Tableau Server 平台安全性

实施企业安全性四大原则

tableau

目录

简介

Tableau 是一个现代企业分析平台，可在管控之下提供大规模自助式分析功能。安全性是数据和内容管控策略的重中之重。Tableau Server 提供全面的功能和深入的集成，帮助应对企业安全的方方面面。Tableau 可帮助组织推广可信数据源，让所有用户都可以通过访问正确的数据，快速做出正确的决定。随着单一集中 EDW 的前景日益衰落，以及云技术推动下数据量的持续加速增长，在所有不同平台之间实现一致的安全性对企业至关重要。

概述

企业应用程序安全性有四个主要组成部分，本白皮书将围绕 Tableau Server 对其进行详细讨论：

1.身份验证

2.授权

3.数据安全性

4.网络–传输安全性

如果实施方式正确，这四个组成部分可以满足所有企业安全性要求，让广大用户能够访问可信数据，构建报告和仪表板，开展协作式分析。业务用户信任安全数据和分析平台提供的信息，这有助于扩大使用范围，实现更大的数据价值。组织可以在不违反企业安全性要求的情况下，为客户和承包商提供相同分析平台的外部访问权限。

Tableau Server 已满足金融服务、政府、医疗和高等教育领域客户的苛刻安全性要求。银行和投资公司直接向自己的客户传送敏感和机密的投资信息。高等院校使用 Tableau Server 直接向学生和教职人员传送个性化报告。所有军种部门以及众多州政府和联邦政府机构都部署了 Tableau Server。此文档说明 Tableau Server 如何提供全面的企业级安全性。

1 身份验证

Tableau Server 支持多种行业标准身份验证，包括 Active Directory、LDAP、Kerberos、OpenID Connect、SAML、受信任票证和证书。Tableau Server 还具备自己的内置用户身份服务，名为"本地身份验证"。

Tableau Server 为登录用户提供可自定义的体验，包括语言和区域设置、个性化开始页面以及个人作品概览。Tableau Server 对用户信息进行跨会话保存，实现一致的个性化体验。为此，Tableau 为系统中的每

个用户名创建和维护一个帐户。此外，作者和发布者可以使用服务器范围的身份信息，针对自己发布的视图的基础数据，控制其他用户的授权级别。

用户身份

如上文所述，您可以使用 Active Directory 管理用户身份，也可以使用"本地身份验证"将身份信息存储在服务器中。下文将说明这两种管理用户身份验证的方法有何差异。

Active directory

如果客户选择将 Tableau Server 与 Active Directory 集成，并将后者用作身份存储区，则 Active Directory 将管理所有用户名和密码。

虽然用户和组均由 Active Directory 集中管理，但 Tableau Server 也会在自己的存储库中存储用户名和组的副本。配置 Active Directory 身份验证时，Tableau 不会存储密码。要与 Active Directory 同步用户和组，可以由管理员手动进行同步，也可以使用 tabcmd 命令行实用工具或 REST API 以编程方式进行同步。

本地身份验证

Tableau Server 还包含内置的用户管理和身份验证服务，名为"本地身份验证"。不愿意使用 Active Directory 或者在 AD 外的客户端上实施部署的组织可使用这种方法。如果使用"本地身份验证"，Tableau Server 负责管理用户、组和整个身份验证流程。管理员可以选择在 Tableau Server 上存储密码。但也可以选择将密码和用户信息委托给外部服务，例如 OpenID 或 SAML。用户列表可以轻松导入到 Tableau Server 中，并且大多数用户管理功能可以通过 tabcmd 或 REST API 以编程方式执行。因此，Tableau 用户可以在自动化预配流程中轻松预配。

LDAP

Linux 版 Tableau Server 支持通过任何 LDAP 提供程序进行身份验证；Windows 版将在近期提供同样的支持。只要支持 LDAP 协议及以下任何一种身份验证机制，任何目录服务均可使用 Active Directory 服务器所能提供的各种身份验证和用户管理功能：GSSAPI、简单绑定、Kerberos 简单绑定。 与您的 IT 部门合作，确定适合自己的选项。

单点登录以及与外部身份验证服务集成

Tableau Server 支持多种类型的单点登录 (SSO) 解决方案和相互 SSL（客户端证书身份验证）。

相互 SSL 在所有设备上提供了安全的 Tableau 自动登录体验。如果使用互相 SSL，当具有有效证书的客户端（Windows 上的 Tableau Desktop、Web 浏览器或 tabcmd.exe）连接到 Tableau Server 时，Tableau Server 会确认存在有效客户端证书，并使用在证书中找到的用户名让用户自动登录系统。

如果使用 SSO，用户无需显式登录 Tableau Server。他们用于通过其他外部身份验证服务进行身份验证

（例如，登录到自己的公司网络）的凭据可以在不显示任何登录提示屏幕的情况下，无缝地用于 Tableau Server 身份验证。SSO 从外部确定用户身份，并将其映射到 Tableau Server 身份存储区中定义的用户身份。

如果将 Tableau Server 配置为使用外部身份验证服务进行 SSO，则该外部身份验证服务将处理所有身份验证。然而，Tableau Server 将根据身份存储区中存储的站点角色来管理用户对 Tableau 资源的访问权限。有关详细信息，请参阅下文中的"授权"部分。

Tableau Server 支持与以下外部身份验证服务的集成：

- **SAML :** 您可以将 Tableau Server 配置为使用 SAML（安全断言标记语言）进行 SSO。使用 SAML 时，外部身份提供程序 (IdP) 验证用户的凭据，然后向 Tableau Server 发送安全断言，其中包含关于用户身份的信息。即便配置了 Active Directory 或本地身份验证，您仍然可以使用 SAML 来访问 Tableau Server。您还可以将 Tableau Server 配置为对每个站点使用不同的 SAML IdP，这称为"站点特定 SAML"。

- **Kerberos :** 如果 Kerberos 已在您的环境中启用，并且 Tableau Server 被配置为使用 Active Directory 身份验证，则您可以根据用户的 Windows 身份为其提供 Tableau Server 访问权限。如果 Tableau Server 配置为使用本地身份验证，则您无法使用 Kerberos。

- **集成 Windows 身份验证 :** 如果 Tableau Server 配置为使用 Active Directory 身份验证，您可以启动自动登录。"自动登录"使用 Microsoft SSPI，根据用户的 Windows 用户名和密码使其登录。系统不会提示用户输入凭据，因此登录体验类似于单点登录 (SSO) 和 Kerberos。

- **OpenID :** OpenID Connect 是一种标准身份验证协议，它让用户可以通过兼容的身份提供程序登录。成功登录自己的身份提供程序后，用户会自动登录 Tableau Server。要将 OpenID Connect 和 Tableau Server 配合使用，Server 必须配置为使用本地身份验证；不支持 Active Directory 身份验证。

- **受信任的身份验证 :** 受信任的身份验证（又称受信任票证）让您可以在 Tableau Server 和一个或多个 Web 服务器之间设置受信任的关系。收到来自受信任 Web 服务器的请求时，Tableau Server 会认为该 Web 服务器已经完成必要的身份验证。Tableau Server 接收带有可赎回令牌或票证的请求，并参考该用户的用户角色和权限为其显示个性化视图。

来宾用户或匿名访问

注意：此选项仅适用于使用基于核心的 *Tableau Server* 许可证的系统。

Tableau Server 可设置为允许通过来宾帐户进行匿名访问。如果要将内容部署到大型用户社区（例如公共 Web）或部署到不要求检查用户身份的社区（例如公司 Intranet），则可以使用这种方法。没有 Tableau Server 帐户的用户可以使用来宾许可证查看嵌入视图并与之进行交互。

为了防止匿名访问者意外接触敏感信息，默认禁止以来宾身份访问 Tableau Server 的功能。如果启用该功能，则系统会将来宾许可证分配给自动生成的来宾用户。鉴于来宾用户是匿名用户（也就是说其身份无法确定），Tableau 只提供一个来宾用户，因为它是通用的。

匿名用户无需登录 Tableau Server 即可加载包含嵌入式可视化的网页，但您可以要求匿名用户在访问 Intranet 或包含该视图的网页时提供凭据。匿名用户不能浏览存储库；他们只能访问嵌入视图（具有"embed=true"参数设置的 URL）。为简便起见，如果匿名用户请求没有嵌入式标志的视图，

Tableau Server 会将该请求视为对嵌入视图的请求。也就是说，系统会适当处理通过电子邮件共享或者从其他网页链接的 URL，使其可供访问。请注意，匿名用户只会看到来宾可以访问的视图（在权限中定义）；不会显示禁止来宾用户访问的任何视图，无论其是否有"embed"标志。

组织可以在所有其他 Tableau Server 用户类型可用的角色、权限和数据安全性的完整范围内，对来宾用户的内容访问权限进行控制。收到嵌入视图请求时，Tableau Server 首先检查该用户是否已经登录（即该请求是否附有尚未过期的登录会话 Cookie）。如果用户未处于有效登录状态，则将该请求当作来宾用户请求处理（如果来宾用户已启用）。

如果将 Active Directory 身份验证设置为启用自动登录，则不能进行来宾用户访问，因为这会在处理无效凭据时引起歧义。

注销

会话的终止是一个经常被忽视的身份验证领域。Tableau Server 中的会话会根据非活动时间长度自动超时。管理员可以更改默认的空闲持续时间超时长度。Tableau Server 还支持配置绝对会话超时。

使用 Active Directory 身份验证并启用自动登录时，系统为用户提供"切换用户"而不是"退出"选项。这是因为如果启动注销，他们会自动重新登录。对于所有其他身份验证方案，系统为用户提供"退出"选项，让他们可以在完成会话时手动注销。

对于集成环境（例如嵌入门户中的视图），最好以编程方式在门户注销的基础上，强制注销 Tableau Server。为此，您只需从客户端调用注销 URL：`https://<Tableau Server>/ manual/auth/logout`。

2 授权

对用户进行适当身份验证并授权用户访问系统后，下一步就是针对内容和服务器访问权限进行授权。Tableau Server 中的站点角色和权限为管理员提供细化控制，包括控制用户可以访问哪些数据、内容或对象，以及用户或群组可对该内容执行什么操作。这些操作通常称为功能，包括查看和交互、添加注释、保存工作簿以及连接到数据源等等。

您还可以通过用户分组，更加轻松地对权限进行成批应用。Tableau Server 让您能够针对每项内容（项目、数据源、工作簿或工作簿中的各个视图）及指定的用户/组，对权限（允许、拒绝或未指定/继承）进行灵活设置。如果未明确针对某项内容进行权限设置，Tableau 将应用一组默认权限。这些默认权限取决于创建内容时的默认设置，并且会从该内容的父级继承。权限并不控制哪些数据将出现在视图中。我们稍后将在"数据访问安全性"部分讨论如何控制用户看到的数据。

以下示例明确拒绝向运营组成员授予任何针对示例视图的功能。而 Joe Doe 获得了针对此视图的所有功能。营销团队的成员获得了查看该内容的权限，但与内容交互和编辑相关的功能尚未指定。这意味着 Tableau Server 自下而上进行检查，首先检查工作簿权限，然后检查项目权限，以便确定该组是否获得了这些权限。如果没有，则会默认拒绝这些权限。

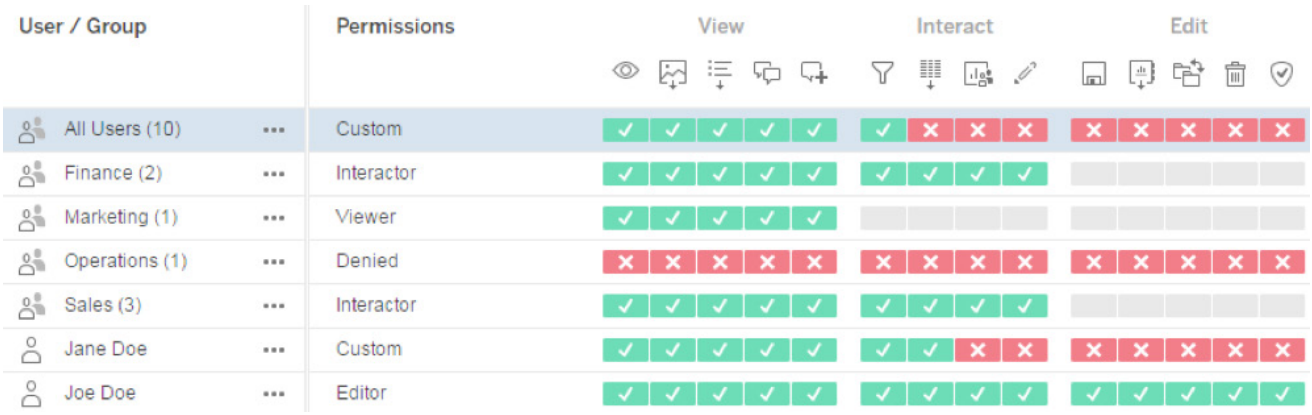

图 1.根据内容为组和用户设置自定义权限。

默认权限和继承

Tableau 通过模板机制设置内容的初始权限。这种机制从默认项目为项目复制初始权限。您务必根据组织的安全性模型，设置适当的默认项目权限。如果在鼓励知识和信息共享的自助式环境（又称为开放式权限模型）中部署 Tableau Server，默认项目权限应包括"所有用户"组，并按照"交互者"权限角色模板进行设置。随后，用户默认可以浏览服务器并与已发布视图进行交互，其访问权限仅仅受限于某些工作簿的自定义权限。如果在需要保证数据安全和访问控制的封闭式权限模型中部署 Tableau Server，"所有用户"组在默认项目中的权限应该为"无"。这会默认移除用户和组的所有权限。随后，用户和组必须获得明确授权才能在新创建的项目中发布和使用内容。

内容权限模型

已发布内容包括数据源、工作簿和视图。内容权限包括典型的内容管理操作，例如查看、创建、修改和删除。还包括用户可以在视图中进行的交互。用户搜索内容以及在 Tableau Server 用户界面导航时，也会应用权限。

内容权限不会保留分层结构；该项内容初次创建时，会从父级内容的权限复制初始权限。Tableau Server 还会从其父级工作簿权限复制视图的初始权限。对父级内容进行的任何权限更改不会自动重新应用到子级内容，除非手动刷新内容并重新定义权限。内容的权限可以不同于其父级内容。根据作者的定义，这些规则可以更加严格或更加宽松。

用户权限模型

与内容的权限模型不同，Tableau Server 为用户和组权限提供继承模型。如果不对用户的具体权限进行明确设置，则该用户会继承其所在组的权限设置。在 Tableau Server 权限管理器视图中，这会显示为未指定权限或灰色方

框（见图 1 和 2）。如果用户或组没有在继承链中明确获得某项功能，则系统会拒绝此功能。对组权限的更改将自动传播到所有用户。

要了解用户或组权限的设置结果，一个有用的技巧是在权限页面选择该组或用户，然后查看底部的用户权限区域。这样，您便可以在应用该组的继承设置后，看到每个用户的实际权限。在具体功能上方悬停同样可以获得相关信息，了解该功能的名称、设置结果以及结果的确定方式。

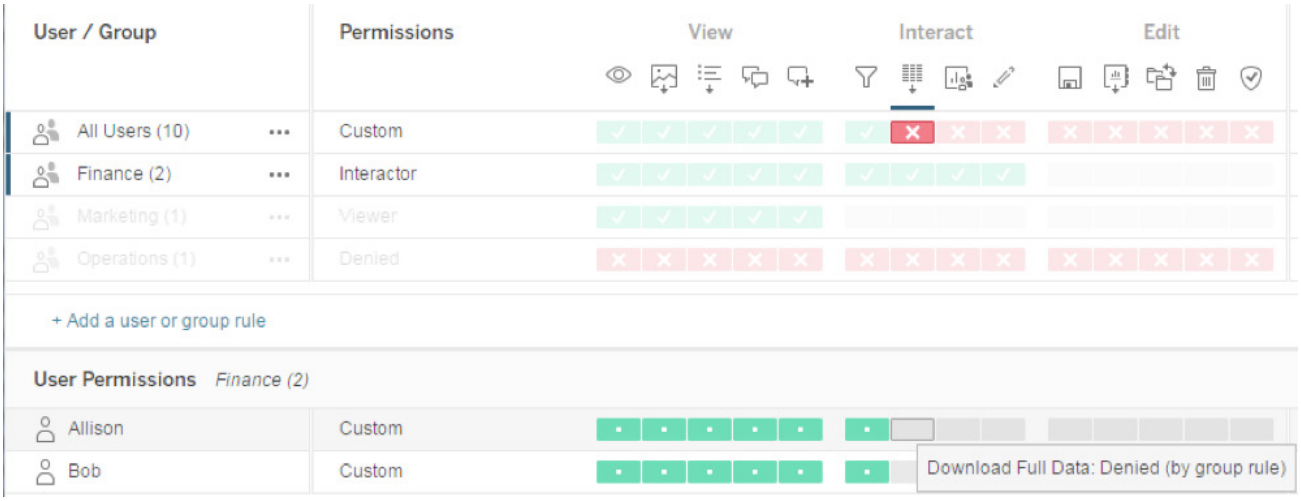

图 2. 查看某个用户的权限设置结果。

Tableau Server 权限

项目

项目控制对该项目发布的所有工作簿、视图和数据源的默认权限。仅站点和服务器管理员可以创建和修改项目及其权限，而获得"项目主管"权限的用户可以完全控制各自项目内的所有内容和权限。具有相关权限的用户可以覆盖任何内容的默认权限。例如，发布者可以完全控制对于自己发布的内容的访问权限。如果管理员需要对特定项目中的权限进行更多控制，他们可以定义和限制该项目的权限。锁定项目中的权限意味着发布到该项目的所有内容均使用管理员为该项目设置的默认权限。此后，无论是在服务器上还是在工作簿发布过程中，内容所有者均无法更改权限。是锁定权限还是允许内容所有者自行管理权限，这取决于管理员以及项目本身的要求。某些项目可以锁定权限，而另一些则保持开放。日后可以根据需求本身的变化轻松修改权限。我们可以想象，在某些项目中锁定权限而让另一些项目保持开放是合理的做法。日后可以根据需求的变化轻松修改权限。

权限模板	说明
查看者	允许用户或组查看项目中的工作簿和视图。
发布者	允许用户或组将工作簿或数据源发布到服务器。
项目主管	允许用户或组为项目中的所有项设置权限。
无	将权限规则的所有功能设置为**未指定**。
已拒绝	将权限规则的所有功能设置为**已拒绝**。
数据源连接器	允许用户或组连接到项目中的数据源。
数据源编辑器	允许用户或组对项目中的数据源进行连接、编辑、下载、删除和权限设置。他们也可以发布数据源。已发布数据源的所有者可以更新连接信息和数据提取刷新计划。该权限涉及在他们访问时连接到数据源的视图。

工作簿和视图

根据您是为工作簿还是视图设置权限，功能列表和可用的权限角色模板会有所差异。如需关于功能定义的信息，请参阅“权限参考”。

权限模板	说明
查看者	允许用户或组查看服务器上的工作簿或视图。
交互者	允许用户或组查看服务器上的工作簿或视图、编辑工作簿视图、应用筛选器、查看基础数据、导出图像和导出数据。所有其他权限均从用户或组的项目权限继承。
编辑者	将规则的所有功能设置为**已允许**。
无	将规则的所有功能设置为**未指定**。
已拒绝	将规则的所有功能设置为**已拒绝**。
自定义	所选功能组合的管理员定义规则

数据源

数据源权限为 Tableau Desktop 和 Tableau Server 用户提供了另一层安全防护。

获得某数据源"连接"权限的用户可以使用 Tableau Desktop，通过 Tableau Server 的 Data Server 组件对该数据源进行查询。该用户可以使用自己的凭据，或保存的原创作者凭据（如果包含）。这意味着 Tableau Desktop 用户无需在自己的计算机上安装数据库驱动程序、下载数据，甚至无需使用每个数据库的凭据即可对数据仓库或 Tableau 数据提取进行实时查询。Data Server 可以起到代理作用，无需直接连接到数据库。

权限模板	说明
连接者	允许用户或组连接到服务器上的数据源。
编辑者	允许用户或组对服务器上的数据源进行连接、下载、删除和权限设置。他们还可以发布数据源，并且只要他们是自己发布的数据源的所有者，他们就可以更新连接信息和数据提取刷新计划。（如果管理员或项目主管更改数据源所有权，则后两项功能不再可用。）
无	将权限规则的所有功能设置为**未指定**。
已拒绝	将权限规则的所有功能设置为**已拒绝**。

此外，如果要访问的视图使用了 Tableau Server 上的已发布数据源，用户必须同时获得了该视图及该基础数据源的权限（数据和视图的"查看"或"连接"权限）。但如果视图发布者选择将自己的凭据嵌入数据源，则有权查看该视图的用户也可以代表发布者连接到该数据源。要详细了解 Data Server，请观看我们的 Data Server 视频。

关于连接的简短说明

Tableau Server 在工作簿和数据源的发布过程中自动创建数据连接。因此，管理员和数据所有者可以在视图之外控制连接属性。无需手动编辑每个工作簿即可更新凭据或迁移到新的数据库服务器。此外，多个工作簿和数据源可以利用同一个连接，从而提高性能并减少重复。这还意味着，缓存数据可以在不同工作簿之间共享，从而进一步降低了数据库服务器负载。

权限和管理员

管理员分为两种类型：服务器管理员和站点管理员。服务器管理员对所有服务器和站点功能、服务器上的所有内容及所有用户具有完全访问权限。他们还可以配置整个服务器群集，包括管理站点、用户、维护、设置、计划以及搜索索引。站点管理员可以管理站点内的用户、组、项目、工作簿和数据连接。根据委托管理方案，站点管理员可以选择为站点添加用户。

所有管理员均会自动获得发布权限。管理员还可以创建与自己级别相同的其他管理员。

多租户部署

在组织内，管理员常常使用组和项目来对内容进行组织和授权，但如果要在同一个 Tableau Server 上支持多个外部参与方（租户），最常见的做法是使用站点。事实上，这就是 Tableau 的托管软件即服务 (SAAS) 产品 Tableau Online 的实施方式。每个站点中的内容（工作簿、数据源、用户等）与该 Tableau Server 实例上的所有其他内容隔离。换一种说法，Tableau Server 允许服务器管理员在服务器上为不同的用户和内容组创建多个站点，以此支持多租户。以"每个站点单独处理"的方式发布、访问、管理和控制所有服务器内容。这意味着无法跨站点共享数据源和连接。这项功能使 Tableau Server 具有稳固的安全性，足以满足金融、健康、教育等领域机构的部署需求，在这些领域中，一个公司的客户在任何情况下均不能查看其他客户的数据。

然而必须注意，在 Tableau Server 上具有管理员或发布者权限的用户可以看到所有 Tableau Server 用户的列表（因为他们要为新内容设置角色权限）。此外，服务器管理员可以查看发布到 Tableau Server 的所有内容，但这并不意味着他们可以访问 Tableau Server 使用的所有数据，因为数据访问有别于内容权限。
下一部分将更加深入地讨论这个主题。

要详细了解 Tableau Server 上的权限，请参阅 Tableau Server：适用于每个人的安装指南 。

3 数据访问安全性

数据访问安全性在任何一家企业都至关重要，尤其是需要满足联邦监管要求的组织以及在外部客户端上部署 Tableau Server 的组织。Tableau 必须提供稳固的功能，让客户可以在当前已实施的数据安全性措施的基础上再进一步，并对任何有缺陷的现有系统进行增强。目标是在同一个位置实施数据安全性措施，
无论用户是通过 Web 和移动设备从已发布视图访问数据，还是通过 Tableau Desktop 访问数据。

为确保数据安全性，有三种主要的方法：

1.仅仅在数据库内部实施安全性措施（数据库身份验证）

2.仅仅在 Tableau 中实施安全性措施

3.创造一种混合式方法，使 Tableau Server 中的用户信息在数据库中有对应的数据元素。

Tableau Server 支持所有三种方法，但客户常常青睐混合式方法，因为它简单灵活，在使用多个不同数据源时尤为理想。

利用数据库安全措施时，务必注意，所选的数据库身份验证方法至关重要。该级别的身份验证不同于上文讨论过的 Tableau Server 身份验证（即，用户登录 Tableau Server 时尚未登录数据库）。这意味着，为了实施数据库级别安全性措施，Tableau Server 用户还需要用于登录数据库的凭据。为了进一步保护您的数据，Tableau 只需要数据库的读取访问凭据，因此您可以将用户的访问限制为只读访问。这可以防止发布者不小心更改基础数据，并且很多时候可以提高查询性能。但在一些情况下，最好让数据库用户获得创建临时表的权限。这既有利于性能，也有利于安全性，因为临时数据存储在仪表板中，而不是 Tableau 中。一方面可以让 Tableau 用户获得有限的写入访问权限，以便创建临时表，另一方面需要将更多数据本地存储在 Tableau Server 中；我们需要对二者进行权衡。

您还可以通过在工作簿和数据源中设置用户筛选器来限制每位用户可以看到哪些数据，以便更好地根据用户的 Tableau Server 登录帐户，控制用户在已发布视图中看到的内容。将这些方法结合起来，您就可以通过发布单个视图或仪表板，为 Tableau Server 上的众多用户提供安全的个性化数据和分析。

数据库身份验证

如果使用 Tableau 的快速数据引擎提取数据，数据库安全性权限就不会传播给最终用户。自动刷新或递增数据提取时，Tableau Server 将使用已保存的一组凭据为每个数据源生成数据提取（使用"用户运行身份"或工作簿中内嵌的凭据）。它将执行用户对数据库的安全性权限。

在 Tableau Server 上发布的具有实时数据连接的视图是动态的，因为它们每次都会查询数据库，以检索最新数据。只要用户打开视图并且数据源是需要登录的数据库（而不是 Excel 工作簿或文本文件等），Tableau Server 就需要知道用于连接和检索数据的数据库用户名和密码。Tableau Server 通过几种相互配合的选项和设置，来指定用于访问数据的数据库用户名和密码。必须明确区分 Tableau Server 的登录方法和数据库登录信息，前者用于访问 Tableau Server 本身，而后者可能是访问数据源时所需的信息。下表总结了创建视图并将其发布到 Tableau Server 时的选项：

Windows 身份验证

Tableau Server 使用"用户运行身份"凭据通过 Windows 连接至数据库。所有 Tableau Server 用户将共享此个人资料的数据库连接信息。不会使用发布者的凭据或登录到 Tableau Server 的用户的凭据。该选项要求数据

身份验证类型	Tableau Server 响应	Tableau Server 利用数据库中内置的基于用户的数据安全性措施？
用户名和密码提示	Tableau 提示每名查看者输入自己的数据库凭据	是的，数据库知道个人用户身份
嵌入式密码	作者在发布视图时指定数据库凭据。系统不会提示查看者输入任何凭据	不是，所有用户共享相同的数据库登录身份，也就是作者的登录身份
查看者/发布者凭据	用户的域用户名和密码用于通过 Kerberos 或 SAML 进行 SSO 身份验证	是的，数据库知道个人用户身份
Windows 集成安全性（NT 身份验证）	Tableau Server 的"用户运行身份"	不是，所有用户共享相同的数据库登录身份
Linux 集成安全性（AD/Kerberos 委派）	Tableau Server 的"用户运行身份"	是的，数据库知道个人用户身份
自定义		所选功能组合的管理员定义规则

库利用 Windows 集成的安全性措施。这在 SQL Server 或 SQL Server Analysis Services 实施中非常常见。安装后，Tableau Server 的默认"用户运行身份"为 Network Authority（网络授权）用户。根据其定义，此网络授权帐户无权连接数据库。要使用支持数据源 NT 身份验证的帐户，请指定包含域名的用户名和密码。

Linux 身份验证

Linux 版 Tableau Server 同样使用"用户运行身份"凭据，但具体做法稍有不同。在 Linux 上，您必须为要用作"用户运行身份"的用户提供密钥表文件。这意味着您需要为给定任务建立不同的"用户运行身份"。 例如，要连接到给定数据库，数据源必须使用数据源"主体运行身份"或"用户运行身份"。数据源"用户运行身份"必须是域用户，而不仅仅是本地用户。

用户名和密码（非嵌入式）

系统将提示每名 Tableau Server 用户使用自己的数据库特定用户名和密码登录数据库。如果您已经进行过数据库安全性设置，这种选项有利于通过 Tableau Server 利用这些安全性设置。如果在 Tableau Server 设置页面打开"保存的凭据"，Tableau Server 用户只需为每个数据源输入一次凭据。 Tableau Server 随后会存储该用户的数据源凭据，并在该名用户下次连接到相同数据源时使用这些凭据。请注意，这些凭据通常不同于登录 Tableau Server 时所用的凭据。Tableau 始终对存储在 Tableau Server 存储库中的所有密码进行加密。数据库密码以强密码方式进行加密。 应使用 tabadmin assetkeys 命令，为每个部署生成新的资产密钥。

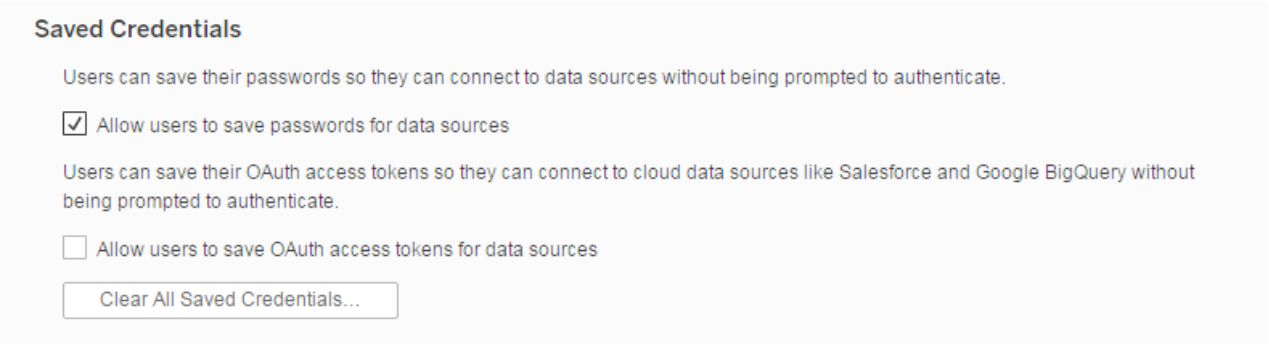

图 3. *Tableau Server*"设置"页面的"保存的凭据"设置。

嵌入式凭据（不适用于 Windows 身份验证）

如果启用嵌入式凭据，Tableau Server 可以记住每个工作簿原创作者的用户名和密码。作者只需在发布时输入该数据库的一组凭据（作者自己的用户名和密码），然后选择"嵌入式凭据"。所有 Tableau Server 用户随后便可使用相同的连接凭据，从该数据源检索数据。Tableau Server 使用前文所述的加密机制来保护存储库中的嵌入式凭据。选择这种方法时应该谨记：密码可能会过期，使用户无法访问数据。

其他数据库特定选项

模拟

对于 Microsoft SQL Server 数据源，Tableau Server 支持在查询运行时进行用户模拟。因此，Tableau 可以利用您已经在 Microsoft SQL Server 中实施的安全性措施。Tableau 将使用"用户运行身份"选项或嵌入式凭据连接到数据库。但在执行所有查询时，系统将假设另一名用户连接到了数据库。Tableau 模拟适用于与遵循 Microsoft 关于使用数据库模拟切换上下文的最佳做法实施的 SQL Server 配合使用。

Kerberos 委派

Kerberos 委派让 Tableau Server 能够使用工作簿查看者（而不是作者）的 Kerberos 凭据来执行查询。这种方法适合以下情况：

- 您需要知道谁在访问数据（数据源的访问日志将显示查看者名称）。
- 您的数据源具有行级别安全性设置，不同用户具有对不同单元格的访问权限。

要使用这种方法，数据库必须支持 Kerberos 委派。Tableau Server 要求进行约束委派，"用户运行身份"帐户需要明确地将权限授予目标数据库服务主体名称 (SPN)。Active Directory 中默认未启用委派。

行级别安全性及初始 SQL 模拟

连接到某些数据库时，您可以指定打开工作簿、刷新数据提取、登录 Tableau Server 或在 Tableau Server 上发布内容时要运行的初始 SQL 命令。这种初始 SQL 与自定义 SQL 连接不同，后者定义查询所针对的关系（表）。

您可以使用此命令来：

- 设置要在会话中使用的临时表
- 设置自定义数据环境

您可以在初始 SQL 语句中将参数传递到数据源。

这种方法的实用性体现在几个方面：您可以使用 TableauServerUser 或 TableauServerUserFull 参数配置模拟。在数据源支持的前提下，您可以设置行级别安全性措施（例如，针对 Oracle VPD 或 SAP Sybase ASE），确保用户只能看到自己有权查看的数据。

查询集束

对于 Teradata 数据源，Tableau Server 支持在查询集束中插入用户信息。这样便可以根据数据库规则或各种其他 Teradata 工作流规则限制数据。此外，使用查询集束还可以提高性能。要在 Tableau Server 中使用查询集束，必须对其进行正确配置。

用户筛选器

用户筛选器是 Tableau Server 的行级别安全性方法。Tableau 使用基于用户名、组成员身份及登录用户其他属性的动态数据筛选。处理视图时，Tableau Server 将对所有数据库查询附加相应的 WHERE 语句，以对当前用户的请求进行适当的数据限制。用户筛选器可用于所有数据源，包括数据提取。

可以使用计算字段构建已发布数据源，以便根据登录用户的用户名或组成员身份控制各种维度和度量。随后，该字段在发布前会被添加为数据源筛选器。通过拒绝下载功能，对于连接到数据源进行临时分析的 Tableau Desktop 和 Tableau Server 用户，用户筛选器都将保持不变。

例如，"订单"表可能包含客户信息（客户 ID）、销售人员信息（员工 ID）及关于订单的详细信息。可以通过在视图中添加单个计算字段来实现用户筛选：username()=customerID OR username()=employeeID。这样，只需向 Tableau Server 发布一个工作簿，即可安全地将正确的数据提供给外部客户和内部销售人员。根据各自的凭据，客户只会看到他们提交的订单，而销售人员只会看到自己处理的订单。

这种方法的好处是，在向系统添加新用户和数据时，无需对视图进行额外维护。筛选器规则内建到视图中，数据库为这些规则动态提供要处理的关键信息。

如果数据库中没有适当的内容来用于以编程方式确定为哪些用户提供哪些数据，则可以手动创建用户筛选器。此类型用户筛选器的处理方式与计算用户筛选器相同，但不会动态适应新用户和数据元素。因此需要对视图进行额外维护。

数据源筛选器

Tableau Server 支持直接对数据源创建筛选器，从而降低了从数据源返回的数据量。例如，您的数据库可能包含此前 5-10 年的数据，但您想让用户只能访问此前 3 年的数据。通过添加数据源筛选器，您可以轻松将显示的数据限制在上述时间范围内。

如果您从已经使用数据源筛选器的数据源创建数据提取，系统会自动建议将这些筛选器用作数据提取筛选器，并且它们会出现在数据提取对话中。这些建议的筛选器并非必须添加到数据提取筛选器列表中，您可以单独将它们从现有的数据源筛选器组中移除。

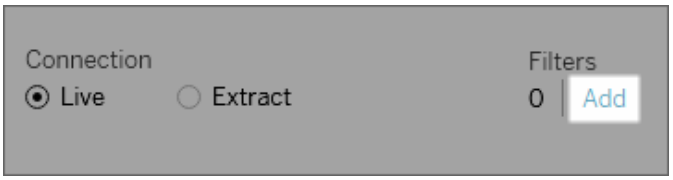

图 4. 从 *Tableau Desktop* 为 *Tableau* 数据源添加筛选器。

数据源筛选器可用于在发布工作簿或数据源时限制用户可以看到的数据。您将数据源发布到 Tableau Server 时，数据源及所有关联文件或数据提取将整体传输到服务器。发布数据源时，您可以定义数据源的下载或修改访问权限，还可以选择能够通过 Tableau Server 针对该数据源远程提交查询的用户和组。如果用户获得查询权限而没有下载权限，则可以共享包含计算字段、别名、群组、集等项目的丰富数据模型，但这些项目仅能用于查询。

此外，查询已发布数据源的用户绝无可能看到或修改基础数据源上的任何数据源筛选器，并且用户的所有查询都将经过该数据源筛选器的处理。这是一种提供限制性数据子集的好方法，例如通过筛选具体用户和组的维度，或者通过定义基于固定或相对日期范围的数据源筛选器。这不但有利于数据安全性，还让您能够管理远程数据库的性能，Tableau Server 最终将代表用户对远程数据库进行查询。对于高度依赖分区或索引的系统，数据源筛选器可以对 Tableau 提交的查询实现极大的性能控制。

数据提取安全性

使用数据提取时，Tableau Server 负责存储和处理视图及工作簿中使用的数据。数据作为 Tableau 数据提取 (TDE) 以编码和压缩的二进制格式存储在文件系统中。描述数据提取的元数据存储在纯文本中。这意味着人类无法阅读这些数据；但我们可以辨别一些数据描述，例如数据类型、字段名称等。为了保护这些文件，Tableau Server 将其存储在"Program Data"目录中并实施访问控制，使其仅能由 Tableau Server"用户运行身份"和计算机本地管理员访问。提取数据文件本身不会在磁盘上加密。

与 Tableau 连接的其他数据库一样，数据引擎数据提取无法直接从 Tableau Server 用户界面直接查询。用户可以执行拖放式分析，但不能通过编写 SQL、MDX 或任何其他语法来与数据引擎数据库直接交互。这有助于防止未授权访问、SQL 注入以及针对数据提取的其他恶意攻击。

可以通过与第三方及 OS 解决方案集成来实现磁盘级别加密（例如 BitLocker）或文件和/或目录级别加密（例如加密文件系统或 EFS），以便进一步增强数据提取文件的安全性。但这些解决方案通常会针对磁盘上的所有数据，因此加密不会仅限于 Tableau Server 数据文件。 此外，启用这些解决方案后，性能可能会受到影响。

存储库安全性

Tableau Server 有一个内部存储库数据库，用于存储关于系统（使用统计、用户、组、权限等）以及内容（工作簿、视图、注释、标记等）的信息。存储库不会存储原始数据或 Tableau 视图和工作簿中使用的提取数据。

默认情况下，存储库不允许外部连接。这意味着，默认情况下只有 Tableau Server 组件才能访问存储库中存储的信息。但希望直接访问这些信息的客户可以使用 tabadmin dbpass 命令来配置存储库，使其允许外部连接。为了防止 Tableau Server 内容和配置遭到恶意使用和意外更改，外部连接仅限于数据的只读视图。存储库还可以配置为仅允许使用 Tableau Server 配置实用工具的 SSL 连接。

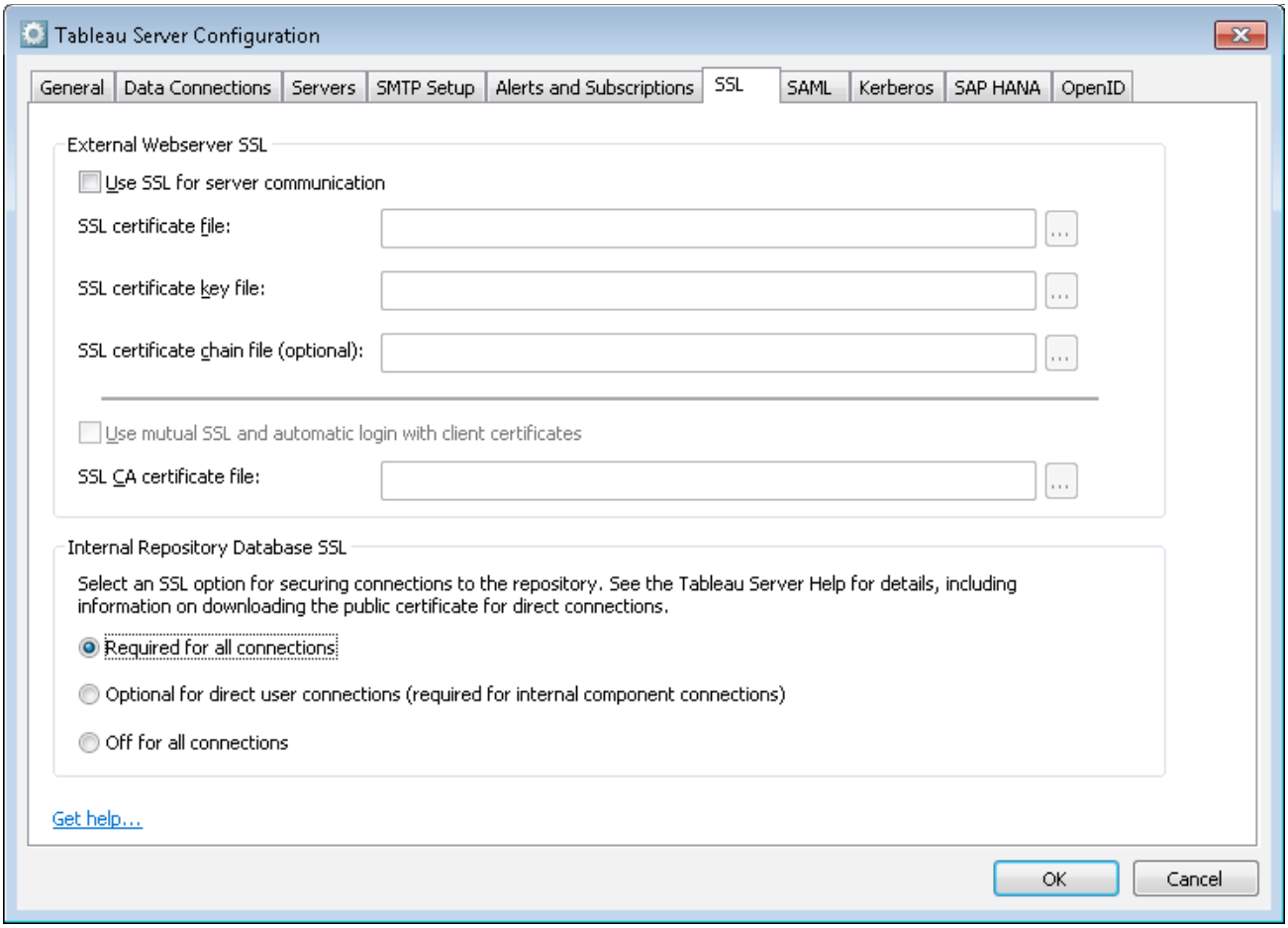

图 5. 配置内部存储库数据库 *SSL*

4 网络 – 传输安全性

针对来自不受信任的网络及 Internet 的威胁，管理员常常使用网络安全性设备来保护本地部署的 Tableau Server 的访问安全性。然而，即便是这样，仍然需要在整个网络安全传输凭据。如果不对 Tableau Server 进行访问限制，在保护敏感数据和凭据以及防止恶意使用 Tableau Server 方面，传输安全性的作用就会愈发关键。无论哪种情况，Tableau Server 都可以提供可靠的传输安全性功能。

Tableau Server 有三个主要网络接口：客户端至 Tableau Server、Tableau Server 至数据库以及 Tableau Server 组件间通信。下文将对其中每个接口进行说明。除了这些宏观的安全性功能，Tableau 特别注意密码在所有层级和接口的存储和传输。

客户端至 Tableau Server

在这里，“客户端”指 Web 浏览器、Tableau Desktop、tabcmd 或 REST API 应用程序。默认情况下，这些通信使用适合大多数内部部署的标准 HTTP 请求和响应。对于外部或其他敏感部署，可以基于客户提供的安全证书，对 Tableau Server 进行 HTTPS (SSL/TLS) 配置。如果对 Tableau Server 进行 HTTPS 配置，所有内容及客户端之间的通信都会加密并使用 HTTPS 协议。应该在需要关注安全性的所有部署中启用 SSL/TLS。

对 Tableau Server 进行 HTTPS 配置后，浏览器和服务器上的 HTTPS 库会通过协商确定共同的加密级别。Tableau 使用 OpenSSL 作为服务器侧 HTTPS 库，并且它被预配置为使用当前公认的标准。通过 SSL 访问 Tableau Server 的每个 Web 浏览器使用该浏览器提供的标准 HTTPS 实施。这种方法甚至适用于嵌入式情况，可以为最终用户营造无缝体验，使他们不会看到安全警告、弹出窗口和意外报告。

Tableau Desktop 使用 HTTP 或 HTTPS 与 Tableau Server 通信。要保护密码传输的安全性，必须启用 HTTPS。

Tableau Server 和数据库之间的通信

Tableau Server 通过与数据库建立动态连接来处理结果集和刷新数据提取。在可能的情况下，Tableau 使用本机驱动程序来连接至数据库。如果没有可用的本机驱动程序，Tableau 会依靠通用 ODBC 配接器。发送到数据库的所有通信内容都会通过这些驱动程序来进行路由。因此，需要在本机驱动程序的安装过程中将驱动程序配置为使用非标准端口进行通信或提供传输加密，此类配置对于 Tableau 是可见的。

Tableau Server 组件之间的通信

本部分内容仅适用于 Tableau Server 的分布式部署。Tableau Server 组件之间的通信有两个方面：信任和传输。Tableau 群集中的每个服务器节点使用一种严格信任模型来确保从群集中的其他节点接收有效请求。系统根据 IP 地址、端口和协议的白名单建立信任。如果上述任何一项无效，请求将被忽略。群集的所有成员可以相互通信。建议通过防火墙将 Tableau Server 与不安全的服务器隔离。

5 其他考虑事项

由于 Extranet 本质上是面向外部的，Tableau Server 具有多种内置的防护机制，可以在暴露的环境中保持完整性。例如，我们要求所有客户端通信通过同一个端口。此外，我们还提供正向和反向代理的配置支持，让您的网络和 Internet 之间的通信可以使用代理服务器进行协调。

Tableau 组建了一个内部安全团队，该团队积极开展漏洞测试并通过每月发布的更新快速解决新威胁。如需最新信息，请访问我们的安全性页面并查看我们的安全开发白皮书.最后，我们强烈建议您同时查看安全性强化检查清单，其中包含关于如何保护 Tableau Server 部署的其他建议。

总结

Tableau Server 提供了一组全面的安全性功能来满足您的部署需求。Tableau 既有无数客户站点上的面向公众的部署，又有安全网络中的内部部署。事实证明这些部署非常成功。Tableau 以现代行业标准为基准，能够对未来的威胁及问题作出快速反应。从行级别安全性到安全网站，包括二者之间的每个安全性细节，Tableau 认真考虑您的安全性问题，并将我们的解决方法直接构建到自己的平台中。

关于 Tableau

Tableau 帮助人们将数据转化为可以付诸行动、发挥重大作用的见解。轻松 连接到以任何形式存储在任意地点的数据。快速执行临时分析，发现隐藏的机会。通过拖放操作，创建包含高级可视化分析的交互式仪表板。然后在整个组织共享，让其他团队成员能够从自己的数据视角进行探索。
从全球性企业到早期初创企业和小企业，
使用 Tableau 的分析平台来查看和理解数据的人无处不在。

资源

Tableau Server 强化指南

Tableau Server 管理员指南

Tableau Server 高可用性：大规模提供任务关键型分析

Tableau Server 可扩展性 – 面向服务器管理员的技术部署指南