Tableau Server Enterprise
Guia de Implantação

Ultima atualização 14/11/2024

Conteúdos

Guia de Implantação do Tableau Server Enterprise

O Guia de Implantação Corporativa do Tableau Server (EDG) foi desenvolvido para fornecer orientação prescritiva para a implantação do Tableau Server (local ou na nuvem). O Guia fornece orientação de implantação para cenários corporativos no contexto de uma arquitetura de referência. Testamos a arquitetura de referência para verificar a conformidade com os referenciais de segurança, escala e desempenho, que estão em conformidade com as práticas recomendadas padrão do setor.

Em um alto nível, os principais recursos de uma implantação corporativa padrão de mercado consistem em uma topologia em camadas, em que cada camada de funcionalidade de aplicativo de servidor (nível de gateway da Web, nível de aplicativo e nível de dados) é vinculada e protegida por sub-redes de acesso controlado. Os usuários que acessam o aplicativo de servidor da Internet são autenticados no nível da Web. Depois de autenticada, a solicitação é enviada por proxy para uma sub-rede protegida, onde o nível de aplicativo trata da lógica de negócios. Os dados de alto valor são protegidos pela terceira sub-rede: o nível de dados. Os serviços no nível do aplicativo se comunicam pela rede protegida com o nível de dados para atender às solicitações de dados às fontes de dados de backend.

Nesta implantação, a segurança está na vanguarda de todas as decisões de design e implementação. No entanto, confiabilidade, desempenho e escalabilidade também são requisitos prioritários. Dado o design distribuído e modular da arquitetura de referência, a confiabilidade e a escala de desempenho de uma forma linearmente previsível, colocalizando estrategicamente serviços compatíveis em cada nó e adicionando serviços em pontos de estrangulamento.

Quem deve ler este guia?

O EDG foi desenvolvido para administradores de TI corporativos que podem exigir:

- Uma implantação de Tableau gerenciada por TI
- Aplicação de conformidade do setor
- Melhores práticas de implantação do setor
- Implantação segura por padrão

O EDG é um guia de implementação para a arquitetura de referência corporativa. Embora esta versão do EDG inclua um exemplo de implementação AWS/Linux, o Guia pode ser usado como um recurso por administradores de TI corporativos experientes para implementar a arquitetura de referência prescrita em qualquer ambiente de data center padrão do setor.

Versão

Esta versão do EDG foi desenvolvida especificamente para a versão 2021.2.3 (ou posterior) do Tableau Server. Embora você possa usar o EDG como uma referência geral para implantar versões mais antigas do Tableau Server, recomendamos que você implante a arquitetura de referência com o Tableau Server 2021.2.3 ou posterior. Alguns recursos e opções não estão disponíveis em versões anteriores do Tableau Server.

Para obter os recursos e aprimoramentos mais atualizados, recomendamos a implantação do EDG com o Tableau Server 2022.1.7 e posterior.

A arquitetura de referência descrita neste guia oferece suporte a todos os clientes Tableau a seguir: criação na Web com navegadores compatíveis, Tableau Mobile e Tableau Desktop versão 2021.2.1 ou posterior. Outros clientes do Tableau (Tableau Prep, Bridge etc.) ainda não foram validados com a arquitetura de referência.

Destacar recursos

A primeira versão da arquitetura de referência do Tableau Server apresenta os seguintes cenários e recursos:

- Pré-autenticação do cliente: todos os clientes Tableau (Desktop, Mobile, Criação na Web) são autenticados com o provedor de autenticação corporativa na camada da

Web antes de acessar o Tableau Server interno. Este processo é gerenciado ao configurar um plug-in authN no Tableau Server Independent Gateway agindo como servidor proxy reverso. Consulte Parte 5 - Configuração do nível da Web.

- Implantação zero trust: como todo o tráfego para os Tableau Servers é pré-autenticado, toda a implantação do Tableau opera em uma sub-rede privada que não requer uma conexão confiável.
- Repositório externo: a arquitetura de referência especifica a instalação do repositório do Tableau em um banco de dados PostgreSQL externo, permitindo que os DBAs gerenciem, otimizem, dimensionem e façam backup do repositório como um banco de dados genérico.
- Recuperação inicial do nó: o EDG apresenta um script que automatiza a restauração inicial do nó em caso de falha.
- Backup e restauração baseados em tar: use backups tar conhecidos em marcos estratégicos da implantação do Tableau. No caso de uma falha ou configuração incorreta de implantação, você pode recuperar rapidamente para o estágio de implantação anterior, recuperando o backup tar associado.
- Melhoria de desempenho: a validação do cliente e do laboratório mostra uma melhoria de desempenho de 15-20% ao executar o EDG em comparação com a implantação padrão.

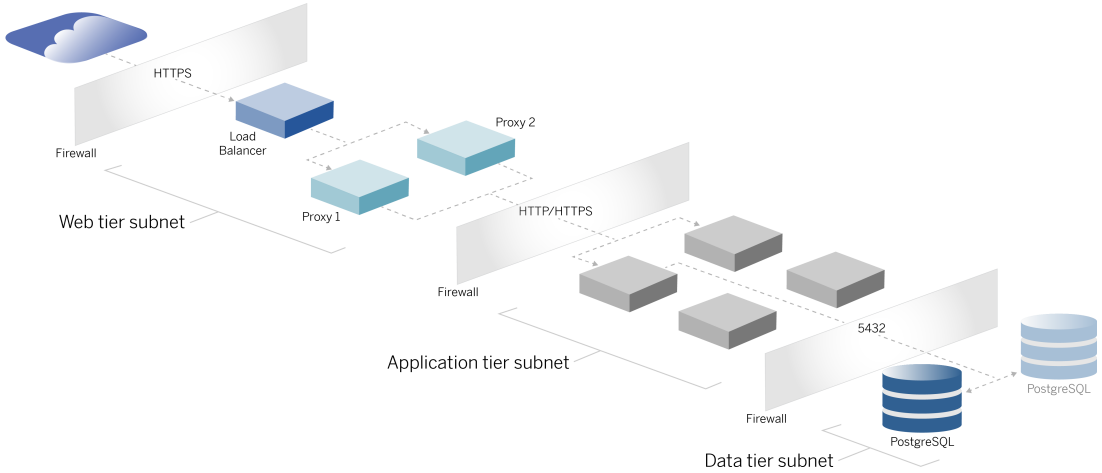
Licenciamento

A arquitetura de referência do Tableau Server prescrita neste Guia requer uma licença do Tableau Advanced Management para habilitar o Repositório Externo do Tableau Server. Você também pode implantar opcionalmente o Armazenamento de arquivos externos do Tableau Server, que também requer a licença do Tableau Advanced Management. Consulte *Sobre o Tableau Advanced Management no Tableau Server* (Linux).

Parte 1 - Compreensão da implantação corporativa

A Parte 1 descreve, com mais detalhes, os recursos e requisitos da implantação corporativa padrão do setor para a qual o Guia de implantação Corporativa do Tableau Server foi desenvolvido.

O diagrama de rede a seguir mostra uma implantação em camadas de data center genérico com a arquitetura de referência do Tableau Server.



Padrões do setor e requisitos de implantação

A seguir estão os recursos de implantações padrão do setor. Estes são os requisitos para os quais a arquitetura de referência foi projetada:

- Um projeto de rede multicamadas: a rede é limitada por sub-redes protegidas para limitar o acesso em cada camada: camada Web, camada de aplicativo e camada de dados. Nenhuma comunicação é capaz de passar pelas sub-redes, pois toda a comunicação é encerrada na próxima sub-rede.

- Portas e protocolos bloqueados por padrão: cada subrede ou grupo de segurança bloqueará todas as portas e protocolos de entrada e saída por padrão. A comunicação é habilitada, em parte, abrindo exceções na configuração da porta ou protocolo.
- Autenticação da Web fora da caixa: as solicitações do usuário da Internet são autenticadas por um módulo de autenticação no proxy reverso no nível da Web. Portanto, todas as solicitações para a camada de aplicativo são autenticadas no nível da Web antes de passar para a camada de aplicativo protegida.
- Independente de plataforma: a solução pode ser implantada com aplicativos de servidor local ou na nuvem.
- Agnóstico de tecnologia: a solução pode ser implantada em um ambiente de máquina virtual ou em contêineres. Também pode ser implantada no Windows ou Linux. No entanto, esta versão inicial da arquitetura de referência e da documentação de suporte foi desenvolvida para Linux em execução na AWS.
- Altamente disponível: todos os componentes do sistema são implantados como um cluster e projetados para operar em uma implantação ativa/ativa ou ativa/passiva
- Funções em silos: cada servidor desempenha uma função discreta. Esse design particiona todos os servidores de forma que o acesso possa ser minimizado para administradores específicos de serviço. Por exemplo, os DBAs gerenciam PostgreSQL para Tableau, os administradores de identidade gerenciam o módulo de autenticação na camada da Web, os administradores de rede e nuvem permitem o tráfego e a conectividade.
- Escalonável linearmente: como funções discretas, você pode escalar cada serviço de nível independentemente de acordo com o perfil de carga.
- Suporte ao cliente: a arquitetura de referência oferece suporte a todos os clientes do Tableau: Tableau Desktop (versões 2021.2 ou posterior), Tableau Mobile e Criação na Web do Tableau.

Medidas de segurança

Conforme declarado, um recurso principal do design de data center padrão da indústria é a segurança.

- Acesso: cada camada é limitada por uma sub-rede que impõe o controle de acesso na camada de rede usando a filtragem da porta. O acesso à comunicação entre sub-redes também pode ser imposto pela camada de aplicativo com serviços autenticados entre os processos.

- Integração: a arquitetura é projetada para se conectar ao provedor de identidade (IdP) no proxy reverso no nível da Web.
- Privacidade: o tráfego no nível da Web é criptografado do cliente com SSL. O tráfego nas sub-redes internas também pode ser criptografado opcionalmente.

Camada de proxy da Web

A camada da Web é uma sub-rede na DMZ (também conhecida como zona de parâmetro) que atua como um buffer de segurança entre a Internet e as sub-redes internas onde os aplicativos são implantados. O nível da Web hospeda servidores proxy reversos que não armazenam informações confidenciais. Os servidores proxy reverso são configurados com um plugin AuthN para pré-autenticar as sessões do cliente com um IdP confiável, antes de redirecionar a solicitação do cliente para o Tableau Server. Para obter mais informações, consulte Pré-autenticação com um módulo AuthN.

Balanceadores de carga

O design de implantação inclui uma solução de balanceamento de carga corporativa na frente dos servidores proxy da Web.

Os balanceadores de carga fornecem melhorias importantes de segurança e desempenho ao

- Virtualizar a URL de front-end para os serviços da nível de Aplicativos.
- Aplicar criptografia SSL
- Descarregar SSL
- Aplicar compactação entre o cliente e os serviços de nível da Web
- Proteger contra ataques DOS
- Fornecer alta disponibilidade

Observação: o Tableau Server versão 2022.1 inclui o Tableau Server Independent Gateway. O Independent Gateway é uma instância autônoma do processo de Gateway do Tableau que funciona como um proxy reverso compatível com o Tableau. No

momento do lançamento, o Independent Gateway foi validado, mas não totalmente testado na arquitetura de referência EDG. Após a conclusão do teste completo, o EDG será atualizado com as orientações prescritivas do Tableau Server Independent Gateway.

Nível de aplicativo

O nível de aplicativo está em uma sub-rede que executa a lógica de negócios principal do aplicativo de servidor. O nível de aplicativo consiste em serviços e processos que são configurados em nós distribuídos em um cluster. O nível de aplicativo só pode ser acessada no nível da Web e não pode ser acessado diretamente pelos usuários.

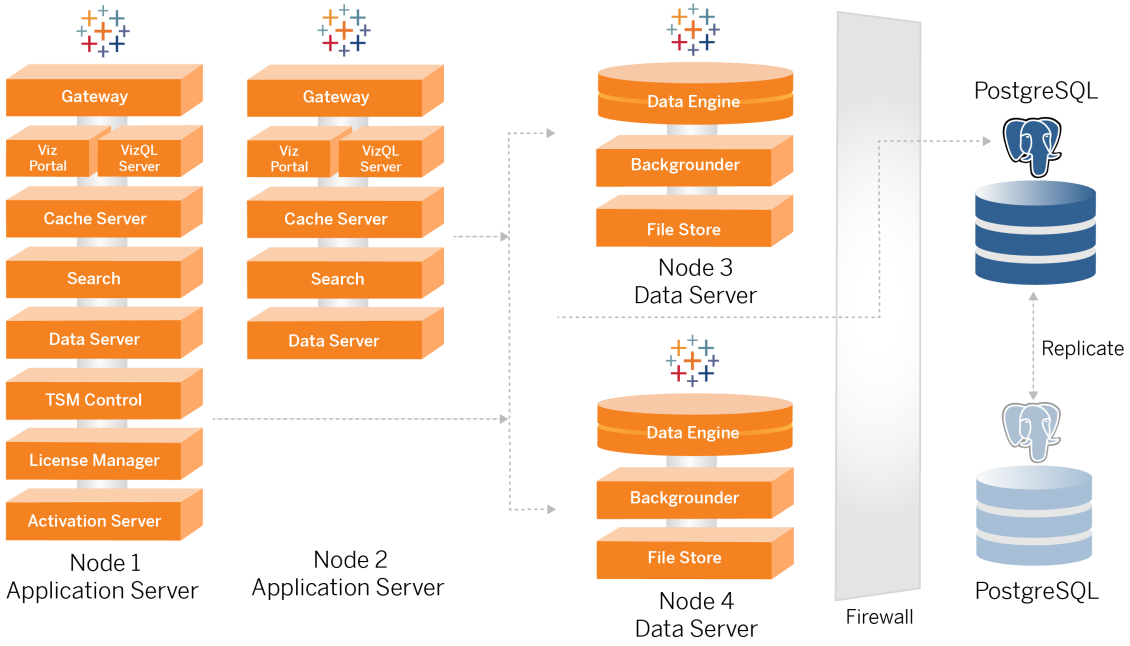
O desempenho e a confiabilidade são aprimorados com a configuração dos processos do aplicativo de forma que os processos com diferentes perfis de uso de recursos (ou seja, uso intensivo de CPU versus uso intensivo de memória) sejam colocados juntos.

Nível de dados

O nível de dados é uma sub-rede que contém dados valiosos. Todo o tráfego para esse nível se origina do nível de aplicativo e, portanto, já está autenticado. Além dos requisitos de acesso na camada de rede com configuração de porta, essa camada deve incluir acesso autenticado e, opcionalmente, o tráfego criptografado com o nível de aplicativo.

Parte 2 - Compreensão da Arquitetura de referência de implantação do Tableau Server

A imagem a seguir mostra os processos relevantes do Tableau Server e como eles são implantados na arquitetura de referência. Essa implantação é considerada a implantação mínima apropriada do Tableau Server para a empresa.



Os diagramas de processo neste tópico destinam-se a mostrar os principais processos de definição de cada nó. Existem muitos processos compatíveis que também são executados nos nós que não são mostrados nos diagramas. Para obter uma lista de todos os processos, consulte a seção de configuração deste guia, Parte 4 - Instalar e configurar o Tableau Server
.

Processos do Tableau Server

A arquitetura de referência do Tableau Server é uma implantação de cluster do Tableau Server de quatro nós com repositório externo no PostgreSQL:

- Nó inicial do Tableau Server (Nó 1): executa os serviços de licenciamento e administrativos TSM necessários que só podem ser executados em um único nó no cluster. No contexto empresarial, o nó inicial do Tableau Server é o nó primário do cluster. Esse nó também executa serviços de aplicativo redundantes com o Nó 2.
- Nós de aplicativo do Tableau Server (Nó 1 e Nó 2): os dois nós atendem às solicitações do cliente, conectam-se e consultam as fontes de dados e os nós de dados.
- Nós de dados do Tableau Server (Nó 3 e Nó 4): dois nós dedicados ao gerenciamento de dados.
- PostgreSQL externo: esse host executa o processo de repositório do Tableau Server. Para implantação de HA, você deve executar um host PostgreSQL adicional para redundância ativa/passiva.

  Você também pode executar o PostgreSQL no Amazon RDS. Para obter mais informações sobre as diferenças entre executar o repositório em RDS e uma instância EC2, consulte *Repositório externo do Tableau Server* (Linux).

  A implantação do Tableau Server com um repositório externo requer uma licença do Tableau Advanced Management.

  Se a sua organização não tiver experiência interna em DBA, você pode, opcionalmente, executar o processo de repositório do Tableau Server na configuração PostgreSQL interna padrão. No cenário padrão, o Repositório é executado em um nó do Tableau com PostgreSQL incorporado. Nesse caso, recomendamos executar o Repositório em um nó dedicado do Tableau e um Repositório passivo em um nó dedicado adicional, para dar suporte ao failover do Repositório. Consulte *Failover do repositório* (Linux).

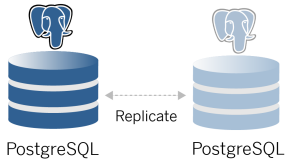
  A título de exemplo, a implementação da AWS descrita neste Guia explica como implantar o repositório externo no PostgreSQL em execução em uma instância EC2.

- Opcional: se sua organização usa armazenamento externo, você pode implantar o Armazenamento de arquivo do Tableau como um serviço externo. Este guia não inclui o armazenamento de arquivo externo no cenário de implantação principal. Consulte *Instalar o Tableau Server com o armazenamento de arquivos externo* (Linux).

  A implantação do Tableau Server com um Armazenamento de arquivo requer uma licença do Tableau Advanced Management.

Repositório PostgresSQL

O Repositório do Tableau Server é um banco de dados que armazena dados do servidor. Estes dados incluem informações sobre usuários, grupos e atribuições de grupo, permissões, projetos, fontes de dados e informações de metadados e atualização de extração do Tableau Server.



A implantação padrão do PostgresSQL consome quase 50% dos recursos de memória do sistema. Com base no uso (para produção e implantações de grande produção), a utilização de recursos pode aumentar. Por esse motivo, recomendamos a execução do processo de Repositório em um computador que não esteja executando nenhum outro componente de servidor que consuma muitos recursos, como VizQL, Processador em segundo plano ou Processador de dados. Executar o processo do Repositório com qualquer um desses componentes criará contenções de ES, restrição de recursos e degradará o desempenho geral da implantação.

Nó 1: nó inicial

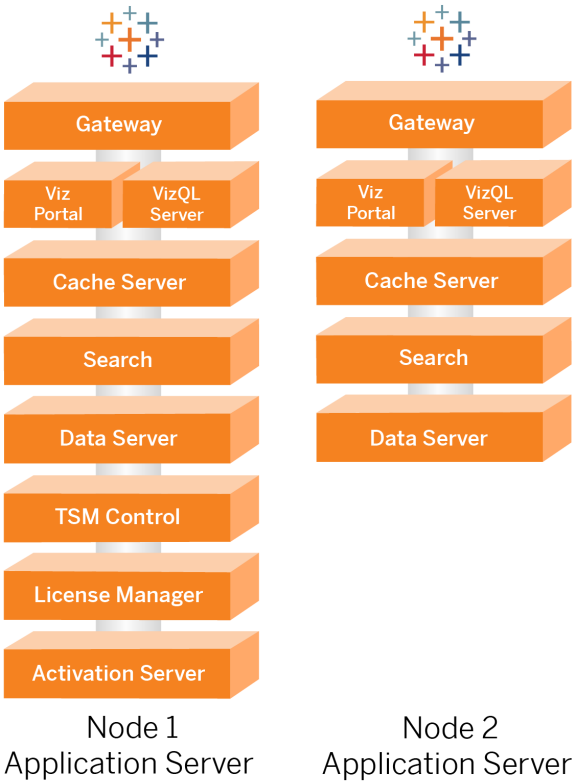
O nó inicial executa um pequeno número de processos importantes e compartilha a carga do aplicativo com o nó 2.

O primeiro computador no qual você instalou o Tableau, o "nó inicial", tem algumas características únicas. Três processos executam apenas no nó inicial e não podem ser movidos para qualquer outro nó exceto em uma situação de falha, o Serviço de Licença (Gerenciador de licenças), o Serviço de Ativação e o Controlador do TSM (Controlador de administração).

Failover do nó 1 e restauração automatizada

Os serviços de Licença, Ativação e Controlador TSM são essenciais para a integridade de uma implantação do Tableau Server. No caso de uma falha do Nó 1, os usuários ainda poderão se conectar à implantação do Tableau Server, pois uma arquitetura de referência configurada corretamente encaminhará as solicitações para o Nó 2. No entanto, sem esses serviços principais, a implantação estará em um estado crítico de falha pendente. Consulte Recuperação automatizada de nó inicial.

Nós 1 e 2: servidores de aplicativos



Os nós 1 e 2 executam os processos do Tableau Server que atendem às solicitações do cliente, consultam fontes de dados, geram visualizações, lidam com conteúdo e administração e outras lógicas comerciais principais do Tableau. Os servidores de aplicativos não armazenam dados do usuário.

Observação: "Servidor de aplicativos" é um termo que também se refere a um processo do Tableau Server listado no TSM. O processo subjacente para "Servidor de aplicativos" é o VizPortal.

Executados em paralelo, o Nó 1 e o Nó 2 são dimensionados para atender às solicitações da lógica de balanceamento de carga executada nos servidores proxy reversos. Como nós redundantes, se um desses nós falhar, as solicitações e serviços do cliente serão tratados pelo nó restante.

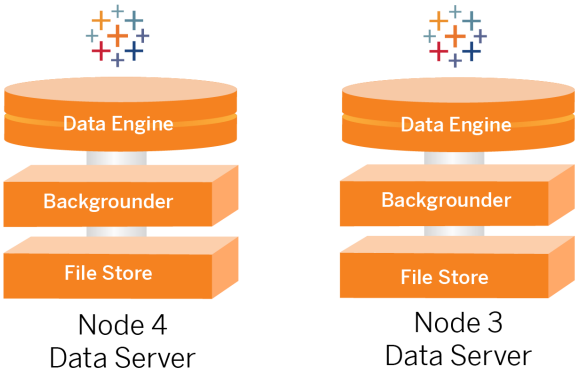
A arquitetura de referência foi projetada para que os processos de aplicativos complementares sejam executados no mesmo computador. Isso significa que os processos não estão competindo por recursos de computação e criando contenção.

Por exemplo, o VizQL, um serviço de processamento central em servidores de aplicativos, é altamente vinculado à CPU e à memória, o VizQL usa quase 60-70% da CPU e da memória do computador. Por esse motivo, a arquitetura de referência é projetada para que nenhum outro processo de vinculado à memória ou à CPU esteja no mesmo nó que o VizQL. O teste mostra que a quantidade de carga ou o número de usuários não afeta a memória ou o uso da CPU nos nós VizQL. Por exemplo, reduzir o número de usuários simultâneos em nosso teste de carga afeta apenas o desempenho do painel ou o processo de carregamento da visualização, mas não reduz a utilização de recursos. Portanto, com base na memória e CPU disponíveis durante o uso de pico, você pode considerar adicionar mais processos VizQL. Como ponto de partida para pastas de trabalho típicas, aloque 4 núcleos por processo VizQL.

Dimensionamento de servidores de aplicativos

A arquitetura de referência é projetada para escala com base em um modelo baseado no uso. Como ponto de partida geral, recomendamos um mínimo de dois servidores de aplicativos, cada um aceitando até 1.000 usuários. Conforme a base de usuários aumenta, planeje adicionar um servidor de aplicativos para cada 1000 usuários adicionais. Monitore o uso e o desempenho para ajustar a base de usuários por host para sua organização.

Nós 3 e 4: servidores de dados



Os processos Armazenamento de arquivos, Processo de dados (Hyper) e Processador em segundo plano estão colocalizados nos nós 3 e 4 pelos seguintes motivos:

- Otimização de extração: a execução de Processador em segundo plano, Hyper e Armazenamento de arquivos no mesmo nó otimiza o desempenho e a confiabilidade. Durante o processo de extração, o Processador em segundo plano consulta o banco de dados de destino, cria o arquivo Hyper no mesmo nó e, em seguida, carrega para o armazenamento de arquivos. Ao colocalizar esses processos no mesmo nó, o fluxo de trabalho de criação da extração não exige a cópia de quantias de dados pela rede ou pelos nós.
- Balanceamento de recursos complementar: o Processador em segundo plano usa principalmente a CPU. O Processador de dados é um processo que consome muita memória. A união desses processos permite a utilização máxima de recursos em cada nó.
- Consolidação de processos de dados: como cada um desses processos são de dados de back-end, faz sentido executá-los no nível de dados mais segura. Em versões futuras da arquitetura de referência, o aplicativo e os servidores de dados serão

executados em níveis separados. No entanto, devido às dependências do aplicativo na arquitetura do Tableau, os servidores de aplicativos e dados devem ser executados no mesmo nível neste momento.

Dimensionamento de servidores de dados

Assim como acontece com os servidores de aplicativos, o planejamento dos recursos necessários para os servidores de dados Tableau requer modelagem baseada no uso. Em geral, suponha que cada servidor de dados possa aceitar até 2.000 trabalhos de atualização de extração por dia. À medida que seus trabalhos de extração aumentam, adicione servidores de dados adicionais sem o serviço de armazenamento de arquivo. Geralmente, a implantação do servidor de dados de dois nós é adequada para implantações que usam o sistema de arquivos local para o serviço de Armazenamento de arquivo. Observe que adicionar mais servidores de aplicativos não afeta o desempenho ou a escala dos servidores de dados de maneira linear. Na verdade, com exceção de alguma sobrecarga de consultas adicionais do usuário, o impacto de adicionar mais hosts de aplicativos e usuários é mínimo.

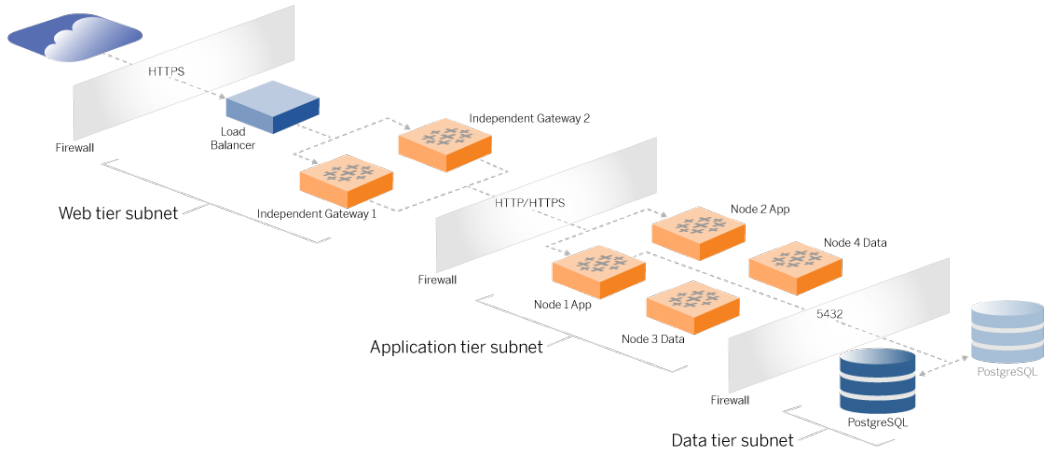
Parte 3 - Preparação para a implantação corporativa do Tableau Server

A Parte 3 descreve os requisitos para preparar sua infraestrutura para implantar a arquitetura de referência do Tableau Server. Antes de começar, recomendamos revisar a Parte 2 - Compreensão da Arquitetura de referência de implantação do Tableau Server .

Além das descrições dos requisitos, este tópico fornece um exemplo de implementação da arquitetura de referência em um ambiente AWS. O restante deste guia baseia-se no exemplo de arquitetura de referência da AWS iniciado neste tópico.

Um princípio básico da arquitetura de referência é a padronização com as melhores práticas de segurança do data center. Especificamente, a arquitetura é projetada para segregar serviços em sub-redes de rede protegidas. A comunicação entre sub-redes é restrita a protocolo específico e tráfego de porta.

O diagrama a seguir ilustra o design da sub-rede da arquitetura de referência para uma implantação local ou na nuvem gerenciada pelo cliente. Para obter um exemplo de implantação de nuvem, consulte a seção abaixo, Exemplo: configurar sub-redes e grupos de segurança na AWS.



Sub-redes

Crie três sub-redes:

- Um nível da Web
- Um nível de aplicativo
- Uma sub-rede de dados.

Regras de grupo de firewall/segurança

As guias abaixo descrevem as regras de firewall para cada nível do datacenter. Para regras de grupo de segurança específicas da AWS, consulte a seção mais adiante neste tópico.

Nível da Web

O nível da Web é uma sub-rede DMZ pública que manipulará as solicitações HTTPS de entrada e fará o proxy das solicitações para o nível do aplicativo. Esse design fornece uma camada de defesa contra malware que pode ser direcionado à sua organização. O nível da Web bloqueia o acesso ao nível de aplicativo/dados.

Tráfego	**Tipo**	**Protocolo**	**Intervalo da porta**	**Fonte**
Entrada	SSH	TCP	22	Sub-rede Bastion (para implantações em nuvem)
Entrada	HTTP	TCP	80	Internet (0.0.0.0/0)
Entrada	HTTPS	TCP	443	Internet (0.0.0.0/0)
Saída	Todo o trá-fego	Todos	Todos	

Nível de aplicativo

A sub-rede de aplicativo é onde reside a implantação do Tableau Server. A sub-rede do aplicativo inclui os servidores de aplicativos Tableau (Nó 1 e Nó 2). Os servidores de aplicativos do Tableau processam as solicitações do usuário para os servidores de dados e executam a lógica comercial principal.

A sub-rede do aplicativo também inclui os servidores de dados Tableau (Nó 3 e Nó 4).

Todo o tráfego do cliente para o nível do aplicativo é autenticado no nível da Web. O acesso administrativo à sub-rede do aplicativo é autenticado e roteado por meio do host Bastion.

Tráfego	**Tipo**	**Protocolo**	**Intervalo da porta**	**Fonte**
Entrada	SSH	TCP	22	Sub-rede Bastion (para implantações em nuvem)
Entrada	HTTPS	TCP	443	Sub-rede de nível da Web
Saída	Todo o tráfego	Todos	Todos	

Nível de dados

A sub-rede dos dados é onde o servidor de banco de dados PostgreSQL externo reside.

Tráfego	**Tipo**	**Protocolo**	**Intervalo da porta**	**Fonte**
Entrada	SSH	TCP	22	Sub-rede Bastion (para implantações em

				nuvem)
Entrada	PostgreSQL	TCP	5432	Sub-rede de nível de aplicativo
Saída	Todo o tráfego	Todos	Todos	

Bastion

A maioria das equipes de segurança corporativa não permite a comunicação direta do sistema administrativo local com os nós implantados na nuvem. Em vez disso, todo o tráfego SSH administrativo para os nós da nuvem é encaminhado por proxy por meio de um host bastion (também conhecido como "servidor de salto"). Para implantações na nuvem, recomendamos a conexão de proxy do host Bastion para todos os recursos na arquitetura de referência. Esta é uma configuração opcional para ambientes locais.

O host Bastion autentica o acesso administrativo e só permite o tráfego por meio do protocolo SSH.

Tráfego	**Tipo**	**Protocolo**	**Intervalo da porta**	**Fonte**	**Destino**
Entrada	SSH	TCP	22	Endereço IP do computador do administrador	
Saída	SSH	TCP	22		Sub-rede de nível da Web
Saída	SSH	TCP	22		Sub-rede de nível de aplicativo

Exemplo: configurar sub-redes e grupos de segurança na AWS

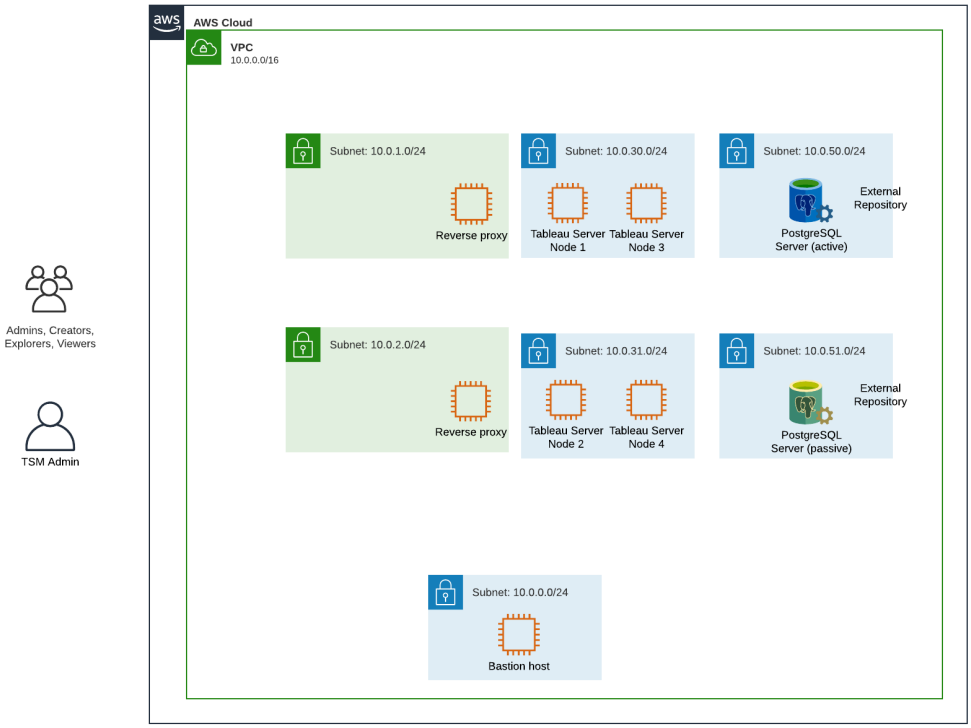
Esta seção fornece procedimentos passo a passo para criar e configurar o ambiente de VPC e rede para a implantação da arquitetura de referência do Tableau Server na AWS.

Os slides abaixo mostram a arquitetura de referência em quatro camadas. Conforme você avança nos slides, os elementos componentes são colocados em camadas no mapa de topologia:

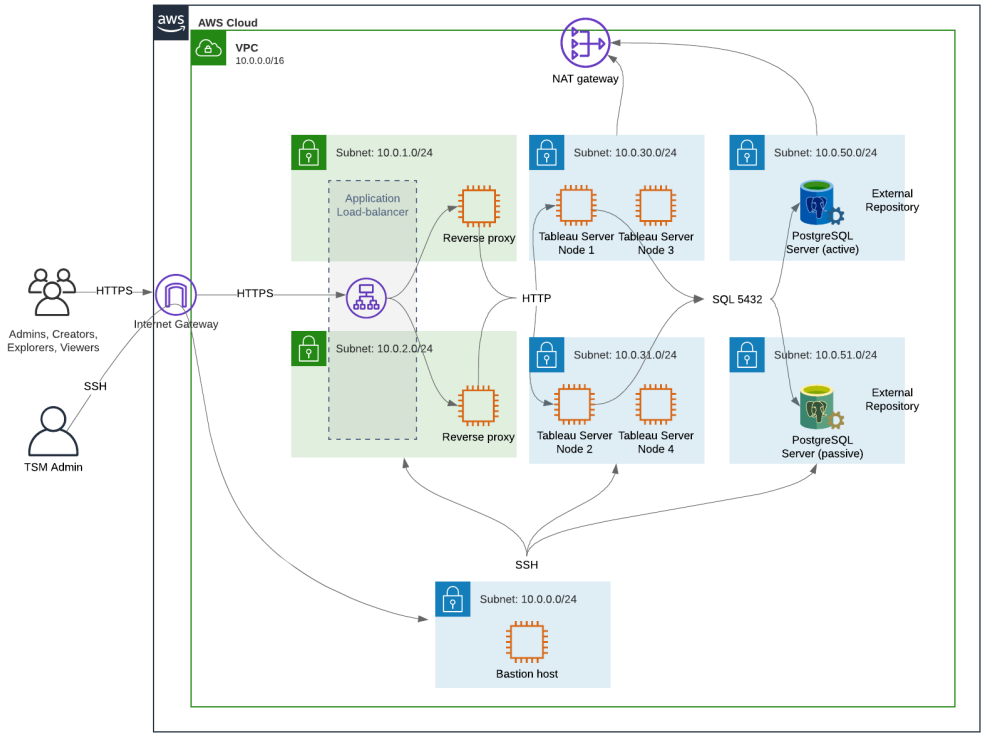
1. Topologia de sub-rede VPC e instâncias EC2: um host bastião, dois servidores proxy reversos, quatro servidores Tableau e pelo menos um servidor PostgreSQL.
2. Fluxo de protocolo e conectividade com a Internet. Todo o tráfego de entrada é gerenciado por meio do gateway de Internet AWS. O tráfego para a Internet é roteado por meio do NAT.
3. Zonas de disponibilidade. Os hosts proxy, Tableau Server e PostgreSQL são implantados uniformemente em duas zonas de disponibilidade.
4. Grupos de segurança. Quatro grupos de segurança (Público, Privado, Dados e Bastion) protegem cada camada no nível do protocolo.

Arquitetura de referência da AWS

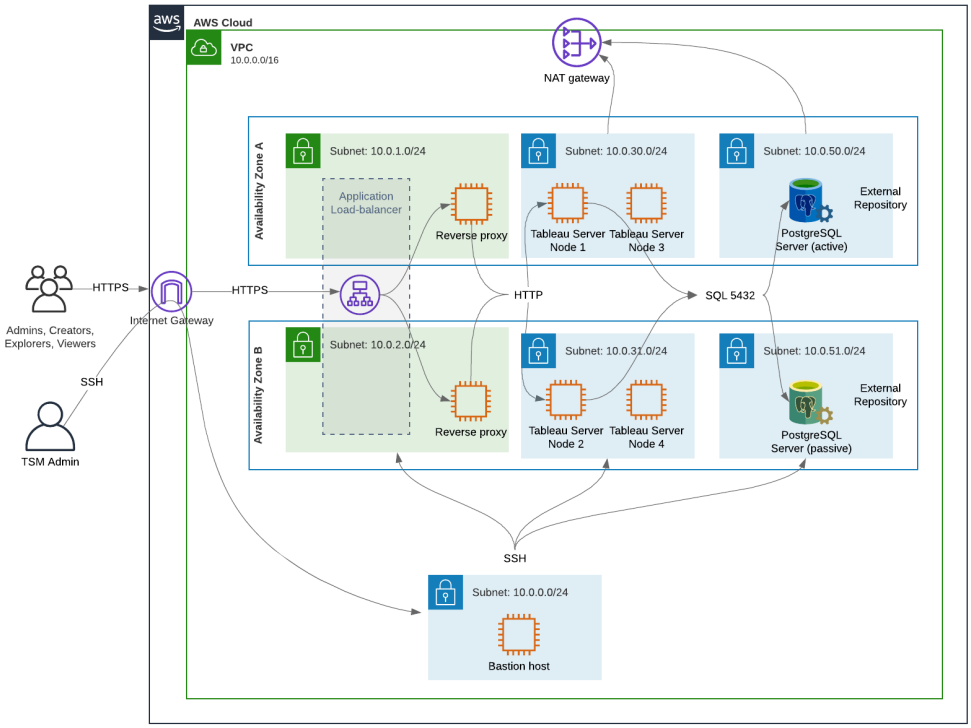
Slide 1: topologia de sub-rede VPC e instâncias EC2



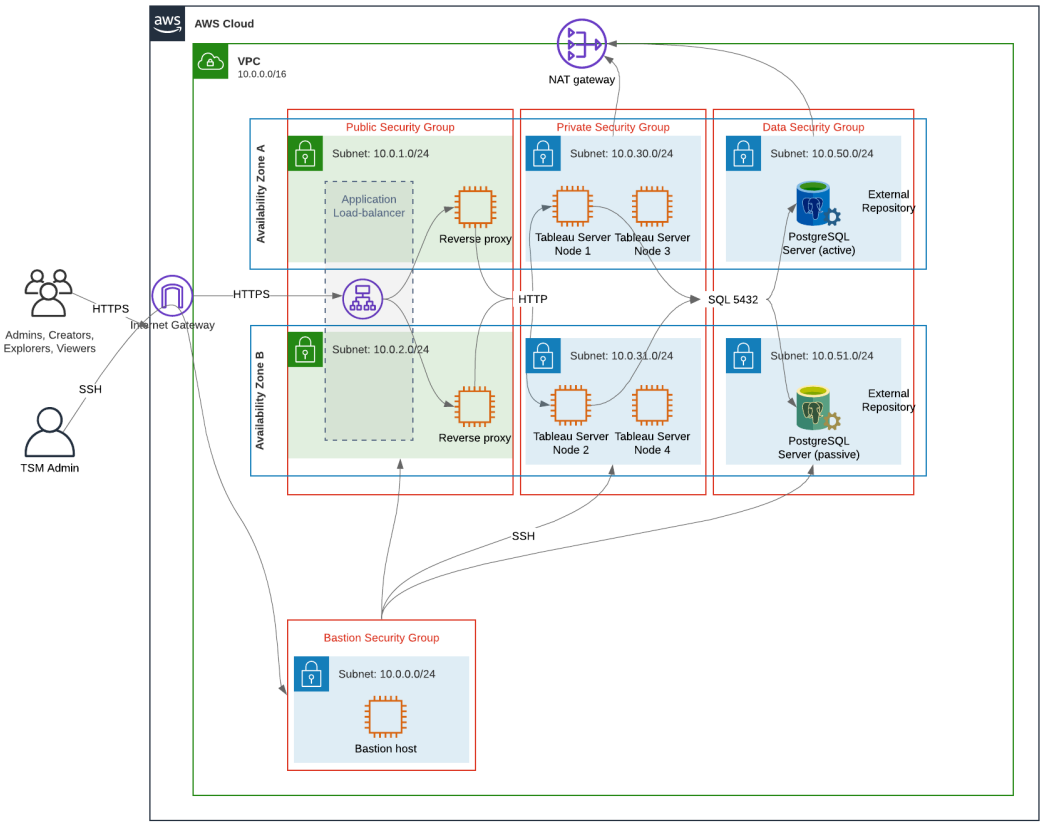
Slide 2: fluxo de protocolo e conectividade



Slide 3: zonas de disponibilidade



Slide 4: grupos de segurança



Zonas de disponibilidade da AWS e alta disponibilidade

A arquitetura de referência conforme apresentada neste Guia especifica uma implantação que fornece disponibilidade por meio de redundância quando um único host falha. No entanto, no caso da AWS em que a arquitetura de referência é implantada em duas zonas de disponibilidade, a disponibilidade é comprometida no caso muito raro em que uma zona de disponibilidade falha.

Configuração VPC

Esta seção descreve como:

- Instalar e configurar a VPC
- Configurar a conectividade à Internet
- Configurar sub-redes
- Criar e configurar grupos de segurança

Configurar a VPC

O procedimento nesta seção é mapeado para a interface do usuário na experiência VPC "clássica". Você pode alternar a IU para exibir a visualização clássica desativando a Nova experiência de VPC no canto superior esquerdo do Painel VPC da AWS.

Execute o assistente da VPC para criar sub-redes privadas e públicas padrão e roteamento e ACL de rede padrão.

1. Antes de configurar um VPC, você deve criar um IP elástico. Crie uma alocação usando todos os padrões.
2. Execute o assistente de VPC > "VPC com sub-redes públicas e privadas"
3. Aceite a maioria dos padrões. Exceto pelo seguinte:
    - Insira um nome de VPC.
    - Especifique a ID de alocação do IP elástico.
    - Especifique as seguintes máscaras CIDR:
        - CIDR IPv4 da sub-rede pública: 10.0.1.0/24, renomeie esta sub-rede como `Public-a`.
        - CIDR IPv4 da sub-rede privada: 10.0.30.0/24, renomeie esta sub-rede como `Private-a`.
    - Zona de disponibilidade: para ambas sub-redes, selecione **a** opção para a região em que você está.

      Observação: para este exemplo, podemos utilizar **a** e **b** para distinguir entre Zonas de disponibilidade em um determinado datacenter AWS. Na AWS, os nomes da zona de disponibilidade podem não corresponder aos exemplos mostrados aqui. Por exemplo, algumas zonas de disponibilidade incluem zonas **c** e **d** em um datacenter.

4. Clique em **Criar VPC**.
5. Depois que o VPC for criado, crie as sub-redes `Public-b` `Private-b`,`Data` e `Bastion`. Para criar uma sub-rede, clique em **Sub-redes** > **Criar sub-rede** .

    - `Public-b`: para a zona de disponibilidade, selecione a opção **b** para a região em que você está. Bloco CIDR: 10.0.2.0/24
    - `Private-b`: para a zona de disponibilidade, selecione a opção **b** para a região em que você está. Bloco CIDR: 10.0.31.0/24
    - `Data`: para a zona de disponibilidade, selecione a zona **a** para a região em que você está. Bloco CIDR: 10.0.50.0/24 Opcional: se você planeja replicar o banco de dados externo em um cluster PostgreSQL, crie uma sub-rede Data-b na Zona de disponibilizade b com um bloco CIDR de 10.0.51.0/24.
    - `Bastion`: para a zona de disponibilidade, selecione uma das zonas. Bloco CIDR: 10.0.0.0/24
6. Depois que as sub-redes forem criadas, edite as tabelas de rota nas sub-redes Pública e Bastion para usar a tabela de rota configurada para o gateway de Internet associado (IGW). E edite as sub-redes Privada e de Dados para usar a tabela de rotas configurada para o conversor de endereço de rede (NAT).
    - Para determinar qual tabela de rota está configurada com o IGW ou o NAT, clique em **Rotear tabelas** no painel AWS. Clique em um dos dois links da tabela de rota para abrir a página de propriedades. Observe o valor de Destino em **Rotas** > **Destino** > **0.0.0.0/0**. O valor de Destino diferencia o tipo de rota e começará com o fragmento `igw-` ou `nat-`.
    - Para atualizar as tabelas de rota, **VPC** > **Sub-redes** > [subnet_name]> **Tabela de rota** > **Editar associação da tabela de rota**.

Configurar grupos de segurança

O assistente VPC cria um único grupo de segurança que você não usará. Crie os seguintes grupos de segurança (**Grupos de segurança** > **Criar grupo de segurança**). Os hosts EC2 serão instalados nesses grupos em duas zonas de disponibilidade, conforme mostrado no diagrama deslizante acima.

- Crie um novo grupo de segurança: **Privado**. Nesse local todos os quatro nós do Tableau Server serão instalados. Posteriormente, no processo de instalação, o grupo de segurança Privado será associado às sub-redes 10.0.30.0/24 e 10.0.31.0/24.

- Crie um novo grupo de segurança: **Público** . É aqui que os servidores proxy serão instalados. Posteriormente, no processo de instalação, o grupo de segurança Público será associado às sub-redes 10.0.1.0/24 e 10.0.2.0/24.
- Crie um novo grupo de segurança: **Dados**. É aqui que o repositório externo do Tableau PostgreSQL será instalado. Posteriormente, no processo de instalação, o grupo de segurança Dados será associado à sub-rede 10.0.50.0/24 (e, opcionalmente, 10.0.51.0/24).
- Crie um novo grupo de segurança: **Bastion**. É aqui que você instalará o host Bastion. Posteriormente, no processo de instalação, o grupo de segurança Bastion será associado à sub-rede 10.0.0.0/24.

Especifique as regras de entrada e saída

Na AWS, os grupos de segurança são análogos aos firewalls em um ambiente local. Você deve especificar o tipo de tráfego (por exemplo, https, https etc), protocolo (TCP ou UDP) e portas ou intervalo de portas (por exemplo, 80, 443, etc) que têm permissão para entrar e/ou sair do grupo de segurança. Para cada protocolo, você também deve especificar o destino ou o tráfego de origem.

Regras do grupo de segurança público

Regras de entrada			
Tipo	**Protocolo**	**Intervalo da porta**	**Fonte**
HTTP	TCP	80	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0
SSH	TCP	22	Grupo de segurança Bastion

Regras de saída			
Tipo	**Protocolo**	**Intervalo da porta**	**Destino**

Todo o tráfego	Todos	Todos	0.0.0.0/0

Regras de grupo de segurança privado

O grupo de segurança privada inclui uma regra de entrada para permitir o tráfego HTTP do grupo de segurança pública. Permita o tráfego HTTP apenas durante o processo de implantação, para verificar a conectividade. Recomendamos remover a regra de entrada HTTP, após terminar de implantar o proxy reverso e configurar SSL para Tableau.

Regras de entrada			
Tipo	**Protocolo**	**Intervalo da porta**	**Fonte**
HTTP	TCP	80	Grupo de segurança Público
HTTPS	TCP	443	Grupo de segurança Público
PostgreSQL	TCP	5432	Grupo de segurança Dados
SSH	TCP	22	Grupo de segurança Bastion
Todo o tráfego	Todos	Todos	Grupo de segurança Privado

Regra de saída			
Tipo	**Protocolo**	**Intervalo da porta**	**Destino**
Todo o tráfego	Todos	Todos	0.0.0.0/0
PostgreSQL	TCP	5432	Grupo de segurança Dados
SSH	TCP	22	Grupo de segurança Bastion

Regras de grupo de segurança Dados

Regras de entrada			
Tipo	**Protocolo**	**Intervalo da porta**	**Fonte**
PostgreSQL	TCP	5432	Grupo de segurança Privado
SSH	TCP	22	Grupo de segurança Bastion

Regras de saída			
Tipo	**Protocolo**	**Intervalo da porta**	**Destino**
Todo o tráfego	Todos	Todos	0.0.0.0/0
PostgreSQL	TCP	5432	Grupo de segurança Privado
SSH	TCP	22	Grupo de segurança Bastion

Regras de grupo de segurança de host Bastion

Regras de entrada			
Tipo	**Protocolo**	**Intervalo da porta**	**Fonte**
SSH	TCP	22	O endereço IP e a máscara de rede do computador que você usará para fazer login na AWS (computador administrador).
SSH	TCP	22	Grupo de segurança Privado
SSH	TCP	22	Grupo de segurança Público

Regras de saída			
Tipo	**Protocolo**	**Intervalo da porta**	**Destino**
SSH	TCP	22	O endereço IP e a máscara de rede do computador que você usará para fazer login na AWS (computador administrador).
SSH	TCP	22	Grupo de segurança Privado
SSH	TCP	22	Grupo de segurança Público
SSH	TCP	22	Grupo de segurança Dados
HTTPS	TCP	443	0.0.0.0/0 (Opcional: crie esta regra se você precisar acessar a Internet para baixar o software de suporte no host Bastion)

Habilitar atribuição automática de IP público

Fornece um endereço IP para conexão com o host dos servidores proxy e Bastion.

Para sub-redes Public e Bastion:

1. Selecione a sub-rede
2. No menu **Ações**, selecione "Modificar configurações de atribuição automática de IP".
3. Clique em "Ativar a atribuição automática de endereços IPv4 públicos".
4. Clique em **Salvar**.

Balanceador de carga

Observação: se você estiver instalando na AWS e seguindo o exemplo de implantação neste guia, deverá instalar e configurar o balanceador de carga da AWS posteriormente

no processo de implantação, conforme descrito na Parte 5 - Configuração do nível da Web.

Para implantações locais, trabalhe com seus administradores de rede para implantar balanceadores de carga para oferecer suporte à camada da Web da arquitetura de referência:

- Um balanceador de carga de aplicativo voltado para a Web que aceita solicitações HTTPS de clientes Tableau e se comunica com os servidores proxy reverso.
- Proxy reverso:
  - Recomendamos um mínimo de dois servidores proxy para redundância e para lidar com a carga do cliente.
  - Recebe tráfego HTTPS do balanceador de carga.
  - Compatível com sessão fixa para o host do Tableau
  - Configure o proxy para balanceamento de carga round robin para cada Tableau Server executando o processo de Gateway.
  - Lida com solicitações de autenticação de IdP externo.
- Proxy de encaminhamento: o Tableau Server requer acesso à Internet para licenciamento e funcionalidade de mapa. Dependendo do seu ambiente de proxy de encaminhamento, você pode precisar configurar listas seguras de proxy de encaminhamento para URLs de serviço do Tableau. Consulte *Comunicação com a Internet* (Linux).

Configurar computadores host

Hardware mínimo recomendado

As recomendações a seguir são baseadas em nossos testes de dados do mundo real na arquitetura de referência.

Servidores de aplicativos:

- CPU: 8 núcleos físicos (16vCPUs),
- RAM: 128 GB (16 GB/núcleo físico)
- Espaço em disco: 100 GB

Servidores de dados

- CPU: 8 núcleos físicos (16vCPUs),
- RAM: 128 GB (16 GB/núcleo físico)
- Espaço em disco: 1 TB. Se sua implantação usará armazenamento externo para o Armazenamento de Arquivo do Tableau, você precisará calcular o espaço em disco apropriado. Consulte *Instalar o Tableau Server com o armazenamento de arquivos externo* (Linux).

Servidores proxy

- CPU: 2 núcleos físicos (4vCPUs),
- RAM: 8 GB (4 GB/núcleo físico)
- Espaço em disco: 100 GB

Banco de dados de repositório externo

- CPU: 8 núcleos físicos (16vCPUs),
- RAM: 128 GB (16 GB/núcleo físico)
- O requisito de espaço em disco depende da carga de dados e de como isso afetará o backup. Consulte a seção *Processos de backup e restauração*, no tópico *Requisitos de espaço em disco* (Linux).

Estrutura de diretório

A arquitetura de referência recomenda instalar o pacote do Tableau Server e os dados em locais não padrão:

- Instale o pacote em: `/app/tableau_server`: crie esse caminho de diretório antes de instalar o pacote do Tableau Server e, a seguir, especifique o caminho durante a instalação.
- Instale os dados do Tableau para:`/data/tableau_data` . Não crie esse diretório antes de instalar o Tableau Server. Em vez disso, você deve especificar o caminho durante a instalação e, em seguida, a instalação do Tableau criará e concederá permissão ao caminho de forma adequada.

Consulte Execute o pacote de instalação e inicialize o TSM para obter detalhes de implementação.

Exemplo: instalar e preparar computadores host na AWS

Esta seção explica como instalar hosts EC2 para cada tipo de servidor na arquitetura de referência do Tableau Server.

A arquitetura de referência requer oito hosts:

- Quatro instâncias para Tableau Server.
- Duas instâncias para servidores proxy (Apache).
- Um exemplo para host Bastion.
- Uma ou duas instâncias de banco de dados EC2 PostgreSQL

Detalhes da instância de host

Instale os computadores host de acordo com os detalhes abaixo.

Tableau Server

- Amazon Linux 2
- Tipo de instância: m5a.8xlarge
- ID do grupo de segurança: Privado
- Armazenamento: tipo de volume EBS, 150 GiB, gp2 Se sua implantação usará armazenamento externo para o Armazenamento de Arquivo do Tableau, você precisará calcular o espaço em disco apropriado. Consulte *Instalar o Tableau Server com o armazenamento de arquivos externo* (Linux).
- Rede: instale dois hosts EC2 em cada sub-rede privada (10.0.30.0/24 e 10.0.31.0/24).
- Copie a última versão de manutenção do pacote rpm do Tableau Server 2021.2 (ou posterior) da página de downloads do Tableau para cada host do Tableau.

Host Bastion

- Amazon Linux 2
- Tipo de instância: t3.micro
- ID do grupo de segurança: Bastion

- Armazenamento: tipo de volume EBS, 50 GiB, gp2
- Rede: sub-rede Bastion 10.0.0.0/24

Tableau Server Independent Gateway

- Amazon Linux 2
- Tipo de instância: t3.xlarge
- ID do grupo de segurança: Público
- Armazenamento: tipo de volume EBS, 100 GiB, gp2
- Rede: instale uma instância EC2 em cada sub-rede pública (10.0.1.0/24 e 10.0.2.0/24)

Host PostgreSQL EC2

- Amazon Linux 2
- Tipo de instância: r5.4xlarge
- ID do grupo de segurança: Dados
- Armazenamento: o requisito de espaço em disco depende da carga de dados e de como isso afetará o backup. Consulte a seção *Processos de backup e restauração*, no tópico *Requisitos de espaço em disco* (Linux).
- Rede: sub-rede de dados 10.0.50.0/24. (Se você estiver replicando PostgreSQL em um cluster HA, instale o segundo host na sub-rede 10.0.51.0/24)

Verificação: conectividade de VPC

Depois de instalar os computadores host, verifique a configuração da rede. Verifique a conectividade entre os hosts conectando-se com o SSH do host no grupo de segurança Bastion aos hosts em cada sub-rede.

Exemplo: conecte-se ao host Bastion na AWS

1. Configure seu computador administrativo para o agente ssh. Isso permite que você se conecte a hosts na AWS, sem colocar o arquivo de chave privada em nenhuma instância do EC2.

   Para configurar o ssh-agent em um Mac, execute o seguinte comando:

`ssh-add -K myPrivateKey.pem` ou para o Mac OS mais recente, `ssh-add --apple-use-keychain myPrivateKey.pem`

Para Windows, consulte o tópico Conectar-se com segurança a instâncias do Linux em execução em uma VPC da Amazon privada .

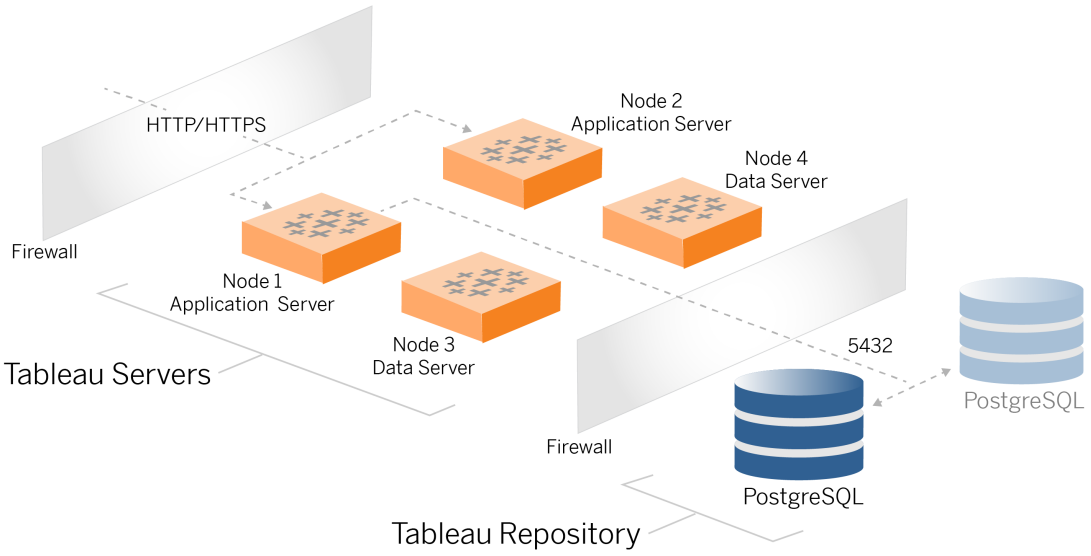
2. Conecte-se ao host Bastion executando o seguinte comando:

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

3. Em seguida, você pode se conectar a outros hosts na VPC do host Bastion, usando o endereço IP privado, por exemplo:

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

Parte 4 - Instalar e configurar o Tableau Server



Este tópico descreve como terminar de instalar e configurar a implantação de linha de base do Tableau Server. O procedimento aqui continua com o exemplo de arquitetura de referência AWS e Linux.

Os exemplos do Linux em todos os procedimentos de instalação mostram comandos para distribuições do tipo RHEL. Especificamente, os comandos aqui foram desenvolvidos com a distribuição Amazon Linux 2. Se você estiver executando a distribuição do Ubuntu, edite os comandos de forma apropriada.

Antes de começar

Você deve preparar e validar seu ambiente conforme descrito na Parte 3 - Preparação para a implantação corporativa do Tableau Server.

Instalar, configurar e PostgreSQL de tar

Esta instância PostgreSQL hospeda o repositório externo para a implantação do Tableau Server. Você deve instalar e configurar o PostgreSQL antes de instalar o Tableau.

Você pode executar o PostgreSQL no Amazon RDS ou em uma instância EC2. Para obter mais informações sobre as diferenças entre executar o repositório em RDS e uma instância EC2, consulte *Repositório externo do Tableau Server* (Linux).

Como exemplo, o procedimento abaixo mostra como instalar e configurar o Postgres em uma instância do Amazon EC2. O exemplo mostrado aqui é uma instalação e configuração genérica para PostgreSQL na arquitetura de referência. Seu DBA deve otimizar a implantação do PostgreSQL com base no tamanho de seus dados e necessidades de desempenho.

Requisitos: observe que você deve estar executando o PostgreSQL 1.6 e deve instalar o módulo uuid-ossp.

Versão PostgreSQL

Você deve instalar versões principais compatíveis do PostgreSQL para o repositório externo do Tableau Server. Além disso, as versões secundárias também devem atender aos requisitos mínimos.

Versões do Tableau Server	**Versões mínimas compatíveis com 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 - 2022.3.11 2023.1.5 - 2023.1.7 2023.3.0 - 2023.3.3	13.11
2024.0 - 2024.x	15.6

Instalar o PostgreSQL

Este procedimento de instalação de exemplo descreve como instalar o PostgreSQL versão 13.6.

Conecte-se ao host EC2 que você criou na parte anterior.

1. Execute a atualização para aplicar as correções mais recentes ao sistema operacional Linux:

   ```
   sudo yum update
   ```

2. Crie e edite o arquivo, pgdg.repo. no caminho `/etc/yum.repos.d/`. Preencha o arquivo com as seguintes informações de configuração:

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

3. Instale o Postgres 13.6:

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

4. Instale o módulo uuid-ossp:

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

5. Inicialize o Postgres:

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

Configurar o PostgreSQL

Conclua a instalação básica configurando o Postgres:

1. Atualize o arquivo de configuração pg_hba,`/var/lib/pgsql/13/data/pg_hba.conf`, com as duas entradas a seguir. Cada entrada deve incluir a máscara das sub-redes em que seus Tableau Servers serão executados:

   ```
   host all all 10.0.30.0/24 password

   host all all 10.0.31.0/24 password
   ```

2. Atualize o arquivo PostgreSQl,`/var/lib/pgsql/13/data/postgresql.conf`, adicionando esta linha:

   ```
   listen_addresses = '*'
   ```

3. Configure para iniciar o Postgres na reinicialização:

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

4. Definir senha de superusuário:

   ```
   sudo su - postgres

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

   > **Observação**: defina uma senha forte. Não use `'StrongPassword'` como mostrado no exemplo aqui.

   ```
   exit
   ```

5. Reinicie o Postgres:

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

Faça backup do tar PostgreSQL da etapa 1

Crie um backup tar da configuração do PostgreSQL. A criação de um instantâneo tar da configuração atual economizará tempo, se você encontrar falhas ao continuar a implantação.

Faremos referência a isso como o backup da "Etapa 1".

No host PostgreSQL:

1. Pare a instância do banco de dados Postgres:

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

2. Execute o comando a seguir para criar o backup tar:

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

3. Inicie o banco de dados Postgres:

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

Restaurar a Etapa 1

Restaure para a Etapa 1, se o nó inicial do Tableau Server falhar durante a instalação.

1. Nos computadores que executam o Tableau, execute o script obliterate para remover completamente o Tableau Server do host:

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

2. Restaure o tar da Etapa 1 do PostgreSQL. No computador do Postgres, execute os comandos a seguir:

   ```
   sudo su
   systemctl stop postgresql-13
   cd /var/lib/pgsql
   ```

```
tar  -xvf step1.13.bkp.tar

systemctl start postgresql-13

exit
```

Retome o processo de instalação do nó inicial do Tableau Server.

Antes da instalação

Se você estiver implantando o Tableau de acordo com o exemplo de implementação AWS/Linux descrito neste Guia, poderá executar o script de instalação automatizado, TabDeploy4EDG. O script TabDeploy4EDG automatiza a instalação de exemplo da implantação do Tableau de quatro nós descrita nos procedimentos a seguir. Consulte o Apêndice - Caixa de ferramentas de implantação da AWS.

Instalação no nó inicial do Tableau Server

Este procedimento descreve como instalar o nó inicial do Tableau Server, conforme definido pela arquitetura de referência. Com exceção da instalação do pacote e da inicialização do TSM, o procedimento aqui usa a linha de comando do TSM sempre que possível. Além de não precisar de plataforma, o uso da CLI do TSM permite uma instalação mais perfeita em ambientes virtualizados e sem periféricos.

Execute o pacote de instalação e inicialize o TSM

Faça login no servidor host do Nó 1.

1. Execute a atualização para aplicar as correções mais recentes ao sistema operacional Linux:

   ```
   sudo yum update
   ```

2. Copie o pacote de instalação da página Downloads do Tableau para o computador host que executará o Tableau Server.

Por exemplo, em um computador executando o sistema operacional semelhante ao Linux RHEL, execute:

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

em que `<version>` é o número da versão.

3. Baixe e instale dependências:

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

4. Crie o caminho `/app/tableau_server` no diretório raiz:

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

5. Execute o programa de instalação e especifique o caminho de instalação `/app/-tableau_server`. Por exemplo, em um sistema operacional semelhante ao Linux RHEL, execute:

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

6. Mudar para o diretório `/app/tableau_server/packages/scripts.<version_code>/` e execute o script `initialize-tsm` localizado lá:

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

7. Após a conclusão da inicialização, saia o shell:

```
exit
```

Ativar e registrar o Tableau Server

1. Faça login no servidor host do Nó 1.
2. Forneça as chaves de produto do Tableau Server nesta etapa. Execute o seguinte comando para cada chave de licença que você comprou:

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

3. Crie um arquivo de registro json com o formato mostrado aqui:

   ```
   {
   "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. Após salvar as alterações no arquivo, passe com a opção `--file` para registrar o Tableau Server:

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

Configurar o armazenamento de identidades

Observação: se a sua implantação usar armazenamento externo para os arquivos do Tableau, você precisará habilitar o armazenamento de arquivos externos antes de configurar o armazenamento de identidade. Consulte *Instalar o Tableau Server com o armazenamento de arquivos externo* (Linux).

A arquitetura de referência padrão usa um armazenamento de identidade local. Configure o host inicial com armazenamento de identidade local passando o arquivo `config.json` com o comando `tsm settings import`.

Importe o arquivo `config.json` de acordo com seu sistema operacional:

O arquivo `config.json` está incluído no caminho do diretório scripts.<version> (por exemplo,`scripts.20204.21.0217.1203`) e é formatado para configurar o armazenamento de identidade.

Execute o comando a seguir para importar o arquivo `config.json`:

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

Configurar Postgres externo

1. Crie um arquivo json de banco de dado externo com as seguintes definições de configuração:

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

2. Depois de salvar as alterações no arquivo, passe o arquivo com o seguinte comando:

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

Você será solicitado a fornecer a senha e nome de usuário primário do Postgres.

A opção, `--no-ssl`, configura o Tableau para usar SSL/TLS somente quando o servidor Postgres estiver configurado para SSL/TLS. Se o Postgres não estiver configurado para SSL/TLS, a conexão não será criptografada. Parte 6 - Configuração pós-instalação descreve como habilitar SSL/TLS para a conexão Postgres depois de concluir a primeira fase de implantação.

3. Aplique as alterações.

   Execute este comando para aplicar as alterações e reiniciar o Tableau Server:

   ```
   tsm pending-changes apply
   ```

4. Exclua o arquivo de configuração usado na Etapa 1.

Concluir a instalação do Nó 1

1. Após a instalação do Tableau Server, você deve inicializar o servidor.

   Execute o seguinte comando:

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

2. Quando a inicialização for concluída, você deve criar uma conta de administrador do Tableau Server.

   Ao contrário da conta do computador que você está usando para instalar e gerenciar os componentes do sistema operacional TSM, a conta do administrador do Tableau Server é uma conta de aplicativo usada para criar usuários, projetos e sites do Tableau Server. O administrador do Tableau Server também aplica permissões aos recursos do Tableau. Execute o comando a seguir para criar a conta de administrador inicial. No exemplo a seguir, o usuário é chamado`tableau-admin`:

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

O Tabcmd solicitará que você defina uma senha para este usuário.

Verificação: configuração do nó 1

1. Execute o seguinte comando para verificar se os serviços TSM estão em execução:

   ```
   tsm status -v
   ```

   O Tableau deve retornar o seguinte:

   ```
   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.
   ...
   ```

   Todos os serviços serão listados.

2. Execute o seguinte comando para verificar se o site administrativo do Tableau está em execução:

   ```
   curl localhost
   ```

   As primeiras linhas devem mostrar Vizportal html, semelhante a este:

   ```
   <!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 ...
```

Fazer backups do tar de Etapa 2

Depois de verificar a instalação inicial, faça dois backups tar:

- PostgreSQL
- Nó inicial do Tableau (Nó 1)

Na maioria dos casos, você pode recuperar a instalação do nó inicial restaurando esses arquivos tar. Restaurar os arquivos tar é muito mais rápido do que reinstalar e reinicializar o nó inicial.

Criar arquivos tar da Etapa 2

1. No nó inicial do Tableau, interrompa o Tableau:

   ```
   tsm stop
   ```

   Espere que o Tableau pare antes de prosseguir para a próxima etapa.

2. No host PostgreSQL, pare a instância do banco de dados Postgres:

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

3. Execute o comando a seguir para criar o backup tar:

   ```
   sudo su
   ```

   ```
   cd /var/lib/pgsql
   ```

```
tar -cvf step2.13.bkp.tar 13

exit
```

4. Verifique se o arquivo tar Postgres foi criado com permissões de raiz:

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

5. No host do Tableau, interrompa os serviços administrativos do Tableau:

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

6. Execute o comando a seguir para criar o backup tar:

   ```
   cd /data

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

7. No host Postgres, inicie o banco de dados Postgres:

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

8. Inicie os serviços administrativos do Tableau:

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

9. Execute o comando `tsm status` para monitorar o estado do TSM antes de reiniciar.

   Na maioria dos casos, o comando retornará primeiro um status DEGRADED ou ERROR. Espere alguns minutos e execute o comando novamente. Se o status de ERROR ou DEGRADED for retornado, continue aguardando. Não tente iniciar o TSM até que o status STOPPED seja retornado. Em seguida, execute os seguintes comandos:

   ```
   tsm start
   ```

Restaurar a Etapa 2

Este processo restaura o nó 1 do Tableau e a instância Postgres para a Etapa 2. Depois de restaurar esta etapa, você pode reimplantar os nós restantes do Tableau.

1. Pare os serviços tsm no host Tableau inicial (Nó 1):

   ```
   tsm stop
   ```

2. Interrompa os serviços administrativos do Tableau em todos os nós da implantação do Tableau Server. Execute o seguinte comando em cada nó, em ordem (Nó 1, Nó 2 e, em seguida, Nó 3):

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

3. Após a interrupção dos serviços do Tableau, restaure o tar da Etapa 2 do PostgreSQL. No computador do Postgres, execute os comandos a seguir:

   - ```
     sudo su

     systemctl stop postgresql-13

     cd /var/lib/pgsql

     tar  -xvf step2.13.bkp.tar

     systemctl start postgresql-13

     exit
     ```

4. Restaure o tar da Etapa 2 do Tableau. No host inicial do Tableau, execute os comandos a seguir:

   ```
   cd /data

   sudo rm -rf tableau_data

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

5. No computador do Nó 1 do Tableau, remova os seguintes arquivos:
   ```

- `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. Inicie os serviços administrativos do Tableau:

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

7. Recarregue os arquivos systmctl do Tableau e execute `start-administrative-services` novamente:

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

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

8. No Nó 1, execute o comando `tsm status` para monitorar o estado do TSM antes de reiniciar.

   Em alguns casos, você obterá um erro, `Cannot connect to server...`. Este erro ocorre porque o serviço tabadmincontroller não foi reiniciado. Continue a executar `tsm status` periodicamente. Se este erro não desaparecer após 10 minutos, execute o comando `start-administrative-services` novamente.

   Depois de alguns momentos, o comando `tsm status` retornará um status DEGRADED e, em seguida, ERROR. Não tente iniciar o TSM até que o status STOPPED seja retornado. Em seguida, execute os seguintes comandos:

   ```
   tsm start
   ```

Retome o processo de instalação para instalar o Tableau Server nos nós restantes.

Instalar o Tableau Server em nós restante

Para continuar a implantação, copie o instalador do Tableau para cada nó.

Visão geral da configuração do nó

Esta seção descreve o processo para configurar os nós 2-4. As seções a seguir fornecem procedimentos detalhados de configuração e validação para cada etapa.

A instalação dos nós 2-4 do Tableau Server requer que você gere, copie e faça referência a um arquivo de bootstrap durante a instalação do nó.

Para gerar o arquivo de bootstrap, você executará um comando TSM no nó inicial. Em seguida, você copiará o arquivo de inicialização para o nó de destino, onde o executará como parte da inicialização do nó.

O conteúdo json a seguir mostra um exemplo de arquivo de bootstrap. (O certificado e os valores relacionados à criptografia foram truncados para tornar o arquivo de exemplo mais fácil de ler.)

```
{
"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" :
"eyJjdHkiOiJKV1QiLCJlbmMiOiJBMTI4Q0JDLUhQ...",
```

```
        "sessionCookieName" : "AUTH_COOKIE"
        }
}
```

O arquivo de bootstrap inclui validação baseada em conexão para autenticar o Nó 1 e cria um canal criptografado para o processo de bootstrap. A sessão de bootstrap é limitada no tempo, e configurar e validar nós consome muito tempo. Planeje criar e copiar novos bootstraps conforme você configura os nós.

Depois de executar o arquivo de bootstrap, você entra no nó inicial do Tableau Server e configura os processos para o novo nó. Ao terminar de configurar os nós, você deve aplicar as alterações e reiniciar o nó inicial. O novo nó é configurado e iniciado. À medida que você adiciona nós, a configuração e a reinicialização da implantação levam mais tempo consecutivamente para serem concluídas.

Os exemplos do Linux em todos os procedimentos de instalação mostram comandos para distribuições do tipo RHEL. Se você estiver executando a distribuição do Ubuntu, edite os comandos de forma apropriada.

1. Execute a atualização para aplicar as correções mais recentes ao sistema operacional Linux:

   ```
   sudo yum update
   ```

2. Baixe e instale dependências:

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

3. Crie o caminho `/app/tableau_server` no diretório raiz:

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

4. Execute o programa de instalação e especifique o caminho de instalação `/app/-tableau_server`. Por exemplo, em um sistema operacional semelhante ao Linux RHEL, execute:

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

Gere, copie e execute o arquivo de bootstrap para inicializar o TSM

O procedimento a seguir mostra como gerar, copiar e usar um arquivo de bootstrap ao inicializar o TSM em outro nó. Neste exemplo, o arquivo de bootstrap é chamado `boot.json`.

Neste exemplo, os computadores host estão em execução na AWS, onde os hosts EC2 executam o Amazon Linux 2.

1. Conecte-se ao nó inicial (Nó 1) e execute o seguinte comando:

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

2. Copie o arquivo de bootstrap para o Nó 2.

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

3. Conecte-se ao Nó 2 e alterne para o diretório de scripts do Tableau Server:

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

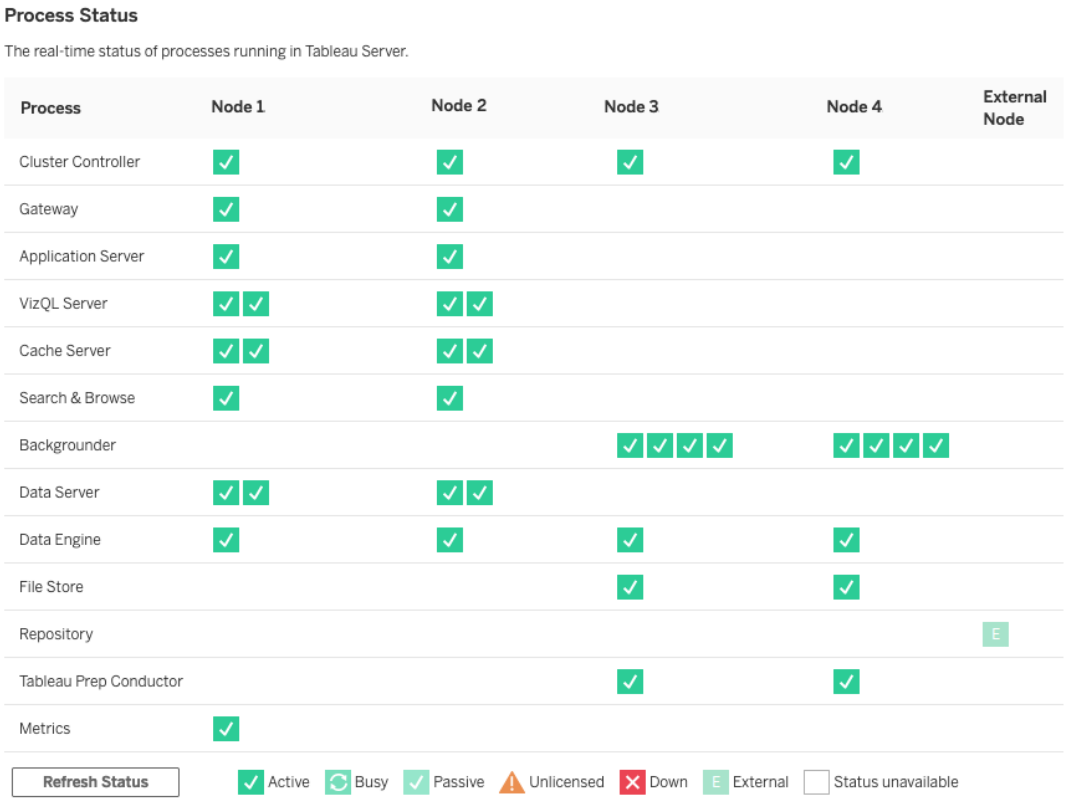
4. Execute o comando `initialize-tsm` e faça referência ao arquivo de bootstap:

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

5. Depois de `initialize-tsm` ser concluído, exclua`boot.json` e saia ou faça logout da sessão.

Configurar processos

Você deve configurar o cluster do Tableau Server no nó em que o Controlador de administração do Tableau Server (controlador TSM) está sendo executado. O controlador TSM é executado no nó inicial.



Configurar o Nó 2

1. Depois de inicializar o TSM usando o arquivo de bootstrap no Nó 2, entre no nó inicial.
2. No nó inicial, (`node1`) execute os seguintes comandos para configurar processos no Nó 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 você estiver instalando a versão 2022.1 ou posterior, adicione também o serviço Índice e Pesquisa:

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

Se você estiver instalando a versão 2023.3 ou posterior, inclua apenas o serviço Índice e Pesquisa. Não adicione o serviço Pesquisar e Navegar (servidor de pesquisa)

3. Revise a configuração antes de aplicá-la. Execute o seguinte comando:

   ```
   tsm pending-changes list
   ```

4. Depois de verificar se suas alterações estão na lista de pendentes (haverá outros serviços na lista de pendentes também), aplique as alterações:

   ```
   tsm pending-changes apply
   ```

   As alterações exigirão uma reinicialização. A configuração e a reinicialização levarão algum tempo.

5. Verificar a configuração do Nó 2. Execute o seguinte comando:

   ```
   tsm status -v
   ```

Configurar o Nó 3

Inicialize o TSM usando o processo de bootstrap no Nó 3 e, em seguida, execute os comandos `tsm topology set-process` abaixo.

Há um aviso do Serviço de coordenação que será exibido sempre que você definir um processo. Você pode ignorar esse aviso ao definir os processos.

1. Depois de inicializar o TSM usando o arquivo de bootstrap no Nó 3, entre no nó inicial (`node1`) e execute os seguintes comandos para configurar processos:

   ```
   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 você estiver instalando a versão 2022.1 ou posterior, adicione também o serviço Índice e Pesquisa:

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

2. Revise a configuração antes de aplicá-la. Execute o seguinte comando:

   ```
   tsm pending-changes list
   ```

3. Depois de verificar se suas alterações estão na lista de pendentes (a lista incluirá outros serviços que são configurados automaticamente), aplique as alterações:

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

   As alterações exigirão uma reinicialização. A configuração e a reinicialização levarão algum tempo.

4. Verifique a configuração ao executar o seguinte comando:

   ```
   tsm status -v
   ```

Implantar o ensemble do serviço de coordenação para os Nós 1-3

Para implantação de arquitetura de referência padrão de quatro nós, execute o seguinte procedimento:

1. Execute os seguintes comandos no Nó 1:

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

   O processo inclui a reinicialização do TSM, o que levará algum tempo.

2. Depois que o serviço de coordenação for implantado, Inicie o TSM.

   ```
   tsm start
   ```

Fazer backups do tar de Etapa 3

Depois de verificar a instalação, faça quatro backups tar:

- PostgreSQL
- Nó inicial do Tableau (Nó 1)
- Nó 2 do Tableau
- Nó 3 do Tableau

Criar arquivos tar da Etapa 3

1. No nó inicial do Tableau, interrompa o Tableau:

   ```
   tsm stop
   ```

2. Depois que o TSM for interrompido, pare os serviços administrativos do Tableau em cada nó. Execute o seguinte comando em cada nó, em ordem (Nó 1, Nó 2 e, em seguida, Nó 3):

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

3. No host PostgreSQL, pare a instância do banco de dados Postgres:

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

4. Execute o comando a seguir para criar o backup tar:

```
sudo su

cd /var/lib/pgsql

tar -cvf step3.12.bkp.tar 12

exit
```

5. Verifique se o arquivo tar Postgres foi criado com permissões de raiz:

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

6. No host Postgres, inicie o banco de dados Postgres:

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

7. Crie o backup de tar no Nó 1, Nó 2 e Nó 3. Execute os seguintes comandos em cada nó:

   - `cd /data`

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

   - Verifique se o arquivo tar do Tableau foi criado com permissões de raiz:

     ```
     ls -al
     ```

8. Inicie os serviços administrativos do Tableau em cada nó em ordem (Nó 1, Nó 2 e, em seguida, Nó 3):

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

9. Execute o comando `tsm status` para monitorar o estado do TSM antes de reiniciar.

Na maioria dos casos, o comando retornará um status DEGRADED e, em seguida, ERROR. Espere alguns instantes e execute o comando novamente. Se o status de ERROR ou DEGRADED for retornado, continue aguardando. Não tente iniciar o TSM até que o status STOPPED seja retornado. Em seguida, execute os seguintes comandos:

```
tsm start
```

Restaurar a Etapa 3

Este processo restaura o Nó 1, Nó 2 e Nó 3 do Tableau. Ele também restaura a instância do Postgres para a Etapa 3. Depois de restaurar esta etapa, você pode implantar o serviço de coordenação, Nó 4 e, a seguir, as configurações finais do nó.

1. Pare o serviço tsm no host Tableau inicial (Nó 1):

   ```
   tsm stop
   ```

2. Depois que o TSM for interrompido, pare os serviços administrativos do Tableau no Nó 1, Nó 2 e Nó 3. Execute os seguintes comandos em cada nó:

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

3. Restaure o tar da Etapa 3 do PostgreSQL. No computador do Postgres, execute os comandos a seguir:

   ```
   sudo su

   systemctl stop postgresql-12

   cd /var/lib/pgsql

   tar -xvf step3.12.bkp.tar

   systemctl start postgresql-12
   ```

```
exit
```

4. Restaure o tar da Etapa 3 do Tableau no Nó 1, Nó 2 e Nó 3. Execute os seguintes comandos em cada nó do Tableau:

   ```
   cd /data
   ```

   ```
   sudo rm -rf tableau_data
   ```

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

5. No computador do Nó 1 do Tableau, remova os seguintes arquivos:

   - `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 o shell retornar um erro "arquivo não encontrado", pode ser necessário alterar o nome do caminho para incrementar o número `<n>` nesta seção do caminho: `. . ./app-zookeeper/<n>/version-2/. . . .`

6. Reinicie os serviços administrativos no Nó 1, Nó 2 e Nó 3. Execute os seguintes comandos em cada nó:

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

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

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

7. No Nó 1, execute o comando `tsm status` para monitorar o estado do TSM antes de reiniciar.

Em alguns casos, você obterá um erro, `Cannot connect to server...`. Este erro ocorre porque o serviço tabadmincontroller não foi reiniciado. Continue a executar `tsm status` periodicamente. Se este erro não desaparecer após 10 minutos, execute o comando `start-administrative-services` novamente.

Depois de alguns momentos, o comando `tsm status` retornará um status DEGRADED e, em seguida, ERROR. Não inicie o TSM até que o status STOPPED seja retornado. Em seguida, execute os seguintes comandos:

```
tsm start
```

Retome o processo de instalação para implantar o serviço de coordenação nos Nós 1-3

Configurar o Nó 4

O processo de configuração do Nó 4 é igual ao do Nó 3.

Defina os mesmos processos que definidos para o Nó 3, executando o mesmo conjunto de comandos como mostrado acima, mas especificando `node4` nos comandos ao invés de `node3`.

Tal como acontece com a verificação do Nó 3, verifique a configuração do Nó 4 executando `tsm status -v`.

Antes de continuar, aguarde até que o processo de armazenamento de arquivo no Nó 4 conclua a sincronização. O status do serviço de Armazenamento de arquivos retornará `is synchronizing` até terminar. Quando o status do serviço de Armazenamento de arquivo retornar `is running`, você poderá continuar.

Configuração e verificação do processo final

A etapa final para processar a configuração é remover processos redundantes do Nó 1.

1. Conecte-se ao nó inicial (`node1`)
2. Descomissione o armazenamento de arquivo no Nó 1. Isso causará um aviso sobre a remoção do armazenamento de arquivo de um controlador colocalizado. Você pode ignorar o aviso. Execute o seguinte comando:

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

3. Quando o armazenamento de arquivos for encerrado, execute o seguinte comando para remover o processo em segundo plano do Nó 1:

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

4. Revise a configuração antes de aplicá-la. Execute o seguinte comando:

   ```
   tsm pending-changes list
   ```

5. Depois de verificar se suas alterações estão na lista pendente, aplique as alterações:

   ```
   tsm pending-changes apply
   ```

   As alterações exigirão uma reinicialização. A configuração e a reinicialização levarão algum tempo.

6. Verifique a configuração:

   ```
   tsm status -v.
   ```

   Antes de continuar, aguarde até que o processo de armazenamento de arquivo no Nó 4 conclua a sincronização. O status do serviço de Armazenamento de arquivos retornará `is synchronizing` até terminar. Quando o status do serviço de Armazenamento de arquivo retornar `is running`, você poderá continuar.

Faça backup

Uma recuperação completa do Tableau Server requer um portfólio de backup que inclui três componentes:

- Um arquivo de backup dos dados do repositório e do armazenamento de arquivos. Este arquivo é gerado pelo comando `tsm maintenance backup`.
- Um arquivo de exportação de topologia e configuração. Este arquivo é gerado pelo comando `tsm settings export`.
- Certificado de autenticação, chave e arquivos keytab.

Para obter uma descrição completa do processo de backup e restauração, consulte o tópico do Tableau Server, *Executar um backup e uma restauração completos do Tableau Server* (Linux).

Nesta fase da implantação, todos os arquivos e ativos relevantes que são necessários para uma restauração completa são incluídos executando os comandos `tsm maintenance backup` e `tsm settings export`.

1. Execute o seguinte comando para exportar a configuração e as definições de topologia para um arquivo chamado `ts_settings_backup.json`

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

2. Execute o seguinte comando para criar um backup do repositório e armazenar os dados de arquivo em um arquivo denominado `ts_backup-<yyyy-mm-dd>.tsbak`. Ignore o aviso sobre o armazenamento de arquivo não estar no nó do controlador.

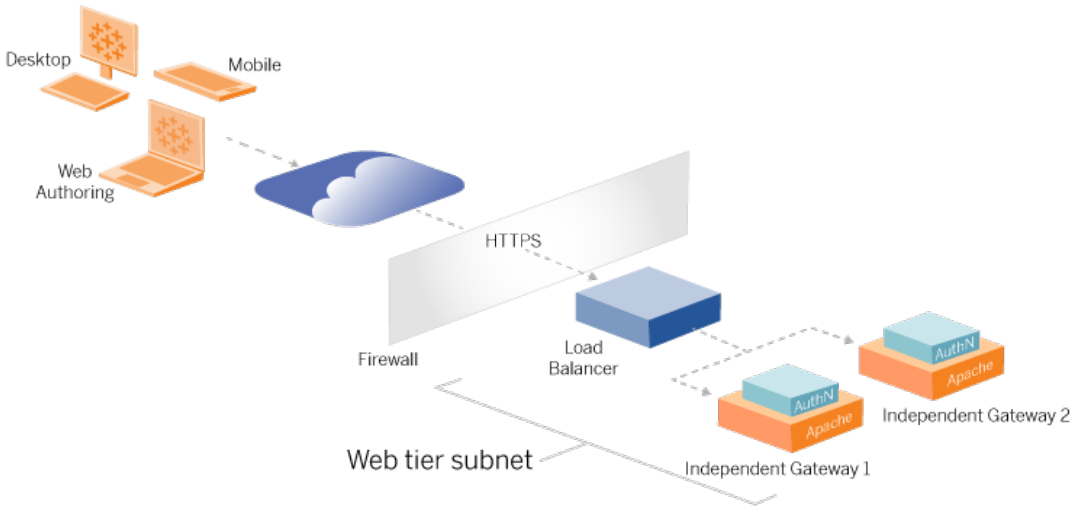
   ```
   tsm maintenance backup -f ts_backup -d --skip-compression
   ```

   Localização do arquivo de backup:

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

3. Copie os dois arquivos e salve-os em um ativo de armazenamento diferente que não é compartilhado por sua implantação do Tableau Server.

Parte 5 - Configuração do nível da Web



A camada da Web da arquitetura de referência deve incluir os seguintes componentes:

- Um balanceador de carga de aplicativo voltado para a Web que aceita solicitações HTTPS de clientes Tableau e se comunica com os servidores proxy reverso.
- Proxy reverso:
  - Recomendamos a implantação do Tableau Server Independent Gateway.
  - Recomendamos um mínimo de dois servidores proxy para redundância e para lidar com a carga do cliente.
  - Recebe tráfego HTTPS do balanceador de carga.
  - Compatível com sessão fixa para o host do Tableau
  - Configure o proxy para balanceamento de carga round robin para cada Tableau Server executando o processo de Gateway.
  - Lida com solicitações de autenticação de IdP externo.
- Proxy de encaminhamento: o Tableau Server requer acesso à Internet para licenciamento e funcionalidade de mapa. Você deve configurar listas seguras de proxy de

encaminhamento para URLs de serviço do Tableau. Consulte *Comunicação com a Internet* (Linux).

- Todo o tráfego relacionado ao cliente pode ser criptografado por HTTPS:
  - Balanceador de carga de cliente para aplicativo
  - Balanceador de carga de aplicativo para servidores proxy reversos
  - Servidor proxy para Tableau Server
  - Manipulador de autenticação em execução em proxy reverso para IdP
  - Tableau Server para IdP

Tableau Server Independent Gateway

O Tableau Server versão 2022.1 lançou o Tableau Server Independent Gateway. O Independent Gateway é uma instância autônoma do processo de Gateway do Tableau que funciona como um proxy reverso compatível com o Tableau.

O Independent Gateway oferece suporte ao balanceamento de carga round robin simples para os Tableau Servers de back-end. No entanto, o Independent Gateway não se destina a servir como balanceador de carga de aplicativos corporativos. Recomendamos executar o Independent Gateway por trás de um balanceador de carga de aplicativos de classe empresarial.

O Independent Gateway requer uma licença de Advanced Management.

Autenticação e autorização

A arquitetura de referência padrão especifica a instalação do Tableau Server com autenticação local configurada. Neste modelo, os clientes devem se conectar ao Tableau Server para serem autenticados pelo processo de autenticação local nativo do Tableau Server. Não recomendamos o uso desse método de autenticação na arquitetura de referência, porque o cenário exige que os clientes não autenticados se comuniquem na camada do aplicativo, o que é um risco à segurança.

Em vez disso, recomendamos a configuração de um provedor de identidade externo de nível empresarial junto com um módulo AuthN para pré-autenticar todo o tráfego para a camada de

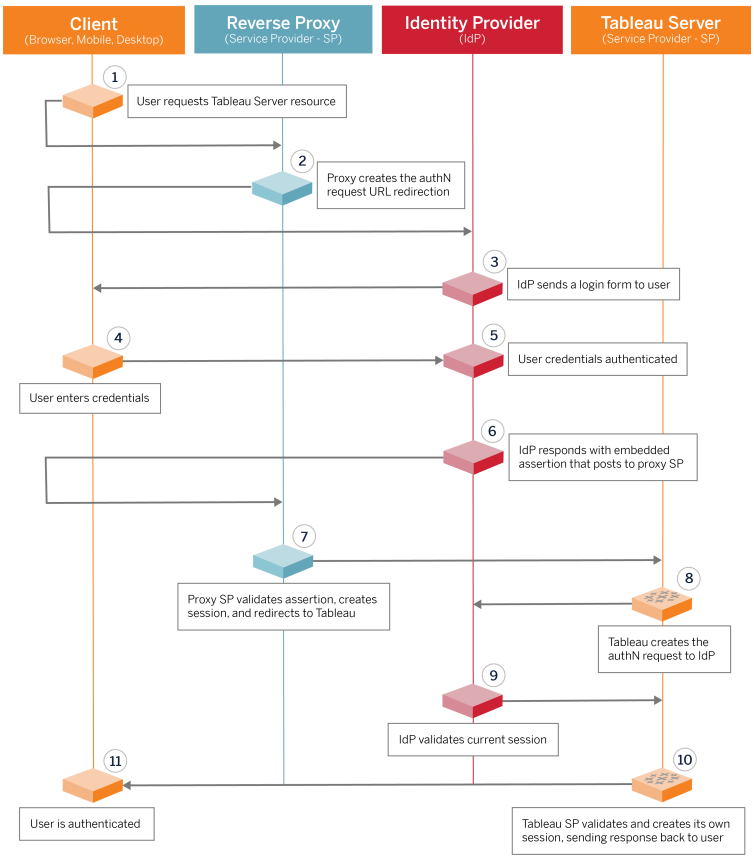
aplicativo. Quando configurado com um IdP externo, o processo de autenticação local nativo do Tableau Server não é usado. O Tableau Server autoriza o acesso a recursos na implantação, depois que o IdP autentica os usuários.

Pré-autenticação com um módulo AuthN

No exemplo documentado neste Guia, o SAML SSO está configurado, mas o processo de pré-autenticação pode ser configurado com a maioria dos provedores de identidade externos e um módulo AuthN.

Na arquitetura de referência, o proxy reverso é configurado para criar uma sessão de autenticação de cliente com o IdP, antes de fazer o proxy dessas solicitações para o Tableau Server. Chamamos esse processo de fase de *pré-autenticação*. O proxy reverso redirecionará apenas sessões de cliente autenticadas para o Tableau Server. O Tableau Server criará uma sessão, verificará a autenticação da sessão com o IdP e retornará a solicitação do cliente.

O diagrama a seguir mostra os detalhes passo a passo do processo de pré-autenticação e autenticação com um módulo AuthN configurado. O proxy reverso pode ser uma solução genérica de terceiros ou o Tableau Server Independent Gateway:



Visão geral da configuração

Esta é uma visão geral do processo de configuração do nível da Web. Verifique a conectividade após cada etapa:

1. Configure dois proxies reversos para fornecer acesso HTTP ao Tableau Server.
2. Configure a lógica de balanceamento de carga com sessões persistentes em servidores proxy para se conectar a cada instância do Tableau Server que executa o processo de Gateway.
3. Configure o balanceamento de carga do aplicativo com sessões persistentes no gateway da Internet para encaminhar solicitações aos servidores proxy reverso.
4. Configure a autenticação com um IdP externo. Você pode configurar o SSO ou SAML instalando um manipulador de autenticação nos servidores proxy reverso. O módulo AuthN gerencia o handshake de autenticação entre o IdP externo e a implantação do

Tableau. O Tableau também atuará como um provedor de serviços IdP e autenticará usuários com o IdP.

5. Para autenticar com o Tableau Desktop nesta implantação, seus clientes devem estar executando o Tableau Desktop 2021.2.1 ou posterior.

Exemplo de configuração de camada da Web com o Tableau Server Independent Gateway

O restante deste tópico fornece um procedimento de ponta a ponta que descreve como implementar o nível da Web no exemplo de arquitetura de referência da AWS usando o Tableau Server Independent Gateway. Para obter um exemplo de configuração usando o Apache como proxy reverso, consulte Apêndice - Camada da Web com exemplo de implantação do Apache.

A configuração de exemplo é inclui os seguintes componentes:

- Balanceador de carga de aplicativo AWS
- Tableau Server Independent Gateway
- Módulo de autenticação Mellon
- Okta IdP
- Autenticação SAML

Observação: o exemplo de configuração de nível da Web apresentado nesta seção inclui procedimentos detalhados para implantação de software e serviços de terceiros. Fizemos o melhor esforço para verificar e documentar os procedimentos para habilitar o cenário de nível da Web. No entanto, o software de terceiros pode mudar ou seu cenário pode ser diferente da arquitetura de referência descrita aqui. Consulte a documentação de terceiros para obter detalhes e suporte de configuração confiável.

Os exemplos do Linux em toda esta seção mostram comandos para distribuições do tipo RHEL. Especificamente, os comandos aqui foram desenvolvidos com a distribuição Amazon

Linux 2. Se você estiver executando a distribuição do Ubuntu, edite os comandos de forma apropriada.

A implementação do nível da Web neste exemplo segue uma configuração passo a passo e procedimento de verificação. A configuração principal da camada da Web consiste nas etapas a seguir para habilitar HTTP entre o Tableau e a Internet. O Independent Gateway é executado e configurado para proxy reverso/balanceamento de carga por trás do balanceador de carga do aplicativo AWS:

1. Preparação do ambiente
2. Desinstalação do Independent Gateway
3. Configuração do servidor Independent Gateway
4. Configure o balanceador de carga do aplicativo AWS

Depois que a camada da Web for configurada, e a conectividade com o Tableau verificada, configure a autenticação com um provedor externo.

Preparar o ambiente

Conclua as tarefas a seguir antes de implementar o Independent Gateway.

1. Alterações do grupo de segurança da AWS. Configure o grupo de segurança pública para permitir o tráfego de manutenção do Independent Gateway de entrada (TCP 21319) do grupo de segurança privada.

2. Instale a versão 22.1.1 (ou posterior) no cluster do Tableau Server de quatro nós, conforme documentado na Parte 4 - Instalar e configurar o Tableau Server.

3. Configure as duas instâncias de proxy do EC2 no grupo de segurança pública conforme documentado em Configurar computadores host.

Desinstalação do Independent Gateway

O Tableau Server Independent Gateway requer uma licença de Advanced Management.

A implantação do Tableau Server Independent Gateway consiste em instalar e executar o pacote .rpm e, em seguida, configurar o estado inicial. O procedimento incluído neste Guia fornece orientação prescritiva para implantação na arquitetura de referência.

Se sua implantação for diferente da arquitetura de referência, consulte a documentação principal do Tableau Server, *Instalar o Tableau Server com Independent Gateway* (Linux).

Importante: configurar o Independent Gateway pode ser um processo propenso a erros. É muito difícil solucionar problemas de configuração em duas instâncias de servidores de Independent Gateway. Por esse motivo, recomendamos configurar um servidor Independent Gateway de cada vez. Depois de configurar o primeiro servidor e verificar a funcionalidade, você deve configurar o segundo servidor Independent Gateway.

Embora você configure cada servidor de Independent Gateway separadamente, execute este procedimento de instalação em ambas as instâncias do EC2 que você instalou no grupo de segurança pública:

1. Execute a atualização para aplicar as correções mais recentes ao sistema operacional Linux:

   ```
   sudo yum update
   ```

2. Se o Apache estiver instalado, remova-o:

   ```
   sudo yum remove httpd
   ```

3. Copie o pacote de instalação da versão 2022.1.1 (ou posterior) do Independent Gateway página Downloads do Tableau para o computador host que executará o Tableau Server.

   Por exemplo, em um computador executando o sistema operacional semelhante ao Linux RHEL, execute:

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

4. Execute o programa de Instalação. Por exemplo, em um sistema operacional semelhante ao Linux RHEL, execute:

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

5. Mude para o diretório `/opt/tableau/tableau_tsig/-packages/scripts.<version_code>/` e execute o script `initialize-tsig` localizado lá: Além do sinalizador `--accepteula`, você deve incluir o intervalo de IP das sub-redes em que a implantação do Tableau Server está sendo executada. Use a opção `-c` para especificar o intervalo de IP. O exemplo abaixo mostra o comando com as sub-redes da AWS de exemplo especificadas:

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

6. Após a conclusão da inicialização, abra o arquivo `tsighk-auth.conf` e copie o segredo de autenticação no arquivo. Você precisará enviar este código para cada instância de Independent Gateway como parte da configuração de back-end do Tableau Server:

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

7. Depois de executar as etapas anteriores nas duas instâncias do Independent Gateway, prepare o arquivo de configuração `tsig.json`. O arquivo de configuração consiste em uma matriz de "independentGateways". A matriz contém objetos de configuração que definem detalhes de conexão para uma instância de Independent Gateway.

   Copie o seguinte JSON e personalize-o de acordo com seu ambiente de implementação. O exemplo aqui mostra um arquivo para uma arquitetura de referência da AWS de exemplo.

O arquivo JSON de exemplo abaixo inclui apenas informações de conexão para um Independent Gateway. Mais tarde no processo, você incluirá as informações de conexão para o segundo servidor Independent Gateway.

Salve o arquivo como `tsig.json` para os procedimentos a seguir.

```
{
"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"`- O nome DNS privado da instância do AWS EC2 que executa o Independent Gateway.
- `"host"`- igual a `"id"`.
- `"port"`- A porta de limpeza, por padrão, `"21319"`.
- `"protocol"`- O protocolo para o tráfego do cliente. Deixe isso como `http` para a configuração inicial.
- `"authsecret"`- O segredo que você copiou na etapa anterior.

Independent Gateway: conexão direta versus relé

Antes de continuar, você deve decidir qual esquema de conexão configurar em sua implantação: conexão direta ou de relé. Cada opção é brevemente descrita aqui, juntamente com os pontos de dados de decisão relevantes.

Conexão de relé: você pode configurar o Independent Gateway para retransmitir a comunicação do cliente por uma única porta para o processo de gateway no Tableau Server. Essa comunicação é chamada conexão de *relé*:

- O processo de relé resulta em um salto extra do Independent Gateway para o processo back-end do Gateway do Tableau Server. O salto extra degrada o desempenho em comparação com a configuração de conexão direta.
- TLS é compatível com o modo de relé. Toda a comunicação no modo de relé é restrita a um único protocolo (HTTP ou HTTPS) e, portanto, pode ser criptografada e autenticada com TLS.

Conexão direta: o Independent Gateway pode se comunicar diretamente com os processos back-end do Tableau Server em várias portas. Essa comunicação é chamada conexão *direta*.

- Como a conexão é direta com o Tableau Server de back-end, o desempenho do cliente é significativamente aprimorado em comparação com a opção de conexão de relé.
- Requer a abertura de mais de 16 portas de sub-redes Públicas para Privadas para comunicação direta do processo do Independent Gateway para computadores do Tableau Server.
- O TLS ainda não é compatível com os processos do Independent Gateway para o Tableau Server.

Configurar a conexão de relé

Para executar o TLS entre o Tableau Server e o Independent Gateway, você deve configurar com uma conexão de retransmissão. Os cenários de exemplo no EDG são configurados com conexão de relé.

1. Cópia de `tsig.json` para o nó 1 de sua implantação do Tableau Server.

2. No Nó 1, execute os comandos a seguir para habilitar o Independent Gateway.

```
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
```

Configurar a conexão direta

Como a conexão direta não oferece suporte a TLS, recomendamos configurar a conexão direta somente se você conseguir proteger todo o tráfego de rede por outros meios. Para executar o TLS entre o Tableau Server e o Independent Gateway, você deve configurar com uma conexão de retransmissão. Os cenários de exemplo no EDG são configurados com conexão de relé.

Se você estiver configurando o Independent Gateway para conexão direta com o Tableau Server, deverá habilitar a configuração para acionar a comunicação. Depois que o Tableau Server se comunicar com o Independent Gateway, os destinos do protocolo serão estabelecidos. Você deve então recuperar o `proxy_targets.csv` do computador do Independent Gateway e abra as portas correspondentes dos grupos de segurança Pública para Privada na AWS.

1. Cópia de `tsig.json` para o nó 1 de sua implantação do Tableau Server.

2. No Nó 1, execute os comandos a seguir para habilitar o Independent Gateway.

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

3. No computador do Independent Gateway, execute o seguinte comando para exibir as portas que o cluster do Tableau Server está usando:

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

4. Configurar grupos de segurança de AWS. Adicione as portas TCP listadas em `proxy_targets.csv` para permitir a comunicação do grupo de segurança pública para o grupo de segurança privada.

   Recomendamos automatizar a configuração de entrada de porta, pois as portas podem ser alteradas se a implantação do Tableau Server for alterada. Adicionar nós

ou reconfigurar processos na implantação do Tableau Server acionará alterações no acesso à porta exigido pelo Independent Gateway.

Verificação: configuração da topologia de base

Você deve conseguir acessar a página de administração do Tableau Server navegando para `http://<gateway-public-IP-address>`.

Se a página de entrada do Tableau Server não carregar ou se o Tableau Server não iniciar, siga estas etapas de solução de problemas:

Rede:

- Verifique a conectividade entre a implantação do Tableau e a instância do Independent Gateway executando o seguinte comando `wget` do Tableau Server Nó1: wget http://<endereço IP interno do Independent Gateway> :21319, por exemplo:

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

  Se a conexão for recusada ou falhar, verifique se o grupo de segurança pública está configurado para permitir o tráfego de manutenção do Independent Gateway (TCP 21319) do grupo de segurança privada.

  Se o grupo de segurança estiver configurado corretamente, verifique se você especificou os endereços IP ou intervalos de IP corretos durante a inicialização do Independent Gateway. Você pode visualizar e alterar esta configuração no arquivo `environment.bash` localizado em `/etc/opt/tableau/tableau_tsig/environment.bash`. Se você fizer uma alteração nesse arquivo, reinicie o serviço tsig-http conforme descrito abaixo.

No host Proxy 1:

1. Substitua o arquivo httpd.conf pelo arquivo stub do Independent Gateway:

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

2. Reinicie o tsig-httpd como uma primeira etapa de solução de problemas:

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

Nó 1 do Tableau

- Verifique novamente o arquivo `tsig.json`. Se você encontrar erros, corrija-os e execute `tsm topology external-services gateway update -c tsig.json`.
- Se estiver executando uma conexão direta, verifique as portas TCP listadas em `proxy_targets.csv` são configurados como portas de entrada de grupos de segurança Público para Privado.

Configure o balanceador de carga do aplicativo AWS

Configure o balanceador de carga como um ouvinte HTTP. O procedimento aqui descreve como adicionar um balanceador de carga na AWS.

Etapa 1: criar grupo de destinos

Um grupo de destino é uma configuração da AWS que define as instâncias do EC2 que executam os servidores proxy. Esses são os destinos do tráfego do LBS.

1. EC2>**Grupos de destino** > **Criar grupo de destino**

2. Na página Criar:
    - Insira um nome para o grupo de destino, por exemplo `TG-internal-HTTP`
    - Tipo de destino: instâncias
    - Protocolo: HTTP
    - Porta: 80
    - VPC: selecione o seu VPC
    - Em **Verificações de integridade** > **Configurações avançadas de verificações de integridade > Códigos de sucesso** , anexe a lista de códigos para ler: `200,303`.
    - Clique em **Criar**

3. Selecione o grupo de destinos que você acabou de criar e clique na guia **Destinos**:
    - Clique em **Editar**.
    - Selecione as instâncias do EC2 (ou instância única, se você estiver configurando uma de cada vez) que estão executando o aplicativo proxy e clique em **Adicionar ao arquivo**.
    - Clique em **Salvar**.

Etapa 2: iniciar o assistente de balanceador de carga

1. EC2 > **Balanceadores de carga**> **Criar balanceador de carga**
2. Na página “Selecionar tipo de balanceador de carga”, crie um Balanceador de carga de aplicativo.

Observação: a interface de usuário exibida para configurar o balanceador de carga não é consistente em datacenters AWS. O procedimento abaixo, "Configuração do assistente," mapeia para o assistente de configuração da AWS que começa na **Etapa 1 Configurar o balanceador de carga**.

Se o seu datacenter exibe todas as configurações em uma única página que inclui um botão **Criar balanceador de carga** na parte inferior da página, siga o procedimento "Configuração de página única" abaixo.

Configuração do assistente

1. Página **Configurar o balanceador de carga**:
    - Especifique o nome
    - Esquema: voltado para a Internet (padrão)
    - Tipo de endereço IP: ipv4 (padrão)
    - Ouvintes (ouvintes e roteamento):
        a. Deixe o ouvinte HTTP padrão
        b. Clique em **Adicionar ouvinte** e adicione `HTTPS:443`

- VPC: selecione o VPC onde você instalou tudo
- Zonas de disponibilidade:
  - Selecione **a** e **b** para suas regiões de datacenter
  - Em cada seletor suspenso correspondente, selecione a sub-rede pública (onde residem seus servidores proxy).
- Clique em: **Definir configurações de segurança**

2. Página **Definir configurações de segurança**

   - Faça upload do seu certificado SSL público.
   - Clique em **Próximo: configurar grupos de segurança**.

3. Página **Definir configurações de segurança**:

   - Selecione o grupo de segurança Pública. Se o grupo de segurança Padrão for selecionado, desmarque essa seleção.
   - Clique em **Próximo: configurar rota**.

4. Página **Configurar roteamento**

   - Grupo de destino: Grupo de destino existente.
   - Nome: selecione o grupo de destino que você criou anteriormente
   - Clique em **Avançar: Registrar destinos**.

5. Página **Registrar destinos**

   - As duas instâncias do servidor proxy que você configurou anteriormente devem ser exibidas.
   - Clique em **Próximo: revisão**.

6. Página **Revisão**

   Clique em **Criar**.

Configuração de página única

Configuração básica

- Especifique o nome
- Esquema: voltado para a Internet (padrão)
- Tipo de endereço IP: ipv4 (padrão)

Mapeamento de rede

- VPC: selecione o VPC onde você instalou tudo
- Mapeamentos:
  - Selecione as Zonas de disponibilidade **a** e **b** (ou comparáveis) para as suas regiões de datacenter
  - Em cada seletor suspenso correspondente, selecione a sub-rede pública (onde residem seus servidores proxy).

Grupos de segurança

Selecione o grupo de segurança Pública. Se o grupo de segurança Padrão for selecionado, desmarque essa seleção.

Ouvintes e roteamento

- Deixe o ouvinte HTTP padrão. Para a **ação padrão**, especifique o grupo-alvo que você configurou anteriormente.
- Clique em **Adicionar ouvinte** e adicione `HTTPS:443`. Para a **ação padrão**, especifique o grupo-alvo que você configurou anteriormente.

Configurações de ouvinte seguro

- Faça upload do seu certificado SSL público.

Clique em **Criar o balanceador de carga**.

Etapa 3: habilitar aderência

1. Depois que o balanceador de carga é criado, você deve habilitar a aderência no grupo de destino.
   - Abra a página Balanceador de carga da AWS (**EC2**> **Balanceadores de carga**> **Grupos de destinos**), selecione a instância do balanceador de carga que você acabou de configurar. No menu **Ação**, selecione **Editar atributos**.

- Na página **Editar atributos**, selecione **Aderência**, especifique uma duração de `1 day` e, em seguida, **Salvar alterações**.

2. No balanceador de carga, ative a aderência no ouvinte HTTP. Selecione o balanceador de carga que você acabou de configurar e clique na guia **Ouvintes:**

    - Para **HTTP: 80**, clique em **Exibir/editar regras**. Na página **Regras**, clique no ícone de edição (uma vez no topo da página e depois novamente na regra) para editar a regra. Exclua a regra THEN existente e substitua-a clicando em **Adicionar ação** > **Encaminhar para....** Na configuração THEN resultante, especifique o mesmo grupo de destino que você criou. Em Aderência em nível de grupo, ative a aderência e defina a duração para 1 dia. Salve a configuração e clique em **Atualizar**.

Etapa 4: definir o tempo limite de inatividade no balanceador de carga

No balanceador de carga, atualize o tempo limite de inatividade para 400 segundos.

Selecione o balanceador de carga que você configurou para esta implantação e clique em **Ações** > **Editar atributos**. Defina o **Tempo limite de inatividade** para `400` segundos e, em seguida, clique em **Salvar**.

Etapa 5: verificar a conectividade LBS

Abra a página Balanceador de carga da AWS (**EC2**> **Balanceadores de carga**), selecione a instância do balanceador de carga que você acabou de configurar.

Em **Descrição** copie o nome DNS e cole-o em um navegador para acessar a página de entrada do Tableau Server.

Se você receber um erro de nível 500, provavelmente precisará reiniciar seus servidores proxy.

Atualize DNS com URL pública do Tableau

Use o nome da zona DNS de seu domínio da descrição do Balanceador de carga da AWS para criar um valor CNAME em seu DNS. O tráfego para a sua URL (tableau.example.com)

deve ser enviado ao nome DNS público da AWS.

Verifique a conectividade

Depois que suas atualizações de DNS forem concluídas, você deverá conseguir navegar para a página de entrada do Tableau Server inserindo a URL pública, por exemplo,`https://-tableau.example.com`.

Exemplo de configuração de autenticação: SAML com IdP externo

O exemplo a seguir descreve como instalar e configurar o SAML com Okta IdP e módulo de autenticação Mellon para uma implantação do Tableau em execução na arquitetura de referência da AWS.

Este exemplo retoma a seção anterior e supõe que você esteja configurando um Independent Gateway por vez.

O exemplo descreve como configurar o Tableau Server e o Independent Gateway por HTTP. O Okta enviará a solicitação ao balanceador de carga AWS por HTTPS, mas todo o tráfego interno se deslocará por HTTP. Ao configurar para este cenário, esteja ciente dos protocolos HTTP vs HTTPS ao configurar cadeias de caractere de URL.

Este exemplo usa o Mellon como um módulo de provedor de serviços de pré-autenticação nos servidores do Independent Gateway. Essa configuração garante que apenas o tráfego autenticado se conecte ao Tableau Server, que também atua como um provedor de serviços com o Okta IdP. Portanto, você deve configurar dois aplicativos IdP: um para o provedor de serviços Mellon e um para o provedor de serviços Tableau.

Crie a conta de administrador do Tableau

Um erro comum ao configurar o SAML é esquecer de criar uma conta de administrador no Tableau Server, antes de habilitar o SSO.

A primeira etapa é criar uma conta no Tableau Server com uma função de Administrador do servidor. Para o exemplo do cenário Okta, o nome de usuário deve estar em um formato de endereço de e-mail válido, por exemplo, usuário@example.com. Você deve definir uma senha para este usuário, mas a senha não será usada após a configuração do SAML.

Configurar aplicativo de pré-autenticação Okta

O cenário de ponta a ponta descrito nesta seção requer dois aplicativos Okta:

- Aplicativo de pré-autenticação Okta
- Aplicativo Okta Tableau Server

Cada um desses aplicativos está associado a metadados diferentes que você precisará configurar no proxy reverso e no Tableau Server, respectivamente.

Este procedimento descreve como criar e configurar o aplicativo de pré-autenticação Okta. Posteriormente neste tópico, você criará o aplicativo Okta Tableau Server. Para uma conta Okta de teste gratuita com usuários limitados, consulte a página da Web do Desenvolvedor do Okta.

Crie uma integração de aplicativo SAML para o provedor de serviços de pré-autenticação Mellon.

1. Abra o painel de administração do Okta> **Aplicativos** > **Criar integração de aplicativo**.
2. Na página **Criar uma nova integração de aplicativo**, selecione **SAML 2.0** e clique em **Avançar**.
3. Na guia **Configurações gerais**, insira um nome de aplicativo, por exemplo `Tableau Pre-Auth` e clique em **Avançar**.
4. Na guia **Configurar SAML**:
    - Logon único (SSO) na URL. O elemento final do caminho na URL de logon único é conhecido como `MellonEndpointPath` no arquivo de configuração

`mellon.conf` posteriormente neste procedimento. Você pode especificar qualquer ponto de extremidade que desejar. Neste exemplo, `sso` é um ponto de extremidade. O último elemento, `postResponse`, é necessário: `https://tableau.example.com/sso/postResponse`.

- Desmarque a caixa de seleção: **Use para URL do destinatário e URL de destino**.
- URL do destinatário: igual à URL do SSO, mas com HTTP. Por exemplo, `http://tableau.example.com/sso/postResponse`.
- URL de destino: igual à URL do SSO, mas com HTTP. Por exemplo, `http://tableau.example.com/sso/postResponse`.
- URI de público (ID da entidade SP). Por exemplo, `https://tableau.example.com`.
- Formato de ID do nome:`EmailAddress`
- Nome de usuário do aplicativo: `Email`
- Declarações de atributos: Nome =`mail`; Formato do nome =`Unspecified`; Valor =`user.email`.

Clique em **Próximo**.

5. Na guia **Feedback**, selecione:
   - **Sou um cliente do Okta adicionando um aplicativo interno**
   - **Este é um aplicativo interno que criamos**
   - Clique em **Concluir**.

6. Crie o arquivo de metadados do IdP de pré-autenticação:
   - No Okta: **Aplicativos** > **Aplicativos** > Seu novo aplicativo (por exemplo,`Tableau Pre-Auth`) > **Entrar**
   - Ao lado de **Certificados de assinatura SAML** , clique em **Exibir instruções de configuração SAML**.
   - Em **Como configurar o SAML 2.0 para<pre-auth> Aplicativo**, na página, role para baixo até a seção **Opcional**, **forneça os seguintes metadados de IDP para seu provedor de SP**.
   - Copie o conteúdo do campo XML e salve-o em um arquivo chamado `pre-auth_idp_metadata.xml`.

7. (Opcional) Configure a autenticação multifator:

- No Okta: **Aplicativos** > **Aplicativos** > Seu novo aplicativo (por exemplo,`Tableau Pre-Auth`) > **Entrar**
- **Em Política de logon**, clique em **Adicionar regra**.
- Na **Regra de logon do aplicativo**, especifique um nome e as diferentes opções de MFA. Para testar a funcionalidade, você pode deixar todas as opções como padrão. No entanto, em **Ações**, você deve selecionar **Solicitar fator** e, a seguir, especificar a frequência com que os usuários devem entrar. Clique em **Salvar**.

Crie e atribua usuário do Okta

1. No Okta, crie um usuário com o mesmo nome de usuário que você criou no Tableau (usuário@example.com): **Diretório** > **Pessoas** > **Adicionar pessoa**.
2. Depois que o usuário for criado, atribua o novo aplicativo Okta a essa pessoa: clique no nome do usuário e atribua o aplicativo em **Atribuir aplicativo**.

Instale o Mellon para pré-autenticação

Este exemplo usa mod_auth_mellon, um módulo de código aberto popular. Algumas distribuições Linux empacotam versões mod_auth_mellon obsoletas de um repositório mais antigo. Essas versões obsoletas podem conter vulnerabilidades de segurança desconhecidas ou problemas funcionais. Se você optar por usar mod_auth_mellon, verifique se está usando uma versão atual.

O módulo mod_auth_mellon é um software de terceiros. Fizemos o melhor esforço para verificar e documentar os procedimentos para habilitar este cenário. No entanto, o software de terceiros pode mudar ou seu cenário pode ser diferente da arquitetura de referência descrita aqui. Consulte a documentação de terceiros para obter detalhes e suporte de configuração confiável.

1. Nas instâncias do EC2 ativo que estão executando o Independent Gateway, instale uma versão atual do módulo de autenticação Mellon.

2. Crie o diretório `/etc/mellon`:

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

Configure o Mellon como módulo de pré-autenticação

Execute este procedimento na primeira instância do Independent Gateway.

Você deve ter uma cópia do arquivo `pre-auth_idp_metadata.xml` que você criou a partir da configuração do Okta.

1. Altere o diretório:

   ```
   cd /etc/mellon
   ```

2. Crie os metadados do provedor de serviços. Execute o script `mellon_create_metadata.sh`. Você deve incluir a ID da entidade e a URL de retorno para sua organização no comando.

   A URL de retorno é conhecida como *URL de logon único* no Okta. O elemento final do caminho na URL de retorno é conhecido como o`MellonEndpointPath` no arquivo de configuração `mellon.conf` posteriormente neste procedimento. Neste exemplo, especificamos `sso` como o caminho do terminal.

   Por exemplo:

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

   O script retorna o certificado do provedor de serviços, a chave e os arquivos de metadados.

3. Renomeie os arquivos do provedor de serviços no diretório `mellon` para facilitar a leitura. Faremos referência a esses arquivos pelos seguintes nomes na documentação:

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

4. Copie o arquivo `pre-auth_idp_metadata.xml` para o mesmo diretório.

5. Altere a propriedade e as permissões em todos os arquivos no diretório `/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. Crie o diretório `/etc/mellon/conf.d`:

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

7. Crie o arquivo `global.conf` no diretório `/etc/mellon/conf.d`.

   Copie o conteúdo do arquivo conforme mostrado abaixo, mas atualize `Mel-lonCookieDomain` com seu nome de domínio raiz. Por exemplo, se o nome de domínio do Tableau for `tableau.example.com`, digitar `example.com` para o domínio raiz.

```
<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. Crie o arquivo `mellonmod.conf` no diretório `/etc/mellon/conf.d`.

   Este arquivo contém uma única diretiva que especifica a localização do arquivo `mod_auth_mellon.so`. O local no exemplo aqui é o local padrão do arquivo. Verifique se o arquivo está neste local ou altere o caminho nesta diretiva para corresponder ao local real de `mod_auth_mellon.so`:

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

Crie o aplicativo Tableau Server no Okta

1. No painel do Okta: **Aplicativos** > **Aplicativos** > **Navegar no catálogo de aplicativos**
2. Em **Procurar catálogo de integração de aplicativos**, pesquise `Tableau`, selecione o bloco do Tableau Server e clique em **Adicionar**.
3. Em **Adicionar Tableau Server** > **Configurações gerais**, insira um rótulo e clique em **Avançar**.
4. Em Opções de logon, selecione **SAML 2.0** role a página para baixo até Configurações de logon avançadas:
   - **ID da entidade SAML**: insira a URL pública, por exemplo, https://-tableau.example.com.
   - **Formato do nome de usuário do aplicativo**: e-mail
5. Clique no **link de metadados do provedor de identidade** para iniciar um navegador. Copie o link do navegador. Esse é o link que você usará ao configurar o Tableau no procedimento a seguir.
6. Clique em **Concluído**.
7. Atribua o novo aplicativo Tableau Server Okta ao seu usuário (usuário@example.com): clique no nome do usuário e atribua o aplicativo em **Atribuir aplicativo**.

Definir a configuração do módulo de autenticação no Tableau Server

Execute os seguintes comandos no Nó 1 do Tableau Server. Esses comandos especificam os locais dos arquivos de configuração do Mellon no computador remoto do Independent Gateway. Verifique novamente se os caminhos de arquivo especificados nesses comandos são mapeados para os caminhos e o local do arquivo no computador remoto do Independent Gateway.

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

Para reduzir o tempo de inatividade, não aplique as alterações até ativar o SAML, conforme descrito na próxima seção.

Habilite SAML no Tableau Server para IdP

Execute este procedimento no nó 1 do Tableau Server.

1. Baixe os metadados do aplicativo Tableau Server no Okta. Use o link que você salvou no procedimento anterior:

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

2. Copie um certificado TLS e o arquivo de chave relacionado para o Tableau Server. O arquivo de chave deve ser uma chave RSA. Para obter mais informações sobre o certificado e requisitos do SAML, consulte *Requisitos do SAML* (Linux).

   Para simplificar o gerenciamento e a implantação de certificados e como prática recomendada de segurança, recomendamos o uso de certificados gerados por uma

autoridade de certificação (CA) de terceiros confiável. Como alternativa, você pode gerar certificados autoassinados ou usar certificados de uma PKI para TLS.

Se você não tiver um certificado TLS, poderá gerar um certificado autoassinado usando o procedimento incorporado a seguir.

Gerar um certificado autoassinado

Execute este procedimento no nó 1 do Tableau Server.

a. Gere a chave de autoridade de certificação raiz (CA) de assinatura:

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

b. Crie o certificado CA raiz:

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

Você será solicitado a inserir valores para os campos do certificado. Por exemplo:

```
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. Crie o certificado e a chave relacionada (`server-saml.csr` e `server-saml.key` no exemplo abaixo) para o computador Postgres. O nome do assunto

do certificado deve corresponder ao nome do host público do host do Tableau. O nome do assunto é definido com a opção `-subj` e o formato`"/CN=<host-name>"`, por exemplo:

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

d. Assine o novo certificado com o certificado CA que você criou antes. O comando a seguir também produz o certificado no formato `crt`:

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

e. Converta o arquivo de chave em RSA. O Tableau requer um arquivo de chave RSA para SAML. Para converter a chave, execute o comando a seguir:

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

3. Configure o SAML. Execute o seguinte comando, especificando seu ID de entidade e URL de retorno, e os caminhos para o arquivo de metadados, arquivo de certificado e arquivo de chave:

```
tsm authentication saml configure --idp-entity-id "https://-
tableau.example.com" --idp-return-url "https://-
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 sua organização estiver executando o Tableau Desktop 2021.4 ou posterior, você deve executar o seguinte comando para habilitar a autenticação por meio dos servidores proxy reverso.

As versões do Tableau Desktop 2021.2.1 - 2021.3 funcionarão sem executar este comando, desde que seu módulo de pré-autenticação (por exemplo, Mellon) esteja configurado para permitir a preservação de cookies de domínio de nível superior.

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

5. Aplique as alterações configuração:

```
tsm pending-changes apply
```

Reiniciar o serviço tsig-httpd

À medida que a implantação do Tableau Server aplica as alterações, entre novamente no computador do Tableau Server Independent Gateway e execute os seguintes comandos para reiniciar o serviço tsig-httpd:

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

Validar a funcionalidade SAML

Para validar a funcionalidade SAML de ponta a ponta, entre no Tableau Server com a URL pública (por exemplo, https://tableau.example.com) com a conta de administrador do Tableau que você criou no início deste procedimento.

Se o TSM não iniciar ("erro de gateway") ou se você receber erros de navegador ao tentar se conectar, consulte Solucionar problemas o Tableau Server Independent Gateway.

Configurar o módulo de autenticação na segunda instância do Independent Gateway

Depois de configurar com êxito a primeira instância do Independent Gateway, implante a segunda instância. O exemplo aqui é o processo final para instalar o cenário AWS/Mellon/Okta descrito neste tópico. O procedimento pressupõe que você já instalou o Independent

Gateway na segunda instância conforme descrito neste tópico anteriormente (Instalar o Independent Gateway).

O processo de implantação do segundo Independent Gateway requer as seguintes etapas:

1. Na segunda instância do Independent Gateway: instale o módulo de autenticação Mellon.

   Não configure o módulo de autenticação Mellon conforme descrito anteriormente neste tópico. Em vez disso, você deve clonar a configuração conforme descrito nas etapas subsequentes.

2. Na (primeira) instância configurada do Independent Gateway:

   Faça uma cópia tar da configuração Mellon existente. O backup tar preservará toda a hierarquia de diretórios e permissões. Execute os seguintes comandos:

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

   Copie `mellon.tar` para a segunda instância do Independent Gateway.

3. Na segunda instância do Independent Gateway:

   Extraia ("descompacte") o arquivo tar para a segunda instância no diretório `/etc`. Execute os seguintes comandos:

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

4. No nó 1 da implantação do Tableau Server: atualize o arquivo de conexão (`tsig.json`) com as informações de conexão do segundo Independent Gateway. Você precisará recuperar a chave de autenticação conforme descrito neste tópico anteriormente (Instalar Independent Gateway).

   Um arquivo de conexão de exemplo (`tsig.json`) é mostrado aqui:

```
{
"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. No nó 1 da implantação do Tableau Server: execute os seguintes comandos para atualizar a configuração:

   ```
   tsm stop

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

   tsm start
   ```

6. Nas duas instâncias do Independent Gateway: conforme o Tableau Server está iniciando, reinicie o processo `tsig-httpd`:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

7. Em AWS **EC2>Grupos de destino** : atualize o grupo de destino para incluir a instância do EC2 que executa a segunda instância do Independent Gateway.

Selecione o grupo de destinos que você acabou de criar e clique na guia Destinos:

- Clique em **Editar**.
- Selecione a instância do EC2 do segundo computador do Independent Gateway e clique em **Adicionar ao registrado**. Clique em **Salvar**.

Parte 6 - Configuração pós-instalação

Configurar SSL/TLS do balanceador de carga para o Tableau Server

Algumas organizações exigem um canal de criptografia de ponta a ponta do cliente para o serviço de back-end. A arquitetura de referência padrão, conforme descrito até este ponto, especifica SSL do cliente para o balanceador de carga em execução na camada da Web de sua organização.

Esta seção descreve como configurar o SSL/TLS para o Tableau Server e o Independent Gateway no exemplo de arquitetura de referência da AWS. Para obter um exemplo de configuração descrevendo como configurar SSL/TLS no Apache na arquitetura de referência da AWS, consulte Exemplo: configurar SSL/TLS na arquitetura de referência da AWS.

No momento, não há suporte para TLS nos processos de back-end do Tableau Server executados no intervalo 8000-9000. Para habilitar o TLS, você deve configurar o Independent Gateway com uma conexão de retransmissão para o Tableau Server.

Este procedimento descreve como habilitar e configurar o TLS no Independent Gateway para o Tableau Server e do Tableau Server para o Independent Gateway. O procedimento criptografa o tráfego de retransmissão em HTTPS/443 e o tráfego de manutenção em HTTPS/21319.

Os procedimentos do Linux em todo este exemplo mostram comandos para distribuições do tipo RHEL. Especificamente, os comandos aqui foram desenvolvidos com a distribuição Amazon Linux 2. Se você estiver executando a distribuição do Ubuntu, edite os comandos de forma apropriada.

A orientação aqui é prescritiva para a arquitetura de referência de exemplo específica da AWS, conforme apresentado neste Guia. Portanto, as configurações opcionais não estão incluídas. Para obter a documentação de referência completa, consulte *Configurar TLS no Independent Gateway* (Linux).

Antes de configurar o TLS

Execute as configurações de TLS fora do horário comercial. A configuração requer pelo menos uma reinicialização do Tableau Server. Se você estiver executando uma implantação completa de arquitetura de referência de quatro nós, a reinicialização pode demorar um pouco.

- Verifique se os clientes podem se conectar ao Tableau Server por HTTP. A configuração de TLS com Independent Gateway é um processo de várias etapas e pode exigir solução de problemas. Portanto, recomendamos começar com uma implantação totalmente operacional do Tableau Server antes de configurar o TLS.
- Colete certificados TLS/SSL, chaves e ativos relacionados. Você precisará de certificados SSL para os Independent Gateways e para o Tableau Server. Para simplificar o gerenciamento e a implantação de certificados e como prática recomendada de segurança, recomendamos o uso de certificados gerados por uma autoridade de certificação (CA) de terceiros confiável. Como alternativa, você pode gerar certificados autoassinados ou usar certificados de uma PKI para TLS.

  A configuração de exemplo neste tópico usa os seguintes nomes de ativos como ilustração:
  - `tsig-ssl.crt`: o certificado TLS/SSL para Independent Gateway.
  - `tsig-ssl.key`: a chave privada para`tsig-ssl.crt` no Independent Gateway.
  - `ts-ssl.crt`: o certificado TLS/SSL para o Tableau Server.
  - `ts-ssl.key`: a chave privada para`tsig-ssl.crt` no Tableau Server.

  - `tableau-server-CA.pem`: o certificado raiz da CA que gera os certificados para os computadores do Tableau Server. Esse certificado geralmente não é necessário se você estiver usando certificados de terceiros confiáveis.
  - `rootTSIG-CACert.pem`: o certificado raiz da CA que gera os certificados para os computadores do Independent Gateway. Esse certificado geralmente não é necessário se você estiver usando certificados de terceiros confiáveis.
  - Existem outros certificados e ativos de arquivos de chave necessários para SAML que são detalhados na Parte 5 deste Guia.
  - Se sua implementação exigir o uso de um arquivo de cadeia de certificados, consulte o artigo da Base de Conhecimento, Configurar TLS no Independent Gateway ao usar um certificado que tenha uma cadeia de certificados .
- Verifique se você tem acesso ao IdP. Se você estiver usando um IdP para autenticação, provavelmente precisará fazer alterações nos URLs de destinatário e destino no IdP depois de configurar o SSL/TLS.

Configurar computadores de Independent Gateway para TLS

A configuração do TLS pode ser um processo propenso a erros. Como a solução de problemas em duas instâncias do Independent Gateway pode ser demorada, recomendamos habilitar e configurar o TLS na implantação do EDG com apenas um Independent Gateway. Depois de validar que o TLS funciona na implantação, configure o segundo computador do Independent Gateway.

Etapa 1: distribuir certificados e chaves para o computador Independent Gateway

Você pode distribuir os ativos para qualquer diretório arbitrário, desde que o usuário tsig-httpd tenha acesso de leitura aos arquivos. Os caminhos para esses arquivos são referenciados em outros procedimentos. Usaremos os caminhos de exemplo em `/etc/ssl`, como mostrado abaixo, ao longo do tópico.

1. Crie um diretório para a chave privada:

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

2. Copie o certificado e os arquivos key para os seguintes caminhos `/etc/ssl`: Por exemplo,

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

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

3. (Opcional) Se você estiver usando um certificado autoassinado ou PKI para SSL/TLS no Tableau Server, também deverá copiar o arquivo de certificado raiz da CA para o computador do Independent Gateway. Por exemplo,

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

Etapa 2: atualizar as variáveis ambientais para TLS

Você deve atualizar as variáveis ambientais de porta e protocolo para a configuração do Independent Gateway.

Altere esses valores atualizando o arquivo,`/etc/opt/tableau/tableau_tsig/environment.bash`, do seguinte modo :

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

Etapa 3: atualizar o arquivo de configuração de stub para o protocolo HK

Edite manualmente o arquivo de configuração stub (`/var/opt/tableau/tableau_tsig/config/httpd.conf.stub`) para definir as diretivas httpd Apache relacionadas ao TLS para o protocolo de manutenção (HK).

O arquivo de configuração stub inclui um bloco de diretivas relacionadas a TLS que são comentadas com um`#TLS#` marcador. Remova os marcadores das diretivas conforme mostrado no exemplo abaixo. Observe que o exemplo mostra o uso do certificado CA raiz para o certificado SSL usado no Tableau Server com a opção `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>
```

Essas alterações serão perdidas se você reinstalar o Independent Gateway. Recomendamos fazer uma cópia de segurança.

Etapa 4: copie o arquivo stub e reinicie o serviço

1. Copie o arquivo que você atualizou na última etapa, para atualizar o httpd.conf com as alterações:

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

2. Reinicie o serviço do Independent Gateway:

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

Após a reinicialização, o Independent Gateway ficará inoperante até que você execute o próximo conjunto de etapas no Tableau Server. Depois de concluir as etapas no Tableau Server, o Independent Gateway captará as alterações e ficará online.

Configurar o nó 1 do Tableau Server para TLS

Execute estas etapas no Nó 1 em sua implantação do Tableau Server:

Etapa 1: copie certificados e chaves e interrompa o TSM

1. Verifique se você tem os certificados e chaves "SSL externo" do Tableau Server copiados para o Nó 1.
2. Para minimizar o tempo de inatividade, recomendamos interromper o TSM, executar as etapas a seguir e iniciar o TSM após a aplicação das alterações:

   ```
   tsm stop
   ```

Etapa 2: definir ativos de certificado e habilitar a configuração do Independent Gateway

1. Especifique o local do certificado e dos arquivos de chave para o Independent Gateway. Esses caminhos fazem referência ao local nos computadores do Independent Gateway. Observe que este exemplo assume que o mesmo certificado e par de chaves são usados para proteger HTTPS e tráfego de manutenção:

   ```
   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. Habilite os protocolos TLS para HTTPS e HK para Independent Gateway:

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

3. (Opcional) Se você estiver usando um certificado autoassinado ou PKI para SSL/TLS no Independent Gateway, deverá carregar o arquivo de certificado raiz da CA. O arquivo de certificado raiz CA é o certificado raiz que foi usado para gerar os certificados para os computadores do Independent Gateway. Por exemplo,

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

4. (Opcional) Se você estiver usando um certificado autoassinado ou PKI para SSL/TLS no Tableau Server, também deverá copiar o arquivo de certificado raiz da CA para o diretório `/etc/ssl/certs` do Independent Gateway. O arquivo de certificado raiz CA é o certificado raiz usado para gerar os certificados para os computadores do Tableau Server. Depois de copiar o certificado para o Independent Gateway, você deve especificar o local do certificado no Nó 1 com o seguinte comando tsm. Por exemplo,

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

5. (Opcional: apenas para fins de teste) Se você estiver usando o compartilhamento de certificados autoassinados ou PKI entre computadores e, portanto, os nomes das entidades nos certificados não corresponderem aos nomes dos computadores, será necessário desabilitar a verificação de certificados.

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

Etapa 3: habilitar "SSL externo" para o Tableau Server e aplicar as alterações

1. Habilite e configure "SSL externo" no Tableau Server:

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

2. Aplique as alterações.

   ```
   tsm pending-changes apply
   ```

Etapa 4: atualize o arquivo JSON de configuração do gateway e inicie o tsm

1. Atualize o arquivo de configuração do Independent Gateway (por exemplo,`tsig.json`) no lado do Tableau Server para especificar o`https` protocolo para os objetos do

Independent Gateway:

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

2. Remova (ou comente) as informações de conexão para a segunda instância do Independent Gateway. Certifique-se de verificar o JSON em um editor externo antes de salvá-lo.

   Depois de configurar e validar o TLS para a instância única do Independent Gateway, você atualizará esse arquivo JSON com as informações de conexão para a segunda instância do Independent Gateway.

3. Execute o comando a seguir para atualizar a configuração do Independent Gateway:

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

4. Inicie o TSM.

   ```
   tsm start
   ```

5. Enquanto o TSM está iniciando, faça login na instância do Independent Gateway e reinicie o serviço `tsig-httpd`:

   ```
   sudo su - tableau-tsig

   systemctl --user restart tsig-httpd

   exit
   ```

Atualizar URLs do módulo de autenticação IdP para HTTPS

Se você configurou um provedor de identidade externo para o Tableau, provavelmente precisará atualizar as URLs de retorno no painel administrativo do IdP.

Por exemplo, se você estiver usando um aplicativo de pré-autenticação Okta, precisará atualizar o aplicativo para usar o protocolo HTTPS para a URL do destinatário e a URL de destino.

Configurar o balanceador de carga AWS para HTTPS

Se você estiver implantando com o balanceador de carga AWS conforme documentado neste guia, reconfigure o balanceador de carga AWS para enviar tráfego HTTPS para os computadores executando Independent Gateway:

1. Exclua o grupo de destino HTTP existente:

   Em **Grupos de destino**, selecione o grupo de destino HTTP que foi configurado para o balanceador de carga, clique em **Ações** e, em seguida, clique em **Excluir**.

2. Crie o grupo de destino HTTPS:

   Grupos de destino > **Criar grupo de destino**

   - Selecione "Instâncias"
   - Insira um nome para o grupo de destino, por exemplo `TG-internal-HTTPS`
   - Selecione o VPC
   - Protocolo: HTTPS 443
   - Em **Verificações de integridade** > **Configurações avançadas de verificações de integridade > Códigos de sucesso** , anexe a lista de códigos para ler: `200,303`.
   - Clique em **Criar**.

3. Selecione o grupo de destinos que você acabou de criar e clique na guia **Destinos**:

   - Clique em **Editar**
   - Selecione a instância EC2 que executa o Tableau Server Independent Gateway que você configurou e clique em **Adicionar para registrada**.
   - Clique em **Salvar**.

4. Depois que o grupo de destino é criado, você deve habilitar a aderência:

   - Abra a página Balanceador de carga da AWS (**EC2**> **Balanceadores de carga**> **Grupos de destinos**), selecione a instância do balanceador de carga que você acabou de configurar. No menu **Ação**, selecione **Editar atributos**.

- Na página **Editar atributos**, selecione **Aderência**, especifique uma duração de `1 day` e, em seguida, **Salvar alterações**.

5. No balanceador de carga, atualize as regras do ouvinte. Selecione o balanceador de carga que você configurou para esta implantação e clique na guia **Ouvintes**

   - Para **HTTP: 80**, clique em **Exibir/editar regras**. Na página **Regras**, clique no ícone de edição (uma vez no topo da página e depois novamente na regra) para editar a regra. Exclua a regra THEN existente e substitua-a clicando em **Adicionar ação** > **Redirecionar para....** Na configuração THEN resultante, especifique `HTTPS` e a porta `443` e deixe as outras opções com as configurações padrão. Salve a configuração e clique em **Atualizar**.
   - Para **HTTPS:443**, clique em **Exibir/editar regras**. Na página **Regras**, clique no ícone de edição (uma vez no topo da página e depois novamente na regra) para editar a regra. Exclua a regra THEN existente e substitua-a clicando em **Adicionar ação** > **Encaminhar para....** Especifique o grupo de destino para o grupo HTTPS que você acabou de criar. Em **Aderência em nível de grupo**, ative a aderência e defina a duração para 1 dia. Salve a configuração e clique em **Atualizar**.

6. No balanceador de carga, atualize o tempo limite de inatividade para 400 segundos. Selecione o balanceador de carga que você configurou para esta implantação e clique em **Ações** > **Editar atributos**. Defina o **Tempo limite de inatividade** para `400` segundos e, em seguida, clique em **Salvar**.

Validar TLS

Para validar a funcionalidade TLS, entre no Tableau Server com a URL pública (por exemplo, https://tableau.example.com) com a conta de administrador do Tableau que você criou no início deste procedimento.

Se o TSM não estiver iniciando ou você receber outros erros, consulte Solucionar problemas o Tableau Server Independent Gateway.

Configurar a segunda instância do Independent Gateway para SSL

Depois de configurar com êxito a primeira instância do Independent Gateway, implante a segunda instância.

O processo de implantação do segundo Independent Gateway requer as seguintes etapas:

1. Na (primeira) instância configurada do Independent Gateway: copie os seguintes arquivos para os locais correspondentes na segunda instância do Independent Gateway:
   - `/etc/ssl/certs/tsig-ssl.crt`
   - `/etc/ssl/private/tsig-ssl.key` (Você precisará criar o diretório `private` na segunda instância).
   - `/var/opt/tableau/tableau_tsig/config/httpd.conf.stub`
   - `/etc/opt/tableau/tableau_tsig/environment.bash`

2. No nó 1 da implantação do Tableau Server: atualize o arquivo de conexão (`tsig.json`) com as informações de conexão do segundo Independent Gateway.

   Um arquivo de conexão de exemplo (`tsig.json`) é mostrado aqui:

```
{
"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. No nó 1 da implantação do Tableau Server: execute os seguintes comandos para atualizar a configuração:

   ```
   tsm stop
   ```

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

   ```
   tsm start
   ```

4. Nas duas instâncias do Independent Gateway: conforme o Tableau Server está iniciando, reinicie o processo `tsig-httpd` em ambas as instâncias do Independent Gateway:

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

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

   ```
   exit
   ```

5. Em AWS **EC2>Grupos de destino** : atualize o grupo de destino para incluir a instância do EC2 que executa a segunda instância do Independent Gateway.

   Selecione o grupo de destinos que você acabou de criar e clique na guia Destinos:

   - Clique em **Editar**.
   - Selecione a instância do EC2 do segundo computador do Independent Gateway e clique em **Adicionar ao registrado**. Clique em **Salvar**.

Configurar SSL para Postgres

Opcionalmente, você pode configurar SSL (TLS) para a conexão Postgres para a conexão do repositório externo no Tableau Server.

Para simplificar o gerenciamento e a implantação de certificados e como prática recomendada de segurança, recomendamos o uso de certificados gerados por uma autoridade de certificação (CA) de terceiros confiável. Como alternativa, você pode gerar certificados autoassinados ou usar certificados de uma PKI para TLS.

Este procedimento descreve como usar o OpenSSL para gerar um certificado autoassinado no host Postgres em uma distribuição Linux como RHEL na arquitetura de referência de exemplo da AWS.

Depois de gerar e assinar o certificado SSL, você deve copiar o certificado CA para o host do Tableau.

No host que executa o Postgres:

1. Gere a chave de autoridade de certificação raiz (CA) de assinatura:

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

2. Crie o certificado CA raiz:

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

   Você será solicitado a inserir valores para os campos do certificado. Por exemplo:

   ```
   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. Crie o certificado e a chave relacionada (`server.csr` e `server.key` no exemplo abaixo) para o computador Postgres. O nome do assunto do certificado deve

corresponder ao nome DNS privado EC2 do host Postgres. O nome do assunto é definido com a opção `-subj` e o formato `"/CN=<private DNS name>"`, por exemplo:

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

4. Assine o novo certificado com o certificado CA que você criou na etapa 2. O comando a seguir também produz o certificado no formato `crt`:

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

5. Copie os arquivos crt e de chave para o Postgres `/var/lib/pgsql/13/data/` caminho:

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

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

6. Mudar para usuário raiz:

   ```
   sudo su
   ```

7. Defina permissões nos arquivos cer e key. Execute os seguintes comandos:

   ```
   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. Atualize o arquivo de configuração pg_haba, `/var/lib/pgsql/13/data/pg_hba.conf` para especificar a confiança md5:

   Altere as instruções de conexão existentes de

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

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

para

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

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

9. Atualize o arquivo postgresql, `/var/lib/pgsql/13/data/postgresql.conf`, adicionando esta linha:

   ```
   ssl = on
   ```

10. Saia do modo de usuário raiz:

    ```
    exit
    ```

11. Reinicie o Postgres:

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

Opcional: habilite a validação de confiança do certificado no Tableau Server para Postgres SSL

Se você seguiu o procedimento de instalação na Parte 4 - Instalar e configurar o Tableau Server, o Tableau Server é configurado com SSL opcional para a conexão Postgres. Isso significa que configurar o SSL no Postgres (como descrito acima) resultará em uma conexão criptografada.

Se você deseja exigir a validação de confiança do certificado para a conexão, execute o seguinte comando no Tableau Server para reconfigurar a conexão do host Postgres:

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

Em que `<filename>.json` é o arquivo de conexão descrito em Configurar Postgres externo. E `CACert.pem` é o arquivo de certificado CA para o certificado SSL/TLS usado pelo Postgres.

Opcional: verifique a conectividade SSL

Para verificar a conectividade SSL, você deve:

- Instale o cliente Postgres no Nó 1 do Tableau Server.
- Copie o certificado raiz que você criou no procedimento anterior para o host do Tableau.
- Conecte-se ao servidor Postgres do Nó 1

Instale o cliente Postgres no Nó 1

Este exemplo mostra como instalar a versão Postgres 13.4. Instale a mesma versão que você está executando para o repositório externo.

1. No nó 1, crie e edite o arquivo, pgdg.repo. no caminho `/etc/yum.repos.d`. Preencha o arquivo com as seguintes informações de configuração.

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

2. Instale o cliente Postgres:

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

Copie o certificado raiz para o nó 1

Copie o certificado CA (`pgsql-rootCACert.pem`) para o host do Tableau:

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

Conecte-se ao host Postgres por SSL no Nó 1

Execute o seguinte comando do Nó 1, especificando o endereço IP do host do servidor Postgres e o certificado CA raiz:

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

Por exemplo:

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

O Postgres solicitará a senha. Após o login bem-sucedido, o shell retornará:

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

Configurar notificações de SMTP e eventos

O Tableau Server envia notificações e-mail para administradores e usuários. Para habilitar isso, você deve configurar o Tableau Server para enviar e-mail ao seu servidor de e-mail. Você também deve especificar os tipos de eventos, limites e informações de assinatura que deseja enviar.

Para a configuração inicial de SMTP e notificações, recomendamos usar o modelo do arquivo de configuração abaixo para criar um arquivo json. Além disso, é possível definir qualquer chave de configuração única listada abaixo com a sintaxe descrita em *tsm configuration set* (Linux).

Execute este procedimento no Nó 1 em sua implantação do Tableau Server:

1. Copie o modelo json abaixo em um arquivo. Personalize o arquivo com suas opções de configuração de SMTP e as notificações de assinatura e alerta para sua organização.

    - Para ver uma lista e descrição de todas as opções SMTP, consulte a *referência de configuração CLI SMTP* (Linux).
    - Para ver uma lista e descrição de todas as opções de evento de notificação, consulte a seção CLI de *Configurar notificação de evento de servidor* (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. Execute `tsm settings import -f file.json` para passar o arquivo json ao Tableau Services Manager.
3. Execute o comando `tsm pending-changes apply` para aplicar as alterações.
4. Execute o `tsm email test-smtp-connection` para exibir e verificar a configuração da conexão.

Instalar o driver do PostgreSQL

Para exibir exibições de administrador no Tableau Server, o driver PostgreSQL deve ser instalado no Node1 da implantação do Tableau Server.

1. Vá para a página download do driver do Tableau e copie a URL do arquivo jar PostgreSQL.
2. Execute o seguinte procedimento em cada nó da implantação do Tableau:
    - Crie o seguinte caminho de arquivo:

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

    - No novo caminho, baixe a versão mais recente do arquivo jar PostgreSQL: Por exemplo:

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

3. No nó inicial, reinicie o Tableau Server:

   ```
   tsm restart
   ```

Configurar política de senha forte

Se você não estiver implantando o Tableau Server com uma solução de autenticação IdP, recomendamos fortalecer a segurança da política de senha padrão do Tableau.

Se você estiver implantando o Tableau Server com um IdP, deverá gerenciar as políticas de senha com o IdP.

O procedimento a seguir inclui a configuração json para definir a política de senha no Tableau Server. Para obter mais informações sobre as opções abaixo, consulte *Autenticação local* (Linux).

1. Copie o modelo json abaixo em um arquivo. Preencha os valores principais com a configuração da política de senha.

```
{
 "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. Execute `tsm settings import -f file.json` para passar o arquivo json ao Tableau Services Manager e configurar o Tableau Server.

3. Execute o comando `tsm pending-changes apply` para aplicar as alterações.

Parte 7 - Validação, ferramentas e solução de problemas

Essa parte inclui etapas de validação pós-instalação e orientações para solução de problemas.

Validação do sistema de failover

Depois de configurar sua implantação, recomendamos a execução de testes simples de failover para validar a redundância do sistema.

Recomendamos executar as seguintes etapas para validar a funcionalidade de failover:

1. Encerre a primeira instância do Independent Gateway (TSIG1). Todo o tráfego de entrada deve ser roteado pela segunda instância do Independent Gateway (TSIG2).
2. Reinicie o TSIG1 e desligue o TSIG2. Todo o tráfego de entrada deve ser roteado pelo TSIG1.
3. Reinicie o TSIG2.

4. Desligue o nó 1 do Tableau Server. Todo o tráfego do serviço Vizportal/Application fará failover para o Nó 2.

   Observação a partir de setembro de 2022, a alta disponibilidade do nó 1 foi comprometida nas versões do Tableau Server 2021.4 e posteriores. As conexões do cliente falharão se o Nó 1 estiver inativo. Esse problema foi corrigido nestas versões de manutenção:

   - 2021.4.15 e posteriores
   - 2022.1.11 e posteriores
   - 2023.1.3 e posterior

> Para garantir que a instalação do Tableau Server usando ativações ATR terá um período de carência de 72 horas após a falha inicial do nó, instale ou atualize para uma dessas versões. Para obter mais detalhes, consulte O Tableau Server HA usando ATR não tem período de carência após a falha inicial do nó na base de dados de conhecimento do Tableau.

5. Reinicie o Node1 e desligue o Node 2. Todo o tráfego do serviço Vizportal/Application fará failover para o Nó 1.
6. Reinicie o Nó 2.

Nesse contexto, "desligar" ou "reiniciar" é feito desligando o sistema operacional ou a máquina virtual sem tentar um desligamento normal do aplicativo antes. O objetivo é simular uma falha de hardware ou máquina virtual.

A etapa mínima de validação para cada teste de failover é autenticar com um usuário e executar operações básicas de exibição.

Você pode receber um erro de navegador "Solicitação inválida" ao tentar entrar após uma falha simulada. Você pode ver esse erro mesmo se limpar o cache no navegador. Frequentemente, esse problema ocorre quando o navegador está armazenando dados em cache de uma sessão anterior do IdP. Se esse erro persistir mesmo depois de limpar o cache do navegador local, valide o cenário do Tableau conectando-se em um navegador diferente.

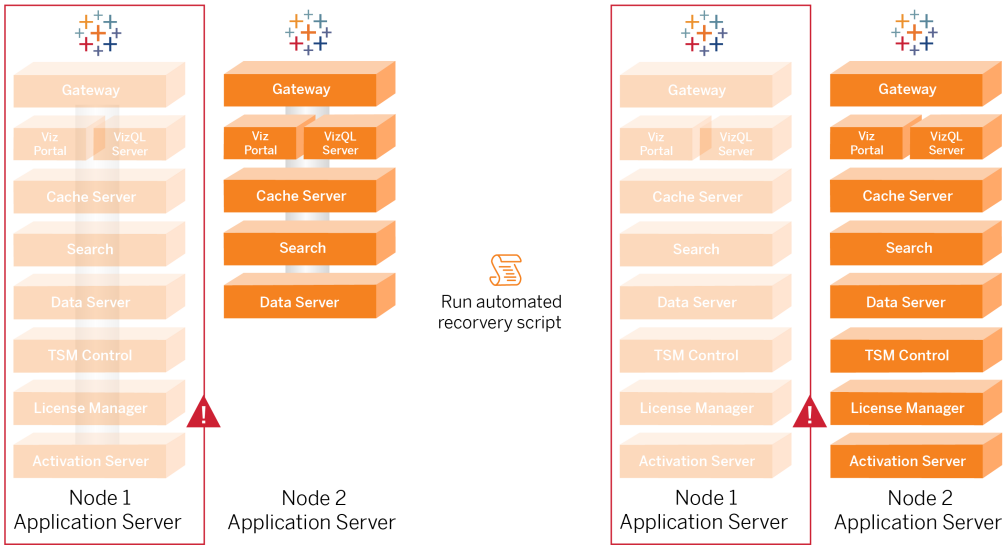
Recuperação automatizada de nó inicial

Tableau Server versão 2021.2.4 e posterior incluem um script de recuperação de nó inicial automatizado,`auto-node-recovery`, no diretório de scripts (`/app/tableau_server/packages/scripts.<version>`)

Se houver um problema com o nó inicial e você tiver processos redundantes no Nó 2, não há garantia de que o Tableau Server continuará em execução. O Tableau Server pode continuar em execução por até 72 horas após uma falha inicial do nó, antes que a falta do serviço de licenciamento afete outros processos. Se afetar, seus usuários ainda poderão fazer logon, ver

e usar seus conteúdos depois da falha no nó inicial, mas você não poderá reconfigurar o Tableau Server, pois não tem acesso ao Controlador de administração.

Mesmo quando configurado com processos redundantes, é possível que o Tableau Server não continue a funcionar após a falha do nó inicial.



Para recuperar a falha do nó inicial (Nó 1)

1. Fazer logon no Nó 2 do Tableau Server.
2. Mude para o diretório de scripts:

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

3. Execute o seguinte comando para iniciar o script:

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

   Onde `<license keys>` é uma lista separada por vírgulas (sem espaços) das chaves de licença para sua implementação. Se você não tiver acesso às suas chaves de licença, visite o Portal do cliente do Tableau para recuperá-las. Por exemplo:

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

O script de recuperação automática do nó executará cerca de 20 etapas para recuperar serviços para o Nó 2. Cada etapa é exibida no terminal à medida que o script avança. Status mais detalhado é registrado em `/data/tableau_data/logs/app-controller-move.log`. Na maioria dos ambientes, o script leva entre 35 e 45 minutos para ser concluído.

Solução de problemas de recuperação de nó inicial

Se a recuperação do nó falhar, você pode achar útil executar o script interativamente para permitir ou proibir etapas discretas no processo. Por exemplo, se o script falhar em parte do processo, você pode revisar o arquivo de registro, fazer alterações na configuração e, em seguida, executar o script novamente. Ao executar no modo interativo, você pode pular todas as etapas até chegar à etapa que falhou.

Para executar no modo interativo, adicione`-i` mude para o argumento do script.

Recompilação do nó com falha

Depois de executar o script, o Nó 2 executará todos os serviços que estavam anteriormente no host do Nó 1 com falha. Para adicionar o nó 4, você precisa implantar um novo host do Tableau Server com o arquivo de bootstrap e configurá-lo como fez para o Nó 2 original, conforme especificado na Parte 4. Consulte Configurar o Nó 2.

switchto

Switchto é um script do Tim que torna mais fácil alternar entre as janelas.

1. Copie o seguinte código em um arquivo chamado`switchto` no diretório inicial do seu host bastião.

   ```
   #!/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. Atualize os endereços IP no script para mapear para suas instâncias EC2 e, em seguida, salve o arquivo.

3. Aplique permissões ao arquivo de script:

   ```
   sudo chmod +x switchto
   ```

Uso:

Para alternar para um host, execute os comandos a seguir:

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

Por exemplo, para mudar para o Nó 1, execute o seguinte comando:

```
./switchto node1
```

Solucionar problemas o Tableau Server Independent Gateway

A configuração de Independent Gateway, Okta, Mellon e SAML no Tableau Server pode ser um processo propenso a erros. A causa raiz mais comum de falhas é um erro de cadeia de caracteres. Por exemplo, uma barra final (`/`) nas URLs do Okta especificadas durante a configuração pode causar um erro de incompatibilidade relacionado à declaração SAML. Isso é apenas um exemplo. Há muitas oportunidades durante a configuração para inserir uma cadeia de caracteres incorreta em qualquer um dos aplicativos.

Reiniciar o serviço tableau-tsig

Sempre inicie (e termine) a solução de problemas reiniciando o serviço tableau-tsig nos computadores do Gateway Independente. Reiniciar esse serviço é rápido e geralmente aciona a configuração atualizada para carregar do Tableau Server.

Execute os comandos a seguir para atualizar o computador do Independent Gateway:

```
sudo su - tableau-tsig

systemctl --user restart tsig-httpd

exit
```

Encontrar cadeias de caracteres incorretas

Se você cometeu um erro de cadeia de caractere (erro de copiar/colar, cadeia de caractere truncada etc.), reserve um tempo para percorrer cada uma das configurações que você configurou:

- Configuração de pré-autenticação do Okta. Revise cuidadosamente as URLs que você definiu. Procure por barras à direita. Verifique HTTP vs HTTPS.
- Histórico de shell para configuração de SAML no nó 1. Reveja o comando `tsm authentication saml configure` que você executou. Verifique se todas as URLs correspondem àquelas que você configurou no Okta. Enquanto estiver revisando o histórico do shell do Nó 1, verifique se os comandos `tsm configuration set` que especificam os caminhos do arquivo de configuração do Mellon mapeiam exatamente para os caminhos do arquivo onde você copiou os arquivos no Independent Gateway.
- Configuração do Mellon no Independent Gateway. Revise o histórico do shell para verificar se você criou os metadados com a mesma cadeia de caractere de URL que você configurou no Okta e no Tableau SAML. Verifique se todos os caminhos especificados em `/etc/mellon/conf.d/global.conf` estão corretos e que `MellonCookieDomain` está definido para seu domínio raiz, não para seu subdomínio do Tableau.

Pesquisar registros relevantes

Se todas as cadeias de caracteres parecem estar configuradas corretamente, você deve inspecionar os registros em busca de erros.

O Tableau Server registra erros e eventos em dezenas de arquivos de registros diferentes. O Independent Gateway também registra em um conjunto de arquivos locais. Recomendamos inspecionar esses registros na seguinte ordem.

Arquivos de registro do Independent Gateway

O local padrão dos registros de arquivos de registro do Independent Gateway estão em `/var/opt/tableau/tableau_tsig/logs`.

- `access.log`: esse registro é útil na medida em que possui entradas que mostram conexões dos nós do Tableau Server. Se você estiver recebendo erros de gateway (não iniciará) ao tentar iniciar o TSM e não houver entradas no arquivo `access.log`, há um problema de conectividade principal. Sempre verifique a configuração do grupo de segurança da AWS como primeira etapa. Outro problema comum é um erro de digitação `tsig.json`. Se você fizer uma atualização para tsig.json, execute `tsm stop` antes de executar r `tsm topology external-services gateway update -c tsig.json`. Depois que o tsig.json for atualizado, execute `tsm start`.
- `error.log`: entre outras entradas, este registro inclui erros SAML e Mellon.

Arquivo de registro do tabadminagent do Tableau Server

O conjunto de arquivos `tabadminagent` (`tabadmincontroller`) são os únicos arquivos de registro relevantes para solucionar erros relacionados ao Independent Gateway.

Você deve localizar onde os erros do Independent Gateway foram registrados no `tabdminagent`. Esses erros podem estar em qualquer nó, mas estão apenas em um nó. Execute as etapas a seguir em cada nó no cluster do Tableau Server até encontrar a cadeia de caracteres “independent”:

1. Localize o local do arquivo de registro tabadminagent nos nós 1-4 do Tableau Server na configuração do EDG:

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

2. Abra o registro mais recente para ler:

   ```
   less tabadminagent_nodeN.log
   ```

   (substitua N pelo número do nó)

3. Pesquise todas as instâncias de “Independent” e “independent” - usando a seguinte cadeia de caracteres de pesquisa:

   ```
   /ndependent
   ```

   Se não houver correspondências, vá para o próximo nó e repita as etapas 1 a 3.

4. Quando você consegue uma correspondência: `Shift + G` para mover para baixo para obter as últimas mensagens de erro.

Recarregue o arquivo stub httpd

O Independent Gateway gerencia a configuração do httpd para Apache. Uma operação genérica que geralmente corrige problemas transitórios é recarregar o arquivo stub httpd que propaga a configuração subjacente do Apache. Execute os comandos a seguir em ambas as instâncias do Gateway Independente.

1. Copie o arquivo stub para httpd.conf:

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

2. Reinicie o serviço do Independent Gateway:

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

Excluir ou mover arquivos de registro

O Independent Gateway registra todos os eventos de acesso. Você precisará gerenciar o armazenamento de arquivos de registro para evitar o preenchimento de espaço em disco. Se o seu disco ficar cheio, o Independent Gateway não poderá gravar eventos de acesso e o serviço falhará. A seguinte mensagem será registrada em error.log no Independent Gateway:

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

Esta falha resultará em um status de `DEGRADED` para o nó `external` quando você executa `tsm status -v` no Nó 1 do Tableau. O nó `external` na saída de status refere-se ao Independent Gateway.

Para resolver esse problema, exclua ou mova os arquivos access.log do disco. Os arquivos de registro são armazenados em `/var/opt/tableau/tableau_tsig/logs`. Depois de limpar o disco, reinicie o serviço tableau-tsig.

Erros do navegador

Solicitação inválida: um erro comum neste cenário é um erro de "Solicitação inválida" da Okta. Frequentemente, esse problema ocorre quando o navegador está armazenando dados em cache de uma sessão anterior do Okta. Por exemplo, se você gerencia os aplicativos Okta como um administrador Okta e, em seguida, tenta acessar o Tableau usando uma conta habilitada para Okta diferente, os dados da sessão dos dados do administrador podem causar o erro "Solicitação inválida". Se esse erro persistir mesmo depois de limpar o cache do navegador local, tente validar o cenário do Tableau conectando-se em um navegador diferente.

Outra causa do erro "Solicitação inválida" é um erro de digitação em uma das muitas URLs que você insere durante os processos de configuração do Okta, Mellon e SAML. Verifique se você digitou tudo isso sem erros.

Muitas vezes o arquivo `error.log` no servidor do Independent Gateway especificará qual URL está causando o erro.

Não encontrado - A URL solicitada não foi encontrado neste servidor: este erro indica um dos muitos erros de configuração.

Se o usuário for autenticado com Okta e receber esse erro, é provável que você tenha carregado o aplicativo de pré-autenticação Okta para o Tableau Server quando configurou o SAML. Verifique se você tem os metadados do aplicativo Okta Tableau Server configurados no Tableau Server, e não os metadados do aplicativo de pré-autenticação Okta

Outras etapas de solução de problemas:

- Revise as configurações do aplicativo de pré-autenticação do Okta. Certifique-se de que os protocolos HTTP vs HTTPS estejam definidos, conforme especificado neste tópico.

- Reinicie o tsig-httpd em ambos os servidores do Independent Gateway.
- Verifique se `sudo apachectl configtest` retorna “Sintaxe OK” em ambos Independent Gateways.
- Verifique se o usuário de teste está atribuído a ambos os aplicativos no Okta.
- Verifique se a aderência está definida no balanceador de carga e grupos de destino associados

Verifique o TLS do Tableau Server para o Independent Gateway

Use o comando `wget` para verificar a conectividade e o acesso do Tableau Server para o Independent Gateway. Variações desse comando podem ajudá-lo a entender se os problemas de certificado estão causando problemas de conexão.

Por exemplo execute este comando `wget` para verificar o protocolo de manutenção (HK) do Tableau Server:

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

Crie a URL com o mesmo endereço de host que você incluiu para a opção de host do arquivo tsig.json. Especifique o protocolo `https` e anexe a URL com a porta HK `21319`.

Para verificar a conectividade e ignorar a verificação do certificado:

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

Para verificar se o certificado CA raiz para TSIG é válido:

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

Se o Tableau conseguir se comunicar, você ainda poderá receber erros relacionados ao conteúdo, mas não receberá erros relacionados à conexão. Se o Tableau não conseguir se conectar, comece verificando a configuração do protocolo nos grupos de firewall/segurança. Por

exemplo, as regras de entrada para o grupo de segurança em que reside o Independent Gateway devem permitir TCP 21319.

Apêndice - Caixa de ferramentas de implantação da AWS

Este tópico inclui ferramentas e opções de implantação alternativas para a arquitetura de referência quando implantada na AWS. Especificamente, este tópico descreve como automatizar o exemplo de implantação da AWS que é descrito em todo o EDG.

Script de instalação automatizada TabDeploy4EDG

O script TabDeploy4EDG automatiza a implementação da implantação do Tableau de quatro nós descrita na Parte 4 - Instalar e configurar o Tableau Server. Se você estiver seguindo o exemplo de implementação da AWS, conforme descrito neste Guia, poderá executar o TabDeploy4EDG.

Requisitos. Para executar o script, você deve preparar e configurar o ambiente AWS de acordo com o exemplo de implementação na Parte 3 - Preparação para a implantação corporativa do Tableau Server:

- VPC, sub-rede e grupos de segurança foram configurados conforme descrito. Os endereços IP não precisam corresponder aos mostrados na implementação de exemplo.
- Quatro instâncias EC2 executando as compilações mais recentes e atualizadas do AWS Linux 2
- O PostgreSQL está instalado e foi configurado conforme descrito em Instalar, configurar e PostgreSQL de tar.
- Um arquivo de backup de tar da Etapa 1 está na instância do EC2 em que o PostgreSQL está instalado, conforme descrito em Faça backup do tar PostgreSQL da etapa 1.
- A instância EC2 que executará o Nó 1 da implantação do Tableau Server foi configurada para se comunicar com o PostgreSQL conforme descrito em Parte 4 - Instalar

e configurar o Tableau Server.
- Você se conectou a cada instância do EC2 com uma sessão SSH do host Bastion.

O script leva cerca de 1,5 a 2 horas para instalar e configurar os quatro servidores Tableau. O script configura o Tableau de acordo com as configurações prescritas da arquitetura de referência. O script executa as seguintes ações:

- Restaura o backup da fase 1 do host PostgreSQL, se você especificar um caminho para o arquivo tar do host PostgreSQL.
- Elimina as instalações existentes do Tableau em todos os nós.
- Executa `sudo yum update` em todos os nós.
- Faz o download e copia o pacote rpm do Tableau para cada nó.
- Faz download e instala dependências para cada nó.
- Cria `/app/tableau_server` e instala o pacote em todos os nós.
- Instala o Nó 1 com um armazenamento de identidade local e configura o repositório externo com PostgreSQL.
- Executa a instalação de bootstrap e a configuração inicial do Nó 2 - Nó 4.
- Exclui o arquivo de inicialização e o arquivo de configuração para TabDeploy4EDG.
- Configura serviços no cluster do Tableau de acordo com as especificações da arquitetura de referência.
- Valida a instalação e retorna o status de cada nó.

Baixar e copiar o script para o host Bastion

1. Copie o script da página de amostras TabDeploy4EDG e cole o código em um arquivo chamado, `TabDeploy4EDG`.
2. Salve o arquivo no diretório inicial do host EC2 que está servindo como host Bastion.
3. Execute o seguinte comando para alterar o modo no arquivo para torná-lo executável:

```
sudo chmod +x TabDeploy4EDG
```

Executar TabDeploy4EDG

O TabDeploy4EDG deve ser executado no host Bastion. O script foi escrito com a suposição de que você está executando no contexto do agente de encaminhamento ssh, conforme descrito em Exemplo: conecte-se ao host Bastion na AWS . Se você não estiver executando com

o contexto do agente de encaminhamento ssh, serão solicitadas senhas durante o processo de instalação.

1. Crie, edite e salve um arquivo de registro (`registration.json`) O arquivo deve ser um arquivo json formatado corretamente. Copie e personalize o seguinte modelo:

   ```
   {
          "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. Execute o seguinte comando para gerar o arquivo de configuração do modelo:

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

3. Abra o arquivo de configuração para editar:

   ```
   sudo nano edg.config
   ```

   No mínimo, você deve adicionar os endereços IP de cada host EC2, um caminho para o arquivo de registro e uma chave de licença válida.

4. Quando terminar de editar o arquivo de configuração, salve-o e feche-o.

5. Para executar o TabDeploy4EDG, execute o seguinte comando:

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

Exemplo: automatizar a implantação da infra-estrutura da AWS com o Terraform

Esta seção descreve como configurar e executar o Terraform para implantar a arquitetura de referência EDG na AWS. O exemplo de configuração do Terraform apresentado aqui implanta um AWS VPC com sub-redes, grupos de segurança e instâncias do EC2 descritos na Parte 3 - Preparação para a implantação corporativa do Tableau Server.

Modelos de exemplo do Terraform estão disponíveis no site de exemplos do Tableau em https://help.tableau.com/samples/en-us/edg/edg-terraform.zip . Esses modelos devem ser configurados e personalizados para sua organização. O conteúdo de configuração fornecido nesta seção descreve as mudanças de modelo mínimas necessárias que você deve personalizar para implantar.

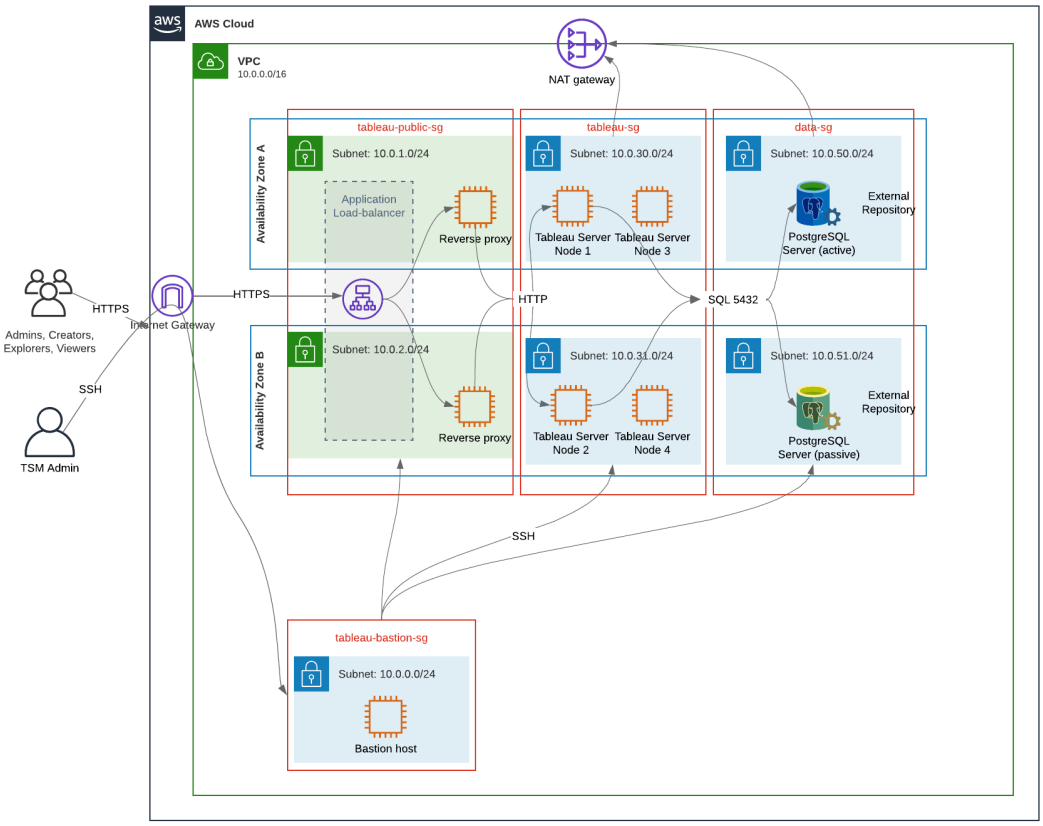
Meta

Os modelos e o conteúdo do Terraform fornecidos aqui destinam-se a fornecer uma amostra funcional que permitirá implantar o EDG rapidamente em um ambiente de teste de desenvolvimento.

Fizemos o possível para testar e documentar o exemplo de implantação do Terraform. No entanto, usar o Terraform para implantar e manter o EDG em um ambiente de produção exigirá conhecimento do Terraform que está além do escopo deste exemplo. O Tableau não oferece suporte para o exemplo de solução Terraform documentado aqui.

Estado final

Siga o procedimento nesta seção para configurar uma VPC na AWS que seja funcionalmente equivalente à VPC especificada na Parte 3 - Preparação para a implantação corporativa do Tableau Server.



Os modelos de amostra do Terraform e o conteúdo de suporte nesta seção:

- Cria uma VPC com um endereço IP elástico, duas zonas de disponibilidade e organização de sub-redes conforme mostrado acima (os endereços IP são diferentes)
- Cria os grupos de segurança Bastion, Público, Privado e Dados.
- Define a maioria das regras de entrada e saída nos grupos de segurança. Você precisará editar grupos de segurança após a execução do Terraform.
- Cria os seguintes hosts EC2 (cada um executando AWS Linux2): bastion, proxy 1 proxy 2, Tableau nó 1, Tableau nó 2, Tableau nó 3, Tableau nó 4.
- Hosts EC2 para PostgreSQL não são criados. Você deve criar o EC2 manualmente no grupo de segurança de dados e, em seguida, instalar e configurar o PostgreSQL conforme descrito em Instalar, configurar e PostgreSQL de tar.

Requisitos

- Conta da AWS - você deve ter acesso a uma conta da AWS que permita criar VPCs.
- Se você estiver executando o Terraform em um computador Windows, precisará instalar a AWS CLI.
- Um endereço IP elástico disponível em sua conta da AWS.
- Um domínio registrado no AWS Route 53. O Terraform criará uma zona DNS e certificados SSL relacionados no Route 53. Portanto, o perfil sob o qual o Terraform é executado também deve ter as permissões apropriadas no Route 53.

Antes de começar

- Os exemplos de linha de comando neste procedimento são para Terminal com sistema operacional Apple. Se você estiver executando o Terraform no Windows, pode ser necessário adaptar comandos com caminhos de arquivo, conforme apropriado.
- Um projeto Terraform é composto de muitos arquivos de configuração de texto (extensão de arquivo .tf). Você configura o Terraform personalizando esses arquivos. Se você não tiver um editor de texto robusto, instale o Atom ou o Text++.
- Se você estiver compartilhando o projeto Terraform com outras pessoas, recomendamos armazenar o projeto no Git para gerenciamento de alterações.

Etapa 1 - Preparar o ambiente

A. Baixe e instale o Terraform:

https://www.terraform.io/downloads

B. Gere o par de chaves públicas-privadas

Essa é a chave que você usará para acessar a AWS e o ambiente VPC resultante. Ao executar o Terraform, você incluirá a chave pública.

Abra o Terminal e execute o seguinte comando:

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

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

2. Crie uma chave pública. Este formato de chave não é usado para Terraform. Você a converterá em uma chave ssh posteriormente neste procedimento:

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

3. Defina as permissões na chave privada:

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

   Para definir permissões no Windows:

   - Localize o arquivo no Windows Explorer, clique com o botão direito do mouse e selecione **Propriedades**. Navegue até a guia **Segurança** e clique em **Avançado**.
   - Altere o proprietário para você, desative a herança e exclua todas as permissões. Conceda a si mesmo o **Controle total** e clique em **Salvar**. Marque o arquivo como somente leitura.

4. Crie a chave pública ssh. Essa é a chave que você copiará para o Terraform posteriormente no processo.

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

C. Baixe o projeto e adicione o diretório de estado

1. Baixe e descompacte o projeto EDG Terraform e salve-o em seu computador local. Depois de descompactar o download, você terá um diretório de nível superior, edg-terraform, e uma série de subdiretórios.

2. Crie um diretório chamado `state` , como um par para o diretório de nível superior`edg-terraform`.

Etapa 2: personalizar o modelos do Terraform

Você deve personalizar os modelos do Terraform para se adequar ao seu ambiente AWS e EDG. O exemplo aqui fornece as personalizações mínimas de modelo que a maioria das organizações precisará fazer. É provável que seu ambiente específico exija outras personalizações.

Esta seção é organizada por nome de modelo.

Certifique-se de salvar todas as alterações antes de prosseguir para a *Etapa 3 - Executar o 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. Abra a chave pública que você gerou na Etapa 1B e copie-a:

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

   Windows: copie o conteúdo de sua chave pública.

2. Copie a cadeia de caracteres da chave pública no argumento public_key, por exemplo:

   ```
   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. Adicione tags de acordo com os requisitos da sua organização. Por exemplo:

```
default_tags {
  tags = {

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

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

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

elb.tf

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

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

Add `idle_timeout`:

```
resource "aws_lb" "tableau" {
name                       = "edg-again-alb"
load_balancer_type         = "application"
subnets                    = [for subnet in aws_subnet.public :
```

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

variables.tf

Atualize o nome do domínio raiz. Esse nome deve corresponder ao domínio que você registrou no Route 53.

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

Por padrão, o subdomínio,`tableau`, é especificado para o nome de domínio VPC DNS. Para mudar isso, atualize `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 necessário, adicione blob de tags:

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

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

- Conforme necessário, opcionalmente, atualize seu armazenamento para lidar com seus requisitos de dados:

  Volume raiz:

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

  Volume de aplicativo:

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

Etapa 3 - Executar o Terraform

A. Inicializar o Terraform

No Terminal, mude para o diretório `edg-terraform` e execute o comando a seguir:

```
terraform init
```

Se a inicialização for bem-sucedida, continue na próxima etapa. Se a inicialização falhou, siga as instruções na saída do Terraform.

B. Planejar o Terraform

No mesmo diretório, execute o comando plan:

```
terraform plan
```

Esse comando pode ser executado várias vezes. Execute quantas vezes forem necessárias para corrigir os erros. Quando este comando for executado sem erros, continue na próxima etapa.

C. Aplicar Terraform

No mesmo diretório, execute o comando apply:

```
terraform apply
```

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

Opcional: Destruir Terraform

Você pode destruir todo o VPC executando o comando destroy:

```
terraform destroy
```

O comando destroy destruirá apenas o que ele criou. Se você fez alterações manuais em alguns objetos na AWS (ou seja, grupos de segurança, sub-redes etc.), o `destroy` vai falhar. Para sair de uma operação de destruição com falha/interrupção, digite `Control + C`. Em seguida, você deve limpar o VPC manualmente para o estado em que estava quando o Terraform o criou originalmente. Você pode executar o comando `destroy`.

Etapa 4 - Conecte-se ao bastion

Todas as conexões de linha de comando são feitas por meio do bastion host no TCP 22 (protocolo SSH).

1. Na AWS, crie uma regra de entrada no grupo de segurança do bastion (**AWS** > **Grupos de segurança** > **Bastion SG** > **Editar regras de entrada**) e crie uma regra para permitir conexões SSH (TCP 22) do endereço IP ou máscara de sub-rede onde você executará os comandos do Terminal.

Opcional: pode ser útil permitir a cópia de arquivos entre as instâncias do EC2 nos grupos Privado e Público durante a implantação. Crie regras SSH de entrada:

- Privado: crie uma regra de entrada para permitir o SSH do Público
- Público: crie regra de entrada para permitir SSH de Privado e Público

2. Use a chave pem que você criou na Etapa 1.B para se conectar ao bastion host:

   No terminal Mac:

   Execute os seguintes comandos no diretório onde a chave pem está armazenada:

   ```
   ssh-add —apple-use-keychain <keyName>.pem
   ```

   If you get a warning about private key being accessible by others, then run this command: `chmod 600 <keyName.pem>` and then run the `ssh-add` command again.

   Connect to the bastion host with this command: `ssh -A ec2-user@IPaddress`

   For example: `ssh -A ec2-user@3.15.12.112`.

   No Windows usando PuTTY e Pageant:

   a. Crie ppk na chave pem: use o gerador de chaves PuTTY. Carregue a chave pem criada na Etapa 1.B. Após as importações de chave, clique em **Salvar chave privada**. Isso cria um arquivo ppk.

   b. No PuTTY - abra a configuração e faça as seguintes alterações:

      - Sessões>Nome do host: adicione o endereço IP do bastion host.
      - Sessões>Porta: 22
      - Conexão>Dados>Nome de usuário de login automático: ec2-user
      - Conexão>SSH>Auth>Permitir encaminhamento de agente
      - Connection>SSH>Auth> Para a chave privada, clique em Procurar e selecione o arquivo .ppk que você acabou de criar.

   c. Instale o Pageant e carregue o ppk no aplicativo.

Etapa 5- instalar o PostgreSQL

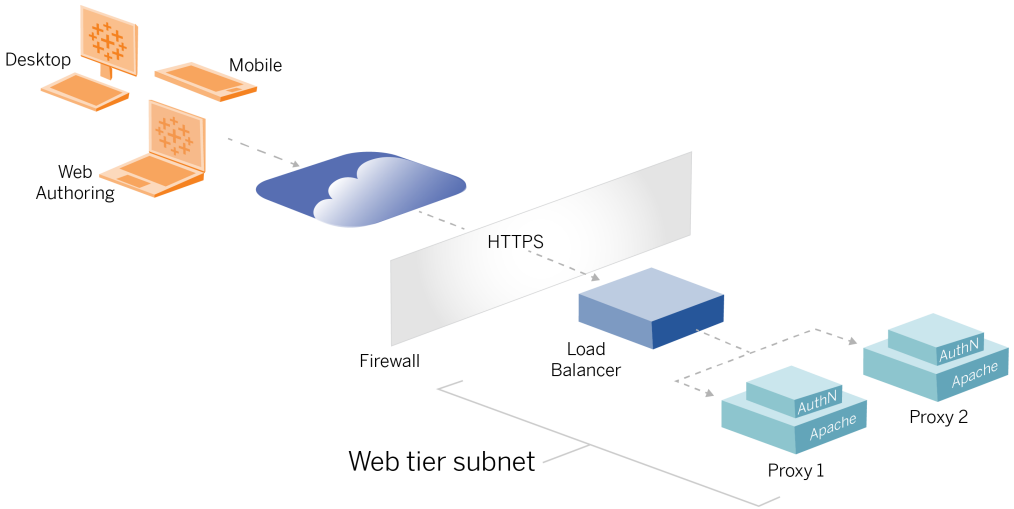
O modelo Terraform não instala o PostgreSQL para uso como repositório externo. No entanto, o grupo de segurança e a sub-rede associados são criados. Se você for instalar o repositório externo em uma instância do EC2 executando PostgreSQL, deverá implantar a instância do EC2 conforme descrito na Parte 3 - Preparação para a implantação corporativa do Tableau Server.

Em seguida, instale, configure e faça o backup tar do PostgreSQL conforme descrito na Parte 4 - Instalar e configurar o Tableau Server.

Etapa 6 - (Opcional) Execute DeployTab4EDG

O script TabDeploy4EDG automatiza a implantação do Tableau de quatro nós descrita na Parte 4. Consulte o Script de instalação automatizada TabDeploy4EDG.

Apêndice - Camada da Web com exemplo de implantação do Apache



Este tópico fornece um procedimento de ponta a ponta que descreve como implementar o nível da Web no exemplo de arquitetura de referência da AWS. A configuração de exemplo é inclui os seguintes componentes:

- Balanceador de carga de aplicativo AWS
- Servidores proxys do Apache
- Módulo de autenticação Mellon
- Okta IdP
- Autenticação SAML

Observação: o exemplo de configuração de nível da Web apresentado nesta seção inclui procedimentos detalhados para implantação de software e serviços de terceiros. Fizemos o melhor esforço para verificar e documentar os procedimentos para habilitar o cenário de nível da Web. No entanto, o software de terceiros pode mudar ou seu cenário

pode ser diferente da arquitetura de referência descrita aqui. Consulte a documentação de terceiros para obter detalhes e suporte de configuração confiável.

Os exemplos do Linux em toda esta seção mostram comandos para distribuições do tipo RHEL. Especificamente, os comandos aqui foram desenvolvidos com a distribuição Amazon Linux 2. Se você estiver executando a distribuição do Ubuntu, edite os comandos de forma apropriada.

A implementação do nível da Web neste exemplo segue uma configuração passo a passo e procedimento de verificação. A configuração principal da camada da Web consiste nas etapas a seguir para habilitar HTTP entre o Tableau e a Internet. O Apache é executado e configurado para proxy reverso/balanceamento de carga por trás do balanceador de carga do aplicativo AWS:

1. Instale o Apache
2. Configure o proxy reverso para testar a conectividade com o Tableau Server
3. Configure o balanceamento de carga no proxy
4. Configure o balanceador de carga do aplicativo AWS

Depois que a camada da Web for configurada, e a conectividade com o Tableau verificada, configure a autenticação com um provedor externo.

Instale o Apache

Execute o procedimento a seguir em ambos os hosts EC2 (Proxy 1 e Proxy 2). Se estiver implantando na AWS de acordo com o exemplo de arquitetura de referência, você deve ter duas zonas de disponibilidade e executar um único servidor proxy em cada zona.

1. Instale o Apache:

   ```
   sudo yum update -y
   sudo yum install -y httpd
   ```

2. Configure para iniciar o Apache na reinicialização:

```
sudo systemctl enable --now httpd
```

3. Verifique se a versão do httpd que você instalou inclui `proxy_hcheck_module`.

   ```
   sudo httpd -M
   ```

   O `proxy_hcheck_module` é necessário. Se a sua versão do httpd não inclui este módulo, atualize para uma versão do httpd que o inclua.

Configure o proxy para testar a conectividade com o Tableau Server

Execute este procedimento em um dos hosts proxy (Proxy 1). O objetivo desta etapa é verificar a conectividade entre a Internet e seu servidor proxy para o Tableau Server no grupo de segurança privada.

1. Crie um arquivo chamado `tableau.conf` e adicione-o ao diretório `/etc/httpd/conf.d`.

   Copie o seguinte código e especifique as chaves `ProxyPass` e `ProxyPassReverse` com o endereço IP privado do Nó 1 do Tableau Server.

   > **Importante**: a configuração mostrada abaixo não é segura e não deve ser usada na produção. Essa configuração só deve ser usada durante o processo de instalação para verificar a conectividade ponta a ponta.

   Por exemplo, se o endereço IP privado do Nó 1 for `10.0.30.32`, então o conteúdo do arquivo `tableau.conf` será:

   ```
   <VirtualHost *:80>
   ProxyPreserveHost On
   ProxyPass "/" "http://10.0.30.32:80/"
   ```

```
ProxyPassReverse "/" "http://10.0.30.32:80/"
</VirtualHost>
```

2. Reinicie o httpd:

   ```
   sudo systemctl restart httpd
   ```

Verificação: configuração da topologia de base

Você deve conseguir acessar a página de administração do Tableau Server navegando para `http://<proxy-public-IP-address>`.

Se a página de login do Tableau Server não carregar em seu navegador, siga estas etapas de solução de problemas no host Proxy 1:

- Pare e inicie o httpd como uma primeira etapa de solução de problemas.
- Verifique novamente o arquivo `tableau.conf`. Verifique se o IP privado do Nó 1 está correto. Verifique as aspas duplas e analise cuidadosamente a sintaxe.
- Execute o comando `curl` com no servidor proxi reverso com o endereço IP privado do Nó 1, por exemplo, `curl 10.0.1.90` . Se o shell não retornar html ou se retornar html para a página da Web de teste do Apache, verifique a configuração do protocolo/porta entre os grupos de segurança Pública e Privada.
- Execute o comando `curl` com endereço IP privado do Proxy 1, por exemplo, `curl 10.0.0.163`. Se o shell retornar o código html para a página da Web de teste do Apache, o arquivo proxy não está configurado corretamente.
- Sempre reinicie o httpd (`sudo systemctl restart httpd`) após qualquer alteração na configuração do arquivo proxy ou dos grupos de segurança.
- Certifique-se de que o TSM esteja em execução no Nó 1.

Configure o balanceamento de carga no proxy

1. No mesmo host proxy (Proxy 1) onde você criou o arquivo `tableau.conf`, remova a configuração do Host virtual existente e edite o arquivo para incluir a lógica de balanceamento de carga.

   Por exemplo:

```
<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. Pare e inicie httpd:

```
sudo systemctl stop httpd
sudo systemctl start httpd
```

3. Verifique a configuração navegando até o endereço IP público do Proxy 1.

Copie a configuração para o segundo servidor proxy

1. Copie o`tableau.conf` arquivo do Proxy 1 e salve-o no diretório `/etc/h-ttpd/conf.d` no host Proxy 2.

2. Pare e inicie httpd:

```
sudo systemctl stop httpd
sudo systemctl start httpd
```

3. Verifique a configuração navegando até o endereço IP público do Proxy 2.

Configure o balanceador de carga do aplicativo AWS

Configure o balanceador de carga como um ouvinte HTTP. O procedimento aqui descreve como adicionar um balanceador de carga na AWS.

Etapa 1: criar grupo de destinos

Um grupo de destino é uma configuração da AWS que define as instâncias do EC2 que executam os servidores proxy. Esses são os destinos do tráfego do LBS.

1. EC2>**Grupos de destino** > **Criar grupo de destino**

2. Na página Criar:

   - Insira um nome para o grupo de destino, por exemplo `TG-internal-HTTP`
   - Tipo de destino: instâncias
   - Protocolo: HTTP
   - Porta: 80
   - VPC: selecione o seu VPC
   - Em **Verificações de integridade** > **Configurações avançadas de verificações de integridade > Códigos de sucesso** , anexe a lista de códigos para ler: `200,303`.
   - Clique em **Criar**

3. Selecione o grupo de destinos que você acabou de criar e clique na guia **Destinos**:

   - Clique em **Editar**.
   - Selecione as instâncias do EC2 (ou instância única, se você estiver configurando uma de cada vez) que estão executando o aplicativo proxy e clique

em **Adicionar ao arquivo**.
- Clique em **Salvar**.

Etapa 2: iniciar o assistente de balanceador de carga

1. EC2 > **Balanceadores de carga**> **Criar balanceador de carga**
2. Na página “Selecionar tipo de balanceador de carga”, crie um Balanceador de carga de aplicativo.

Observação: a interface de usuário exibida para configurar o balanceador de carga não é consistente em datacenters AWS. O procedimento abaixo, "Configuração do assistente," mapeia para o assistente de configuração da AWS que começa na **Etapa 1 Configurar o balanceador de carga**.

Se o seu datacenter exibe todas as configurações em uma única página que inclui um botão **Criar balanceador de carga** na parte inferior da página, siga o procedimento "Configuração de página única" abaixo.

Configuração do assistente

1. Página **Configurar o balanceador de carga**:
    - Especifique o nome
    - Esquema: voltado para a Internet (padrão)
    - Tipo de endereço IP: ipv4 (padrão)
    - Ouvintes (ouvintes e roteamento):
        a. Deixe o ouvinte HTTP padrão
        b. Clique em **Adicionar ouvinte** e adicione `HTTPS:443`

- VPC: selecione o VPC onde você instalou tudo
- Zonas de disponibilidade:
  - Selecione **a** e **b** para suas regiões de datacenter
  - Em cada seletor suspenso correspondente, selecione a sub-rede pública (onde residem seus servidores proxy).
- Clique em: **Definir configurações de segurança**

2. Página **Definir configurações de segurança**

   - Faça upload do seu certificado SSL público.
   - Clique em **Próximo: configurar grupos de segurança**.

3. Página **Definir configurações de segurança**:

   - Selecione o grupo de segurança Pública. Se o grupo de segurança Padrão for selecionado, desmarque essa seleção.
   - Clique em **Próximo: configurar rota**.

4. Página **Configurar roteamento**

   - Grupo de destino: Grupo de destino existente.
   - Nome: selecione o grupo de destino que você criou anteriormente
   - Clique em **Avançar: Registrar destinos**.

5. Página **Registrar destinos**

   - As duas instâncias do servidor proxy que você configurou anteriormente devem ser exibidas.
   - Clique em **Próximo: revisão**.

6. Página **Revisão**

   Clique em **Criar**.

Configuração de página única

Configuração básica

- Especifique o nome
- Esquema: voltado para a Internet (padrão)
- Tipo de endereço IP: ipv4 (padrão)

Mapeamento de rede

- VPC: selecione o VPC onde você instalou tudo
- Mapeamentos:
  - Selecione as Zonas de disponibilidade **a** e **b** (ou comparáveis) para as suas regiões de datacenter
  - Em cada seletor suspenso correspondente, selecione a sub-rede pública (onde residem seus servidores proxy).

Grupos de segurança

Selecione o grupo de segurança Pública. Se o grupo de segurança Padrão for selecionado, desmarque essa seleção.

Ouvintes e roteamento

- Deixe o ouvinte HTTP padrão. Para a **ação padrão**, especifique o grupo-alvo que você configurou anteriormente.
- Clique em **Adicionar ouvinte** e adicione `HTTPS:443`. Para a **ação padrão**, especifique o grupo-alvo que você configurou anteriormente.

Configurações de ouvinte seguro

- Faça upload do seu certificado SSL público.

Clique em **Criar o balanceador de carga**.

Etapa 3: habilitar aderência

1. Depois que o balanceador de carga é criado, você deve habilitar a aderência no grupo de destino.
   - Abra a página Balanceador de carga da AWS (**EC2**> **Balanceadores de carga**> **Grupos de destinos**), selecione a instância do balanceador de carga que você acabou de configurar. No menu **Ação**, selecione **Editar atributos**.

- Na página **Editar atributos**, selecione **Aderência**, especifique uma duração de `1 day` e, em seguida, **Salvar alterações**.

2. No balanceador de carga, ative a aderência no ouvinte HTTP. Selecione o balanceador de carga que você acabou de configurar e clique na guia **Ouvintes:**

    - Para **HTTP: 80**, clique em **Exibir/editar regras**. Na página **Regras**, clique no ícone de edição (uma vez no topo da página e depois novamente na regra) para editar a regra. Exclua a regra THEN existente e substitua-a clicando em **Adicionar ação** > **Encaminhar para....** Na configuração THEN resultante, especifique o mesmo grupo de destino que você criou. Em Aderência em nível de grupo, ative a aderência e defina a duração para 1 dia. Salve a configuração e clique em **Atualizar**.

Etapa 4: definir o tempo limite de inatividade no balanceador de carga

No balanceador de carga, atualize o tempo limite de inatividade para 400 segundos.

Selecione o balanceador de carga que você configurou para esta implantação e clique em **Ações** > **Editar atributos**. Defina o **Tempo limite de inatividade** para `400` segundos e, em seguida, clique em **Salvar**.

Etapa 5: verificar a conectividade LBS

Abra a página Balanceador de carga da AWS (**EC2**> **Balanceadores de carga**), selecione a instância do balanceador de carga que você acabou de configurar.

Em **Descrição** copie o nome DNS e cole-o em um navegador para acessar a página de entrada do Tableau Server.

Se você receber um erro de nível 500, provavelmente precisará reiniciar seus servidores proxy.

Atualize DNS com URL pública do Tableau

Use o nome da zona DNS de seu domínio da descrição do Balanceador de carga da AWS para criar um valor CNAME em seu DNS. O tráfego para a sua URL (tableau.example.com)

deve ser enviado ao nome DNS público da AWS.

Verifique a conectividade

Depois que suas atualizações de DNS forem concluídas, você deverá conseguir navegar para a página de entrada do Tableau Server inserindo a URL pública, por exemplo,`https://-tableau.example.com`.

Exemplo de configuração de autenticação: SAML com IdP externo

O exemplo a seguir descreve como instalar e configurar o SAML com Okta IdP e módulo de autenticação Mellon para uma implantação do Tableau em execução na arquitetura de referência da AWS. O exemplo descreve como configurar o Tableau Server e os servidores proxy Apache para usar HTTP. O Okta enviará a solicitação ao balanceador de carga AWS por HTTPS, mas todo o tráfego interno se deslocará por HTTP. Ao configurar para este cenário, esteja ciente dos protocolos HTTP vs HTTPS ao configurar cadeias de caractere de URL.

Este exemplo usa o Mellon como um módulo de provedor de serviços de pré-autenticação nos servidores proxy reversos. Essa configuração garante que apenas o tráfego autenticado se conecte ao Tableau Server, que também atua como um provedor de serviços com o Okta IdP. Portanto, você deve configurar dois aplicativos IdP: um para o provedor de serviços Mellon e um para o provedor de serviços Tableau.

Crie a conta de administrador do Tableau

Um erro comum ao configurar o SAML é esquecer de criar uma conta de administrador no Tableau Server, antes de habilitar o SSO.

A primeira etapa é criar uma conta no Tableau Server com uma função de Administrador do servidor. Para o exemplo do cenário Okta, o nome de usuário deve estar em um formato de

endereço de e-mail válido, por exemplo, usuário@example.com. Você deve definir uma senha para este usuário, mas a senha não será usada após a configuração do SAML.

Configurar aplicativo de pré-autenticação Okta

O cenário de ponta a ponta descrito nesta seção requer dois aplicativos Okta:

- Aplicativo de pré-autenticação Okta
- Aplicativo Okta Tableau Server

Cada um desses aplicativos está associado a metadados diferentes que você precisará configurar no proxy reverso e no Tableau Server, respectivamente.

Este procedimento descreve como criar e configurar o aplicativo de pré-autenticação Okta. Posteriormente neste tópico, você criará o aplicativo Okta Tableau Server. Para uma conta Okta de teste gratuita com usuários limitados, consulte a página da Web do Desenvolvedor do Okta.

Crie uma integração de aplicativo SAML para o provedor de serviços de pré-autenticação Mellon.

1. Abra o painel de administração do Okta> **Aplicativos** > **Criar integração de aplicativo**.

2. Na página **Criar uma nova integração de aplicativo**, selecione **SAML 2.0** e clique em **Avançar**.

3. Na guia **Configurações gerais**, insira um nome de aplicativo, por exemplo `Tableau Pre-Auth` e clique em **Avançar**.

4. Na guia **Configurar SAML**:

    - Logon único (SSO) na URL. O elemento final do caminho na URL de logon único é conhecido como `MellonEndpointPath` no arquivo de configuração `mellon.conf` posteriormente neste procedimento. Você pode especificar qualquer ponto de extremidade que desejar. Neste exemplo, `sso` é um ponto de

extremidade. O último elemento, `postResponse`, é necessário: `https://-tableau.example.com/sso/postResponse`.

- Desmarque a caixa de seleção: **Use para URL do destinatário e URL de destino**.
- URL do destinatário: igual à URL do SSO, mas com HTTP. Por exemplo, `http://tableau.example.com/sso/postResponse`.
- URL de destino: igual à URL do SSO, mas com HTTP. Por exemplo, `http://-tableau.example.com/sso/postResponse`.
- URI de público (ID da entidade SP). Por exemplo, `https://-tableau.example.com`.
- Formato de ID do nome:`EmailAddress`
- Nome de usuário do aplicativo: `Email`
- Declarações de atributos: Nome =`mail`; Formato do nome =`Unspecified`; Valor =`user.email`.

Clique em **Próximo**.

5. Na guia **Feedback**, selecione:
   - **Sou um cliente do Okta adicionando um aplicativo interno**
   - **Este é um aplicativo interno que criamos**
   - Clique em **Concluir**.

6. Crie o arquivo de metadados do IdP de pré-autenticação:
   - No Okta: **Aplicativos** > **Aplicativos** > Seu novo aplicativo (por exemplo,`Tableau Pre-Auth`) > **Entrar**
   - Ao lado de **Certificados de assinatura SAML** , clique em **Exibir instruções de configuração SAML**.
   - Em **Como configurar o SAML 2.0 para<pre-auth> Aplicativo**, na página, role para baixo até a seção **Opcional**, **forneça os seguintes metadados de IDP para seu provedor de SP**.
   - Copie o conteúdo do campo XML e salve-o em um arquivo chamado `pre-auth_idp_metadata.xml`.

7. (Opcional) Configure a autenticação multifator:

- No Okta: **Aplicativos** > **Aplicativos** > Seu novo aplicativo (por exemplo,`Tableau Pre-Auth`) > **Entrar**
- **Em Política de logon**, clique em **Adicionar regra**.
- Na **Regra de logon do aplicativo**, especifique um nome e as diferentes opções de MFA. Para testar a funcionalidade, você pode deixar todas as opções como padrão. No entanto, em **Ações**, você deve selecionar **Solicitar fator** e, a seguir, especificar a frequência com que os usuários devem entrar. Clique em **Salvar**.

Crie e atribua usuário do Okta

1. No Okta, crie um usuário com o mesmo nome de usuário que você criou no Tableau (usuário@example.com): **Diretório** > **Pessoas** > **Adicionar pessoa**.
2. Depois que o usuário for criado, atribua o novo aplicativo Okta a essa pessoa: clique no nome do usuário e atribua o aplicativo em **Atribuir aplicativo**.

Instale o Mellon para pré-autenticação

1. Nas instâncias EC2 que estão executando o servidor proxy Apache, execute os seguintes comandos para instalar os módulos PHP e Mellon:

   ```
   sudo yum install httpd php mod_auth_mellon
   ```

2. Crie o diretório `/etc/httpd/mellon`

Configure o Mellon como módulo de pré-autenticação

Execute este procedimento em ambos os servidores proxy.

Você deve ter uma cópia do arquivo `pre-auth_idp_metadata.xml` que você criou a partir da configuração do Okta.

1. Altere o diretório:

   ```
   cd /etc/httpd/mellon
   ```

2. Crie os metadados do provedor de serviços. Execute o script `mellon_create_metadata.sh`. Você deve incluir a ID da entidade e a URL de retorno para sua organização no comando.

   A URL de retorno é conhecida como *URL de logon único* no Okta. O elemento final do caminho na URL de retorno é conhecido como o`MellonEndpointPath` no arquivo de configuração `mellon.conf` posteriormente neste procedimento. Neste exemplo, especificamos `sso` como o caminho do terminal.

   Por exemplo:

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

   O script retorna o certificado do provedor de serviços, a chave e os arquivos de metadados.

3. Renomeie os arquivos do provedor de serviços no diretório `mellon` para facilitar a leitura. Faremos referência a esses arquivos pelos seguintes nomes na documentação:

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

4. Copie o arquivo `pre-auth_idp_metadata.xml` para o mesmo diretório.

5. Crie o arquivo `mellon.conf` no diretório `/etc/httpd/conf.d`:

   ```
   sudo nano /etc/httpd/conf.d/mellon.conf
   ```

6. Copie o seguinte conteúdo para `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. Adicione o conteúdo a seguir no arquivo `tableau.conf` existente:

   Dentro do bloco `<VirtualHost *:80>`, adicione o seguinte conteúdo. Atualize `ServerName` com o nome de host público em sua ID de entidade:

   ```
   DocumentRoot /var/www/html
   ServerName tableau.example.com
   ServerSignature Off
   ErrorLog logs/error_sp.log
   CustomLog logs/access_sp.log combined
   LogLevel info
   ```

   Adicione o bloco de localização fora do bloco `<VirtualHost *:80>`. Atualize `MellonCookieDomain` com o domínio de nível superior para preservar as informações do cookie, conforme mostrado:

   ```
   <Location />
   AuthType Mellon
   MellonEnable auth
   Require valid-user
   MellonCookieDomain example.com
   </Location>
   ```

   O arquivo `tableau.conf` completo deve ser parecido com o exemplo a seguir:

   ```
   <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. Verifique a configuração. Execute o seguinte comando:

   ```
   sudo apachectl configtest
   ```

   Se o teste de configuração retornar um erro, corrija os erros e execute configtest novamente. Uma configuração bem-sucedida retornará,`Syntax OK`.

9. Reinicie o httpd:

```
sudo systemctl restart httpd
```

Crie o aplicativo Tableau Server no Okta

1. No painel do Okta: **Aplicativos** > **Aplicativos** > **Navegar no catálogo de aplicativos**
2. Em **Procurar catálogo de integração de aplicativos**, pesquise `Tableau`, selecione o bloco do Tableau Server e clique em **Adicionar**.
3. Em **Adicionar Tableau Server** > **Configurações gerais**, insira um rótulo e clique em **Avançar**.
4. Em Opções de logon, selecione **SAML 2.0** role a página para baixo até Configurações de logon avançadas:
    - **ID da entidade SAML**: insira a URL pública, por exemplo, https://-tableau.example.com.
    - **Formato do nome de usuário do aplicativo**: e-mail
5. Clique no **link de metadados do provedor de identidade** para iniciar um navegador. Copie o link do navegador. Esse é o link que você usará ao configurar o Tableau no procedimento a seguir.
6. Clique em **Concluído**.
7. Atribua o novo aplicativo Tableau Server Okta ao seu usuário (usuário@example.com): clique no nome do usuário e atribua o aplicativo em **Atribuir aplicativo**.

Habilite SAML no Tableau Server para IdP

Execute este procedimento no nó 1 do Tableau Server.

1. Baixe os metadados do aplicativo Tableau Server no Okta. Use o link que você salvou no procedimento anterior:

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

2. Copie um certificado TLS e o arquivo de chave relacionado para o Tableau Server. O arquivo de chave deve ser uma chave RSA. Para obter mais informações sobre o certificado e requisitos do SAML, consulte *Requisitos do SAML* (Linux).

   Para simplificar o gerenciamento e a implantação de certificados e como prática recomendada de segurança, recomendamos o uso de certificados gerados por uma autoridade de certificação (CA) de terceiros confiável. Como alternativa, você pode gerar certificados autoassinados ou usar certificados de uma PKI para TLS.

   Se você não tiver um certificado TLS, poderá gerar um certificado autoassinado usando o procedimento incorporado a seguir.

Gerar um certificado autoassinado

Execute este procedimento no nó 1 do Tableau Server.

a. Gere a chave de autoridade de certificação raiz (CA) de assinatura:

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

b. Crie o certificado CA raiz:

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

   Você será solicitado a inserir valores para os campos do certificado. Por exemplo:

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

```
Organizational Unit Name (eg, section) []:Operations
Common Name (eg, your name or your server's hostname)
[]:tableau.example.com
Email Address []:example@tableau.com
```

c. Crie o certificado e a chave relacionada (`server-saml.csr` e `server-saml.key` no exemplo abaixo) para o computador Postgres. O nome do assunto do certificado deve corresponder ao nome do host público do host do Tableau. O nome do assunto é definido com a opção `-subj` e o formato `"/CN=<host-name>"`, por exemplo:

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

d. Assine o novo certificado com o certificado CA que você criou antes. O comando a seguir também produz o certificado no formato `crt`:

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

e. Converta o arquivo de chave em RSA. O Tableau requer um arquivo de chave RSA para SAML. Para converter a chave, execute o comando a seguir:

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

3. Configure o SAML. Execute o seguinte comando, especificando seu ID de entidade e URL de retorno, e os caminhos para o arquivo de metadados, arquivo de certificado e arquivo de chave:

```
tsm authentication saml configure --idp-entity-id "https://-
tableau.example.com" --idp-return-url "https://-
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 sua organização estiver executando o Tableau Desktop 2021.4 ou posterior, você deve executar o seguinte comando para habilitar a autenticação por meio dos servidores proxy reverso.

   As versões do Tableau Desktop 2021.2.1 - 2021.3 funcionarão sem executar este comando, desde que seu módulo de pré-autenticação (por exemplo, Mellon) esteja configurado para permitir a preservação de cookies de domínio de nível superior.

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

5. Aplique as alterações configuração:

   ```
   tsm pending-changes apply
   ```

Validar a funcionalidade SAML

Para validar a funcionalidade SAML de ponta a ponta, entre no Tableau Server com a URL pública (por exemplo, https://tableau.example.com) com a conta de administrador do Tableau que você criou no início deste procedimento.

Solução de problemas de validação

Solicitação inválida: um erro comum neste cenário é um erro de "Solicitação inválida" da Okta. Frequentemente, esse problema ocorre quando o navegador está armazenando dados em cache de uma sessão anterior do Okta. Por exemplo, se você gerencia os aplicativos Okta como um administrador Okta e, em seguida, tenta acessar o Tableau usando uma conta habilitada para Okta diferente, os dados da sessão dos dados do administrador podem causar o erro "Solicitação inválida". Se esse erro persistir mesmo depois de limpar o cache do navegador local, tente validar o cenário do Tableau conectando-se em um navegador diferente.

Outra causa do erro "Solicitação inválida" é um erro de digitação em uma das muitas URLs que você insere durante os processos de configuração do Okta, Mellon e SAML. Verifique tudo isso com atenção.

Muitas vezes o arquivo de httpd `error.log` no servidor Apache especificará qual URL está causando o erro.

Não encontrado - A URL solicitada não foi encontrado neste servidor: este erro indica um dos muitos erros de configuração.

Se o usuário for autenticado com Okta e receber esse erro, é provável que você tenha carregado o aplicativo de pré-autenticação Okta para o Tableau Server quando configurou o SAML. Verifique se você tem os metadados do aplicativo Okta Tableau Server configurados no Tableau Server, e não os metadados do aplicativo de pré-autenticação Okta

Outras etapas de solução de problemas:

- Analise o `tableau.conf` com cuidado para verificar os erros de digitação ou configuração
- Revise as configurações do aplicativo de pré-autenticação do Okta. Certifique-se de que os protocolos HTTP vs HTTPS estejam definidos, conforme especificado neste tópico.
- Reinicie o httpd em ambos os servidores proxy.
- Verifique se `sudo apachectl configtest` retorna “Sintaxe OK” em ambos os servidores proxy.
- Verifique se o usuário de teste está atribuído a ambos os aplicativos no Okta.
- Verifique se a aderência está definida no balanceador de carga e grupos de destino associados

Configurar SSL/TLS do balanceador de carga para o Tableau Server

Algumas organizações exigem um canal de criptografia de ponta a ponta do cliente para o serviço de back-end. A arquitetura de referência padrão, conforme descrito até este ponto,

especifica SSL do cliente para o balanceador de carga em execução na camada da Web de sua organização.

Para configurar SSL do balanceador de carga para o Tableau Server, você deve:

- Instalar um certificado SSL válido nos servidores Tableau e proxy.
- Configurar o SSL do balanceador de carga para os servidores proxy reversos.
- Configurar o SSL dos servidores proxy para o Tableau Server.
- Você também pode configurar o SSL do Tableau Server para a instância PostgreSQL.

O restante deste tópico descreve essa implementação no contexto do exemplo de arquitetura de referência da AWS.

Exemplo: configurar SSL/TLS na arquitetura de referência da AWS

Esta seção descreve como configurar SSL no Tableau e configurar SSL em um servidor proxy Apache, tudo em execução na arquitetura de referência de exemplo da AWS.

Os procedimentos do Linux em todo este exemplo mostram comandos para distribuições do tipo RHEL. Especificamente, os comandos aqui foram desenvolvidos com a distribuição Amazon Linux 2. Se você estiver executando a distribuição do Ubuntu, edite os comandos de forma apropriada.

Etapa 1: coletar certificados e chaves relacionadas

Para simplificar o gerenciamento e a implantação de certificados e como prática recomendada de segurança, recomendamos o uso de certificados gerados por uma autoridade de certificação (CA) de terceiros confiável.

Como alternativa, você pode gerar certificados autoassinados ou usar certificados de uma PKI para TLS.

O procedimento a seguir como gerar certificados autoassinados. Se você estiver usando certificados de terceiros como recomendamos, pule este procedimento.

Execute este procedimento em um dos hosts proxy. Depois de gerar o certificado e a chave associada, você os compartilhará com o outro host proxy e com o nó 1 do Tableau Server.

1. Gere a chave de autoridade de certificação raiz (CA) de assinatura:

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

2. Crie o certificado CA raiz:

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

   Você será solicitado a inserir valores para os campos do certificado. Por exemplo:

   ```
   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. Crie o certificado e a chave relacionada (`serverssl.csr` e `serverssl.key` no exemplo abaixo) para o computador Postgres. O nome do assunto do certificado deve corresponder ao nome do host público do host do Tableau. O nome do assunto é definido com a opção `-subj` e o formato`"/CN=<host-name>"`, por exemplo:

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

4. Assine o novo certificado com o certificado CA que você criou na etapa 2. O comando a seguir também produz o certificado no formato `crt`:

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

Etapa 2: configurar o servidor proxy para SSL

Execute este procedimento em ambos os servidores proxy.

1. Instale o módulo Apache ssl:

   ```
   sudo yum install mod_ssl
   ```

2. Crie o diretório `/etc/ssl/private`:

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

3. Copie os arquivos crt e key para os seguintes caminho `/etc/ssl/` paths:

   ```
   sudo cp serverssl.crt /etc/ssl/certs/

   sudo cp serverssl.key /etc/ssl/private/
   ```

4. Atualize o `tableau.conf` existente com as seguintes atualizações:

   - Adicione o bloco de reconfiguração SSL:

     ```
     RewriteEngine on
     RewriteCond %{SERVER_NAME} =tableau.example.com
     RewriteRule ^ https://%{SERVER_NAME}%{REQUEST_URI}
     [END,NE,R=permanent]
     ```

   - No bloco de reconfiguração SSL, atualize o nome do servidor `RewriteCond`: adicione seu nome de host público, por exemplo,`tableau.example.com`
   - Altere `<VirtualHost *:80>` para `<VirtualHost *:443>`.
   - Conclua os blocos `<VirtualHost *:443>` e `<Location />` com `<IfModule mod_ssl.c>` ... `</IfModule>`.
   - `BalancerMember`: altere o protocolo de `http` para `https`.

- Adicione os elementos `SSL*` dentro do bloco `<VirtualHost *:443>`:

  ```
  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/serverssl.crt
  SSLCertificateKeyFile /etc/ssl/private/serverssl.key
  SSLProxyEngine on
  SSLProxyVerify none
  SSLProxyCheckPeerName off
  SSLProxyCheckPeerExpire off
  ```

- No elemento `LogLevel`: adicione `ssl:warn`.
- Opcional: se você instalou e configurou um módulo de autenticação, pode ter elementos adicionais no arquivo tableau.conf. Por exemplo, o bloco `<Location /> </Location>` incluirá elementos.

Um exemplo de arquivo tableau.conf configurado para SSL é mostrado aqui:

```
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. Adicione o arquivo index.html para suprimir os erros 403:

   ```
   sudo touch /var/www/html/index.html
   ```

6. Reinicie o httpd:

   ```
   sudo systemctl restart httpd
   ```

Etapa 3: configurar o Tableau Server para SSL externo

Copie os arquivos serverssl.crt e serverssl.key do host Proxy 1 para o Tableau Server inicial (Nó 1).

Execute os seguintes comandos no Nó 1:

```
tsm security external-ssl enable --cert-file serverssl.crt --key-
file serverssl.key
tsm pending-changes apply
```

Etapa 5: configuração de autenticação opcional

Se você configurou um provedor de identidade externo para o Tableau, provavelmente precisará atualizar as URLs de retorno no painel administrativo do IdP.

Por exemplo, se você estiver usando um aplicativo de pré-autenticação Okta, precisará atualizar o aplicativo para usar o protocolo HTTPS para a URL do destinatário e a URL de destino.

Etapa 5: configurar o balanceador de carga AWS para HTTPS

Se você estiver implantando com o balanceador de carga AWS conforme documentado neste guia, reconfigure o balanceador de carga AWS para enviar tráfego HTTPS para os servidores proxy:

1. Cancele o registro do grupo de destino HTTP existente:

   Em **Grupos de destino**, selecione o grupo de destino HTTP que foi configurado para o balanceador de carga, clique em **Ações** e, em seguida, clique em **Registrar e cancelar o registro da instância**.

   Na página **Registrar e cancelar o registro de destinos**, selecione as instâncias que estão configuradas atualmente, clique em **Cancelar o registro** e em **Salvar**.

2. Crie o grupo de destino HTTPS:

   Grupos de destino > **Criar grupo de destino**

   - Selecione "Instâncias"
   - Insira um nome para o grupo de destino, por exemplo `TG-internal-HTTPS`

- Selecione o VPC
- Protocolo: HTTPS 443
- Em **Verificações de integridade** > **Configurações avançadas de verificações de integridade > Códigos de sucesso** , anexe a lista de códigos para ler: `200,303`.
- Clique em **Criar**.

3. Selecione o grupo de destinos que você acabou de criar e clique na guia **Destinos**:

    - Clique em **Editar**
    - Selecione as instâncias EC2 que executam o aplicativo proxy e clique em **Adicionar para registrada**.
    - Clique em **Salvar**.

4. Depois que o grupo de destino é criado, você deve habilitar a aderência:

    - Abra a página Balanceador de carga da AWS (**EC2**> **Balanceadores de carga**> **Grupos de destinos**), selecione a instância do balanceador de carga que você acabou de configurar. No menu **Ação**, selecione **Editar atributos**.
    - Na página **Editar atributos**, selecione **Aderência**, especifique uma duração de `1 day` e, em seguida, **Salvar alterações**.

5. No balanceador de carga, atualize as regras do ouvinte. Selecione o balanceador de carga que você configurou para esta implantação e clique na guia **Ouvintes**

    - Para **HTTP: 80**, clique em **Exibir/editar regras**. Na página **Regras**, clique no ícone de edição (uma vez no topo da página e depois novamente na regra) para editar a regra. Exclua a regra THEN existente e substitua-a clicando em **Adicionar ação** > **Redirecionar para....** Na configuração THEN resultante, especifique `HTTPS` e a porta `443` e deixe as outras opções com as configurações padrão. Salve a configuração e clique em **Atualizar**.
    - Para **HTTP:443**, clique em **Exibir/editar regras**. Na página **Regras**, clique no ícone de edição (uma vez no topo da página e depois novamente na regra) para editar a regra. Na configuração **THEN**, em **Encaminhar para ...** altere o grupo de destino para o grupo HTTPS que você acabou de criar. Em **Aderência em nível de grupo**, ative a aderência e defina a duração para 1 dia. Salve a configuração e clique em **Atualizar**.

Etapa 6: verificar SSL

Verifique a configuração navegando para https://tableau.example.com.