Seguridad de la plataforma de Tableau Server

Implementación de los cuatro principios de seguridad empresarial

tableau

Contenido

Introducción

Tableau es una plataforma de análisis empresarial moderna que permite un análisis de autoservicio escalable mediante la gobernanza. La seguridad es, ante todo, lo más importante de una estrategia de gobernanza de datos y contenido. Tableau Server proporciona las funcionalidades exhaustivas y la integración profunda necesarias para abarcar todos los aspectos de la seguridad empresarial. Tableau ayuda a las organizaciones a promover fuentes de datos confiables entre todos sus usuarios. De este modo, se utilizan los datos adecuados para tomar las decisiones correctas con rapidez. Con la desvanecida promesa de un único almacén central de datos de la empresa (EDW) y la cada vez mayor proliferación de datos fomentada por la nube, una estrategia de seguridad homogénea entre las diversas plataformas se vuelve un factor fundamental para sus empresas.

Descripción general

Hay cuatro componentes generales relacionados con la seguridad de aplicaciones empresariales. En este informe, encontrará un tratamiento detallado de cada uno para Tableau Server:

1. Autenticación

2. Autorización

3. Seguridad de datos

4. Red: seguridad de la transmisión

Cuando se implementan de manera adecuada, estos cuatro componentes satisfacen todos los requisitos de seguridad empresarial y permiten que una mayor cantidad de usuarios pueda acceder a datos confiables y generar informes, dashboards y análisis colaborativos. Los usuarios corporativos confían en la información que proporciona una plataforma segura de datos y análisis. Esto promueve el uso generalizado y posibilita una mayor obtención de valor de los datos. Los clientes y contratistas también pueden tener acceso externo a la misma plataforma de análisis, sin dejar de cumplir con los requisitos de seguridad empresarial.

Tableau Server ha superado estrictos requisitos de seguridad de clientes en los sectores de los servicios financieros, gubernamentales, sanitarios y estudios superiores. Los bancos y las empresas de inversión transmiten información confidencial sobre inversiones directamente a sus clientes. Las universidades usan Tableau Server para enviar informes personalizados directamente a los estudiantes y profesores. Muchas divisiones del ejército y diversas agencias gubernamentales a nivel estatal y federal implementaron Tableau Server. En este documento, se describe cómo Tableau Server proporciona una seguridad exhaustiva a escala empresarial.

1 Autenticación

Tableau Server es compatible con varios métodos de autenticación estándar del sector, entre los que se incluyen Active Directory, LDAP, Kerberos, OpenID Connect, SAML, tickets confiables y certificados. Tableau Server también cuenta con su propio servicio incorporado de identidad de usuario denominado autenticación local.

Una vez que el usuario inicia sesión, Tableau Server proporciona una experiencia personalizable, que incluye el idioma y configuración regional, una página de inicio personalizada y una descripción general del contenido creado para el usuario. Tableau Server retiene la información del usuario entre sesiones para una experiencia homogénea y personalizada. Para lograrlo, Tableau crea y mantiene una cuenta para cada usuario reconocido en el sistema. Además, los autores y editores pueden usar información de identidad en todo el servidor para controlar el nivel de autorización que otros usuarios tienen para los datos subyacentes de las vistas que publican.

Identidad de usuario

Como se mencionó anteriormente, puede administrar las identidades de usuarios con Active Directory o con la autenticación local, que los almacena en el servidor. A continuación, describimos las diferencias existentes entre estos dos métodos para administrar la autenticación de usuarios.

Active Directory

Cuando los clientes elijen integrar Tableau Server con Active Directory como almacén de identidades, Active Directory administra todos los nombres de usuario y contraseñas.

A pesar de que Active Directory administra de manera centralizada los usuarios y grupos, Tableau Server almacena una copia de los nombres de usuario y grupos en su propio repositorio. En una configuración de autenticación de Active Directory, Tableau no almacena contraseñas. Los usuarios y grupos se pueden sincronizar con Active Directory tanto de manera manual por parte de un administrador como de manera programática mediante la utilidad de línea de comandos tabcmd o la API de REST.

Autenticación local

Tableau Server también incluye un servicio incorporado de administración y autenticación de usuarios denominado Autenticación local. Ciertas organizaciones utilizan este método cuando no desean emplear Active Directory o cuando sus clientes son ajenos a AD. Con la Autenticación local, Tableau Server es responsable de administrar usuarios, grupos y todo el proceso de autenticación. El administrador tiene la opción de almacenar las contraseñas en Tableau Server. Sin embargo, también tiene la opción de delegar la información de usuarios y contraseñas a un servicio externo, como OpenID o SAML. Las listas de usuarios se pueden importar con facilidad en Tableau Server. La mayoría de las funciones de administración de usuarios se puede realizar de manera programática a través de tabcmd o la API de REST. Esto facilita la configuración de usuarios de Tableau como parte del proceso de aprovisionamiento automatizado.

LDAP

Tableau Server en Linux incorpora compatibilidad con cualquier proveedor de LDAP para la autenticación. Próximamente, estará disponible también para Windows. Todas las mismas funciones de autenticación y administración de usuarios disponibles con el servidor de Active Directory también lo están para cualquier servicio de directorio que sea compatible con el protocolo LDAP y cualquiera de los siguientes mecanismos de autenticación: GSSAPI, enlace simple, enlace simple con Kerberos. Consulte con su departamento de TI para determinar cuál es el método que más le conviene.

Inicio de sesión único e integración con servicios de autenticación externos

Tableau Server es compatible con varios tipos de soluciones de inicio de sesión único (SSO), además de SSL mutua (autenticación con certificados de cliente).

La SSL mutua proporciona una experiencia de inicio de sesión segura y automática con Tableau para todos los dispositivos. Con la SSL mutua, cuando un cliente (Tableau Desktop en Windows, un navegador web o tabcmd.exe) con un certificado válido se conecta a Tableau Server, este confirma la existencia de un certificado de cliente válido e inicia la sesión del usuario de manera automática con el nombre de usuario que encuentra en el certificado.

Con el SSO, no es necesario que los usuarios inicien sesión explícitamente en Tableau Server. En su lugar, pueden utilizar las credenciales que utilizan con otros servicios de autenticación externos (por ejemplo, al iniciar sesión en su red corporativa) para autenticarlos sin inconvenientes en Tableau Server y sin que aparezca una pantalla de inicio de sesión. El SSO determina la identidad de usuario de manera externa y la asigna a una identidad de usuario definida en el almacén de identidades de Tableau Server.

Cuando se configura Tableau Server con un servicio de autenticación externo de SSO, dicho servicio administra todo el proceso de autenticación. Sin embargo, Tableau Server administrará el acceso de los usuarios a los recursos de Tableau sobre la base de las funciones de sitio guardadas en el almacén de identidades. Consulte la sección Autorización para conocer más detalles.

Tableau Server permite la integración con los siguientes servicios de autenticación externos:

- **SAML:** En Tableau Server, puede utilizar SAML (lenguaje de marcado de aserción de seguridad) para el SSO. Con SAML, un proveedor externo de identidades (IdP) autentica las credenciales del usuario y, luego, envía a Tableau Server una aserción de seguridad que contiene información sobre la identidad del usuario. Puede utilizar SAML para acceder a Tableau Server independientemente de su configuración de Active Directory o autenticación local. También puede configurar Tableau Server para que emplee un IdP de SAML diferente en cada sitio, lo que se conoce como SAML específico del sitio.

- **Kerberos:** Si Kerberos está habilitado en su entorno y Tableau Server está configurado para utilizar autenticación de Active Directory, puede proveer a los usuarios acceso a Tableau Server sobre la base de su identidad de Windows. No podrá usar Kerberos si configuró la autenticación local en su instancia de Tableau Server.

- **Autenticación integrada con Windows:** Si su instancia de Tableau Server tiene configurada la autenticación de Active Directory, puede habilitar el inicio de sesión automático. El inicio de sesión automático emplea SSPI de Microsoft para iniciar la sesión de los usuarios sobre la base de sus nombres de usuario y contraseñas de Windows. No se les solicitarán las credenciales a los usuarios, lo que genera una experiencia similar a la del inicio de sesión único (SSO) y Kerberos.

- **OpenID:** OpenID Connect es un protocolo de autenticación estándar que permite a los usuarios iniciar sesión a través de un proveedor de identidades compatible. Después de haber iniciado sesión correctamente con su proveedor de identidades, la sesión de los usuarios se inicia automáticamente en Tableau Server. Para utilizar OpenID Connect con Tableau Server, el servidor debe configurarse para usar la autenticación local. No es compatible con la autenticación de Active Directory.
- **Autenticación de confianza:** La autenticación de confianza (también conocida como tickets confiables) le permite configurar una relación confiable entre Tableau Server y uno o varios servidores web. Cuando Tableau Server recibe las solicitudes de un servidor web de confianza, asume que el servidor web ya resolvió la autenticación necesaria. Tableau Server recibe la solicitud con un ticket o token canjeable, y presenta al usuario una vista personalizada que tiene en cuenta la función y los permisos del usuario.

Usuario invitado o acceso anónimo

Nota: Esta opción solo está disponible para licencias de Tableau Server basadas en núcleos.

En Tableau Server, puede habilitar el acceso anónimo a vistas a través de una cuenta de invitado. Resulta útil cuando debe distribuir contenido en grandes comunidades de usuarios, como la web pública o comunidades donde la identidad del usuario no es necesaria, como una intranet corporativa. La licencia de invitado permite que los usuarios sin una cuenta de Tableau Server puedan ver e interactuar con vistas insertadas.

Para evitar que, por accidente, se acceda de manera anónima a datos confidenciales, la capacidad de acceder a Tableau Server como invitado está deshabilitada de manera predeterminada. Cuando está habilitada, la licencia de invitado se asigna a un usuario invitado generado automáticamente. Como los usuarios invitados son anónimos (es decir, no hay forma de identificar quiénes son), Tableau proporciona un solo usuario invitado, puesto que es universal.

Los usuarios anónimos pueden cargar páginas web que contienen visualizaciones insertadas sin tener que iniciar sesión en Tableau Server. Sin embargo, puede optar por solicitar las credenciales para acceder a la intranet o a la página web que hospeda la vista. Los usuarios anónimos no pueden navegar por el repositorio. Solo pueden acceder a vistas insertadas (URL que tengan el parámetro "embed=true" configurado). Para una mayor simplicidad, si un usuario anónimo solicita una vista que no tiene la marca de inserción, Tableau Server la interpretará como una solicitud de vista insertada. Esto significa que se procesarán de manera adecuada las URL compartidas por correo electrónico o provenientes de otras páginas web y estarán disponibles para usuarios anónimos. Tenga en cuenta que solo se mostrarán a los usuarios anónimos las vistas que permitan acceso de invitado (según la configuración de permisos). Todas las vistas que no tengan habilitado el acceso de invitado no se mostrarán, independientemente de si tienen o no la marca de inserción.

El permiso de usuario invitado para cierto contenido se puede controlar mediante el alcance completo de las funciones, los permisos y la seguridad de datos disponibles para todos los demás tipos de usuarios en Tableau Server. Cuando Tableau Server recibe una solicitud de vista insertada, primero verifica si el usuario tiene una sesión iniciada (es decir, si la solicitud viene acompañada de una cookie de inicio de sesión correspondiente a una sesión que no ha expirado). Si el usuario no tiene una sesión iniciada y activa, se procesa la solicitud como si fuese un usuario invitado, en el caso de que esté habilitada dicha opción.

El acceso de usuario invitado no funcionará cuando la autenticación de Active Directory esté configurada para permitir el inicio de sesión automático, debido a la ambigüedad en el momento de procesar credenciales no válidas.

Cerrar sesión

Uno de los aspectos habitualmente descuidados de la autenticación es el cierre de sesión. Tableau Server cuenta con tiempos de espera automáticos de sesión basados en la duración de la inactividad. Los administradores pueden modificar la duración predeterminada del tiempo de espera de inactividad. Tableau Server también permite la configuración de un tiempo de espera absoluto para la sesión.

Cuando emplee la autenticación de Active Directory con inicio de sesión automático, los usuarios dispondrán de la opción "Cambiar de usuario" en lugar de la opción "Cerrar sesión". Esto se debe a que su sesión se reiniciaría de manera automática en el caso de que la cerraran. Para todos los demás escenarios de autenticación, los usuarios disponen de la opción "Cerrar sesión" para poder hacerlo de manera manual cuando terminen de trabajar en su sesión.

En el caso de los entornos integrados, como las vistas insertadas en un portal, resulta útil forzar mediante programación un cierre de sesión de Tableau Server, además del cierre de sesión del portal. Esto se puede lograr fácilmente invocando una URL de cierre de sesión desde el cliente: `https://<Tableau Server>/manual/auth/logout`.

2 Autorización

Una vez que haya autenticado adecuadamente a un usuario y le haya otorgado acceso al sistema, el paso siguiente consiste en autorizar el contenido y los permisos del servidor de que dispone. Las funciones de sitio y los permisos de Tableau Server proporcionan a los administradores un control detallado de los datos, el contenido y los objetos a los que un usuario puede acceder, además de las acciones que un usuario o grupo pueden realizar en dicho contenido. A menudo, a estas acciones se las denomina funcionalidades e incluyen la capacidad de ver e interactuar, agregar comentarios, guardar libros de trabajo y conectarse a fuentes de datos, entre otras.

También puede agrupar usuarios para aplicar permisos en lotes con mayor facilidad. Tableau Server le proporciona la flexibilidad de configurar permisos (permitir, denegar o no especificado/heredado) para cada sección de contenido (proyecto, fuente de datos, libro de trabajo y vistas individuales dentro de los libros de trabajo) y para usuarios o grupos específicos. Si no se han configurado explícitamente los permisos de una sección de contenido, Tableau aplica el conjunto predeterminado de permisos. Estos permisos predeterminados dependerán de la configuración predeterminada en el momento de crear el contenido y se heredan del contenido principal al que esté vinculado el contenido anterior. Los permisos no controlan qué datos aparecen dentro de una vista. El control de lo que los usuarios pueden ver se trata más adelante en la sección Seguridad de acceso a datos.

En el ejemplo a continuación, se les denegó explícitamente a los miembros del grupo de operaciones todas las funcionalidades de la vista de muestra. Por otro lado, Joe Doe tiene permiso para utilizar todas las funcionalidades en esta vista en particular. Los miembros del grupo de marketing tienen permisos para ver el contenido, pero no se especificó si pueden interactuar con el contenido o

editarlo. Esto quiere decir que, para determinar si el grupo cuenta con estos permisos, Tableau Server verificará la cadena: en primer lugar, los permisos del libro de trabajo y, luego, los del proyecto. De lo contrario, los permisos están denegados de manera implícita.

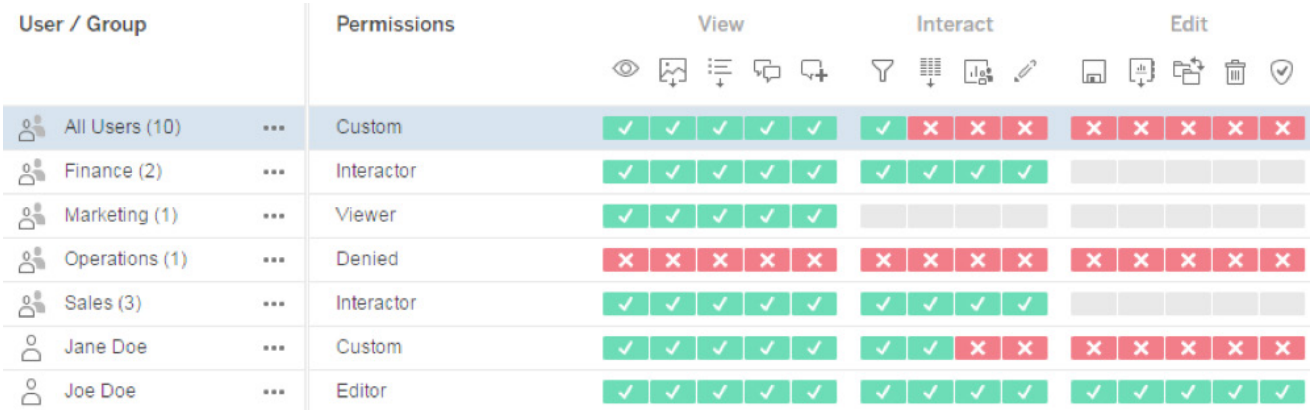

Figura 1. Configuración de permisos personalizados para grupos y usuarios sobre la base del contenido.

Permisos predeterminados y herencia

Tableau establece permisos iniciales para el contenido a través de un mecanismo de plantillas. Copia los permisos iniciales para el proyecto a partir de un proyecto predeterminado. Es importante configurar los permisos del proyecto predeterminado para que concuerden con el modelo de seguridad de su organización. Si implementa Tableau Server en un entorno de autoservicio, en el que se promueve compartir el conocimiento y la información, también conocido como modelo de permisos abierto, los permisos del proyecto predeterminado deben incluir el grupo "Todos los usuarios" configurado según la plantilla con la función de permisos Interaccionador. Luego, los usuarios podrán navegar de manera predeterminada por el servidor e interactuar con las vistas publicadas. La única limitación que tienen es el acceso a los libros de trabajo cuyos permisos estén personalizados. Si está implementando Tableau Server con un modelo de permisos cerrado, en el que se necesita mantener los datos seguros y controlar los accesos, el grupo "Todos los usuarios" del proyecto predeterminado no debería contar con ningún permiso. Se quitarán todos los permisos para los usuarios y grupos de manera predeterminada. De ser así, se deberán asignar explícitamente los permisos para publicar y consumir contenido a los usuarios y grupos en los nuevos proyectos que se creen.

Modelo de permisos para el contenido

El contenido publicado incluye fuentes de datos, libros de trabajo y vistas. Los permisos para el contenido incluyen las acciones de administración de contenido habituales, como ver, crear, modificar y eliminar. También incluyen las interacciones que un usuario puede hacer dentro de una vista. Los permisos también entran en efecto cuando un usuario busca contenido y navega por la interfaz de usuario de Tableau Server.

Los permisos sobre el contenido no mantienen el orden jerárquico. En su lugar, se copian los permisos iniciales de los permisos principales en el momento en que se genera el elemento por primera vez. Tableau Server también copia los permisos iniciales de la vista desde los permisos de su libro de trabajo principal. Cualquier cambio en los permisos del contenido principal no se replicará automáticamente en el secundario, a menos que el contenido se actualice manualmente

y se redefinan los permisos. El contenido puede tener permisos diferentes a los del contenido principal. Pueden ser más estrictos o más permisivos, dependiendo de cómo los defina el autor.

Modelo de permisos de usuario

A diferencia del modelo de permisos para el contenido, Tableau Server proporciona un modelo de herencia para los permisos de usuarios y grupos. Si un usuario no cuenta con un conjunto de permisos explícitamente establecidos, la configuración se heredará de los grupos a los que pertenezca el usuario. En la vista del administrador de permisos de Tableau Server, aparece como permisos no especificados o cuadros grises (ver figuras 1 y 2). Si a un usuario y a un grupo no se les asigna explícitamente una funcionalidad en la cadena de herencias, se les denegará la funcionalidad. Los cambios en los permisos de grupo se propagarán a todos los usuarios de manera automática.

Un consejo útil para ver los permisos resultantes para un usuario o grupo: seleccione el grupo o usuario en la página de permisos y consulte el área de permisos de usuario en la parte inferior. Esto le permite ver los permisos efectivos para cada usuario individual una vez aplicada la configuración de herencias del grupo. Al situar el puntero del mouse sobre la funcionalidad, también puede obtener información sobre el nombre de la funcionalidad, la configuración resultante y cómo se determinan los resultados.

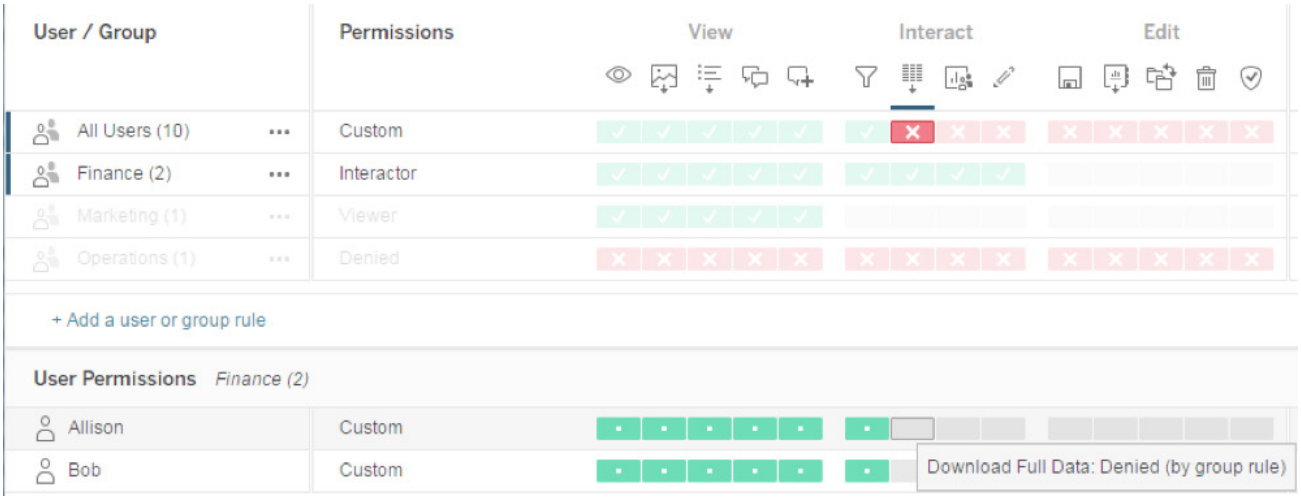

Figura 2. Consulta de los permisos resultantes para un usuario individual.

Permisos de Tableau Server

Proyectos

Los proyectos controlan los permisos predeterminados para todos los libros de trabajo, las vistas y las fuentes de datos publicados en el proyecto. Solo los administradores de sitio y servidor pueden crear y modificar proyectos y sus permisos. Los usuarios con los permisos de "líder de proyecto" pueden controlar completamente todo el contenido y los permisos dentro de sus proyectos. Los usuarios que cuenten con los permisos apropiados podrán reemplazar los permisos de cualquier parte del contenido. Por ejemplo, los editores tienen la capacidad de controlar por completo los permisos de acceso al contenido que publican. Cuando los administradores exigen

más control sobre los permisos dentro de un proyecto específico, tienen la capacidad de definir y restringir los permisos para dicho proyecto. Cuando se bloquean los permisos dentro de un proyecto, todo el contenido publicado en ese proyecto utiliza los permisos predeterminados que el administrador configuró en el proyecto. Como consecuencia, los propietarios de contenido no pueden modificar permisos, ni en el servidor ni durante el proceso de publicación de un libro de trabajo. Independientemente de si bloquea los permisos o permite que los propietarios de contenido administren los permisos ellos mismos, la última palabra la tienen el administrador y los requisitos del proyecto en sí. Algunos proyectos pueden dejar los permisos bloqueados, mientras que otros los dejan liberados. En un futuro, los permisos se pueden modificar con facilidad según las necesidades. Tenga en cuenta que, mientras que para algunos proyectos puede ser lógico bloquear los permisos, para otros será lógico dejarlos liberados. En un futuro, los permisos se pueden modificar con facilidad según las necesidades.

Plantilla de permisos	Descripciones
Observador	Permite que el usuario o grupo vea los libros de trabajo y las vistas del proyecto.
Editor	Permite que el usuario o grupo publique libros de trabajo y fuentes de datos en el servidor.
Líder de proyecto	Permite que el usuario o grupo establezca permisos para todos los elementos del proyecto.
Ninguno	Establece todas las funcionalidades para las reglas de permisos en **No especificado**.
Denegado	Establece todas las funcionalidades para las reglas de permisos en **Denegado**.
Conector de fuente de datos	Permite que el usuario o grupo se conecte a fuentes de datos del proyecto.
Editor de fuente de datos	Permite al usuario o grupo conectarse a una fuente de datos de los proyectos, además de editarla, descargarla, eliminarla y configurar sus permisos. También puede publicar fuentes de datos. Los propietarios de las fuentes de datos publicadas pueden actualizar información de conexión y extraer programas de actualización. Este permiso es pertinente para las vistas cuando la vista a la que se accede se conecta a una fuente de datos.

Libros de trabajo y vistas

La lista de funcionalidades y las plantillas de funciones de permisos disponibles varían según si configura permisos para un libro de trabajo o una vista. Para obtener las definiciones de funcionalidades, consulte la sección Referencia de permisos.

Plantilla de permisos	Descripciones
Observador	Permite que el usuario o grupo vea el libro de trabajo o vista del servidor.
Interaccionador	Permite que el usuario o grupo vea el libro de trabajo o vista del servidor, edite vistas de libros de trabajo, aplique filtros, vea datos subyacentes, y exporte imágenes y datos. Todos los demás permisos se heredan de los permisos de proyecto del usuario o grupo.
Editor	Establece todas las funcionalidades para la regla en **Permitido**.
Ninguno	Establece todas las funcionalidades para la regla en **No especificado**.
Denegado	Establece todas las funcionalidades para la regla en **Denegado**.
Personalizado	Regla definida por el administrador para la combinación seleccionada de funcionalidades.

Fuentes de datos

Los permisos de fuentes de datos proporcionan otra capa de seguridad tanto para los usuarios de Tableau Desktop como para los de Tableau Server.

Un usuario con el permiso de "conexión" para una fuente de datos puede usar Tableau Desktop para realizar consultas a dicha fuente de datos a través del componente Servidor de datos de Tableau Server. El usuario puede proporcionar sus propias credenciales o, si se incluyen, las credenciales guardadas del autor original. Esto permite que los usuarios de Tableau Desktop no necesiten instalar controladores de base de datos en sus equipos, descargar datos ni tener credenciales de base de datos individuales para ejecutar consultas en tiempo real en un almacén de datos o una extracción de datos de Tableau. El Servidor de datos funciona como un proxy sin la necesidad de disponer de conectividad directa a la base de datos.

Plantilla de permisos	Descripciones
Conector	Permite que el usuario o grupo se conecte a la fuente de datos en el servidor.
Editor	Permite al usuario o grupo conectarse a fuentes de datos del servidor, además de editarlas, descargarlas, eliminarlas y configurar sus permisos. También puede publicar fuentes de datos y, siempre y cuando sea el propietario de la fuente de datos que publica, puede actualizar la información de conexión y extraer programas de actualización. Las dos últimas funcionalidades no estarán disponibles si un administrador o líder de proyecto cambia la propiedad (pertenencia) de la fuente de datos.
Ninguno	Establece todas las funcionalidades para las reglas de permisos en **No especificado**.
Denegado	Establece todas las funcionalidades para las reglas de permisos en **Denegado**.

Además, solo los usuarios que tengan permisos tanto para la vista como para la fuente de datos subyacente (ya sean permisos de "ver" o "conectarse" para los datos y la vista) pueden acceder a las vistas que usan fuentes de datos publicadas en Tableau Server. Sin embargo, si el editor de la vista optó por insertar sus credenciales en la fuente de datos, los usuarios con permisos para ver también podrán conectarse a la fuente de datos en nombre del editor. Para obtener más información sobre el Servidor de datos, vea nuestro video sobre el Servidor de datos.

Comentario sobre las conexiones

Tableau Server crea de manera automática conexiones de datos durante el proceso de publicación tanto para libros de trabajo como para fuentes de datos. Esto permite que los administradores y los propietarios de fuentes de datos controlen los atributos de conexión por separado de la vista. De esta manera, las credenciales se pueden actualizar y se puede realizar la migración a nuevos servidores de bases de datos sin necesidad de editar manualmente cada libro de trabajo individual. Asimismo, varios libros de trabajo y fuentes de datos pueden aprovechar una única conexión, lo que mejora el rendimiento y reduce la duplicación. También permite que se compartan los datos en caché entre libros de trabajo para reducir aún más la carga en su servidor de bases de datos.

Permisos y administradores

Hay dos tipos de administradores: administradores de servidor y administradores de sitio. Los administradores de servidor tienen acceso completo a todas las funcionalidades de servidor y sitio, a todo el contenido del servidor y a todos los usuarios. También pueden configurar todo el clúster de servidores, lo que incluye administrar sitios, usuarios, mantenimiento, configuración,

programas y el índice de búsqueda. Los administradores de sitio pueden administrar usuarios, grupos, proyectos, libros de trabajo y conexiones de datos dentro de un sitio. Opcionalmente, los administradores de sitio pueden agregar usuarios al sitio para delegar tareas administrativas.

Todos los administradores tienen privilegios de publicación de manera automática. Los administradores también pueden crear otros administradores de su mismo nivel.

Implementaciones multiinquilino

Mientras que, para los administradores, el uso de grupos y proyectos es una manera común de organizar el contenido y otorgar permisos dentro de una organización, la práctica más común de tener múltiples partes externas (inquilinos) en una misma instancia de Tableau Server es a través del uso de sitios. De hecho, es así cómo se implementa Tableau Online, la oferta hospedada de software como servicio (SAAS) de Tableau. El contenido (libros de trabajo, fuentes de datos, usuarios, etc.) de cada sitio es independiente de todo el contenido restante de la instancia de Tableau Server. En otras palabras, para que Tableau Server sea compatible con la configuración multiinquilino, los administradores de servidor pueden crear diversos sitios en el servidor para diferentes conjuntos de usuarios y contenido. Es posible publicar, administrar y controlar todo el contenido del servidor, y acceder a él, individualmente para cada sitio. Esto implica que no se pueden compartir entre sitios las fuentes de datos ni las conexiones. Esta funcionalidad hace que Tableau Server sea lo suficientemente eficaz como para satisfacer las exigencias de implementaciones para servicios financieros, sanitarios, educativos y para otras instituciones en las que los clientes de una empresa no deban ver los datos de otros clientes bajo ninguna circunstancia.

Sin embargo, se debe tener en cuenta que en Tableau Server los usuarios con derechos administrativos o de publicación serán capaces de ver una lista de todos los usuarios de Tableau Server (ya que estos establecen los permisos de función para el contenido nuevo). Además, los administradores de servidor pueden ver todo el contenido publicado en Tableau Server, pero esto no implica que tengan acceso a todos los datos utilizados por Tableau Server, puesto que el acceso a los datos es independiente de los permisos para el contenido. Este aspecto se tratará con mayor profundidad en la sección siguiente.

Para obtener más información sobre permisos en Tableau Server, consulte Tableau Server: Guía de instalación para todos.

3 Seguridad de acceso a datos

La seguridad de acceso a datos es extremadamente importante para todas las empresas, pero particularmente para las organizaciones con requisitos normativos gubernamentales y aquellas que implementen Tableau Server con clientes externos. Es fundamental que Tableau proporcione funcionalidades eficaces para permitir que los clientes puedan aprovechar sus implementaciones de seguridad de datos existentes y mejorar los sistemas deficientes que ya tienen instalados. El objetivo es contar con un lugar centralizado para aplicar la seguridad de datos, independientemente de si los usuarios acceden a los datos desde vistas publicadas en la web y dispositivos móviles, o lo hacen a través de Tableau Desktop.

Hay tres enfoques principales para la seguridad de datos:

1. Implementar la seguridad únicamente dentro de la base de datos (autenticación de base de datos).
2. Implementar la seguridad únicamente en Tableau.

3. Crear una solución híbrida, en la que la información de usuarios en Tableau Server tenga elementos de datos que correspondan con algunos de la base de datos.

Tableau Server permite la implementación de los tres enfoques, pero, a menudo, los clientes se inclinan por el enfoque híbrido por su simplicidad y flexibilidad, especialmente cuando se usan fuentes de datos múltiples y diversas.

Para aprovechar al máximo la seguridad de las bases de datos, es importante tener en cuenta que el método elegido de autenticación para la base de datos es clave. Este nivel de autenticación es distinto del que se mencionó anteriormente para Tableau Server (es decir, cuando un usuario inicia sesión en Tableau Server, aún no tiene una sesión iniciada en la base de datos). Esto implica que los usuarios de Tableau Server también necesitarán credenciales para iniciar sesión en la base de datos a fin de que se pueda aplicar la seguridad en el nivel de la base de datos. Para proteger aún más sus datos, Tableau solo necesita credenciales de acceso de lectura a la base de datos. Esto le permite limitar el acceso de los usuarios al permiso de solo lectura. Así se evita que los editores modifiquen accidentalmente los datos subyacentes y, en muchos casos, contribuye a mejorar el rendimiento de las consultas. Como alternativa, en algunos casos, resulta útil otorgar permiso de usuario a la base de datos para crear tablas temporales. Esto puede tener ventajas tanto para el rendimiento como para la seguridad, ya que los datos temporales se almacenan en la base de datos, y no en Tableau. Así, se produce una compensación entre otorgar acceso de escritura limitado a los usuarios de Tableau para crear tablas temporales y almacenar más datos de manera local en Tableau Server.

También, para limitar los datos que los usuarios pueden ver, es posible configurar filtros de usuarios en libros de trabajo y fuentes de datos a fin de tener un mejor control de los datos que los usuarios pueden ver en una vista publicada sobre la base de su cuenta de inicio de sesión en Tableau Server. Con una combinación de estas técnicas, puede publicar una única vista o dashboard y, así, proporcionar datos y análisis personalizados y seguros a una gran cantidad de usuarios en Tableau Server.

Autenticación de base de datos

Si los datos se extraen con el veloz motor de datos de Tableau, los permisos de seguridad de base de datos no se propagarán a los usuarios finales. Cuando se actualizan o incrementan las extracciones de manera automática, Tableau Server utiliza un único conjunto de credenciales guardadas para generar extracciones para cada fuente de datos (ya sea con la cuenta “ejecutar como usuario” o las credenciales insertadas en el libro de trabajo). Impone los privilegios de seguridad del usuario sobre la base de datos.

En Tableau Server, las vistas publicadas con conexión de datos en tiempo real son dinámicas, puesto que consultan la base de datos cada vez para recuperar datos actualizados. Siempre que un usuario abra una vista y la fuente de datos sea una base de datos que exija un inicio de sesión (a diferencia de otro tipo de archivo, como un libro de trabajo de Excel o un archivo de texto), Tableau Server necesitará conocer el nombre de usuario y contraseña de la base de datos para conectarse y recuperar los datos. Tableau Server cuenta con diversas opciones y ajustes que trabajan solidariamente para especificar qué nombre de usuario y qué contraseña de base de datos se utilizarán para acceder a los datos. Es importante establecer una clara distinción entre las técnicas de inicio de sesión de Tableau Server, que se utilizan para acceder al propio Tableau Server, y el inicio de sesión a la base de datos, que puede ser un requisito de la fuente de datos. En la tabla siguiente se resumen las opciones de que dispone al crear y publicar vistas en Tableau Server:

Tipo de autenticación	Respuesta de Tableau Server	¿Tableau Server aprovecha la seguridad de datos basada en usuarios ya incorporada en la base de datos?
Solicitud de nombre de usuario y contraseña	Tableau solicita a cada observador que introduzca sus propias credenciales de base de datos.	Sí, la base de datos conoce la identidad de usuario individual.
Contraseña insertada	El autor especifica las credenciales de base de datos cuando se publica la vista. A los observadores no se les solicita ninguna credencial.	No, todos los usuarios comparten el mismo inicio de sesión en la base de datos, que es la del autor.
Credenciales de observador/editor	El nombre de usuario y contraseña del dominio del usuario se utilizan para la autenticación a través de SSO por medio de Kerberos o SAML.	Sí, la base de datos conoce la identidad de usuario individual.
Seguridad integrada en Windows (autenticación NT)	"Ejecutar como usuario" de Tableau Server	No, todos los usuarios comparten el mismo inicio de sesión en la base de datos.
Seguridad integrada de Linux (delegación de Kerberos/AD)	"Ejecutar como usuario" de Tableau Server	Sí, la base de datos conoce la identidad de usuario individual.
Personalizado		Regla definida por el administrador para la combinación seleccionada de funcionalidades.

Autenticación de Windows

Tableau Server emplea las credenciales de la cuenta "ejecutar como usuario" para conectarse a la base de datos en Windows. Todos los usuarios de Tableau Server compartirán esta información de conexión del perfil para la base de datos. No utiliza las credenciales del editor ni las del usuario con la sesión activa en Tableau Server. Esta opción exige que la base de datos aproveche la seguridad integrada de Windows. Esto es muy común para implementaciones de SQL Server o SQL Server Analysis Services. Tras la instalación, la cuenta "ejecutar como usuario" predeterminada para Tableau Server es el usuario Autoridad de red. Por definición, esta cuenta de autoridad de red

no tiene derechos para conectarse a bases de datos. Si desea utilizar una cuenta que aproveche la autenticación NT con fuentes de datos, especifique un nombre de usuario y contraseña, junto con el nombre de dominio.

Autenticación en Linux

Tableau Server en Linux también emplea las credenciales "ejecutar como usuario", aunque de una manera ligeramente distinta. En Linux, debe proporcionar un archivo keytab para el usuario que desea utilizar con la cuenta "ejecutar como usuario". Esto significa que deberá establecer un "ejecutar como usuario" diferente para una tarea dada. Por ejemplo, para conectarse con una base de datos específica, esta debe usar una fuente de datos con cuentas "ejecutar como entidad principal" o "ejecutar como usuario". La fuente de datos "ejecutar como usuarios" debe funcionar con los usuarios del dominio, no únicamente usuarios locales.

Nombre de usuario y contraseña (no insertados)

A cada usuario de Tableau Server se le solicitará que inicie sesión en la base de datos con su nombre de usuario y contraseña específicos de la base de datos. Si ya cuenta con una configuración de seguridad de base de datos preexistente, se recomienda aprovechar este tipo de seguridad a través de Tableau Server. Si habilita la opción "credenciales guardadas" en la página de configuración de Tableau Server, los usuarios de Tableau Server solo necesitarán introducir las credenciales una vez por cada fuente de datos. Luego, Tableau Server almacena las credenciales del usuario para la fuente de datos y las vuelve a utilizar solo para ese usuario la próxima vez que se conecte a la misma fuente de datos. Tenga en cuenta que esas credenciales son por lo general diferentes a las utilizadas para iniciar sesión en Tableau Server. Tableau siempre cifra las contraseñas que se almacenan en el repositorio de Tableau Server. Las contraseñas de base de datos están cifradas con una clave de alta seguridad. Se deben generar claves de elementos nuevas para cada implementación con el comando `tabadmin assetkeys`.

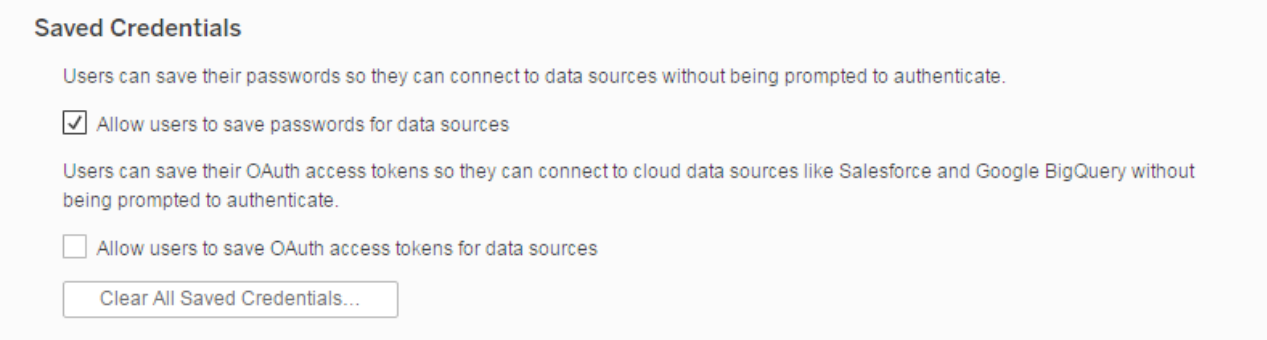

Figura 3. Configuración de credenciales guardadas en la página de configuración de Tableau Server.

Credenciales insertadas (no disponible para la autenticación de Windows)

Cuando habilita las credenciales insertadas, Tableau Server puede recordar el nombre de usuario y contraseña del autor original de cada libro de trabajo. En el momento de la publicación, el autor simplemente introduce un conjunto de credenciales para la base de datos (su nombre de usuario y contraseña) y selecciona la opción "Incrustar credenciales". Todos los usuarios de Tableau Server

utilizarán estas mismas credenciales de conexión cuando recuperen datos de esa fuente de datos. Tableau Server utilizará el mismo mecanismo de cifrado descrito anteriormente para almacenar de manera segura las credenciales insertadas en el repositorio. Debe tener en cuenta que, cuando elije este método, las contraseñas pueden caducar, lo que impedirá que los usuarios puedan acceder a los datos.

Opciones adicionales y específicas de base de datos

Suplantación

Para las fuentes de datos de Microsoft SQL Server, Tableau Server es compatible con la suplantación de usuarios cuando se ejecutan consultas. Esto permite a Tableau aprovechar la seguridad ya implementada en Microsoft SQL Server. Tableau se conectará con la base de datos mediante la opción "ejecutar como usuario" o con las credenciales insertadas. Sin embargo, todas las consultas se ejecutarán como si otro usuario estuviese conectado. La suplantación de Tableau está diseñada para funcionar junto con implementaciones de SQL Server que satisfagan las prácticas recomendadas de Microsoft para el cambio de contexto mediante la suplantación de base de datos.

Delegación de Kerberos

La delegación de Kerberos permite que Tableau Server utilice las credenciales de Kerberos del observador de un libro de trabajo para ejecutar una consulta en lugar del autor. Resulta útil en las siguientes situaciones:

- Debe saber quién accede a los datos (el nombre del observador aparecerá en los registros de acceso para la fuente de datos).
- Su fuente de datos cuenta con seguridad de nivel de fila, en la que los diferentes usuarios tienen acceso a diferentes celdas.

Para que esta opción funcione, la base de datos debe ser compatible con la delegación de Kerberos. Tableau Server requiere una delegación restringida, con derechos de delegación específicamente asignados a la cuenta "ejecutar como usuario" para los nombres de entidad de seguridad de servicio (SPN) de la base de datos de destino. La delegación no está habilitada de manera predeterminada en Active Directory.

Seguridad de nivel de fila y suplantación con SQL inicial

Al conectarse a determinadas bases de datos, puede especificar un comando de SQL inicial para que se ejecute cuando abra el libro de trabajo, actualice una extracción, inicie sesión en Tableau Server o publique en Tableau Server. Este SQL inicial es diferente de una conexión de SQL personalizado, que define una relación (tabla) sobre la que se emitirán las consultas.

Puede utilizar este comando para lo siguiente:

- Configurar tablas temporales para usar durante la sesión.
- Configurar un entorno de datos personalizado.

Puede transmitir parámetros a su fuente de datos mediante una declaración de SQL inicial.

Esto resulta útil por varias razones: Puede configurar la suplantación mediante los parámetros **TableauServerUser** o **TableauServerUserFull**. Si su fuente de datos es compatible, puede configurar seguridad de nivel de fila (por ejemplo, para Oracle VPD o SAP Sybase ASE) a fin de asegurarse de que los usuarios vean solo los datos para están autorizados a ver.

Marcado de consultas

Para las fuentes de datos Teradata, Tableau Server admite la inserción de información del usuario en la marca de consulta. De este modo, se permite que los datos se restrinjan sobre la base de las reglas de la base de datos o una variedad de otras reglas de flujo de trabajo de Teradata. Además, el uso de marcas de consultas permite mejorar el rendimiento. Para que la marca de consulta funcione en Tableau Server, la debe configurar adecuadamente.

Filtros de usuarios

Los filtros de usuarios son la manera en que Tableau Server resuelve la seguridad de nivel de fila. Tableau utiliza filtros de datos dinámicos sobre la base del nombre de usuario, la pertenencia a grupos y otros atributos del usuario con sesión activa. Cuando se ejecuta la vista, Tableau Server le agregará una cláusula WHERE apropiada a todas las consultas a la base de datos a fin de restringir adecuadamente los datos para la solicitud del usuario activo. Los filtros de usuarios se pueden utilizar con todas las fuentes de datos, lo que incluye extracciones de datos.

Las fuentes de datos publicadas se pueden generar con campos calculados para controlar una variedad de dimensiones y medidas sobre la base del nombre de usuario o la pertenencia a grupos de los usuarios activos. Luego, este campo se agrega como un filtro de fuentes de datos antes de la publicación. Si bloquea la funcionalidad de descarga, el filtro de usuario quedará inmutable para los usuarios de Tableau Desktop y Tableau Server que se conecten a la fuente de datos para realizar análisis ad hoc.

Por ejemplo, una tabla de pedidos puede contener información de los clientes (customerID), información del vendedor (employeeID) y detalles sobre el pedido. Se puede agregar un campo calculado único a la vista para habilitar el filtro de usuario: username()=customerID OR username()=employeeID. De este modo, se permite que un único libro de trabajo publicado en Tableau Server pueda enviar los datos adecuados de manera segura a los clientes, externamente, y a los vendedores, internamente. Los clientes solo verán los pedidos que cursaron, mientras que los vendedores solo verán los pedidos que vendieron, todo esto basado en las credenciales.

El beneficio de este enfoque es que no es necesario realizar mantenimiento adicional para las vistas al agregar nuevos usuarios y datos al sistema. Las reglas de filtrado se incorporan a las vistas, y la base de datos proporciona de manera dinámica las claves para que dichas reglas se procesen.

Si en la base de datos no hay contenido apto para identificar mediante programación qué datos proporcionar a qué usuario, se puede crear un filtro de usuario manual. Aunque este tipo de filtro de usuarios se procesa de la misma manera que un filtro calculado, no se adapta dinámicamente a los nuevos usuarios y elementos de datos. Por lo tanto, requiere mantenimiento adicional en las vistas.

Filtros de fuentes de datos

Tableau Server admite la creación de filtros directamente en la fuente de datos, para así reducir la cantidad de datos que se devuelven desde la fuente de datos. Por ejemplo, es posible que su base de datos incluya datos de los últimos 5 a 10 años. Sin embargo, solo desea que sus usuarios tengan

acceso a los últimos tres años de datos. La agregación de un filtro de fuentes de datos facilita la posibilidad de mostrar solo ese período.

Si crea una extracción desde una fuente de datos que ya cuenta con filtros de fuentes de datos, dichos filtros se muestran automáticamente como recomendaciones de filtros de extracción y aparecen en el diálogo de extracción. No es necesario que esos filtros recomendados aparezcan como parte de la lista de filtros de extracción; además, se pueden eliminar del conjunto de filtros de fuentes de datos existente de manera independiente.

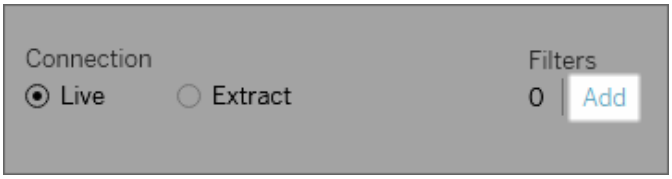

Figura 4. Agregación de filtros a fuentes de datos de Tableau desde Tableau Desktop.

Los filtros de fuentes de datos pueden resultar útiles para restringir los datos que pueden ver los usuarios cuando publica un libro de trabajo o una fuente de datos. Cuando publica una fuente de datos en Tableau Server, esta y las extracciones o los archivos asociados se transfieren en su totalidad al servidor. Cuando publica una fuente de datos, puede definir permisos de acceso para descargar o modificar la fuente de datos. También puede elegir los usuarios y grupos que podrán emitir consultas a esa fuente de datos remotamente a través de Tableau Server. Cuando los usuarios tienen permiso de consulta pero no de descarga, puede compartir un modelo de datos enriquecido que tenga campos calculados, alias, grupos y conjuntos, entre otros, pero solo limitado para consulta.

Además, los usuarios que consultan fuentes de datos publicadas nunca podrán ver ni modificar los filtros de fuentes de datos presentes en la fuente de datos subyacente publicada. Además, todas las consultas de los usuarios estarán sujetas a los filtros de esa fuente de datos. Se trata de una excelente forma de ofrecer un subconjunto restringido de datos, por ejemplo, al filtrar dimensiones para usuarios y grupos específicos, o al definir filtros de fuentes de datos basados en un rango de fechas fijo o relativo. Este método resulta útil para la seguridad de datos, pero también permite administrar el rendimiento de la base de datos remota, que Tableau Server consultará, en última instancia, en nombre del usuario. Para los sistemas que dependen en gran medida del particionamiento o el indexado, los filtros de fuentes de datos pueden proporcionar un enorme control sobre el rendimiento de las consultas realizadas por Tableau.

Seguridad de extracciones

Cuando se utilizan las extracciones de datos, Tableau Server es responsable de almacenar y procesar datos utilizados en vistas y libros de trabajo. Los datos se almacenan en el sistema de archivos como una extracción de datos de Tableau (TDE) en un formato codificado, comprimido y binario. Los metadatos que describen las extracciones se almacenan como texto sin formato. Esto significa que los datos no son legibles por parte del usuario. Sin embargo, podemos distinguir algunas descripciones de los datos, como tipos de datos o nombres de campos, entre otras. Para proteger estos archivos, Tableau Server los almacena en el directorio “Datos de programa” con controles de acceso

restringidos a la cuenta "ejecutar como usuario" de Tableau Server y a los administradores locales del equipo. Los archivos de datos de extracción propiamente dichos no están cifrados en el disco.

Al igual que otras bases de datos con las que Tableau se conecta, no se pueden consultar las extracciones del motor de datos de manera directa desde la interfaz de usuario de Tableau Server. A pesar de que los usuarios pueden realizar análisis de arrastrar y soltar, no pueden escribir SQL, MDX ni ninguna otra sintaxis para interactuar directamente con la base de datos del motor de datos. De este modo se evita el acceso no autorizado, la inyección de código SQL y otros ataques maliciosos a las extracciones.

Para mejorar aún más la seguridad de los archivos de extracciones de datos, es posible la integración con soluciones de terceros y del sistema operativo para el cifrado en el nivel de disco (por ejemplo, BitLocker) o para el cifrado en el nivel de archivo o directorio (por ejemplo, Encrypting File System o EFS). No obstante, por lo general, estas soluciones operan en todos los datos del disco, por lo que el cifrado no estará limitado a los archivos de datos de Tableau Server. Además, es posible que la habilitación de estas soluciones tenga un impacto en el rendimiento.

Seguridad del repositorio

Tableau Server cuenta con una base de datos de repositorio interno, en la que se almacena información sobre el sistema (estadísticas de uso, usuarios, grupos, permisos, etc.), además de contenido (libros de trabajo, vistas, comentarios, etiquetas, etc.). En el repositorio no se almacenan datos sin procesar o datos de extracción utilizados en vistas y libros de trabajo de Tableau.

De manera predeterminada, el repositorio no permite conexiones externas. Esto implica que el acceso a la información almacenada en el repositorio está restringido a solo los componentes de Tableau Server. Sin embargo, los clientes que deseen acceder directamente a esta información pueden configurar el repositorio mediante el comando tabadmin dbpass para permitir conexiones externas. Las conexiones externas están restringidas a vistas de solo lectura de los datos para evitar un uso malicioso y cambios accidentales en el contenido o la configuración de Tableau Server. También puede configurar el repositorio para permitir que solo las conexiones SSL utilicen la utilidad de configuración de Tableau Server.

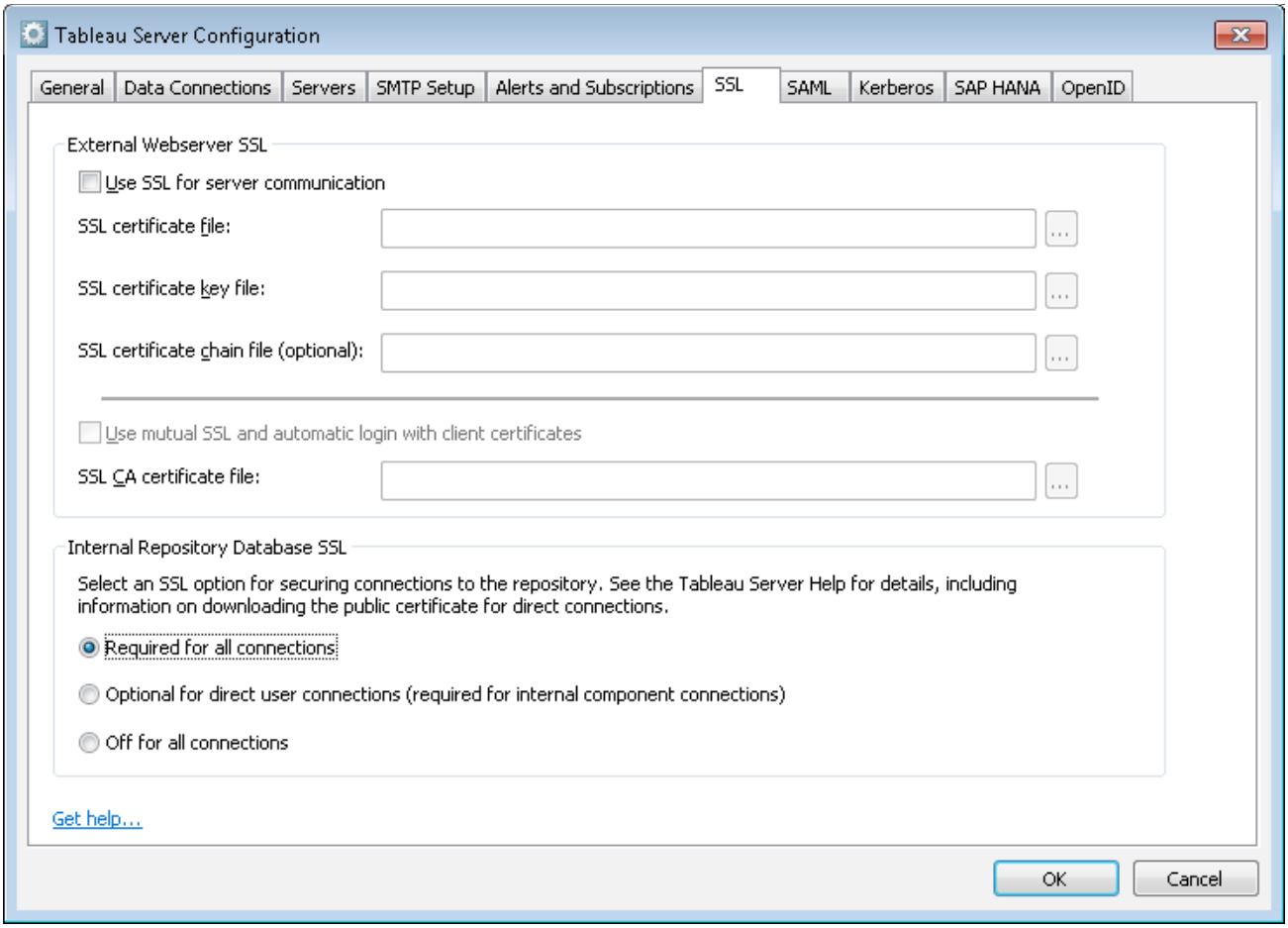

Figura 5. Configuración de la base de datos interna de repositorio SSL.

4 Red: seguridad de la transmisión

A menudo, los administradores utilizan dispositivos de seguridad de red para proteger el acceso a una instancia de Tableau Server implementada en las instalaciones físicas desde redes no confiables e Internet. Sin embargo, incluso en estos casos, las credenciales se deben transmitir de manera segura por la red. Cuando no se restringe el acceso a Tableau Server, la seguridad de transmisión se torna incluso más fundamental para proteger datos y credenciales confidenciales, y evitar el uso malicioso de Tableau Server. Independientemente de su situación, Tableau Server cuenta con funcionalidades de seguridad de transmisión eficaces.

Hay tres interfaces de red principales para Tableau Server: de cliente a Tableau Server, de Tableau Server a base de datos y las comunicaciones entre los componentes de Tableau Server. Cada una de estas interfaces se describe a continuación. Además de estas funcionalidades de seguridad generales, Tableau presta especial atención al almacenamiento y transmisión de contraseñas en todas las capas e interfaces.

De cliente a Tableau Server

En este caso, "cliente" significa un navegador web, Tableau Desktop, tabcmd o aplicaciones de la API de REST. De manera predeterminada, estas comunicaciones utilizan solicitudes y respuestas HTTP estándar que son aptas para la mayoría de implementaciones internas. Para otras implementaciones externas o confidenciales, Tableau Server se puede configurar para HTTPS (SSL/TLS) con certificados de seguridad proporcionados por el cliente. Cuando Tableau Server se configura para HTTPS, todo el contenido y las comunicaciones entre clientes están cifrados y utilizan el protocolo HTTPS. Se debe habilitar SSL/TLS para todas aquellas implementaciones en las que la seguridad sea de vital importancia.

Cuando se configura Tableau Server para HTTPS, el navegador y la biblioteca HTTPS del servidor negocian un nivel de cifrado en común. Tableau emplea OpenSSL como biblioteca HTTPS de servidor y cuenta con una configuración previa que utiliza los estándares actualmente aceptados. Cada navegador web con el que se accede a Tableau Server a través de SSL utiliza la implementación HTTPS estándar provista por ese navegador. Este método funciona incluso con inserciones y proporciona una experiencia sin inconvenientes para el usuario final, puesto que no se generan advertencias de seguridad, mensajes emergentes ni excepciones.

Tableau Desktop se comunica con Tableau Server mediante HTTP o HTTPS. La protección para la transmisión de contraseñas de manera segura requiere que HTTPS esté habilitado.

Comunicación entre Tableau Server y la base de datos

Tableau Server establece conexiones dinámicas con bases de datos para procesar conjuntos de resultados y actualizar extracciones. Tableau usa controladores nativos para conectarse a bases de datos siempre que sea posible. Tableau depende de un adaptador ODBC genérico cuando los controladores nativos no están disponibles. Todas las comunicaciones con la base de datos se realizan a través de estos controladores. De esta manera, parte de la instalación del controlador nativo es configurarlo para que se comunique a través de puertos no estándar o que proporcione cifrado de transmisión. Este tipo de configuración es inteligible para Tableau.

Comunicación entre componentes de Tableau Server

Esta sección solo se aplica a implementaciones distribuidas de Tableau Server. Hay dos aspectos importantes para la comunicación entre los componentes de Tableau Server: confianza y transmisión. Cada nodo de servidor de un clúster de Tableau utiliza un modelo de confianza estricto para garantizar que esté recibiendo solicitudes válidas de otros nodos del clúster. La fiabilidad se establece por medio de una lista de autorizaciones que contiene dirección IP, puerto y protocolo. Si alguno de estos elementos no es válido, se ignora la solicitud. Todos los miembros del clúster pueden comunicarse entre sí. Se recomienda que Tableau Server cuente con la protección de un firewall contra servidores no seguros.

5 Otras consideraciones

Debido a la evidente exposición de las extranets, Tableau Server cuenta con varios elementos de protección para mantener la integridad de un entorno expuesto. Por ejemplo, es requisito que todas las comunicaciones de clientes se realicen a través de un solo puerto. Además, proporcionamos soporte para configurar proxy inversos y de reenvío a fin de que las comunicaciones entre su red e Internet estén mediadas por servidores proxy.

Tableau invirtió en un equipo de seguridad interno que realiza activamente comprobaciones de vulnerabilidad y soluciona de manera rápida las nuevas amenazas con actualizaciones mensuales. Para obtener información actualizada, visite nuestra página de seguridad y revise nuestro informe sobre implementaciones seguras. Por último, le recomendamos enfáticamente que consulte también la Lista de comprobación de mejora de la seguridad que proporciona sugerencias adicionales para proteger su implementación de Tableau Server.

Resumen

Tableau Server proporciona un conjunto exhaustivo de funcionalidades de seguridad para satisfacer sus necesidades de implementación. Tableau cuenta con exitosas implementaciones expuestas al público en innumerables instalaciones de clientes e implementaciones internas en redes seguras. Tableau utiliza estándares modernos del sector como base y cuenta con capacidad de respuesta para amenazas y problemas futuros. Desde la seguridad de nivel de fila hasta sitios web seguros, pasando por los detalles de seguridad intermedios, Tableau tiene en cuenta sus inquietudes de seguridad y las incorpora directamente a su plataforma.

Acerca de Tableau

Tableau ayuda a las personas a transformar los datos en información útil para generar un impacto positivo. Conéctese con facilidad a datos almacenados en cualquier formato y lugar. Haga, rápidamente, análisis ad hoc que revelen oportunidades ocultas. Arrastre y suelte para crear dashboards interactivos con análisis visuales avanzados. Después, compártalos con toda su organización y permita que sus compañeros de equipo exploren los datos por sí mismos. Multinacionales, empresas pequeñas y emergentes... Todo el mundo usa la plataforma de análisis de Tableau para ver y comprender sus datos.

Recursos

Guía de mejora de la seguridad de Tableau Server

Guía del administrador de Tableau Server

Alta disponibilidad de Tableau Server: análisis imprescindibles a gran escala

Escalabilidad de Tableau Server: guía de implementación técnica para administradores de servidor