Sicherheit bei Tableau Server

Implementierung der vier Grundsätze der Unternehmenssicherheit

tableau

Inhalt

Einleitung

Tableau ist eine moderne Plattform für Unternehmensanalysen, mit der Sie umfangreiche Selfservice-Analytics bei gleichzeitiger Governance durchführen können. Die Sicherheit ist der primäre und kritischste Aspekt einer Governance-Strategie für Daten und Inhalte. Tableau Server bietet umfangreiche Funktionen und eine umfassende Integration, um alle Aspekte der Unternehmenssicherheit abdecken zu können. Tableau unterstützt Unternehmen auch bei der Bereitstellung vertrauenswürdiger Datenquellen, damit alle Benutzer Zugriff auf die erforderlichen Daten haben, um schnell die richtigen Entscheidungen treffen zu können. Da einzelne zentrale Enterprise Data Warehouses (EDW) an Attraktivität verlieren und sich die Zunahme der Datenmenge durch die Cloud weiter beschleunigt, wird die Sicherstellung einer einheitlichen Sicherheitsumgebung für die verschiedenen Plattformen zu einer zentralen Aufgabe der Unternehmen.

Übersicht

Die vier allgemeinen Komponenten, die zur Anwendungssicherheit in einem Unternehmen beitragen, werden in diesem Whitepaper in Bezug auf Tableau Server ausführlicher erörtert:

1. Authentifizierung

2. Autorisierung

3. Datensicherheit

4. Netzwerk – Übertragungssicherheit

Bei ordnungsgemäßer Implementierung erfüllen diese vier Komponenten sämtliche Sicherheitsanforderungen eines Unternehmens und ermöglichen einer breiten Benutzerbasis den Zugriff auf vertrauenswürdige Daten sowie die Erstellung von Berichten, Dashboards und gemeinsamen Analysen. Geschäftsanwender vertrauen den Informationen, die von einer sicheren Daten- und Analyseplattform bereitgestellt werden, was zu einer vermehrten Nutzung der Daten sowie zu einer größeren Wertschöpfung aus den Daten ermutigt. Auftraggebern und Auftragnehmern kann externer Zugriff auf dieselbe Analyseplattform gewährt werden, während die Sicherheitsanforderungen des Unternehmens auch weiterhin erfüllt werden.

Tableau Server erfüllt die strengen Sicherheitsanforderungen von Kunden aus dem Finanzdienstleistungssektor, aus dem Gesundheits- und Hochschulwesen sowie aus dem Bereich der Behörden. Banken und Investmentfirmen übermitteln vertrauliche Investitionsdaten direkt an ihre Kunden. Hochschulen und Universitäten verwenden Tableau Server, um personalisierte Berichte direkt an die Studierenden und Dozenten zu übermitteln. Tableau Server wird von allen Teilstreitkräften des US-Militärs sowie von vielen Behörden der unterschiedlichen Regierungsebenen verwendet. In diesem Dokument wird beschrieben, wie Tableau Server umfassende Sicherheit auf Unternehmensebene bietet.

1. Authentifizierung

Tableau Server unterstützt verschiedene Formen der Authentifizierung nach Branchenstandard, unter anderem Active Directory, Kerberos, OpenID Connect, SAML, vertrauenswürdige Tickets und Zertifikate. Tableau Server verfügt darüber hinaus über einen eigenen integrierten Benutzeridentitätsdienst, die so genannte lokale Authentifizierung.

Wenn sich ein Benutzer anmeldet, gibt ihm Tableau Server die Möglichkeit, einige persönliche Einstellungen vorzunehmen. Er kann zum Beispiel die Sprache und das Gebietsschema auswählen, eine personalisierte Startseite einrichten und eine Übersicht der persönlich erstellten Inhalte anzeigen. Tableau Server behält die Benutzerdaten sitzungsübergreifend bei, um dem Benutzer eine konsistente persönliche Erfahrung zu bieten. Tableau erstellt und pflegt zu diesem Zweck ein Konto für jeden benannten Benutzer im System. Darüber hinaus können Autoren und Veröffentlicher die auf einem Server vorhandenen Identitätsdaten verwenden, um die Autorisierungsebene für andere Benutzer festzulegen, damit diese auf die zugrunde liegenden Daten ihrer veröffentlichten Ansichten zugreifen können.

Benutzeridentität

Wie oben erwähnt, können Sie die Benutzeridentitäten mithilfe von Active Directory verwalten – oder indem Sie sie unter Verwendung der lokalen Authentifizierung auf dem Server speichern. Nachstehend werden wir den Unterschied zwischen diesen beiden Methoden zur Verwaltung der Benutzerauthentifizierung beschreiben.

Active Directory

Wenn die Kunden sich dazu entscheiden, Active Directory als Identitätsspeicher in Tableau Server zu integrieren, verwaltet Active Directory alle Benutzernamen und Kennwörter.

Obwohl Benutzer und Gruppen zentral von Active Directory verwaltet werden, speichert Tableau Server eine Kopie der Benutzernamen und Gruppen in seinem eigenem Repository. Wenn Tableau für die Active Directory-Authentifizierung konfiguriert ist, speichert es keine Kennwörter. Benutzer und Gruppen können entweder manuell von einem Administrator mit Active Directory synchronisiert werden – oder programmgesteuert unter Verwendung des Befehlszeilenprogramms „tabcmd“ bzw. anhand von REST API.

Lokale Authentifizierung

Tableau Server enthält auch einen integrierten Dienst zur Benutzerverwaltung und -authentifizierung, der als „lokale Authentifizierung“ bezeichnet wird. Diese Methode wird von Organisationen verwendet, die Active Directory nicht nutzen möchten oder die mit Auftraggebern ohne Zugang zu Active Directory zusammenarbeiten. Bei Nutzung der lokalen Authentifizierung ist Tableau Server für die Verwaltung der Benutzer, der Gruppen und des gesamten Authentifizierungsprozesses verantwortlich. Der Administrator hat die Option, Kennwörter unter Tableau Server zu speichern. Darüber hinaus besteht jedoch auch die Möglichkeit, Kennwörter und Benutzerdaten an einen externen Dienst wie OpenID oder SAML

zu delegieren. Benutzerlisten lassen sich mühelos in Tableau Server importieren, und die meisten Benutzerverwaltungsfunktionen können mithilfe von tabcmd oder REST API programmgesteuert ausgeführt werden. So lassen sich Tableau-Benutzer ganz einfach im Rahmen Ihres automatisierten Bereitstellungsprozesses einrichten.

LDAP

Tableau Server für Linux unterstützt die Authentifizierung durch einen beliebigen LDAP-Anbieter. Demnächst kommt auch die Windows-Unterstützung heraus. Genau dieselben Authentifizierungs- und Benutzerverwaltungsfunktionen, die mit einem Active Directory-Server verfügbar sind, gibt es auch für jeden Verzeichnisdienst, der das LDAP-Protokoll und einen der folgenden Authentifizierungsmechanismen unterstützt: GSSAPI, einfache Bindung, einfache Bindung mit Kerberos. Arbeiten Sie mit Ihrer IT-Abteilung zusammen, um die richtige Lösung für Ihr Unternehmen zu finden.

Einmalige Anmeldung (Single Sign-On, SSO) und Integration in externe Authentifizierungsdienste

Tableau Server unterstützt mehrere Typen von SSO-Lösungen sowie gegenseitige SSL-Authentifizierung (Authentifizierung per Client-Zertifikat).

Die gegenseitige SSL-Authentifizierung bietet auf allen Geräten eine sichere automatische Anmeldung bei Tableau. Wenn bei gegenseitiger SSL-Authentifizierung ein Client (Tableau Desktop für Windows, ein Webbrowser oder tabcmd.exe) mit gültigem Zertifikat eine Verbindung zu Tableau Server herstellt, bestätigt Tableau Server das Vorhandensein eines gültigen Client-Zertifikats und meldet den Benutzer automatisch mit dem Benutzernamen an, der im Zertifikat enthalten ist.

Bei Verwendung von SSO müssen sich die Benutzer nicht explizit bei Tableau Server anmelden. Stattdessen können die Anmeldeinformationen verwendet werden, mit denen sich die Benutzer bei anderen externen Authentifizierungsdiensten authentifizieren (um sich zum Beispiel in ihrem Unternehmensnetzwerk anzumelden), um sie nahtlos bei Tableau Server anzumelden und zu authentifizieren – und zwar ohne Eingabeaufforderung auf einem Anmeldebildschirm. SSO stellt die Identität des Benutzers extern fest und ordnet diese einer im Identitätsspeicher von Tableau Server definierten Benutzeridentität zu.

Wenn Sie Tableau Server für die Nutzung eines externen Authentifizierungsdienstes mit SSO konfigurieren, übernimmt der externe Authentifizierungsdienst die gesamte Authentifizierung. Tableau Server verwaltet jedoch den Benutzerzugriff auf Tableau-Ressourcen anhand der im lokalen Identitätsspeicher gespeicherten Site-Rollen. Weitere Details finden Sie unten im Abschnitt „Autorisierung“.

Die folgenden externen Authentifizierungsdienste können in Tableau Server integriert werden:

- **SAML:** Sie können Tableau Server so konfigurieren, dass SAML (Security Assertion Markup Language) für SSO verwendet wird. Bei der Nutzung von SAML authentifiziert ein externer Identitätsanbieter (Identity Provider, IdP) die Anmeldeinformationen des Benutzers und sendet dann eine Sicherheitsbestätigung mit Angaben zur Identität des Benutzers an Tableau Server.

Unabhängig davon, ob Sie Active Directory nutzen oder die lokale Authentifizierung konfiguriert haben, können Sie SAML verwenden, um auf Tableau Server zuzugreifen. Sie können Tableau Server aber auch so konfigurieren, dass für jede Site ein anderer SAML IdP verwendet wird. Diese Konfiguration wird als „Site-Specific SAML“ bezeichnet.

- **Kerberos:** Wenn Kerberos in Ihrer Umgebung aktiviert ist und Tableau Server für die Nutzung der Active Directory-Authentifizierung konfiguriert ist, können Sie den Benutzern basierend auf deren Windows-Identität Zugriff auf Tableau Server gewähren. Sie können Kerberos nicht verwenden, wenn Tableau Server bei Ihnen für die lokale Authentifizierung konfiguriert ist.

- **Integrierte Windows-Authentifizierung:** Falls Sie Tableau Server mit Active Directory-Authentifizierung konfiguriert haben, können Sie die automatische Anmeldung aktivieren. Für die automatische Anmeldung wird Microsoft SSPI verwendet, um Benutzer basierend auf ihren Windows-Benutzernamen und ihren Windows-Kennwörtern anzumelden. Benutzer werden nicht zur Eingabe von Anmeldeinformationen aufgefordert, was mit dem Anmeldeerlebnis über Single Sign-On (SSO) und Kerberos vergleichbar ist.

- **OpenID:** OpenID Connect ist ein standardmäßiges Authentifizierungsprotokoll, das Benutzern die Anmeldung über einen kompatiblen Identitätsanbieter (Identity Provider, IdP) ermöglicht. Nach der erfolgreichen Anmeldung bei ihrem IdP werden die Benutzer automatisch bei Tableau Server angemeldet. Um OpenID Connect mit Tableau Server zu verwenden, muss der Server für die lokale Authentifizierung konfiguriert werden. Die Active Directory-Authentifizierung wird nicht unterstützt.

- **Vertrauenswürdige Authentifizierung:** Bei der vertrauenswürdigen Authentifizierung (oder „vertrauenswürdigen Tickets“) stellen Sie eine vertrauenswürdige Beziehung zwischen Tableau Server und mindestens einem Webserver her. Beim Empfang von Anforderungen von einem vertrauenswürdigen Webserver geht Tableau Server davon aus, dass der Webserver die erforderliche Authentifizierung bereits durchgeführt hat. Tableau Server empfängt die Anforderung mit einem einlösbaren Token oder Ticket und präsentiert dem Benutzer eine personalisierte Ansicht, die die Rolle und die Berechtigungen des Benutzers berücksichtigt.

Gastbenutzer oder anonymer Zugriff

Hinweis: Diese Option ist nur mit einer Core-basierten Tableau Server-Lizenz verfügbar.

Tableau Server kann so eingerichtet werden, dass anonymer Zugriff auf Ansichten über ein Gastkonto zugelassen wird. Dieses Feature ist hilfreich, um großen Benutzer-Communitys Inhalte bereitzustellen. Hierzu zählen das öffentliche Web und die Intranets von Unternehmen, wo die Identität des Benutzers nicht bekannt sein muss. Die Gastlizenz gestattet Benutzern ohne Konto bei Tableau Server, die eingebetteten Ansichten zu betrachten und mit ihnen zu interagieren.

Um den versehentlichen anonymen Zugriff auf vertrauliche Daten zu verhindern, ist die Option, als Gast auf Tableau Server zuzugreifen, standardmäßig deaktiviert. Ist die Option aktiviert, wird die Gastlizenz einem automatisch generierten Gastbenutzer zugewiesen. Da Gastbenutzer anonym sind und folglich nicht identifiziert werden können, gibt es bei Tableau nur einen einzigen universellen Gastbenutzer.

Anonyme Benutzer können Webseiten laden, die eingebettete Visualisierungen enthalten, ohne sich bei Tableau Server anmelden zu müssen. Sie können Tableau Server jedoch so einrichten, dass Anmeldeinformationen erforderlich sind, um auf das Intranet oder die Seite zuzugreifen, die die Ansicht hostet. Anonyme Benutzer können das Repository nicht durchsuchen. Sie haben nur Zugriff auf eingebettete Ansichten, d. h. auf URLs für die folgender Parameter festgelegt ist: „embed=true“. Einfacher ausgedrückt: Wenn ein anonymer Benutzer eine Ansicht anfordert, die die das eingebettete Flag nicht enthält, interpretiert Tableau Server diese Anfrage als Anforderung einer eingebetteten Ansicht. Das heißt, die per E-Mail übermittelten oder auf anderen Webseiten verlinkten URLs werden ordnungsgemäß für anonyme Benutzer verarbeitet und ihnen zugänglich gemacht. Beachten Sie, dass nur die für Gäste zugänglichen (in den Berechtigungen dementsprechend festgelegten) Ansichten für anonyme Benutzer gerendert werden. Jegliche Ansichten, die für Gastbenutzer unzugänglich sind, werden ungeachtet des „embed“-Flags nicht gerendert.

Die Benutzerberechtigungen des Gastes für den Zugriff auf Inhalte lassen sich mit dem vollen Spektrum an Rollen, Berechtigungen und Datensicherheitsfunktionen steuern, die auch für alle anderen Benutzertypen in Tableau Server verfügbar sind. Bei Empfang der Anforderung einer eingebetteten Ansicht überprüft Tableau Server als Erstes, ob der Benutzer angemeldet ist, genauer gesagt, ob an die Anforderung ein Cookie der Anmeldesitzung für eine noch nicht abgelaufene Anmeldung angehängt ist. Falls der Benutzer sich nicht aktiv angemeldet hat, wird die Anfrage als Gastbenutzer verarbeitet, sofern diese Option aktiviert ist.

Der Zugriff als Gastbenutzer funktioniert nicht, wenn für die Active Directory-Authentifizierung die automatische Anmeldung aktiviert ist. Das liegt an der Mehrdeutigkeit bei der Verarbeitung ungültiger Anmeldeinformationen.

Abmeldung

Das Beenden einer Sitzung wird bei der Authentifizierung oft vernachlässigt. In Tableau Server gibt es automatische Zeitüberschreitungslimits für Sitzungen, die auf der Inaktivitätsdauer basieren. Administratoren können die Standard-Inaktivitätsdauer ändern. Tableau Server gestattet zudem die Festlegung eines absoluten Zeitüberschreitungslimits für Sitzungen.

Bei Verwendung der Active Directory-Authentifizierung mit aktivierter automatischer Anmeldung verfügen die Benutzer über die Option „Benutzer wechseln“ anstatt über eine Option zum „Abmelden“. Das liegt daran, dass sie automatisch wieder neu angemeldet werden würden, wenn sie die Abmeldung initiiert hätten. In allen anderen Authentifizierungsszenarien verfügen die Benutzer über eine Option zum „Abmelden“, damit sie sich nach Beendigung ihrer Sitzung abmelden können.

In integrierten Umgebungen, zum Beispiel wenn Ansichten in ein Portal eingebettet sind, empfiehlt es sich, zusätzlich zur Abmeldung bei dem Portal eine programmgesteuerte Abmeldung bei Tableau Server zu erzwingen. Das lässt sich ganz leicht durchführen, indem Sie eine Abmeldungs-URL vom Client anfordern: `https://<Tableau Server>/manual/auth/logout`.

2. Autorisierung

Nachdem Sie einen Benutzer ordnungsgemäß authentifiziert und ihm Zugriff auf das System gewährt haben, folgt als nächster Schritt die Autorisierung, über welche Inhalts- und Serverberechtigungen er verfügen soll. Die Rollen und Berechtigungen in Tableau Server lassen Administratoren exakt steuern, auf welche Daten, Inhalte und Objekte ein Benutzer zugreifen kann und welchen Aktionen ein Benutzer oder eine Gruppe diese Inhalte unterziehen darf. Diese Aktionen werden häufig als Funktionen bezeichnet und umfassen unter anderem die Fähigkeit zum Anzeigen und Interagieren, das Hinzufügen von Kommentaren, das Speichern von Arbeitsmappen und das Herstellen von Verbindungen zu Datenquellen.

Sie können Benutzer auch gruppieren, um Berechtigungen leichter in Batches zu übernehmen. Tableau Server bietet Ihnen die Flexibilität, für bestimmte Benutzer/Gruppen die Berechtigungen „Zulassen“, „Verweigern“, „Keine Angabe“/„Geerbt“ zu jedem Inhalt (Projekt, Datenquelle, Arbeitsmappe und einzelne Ansichten in Arbeitsmappen) festzulegen. Wenn für einen bestimmten Inhalt keine expliziten Berechtigungen festgelegt wurden, übernimmt Tableau für diesen Inhalt eine Reihe von Standardberechtigungen. Diese Standardberechtigungen sind von den Standardeinstellungen zum Zeitpunkt der Inhaltserstellung abhängig und werden vom übergeordneten Element des fraglichen Inhalts geerbt. Berechtigungen steuern nicht, welche Daten in einer Ansicht angezeigt werden. Wie Sie steuern können, welche Daten die Benutzer angezeigt bekommen, erfahren Sie später im Abschnitt „Datenzugriffssicherheit“.

In dem Beispiel unten wurden den Mitgliedern der Gruppe „Operations“ (Operativer Betrieb) explizit die Berechtigungen für sämtliche Funktionen der Beispielansicht verweigert. John Doe wurde dagegen für diese konkrete Ansicht die Berechtigung zu sämtlichen Funktionen erteilt. Den Mitgliedern des Marketingteams wurde die Berechtigung zum Anzeigen des Inhalts erteilt, doch die Berechtigungen zum Interagieren und zum Bearbeiten des Inhalts wurden nicht festgelegt (Option „Keine Angabe“). Die Berechtigungen in Tableau Server werden somit von unten nach oben geprüft, also zuerst die Berechtigungen für die Arbeitsmappe und dann die Berechtigungen für das Projekt, um festzustellen, ob der fraglichen Gruppe diese Berechtigungen erteilt wurden. Sollte dies nicht der Fall sein, werden diese Berechtigungen implizit verweigert.

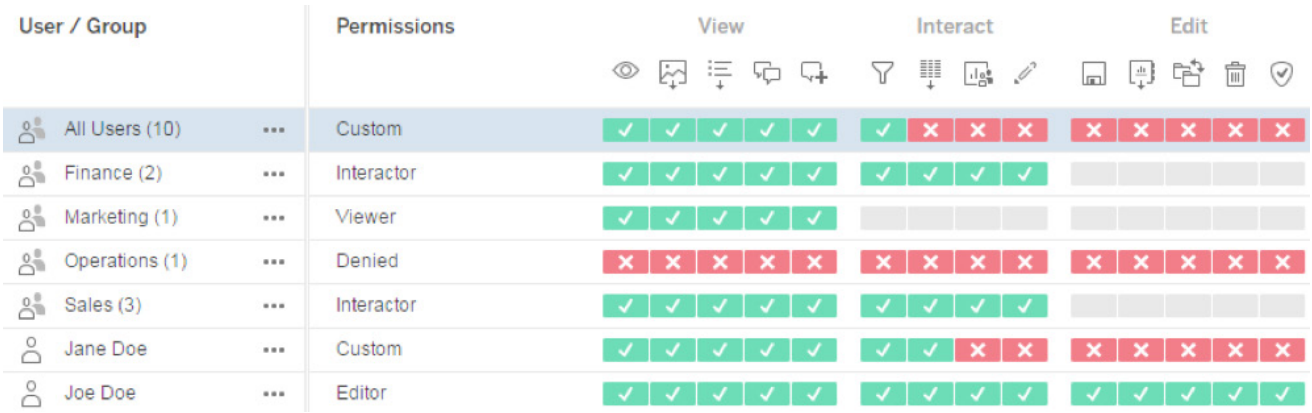

Abbildung 1: Festlegen angepasster Berechtigungen für Gruppen und Benutzer – basierend auf dem Inhalt

Standardberechtigungen und Vererbung

Tableau legt mithilfe eines Vorlagenmechanismus Ausgangsberechtigungen für Inhalte fest. Tableau kopiert die Ausgangsberechtigungen für ein Projekt aus dem Standardprojekt. Sie müssen die Berechtigungen im Standardprojekt unbedingt so festlegen, dass sie für das Sicherheitsmodell Ihrer Organisation angemessen sind. Wenn Sie Tableau Server in einer Selfservice-Umgebung bereitstellen, in der ein Wissens- und Informationsaustausch ausdrücklich gewünscht ist (sozusagen in einem offenen Berechtigungsmodell), dann sollten die Standardprojektberechtigungen die Gruppe „Alle Benutzer“ umfassen. Außerdem sollte in den Standardprojektberechtigungen die Berechtigungsrollenvorlage „Interaktor“ ausgewählt sein. Die Benutzer können dann standardmäßig den Server durchsuchen und mit veröffentlichten Ansichten interagieren. Eingeschränkt ist nur ihr Zugriff auf Arbeitsmappen, für die benutzerdefinierte Berechtigungen definiert wurden. Wenn Sie Tableau Server in einem geschlossenen Berechtigungsmodell bereitstellen, für das Datensicherheit und Zugriffskontrolle erforderlich sind, dann sollten der Gruppe „Alle Benutzer“ im Standardprojekt keine Berechtigungen erteilt werden. Durch die Auswahl der Option „Keine“ werden standardmäßig sämtliche Berechtigungen für Benutzer und Gruppen entfernt. Benutzer und Gruppen benötigen dann eine explizite Berechtigung, um Inhalte in neu erstellten Projekten zu veröffentlichen und zu nutzen.

Inhaltsberechtigungsmodell

Zu den veröffentlichten Inhalten zählen Datenquellen, Arbeitsmappen und Ansichten. Inhaltsberechtigungen umfassen die typischen Aktionen für die Inhaltsverwaltung wie das Anzeigen, Erstellen, Ändern und Löschen. Des Weiteren gehören auch die Interaktionen dazu, die ein Benutzer in einer Ansicht ausführen kann. Berechtigungen finden auch Anwendung, wenn ein Benutzer Inhalte durchsucht und auf der Benutzeroberfläche von Tableau Server navigiert.

Bei den Inhaltsberechtigungen wird die Hierarchie nicht beibehalten. Vielmehr werden die Berechtigungen des übergeordneten Elements kopiert, um als Ausgangsberechtigungen zu dienen, wenn das fragliche Element erstmals generiert wird. In Tableau Server werden auch die Berechtigungen der übergeordneten Arbeitsmappe kopiert, um als Ausgangsberechtigungen für eine Ansicht genutzt werden zu können. Änderungen an den Berechtigungen eines übergeordneten Elements werden nicht automatisch von den untergeordneten Elementen übernommen, außer die Inhalte werden manuell aktualisiert und die Berechtigungen werden neu festgelegt. Für Inhalte können andere Berechtigungen gelten als für ihre übergeordneten Elemente. Je nach Autor können strengere oder lockerere Berechtigungen festgelegt werden.

Benutzerberechtigungsmodell

Anders als beim Inhaltsberechtigungsmodell stellt Tableau Server ein Vererbungsmodell mit Berechtigungen für Benutzer und Gruppen bereit. Wenn für einen Benutzer eine bestimmte Berechtigung nicht explizit festgelegt wurde, erbt er die Einstellung von der Gruppe oder den Gruppen, der bzw. denen er angehört. In der Tableau Server-Ansicht „Permissions Manager“ (Berechtigungsmanager) werden vererbte Berechtigungen als nicht angegebene Berechtigungen (Option „Keine Angabe“) oder graue Felder dargestellt (siehe Abbildung 1 & 2). Wird einem Benutzer die Berechtigung zu einer Funktion nicht explizit in der Vererbungskette erteilt, wird ihm

die Berechtigung für diese Funktion verweigert. Änderungen an Gruppenberechtigungen werden automatisch an jeden einzelnen Benutzern verteilt.

Nützlicher Tipp: Um die resultierenden Berechtigungen für einen Benutzer oder eine Gruppe anzuzeigen, wählen Sie einfach die Gruppe oder den Benutzer auf der Berechtigungsseite aus und betrachten den Bereich mit den Benutzerberechtigungen am unteren Rand. Dort finden Sie die tatsächlichen Berechtigungen für jeden einzelnen Benutzer, nachdem Sie die Vererbungseinstellungen der Gruppe übernommen haben. Wenn Sie mit der Maus auf eine bestimmte Funktion zeigen, werden Informationen eingeblendet, zum Beispiel der Name der Funktion, die resultierende Einstellung und die Art und Weise, wie die Ergebnisse ermittelt werden.

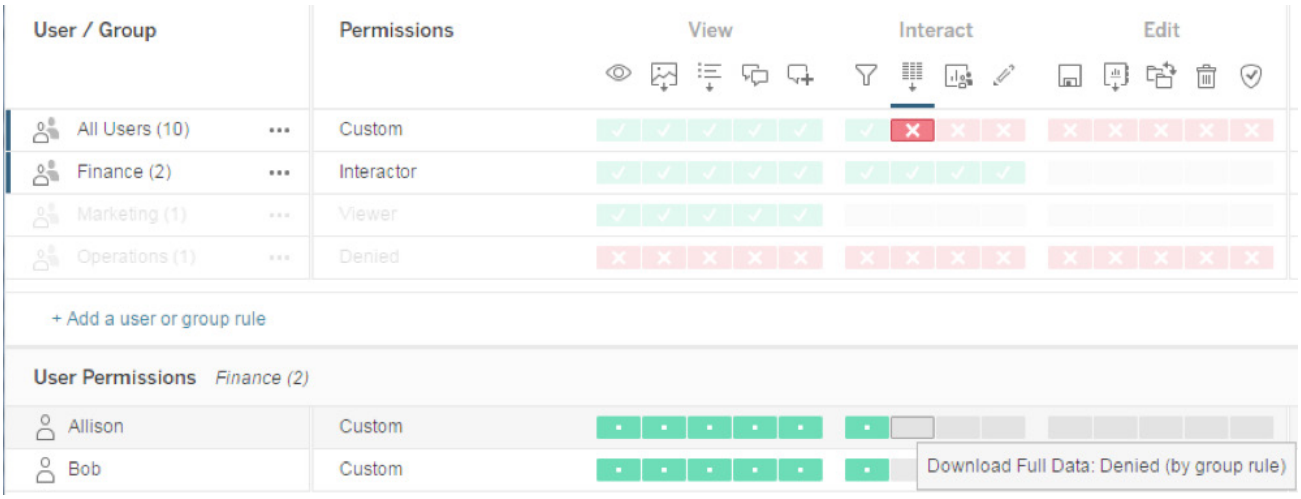

Abbildung 2: Anzeige der resultierenden Berechtigungen eines einzelnen Benutzers

Tableau Server-Berechtigungen

Projekte

Über die Projekte werden die Standardberechtigungen für alle im Projekt veröffentlichten Arbeitsmappen, Ansichten und Datenquellen festgelegt. Nur Site- und Serveradministratoren können Projekte sowie die dazugehörigen Berechtigungen erstellen und ändern. Benutzer mit der Berechtigung „Projektleiter“ können dagegen sämtliche Inhalte und Berechtigungen innerhalb ihrer Projekte steuern. Benutzer mit den entsprechenden Berechtigungen können die Standardberechtigungen für jeden Inhalt außer Kraft setzen. Veröffentlicher haben zum Beispiel die volle Kontrolle über die Zugriffsberechtigungen für die von ihnen veröffentlichten Inhalte. Wenn Administratoren mehr Kontrolle über die Berechtigungen innerhalb eines bestimmten Projekts benötigen, können sie die Berechtigungen für dieses Projekt festlegen und einschränken. Durch das Sperren von Berechtigungen innerhalb des Projekts werden für alle im Projekt veröffentlichten Inhalte die Standardberechtigungen verwendet, die der Administrator für das Projekt festgelegt hat. Inhaltsbesitzer können die Berechtigungen dann weder auf dem Server ändern, noch während der Veröffentlichung der Arbeitsmappe. Der Administrator und die Anforderungen des Projekts entscheiden darüber, ob Sie Berechtigungen sperren oder den Inhaltsbesitzern gestatten, die

Berechtigungen selbst zu verwalten. In manchen Projekten kann es gesperrte Berechtigungen geben, in anderen Projekten werden die Berechtigungen offen gelassen. Die Berechtigungen können in Zukunft mühelos angepasst werden, wenn sich die Anforderungen ändern. Beachten Sie, dass es sinnvoll sein kann, in manchen Projekten die Berechtigungen zu sperren, während sie in anderen Projekten besser offen gelassen werden sollten. Die Berechtigungen können in Zukunft mühelos angepasst werden, wenn sich die Anforderungen ändern.

Berechtigungsvorlage	Beschreibungen
Betrachter	Der Benutzer oder die Gruppe kann die Arbeitsmappen und Ansichten im Projekt anzeigen.
Veröffentlicher	Der Benutzer oder die Gruppe kann Arbeitsmappen und Datenquellen auf dem Server veröffentlichen.
Projektleiter	Der Benutzer oder die Gruppe kann Berechtigungen für alle Objekte in einem Projekt festlegen.
Keine	Legt alle Funktionen der Berechtigungsregel auf **Keine Angabe** fest.
Verweigert	Legt alle Funktionen der Berechtigungsregel auf **Verweigert** fest.
Datenquellen-Connector	Der Benutzer oder die Gruppe kann eine Verbindung mit den Datenquellen im Projekt herstellen.
Datenquellen-Editor	Der Benutzer oder die Gruppe kann eine Verbindung zu einer Datenquelle in den Projekten herstellen, die Datenquelle bearbeiten, herunterladen und löschen sowie Berechtigungen für die Datenquelle festlegen. Der Benutzer oder die Gruppe kann auch Datenquellen veröffentlichen. Die Besitzer veröffentlichter Datenquellen können Verbindungsinformationen und Zeitpläne für Extraktaktualisierungen aktualisieren. Diese Berechtigung ist relevant, wenn die Ansicht, auf die zugegriffen wird, eine Verbindung zu einer Datenquelle herstellt.

Arbeitsmappen und Ansichten

Die Liste der Funktionen und die verfügbaren Berechtigungsrollenvorlagen sind davon abhängig, ob Sie Berechtigungen für eine Arbeitsmappe oder Ansicht festlegen. Informationen über Funktionsdefinitionen finden Sie unter „Berechtigungsreferenz“.

Berechtigungsvorlage	Beschreibungen
Betrachter	Der Benutzer oder die Gruppe kann die Arbeitsmappe oder die Ansicht auf dem Server anzeigen.
Interaktor	Der Benutzer oder die Gruppe kann die Arbeitsmappe oder die Ansicht auf dem Server anzeigen, Arbeitsmappenansichten bearbeiten, Filter anwenden, die zugrunde liegenden Daten anzeigen sowie Bilder und Daten exportieren. Alle anderen Berechtigungen werden von den Projektberechtigungen der Benutzer oder Gruppe geerbt.
Editor	Setzt alle verfügbaren Aktionen für die Regel auf **Zulässig**.
Keine	Setzt alle verfügbaren Aktionen für die Regel auf **Keine Angabe**.
Verweigert	Setzt alle verfügbaren Aktionen für die Regel auf **Verweigert**.
Benutzerdefiniert	Vom Administrator festgelegte Regel für die ausgewählte Kombination von Funktionen

Datenquellen

Datenquellenberechtigungen stellen eine zusätzliche Sicherheitsebene sowohl für Tableau Desktop-Benutzer als auch für Tableau Server-Benutzer dar.

Ein Benutzer, dem die Berechtigung erteilt wurde, die Verbindung zu einer Datenquelle herzustellen, kann Tableau Desktop verwenden, um über die Datenserver-Komponente von Tableau Server Abfragen dieser Datenquelle auszuführen. Der Benutzer kann entweder seine Anmeldeinformationen angeben oder die gespeicherten Anmeldeinformationen des ursprünglichen Autors, sofern diese enthalten sind. Das heißt, die Tableau Desktop-Benutzer müssen keine Datenbanktreiber auf ihren Computern installieren und auch nicht über eigene Datenbankanmeldeinformationen verfügen, um Live-Abfragen eines Data Warehouse oder eines Tableau-Datenextrakts auszuführen. Der Datenserver fungiert als Proxyserver, der keine direkte Verbindung zur Datenbank benötigt.

Berechtigungsvorlage	Beschreibungen
Connector	Der Benutzer oder die Gruppe kann eine Verbindung mit der Datenquelle auf dem Server herstellen.
Editor	Der Benutzer oder die Gruppe kann eine Verbindung zu den Datenquellen auf dem Server herstellen, die Datenquellen bearbeiten, herunterladen und löschen sowie Berechtigungen für die Datenquellen festlegen. Der Benutzer oder die Gruppe kann auch Datenquellen veröffentlichen und als Besitzer der veröffentlichten Datenquelle zudem Verbindungsinformationen und Zeitpläne für Extraktaktualisierungen aktualisieren. (Die beiden letzten Möglichkeiten sind nicht mehr verfügbar, wenn ein Administrator oder Projektleiter Änderungen an den Besitzverhältnissen der Datenquelle vorgenommen hat.)
Keine	Legt alle Funktionen der Berechtigungsregel auf **Keine Angabe** fest.
Verweigert	Legt alle Funktionen der Berechtigungsregel auf **Verweigert** fest.

Außerdem haben nur Benutzer, die über die Berechtigung verfügen, sowohl auf die Ansicht als auch auf die zugrunde liegenden Datenquelle zuzugreifen, Zugriff auf Ansichten, die veröffentlichte Datenquellen in Tableau Server nutzen. Das heißt, der Benutzer verfügt entweder über die Berechtigung zum „Anzeigen“ oder zum „Verbinden“ der Daten und der Ansicht. Falls der Veröffentlicher der Ansicht jedoch beschlossen hat, seine Anmeldeinformationen in die Datenquelle einzubetten, können auch Benutzer mit der Berechtigung zum Anzeigen der Ansicht im Namen des Veröffentlichers auf die Datenquelle zugreifen. Sehen Sie sich bitte unser Datenserver-Video an, um Näheres über den Datenserver zu erfahren.

Ein kurzer Hinweis zu Verbindungen

Tableau Server stellt während der Veröffentlichung von Arbeitsmappen und Datenquellen automatisch Datenverbindungen her. Das versetzt Administratoren und Datenquellenbesitzer in die Lage, Verbindungsattribute getrennt von der Ansicht festzulegen. Das ermöglicht Aktualisierungen der Anmeldeinformationen oder die Migration auf neue Datenbankserver, ohne jede einzelne Arbeitsmappe manuell bearbeiten zu müssen. Darüber hinaus können mehrere Arbeitsmappen und Datenquellen eine einzige Verbindung nutzen, was die Leistung steigert und weniger Duplizierung erfordert. Das bedeutet auch, dass im Cache vorgehaltene Daten von den Arbeitsmappen gemeinsam genutzt werden, wodurch die Last auf Ihrem Datenbankserver noch weiter reduziert wird.

Berechtigungen und Administratoren

Es gibt zwei Typen von Administratoren: Serveradministratoren und Site-Administratoren. Serveradministratoren haben vollen Zugriff auf alle Server- und Site-Funktionen, auf alle Inhalte auf dem Server sowie auf alle Benutzer. Sie können auch den gesamten Servercluster konfigurieren, einschließlich der Verwaltung von Sites, Benutzern, Wartungsmaßnahmen, Einstellungen und Zeitplänen sowie des Suchindex. Site-Administratoren können die Benutzer, Gruppen, Projekte, Arbeitsmappen und Datenverbindungen auf einer Site verwalten. Optional können Site-Administratoren für delegierte administrative Szenarien Benutzer zur Site hinzufügen.

Alle Administratoren besitzen automatisch das Recht zum Veröffentlichen. Administratoren können auch zusätzliche Administratoren auf ihrer eigenen Ebene erstellen.

Mandantenfähige Bereitstellungen

Die Verwendung von Gruppen und Projekten ist eine gängige Methode für Administratoren, um die Inhalte innerhalb einer Organisation zu organisieren und durch Erteilung von Berechtigungen zugänglich zu machen. Um jedoch mehrere externe Parteien (Mandanten) in einer einzelnen Tableau Server-Bereitstellung zu unterstützen, werden am häufigsten Sites verwendet. Tableau Online, das gehostete SAAS-Angebot von Tableau, wird übrigens auf genau dieselbe Weise bereitgestellt. Die Inhalte (Arbeitsmappen, Datenquellen, Benutzer usw.) innerhalb der einzelnen Sites werden von jeglichen anderen Inhalten auf dieser Instanz von Tableau Server isoliert. Man könnte auch sagen, dass Tableau Server die Mehrmandantenfähigkeit unterstützt, indem Server-Administratoren gestattet wird, mehrere Sites auf dem Server für unterschiedliche Benutzer- und Inhaltssätze zu erstellen. Die Veröffentlichung, Verwaltung und Steuerung sämtlicher Serverinhalte sowie der Zugriff auf diese Inhalte erfolgen auf den jeweiligen Sites. Folglich können die Datenquellen und Verbindungen nicht von allen Sites gemeinsam genutzt werden Diese Funktionalität verleiht der Sicherheit von Tableau Server genügend Robustheit, um die Anforderungen an die Bereitstellungen im Finanzsektor, Gesundheitswesen, Bildungswesen und in anderen Branchen zu erfüllen, wo die Kunden eines Unternehmens unter gar keinen Umständen die Daten anderer Kunden sehen dürfen.

Es sollte jedoch beachtet werden, dass Benutzer mit Administrator- und Veröffentlicherrechten in Tableau Server eine Liste aller Tableau Server Benutzer anzeigen können, weil sie die Rollenberechtigungen für neue Inhalte festlegen. Darüber hinaus können Serveradministratoren sämtliche in Tableau Server veröffentlichten Inhalte sehen, was aber nicht heißt, dass sie Zugriff auf alle Daten hätten, die von Tableau Server verwendet werden, denn der Datenzugriff erfolgt getrennt von den Inhaltsberechtigungen. Im nächsten Abschnitt wird dieser Aspekt noch ausführlicher erörtert.

Weitere Informationen über Berechtigungen in Tableau Server finden Sie unter Tableau Server: Allgemeines Installationshandbuch

3. Datenzugriffssicherheit

Die Datenzugriffssicherheit ist für jedes Unternehmen von größter Bedeutung. Noch stärker trifft dies allerdings auf Organisationen zu, die den Vorschriften der US-Regierung unterliegen oder die Tableau Server externen Kunden bereitstellen. Es ist ganz entscheidend, dass Tableau robuste Funktionen bereitstellt, die es den Kunden gestatten, auf ihren vorhandenen Datensicherheitsimplementierungen aufzubauen und vorhandene unzulängliche Systeme zu verbessern. Ziel ist es, an einem einzigen Ort für die Datensicherheit zu sorgen, ungeachtet dessen, ob die Benutzer über veröffentlichte Ansichten im Web oder auf Mobilgeräten bzw. über Tableau Desktop auf die Daten zugreifen.

Es gibt drei wesentliche Methoden, um für Datensicherheit zu sorgen:

1. Implementieren der Sicherheit ausschließlich innerhalb der Datenbank (Datenbankauthentifizierung)

2. Implementieren der Sicherheit ausschließlich in Tableau

3. Entwicklung einer Hybridmethode, bei der es zu den Benutzerinformationen in Tableau Server entsprechende Datenelemente in der Datenbank gibt

Tableau Server unterstützt alle drei Methoden, doch die Kunden geben wegen ihrer Einfachheit und Flexibilität häufig der Hybridmethode den Vorzug, vor allem wenn mehrere verschiedenartige Datenquellen verwendet werden.

Bei Nutzung der Datenbanksicherheit muss unbedingt beachtet werden, dass es dabei auf die für die Authentifizierung der Datenbank gewählte Methode ankommt. Die Authentifizierung auf dieser Ebene erfolgt separat von der oben besprochenen Tableau Server-Authentifizierung, das heißt, ein Benutzer, der sich bei Tableau Server anmeldet, ist noch nicht bei der Datenbank angemeldet. Folglich benötigen die Tableau Server-Benutzer zusätzlich Anmeldeinformationen für die Anmeldung bei der Datenbank, damit die Sicherheitsmaßnahmen auf Datenbankebene zum Tragen kommen. Um Ihre Daten noch besser zu schützen, benötigt Tableau nur Anmeldeinformationen für den Lesezugriff, sodass Sie den Zugriff einschränken und den Benutzern nur den Zugang zu schreibgeschützten Daten gewähren können. Das verhindert, dass Veröffentlicher versehentlich die zugrunde liegenden Daten ändern, und bewirkt häufig eine verbesserte Abfrageleistung. Mitunter ist es jedoch hilfreich, der Datenbank Benutzerberechtigungen zu erteilen, um temporäre Tabellen zu erstellen. Das kann sowohl für die Leistung als auch für die Sicherheit vorteilhaft sein, denn die temporären Daten werden dann in der Datenbank gespeichert anstatt in Tableau. Es herrscht ein Kompromiss zwischen dem begrenzten Schreibzugriff, der Tableau-Benutzern gewährt wird, um temporäre Tabellen zu erstellen, und der lokalen Speicherung von mehr Daten in Tableau Server.

Sie können auch einschränken, welche Benutzer welche Daten sehen, indem Sie Benutzerfilter in Arbeitsmappen und Datenquellen festlegen, um anhand des Tableau Server-Anmeldekontos der Datenbenutzer besser zu steuern, was sie in einer veröffentlichten Ansicht sehen können. Durch Kombination dieser Methoden können Sie eine einzelne Ansicht oder ein einzelnes Dashboard so veröffentlichen, dass einem breiten Benutzerspektrum sichere personalisierte Daten und Analysen in Tableau Server bereitgestellt werden.

Datenbankauthentifizierung

Wenn Daten mithilfe der schnellen Daten-Engine von Tableau extrahiert werden, dann werden die Sicherheitsberechtigungen der Datenbank nicht an die Endbenutzer verteilt. Wenn Extrakte automatisch aktualisiert oder inkrementiert werden, verwendet Tableau Server einen einzelnen Satz gespeicherter Anmeldeinformationen, um Extrakte für jede Datenquelle zu extrahieren (entweder mithilfe des Kontos „Als Benutzer ausführen“ oder unter Verwendung der in der Arbeitsmappe eingebetteten Anmeldeinformationen). Dadurch werden die Sicherheitsrechte dieses Benutzers in die Datenbank übernommen.

Die mithilfe von Live-Datenverbindungen in Tableau Server veröffentlichten Ansichten sind insofern dynamisch, als sie die Datenbank jedes Mal abfragen, um aktuelle Daten abzurufen. Immer wenn ein Benutzer eine Ansicht öffnet und die Datenquelle eine Datenbank ist, die eine Anmeldung erfordert (im Gegensatz zu einer Excel-Arbeitsmappe oder einer Textdatei), benötigt Tableau Server den Benutzernamen und das Kennwort für die Datenbank, um die Verbindung herzustellen und die Daten abzurufen. In Tableau Server gibt es mehrere Optionen und Einstellungen, die zusammenwirken, um anzugeben, welcher Benutzername und welches Kennwort für die Datenbank zu verwenden ist, um auf die Daten zuzugreifen. Der Unterschied zwischen den Anmeldeverfahren für Tableau Server, die verwendet werden, um Zugriff auf Tableau Server selbst zu erhalten, und der Datenbankanmeldung, die für die Datenquelle erforderlich sein könnte, muss Ihnen unbedingt klar sein. Die nachstehende Tabelle fasst die Optionen beim Erstellen und Veröffentlichen von Ansichten in Tableau Server zusammen:

Authentifizierungstyp	Reaktion von Tableau Server	Nutzt Tableau Server die in die Datenbank integrierte benutzerbasierte Datensicherheit?
Benutzername und Kennwort Eingabeaufforderung	Tableau fordert jeden Betrachter auf, die eigenen Datenbankanmeldeinformationen einzugeben.	Ja, die jeweilige Benutzeridentität ist der Datenbank bekannt.
Eingebettetes Kennwort	Bei Veröffentlichung der Ansicht legt der Autor die Datenbankanmeldeinformationen fest. Betrachter werden nicht zur Eingabe von Anmeldeinformationen aufgefordert.	Nein, alle Benutzer verwenden dieselben ankanmeldeinformationen wie der Autor.

Authentifizierungstyp	Reaktion von Tableau Server	Nutzt Tableau Server die in die Datenbank integrierte benutzerbasierte Datensicherheit?
Anmeldeinformationen des Veröffentlichers/ Betrachters	Die Domänenanmeldeinformationen (Benutzername und Kennwort) des Benutzers werden für die Authentifizierung per SSO über Kerberos oder SAML verwendet.	Ja, die jeweilige Benutzeridentität ist der Datenbank bekannt.
In Windows integrierte Sicherheitsfunktionen (NT-Authentifizierung)	„Als Benutzer ausführen“ ist das von Tableau Server verwendete Konto.	Nein, alle Benutzer verwenden dieselben ankanmeldeinformationen
In Linux integrierte Sicherheitsfunktionen (Active Directory/ Kerberos-Delegierung)	„Als Benutzer ausführen“ ist das von Tableau Server verwendete Konto.	Ja, die jeweilige Benutzeridentität ist der Datenbank bekannt.
Benutzerdefiniert		Vom Administrator festgelegte Regel für die ausgewählte Kombination von Funktionen

Windows-Authentifizierung

Tableau Server verwendet die Anmeldeinformationen für das Konto „Als Benutzer ausführen“, um die Verbindung zur Datenbank über Windows herzustellen. Alle Tableau Server-Benutzer benutzen gemeinsam die Verbindungsinformationen dieses Profils für die Datenbank. Hierfür werden nicht die Anmeldeinformationen des Veröffentlichers oder des bei Tableau Server angemeldeten Benutzers verwendet. Diese Option erfordert, dass die Datenbank die in Windows integrierten Sicherheitsfunktionen nutzt. Das ist sehr häufig bei SQL-Server und SQL Server Analysis Services der Fall. Bei der Installation ist für Tableau Server standardmäßig der Benutzer „Netzwerkautorität“ für das Konto „Als Benutzer ausführen“ festgelegt. Laut Definition verfügt dieses Netzwerkautoritätskonto über keine Rechte, um Verbindungen zu Datenbanken herzustellen. Wenn Sie ein Konto verwenden möchten, das eine NT-Authentifizierung mit Datenquellen zulässt, dann geben Sie einen Benutzernamen und ein Kennwort einschließlich des Domänennamens an.

Linux-Authentifizierung

Für Tableau Server für Linux werden ebenfalls die Anmeldeinformationen für das Konto „Als Benutzer ausführen“ verwendet, allerdings geschieht dies auf eine etwas andere Weise. Unter

Linux müssen Sie eine Schlüsseltabellendatei für den Benutzer bereitstellen, den Sie für das Konto „Als Benutzer ausführen“ verwenden möchten Sie müssen also für jede Aufgabe einen anderen Benutzer für das Konto „Als Benutzer ausführen“ festlegen. Um zum Beispiel die Verbindung zu einer bestimmten Datenbank herzustellen, muss eine Datenquelle unter dem Konto „Als Prinzipal ausführen“ oder „Als Benutzer ausführen“ verwendet werden. Die Datenquelle unter dem Konto „Als Benutzer ausführen“ muss Domänenbenutzer enthalten, nicht einfach nur lokale Benutzer.

Benutzername und Kennwort (nicht eingebettet)

Jeder Tableau Server-Benutzer wird aufgefordert, sich mit seinem datenbankspezifischen Benutzernamen und Kennwort bei der Datenbank anzumelden. Wenn Sie schon vorab Datenbanksicherheit eingerichtet haben, ist dies eine gute Option, um diese vorhandenen Sicherheitsfunktionen über Tableau Server zu nutzen. Wenn Sie auf der Tableau Server-Seite „Einstellungen“ die Option „Gespeicherte Anmeldeinformationen“ aktiviert haben, muss ein Tableau Server-Benutzer die Anmeldeinformationen nur einmal pro Datenquelle eingeben. Tableau Server speichert dann die Anmeldeinformationen des Benutzers für die jeweilige Datenquelle und verwendet sie dann nur für die nächste Verbindung dieses Benutzers mit derselben Datenquelle. Beachten Sie, dass es sich hierbei normalerweise um andere Anmeldeinformationen handelt, als Sie für die Anmeldung bei Tableau Server verwenden. Tableau verschlüsselt stets alle Kennwörter, die im Tableau Server-Repository gespeichert sind. Datenbankkennwörter sind mit einem starken Schlüssel verschlüsselt. Für jede Bereitstellung sollten neue Ressourcenschlüssel mithilfe des Befehls `tabadmin assetkeys` generiert werden.

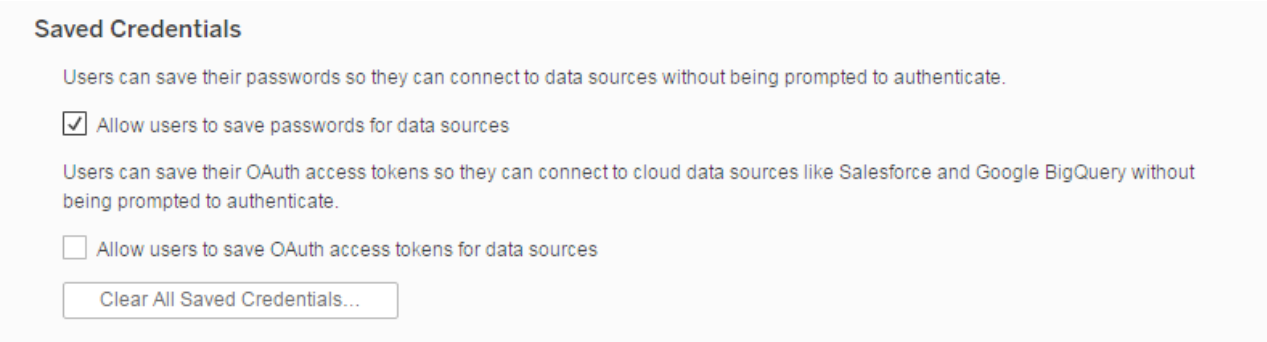

Abbildung 3: Gespeicherte Anmeldeinformationen auf der Tableau Server-Seite „Einstellungen“

Eingebettete Anmeldeinformationen (nicht geeignet für die Windows-Authentifizierung)

Wenn Sie eingebettete Anmeldeinformationen aktivieren, kann sich Tableau Server den Benutzernamen und das Kennwort des ursprünglichen Autors jeder Arbeitsmappe „merken“. Zum Zeitpunkt der Veröffentlichung gibt der Autor einfach einen Satz Anmeldeinformationen (seinen Benutzernamen und sein Kennwort) für die Datenbank ein und wählt die Option „Eingebettete Anmeldeinformationen“. Alle Tableau Server-Benutzer verwenden dann dieselben Verbindungsanmeldeinformationen, wenn sie Daten von dieser Datenquelle abrufen. In Tableau Server wird derselbe Verschlüsselungsmechanismus verwendet, der zuvor beschrieben wurde, um die eingebetteten Anmeldeinformationen im Repository zu sichern. Wenn Sie sich für diese Methode entscheiden, sollten Sie sich des Nachteils bewusst sein, dass Kennwörter ablaufen können und die Benutzer dann am Zugriff auf die Daten gehindert werden.

Weitere datenbankspezifische Optionen

Identitätswechsel

Bei Microsoft SQL Server-Datenquellen unterstützt Tableau Server den Identitätswechsel von Benutzern beim Ausführen von Abfragen. So kann Tableau die von Ihnen unter Umständen bereits in Microsoft SQL Server implementierten Sicherheitsfunktionen nutzen. Tableau stellt entweder mithilfe des Kontos „Als Benutzer ausführen“ oder anhand eingebetteter Anmeldeinformationen eine Verbindung zur Datenbank her. Doch alle Abfragen werden so ausgeführt, als hätte ein anderer Benutzer die Verbindung hergestellt. Der Tableau-Identitätswechsel ist auf das Zusammenspiel mit SQL Server-Implementierungen ausgelegt, die die Best Practices von Microsoft für Kontextwechsel mithilfe des Datenbank-Identitätswechsels einhalten.

Kerberos-Delegierung

Die Kerberos-Delegierung ermöglicht Tableau Server die Nutzung der Kerberos-Anmeldeinformationen des Betrachters einer Arbeitsmappe, um eine Abfrage anstelle des Autors auszuführen. Dies ist in den folgenden Situationen hilfreich:

- Sie müssen wissen, wer auf die Daten zugreift (der Name des Betrachters wird in den Zugriffsprotokollen für die Datenquelle angegeben).
- Für Ihre Datenquelle ist Sicherheit auf Zeilenebene festgelegt, das heißt, unterschiedliche Benutzer können auf unterschiedliche Zellen zugreifen.

Damit das funktioniert, muss die Datenbank die Kerberos-Delegierung unterstützen. Tableau Server erfordert eine eingeschränkte Delegierung, bei der dem Konto „Als Benutzer ausführen“ spezielle Delegierungsrechte für die Skript-Dienstprinzipalnamen (Service Principal Names, SPNs) der Zieldatenbank gewährt werden. Die Delegierung ist in Active Directory standardmäßig nicht aktiviert.

Sicherheit auf Zeilenebene und Identitätswechsel mit SQL-Anfangsdaten

Wenn Sie eine Verbindung zu bestimmten Datenbanken herstellen, können Sie einen SQL-Anfangsdatenbefehl angeben, der ausgeführt wird, wenn Sie die Arbeitsmappe öffnen, ein Extrakt aktualisieren, sich bei Tableau Server anmelden oder etwas in Tableau Server veröffentlichen. Diese SQL-Anfangsdaten unterscheiden sich von einer benutzerdefinierten SQL-Verbindung, die eine Beziehung (Tabelle) definiert, zu der Abfragen erstellt werden.

Mit diesem Befehl können Sie Folgendes tun:

- Temporäre Tabellen einrichten, die während der Sitzung verwendet werden
- Eine benutzerdefinierte Datenumgebung einrichten

Sie können Parameter in einer SQL-Anfangsdatenanweisung an Ihre Datenquelle weiterleiten.

Dies ist aus mehreren Gründen hilfreich: Sie können einen Identitätswechsel mithilfe der Parameter **TableauServerUser** oder **TableauServerUserFull** konfigurieren. Sofern Ihre Datenquelle

dies unterstützt, können Sie die Sicherheit auf Zeilenebene implementieren (z. B. für Oracle VPD oder SAP Sybase ASE), um sicherzustellen, dass die Benutzer nur die Daten sehen, zu deren Anzeige sie autorisiert sind.

Abfragenverbund

Bei Teradata-Datenquellen unterstützt Tableau Server das Einfügen von Benutzerinformationen in den Abfragenverbund. So lassen sich Daten auf der Grundlage von Datenbankregeln oder basierend auf diversen anderen Teradata-Workflowregeln einschränken. Darüber hinaus kann durch die Nutzung eines Abfragenverbunds auch die Leistung gesteigert werden. Der Abfragenverbund muss richtig konfiguriert werden, damit er in Tableau Server funktioniert.

Benutzerfilter

In Tableau Server werden die Benutzerfilter dazu verwendet, Sicherheit auf Zeilenebene zu implementieren. In Tableau werden Daten dynamisch gefiltert, und zwar nach Benutzernamen, Gruppenmitgliedschaft und anderen Attributen des angemeldeten Benutzers. Wenn die Ansicht ausgeführt wird, fügt Tableau Server alle Abfragen mit einer geeigneten WHERE-Klausel an die Datenbank an, um die Daten für die aktuelle Anforderung des Benutzers ordnungsgemäß einzuschränken. Benutzerfilter können mit allen Datenquellen, einschließlich Datenextrakten, verwendet werden.

Veröffentlichte Datenquellen können mit berechneten Feldern erstellt werden, um diverse Dimensionen oder Kennzahlen zu steuern, und zwar basierend auf dem Benutzernamen oder der Gruppenmitgliedschaft des angemeldeten Benutzers. Dieses Feld wird dann vor dem Veröffentlichen als Datenquellenfilter hinzugefügt. Indem Sie die Berechtigung zum Herunterladen verweigern, lässt sich der Benutzerfilter nicht mehr verändern, und zwar weder von Tableau Desktop-Benutzern noch von Tableau Server-Benutzern, die für eine Ad-Hoc-Analyse eine Verbindung zur Datenquelle herstellen.

Eine Tabelle mit dem Namen „Bestellung“ könnte zum Beispiel Kundendaten (Kundennummer), Informationen zum Vertriebsmitarbeiter (Mitarbeiternummer) und Details zur Bestellung enthalten. Ein einzelnes berechnetes Feld kann zur Ansicht hinzugefügt werden, um den Benutzerfilter zu aktivieren: username()=Kundennummer OR username()=Mitarbeiternummer. So lässt sich eine einzelne Arbeitsmappe auf Tableau Server veröffentlichen, um den externen Kunden und den internen Vertriebsmitarbeitern die entsprechenden Daten sicher zur Verfügung zu stellen. Kunden sehen nur die von ihnen aufgegebenen Bestellungen, wohingegen die Vertriebsmitarbeiter nur die von ihnen abgewickelten Bestellungen (ihre Verkäufe) angezeigt bekommen. All dies erfolgt auf der Grundlage der jeweiligen Anmeldeinformationen.

Der Vorteil dieser Methode besteht darin, dass keine zusätzliche Wartung der Ansichten erforderlich ist, wenn neue Benutzer und Daten zum System hinzugefügt werden. Die Filterregeln sind in die Ansichten integriert, und die Datenbank stellt die Schlüssel dynamisch bereit, damit diese Regeln verarbeitet werden können.

Sind keine passenden Inhalte in der Datenbank vorhanden, um programmgesteuert zu erkennen, welche Daten welchem Benutzer bereitzustellen sind, dann kann ein Benutzerfilter manuell

erstellt werden. Dieser Typ von Benutzerfilter wird auf dieselbe Art und Weise wie berechnete Benutzerfilter verarbeitet, allerdings passt er sich nicht dynamisch an neue Benutzer oder Datenelemente an. Deshalb ist eine zusätzliche Wartung der Ansichten erforderlich.

Datenquellenfilter

In Tableau Server können Filter direkt für eine Datenquelle erstellt werden, wodurch die Menge der von der Datenquelle zurückgegebenen Daten reduziert wird. Ihre Datenbank könnte zum Beispiel die Daten der letzten 5 bis 10 Jahre enthalten, doch Sie möchten, dass Ihre Benutzer nur Zugriff auf die Daten der letzten drei Jahre haben. Durch Hinzufügen eines Datenquellenfilters ist es ganz leicht, nur die Daten aus diesem Zeitraum anzuzeigen.

Wenn Sie einen Extrakt von einer Datenquelle mit bereits eingerichteten Datenquellenfiltern erstellen, werden diese Filter automatisch als Extraktfilter empfohlen und im Dialogfeld „Extrakt“ angezeigt. Diese empfohlenen Filter müssen nicht in der Extraktfilterliste enthalten sein. Sie können unabhängig vom vorhandenen Satz an Datenquellenfiltern entfernt werden.

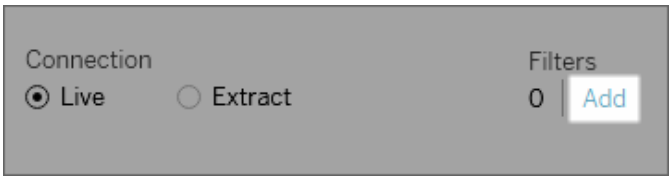

Abbildung 4: Hinzufügen von Filtern zu Tableau-Datenquellen von Tableau Desktop aus

Datenquellenfilter können nützlich sein, um die Daten zu beschränken, die Benutzer sehen können, wenn Sie eine Arbeitsmappe oder Datenquelle veröffentlichen. Wenn Sie eine Datenquelle in Tableau Server veröffentlichen, werden die Datenquelle und alle zugehörigen Dateien oder Extrakte in ihrer Gesamtheit zu dem Server transportiert. Beim Veröffentlichen einer Datenquelle können Sie Zugriffsberechtigungen zum Herunterladen oder Ändern der Datenquelle definieren. Sie können auch auswählen, welche Benutzer und Gruppen über Tableau Online externe Remote-Abfragen der Datenquelle durchführen können. Wenn Benutzer zu Abfragen berechtigt sind, aber keine Berechtigung zum Herunterladen haben, können Sie ein umfangreiches Datenmodell mit berechneten Feldern, Aliasen, Gruppen, Sätzen und vielem mehr bereitstellen. Dieses Datenmodell beschränkt sich allerdings nur auf Abfragen.

Darüber hinaus können Benutzer, die die veröffentlichte Datenquelle abfragen, nie etwaige Datenquellenfilter sehen oder ändern, die in der zugrunde liegenden veröffentlichten Datenquelle vorhanden sind, und alle Abfragen dieser Benutzer unterliegen den Filtern dieser Datenquelle. Dies ist eine großartige Möglichkeit, einen beschränkten Teilsatz Ihrer Daten bereitzustellen. So können Sie beispielsweise die Dimensionen nach bestimmten Benutzern und Gruppen filtern oder einen Datenquellenfilter basierend auf einem festen oder relativen Datumsbereich festlegen. Dies ist häufig aus Datensicherheitsgründen nützlich und gestattet Ihnen, die Leistung der Remote-Datenbank zu verwalten, die Tableau Server letztendlich im Namen eines Benutzers abfragt. Für Systeme, die im hohen Maße auf Partitionen oder einer Indizierung beruhen, bieten Datenquellenfilter eine starke Kontrolle über die Leistung der von Tableau erstellten Abfragen.

Extraktsicherheit

Bei Nutzung von Datenextrakten ist Tableau Server für das Speichern und Verarbeiten der in Ansichten und Arbeitsmappen verwendeten Daten verantwortlich. Die Daten werden im Dateisystem in einem verschlüsselten, komprimierten und binären Format als Tableau-Datenextrakt (TDE) gespeichert. Die Metadaten, die die Extrakte beschreiben, werden im Nur-Text-Format gespeichert. Das heißt, die Metadaten sind für Menschen nicht lesbar. Wir können jedoch einige Beschreibungen der Daten wie die Datentypen, Feldnamen usw. erkennen. Tableau Server speichert diese Dateien zum Schutz im Verzeichnis „Programmdaten“, wobei die Zugriffskontrolle auf den Tableau Server-Benutzer des Kontos „Als Benutzer ausführen“ sowie auf die lokalen Administratoren des Computers beschränkt ist. Die Extraktdatendateien selbst werden auf der Festplatte nicht verschlüsselt.

Daten-Engine-Extrakte können ebenso wenig direkt von der Tableau Server-Benutzeroberfläche aus abgefragt werden wie andere Datenbanken, zu denen Tableau eine Verbindung herstellt. Die Benutzer können zwar eine „Drag & Drop“-Analyse durchführen, doch sie können keine Abfragen in SQL, MDX oder irgendeiner anderen Syntax verfassen, um mit der Daten-Engine-Datenbank zu interagieren. Das hilft, nicht autorisierten Zugriff, SQL-Injection-Angriffe und andere böswillige Angriffe auf Extrakte zu verhindern.

Die Integration in Drittanbieter- und BS-Lösungen zur Verschlüsselung auf Festplattenebene (z. B. BitLocker) bzw. auf Datei- und/oder Verzeichnisebene (z. B. Encrypting File System, kurz EFS) ist möglich, um die Sicherheit der Datenextraktdateien noch weiter zu optimieren. Doch diese Lösungen zielen im Allgemeinen auf sämtliche Daten auf der Festplatte ab, sodass die Verschlüsselung nicht auf die Tableau Server-Datendateien beschränkt wäre. Darüber hinaus könnte durch die Aktivierung dieser Lösungen auch die Leistung beeinträchtigt werden.

Repository-Sicherheit

Tableau Server verfügt über eine interne Repository-Datenbank, die Informationen über das System (Nutzungsstatistiken, Benutzer, Gruppen, Berechtigungen usw.) sowie Inhalte (Arbeitsmappen, Ansichten, Kommentare, Tags usw.) speichert. Das Repository speichert weder Rohdaten noch extrahierte Daten, die in Tableau-Ansichten und -Arbeitsmappen verwendet werden.

Das Repository gestattet standardmäßig keine externen Verbindungen. Das heißt, dass die im Repository gespeicherten Informationen standardmäßig ausschließlich den Tableau Server-Komponenten vorbehalten sind. Kunden, die direkten Zugriff auf diese Informationen wünschen, können das Repository jedoch mithilfe des Befehls „tabadmin dbpass“ so konfigurieren, dass externe Verbindungen zugelassen sind. Externe Verbindungen sind auf schreibgeschützte Ansichten der Daten beschränkt, um eine böswillige Nutzung und versehentliche Änderungen der Inhalte oder der Konfiguration von Tableau Server zu verhindern. Sie können das Repository auch so konfigurieren, dass nur SSL-Verbindungen über das Tableau Server-Konfigurationsdienstprogramm zugelassen werden.

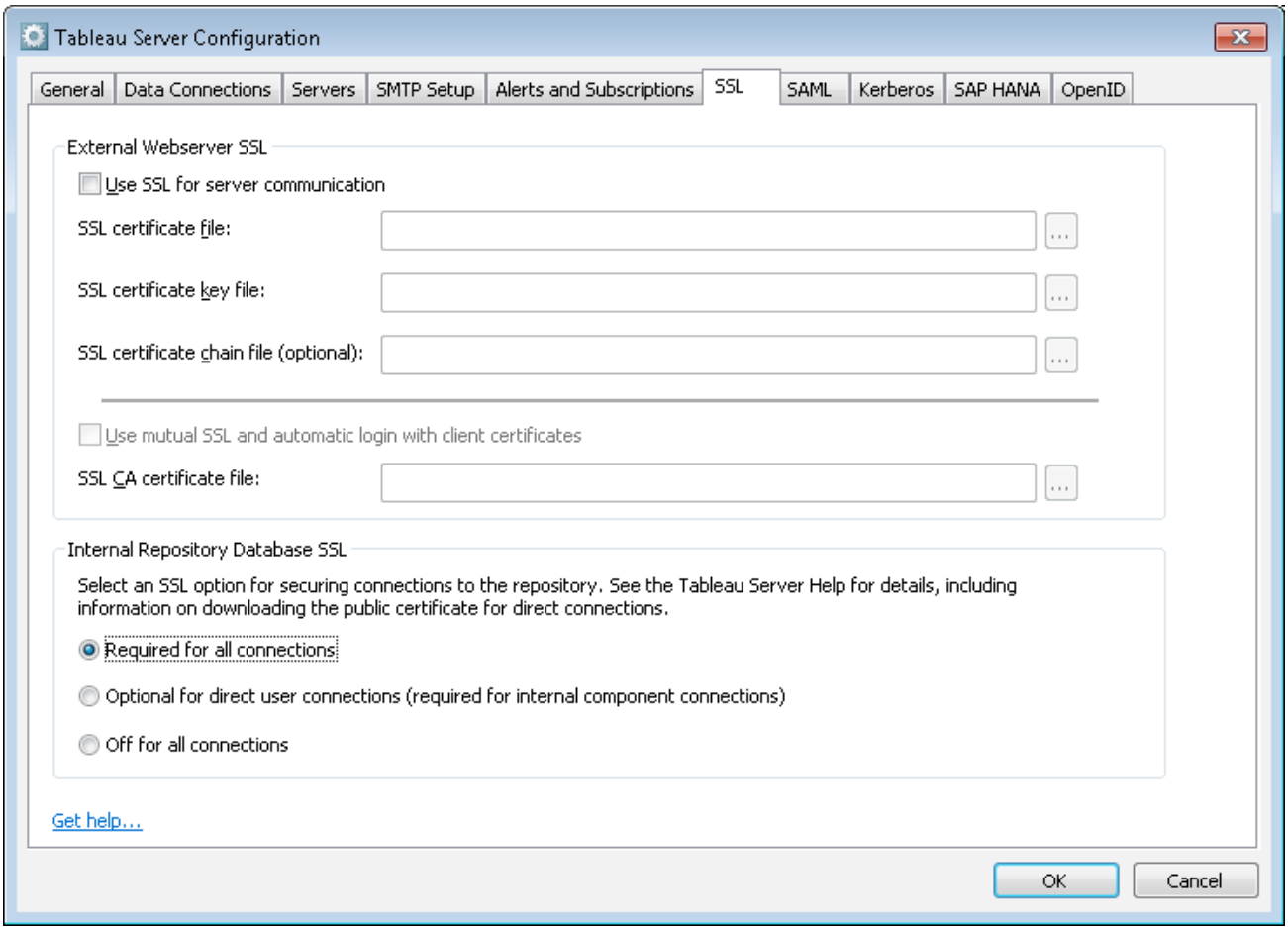

Abbildung 5: Konfigurieren von SSL für die interne Repository-Datenbank

4. Netzwerk – Übertragungssicherheit

Administratoren verwenden häufig Netzwerksicherheitsgeräte, um lokal bereitgestellte Instanzen von Tableau Server vor dem Zugriff aus nicht vertrauenswürdigen Netzwerken und aus dem Internet zu schützen. Doch auch in solchen Fällen müssen die Anmeldeinformationen sicher im Netzwerk übertragen werden. Wenn der Zugriff auf Tableau Server nicht eingeschränkt ist, gewinnt die Übertragungssicherheit sogar noch größere Bedeutung für den Schutz vertraulicher Daten und Anmeldeinformationen sowie für die Vermeidung einer böswilligen Nutzung von Tableau Server. Unabhängig von Ihrer jeweiligen Situation verfügt Tableau Server über robuste Übertragungssicherheitsfunktionen.

Es gibt drei Hauptnetzwerkschnittstellen: die Schnittstelle zwischen Client und Tableau Server, die Schnittstelle zwischen Tableau Server und der Datenbank sowie die Schnittstelle für die Kommunikation zwischen den Tableau Server-Komponenten. Jede dieser Schnittstellen wird nachstehend beschrieben. Neben diesen umfassenden Sicherheitsfunktionen achtet Tableau besonders auf die Speicherung und Übertragung von Kennwörtern auf allen Ebenen und Schnittstellen.

Schnittstelle zwischen Client und Tableau Server

In diesem Fall ist mit „Client“ ein Webbrowser, Tableau Desktop, tabcmd oder eine REST API-Anwendung gemeint. Für diese Kommunikation werden üblicherweise standardmäßige HTTP-Anfragen und -Antworten verwendet, die sich für die meisten internen Bereitstellungen eignen. Für externe oder vertrauliche Bereitstellungen lässt sich Tableau Server mit vom Kunden bereitgestellten Sicherheitszertifikaten für HTTPS (SSL/TLS) konfigurieren. Wenn Tableau Server für HTTPS konfiguriert ist, werden der gesamte Inhalt und die gesamte Kommunikation zwischen den Clients verschlüsselt, und das HTTPS-Protokoll wird verwendet. SSL/TLS sollte für alle Bereitstellungen aktiviert werden, bei denen es auf die Sicherheit ankommt.

Wenn Tableau Server für HTTPS konfiguriert ist, handeln der Browser und die HTTPS-Bibliothek auf dem Server eine gemeinsame Verschlüsselungsebene aus. Tableau Server verwendet OpenSSL als serverseitige HTTPS-Bibliothek und ist so vorkonfiguriert, dass die derzeit akzeptierten Standards genutzt werden. Jeder Webbrowser, der über SSL auf Tableau Server zugreift, verwendet die von dem betreffenden Browser bereitgestellte HTTPS-Standardimplementierung. Das funktioniert selbst bei Nutzung eingebetteter Anmeldeinformationen und beschert dem Endbenutzer eine nahtlose Erfahrung ohne Sicherheitswarnungen, Pop-up-Fenster oder Ausnahmen.

Tableau Desktop kommuniziert entweder mithilfe von HTTP oder über HTTPS mit Tableau Server. Um sicheren Schutz bei der Übertragung von Kennwörtern zu bieten, muss HTTPS aktiviert sein.

Kommunikation zwischen Tableau Server und der Datenbank

Tableau Server stellt während der Ausführung Verbindungen zu Datenbanken her, um Ergebnissätze zu verarbeiten und Extrakte zu aktualisieren. Tableau verwendet möglichst immer native Treiber, um Verbindungen zu Datenbanken herzustellen. Tableau nutzt einen generischen ODBC-Adapter, wenn keine nativen Treiber verfügbar sind. Die gesamte Kommunikation mit der Datenbank wird über diese Treiber geleitet. Daher wird der Treiber im Rahmen der Installation der nativen Treiber so konfiguriert, dass er über andere Ports als die Standardports kommuniziert oder die Transportverschlüsselung bereitstellt. Diese Art von Konfiguration ist für Tableau transparent.

Kommunikation zwischen Tableau Server-Komponenten

Dieser Abschnitt gilt nur für verteilte Bereitstellungen von Tableau Server. Die Kommunikation zwischen Tableau Server-Komponenten basiert auf zwei wichtigen Faktoren: Vertrauensstellung und Übertragung. In einem Tableau-Cluster verwendet jeder Server ein stringentes Vertrauensstellungsmodell, um den Empfang gültiger Anforderungen von anderen Servern im Cluster sicherzustellen. Die Vertrauensstellung wird durch eine Whitelist mit vertrauenswürdigen IP-Adressen, Ports und Protokollen begründet. Ist eines dieser Elemente ungültig, so wird die Anforderung ignoriert. Alle Mitglieder des Clusters können miteinander kommunizieren. Es wird empfohlen, Tableau Server mit einer Firewall vor unsicheren Servern zu schützen.

5. Weitere Überlegungen

Extranets sind von Natur aus nach außen gerichtet. Deshalb verfügt Tableau Server über zahlreiche integrierte Schutzfunktionen, um seine Integrität in einer exponierten Umgebung sicherzustellen. Wir setzen zum Beispiel voraus, dass die gesamte Client-Kommunikation über einen einzelnen Port erfolgt. Darüber hinaus unterstützen wir die Konfiguration von Weiterleitungs- und Reverseproxys, damit die Kommunikation zwischen Ihrem Netzwerk und dem Internet über Proxyserver erfolgt.

Tableau hat in ein internes Sicherheitsteam investiert, das aktiv nach Sicherheitsrisiken sucht und mit monatlichen Updates schnell auf neue Bedrohungen reagiert. Besuchen Sie die Seite „Sicherheit“ und lesen Sie unser Whitepaper über die Entwicklung sicherer Software, um sich die neusten Informationen zu holen. Abschließend möchten wir Ihnen dringend nahelegen, sich auch die Checkliste für die Absicherung anzusehen, die weitere Empfehlungen für den Schutz Ihrer Tableau Server-Bereitstellung enthält.

Zusammenfassung

Tableau Server stellt ein umfassendes Spektrum an Sicherheitsfunktionen bereit, um Ihre Bereitstellungsanforderungen zu erfüllen. Tableau hat nicht nur kundenorientierte Bereitstellungen an unzähligen Kundenstandorten erfolgreich implementiert, sondern auch interne Bereitstellungen in sicheren Netzwerken. Tableau verwendet moderne Industriestandards als Baseline und reagiert rasch auf künftige Bedrohungen und Probleme. Tableau hat die Antworten auf Ihre Sicherheitsfragen direkt in seine Plattform integriert, um von der Sicherheit auf Zeilenebene bis zu sicheren Websites jedes relevante Sicherheitsdetail abzudecken.

Über Tableau

Tableau unterstützt Benutzer bei der Umwandlung von Daten in praktisch umsetzbare Erkenntnisse, die den Unternehmenserfolg fördern. Sie können einfach eine Verbindung zu beliebigen Daten herstellen, ganz gleich, wo und in welchem Format sie gespeichert sind. Führen Sie auf schnelle Weise Ad-hoc-Analysen durch, um potenzielle Geschäftschancen zu ermitteln. Erstellen Sie per Drag & Drop interaktive Dashboards mit fortgeschrittenen visuellen Analysen. Anschließend können Sie diese in Ihrem Unternehmen gemeinsam nutzen und so Kollegen die Möglichkeit geben, die Daten aus ihrer Perspektive auszuwerten. Von globalen Unternehmen über neu gegründete Startups bis hin zu kleinen Firmen können Benutzer mit der Analyseplattform von Tableau überall ihre Daten sichtbar und verständlich machen.

Weitere Informationen

Tableau Server Hardening Guide (Leitfaden zur Absicherung von Tableau Server)

Administratorhandbuch zu Tableau Server

Tableau Server High Availability: Delivering mission-critical analytics at scale (Hochverfügbarkeit von Tableau Server: Bereitstellung erfolgsentscheidender Analysen in großem Umfang)

Tableau Server Scalability – A Technical Deployment Guide for Server Administrators (Skalierbarkeit von Tableau Server – Technisches Handbuch zur Bereitstellung für Serveradministratoren)