Tableau Server per le organizzazioni di grandi dimensioni Guida alla distribuzione

Ultimo aggiornamento 13/02/2025

Contenuti

Guida alla distribuzione di Tableau Server per le organizzazioni di grandi dimensioni

La Guida alla distribuzione di Tableau Server per le organizzazioni di grandi dimensioni è stata sviluppata per fornire indicazioni prescrittive per la distribuzione di Tableau Server (in locale o nel cloud). La guida fornisce indicazioni di distribuzione per gli scenari aziendali nel contesto di un'architettura di riferimento. Abbiamo testato l'architettura di riferimento per verificare la conformità ai benchmark di sicurezza, scalabilità e prestazioni, a loro volta conformi alle procedure consigliate standard di settore.

A livello generale, le caratteristiche principali di una distribuzione aziendale standard di settore sono costituite da una topologia a più livelli in cui ogni livello di funzionalità dell'applicazione server (livello gateway Web, livello applicazione e livello dati) è vincolato e protetto da subnet con controllo dell'accesso. Gli utenti che accedono all'applicazione server da Internet vengono autenticati al livello Web. Una volta autenticata, la richiesta viene inviata tramite proxy a una subnet protetta, in cui il livello dell'applicazione gestisce la logica business. I dati di alto valore sono protetti dalla terza subnet: il livello dati. I servizi nel livello applicazione comunicano tramite la rete protetta con il livello dati per trasmettere le richieste di dati alle origini dati back-end.

In questa distribuzione, la sicurezza è al primo posto in tutte le decisioni di progettazione e implementazione. Tuttavia, anche l'affidabilità, le prestazioni e la scalabilità sono requisiti prioritari. Dato il design distribuito e modulare dell'architettura di riferimento, l'affidabilità e le prestazioni scalano in modo lineare e prevedibile, posizionando strategicamente i servizi compatibili in ogni nodo e aggiungendo servizi ai colli di bottiglia.

Chi dovrebbe leggere questa guida

La Guida alla distribuzione per le organizzazioni di grandi dimensioni è stata sviluppata per gli amministratori IT aziendali che potrebbero richiedere:

- Una distribuzione di Tableau gestita dal reparto IT
- Applicazione della conformità a livello di settore
- Procedure consigliate per l'implementazione a livello di settore
- Distribuzione sicura per impostazione predefinita

La Guida alla distribuzione per le organizzazioni di grandi dimensioni è una guida all'implementazione per la distribuzione dell'architettura di riferimento aziendale. Sebbene questa versione includa un esempio di implementazione AWS/Linux, la guida può essere utilizzata come risorsa dagli amministratori IT aziendali esperti per distribuire l'architettura di riferimento prescritta in qualsiasi ambiente di data center standard di settore.

Versione

Questa versione della Guida alla distribuzione per le organizzazioni di grandi dimensioni è stata sviluppata per la versione 2021.2.3 (o successive) di Tableau Server. Sebbene sia possibile utilizzare questa guida come riferimento generale per la distribuzione delle versioni precedenti di Tableau Server, è consigliabile distribuire l'architettura di riferimento con Tableau Server 2021.2.3 o versioni successive. Alcune funzionalità e opzioni non sono disponibili nelle versioni precedenti di Tableau Server.

Per le funzionalità e i miglioramenti più aggiornati, è consigliabile distribuire la Guida alla distribuzione per le organizzazioni di grandi dimensioni con Tableau Server 2022.1.7 e versioni successive.

L'architettura di riferimento descritta in questa guida supporta i seguenti client Tableau: Web authoring con browser compatibili, Tableau Mobile e Tableau Desktop versione 2021.2.1 o successive. Gli altri client Tableau (Tableau Prep, Bridge e così via) non sono stati ancora convalidati con l'architettura di riferimento.

Funzionalità in evidenza

La prima versione dell'architettura di riferimento di Tableau Server introduce gli scenari e le funzionalità seguenti:

- Pre-autenticazione dei client: i client Tableau (Desktop, Mobile, Web authoring) eseguono l'autenticazione con il provider di autenticazione aziendale nel livello Web prima di accedere al sistema Tableau Server interno. Questo processo è gestito configurando un plug-in AuthN sul gateway indipendente Tableau Server che funge da server proxy inverso. Consulta Parte 5 - Configurazione del livello Web.
- Distribuzione "zero trust": poiché tutto il traffico verso Tableau Server è pre-autenticato, l'intera distribuzione di Tableau opera in una subnet privata che non richiede una connessione attendibile.
- Repository esterno: l'architettura di riferimento specifica l'installazione del repository di Tableau su un database PostgreSQL esterno, consentendo agli amministratori di database di gestire, ottimizzare, ridimensionare ed eseguire il backup del repository come un database generico.
- Ripristino del nodo iniziale: la Guida alla distribuzione per le organizzazioni di grandi dimensioni introduce uno script che automatizza il ripristino del nodo iniziale in caso di errore.
- Backup e ripristino basati su file tar: utilizza i backup tar nelle fasi strategiche della distribuzione di Tableau. In caso di errore o di configurazione errata della distribuzione, potrai ripristinare rapidamente la fase di distribuzione precedente eseguendo il ripristino del backup tar corrispondente.
- Miglioramento delle prestazioni: la convalida presso i clienti e in laboratorio mostra un miglioramento delle prestazioni del 15-20% durante l'esecuzione della Guida alla distribuzione per le organizzazioni di grandi dimensioni rispetto alla distribuzione standard.

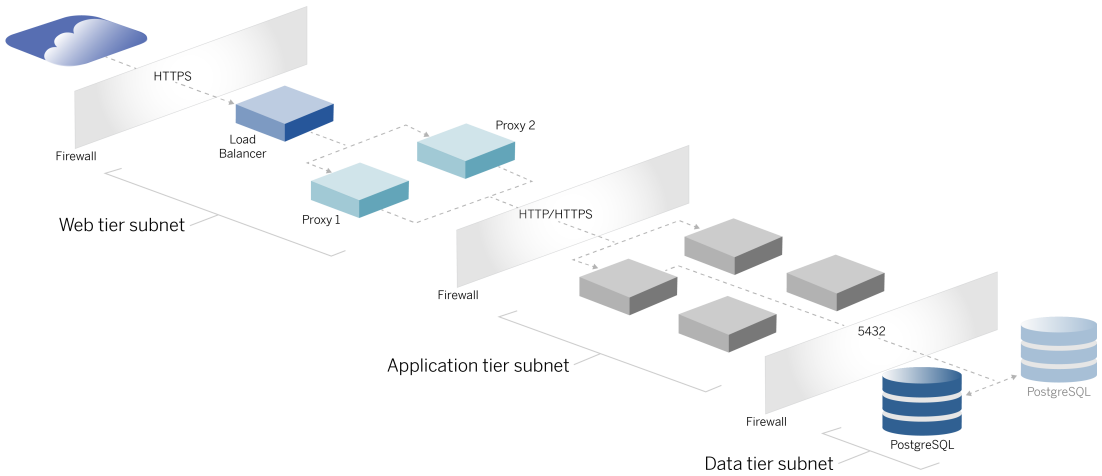
Gestione licenze

L'architettura di riferimento di Tableau Server prescritta in questa Guida richiede una licenza per Tableau Advanced Management per abilitare il repository esterno di Tableau Server. Puoi anche distribuire facoltativamente l'archivio file esterno di Tableau Server, che richiede anche la licenza per Tableau Advanced Management. Consulta *Informazioni su Tableau Advanced Management Add-on in Tableau Server* (Linux).

Parte 1 - Informazioni sulla distribuzione per le organizzazioni di grandi dimensioni

La parte 1 descrive, in modo più dettagliato, le caratteristiche e i requisiti della distribuzione standard di settore per cui è stata progettata la Guida alla distribuzione di Tableau Server per le organizzazioni di grandi dimensioni.

Il seguente diagramma di rete mostra una distribuzione generica a più livelli di un data center con l'architettura di riferimento di Tableau Server.



Standard di settore e requisiti di implementazione

Di seguito sono riportate le caratteristiche delle distribuzioni standard di settore. Questi sono i requisiti per cui è stata progettata l'architettura di riferimento:

- Una struttura di rete a più livelli: la rete è vincolata da subnet protette per limitare l'accesso a ogni livello, ovvero livello Web, livello applicazione e livello dati. Nessuna

singola comunicazione è in grado di passare attraverso le subnet, poiché tutte le comunicazioni vengono terminate nella subnet successiva.
- Porte e protocolli bloccati per impostazione predefinita: ogni subnet o gruppo di sicurezza bloccherà tutte le porte e i protocolli in ingresso e in uscita per impostazione predefinita. La comunicazione viene abilitata, in parte, aprendo eccezioni nella configurazione di porta o protocollo.
- Autenticazione Web off-box: le richieste degli utenti da Internet vengono autenticate da un modulo di autenticazione sul proxy inverso nel livello Web. Pertanto, tutte le richieste al livello applicazione vengono autenticate nel livello Web prima di passare al livello applicazione protetto.
- Indipendenza dalla piattaforma: la soluzione può essere distribuita con applicazioni server in locale o nel cloud.
- Indipendenza dalla tecnologia: la soluzione può essere distribuita in un ambiente con macchine virtuali o in contenitori. Può anche essere distribuita in Windows o Linux. Tuttavia, questa versione iniziale dell'architettura di riferimento e della documentazione di supporto è stata sviluppata per Linux in esecuzione in AWS.
- Disponibilità elevata: tutti i componenti del sistema sono distribuiti come un cluster e progettati per operare in una distribuzione attiva/attiva o attiva/passiva.
- Ruoli isolati: ogni server esegue un ruolo distinto. Questa struttura partiziona tutti i server in modo da ridurre al minimo l'accesso agli amministratori specifici del servizio. Ad esempio, gli amministratori di database gestiscono PostgreSQL per Tableau, gli amministratori dell'identità gestiscono il modulo di autenticazione nel livello Web, gli amministratori di rete e cloud abilitano il traffico e la connettività.
- Scalabilità lineare: essendo ruoli distinti, puoi ridimensionare il servizio di ogni livello in modo indipendente in base al profilo del carico.
- Supporto client: l'architettura di riferimento supporta tutti i client Tableau: Tableau Desktop (versioni 2021.2 o successive), Tableau Mobile e Tableau Web Authoring.

Misure di sicurezza

Come accennato, una caratteristica principale della progettazione di un data center standard di settore è la sicurezza.

- Accesso: ogni livello è vincolato da una subnet che applica il controllo dell'accesso a livello di rete utilizzando il filtro della porta. L'accesso alla comunicazione tra le subnet può anche essere imposto dal livello applicazione con servizi autenticati tra i processi.

- Integrazione: l'architettura è progettata per integrarsi con il provider di identità (IdP) sul proxy inverso nel livello Web.
- Privacy: il traffico nel livello Web viene crittografato dal client con SSL. Anche il traffico nelle subnet interne può essere facoltativamente crittografato.

Livello proxy Web

Il livello Web è una subnet nella DMZ (anche denominata zona perimetrale) che opera come buffer di sicurezza tra Internet e le subnet interne in cui vengono distribuite le applicazioni. Il livello Web ospita server proxy inversi che non archiviano informazioni sensibili. I server proxy inversi sono configurati con un plug-in AuthN per pre-autenticare le sessioni client con un IdP attendibile, prima di reindirizzare la richiesta client a Tableau Server. Per maggiori informazioni, consulta Pre-autenticazione con un modulo AuthN.

Servizi di bilanciamento del carico

La struttura della distribuzione include una soluzione di bilanciamento del carico aziendale davanti ai server proxy inversi.

I servizi di bilanciamento del carico forniscono importanti miglioramenti in termini di sicurezza e prestazioni grazie a:

- Virtualizzazione dell'URL front-end per i servizi del livello applicazione
- Applicazione della crittografia SSL
- Offload di SSL
- Applicazione della compressione tra il client e i servizi di livello Web
- Protezione dagli attacchi DOS
- Disponibilità elevata

Nota: Tableau Server versione 2022.1 include Gateway indipendente di Tableau Server. Gateway indipendente è un'istanza autonoma del processo Gateway di Tableau che opera come proxy inverso compatibile con Tableau. Al momento del rilascio, Gateway indipendente è stato convalidato, ma non completamente testato nell'architettura di

riferimento per la Guida alla distribuzione per le organizzazioni di grandi dimensioni. Al termine del test completo, la Guida alla distribuzione per le organizzazioni di grandi dimensioni verrà aggiornata con le linee guida prescrittive di Gateway indipendente di Tableau Server.

Livello applicazione

Il livello applicazione si trova in una subnet che esegue la logica business principale dell'applicazione server. Il livello applicazione è costituito da servizi e processi configurati tra i nodi distribuiti in un cluster. Il livello applicazione è accessibile solo dal livello Web e non è direttamente accessibile dagli utenti.

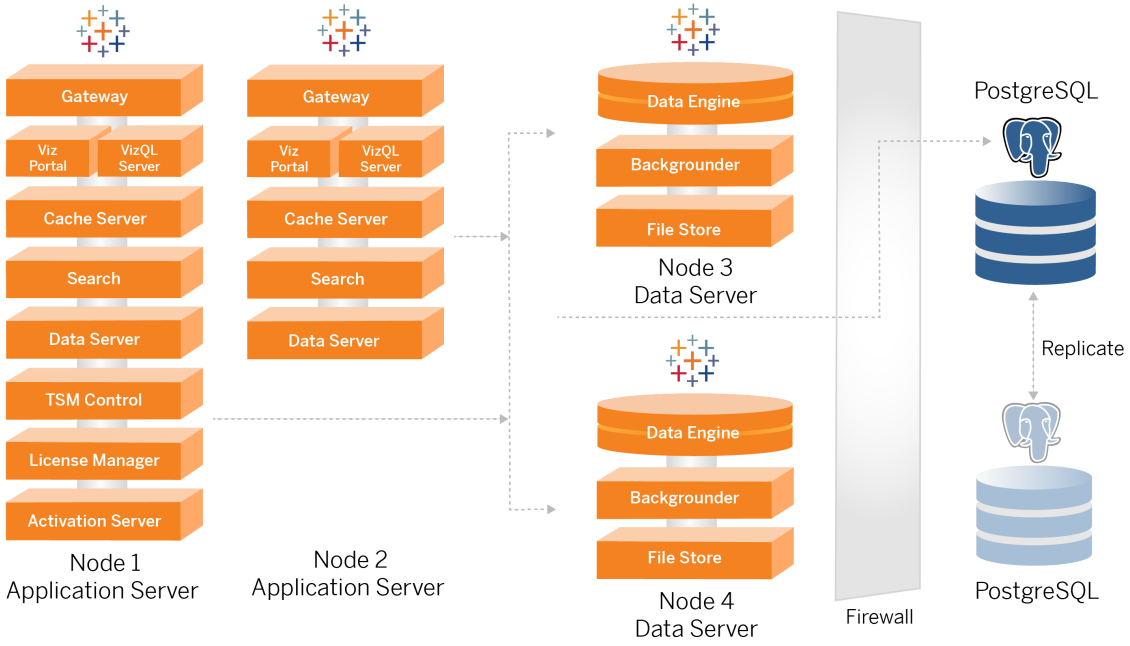
Le prestazioni e l'affidabilità vengono migliorate configurando i processi dell'applicazione in modo tale che i processi con diversi profili di utilizzo delle risorse (ad esempio, utilizzo intensivo della CPU rispetto all'utilizzo intensivo della memoria) siano posizionati insieme.

Livello dati

Il livello dati è una subnet che contiene dati importanti. Tutto il traffico verso questo livello proviene dal livello applicazione ed è quindi già autenticato. Oltre ai requisiti di accesso a livello di rete con la configurazione della porta, questo livello dovrebbe includere l'accesso autenticato e facoltativamente il traffico crittografato con il livello applicazione.

Parte 2 - Informazioni sull'architettura di riferimento per la distribuzione di Tableau Server

L'immagine seguente mostra i processi rilevanti di Tableau Server e come sono distribuiti nell'architettura di riferimento. Questa distribuzione è considerata la distribuzione minima di Tableau Server appropriata per un'organizzazione di grandi dimensioni.



I diagrammi dei processi in questo argomento hanno lo scopo di illustrare i principali processi per ciascun nodo. Nei nodi vengono eseguiti anche molti processi di supporto che non sono mostrati nei diagrammi. Per un elenco di tutti i processi, consulta la sezione di questa guida relativa alla configurazione, Parte 4 - Installazione e configurazione di Tableau Server.

Processi di Tableau Server

L'architettura di riferimento di Tableau Server è una distribuzione cluster di Tableau Server a quattro nodi con il repository esterno in PostgreSQL:

- Nodo iniziale di Tableau Server (Nodo 1): esegue i servizi amministrativi e di licenza di TSM richiesti che possono essere eseguiti solo su un singolo nodo nel cluster. Nel contesto aziendale, il nodo iniziale di Tableau Server è il nodo primario del cluster. Questo nodo esegue anche servizi applicativi ridondanti con il Nodo 2.
- Nodi dell'applicazione Tableau Server (Nodo 1 e Nodo 2): i due nodi elaborano le richieste client, si connettono a origini dati e nodi di dati ed eseguono query.
- Nodi di dati di Tableau Server (Nodo 3 e Nodo 4): due nodi dedicati alla gestione dei dati.
- PostgreSQL esterno: questo host esegue il processo di repository di Tableau Server. Per la distribuzione a disponibilità elevata è necessario eseguire un host PostgreSQL aggiuntivo per la ridondanza attiva/passiva.

  Puoi anche eseguire PostgreSQL su Amazon RDS. Per maggiori informazioni sulle differenze tra l'esecuzione del repository su RDS rispetto a un'istanza EC2, consulta *Repository esterno di Tableau Server* (Linux).

  La distribuzione di Tableau Server con un repository esterno richiede una licenza Tableau Advanced Management.

  Se la tua organizzazione non dispone di competenze interne di amministrazione dei database, puoi facoltativamente eseguire il processo Repository di Tableau Server nella configurazione PostgreSQL interna predefinita. Nello scenario predefinito, il repository viene eseguito su un nodo Tableau con PostgreSQL incorporato. In questo caso, è consigliabile eseguire il repository su un nodo Tableau dedicato e un repository passivo su un nodo dedicato aggiuntivo per supportare il failover del repository. Vedi *Failover del repository* (Linux).

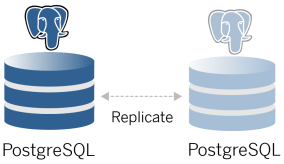
  A titolo di esempio, l'implementazione AWS descritta in questa Guida spiega come distribuire il repository esterno su PostgreSQL in esecuzione in un'istanza EC2.

- Facoltativo: se la tua organizzazione utilizza l'archiviazione esterna, puoi distribuire l'archivio file di Tableau come servizio esterno. Questa guida non include l'archivio file esterno nello scenario di distribuzione principale. Vedi *Installare Tableau Server con l'archivio file esterno* (Linux).

  La distribuzione di Tableau Server con un Archivio file esterno richiede una licenza Tableau Advanced Management.

Repository PostgresSQL

Il repository di Tableau Server è un database che archivia i dati del server. Questi dati includono informazioni sugli utenti di Tableau Server, i gruppi e le assegnazioni di gruppo, le autorizzazioni, i progetti, le origini dati, l'estrazione di metadati e le informazioni di aggiornamento.



La distribuzione predefinita di PostgresSQL utilizza quasi il 50% delle risorse di memoria del sistema. In base al relativo utilizzo (per distribuzioni di produzione e di grandi dimensioni), l'utilizzo delle risorse può aumentare. Per questo motivo, è consigliabile eseguire il processo Repository in un computer che non esegue altri componenti server con un utilizzo intensivo delle risorse, come VizQL, Gestione componenti in background o Motore dati. L'esecuzione del processo Repository insieme a uno di questi componenti creerà conflitti di I/O o vincoli di risorse e ridurrà le prestazioni complessive della distribuzione.

Nodo 1: nodo iniziale

Il nodo iniziale esegue un numero limitato di processi importanti e condivide il carico dell'applicazione con il Nodo 2.

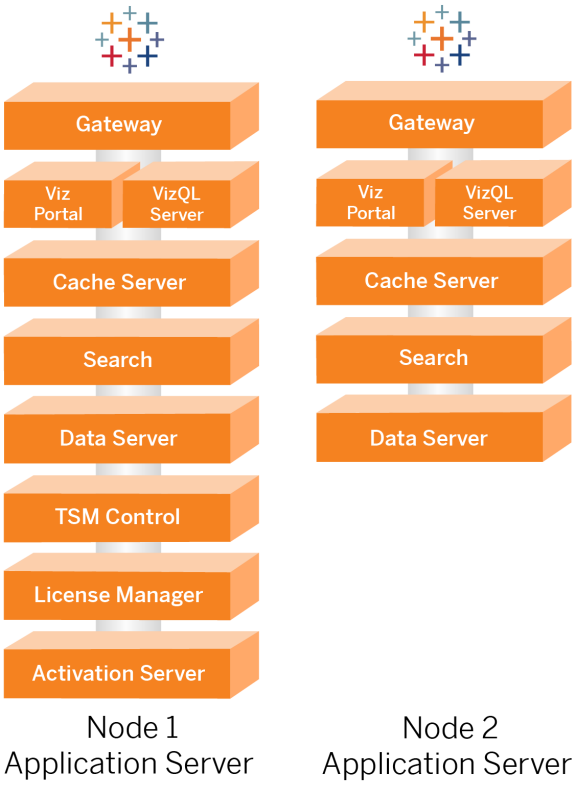
Il primo computer su cui si installa Tableau, il "nodo iniziale", ha alcune caratteristiche uniche. Tre processi, il servizio licenze (Gestione licenze), il servizio di attivazione e il controller TSM

(Controller di amministrazione), vengono eseguiti solo sul nodo iniziale e non possono essere spostati su nessun altro nodo, se non in caso di guasto.

Failover e ripristino automatizzato del Nodo 1

Il servizio licenze, quello di attivazione e il controller TSM sono fondamentali per l'integrità di una distribuzione di Tableau Server. In caso di errore del Nodo 1, gli utenti potranno comunque connettersi alla distribuzione di Tableau Server, poiché un'architettura di riferimento configurata correttamente indirizzerà le richieste al Nodo 2. Tuttavia, senza questi servizi di base, la distribuzione sarà in uno stato critico di errore in sospeso. Vedi Ripristino automatizzato del nodo iniziale.

Nodi 1 e 2: server applicazioni



I Nodi 1 e 2 eseguono i processi di Tableau Server che elaborano le richieste client, eseguono query sulle origini dati, generano visualizzazioni, gestiscono il contenuto e l'amministrazione e altre funzionalità principali della logica di business di Tableau. I server applicazioni non memorizzano i dati degli utenti.

Nota: "Server applicazioni" è un termine che si riferisce anche a un processo di Tableau Server elencato in TSM. Il processo sottostante per "Server applicazioni" è VizPortal.

Eseguiti in parallelo, il Nodo 1 e il Nodo 2 si adattano alle richieste di servizio dalla logica di bilanciamento del carico eseguite sui server proxy inversi. In quanto nodi ridondanti, in caso di problemi di uno di questi nodi, le richieste e i servizi client vengono gestiti dal nodo rimanente.

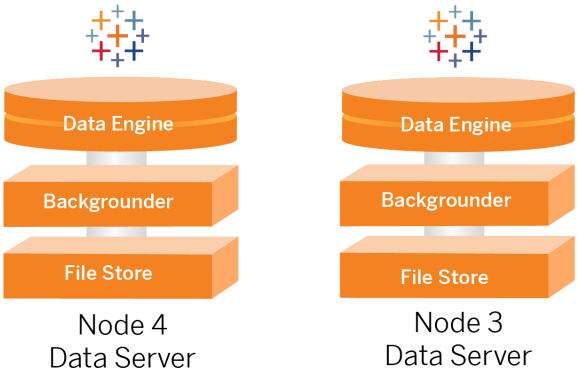
L'architettura di riferimento è stata progettata in modo che processi applicativi complementari vengano eseguiti sullo stesso computer. Ciò significa che i processi non sono in competizione per le risorse di calcolo e non creano contese.

Ad esempio, VizQL, un servizio di elaborazione di base nei server applicazioni, è altamente vincolato dalla CPU e dalla memoria: utilizza quasi il 60-70% della CPU e della memoria del computer. Per questo motivo, l'architettura di riferimento è progettata in modo che nessun altro processo vincolato dalla memoria o dalla CPU si trovi nello stesso nodo di VizQL. I test mostrano che la quantità di carico o il numero di utenti non influisce sull'utilizzo della memoria o della CPU nei nodi VizQL. Ad esempio, la riduzione del numero di utenti simultanei nel nostro test di carico ha effetto solo sulle prestazioni del processo di caricamento della dashboard o della visualizzazione, ma non riduce l'utilizzo delle risorse. Pertanto, in base alla disponibilità di memoria e CPU durante i picchi di utilizzo, potresti prendere in considerazione l'aggiunta di più processi VizQL. Come punto di partenza per cartelle di lavoro tipiche, alloca 4 core per ogni processo VizQL.

Scalabilità dei server applicazioni

L'architettura di riferimento è progettata per la scalabilità in base a un modello basato sull'utilizzo. Come punto di partenza generale, è consigliabile un minimo di due server applicazioni, ciascuno dei quali supporta fino a 1000 utenti. Con l'aumento della base di utenti, pianifica l'aggiunta di un server applicazioni per ogni 1000 utenti aggiuntivi. Monitora l'utilizzo e le prestazioni per ottimizzare la base di utenti per ogni host dell'organizzazione.

Nodi 3 e 4: Data Server



I processi Archivio file, Motore dati (Hyper) e Gestione componenti in background si trovano nei Nodi 3 e 4 per i seguenti motivi:

- Ottimizzazione dell'estrazione: l'esecuzione di Gestione componenti in background, Hyper e Archivio file nello stesso nodo ottimizza le prestazioni e l'affidabilità. Durante il processo di estrazione, Gestione componenti in background esegue query sul database di destinazione, crea il file Hyper sullo stesso nodo e quindi effettua il caricamento nell'archivio file. Posizionando insieme questi processi nello stesso nodo, il flusso di lavoro di creazione delle estrazioni non richiede la copia di volumi elevati di dati attraverso la rete o i nodi.
- Bilanciamento delle risorse complementare: Gestione componenti in background richiede principalmente risorse CPU. Motore dati è un processo che richiede molta memoria. L'associazione di questi processi consente il massimo utilizzo delle risorse in ciascun nodo.
- Consolidamento dei processi dati: poiché tutti questi processi sono processi dati back-end, è opportuno eseguirli nel livello di dati più sicuro. Nelle versioni future

dell'architettura di riferimento, i server applicazioni e i Data Server verranno eseguiti in livelli distinti. Tuttavia, a causa delle dipendenze dell'applicazione nell'architettura di Tableau, attualmente i server applicazioni e i Data Server devono essere eseguiti nello stesso livello.

Scalabilità dei Data Server

Come nel caso dei server applicazioni, la pianificazione delle risorse necessarie per i Data Server di Tableau richiede la modellazione basata sull'utilizzo. In generale, presupponi che ogni Data Server possa supportare fino a 2000 processi di aggiornamento delle estrazioni al giorno. Con l'aumento dei processi di estrazione, aggiungi altri Data Server senza il servizio Archivio file. In genere, la distribuzione del Data Server a due nodi è adatta per le distribuzioni che utilizzano il file system locale per il servizio Archivio file. Tieni presente che l'aggiunta di altri server applicazioni non influisce in modo lineare sulle prestazioni o sulla scalabilità dei Data Server. Infatti, con l'eccezione di un sovraccarico derivante da ulteriori query degli utenti, l'impatto dell'aggiunta di più host e utenti dell'applicazione è minimo.

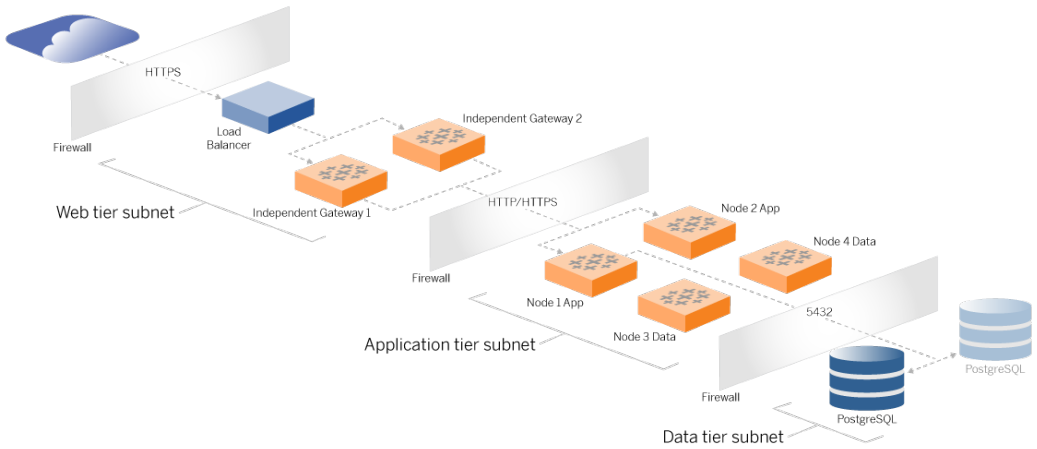
Parte 3 - Preparazione per la distribuzione di Tableau Server per le organizzazioni di grandi dimensioni

Nella parte 3 sono descritti i requisiti per preparare la tua infrastruttura alla distribuzione dell'architettura di riferimento di Tableau Server. Prima di iniziare, è consigliabile esaminare la sezione Parte 2 - Informazioni sull'architettura di riferimento per la distribuzione di Tableau Server.

Oltre alle descrizioni dei requisiti, questo argomento fornisce un esempio di implementazione dell'architettura di riferimento in un ambiente AWS. Il resto di questa guida si basa sull'esempio dell'architettura di riferimento AWS iniziato in questo argomento.

Un principio fondamentale dell'architettura di riferimento è la standardizzazione con le procedure consigliate di sicurezza per i data center. In particolare, l'architettura è progettata per separare i servizi in subnet di rete protette. La comunicazione tra le subnet è limitata al traffico di protocolli e porte specifici.

Il diagramma seguente illustra la progettazione delle subnet dell'architettura di riferimento per una distribuzione in locale o una distribuzione cloud gestita dal cliente. Per un esempio di distribuzione cloud, consulta la sezione seguente Esempio: configurare subnet e gruppi di sicurezza in AWS.



Subnet

Crea tre subnet:

- Un livello Web
- Un livello applicazione
- Una subnet dati.

Regole firewall/dei gruppi di sicurezza

Le schede seguenti descrivono le regole firewall per ogni livello del data center. Per le regole dei gruppi di sicurezza specifiche di AWS, consulta la sezione più avanti in questo argomento.

Livello Web

Il livello Web è una subnet DMZ pubblica che gestirà le richieste HTTPS in entrata e invierà le richieste al livello applicazione. Questa struttura fornisce un livello di difesa dal malware che potrebbe colpire la tua organizzazione. Il livello Web blocca l'accesso al livello applicazione/dati.

Traffico	Tipo	Protocollo	Intervallo di porte	Origine
In entrata	SSH	TCP	22	Subnet bastion (per le distribuzioni cloud)
In entrata	HTTP	TCP	80	Internet (0.0.0.0/0)
In entrata	HTTPS	TCP	443	Internet (0.0.0.0/0)
In uscita	Tutto il traffico	Tutti	Tutti	

Livello applicazione

La subnet applicazione è quella in cui risiede la distribuzione di Tableau Server. La subnet applicazione include i server applicazioni di Tableau (Nodo 1 e Nodo 2). I server applicazioni di Tableau elaborano le richieste degli utenti ai Data Server ed eseguono la logica di business principale.

La subnet applicazione include anche i Data Server di Tableau (Nodo 3 e Nodo 4).

Tutto il traffico client verso il livello applicazione viene autenticato al livello Web. L'accesso amministrativo alla subnet applicazione viene autenticato e instradato tramite l'host bastion.

Traffico	Tipo	Protocollo	Intervallo di porte	Origine
In entrata	SSH	TCP	22	Subnet bastion (per le distribuzioni cloud)
In entrata	HTTPS	TCP	443	Subnet del livello Web
In uscita	Tutto il traffico	Tutti	Tutti	

Livello dati

La subnet dei dati è quella in cui risiede il server di database PostgreSQL esterno.

Traffico	Tipo	Protocollo	Intervallo di porte	Origine
In entrata	SSH	TCP	22	Subnet bastion (per le distribuzioni cloud)
In entrata	PostgreSQL	TCP	5432	Subnet del livello applicazione
In uscita	Tutto il traffico	Tutti	Tutti	

Bastion

La maggior parte dei team di sicurezza aziendale non consente la comunicazione diretta dal sistema amministrativo locale ai nodi distribuiti nel cloud. Invece, tutto il traffico SSH amministrativo verso i nodi cloud viene inoltrato tramite proxy attraverso un host bastion (anche denominato "server jump"). Per le distribuzioni cloud, è consigliabile una connessione proxy host bastion a tutte le risorse nell'architettura di riferimento. Questa è una configurazione facoltativa per gli ambienti locali.

L'host bastion autentica l'accesso amministrativo e consente solo il traffico tramite il protocollo SSH.

Traffico	Tipo	Protocollo	Intervallo di porte	Origine	Destinazione
In entrata	SSH	TCP	22	Indirizzo IP del computer di amministrazione	

In uscita	SSH	TCP	22		Subnet del livello Web
In uscita	SSH	TCP	22		Subnet del livello applicazione

Esempio: configurare subnet e gruppi di sicurezza in AWS

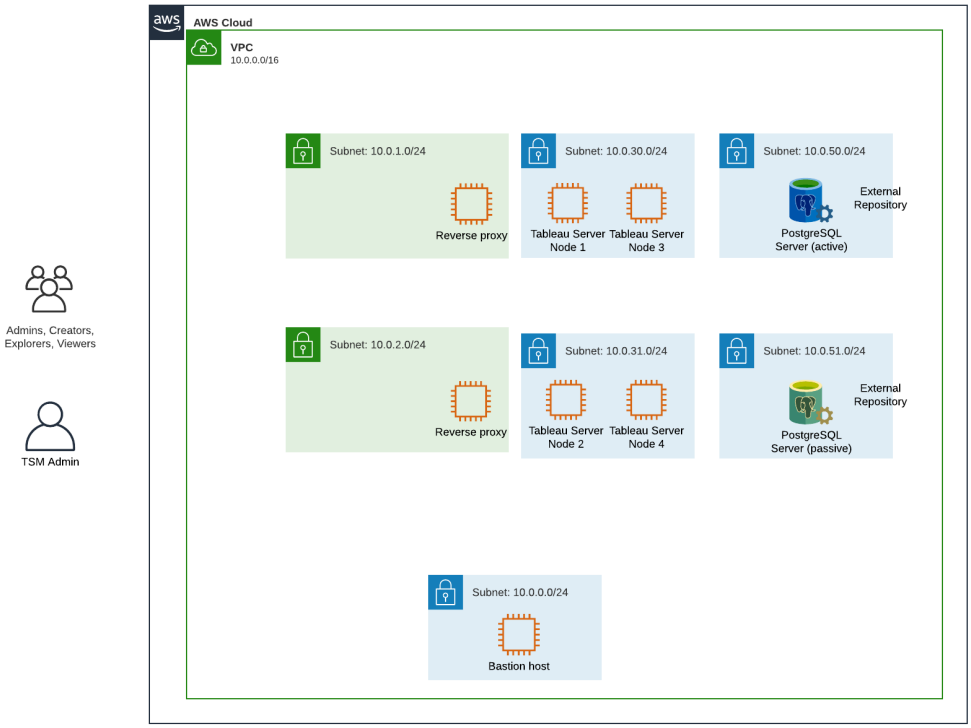
In questa sezione vengono fornite le procedure dettagliate per creare e configurare l'ambiente VPC e di rete per la distribuzione dell'architettura di riferimento di Tableau Server in AWS.

Le diapositive seguenti mostrano l'architettura di riferimento in quattro livelli. Man mano che procedi nelle diapositive, gli elementi dei componenti vengono sovrapposti sulla mappa della topologia:

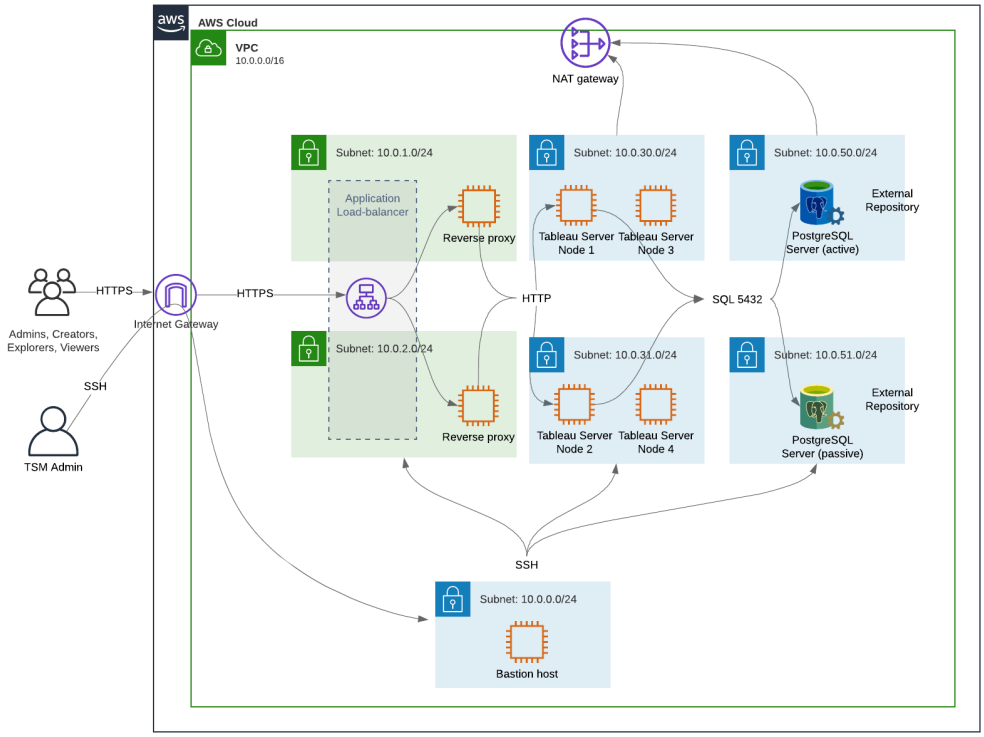
1. Topologia della sottorete VPC e istanze EC2: un host bastion, due server proxy inversi, quattro sistemi Tableau Server e almeno un server PostgreSQL.
2. Flusso del protocollo e connettività Internet. Tutto il traffico in entrata viene gestito tramite il gateway Internet di AWS. Il traffico verso Internet viene instradato attraverso il NAT.
3. Aree di disponibilità. Il proxy, Tableau Server e gli host PostgreSQL vengono distribuiti uniformemente in due aree di disponibilità.
4. Gruppi di sicurezza. Quattro gruppi di sicurezza (Pubblico, Privato, Dati e Bastion) proteggono ogni livello a livello di protocollo.

Architettura di riferimento AWS

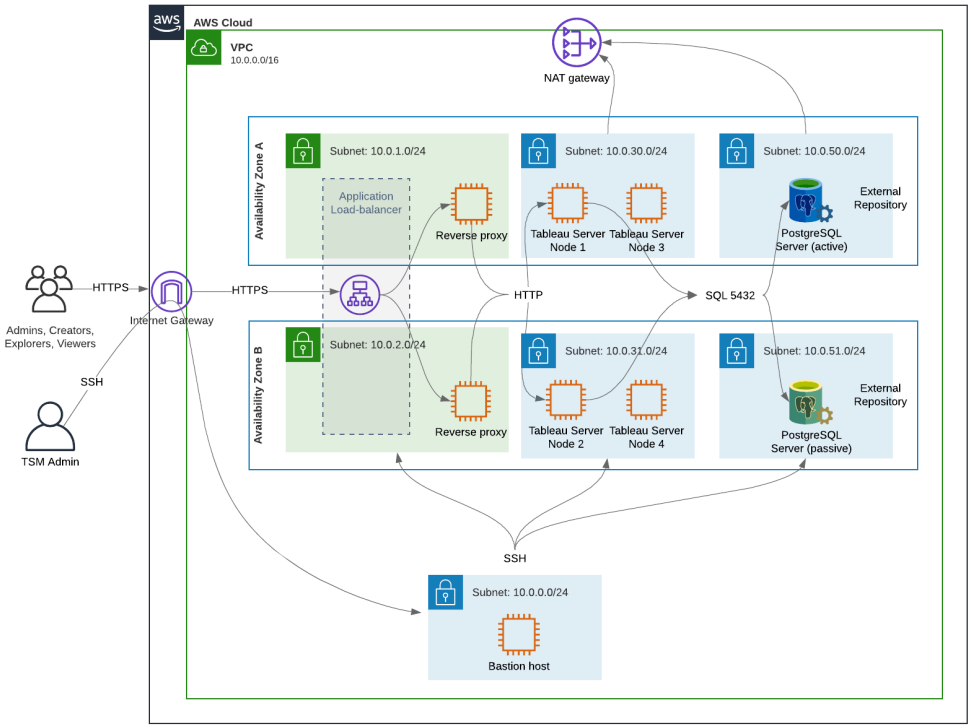
Diapositiva 1: topologia della subnet VPC e istanze EC2



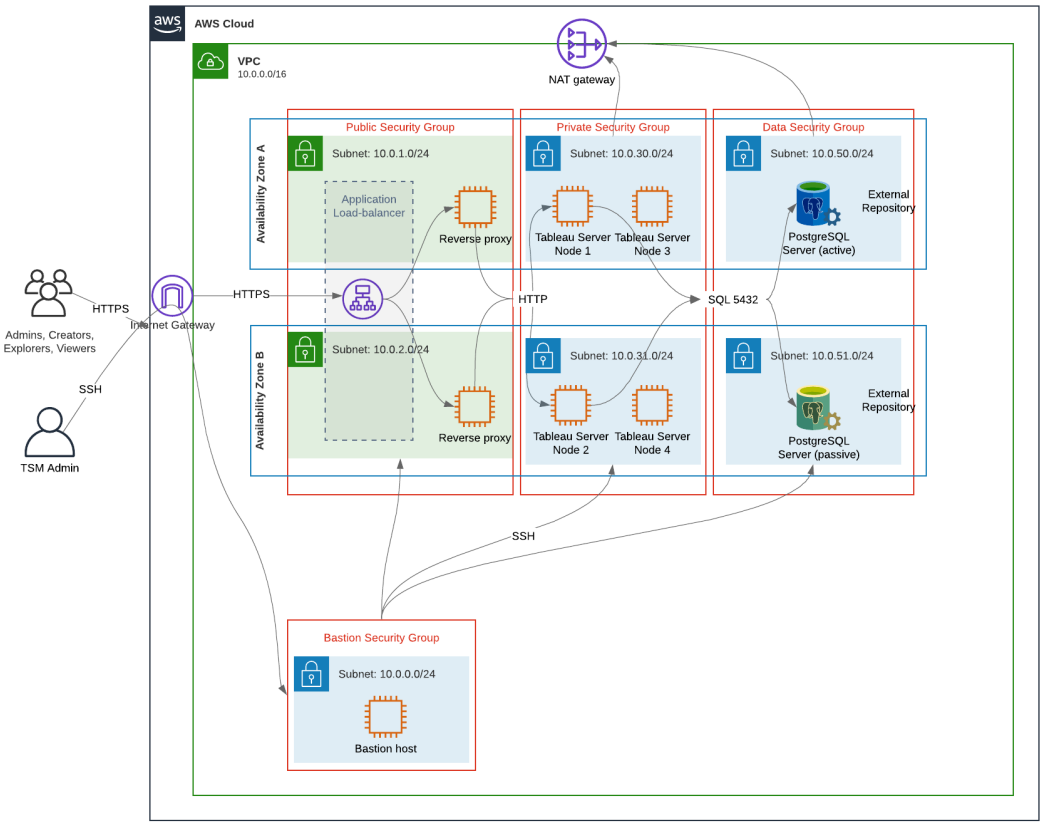
Diapositiva 2: flusso del protocollo e connettività



Diapositiva 3: aree di disponibilità



Diapositiva 4: gruppi di sicurezza



Aree di disponibilità AWS e disponibilità elevata

L'architettura di riferimento presentata in questa Guida specifica una distribuzione che assicura la disponibilità tramite ridondanza in caso di problemi di un singolo host. Tuttavia, nel caso AWS in cui l'architettura di riferimento è distribuita in due aree di disponibilità, la disponibilità risulta compromessa nella situazione molto rara in cui si verifica un problema in un'area di disponibilità.

Configurazione del VPC

In questa sezione viene descritto come:

- Installare e configurare il VPC
- Configurare la connettività Internet
- Configurare le subnet
- Creare e configurare i gruppi di sicurezza

Configurare il VPC

La procedura in questa sezione viene mappata all'interfaccia utente nell'esperienza VPC "classica". Puoi attivare o disattivare l'interfaccia utente per mostrare la visualizzazione classica disattivando la nuova esperienza VPC nell'angolo in alto a sinistra di AWS VPC Dashboard.

Esegui la procedura guidata VPC per creare le subnet private e pubbliche predefinite, il routing predefinito e gli ACL di rete.

1. Prima di configurare un VPC, devi creare un IP Elastic. Crea un'allocazione utilizzando tutte le impostazioni predefinite.
2. Esegui la procedura guidata VPC > "VPC con subnet pubbliche e private"
3. Accetta la maggior parte delle impostazioni predefinite, ad eccezione di quanto segue:
    - Immetti il nome di un VPC.
    - Specifica l'ID di allocazione dell'IP Elastic.
    - Specifica le seguenti maschere CIDR:
        - CIDR IPv4 della subnet pubblica: 10.0.1.0/24, rinomina questa subnet `Public-a`.
        - CIDR IPv4 della subnet privata: 10.0.30.0/24, rinomina questa subnet `Private-a`.
    - Area di disponibilità: per entrambe le subnet, seleziona l'opzione **a** per la regione in cui ti trovi.

      Nota: ai fini di questo esempio, vengono utilizzati **a** e **b** per distinguere tra le aree di disponibilità in un determinato data center AWS. In AWS, i nomi delle aree di disponibilità potrebbero non corrispondere agli esempi riportati

in questo documento. Ad esempio, alcune aree di disponibilità includono le aree **c** e **d** all'interno di un data center.

4. Fai clic su **Crea VPC**.
5. Dopo aver creato il VPC, crea le subnet `Public-b`, `Private-b`, `Data` e `Bastion`. Per creare una subnet, fai clic su **Subnet** > **Crea subnet**.
    - `Public-b`: per l'area di disponibilità, seleziona l'opzione **b** per la regione in cui ti trovi. Blocco CIDR: 10.0.2.0/24
    - `Private-b`: per l'area di disponibilità, seleziona l'opzione **b** per la regione in cui ti trovi. Blocco CIDR: 10.0.31.0/24
    - `Data`: per l'area di disponibilità, seleziona l'area **a** per la regione in cui ti trovi. Blocco CIDR: 10.0.50.0/24. Facoltativo: se prevedi di replicare il database esterno in un cluster PostgreSQL, crea una subnet Data-b nell'area di disponibilità b con un blocco CIDR di 10.0.51.0/24.
    - `Bastion`: per l'area di disponibilità, seleziona una delle due aree. Blocco CIDR: 10.0.0.0/24
6. Dopo aver creato le subnet, modifica le tabelle di route sulle subnet Public e Bastion in modo da utilizzare la tabella di route configurata per il gateway Internet (IGW) associato. Modifica inoltre le subnet Private e Data in modo da utilizzare la tabella di route configurata per Network Address Translation (NAT).
    - Per determinare quale tabella di route è configurata con IGW o NAT, fai clic su **Tabelle di route** nella dashboard di AWS. Seleziona uno dei due collegamenti alla tabella di route per aprire la pagina delle proprietà. Osserva il valore Destinazione in **Route** > **Destinazione** > **0.0.0.0/0**. Il valore Destinazione differenzia il tipo di route e inizierà con la stringa `igw-` o `nat-`.
    - Per aggiornare le tabelle di route, scegli **VPC** > **Subnet** > [nome_subnet] > **Tabella di route** > **Modifica associazione tabella di route**.

Configurare i gruppi di sicurezza

La procedura guidata VPC crea un singolo gruppo di sicurezza che non verrà utilizzato. Crea i seguenti gruppi di sicurezza (**Gruppi di sicurezza** > **Crea gruppo di sicurezza**). Gli host

EC2 verranno installati in questi gruppi in due aree di disponibilità, come mostrato nel diagramma precedente.

- Crea un nuovo gruppo di sicurezza: **Privato**. Qui verranno installati tutti e 4 i nodi di Tableau Server. In una fase successiva del processo di installazione, il gruppo di sicurezza Privato sarà associato alle subnet 10.0.30.0/24 e 10.0.31.0/24.
- Crea un nuovo gruppo di sicurezza: **Pubblico**. Qui verranno installati i server proxy. In una fase successiva del processo di installazione, il gruppo di sicurezza Pubblico sarà associato alle subnet 10.0.1.0/24 e 10.0.2.0/24.
- Crea un nuovo gruppo di sicurezza: **Dati**. Qui verrà installato il repository di Tableau esterno PostgreSQL. In una fase successiva del processo di installazione, il gruppo di sicurezza Dati sarà associato alle subnet 10.0.50.0/24 (e, facoltativamente, 10.0.51.0/24).
- Crea un nuovo gruppo di sicurezza: **Bastion**. Qui verrà installato l'host bastion. In una fase successiva del processo di installazione, il gruppo di sicurezza Bastion sarà associato alla subnet 10.0.0.0/24.

Specificare le regole in entrata e in uscita

In AWS, i gruppi di sicurezza sono analoghi ai firewall in un ambiente locale. Devi specificare il tipo di traffico (ad esempio, https, http e così via), il protocollo (TCP o UDP) e le porte o l'intervallo di porte (ad esempio, 80, 443 e così via) a cui è consentito il passaggio verso e/o dal gruppo di sicurezza. Per ogni protocollo devi specificare anche il traffico di destinazione o di origine.

Regole del gruppo di sicurezza Pubblico

Regole in entrata			
Tipo	**Protocollo**	**Intervallo di porte**	**Origine**
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	Gruppo di sicurezza Bastion

Regole in uscita			
Tipo	**Protocollo**	**Intervallo di porte**	**Destinazione**
Tutto il traffico	Tutti	Tutti	0.0.0.0/0

Regole del gruppo di sicurezza Privato

Il gruppo di sicurezza Privato include una regola in entrata per consentire il traffico HTTP dal gruppo di sicurezza Pubblico. Consenti il traffico HTTP solo durante il processo di distribuzione per verificare la connettività. È consigliabile rimuovere la regola in entrata HTTP dopo aver completato la distribuzione del proxy inverso e la configurazione di SSL in Tableau.

Regole in entrata			
Tipo	**Protocollo**	**Intervallo di porte**	**Origine**
HTTP	TCP	80	Gruppo di sicurezza Pubblico
HTTPS	TCP	443	Gruppo di sicurezza Pubblico
PostgreSQL	TCP	5432	Gruppo di sicurezza Dati
SSH	TCP	22	Gruppo di sicurezza Bastion
Tutto il traffico	Tutti	Tutti	Gruppo di sicurezza Privato

Regola in uscita			
Tipo	**Protocollo**	**Intervallo di porte**	**Destinazione**
Tutto il traffico	Tutti	Tutti	0.0.0.0/0
PostgreSQL	TCP	5432	Gruppo di sicurezza Dati
SSH	TCP	22	Gruppo di sicurezza Bastion

Regole del gruppo di sicurezza Dati

Regole in entrata			
Tipo	**Protocollo**	**Intervallo di porte**	**Origine**
PostgreSQL	TCP	5432	Gruppo di sicurezza Privato
SSH	TCP	22	Gruppo di sicurezza Bastion

Regole in uscita			
Tipo	**Protocollo**	**Intervallo di porte**	**Destinazione**
Tutto il traffico	Tutti	Tutti	0.0.0.0/0
PostgreSQL	TCP	5432	Gruppo di sicurezza Privato
SSH	TCP	22	Gruppo di sicurezza Bastion

Regole del gruppo di sicurezza host Bastion

Regole in entrata			
Tipo	**Protocollo**	**Intervallo di porte**	**Origine**
SSH	TCP	22	L'indirizzo IP e la subnet mask del computer che utilizzerai per accedere ad AWS (computer di amministrazione).
SSH	TCP	22	Gruppo di sicurezza Privato
SSH	TCP	22	Gruppo di sicurezza Pubblico

Regole in uscita			
Tipo	**Protocollo**	**Intervallo di porte**	**Destinazione**
SSH	TCP	22	L'indirizzo IP e la subnet mask del computer che utilizzerai per accedere ad AWS (computer di amministrazione).
SSH	TCP	22	Gruppo di sicurezza Privato
SSH	TCP	22	Gruppo di sicurezza Pubblico
SSH	TCP	22	Gruppo di sicurezza Dati
HTTPS	TCP	443	0.0.0.0/0 (facoltativo: crea questa regola se è necessario accedere a Internet per scaricare software di supporto sull'host bastion)

Abilitare l'assegnazione automatica dell'IP pubblico

In questo modo, ti viene fornito un indirizzo IP per la connessione ai server proxy e all'host bastion.

Per le subnet Public e Bastion:

1. Seleziona la subnet
2. Nel menu **Azioni** seleziona "Modifica impostazioni IP di assegnazione automatica".
3. Fai clic su "Abilita assegnazione automatica indirizzi IPv4 pubblici".
4. Fai clic su **Salva**.

Servizio di bilanciamento del carico

Nota : se stai effettuando l'installazione in AWS e seguendo la distribuzione di esempio in questa guida, devi installare e configurare il servizio di bilanciamento del carico AWS in una fase successiva del processo di distribuzione, come descritto in Parte 5 - Configurazione del livello Web.

Per le distribuzioni locali, collabora con gli amministratori di rete per distribuire i servizi di bilanciamento del carico in modo da supportare il livello Web dell'architettura di riferimento:

- Un servizio di bilanciamento del carico dell'applicazione rivolto al Web che accetta le richieste HTTPS dai client Tableau e comunica con i server proxy inversi.
- Proxy inverso:
  - È consigliabile un minimo di due server proxy per la ridondanza e per gestire il carico client.
  - Riceve il traffico HTTPS dal servizio di bilanciamento del carico.
  - Supporta la sessione permanente per l'host Tableau.
  - Configura il proxy per il bilanciamento del carico round robin in ogni sistema Tableau Server che esegue il processo Gateway.
  - Gestisce le richieste di autenticazione dall'IdP esterno.
- Proxy di inoltro: Tableau Server richiede l'accesso a Internet per la gestione delle licenze e le funzionalità per le mappe. A seconda dell'ambiente del proxy di inoltro, potrebbe essere necessario configurare gli elenchi consentiti del proxy di inoltro per gli URL del servizio Tableau. Vedi *Comunicare con Internet* (Linux).

Configurare computer host

Hardware minimo consigliato

Le seguenti raccomandazioni si basano sui nostri test con dati reali nell'architettura di riferimento.

Server applicazioni:

- CPU: 8 core fisici (16 vCPU),
- RAM: 128 GB (16 GB/core fisico)
- Spazio su disco: 100 GB

Data Server

- CPU: 8 core fisici (16 vCPU),
- RAM: 128 GB (16 GB/core fisico)
- Spazio su disco: 1 TB. Se la tua distribuzione utilizzerà l'archiviazione esterna per l'archivio file di Tableau, dovrai calcolare lo spazio su disco appropriato. Vedi *Installare Tableau Server con l'archivio file esterno* (Linux).

Server proxy

- CPU: 2 core fisici (4 vCPU),
- RAM: 8 GB (4 GB/core fisico)
- Spazio su disco: 100 GB

Database del repository esterno

- CPU: 8 core fisici (16 vCPU),
- RAM: 128 GB (16 GB/core fisico)
- Il requisito per lo spazio su disco dipende dal carico dei dati e dall'impatto che avrà sul backup. Consulta la sezione *Processi di backup e ripristino* nell'argomento *Requisiti di spazio su disco* (Linux).

Struttura delle directory

In base all'architettura di riferimento, è consigliabile installare il pacchetto di Tableau Server e i dati in percorsi non predefiniti:

- Installa il pacchetto in: `/app/tableau_server`. Crea questo percorso di directory prima di installare il pacchetto di Tableau Server, quindi specifica questo percorso durante l'installazione.
- Installa i dati di Tableau in: `/data/tableau_data`. Non creare questa directory prima di installare Tableau Server. Devi invece specificare il percorso durante l'installazione, quindi il programma di installazione di Tableau creerà e autorizzerà il percorso in modo appropriato.

Consulta Eseguire il pacchetto di installazione e inizializzare TSM per i dettagli sull'implementazione.

Esempio: installare e preparare i computer host in AWS

In questa sezione viene descritto come installare gli host EC2 per ogni tipo di server nell'architettura di riferimento di Tableau Server.

L'architettura di riferimento richiede otto host:

- Quattro istanze per Tableau Server.
- Due istanze per i server proxy (Apache).
- Un'istanza per l'host bastion.
- Una o due istanze di database PostgreSQL EC2

Dettagli dell'istanza host

Installa i computer host in base alle informazioni riportate di seguito.

Tableau Server

- Amazon Linux 2
- Tipo di istanza: m5a.8xlarge
- ID gruppo di sicurezza: Privato
- Archiviazione: EBS, 150 GiB, tipo di volume gp2. Se la tua distribuzione utilizzerà l'archiviazione esterna per l'archivio file di Tableau, dovrai calcolare lo spazio su disco appropriato. Vedi *Installare Tableau Server con l'archivio file esterno* (Linux).
- Rete: installa due host EC2 in ciascuna subnet privata (10.0.30.0/24 e 10.0.31.0/24).
- Copia la versione di manutenzione più recente del pacchetto rpm di Tableau Server 2021.2 (o versione successiva) dalla pagina dei download di Tableau in ciascun host Tableau.

Host bastion

- Amazon Linux 2
- Tipo di istanza: t3.micro
- ID gruppo di sicurezza: Bastion
- Archiviazione: EBS, 50 GiB, tipo di volume gp2
- Rete: subnet Bastion 10.0.0.0/24

Gateway indipendente Tableau Server

- Amazon Linux 2
- Tipo di istanza: t3.xlarge
- ID gruppo di sicurezza: Pubblico
- Archiviazione: EBS, 100 GiB, tipo di volume gp2
- Rete: installa un'istanza EC2 in ciascuna subnet pubblica (10.0.1.0/24 e 10.0.2.0/24)

Host EC2 PostgreSQL

- Amazon Linux 2
- Tipo di istanza: r5.4xlarge
- ID gruppo di sicurezza: Dati
- Archiviazione: il requisito per lo spazio su disco dipende dal carico dei dati e dall'impatto che avrà sul backup. Consulta la sezione *Processi di backup e ripristino* nell'argomento *Requisiti di spazio su disco* (Linux).
- Rete: subnet Data 10.0.50.0/24. Se prevedi di replicare PostgreSQL in un cluster a disponibilità elevata, installa il secondo host nella subnet 10.0.51.0/24)

Verifica: connettività del VPC

Dopo aver installato i computer host, verifica la configurazione di rete. Verifica la connettività tra gli host connettendoti con SSH dall'host nel gruppo di sicurezza Bastion agli host in ogni subnet.

Esempio: connettersi all'host bastion in AWS

1. Configura il computer di amministrazione per ssh-agent. Questo ti consente di connetterti agli host in AWS senza posizionare il file della chiave privata in un'istanza EC2.

   Per configurare ssh-agent su un Mac, esegui questo comando:

   `ssh-add -K myPrivateKey.pem` o per l'ultimo Mac OS: `ssh-add --apple-use-keychain myPrivateKey.pem`

   Per Windows, consulta l'argomento Securely Connect to Linux Instances Running in a Private Amazon VPC.

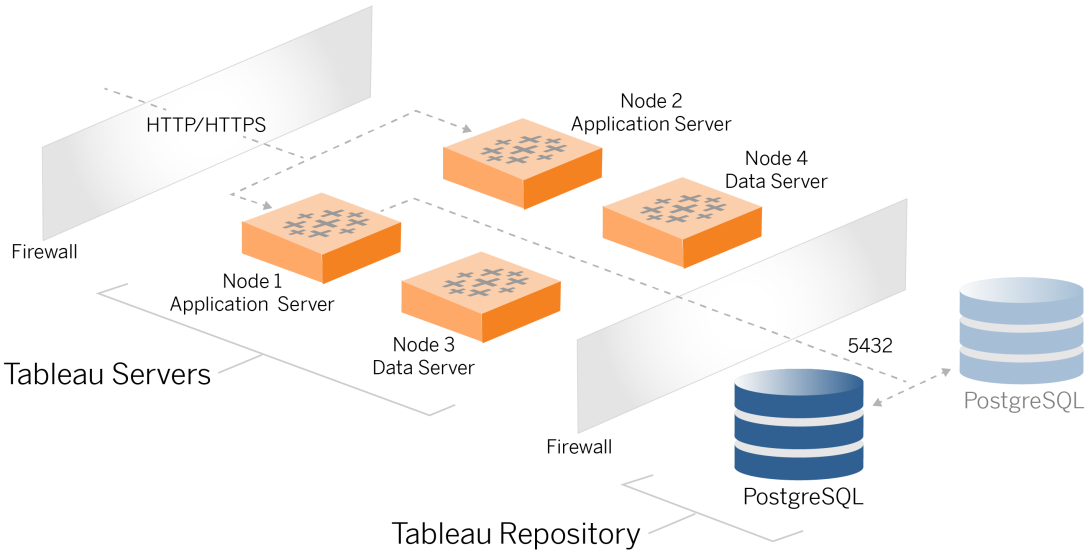
2. Connettiti all'host bastion eseguendo questo comando:

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

3. Potrai quindi connetterti agli altri host nel VPC dall'host bastion utilizzando l'indirizzo IP privato, ad esempio:

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

Parte 4 - Installazione e configurazione di Tableau Server



In questo argomento viene descritto come completare l'installazione e la configurazione della distribuzione di base di Tableau Server. La procedura descritta qui continua con l'esempio di architettura di riferimento AWS e Linux.

Gli esempi relativi a Linux nelle procedure di installazione mostrano i comandi per le distribuzioni di tipo RHEL. In particolare, i comandi riportati di seguito sono stati sviluppati con la distribuzione Amazon Linux 2. Se esegui una distribuzione di Ubuntu, modifica i comandi di conseguenza.

Prima di iniziare

Devi preparare e convalidare l'ambiente come descritto in Parte 3 - Preparazione per la distribuzione di Tableau Server per le organizzazioni di grandi dimensioni.

Installare, configurare e creare il backup tar di PostgreSQL

Questa istanza di PostgreSQL ospita il repository esterno per la distribuzione di Tableau Server. Devi installare e configurare PostgreSQL prima di installare Tableau.

Puoi eseguire PostgreSQL su Amazon RDS o su un'istanza EC2. Per maggiori informazioni sulle differenze tra l'esecuzione del repository su RDS rispetto a un'istanza EC2, consulta *Repository esterno di Tableau Server* (Linux).

A titolo di esempio, la procedura seguente illustra come installare e configurare Postgres in un'istanza Amazon EC2. L'esempio mostrato di seguito si riferisce a un'installazione e una configurazione generiche per PostgreSQL nell'architettura di riferimento. Il tuo amministratore di database dovrebbe ottimizzare la distribuzione di PostgreSQL in base alle dimensioni dei dati e alle esigenze di prestazioni.

Requisiti: è necessario eseguire PostgreSQL 1.6 e installare il modulo uuid-ossp.

Gestione delle versioni di PostgreSQL

Devi installare le versioni principali compatibili di PostgreSQL per il repository esterno di Tableau Server. Inoltre, anche le versioni secondarie devono soddisfare i requisiti minimi.

Versioni di Tableau Server	**Versioni minime compatibili con PostgreSQL**
2021.2.3 - 2021.2.8 2021.3.0 - 2021.3.7 2021.4.0 - 2021.4.3	12.6
2021.2.10 - 2021.2.14 2021.3.8 - 2021.3.13 2021.4.4 - 2021.4.8	12.8

2021.2.15 - 2021.2.16 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 2023.1.16 - 2023.1.x 2023.3.9 - 2023.3.x	13.14

2024,0 - 2024.x	15.6

Installare PostgreSQL

Questa procedura di installazione di esempio descrive come installare PostgreSQL versione 13.6.

Accedi all'host EC2 che hai creato nella parte precedente.

1. Esegui l'aggiornamento per applicare le correzioni più recenti al sistema operativo Linux:

   ```
   sudo yum update
   ```

2. Crea e modifica il file pgdg.repo nel percorso `/etc/yum.repos.d/`. Inserisci nel file le seguenti informazioni di configurazione:

   ```
   [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. Installa Postgres 13.6:

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

4. Installa il modulo uuid-ossp:

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

5. Inizializza Postgres:

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

Configurare Postgres

Completa l'installazione del database configurando Postgres:

1. Aggiorna il file di configurazione pg_hba, `/var/lib/pgsql/13/data/pg_hba.conf`, con le due voci seguenti. Ogni voce deve includere la maschera delle subnet in cui verranno eseguiti i sistemi Tableau Server:

   ```
   host all all 10.0.30.0/24 password

   host all all 10.0.31.0/24 password
   ```

2. Aggiorna il file PostgreSQL,`/var/lib/pgsql/13/data/postgresql.conf`, aggiungendo questa riga:

   ```
   listen_addresses = '*'
   ```

3. Configura l'avvio di Postgres al riavvio:

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

4. Imposta la password dell'utente con privilegi avanzati:

   ```
   sudo su - postgres

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

   > **Nota**: imposta una password complessa. Non utilizzare `'StrongPassword'` come mostrato nell'esempio.

   ```
   exit
   ```

5. Riavvia Postgres:

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

Creare il backup tar di PostgreSQL della fase 1

Crea un backup tar della configurazione di PostgreSQL. La creazione di uno snapshot tar della configurazione corrente ti consentirà di risparmiare tempo se riscontri problemi mentre prosegui con la distribuzione.

Faremo riferimento a questo backup come backup della "fase 1".

Nell'host PostgreSQL:

1. Arresta l'istanza del database Postgres:

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

2. Esegui questi comandi per creare il backup tar:

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

3. Avvia il database Postgres:

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

Eseguire il ripristino alla fase 1

Esegui il ripristino alla fase 1 se si verifica un problema nel nodo iniziale di Tableau Server durante l'installazione.

1. Nel computer con Tableau esegui lo script obliterate per rimuovere completamente Tableau Server dall'host:

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

2. Esegui il ripristino del file tar di PostgreSQL della fase 1. Nel computer con Postgres esegui questi comandi:

```
sudo su

systemctl stop postgresql-13

cd /var/lib/pgsql

tar  -xvf step1.13.bkp.tar

systemctl start postgresql-13

exit
```

Riprendi il processo di installazione per installare il nodo iniziale di Tableau Server.

Prima dell'installazione

Se stai distribuendo Tableau in base all'esempio di implementazione AWS/Linux descritto in questa guida, potresti essere in grado di eseguire lo script di installazione automatizzata TabDeploy4EDG. Lo script TabDeploy4EDG automatizza l'installazione di esempio della distribuzione di Tableau a quattro nodi descritta nelle procedure seguenti. Vedi Appendice - Toolbox per la distribuzione di AWS.

Installare il nodo iniziale di Tableau Server

Questa procedura descrive come installare il nodo iniziale di Tableau Server nel modo definito dall'architettura di riferimento. Ad eccezione dell'installazione del pacchetto e dell'inizializzazione di TSM, nel corso della procedura viene utilizzata la riga di comando di TSM quando possibile. Oltre a essere indipendente dalla piattaforma, l'utilizzo dell'interfaccia a riga di comando di TSM semplifica l'installazione negli ambienti virtualizzati e headless.

Eseguire il pacchetto di installazione e inizializzare TSM

Accedi al server host Nodo 1.

1. Esegui l'aggiornamento per applicare le correzioni più recenti al sistema operativo Linux:

   ```
   sudo yum update
   ```

2. Copia il pacchetto di installazione dalla pagina dei download di Tableau nel computer host che eseguirà Tableau Server.

   Ad esempio, su un computer con sistema operativo Linux di tipo RHEL, esegui

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

   dove `<version>` è il numero di versione.

3. Scarica e installa le dipendenze:

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

4. Crea il percorso `/app/tableau_server` nella directory principale:

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

5. Esegui il programma di installazione e specifica il percorso di installazione `/ap-p/tableau_server`. Ad esempio, su un sistema operativo Linux di tipo RHEL, esegui:

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

6. Passa alla directory `/app/tableau_server/packages/scripts.<version_code>/` ed esegui lo script `initialize-tsm` disponibile in tale posizione:

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

7. Una volta completata l'inizializzazione, chiudi la shell:

   ```
   exit
   ```

Attivare e registrare Tableau Server

1. Accedi al server host Nodo 1.

2. Specifica i codici prodotto di Tableau Server in questa fase. Esegui il seguente comando per ogni codice prodotto acquistato:

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

3. Crea un file di registrazione json con il formato mostrato di seguito:

   ```
   {
   "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. Dopo aver salvato le modifiche al file, passalo con l'opzione `--file` per registrare Tableau Server:

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

Configurare l'archivio identità

> **Nota**: se la tua distribuzione utilizzerà l'archiviazione esterna per l'archivio file di Tableau, dovrai abilitare l'archivio file esterno prima di configurare l'archivio identità. Vedi *Installare Tableau Server con l'archivio file esterno* (Linux).

L'architettura di riferimento predefinita utilizza un archivio identità locale. Configura l'host iniziale con l'archivio identità locale passando il file `config.json` con il comando `tsm settings import`.

Importa il file `config.json` in base al tuo sistema operativo:

Il file `config.json` è incluso nel percorso di directory scripts.<versione> (ad esempio, `scripts.20204.21.0217.1203`) ed è formattato per configurare l'archivio identità.

Esegui questo comando per importare il file `config.json`:

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

Configurare Postgres esterno

1. Crea un file json di un database esterno con le seguenti impostazioni di configurazione:

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

```
"port":5432
}
```

2. Dopo aver salvato le modifiche al file, passa il file con questo comando:

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

   Ti sarà richiesta la password utente master Postgres.

   L'opzione `--no-ssl` consente di configurare Tableau per l'uso di SSL/TLS solo quando il server Postgres è configurato per SSL/TLS. Se Postgres non è configurato per SSL/TLS, la connessione non è crittografata. In Parte 6 - Configurazione post-installazione viene descritto come abilitare SSL/TLS per la connessione Postgres dopo aver completato la prima fase della distribuzione.

3. Applica le modifiche.

   Esegui questo comando per applicare le modifiche e riavviare Tableau Server:

   ```
   tsm pending-changes apply
   ```

4. Elimina il file di configurazione che hai utilizzato nella fase 1.

Terminare l'installazione del Nodo 1

1. Dopo l'installazione di Tableau Server, devi inizializzare il server.

   Esegui questo comando:

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

2. Al termine dell'inizializzazione, devi creare un account amministratore di Tableau Server.

   A differenza dell'account computer che utilizzi per installare e gestire i componenti del sistema operativo di TSM, l'account amministratore di Tableau Server è un account

dell'applicazione che viene utilizzato per creare utenti, progetti e siti di Tableau Server. L'amministratore di Tableau Server applica anche le autorizzazioni alle risorse di Tableau. Esegui questo comando per creare l'account di amministratore iniziale. Nell'esempio seguente l'utente è denominato `tableau-admin`:

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

Tabcmd ti richiederà di impostare una password per questo utente.

Verifica: configurazione di Nodo 1

1. Esegui questo comando per verificare che i servizi TSM siano in esecuzione:

   ```
   tsm status -v
   ```

   Tableau dovrebbe restituire quanto segue:

   ```
   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.
   ...
   ```

   Verranno elencati tutti i servizi.

2. Esegui questo comando per verificare che il sito amministrativo di Tableau sia in esecuzione:

   ```
   curl localhost
   ```

Le prime righe dovrebbero mostrare Vizportal html, in modo simile al seguente:

```
<!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 ...
```

Creare i backup tar della fase 2

Dopo aver verificato l'installazione iniziale, crea due backup tar:

- PostgreSQL
- Nodo iniziale di Tableau (Nodo 1)

Nella maggior parte dei casi puoi ripristinare l'installazione del nodo iniziale ripristinando questi file tar. Il ripristino dei file tar è molto più rapido rispetto alla reinstallazione e alla reinizializzazione del nodo iniziale.

Creare i file tar della fase 2

1. Nel nodo iniziale di Tableau arresta Tableau:

   ```
   tsm stop
   ```

   Attendi che Tableau venga arrestato prima di continuare con il passaggio successivo.

2. Nell'host PostgreSQL arresta l'istanza del database Postgres:

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

3. Esegui questi comandi per creare il backup tar:

   ```
   sudo su

   cd /var/lib/pgsql

   tar -cvf step2.13.bkp.tar 13

   exit
   ```

4. Verifica che il file tar di Postgres sia stato creato con le autorizzazioni root:

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

5. Nell'host Tableau arresta i servizi amministrativi di Tableau:

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

6. Esegui questi comandi per creare il backup tar:

   ```
   cd /data

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

7. Nell'host Postgres avvia il database Postgres:

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

8. Avvia i servizi amministrativi di Tableau:

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

9. Esegui il comando `tsm status` per monitorare lo stato di TSM prima del riavvio.

   Nella maggior parte dei casi, il comando restituirà prima lo stato DEGRADED o ERROR. Attendi qualche minuto ed esegui nuovamente il comando. Se viene restituito

lo stato ERROR o DEGRADED, continua ad attendere. Non tentare di avviare TSM finché non viene restituito lo stato STOPPED. Esegui quindi questo comando:

```
tsm start
```

Eseguire il ripristino alla fase 2

Questo processo ripristina il Nodo 1 di Tableau e l'istanza di Postgres alla fase 2. Dopo aver eseguito il ripristino a questa fase, puoi ridistribuire i nodi restanti di Tableau.

1. Arresta i servizi tsm nell'host Tableau iniziale (Nodo 1):

   ```
   tsm stop
   ```

2. Arresta i servizi amministrativi di Tableau in tutti i nodi della distribuzione di Tableau Server. Esegui questo comando in ciascun nodo, in ordine (Nodo 1, Nodo 2 e quindi Nodo 3):

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

3. Dopo l'arresto dei servizi di Tableau, ripristina il file tar di PostgreSQL della fase 2. Nel computer con Postgres esegui questi comandi:

   - ```
     sudo su

     systemctl stop postgresql-13

     cd /var/lib/pgsql

     tar  -xvf step2.13.bkp.tar

     systemctl start postgresql-13

     exit
     ```
     ```

4. Esegui il ripristino del file tar di Tableau della fase 2. Nell'host Tableau iniziale esegui questi comandi:

   ```
   cd /data

   sudo rm -rf tableau_data

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

5. Sul computer Nodo 1 di Tableau, rimuovi i seguenti file:

   - `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. Avvia i servizi amministrativi di Tableau:

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

7. Ricarica i file systmctl di Tableau ed esegui di nuovo `start-administrative-services`:

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

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

8. Su Nodo 1, esegui il comando `tsm status` per monitorare lo stato di TSM prima del riavvio.

   In alcuni casi, verrà visualizzato un errore `Cannot connect to server...`. Questo errore si verifica perché il servizio tabadmincontroller non è stato riavviato. Con-

tinua a eseguire `tsm status` periodicamente. Se questo errore non scompare dopo 10 minuti, esegui di nuovo il comando `start-administrative-services`.

Dopo pochi istanti, il comando `tsm status` restituirà lo stato DEGRADED e quindi ERROR. Non avviare TSM finché non viene restituito lo stato STOPPED. Esegui quindi questo comando:

```
tsm start
```

Riprendi il processo di installazione per installare Tableau Server sui nodi rimanenti.

Installare Tableau Server nei nodi rimanenti

Per continuare la distribuzione, copia il programma di installazione di Tableau su ciascun nodo.

Panoramica della configurazione dei nodi

In questa sezione viene descritto il processo per la configurazione dei Nodi 2-4. Le sezioni che seguono forniscono procedure dettagliate di configurazione e convalida per ogni passaggio.

L'installazione dei Nodi 2-4 di Tableau Server richiede di generare, copiare e fare riferimento a un file di bootstrap durante l'installazione del nodo.

Per generare il file di bootstrap, devi eseguire un comando TSM sul nodo iniziale. Dovrai quindi copiare il file di bootstrap nel nodo di destinazione, dove verrà eseguito nell'ambito dell'inizializzazione del nodo.

Il seguente contenuto json mostra un esempio di file di bootstrap. Il certificato e i valori relativi alla crittografia sono stati troncati per facilitare la lettura del file di esempio.

```
{
"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" : "eyJ-
jdHkiOiJKV1QiLCJlbmMiOiJBMTI4Q0JDLUhQ...",
        "sessionCookieName" : "AUTH_COOKIE"
        }
}
```

Il file di bootstrap include la convalida basata sulla connessione per l'autenticazione di Nodo 1 e crea un canale crittografato per il processo di bootstrap. La sessione di bootstrap è limitata nel tempo e la configurazione e la convalida dei nodi richiedono diverso tempo. Pianifica la creazione e la copia di nuovi file di bootstrap durante la configurazione dei nodi.

Dopo aver eseguito il file di bootstrap, accedi al nodo iniziale di Tableau Server e configura i processi per il nuovo nodo. Al termine della configurazione dei nodi, devi applicare le modifiche e riavviare il nodo iniziale. Il nuovo nodo viene configurato e avviato. Man mano che aggiungi i nodi, il completamento della configurazione e del riavvio della distribuzione richiederanno consecutivamente più tempo.

Gli esempi relativi a Linux nelle procedure di installazione mostrano i comandi per le distribuzioni di tipo RHEL. Se esegui una distribuzione di Ubuntu, modifica i comandi di conseguenza.

1. Esegui l'aggiornamento per applicare le correzioni più recenti al sistema operativo Linux:

   ```
   sudo yum update
   ```

2. Scarica e installa le dipendenze:

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

3. Crea il percorso `/app/tableau_server` nella directory principale:

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

4. Esegui il programma di installazione e specifica il percorso di installazione `/ap-p/tableau_server`. Ad esempio, su un sistema operativo Linux di tipo RHEL, esegui:

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

Generare, copiare e utilizzare il file di bootstrap per inizializzare TSM

La seguente procedura mostra come generare, copiare e utilizzare un file di bootstrap per l'inizializzazione di TSM su un altro nodo. In questo esempio, il campo di bootstrap è denominato `boot.json`.

In questo esempio, i computer host sono in esecuzione in AWS, mentre gli host EC2 eseguono Amazon Linux 2.

1. Connettiti al nodo iniziale (Nodo 1) ed esegui questo comando:

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

2. Copia il file di bootstrap in Nodo 2.

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

3. Connettiti a Nodo 2 e passa alla directory degli script di Tableau Server:

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

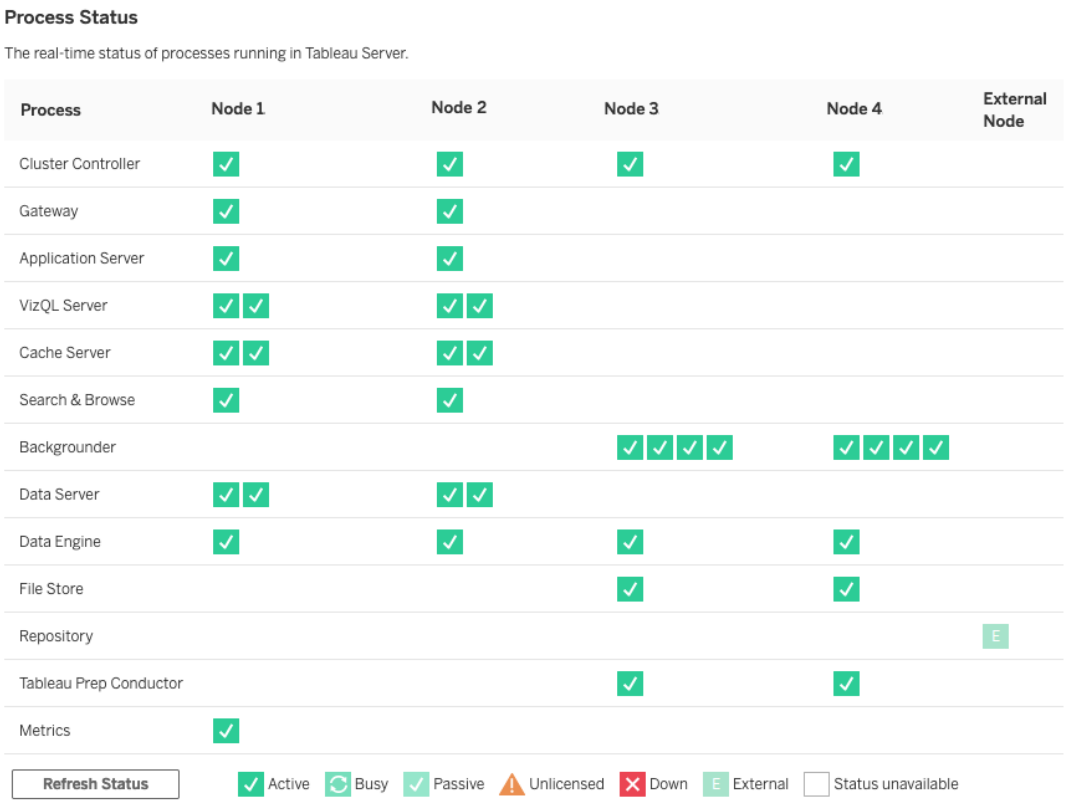
4. Esegui il comando `initialize-tsm` e fai riferimento al file di bootstrap:

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

5. Dopo il completamento di `initialize-tsm`, elimina `boot.json`, quindi chiudi o disconnettiti dalla sessione.

Configurare i processi

Devi configurare il cluster Tableau Server sul nodo in cui è in esecuzione il controller di amministrazione di Tableau Server (controller TSM). Il controller TSM viene eseguito sul nodo iniziale.



Configurare Nodo 2

1. Dopo aver inizializzato TSM utilizzando il file di bootstrap su Nodo 2, accedi al nodo iniziale.

2. Nel nodo iniziale (`node1`) esegui questi comandi per configurare i processi su Nodo 2:

   ```
   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
   ```

   Se stai installando la versione 2022.1 o successiva, aggiungi anche il servizio Indice e ricerca:

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

   Se stai installando la versione 2023.3 o successiva, includi solo il server di indicizzazione e ricerca. Non aggiungere il servizio Ricerca e sfoglia (searchserver).

3. Esamina la configurazione prima di applicarla. Esegui questo comando:

   ```
   tsm pending-changes list
   ```

4. Dopo aver verificato che le modifiche siano nell'elenco in sospeso (saranno presenti anche altri servizi in tale elenco), applica le modifiche:

   ```
   tsm pending-changes apply
   ```

   Le modifiche richiederanno un riavvio. La configurazione e il riavvio richiederanno del tempo.

5. Verifica la configurazione di Nodo 2. Esegui questo comando:

   ```
   tsm status -v
   ```

Configurare Nodo 3

Inizializza TSM utilizzando il processo di bootstrap su Nodo 3, quindi esegui i comandi `tsm topology set-process` riportati di seguito.

Ogni volta che imposti un processo, verrà visualizzato un avviso del servizio di coordinamento. Puoi ignorare questo avviso durante l'impostazione dei processi.

1. Dopo aver inizializzato TSM utilizzando il file di bootstrap su Nodo 3, accedi al nodo iniziale (`node1`) ed esegui questi comandi per configurare i processi:

   ```
   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
   ```

   Se stai installando la versione 2022.1 o successiva, aggiungi anche il servizio Indice e ricerca:

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

2. Esamina la configurazione prima di applicarla. Esegui questo comando:

   ```
   tsm pending-changes list
   ```

3. Dopo aver verificato che le modifiche siano nell'elenco in sospeso (l'elenco includerà altri servizi configurati automaticamente), applica le modifiche:

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

   Le modifiche richiederanno un riavvio. La configurazione e il riavvio richiederanno del tempo.

4. Verifica la configurazione eseguendo questo comando:

   ```
   tsm status -v
   ```

Distribuire l'insieme dei servizi di coordinamento nei Nodi 1-3

Per la distribuzione a quattro nodi dell'architettura di riferimento standard, procedi come segue:

1. Esegui questo comando su Nodo 1:

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

   Il processo include un riavvio di TSM, che richiederà del tempo.

2. Al termine della distribuzione del servizio di coordinamento, avvia TSM:

   ```
   tsm start
   ```

Creare i backup tar della fase 3

Dopo aver verificato l'installazione, crea quattro backup tar:

- PostgreSQL
- Nodo iniziale di Tableau (Nodo 1)
- Nodo 2 di Tableau
- Nodo 3 di Tableau

Creare i file tar della fase 3

1. Nel nodo iniziale di Tableau arresta Tableau:

   ```
   tsm stop
   ```

2. Dopo l'arresto di TSM, arresta i servizi amministrativi di Tableau su ciascun nodo. Esegui questo comando in ciascun nodo, in ordine (Nodo 1, Nodo 2 e quindi Nodo 3):

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

3. Nell'host PostgreSQL arresta l'istanza del database Postgres:

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

4. Esegui questi comandi per creare il backup tar:

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

5. Verifica che il file tar di Postgres sia stato creato con le autorizzazioni root:

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

6. Nell'host Postgres avvia il database Postgres:

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

7. Crea il backup tar su Nodo 1, Nodo 2 e Nodo 3. Esegui questi comandi su ogni nodo:

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

- Verifica che il file tar di Tableau sia stato creato con le autorizzazioni root:

  ```
  ls -al
  ```

8. Avvia i servizi amministrativi di Tableau su ciascun nodo in ordine (Nodo 1, Nodo 2 e quindi Nodo 3):

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

9. Esegui il comando `tsm status` per monitorare lo stato di TSM prima del riavvio.

   Nella maggior parte dei casi, il comando restituirà lo stato DEGRADED e quindi ERROR. Attendi qualche istante ed esegui nuovamente il comando. Se viene restituito lo stato ERROR o DEGRADED, continua ad attendere. Non tentare di avviare TSM finché non viene restituito lo stato STOPPED. Esegui quindi questo comando:

   ```
   tsm start
   ```

Eseguire il ripristino alla fase 3

Questo processo esegue il ripristino di Nodo 1, Nodo 2 e Nodo 3 di Tableau. Ripristina anche l'istanza di Postgres alla fase 3. Dopo aver eseguito il ripristino a questa fase, puoi distribuire il servizio di coordinamento, Nodo 4, e quindi le configurazioni finali dei nodi.

1. Arresta il servizio tsm nell'host Tableau iniziale (Nodo 1):

   ```
   tsm stop
   ```

2. Dopo l'arresto di TSM, arresta i servizi amministrativi di Tableau su Nodo 1, Nodo 2 e Nodo 3. Esegui questo comando su ogni nodo:

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

3. Esegui il ripristino del file tar di PostgreSQL della fase 3. Nel computer con Postgres esegui questi comandi:

   ```
   sudo su

   systemctl stop postgresql-12

   cd /var/lib/pgsql

   tar -xvf step3.12.bkp.tar

   systemctl start postgresql-12

   exit
   ```

4. Esegui il ripristino del file tar di Tableau della fase 3 su Nodo 1, Nodo 2 e Nodo 3. Esegui questi comandi su ogni nodo di Tableau:

   ```
   cd /data

   sudo rm -rf tableau_data

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

5. Sul computer Nodo 1 di Tableau, rimuovi i seguenti file:

   - `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`

   Se la shell restituisce un errore "file non trovato", potrebbe essere necessario modificare il nome del percorso per incrementare il numero `<n>` in questa sezione del percorso: `.../appzookeeper/<n>/version-2/...`.

6. Riavvia i servizi amministrativi su Nodo 1, Nodo 2 e Nodo 3. Esegui questi comandi su ogni nodo:

   ```
   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. Su Nodo 1, esegui il comando `tsm status` per monitorare lo stato di TSM prima del riavvio.

   In alcuni casi, verrà visualizzato un errore `Cannot connect to server...`. Questo errore si verifica perché il servizio tabadmincontroller non è stato riavviato. Continua a eseguire `tsm status` periodicamente. Se questo errore non scompare dopo 10 minuti, esegui di nuovo il comando `start-administrative-services`.

   Dopo pochi istanti, il comando `tsm status` restituirà lo stato DEGRADED e quindi ERROR. Non avviare TSM finché non viene restituito lo stato STOPPED. Esegui quindi questo comando:

   ```
   tsm start
   ```

Riprendi il processo di installazione per distribuire il servizio di coordinamento nei Nodi 1-3.

Configurare Nodo 4

Il processo per la configurazione di Nodo 4 è lo stesso di Nodo 3.

Imposta gli stessi processi impostati per Nodo 3, eseguendo lo stesso set di comandi mostrato in precedenza, ma specificando `node4` nei comandi anziché `node3`.

Come per la verifica di Nodo 3, verifica la configurazione di Nodo 4 eseguendo `tsm status -v`.

Prima di procedere, attendi che il processo Archivio file su Nodo 4 termini la sincronizzazione. Lo stato del servizio Archivio file tornerà `is synchronizing` fino al completamento. Quando lo stato del servizio Archivio file ritorna `is running`, puoi procedere.

Configurazione e verifica del processo finale

Il passaggio finale per la configurazione dei processi è la rimozione dei processi ridondanti da Nodo 1.

1. Connettiti al nodo iniziale (`node1`).
2. Disattiva l'archivio file su Nodo 1. Verrà visualizzato un avviso relativo alla rimozione dell'archivio file da un controller nella stessa posizione. Puoi ignorare l'avviso. Esegui questo comando:

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

3. Quando l'archivio file è disattivato, esegui questo comando per rimuovere il processo di Gestione componenti in background da Nodo 1:

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

4. Esamina la configurazione prima di applicarla. Esegui questo comando:

   ```
   tsm pending-changes list
   ```

5. Dopo aver verificato che le modifiche siano nell'elenco in sospeso, applica le modifiche:

   ```
   tsm pending-changes apply
   ```

   Le modifiche richiederanno un riavvio. La configurazione e il riavvio richiederanno del tempo.

6. Verifica la configurazione:

   ```
   tsm status -v.
   ```

Prima di procedere, attendi che il processo Archivio file su Nodo 4 termini la sincronizzazione. Lo stato del servizio Archivio file tornerà `is synchronizing` fino al completamento. Quando lo stato del servizio Archivio file ritorna `is running`, puoi procedere.

Eseguire il backup

Un ripristino completo di Tableau Server richiede un portfolio di backup che include tre componenti:

- Un file di backup dei dati del repository e dell'archivio file. Questo file è generato dal comando `tsm maintenance backup`.
- Un file di esportazione della topologia e della configurazione. Questo file è generato dal comando `tsm settings export`.
- Certificato di autenticazione, chiave e file keytab.

Per una descrizione completa del processo di backup e ripristino, consulta l'argomento di Tableau Server *Eseguire un backup completo e ripristinare Tableau Server* (Linux).

In questa fase della distribuzione, tutti i file e le risorse rilevanti necessari per un ripristino completo sono inclusi eseguendo i comandi `tsm maintenance backup` e `tsm settings export`.

1. Esegui questo comando per esportare le impostazioni di configurazione e topologia in un file denominato `ts_settings_backup.json`

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

2. Esegui questo comando per creare un backup dei dati del repository e dell'archivio file in un file denominato `ts_backup-<yyyy-mm-dd>.tsbak`. Ignora l'avviso che indica che l'archivio file non si trova nel nodo del controller.

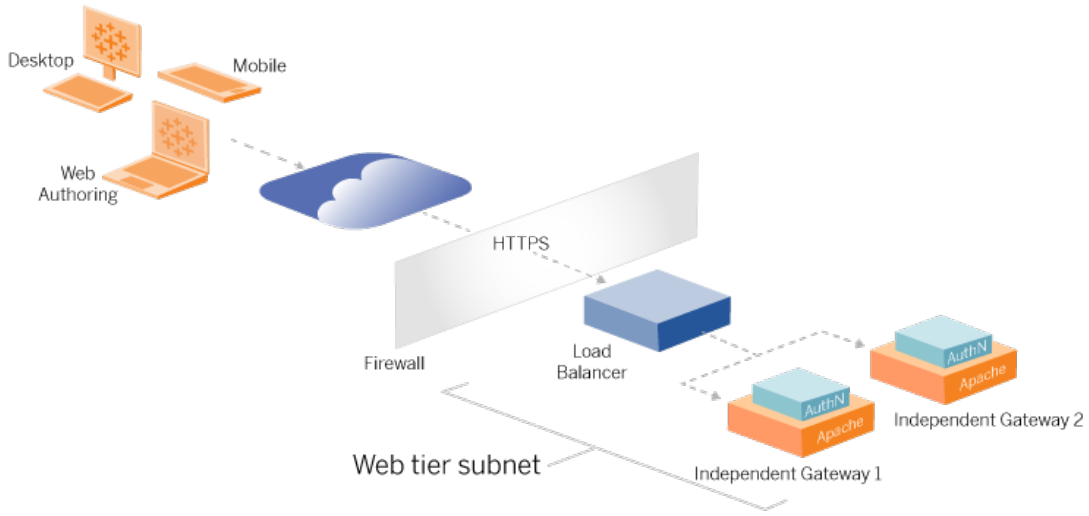
   ```
   tsm maintenance backup -f ts_backup -d --skip-compression
   ```

   Percorso del file di backup:

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

3. Copia entrambi i file e salvali in una risorsa di archiviazione diversa, non condivisa dalla distribuzione di Tableau Server.

Parte 5 - Configurazione del livello Web



Il livello Web dell'architettura di riferimento deve includere i seguenti componenti:

- Un servizio di bilanciamento del carico dell'applicazione rivolto al Web che accetta le richieste HTTPS dai client Tableau e comunica con i server proxy inversi.
- Proxy inverso:
  - È consigliabile distribuire Gateway indipendente Tableau Server.
  - È consigliabile un minimo di due server proxy per la ridondanza e per gestire il carico client.
  - Riceve il traffico HTTPS dal servizio di bilanciamento del carico.
  - Supporta la sessione permanente per l'host Tableau.
  - Configura il proxy per il bilanciamento del carico round robin in ogni sistema Tableau Server che esegue il processo Gateway.
  - Gestisce le richieste di autenticazione dall'IdP esterno.
- Proxy di inoltro: Tableau Server richiede l'accesso a Internet per la gestione delle licenze e le funzionalità per le mappe. Devi configurare gli elenchi consentiti del proxy di inoltro per gli URL dei servizi Tableau. Vedi *Comunicare con Internet* (Linux).

- Tutto il traffico relativo ai client può essere crittografato su HTTPS:
  - Dal client al servizio di bilanciamento del carico dell'applicazione
  - Dal servizio di bilanciamento del carico dell'applicazione ai server proxy inversi
  - Dal server proxy a Tableau Server
  - Dal gestore di autenticazione in esecuzione su un proxy inverso all'IdP
  - Da Tableau Server all'IdP

Gateway indipendente Tableau Server

In Tableau Server versione 2022.1 è stato introdotto Gateway indipendente Tableau Server. Gateway indipendente è un'istanza autonoma del processo Gateway di Tableau che opera come proxy inverso compatibile con Tableau.

Gateway indipendente supporta il bilanciamento del carico round robin semplice nelle istanze back-end di Tableau Server. Gateway indipendente non deve tuttavia essere utilizzato come servizio di bilanciamento del carico delle applicazioni aziendali. Ti consigliamo di eseguire Gateway indipendente dietro un servizio di bilanciamento del carico delle applicazioni aziendali.

Gateway indipendente richiede una licenza Advanced Management.

Autenticazione e autorizzazione

L'architettura di riferimento predefinita specifica l'installazione di Tableau Server con l'autenticazione locale configurata. In questo modello, i client devono connettersi a Tableau Server per essere autenticati dal processo di autenticazione locale nativo di Tableau Server. Non è consigliabile utilizzare questo metodo di autenticazione nell'architettura di riferimento perché lo scenario richiede che i client non autenticati comunichino nel livello applicazione, il che rappresenta un rischio per la sicurezza.

È invece consigliabile configurare un provider di identità esterno di livello aziendale, associato a un modulo AuthN per pre-autenticare tutto il traffico verso il livello applicazione. Se configurato con un IdP esterno, il processo di autenticazione locale nativo di Tableau Server

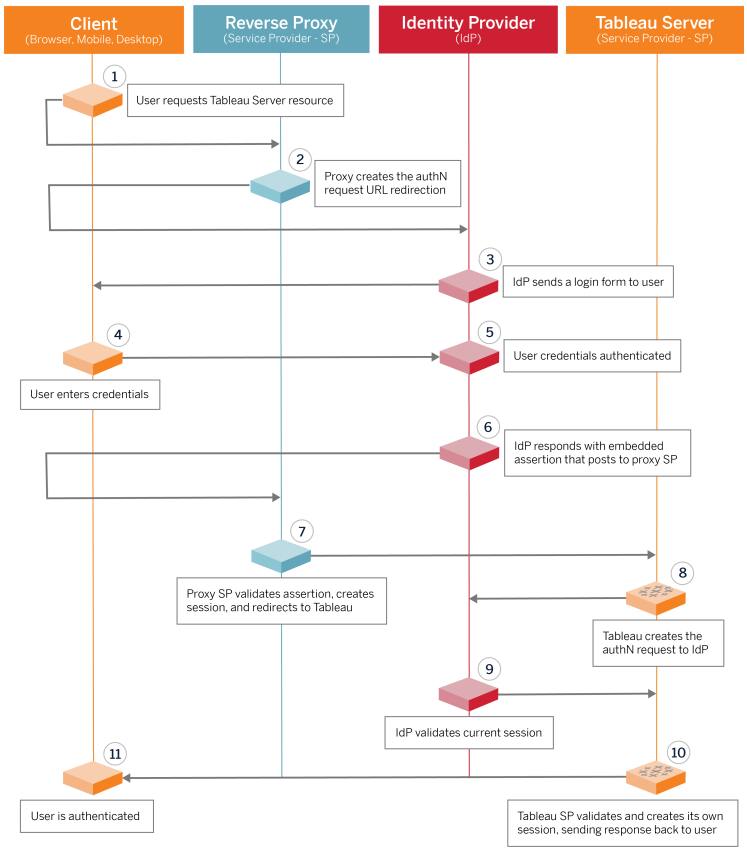
non viene utilizzato. Tableau Server autorizza l'accesso alle risorse nella distribuzione dopo che l'IdP ha autenticato gli utenti.

Pre-autenticazione con un modulo AuthN

Nell'esempio documentato in questa guida è configurato l'accesso SSO SAML, ma il processo di pre-autenticazione può essere configurato con la maggior parte dei provider di identità esterni e un modulo AuthN.

Nell'architettura di riferimento, il proxy inverso è configurato per creare una sessione di autenticazione client con l'IdP prima di inoltrare tali richieste a Tableau Server. Ci riferiamo a questo processo come fase di *pre-autenticazione*. Il proxy inverso reindirizzerà solo le sessioni client autenticate a Tableau Server. Tableau Server creerà una sessione, verificherà l'autenticazione della sessione con l'IdP e quindi restituirà la richiesta client.

Il diagramma seguente mostra i dettagli passo passo del processo di pre-autenticazione e autenticazione con un modulo AuthN configurato. Il proxy inverso può essere una soluzione generica di terze parti o Gateway indipendente Tableau Server:



Panoramica della configurazione

Questa è una panoramica del processo per configurare il livello Web. Verifica la connettività dopo ogni passaggio:

1. Configura due proxy inversi per fornire l'accesso HTTP a Tableau Server.
2. Configura la logica di bilanciamento del carico con sessioni permanenti sui server proxy per connetterti a ogni istanza di Tableau Server che esegue il processo Gateway.
3. Configura il bilanciamento del carico dell'applicazione con sessioni permanenti sul gateway Internet per inoltrare le richieste ai server proxy inversi.
4. Configura l'autenticazione con un IdP esterno. Puoi configurare SSO o SAML installando un gestore di autenticazione sui server proxy inversi. Il modulo AuthN gestisce

l'handshake di autenticazione tra l'IdP esterno e la distribuzione di Tableau. Tableau opererà anche come fornitore di servizi IdP e autenticherà gli utenti con l'IdP.

5. Per eseguire l'autenticazione con Tableau Desktop in questa distribuzione, i client devono eseguire Tableau Desktop 2021.2.1 o versione successiva.

Esempio di configurazione del livello Web con Gateway indipendente Tableau Server

Il resto di questo argomento fornisce una procedura end-to-end che descrive come implementare il livello Web nell'architettura di riferimento AWS utilizzando Gateway indipendente Tableau Server. Per un esempio di configurazione che utilizza Apache come proxy inverso, consulta Appendice - Livello Web con distribuzione di esempio di Apache.

La configurazione di esempio è composta dai seguenti componenti:

- Servizio di bilanciamento del carico dell'applicazione AWS
- Gateway indipendente Tableau Server
- Modulo di autenticazione Mellon
- IdP Okta
- Autenticazione SAML

Nota: la configurazione del livello Web di esempio presentata in questa sezione include procedure dettagliate per la distribuzione di software e servizi di terze parti. Abbiamo fatto del nostro meglio per verificare e documentare le procedure necessarie per abilitare lo scenario del livello Web. Tuttavia, il software di terze parti potrebbe cambiare o lo scenario potrebbe differire dall'architettura di riferimento descritta in questo documento. Fai riferimento alla documentazione di terze parti per i dettagli della configurazione e il supporto.

Gli esempi relativi a Linux in questa sezione mostrano i comandi per le distribuzioni di tipo RHEL. In particolare, i comandi riportati di seguito sono stati sviluppati con la distribuzione Amazon Linux 2. Se esegui una distribuzione di Ubuntu, modifica i comandi di conseguenza.

La distribuzione del livello Web in questo esempio adotta una configurazione graduale e una procedura di verifica. La configurazione principale del livello Web comprende le fasi seguenti per abilitare HTTP tra Tableau e Internet. Gateway indipendente viene eseguito e configurato per il proxy inverso/bilanciamento del carico dietro il servizio di bilanciamento del carico dell'applicazione AWS:

1. Preparare l'ambiente
2. Installare Gateway indipendente
3. Configurare server di Gateway indipendente
4. Configurare il servizio di bilanciamento del carico dell'applicazione AWS

Dopo aver configurato il livello Web e verificato la connettività con Tableau, configura l'autenticazione con un provider esterno.

Preparare l'ambiente

Completa le seguenti attività prima di distribuire Gateway indipendente.

1. Modifiche al gruppo di sicurezza AWS. Configurare il gruppo di sicurezza Pubblico per consentire il traffico di Housekeeping di Gateway indipendente in entrata (TCP 21319) dal gruppo di sicurezza Privato.

2. Installa la versione 22.1.1 (o successiva) su un cluster Tableau Server a quattro nodi come documentato in Parte 4 - Installazione e configurazione di Tableau Server.

3. Configura le due istanze EC2 proxy nel gruppo di sicurezza Pubblico come documentato in Configurare computer host.

Installare Gateway indipendente

Gateway indipendente Tableau Server richiede una licenza Advanced Management.

La distribuzione di Gateway indipendente Tableau Server comprende l'installazione e l'esecuzione del pacchetto .rpm e quindi la configurazione dello stato iniziale. La procedura inclusa in questa guida fornisce indicazioni prescrittive per l'implementazione nell'architettura di riferimento.

Se la tua distribuzione differisce dall'architettura di riferimento, consulta la documentazione di base di Tableau Server, *Installare Tableau Server con Gateway indipendente* (Linux).

> **Importante**: la configurazione del Gateway indipendente può essere un processo soggetto a errori. È molto difficile risolvere i problemi di configurazione in due istanze di server Gateway indipendenti. Per questo motivo, consigliamo di configurare un server Gateway indipendente alla volta. Dopo aver configurato il primo server e averne verificato la funzionalità, devi configurare il secondo server Gateway indipendente.

Sebbene configurerai ciascun server Gateway indipendente separatamente, esegui questa procedura di installazione su entrambe le istanze EC2 installate nel gruppo di sicurezza Pubblico:

1. Esegui l'aggiornamento per applicare le correzioni più recenti al sistema operativo Linux:

   ```
   sudo yum update
   ```

2. Se Apache è installato, rimuovilo:

   ```
   sudo yum remove httpd
   ```

3. Copia la versione 2022.1.1 (o successiva) del pacchetto di installazione di Gateway indipendente dalla pagina dei download di Tableau nel computer host che eseguirà Tableau Server.

   Ad esempio, su un computer con sistema operativo Linux di tipo RHEL, esegui

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

4. Esegui il programma di installazione. Ad esempio, su un sistema operativo Linux di tipo RHEL, esegui:

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

5. Passa alla directory `/opt/tableau/tableau_tsig/packages/scripts.<version_code>/` ed esegui lo script `initialize-tsig` disponibile in tale posizione. In aggiunta al flag `--accepteula`, devi includere l'intervallo IP delle subnet in cui è in esecuzione la distribuzione di Tableau Server. Utilizza l'opzione `-c` per specificare l'intervallo IP. L'esempio seguente mostra il comando con le subnet AWS di esempio specificate:

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

6. Al termine dell'inizializzazione, apri il file `tsighk-auth.conf` e copia il segreto di autenticazione nel file. Dovrai inviare questo codice per ogni istanza di Gateway indipendente come parte della configurazione back-end di Tableau Server:

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

7. Dopo aver eseguito le fasi precedenti su entrambe le istanze di Gateway indipendente, prepara il file di configurazione `tsig.json`. Il file di configurazione è costituito da una matrice "independentGateways". La matrice contiene oggetti di configurazione, ciascuno dei quali definisce i dettagli di connessione per un'istanza di Gateway indipendente.

   Copia il seguente codice JSON e personalizzalo in base al tuo ambiente di distribuzione. L'esempio mostra un file per un'architettura di riferimento AWS di esempio.

   Il file JSON di esempio riportato di seguito include solo le informazioni di connessione per un Gateway indipendente. Più avanti nel processo, includerai le informazioni di connessione per il secondo server Gateway indipendente.

   Salva il file come `tsig.json` per le procedure che seguono.

```
{
"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"`: il nome DNS privato dell'istanza EC2 AWS che esegue Gateway indipendente.
- `"host"`: uguale a `"id"`.
- `"port"`: porta di Housekeeping, per impostazione predefinita `"21319"`.
- `"protocol"`: il protocollo per il traffico client. Mantieni `http` per la configurazione iniziale.
- `"authsecret"`: il segreto che hai copiato nella fase precedente.

Gateway indipendente: confronto tra connessione diretta e di inoltro

Prima di procedere, è necessario decidere quale schema di connessione configurare nella distribuzione: connessione diretta o di inoltro. Ciascuna opzione è descritta brevemente di seguito, insieme ai dati rilevanti per prendere una decisione.

Connessione di inoltro: puoi configurare Gateway indipendente per inoltrare la comunicazione del client su un'unica porta al processo gateway su Tableau Server. Questa configurazione viene definita connessione di *inoltro*:

- Il processo di inoltro comporta un passaggio aggiuntivo da Gateway indipendente al processo gateway di back-end di Tableau Server. Il passaggio in più riduce le prestazioni rispetto alla configurazione con connessione diretta.

- TLS è supportato per la modalità di inoltro. Tutte le comunicazioni in modalità di inoltro sono limitate a un unico protocollo (HTTP o HTTPS) e possono quindi essere crittografate e autenticate con TLS.

Connessione diretta: Gateway indipendente può comunicare direttamente con i processi back-end di Tableau Server su più porte. Questo tipo di comunicazione viene definita connessione *diretta*:

- Poiché la connessione avviene in modo diretto al back-end di Tableau Server, le prestazioni dei client risultano notevolmente superiori rispetto all'opzione con connessione di inoltro.
- Richiede l'apertura di oltre 16 porte dalle subnet pubbliche a private per la comunicazione diretta del processo da Gateway indipendente ai computer Tableau Server.
- TLS non è ancora supportato per i processi da Gateway indipendente a Tableau Server.

Configurare la connessione di inoltro

Per eseguire TLS fra Tableau Server e il Gateway indipendente, devi configurare con una connessione di inoltro. Gli scenari di esempio nella Guida alla distribuzione sono configurati con una connessione di inoltro.

1. Copia `tsig.json` in Nodo 1 della distribuzione di Tableau Server.

2. In Nodo 1 esegui questi comandi per abilitare Gateway indipendente.

```
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
```

Configurare la connessione diretta

Poiché la connessione diretta non supporta TLS, ti consigliamo di configurare la connessione diretta solo se sei in grado di proteggere tutto il traffico di rete con altri mezzi. Per eseguire TLS fra Tableau Server e il Gateway indipendente, devi configurare con una connessione di inoltro. Gli scenari di esempio nella Guida alla distribuzione sono configurati con una connessione di inoltro.

Se stai configurando Gateway indipendente per la connessione diretta a Tableau Server, devi abilitare la configurazione per attivare la comunicazione. Una volta che Tableau Server comunica con Gateway indipendente, verranno stabilite le destinazioni del protocollo. È quindi necessario recuperare `proxy_targets.csv` dal computer Gateway indipendente e aprire le porte corrispondenti dal gruppo di sicurezza Pubblico a quello Privato in AWS.

1. Copia `tsig.json` in Nodo 1 della distribuzione di Tableau Server.
2. In Nodo 1 esegui questi comandi per abilitare Gateway indipendente.

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

3. Nel computer Gateway indipendente esegui questo comando per visualizzare le porte utilizzate dal cluster di Tableau Server:

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

4. Configura i gruppi di sicurezza AWS. Aggiungi le porte TCP elencate in `proxy_targets.csv` per consentire la comunicazione dal gruppo di sicurezza Pubblico al gruppo di sicurezza Privato.

   È consigliabile automatizzare la configurazione di ingresso sulle porte poiché le porte potrebbero cambiare se la distribuzione di Tableau Server cambia. L'aggiunta di nodi o

la riconfigurazione dei processi sulla distribuzione di Tableau Server attiveranno le modifiche all'accesso alla porta richiesto da Gateway indipendente.

Verifica: configurazione della topologia di base

Dovresti essere in grado di accedere alla pagina di amministrazione di Tableau Server visitando `http://<gateway-public-IP-address>`.

Se la pagina di accesso di Tableau Server non viene caricata o se Tableau Server non si avvia, segui queste fasi di risoluzione dei problemi:

Rete:

- Verifica la connettività fra la distribuzione di Tableau e l'istanza del Gateway indipendente eseguendo il seguente comando `wget` da Tableau Server Nodo 1: wget http://<indirizzo IP interno del Gateway indipendente>:21319, ad esempio:

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

  Se la connessione viene rifiutata o non riesce, verifica che il gruppo di sicurezza Pubblico sia configurato per consentire il traffico di gestione del Gateway indipendente (TCP 21319) dal gruppo di sicurezza Privato.

  Se il gruppo di sicurezza è configurato correttamente, verifica di aver specificato gli indirizzi IP o gli intervalli IP corretti durante l'inizializzazione del Gateway indipendente. Puoi visualizzare e modificare questa configurazione nel file `environment.bash` che si trova in `/etc/opt/tableau/tableau_tsig/environment.bash`. Se apporti una modifica a questo file, riavvia il servizio tsig-http come descritto di seguito.

Nell'host Proxy 1:

1. Sovrascrivi il file httpd.conf con il file stub del Gateway indipendente:

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

2. Riavvia tsig-httpd come prima fase per la risoluzione dei problemi:

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

In Tableau Nodo 1

- Controlla il file `tsig.json`. Se rilevi degli errori, correggili, quindi esegui `tsm topology external-services gateway update -c tsig.json`.
- Se utilizzi una connessione diretta, verifica che le porte TCP elencate in `proxy_targets.csv` siano configurate come porte di ingresso dal gruppo di sicurezza Pubblico a quello Privato.

Configurare il servizio di bilanciamento del carico dell'applicazione AWS

Configura il servizio di bilanciamento del carico come un listener HTTP. La procedura seguente descrive come aggiungere un servizio di bilanciamento del carico in AWS.

Fase 1. Creare un gruppo di destinazione

Un gruppo di destinazione è una configurazione di AWS che definisce le istanze EC2 che eseguono i server proxy. Questi sono le destinazioni per il traffico da LBS.

1. EC2 > **Gruppi di destinazione** > **Crea gruppo di destinazione**

2. Nella pagina Crea:
    - Inserisci un nome per il gruppo di destinazione, ad esempio `TG-internal-HTTP`
    - Tipo di destinazione: istanze
    - Protocollo: HTTP
    - Porta: 80
    - VPC: seleziona il VPC
    - In **Controlli di integrità > Impostazioni avanzate controlli di integrità** >

Codici di riuscita aggiungi la lista dei codici da leggere:`200,303`.

- Fai clic su **Crea**.

3. Seleziona il gruppo di destinazione appena creato, quindi fai clic sulla scheda **Destinazione**:
    - Fai clic su **Modifica**.
    - Seleziona le istanze EC2 (o una singola istanza se ne stai configurando una alla volta) che eseguono l'applicazione proxy, quindi fai clic su **Aggiungi a registrati**.
    - Fai clic su **Salva**.

Fase 2. Avviare la procedura guidata per il servizio di bilanciamento del carico

1. EC2 > **Servizi di bilanciamento del carico** > **Crea servizio di bilanciamento del carico**
2. Nella pagina "Seleziona il tipo di servizio di bilanciamento del carico" crea un servizio di bilanciamento del carico dell'applicazione.

Nota: l'interfaccia utente visualizzata per configurare il servizio di bilanciamento del carico non è uniforme tra i data center AWS. La procedura seguente, "Configurazione tramite procedura guidata", è associata alla procedura guidata di configurazione di AWS che inizia con **Fase 1. Configurare il servizio di bilanciamento del carico**.

Se il tuo data center visualizza tutte le configurazioni in un'unica pagina che include un pulsante **Crea servizio di bilanciamento del carico** nella parte inferiore, segui la procedura "Configurazione con pagina singola" di seguito.

Configurazione tramite procedura guidata

1. Pagina **Configura servizio di bilanciamento del carico**:
    - Specifica il nome
    - Schema: internet-facing (predefinito)
    - Tipo di indirizzo IP: ipv4 (predefinito)
    - Listener (Listener e routing):
        a. mantieni il listener HTTP predefinito
        b. Fai clic su **Aggiungi listener**, quindi aggiungi `HTTPS:443`
    - VPC: seleziona il VPC in cui hai installato tutti i componenti
    - Aree di disponibilità:
        - Seleziona **a** e **b** per le regioni del data center
        - In ogni selettore a discesa corrispondente, seleziona la subnet pubblica (in cui risiedono i server proxy).
    - Fai clic su **Configura impostazioni di sicurezza**

2. Pagina **Configura impostazioni di sicurezza**
    - Carica il certificato SSL pubblico.
    - Fai clic su **Avanti: Configura gruppi di sicurezza**.

3. Pagina **Configura gruppi di sicurezza**:
    - Seleziona il gruppo di sicurezza Pubblico. Se è selezionato il gruppo di sicurezza Predefinito, deselezionarlo.
    - Fai clic su **Avanti: Configura routing**.

4. Pagina **Configura routing**
    - Gruppo di destinazione: gruppo di destinazione esistente.
    - Nome: seleziona il gruppo di destinazione che hai creato in precedenza
    - Fai clic su **Avanti: Registra destinazioni**.

5. Pagina **Registra destinazioni**
    - Dovrebbero essere visualizzate le due istanze del server proxy configurate in precedenza.
    - Fai clic su **Avanti: Verifica**.

6. Pagina **Verifica**

Fai clic su **Crea**.

Configurazione con pagina singola

Configurazione di base

- Specifica il nome
- Schema: internet-facing (predefinito)
- Tipo di indirizzo IP: ipv4 (predefinito)

Mapping di rete

- VPC: seleziona il VPC in cui hai installato tutti i componenti
- Mapping:
  - seleziona le aree di disponibilità **a** e **b** (o equivalenti) per le regioni del data center
  - In ogni selettore a discesa corrispondente, seleziona la subnet pubblica (in cui risiedono i server proxy).

Gruppi di sicurezza

Seleziona il gruppo di sicurezza Pubblico. Se è selezionato il gruppo di sicurezza Predefinito, deselezionarlo.

Listener e routing

- Mantieni il listener HTTP predefinito. Per **Azione predefinita** specifica il gruppo di destinazione impostato precedentemente.
- Fai clic su **Aggiungi listener**, quindi aggiungi `HTTPS:443`. Per **Azione predefinita** specifica il gruppo di destinazione impostato precedentemente.

Impostazioni del listener sicure

- Carica il certificato SSL pubblico.

Fai clic su **Crea servizio di bilanciamento del carico**.

Fase 3. Abilitare la persistenza

1. Dopo aver creato il servizio di bilanciamento del carico, è necessario abilitare la persistenza per il gruppo di destinazione.
    - Apri la pagina del gruppo di destinazione AWS (**EC2** > **Bilanciamento del carico** > **Gruppi di destinazione**), quindi seleziona l'istanza del gruppo di destinazione appena configurata. Nel menu **Azione** seleziona **Modifica attributi**.
    - Nella pagina **Modifica attributi** seleziona **Persistenza**, specifica una durata di `1 day`, quindi scegli **Salva modifiche**.
2. Nel servizio di bilanciamento del carico, abilita la persistenza sul listener HTTP. Seleziona il servizio di bilanciamento del carico appena configurato, quindi fai clic sulla scheda **Listener**:
    - Per **HTTP:80**, fai clic su **Visualizza/modifica regole**. Nella pagina **Regole** visualizzata fai clic sull'icona di modifica (una volta nella parte superiore della pagina e quindi di nuovo accanto alla regola) per modificare la regola. Elimina la regola THEN esistente e sostituiscila facendo clic su **Aggiungi azione** > **Inoltra a...**. Nella configurazione THEN risultante specifica lo stesso gruppo di destinazione che hai creato. In Persistenza a livello di gruppo abilita la persistenza e imposta la durata su 1 giorno. Salva l'impostazione, quindi fai clic su **Aggiorna**.

Fase 4. Impostare il timeout di inattività sul sistema di bilanciamento del carico

Nel servizio di bilanciamento del carico aggiorna il timeout di inattività a 400 secondi.

Seleziona il servizio di bilanciamento del carico che hai configurato per questa distribuzione, quindi fai clic su **Azioni** > **Modifica attributi**. Imposta **Timeout di inattività** su `400` secondi, quindi fai clic su **Salva**.

Fase 5. Verificare la connettività di LBS

Apri la pagina del servizio di bilanciamento del carico AWS (**EC2** > **Servizi di bilanciamento del carico**), quindi seleziona l'istanza del servizio di bilanciamento del carico appena configurata.

In **Descrizione** copia il nome DNS e incollalo in un browser per accedere alla pagina di accesso di Tableau Server.

Se viene visualizzato un errore di livello 500, potrebbe essere necessario riavviare i server proxy.

Aggiornare DNS con l'URL pubblico di Tableau

Utilizza il nome della zona DNS del tuo dominio dalla descrizione del servizio di bilanciamento del carico AWS per creare un valore CNAME nel DNS. Il traffico verso il tuo URL (tableau.esempio.com) deve essere inviato al nome DNS pubblico di AWS.

Verificare la connettività

Al termine degli aggiornamenti del DNS, dovresti essere in grado di accedere alla pagina di accesso di Tableau Server inserendo il tuo URL pubblico, ad esempio `http-s://tableau.example.com`.

Esempio di configurazione dell'autenticazione: SAML con IdP esterno

L'esempio seguente descrive come impostare e configurare SAML con l'IdP Okta e il modulo di autenticazione Mellon per una distribuzione di Tableau in esecuzione nell'architettura di riferimento AWS.

Questo esempio riprende dalla sezione precedente e presuppone che si stia configurando un Gateway indipendente alla volta.

L'esempio descrive come configurare Tableau Server e Gateway indipendente su HTTP. Okta invierà la richiesta al sistema di bilanciamento del carico AWS tramite HTTPS, ma tutto il traffico interno sarà trasmesso tramite HTTP. Durante la configurazione per questo scenario, tieni presente i protocolli HTTP e HTTPS quando imposti le stringhe URL.

Questo esempio utilizza Mellon come modulo del provider di servizi di pre-autenticazione sui server del Gateway indipendente. Questa configurazione garantisce che solo il traffico autenticato si connetta a Tableau Server, che opera anche come provider di servizi con l'IdP Okta. Pertanto, devi configurare due applicazioni IdP: una per il provider di servizi Mellon e una per il provider di servizi Tableau.

Creare l'account amministratore di Tableau

Un errore comune durante la configurazione di SAML è dimenticare di creare un account amministratore su Tableau Server prima di abilitare SSO.

Il primo passaggio consiste nel creare un account su Tableau Server con un ruolo di amministratore del server. Per lo scenario Okta di esempio, il nome utente deve essere in un formato di indirizzo email valido, per esempio, user@example.com. È necessario impostare una password per questo utente, ma la password non verrà utilizzata dopo la configurazione di SAML.

Configurare l'applicazione di pre-autorizzazione Okta

Lo scenario end-to-end descritto in questa sezione richiede due applicazioni Okta:

- Applicazione di pre-autenticazione Okta
- Applicazione Tableau Server Okta

Ognuna di queste applicazioni è associata a diversi metadati, che dovrai configurare rispettivamente sul proxy inverso e su Tableau Server.

Questa procedura descrive come creare e configurare l'applicazione di pre-autenticazione Okta. Più avanti in questo argomento verrà creata l'applicazione Tableau Server Okta. Per un account Okta di prova gratuito con utenti limitati, vedi la pagina Web degli sviluppatori Okta .

Crea un'integrazione dell'app SAML per il provider di servizi di pre-autenticazione Mellon.

1. Apri la dashboard di amministrazione di Okta > **Applicazioni** > **Crea integrazione app**.

2. Nella pagina **Crea una nuova integrazione app** seleziona **SAML 2.0**, quindi fai clic su **Avanti**.

3. Nella scheda **Impostazioni generali** immetti un nome per l'app, ad esempio `Tableau Pre-Auth`, quindi fai clic su **Avanti**.

4. Nella scheda **Configura SAML**:

   - URL Single Sign-On (SSO). L'elemento finale del percorso nell'URL Single Sign-On è indicato come `MellonEndpointPath` nel file di configurazione `mellon.conf` riportato più avanti in questa procedura. Puoi specificare qualsiasi endpoint desideri. In questo esempio, l'endpoint è `sso`. L'ultimo elemento, `postResponse`, è obbligatorio: `https://tableau.example.com/sso/postResponse`.
   - Deseleziona la casella di controllo: **Utilizzalo per URL destinatario e URL di destinazione**.
   - URL destinatario: uguale all'URL SSO, ma con HTTP. Ad esempio, `http://tableau.example.com/sso/postResponse`.
   - URL di destinazione: uguale all'URL SSO, ma con HTTP. Ad esempio, `http://tableau.example.com/sso/postResponse`.
   - URI destinatario (ID entità del provider di servizi). Ad esempio, `https://tableau.example.com`.
   - Formato ID nome: `EmailAddress`
   - Nome utente applicazione: `Email`
   - Dichiarazioni attributi: Nome = `mail`; Formato nome = `Unspecified`; Valore = `user.email`.

   Fai clic su **Avanti**.

5. Nella scheda **Feedback** seleziona:

   - **Sono un cliente Okta che aggiunge un'app interna**
   - **Questa è un'app interna che abbiamo creato**
   - Fai clic su **Fine**.

6. Crea il file di metadati IdP pre-autenticazione:
    - In Okta: **Applicazioni** > **Applicazioni** > La tua nuova applicazione (ad esempio, `Tableau Pre-Auth`) > **Accesso**
    - Accanto a **Certificati di firma SAML**, fai clic su **Visualizza istruzioni di configurazione SAML**.
    - Nella pagina **Come configurare SAML 2.0 per l'applicazione <pre-auth>**, scorri verso il basso fino alla sezione **Facoltativa**, **Fornisci i seguenti metadati IDP al tuo fornitore di servizi**.
    - Copia il contenuto del campo XML e salvalo in un file chiamato `pre-auth_idp_metadata.xml`.
7. (Facoltativo) Configura l'autenticazione a più fattori:
    - In Okta: **Applicazioni** > **Applicazioni** > La tua nuova applicazione (ad esempio, `Tableau Pre-Auth`) > **Accesso**
    - In **Criterio di accesso** fai clic su **Aggiungi regola**.
    - In **Regola di accesso all'app** specifica un nome e le diverse opzioni MFA. Per testare la funzionalità, puoi mantenere tutte le opzioni predefinite. Tuttavia, in **Azioni** devi selezionare **Richiedi fattore** e quindi specificare la frequenza con cui gli utenti devono eseguire l'accesso. Fai **clic** su Salva.

Creare e assegnare un utente Okta

1. In Okta, crea un utente con lo stesso nome utente che hai creato in Tableau (utente@example.com): **Directory** > **Persone** > **Aggiungi persona**.
2. Dopo che l'utente è stato creato, assegna la nuova app Okta a tale persona: fai clic sul nome utente, quindi assegna l'applicazione in **Assegna applicazione**.

Installare Mellon per la pre-autenticazione

In questo esempio viene utilizzato mod_auth_mellon, un popolare modulo open source. Alcune distribuzioni Linux includono versioni obsolete di mod_auth_mellon da un repository precedente. Tali versioni obsolete possono contenere vulnerabilità di sicurezza sconosciute o problemi funzionali. Se scegli di utilizzare mod_auth_mellon, verifica di utilizzare una versione corrente.

Il modulo mod_auth_mellon è un software di terze parti. Abbiamo fatto del nostro meglio per verificare e documentare le procedure necessarie per abilitare questo scenario. Tuttavia, il software di terze parti potrebbe cambiare o lo scenario potrebbe differire dall'architettura di riferimento descritta in questo documento. Fai riferimento alla documentazione di terze parti per i dettagli della configurazione e il supporto.

1. Nell'istanza attiva EC2 che esegue il Gateway indipendente, installa una versione corrente del modulo di autenticazione Mellon.
2. Crea la directory `/etc/mellon`:

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

Configurare Mellon come modulo di pre-autenticazione

Esegui questa procedura sulla prima istanza del Gateway indipendente.

Devi disporre di una copia del file `pre-auth_idp_metadata.xml` che hai creato dalla configurazione di Okta.

1. Cambia directory:

   ```
   cd /etc/mellon
   ```

2. Crea i metadati del provider di servizi. Esegui lo script `mellon_create_metadata.sh`. Devi includere l'ID entità e l'URL restituito per la tua organizzazione nel comando.

   L'URL restituito è indicato come *URL Single Sign-On* in Okta. L'elemento finale del percorso nell'URL restituito è indicato come `MellonEndpointPath` nel file di configurazione `mellon.conf` riportato più avanti in questa procedura. In questo esempio, specifichiamo `sso` come percorso dell'endpoint.

   Ad esempio:

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

Lo script restituisce il certificato, la chiave e i file dei metadati del provider di servizi.

3. Rinomina i file del provider di servizi nella directory `mellon` per una maggiore leggibilità. Nella documentazione verrà fatto riferimento a questi file con i seguenti nomi:

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

4. Copia il file `pre-auth_idp_metadata.xml` nella stessa directory.

5. Modifica la proprietà e le autorizzazioni per tutti i file nella directory `/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. Crea la directory `/etc/mellon/conf.d`:

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

7. Crea il file `global.conf` nella directory `/etc/mellon/conf.d`.

Copia il contenuto del file come mostrato di seguito, ma aggiorna `MellonCookieDomain` con il tuo nome di dominio radice. Ad esempio, se il nome di dominio per Tableau è `tableau.example.com`, inserisci `example.com` per il dominio radice.

```
<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. Crea il file `mellonmod.conf` nella directory `/etc/mellon/conf.d`.

   Questo file contiene una singola direttiva che specifica il percorso del file `mod_auth_mellon.so`. Il percorso nell'esempio indicato è il percorso predefinito del file. Verifica che il file sia presente in tale percorso o modifica il percorso in questa direttiva in modo che corrisponda al percorso effettivo di `mod_auth_mellon.so`:

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

Creare un'applicazione Tableau Server in Okta

1. Nella dashboard di Okta: **Applicazioni** > **Applicazioni** > **Sfoglia catalogo app**
2. In **Sfoglia catalogo integrazione app** cerca `Tableau`, seleziona il riquadro Tableau Server, quindi fai clic su **Aggiungi**.
3. In **Aggiungi Tableau Server** > **Impostazioni generali** immetti un'etichetta, quindi fai clic su **Avanti**.
4. In Opzioni di accesso, seleziona **SAML 2.0**, quindi scorri verso il basso fino ad Impostazioni di accesso avanzate:
   - **ID entità SAML**: inserisci l'URL pubblico, ad esempio https://tableau.example.com.

- **Formato nome utente applicazione**: E-mail

5. Fai clic sul collegamento **Metadati del provider di identità** per avviare un browser. Copia il collegamento nel browser. Questo è il collegamento che utilizzerai durante la configurazione di Tableau nella procedura seguente.
6. Fai clic su **Fine**.
7. Assegna la nuova app Okta Tableau Server all'utente (utente@example.com): fai clic sul nome utente, quindi assegna l'applicazione in **Assegna applicazione**.

Impostare la configurazione del modulo di autenticazione in Tableau Server

Esegui i comandi indicati di seguito sul Nodo 1 di Tableau Server. Questi comandi specificano le posizioni dei file di configurazione di Mellon sul computer remoto del Gateway indipendente. Verifica che i percorsi dei file specificati in questi comandi siano mappati ai percorsi e alla posizione dei file sul computer remoto del Gateway indipendente.

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

Per ridurre i tempi di inattività, non applicare le modifiche prima di aver abilitato SAML come descritto nella sezione successiva.

Abilitare SAML su Tableau Server per l'IdP

Esegui questa procedura su Nodo 1 di Tableau Server.

1. Scarica i metadati dell'applicazione Tableau Server da Okta. Usa il collegamento che hai salvato dalla procedura precedente:

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

2. Copia un certificato TLS e il relativo file chiave in Tableau Server. Il file chiave deve essere una chiave RSA. Per maggiori informazioni sui requisiti del certificato SAML e dell'IdP, consulta *Requisiti SAML* (Linux).

   Per semplificare la gestione e la distribuzione dei certificati e come procedura consigliata per la sicurezza, è consigliabile utilizzare i certificati generati da un'importante e affidabile autorità di certificazione (CA) terza. In alternativa, puoi generare certificati autofirmati o utilizzare i certificati di un'infrastruttura a chiave pubblica per TLS.

   Se non disponi di un certificato TLS, puoi generare un certificato autofirmato utilizzando la procedura incorporata riportata di seguito.

Generare un certificato autofirmato

Esegui questa procedura su Nodo 1 di Tableau Server.

a. Genera la chiave dell'autorità di certificazione (CA) radice di firma:

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

b. Crea il certificato CA radice:

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

Ti verrà richiesto di inserire i valori per i campi del certificato. Ad esempio:

```
Country Name (2 letter code) [XX]:US
State or Province Name (full name) []:Washington
Locality Name (eg, city) [Default City]:Seattle
Organization Name (eg, company) [Default Company Ltd]:Ta-
bleau
Organizational Unit Name (eg, section) []:Operations
```

```
Common Name (eg, your name or your server's hostname) []:ta-
bleau.example.com
Email Address []:example@tableau.com
```

c. Crea il certificato e la relativa chiave (`server-saml.csr` e `server-saml.key` nell'esempio seguente). Il nome del soggetto per il certificato deve corrispondere al nome host pubblico dell'host Tableau. Il nome del soggetto è impostato con l'opzione `-subj` con il formato `"/CN=<host-name>"`, ad esempio:

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

d. Firma il nuovo certificato con il certificato CA che hai creato in precedenza. Il seguente comando invia in output anche il certificato nel formato `crt`:

```
openssl x509 -req -in server-saml.csr -days 3650 -CA roo-
tCACert-saml.pem -CAkey rootCAKey-saml.pem -CAcreateserial
-out server-saml.crt
```

e. Converti il file chiave in RSA. Tableau richiede un file chiave RSA per SAML. Per convertire la chiave, esegui questo comando:

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

3. Configura SAML. Esegui questo comando, specificando l'ID dell'entità e l'URL restituito, nonché i percorsi del file dei metadati, del file del certificato e del file chiave:

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

tsm authentication saml enable
```

4. Se la tua organizzazione esegue Tableau Desktop 2021.4 o versione successiva, devi eseguire questo comando per abilitare l'autenticazione tramite i server proxy inversi.

   Le versioni di Tableau Desktop 2021.2.1-2021.3 funzioneranno senza eseguire questo comando, a condizione che il modulo di pre-autenticazione (ad esempio, Mellon) sia configurato in modo da consentire la conservazione dei cookie del dominio di primo livello.

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

5. Applica le modifiche alla configurazione:

   ```
   tsm pending-changes apply
   ```

Riavviare il servizio tsig-httpd

Quando la distribuzione di Tableau Server applica le modifiche, accedi nuovamente al computer del Gateway indipendente di Tableau Server ed esegui i seguenti comandi per riavviare il servizio tsig-httpd:

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

Convalidare la funzionalità SAML

Per convalidare la funzionalità SAML end-to-end, accedi a Tableau Server con l'URL pubblico (ad esempio, https://tableau.example.com) tramite l'account amministratore di Tableau creato all'inizio di questa procedura.

Se TSM non si avvia ("errore del gateway") o se vengono visualizzati errori del browser quando tenti di connetterti, consulta Risolvere i problemi del Gateway indipendente di Tableau Server.

Configurare il modulo di autenticazione nella seconda istanza del Gateway indipendente

Dopo aver configurato correttamente la prima istanza di Gateway indipendente, distribuisci la seconda istanza. Questo esempio è il processo finale per l'installazione dello scenario AWS/Mellon/Okta descritto in questo argomento. La procedura presuppone che tu abbia già installato il Gateway indipendente sulla seconda istanza, come descritto in questo argomento in precedenza (Installazione del Gateway indipendente).

Il processo per la distribuzione del secondo Gateway indipendente richiede i seguenti passaggi:

1. Nella seconda istanza del Gateway indipendente: installa il modulo di autorizzazione Mellon.

   Non configurare il modulo di autenticazione Mellon come descritto in precedenza in questo argomento. Devi invece clonare la configurazione come descritto nelle fasi successive.

2. Sulla (prima) istanza configurata di Gateway indipendente:

   Esegui una copia tar della configurazione Mellon esistente. Il backup tar conserverà tutta la gerarchia di directory e le autorizzazioni. Esegui questi comandi:

   ```
   cd /etc
   sudo tar -cvf mellon.tar mellon
   ```

   Copia `mellon.tar` nella seconda istanza del Gateway indipendente.

3. Nella seconda istanza del Gateway indipendente:

   Estrai ("decomprimi") il file tar nella seconda istanza nella directory `/etc`. Esegui questi comandi:

   ```
   cd /etc
   ```

```
sudo tar -xvf mellon.tar
```

4. Sul nodo 1 della distribuzione di Tableau Server: aggiorna il file di connessione (`tsig.-json`) con le informazioni di connessione dal secondo Gateway indipendente. Dovrai recuperare la chiave di autenticazione come descritto in questo argomento in precedenza (Installare il Gateway indipendente).

   Un esempio di file di connessione (`tsig.json`) è riportato qui:

```
{
"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. Sul nodo 1 della distribuzione di Tableau Server: esegui i seguenti comandi per aggiornare la configurazione:

```
tsm stop

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

tsm start
```

6. In entrambe le istanze del Gateway indipendente: all'avvio di Tableau Server, riavvia il processo `tsig-httpd`:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

7. In AWS **EC2>Gruppi di destinazione**: aggiorna il gruppo di destinazione per includere l'istanza EC2 che esegue la seconda istanza del Gateway indipendente.

   Seleziona il gruppo di destinazione appena creato, quindi fai clic sulla scheda Destinazione:

   - Fai clic su **Modifica**.
   - Seleziona l'istanza EC2 del secondo computer Gateway indipendente, quindi fai clic su **Aggiungi a registrato**. Fai clic su **Salva**.

Parte 6 - Configurazione post-installazione

Configurare SSL/TLS dal servizio di bilanciamento del carico a Tableau Server

Alcune organizzazioni richiedono un canale di crittografia end-to-end dal client al servizio back-end. L'architettura di riferimento predefinita, come descritto fino a questo punto, specifica SSL dal client al servizio di bilanciamento del carico in esecuzione nel livello Web dell'organizzazione.

In questa sezione viene descritto come configurare SSL/TLS per Tableau Server e Gateway indipendente nell'architettura di riferimento AWS di esempio. Per un esempio di configurazione che descrive come configurare SSL/TLS su Apache nell'architettura di riferimento AWS, consulta Esempio: configurare SSL/TLS nell'architettura di riferimento AWS.

Al momento, TLS non è supportato per i processi back-end di Tableau Server eseguiti nell'intervallo 8000-9000. Per abilitare TLS, devi configurare Gateway indipendente con una connessione di inoltro a Tableau Server.

Questa procedura descrive come abilitare e configurare TLS in Gateway indipendente per Tableau Server e in Tableau Server per Gateway indipendente. La procedura crittografa il traffico di inoltro su HTTPS/443 e il traffico di Housekeeping su HTTPS/21319.

Le procedure relative a Linux in questo esempio mostrano i comandi per le distribuzioni di tipo RHEL. In particolare, i comandi riportati di seguito sono stati sviluppati con la distribuzione Amazon Linux 2. Se esegui una distribuzione di Ubuntu, modifica i comandi di conseguenza.

Le indicazioni riportate sono prescrittive per la specifica architettura di riferimento AWS di esempio presentata in questa guida. Pertanto, le configurazioni opzionali non sono incluse.

Per la documentazione di riferimento completa, consulta *Configurare TLS in Gateway indipendente* (Linux).

Prima di configurare TLS

Esegui le configurazioni di TLS al di fuori dell'orario lavorativo. La configurazione richiede almeno un riavvio di Tableau Server. Se si esegue una distribuzione completa dell'architettura di riferimento a quattro nodi, il riavvio può richiedere tempo.

- Verifica che i client possano connettersi a Tableau Server tramite HTTP. La configurazione di TLS con Gateway indipendente è un processo in più fasi e potrebbe richiedere la risoluzione dei problemi. Pertanto, è consigliabile iniziare con una distribuzione di Tableau Server completamente operativa prima di configurare TLS.

- Raccogli i certificati TLS/SSL, le chiavi e le risorse correlate. Avrai bisogno di certificati SSL per le istanze di Gateway indipendente e per Tableau Server. Per semplificare la gestione e la distribuzione dei certificati e come procedura consigliata per la sicurezza, è consigliabile utilizzare i certificati generati da un'importante e affidabile autorità di certificazione (CA) terza. In alternativa, puoi generare certificati autofirmati o utilizzare i certificati di un'infrastruttura a chiave pubblica per TLS.

  La configurazione di esempio in questo argomento utilizza i seguenti nomi di risorse a titolo illustrativo:

  - `tsig-ssl.crt`: il certificato TLS/SSL per il Gateway indipendente.
  - `tsig-ssl.key`: la chiave privata per `tsig-ssl.crt` nel Gateway Indipendente.
  - `ts-ssl.crt`: il certificato TLS/SSL per Tableau Server.
  - `ts-ssl.key`: la chiave privata per `tsig-ssl.crt` in Tableau Server.
  - `tableau-server-CA.pem`: il certificato radice dell'autorità di certificazione che genera i certificati per i computer di Tableau Server. Questo certificato in genere non è necessario se si utilizzano certificati di importanti terze parti affidabili.
  - `rootTSIG-CACert.pem`: il certificato radice dell'autorità di certificazione che genera i certificati per i computer del Gateway indipendente. Questo certificato in

genere non è necessario se si utilizzano certificati di importanti terze parti affidabili.

- Ci sono altri certificati e risorse di file chiave necessari per SAML che sono descritti in dettaglio nella Parte 5 di questa Guida.
- Se l'implementazione richiede l'uso di un file della catena di certificati, consulta l'articolo della Knowledge Base Configurare TLS su gateway indipendente quando si usa un certificato con una catena di certificati.

- Verifica di avere accesso all'IdP. Se stai utilizzando un IdP per l'autenticazione, probabilmente dovrai apportare modifiche al destinatario e agli URL di destinazione nell'IdP dopo aver configurato SSL/TLS.

Configurare i computer Gateway indipendente per TLS

La configurazione di TLS può essere un processo soggetto a errori. Poiché la risoluzione dei problemi in due istanze di Gateway indipendente può richiedere molto tempo, consigliamo di abilitare e configurare TLS sull'implementazione EDG con un solo Gateway indipendente. Dopo aver verificato che TLS funzioni nella distribuzione, configura il secondo computer Gateway indipendente.

Fase 1: distribuire certificati e chiavi al computer Gateway indipendente

Puoi distribuire le risorse in qualsiasi directory arbitraria, purché l'utente tsig-httpd abbia accesso in lettura ai file. I percorsi di questi file sono indicati in altre procedure. Useremo i percorsi di esempio in `/etc/ssl`, come mostrato di seguito, in tutto l'argomento.

1. Crea la directory per la chiave privata:

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

2. Copia i file del certificato e della chiave nei percorsi `/etc/ssl`. Ad esempio,

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

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

3. (Facoltativo) Se utilizzi un certificato autofirmato o PKI per SSL/TLS su Tableau Server, devi copiare anche il file del certificato radice della CA sul computer Gateway indipendente. Ad esempio,

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

Fase 2: aggiornare le variabili di ambiente per TLS

È necessario aggiornare le variabili di ambiente della porta e del protocollo per la configurazione di Gateway indipendente.

Modifica questi valori aggiornando il file, `/etc/opt/tableau/tableau_tsig/environment.bash`, come segue:

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

Fase 3: aggiornare il file di configurazione dello stub per il protocollo HK

Modifica manualmente il file di configurazione dello stub (`/var/opt/tableau/tableau_tsig/config/httpd.conf.stub`) per impostare le direttive httpd Apache relative a TLS per il protocollo di Housekeeping (HK).

Il file di configurazione dello stub include un blocco di direttive relative a TLS commentate con un indicatore `#TLS#`. Rimuovi gli indicatori dalle direttive come mostrato nell'esempio seguente. Tieni presente che l'esempio mostra l'uso del certificato CA radice per il certificato SSL utilizzato in Tableau Server con l'opzione `SSLCACertificateFile`.

```
#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>
```

Queste modifiche andranno perse se si reinstalla Gateway indipendente. È consigliabile creare una copia di backup.

Fase 4: copiare il file stub e riavviare il servizio

1. Copia il file che hai aggiornato nell'ultima fase per aggiornare httpd.conf con le modifiche:

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

2. Riavvia il servizio Gateway indipendente:

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

Dopo il riavvio, Gateway indipendente non sarà operativo finché non esegui la serie di fasi successiva in Tableau Server. Dopo aver completato le fasi in Tableau Server, Gateway indipendente raccoglierà le modifiche e sarà online.

Configurare Nodo 1 di Tableau Server per TLS

Esegui queste fasi su Nodo 1 nella distribuzione di Tableau Server.

Fase 1: copiare certificati e chiavi e arrestare TSM

1. Verifica di avere copiato i certificati e le chiavi "SSL esterno" di Tableau Server in Nodo 1.

2. Per ridurre al minimo i tempi di inattività, è consigliabile arrestare TSM, eseguire le fasi seguenti e quindi avviare TSM dopo l'applicazione delle modifiche:

   ```
   tsm stop
   ```

Fase 2: impostare le risorse del certificato e abilitare la configurazione di Gateway indipendente

1. Specifica la posizione dei file del certificato e della chiave per Gateway indipendente. Questi percorsi fanno riferimento alla posizione sui computer Gateway indipendente. Tieni presente che questo esempio presuppone che lo stesso certificato e la stessa coppia di chiavi vengano utilizzati per proteggere il traffico HTTPS e di Housekeeping:

   ```
   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. Abilita TLS per i protocolli HTTPS e HK per Gateway indipendente:

   ```
   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. (Facoltativo) Se utilizzi un certificato autofirmato o PKI per SSL/TLS su Gateway indipendente, devi caricare il file del certificato radice della CA. Il file del certificato radice dell'autorità di certificazione è il certificato radice utilizzato per generare i certificati per i computer del gateway indipendente. Ad esempio,

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

4. (Facoltativo) Se utilizzi un certificato autofirmato o PKI per SSL/TLS su Tableau Server, devi copiare il file del certificato radice dell'autorità di certificazione nella directory `/etc/ssl/certs` del Gateway indipendente. Il file del certificato radice dell'autorità di certificazione è il certificato radice utilizzato per generare i certificati per i computer di Tableau Server. Dopo aver copiato il certificato nel Gateway indipendente devi specificare la posizione del certificato sul Nodo 1 con il seguente comando tsm. Ad esempio,

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

5. (Facoltativo: solo a scopo di test) Se stai utilizzando la condivisione di certificati auto-firmati o PKI tra i computer e quindi i nomi dei soggetti nei certificati non corrispondono ai nomi dei computer, devi disabilitare la verifica dei certificati.

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

Fase 3: abilitare "SSL esterno" per Tableau Server e applicare le modifiche

1. Abilita e configura "SSL esterno" in Tableau Server:

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

2. Applica le modifiche.

   ```
   tsm pending-changes apply
   ```

Fase 4: aggiornare il file JSON di configurazione del gateway e avviare tsm

1. Aggiorna il file di configurazione di Gateway indipendente (ad esempio, `tsig.json`) sul lato Tableau Server per specificare il protocollo `https` per gli oggetti di Gateway indipendente:

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

2. Rimuovi (o commenta) le informazioni di connessione per la seconda istanza di Gateway indipendente. Assicurati di verificare il JSON in un editor esterno prima di salvarlo.

Dopo aver configurato e convalidato TLS per la singola istanza di Gateway indipendente, aggiorna il file JSON con le informazioni di connessione per la seconda istanza di Gateway indipendente.

3. Esegui questo comando per aggiornare la configurazione di Gateway indipendente:

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

4. Avvia TSM.

   ```
   tsm start
   ```

5. Durante l'avvio di TSM, accedi all'istanza di Gateway indipendente e riavvia il servizio `tsig-httpd`:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

Aggiornare a HTTPS gli URL del modulo di autenticazione dell'IdP

Se hai configurato un provider di identità esterno per Tableau, probabilmente dovrai aggiornare gli URL restituiti nella dashboard amministrativa dell'IdP.

Ad esempio, se utilizzi un'applicazione di pre-autenticazione Okta, dovrai aggiornare l'applicazione in modo da utilizzare il protocollo HTTPS per l'URL destinatario e l'URL di destinazione.

Configurare il servizio di bilanciamento del carico AWS per HTTPS

Se stai eseguendo la distribuzione con il servizio di bilanciamento del carico AWS come documentato in questa guida, riconfigura il servizio di bilanciamento del carico AWS in modo da inviare il traffico HTTPS ai computer che eseguono Gateway indipendente:

1. Elimina il gruppo di destinazione HTTP esistente:

   In **Gruppi di destinazione** seleziona il gruppo di destinazione HTTP che è stato configurato per il servizio di bilanciamento del carico, fai clic su **Azioni** e quindi su **Elimina**.

2. Crea il gruppo di destinazione HTTPS:

   Gruppi di destinazione > **Crea gruppo di destinazione**

   - Seleziona "Istanze"
   - Inserisci un nome per il gruppo di destinazione, ad esempio `TG-internal-HTTPS`
   - Seleziona il VPC
   - Protocollo: HTTPS 443
   - In **Controlli di integrità > Impostazioni avanzate controlli di integrità** > **Codici di riuscita** aggiungi la lista dei codici da leggere:`200,303`.
   - Fai clic su **Crea**.

3. Seleziona il gruppo di destinazione appena creato, quindi fai clic sulla scheda **Destinazione**:

   - Fai clic su **Modifica**.
   - Seleziona l'istanza EC2 che esegue il Gateway indipendente Tableau Server configurato, quindi fai clic su **Aggiungi a registrate**.
   - Fai clic su **Salva**.

4. Dopo aver creato il gruppo di destinazione, è necessario abilitare la persistenza:

   - Apri la pagina del gruppo di destinazione AWS (**EC2** > **Bilanciamento del carico** > **Gruppi di destinazione**), quindi seleziona l'istanza del gruppo di destinazione appena configurata. Nel menu **Azione** seleziona **Modifica attributi**.
   - Nella pagina **Modifica attributi** seleziona **Persistenza**, specifica una durata di `1 day`, quindi scegli **Salva modifiche**.

5. Sul servizio di bilanciamento del carico, aggiorna le regole del listener. Seleziona il servizio di bilanciamento del carico che hai configurato per questa distribuzione, quindi fai clic sulla scheda **Listener**.

- Per **HTTP:80**, fai clic su **Visualizza/modifica regole**. Nella pagina **Regole** visualizzata fai clic sull'icona di modifica (una volta nella parte superiore della pagina e quindi di nuovo accanto alla regola) per modificare la regola. Elimina la regola THEN esistente e sostituiscila facendo clic su **Aggiungi azione** > **Reindirizza a...**. Nella configurazione THEN risultante, specifica `HTTPS` e la porta `443` e mantieni le impostazioni predefinite per le altre opzioni. Salva l'impostazione, quindi fai clic su **Aggiorna**.
- Per **HTTPS:443**, fai clic su **Visualizza/modifica regole**. Nella pagina **Regole** visualizzata fai clic sull'icona di modifica (una volta nella parte superiore della pagina e quindi di nuovo accanto alla regola) per modificare la regola. Elimina la regola THEN esistente e sostituiscila facendo clic su **Aggiungi azione** > **Inoltra a...**. Specifica come gruppo di destinazione il gruppo HTTPS che hai appena creato. In **Persistenza a livello di gruppo** abilita la persistenza e imposta la durata su 1 giorno. Salva l'impostazione, quindi fai clic su **Aggiorna**.

6. Nel servizio di bilanciamento del carico aggiorna il timeout di inattività a 400 secondi. Seleziona il servizio di bilanciamento del carico che hai configurato per questa distribuzione, quindi fai clic su **Azioni** > **Modifica attributi**. Imposta **Timeout di inattività** su `400` secondi, quindi fai clic su **Salva**.

Convalidare TLS

Per convalidare la funzionalità TLS, accedi a Tableau Server con l'URL pubblico (ad esempio, https://tableau.example.com) tramite l'account amministratore di Tableau creato all'inizio di questa procedura.

Se TSM non si avvia o vengono visualizzati altri errori, consulta Risolvere i problemi del Gateway indipendente di Tableau Server.

Configurare la seconda istanza di Gateway indipendente per SSL

Dopo aver configurato correttamente la prima istanza di Gateway indipendente, distribuisci la seconda istanza.

Il processo per la distribuzione del secondo Gateway indipendente richiede i seguenti passaggi:

1. Nella (prima) istanza configurata del Gateway indipendente: copia i seguenti file nelle posizioni corrispondenti della seconda istanza del gateway indipendente:
   - `/etc/ssl/certs/tsig-ssl.crt`
   - `/etc/ssl/private/tsig-ssl.key` (dovrai creare la directory `private` nella seconda istanza).
   - `/var/opt/tableau/tableau_tsig/config/httpd.conf.stub`
   - `/etc/opt/tableau/tableau_tsig/environment.bash`

2. Sul nodo 1 della distribuzione di Tableau Server: aggiorna il file di connessione (`tsig.json`) con le informazioni di connessione dal secondo Gateway indipendente.

   Un esempio di file di connessione (`tsig.json`) è riportato qui:

```
{
"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. Sul nodo 1 della distribuzione di Tableau Server: esegui i seguenti comandi per aggiornare la configurazione:

   ```
   tsm stop
   ```

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

   ```
   tsm start
   ```

4. Su entrambe le istanze di Gateway indipendente: all'avvio di Tableau Server, riavvia il processo `tsig-httpd` su entrambe le istanze di Gateway indipendente:

   ```
   sudo su - tableau-tsig
   ```

   ```
   systemctl --user restart tsig-httpd
   ```

   ```
   exit
   ```

5. In AWS **EC2>Gruppi di destinazione**: aggiorna il gruppo di destinazione per includere l'istanza EC2 che esegue la seconda istanza del Gateway indipendente.

   Seleziona il gruppo di destinazione appena creato, quindi fai clic sulla scheda Destinazione:

   - Fai clic su **Modifica**.
   - Seleziona l'istanza EC2 del secondo computer Gateway indipendente, quindi fai clic su **Aggiungi a registrato**. Fai clic su **Salva**.

Configurare SSL per Postgres

Puoi facoltativamente configurare SSL (TSL) per Postgres per la connessione al repository esterno su Tableau Server.

Per semplificare la gestione e la distribuzione dei certificati e come procedura consigliata per la sicurezza, è consigliabile utilizzare i certificati generati da un'importante e affidabile autorità di certificazione (CA) terza. In alternativa, puoi generare certificati autofirmati o utilizzare i certificati di un'infrastruttura a chiave pubblica per TLS.

Questa procedura descrive come utilizzare OpenSSL per generare un certificato autofirmato nell'host Postgres in una distribuzione Linux di tipo RHEL nell'architettura di riferimento AWS di esempio.

Dopo aver generato e firmato il certificato SSL, devi copiare il certificato CA nell'host Tableau.

Nell'host che esegue Postgres:

1. Genera la chiave dell'autorità di certificazione (CA) radice di firma:

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

2. Crea il certificato CA radice:

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

   Ti verrà richiesto di inserire i valori per i campi del certificato. Ad esempio:

   ```
   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. Crea il certificato e la relativa chiave (`server.csr` e `server.key` nell'esempio seguente) per il computer Postgres. Il nome del soggetto per il certificato deve corrispondere al nome DNS privato EC2 dell'host Postgres. Il nome del soggetto è

impostato con l'opzione `-subj` con il formato `"/CN=<private DNS name>"`, ad esempio:

```
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. Firma il nuovo certificato con il certificato CA che hai creato nella fase 2. Il seguente comando invia in output anche il certificato nel formato `crt`:

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

5. Copia i file crt e i file chiave key nel percorso `/var/lib/pgsql/13/data/` di Postgres:

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

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

6. Passa all'utente radice:

   ```
   sudo su
   ```

7. Imposta le autorizzazioni sui file cer e i file chiave. Esegui questi comandi:

   ```
   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. Aggiorna il file di configurazione pg_haba, `/var/lib/pgsql/13/data/pg_hba.conf` per specificare il trust md5:

   Modifica le istruzioni di connessione esistenti da

   ```
   host all all 10.0.30.0/24 password
   ```
   e

```
host all all 10.0.31.0/24 password
```

a

```
host all all 10.0.30.0/24 md5
```
e

```
host all all 10.0.31.0/24 md5.
```

9. Aggiorna il file postgresql, `/var/lib/pgsql/13/data/postgresql.conf`, aggiungendo questa riga:

   ```
   ssl = on
   ```

10. Esci dalla modalità utente radice:

    ```
    exit
    ```

11. Riavvia Postgres:

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

Facoltativo: abilitare la convalida dell'attendibilità del certificato su Tableau Server per Postgres SSL

Se hai seguito la procedura di installazione nella Parte 4 - Installazione e configurazione di Tableau Server, Tableau Server è configurato con SSL opzionale per la connessione Postgres. Ciò significa che la configurazione di SSL su Postgres (come descritto sopra) risulterà in una connessione crittografata.

Se desideri richiedere la convalida dell'attendibilità del certificato per la connessione, devi eseguire il seguente comando su Tableau Server per riconfigurare la connessione host di Postgres:

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

Dove `<filename>.json` è il file di connessione descritto in Configurare Postgres esterno. E `CACert.pem` è il file del certificato dell'autorità di certificazione per il certificato SSL/TLS utilizzato da Postgres.

Facoltativo: verifica la connettività SSL

Per verificare la connettività SSL, devi:

- Installare il client Postgres su Tableau Server Nodo 1.
- Copiare il certificato radice che hai creato nella procedura precedente sull'host di Tableau.
- Connetterti al server Postgres dal Nodo 1

Installare il client Postgres sul Nodo 1

In questo esempio viene illustrato come installare Postgres versione 13.4. Installa la stessa versione in esecuzione per il repository esterno.

1. Nel Nodo 1, Crea e modifica il file pgdg.repo nel percorso `/etc/yum.repos.d`. Popola il file con le seguenti informazioni di configurazione.

   ```
   [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. Installa il client Postgres:

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

Copiare il certificato radice nel Nodo 1

Copia il certificato dell'autorità di certificazione (`pgsql-rootCACert.pem`) nell'host di Tableau:

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

Connettersi all'host Postgres tramite SSL dal Nodo 1:

esegui il comando seguente dal Nodo 1, specificando l'indirizzo IP dell'host del server Postgres e il certificato radice:

```
psql "postgresql://postgres@<IP-addres-
s>:5432/postgres?sslmode=verify-ca&sslrootcert=pgsql-roo-
tCACert.pem"
```

Ad esempio:

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

Postgres richiederà la password. Dopo aver effettuato l'accesso, la shell restituirà:

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

Configurare SMTP e le notifiche degli eventi

Tableau Server invia notifiche tramite e-mail ad amministratori e utenti. Per abilitare questa funzionalità, devi configurare Tableau Server per inviare la posta al tuo server e-mail. È inoltre necessario specificare i tipi di eventi, le soglie e le informazioni sulla sottoscrizione che si desidera inviare.

Per la configurazione iniziale di SMTP e delle notifiche è consigliabile utilizzare il modello di file di configurazione seguente per creare un file json. Puoi anche impostare qualsiasi singola chiave di configurazione riportata di seguito con la sintassi descritta in *tsm configuration set* (Linux).

Esegui questa procedura su Nodo 1 nella distribuzione di Tableau Server:

1. Copia il modello json seguente in un file. Personalizza il file con le opzioni di configurazione SMTP, la sottoscrizione e le notifiche di avviso per la tua organizzazione.
   - Per visualizzare un elenco e una descrizione di tutte le opzioni SMTP, consulta *Riferimento per la configurazione dell'interfaccia a riga di comando SMTP* (Linux).
   - Per visualizzare un elenco e una descrizione di tutte le opzioni degli eventi di notifica, consulta la sezione relativa all'interfaccia a riga di comando in *Configurare la notifica degli eventi del server* (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. Esegui `tsm settings import -f file.json` per passare il file json a Tableau Services Manager.
3. Esegui il comando `tsm pending-changes apply` per applicare le modifiche.
4. Esegui `tsm email test-smtp-connection` per visualizzare e verificare la configurazione della connessione.

Installare il driver PostgreSQL

Per visualizzare le viste amministratore su Tableau Server, il driver PostgreSQL deve essere installato nel Nodo 1 della distribuzione di Tableau Server.

1. Visita la pagina di download dei driver di Tableau e copia l'URL per il file jar PostgreSQL.
2. Esegui la procedura seguente su ciascun nodo della distribuzione di Tableau:
   - Crea il percorso file seguente:

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

   - Dal nuovo percorso, scarica la versione più recente del file jar PostgreSQL. Ad esempio:

```
sudo wget http-
s://-
downloads.tableau.com/drivers/linux/postgresql/postgresql-
42.2.22.jar
```

3. Sul nodo iniziale, riavvia Tableau Server:

```
tsm restart
```

Configurare un criterio per le password complesse

Se non stai distribuendo Tableau Server con una soluzione di autenticazione IdP, è consigliabile rafforzare la sicurezza del criterio predefinito per le password di Tableau.

Se stai distribuendo Tableau Server con un IdP, devi gestire i criteri per le password con l'IdP.

La procedura seguente include la configurazione json per l'impostazione dei criteri per le password in Tableau Server. Per maggiori informazioni sulle opzioni seguenti, consulta *Autenticazione locale* (Linux).

1. Copia il modello json seguente in un file. Compila i valori chiave con la configurazione dei criteri password.

```
{
 "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. Esegui il comando `tsm settings import -f file.json` per passare il file json a Tableau Services Manager per configurare Tableau Server.

3. Esegui il comando `tsm pending-changes apply` per applicare le modifiche.

Parte 7 - Convalida, strumenti e risoluzione dei problemi

Questa parte include le fasi di convalida post-installazione e la guida alla risoluzione dei problemi.

Convalida del sistema di failover

Dopo aver configurato la distribuzione, ti consigliamo di eseguire semplici test di failover per convalidare la ridondanza del sistema.

Ti consigliamo di eseguire le seguenti fasi per convalidare la funzionalità di failover:

1. Arresta la prima istanza del Gateway indipendente (TSIG1). Tutto il traffico in entrata deve essere instradato attraverso la seconda istanza del Gateway indipendente (TSIG2).
2. Riavvia TSIG1 e quindi arresta TSIG2. Tutto il traffico in entrata dovrebbe instradarsi attraverso TSIG1.
3. Riavvia TSIG2.

4. Arresta Tableau Server Nodo 1. Tutto il traffico del servizio Vizportal/Applicazione passerà al Nodo 2.

   Nota: a partire da settembre 2022, la disponibilità elevata del Nodo 1 risultava compromessa in determinate versioni di Tableau Server 2021.4 e versioni successive. Le connessioni dei client non riusciranno se il Nodo 1 è inattivo. Questo problema è stato risolto nelle seguenti versioni di manutenzione:

   - 2021.4.15 e successive
   - 2022.1.11 e successive
   - 2023.1.3 e successive

> Per garantire che l'installazione di Tableau Server che utilizza le attivazioni ATR abbia un periodo di tolleranza di 72 ore dopo l'errore iniziale del nodo, installa o esegui l'upgrade a una di queste versioni. Per maggiori dettagli, consulta Tableau Server con disponibilità elevata che utilizza ATR non ha un periodo di tolleranza dopo l'errore iniziale del nodo nella Knowledge Base di Tableau.

5. Riavvia il Nodo 1 e arresta il Nodo 2. Tutto il traffico del servizio Vizportal/Applicazione passerà al Nodo 1.
6. Riavvia il Nodo 2.

In questo contesto, l'"arresto" o il "riavvio" viene eseguito spegnendo il sistema operativo o la macchina virtuale senza prima tentare una chiusura regolare dell'applicazione. L'obiettivo è simulare un guasto dell'hardware o della macchina virtuale.

La fase minima di convalida per ogni test di failover consiste nell'autenticarsi con un utente ed eseguire operazioni di visualizzazione di base.

Potresti ricevere un errore del browser "Richiesta errata" quando tenti di accedere dopo un guasto simulato. Potresti visualizzare questo errore anche se svuoti la cache nel browser. Spesso questo problema si verifica quando il browser memorizza nella cache i dati della sessione precedente di IdP. Se questo errore persiste anche dopo aver cancellato la cache del browser locale, convalida lo scenario di Tableau connettendoti con un browser diverso.

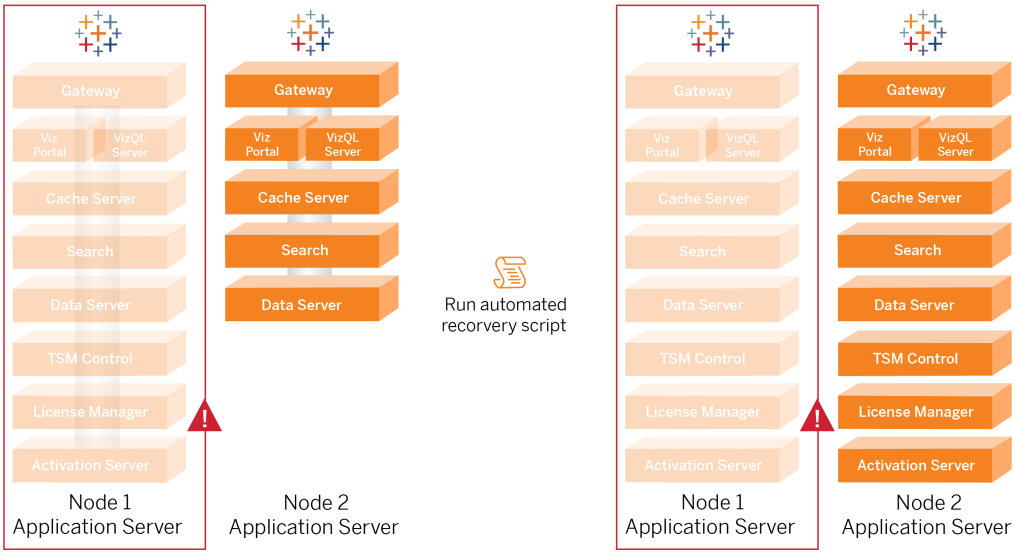
Ripristino automatizzato del nodo iniziale

Tableau Server versione 2021.2.4 e successive includono uno script di ripristino automatizzato del nodo iniziale, `auto-node-recovery`, nella directory degli script (`/app/tableau_server/packages/scripts.<version>`).

Se si verifica un problema con il nodo iniziale e sono presenti processi ridondanti nel Nodo 2, non è garantito che Tableau Server continui a funzionare. Tableau Server può continuare a funzionare fino a 72 ore dopo un errore del nodo iniziale, prima che la mancanza del servizio

di gestione licenze influisca su altri processi. In tal caso, gli utenti potrebbero continuare a effettuare l'accesso e a visualizzare e a utilizzare il loro contenuto dopo il problema nel nodo iniziale, ma non potrai riconfigurare Tableau Server perché non disporrai più dell'accesso al controller di amministrazione.

Anche se configurato con processi ridondanti, Tableau Server potrebbe non continuare a funzionare dopo un problema nel nodo iniziale.



Per ripristinare il nodo iniziale (Nodo 1) in seguito a un errore:

1. Accedi al Nodo 2 di Tableau Server.
2. Passa alla directory degli script:

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

3. Esegui questo comando per avviare lo script:

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

Dove `<license keys>` è un elenco separato da virgole (senza spazi) delle chiavi di licenza per la tua distribuzione. Se non hai accesso alle chiavi di licenza, visita il Portale clienti di Tableau per recuperarle. Ad esempio:

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

Lo script auto-node-recovery eseguirà circa 20 passaggi per ripristinare i servizi sul Nodo 2. Ogni passaggio viene visualizzato nel terminale durante l'avanzamento dello script. Lo stato più dettagliato è registrato in `/data/tableau_data/logs/app-controller-move.-log`. Nella maggior parte degli ambienti, il completamento dello script richiede dai 35 ai 45 minuti.

Risoluzione dei problemi di ripristino del nodo iniziale

Se il ripristino del nodo non riesce, potrebbe essere utile eseguire lo script in modo interattivo per consentire o meno specifici passaggi nel corso del processo. Ad esempio, se lo script non riesce a un certo punto del processo, puoi esaminare il file di log, apportare modifiche alla configurazione e quindi eseguire nuovamente lo script. Tramite l'esecuzione in modalità interattiva, puoi saltare tutti i passaggi fino a raggiungere quello che non è riuscito.

Per eseguire lo script in modalità interattiva, aggiungi lo switch `-i` all'argomento script.

Ricostruzione del nodo con errori

Dopo aver eseguito lo script, il Nodo 2 eseguirà tutti i servizi che erano precedentemente sull'host Nodo 1 in cui si è verificato il problema. Per aggiungere il Nodo 4, devi distribuire un nuovo host Tableau Server con il file di bootstrap e configurarlo come hai fatto per il Nodo 2 originale, come specificato nella parte 4. Consulta Configurare Nodo 2.

switchto

Switchto è uno script di Tim che semplifica il passaggio da una finestra all'altra.

1. Copia il codice seguente in un file denominato `switchto` nella home directory dell'host bastion.

```
#!/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. Aggiorna gli indirizzi IP nello script per mapparli alle tue istanze EC2, quindi salva il file.
3. Applica le autorizzazioni al file di script:

```
sudo chmod +x switchto
```

Uso:

Per passare a un host, esegui questo comando:

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

Ad esempio, per passare a Nodo 1, esegui questo comando:

```
./switchto node1
```

Risolvere i problemi del Gateway indipendente di Tableau Server

La configurazione di Gateway indipendente, Okta, Mellon e SAML su Tableau Server può essere un processo soggetto a errori. La causa principale più comune è un errore della stringa. Ad esempio, una barra finale (`/`) sugli URL Okta specificati durante la configurazione può causare un errore di mancata corrispondenza relativo all'asserzione SAML. Questo è solo un esempio. Durante la configurazione esistono molte opportunità di inserire una stringa errata in una qualsiasi delle applicazioni.

Riavviare il servizio tableau-tsig

Comincia (e concludi) la risoluzione dei problemi riavviando sempre il servizio tableau-tsig sui computer del Gateway indipendente. Il riavvio di questo servizio è rapido e spesso fa scattare il caricamento della configurazione aggiornata da Tableau Server.

Esegui questo comando sul computer del Gateway indipendente:

```
sudo su - tableau-tsig

systemctl --user restart tsig-httpd

exit
```

Trovare le stringhe errate

Se hai commesso un errore nella stringa (errore di copia/incolla, stringa troncata ecc.), dedica del tempo a esaminare ciascuna delle impostazioni che hai configurato:

- Configurazione della preautenticazione Okta. Esamina attentamente gli URL che hai impostato. Guarda le barre finali. Verifica HTTP e HTTPS.
- Cronologia della shell per la configurazione SAML sul Nodo 1. Esamina il comando `tsm authentication saml configure` che hai eseguito. Verifica che tutti gli URL corrispondano a quelli che hai configurato in Okta. Durante la revisione della cronologia della shell dal Nodo 1, verifica che i comandi `tsm configuration set` che specificano i percorsi dei file di configurazione di Mellon vengano mappati esattamente ai percorsi del Gateway indipendente in cui hai copiato i file.
- Configurazione di Mellon sul Gateway indipendente. Esamina la cronologia della shell per verificare di aver creato i metadati con la stessa stringa URL che hai configurato in Okta e Tableau SAML. Verifica che tutti i percorsi specificati in `/etc/mellon/conf.d/global.conf` siano corretti e che il `MellonCookieDomain` sia impostato sul tuo dominio principale, non sul tuo sottodominio Tableau.

Cercare nei registri pertinenti

Se tutte le stringhe sembrano essere impostate correttamente, controlla i registri per individuare eventuali errori.

Tableau Server registra errori ed eventi in decine di file di registro diversi. Il Gateway indipendente registra anche in un insieme di file locali. Ti consigliamo di ispezionare questi registri nel seguente ordine.

File di registro del Gateway indipendente

Il percorso predefinito dei file di registro del Gateway indipendente è `/var/opt/tableau/tableau_tsig/logs`.

- `access.log`: questo registro è utile in quanto contiene delle voci che mostrano le connessioni dai nodi di Tableau Server. Se ricevi degli errori del gateway (non si avvia) quando provi ad avviare TSM e non ci sono voci nel file `access.log`, allora esiste un problema di connettività principale. Verifica sempre la configurazione del gruppo di sicurezza AWS come prima fase. Un altro problema comune è un errore di battitura in `tsig.json`. Se esegui un aggiornamento di tsig.json, esegui `tsm stop` prima di eseguire `tsm topology external-services gateway update -c tsig.json`. Dopo che tsig.json è stato aggiornato, esegui `tsm start`.
- `error.log`: tra le altre voci, questo registro include gli errori di SAML e Mellon.

File di registro tabadminagent di Tableau Server

La serie di file `tabadminagent` (non `tabadmincontroller`) contiene gli unici file di registro pertinenti per la risoluzione degli errori relativi al Gateway indipendente.

Devi trovare il luogo in cui sono stati registrati gli errori del Gateway indipendente su `tabdminagent`. Questi errori possono trovarsi su qualsiasi nodo, ma su un unico nodo. Esegui le seguenti fasi su ciascun nodo nel cluster di Tableau Server fino a trovare la stringa "independent":

1. Individua la posizione del file di registro tabadminagent sui nodi 1-4 di Tableau Server nella configurazione della Guida alla distribuzione:

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

2. Apri l'ultimo registro per leggere:

   ```
   less tabadminagent_nodeN.log
   ```

   (sostituisci N con il numero del nodo)

3. Cerca tutte le istanze di "Independent" e "independent", utilizzando la seguente stringa di ricerca:

   ```
   /ndependent
   ```

   Se non ci sono corrispondenze, vai al nodo successivo e ripeti le fasi 1-3.

4. Quando ottieni una corrispondenza: premi `Shift + G` per spostarti in basso e ottenere gli ultimi messaggi di errore.

Ricaricare il file stub httpd

Il Gateway indipendente gestisce la configurazione di httpd per Apache. Un'operazione generica che risolverà spesso problemi temporanei consiste nel ricaricare il file stub httpd che esegue il seeding della configurazione Apache sottostante. Esegui i seguenti comandi su entrambe le istanze del Gateway indipendente.

1. Copia il file stub su httpd.conf:

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

2. Riavvia il servizio Gateway indipendente:

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

Eliminare o spostare i file di registro

Il Gateway indipendente registra tutti gli eventi di accesso. Dovrai gestire l'archiviazione dei file di registro per evitare di riempire lo spazio su disco. Se il tuo disco si riempie, il Gateway indipendente non sarà in grado di scrivere gli eventi di accesso e il servizio fallirà. Il seguente messaggio verrà registrato in error.log sul Gateway indipendente:

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

Questo errore comporterà uno stato `DEGRADED` per il nodo `external` durante l'esecuzione di `tsm status -v` su Tableau Nodo 1. Il nodo `external` nell'uscita di stato si riferisce al Gateway indipendente.

Per risolvere questo problema, elimina o sposta i file access.log dal disco. I file Access.log vengono archiviati in `/var/opt/tableau/tableau_tsig/logs`. Dopo aver cancellato il disco, riavvia il servizio tableau-tsig.

Errori del browser

Richiesta non valida: un errore comune per questo scenario è l'errore "Richiesta non valida" di Okta. Spesso questo problema si verifica quando il browser memorizza nella cache i dati della sessione precedente di Okta. Ad esempio, se gestisci le applicazioni Okta come amministratore di Okta e quindi tenti di accedere a Tableau con un diverso account abilitato per Okta, i dati della sessione dai dati dell'amministratore potrebbero causare l'errore "Richiesta non valida". Se questo errore persiste anche dopo aver cancellato la cache del browser locale, prova a convalidare lo scenario di Tableau connettendoti con un browser diverso.

Un'altra causa dell'errore "Richiesta non valida" è un errore di battitura in uno dei tanti URL che inserisci durante i processi di configurazione di Okta, Mellon e SAML. Verifica di averli inseriti tutti senza errori.

Spesso il file `error.log` sul server Gateway indipendente specificherà quale URL sta causando l'errore.

Non trovato - L'URL richiesto non è stato trovato su questo server: questo errore indica uno di diversi possibili errori di configurazione.

Se l'utente è autenticato con Okta e riceve questo errore, probabilmente hai caricato l'applicazione di pre-autenticazione Okta in Tableau Server quando hai configurato SAML.

Verifica di avere configurato in Tableau Server i metadati dell'applicazione Tableau Server Okta, anziché i metadati dell'applicazione di pre-autenticazione Okta

Altre fasi per la risoluzione dei problemi:

- Esamina le impostazioni dell'applicazione di pre-autenticazione Okta. Verifica che i protocolli HTTP e HTTPS siano impostati come specificato in questo argomento.
- Riavvia tsig-httpd su entrambi i server del Gateway indipendente.
- Verifica che `sudo apachectl configtest` restituisca "Sintassi OK" in entrambi i Gateway indipendenti.
- Verifica che l'utente di test sia assegnato a entrambe le applicazioni in Okta.
- Verifica che la permanenza sia impostata sul servizio di bilanciamento del carico e sui gruppi di destinazione associati

Verificare la connessione TLS da Tableau Server al Gateway indipendente

Utilizza il comando `wget` per verificare la connettività e l'accesso da Tableau Server al Gateway indipendente. Le variazioni di questo comando possono aiutarti a capire se i problemi di certificato stanno causando problemi di connessione.

Ad esempio, esegui questo comando `wget` per verificare il protocollo di pulizia (HK) da Tableau Server:

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

Crea l'URL con lo stesso indirizzo host che hai incluso per l'opzione host del file tsig.json. Specifica il protocollo `https` e aggiungi l'URL con la porta HK `21319`.

Per verificare la connettività e ignorare la verifica del certificato:

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

Per verificare che il certificato radice dell'autorità di certificazione per TSIG sia valido:

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

Se Tableau è in grado di comunicare, potresti comunque ricevere errori relativi al contenuto, ma non riceverai errori relativi alla connessione. Se Tableau non riesce a connettersi, inizia verificando la configurazione del protocollo nei gruppi firewall/di sicurezza. Ad esempio, le regole in entrata per il gruppo di sicurezza in cui risiede il Gateway indipendente devono consentire TCP 21319.

Appendice - Toolbox per la distribuzione di AWS

Questo argomento include strumenti e opzioni di distribuzione alternative per l'architettura di riferimento quando viene distribuita in AWS. Nello specifico, questo argomento descrive come automatizzare la distribuzione AWS di esempio illustrata nella Guida alla distribuzione per le organizzazioni di grandi dimensioni.

Script di installazione automatizzata TabDeploy4EDG

Lo script TabDeploy4EDG automatizza l'implementazione della distribuzione di Tableau a quattro nodi descritta in Parte 4 - Installazione e configurazione di Tableau Server. Se stai seguendo l'esempio di implementazione AWS descritto in questa guida, potresti essere in grado di eseguire TabDeploy4EDG.

Requisiti. Per eseguire lo script, devi preparare e configurare l'ambiente AWS in base all'implementazione di esempio in Parte 3 - Preparazione per la distribuzione di Tableau Server per le organizzazioni di grandi dimensioni:

- VPC, la subnet e i gruppi di sicurezza sono stati configurati come descritto. Gli indirizzi IP non devono corrispondere a quelli mostrati nell'implementazione di esempio.
- Quattro istanze EC2 che eseguono le build più recenti e aggiornate di AWS Linux 2
- PostgreSQL è installato ed è stato configurato come descritto in Installare, configurare e creare il backup tar di PostgreSQL.
- Un file di backup tar della fase 1 è disponibile nell'istanza EC2 in cui è installato PostgreSQL, come descritto in Creare il backup tar di PostgreSQL della fase 1.
- L'istanza EC2 che eseguirà il Nodo 1 della distribuzione di Tableau Server è stata configurata in modo da comunicare con PostgreSQL come descritto in Parte 4 - Installazione e configurazione di Tableau Server.

- Hai effettuato l'accesso a ciascuna istanza EC2 con una sessione SSH dall'host bastion.

Lo script impiega circa 1,5-2 ore per installare e configurare i quattro sistemi Tableau Server.

Lo script configura Tableau in base alle impostazioni prescritte dell'architettura di riferimento.

Lo script esegue le seguenti azioni:

- Ripristina il backup della fase 1 dell'host PostgreSQL, se specifichi un percorso del file tar dell'host PostgreSQL.
- Rimuove le installazioni di Tableau esistenti su tutti i nodi.
- Esegue `sudo yum update` su tutti i nodi.
- Scarica e copia il pacchetto rpm di Tableau in ogni nodo.
- Scarica e installa le dipendenze in ogni nodo.
- Crea `/app/tableau_server` e installa il pacchetto in tutti i nodi.
- Installa il Nodo 1 con un archivio identità locale e configura il repository esterno con PostgreSQL.
- Esegue l'installazione bootstrap e la configurazione iniziale di Nodo 2-Nodo 4.
- Elimina il file di bootstrap e il file di configurazione per TabDeploy4EDG.
- Configura i servizi nel cluster Tableau in base alle specifiche dell'architettura di riferimento.
- Convalida l'installazione e restituisce lo stato per ogni nodo.

Scaricare e copiare lo script sull'host bastion

1. Copia lo script dalla pagina degli esempi di TabDeploy4EDG e incolla il codice in un file denominato `TabDeploy4EDG`.
2. Salva il file nella home directory dell'host EC2 che opera come host bastion.
3. Esegui questo comando per modificare la modalità sul file in modo da renderlo eseguibile:

```
sudo chmod +x TabDeploy4EDG
```

Eseguire TabDeploy4EDG

TabDeploy4EDG deve essere eseguito dall'host bastion. Lo script è stato creato partendo dal presupposto che l'esecuzione avvenga nel contesto dell'agente di inoltro ssh come descritto in

Esempio: connettersi all'host bastion in AWS. Se l'esecuzione non avviene nel contesto dell'agente di inoltro ssh, ti verranno richieste le password durante il processo di installazione.

1. Crea, modifica e salva un file di registrazione (`registration.json`). Il file deve essere un file json formattato correttamente. Copia e personalizza il seguente modello:

   ```
   {
          "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. Esegui questo comando per generare un file di configurazione modello:

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

3. Apri il file di configurazione da modificare:

   ```
   sudo nano edg.config
   ```

   Come minimo, devi aggiungere gli indirizzi IP di ciascun host EC2, il percorso del file di registrazione e un codice di licenza valido.

4. Al termine della modifica del file di configurazione, salvalo e chiudilo.

5. Per eseguire TabDeploy4EDG, esegui questo comando:

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

Esempio: automatizza la distribuzione dell'infrastruttura AWS con Terraform

Questa sezione descrive come configurare ed eseguire Terraform per distribuire l'architettura di riferimento EDG in AWS. La configurazione Terraform di esempio presentata qui distribuisce un VPC AWS con le sottoreti, i gruppi di sicurezza e le istanze EC2 descritti nella Parte 3 - Preparazione per la distribuzione di Tableau Server per le organizzazioni di grandi dimensioni.

I modelli Terraform di esempio sono disponibili sul sito web Tableau Samples all'indirizzo https://help.tableau.com/samples/en-us/edg/edg-terraform.zip . Questi modelli devono essere configurati e personalizzati per la tua organizzazione. Il contenuto della configurazione fornito in questa sezione descrive le modifiche minime richieste al modello da personalizzare per la distribuzione.

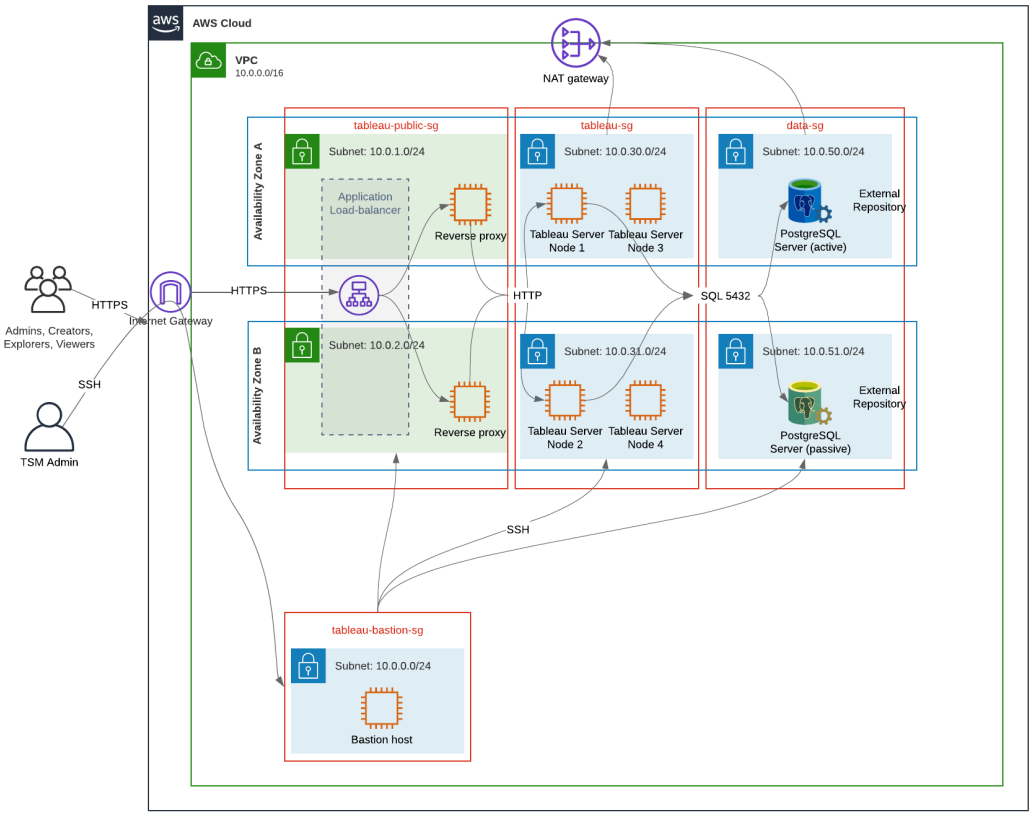
Obiettivo

I modelli e i contenuti Terraform qui forniti hanno lo scopo di fornire un esempio funzionante che ti consentirà di distribuire rapidamente EDG in un ambiente di test di sviluppo.

Abbiamo fatto del nostro meglio per testare e documentare la distribuzione Terraform di esempio. Tuttavia, l'utilizzo di Terraform per distribuire e mantenere EDG in un ambiente di produzione richiede competenze su Terraform che esulano dall'ambito di questo esempio. Tableau non fornisce supporto per la soluzione Terraform di esempio qui documentata.

Stato finale

Segui la procedura in questa sezione per configurare un VPC in AWS che sia funzionalmente equivalente al VPC specificato nella Parte 3 - Preparazione per la distribuzione di Tableau Server per le organizzazioni di grandi dimensioni.



Modelli Terraform di esempio e contenuti di supporto in questa sezione:

- Crea un VPC con un indirizzo IP elastico, due zone di disponibilità e un'organizzazione di sottoreti come mostrato sopra (gli indirizzi IP sono diversi)
- Crea i gruppi di sicurezza Bastion, Pubblico, Privato e Dati.
- Imposta la maggior parte delle regole di ingresso e uscita sui gruppi di sicurezza. Dopo l'esecuzione di Terraform dovrai modificare i gruppi di sicurezza.
- Crea i seguenti host EC2 (ciascuno esegue AWS Linux2): bastion, proxy 1 proxy 2, Tableau node 1, Tableau node 2, Tableau node 3, Tableau node 4.
- Gli host EC2 per PostgreSQL non vengono creati. È necessario creare manualmente EC2 nel gruppo di sicurezza Dati, quindi installare e configurare PostgreSQL come descritto in Installare, configurare e creare il backup tar di PostgreSQL.

Requisiti

- Account AWS: devi avere accesso a un account AWS che ti consenta di creare i VPC.
- Se esegui Terraform da un computer Windows, dovrai installare AWS CLI.
- Un indirizzo IP elastico disponibile nel tuo account AWS.
- Un dominio registrato in AWS Route 53. Terraform creerà una zona DNS e i relativi certificati SSL in Route 53. Pertanto, anche il profilo con cui viene eseguito Terraform deve disporre delle autorizzazioni appropriate in Route 53.

Prima di iniziare

- Gli esempi di riga di comando in questa procedura sono per un terminale con sistema operativo Apple. Se esegui Terraform su Windows, potresti dover adattare i comandi con i percorsi dei file in modo appropriato.
- Un progetto Terraform è costituito da molti file di configurazione di testo (estensione file .tf). Puoi configurare Terraform personalizzando questi file. Se non disponi di un editor di testo affidabile, installa Atom o Text++.
- Se condividi il progetto Terraform con altri, ti consigliamo di archiviare il progetto in Git per la gestione delle modifiche.

Fase 1: preparare l'ambiente

A. Scarica e installa Terraform

https://www.terraform.io/downloads

B. Genera una coppia di chiavi pubblica-privata

Queste sono le chiavi che utilizzerai per accedere ad AWS e all'ambiente VPC risultante. Quando esegui Terraform, includerai la chiave pubblica.

Apri il terminale ed esegui i seguenti comandi:

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

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

2. Crea una chiave pubblica. Questo formato di chiave non viene utilizzato per Terraform. Lo convertirai in una chiave ssh più avanti in questa procedura:

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

3. Imposta le autorizzazioni sulla chiave privata:

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

   Per impostare le autorizzazioni in Windows:

   - Individua il file in Esplora risorse, fai clic con il pulsante destro del mouse su di esso, quindi seleziona **Proprietà**. Passa alla scheda **Sicurezza** e poi fai clic su **Avanzate**.
   - Cambia il proprietario in te, disabilita l'ereditarietà ed elimina tutte le autorizzazioni. Concediti il **Controllo completo** e fai clic su **Salva**. Contrassegna il file come di sola lettura.

4. Crea una chiave pubblica ssh. Questa è la chiave che copierai in Terraform più avanti nella procedura.

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

C. Scarica il progetto e aggiungi la directory di stato

1. Scarica e decomprimi il progetto EDG Terraform e salvalo nel tuo computer locale. Dopo aver decompresso il download avrai una directory di primo livello, edg-terraform, e una serie di sottodirectory.

2. Crea una directory con il nome `state` allo stesso livello della directory `edg-terraform`.

Fase 2: personalizzare i modelli Terraform

Devi personalizzare i modelli Terraform per adattarli al tuo ambiente AWS ed EDG. L'esempio qui fornisce le personalizzazioni minime del modello che deve effettuare la maggior parte delle organizzazioni. È probabile che il tuo particolare ambiente richieda altre personalizzazioni.

Questa sezione è organizzata per nome del modello.

Assicurati di salvare tutte le modifiche prima di procedere alla *Fase 3: eseguire Terraform*.

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. Apri la chiave pubblica che hai generato nella fase 1B e copiala:

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

   Windows: copia il contenuto della tua chiave pubblica.

2. Copia la stringa della chiave pubblica nell'argomento public_key, ad esempio:

   ```
   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. Aggiungi dei tag in base ai requisiti della tua organizzazione. Ad esempio:

```
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-bac-
kend"
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 :
```

```
subnet.id]
security_groups            = [aws_security_group.public.id]
drop_invalid_header_fields = true
idle_timeout               = 400
tags = {
Name = "edg-again-alb"
}
                       }
```

variables.tf

Aggiorna il nome del dominio principale. Il nome deve corrispondere al dominio che hai registrato in Route 53.

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

Per impostazione predefinita, il sottodominio `tableau` è specificato per il nome di dominio DNS VPC. Per cambiarlo, aggiorna `subdomain`:

```
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`.

- Se necessario, aggiungi un blob di tag:

```
tags = {
 "Name" : var.ec2_name,
 "user.owner" = "ALIAS",
 "Application" = "tableau",
 "Creator" = "ALIAS@example.com",
 "DeptCode" = "8675309",
```

```
 "Description" = "EDG",
 "Environment" = "test",
 "Group" = "itcloud@example.com"
 }
}
```

- Se necessario, aggiorna facoltativamente lo spazio di archiviazione per gestire i tuoi requisiti di dati:

  Volume radice:

  ```
  root_block_device {
   volume_size = 100
   volume_type = "gp3"
  }
  ```

  Volume dell'applicazione:

  ```
  resource "aws_ebs_volume" "tableau" {
   availability_zone = data.aws_subnet.tableau.availability_zone
   size              = 500
   type              = "gp3"
  }
  ```

Fase 3: eseguire Terraform

A. Inizializza Terraform

Nel terminale, cambia la directory in `edg-terraform` ed esegui il comando seguente:

```
terraform init
```

Se l'inizializzazione ha esito positivo, vai alla fase successiva. Se l'inizializzazione non riesce, segui le istruzioni nell'output di Terraform.

B. Pianificare Terraform

Dalla stessa directory, esegui il comando plan:

```
terraform plan
```

Questo comando può essere eseguito più volte. Eseguilo tutte le volte necessarie per correggere gli errori. Quando questo comando viene eseguito senza errori, vai alla fase successiva.

C. Applicare Terraform

Dalla stessa directory esegui il comando apply:

```
terraform apply
```

Terraform will prompt you to verify deployment, type `Yes`.

Opzionale: distruggere Terraform

Puoi distruggere l'intero VPC eseguendo il comando destroy:

```
terraform destroy
```

Il comando destroy distruggerà solo ciò che ha creato. Se hai apportato modifiche manuali ad alcuni oggetti in AWS (ad esempio, gruppi di sicurezza, sottoreti ecc.), il comando `destroy` avrà esito negativo. Per uscire da un'operazione di distruzione in errore/sospesa, digita `Control + C`. Poi devi ripulire manualmente il VPC riportandolo allo stato in cui si trovava quando Terraform lo ha originariamente creato. Potrai poi eseguire il comando `destroy`.

Fase 4: connessione al bastion

Tutta la connessione della riga di comando avviene tramite l'host bastion su TCP 22 (protocollo SSH).

1. In AWS crea una regola in entrata nel gruppo di sicurezza bastion (**AWS** > **Gruppi di sicurezza** > **GS Bastion** > **Modifica regole in entrata**) e crea una regola per consentire le connessioni SSH (TCP 22) dall'indirizzo IP o dalla maschera di sottorete in cui eseguirai i comandi del terminale.

Facoltativo: potresti trovare utile consentire la copia dei file tra le istanze EC2 nei gruppi privato e pubblico durante la distribuzione. Crea regole SSH in entrata:

- Privato: crea una regola in entrata per consentire SSH da Pubblico
- Pubblico: crea una regola in entrata per consentire SSH da privato e da pubblico

2. Usa la chiave pem che hai creato nella Fase 1.B per connetterti all'host bastion:

   Sul terminale Mac:

   Esegui i seguenti comandi dalla directory in cui è memorizzata la chiave pem:

   `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`

   Ad esempio: `ssh -A ec2-user@3.15.12.112`.

   Su Windows usando PuTTY e Pageant:

   a. Crea un ppk dalla chiave pem: usa PuTTY Key Generator. Carica la chiave pem che hai creato nella fase 1.B. Dopo l'importazione della chiave, fai clic su **Salva chiave privata**. Questo crea un file ppk.

   b. In PuTTY: apri la configurazione e apporta le seguenti modifiche:

      - Sessioni>Nome host: aggiungi l'indirizzo IP dell'host bastion.
      - Sessioni>Porta: 22
      - Connessione>Dati>Nome utente accesso automatico: ec2-user
      - Connessione>SSH>Auth>Consenti inoltro agente
      - Connessione>SSH>Auth> Per la chiave privata, fai clic su Sfoglia e seleziona il file .ppk appena creato.

   c. Installa Pageant e carica il ppk nell'applicazione.

Fase 5: installare PostgreSQL

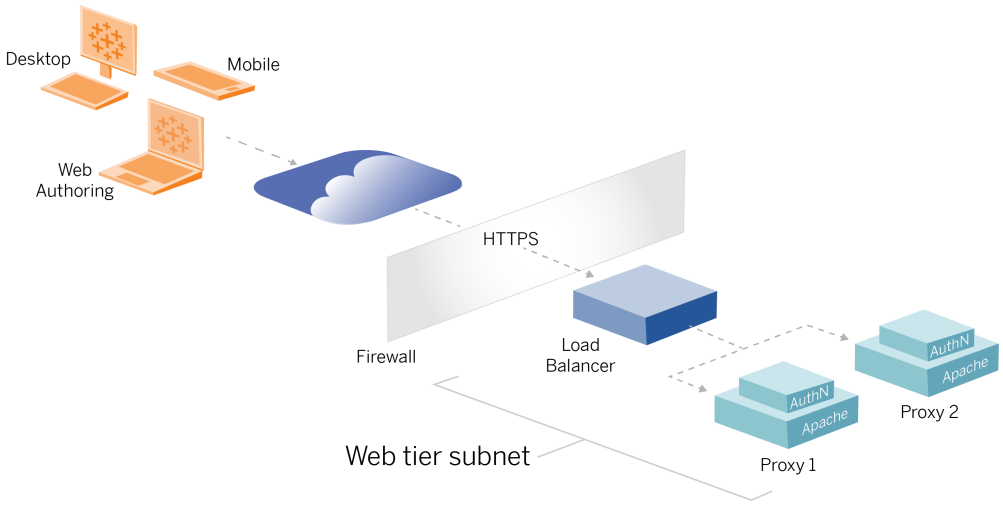
Il modello Terraform non installa PostgreSQL per l'uso come repository esterno. Tuttavia, vengono creati il gruppo di sicurezza e la sottorete associati. Se installi il repository esterno su un'istanza EC2 che esegue PostgreSQL, devi distribuire l'istanza EC2 come descritto nella Parte 3 - Preparazione per la distribuzione di Tableau Server per le organizzazioni di grandi dimensioni.

Quindi installa, configura ed esegui il backup di PostgreSQL come descritto nella Parte 4 - Installazione e configurazione di Tableau Server.

Fase 6: (facoltativo) eseguire DeployTab4EDG

Lo script TabDeploy4EDG automatizza l'implementazione della distribuzione di Tableau a quattro nodi descritta nella Parte 4. Vedi Script di installazione automatizzata TabDeploy4EDG.

Appendice - Livello Web con distribuzione di esempio di Apache



Questo argomento fornisce una procedura end-to-end che descrive come implementare il livello Web nell'architettura di riferimento AWS. La configurazione di esempio è composta dai seguenti componenti:

- Servizio di bilanciamento del carico dell'applicazione AWS
- Server proxy Apache
- Modulo di autenticazione Mellon
- IdP Okta
- Autenticazione SAML

Nota: la configurazione del livello Web di esempio presentata in questa sezione include procedure dettagliate per la distribuzione di software e servizi di terze parti. Abbiamo fatto del nostro meglio per verificare e documentare le procedure necessarie per abilitare lo scenario del livello Web. Tuttavia, il software di terze parti potrebbe cambiare o lo scenario potrebbe differire dall'architettura di riferimento descritta in questo documento. Fai

> riferimento alla documentazione di terze parti per i dettagli della configurazione e il supporto.

Gli esempi relativi a Linux in questa sezione mostrano i comandi per le distribuzioni di tipo RHEL. In particolare, i comandi riportati di seguito sono stati sviluppati con la distribuzione Amazon Linux 2. Se esegui una distribuzione di Ubuntu, modifica i comandi di conseguenza.

La distribuzione del livello Web in questo esempio adotta una configurazione graduale e una procedura di verifica. La configurazione principale del livello Web comprende le fasi seguenti per abilitare HTTP tra Tableau e Internet. Apache viene eseguito e configurato per il proxy inverso/bilanciamento del carico dietro il servizio di bilanciamento del carico dell'applicazione AWS:

1. Installare Apache
2. Configurare il proxy inverso per testare la connettività verso Tableau Server
3. Configurare il bilanciamento del carico sul proxy
4. Configurare il servizio di bilanciamento del carico dell'applicazione AWS

Dopo aver configurato il livello Web e verificato la connettività con Tableau, configura l'autenticazione con un provider esterno.

Installare Apache

Esegui questa procedura su entrambi gli host EC2 (Proxy 1 e Proxy 2). Se stai eseguendo la distribuzione in AWS secondo l'esempio dell'architettura di riferimento, dovrebbero essere presenti due aree di disponibilità con un singolo server proxy in ogni area.

1. Installa Apache:

   ```
   sudo yum update -y
   sudo yum install -y httpd
   ```

2. Configura l'avvio di Apache al riavvio:

```
sudo systemctl enable --now httpd
```

3. Verifica che la versione di httpd che hai installato includa`proxy_hcheck_module`:

   ```
   sudo httpd -M
   ```

   `proxy_hcheck_module` è obbligatorio. Se la tua versione di httpd non include questo modulo, esegui l'aggiornamento a una versione di httpd che lo includa.

Configurare il proxy per testare la connettività verso Tableau Server

Esegui questa procedura su uno degli host proxy (Proxy 1). Lo scopo di questa fase è verificare la connettività tra Internet, il server proxy e Tableau Server nel gruppo di sicurezza privato.

1. Crea un file denominato `tableau.conf` e aggiungilo alla directory `/etc/httpd/conf.d`.

   Copia il codice seguente e specifica le chiavi `ProxyPass` e `ProxyPassReverse` con l'indirizzo IP privato del Nodo 1 di Tableau Server.

   > **Importante**: la configurazione mostrata di seguito non è sicura e non deve essere utilizzata in produzione. Questa configurazione deve essere utilizzata solo durante il processo di installazione per verificare la connettività end-to-end.

   Ad esempio, se l'indirizzo IP privato del Nodo 1 è `10.0.30.32`, il contenuto del file `tableau.conf` sarà:

   ```
   <VirtualHost *:80>
   ProxyPreserveHost On
   ProxyPass "/" "http://10.0.30.32:80/"
   ```

```
ProxyPassReverse "/" "http://10.0.30.32:80/"
</VirtualHost>
```

2. Riavvia httpd:

```
sudo systemctl restart httpd
```

Verifica: configurazione della topologia di base

Dovresti essere in grado di accedere alla pagina di amministrazione di Tableau Server visitando `http://<proxy-public-IP-address>`.

Se la pagina di accesso di Tableau Server non viene caricata nel browser, segui queste fasi per la risoluzione dei problemi nell'host Proxy 1:

- Arresta e quindi avvia httpd come prima fase per la risoluzione dei problemi.
- Controlla il file `tableau.conf`. Verifica che l'IP privato di Nodo 1 sia corretto. Verifica le virgolette doppie e controlla attentamente la sintassi.
- Esegui il comando `curl` sul server proxy inverso con l'indirizzo IP privato di Nodo 1, ad esempio `curl 10.0.1.90`. Se la shell non restituisce codice html, o se restituisce il codice html per la pagina Web di test di Apache, verifica la configurazione di protocollo/porta tra i gruppi di sicurezza Pubblico e Privato.
- Esegui il comando `curl` con l'indirizzo IP privato di Proxy 1, ad esempio `curl 10.0.0.163`. Se la shell restituisce il codice html per la pagina Web di test di Apache, il file proxy non è configurato correttamente.
- Riavvia sempre httpd (`sudo systemctl restart httpd`) dopo ogni modifica della configurazione del file proxy o dei gruppi di sicurezza.
- Assicurati che TSM sia in esecuzione su Nodo 1.

Configurare il bilanciamento del carico sul proxy

1. Sullo stesso host proxy (Proxy 1) in cui hai creato il file `tableau.conf`, rimuovi la configurazione dell'host virtuale esistente e modifica il file per includere la logica di

bilanciamento del carico.

Ad esempio:

```
<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. Arresta e quindi avvia httpd:

```
sudo systemctl stop httpd
sudo systemctl start httpd
```

3. Verifica la configurazione visitando l'indirizzo IP pubblico del Proxy 1.

Copiare la configurazione sul secondo server proxy

1. Copia il file `tableau.conf` da Proxy 1 e salvalo nella directory `/etc/httpd/conf.d` sull'host Proxy 2.

2. Arresta e quindi avvia httpd:

```
sudo systemctl stop httpd
sudo systemctl start httpd
```

3. Verifica la configurazione visitando l'indirizzo IP pubblico del Proxy 2.

Configurare il servizio di bilanciamento del carico dell'applicazione AWS

Configura il servizio di bilanciamento del carico come un listener HTTP. La procedura seguente descrive come aggiungere un servizio di bilanciamento del carico in AWS.

Fase 1. Creare un gruppo di destinazione

Un gruppo di destinazione è una configurazione di AWS che definisce le istanze EC2 che eseguono i server proxy. Questi sono le destinazioni per il traffico da LBS.

1. EC2 > **Gruppi di destinazione** > **Crea gruppo di destinazione**

2. Nella pagina Crea:
   - Inserisci un nome per il gruppo di destinazione, ad esempio `TG-internal-HTTP`
   - Tipo di destinazione: istanze
   - Protocollo: HTTP
   - Porta: 80
   - VPC: seleziona il VPC
   - In **Controlli di integrità > Impostazioni avanzate controlli di integrità** > **Codici di riuscita** aggiungi la lista dei codici da leggere:`200,303`.
   - Fai clic su **Crea**.

3. Seleziona il gruppo di destinazione appena creato, quindi fai clic sulla scheda **Destinazione**:

- Fai clic su **Modifica**.
- Seleziona le istanze EC2 (o una singola istanza se ne stai configurando una alla volta) che eseguono l'applicazione proxy, quindi fai clic su **Aggiungi a registrati**.
- Fai clic su **Salva**.

Fase 2. Avviare la procedura guidata per il servizio di bilanciamento del carico

1. EC2 > **Servizi di bilanciamento del carico** > **Crea servizio di bilanciamento del carico**

2. Nella pagina "Seleziona il tipo di servizio di bilanciamento del carico" crea un servizio di bilanciamento del carico dell'applicazione.

Nota: l'interfaccia utente visualizzata per configurare il servizio di bilanciamento del carico non è uniforme tra i data center AWS. La procedura seguente, "Configurazione tramite procedura guidata", è associata alla procedura guidata di configurazione di AWS che inizia con **Fase 1. Configurare il servizio di bilanciamento del carico**.

Se il tuo data center visualizza tutte le configurazioni in un'unica pagina che include un pulsante **Crea servizio di bilanciamento del carico** nella parte inferiore, segui la procedura "Configurazione con pagina singola" di seguito.

Configurazione tramite procedura guidata

1. Pagina **Configura servizio di bilanciamento del carico**:
    - Specifica il nome
    - Schema: internet-facing (predefinito)
    - Tipo di indirizzo IP: ipv4 (predefinito)

- Listener (Listener e routing):
  a. mantieni il listener HTTP predefinito
  b. Fai clic su **Aggiungi listener**, quindi aggiungi `HTTPS:443`
- VPC: seleziona il VPC in cui hai installato tutti i componenti
- Aree di disponibilità:
  - Seleziona **a** e **b** per le regioni del data center
  - In ogni selettore a discesa corrispondente, seleziona la subnet pubblica (in cui risiedono i server proxy).
- Fai clic su **Configura impostazioni di sicurezza**

2. Pagina **Configura impostazioni di sicurezza**

   - Carica il certificato SSL pubblico.
   - Fai clic su **Avanti: Configura gruppi di sicurezza**.

3. Pagina **Configura gruppi di sicurezza**:

   - Seleziona il gruppo di sicurezza Pubblico. Se è selezionato il gruppo di sicurezza Predefinito, deselezionarlo.
   - Fai clic su **Avanti: Configura routing**.

4. Pagina **Configura routing**

   - Gruppo di destinazione: gruppo di destinazione esistente.
   - Nome: seleziona il gruppo di destinazione che hai creato in precedenza
   - Fai clic su **Avanti: Registra destinazioni**.

5. Pagina **Registra destinazioni**

   - Dovrebbero essere visualizzate le due istanze del server proxy configurate in precedenza.
   - Fai clic su **Avanti: Verifica**.

6. Pagina **Verifica**

   Fai clic su **Crea**.

Configurazione con pagina singola

Configurazione di base

- Specifica il nome
- Schema: internet-facing (predefinito)
- Tipo di indirizzo IP: ipv4 (predefinito)

Mapping di rete

- VPC: seleziona il VPC in cui hai installato tutti i componenti
- Mapping:
    - seleziona le aree di disponibilità **a** e **b** (o equivalenti) per le regioni del data center
    - In ogni selettore a discesa corrispondente, seleziona la subnet pubblica (in cui risiedono i server proxy).

Gruppi di sicurezza

Seleziona il gruppo di sicurezza Pubblico. Se è selezionato il gruppo di sicurezza Predefinito, deselezionarlo.

Listener e routing

- Mantieni il listener HTTP predefinito. Per **Azione predefinita** specifica il gruppo di destinazione impostato precedentemente.
- Fai clic su **Aggiungi listener**, quindi aggiungi `HTTPS:443`. Per **Azione predefinita** specifica il gruppo di destinazione impostato precedentemente.

Impostazioni del listener sicure

- Carica il certificato SSL pubblico.

Fai clic su **Crea servizio di bilanciamento del carico**.

Fase 3. Abilitare la persistenza

1. Dopo aver creato il servizio di bilanciamento del carico, è necessario abilitare la persistenza per il gruppo di destinazione.
    - Apri la pagina del gruppo di destinazione AWS (**EC2** > **Bilanciamento del carico** > **Gruppi di destinazione**), quindi seleziona l'istanza del gruppo di destinazione appena configurata. Nel menu **Azione** seleziona **Modifica attributi**.
    - Nella pagina **Modifica attributi** seleziona **Persistenza**, specifica una durata di `1 day`, quindi scegli **Salva modifiche**.
2. Nel servizio di bilanciamento del carico, abilita la persistenza sul listener HTTP. Seleziona il servizio di bilanciamento del carico appena configurato, quindi fai clic sulla scheda **Listener**:
    - Per **HTTP:80**, fai clic su **Visualizza/modifica regole**. Nella pagina **Regole** visualizzata fai clic sull'icona di modifica (una volta nella parte superiore della pagina e quindi di nuovo accanto alla regola) per modificare la regola. Elimina la regola THEN esistente e sostituiscila facendo clic su **Aggiungi azione** > **Inoltra a...**. Nella configurazione THEN risultante specifica lo stesso gruppo di destinazione che hai creato. In Persistenza a livello di gruppo abilita la persistenza e imposta la durata su 1 giorno. Salva l'impostazione, quindi fai clic su **Aggiorna**.

Fase 4. Impostare il timeout di inattività sul sistema di bilanciamento del carico

Nel servizio di bilanciamento del carico aggiorna il timeout di inattività a 400 secondi.

Seleziona il servizio di bilanciamento del carico che hai configurato per questa distribuzione, quindi fai clic su **Azioni** > **Modifica attributi**. Imposta **Timeout di inattività** su `400` secondi, quindi fai clic su **Salva**.

Fase 5. Verificare la connettività di LBS

Apri la pagina del servizio di bilanciamento del carico AWS (**EC2** > **Servizi di bilanciamento del carico**), quindi seleziona l'istanza del servizio di bilanciamento del carico appena configurata.

In **Descrizione** copia il nome DNS e incollalo in un browser per accedere alla pagina di accesso di Tableau Server.

Se viene visualizzato un errore di livello 500, potrebbe essere necessario riavviare i server proxy.

Aggiornare DNS con l'URL pubblico di Tableau

Utilizza il nome della zona DNS del tuo dominio dalla descrizione del servizio di bilanciamento del carico AWS per creare un valore CNAME nel DNS. Il traffico verso il tuo URL (tableau.esempio.com) deve essere inviato al nome DNS pubblico di AWS.

Verificare la connettività

Al termine degli aggiornamenti del DNS, dovresti essere in grado di accedere alla pagina di accesso di Tableau Server inserendo il tuo URL pubblico, ad esempio `http-s://tableau.example.com`.

Esempio di configurazione dell'autenticazione: SAML con IdP esterno

L'esempio seguente descrive come impostare e configurare SAML con l'IdP Okta e il modulo di autenticazione Mellon per una distribuzione di Tableau in esecuzione nell'architettura di riferimento AWS. L'esempio descrive come configurare Tableau Server e i server proxy Apache per l'utilizzo di HTTP. Okta invierà la richiesta al sistema di bilanciamento del carico AWS tramite HTTPS, ma tutto il traffico interno sarà trasmesso tramite HTTP. Durante la configurazione per questo scenario, tieni presente i protocolli HTTP e HTTPS quando imposti le stringhe URL.

Questo esempio utilizza Mellon come modulo del provider di servizi di pre-autenticazione sui server proxy inversi. Questa configurazione garantisce che solo il traffico autenticato si connetta a Tableau Server, che opera anche come provider di servizi con l'IdP Okta. Pertanto, devi configurare due applicazioni IdP: una per il provider di servizi Mellon e una per il provider di servizi Tableau.

Creare l'account amministratore di Tableau

Un errore comune durante la configurazione di SAML è dimenticare di creare un account amministratore su Tableau Server prima di abilitare SSO.

Il primo passaggio consiste nel creare un account su Tableau Server con un ruolo di amministratore del server. Per lo scenario Okta di esempio, il nome utente deve essere in un formato di indirizzo email valido, per esempio, user@example.com. È necessario impostare una password per questo utente, ma la password non verrà utilizzata dopo la configurazione di SAML.

Configurare l'applicazione di pre-autorizzazione Okta

Lo scenario end-to-end descritto in questa sezione richiede due applicazioni Okta:

- Applicazione di pre-autenticazione Okta
- Applicazione Tableau Server Okta

Ognuna di queste applicazioni è associata a diversi metadati, che dovrai configurare rispettivamente sul proxy inverso e su Tableau Server.

Questa procedura descrive come creare e configurare l'applicazione di pre-autenticazione Okta. Più avanti in questo argomento verrà creata l'applicazione Tableau Server Okta. Per un account Okta di prova gratuito con utenti limitati, vedi la pagina Web degli sviluppatori Okta .

Crea un'integrazione dell'app SAML per il provider di servizi di pre-autenticazione Mellon.

1. Apri la dashboard di amministrazione di Okta > **Applicazioni** > **Crea integrazione app**.

2. Nella pagina **Crea una nuova integrazione app** seleziona **SAML 2.0**, quindi fai clic su **Avanti**.

3. Nella scheda **Impostazioni generali** immetti un nome per l'app, ad esempio `Tableau Pre-Auth`, quindi fai clic su **Avanti**.

4. Nella scheda **Configura SAML**:

   - URL Single Sign-On (SSO). L'elemento finale del percorso nell'URL Single Sign-On è indicato come `MellonEndpointPath` nel file di configurazione `mellon.conf` riportato più avanti in questa procedura. Puoi specificare qualsiasi endpoint desideri. In questo esempio, l'endpoint è `sso`. L'ultimo elemento, `postResponse`, è obbligatorio: `https://tableau.example.com/sso/postResponse`.
   - Deseleziona la casella di controllo: **Utilizzalo per URL destinatario e URL di destinazione**.
   - URL destinatario: uguale all'URL SSO, ma con HTTP. Ad esempio, `http://tableau.example.com/sso/postResponse`.
   - URL di destinazione: uguale all'URL SSO, ma con HTTP. Ad esempio, `http://tableau.example.com/sso/postResponse`.
   - URI destinatario (ID entità del provider di servizi). Ad esempio, `https://tableau.example.com`.
   - Formato ID nome: `EmailAddress`
   - Nome utente applicazione: `Email`
   - Dichiarazioni attributi: Nome = `mail`; Formato nome = `Unspecified`; Valore = `user.email`.

   Fai clic su **Avanti**.

5. Nella scheda **Feedback** seleziona:

   - **Sono un cliente Okta che aggiunge un'app interna**
   - **Questa è un'app interna che abbiamo creato**
   - Fai clic su **Fine**.

6. Crea il file di metadati IdP pre-autenticazione:
    - In Okta: **Applicazioni** > **Applicazioni** > La tua nuova applicazione (ad esempio, `Tableau Pre-Auth`) > **Accesso**
    - Accanto a **Certificati di firma SAML**, fai clic su **Visualizza istruzioni di configurazione SAML**.
    - Nella pagina **Come configurare SAML 2.0 per l'applicazione <pre-auth>**, scorri verso il basso fino alla sezione **Facoltativa**, **Fornisci i seguenti metadati IDP al tuo fornitore di servizi**.
    - Copia il contenuto del campo XML e salvalo in un file chiamato `pre-auth_idp_metadata.xml`.
7. (Facoltativo) Configura l'autenticazione a più fattori:
    - In Okta: **Applicazioni** > **Applicazioni** > La tua nuova applicazione (ad esempio, `Tableau Pre-Auth`) > **Accesso**
    - In **Criterio di accesso** fai clic su **Aggiungi regola**.
    - In **Regola di accesso all'app** specifica un nome e le diverse opzioni MFA. Per testare la funzionalità, puoi mantenere tutte le opzioni predefinite. Tuttavia, in **Azioni** devi selezionare **Richiedi fattore** e quindi specificare la frequenza con cui gli utenti devono eseguire l'accesso. Fai **clic** su Salva.

Creare e assegnare un utente Okta

1. In Okta, crea un utente con lo stesso nome utente che hai creato in Tableau (utente@example.com): **Directory** > **Persone** > **Aggiungi persona**.
2. Dopo che l'utente è stato creato, assegna la nuova app Okta a tale persona: fai clic sul nome utente, quindi assegna l'applicazione in **Assegna applicazione**.

Installare Mellon per la pre-autenticazione

1. Nelle istanze EC2 che eseguono il server proxy Apache esegui questi comandi per installare i moduli PHP e Mellon:

    ```
    sudo yum install httpd php mod_auth_mellon
    ```

2. Crea la directory `/etc/httpd/mellon`

Configurare Mellon come modulo di pre-autenticazione

Esegui questa procedura su entrambi i server proxy.

Devi disporre di una copia del file `pre-auth_idp_metadata.xml` che hai creato dalla configurazione di Okta.

1. Cambia directory:

   ```
   cd /etc/httpd/mellon
   ```

2. Crea i metadati del provider di servizi. Esegui lo script `mellon_create_metadata.sh`. Devi includere l'ID entità e l'URL restituito per la tua organizzazione nel comando.

   L'URL restituito è indicato come *URL Single Sign-On* in Okta. L'elemento finale del percorso nell'URL restituito è indicato come `MellonEndpointPath` nel file di configurazione `mellon.conf` riportato più avanti in questa procedura. In questo esempio, specifichiamo `sso` come percorso dell'endpoint.

   Ad esempio:

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

   Lo script restituisce il certificato, la chiave e i file dei metadati del provider di servizi.

3. Rinomina i file del provider di servizi nella directory `mellon` per una maggiore leggibilità. Nella documentazione verrà fatto riferimento a questi file con i seguenti nomi:

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

4. Copia il file `pre-auth_idp_metadata.xml` nella stessa directory.

5. Crea il file `mellon.conf` nella directory `/etc/httpd/conf.d`:

   ```
   sudo nano /etc/httpd/conf.d/mellon.conf
   ```

6. Copia i seguenti contenuti 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. Aggiungi i seguenti contenuti al file `tableau.conf` esistente:

   Nel blocco `<VirtualHost *:80>` aggiungi il seguente contenuto. Aggiorna `ServerName` con il nome host pubblico nel tuo ID entità:

   ```
   DocumentRoot /var/www/html
   ServerName tableau.example.com
   ServerSignature Off
   ErrorLog logs/error_sp.log
   CustomLog logs/access_sp.log combined
   LogLevel info
   ```

   Aggiungi il blocco Location al di fuori del blocco `<VirtualHost *:80>`. Aggiorna `MellonCookieDomain` con il dominio di primo livello per conservare le informazioni sui cookie, nel modo indicato:

   ```
   <Location />
   AuthType Mellon
   MellonEnable auth
   Require valid-user
   ```

```
MellonCookieDomain example.com
</Location>
```

Il file `tableau.conf` completo dovrebbe essere simile a quello nell'esempio seguente:

```
<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. Verifica la configurazione. Esegui questo comando:

```
sudo apachectl configtest
```

Se il test della configurazione restituisce un errore, correggi gli eventuali errori ed esegui nuovamente configtest. Verrà restituito un messaggio che indica che la configurazione è corretta: `Syntax OK`.

9. Riavvia httpd:

```
sudo systemctl restart httpd
```

Creare un'applicazione Tableau Server in Okta

1. Nella dashboard di Okta: **Applicazioni** > **Applicazioni** > **Sfoglia catalogo app**
2. In **Sfoglia catalogo integrazione app** cerca `Tableau`, seleziona il riquadro Tableau Server, quindi fai clic su **Aggiungi**.
3. In **Aggiungi Tableau Server** > **Impostazioni generali** immetti un'etichetta, quindi fai clic su **Avanti**.
4. In Opzioni di accesso, seleziona **SAML 2.0**, quindi scorri verso il basso fino ad Impostazioni di accesso avanzate:
   - **ID entità SAML**: inserisci l'URL pubblico, ad esempio https://tableau.example.com.
   - **Formato nome utente applicazione**: E-mail
5. Fai clic sul collegamento **Metadati del provider di identità** per avviare un browser. Copia il collegamento nel browser. Questo è il collegamento che utilizzerai durante la configurazione di Tableau nella procedura seguente.
6. Fai clic su **Fine**.
7. Assegna la nuova app Okta Tableau Server all'utente (utente@example.com): fai clic sul nome utente, quindi assegna l'applicazione in **Assegna applicazione**.

Abilitare SAML su Tableau Server per l'IdP

Esegui questa procedura su Nodo 1 di Tableau Server.

1. Scarica i metadati dell'applicazione Tableau Server da Okta. Usa il collegamento che hai salvato dalla procedura precedente:

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

2. Copia un certificato TLS e il relativo file chiave in Tableau Server. Il file chiave deve essere una chiave RSA. Per maggiori informazioni sui requisiti del certificato SAML e dell'IdP, consulta *Requisiti SAML* (Linux).

   Per semplificare la gestione e la distribuzione dei certificati e come procedura consigliata per la sicurezza, è consigliabile utilizzare i certificati generati da un'importante e affidabile autorità di certificazione (CA) terza. In alternativa, puoi generare certificati autofirmati o utilizzare i certificati di un'infrastruttura a chiave pubblica per TLS.

   Se non disponi di un certificato TLS, puoi generare un certificato autofirmato utilizzando la procedura incorporata riportata di seguito.

Generare un certificato autofirmato

Esegui questa procedura su Nodo 1 di Tableau Server.

a. Genera la chiave dell'autorità di certificazione (CA) radice di firma:

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

b. Crea il certificato CA radice:

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

   Ti verrà richiesto di inserire i valori per i campi del certificato. Ad esempio:

   ```
   Country Name (2 letter code) [XX]:US
   State or Province Name (full name) []:Washington
   ```

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

c. Crea il certificato e la relativa chiave (`server-saml.csr` e `server-saml.key` nell'esempio seguente). Il nome del soggetto per il certificato deve corrispondere al nome host pubblico dell'host Tableau. Il nome del soggetto è impostato con l'opzione `-subj` con il formato `"/CN=<host-name>"`, ad esempio:

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

d. Firma il nuovo certificato con il certificato CA che hai creato in precedenza. Il seguente comando invia in output anche il certificato nel formato `crt`:

```
openssl x509 -req -in server-saml.csr -days 3650 -CA roo-
tCACert-saml.pem -CAkey rootCAKey-saml.pem -CAcreateserial
-out server-saml.crt
```

e. Converti il file chiave in RSA. Tableau richiede un file chiave RSA per SAML. Per convertire la chiave, esegui questo comando:

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

3. Configura SAML. Esegui questo comando, specificando l'ID dell'entità e l'URL restituito, nonché i percorsi del file dei metadati, del file del certificato e del file chiave:

```
tsm authentication saml configure --idp-entity-id "http-
s://tableau.example.com" --idp-return-url "http-
s://tableau.example.com" --idp-metadata idp_metadata.xml --
```

```
cert-file "server-saml.crt" --key-file "server-saml-rsa.key"

tsm authentication saml enable
```

4. Se la tua organizzazione esegue Tableau Desktop 2021.4 o versione successiva, devi eseguire questo comando per abilitare l'autenticazione tramite i server proxy inversi.

   Le versioni di Tableau Desktop 2021.2.1-2021.3 funzioneranno senza eseguire questo comando, a condizione che il modulo di pre-autenticazione (ad esempio, Mellon) sia configurato in modo da consentire la conservazione dei cookie del dominio di primo livello.

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

5. Applica le modifiche alla configurazione:

   ```
   tsm pending-changes apply
   ```

Convalidare la funzionalità SAML

Per convalidare la funzionalità SAML end-to-end, accedi a Tableau Server con l'URL pubblico (ad esempio, https://tableau.example.com) tramite l'account amministratore di Tableau creato all'inizio di questa procedura.

Risoluzione dei problemi di convalida

Richiesta non valida: un errore comune per questo scenario è l'errore "Richiesta non valida" di Okta. Spesso questo problema si verifica quando il browser memorizza nella cache i dati della sessione precedente di Okta. Ad esempio, se gestisci le applicazioni Okta come amministratore di Okta e quindi tenti di accedere a Tableau con un diverso account abilitato per Okta, i dati della sessione dai dati dell'amministratore potrebbero causare l'errore "Richiesta non valida". Se questo errore persiste anche dopo aver cancellato la cache del browser locale, prova a convalidare lo scenario di Tableau connettendoti con un browser diverso.

Un'altra causa dell'errore "Richiesta non valida" è un errore di battitura in uno dei tanti URL che inserisci durante i processi di configurazione di Okta, Mellon e SAML. Controllali tutti attentamente.

Spesso il file httpd `error.log` nel server Apache specificherà quale URL sta causando l'errore.

Non trovato - L'URL richiesto non è stato trovato su questo server: questo errore indica uno di diversi possibili errori di configurazione.

Se l'utente è autenticato con Okta e riceve questo errore, probabilmente hai caricato l'applicazione di pre-autenticazione Okta in Tableau Server quando hai configurato SAML. Verifica di avere configurato in Tableau Server i metadati dell'applicazione Tableau Server Okta, anziché i metadati dell'applicazione di pre-autenticazione Okta

Altre fasi per la risoluzione dei problemi:

- Esamina attentamente `tableau.conf` per verificare se sono presenti errori di battitura o di configurazione
- Esamina le impostazioni dell'applicazione di pre-autenticazione Okta. Verifica che i protocolli HTTP e HTTPS siano impostati come specificato in questo argomento.
- Riavvia httpd su entrambi i server proxy.
- Verifica che `sudo apachectl configtest` restituisca "Sintassi OK" in entrambi i server proxy.
- Verifica che l'utente di test sia assegnato a entrambe le applicazioni in Okta.
- Verifica che la permanenza sia impostata sul servizio di bilanciamento del carico e sui gruppi di destinazione associati

Configurare SSL/TLS dal servizio di bilanciamento del carico a Tableau Server

Alcune organizzazioni richiedono un canale di crittografia end-to-end dal client al servizio back-end. L'architettura di riferimento predefinita, come descritto fino a questo punto, specifica

SSL dal client al servizio di bilanciamento del carico in esecuzione nel livello Web dell'organizzazione.

Per configurare SSL dal servizio di bilanciamento del carico a Tableau Server, procedi come segue:

- Installa un certificato SSL valido sia in Tableau che nei server proxy.
- Configura SSL dal servizio di bilanciamento del carico ai server proxy inversi.
- Configura SSL dai server proxy a Tableau Server.
- Puoi anche configurare SSL da Tableau Server all'istanza PostgreSQL.

Il resto del presente argomento descrive questa implementazione nel contesto dell'architettura di riferimento AWS di esempio.

Esempio: configurare SSL/TLS nell'architettura di riferimento AWS

Questa sezione descrive come configurare SSL su Tableau e configurare SSL su un server proxy Apache, il tutto in esecuzione nell'architettura di riferimento AWS di esempio.

Le procedure relative a Linux in questo esempio mostrano i comandi per le distribuzioni di tipo RHEL. In particolare, i comandi riportati di seguito sono stati sviluppati con la distribuzione Amazon Linux 2. Se esegui una distribuzione di Ubuntu, modifica i comandi di conseguenza.

Fase 1. Raccogliere i certificati e le relative chiavi

Per semplificare la gestione e la distribuzione dei certificati e come procedura consigliata per la sicurezza, è consigliabile utilizzare i certificati generati da un'importante e affidabile autorità di certificazione (CA) terza.

In alternativa, puoi generare certificati autofirmati o utilizzare i certificati di un'infrastruttura a chiave pubblica per TLS.

La procedura seguente spiega come generare i certificati autofirmati. Se stai utilizzando certificati di terze parti come consigliato, puoi saltare questa procedura.

Esegui questa procedura su uno degli host proxy. Dopo aver generato il certificato e la chiave associata, li condividerai con l'altro host proxy e con Nodo 1 di Tableau Server.

1. Genera la chiave dell'autorità di certificazione (CA) radice di firma:

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

2. Crea il certificato CA radice:

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

   Ti verrà richiesto di inserire i valori per i campi del certificato. Ad esempio:

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

3. Crea il certificato e la relativa chiave (`serverssl.csr` e `serverssl.key` nell'esempio seguente). Il nome del soggetto per il certificato deve corrispondere al nome host pubblico dell'host Tableau. Il nome del soggetto è impostato con l'opzione `-subj` con il formato `"/CN=<host-name>"`, ad esempio:

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

4. Firma il nuovo certificato con il certificato CA che hai creato nella fase 2. Il seguente comando invia in output anche il certificato nel formato `crt`:

```
openssl x509 -req -in serverssl.csr -days 3650 -CA roo-
tCACert.pem -CAkey rootCAKey.pem -CAcreateserial -out ser-
verssl.crt
```

Fase 2. Configurare il server proxy per SSL

Esegui questa procedura su entrambi i server proxy.

1. Installa il modulo SSL di Apache:

   ```
   sudo yum install mod_ssl
   ```

2. Crea la directory `/etc/ssl/private`:

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

3. Copia i file .crt e .key nei percorsi `/etc/ssl/` seguenti:

   ```
   sudo cp serverssl.crt /etc/ssl/certs/

   sudo cp serverssl.key /etc/ssl/private/
   ```

4. Aggiorna il file `tableau.conf` esistente con i seguenti aggiornamenti:

   - Aggiungi il blocco di riscrittura SSL:

     ```
     RewriteEngine on
     RewriteCond %{SERVER_NAME} =tableau.example.com
     RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI}
     [END,NE,R=permanent]
     ```

   - Nel blocco di riscrittura SSL aggiorna il nome del server `RewriteCond`: aggiungi il tuo nome host pubblico, ad esempio `tableau.example.com`
   - Cambia `<VirtualHost *:80>` in `<VirtualHost *:443>`.
   - Racchiudi i blocchi `<VirtualHost *:443>` e `<Location />` con `<IfModule mod_ssl.c>` ... `</IfModule>`.
   - `BalancerMember`: cambia il protocollo da`http` in `https`.

- Aggiungi elementi `SSL*` all'interno del blocco `<VirtualHost *:443>`:

```
SSLEngine on
SSLCertificateFile /etc/ssl/certs/serverssl.crt
SSLCertificateKeyFile /etc/ssl/private/serverssl.key
SSLProxyEngine on
SSLProxyVerify none
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off
```

- Nell'elemento `LogLevel`: aggiungi `ssl:warn`.
- Facoltativo: se hai installato e configurato un modulo di autenticazione, potrebbero essere presenti ulteriori elementi nel file tableau.conf. Ad esempio, il blocco `<Location /> </Location>` includerà elementi.

Un esempio di file tableau.conf configurato per SSL è mostrato di seguito:

```
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. Aggiungi il file index.html per eliminare gli errori 403:

   ```
   sudo touch /var/www/html/index.html
   ```

6. Riavvia httpd:

   ```
   sudo systemctl restart httpd
   ```

Fase 3. Configurare Tableau Server per SSL esterno

Copia i file serverssl.crt e serverssl.key dall'host Proxy 1 al sistema Tableau Server iniziale (Nodo 1).

Esegui questo comando su Nodo 1:

```
tsm security external-ssl enable --cert-file serverssl.crt --key-
file serverssl.key
tsm pending-changes apply
```

Fase 4. Configurare l'autenticazione facoltativa

Se hai configurato un provider di identità esterno per Tableau, probabilmente dovrai aggiornare gli URL restituiti nella dashboard amministrativa dell'IdP.

Ad esempio, se utilizzi un'applicazione di pre-autenticazione Okta, dovrai aggiornare l'applicazione in modo da utilizzare il protocollo HTTPS per l'URL destinatario e l'URL di destinazione.

Fase 5. Configurare il servizio di bilanciamento del carico AWS per HTTPS

Se stai eseguendo la distribuzione con il servizio di bilanciamento del carico AWS come documentato in questa guida, riconfigura il servizio di bilanciamento del carico AWS in modo da inviare il traffico HTTPS ai server proxy:

1. Annulla la registrazione del gruppo di destinazione HTTP esistente:

   In **Gruppi di destinazione** seleziona il gruppo di destinazione HTTP che è stato configurato per il servizio di bilanciamento del carico, fai clic su **Azioni** e quindi su **Registra e annulla la registrazione dell'istanza**.

   Nella pagina **Registra e annulla la registrazione delle destinazioni** seleziona le istanze attualmente configurate, fai clic su **Annulla registrazione** e quindi su **Salva**.

2. Crea il gruppo di destinazione HTTPS:

   Gruppi di destinazione > **Crea gruppo di destinazione**

- Seleziona "Istanze"
- Inserisci un nome per il gruppo di destinazione, ad esempio `TG-internal-HTTPS`
- Seleziona il VPC
- Protocollo: HTTPS 443
- In **Controlli di integrità > Impostazioni avanzate controlli di integrità** > **Codici di riuscita** aggiungi la lista dei codici da leggere:`200,303`.
- Fai clic su **Crea**.

3. Seleziona il gruppo di destinazione appena creato, quindi fai clic sulla scheda **Destinazione**:

    - Fai clic su **Modifica**.
    - Seleziona le istanze EC2 che eseguono l'applicazione proxy, quindi fai clic su **Aggiungi a registrate**.
    - Fai clic su **Salva**.

4. Dopo aver creato il gruppo di destinazione, è necessario abilitare la persistenza:

    - Apri la pagina del gruppo di destinazione AWS (**EC2** > **Bilanciamento del carico** > **Gruppi di destinazione**), quindi seleziona l'istanza del gruppo di destinazione appena configurata. Nel menu **Azione** seleziona **Modifica attributi**.
    - Nella pagina **Modifica attributi** seleziona **Persistenza**, specifica una durata di `1 day`, quindi scegli **Salva modifiche**.

5. Sul servizio di bilanciamento del carico, aggiorna le regole del listener. Seleziona il servizio di bilanciamento del carico che hai configurato per questa distribuzione, quindi fai clic sulla scheda **Listener**.

    - Per **HTTP:80**, fai clic su **Visualizza/modifica regole**. Nella pagina **Regole** visualizzata fai clic sull'icona di modifica (una volta nella parte superiore della pagina e quindi di nuovo accanto alla regola) per modificare la regola. Elimina la regola THEN esistente e sostituiscila facendo clic su **Aggiungi azione** > **Reindirizza a...**. Nella configurazione THEN risultante, specifica `HTTPS` e la porta `443` e mantieni le impostazioni predefinite per le altre opzioni. Salva l'impostazione, quindi fai clic su **Aggiorna**.

- Per **HTTP:443**, fai clic su **Visualizza/modifica regole**. Nella pagina **Regole** visualizzata fai clic sull'icona di modifica (una volta nella parte superiore della pagina e quindi di nuovo accanto alla regola) per modificare la regola. Nella configurazione **THEN**, in **Inoltra a...**, cambia il gruppo di destinazione nel gruppo HTTPS appena creato. In **Persistenza a livello di gruppo** abilita la persistenza e imposta la durata su 1 giorno. Salva l'impostazione, quindi fai clic su **Aggiorna**.

Fase 6. Verificare SSL

Verifica la configurazione visitando https://tableau.example.com.