Sécurité de la plate-forme Tableau Server

Application des quatre principes clés en matière de sécurité professionnelle

tableau

Sommaire

Introduction

Tableau est une plate-forme analytique moderne qui permet des analyses en libre-service évolutives via la gouvernance. La sécurité constitue la partie la plus critique d'une stratégie de gouvernance du contenu et des données. Tableau Server propose des fonctionnalités exhaustives et une intégration poussée pour relever tous les défis en matière de sécurité professionnelle. Tableau aide les entreprises à promouvoir des sources de données de confiance, pour que tous les utilisateurs puissent accéder aux données dont ils ont besoin pour prendre rapidement des décisions éclairées. Alors que la promesse d'un entrepôt de données centralisé s'éloigne de plus en plus et que le cloud continue d'accélérer la prolifération des données, il devient indispensable pour les entreprises de garantir un niveau de sécurité cohérent pour toutes leurs plates-formes.

Vue d'ensemble

La sécurité des applications d'entreprise repose sur quatre composants majeurs que nous aborderons plus en détail dans ce document pour Tableau Server.

1. Authentification

2. Autorisation

3. Sécurité des données

4. Réseau : sécurité des transmissions

Lorsqu'ils sont correctement mis en œuvre, ces quatre composants répondent à l'ensemble des exigences de sécurité des entreprises. Un large éventail d'utilisateurs peut également accéder à des données fiables, créer des rapports ainsi que des tableaux de bord, et réaliser des analyses collaboratives. Les utilisateurs métier font confiance aux informations fournies par une plate-forme analytique de données sécurisée et sont plus enclins à les exploiter à grande échelle afin de tirer pleinement parti de leurs données. Par ailleurs, le respect de ces exigences de sécurité professionnelle est garanti lors de l'accès à cette même plate-forme par des clients et prestataires externes.

Tableau Server répond aux exigences de sécurité rigoureuses des acteurs des services financiers, des administrations, de l'enseignement supérieur et du secteur de la santé. Les banques et sociétés d'investissement communiquent des renseignements sensibles et confidentiels sur les placements directement à leurs clients. Les universités utilisent Tableau Server pour fournir des rapports personnalisés directement aux étudiants et aux membres du personnel enseignant. Enfin, Tableau Server est déployé par tous les corps des forces armées et par de nombreux organismes gouvernementaux étatiques et fédéraux. Ce document a pour but de décrire comment Tableau Server assure une sécurité optimale à l'échelle des entreprises.

1 Authentification

Tableau Server prend en charge plusieurs types d'authentification conformes aux normes du secteur, notamment Active Directory, LDAP, Kerberos, OpenID Connect, SAML, les tickets de confiance et des certificats. Tableau Server dispose également de son propre service de gestion des identités : l'authentification locale.

Une fois l'utilisateur connecté, Tableau Server lui propose une expérience personnalisée (langue et paramètres locaux, page de démarrage personnalisée et aperçu du contenu personnel). Tableau Server conserve les informations de l'utilisateur d'une session à l'autre pour garantir une expérience personnalisée et cohérente. Pour ce faire, Tableau crée et gère un compte pour chaque utilisateur identifié sur le système. Par ailleurs, les auteurs et publicateurs peuvent utiliser des informations d'identification à l'échelle du serveur afin de contrôler le niveau d'accès des autres utilisateurs aux données sous-jacentes des vues qu'ils publient.

Identité de l'utilisateur

Comme mentionné ci-dessus, vous pouvez gérer les identités des utilisateurs avec Active Directory ou en les conservant sur le serveur à l'aide de l'authentification locale. Vous trouverez ci-dessous plus de détails concernant les différences entre ces deux méthodes de gestion de l'authentification des utilisateurs.

Active Directory

Lorsque les clients optent pour l'intégration de Tableau Server à Active Directory en tant que système local de gestion des identités, ce dernier gère l'ensemble des noms d'utilisateur et des mots de passe.

Bien que les utilisateurs et les groupes soient gérés de manière centralisée par Active Directory, Tableau Server conserve une copie des informations les concernant dans son propre référentiel. Tableau ne conserve pas les mots de passe configurés dans le cadre d'une authentification par Active Directory. Les utilisateurs et les groupes peuvent être synchronisés avec Active Directory de deux manières : manuellement par un administrateur, ou à l'aide d'un programme grâce à l'utilitaire de ligne de commande tabcmd ou de l'API REST.

Authentification locale

Tableau Server intègre également un service d'authentification et de gestion des utilisateurs : l'authentification locale. Cette méthode est avant tout conçue pour les entreprises qui ne souhaitent pas utiliser Active Directory ou qui déploient la solution auprès de clients n'ayant pas recours à Active Directory. Si vous optez pour l'authentification locale, Tableau Server se charge de gérer les utilisateurs, les groupes ainsi que l'ensemble du processus d'authentification. L'administrateur peut choisir de conserver les mots de passe sur Tableau Server. Toutefois, il peut également décider de confier le stockage des mots de passe et des informations de l'utilisateur à un service externe, comme Open ID ou SAML. Les listes d'utilisateurs s'importent facilement dans Tableau Server,

et la plupart des fonctionnalités de gestion des utilisateurs peuvent être effectuées à l'aide d'un programme via tabcmd ou l'API REST. Cette méthode permet de rendre facilement opérationnels les utilisateurs Tableau dans le cadre de votre processus de mise à disposition automatisé.

LDAP

Tableau Server sous Linux prend en charge n'importe quel fournisseur d'authentification LDAP ; la prise en charge de Windows sera bientôt disponible. Les fonctionnalités d'authentification et de gestion des utilisateurs disponibles avec un serveur Active Directory le sont également pour tout service d'annuaire prenant en charge le protocole LDAP ainsi que l'un des mécanismes d'authentification suivants : GSSAPI, liaison simple et liaison simple avec Kerberos. Veuillez contacter votre service IT pour choisir la solution qui répond le mieux à vos besoins.

Authentification unique et intégration avec les services d'authentification externes

Tableau Server prend en charge plusieurs types de solutions d'authentification unique ainsi que l'authentification SSL mutuelle (authentification avec des certificats client).

L'authentification SSL mutuelle offre une connexion automatique sécurisée aux utilisateurs Tableau sur tous les appareils. Grâce à cette méthode d'authentification, lorsqu'un client (Tableau Desktop sous Windows, un navigateur Web ou tabcmd.exe) disposant d'un certificat valide se connecte à Tableau Server, la plate-forme confirme l'existence d'un certificat client valide et connecte automatiquement l'utilisateur avec le nom d'utilisateur associé au certificat.

Avec l'authentification unique, les utilisateurs ne doivent pas explicitement se connecter à Tableau Server. En effet, les informations d'identification dont ils se servent pour s'authentifier auprès d'autres services d'authentification externes (par exemple, pour se connecter au réseau de leur entreprise) peuvent être utilisées pour les authentifier dans Tableau Server sans passer par un écran de connexion. L'authentification unique établit l'identité de l'utilisateur de manière externe et l'associe à l'identité d'un utilisateur définie dans le système de gestion d'identités de Tableau Server.

Si vous configurez Tableau Server de manière à utiliser un service d'authentification externe pour l'authentification unique, le service d'authentification externe se charge de gérer l'intégralité du processus d'authentification. Cependant, Tableau Server gère l'accès aux ressources Tableau en fonction des rôles stockés dans le système local de gestion des identités. Reportez-vous à la section Autorisation pour en savoir plus.

Tableau Server s'intègre aux services d'authentification externes suivants :

- **SAML :** vous pouvez configurer Tableau Server de façon à utiliser SAML (Security Assertion Markup Language) pour l'authentification unique. Avec SAML, un fournisseur d'identités externe authentifie les informations d'identification de l'utilisateur, puis envoie une assertion de sécurité à Tableau Server qui fournit des informations sur l'identité de ce dernier. Vous pouvez utiliser SAML pour accéder à Tableau Server, peu importe la configuration de votre

authentification Active Directory ou de votre authentification locale. Vous pouvez également configurer Tableau Server afin qu'il utilise un fournisseur d'identités SAML distinct pour chaque site. Il s'agit alors d'une authentification SAML spécifique à chaque site.

- **Kerberos :** si Kerberos est activé dans votre environnement et si Tableau Server est configuré pour utiliser l'authentification Active Directory, vous pouvez permettre aux utilisateurs d'accéder à Tableau Server avec leur identité Windows. Si votre Tableau Server est configuré pour l'authentification locale, vous ne pouvez pas utiliser Kerberos.

- **Authentification Windows intégrée :** si vous avez configuré Tableau Server pour utiliser l'authentification Active Directory, vous pouvez activer la connexion automatique. La connexion automatique utilise l'interface SSPI (Security Support Provider Interface) de Microsoft pour connecter les utilisateurs en fonction de leur nom d'utilisateur et de leur mot de passe Windows. Ces derniers n'ont pas à saisir leurs informations d'identification, ce qui rend cette méthode de connexion similaire à l'authentification unique (SSO) et à Kerberos.

- **OpenID :** OpenID Connect est un protocole d'authentification standard qui permet aux utilisateurs de se connecter par l'intermédiaire d'un fournisseur d'identités compatible. Une fois l'authentification auprès de leur fournisseur d'identités établie, ils sont automatiquement connectés à Tableau Server. Pour utiliser OpenID Connect avec Tableau Server, le serveur doit être configuré pour utiliser l'authentification locale, l'authentification Active Directory n'étant pas prise en charge.

- **Authentification de confiance :** l'authentification de confiance (également appelée tickets de confiance) vous permet de configurer une relation de confiance entre Tableau Server et un ou plusieurs serveurs Web. Lorsque Tableau Server reçoit des requêtes d'un serveur Web de confiance, il présume que ce serveur s'est déjà occupé de l'authentification requise. Tableau Server reçoit la requête avec un jeton ou un ticket à utiliser, et propose à l'utilisateur une vue personnalisée qui tient compte de son rôle et des autorisations qui lui ont été octroyées.

Accès invité ou anonyme

Remarque : cette option est disponible uniquement pour les licences Tableau Server basées sur les cœurs.

Tableau Server peut être configuré de manière à autoriser un accès anonyme aux vues à l'aide d'un compte invité. Cette option est particulièrement utile lorsque vous partagez du contenu avec de vastes communautés d'utilisateurs (par exemple, sur un site Web public) ou avec des communautés qui n'imposent pas à l'utilisateur de s'authentifier (par exemple, sur l'Intranet d'une entreprise). La licence Invité permet aux utilisateurs ne disposant pas d'un compte Tableau Server de consulter des vues intégrées et d'interagir avec.

Pour éviter tout accès anonyme involontaire à des données sensibles, l'accès à Tableau Server en tant qu'invité est désactivé par défaut. Lorsque cette option est activée, la licence Invité est attribuée à un utilisateur invité généré automatiquement. Étant donné que les utilisateurs invités sont anonymes et qu'il n'existe aucun moyen de les identifier, Tableau ne génère qu'un seul utilisateur invité, car celui-ci est universel.

Les utilisateurs anonymes peuvent charger des pages Web contenant des visualisations intégrées sans avoir à se connecter à Tableau Server, mais vous pouvez exiger des informations d'identification pour accéder à l'Intranet ou à la page hébergeant la vue. Les utilisateurs anonymes ne peuvent pas parcourir le référentiel ; seules les vues intégrées leur sont accessibles (les URL pour lesquelles le paramètre « embed=true » est défini). Par souci de simplicité, si un utilisateur anonyme demande à consulter une vue qui ne possède pas de paramètre « embed », Tableau Server l'interprétera comme une demande de consultation d'une vue intégrée. Cela signifie que les URL partagées par e-mail ou liées à d'autres pages Web seront traitées correctement pour les utilisateurs anonymes et que ces derniers pourront y accéder. Notez que seules les vues accessibles à l'utilisateur Invité (tel que défini dans les autorisations) peuvent être visualisées par les utilisateurs anonymes. Les vues que les utilisateurs invités n'ont pas le droit de consulter ne s'afficheront pas, quel que soit le statut du paramètre « embed ».

Les autorisations d'accès au contenu de l'utilisateur Invité peuvent être contrôlées à l'aide de tous les rôles, de toutes les autorisations et de toutes les fonctionnalités de sécurité des données dont les autres types d'utilisateurs de Tableau Server disposent. Lorsque Tableau Server reçoit une demande de consultation d'une vue intégrée, le logiciel vérifie d'abord si l'utilisateur est connecté (la demande s'accompagne d'un cookie de session de connexion si la connexion est toujours valide). Lorsque cette option est activée, si l'utilisateur n'est pas activement connecté, la requête est traitée comme si elle provenait d'un utilisateur invité.

L'accès invité ne fonctionnera pas si la connexion automatique a été activée avec l'authentification Active Directory. Cela permet d'éviter toute ambiguïté concernant le traitement d'informations d'identification non valides.

Déconnexion

La fermeture d'une session est un aspect de l'authentification trop souvent négligé. Tableau Server propose des délais d'expiration de session automatique en fonction de la durée de l'inactivité. Les administrateurs peuvent modifier la durée d'inactivité par défaut avant l'expiration de la session. Tableau Server permet également de configurer le délai d'expiration absolu d'une session.

Les utilisateurs ayant opté pour l'authentification Active Directory et activé la connexion automatique peuvent choisir de « changer d'utilisateur » plutôt que de « se déconnecter ». En effet, avec une telle configuration, le lancement de la procédure de déconnexion les reconnecterait automatiquement. Dans tous les autres cas de figure, les utilisateurs disposent d'une option de déconnexion qui leur permet de se déconnecter manuellement à la fin de leur session.

Pour les environnements intégrés, tels que des vues intégrées au sein d'un portail, il peut être utile de programmer la déconnexion automatique sur Tableau Server en plus de la déconnexion du portail. Vous pouvez le faire très facilement en appelant une URL de déconnexion depuis le client : `https://<Tableau Server>/manual/auth/logout`.

2 Autorisation

Après avoir authentifié un utilisateur et lui avoir octroyé l'accès au système, l'étape suivante consiste à déterminer le contenu qu'il peut consulter ainsi que ses autorisations sur le serveur. Dans Tableau Server, le rôle sur le site et les autorisations permettent aux administrateurs de contrôler avec précision les données, le contenu et les objets auxquels un utilisateur peut accéder, ainsi que les actions qu'un utilisateur ou groupe d'utilisateurs peut exécuter avec ce contenu. Ces actions sont généralement des fonctionnalités qui permettent, entre autres, de consulter du contenu et d'interagir avec, d'ajouter des commentaires, d'enregistrer des classeurs et de se connecter à des sources de données.

Vous pouvez également regrouper des utilisateurs afin d'attribuer des autorisations à un groupe plus facilement. Grâce à Tableau Server, vous pouvez définir des autorisations (autoriser, refuser, non spécifié/hérité) pour chaque élément de contenu (projet, source de données, classeur et vues individuelles au sein des classeurs) et pour des utilisateurs ou groupes en particulier. Lorsqu'aucune autorisation n'est explicitement définie pour un contenu en particulier, Tableau définit un ensemble d'autorisations par défaut. Celles-ci dépendent des paramètres par défaut au moment de la création du contenu en question et correspondent aux autorisations du parent de ce contenu. Les autorisations ne permettent pas de contrôler les données qui apparaissent dans une vue. Le contrôle des données auxquelles les utilisateurs ont accès sera abordé dans la section intitulée Sécurité en matière d'accès aux données.

Dans l'exemple ci-dessous, les membres du groupe Operations n'ont accès à aucune fonctionnalité de la vue. En revanche, Joe Doe peut, quant à lui, utiliser toutes les fonctionnalités. Les membres de l'équipe Marketing ont été autorisés à consulter le contenu. Toutefois, les fonctionnalités relatives à l'interaction avec ce contenu et à la modification de celui-ci n'ont pas été définies. Tableau Server vérifiera alors la chaîne du contenu parent, en commençant par les autorisations du classeur, puis celles du projet, pour voir si elles ont été attribuées à ce groupe. Dans le cas contraire, ces autorisations leur seront refusées de manière implicite.

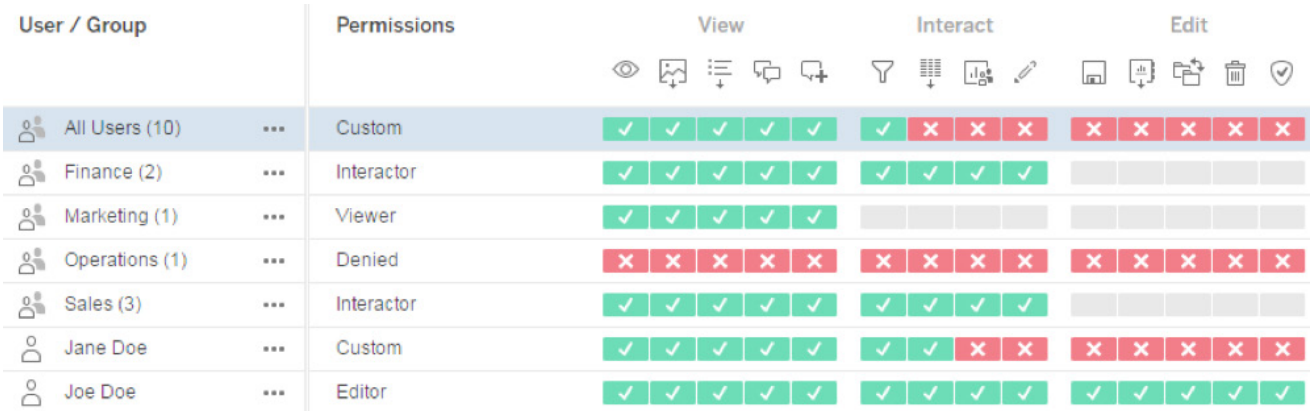

Figure 1 : Attribution des autorisations personnalisées pour les groupes et utilisateurs en fonction du contenu

Autorisations par défaut et héritées

Tableau définit des autorisations initiales pour le contenu via un système de modèles. La solution propage les autorisations initiales du projet par défaut à un projet donné. Les autorisations attribuées au projet par défaut doivent impérativement être adaptées au modèle de sécurité de votre organisation. Si vous déployez Tableau Server dans un environnement en libre-service où la connaissance et l'échange d'informations sont encouragés, soit un modèle d'autorisations ouvert, les autorisations par défaut du projet doivent inclure le groupe « Tous les utilisateurs » et être définies sur le modèle d'autorisations du rôle Interacteur. Les utilisateurs pourront alors, par défaut, parcourir le serveur et interagir avec les vues publiées. L'accès ne sera limité que pour les classeurs ayant des autorisations personnalisées définies. Si vous déployez Tableau Server avec un modèle d'autorisations fermé afin de garantir la sécurité des données et de contrôler l'accès aux données, aucune autorisation pour le groupe « Tous les utilisateurs » ne doit être spécifiée dans le projet par défaut. Cela permet de retirer, par défaut, toutes les autorisations pour les utilisateurs et les groupes. Les utilisateurs et les groupes devront alors obtenir des autorisations explicites pour publier et consulter du contenu dans les nouveaux projets.

Modèle d'autorisations de contenu

Le contenu publié comprend les sources de données, les classeurs et les vues. Les autorisations de contenu comprennent les actions de gestion de contenu classiques telles que l'affichage, la création, la modification et la suppression. Elles comprennent également les interactions qu'un utilisateur peut effectuer au sein d'une vue. Ces autorisations s'appliquent également lorsque l'utilisateur recherche du contenu et parcourt l'interface utilisateur de Tableau Server.

Les autorisations de contenu ne conservent aucun niveau de hiérarchie ; les autorisations initiales sont copiées à partir des autorisations du parent lors de la création initiale du contenu. Tableau Server copie également les autorisations initiales pour une vue à partir des autorisations de son classeur parent. Les modifications apportées aux autorisations du parent ne se propageront pas automatiquement au contenu subordonné, à moins que le contenu ne soit actualisé manuellement et que les autorisations ne soient redéfinies. Le contenu peut avoir des autorisations différentes de celles de son parent. Elles peuvent être plus ou moins rigoureuses, selon la façon dont l'auteur les configure.

Modèle d'autorisations utilisateur

À l'inverse du modèle d'autorisations de contenu, Tableau Server propose un modèle d'héritage pour les autorisations attribuées aux utilisateurs et aux groupes. Si aucune autorisation explicite n'a été définie pour un utilisateur, le paramètre sera hérité du ou des groupes auxquels l'utilisateur appartient. Dans la vue Gestionnaire des autorisations de Tableau Server, cela se traduit par des autorisations non spécifiées représentées par des cases grisées (cf. figures 1 et 2). Si une fonctionnalité n'est pas explicitement octroyée à un utilisateur ou à un groupe dans la chaîne des héritages, ces derniers ne pourront pas l'utiliser. Les modifications apportées aux autorisations de groupe se propageront automatiquement à tous les utilisateurs individuels.

Pour consulter les nouvelles autorisations attribuées à un utilisateur ou à un groupe, il est conseillé de sélectionner le groupe ou l'utilisateur sur la page des autorisations et de consulter la section Autorisations utilisateur en bas de la page. Vous y trouverez les autorisations effectives octroyées à chaque utilisateur après avoir appliqué les paramètres d'héritage du groupe. Survoler une fonctionnalité spécifique permet d'obtenir des informations concernant le nom de la fonctionnalité, le paramètre actualisé et la façon dont les résultats ont été déterminés.

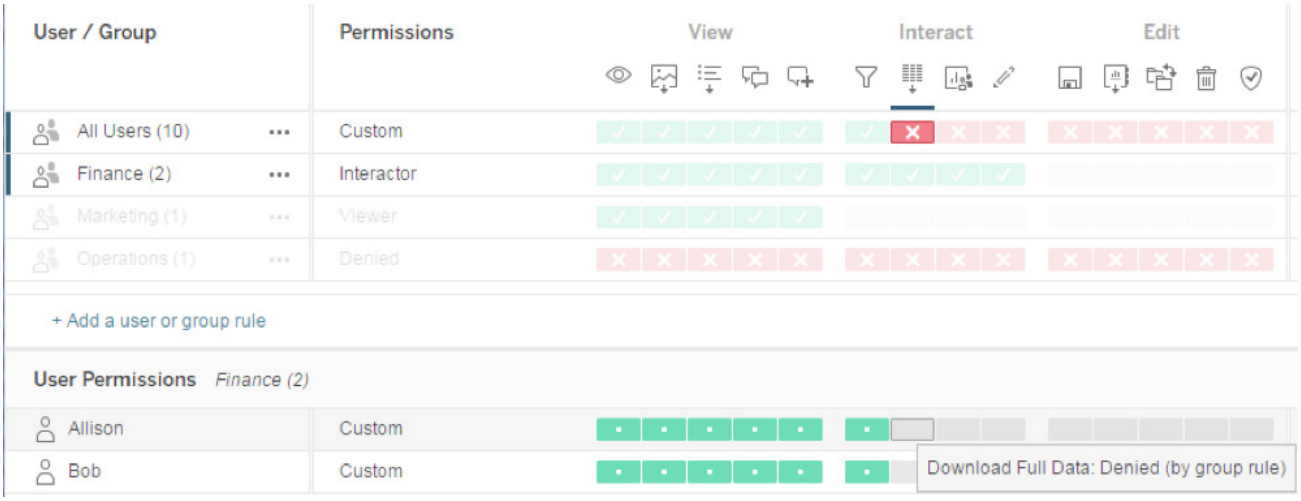

Figure 2 : Affichage des nouvelles autorisations d'un utilisateur

Autorisations Tableau Server

Projets

Les projets servent à contrôler les autorisations par défaut pour l'ensemble des classeurs, des vues et des sources de données publiés vers le projet. Seuls les administrateurs de site et de serveur peuvent créer et modifier des projets ainsi que leurs autorisations. Les utilisateurs disposant de l'autorisation « Responsable du projet » peuvent contrôler l'ensemble du contenu et des autorisations au sein de leurs projets. Les utilisateurs qui possèdent des autorisations adéquates peuvent modifier les autorisations par défaut d'un élément de contenu spécifique. Les publicateurs disposent par exemple d'un contrôle total sur les autorisations d'accès au contenu qu'ils publient. Lorsque les administrateurs exigent davantage de contrôle sur les autorisations au sein d'un projet spécifique, ils peuvent définir et limiter les autorisations du projet en question. Le verrouillage des autorisations au sein d'un projet signifie que tout le contenu publié dans celui-ci utilise les autorisations par défaut définies par l'administrateur sur ce projet. Les propriétaires de contenu ne pourront dès lors plus modifier les autorisations, que ce soit sur le serveur ou pendant le processus de publication des classeurs. Que vous choisissiez de verrouiller les autorisations ou de permettre aux propriétaires de contenu de les gérer eux-mêmes, la décision finale reviendra toujours à l'administrateur et dépendra des exigences du projet. Certains projets peuvent contenir des autorisations verrouillées, d'autres non. Les autorisations peuvent facilement être modifiées ultérieurement selon vos besoins. Gardez à l'esprit qu'il peut être intéressant de verrouiller les

autorisations de certains projets, tout comme il peut être pertinent d'autoriser leur modification pour d'autres projets. Les autorisations peuvent facilement être modifiées ultérieurement selon vos besoins.

Modèle d'autorisations	Descriptions
Observateur	Autorise l'utilisateur ou le groupe à voir les classeurs et les vues du projet.
Éditeur	Autorise l'utilisateur ou le groupe à publier des classeurs et des sources de données sur le serveur.
Responsable de projet	Autorise l'utilisateur ou le groupe à définir les autorisations pour tous les éléments d'un projet.
Aucun	Définit toutes les fonctionnalités de la règle d'autorisation sur **Non spécifié**.
Refusé	Définit toutes les fonctionnalités de la règle d'autorisation sur **Refusé**.
Connecteur de source de données	Autorise l'utilisateur ou le groupe à se connecter aux sources de données du projet.
Éditeur de source de données	Autorise l'utilisateur ou le groupe à se connecter à une source de données, à la modifier, à la télécharger, à la supprimer et à définir des autorisations pour celle-ci dans les projets. Il peut également publier des sources de données. Les propriétaires des sources de données publiées peuvent mettre à jour les informations de connexion et les programmations d'actualisation des extraits. Cette autorisation concerne les vues auxquelles ils ont accès qui se connectent à une source de données.

Classeurs et vues

La liste des fonctionnalités et des modèles d'autorisations disponibles pour chaque rôle varie selon que vous définissiez des autorisations pour un classeur ou une vue. Pour en savoir plus sur la définition des fonctionnalités, reportez-vous à la section Référence d'autorisations.

Modèle d'autorisations	Descriptions
Observateur	Autorise l'utilisateur ou le groupe à consulter le classeur ou la vue sur le serveur.
Interacteur	Autorise l'utilisateur ou le groupe à consulter le classeur ou la vue sur le serveur, à modifier les vues du classeur, à appliquer des filtres, à voir les données sous-jacentes, à exporter des images et à exporter des données. Toutes les autres autorisations proviennent des autorisations de l'utilisateur ou du groupe pour le projet.
Éditeur	Définit toutes les fonctionnalités de la règle sur **Autorisé**.
Aucun	Définit toutes les fonctionnalités de la règle sur **Non spécifié**.
Refusé	Définit toutes les fonctionnalités de la règle sur **Refusé**.
Personnalisé	Règle définie par l'administrateur pour la combinaison de fonctionnalités sélectionnée.

Sources de données

Les autorisations définies pour une source de données apportent une couche de sécurité supplémentaire pour les utilisateurs de Tableau Desktop et de Tableau Server.

Un utilisateur avec l'autorisation de connexion à une source de données peut se servir de Tableau Desktop pour exécuter des requêtes sur cette source de données par l'intermédiaire du composant Serveur de données de Tableau Server. L'utilisateur peut renseigner ses propres informations d'identification ou les informations d'identification enregistrées de l'auteur d'origine, le cas échéant. Les utilisateurs de Tableau Desktop n'ont donc pas besoin d'installer de pilotes de base de données sur leur ordinateur, de télécharger les données ou de disposer d'informations d'identification de base de données individuelles pour exécuter des requêtes en direct sur un entrepôt de données ou un extrait de données Tableau. Le composant Serveur de données fait office de proxy et ne nécessite aucune connexion directe vers la base de données.

Modèle d'autorisations	Descriptions
Connecteur	Autorise l'utilisateur ou le groupe à se connecter à la source de données sur le serveur.
Éditeur	Autorise l'utilisateur ou le groupe à se connecter aux sources de données, à les télécharger, à les supprimer et à définir des autorisations pour celles-ci sur le serveur. Il peut également publier des sources de données et, s'il en est le propriétaire, mettre à jour les informations de connexion et les programmations d'actualisation des extraits. Ces deux dernières fonctionnalités ne sont plus disponibles si un administrateur ou un responsable de projet modifie la propriété de la source de données.
Aucun	Définit toutes les fonctionnalités de la règle d'autorisation sur **Non spécifié**.
Refusé	Définit toutes les fonctionnalités de la règle d'autorisation sur **Refusé**.

Par ailleurs, les vues utilisant des sources de données publiées sur Tableau Server sont uniquement accessibles aux utilisateurs disposant des autorisations requises pour afficher la vue et la source de données originale (les autorisations d'affichage et de connexion pour les données et la vue). En revanche, si le publicateur de la vue a choisi d'intégrer ses informations d'identification à la source de données, les utilisateurs disposant de l'autorisation requise pour consulter la vue peuvent également se connecter à la source de données au nom de l'éditeur. Pour en savoir plus sur le composant Serveur de données, regardez notre vidéo sur le sujet.

Un mot sur les connexions

Tableau Server crée automatiquement des connexions de données pendant le processus de publication pour les classeurs et les sources de données. Les administrateurs et les propriétaires des sources de données peuvent ainsi contrôler les attributs de connexion indépendamment de la vue. Cela permet notamment de mettre à jour les informations d'identification ou d'effectuer une migration vers de nouveaux serveurs de bases de données sans avoir à modifier manuellement chaque classeur. Par ailleurs, plusieurs classeurs et sources de données peuvent exploiter une connexion unique pour des performances accrues et une réduction de la duplication. Cela implique également que les données mises en cache sont partagées entre les classeurs pour diminuer davantage la charge sur votre serveur de bases de données.

Autorisations et administrateurs

Il existe deux types d'administrateurs : les administrateurs de serveur et les administrateurs de site. Les administrateurs de serveur peuvent accéder à toutes les fonctionnalités du serveur et du site, à l'ensemble du contenu sur le serveur et à tous les utilisateurs. Ils peuvent également configurer l'intégralité du cluster de serveurs, y compris la gestion des sites, des utilisateurs, de la maintenance, des paramètres, des programmations et de l'index de recherche. Les administrateurs de site peuvent gérer les utilisateurs, les groupes, les projets, les classeurs et les connexions de données au sein d'un site. S'ils le souhaitent, ils peuvent également ajouter des utilisateurs au site afin de déléguer une partie de l'administration.

L'autorisation de publication est automatiquement accordée à l'ensemble des administrateurs. Les administrateurs peuvent également créer d'autres administrateurs de leur niveau.

Déploiements multilocataires

Bien que les administrateurs aient régulièrement recours aux groupes et aux projets pour organiser le contenu et définir les autorisations associées au sein d'une entreprise, il est plus courant d'utiliser des sites pour prendre en charge plusieurs parties externes (locataires) sur une instance de Tableau Server. C'est notamment sur ce principe que fonctionne Tableau Online, la solution logiciel en tant que service (SaaS) de Tableau. Les éléments de contenu (classeurs, sources de données, utilisateurs, etc.) de chaque site sont cloisonnés les uns par rapport aux autres sur cette instance de Tableau Server. Autrement dit, Tableau Server prend en charge l'architecture multilocataire en autorisant les administrateurs de serveur à créer plusieurs sites sur le serveur pour différents groupes d'utilisateurs et de contenu. Le contenu du serveur est publié, consulté, géré et contrôlé pour chaque site. Les sources de données et les connexions ne peuvent donc pas être partagées entre différents sites. Cette fonctionnalité permet à Tableau Server de répondre aux exigences de sécurité des entreprises évoluant dans le secteur de la finance, de la santé et de l'éducation, et de toute autre institution pour laquelle les clients d'une entreprise ne peuvent en aucun cas avoir accès aux données d'autres clients.

Il est toutefois bon de rappeler que les utilisateurs disposant des droits d'administrateur ou de publicateur sur Tableau Server peuvent consulter une liste de tous les utilisateurs de Tableau Server, étant donné qu'ils définissent les autorisations des rôles pour tout nouveau contenu. Par ailleurs, les administrateurs de serveur peuvent consulter tout le contenu publié sur Tableau Server, mais ne pourront pas accéder à toutes les données utilisées par Tableau Server, puisque l'accès aux données et les autorisations de contenu sont deux choses distinctes. Nous aborderons cet aspect dans la prochaine section.

Pour en savoir plus sur les autorisations sur Tableau Server, consultez le document Tableau Server : guide d'installation à l'usage de tous.

3 Sécurité de l'accès aux données

La sécurité de l'accès aux données est essentielle au sein d'une entreprise. Cela est particulièrement vrai pour les organisations devant répondre à des exigences réglementaires fédérales et à celles qui déploient Tableau Server auprès de clients externes. Tableau se doit de fournir des fonctionnalités fiables que les clients pourront exploiter pour renforcer leur système existant de sécurité des données et améliorer tout système obsolète. L'objectif est d'appliquer des mesures de sécurité de façon centralisée, quel que soit le moyen employé par les utilisateurs pour accéder aux données des vues publiées, qu'il s'agisse d'Internet, d'un appareil mobile ou de Tableau Desktop.

Voici les trois principales approches en matière de sécurité des données :

1. La mise en place de mesures de sécurité uniquement au sein de la base de données (authentification à la base de données)

2. La mise en place d'une sécurité limitée uniquement à Tableau

3. La création d'un modèle hybride dans lequel les informations des utilisateurs dans Tableau Server correspondent à des éléments de données dans la base de données.

Tableau Server prend en charge ces trois approches, mais les clients privilégient souvent le modèle hybride en raison de sa simplicité et de sa flexibilité, en particulier lors de l'utilisation de plusieurs sources de données disparates.

La méthode d'authentification à la base de données joue un rôle essentiel dans la sécurisation des bases de données. Ce processus d'authentification est différent de celui de Tableau Server abordé plus haut : lorsqu'un utilisateur se connecte à Tableau Server, il n'est pas encore connecté à la base de données. De ce fait, les utilisateurs devront disposer d'informations d'identification pour se connecter à chaque base de données. Afin de protéger encore plus vos données, Tableau ne nécessite que les informations d'identification d'accès en lecture à la base de données. Ainsi, cela vous permet de limiter l'accès des utilisateurs au mode Lecture seule. Les publicateurs ne peuvent donc pas modifier accidentellement les données sous-jacentes, ce qui améliore bien souvent les performances des requêtes. Dans certains cas, vous pouvez également autoriser un utilisateur d'une base de données à créer des tables temporaires. Cela peut renforcer à la fois votre sécurité et vos performances, les données temporaires étant stockées dans la base de données et non dans Tableau. Il faut donc faire un compromis entre l'attribution d'un accès en écriture limité aux utilisateurs Tableau, afin qu'ils puissent créer des tables temporaires, et le stockage local d'un plus grand volume de données dans Tableau Server.

Vous pouvez également limiter l'accès d'utilisateurs spécifiques à certaines données, en définissant des filtres utilisateur dans les classeurs et les sources de données. Cette fonctionnalité vise à mieux contrôler les données que les utilisateurs peuvent visualiser dans une vue publiée, en fonction de leur compte de connexion Tableau Server. En combinant ces méthodes, vous pouvez publier une vue ou un tableau de bord afin de permettre à un large éventail d'utilisateurs de Tableau Server d'analyser des données personnalisées et sécurisées.

Authentification sur la base de données

Si les données sont extraites à l'aide du moteur de données rapide de Tableau, les autorisations liées à la sécurité de la base de données ne se propageront pas aux utilisateurs finaux. Lors de l'actualisation ou de l'incrémentation automatique des extraits, Tableau Server utilise un seul ensemble d'informations d'identification enregistrées afin de générer des extraits pour chaque source de données (que ce soit avec l'option « Exécuter en tant qu'utilisateur » ou avec les informations d'identification intégrées au classeur). Les privilèges de sécurité de l'utilisateur concerné sont ensuite appliqués à la base de données.

Les vues publiées avec des connexions de données en direct sur Tableau Server sont dynamiques, car elles interrogent systématiquement la base de données pour récupérer les données actuelles. Chaque fois qu'un utilisateur ouvre une vue, si la source de données est une base de données nécessitant un identifiant (contrairement à un classeur Excel ou à un fichier texte, par exemple), Tableau Server doit connaître le nom d'utilisateur et le mot de passe associés à la base de données pour se connecter et récupérer les données. Tableau Server comporte plusieurs options et paramètres fonctionnant de concert afin d'identifier le nom d'utilisateur et le mot de passe de la source de données qui seront utilisés pour accéder aux données. Rappelons qu'il convient de distinguer les méthodes de connexion de Tableau Server, qui permettent d'accéder à Tableau Server, et la connexion à la base de données, qui peut être exigée pour accéder à la source de données. Le tableau ci-dessous présente les options disponibles lors de la création et de la publication de vues sur Tableau Server :

Type d'authentification	Réponse de Tableau Server	Tableau Server exploite-t-il la sécurité des données basée sur les utilisateurs intégrée à la base de données ?
Demande de nom d'utilisateur et de mot de passe	Tableau invite chaque observateur à saisir ses propres informations d'identification pour la base de données.	Oui, l'identité de l'utilisateur est connue par la base de données.
Mot de passe intégré	L'auteur saisit les informations d'identification pour la base de données lors de la publication de la vue. Les observateurs ne sont invités à saisir aucune information d'identification.	Non, tous les utilisateurs partagent les mêmes informations d'identification pour la base de données, celles de l'auteur.

Type d'authentification	Réponse de Tableau Server	Tableau Server exploite-t-il la sécurité des données basée sur les utilisateurs intégrée à la base de données ?
Identifiants de l'observateur/ du publicateur	Le nom d'utilisateur et le mot de passe du domaine de l'utilisateur sont utilisés pour s'authentifier à l'aide d'une authentification unique par le biais de Kerberos ou SAML.	Oui, l'identité de l'utilisateur est connue par la base de données.
Sécurité intégrée à Windows (authentification NT)	« Exécuter en tant qu'utilisateur » de Tableau Server	Non, tous les utilisateurs partagent les mêmes informations d'identification pour la base de données.
Sécurité intégrée à Linux (Active Directory/ délégation Kerberos)	« Exécuter en tant qu'utilisateur » de Tableau Server	Oui, l'identité de l'utilisateur est connue par la base de données.
Personnalisé		Règle définie par l'administrateur pour la combinaison de fonctionnalités sélectionnée.

Authentification Windows

Tableau Server utilise les informations d'identification du compte « Exécuter en tant qu'utilisateur » pour se connecter à la base de données avec Windows. Tous les utilisateurs de Tableau Server partageront les informations de connexion de ce profil pour la base de données. Cette méthode d'authentification n'utilise pas les informations d'identification du publicateur ni celles de l'utilisateur connecté à Tableau Server, et nécessite que la base de données tire parti de la sécurité intégrée de Windows. Cette pratique est très courante lors de l'implémentation de SQL Server ou de SQL Server Analysis Services. Une fois l'installation terminée, le compte « Exécuter en tant qu'utilisateur » par défaut pour Tableau Server devient l'utilisateur Autorité de réseau. Par définition, ce compte ne dispose pas des droits nécessaires pour se connecter aux bases de données. Pour utiliser un compte permettant l'authentification NT avec des sources de données, spécifiez un nom d'utilisateur et un mot de passe incluant le nom de domaine.

Authentification Linux

Tableau Server sous Linux utilise également les informations d'identification du compte « Exécuter en tant qu'utilisateur », mais selon un processus quelque peu différent. Sous Linux,

vous devez fournir un fichier keytab pour l'utilisateur qui sera associé au compte « Exécuter en tant qu'utilisateur ». Cela signifie que vous devez définir un compte « Exécuter en tant qu'utilisateur » différent pour une tâche donnée. Par exemple, pour se connecter à une base de données spécifique, la source de données doit utiliser une source de données « Exécuter en tant que principal » ou « Exécuter en tant qu'utilisateur ». La source de données « Exécuter en tant qu'utilisateur » doit inclure les utilisateurs du domaine, pas uniquement les utilisateurs locaux.

Nom d'utilisateur et mot de passe (non intégrés)

Chaque utilisateur de Tableau Server sera invité à se connecter à la base de données avec le nom d'utilisateur et le mot de passe prévus à cet effet. Si vous avez déjà configuré la sécurité des bases de données, vous pouvez en tirer parti par l'intermédiaire de Tableau Server. Si vous activez l'option « Informations d'identification enregistrées » sur la page des paramètres de Tableau Server, les utilisateurs Tableau Server ne doivent saisir les informations d'identification qu'une seule fois par source de données. Tableau Server conserve ensuite les informations d'identification de l'utilisateur pour cette source de données et les réutilise uniquement lors de la prochaine connexion de cet utilisateur à cette source de données. Notez que ces informations d'identification sont généralement différentes de celles utilisées pour se connecter à Tableau Server. Tableau chiffre systématiquement les mots de passe stockés dans le référentiel de Tableau Server. Les mots de passe des bases de données sont chiffrés avec une clé forte. Les clés des ressources récentes doivent être générées pour chaque déploiement au moyen de la commande `tabadmin assetkeys`.

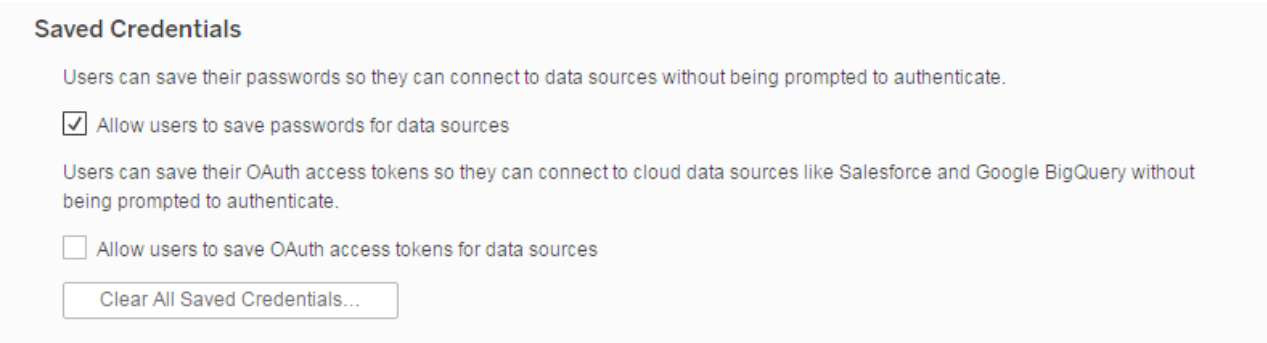

Figure 3 : Informations d'identification enregistrées sur la page des paramètres de Tableau Server

Informations d'identification intégrées (non compatible avec l'authentification Windows)

Lorsque vous activez les informations d'identification intégrées, Tableau Server peut se souvenir du nom d'utilisateur et du mot de passe de l'auteur original de chaque classeur. Lors de la publication, l'auteur se contente de saisir un ensemble d'informations d'identification pour la base de données (son nom d'utilisateur et son mot de passe) et de sélectionner « intégrer les informations d'identification ». Tous les utilisateurs de Tableau Server utiliseront alors les mêmes identifiants de connexion lorsqu'ils récupéreront des données provenant de cette source de données. Tableau Server utilise le même mécanisme de chiffrement décrit plus haut pour

sécuriser les informations d'identification intégrées dans le référentiel. Toutefois, lorsque vous choisissez cette méthode, n'oubliez pas que les mots de passe peuvent expirer, ce qui empêchera les utilisateurs d'accéder aux données.

Options supplémentaires spécifiques aux bases de données

Emprunt d'identité

Pour les sources de données Microsoft SQL Server, Tableau Server prend en charge l'emprunt d'identité des utilisateurs lors de l'exécution de requêtes. Cela permet à Tableau d'exploiter les mesures de sécurité que vous avez peut-être déjà mises en œuvre dans Microsoft SQL Server. Tableau se connecte à la base de données à l'aide de l'option « Exécuter en tant qu'utilisateur » ou d'informations d'identification intégrées. Toutes les requêtes seront cependant exécutées comme si un autre utilisateur s'était connecté. L'emprunt d'identité de Tableau est conçu pour fonctionner en association avec les mises en œuvre de SQL Server conformes aux meilleures pratiques de Microsoft pour le changement de contexte à l'aide de l'emprunt d'identité de la base de données.

Délégation Kerberos

La délégation Kerberos permet à Tableau Server d'utiliser les identifiants Kerberos de l'observateur d'un classeur pour exécuter une requête à la place de l'auteur. Cette fonctionnalité peut s'avérer particulièrement utile dans les cas suivants :

- Vous devez savoir qui accède aux données (le nom de l'observateur apparaîtra dans les journaux d'accès pour la source de données).
- Votre source de données dispose de mesures de sécurité au niveau des lignes, afin que différents utilisateurs aient accès à différentes cellules.

Pour que cela fonctionne, la base de données doit prendre en charge la délégation Kerberos. Tableau Server requiert une délégation contrainte, pour laquelle le compte « Exécuter en tant qu'utilisateur » a reçu des droits de délégation spécifiques pour accéder aux noms principaux de service (SPN) de la base de données cible. Par défaut, la délégation n'est pas activée dans Active Directory.

Sécurité au niveau des lignes et emprunt d'identité avec une commande SQL initiale

Lorsque vous vous connectez à certaines bases de données, vous pouvez spécifier une commande SQL initiale à exécuter lors de l'ouverture d'un classeur, de l'actualisation d'un extrait, de la connexion à Tableau Server ou de la publication sur Tableau Server. Cette commande SQL initiale diffère d'une connexion SQL personnalisée qui définit, quant à elle, une relation (table) à interroger à l'aide de requêtes.

Vous pouvez utiliser cette commande pour :

- Configurer des tables temporaires à utiliser pendant la session
- Configurer un environnement de données personnalisé

Vous pouvez transmettre des paramètres à votre source de données dans une instruction SQL initiale.

Cela présente plusieurs utilités : vous pouvez configurer l'emprunt d'identité à l'aide des paramètres **TableauServerUser** ou **TableauServerUserFull**. Si votre source de données le permet, vous pouvez configurer des mesures de sécurité au niveau des lignes (par exemple, Oracle VPD ou SAP Sybase ASE) pour vous assurer que les utilisateurs ont accès uniquement aux données qu'ils sont autorisés à consulter.

Query banding

Pour les sources de données Teradata, Tableau Server prend en charge l'insertion des informations de l'utilisateur dans la « query band ». Cela permet de limiter les données en fonction des règles de base de données ou d'autres règles de workflow Teradata. De plus, l'utilisation d'une query band peut améliorer les performances. Pour que le query banding fonctionne dans Tableau Server, vous devez le configurer de façon appropriée.

Filtres utilisateur

Les filtres utilisateur constituent l'outil de sécurité au niveau des lignes de Tableau Server. Tableau utilise des filtres de données dynamiques basés sur le nom d'utilisateur, l'adhésion à un groupe ainsi que d'autres attributs de l'utilisateur connecté. Lors de l'exécution de la vue, Tableau Server ajoute toutes les requêtes à la base de données avec une clause WHERE appropriée afin de limiter les données pour la requête de l'utilisateur. Les filtres utilisateur peuvent être utilisés avec toutes les sources de données, y compris les extraits.

Les sources de données publiées peuvent être créées avec des champs calculés afin de contrôler diverses dimensions ou mesures en fonction du nom d'utilisateur ou de l'adhésion à un groupe d'utilisateurs connectés. Ce champ est ensuite ajouté en tant que filtre de source de données avant la publication. Grâce à la fonctionnalité d'interdiction de téléchargement, le filtre utilisateur devient non modifiable pour les utilisateurs de Tableau Desktop et de Tableau Server se connectant à la source de données pour une analyse ad hoc.

Par exemple, une table Achats peut contenir l'ID du client, l'ID du commercial et les détails de la commande. Un champ calculé unique peut être ajouté à la vue pour permettre le filtrage des utilisateurs : USERNAME()=customerID OU USERNAME()=employeeID. Ainsi, un seul classeur publié sur Tableau Server peut fournir en toute sécurité les données appropriées en externe aux clients et en interne aux commerciaux. Les clients n'auront accès qu'aux commandes qu'ils ont passées, tandis que les commerciaux ne verront que celles qu'ils ont vendues. Les données pertinentes s'afficheront en fonction de leurs informations d'identification.

Cette approche a pour avantage d'éliminer les besoins en maintenance supplémentaire pour les vues lorsque de nouveaux utilisateurs et de nouvelles données sont ajoutés au système. Les règles de filtrage sont intégrées aux vues et la base de données leur fournit de façon dynamique les clés pour s'exécuter.

Si aucun contenu de la base de données ne permet d'identifier à l'aide d'un programme les données devant être fournies aux utilisateurs, un filtre utilisateur manuel peut être créé. Ce type de filtre utilisateur procède de la même façon que les filtres utilisateur calculés, mais il ne s'adapte pas aux nouveaux utilisateurs et aux nouveaux éléments de données de manière dynamique. Il nécessite donc une maintenance supplémentaire des vues.

Filtres de sources de données

Tableau Server prend en charge la création de filtres directement dans une source de données, ce qui réduit la quantité de données renvoyées depuis la source de données. Par exemple, imaginons que votre base de données contienne les données des 5 à 10 dernières années, mais que vous souhaitiez que vos utilisateurs aient uniquement accès à celles des trois dernières années. En ajoutant un filtre de source de données, vous pouvez facilement donner accès à cette période spécifique.

Si vous créez un extrait à partir d'une source de données possédant déjà des filtres de source de données définis, ces filtres sont automatiquement recommandés comme des filtres d'extrait et apparaîtront dans la boîte de dialogue d'extraits. Ces filtres recommandés ne doivent pas nécessairement faire partie de la liste des filtres d'extrait. Ils peuvent être supprimés séparément de l'ensemble de filtres de source de données existant.

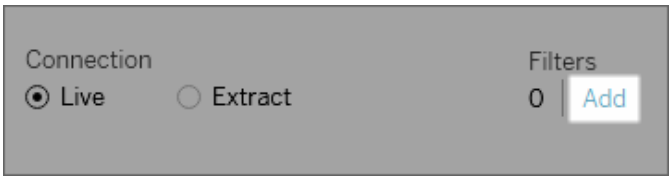

Figure 4 : Ajout de filtres aux sources de données Tableau de Tableau Desktop

Les filtres de source de données permettent de limiter les données que les utilisateurs peuvent afficher lorsque vous publiez un classeur ou une source de données. Lorsque vous publiez une source de données sur Tableau Server, la source elle-même et tous les fichiers ou extraits associés sont intégralement envoyés sur le serveur. Lors de la publication d'une source de données, vous pouvez définir les autorisations d'accès pour télécharger ou modifier cette source, et vous pouvez choisir les utilisateurs et groupes pouvant envoyer des requêtes à distance sur cette source par le biais de Tableau Server. Lorsque des utilisateurs sont autorisés à envoyer des requêtes mais pas à télécharger la source, vous pouvez partager un modèle de données enrichi disposant de champs calculés, d'alias, de groupes et d'ensembles, qui sera limité aux requêtes.

Par ailleurs, les utilisateurs qui interrogent des sources de données publiées ne pourront jamais voir ou modifier les filtres présents dans la source de données publiée d'origine, et ces filtres seront appliqués à chacune de leurs requêtes. Vous disposez ainsi d'un moyen efficace pour proposer un sous-ensemble bien défini de vos données : vous pouvez par exemple filtrer les dimensions pour certains utilisateurs et groupes, ou définir des filtres de source de données en fonction d'une plage de dates relatives ou fixes. Cette méthode contribue à sécuriser les données, mais vous permet également de gérer les performances de la base de données à distance que Tableau Server interrogera au nom d'un client Pour les systèmes qui s'appuient sur des partitions ou des indexations, les filtres de source de données peuvent offrir un contrôle considérable sur les performances des requêtes émises par Tableau.

Sécurité des extraits

Lorsque des extraits sont utilisés, Tableau Server se charge de stocker et de traiter les données utilisées dans des vues et des classeurs. Les données sont stockées sur le système de fichiers sous la forme d'un extrait de données Tableau dans un format binaire compressé et codé. Les métadonnées qui décrivent les extraits sont stockées au format texte. Ainsi, les données ne sont pas lisibles par les utilisateurs, mais il est possible de lire les descriptions des données, comme les types de données, les noms de champ, etc. Pour protéger ces fichiers, Tableau Server les stocke dans le répertoire « Program Data » qui dispose de contrôles d'accès limités aux comptes « Exécuter en tant qu'utilisateur » de Tableau Server et aux administrateurs locaux de la machine. Les fichiers des extraits ne sont pas eux-mêmes chiffrés sur le disque.

Tout comme les autres bases de données auxquelles Tableau se connecte, les extraits du moteur de données ne peuvent pas être interrogés directement depuis l'interface utilisateur de Tableau Server. Les utilisateurs peuvent effectuer des analyses par glisser-déposer, mais ils ne peuvent pas rédiger de requête en SQL, MDX ou toute autre syntaxe pour interagir directement avec la base de données du moteur de données. Cela permet d'empêcher les accès non autorisés, les injections SQL et autres attaques malveillantes sur les extraits.

L'intégration avec des solutions tierces et des solutions de système d'exploitation est possible pour obtenir un chiffrement au niveau du disque (par exemple, BitLocker) ou un chiffrement au niveau des fichiers et/ou des répertoires (par exemple, Encrypting File System ou EFS) afin de renforcer la sécurité des fichiers d'extraits de données. Toutefois, ces solutions ciblent généralement toutes les données présentes sur le disque, et le chiffrement ne se limite donc pas aux fichiers de données de Tableau Server. De plus, la mise en œuvre de ces solutions peut affecter les performances.

Sécurité du référentiel

Tableau Server dispose d'une base de données de référentiel interne qui stocke les informations sur le système (statistiques d'utilisation, utilisateurs, groupes, autorisations, etc.) ainsi que le contenu (classeurs, vues, commentaires, balises, etc.). Le référentiel ne stocke pas les données brutes ou les données extraites utilisées dans les vues et les classeurs Tableau.

Par défaut, le référentiel n'autorise pas les connexions externes. Cela signifie que l'accès aux informations stockées dans le référentiel se limite par défaut aux composants de Tableau Server. Cependant, les clients qui souhaitent avoir un accès direct à ces informations peuvent configurer le référentiel à l'aide de la commande tabadmin dbpass pour activer les connexions externes. Les connexions externes sont limitées aux vues en lecture seule des données afin d'empêcher une utilisation malveillante et des modifications involontaires du contenu ou de la configuration de Tableau Server. Vous pouvez également configurer le référentiel pour autoriser uniquement les connexions SSL à l'aide de l'utilitaire de configuration de Tableau Server.

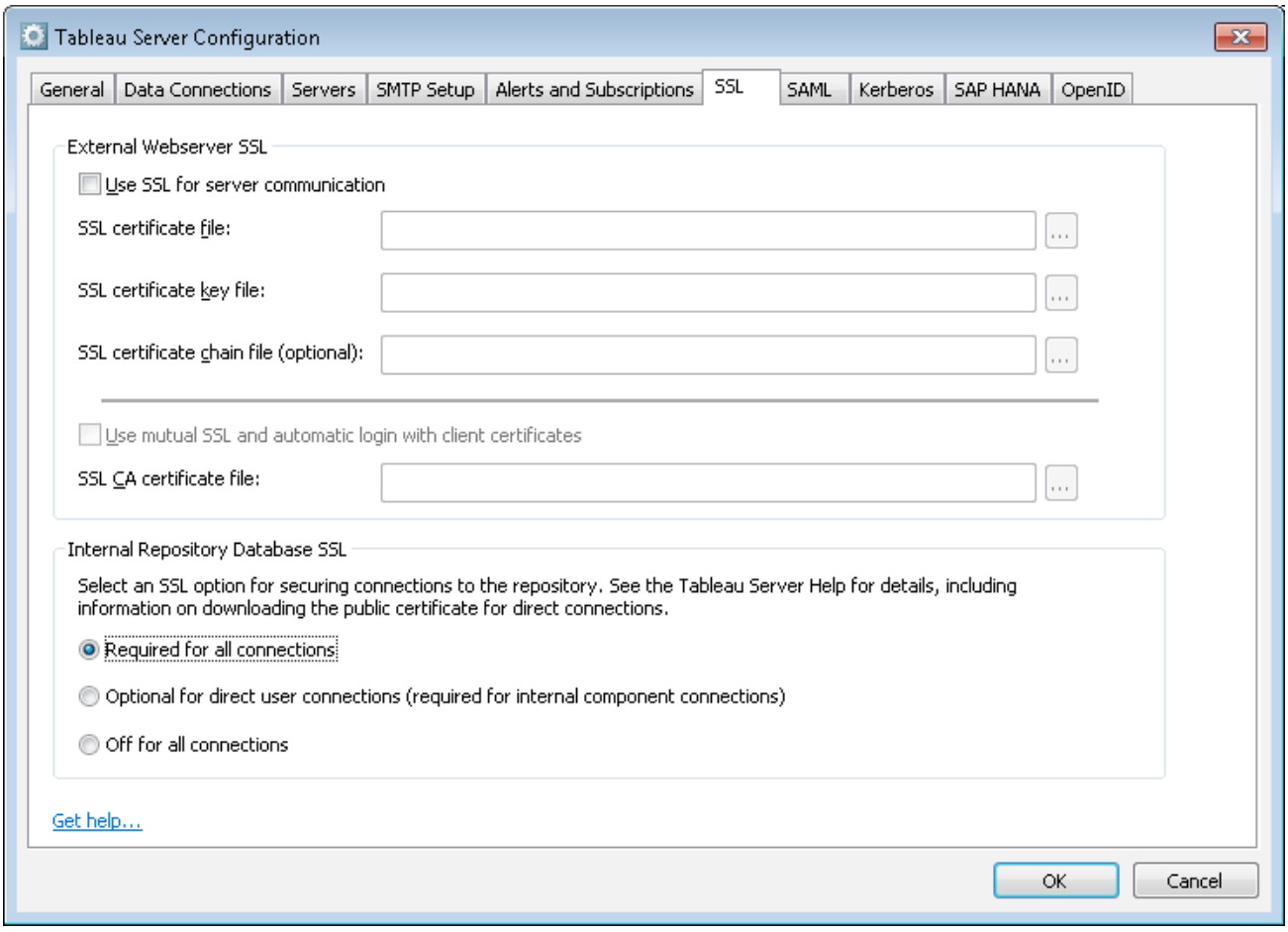

Figure 5 : Configuration de la fonctionnalité SSL interne de la base de données du référentiel

4 Réseau : sécurité des transmissions

Les administrateurs utilisent souvent des appareils de sécurité réseau pour protéger votre déploiement sur site de Tableau Server contre les accès depuis Internet et par des réseaux non sécurisés. Cependant, dans certains cas, les informations d'identification doivent tout de même être transmises de façon sécurisée via le réseau. Lorsque l'accès à Tableau Server n'est pas limité,

la sécurité des transmissions devient encore plus critique pour protéger les données sensibles et les informations d'identification, et pour empêcher une utilisation malveillante de Tableau Server. Quelle que soit votre situation, Tableau Server dispose de fonctionnalités de sécurité de transmissions robustes.

Tableau Server comporte trois interfaces réseau principales : les communications du client vers Tableau Server, celles de Tableau Server vers la base de données et celles entre les composants de Tableau Server. Chacune de ces interfaces est décrite ci-dessous. Outre ces fonctionnalités de sécurité étendues, Tableau accorde une attention particulière au stockage et aux transmissions des mots de passe au niveau de toutes les couches et de toutes les interfaces.

Communications du client vers Tableau Server

Ici, le terme « client » renvoie à un navigateur Web, Tableau Desktop, tabcmd ou des applications API REST. Par défaut, ces communications utilisent les requêtes et les réponses HTTP standard qui conviennent à la plupart des déploiements internes. Pour les déploiements externes ou autres déploiements sensibles, Tableau Server peut être configuré pour prendre en charge le protocole HTTPS (SSL/TLS) avec des certificats de sécurité fournis par le client. Dans ce cas, tout le contenu et toutes les communications entre les clients sont chiffrés et utilisent le protocole HTTPS. Il est recommandé d'activer les fonctionnalités SSL/TLS pour tous les déploiements où la sécurité est essentielle.

Lorsque vous configurez Tableau Server pour prendre en charge le protocole HTTPS, le navigateur et la bibliothèque HTTPS du serveur négocient un niveau de chiffrement commun. Tableau utilise OpenSSL comme bibliothèque HTTPS côté serveur et est préconfiguré pour utiliser les normes actuellement en vigueur. Chaque navigateur Web qui accède à Tableau Server via SSL utilise l'implémentation HTTPS standard fournie. Cette méthode fonctionne même dans les situations intégrées. L'utilisateur final bénéficie d'une expérience fluide, sans avertissements de sécurité, fenêtres contextuelles, ni exceptions.

Tableau Desktop communique avec Tableau Server à l'aide d'un protocole HTTP ou HTTPS. Pour protéger la transmission de mots de passe, un protocole HTTPS doit être activé.

Communications entre Tableau Server et la base de données

Tableau Server établit des connexions dynamiques vers les bases de données afin de traiter les ensembles de résultats et d'actualiser les extraits. Tableau utilise des pilotes natifs pour se connecter aux bases de données aussi souvent que possible. Il s'appuie sur un adaptateur ODBC générique lorsqu'aucun pilote natif n'est disponible. Toutes les communications avec la base de données sont acheminées par l'intermédiaire de ces pilotes. Ainsi, la configuration du pilote pour communiquer sur les ports non standard ou chiffrer les transmissions fait partie de l'installation du pilote natif, et ce type de configuration est transparent pour Tableau.

Communication entre les composants de Tableau Server

Cette section ne concerne que les déploiements distribués de Tableau Server. Deux aspects régissent la communication entre les composants de Tableau Server : la confiance et la transmission. Chaque nœud de serveur d'un cluster Tableau utilise un modèle de confiance rigoureux, ce qui garantit qu'il reçoit des requêtes valides des autres nœuds présents dans le cluster. Ce modèle repose sur une liste blanche d'adresses IP, de ports et de protocoles. Si l'un de ces éléments n'est pas valide, la requête est ignorée. Tous les membres du cluster peuvent communiquer entre eux. Il est recommandé d'installer un pare-feu pour protéger Tableau Server des serveurs non sécurisés.

5 Autres considérations

En raison de l'orientation axée vers l'extérieur des extranets, Tableau Server dispose de nombreuses protections intégrées pour maintenir son intégrité dans un environnement exposé. Par exemple, nous exigeons que toutes les communications clients s'effectuent via un seul port. De plus, nous fournissons une assistance pour configurer des proxy de transfert et des proxy inverses, de façon à ce que les communications entre votre réseau et Internet puissent être prises en charge par des serveurs proxy.

Tableau a mis en place une équipe de sécurité interne qui soumet les produits à de nombreux tests pour identifier les vulnérabilités et répondre rapidement aux nouvelles menaces à l'aide de mises à jour mensuelles. Pour connaître les dernières informations, consultez notre page sur la sécurité ainsi que notre livre blanc sur la sécurité dans le développement (en anglais). Enfin, nous vous recommandons vivement de consulter également la liste de contrôle pour une sécurité renforcée qui fournit des suggestions supplémentaires pour sécuriser votre déploiement de Tableau Server.

Résumé

Tableau Server offre un ensemble complet de fonctionnalités de sécurité pour répondre à vos besoins en matière de déploiement. Tableau s'est montré efficace au niveau des déploiements publics sur d'innombrables sites de clients, ainsi qu'au niveau des déploiements internes sur des réseaux sécurisés. Tableau utilise les normes modernes du secteur comme point de départ et s'adapte aux menaces et problèmes qui émergent. De la sécurité au niveau des lignes jusqu'à la sécurité des sites Web, en passant par tous les échelons entre les deux, Tableau répond à toutes vos exigences en matière de sécurité.

À propos de Tableau

Tableau aide les utilisateurs à transformer leurs données en informations exploitables qui marquent les esprits. Connectez-vous facilement à vos données, peu importe leur format ou leur emplacement de stockage. Réalisez rapidement des analyses ad hoc pour identifier des opportunités à explorer. Créez des tableaux de bord interactifs par glisser-déplacer et réalisez des analyses visuelles sophistiquées, puis partagez-les dans votre entreprise pour permettre à vos collègues d'explorer les données comme ils l'entendent. Des grandes multinationales aux startups naissantes en passant par les TPE, tout le monde utilise la plate-forme analytique de Tableau pour voir et comprendre ses données.

Ressources

Guide de la sécurité renforcée sur Tableau Server

Guide de l'administrateur de Tableau Server

Haute disponibilité de Tableau Server : fournir des analyses stratégiques essentielles et évolutives (en anglais)

Évolutivité de Tableau Server : un guide de déploiement technique pour les administrateurs de Tableau Serveur (en anglais)