Segurança da plataforma do Tableau Server

Implementando os quatro princípios da segurança empresarial

tableau

Conteúdo

Introdução

O Tableau é uma moderna plataforma de análise empresarial que permite análises de autoatendimento em grande escala por meio da governança. A segurança é a primeira parte (e também a mais essencial) de uma estratégia de governança de dados e conteúdo. O Tableau Server fornece recursos abrangentes e uma profunda integração para abordar todos os aspectos da segurança empresarial. O Tableau ajuda as organizações a promover fontes de dados confiáveis, para que todos os usuários tenham acesso aos dados corretos para tomar as decisões certas rapidamente. À medida que a promessa de um único EDW central perde a força, e a proliferação dos dados continua a se acelerar impulsionada pela nuvem, o gerenciamento consistente da segurança em todas as diversas plataformas torna-se crucial para o seu empreendimento.

Visão geral

Existem quatro componentes gerais para a segurança dos aplicativos empresariais, que este documento debaterá em maior profundidade para o Tableau Server:

1. Autenticação

2. Autorização

3. Segurança dos dados

4. Segurança de transmissões pela rede

Quando implementados corretamente, esses quatro componentes atendem a todos os requisitos de segurança empresarial e permitem que uma ampla base de usuários acesse dados confiáveis e construa relatórios, painéis e análises colaborativas. Os usuários corporativos confiam nas informações fornecidas por uma plataforma segura de dados e análises, incentivando o uso difundido e obtendo mais valor com os seus dados. O acesso externo à mesma plataforma de análises pode ser disponibilizado aos clientes e fornecedores e, ao mesmo tempo, ainda manter a conformidade com os requisitos de segurança da empresa.

O Tableau Server passou pelas rigorosas exigências de segurança dos clientes nos setores financeiro, governamental, de saúde e de ensino superior. Bancos e firmas de investimento enviam informações de investimento confidenciais diretamente aos seus clientes. Faculdades e universidades usam o Tableau Server para entregar relatórios personalizados diretamente a alunos e professores. O Tableau Server é implantado por todos os ramos das forças armadas e por muitas agências governamentais estaduais e federais. Este documento descreve como o Tableau Server fornece segurança abrangente em escala empresarial.

1 Autenticação

O Tableau Server oferece suporte a várias formas de autenticação padrão do setor, incluindo Active Directory, LDAP, Kerberos, OpenID Connect, SAML, Tickets confiáveis e certificados. O Tableau Server tem também seu próprio serviço de identidade de usuário interno, chamado de Autenticação local.

Depois que um usuário se conecta, o Tableau Server oferece uma experiência personalizável, incluindo idioma e localidade, uma página inicial personalizada e uma visão geral do conteúdo pessoalmente criado. O Tableau Server mantém as informações do usuário entre sessões para proporcionar uma experiência personalizada consistente. O Tableau faz isso criando e mantendo uma conta para cada usuário nomeado no sistema. Além disso, autores e publicadores podem usar informações de identidade no âmbito do servidor para controlar o nível de autorização que os outros usuários têm aos dados subjacentes para as exibições que eles publicam.

Identidade de usuário

Conforme mencionado acima, você pode gerenciar identidades de usuários com o Active Directory ou armazenando-as no servidor com o uso da Autenticação local. Descrevemos abaixo a diferença entre esses dois métodos de gerenciar a autenticação do usuário.

Active Directory

Quando os clientes optam por integrar o Tableau Server ao Active Directory como repositório de identidades, o Active Directory gerencia todos os nomes de usuário e senhas.

Mesmo que os usuários e grupos sejam centralmente gerenciados pelo Active Directory, o Tableau Server armazena uma cópia dos nomes de usuários e grupos em seu próprio repositório. O Tableau não armazena senhas quando configurado para autenticação via Active Directory. Usuários e grupos podem ser sincronizados com o Active Directory manualmente por um administrador ou via programação, usando o utilitário de linha de comando tabcmd ou a API REST.

Autenticação local

O Tableau Server também contém um serviço de autenticação e gerenciamento de usuários internos chamado de Autenticação local. Esse método é usado por organizações que optaram por não usar o Active Directory ou que estão fazendo implantações em clientes externos ao AD. Com a Autenticação local, o Tableau Server é responsável por gerenciar usuários, grupos e todo o processo de autenticação. O administrador tem a opção de armazenar senhas no Tableau Server. No entanto, a opção de delegar senhas e informações de usuário a um serviço externo, como o OpenID ou o SAML, também é uma possibilidade. Listas de usuários podem ser facilmente importadas para o Tableau Server, e a maioria das funções de gerenciamento de usuários pode ser realizada via programação por meio do tabcmd ou da API REST. Isso facilita o provisionamento de usuários do Tableau como parte do processo de provisionamento automatizado.

LDAP

O Tableau Server no Linux oferece suporte para autenticação em qualquer provedor LDAP, e o suporte para Windows será disponibilizado em breve. Todos os mesmos recursos de autenticação e gerenciamento de usuários disponíveis com um servidor do Active Directory estão disponíveis para qualquer serviço de diretório que ofereça suporte ao protocolo LDAP e a qualquer um dos seguintes mecanismos de autenticação: GSSAPI, associação simples, associação simples com Kerberos. Trabalhe com seu departamento de TI para determinar a opção ideal para você.

Logon único e integração com os serviços de autenticação externos

O Tableau Server oferece suporte a vários tipos de soluções de logon único (SSO), bem como SSL mútuo (autenticação de certificado do cliente).

O SSL mútuo proporciona uma experiência segura de logon automático com o Tableau em todos os dispositivos. Com o SSL mútuo, quando um cliente (Tableau Desktop no Windows, um navegador da Web ou tabcmd.exe) com um certificado válido se conecta ao Tableau Server, este último confirma a existência de um certificado de cliente válido e conecta automaticamente o usuário com o nome de usuário que ele encontra nesse certificado.

Com o SSO, os usuários não precisam se conectar explicitamente ao Tableau Server. Em vez disso, as credenciais que eles utilizam para se autenticar em outros serviços de autenticação externos (por exemplo, fazendo logon em suas redes corporativas) podem ser usadas para autenticá-los perfeitamente no Tableau Server sem requerer uma tela de logon. O SSO estabelece a identidade do usuário externamente e a mapeia para uma identidade de usuário definida no repositório de identidades do Tableau Server.

Quando você configura o Tableau Server para uso com um serviço de autenticação externo para SSO, o serviço de autenticação externo lida com toda a autenticação. No entanto, o Tableau Server gerenciará o acesso dos usuários aos recursos do Tableau com base nas funções do usuário no site definidas no repositório de identidades. Consulte a seção sobre autorização abaixo para obter mais detalhes.

O Tableau Server oferece suporte para integração com os seguintes serviços de autenticação externos:

- **SAML:** você pode configurar o Tableau Server para usar a SAML (Security Assertion Markup Language) para SSO. Com a SAML, um provedor de identidade (IdP) externo autentica as credenciais do usuário e depois envia ao Tableau Server uma declaração de segurança que fornece informações sobre a identidade do usuário. Você pode usar a SAML para acessar o Tableau Server, independentemente da sua configuração de autenticação local ou via Active Directory. Também é possível configurar o Tableau Server para usar um IdP SAML diferente para cada site, método conhecido como SAML específica para o site.

- **Kerberos:** se o Kerberos estiver habilitado no seu ambiente, e o Tableau Server estiver configurado para usar a autenticação via Active Directory, você poderá fornecer acesso ao Tableau Server para os usuários com base na sua identidade do Windows. Você não poderá usar o Kerberos se o Tableau Server estiver configurado para autenticação local.

- **Autenticação integrada do Windows:** se você tiver o Tableau Server configurado com autenticação via Active Directory, poderá habilitar o logon automático. O logon automático usa o Microsoft SSPI para conectar os usuários com base em seus nomes de usuário e senhas

do Windows. Os usuários não são solicitados a inserir credenciais, o que cria uma experiência semelhante ao logon único (SSO) e ao Kerberos.

- **OpenID:** o OpenID Connect é um protocolo de autenticação padrão que os usuários podem usar para fazer logon por meio de um provedor de identidade compatível. Após o logon bem-sucedido com seus provedores de identidade, os usuários se conectam automaticamente ao Tableau Server. Para usar o OpenID Connect com o Tableau Server, o servidor deve estar configurado para usar a autenticação local. Não há suporte para a autenticação via Active Directory.
- **Autenticação confiável:** a autenticação confiável (também conhecida como Tickets confiáveis) permite que você configure um relacionamento confiável entre o Tableau Server e um ou mais servidores Web. Quando o Tableau Server recebe solicitações de um servidor Web confiável, ele supõe que esse servidor Web já tenha manipulado a autenticação necessária. O Tableau Server recebe a solicitação com um token ou ticket resgatável e apresenta ao usuário uma exibição personalizada que leva em consideração a função e as permissões do usuário.

Usuário convidado ou acesso anônimo

Observação: essa opção só está disponível com uma licença do Tableau Server baseada em núcleo.

O Tableau Server pode ser configurado para permitir acesso anônimo a exibições por meio de uma conta de convidado. Isso é útil para a implantação de conteúdo em grandes comunidades de usuários, como a Web pública, ou para comunidades em que a identidade do usuário não é necessária, como uma intranet corporativa. A licença de convidado permite que usuários sem uma conta no Tableau Server visualizem exibições incorporadas e interajam com elas.

Para evitar o acesso anônimo acidental a dados confidenciais, a capacidade de acessar o Tableau Server como convidado está desabilitada por padrão. Quando habilitada, a licença de convidado é atribuída a um usuário convidado gerado automaticamente. Como os usuários convidados são anônimos, o que significa que não há como identificar quem são, o Tableau fornece apenas um usuário convidado, pois esse tipo de usuário é universal.

Os usuários anônimos podem carregar páginas da Web contendo exibições incorporadas sem mesmo precisarem fazer logon no Tableau Server, embora você possa optar por exigir credenciais para acesso à intranet ou à página que hospeda essas exibições. Os usuários anônimos não podem navegar no repositório. Eles só podem acessar exibições incorporadas (URLs que possuem o parâmetro: “embed=true” definido). Por questões de simplicidade, se um usuário anônimo solicitar uma exibição que não possui o sinalizador de incorporação, o Tableau Server a interpretará como uma solicitação de exibição incorporada. Isso significa que as URLs compartilhadas por e-mail ou vinculadas a partir de outras páginas da Web serão processadas corretamente para usuários anônimos e devidamente disponibilizadas. Observe que somente as exibições acessíveis para convidados (conforme definido nas permissões) serão renderizadas para usuários anônimos. Nenhuma exibição restrita para usuários convidados será processada, independentemente do sinalizador de incorporação.

A permissão de usuário convidado para o conteúdo pode ser controlada com o escopo completo de funções, permissões e segurança de dados disponíveis para todos os outros tipos de usuários no Tableau Server. Quando o Tableau Server recebe uma solicitação de exibição incorporada, ele primeiro verifica se o usuário está conectado (ou seja, se a solicitação está acompanhada por um

cookie de sessão de logon para um logon que não expirou). Se o usuário não estiver ativamente conectado, a solicitação será processada como usuário convidado, se esta opção estiver habilitada.

O acesso de usuário convidado não funcionará quando a autenticação via Active Directory estiver definida para permitir o logon automático, devido à ambiguidade no tratamento de credenciais inválidas.

Logout

Uma área de autenticação frequentemente negligenciada é o encerramento de uma sessão. O Tableau Server possui limites de tempo de sessão automáticos com base no período de inatividade. Os administradores podem alterar a duração padrão do limite de tempo de inatividade. O Tableau Server também permite que um limite de tempo de sessão absoluto seja configurado.

Ao usarem a autenticação via Active Directory com o logon automático habilitado, os usuários têm uma opção para "trocar de usuário" em vez de uma opção para "sair". Essa opção existe porque os usuários seriam automaticamente reconectados se iniciassem um logout. Para todos os outros cenários de autenticação, os usuários recebem uma opção para "sair", para que eles possam fazer logout manualmente quando encerrarem suas sessões.

Para ambientes integrados, como exibições incorporadas em um portal, é útil forçar um logout por programação no Tableau Server além do logout do portal. Isso pode ser feito facilmente chamando uma URL de logout do cliente: `https://<Tableau Server>/manual/auth/logout`.

2 Autorização

Depois de autenticar corretamente um usuário e lhe conceder acesso ao sistema, o próximo passo é autorizar quais permissões de conteúdo e servidor esse usuário possui. No Tableau Server, permissões e funções no site proporcionam aos administradores um controle granular sobre os dados, o conteúdo ou os objetos que um usuário pode acessar e sobre as ações que um usuário ou grupo pode realizar nesse conteúdo. Essas ações são muitas vezes chamadas de recursos e incluem a capacidade de visualizar e interagir, adicionar comentários, salvar pastas de trabalho e conectar-se a fontes de dados, entre outras.

Você também pode agrupar usuários para aplicar permissões em lotes com mais facilidade. O Tableau Server fornece a flexibilidade de definir permissões (permitir, negar ou não especificado/herdado) em cada conteúdo (projeto, fonte de dados, pasta de trabalho e exibições individuais em pastas de trabalho) e para os usuários/grupos especificados. Quando permissões não estiverem definidas explicitamente em um conteúdo, o Tableau aplicará um conjunto padrão de permissões. Essas permissões padrão dependerão das configurações padrão no momento em que o conteúdo foi criado e são herdadas do pai desse conteúdo. Permissões não controlam quais dados serão mostrados em uma exibição. O controle sobre o que os usuários dos dados podem visualizar é abordado mais adiante na seção Segurança do acesso aos dados.

No exemplo abaixo, todos os recursos para a amostra de exibição foram explicitamente negados aos membros do grupo de operações. Por outro lado, Joe Doe tem todos os recursos permitidos nessa exibição específica. Os membros da equipe de marketing receberam permissões para

visualizar o conteúdo, mas os recursos de edição e interação com o conteúdo não estão especificados. Isso significa que o Tableau Server verificará a cadeia, primeiro para as permissões da pasta de trabalho e depois para o projeto, para determinar se essas permissões foram autorizadas para esse grupo. Em caso negativo, essas permissões serão implicitamente negadas.

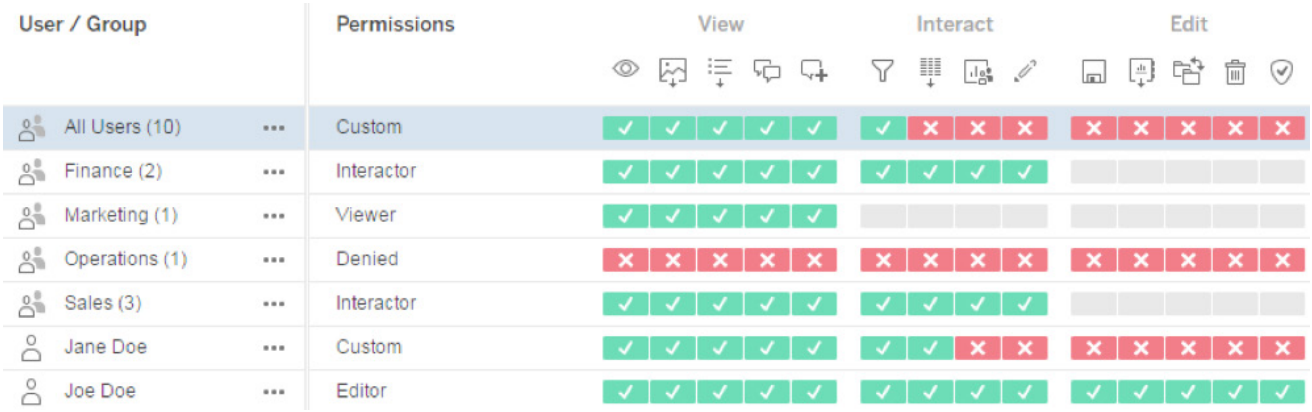

Figura 1. Definindo permissões personalizadas para grupos e usuários com base no conteúdo.

Permissões e herança padrão

O Tableau define permissões iniciais para o conteúdo por meio de um mecanismo de modelo. Ele copia do projeto padrão as permissões iniciais para um projeto. É importante que você defina a permissão no projeto padrão para que ela seja apropriada ao modelo de segurança da sua organização. Se você implantar o Tableau Server em um ambiente de autoatendimento que incentive o compartilhamento de conhecimentos e informações, também conhecido como um modelo de permissões aberto, as permissões do projeto padrão deverão incluir o grupo "Todos os usuários" e ser definidas como o modelo de função de permissões do Interagente. Dessa forma, os usuários poderão, por padrão, navegar pelo servidor e interagir com exibições publicadas, sendo apenas limitados no acesso a pastas de trabalho que possuem permissões personalizadas definidas. Se você estiver implantando o Tableau Server em um modelo de permissões fechado, no qual a segurança de dados e o controle do acesso são necessários, as permissões para o grupo "Todos os usuários" no projeto padrão deverão ser definidas como Nenhuma. Isso removerá todas as permissões para usuários e grupos por padrão. Esses usuários e grupos precisarão de uma permissão explícita para publicar e consumir conteúdo em projetos recém-criados.

Modelo de permissões de conteúdo

O conteúdo publicado inclui fontes de dados, pastas de trabalho e exibições. Permissões de conteúdo incluem as ações típicas de gerenciamento de conteúdo, como exibir, criar, modificar e excluir. Elas também incluem as interações que um usuário pode ter dentro de uma exibição. Permissões também são aplicadas quando um usuário procura conteúdo e navega pela IU do Tableau Server.

As permissões de conteúdo não mantêm a hierarquia. Em vez disso, as permissões iniciais são copiadas das permissões do pai no momento em que o item é gerado pela primeira vez. O Tableau Server também copia as permissões iniciais para uma exibição a partir das permissões da sua pasta de trabalho pai. Nenhuma alteração nas permissões do pai será reaplicada automaticamente

aos filhos, a não ser que o conteúdo seja atualizado manualmente e as permissões sejam redefinidas. O conteúdo pode ter permissões diferentes do seu pai. Estas podem ser mais rigorosas ou mais relaxadas, conforme definido pelo autor.

Modelo de permissões do usuário

Ao contrário do modelo de permissões para conteúdo, o Tableau Server fornece um modelo de herança para permissões em usuários e grupos. Se um usuário não tiver uma determinada permissão explicitamente definida, a configuração será herdada de um ou mais grupos aos quais esse usuário pertence. Na exibição do Gerenciador de permissões do Tableau Server, isso é indicado por permissões indefinidas ou caixas cinzas (consulte as figuras 1 e 2). Se um usuário e um grupo não receberem uma permissão de recurso explicitamente na cadeia de herança, esse recurso será negado. As alterações nas permissões do grupo serão propagadas para todos os usuários individuais automaticamente.

Uma dica útil para ver as permissões resultantes de um usuário ou grupo é selecionar o grupo ou usuário na página de permissões e observar a área de permissões do usuário na parte inferior. Isso permite que você veja as permissões reais para cada usuário individual depois de aplicar as configurações de herança do grupo. Focalizar o cursor do mouse sobre um recurso específico também fornece informações sobre o nome do recurso, a configuração resultante e como os resultados são determinados.

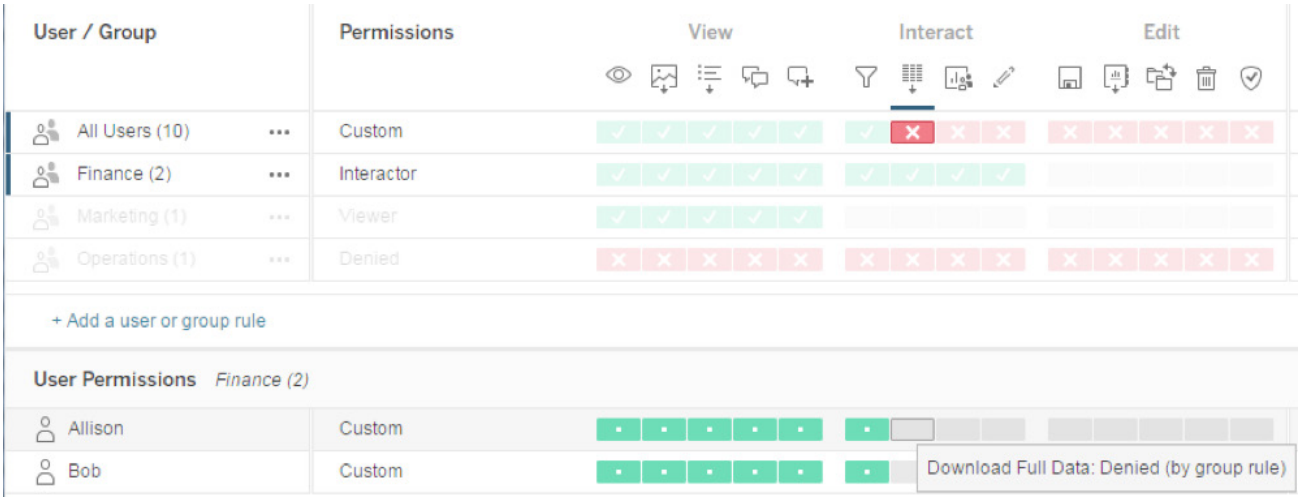

Figura 2. Exibindo as permissões resultantes de um usuário individual.

Permissões do Tableau Server

Projetos

Projetos controlam as permissões padrão para todas as pastas de trabalho, exibições e fontes de dados publicadas para o projeto. Apenas os administradores de sites e servidores podem criar e modificar projetos e suas permissões, enquanto os usuários com a permissão de "líder de projeto" podem controlar totalmente todo o conteúdo e as permissões dentro de seus projetos. Os usuários com as permissões apropriadas podem substituir as permissões padrão para qualquer conteúdo. Por exemplo, os publicadores têm a capacidade de controlar completamente as permissões de acesso ao conteúdo que eles publicam. Quando os administradores exigem mais controle sobre as

permissões em um projeto específico, eles têm a capacidade de definir e restringir as permissões desse projeto. O bloqueio de permissões no projeto significa que todo o conteúdo nele publicado usa as permissões padrão definidas pelo administrador para esse projeto. Os proprietários do conteúdo não conseguem alterar as permissões, seja no servidor ou durante o processo de publicação da pasta de trabalho. O administrador e os requisitos do próprio projeto determinam se você bloqueia permissões ou permite que os proprietários de conteúdo gerenciem as próprias permissões. Alguns projetos podem ter permissões bloqueadas, enquanto outros permanecem abertos. As permissões podem ser facilmente modificadas no futuro conforme as necessidades mudarem. Considere que pode fazer sentido bloquear permissões em alguns projetos, mas deixar outros abertos. As permissões podem ser facilmente modificadas no futuro conforme as necessidades mudarem.

Modelo de permissões	Descrições
Visualizador	Permite que o usuário ou grupo visualize as pastas de trabalho e as exibições no projeto.
Publicador	Permite que o usuário ou grupo publique pastas de trabalho e fontes de dados no servidor.
Líder do projeto	Permite que o usuário ou grupo defina permissões para todos os itens em um projeto.
Nenhuma	Define todos os recursos para a regra de permissão como **Não especificado**.
Negada	Define todos os recursos para a regra de permissão como **Negado**.
Conector de fonte de dados	Permite que o usuário ou grupo se conecte a fontes de dados no projeto.
Editor de fonte de dados	Permite que o usuário ou grupo estabeleça conexões, edite, baixe, exclua e defina permissões para uma fonte de dados nos projetos. Eles também podem publicar fontes de dados. Os proprietários de fontes de dados publicadas podem atualizar informações de conexão e extrair agendas de atualização. Essa permissão é relevante para exibições quando a exibição que eles acessam conecta-se a uma fonte de dados.

Pastas de trabalho e exibições

A lista de recursos e os modelos de função de permissão disponíveis variam dependendo de você estar definindo permissões para uma pasta de trabalho ou uma exibição. Para obter informações sobre definições de recursos, consulte a Referência de permissões.

Modelo de permissões	Descrições
Visualizador	Permite que o usuário ou grupo visualize a pasta de trabalho ou exibição no servidor.
Interagente	Permite que o usuário ou grupo visualize a pasta de trabalho ou exibição no servidor, edite exibições de pasta de trabalho, aplique filtros, visualize dados subjacentes, exporte imagens e exporte dados. Todas as outras permissões são herdadas das permissões de projeto do usuário ou grupo.
Editor	Define todos os recursos para a regra como **Permitido**.
Nenhuma	Define todos os recursos para a regra como **Não especificado**.
Negada	Define todos os recursos para a regra como **Negado**.
Personalizada	Regra definida pelo administrador para a combinação selecionada de recursos

Fontes de dados

Permissões de fontes de dados fornecem outra camada de segurança para usuários do Tableau Desktop e do Tableau Server.

Um usuário que recebe a permissão "conectar" para uma fonte de dados pode usar o Tableau Desktop para executar consultas nessa fonte de dados por meio do componente Servidor de dados do Tableau Server. O usuário tem a opção de fornecer suas próprias credenciais ou, se incluídas, as credenciais salvas do autor original. Isso significa que, para executar consultas em tempo real em um data warehouse ou em uma extração de dados do Tableau, os usuários do Tableau Desktop não precisam instalar drivers de banco de dados em suas máquinas, baixar dados nem sequer ter credenciais de banco de dados individuais. O Servidor de dados atua como um proxy, sem a necessidade de conectividade direta com o banco de dados.

Modelo de permissões	Descrições
Conector	Permite que o usuário ou grupo conecte-se à fonte de dados no servidor.
Editor	Permite que o usuário ou grupo conecte-se, baixe, exclua e defina permissões de fontes de dados no servidor. Eles também podem publicar fontes de dados e, desde que sejam proprietários de uma fonte de dados publicada, podem atualizar informações de conexão e extrair agendas de atualização (os dois últimos recursos deixarão de estar disponíveis se um administrador ou líder de projeto alterar a propriedade da fonte de dados).
Nenhuma	Define todos os recursos para a regra de permissão como **Não especificado**.
Negada	Define todos os recursos para a regra de permissão como **Negado**.

Além disso, as exibições que usam fontes de dados publicadas no Tableau Server só podem ser acessadas por usuários com permissão para a exibição e a fonte de dados subjacentes (permissões "exibir" ou "conectar" para os dados e a exibição). No entanto, se o publicador da exibição tiver optado por inserir suas credenciais na fonte de dados, os usuários com permissão para visualizar essa exibição também poderão se conectar à fonte de dados em nome do editor. Para saber mais sobre o Servidor de dados, assista ao nosso vídeo sobre o Servidor de dados.

Considerações sobre conexões

O Tableau Server cria conexões de dados automaticamente durante o processo de publicação para pastas de trabalho e fontes de dados. Isso permite que administradores e proprietários de fontes de dados controlem os atributos de conexão separadamente da exibição. Por sua vez, isso permite atualizações de credenciais ou a migração para novos servidores de banco de dados sem a necessidade de editar manualmente cada pasta de trabalho individual. Além disso, várias pastas de trabalho e fontes de dados podem aproveitar uma única conexão, aumentando o desempenho e reduzindo as duplicações. Isso também significa que os dados armazenados em cache são compartilhados entre pastas de trabalho para reduzir ainda mais a carga no seu servidor de banco de dados.

Permissões e administradores

Existem dois tipos de administradores: administradores de servidor e administradores de site. Os administradores de servidor têm acesso completo a todas as funcionalidades do servidor e do site, a todo o conteúdo no servidor e a todos os usuários. Eles também podem configurar todo o cluster do servidor, incluindo o gerenciamento de sites, usuários, tarefas de manutenção, configurações, agendas e o índice de pesquisa. Os administradores de site podem gerenciar usuários, grupos, projetos, pastas de trabalho e conexões de dados em um site. Opcionalmente, os administradores de site podem adicionar usuários ao site para cenários administrativos delegados.

Todos os administradores têm automaticamente o privilégio de publicação. Os administradores também podem criar administradores adicionais no mesmo nível.

Implantações em vários locatários

Embora o uso de grupos e projetos seja uma maneira comum para os administradores organizarem o conteúdo e concederem as devidas permissões em uma organização, a prática mais comum para oferecer suporte a várias partes externas (locatários) em um único Tableau Server é por meio do uso de sites. Na verdade, é assim que o Tableau Online, a oferta hospedada de software como servidor (SAAS) da Tableau, é implementado. O conteúdo (pastas de trabalho, fontes de dados, usuários etc.) em cada site é isolado de todos os outros conteúdos na instância do Tableau Server. Outra maneira de explicar isso é dizer que o Tableau Server oferece suporte para locação múltipla, permitindo que os administradores de servidor criem vários sites no servidor para diferentes conjuntos de usuários e conteúdos. Todo o conteúdo do servidor é publicado, acessado, gerenciado e controlado para cada site. Isso significa que fontes de dados e conexões não podem ser compartilhadas entre sites. Essa funcionalidade torna a segurança do Tableau Server robusta o suficiente para atender às demandas de implantações em instituições financeiras, de saúde e de ensino, bem como em outras instituições nas quais, em nenhuma circunstância, os clientes de uma empresa podem ver os dados dos outros clientes.

No entanto, deve notar-se que os usuários com direitos de administrador ou publicador no Tableau Server poderão ver uma lista de todos os usuários do Tableau Server (depois de definirem permissões de função para novos conteúdos). Além disso, os administradores de servidor podem ver todo o conteúdo publicado no Tableau Server, embora isso não signifique que eles terão acesso a todos os dados usados pelo Tableau Server, já que o acesso aos dados é separado das permissões de conteúdo. Isso será debatido mais detalhadamente na próxima seção.

Para obter mais informações sobre permissões no Tableau Server, consulte Tableau Server: Guia de instalação para todos.

3 Segurança do acesso aos dados

A segurança do acesso aos dados é de extrema importância em todas as empresas, especialmente para organizações com requisitos federais de regulamentação e para aquelas que estão implantando o Tableau Server em clientes externos. É fundamental que o Tableau forneça recursos robustos para permitir que os clientes incrementem suas implementações de segurança de dados existentes e reforcem quaisquer sistemas deficientes pré-existentes. O objetivo é ter um único local para impor a segurança dos dados, independentemente de os usuários estarem acessando os dados de exibições publicadas na Web e em dispositivos móveis ou por meio do Tableau Desktop.

Existem três abordagens principais para a segurança dos dados:

1. Implementar a segurança exclusivamente no banco de dados (autenticação de banco de dados)
2. Implementar a segurança unicamente no Tableau
3. Criar uma abordagem híbrida na qual as informações do usuário no Tableau Server tenham elementos de dados correspondentes no banco de dados.

O Tableau Server oferece suporte a todas as três abordagens, mas os clientes geralmente preferem a abordagem híbrida por sua simplicidade e flexibilidade, especialmente quando várias fontes de dados diferentes são utilizadas.

Ao usar a segurança do banco de dados, é importante observar que o método escolhido para autenticação no banco de dados é essencial. Esse nível de autenticação é separado da autenticação do Tableau Server discutida acima (ou seja, quando um usuário faz logon no Tableau Server, ele ainda não está fazendo logon no banco de dados). Isso significa que os usuários do Tableau Server também precisarão ter credenciais para fazer logon no banco de dados para que a segurança em nível de banco de dados seja aplicada. Para proteger ainda mais seus dados, o Tableau precisa apenas de credenciais de acesso de leitura ao banco de dados, permitindo limitar o acesso dos usuários como somente leitura. Isso evita que os publicadores alterem acidentalmente os dados subjacentes e pode resultar em um melhor desempenho de consultas em muitos casos. Como alternativa, em alguns casos, é útil dar permissão ao usuário do banco de dados para criar tabelas temporárias. Isso pode oferecer tanto vantagens de desempenho quanto de segurança, pois os dados temporários são armazenados no banco de dados, em vez de no Tableau. Existe um dilema entre conceder acesso de gravação limitado aos usuários do Tableau para criar tabelas temporárias e armazenar mais dados localmente no Tableau Server.

Você também pode limitar quais usuários visualizam determinados tipos de dados, definindo filtros de usuário em pastas de trabalho e fontes de dados para melhor controlar o que os usuários dos dados podem ver em uma exibição publicada com base em suas contas de logon do Tableau Server. Ao combinar essas técnicas, você pode publicar uma única exibição ou painel de uma maneira capaz de fornecer dados e análises personalizados e seguros a uma ampla seleção de usuários no Tableau Server.

Autenticação do banco de dados

Se os dados forem extraídos com o rápido Processador de dados do Tableau, as permissões de segurança do banco de dados não serão propagadas aos usuários finais. Ao atualizar ou incrementar extrações automaticamente, o Tableau Server usará um único conjunto de credenciais salvas para gerar extrações para cada fonte de dados (seja como o "usuário Run as" ou com as credenciais inseridas na pasta de trabalho). Ele aplicará os privilégios de segurança desse usuário ao banco de dados.

As exibições publicadas com conexões de dados em tempo real no Tableau Server são dinâmicas por sempre consultarem o banco de dados para recuperar dados atuais. Sempre que um usuário abre uma exibição e a fonte de dados é um banco de dados que exige logon (em oposição a algo como uma pasta de trabalho do Excel ou um arquivo de texto), o Tableau Server precisa saber o nome de usuário e a senha do banco de dados para estabelecer a conexão e recuperar os dados. O Tableau Server tem várias opções e configurações que funcionam em conjunto para especificar qual combinação de nome de usuário e senha de banco de dados será usada para acessar os dados. É importante manter uma distinção clara entre as técnicas de logon do Tableau Server, que são usadas para obter acesso ao Tableau Server propriamente dito, e o logon no banco de dados, que pode ser necessário para a fonte de dados. A tabela abaixo resume as opções ao criar e publicar exibições no Tableau Server:

Tipo de autenticação	Resposta do Tableau Server	O Tableau Server aproveita a segurança de dados baseada em usuário e integrada no banco de dados?
Prompt para nome de usuário e senha	O Tableau solicita a cada visualizador que insira suas próprias credenciais de banco de dados	Sim, a identidade de usuário individual é conhecida pelo banco de dados
Senha incorporada	O autor especifica as credenciais de banco de dados ao publicar a exibição. Os visualizadores não são solicitados a inserir credenciais	Não, todos os usuários compartilham o mesmo logon no banco de dados que o do autor
Credenciais de visualizador/publicador	O nome de usuário e a senha de domínio do usuário são usados para autenticação por SSO via Kerberos ou SAML	Sim, a identidade de usuário individual é conhecida pelo banco de dados
Segurança integrada do Windows (autenticação NT)	"Usuário Run as" do Tableau Server	Não, todos os usuários compartilham o mesmo logon no banco de dados
Segurança integrada do Linux (delegação ad/ kerberos)	"Usuário Run as" do Tableau Server	Sim, a identidade de usuário individual é conhecida pelo banco de dados
Personalizado		Regra definida pelo administrador para a combinação selecionada de recursos

Autenticação do Windows

O Tableau Server usa as credenciais do "usuário Run as" para se conectar ao banco de dados com o Windows. Todos os usuários do Tableau Server compartilharão as informações de conexão desse perfil para o banco de dados. Isso não usa as credenciais do publicador ou as credenciais do usuário conectado ao Tableau Server. Essa opção exige que o banco de dados utilize a segurança integrada do Windows. Isso é muito comum para implementações do SQL Server ou do SQL Server Analysis Services. Após a instalação, o "usuário Run as" padrão do Tableau Server é o usuário de Autoridade da rede. Por definição, essa conta de autoridade de rede não tem direitos para se conectar a bancos de dados. Para usar uma conta que permita a autenticação NT com fontes de dados, especifique um nome de usuário e uma senha, incluindo o nome de domínio.

Autenticação do Linux

O Tableau Server no Linux também usa as credenciais do "usuário Run as". No entanto, isso é feito de uma maneira um pouco diferente. No Linux, é necessário fornecer um arquivo de chaves para o usuário que você deseja usar como o "usuário Run as". Isso significa que você precisará estabelecer um "usuário Run as" diferente para uma determinada tarefa. Por exemplo, para se conectar a um determinado banco de dados, a fonte de dados deve usar uma fonte de dados "executada como principal" ou "executada como usuário". Os "usuários Run as" da fonte de dados devem ser usuários do domínio, e não apenas usuários locais.

Nome de usuário e senha (não incorporados)

Cada usuário do Tableau Server será solicitado a fazer logon no banco de dados com sua combinação de nome de usuário e senha específica para o banco de dados. Se você já tem a segurança de banco de dados pré-existente configurada, esta é uma boa oportunidade para aproveitar esse tipo segurança no Tableau Server. Se você ativar a opção de "credenciais salvas" na página Configurações do Tableau Server, um usuário do Tableau Server só precisará inserir credenciais uma vez para cada fonte de dados. Em seguida, o Tableau Server armazenará as credenciais da fonte de dados do usuário e as reutilizará apenas para a próxima conexão desse usuário com a mesma fonte de dados. Observe que essas credenciais são geralmente separadas daquelas usadas para fazer logon no Tableau Server. O Tableau sempre criptografa todas as senhas que estão armazenadas no Repositório do Tableau Server. As senhas de bancos de dados são criptografadas com uma chave forte. Novas chaves de ativos devem ser geradas para cada implantação usando o comando `tabadmin assetkeys`.

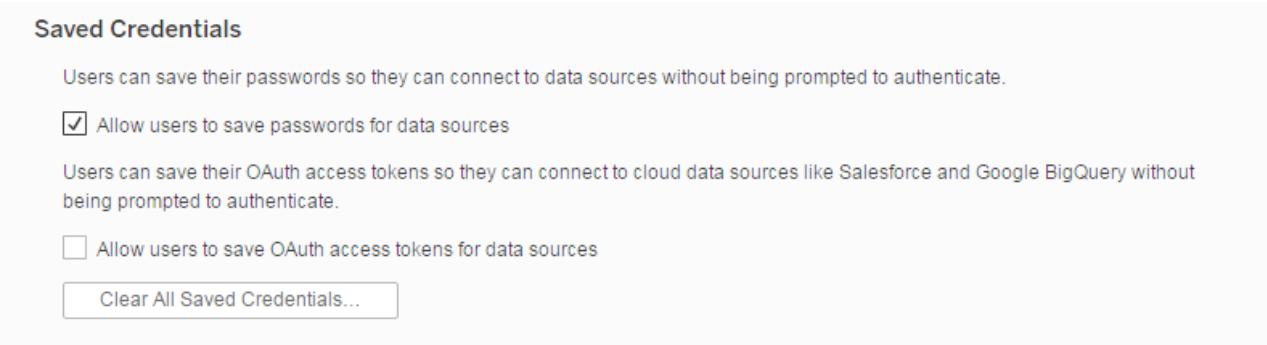

Figura 3. Configurações de credenciais salvas na página Configurações do Tableau Server.

Credenciais incorporadas (não para uso com a Autenticação do Windows)

Quando você habilita credenciais incorporadas, o Tableau Server pode memorizar o nome de usuário e a senha do autor original de cada pasta de trabalho. No momento da publicação, o autor simplesmente insere um conjunto de credenciais para o banco de dados (nome de usuário e senha) e seleciona "Inserir credenciais". Todos os usuários do Tableau Server usarão essas mesmas credenciais de conexão ao recuperarem dados dessa fonte de dados. O Tableau Server usará o mesmo mecanismo de criptografia descrito anteriormente para proteger as credenciais incorporadas no Repositório. Uma ressalva a considerar ao escolher esse método é que as senhas podem expirar, impedindo assim que os usuários acessem os dados.

Opções adicionais específicas do banco de dados

Representação

Para fontes de dados do Microsoft SQL Server, o Tableau Server oferece suporte para a representação de usuários ao executar consultas. Isso permite que o Tableau otimize a segurança que talvez já esteja implementada no Microsoft SQL Server. O Tableau se conectará ao banco de dados usando a opção de "usuário Run as" ou com credenciais inseridas. Porém, todas as consultas serão executadas como se outro usuário tivesse se conectado. A representação do Tableau foi projetada para funcionar em conjunto com implementações do SQL Server que aderem às práticas recomendadas da Microsoft para mudança de contexto usando a representação do banco de dados.

Delegação Kerberos

A delegação Kerberos permite que o Tableau Server use as credenciais Kerberos do visualizador de uma pasta de trabalho para executar uma consulta no lugar do autor. Isso é útil nas seguintes situações:

- Você precisa saber quem está acessando os dados (o nome do visualizador aparecerá nos registros de acesso da fonte de dados).
- Sua fonte de dados tem segurança no nível da linha, na qual diferentes usuários têm acesso a diferentes células.

Para que isso funcione, o banco de dados deve oferecer suporte para a delegação Kerberos. O Tableau Server requer uma delegação restrita, com a conta de "usuário Run as" possuindo direitos de delegação especificamente concedidos para os Nomes principais de servidor (SPNs) do banco de dados de destino. A delegação não está habilitada por padrão no Active Directory.

Segurança em nível de linha e representação com SQL inicial

Ao se conectar a alguns bancos de dados, é possível especificar um comando SQL inicial a ser executado quando você abrir a pasta de trabalho, atualizar uma extração, fazer logon no Tableau Server ou publicar no Tableau Server. Esse SQL inicial é diferente de uma conexão SQL personalizada, que define uma relação (tabela) com base na qual emitir consultas.

Você pode usar esse comando para:

- Configurar tabelas temporárias a serem usadas durante a sessão
- Configurar um ambiente de dados personalizado

Você pode transmitir parâmetros para sua fonte de dados em uma instrução SQL inicial.

Isso é útil por vários motivos: você pode configurar a representação usando os parâmetros **TableauServerUser** ou **TableauServerUserFull**. Caso sua fonte de dados ofereça suporte, você pode configurar a segurança em nível de linha (por exemplo, para o Oracle VPD ou o SAP Sybase ASE), para garantir que os usuários vejam apenas os dados que estão autorizados a ver.

Faixas de consulta

Para fontes de dados Teradata, o Tableau Server oferece suporte à inserção de informações do usuário na faixa de consulta. Isso pode permitir que os dados sejam restritos com base em regras de banco de dados ou em uma variedade de outras regras de fluxo de trabalho do Teradata. Além disso, o uso de uma Faixa de consulta pode aumentar o desempenho. Para que o recurso de faixas de consulta funcione no Tableau Server, você deve configurá-lo adequadamente.

Filtros de usuário

Filtros de usuário são a abordagem do Tableau Server à segurança em nível de linha. O Tableau usa a filtragem dinâmica de dados com base no nome do usuário, na associação de grupo e em outros atributos do usuário conectado. Ao executar a exibição, o Tableau Server anexará todas as consultas ao banco de dados com uma cláusula WHERE apropriada, para restringir corretamente os dados da solicitação do usuário atual. Filtros de usuário podem ser usados com todas as fontes de dados, incluindo extrações de dados.

Fontes de dados publicadas podem ser construídas com campos calculados para controlar várias dimensões ou medidas com base no nome de usuário ou na associação de grupo dos usuários conectados. Esse campo é então adicionado como um filtro de fonte de dados antes da publicação. Ao negar o recurso de download, isso torna o filtro de usuário imutável para os usuários do Tableau Desktop e do Tableau Server que se conectam à fonte de dados para análises ad hoc.

Por exemplo, uma tabela de Pedidos pode conter informações sobre o cliente (customerID), informações sobre o vendedor (employeeID) e detalhes sobre o pedido. Um único campo calculado pode ser adicionado à exibição para habilitar a filtragem de usuários: username()=customerID OU username()=employeeID. Isso permite que uma única pasta de trabalho publicada no Tableau Server forneça com segurança os dados apropriados externamente para os clientes e internamente para os vendedores. Os clientes apenas verão os pedidos que eles efetuaram, enquanto os vendedores apenas verão os pedidos vendidos, tudo isso com base em suas credenciais.

O benefício dessa abordagem é que nenhuma manutenção adicional é necessária para as exibições quando novos usuários e dados são adicionados ao sistema. As regras de filtragem são incorporadas nas exibições, e o banco de dados fornece dinamicamente as chaves para que essas regras sejam processadas.

Se não houver um conteúdo apropriado no banco de dados para identificar de forma programática quais dados devem ser fornecidos para qual usuário, um filtro de usuário manual poderá ser criado. Esse tipo de filtro de usuário é processado da mesma forma que um filtro de usuário calculado, mas não se adapta dinamicamente a novos usuários e elementos de dados. Portanto, é necessária uma manutenção adicional nas exibições.

Filtros de fontes de dados

O Tableau Server oferece suporte para a criação de filtros diretamente em uma fonte de dados, reduzindo assim a quantidade de dados retornados da fonte de dados. Por exemplo, seu banco de dados pode incluir dados dos últimos 5 a 10 anos, mas você quer apenas que os seus usuários tenham acesso aos últimos três anos de dados. Adicionar um filtro de fonte de dados facilita mostrar apenas esse cronograma.

Se você criar uma extração de uma fonte de dados que já possui filtros de fonte de dados em vigor, esses filtros serão recomendados automaticamente como filtros de extração e aparecerão na caixa de diálogo de extração. Esses filtros recomendados não precisam fazer parte da lista de filtros de extração e podem ser removidos independentemente do conjunto existente de filtros de fonte de dados.

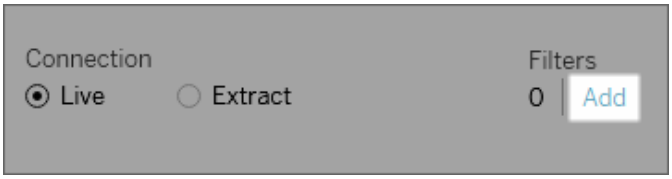

Figura 4. Adicionando filtros a fontes de dados do Tableau a partir do Tableau Desktop.

Os filtros de fontes de dados podem ser úteis para restringir o que os usuários dos dados podem ver quando você publica uma pasta de trabalho ou uma fonte de dados. Quando você publica uma fonte de dados no Tableau Server, essa fonte e todas as extrações ou arquivos associados são completamente transferidos ao servidor. Ao publicar uma fonte de dados, você pode definir permissões de acesso para baixar ou modificar a fonte de dados e também pode escolher os usuários e grupos que podem enviar consultas remotamente para essa fonte de dados por meio do Tableau Server. Quando os usuários têm a permissão de consulta, mas não a permissão de download, você pode compartilhar um amplo modelo de dados com campos calculados, aliases, grupos, conjuntos e muito mais, mas limitado apenas para consultas.

Além disso, os usuários que consultarem fontes de dados publicadas nunca poderão ver ou modificar os filtros de fonte de dados presentes na fonte de dados publicada subjacente, e todas as consultas dos usuários estarão sujeitas aos filtros dessa fonte de dados. Essa é uma ótima maneira de oferecer um subconjunto restrito dos seus dados, por exemplo, filtrando dimensões para usuários e grupos específicos ou definindo filtros de fonte de dados com base em um intervalo de datas fixas ou relativas. Isso é útil para a segurança de dados, mas também permite que você gerencie o desempenho do banco de dados remoto, que o Tableau Server acabará consultando em nome de um usuário. Para sistemas que dependem fortemente de partições ou indexação, os filtros de fonte de dados podem conferir um tremendo controle sobre o desempenho das consultas emitidas pelo Tableau.

Segurança das extrações

Quando extrações de dados são usadas, o Tableau Server é responsável por armazenar e processar os dados usados em exibições e pastas de trabalho. Os dados são armazenados no sistema de arquivos como uma extração de dados do Tableau (TDE) em um formato binário codificado e compactado. Os metadados que descrevem as extrações são armazenados em texto simples. Isso significa que os dados não são humanamente legíveis, mas podemos discernir algumas de suas descrições, como os tipos de dados, os nomes de campos e assim por diante. Para proteger esses arquivos, o Tableau Server os armazena no diretório "Dados do programa" com controles de acesso restritos ao "usuário Run as" do Tableau Server e aos administradores locais da máquina. Os arquivos de dados de extração propriamente ditos não são criptografados no disco.

Assim como outros bancos de dados aos quais o Tableau se conecta, as extrações do Processador de dados não podem ser consultadas diretamente na interface do usuário do Tableau Server. Embora os usuários possam realizar análises ao estilo arrastar e soltar, eles não podem compor sintaxes SQL, MDX ou qualquer outra sintaxe para interagir diretamente com o banco de dados do Processador de dados. Isso ajuda a impedir acesso não autorizado, injeção de SQL e outros ataques mal-intencionados a extrações.

É possível fazer integrações com soluções de sistemas operacionais e de terceiros para criptografia em nível de disco (como o BitLocker) ou criptografia em nível de arquivo e/ou diretório (como o Sistema de arquivos de criptografia, ou EFS), para melhorar ainda mais a segurança dos arquivos de extração de dados. Porém, essas soluções geralmente englobam todos os dados no disco e, portanto, a criptografia não estará limitada aos arquivos de dados do Tableau Server. Além disso, pode haver um impacto sobre o desempenho ao habilitar essas soluções.

Segurança de repositório

O Tableau Server tem um banco de dados de repositório interno que armazena informações sobre o sistema (estatísticas de uso, usuários, grupos, permissões etc.), bem como conteúdo (pastas de trabalho, exibições, comentários, tags, etc.). O Repositório não armazena os dados brutos nem os dados extraídos usados nas exibições e pastas de trabalho do Tableau.

Por padrão, o Repositório não permite conexões externas. Isso significa que o acesso às informações armazenadas no Repositório é, por padrão, restrito exclusivamente aos componentes do Tableau Server. No entanto, os clientes que quiserem ter acesso direto a essas informações poderão configurar o Repositório usando o comando tabadmin dbpass para permitir conexões externas. Conexões externas são restritas a exibições somente leitura dos dados, para evitar o uso mal-intencionado e alterações acidentais no conteúdo ou na configuração do Tableau Server. Você também pode configurar o Repositório para permitir apenas conexões SSL usando o utilitário de configuração do Tableau Server.

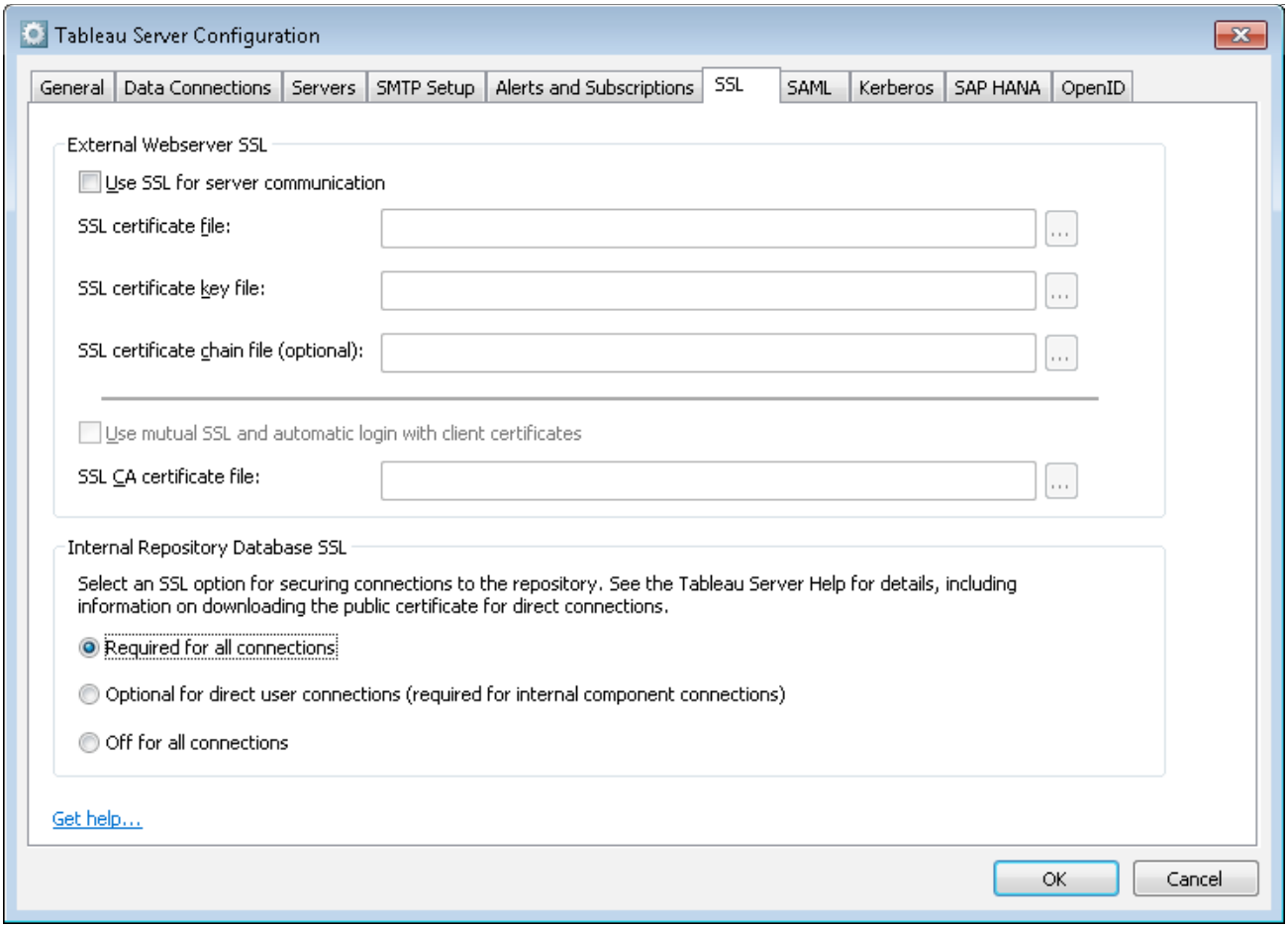

Figura 5. Configurando o SSL do banco de dados do Repositório interno

4 Segurança de transmissões pela rede

Os administradores geralmente usam dispositivos de segurança de rede para proteger o acesso ao Tableau Server implantado no local por redes não confiáveis e pela Internet. No entanto, mesmo nesses casos, as credenciais ainda precisam ser transmitidas de forma segura pela rede. Quando o acesso ao Tableau Server não é restrito, a segurança das transmissões torna-se ainda mais essencial para proteger credenciais e dados confidenciais e para impedir o uso mal-intencionado do Tableau Server. Seja qual for a sua situação, o Tableau Server possui recursos robustos de segurança de transmissão.

Existem três interfaces de rede principais para o Tableau Server: cliente para o Tableau Server, Tableau Server para o banco de dados e comunicação entre componentes do Tableau Server. Cada uma dessas interfaces está descrita abaixo. Além desses amplos recursos de segurança, o Tableau presta especial atenção ao armazenamento e às transmissões de senhas em todas as camadas e interfaces.

Cliente para o Tableau Server

Neste caso, "cliente" significa um navegador da Web, o Tableau Desktop, o tabcmd ou aplicativos de API REST. Por padrão, essas comunicações usam solicitações e respostas HTTP padrão, que são adequadas para a maioria das implantações internas. Para implantações externas ou outras implantações sensíveis, o Tableau Server pode ser configurado para HTTPS (SSL/TLS) com certificados de segurança fornecidos pelo cliente. Quando o Tableau Server está configurado para HTTPS, todos os conteúdos e comunicações entre clientes são criptografados e usam o protocolo HTTPS. O SSL/TLS deve ser habilitado para todas as implantações nas quais a segurança é uma preocupação.

Quando o Tableau Server está configurado para HTTPS, o navegador e a biblioteca HTTPS no servidor negociam um nível de criptografia comum. O Tableau usa o OpenSSL como a biblioteca HTTPS no lado do servidor e está pré-configurado para usar padrões atualmente aceitos. Cada navegador da Web que acessa o Tableau Server via SSL usa a implementação HTTPS padrão fornecida pelo navegador em questão. Isso funciona até mesmo em situações incorporadas e resulta em uma experiência perfeita para o usuário final, sem avisos de segurança, pop-ups nem exceções.

O Tableau Desktop se comunica com o Tableau Server usando HTTP ou HTTPS. A proteção da transmissão de senhas de forma segura exige que o HTTPS esteja habilitado.

Comunicação entre o Tableau Server e o banco de dados

O Tableau Server estabelece conexões dinâmicas com bancos de dados para processar conjuntos de resultados e atualizar extrações. O Tableau usa drivers nativos para se conectar a bancos de dados sempre que possível. O Tableau depende de um adaptador ODBC genérico quando os drivers nativos não estão disponíveis. Todas as comunicações com o banco de dados são roteadas através desses drivers. Desse modo, configurar o driver para se comunicar em portas não padronizadas ou fornecer criptografia de transporte faz parte da instalação do driver nativo, e esse tipo de configuração é transparente para o Tableau.

Comunicação entre os componentes do Tableau Server

Esta seção aplica-se somente a implantações distribuídas do Tableau Server. Existem dois aspectos da comunicação entre os componentes do Tableau Server: confiança e transmissão. Cada nó de servidor em um conjunto do Tableau usa um modelo de confiança rigoroso para garantir que ele esteja recebendo solicitações válidas dos outros nós no cluster. A confiança é estabelecida por uma lista de permissões de endereços IP, portas e protocolos. Se qualquer um desses componentes for inválido, a solicitação será ignorada. Todos os membros do cluster podem se comunicar entre si. Recomenda-se que o Tableau Server permaneça fora do firewall de servidores não seguros.

5 Outras considerações

Devido à natureza de orientação externa das extranets, o Tableau Server possui muitos meios de proteção internos para manter a integridade em um ambiente exposto. Por exemplo, exigimos que todas as comunicações do cliente passem por uma única porta. Além disso, fornecemos suporte para a configuração de proxies diretos e reversos, para que as comunicações entre a sua rede e a Internet possam ser mediadas usando servidores proxy.

A Tableau investiu em uma equipe de segurança interna que testa vulnerabilidades ativamente e elimina rapidamente novas ameaças com atualizações mensais. Para obter as informações mais recentes, visite nossa página de Segurança e reveja nosso whitepaper sobre desenvolvimento seguro. Por último, também é altamente recomendável rever a Lista de verificação de reforço de segurança, que fornece sugestões adicionais para proteger sua implantação do Tableau Server.

Resumo

O Tableau Server fornece um conjunto abrangente de recursos de segurança para atender às suas necessidades de implantação. O Tableau demonstrou implantações públicas bem-sucedidas em inúmeros sites de clientes e também implantações internas em redes seguras. O Tableau usa padrões modernos do setor como linha de base e é ágil em suas respostas a ameaças e problemas futuros. Desde a segurança em nível de linha até sites da Web seguros, e abrangendo todos os detalhes de segurança entre eles, o Tableau possui considerações para as suas questões de segurança construídas diretamente na nossa plataforma.

Sobre a Tableau

O Tableau ajuda as pessoas a transformar dados em informações acionáveis que causam impacto. Conecte-se facilmente a dados armazenados em qualquer lugar e em qualquer formato. Faça análises rápidas sob demanda que revelam oportunidades ocultas. Arraste e solte para criar painéis interativos com análises visuais avançadas. Em seguida, compartilhe com toda a organização e permita que seus companheiros de equipe explorem seus pontos de vista sobre os dados. De multinacionais a startups recém-fundadas e pequenas empresas, pessoas em todo o mundo usam a plataforma de análise do Tableau para ver e entender seus dados.

Recursos

Guia de reforço de segurança do Tableau Server

Guia do administrador do Tableau Server

Alta disponibilidade do Tableau Server: possibilitando análises essenciais escalonáveis

Escalabilidade do Tableau Server – Guia técnico de implantação para administradores do Tableau Server