von AWS Linux 2 ausgeführt werden
- PostgreSQL ist installiert und wurde wie unter Installieren, Konfigurieren und Anfertigen einer tar-Sicherung von PostgreSQL beschrieben konfiguriert.
- Eine tar-Sicherungsdatei für Schritt 1 befindet sich auf der EC2-Instanz, auf der PostgreSQL installiert ist, wie in Anfertigen einer "Schritt 1"-tar-Sicherung von PostgreSQL beschrieben.
- Die EC2-Instanz, auf der der Knoten 1 der Tableau Server-Bereitstellung ausgeführt werden soll, wurde für die Kommunikation mit PostgreSQL konfiguriert, wie unter Teil 4 – Installieren und Konfigurieren von Tableau Server beschrieben.

- Sie haben sich bei jeder EC2-Instanz mit einer SSH-Sitzung vom Bastion-Host aus angemeldet.

Das Skript braucht rund 1,5 bis 2 Stunden, um die vier Tableau-Server zu installieren und zu konfigurieren. Das Skript konfiguriert Tableau gemäß den vorgeschriebenen Einstellungen der Referenzarchitektur. Das Skript führt die folgenden Aktionen aus:

- Stellt die Sicherung der Stufe 1 des PostgreSQL-Hosts wieder her, wenn Sie einen Pfad zur tar-Datei des PostgreSQL-Hosts angeben.
- Es entfernt vorhandene Tableau-Installationen auf allen Knoten.
- Es führt den Befehl `sudo yum update` auf allen Knoten aus.
- Es lädt das Tableau-RPM-Paket herunter und kopiert es auf jeden Knoten.
- Es lädt Abhängigkeiten auf jeden Knoten herunter und installiert sie.
- Es erstellt `/app/tableau_server` und installiert das Paket auf allen Knoten.
- Es installiert Knoten 1 mit einem lokalen Identitätsspeicher und konfiguriert ein externes Repository mit PostgreSQL.
- Es führt die Bootstrap-Installation und die Erstkonfiguration von Knoten 2 bis Knoten 4 durch.
- Löscht die Bootstrap-Datei und die Konfigurationsdatei für TabDeploy4EDG.
- Es konfiguriert Dienste im gesamten Tableau-Cluster gemäß den Spezifikationen der Referenzarchitektur.
- Validiert die Installation und gibt den Status für jeden Knoten zurück.

Herunterladen und Kopieren des Skripts auf den Bastion-Host

1. Kopieren Sie das Skript auf der TabDeploy4EDG-Beispielseite und fügen Sie den Code in eine Datei namens `TabDeploy4EDG` ein.
2. Speichern Sie die Datei im Basisverzeichnis auf dem EC2-Host, der als Bastion-Host dient.
3. Führen Sie den folgenden Befehl aus, um den Modus der Datei so zu ändern, dass sie ausgeführt werden kann:

```
sudo chmod +x TabDeploy4EDG
```

Ausführen von TabDeploy4EDG

TabDeploy4EDG muss auf dem Bastion-Host ausgeführt werden. Das Skript wurde unter der Annahme geschrieben, dass Sie im Kontext des ssh-Forward-Agenten arbeiten, wie unter Beispiel: Herstellen einer Verbindung mit dem Bastion-Host in AWS beschrieben. Wenn Sie nicht mit ssh-Forward-Agent-Kontext arbeiten, werden Sie während des gesamten Installationsprozesses zur Eingabe von Kennwörtern aufgefordert.

1. Erstellen, bearbeiten und speichern Sie eine Registrierungsdatei (`registration.json`). Die Datei muss eine ordnungsgemäß formatierte JSON-Datei sein. Kopieren Sie die folgende Vorlage und passen Sie sie an:

   ```
   {
          "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. Führen Sie den folgenden Befehl aus, um eine Beispielkonfigurationsdatei zu erstellen:

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

3. Öffnen Sie die Konfigurationsdatei zum Bearbeiten:

   ```
   sudo nano edg.config
   ```

   Sie müssen mindestens die IP-Adressen der einzelnen EC2-Hosts, einen Dateipfad zur Registrierungsdatei und einen gültigen Lizenzschlüssel hinzufügen.

4. Wenn Sie mit dem Bearbeiten der Konfigurationsdatei fertig sind, speichern und schließen Sie sie.

5. Führen Sie TabDeploy4EDG mit dem folgenden Befehl aus:

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

Beispiel: Automatisieren der Bereitstellung einer AWS-Infrastruktur mit Terraform

In diesem Abschnitt wird beschrieben, wie Terraform konfiguriert und ausgeführt wird, um die EDG-Referenzarchitektur in AWS bereitzustellen. Die hier vorgestellte Terraform-Beispielkonfiguration stellt einen AWS VPC mit den Subnetzen, Sicherheitsgruppen und EC2-Instanzen bereit, die in Teil 3 - Vorbereiten der Bereitstellung von Tableau Server Enterprise beschrieben werden.

Terraform-Beispielvorlagen sind auf der Tableau-Website für Beispiele unter https://help.tableau.com/samples/en-us/edg/edg-terraform.zip verfügbar. Diese Vorlagen müssen für Ihre Organisation konfiguriert und angepasst werden. Der in diesem Abschnitt bereitgestellte Konfigurationsinhalt beschreibt die mindestens erforderlichen Vorlagenänderungen, die Sie für die Bereitstellung anpassen müssen.

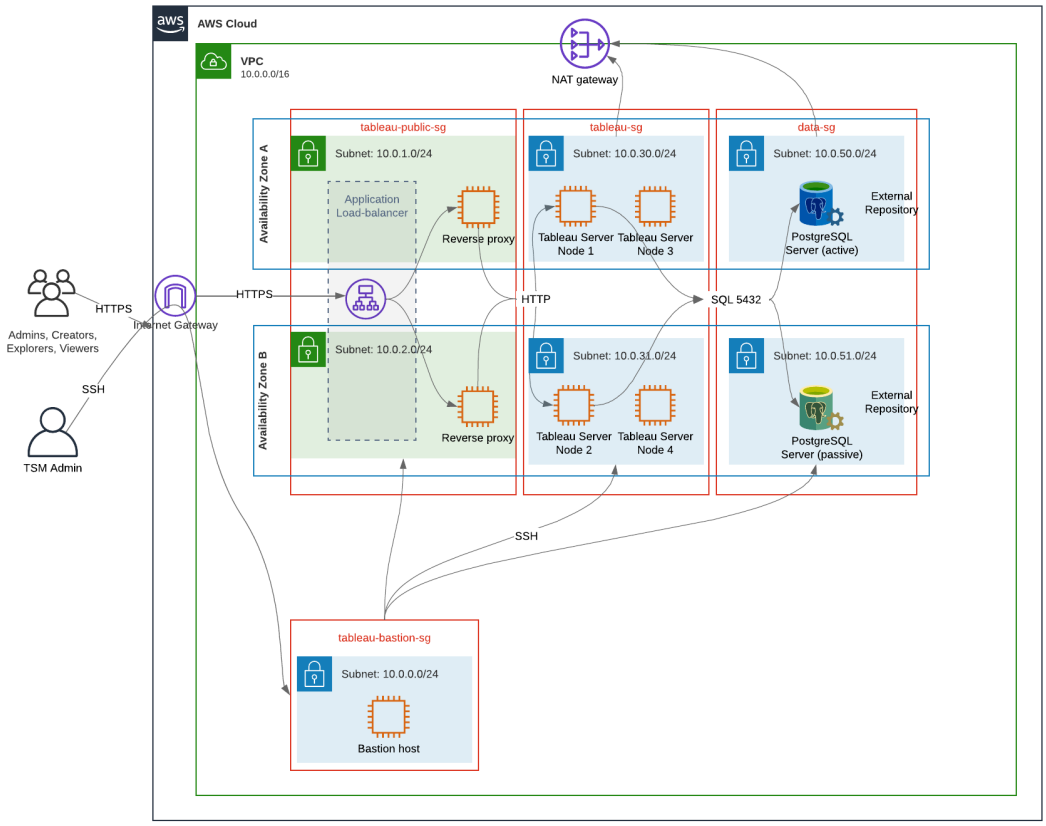
Ziel

Die hier bereitgestellten Terraform-Vorlagen und -Inhalte sollen Ihnen ein funktionierendes Beispiel bieten, mit dem Sie EDG in einer Entwicklungstestumgebung schnell bereitstellen können.

Wir haben uns nach Kräften bemüht, die Terraform-Beispielbereitstellung zu überprüfen und zu dokumentieren. Die Verwendung von Terraform zum Bereitstellen und Verwalten von EDG in einer Produktionsumgebung erfordert jedoch gründliche Fachkenntnisse über Terraform, die den Rahmen dieses Beispiels sprengen würden. Tableau bietet keinen Support für die hier dokumentierte Terraform-Beispiellösung.

Endergebnis

Folgen Sie den Verfahren in diesem Abschnitt, um einen VPC in AWS einzurichten, der funktional dem VPC entspricht, der in Teil 3 - Vorbereiten der Bereitstellung von Tableau Server Enterprise spezifiziert ist.



Die Terraform-Beispielvorlagen und unterstützende Inhalte in diesem Abschnitt:

- Erstellen einen VPC mit einer elastischen IP-Adresse, zwei Verfügbarkeitszonen und einer Subnetzorganisation, wie oben gezeigt (IP-Adressen sind unterschiedlich)
- Erstellen die Sicherheitsgruppen "Bastion", "Public", "Private" und "Data".
- Legen die meisten Eingangs- und Ausgangsregeln für die Sicherheitsgruppen fest. Sie müssen Sicherheitsgruppen bearbeiten, nachdem Terraform ausgeführt wird.

- Erstellen die folgenden EC2-Hosts (auf denen jeweils AWS Linux2 ausgeführt wird): "Bastion", "Proxy 1", "Proxy 2", "Tableau-Knoten 1", "Tableau-Knoten 2", "Tableau-Knoten 3" und "Tableau-Knoten 4".
- EC2-Hosts für PostgreSQL werden nicht erstellt. Sie müssen den EC2 manuell in der Daten-Sicherheitsgruppe "Datensicherheit" erstellen und dann PostgreSQL installieren und konfigurieren, wie unter Installieren, Konfigurieren und Anfertigen einer tar-Sicherung von PostgreSQL beschrieben.

Anforderungen

- AWS-Konto – Sie müssen Zugriff auf ein AWS-Konto haben, mit dem Sie VPCs erstellen können.
- Wenn Sie Terraform auf einem Windows-Computer ausführen, müssen Sie AWS CLI installieren.
- Eine verfügbare elastische IP-Adresse in Ihrem AWS-Konto.
- Eine Domäne, die in AWS Route 53 registriert ist. Terraform wird eine DNS-Zone und zugehörige SSL-Zertifikate in Route 53 erstellen. Daher muss das Profil, unter dem Terraform ausgeführt wird, auch über entsprechende Berechtigungen in Route 53 verfügen.

Voraussetzungen

- Die Befehlszeilenbeispiele in diesem Verfahren sind für Terminal mit Apple iOS gedacht. Wenn Sie Terraform unter Windows ausführen, müssen Sie möglicherweise Befehle mit Dateipfaden entsprechend anpassen.
- Ein Terraform-Projekt besteht aus vielen Textkonfigurationsdateien (Dateierweiterung .tf). Sie konfigurieren Terraform, indem Sie diese Dateien anpassen. Wenn Sie keinen soliden Texteditor haben, installieren Sie Atom oder Text++.
- Wenn Sie das Terraform-Projekt mit anderen teilen, empfehlen wir, das Projekt zur Änderungsverwaltung in Git zu speichern.

Schritt 1: Vorbereiten der Umgebung

A.) Herunterladen und Installieren von Terraform

https://www.terraform.io/downloads

B.) Generieren eines privaten/öffentlichen-Schlüsselpaares

Das ist der Schlüssel, den Sie verwenden werden, um auf AWS und die resultierende VPC-Umgebung zuzugreifen. Wenn Sie Terraform ausführen, werden Sie den öffentlichen Schlüssel mit einbeziehen.

Öffnen Sie ein Terminal und führen Sie die folgenden Befehle aus:

1. Create a private key. For example, `my-key.pem`:

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

2. Erstellen Sie einen öffentlichen Schlüssel. Dieses Schlüsselformat wird für Terraform nicht verwendet. Sie werden ihn später in diesem Verfahren in einen SSH-Schlüssel konvertieren:

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

3. Legen Sie Berechtigungen für den privaten Schlüssel fest:

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

   So legen Sie Berechtigungen unter Windows fest:

   - Suchen Sie die Datei im Windows Explorer, klicken Sie mit der rechten Maustaste auf die Datei und wählen Sie dann **Eigenschaften** aus. Navigieren Sie auf die Registerkarte **Sicherheit** und klicken Sie dann auf **Erweitert**.
   - Ändern Sie den Eigentümer so, dass Sie es sind, deaktivieren Sie Vererbung und löschen Sie alle Berechtigungen. Gewähren Sie sich **Vollzugriff** und klicken Sie dann auf **Speichern**. Kennzeichnen Sie die Datei als schreibgeschützt.

4. Erstellen Sie den öffentlichen SSH-Schlüssel. Das ist der Schlüssel, den Sie später in diesem Verfahren nach Terraform kopieren werden.

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

C.) Herunterladen des Projekts und Hinzufügen eines "State"-Verzeichnisses

1. Laden Sie das EDG-Terraform-Projekt herunter, entpacken Sie es und speichern Sie alles auf Ihrem lokalen Computer. Nachdem Sie den Download entpackt haben, verfügen Sie über ein Verzeichnis der obersten Ebene ("edg-terraform") und eine Reihe von Unterverzeichnissen.
2. Erstellen Sie ein Verzeichnis namens `state` als gleichwertiges Gegenstück zu dem `edg-terraform`-Verzeichnis der obersten Ebene.

Schritt 2: Anpassen der Terraform-Vorlagen

Sie müssen die Terraform-Vorlagen an Ihre AWS- und EDG-Umgebung anpassen. Das hier gezeigte Beispiel gibt die mindestens erforderlichen Anpassungen an, die in den meisten Organisationen vorgenommen werden müssen. Es ist wahrscheinlich, dass Ihre konkrete Umgebung andere Anpassungen erfordert.

Dieser Abschnitt ist nach Vorlagennamen organisiert.

Vergessen Sie nicht, alle vorgenommenen Änderungen zu speichern, bevor Sie mit *Schritt 3: Ausführen von Terraform* – fortfahren.

versions.tf

There are three instances of `versions.tf` files where the `required_version` field must match the version of terraform.exe you're using. Check the version of terraform (`terraform.exe -version`) and update each of the following instances:

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

key-pair.tf

1. Öffnen Sie den öffentlichen Schlüssel, den Sie in Schritt 1B generiert haben, und kopieren Sie den Schlüssel:

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

   Windows: Kopieren Sie den Inhalt Ihres öffentlichen Schlüssels.

2. Kopieren Sie die Zeichenfolge des öffentlichen Schlüssels in das Argument "public_key", zum Beispiel:

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

Ensure that the `key_name` value is unique in the datacenter or `terraform apply` will fail.

locals.tf

Update `user.owner` to your name or alias. The value you enter here will be used for the "Name" tag in AWS on the resources that Terraform creates.

providers.tf

1. Fügen Sie Tags gemäß den Anforderungen Ihrer Organisation hinzu. Beispiel:

   ```
   default_tags {
     tags = {

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

```
  }
}
```

2. If using `provider`, comment out the `assume_role` lines:

```
/* assume_role {
role_arn     = "arn:aws:iam::310946706895:role/terraform-
backend"
session_name = "terraform"
}*/
```

elb.tf

Under `'resource "aws_lb" "tableau" {'` choose a unique value to use for `name` and `tags.Name`.

If another AWS load balancer has the same name in the datacenter, then `terraform apply` will fail.

Add `idle_timeout`:

```
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"
}
                      }
```

variables.tf

Aktualisieren Sie den Namen der Stammdomäne. Dieser Name muss mit der Domäne übereinstimmen, die Sie in Route 53 registriert haben.

```
variable "root_domain_name" {
 default = "example.com"
 }
```

In der Standardeinstellung ist die Unterdomäne `tableau` als VPC-DNS-Domänenname angegeben. Um dies zu ändern, aktualisieren Sie`subdomain` wie folgt:

```
variable "subdomain" {
 default = "tableau"
}
```

modules/tableau_instance/ec2.tf

There are two ec2.tf files in the project. This customization is for the Tableau instance of the ec2.tf in the directory: `modules/tableau_instance/ec2.tf`.

- Falls erforderlich, fügen Sie einen Tags-Blob hinzu:

  ```
  tags = {
   "Name" : var.ec2_name,
   "user.owner" = "ALIAS",
   "Application" = "tableau",
   "Creator" = "ALIAS@example.com",
   "DeptCode" = "8675309",
   "Description" = "EDG",
   "Environment" = "test",
   "Group" = "itcloud@example.com"
   }
  }
  ```

- Aktualisieren Sie gegebenenfalls Ihren Speicher, um Ihre Datenanforderungen zu erfüllen:

  Stammvolume:

  ```
  root_block_device {
   volume_size = 100
  ```

```
 volume_type = "gp3"
}
```

Anwendungsvolume:

```
resource "aws_ebs_volume" "tableau" {
 availability_zone = data.aws_subnet.tableau.availability_zone
 size              = 500
 type              = "gp3"
}
```

Schritt 3: Ausführen von Terraform

A.) Initialisieren von Terraform

Wechseln Sie in Terminal in das Verzeichnis `edg-terraform` und führen Sie den folgenden Befehl aus:

```
terraform init
```

Wenn die Initialisierung erfolgreich war, fahren Sie mit dem nächsten Schritt fort. Wenn die Initialisierung fehlgeschlagen ist, folgen Sie den Anweisungen in der Terraform-Ausgabe.

B.) Planen von Terraform

Führen Sie im gleichen Verzeichnis den Planbefehl ("plan") aus:

```
terraform plan
```

Dieser Befehl kann mehrmals ausgeführt werden. Führen Sie ihn so oft aus, bis alle Fehler behoben sind. Sobald dieser Befehl fehlerfrei ausgeführt wird, können Sie mit dem nächsten Schritt fortfahren.

C.) Anwenden von Terraform

Führen Sie im gleichen Verzeichnis den Anwendungsbefehl ("apply") aus:

```
terraform apply
```

Terraform will prompt you to verify deployment, type `Yes`.

Optional: Löschen von Terraform

Sie können den gesamten VPC löschen, indem Sie den Löschbefehl ("destroy") ausführen:

```
terraform destroy
```

Dieser Befehl löscht nur das, was er geschaffen hat. Wenn Sie an einigen Objekten in AWS (z. B. Sicherheitsgruppen, Subnetze usw.) manuelle Änderungen vorgenommen haben, wird der `destroy`-Befehl fehlschlagen. Um einen fehlgeschlagenen oder nicht mehr reagierenden Löschvorgang zu beenden, geben Sie die Tastenkombination `Control + C` ein. Anschließend müssen Sie den VPC manuell so bereinigen, dass der Originalzustand wiederhergestellt wird, in dem er ursprünglich von Terraform erstellt wurde. Dann können Sie den Befehl `destroy` ausführen.

Schritt 4: Herstellen einer Verbindung zu Bastion

Alle Befehlszeilenverbindungen erfolgen über den Bastion-Host an TCP 22 (SSH-Protokoll).

1. Erstellen Sie in AWS eine Regel für eingehenden Datenverkehr in der Bastion-Sicherheitsgruppe (**AWS** > **Security Groups** > **Bastion SG** > **Edit inbound rules** (AWS > Sicherheitsgruppen > Bastion-SG > Eingangsregel bearbeiten)) und erstellen Sie eine Regel, um SSH-Verbindungen (TCP 22) von der IP-Adresse oder Subnetzmaske zuzulassen, von der aus Sie Terminal-Befehle ausführen werden.

   Optional: Es kann hilfreich sein, während der Bereitstellung das Kopieren von Dateien zwischen den EC2-Instanzen in der privaten und der öffentlichen Gruppe ("Private" und "Public") zu erlauben. Erstellen von Regeln für eingehenden SSH-Datenverkehr:

   - Private: Erstellen Sie eine eingehende Regel, um SSH von "Public" zuzulassen.
   - Public: Erstellen Sie eine eingehende Regel, um SSH von "Private" und von "Public" zuzulassen.

2. Verwenden Sie den pem-Schlüssel, den Sie in Schritt 1.B erstellt haben, um eine Verbindung zu dem Bastion-Host herzustellen:

In einem Mac-Terminal:

Führen Sie die folgenden Befehle in dem Verzeichnis aus, in dem der pem-Schlüssel gespeichert ist:

```
ssh-add —apple-use-keychain <keyName>.pem
```

If you get a warning about private key being accessible by others, then run this command: `chmod 600 <keyName.pem>` and then run the `ssh-add` command again.

Connect to the bastion host with this command: `ssh -A ec2-user@IPaddress`

For example: `ssh -A ec2-user@3.15.12.112.`

Unter Windows mit PuTTY und Pageant:

a. Erstellen Sie eine ppk-Datei aus dem pem-Schlüssel: Verwenden Sie den PuTTY Key Generator. Laden Sie den pem-Schlüssel, den Sie in Schritt 1.B erstellt haben. Klicken Sie nach dem Schlüsselimport auf **Privaten Schlüssel speichern**. Dadurch wird eine ppk-Datei erstellt.

b. In PuTTY: Öffnen Sie die Konfiguration und nehmen Sie die folgenden Änderungen vor:

   - Sessions > Host name (Sitzungen > Hostname): Fügen Sie die IP-Adresse des Bastion-Hosts hinzu.
   - Sessions > Port (Sitzungen > Port): 22
   - Connection > Data > Auto-login username (Verbindung > Daten > Benutzername für automatische Anmeldung): ec2-user
   - Connection > SSH > Auth > Allow agent forwarding (Verbindung > SSH > Authentifizierung > Agentenweiterleitung zulassen)
   - Connection > SSH > Auth > (Verbindung > SSH > Authentifizierung >) Klicken Sie für den privaten Schlüssel auf "Browse" (Durchsuchen) und wählen Sie die .ppk-Datei aus, die Sie eben erstellt haben.

c. Installieren Sie Pageant und laden Sie die ppk in die Anwendung.

Schritt 5: Installieren von PostgreSQL

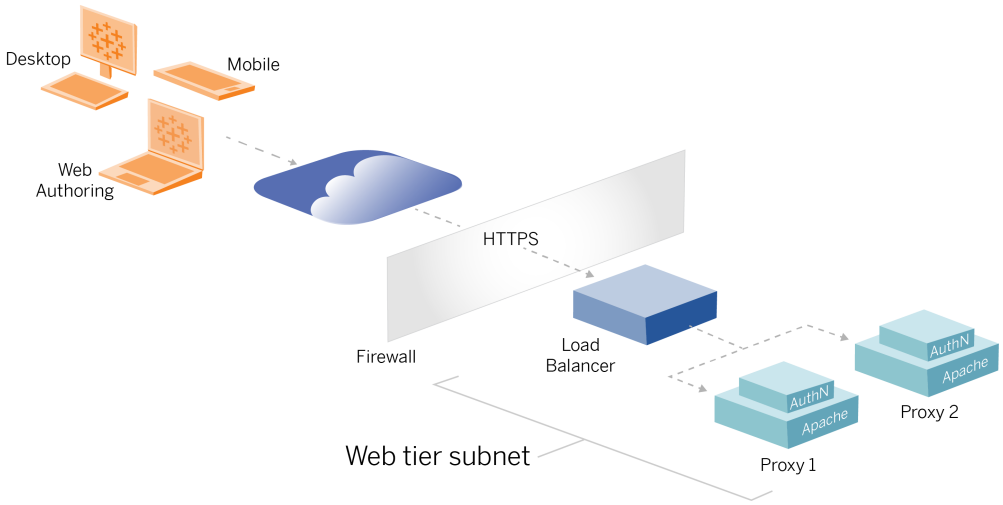
Die Terraform-Vorlage installiert nicht PostgreSQL, um als externes Repository verwendet zu werden. Allerdings werden die zugehörige Sicherheitsgruppe und das Subnetz erstellt. Wenn Sie das externe Repository auf einer EC2-Instanz installieren möchten, auf der PostgreSQL ausgeführt wird, müssen Sie die EC2-Instanz wie in Teil 3 - Vorbereiten der Bereitstellung von Tableau Server Enterprise beschrieben bereitstellen.

Installieren, konfigurieren und sichern Sie dann PostgreSQL in einer tar-Datei, wie in Teil 4 – Installieren und Konfigurieren von Tableau Server beschrieben.

Schritt 6 (optional): Ausführen von DeployTab4EDG

Das Skript "TabDeploy4EDG" automatisiert die Implementierung der Tableau-Bereitstellung auf vier Knoten, die in Teil 4 beschrieben wird. Siehe dazu TabDeploy4EDG – Skript für automatisierte Installation.

Anhang - Webschicht mit Apache-Beispielbereitstellung



Dieses Thema enthält ein komplettes Verfahren, in dem beschrieben wird, wie die Webschicht in der beispielhaften AWS-Referenzarchitektur implementiert wird. Die Beispielkonfiguration setzt sich aus folgenden Komponenten zusammen:

- AWS-Anwendungslastenausgleich
- Apache-Proxyserver
- Mellon-Authentifizierungsmodul
- Okta-IdP
- SAML-Authentifizierung

Hinweis: Die in diesem Abschnitt vorgestellte Beispielkonfiguration für die Webschicht enthält detaillierte Verfahren zum Bereitstellen von Software und Diensten von Drittanbietern. Wir haben uns nach Kräften bemüht, die Verfahren zur Aktivierung des Webschicht-Szenarios zu überprüfen und zu dokumentieren. Die Software von Drittanbietern kann sich jedoch ändern oder Ihr Szenario kann von der hier beschriebenen

Referenzarchitektur abweichen. Verbindliche Konfigurationsdetails und Support finden Sie in der Dokumentation der Drittanbieter.

Die Linux-Beispiele in diesem Abschnitt zeigen Befehle für RHEL-ähnliche Distributionen. Die hier angegebenen spezifischen Befehle wurden mit der Amazon Linux 2-Distribution entwickelt. Wenn Sie die Ubuntu-Distribution ausführen, bearbeiten Sie die Befehle entsprechend.

Die Bereitstellung der Webschicht in diesem Beispiel erfolgt nach einem schrittweisen Konfigurations- und Überprüfungsverfahren. Die Konfiguration der zentralen Web-Ebene umfasst die folgenden Schritte, um HTTP zwischen Tableau und dem Internet zu aktivieren. Apache wird für Reverse-Proxy/Lastenausgleich hinter dem AWS-Anwendunglastenausgleich ausgeführt und konfiguriert:

1. Installieren von Apache
2. Konfigurieren des Reverse-Proxys zum Testen der Konnektivität zu Tableau Server
3. Konfigurieren von Lastenausgleich auf dem Proxy
4. Konfigurieren von AWS-Anwendungslastenausgleich

Nachdem die Web-Ebene eingerichtet und die Konnektivität zu Tableau überprüft wurde, konfigurieren Sie die Authentifizierung bei einem externen Anbieter.

Installieren von Apache

Führen Sie das folgende Verfahren auf beiden EC2-Hosts (Proxy 1 und Proxy 2) aus. Wenn Sie die Bereitstellung in AWS gemäß dem Beispiel der Referenzarchitektur vornehmen, sollten Sie zwei Verfügbarkeitszonen haben und in jeder Zone einen einzelnen Proxyserver ausführen.

1. Installieren Sie Apache:

```
sudo yum update -y
sudo yum install -y httpd
```

2. Konfigurieren Sie Apache für den Start beim Neustart:

   ```
   sudo systemctl enable --now httpd
   ```

3. Stellen Sie sicher, dass die Version von httpd, die Sie installiert haben, Folgendes enthält: `proxy_hcheck_module`:

   ```
   sudo httpd -M
   ```

   `proxy_hcheck_module` ist erforderlich. Wenn Ihre Version von httpd dieses Modul nicht enthält, aktualisieren Sie auf eine Version von httpd, die es enthält.

Konfigurieren des Proxys zum Testen der Konnektivität zu Tableau Server

Führen Sie dieses Verfahren auf einem der Proxy-Hosts (Proxy 1) aus. Der Zweck dieses Schritts besteht darin, die Konnektivität zwischen dem Internet zu Ihrem Proxyserver für den Tableau Server in der privaten Sicherheitsgruppe zu überprüfen.

1. Erstellen Sie eine Datei mit dem Namen `tableau.conf` und fügen Sie sie dem Verzeichnis `/etc/httpd/conf.d` hinzu.

   Kopieren Sie den folgenden Code und geben Sie die Schlüssel `ProxyPass` und `ProxyPassReverse` mit der privaten IP-Adresse des Tableau Server-Knotens 1 an.

   > **Wichtig**: Die unten gezeigte Konfiguration ist keine sichere Konfiguration und sollte nicht in der Produktion verwendet werden. Diese Konfiguration sollte nur während des Installationsprozesses verwendet werden, um die durchgehende Konnektivität zu überprüfen.

   Wenn beispielsweise die IP-Adresse von Knoten 1 `10.0.30.32` lautet, würde in der Datei `tableau.conf` Folgendes stehen:

```
<VirtualHost *:80>
ProxyPreserveHost On
ProxyPass "/" "http://10.0.30.32:80/"
ProxyPassReverse "/" "http://10.0.30.32:80/"
</VirtualHost>
```

2. Starten Sie httpd neu:

```
sudo systemctl restart httpd
```

Überprüfung: Konfiguration der Basistopologie

Sie sollten auf die Tableau Server-Administrationsseite zugreifen können, indem Sie zu `http://<proxy-public-IP-address>` navigieren.

Falls die Tableau Server-Administrationsseite in Ihrem Browser nicht geladen wird, führen Sie die folgenden Schritte zur Fehlerbehebung auf dem Proxy 1-Host aus:

- Als erstes stoppen Sie httpd und starten Sie es dann erneut.
- Überprüfen Sie die Datei `tableau.conf` noch einmal. Stellen Sie sicher, dass die private IP-Adresse von Knoten 1 korrekt ist. Prüfen Sie auf doppelte Anführungszeichen und überprüfen Sie auch die Syntax sorgfältig.
- Führen Sie den Befehl `curl` auf dem Reverse-Proxyserver mit der privaten IP-Adresse von Knoten 1 aus (z. B. `curl 10.0.1.90`). Wenn die Shell nicht HTML zurück gibt oder wenn sie HTML für die Apache-Testwebseite zurück gibt, überprüfen Sie die Protokoll-/Portkonfiguration zwischen der öffentlichen und der privaten Sicherheitsgruppe.
- Führen Sie den Befehl `curl` mit der privaten IP-Adresse von Proxy 1 aus (z. B.`curl 10.0.0.163`). Wenn die Shell den HTML-Code für die Apache-Testwebseite zurück gibt, ist die Proxy-Datei nicht korrekt konfiguriert.
- Starten Sie httpd immer neu (`sudo systemctl restart httpd`), wenn Sie die Konfiguration der Proxy-Datei oder der Sicherheitsgruppen geändert haben.
- Stellen Sie sicher, dass TSM auf Knoten 1 ausgeführt wird.

Konfigurieren von Lastenausgleich auf dem Proxy

1. Entfernen Sie auf dem demselben Proxy-Host (Proxy 1), auf dem Sie die Datei `tableau.conf` erstellt haben, die vorhandene Konfiguration für den virtuellen Host, und bearbeiten Sie die Datei so, dass sie die Logik für den Lastenausgleich enthält.

   Beispiel:

   ```
   <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. Stoppen und starten Sie anschließend httpd:

   ```
   sudo systemctl stop httpd
   sudo systemctl start httpd
   ```

3. Überprüfen Sie die Konfiguration, indem Sie zu der öffentlichen IP-Adresse von Proxy 1 navigieren.

Kopieren der Konfiguration auf den zweiten Proxyserver

1. Kopieren Sie die Datei `tableau.conf` von Proxy 1 und speichern Sie sie auf dem Proxy 2-Host in dem Verzeichnis `/etc/httpd/conf.d`.
2. Stoppen und starten Sie anschließend httpd:

```
sudo systemctl stop httpd
sudo systemctl start httpd
```

3. Überprüfen Sie die Konfiguration, indem Sie zu der öffentlichen IP-Adresse von Proxy 2 navigieren.

Konfigurieren von AWS-Anwendungslastenausgleich

Konfigurieren Sie den Lastenausgleich als HTTP-Listener. Im hier vorliegenden Verfahren wird beschrieben, wie Sie einen Lastenausgleich in AWS hinzufügen.

Schritt 1: Erstellen einer Zielgruppe

Eine Zielgruppe ist eine AWS-Konfiguration, welche die EC2-Instances definiert, auf denen Ihre Proxyserver ausgeführt werden. Dies sind die Ziele für den Datenverkehr von der LBS.

1. EC2 > **Target groups** > **Create target group** (EC2 > Zielgruppen > Zielgruppe erstellen)
2. Auf der Seite "Create" (Erstellen):

- Geben Sie einen Zielgruppennamen ein, zum Beispiel `TG-internal-HTTP`.
- Zieltyp: Instanzen
- Protokoll: HTTP
- Port: 80
- VPC: Wählen Sie Ihre VPC aus.
- Fügen Sie unter **Health checks** (Integritätsprüfungen) > **Advanced health checks settings** (Einstellungen für erweiterte Integritätsprüfungen) > **Success codes** (Erfolgscodes) die Codeliste zum Lesen hinzu: `200,303`.
- Klicken Sie auf **Create** (Erstellen).

3. Wählen Sie die Zielgruppe aus, die Sie eben erstellt haben, und klicken Sie dann auf die Registerkarte **Targets** (Ziele):
    - Klicken Sie auf **Edit** (Bearbeiten).
    - Wählen Sie die EC2-Instanzen (oder eine einzelne Instanz, wenn Sie einzeln konfigurieren) aus, auf denen die Proxyanwendung ausgeführt wird. Klicken Sie dann auf **Zu registriert hinzufügen**.
    - Klicken Sie auf **Speichern**.

Schritt 2: Starten des Assistenten für Lastenausgleich

1. EC2 > **Load Balancers** > **Create Load Balancer** (EC2 > Lastenausgleichsmodule > Lastenausgleich erstellen)

2. Erstellen Sie auf der Seite "Select load balancer type" (Lastenausgleichstyp auswählen) einen Anwendungslastenausgleich.

Hinweis: Die Benutzeroberfläche, die zur Konfiguration des Lastenausgleichsmodulen angezeigt wird, ist in den AWS-Rechenzentren nicht einheitlich. Das folgende Verfahren "Assistenten-Konfiguration" bezieht sich auf den AWS-Konfigurationsassistenten, der mit **Schritt 1 Lastenausgleichsmodul konfigurieren** beginnt.

Wenn Ihr Rechenzentrum alle Konfigurationen auf einer einzigen Seite anzeigt, die

unten auf der Seite eine Schaltfläche **Create Load Balancer** enthält, befolgen Sie das nachstehende Verfahren "Konfiguration auf einer Seite".

Assistenten-Konfiguration

1. Die Seite **Configure load balancer** (Lastenausgleich konfigurieren):
    - Geben Sie den Namen an
    - Schema: Internetzugriff (Standard)
    - IP-Adresstyp: IPv4 (Standard)
    - Listener (Listener und Routing):
        a. Behalten Sie den Standard-HTTP-Listener bei.
        b. Klicken Sie auf **Listener hinzufügen** und fügen Sie `HTTPS:443` hinzu.
    - VPC: Wählen Sie die VPC aus, in der Sie alles installiert haben.
    - Verfügbarkeitszonen:
        - Wählen Sie **a** und **b** für Ihre Rechenzentrumsregionen aus.
        - Wählen Sie in der entsprechenden Dropdown-Liste das öffentliche Subnetz aus (in dem sich Ihre Proxyserver befinden).
    - Klicken Sie auf **Configure Security Settings** (Sicherheitseinstellungen konfigurieren)
2. Die Seite **Configure Security Settings** (Sicherheitseinstellungen konfigurieren)
    - Laden Sie Ihr öffentliches SSL-Zertifikat hoch.
    - Klicken Sie auf **Next: Configure Security Groups** (Weiter: Sicherheitsgruppen konfigurieren).
3. Die Seite **Configure Security Groups** (Sicherheitsgruppen konfigurieren):
    - Wählen Sie die öffentliche Sicherheitsgruppe aus. Wenn die Standardsicherheitsgruppe ausgewählt ist, deaktivieren Sie diese Auswahl.
    - Klicken Sie auf **Next: Configure Routing** (Weiter: Routing konfigurieren).
4. Die Seite **Configure Routing** (Routing konfigurieren)

- Zielgruppe: Bestehende Zielgruppe.
- Name: Wählen Sie eine Zielgruppe aus, die Sie zuvor erstellt haben.
- Klicken Sie auf **Next: Register Targets** (Weiter: Ziele registrieren).

5. Die Seite **Register Targets** (Ziele registrieren)
    - Die beiden Proxyserver-Instanzen, die Sie zuvor konfiguriert haben, sollten angezeigt werden.
    - Klicken Sie auf **Next: Review** (Weiter: Überprüfung).

6. Die Seite **Review** (Überprüfen)

    Klicken Sie auf **Erstellen**.

Konfiguration auf einer Seite

Grundlegende Konfiguration

- Geben Sie den Namen an
- Schema: Internetzugriff (Standard)
- IP-Adresstyp: IPv4 (Standard)

Netzwerkzuordnung

- VPC: Wählen Sie die VPC aus, in der Sie alles installiert haben.
- Zuordnungen:
    - Wählen Sie die Verfügbarkeitszonen **a** und **b** (oder vergleichbare) für Ihre Rechenzentrumsregionen aus.
    - Wählen Sie in der entsprechenden Dropdown-Liste das öffentliche Subnetz aus (in dem sich Ihre Proxyserver befinden).

Sicherheitsgruppen

Wählen Sie die öffentliche Sicherheitsgruppe aus. Wenn die Standardsicherheitsgruppe ausgewählt ist, deaktivieren Sie diese Auswahl.

Listener und Routing

- Behalten Sie den Standard-HTTP-Listener bei. Geben Sie bei **Standardaktion** die zuvor eingerichtete Zielgruppe an.
- Klicken Sie auf **Listener hinzufügen** und fügen Sie `HTTPS:443` hinzu. Geben Sie bei **Standardaktion** die zuvor eingerichtete Zielgruppe an.

Sichere Listener-Einstellungen

- Laden Sie Ihr öffentliches SSL-Zertifikat hoch.

Klicken Sie auf **Create Load Balancer**.

Schritt 3: Stickiness aktivieren

1. Nachdem der Lastenausgleich erstellt wurde, müssen Sie Stickiness für die Zielgruppe aktivieren.
    - Öffnen Sie die AWS-Seite für die Zielgruppe (**EC2** > **Load Balancing** (Lastenausgleich) > **Target groups** (Zielgruppen)), und wählen Sie die Zielgruppeninstanz aus, die Sie gerade eingerichtet haben. Wählen Sie im Menü **Actions** (Aktionen) die Option **Edit attributes** (Attribute bearbeiten) aus.
    - Wählen Sie auf der Seite **Edit attributes** (Attribute bearbeiten) die Option **Stickiness** (Bindung) aus, geben Sie eine Zeitdauer von `1 day` (1 Tag) an, und klicken Sie dann auf **Save changes** (Änderungen speichern).
2. Aktivieren Sie beim Lastenausgleich Stickiness auf dem HTTP-Listener. Wählen Sie den Lastenausgleich aus, den Sie gerade konfiguriert haben, und klicken Sie dann auf die Registerkarte **Listeners**:
    - Klicken Sie für **HTTP:80** auf **View/edit rules** (Regeln anzeigen/bearbeiten). Klicken Sie auf der Seite **Rules** (Regeln), die daraufhin angezeigt wird, auf das Bearbeitungssymbol (zuerst oben auf der Seite und dann noch einmal für die Regel), um die Regel zu bearbeiten. Löschen Sie die vorhandene THEN-Regel ("DANN-Regel") und ersetzen Sie sie, indem Sie auf **Add action** (Aktion hinzufügen) > **Forward to...** (Weiterleiten an...) klicken. Geben Sie in der resultierenden THEN-Konfiguration die gleiche Zielgruppe an, die Sie erstellt haben. Aktivieren Sie unter "Group-level stickiness" (Bindung auf Gruppenebene) den Punkt "Stickiness", und legen Sie "Duration" (Zeitdauer) auf "1 Day" (1 Tag) fest. Speichern Sie die Einstellung und klicken Sie dann auf **Update** (Aktualisieren).

Schritt 4: Festlegen des Leerlaufzeitlimits für den Lastenausgleich

Aktualisieren Sie für den Lastenausgleich das Leerlaufzeitlimit auf 400 Sekunden.

Wählen Sie den Lastenausgleich, den Sie für diese Bereitstellung konfiguriert haben, und klicken Sie dann auf **Aktionen** > **Attribute bearbeiten**. Stellen Sie das **Leerlaufzeitlimit** auf `400` Sekunden ein und klicken Sie dann auf **Speichern**.

Schritt 5: Überprüfen der LBS-Verbindung

Öffnen Sie die Seite "AWS Load Balancer" (AWS-Lastenausgleich) (**EC2**> **Load Balancers** (Lastenausgleich)), wählen Sie die Lastenausgleichsinstanz aus, die Sie gerade eingerichtet haben.

Kopieren Sie unter **Description** (Beschreibung) den DNS-Namen und fügen Sie ihn in einen Browser ein, um auf die Tableau Server-Anmeldeseite zuzugreifen.

Wenn ein Fehler auf 500-Niveau angezeigt wird, müssen Sie wahrscheinlich Ihre Proxyserver neu starten.

Aktualisieren des DNS mit der öffentlichen Tableau-URL

Verwenden Sie den DNS-Zonennamen Ihrer Domäne aus der AWS-Seite "Load Balancer" (Lastenausgleich) > "Description" (Beschreibung), um einen CNAME-Wert in Ihrem DNS zu erstellen. Datenverkehr zu Ihrer URL (tableau.example.com) sollte an den öffentlichen AWS-DNS-Namen gesendet werden.

Überprüfen der Konnektivität

Nachdem Ihre DNS-Updates abgeschlossen sind, sollten Sie zu der Tableau Server-Anmeldeseite navigieren können, indem Sie Ihre öffentliche URL eingeben, zum Beispiel:`https://tableau.example.com`.

Beispiel für eine Konfiguration für Authentifizierung: SAML mit externem IdP

Im folgenden Beispiel wird beschrieben, wie Sie SAML mit Okta-IdP und Mellon-Authentifizierungsmodul für eine Tableau-Bereitstellung einrichten und konfigurieren, die in der AWS-Referenzarchitektur ausgeführt wird. In dem Beispiel wird beschrieben, wie Tableau Server und die Apache-Proxyserver für die Verwendung von HTTP konfiguriert werden. Okta wird Anfragen an den AWS-Lastenausgleich über HTTPS senden, aber sämtlicher interner Datenverkehr wird über HTTP erfolgen. Beachten Sie bei der Konfiguration für dieses Szenario die Unterschiede von HTTP und HTTPS, wenn Sie URL-Zeichenfolgen festlegen.

In diesem Beispiel wird Mellon als Dienstanbietermodul für Vorauthentifizierung auf den Reverse-Proxyservern verwendet. Diese Konfiguration stellt sicher, dass nur authentifizierter Datenverkehr mit Tableau Server verbunden wird, der auch als Dienstanbieter mit dem Okta-IdP agiert. Daher müssen Sie zwei IdP-Anwendungen konfigurieren: eine für den Mellon-Dienstanbieter und eine für den Tableau-Dienstanbieter.

Erstellen des Tableau-Administratorkontos

Ein häufiger Fehler beim Konfigurieren von SAML ist, die Erstellung eines Administratorkontos in Tableau Server zu vergessen, bevor SSO aktiviert wird.

Der erste Schritt besteht darin, ein Konto in Tableau Server mit einer Serveradministratorrolle zu erstellen. Für das Okta-Beispielszenario muss der Benutzername in einem gültigen E-Mail-Adressformat angegeben werden (z. B. user@example.com). Sie müssen für diesen Benutzer ein Kennwort festlegen, das jedoch nach der Konfiguration von SAML nicht mehr verwendet wird.

Konfigurieren der Vor-Authentifizierungsanwendung von Okta

Das in diesem Abschnitt beschriebene End-to-End-Szenario erfordert zwei Okta-Anwendungen:

- Vor-Authentifizierungsanwendung von Okta
- Tableau Server-Anwendung von Okta

Jede dieser Anwendungen ist mit unterschiedlichen Metadaten verbunden, die Sie auf dem Reverse-Proxy bzw. Tableau Server konfigurieren müssen.

In diesem Verfahren wird beschrieben, wie Sie die Vor-Authentifizierungsanwendung von Okta erstellen und konfigurieren. Später in diesem Thema ist vorgesehen, dass Sie die Tableau Server-Anwendung von Okta erstellen. Ein kostenloses Okta-Testkonto mit eingeschränkten Benutzern finden Sie auf der Okta-Entwickler-Webseite.

Erstellen Sie eine SAML-App-Integration für den Mellon-Vorauthentifizierungs-Dienstanbieter.

1. Öffnen Sie das Okta-Administrations-Dashboard, und klicken Sie auf **Applications** > **Create App Integration** (Anwendungen > App-Integration erstellen).
2. Wählen Sie auf der Seite **Create a new app integration** (Neue App-Integration erstellen) die Option **SAML 2.0** aus, und klicken Sie dann auf **Next** (Weiter).
3. Geben Sie auf der Registerkarte **General Settings** (Allgemeine Einstellungen) einen App-Namen ein (z. B. `Tableau Pre-Auth`), und klicken Sie dann auf **Next** (Weiter).
4. Auf der Registerkarte **Configure SAML** (SAML konfigurieren):
    - SSO-URL (Single Sign-On): Das letzte Element des Pfads in der Single Sign-On-URL wird als der `MellonEndpointPath` in der `mellon.conf` Konfigurationsdatei bezeichnet, die später in diesem Verfahren behandelt wird. Sie können einen beliebigen Endpunkt angeben. In diesem Beispiel ist `sso` der Endpunkt. Das letzte Element, `postResponse`, ist erforderlich: `https://tableau.example.com/sso/postResponse`.
    - Deaktivieren Sie das Kontrollkästchen **Use this for Recipient URL and Destination URL** (Dieses für Empfänger-URL und Ziel-URL verwenden).
    - Recipient URL (Empfänger-URL): Ist die gleiche wie die SSO-URL, jedoch mit HTTP. Zum Beispiel: `http://tableau.example.com/sso/postResponse`.

- Destination URL (Ziel-URL): Ist die gleiche wie die SSO-URL, jedoch mit HTTP. Zum Beispiel: `http://tableau.example.com/sso/postResponse`.
- Audience URI (SP Entity ID) (Zielgruppen-URI (SP-Entitäts-ID)). Zum Beispiel: `https://tableau.example.com`.
- Name ID Format (Format der Namens-ID): `EmailAddress`
- Application Username (Anwendungsbenutzername): `Email`
- Attributes Statements (Attributangaben): Name = `mail`; Name format (Namensformat) = `Unspecified`; Value (Wert) = `user.email`.

Klicken Sie auf **Next** (Weiter).

5. Wählen Sie auf der Registerkarte **Feedback** Folgendes aus:
   - **I'm an Okta customer adding an internal app (Ich bin ein Okta-Kunde und füge eine interne App hinzu)**
   - **This is an internal app that we have created (Dies ist eine interne App, die wir erstellt haben)**
   - Klicken Sie auf **Finish** (Fertigstellen).

6. Erstellen Sie die IdP-Metadatendatei vor der Authentifizierung:
   - In Okta: **Applications** (Anwendungen) > **Applications** (Anwendungen) > Ihre neue Anwendung (z. B. `Tableau Pre-Auth`) > **Sign On** (Anmelden)
   - Klicken Sie neben **SAML-Signaturzertifikate** auf **Anweisungen zur SAML-Einrichtung anzeigen**.
   - Führen Sie auf der Seite **Konfigurieren von SAML 2.0 für die Anwendung vor der Authentifizierung** einen Bildlauf nach unten zum Abschnitt **Optional** durch, **Stellen Sie die folgenden IDP-Metadaten für Ihren SP-Anbieter bereit**.
   - Kopieren Sie den Inhalt des XML-Felds, und speichern Sie ihn in einer Datei mit dem Namen `pre-auth_idp_metadata.xml`.

7. (Optional) Konfigurieren Sie Multi-Faktor-Authentifizierung (MFA):
   - In Okta: **Applications** (Anwendungen) > **Applications** (Anwendungen) > Ihre neue Anwendung (z. B. `Tableau Pre-Auth`) > **Sign On** (Anmelden)
   - Klicken Sie unter **Sign On Policy** (Anmelderichtlinie) auf **Add Rule** (Regel hinzufügen).

- Geben Sie in der **App Sign On Rule** (App-Anmelderegel) einen Namen und die verschiedenen MFA-Optionen an. Um die Funktionalität zu testen, können Sie alle Optionen in der jeweiligen Standardeinstellung belassen. Sie müssen jedoch unter **Actions** (Aktionen) den Punkt **Prompt for factor** (Zur Eingabe des Faktors auffordern) auswählen und dann angeben, wie oft sich Benutzer anmelden müssen. Klicken Sie auf **Save** (Speichern).

Erstellen und Zuweisen eines Okta-Benutzers

1. Erstellen Sie in Okta einen Benutzer mit dem gleichen Benutzernamen, den Sie in Tableau erstellt haben (user@example.com): **Directory** (Verzeichnis) > **People** (Personen) > **Add person** (Person hinzufügen).
2. Nachdem der Benutzer erstellt wurde, weisen Sie ihm die neue Okta-App zu: Klicken Sie auf den Benutzernamen und weisen Sie dann die Anwendung in **Assign Application** (Anwendung zuweisen) zu.

Installieren von Mellon für die Vor-Authentifizierung

1. Führen Sie die folgenden Befehle auf der EC2-Instanz aus, auf der der Apache-Proxyserver ausgeführt wird, um PHP- und Mellon-Module zu installieren:

   ```
   sudo yum install httpd php mod_auth_mellon
   ```

2. Erstellen Sie das Verzeichnis `/etc/httpd/mellon`.

Konfigurieren von Mellon als Vor-Authentifizierungsmodul

Führen Sie dieses Verfahren auf beiden Proxyservern aus.

Sie müssen eine Kopie der Datei `pre-auth_idp_metadata.xml` haben, die Sie aus der Okta-Konfiguration erstellt haben.

1. Wechseln Sie das Verzeichnis:

   ```
   cd /etc/httpd/mellon
   ```

2. Erstellen Sie die Dienstanbieter-Metadaten. Führen Sie das Skript `mellon_create_metadata.sh` aus. Sie müssen in dem Befehl die Entitäts-ID und die Rückgabe-URL für Ihre Organisation mit angeben.

   Die Rückgabe-URL wird in Okta als *Single Sign On URL* (SSO-URL) bezeichnet. Das letzte Element des Pfads in der Rückgabe-URL wird als `MellonEndpointPath` in der Konfigurationsdatei `mellon.conf` bezeichnet, die später in diesem Verfahren folgt. In diesem Beispiel geben wir `sso` als EndpointPath an.

   Beispiel:

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

   Das Skript gibt das Dienstanbieterzertifikat, den Schlüssel und Metadatendateien zurück.

3. Benennen Sie die Dienstanbieterdateien im Verzeichnis `mellon` so um, dass sie leichter verständlich sind. Wir werden diese Dateien in der Dokumentation mit den folgenden Namen bezeichnen:

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

4. Kopieren Sie die Datei `pre-auth_idp_metadata.xml` in dasselbe Verzeichnis.

5. Erstellen Sie die Datei `mellon.conf` im Verzeichnis `/etc/httpd/conf.d`:

   ```
   sudo nano /etc/httpd/conf.d/mellon.conf
   ```

6. Kopieren Sie den folgenden Inhalt in `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_meta-
data.xml
MellonEndpointPath /sso
MellonEnable "info"
</Location>
```

7. Kopieren Sie den folgenden Inhalt in die vorhandene `tableau.conf`-Datei:

   Fügen Sie den folgenden Inhalt innerhalb des Blocks `<VirtualHost *:80>` hinzu. Aktualisieren Sie `ServerName` mit dem öffentlichen Hostnamen in Ihrer Entitäts-ID:

   ```
   DocumentRoot /var/www/html
   ServerName tableau.example.com
   ServerSignature Off
   ErrorLog logs/error_sp.log
   CustomLog logs/access_sp.log combined
   LogLevel info
   ```

   Fügen Sie den Block "Location" außerhalb des Blocks `<VirtualHost *:80>` hinzu. Aktualisieren Sie `MellonCookieDomain` mit der Domäne der obersten Ebene, um Cookie-Informationen wie gezeigt aufzubewahren:

   ```
   <Location />
   AuthType Mellon
   MellonEnable auth
   Require valid-user
   MellonCookieDomain example.com
   </Location>
   ```

   Die komplette `tableau.conf`-Datei sollte wie das folgende Beispiel aussehen:

   ```
   <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. Überprüfen Sie die Konfiguration. Führen Sie den folgenden Befehl aus:

   ```
   sudo apachectl configtest
   ```

   Wenn der Konfigurationstest einen oder mehrere Fehler zurückgibt, beheben Sie diese, und führen Sie configtest erneut aus. Bei einer erfolgreichen Konfiguration wird `Syntax OK` zurückgegeben.

9. Starten Sie httpd neu:

```
sudo systemctl restart httpd
```

Erstellen einer Tableau Server-Anwendung in Okta

1. Im Okta-Dashboard: **Applications** (Anwendungen) > **Applications** (Anwendungen) > **Browse App Catalog** (App-Katalog durchsuchen)
2. Suchen Sie in **Browse App Integration Catalog** (App-Integrationskatalog durchsuchen) nach `Tableau`, wählen Sie die Kachel "Tableau Server" aus und klicken Sie dann auf **Add** (Hinzufügen).
3. Geben Sie unter **Add Tableau Server** (Tableau Server hinzufügen) > **General Settings** (Allgemeine Einstellungen) ein "Label" (Beschriftung) ein, und klicken Sie dann auf **Next** (Weiter).
4. Wählen Sie in "Sign-On Options" (Anmeldeoptionen) die Option **SAML 2.0** aus und führen Sie dann einen Bildlauf nach unten durch, bis "Advanced Sign-on Settings" (Erweiterte Anmeldeeinstellungen) angezeigt wird:
    - **SAML Entity ID** (SAML-Entitäts-ID): Geben Sie die öffentliche URL ein (z. B. https://tableau.example.com).
    - **Application user name format** (Format des Anwendungsbenutzernamens): Email (E-Mail)
5. Klicken Sie auf den Link **Identity Provider metadata** (Identitätsanbieter-Metadaten), um einen Browser zu starten. Kopieren Sie den Browserlink. Das ist der Link, den Sie verwenden werden, wenn Sie Tableau im folgenden Verfahren konfigurieren.
6. Klicken Sie auf **Done** (Fertig).
7. Weisen Sie Ihrem Benutzer (user@example.com) die neue Tableau Server-Okta-App zu: Klicken Sie auf den Benutzernamen und weisen Sie dann die Anwendung in **Assign Application** (Anwendung zuweisen) zu.

Aktivieren von SAML in Tableau Server für IdP

Führen Sie dieses Verfahren auf dem Tableau Server-Knoten 1 aus.

1. Laden Sie die Metadaten der Tableau Server-Anwendung von Okta herunter. Verwenden Sie den Link, den Sie im vorherigen Verfahren gespeichert haben:

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

2. Kopieren Sie ein TLS-Zertifikat und die zugehörige Schlüsseldatei auf Tableau Server. Die Schlüsseldatei muss ein RSA-Schlüssel sein. Weitere Informationen zu SAML-Zertifikat- und Identitätsanbieteranforderungen finden Sie unter *SAML-Anforderungen* (Linux).

   Zur Vereinfachung der Zertifikatsverwaltung und -bereitstellung sowie als bewährte Sicherheitspraxis empfehlen wir die Verwendung von Zertifikaten, die von einer bedeutenden vertrauenswürdigen Zertifizierungsstelle (CA) eines Drittanbieters erstellt wurden. Alternativ dazu können Sie auch selbstsignierte Zertifikate generieren oder Zertifikate von einer PKI für TLS verwenden.

   Wenn Sie nicht über ein TLS-Zertifikat verfügen, können Sie nach der folgenden Vorgehensweise ein selbstsigniertes Zertifikat generieren.

Generieren eines selbstsignierten Zertifikats

Führen Sie dieses Verfahren auf dem Tableau Server-Knoten 1 aus.

a. Generieren Sie den Schlüssel der signierenden Stammzertifizierungsstelle (CA):

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

b. Erstellen Sie das Zertifikat der Stammzertifizierungsstelle:

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

   Sie werden aufgefordert, Werte für die Zertifikatfelder einzugeben. Beispiel:

```
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. Erstellen Sie das Zertifikat und den zugehörigen Schlüssel (im Beispiel unten als `server-saml.csr` und `server-saml.key` bezeichnet). Der Antragstellername ("Subject Name") für das Zertifikat muss mit dem öffentlichen Hostnamen des Tableau-Hosts übereinstimmen. Der Antragstellername wird mit der Option `-subj` im Format `"/CN=<host-name>"` festgelegt, beispielsweise:

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

d. Signieren Sie das neue Zertifikat mit dem CA-Zertifikat, das Sie oben erstellt haben. Der folgende Befehl gibt das Zertifikat auch im `crt`-Format aus:

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

e. Konvertieren Sie die Schlüsseldatei in RSA. Tableau erfordert eine RSA-Schlüsseldatei für SAML. Führen Sie den folgenden Befehl aus, um den Schlüssel zu konvertieren:

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

3. Konfigurieren Sie SAML. Führen Sie den folgenden Befehl aus und geben Sie Ihre Entitäts-ID und die Rückgabe-URL sowie die Pfade zur Metadatendatei, zur Zertifikatsdatei und zur Schlüsseldatei an:

```
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. Wenn in Ihrer Organisation Tableau Desktop 2021.4 oder höher ausgeführt wird, müssen Sie den folgenden Befehl ausführen, um Authentifizierung über die Reverse-Proxyserver zu aktivieren.

   Die Tableau Desktop-Versionen 2021.2.1 bis 2021.3 funktionieren ohne Ausführung dieses Befehls, vorausgesetzt, Ihr Vorauthentifizierungsmodul (z. B. Mellon) ist so konfiguriert, dass es die Aufbewahrung von Cookies auf der Domäne der obersten Ebene erlaubt.

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

5. Übernehmen Sie die Konfigurationsänderungen:

   ```
   tsm pending-changes apply
   ```

Validierung der SAML-Funktionalität

Um die End-to-End-SAML-Funktionalität zu validieren, melden Sie sich bei Tableau Server mit der öffentlichen URL (z. B. https://tableau.example.com) mit dem Tableau-Administratorkonto an, das Sie zu Beginn dieses Verfahrens erstellt haben.

Fehlerbehebung bei der Validierung

Bad Request: Ein häufiger Fehler in diesem Szenario ist ein Fehler vom Typ "Bad Request" (Ungültige Anforderung) von Okta. Dieses Problem tritt häufig auf, wenn der Browser Daten aus einer früheren Okta-Sitzung zwischenspeichert. Wenn Sie beispielsweise die Okta-Anwendungen als Okta-Administrator verwalten und dann versuchen, mit einem anderen Okta-

fähigen Konto auf Tableau zuzugreifen, können Sitzungsdaten aus den Administratordaten den Fehler "Bad Request" verursachen. Wenn dieser Fehler auch dann noch auftritt, wenn Sie den lokalen Browser-Cache löschen, versuchen Sie, das Tableau-Szenario zu validieren, indem Sie eine Verbindung mit einem anderen Browser herstellen.

Eine weitere Ursache für Fehler vom Typ "Bad Request" (ungültige Anforderung) sind Schreibfehler in einer der vielen URLs, die Sie während der Okta-, Mellon- und SAML-Konfigurationsprozesse eingeben. Überprüfen Sie alle diese Eingaben sorgfältig.

Oft gibt die HTTPD-Datei `error.log` auf dem Apache-Server an, welche URL den Fehler verursacht.

Not Found – The requested URL was not found on this server: Diese Fehlermeldung weist auf einen von vielen Konfigurationsfehlern hin.

Wenn der Benutzer mit Okta authentifiziert ist und dann diese Fehlermeldung erhält, haben Sie wahrscheinlich die Vor-Authentifizierungsanwendung von Okta bei der Konfiguration von SAML auf Tableau Server hochgeladen. Stellen Sie sicher, dass Sie die Metadaten der Tableau Server-Anwendung von Okta auf Tableau Server konfiguriert haben und nicht die Metadaten der Vor-Authentifizierungsanwendung von Okta.

Weitere Fehlerbehebungsschritte

- Überprüfen Sie die Datei `tableau.conf` sorgfältig auf Tippfehler oder Konfigurationsfehler.
- Überprüfen Sie die Einstellungen der Vor-Authentifizierungsanwendung von Okta. Stellen Sie sicher, dass die Protokolle HTTP und HTTPS wie in diesem Thema beschrieben festgelegt sind.
- Starten Sie httpd auf beiden Proxyservern neu.
- Überprüfen Sie, ob `sudo apachectl configtest` auf beiden Proxyservern "Syntax OK" zurückgibt.
- Stellen Sie sicher, dass der Testbenutzer in Okta beiden Anwendungen zugewiesen ist.
- Überprüfen Sie, ob die Stickiness-Funktion für das Lastenausgleichsmodul und die zugehörigen Zielgruppen aktiviert ist.

Konfigurieren von SSL/TLS vom Lastenausgleichsmodul zu Tableau Server

Einige Organisationen verlangen eine Ende-zu-Ende-Verschlüsselung vom Client zum Backend-Dienst. Die bis hierhin beschriebene Standardreferenzarchitektur sieht SSL vom Client zum Lastenausgleich vor, der in der Webschicht Ihrer Organisation ausgeführt wird.

Um SSL vom Lastenausgleich zu Tableau Server zu konfigurieren, müssen Sie Folgendes tun:

- Installieren Sie ein gültiges SSL-Zertifikat sowohl auf dem Tableau- als auch auf dem Proxyserver.
- Konfigurieren Sie SSL vom Lastenausgleich zu den Reverse-Proxyservern.
- Konfigurieren Sie SSL von den Proxyservern zu Tableau Server.
- Sie können auch SSL zwischen Tableau Server und der PostgreSQL-Instanz konfigurieren.

Der Rest dieses Themas beschreibt diese Implementierung im Kontext der AWS-Beispielreferenzarchitektur.

Beispiel: Konfigurieren von SSL/TLS in der AWS-Referenzarchitektur

In diesem Abschnitt wird beschrieben, wie Sie SSL auf Tableau konfigurieren und SSL auf einem Apache-Proxyserver konfigurieren – wobei alles in der beispielhaften AWS-Referenzarchitektur ausgeführt wird.

Die Linux-Beispiele in diesem Abschnitt zeigen Befehle für RHEL-ähnliche Distributionen. Die hier angegebenen spezifischen Befehle wurden mit der Amazon Linux 2-Distribution entwickelt. Wenn Sie die Ubuntu-Distribution ausführen, bearbeiten Sie die Befehle entsprechend.

Schritt 1: Sammeln von Zertifikaten und zugehörigen Schlüsseln

Zur Vereinfachung der Zertifikatsverwaltung und -bereitstellung sowie als bewährte Sicherheitspraxis empfehlen wir die Verwendung von Zertifikaten, die von einer bedeutenden vertrauenswürdigen Zertifizierungsstelle (CA) eines Drittanbieters erstellt wurden.

Alternativ dazu können Sie auch selbstsignierte Zertifikate generieren oder Zertifikate von einer PKI für TLS verwenden.

Im Folgenden wird beschrieben, wie Sie selbstsignierte Zertifikate erstellen. Wenn Sie, wie von uns empfohlen, Zertifikate von Drittanbietern verwenden, können Sie diesen Vorgang überspringen.

Führen Sie dieses Verfahren auf einem der Proxy-Hosts aus. Nachdem Sie das Zertifikat und den zugehörigen Schlüssel generiert haben, werden Sie es für den anderen Proxy-Host und Tableau Server-Knoten 1 freigeben.

1. Generieren Sie den Schlüssel der signierenden Stammzertifizierungsstelle (CA):

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

2. Erstellen Sie das Zertifikat der Stammzertifizierungsstelle:

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

   Sie werden aufgefordert, Werte für die Zertifikatfelder einzugeben. Beispiel:

   ```
   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)
   ```

```
[]:tableau.example.com
Email Address []:example@tableau.com
```

3. Erstellen Sie das Zertifikat und den zugehörigen Schlüssel (im Beispiel unten als `serverssl.csr` und `serverssl.key` bezeichnet). Der Antragstellername ("Subject Name") für das Zertifikat muss mit dem öffentlichen Hostnamen des Tableau-Hosts übereinstimmen. Der Antragstellername wird mit der Option `-subj` im Format `"/CN=<host-name>"` festgelegt, beispielsweise:

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

4. Signieren Sie das neue Zertifikat mit dem CA-Zertifikat, das Sie in Schritt 2 erstellt haben. Der folgende Befehl gibt das Zertifikat auch im `crt`-Format aus:

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

Schritt 2: Konfigurieren von Proxyservern für SSL

Führen Sie dieses Verfahren auf beiden Proxyservern aus.

1. Installieren Sie das Apache-SSL-Modul:

   ```
   sudo yum install mod_ssl
   ```

2. Erstellen Sie das Verzeichnis `/etc/ssl/private`:

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

3. Kopieren Sie die Zertifikat- und die Schlüsseldatei in die folgenden `/etc/ssl/`-Pfade:

   ```
   sudo cp serverssl.crt /etc/ssl/certs/

   sudo cp serverssl.key /etc/ssl/private/
   ```

4. Aktualisieren Sie die vorhandene `tableau.conf`-Datei mit den folgenden Änderungen:

    - Fügen Sie den SSL-Rewrite-Block hinzu:

      ```
      RewriteEngine on
      RewriteCond %{SERVER_NAME} =tableau.example.com
      RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI}
      [END,NE,R=permanent]
      ```

    - Aktualisieren Sie im SSL-Rewrite-Block den`RewriteCond`-Servernamen: Fügen Sie Ihren öffentlichen Hostnamen hinzu, zum Beispiel `tableau.example.com`
    - Ändern Sie `<VirtualHost *:80>` zu `<VirtualHost *:443>`.
    - Schließen Sie die `<VirtualHost *:443>`- und `<Location />`-Blöcke mit `<IfModule mod_ssl.c>` ... `</IfModule>`.
    - `BalancerMember`: Ändern Sie das Protokoll von `http` zu `https`.
    - Fügen Sie `SSL*`-Elemente innerhalb des `<VirtualHost *:443>`-Blocks hinzu:

      ```
      SSLEngine on
      SSLCertificateFile /etc/ssl/certs/serverssl.crt
      SSLCertificateKeyFile /etc/ssl/private/serverssl.key
      SSLProxyEngine on
      SSLProxyVerify none
      SSLProxyCheckPeerName off
      SSLProxyCheckPeerExpire off
      ```

    - Fügen Sie in dem `LogLevel`-Element die Zeichenfolge `ssl:warn` hinzu.
    - Optional: Wenn Sie ein Authentifizierungsmodul installiert und konfiguriert haben, enthält die tableau.conf-Datei möglicherweise weitere Elemente. So wird zum Beispiel der `<Location /> </Location>`-Block über Elemente verfügen.

    So sieht eine für SSL konfigurierte tableau.conf-Beispieldatei aus:

    ```
    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. Fügen Sie die Datei "index.html" hinzu, um 403-Fehler zu unterdrücken:

   ```
   sudo touch /var/www/html/index.html
   ```

6. Starten Sie httpd neu:

   ```
   sudo systemctl restart httpd
   ```

Schritt 3: Konfigurieren von Tableau Server für externes SSL

Kopieren Sie die Dateien serverssl.crt und serverssl.key vom Proxy 1-Host auf den ursprünglichen Tableau Server (Knoten 1).

Führen Sie die folgenden Befehle auf Knoten 1 aus:

```
tsm security external-ssl enable --cert-file serverssl.crt --key-
file serverssl.key
tsm pending-changes apply
```

Schritt 4: Optionale Authentifizierungskonfiguration

Wenn Sie einen externen Identitätsanbieter für Tableau konfiguriert haben, müssen Sie wahrscheinlich die Rückgabe-URLs im IdP-Verwaltungsdashboard aktualisieren.

Wenn Sie beispielsweise eine Vor-Authentifizierungsanwendung von Okta verwenden, müssen Sie die Anwendung so aktualisieren, dass das HTTPS-Protokoll für die Empfänger-URL und die Ziel-URL verwendet wird.

Schritt 5: Konfigurieren von AWS-Lastenausgleich für HTTPS

Wenn Sie – wie in diesem Handbuch beschrieben – mit AWS-Lastenausgleich bereitstellen, ändern Sie die Konfiguration so, dass der AWS-Lastenausgleich HTTPS-Datenverkehr an die Proxyserver sendet:

1. Heben Sie die Registrierung der vorhandenen HTTP-Zielgruppe auf:

   Wählen Sie in **Target Groups** (Zielgruppen) die HTTP-Zielgruppe aus, die für den Lastenausgleich konfiguriert wurde, klicken Sie auf **Actions** (Aktionen), und klicken Sie dann auf **Register and deregister instance** (Registrierung von Instanz vornehmen und aufheben).

   Wählen Sie auf der Seite **Register and deregister targets** (Registrierung von Zielen vornehmen und aufheben) die Instanzen aus, die derzeit konfiguriert sind, klicken Sie auf **Deregister** (Registrierung aufheben) und klicken Sie dann auf **Save** (Speichern).

2. Erstellen Sie die HTTPS-Zielgruppe:

   Zielgruppen (Zielgruppen) > **Create target group** (Zielgruppe erstellen)

   - Wählen Sie "Instances" (Instanzen) aus.
   - Geben Sie einen Zielgruppennamen ein, zum Beispiel `TG-internal-HTTPS`.
   - Wählen Sie Ihre VPC aus.
   - Protokoll: HTTPS 443
   - Fügen Sie unter **Health checks** (Integritätsprüfungen) > **Advanced health checks settings** (Einstellungen für erweiterte Integritätsprüfungen) > **Success codes** (Erfolgscodes) die Codeliste zum Lesen hinzu: `200,303`.
   - Klicken Sie auf **Erstellen**.

3. Wählen Sie die Zielgruppe aus, die Sie eben erstellt haben, und klicken Sie dann auf die Registerkarte **Targets** (Ziele):

   - Klicken Sie auf **Edit** (Bearbeiten).
   - Wählen Sie die EC2-Instanzen aus, auf denen die Proxyanwendung ausgeführt wird, und klicken Sie dann auf **Add to registered** (Zu registriert hinzufügen).
   - Klicken Sie auf **Speichern**.

4. Nachdem die Zielgruppe erstellt wurde, müssen Sie "Stickiness" aktivieren:

   - Öffnen Sie die AWS-Seite für die Zielgruppe (**EC2** > **Load Balancing** (Lastenausgleich) > **Target groups** (Zielgruppen)), und wählen Sie die Zielgruppeninstanz aus, die Sie gerade eingerichtet haben. Wählen Sie im Menü

Actions (Aktionen) die Option **Edit attributes** (Attribute bearbeiten) aus.
- Wählen Sie auf der Seite **Edit attributes** (Attribute bearbeiten) die Option **Stickiness** (Bindung) aus, geben Sie eine Zeitdauer von `1 day` (1 Tag) an, und klicken Sie dann auf **Save changes** (Änderungen speichern).

5. Aktualisieren Sie für den Lastenausgleich die Listener-Regeln. Wählen Sie den Lastenausgleich aus, den Sie für diese Bereitstellung konfiguriert haben, und klicken Sie dann auf die Registerkarte **Listeners**.

    - Klicken Sie für **HTTP:80** auf **View/edit rules** (Regeln anzeigen/bearbeiten). Klicken Sie auf der Seite **Rules** (Regeln), die daraufhin angezeigt wird, auf das Bearbeitungssymbol (zuerst oben auf der Seite und dann noch einmal für die Regel), um die Regel zu bearbeiten. Löschen Sie die vorhandene THEN-Regel ("DANN") und ersetzen Sie sie, indem Sie auf **Add action** (Aktion hinzufügen) > **Redirect to...** (Umleiten an...) klicken. Geben Sie in der daraus resultierenden THEN-Konfiguration `HTTPS` und Port `443` an und belassen Sie die anderen Optionen auf den Standardeinstellungen. Speichern Sie die Einstellung und klicken Sie dann auf **Update** (Aktualisieren).
    - Klicken Sie für **HTTP:443** auf **View/edit rules** (Regeln anzeigen/bearbeiten). Klicken Sie auf der Seite **Rules** (Regeln), die daraufhin angezeigt wird, auf das Bearbeitungssymbol (zuerst oben auf der Seite und dann noch einmal für die Regel), um die Regel zu bearbeiten. Ändern Sie in der **THEN**-Konfiguration unter **Forward to...** (Weiterleiten an...) die Zielgruppe in die soeben erstellte HTTPS-Gruppe. Aktivieren Sie unter **Group-level stickiness** (Bindung auf Gruppenebene) den Punkt "Stickiness", und legen Sie "Duration" (Zeitdauer) auf "1 Day" (1 Tag) fest. Speichern Sie die Einstellung und klicken Sie dann auf **Update** (Aktualisieren).

Schritt 6: Überprüfen von SSL

Überprüfen Sie die Konfiguration, indem Sie zu https://tableau.example.com navigieren.