Tenable Identity Exposure 最佳实践指南

上次修订时间：2025 年 7 月 2 日

目录

欢迎使用 Tenable Identity Exposure 最佳实践指南

上次更新日期：七月 30, 2025

Tenable Identity Exposure 可对 Microsoft Active Directory (AD) 基础设施进行实时安全监控。Tenable 利用基于 AD 复制过程的非侵入式方法，让安全团队可以执行审核、威胁搜寻、检测和事件响应任务。

关于本指南

本指南可作为最佳实践的综合指南，旨在通过定制的指导、建议和行之有效的方法来提升用户体验。其中涵盖各种主题，包括部署前后的注意事项、升级前后的策略以及改善用户体验的最佳实践。

本指南基于《**Tenable Identity Exposure 本地用户指南**》，提供以下信息：

- 将 Tenable Identity Exposure 作为与 Internet 断开连接的本地平台进行部署和操作所需满足的技术要求。
- 网络和应用程序方面的环境规范。
- 启用安全监控之前要执行的任务。

为了成功部署平台，请遵循 开始使用 Tenable Identity Exposure 3.77 本地。

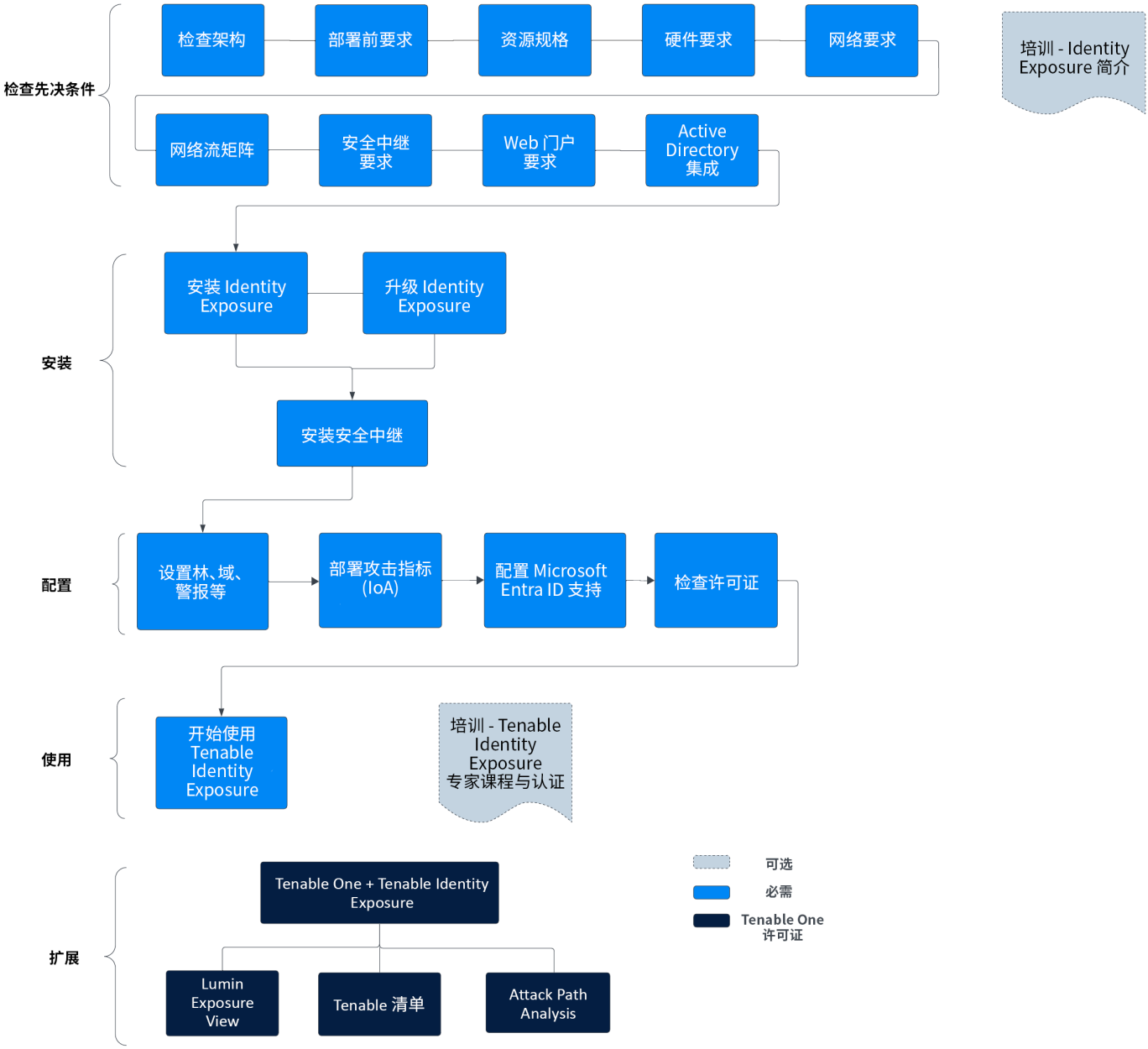
有关安装和升级的完整信息，请参阅适用于 3.42 或 3.59 的《Tenable Identity Exposure 本地安装指南》。

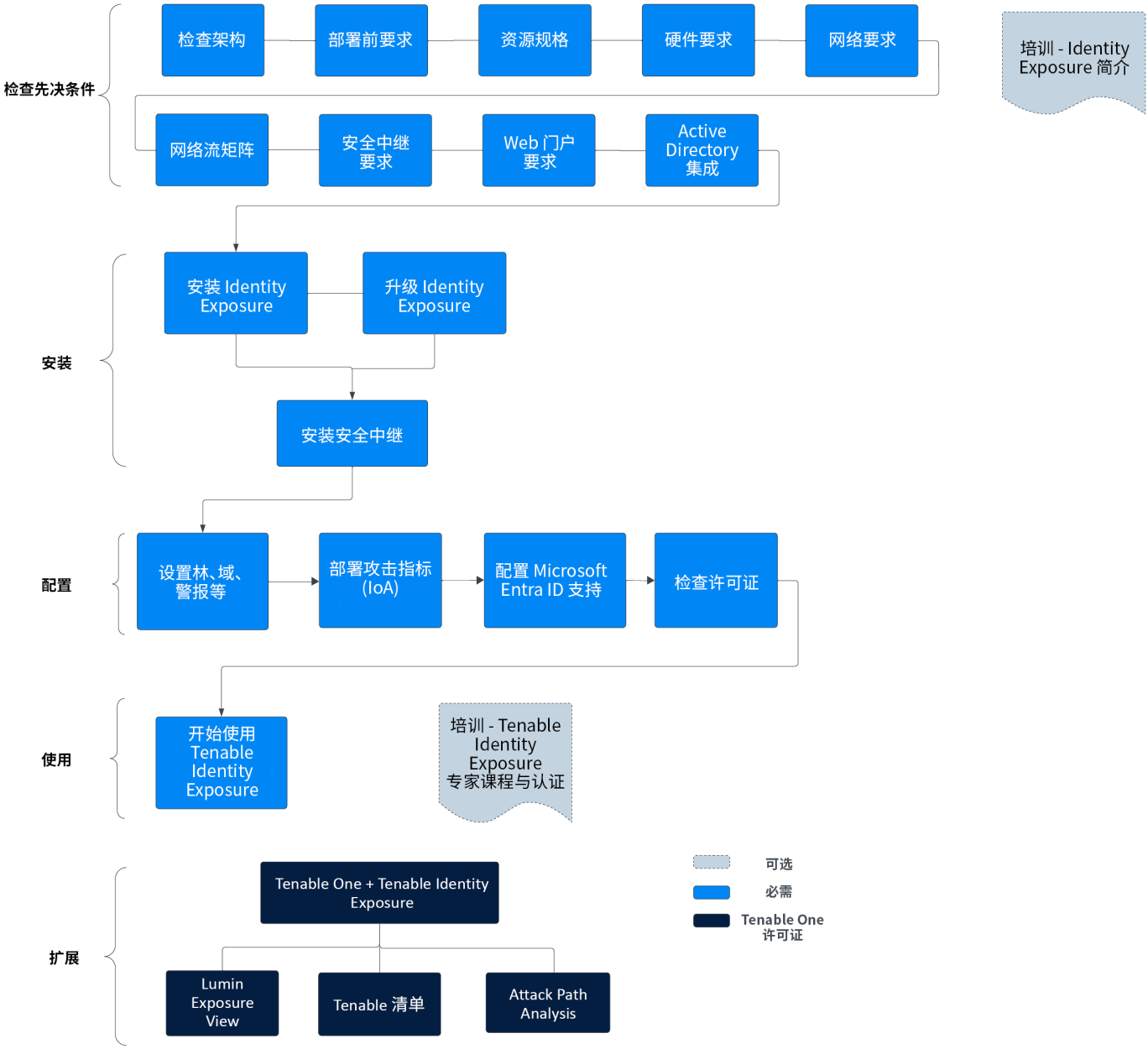
迁移

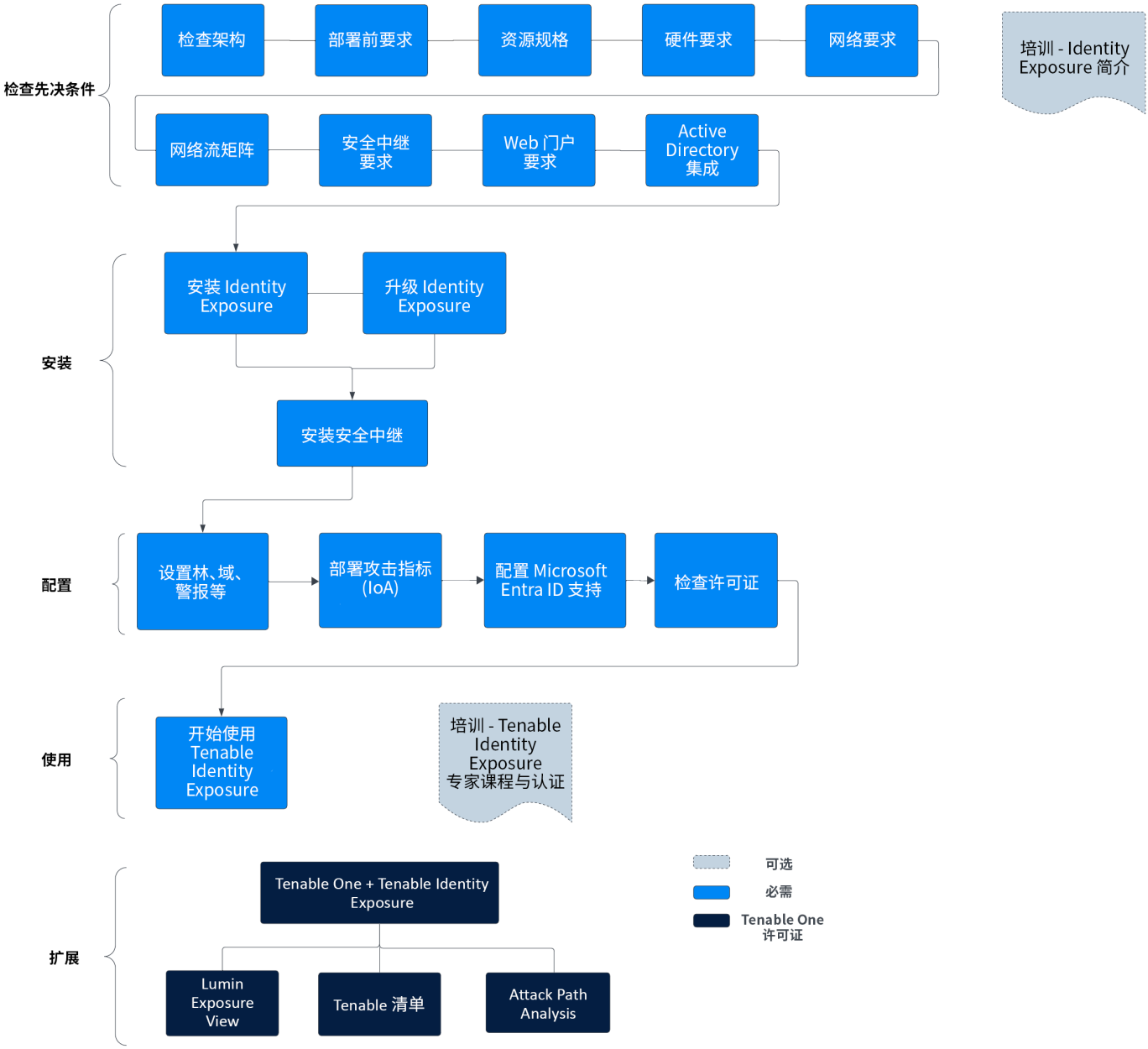
借助可轻松获取的 **Tenable 专业服务**，顺利完成迁移。我们会根据您的需求精心设计完美的解决方案，并确保您轻松完成从开始到结束的全过程。相信我们人性化的指导，尽享顺畅迁移体验。准备好获取专家指导了吗？立即拨打 Tenable 免费电话并获取报价。

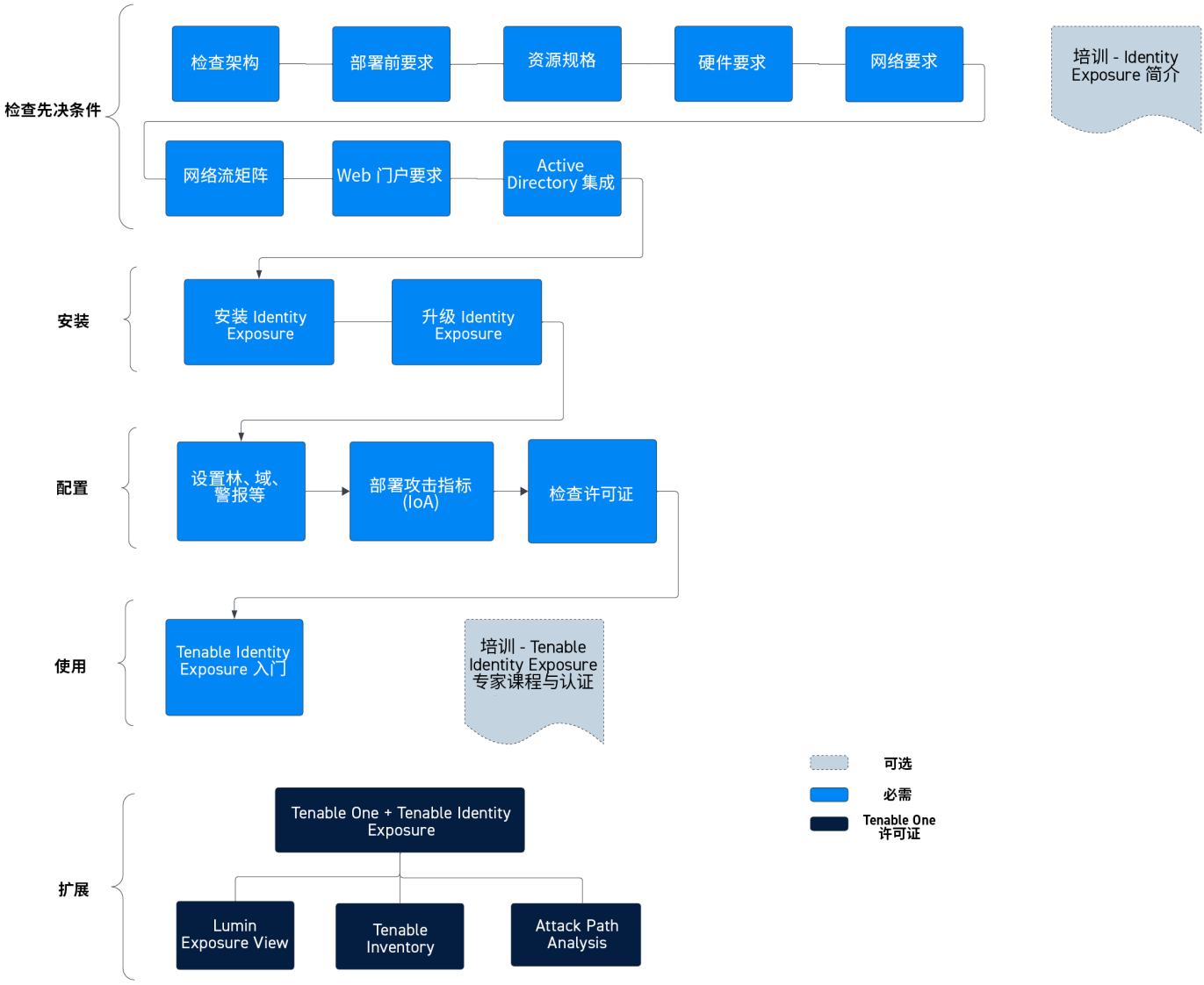
开始使用 Tenable Identity Exposure 3.77 本地

请使用以下工作流部署 Tenable Identity Exposure 3.77。


检查先决条件
检查架构
部署前要求
资源规格
硬件要求
网络要求
网络流矩阵
安全中继要求
Web 门户要求
Active Directory 集成
培训 - Identity Exposure 简介
安装
安装 Identity Exposure
升级 Identity Exposure
安装安全中继
配置
设置林、域、警报等
部署攻击指标 (IoA)
配置 Microsoft Entra ID 支持
检查许可证
使用
开始使用 Tenable Identity Exposure
培训 - Tenable Identity Exposure 专家课程与认证
扩展
Tenable One + Tenable Identity Exposure
Lumin Exposure View
Tenable 清单
Attack Path Analysis
可选
必需
Tenable One 许可证


检查先决条件
检查架构
部署前要求
资源规格
硬件要求
网络要求
网络流矩阵
安全中继要求
Web 门户要求
Active Directory 集成
培训 - Identity Exposure 简介
安装
安装 Identity Exposure
升级 Identity Exposure
安装安全中继
配置
设置林、域、警报等
部署攻击指标 (IoA)
配置 Microsoft Entra ID 支持
检查许可证
使用
开始使用 Tenable Identity Exposure
培训 - Tenable Identity Exposure 专家课程与认证
扩展
Tenable One + Tenable Identity Exposure
Lumin Exposure View
Tenable 清单
Attack Path Analysis
可选
必需
Tenable One 许可证


检查先决条件
检查架构
部署前要求
资源规格
硬件要求
网络要求
网络流矩阵
安全中继要求
Web 门户要求
Active Directory 集成
培训 - Identity Exposure 简介
安装
安装 Identity Exposure
升级 Identity Exposure
安装安全中继
配置
设置林、域、警报等
部署攻击指标 (IoA)
配置 Microsoft Entra ID 支持
检查许可证
使用
开始使用 Tenable Identity Exposure
培训 - Tenable Identity Exposure 专家课程与认证
扩展
Tenable One + Tenable Identity Exposure
Lumin Exposure View
Tenable 清单
Attack Path Analysis
可选
必需
Tenable One 许可证



检查先决条件

1. **查看**版本说明。
2. **选择**您的本地架构：根据您的特定需求，Tenable Identity Exposure 提供两种部署选项。
3. **检查**部署前要求：为获得最佳性能，您需要对 Tenable Identity Exposure 仔细进行资源规划，包括分析 Active Directory 环境（特别是对象的总数），以确定必要的内存和处理能力。

> **注意**：从 Tenable Identity Exposure **3.59.5** 版开始，请确保您的 **TLS 证书使用 OpenSSL 3.0.x**。

安装

1. **选择您的部署：**

   - 安装 Tenable Identity Exposure.
   - 升级 Tenable Identity Exposure.

     提示：如果您从 **v.3.42** 升级到 **3.77**，请务必查看 Secure Relay Requirements 和 本地平台的安全中继架构 这两部分。

2. **安装** 适用于 Tenable Identity Exposure 3.77 的安全中继。

配置

1. **部署后任务：**重新启动服务、故障排除日志、部署后任务。
2. **查看** Tenable Identity Exposure Licensing。

使用

- Start Using Tenable Identity Exposure

将 Tenable Identity Exposure 扩展为 Tenable One

注意：需要有 Tenable One 许可证才能执行此操作。有关更多试用 Tenable One 的信息，请参阅“Tenable One”。

将 Tenable Identity Exposure 与 Tenable One 集成并利用以下功能：

- 在 Lumin Exposure View 中，通过为关键业务服务、流程和功能获取与业务一致的网络风险暴露评分来获取关键业务环境，并根据 SLA 跟踪交付情况。跟踪总体身份风险，以了解 Web 应用程序对总体网络风险暴露评分的风险贡献。
  - 查看**全局**风险暴露卡，了解您的整体评分。单击**“每个风险暴露”**，了解影响评分的因素以及影响程度。
  - 查看 **Active Directory** 风险暴露卡。

- 配置风险暴露视图设置以设置自定义**卡片目标**，并根据公司策略配置**修复 SLA** 和 **SLA 效率**。
- 根据业务环境（例如域、域管理员、资产重要性、关键用户/关键资产或服务帐户）创建自定义风险暴露卡。

- 在 Tenable Inventory 中，通过深入分析资产信息（包括相关攻击路径、标签、风险暴露卡、用户、关系等）增强资产情报。借助可评估总资产风险和资产对身份重要性的资产风险暴露评分，更全面地了解资产风险暴露情况，进而改善风险评分。
  - 检查 AD 资产，了解接口的战略性质。这应有助于您决定在 Tenable Inventory 中要使用哪些功能以及何时使用这些功能。
  - 查看您可以使用和编辑的 **Tenable 查询**，并为其添加书签。
  - 熟悉全局搜索查询生成器及其对象和属性。为自定义查询添加书签以供日后使用。

    提示：快速查看可用属性的步骤如下：
    - 在查询生成器中，输入“*has*”。此时会出现建议资产属性的列表。
    - 通过添加列来自定义列表。此时会出现可用的列/属性列表。
  - 深入了解“资产详细信息”页面以查看资产属性和所有关联的上下文视图。
  - （可选）创建标签，结合不同资产类别。
- 在 Attack Path Analysis 中，通过暴露遍历攻击面的风险攻击路径（包括 Web 应用、IT、OT、IoT、身份、ASM）来优化风险优先级，并防止引起重大影响。通过识别汇合点来中断攻击路径并提供缓解指导，从而简化缓解措施，并通过 AI 见解获得深入的专业知识。
  - 查看**“Attack Path Analysis”仪表盘**，获取易受攻击资产的概览视图，例如通向这些关键资产的攻击路径的数量、未解决的结果的数量及其严重性、一个矩阵，用于查看具有不同源节点风险暴露评分和 ACR 目标值组合的路径，以及趋势攻击路径列表。
    - 查看**主要攻击路径矩阵**，然后单击“**主要攻击路径**”磁贴，查看更多有关通向“核心资产”或域管理员的路径信息。

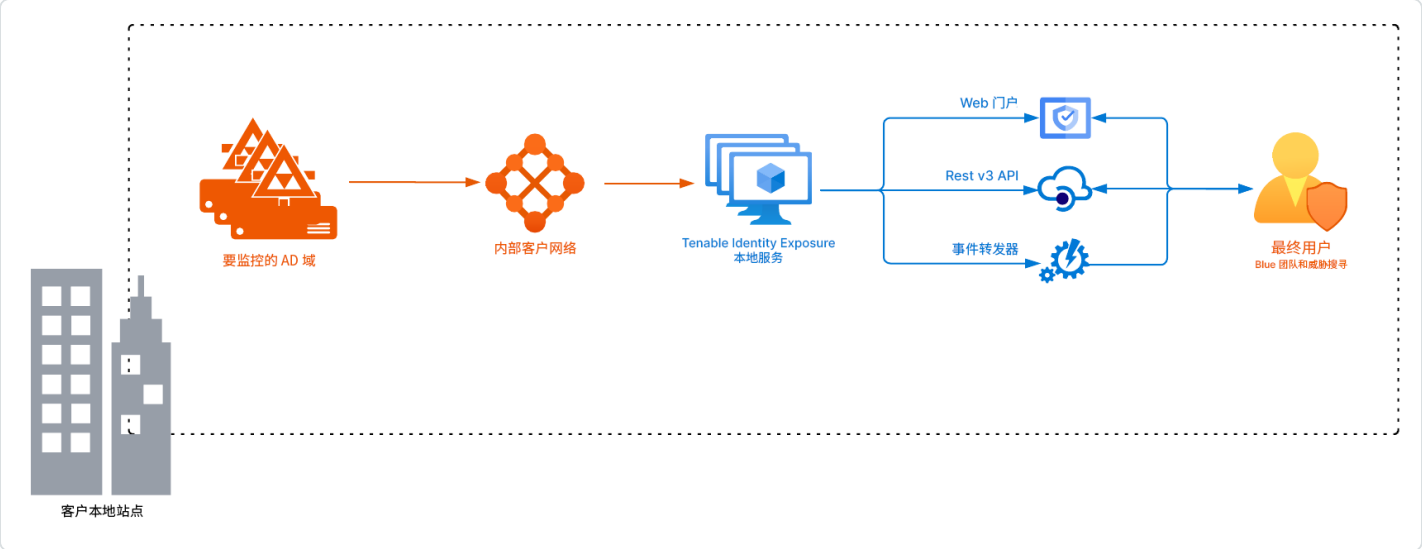
如有需要，您可以调整这些设置，以确保查看最关键的攻击路径数据和结果。

- 在“**结果**”页面上，通过将数据与高级图形分析和 MITRE ATT&CK® 框架相结合，查看所有存在于一条或多条通往一个或多个关键资产的攻击路径中的攻击技术，从而生成“结果”，这使您能够理解和应对那些导致并加剧对资产和信息威胁影响的未知因素。
- 在“**发现**”页面上，生成攻击路径查询，以查看作为潜在攻击路径一部分的资产：
  - 使用内置查询生成攻击路径
  - 使用资产查询生成器生成资产查询
  - 使用攻击路径查询生成器生成攻击路径查询

  然后，您可以通过查询结果列表和交互图，查看攻击路径查询和资产查询数据，并与之交互。

本地架构

Tenable Identity Exposure 平台依赖虚拟机 (VM) 上托管的多项 Windows 服务。您的环境必须支持以下基础设施：



Tenable Identity Exposure 平台由以下组件组成：

- **存储管理器**：存储管理器不仅提供热存储和冷存储支持，还能监控目录侦听器和安全引擎节点的服务数据。此组件是唯一必须持久保存信息的组件。在内部，它们使用 Microsoft MS SQL 服务器存储内部数据和配置。
- **安全引擎节点**：通过托管分析相关的服务，安全引擎节点可以为 Tenable Identity Exposure 安全引擎、内部通信总线和最终用户应用程序（如 Web 门户、REST API 或警报通知程序）提供支持。此组件基于被隔离的不同 Windows 服务构建而来。
- **目录侦听器**：通过与受监控的域控制器密切配合，目录侦听器可以接收实时 Active Directory 流并应用多种处理方法来解码、隔离和关联安全更改。
- **安全中继**：使用传输层安全 (TLS) 而非 VPN 将 Active Directory 数据从网络传输到 Tenable Identity Exposure 的模式。如果您的网络需要代理服务器才能访问互联网，中继功能也支持有身份验证或无身份验证的 HTTP 代理。Tenable Identity Exposure 可以支持多种安全中继，您可以根据需要将其映射到域。请参阅本地平台的安全中继架构。

对于这些组件的数量和规格，请参阅“资源规格”。

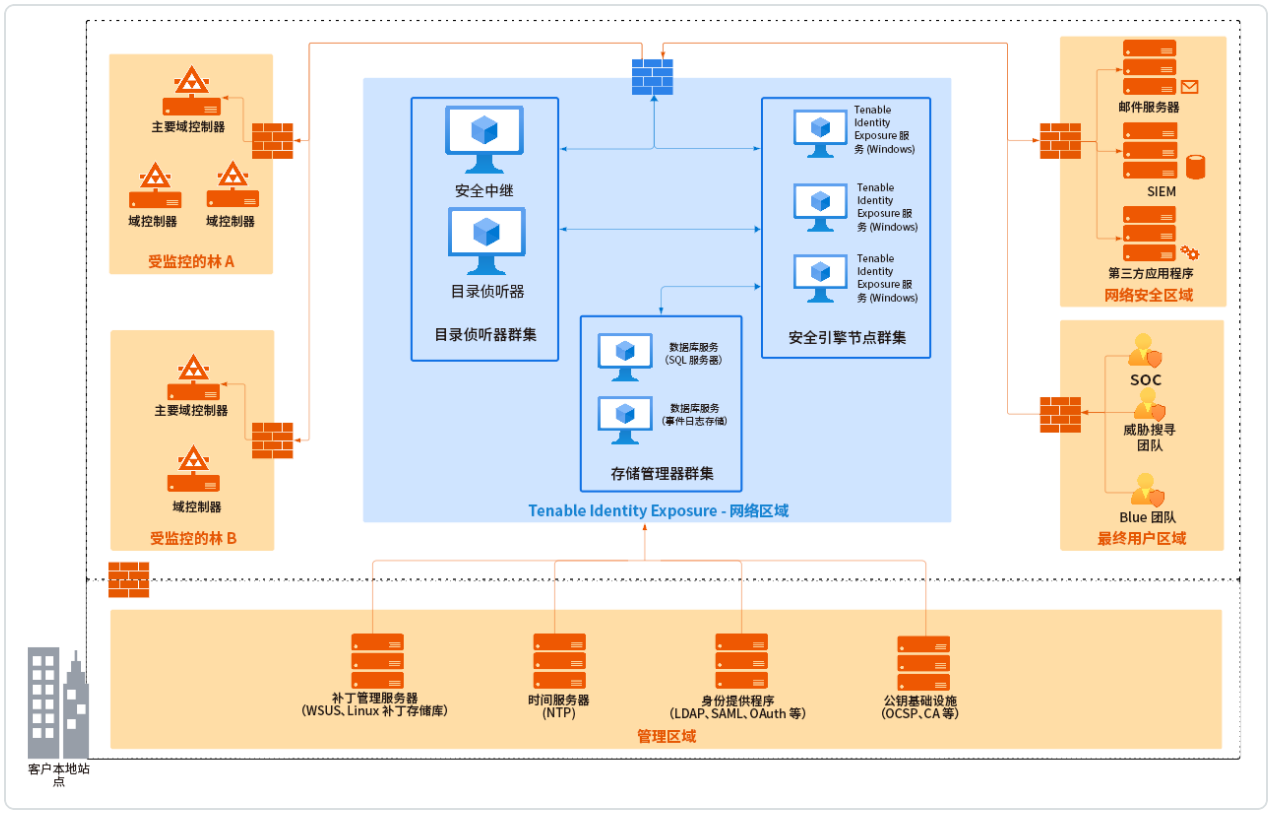
架构

Tenable Identity Exposure 的本地解决方案使用托管在您提供和管理的专用 Windows Server 环境中的软件包，基于以下架构：

集中式架构

集中式架构在同一网络区域中托管所有 Tenable Identity Exposure 组件。

- 主要组件（安全中继、目录侦听器、安全引擎节点和存储管理器）在未经任何网络筛选的情况下并行工作，并且相互通信。
- 为确保适当的网络安全，Tenable 建议您在区域入口设置防火墙，以保护此架构。下图显示了“网络流矩阵”中所述的传入和传出网络流。



优点：此架构可在可管理性与安全性之间达到最佳平衡：

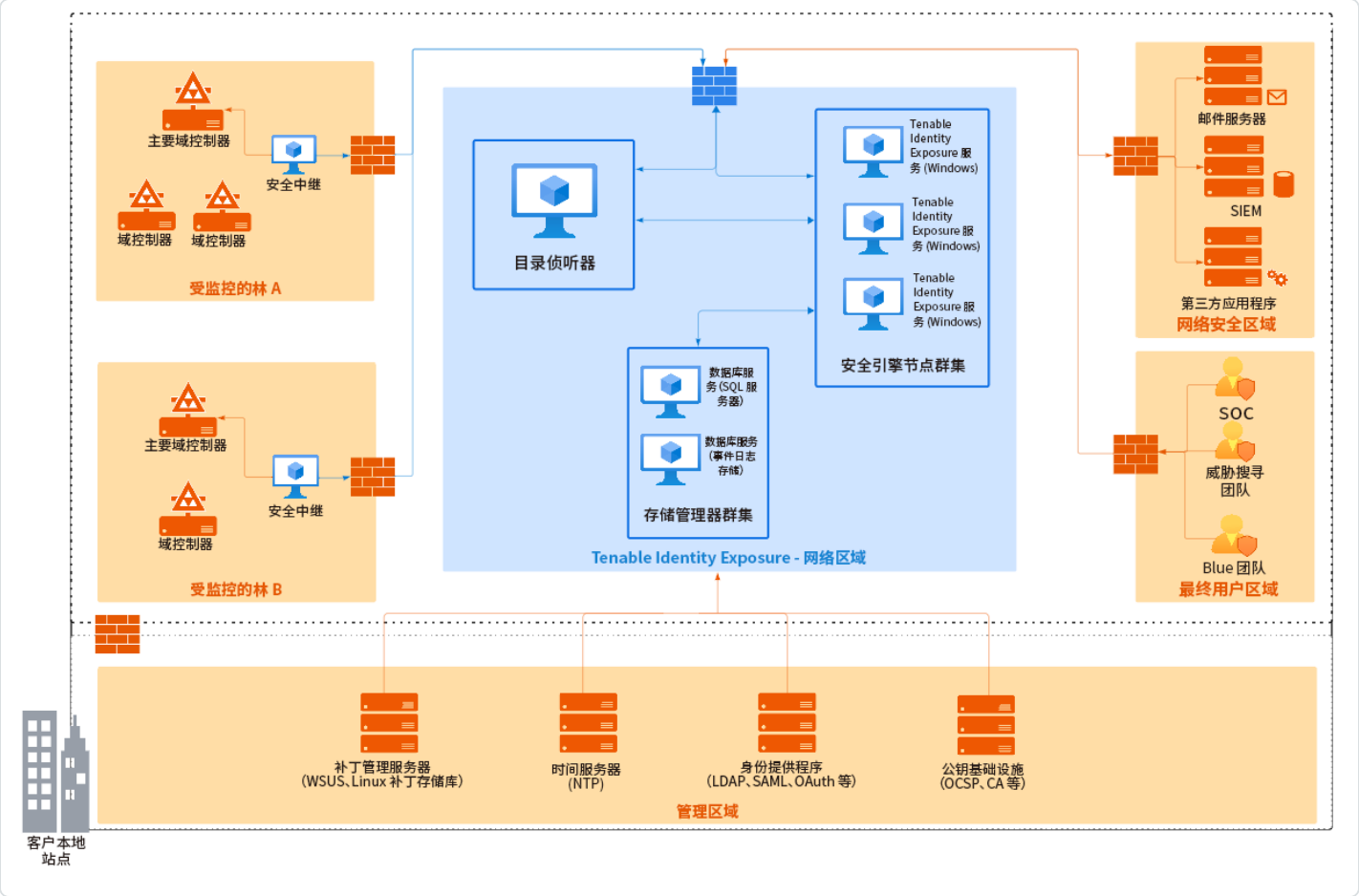
- 每个 Tenable Identity Exposure 服务都位于唯一防火墙后面的同一逻辑位置。
- 每个服务流（Active Directory、最终用户、警报等）都经过相同的网络设备。
- 由于无需在目标域中使用服务或进行额外配置，此架构可轻松关联新的 Active Directory 域。

缺点:集中式架构会消耗带宽,因为它必须将每个 Active Directory 流从受监控的域控制器传输到 Tenable Identity Exposure 网络区域。

> **提示**:Tenable 建议使用集中式架构,因为灵活性更好且部署更轻松。

分布式架构

分布式架构将目录侦听器放置在域控制器所在的网络区域中,并在另一个网络区域中托管安全引擎节点和存储管理器,如下图所示:



优点

- 带宽减少:监控大型目录时,Active Directory 流可能会很大。通过筛选相关的安全更改并压缩对象,目录侦听器可以减少平台的带宽用量。
- 优化网络筛选:

- Active Directory 基础设施需要使用大量的 TCP 和 UDP 端口，但这些端口可能成为网络攻击的目标。根据最小特权原则，Tenable 建议您仅在绝对必要时才公开这些网络端口。
- 通过将目录侦听器放置在域控制器所在的网络区域中，Tenable Identity Exposure 便无需向其他网络区域公开 Active Directory 端口。

- 被隔离的基础设施：在特定上下文中，有时需要将 Active Directory 基础设施与信息系统的其余部分完全隔离。使用分布式架构，Tenable Identity Exposure 的平台仅需要使用一个入站和一个出站网络流，从而保证被隔离基础设施的安全。
- 网络安全：Tenable Identity Exposure 的目录侦听器使用基于主机的特定防火墙。Tenable 还建议您在托管安全引擎节点和存储管理器的区域的入口使用特定防火墙。有关入站和出站网络流的更多信息，请参阅“网络流矩阵”。

缺点：Tenable 建议仅将此架构用于需要高级网络隔离的高度敏感环境。

- 分布式架构的部署和维护流程更为复杂，因为需要在不同网络位置进行多种网络配置。
- 此架构的灵活性也更低，因为每次客户希望添加要监控的新域时，都需要部署新的目录侦听器。

部署前要求

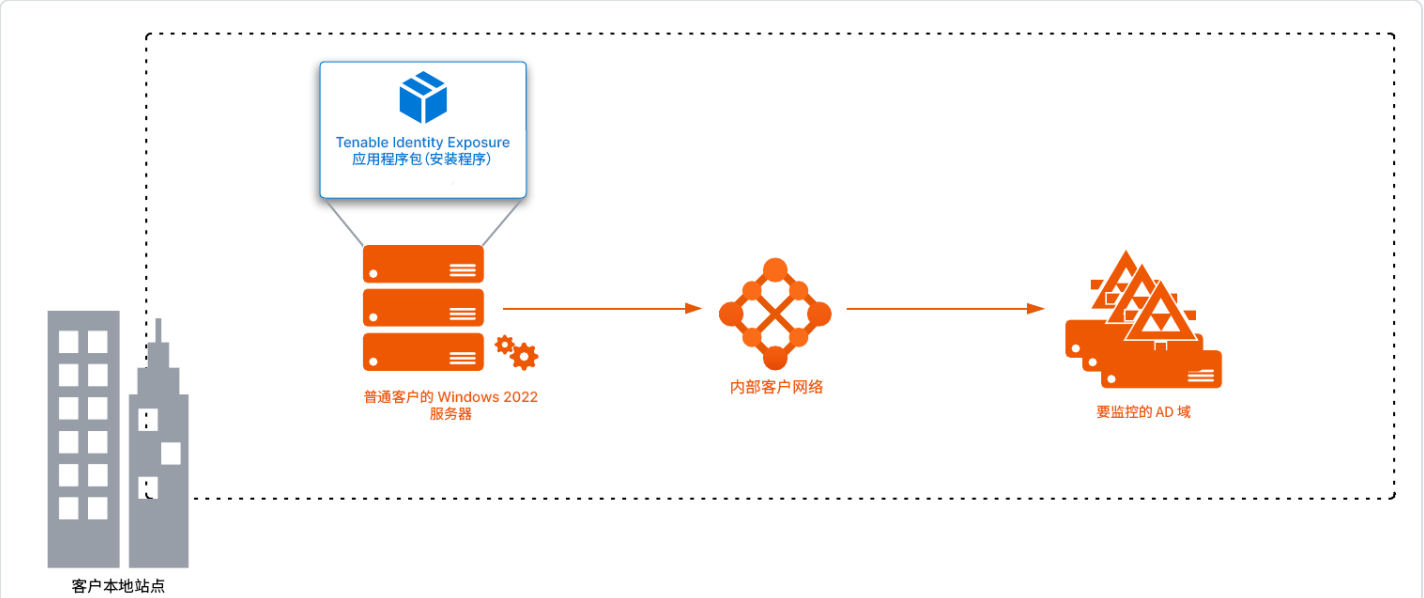
开始之前，请检查是否满足以下先决条件，以确保安装过程顺利进行。

安装概述

您可以将 Tenable Identity Exposure 作为应用程序包安装在专用的 Windows 环境中，该环境必须满足特定的托管规范。Tenable Identity Exposure需要在安装了它的操作系统上访问操作系统的主映像。

Tenable 会预先配置应用程序包，其中仅包含 Tenable 服务和您的特定要求。此部署选项可提供最大的灵活性，并顺畅集成到您的特定环境中。

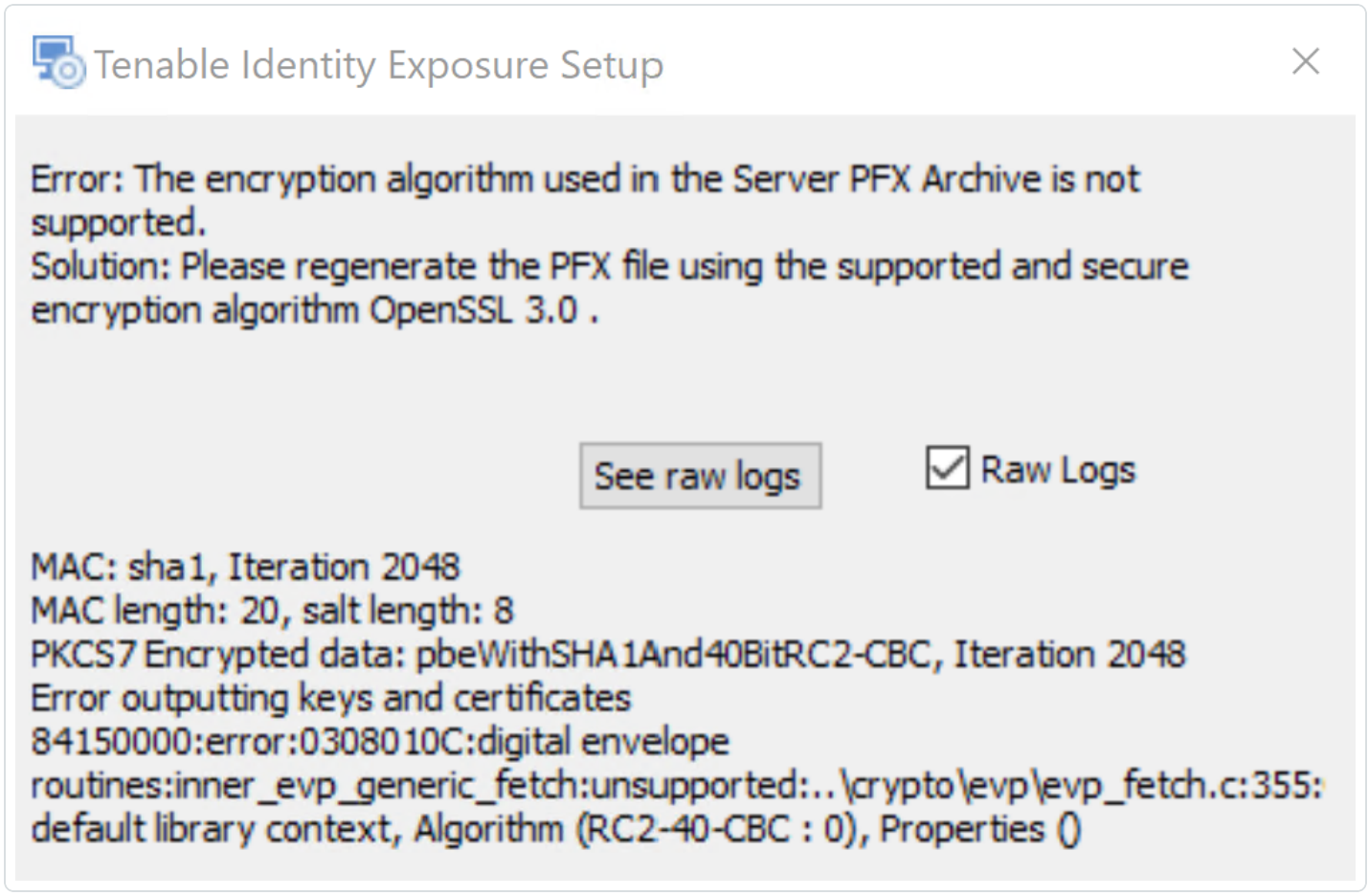
Tenable Identity Exposure 在嵌入到 Windows 服务中的微服务架构上运行。这些服务有专用用途(存储、安全分析、应用程序等)，均为强制性服务。因此，您只能在支持微服务模型的操作系统上安装 Tenable Identity Exposure。

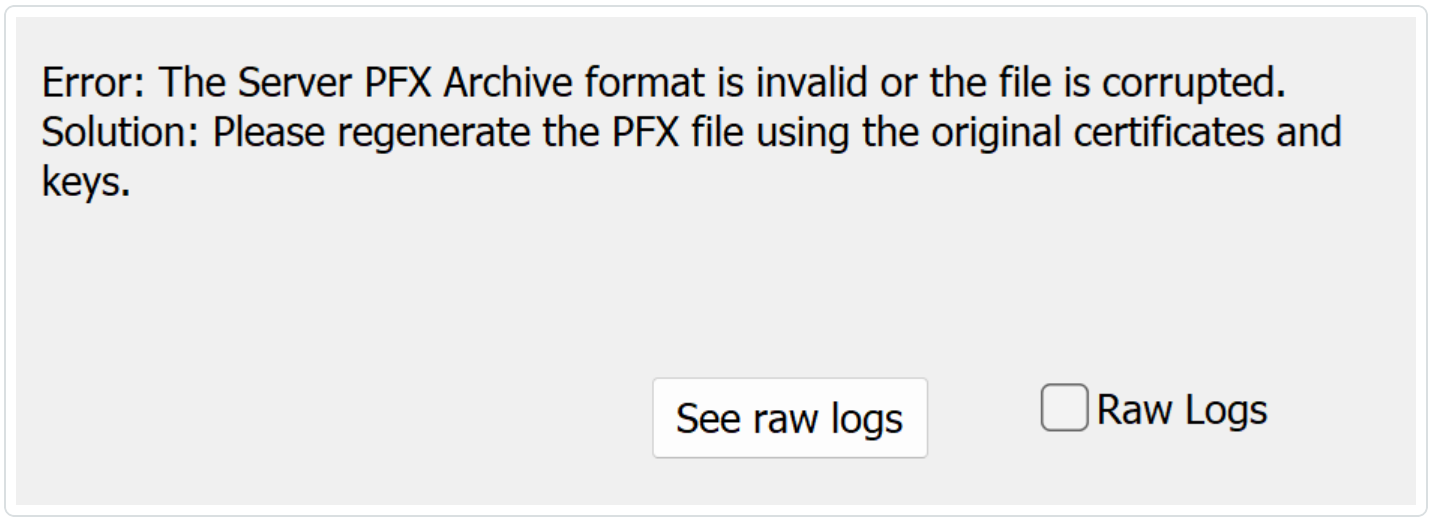


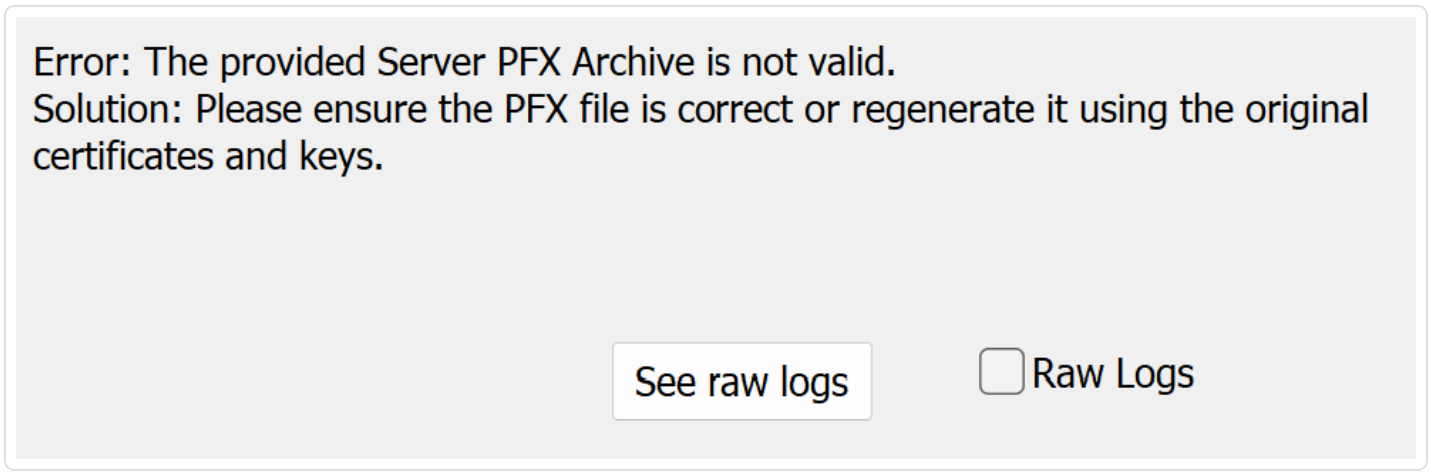
TLS 证书

OpenSSL 3.0 支持 - 从 **3.59.5** 版开始，Tenable Identity Exposure 使用 **OpenSSL 3.0.x**。因此，以 SHA1 签名的 X.509 证书在第 1 级或更高的安全级别下不再有效。TLS 默认为第 1 级的安全级别，这使 SHA1 签名的证书不受信任，无法对服务器或客户端进行身份验证。

您必须升级证书以响应此变更。如果继续安装而不将证书更新为使用 OpenSSL 3.0，则 Tenable Identity Exposure 安装程序会返回以下错误消息和建议的补丁：







帐户特权

以本地或内置管理员组的本地帐户成员身份，或以安装有 Tenable Identity Exposure 的服务器上的管理员身份执行安装。

注意：使用**域外的本地管理员帐户**登录计算机。**请勿以域内本地管理员的身份登录**。

帐户需要拥有以下权限：

- `SeBackupPrivilege`
- `SeDebugPrivilege`
- `SeSecurityPrivilege`

杀毒软件 (AV) 与端点检测和响应 (EDR)

安装之前，禁用主机上的任何 AV 和/或 EDR 解决方案。不这样做会在安装期间触发回滚。安装完成后，您可以安全启用 AV/EDR；但请注意，由于频繁的磁盘 I/O 操作，这可能会影响产品性能。

待重新启动

在安装之前，执行任何所需的重新启动。在服务器上启动安装程序时，请检查以下内容：

- 系统未处于待重新启动状态。
- 服务器在不到 11 分钟前已正确重新启动。

- MSI 会检查以下注册表键：
  - `HKLM: \ Software \ Microsoft \ Windows \ CurrentVersion \ Component Based Servicing \ RebootPending`
  - `HKLM: \SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ WindowsUpdate \ Auto Update \ RebootRequired`
  - `HKLM: \SYSTEM \ CurrentControlSet \ Control \Session Manager -> PendingFileRenameOperations`

服务帐户

必须允许在操作系统上使用服务帐户。

注意：此服务帐户必须能够读取所有对象属性。

攻击指标

Windows 事件日志的最短保留时间必须为 5 分钟，以确保应用程序可以准确检索所有事件。

不支持的配置

下表详细说明了不支持的配置：

配置	描述
主动杀毒软件或端点检测和响应 (EDR) 解决方案	Tenable Identity Exposure 平台需要容纳大量磁盘 I/O。 • 使用杀毒软件和 EDR 会大大降低平台性能。 • 您必须在出现例外情况才能允许使用 Tenable Identity Exposure 服务和数据文件夹。
防火墙	执行以下操作，允许 Tenable Identity Exposure 服务相互通信以进行可靠的安全监控： • 禁用阻止流量传出的本地防火墙规则。 • 制定本地防火墙规则，允许 Tenable Identity Exposure 服务的流量传入。

Erlang	• 请勿自定义 HOMEDRIVE 环境变量。 • PATHEXT 环境变量必须包含 .exe 和 .bat 文件扩展名。

第三方应用程序

在未经认证的环境中部署 Tenable Identity Exposure 的平台会造成意外负面影响。

特别是，在主映像中部署第三方应用程序(如特定代理或后台程序)会导致稳定性或性能问题。

Tenable 强烈建议您尽可能减少第三方应用程序的数量。

访问权限

Tenable Identity Exposure 的平台需要有本地管理权限才能操作，并确保进行适当的服务管理。

- 您必须为 Tenable 技术负责人提供与主机管理帐户关联的凭据(用户名和密码)。
- 部署到生产环境时，请考虑由您与 Tenable 技术负责人共同验证密码更新流程。

产品更新

作为升级计划的一部分，Tenable 会经常发布系统更新，以提供新的检测功能和新的产品功能。

- 在此项部署中，Tenable 仅提供 Tenable Identity Exposure 组件的更新。您必须确保正确管理操作系统，包括频繁部署安全补丁。有关 Tenable Identity Exposure 版本的更多信息，请参阅“Tenable Identity Exposure 版本说明”。
- Tenable Identity Exposure 的微服务架构支持立即应用操作系统补丁。

其他要求

- Tenable Identity Exposure 与 硬件要求 中列出的包含最新可用更新的 Windows Server 兼容。

- Tenable Identity Exposure 安装程序要求**在 Windows Server 2016 或更高版本上拥有本地管理员权限**。如果用于安装的帐户为默认帐户，请确保此帐户运行程序可以不受限制。
- Tenable Identity Exposure 服务需要有本地管理员权限才能在计算机上运行本地服务。
- Tenable Identity Exposure 需要有专用的数据分区。请勿在 OS 分区上运行 Tenable Identity Exposure，以免在分区已满的情况下发生系统冻结。
- Tenable Identity Exposure SQL 实例要求具备虚拟帐户使用情况功能。
- 如果在实施更严格的安全措施后安装或升级 Microsoft SQL 服务器，安装过程会因用户权限不足而失败。检查您是否有必要的权限来确保成功安装。有关更多信息，请参阅“Microsoft 文档”。
- Tenable Identity Exposure 必须作为黑盒运行。将每台计算机专用于 Tenable Identity Exposure 且不与其他产品共享。
- Tenable Identity Exposure 可在数据分区上创建任何以“Alsid”或“Tenable”前缀开头的文件夹。因此，请勿在数据分区上创建以“Alsid”或“'Tenable”开头的文件夹。
- Erlang：请勿修改 `HOMEDRIVE` 环境变量。`PATHEXT` 环境变量必须包含 `.exe` 和 `.bat` 文件扩展名。
- 如果您必须将 Tenable Identity Exposure 的 AD 服务帐户设置为受保护用户组成员，请确保您的 Tenable Identity Exposure 配置支持 Kerberos 身份验证，因为受保护用户无法使用 NTLM 身份验证。

预安装清单

此表以便捷清单的形式概述了安装的先决条件。

要保留的信息或资源	状态
必要的协议（NDA、评估软件许可证）（如果适用）。	
目标域中要监控的活跃 AD 用户的数量。	
计算和内存资源基于 Tenable Identity Exposure 的规格矩阵。请参阅资源规格。	
每个虚拟机的私有 IP，用于部署 Tenable 平台。	
更新管理基础设施、时间服务器、PKI 服务器和身份提供程序的类型和 IP 地址。	

为 Tenable Identity Exposure 需要的每项服务打开所需的网络流。请参阅网络流矩阵。	
每个主域控制器仿真器的私有 IP 地址。	
在每个 Active Directory 林上创建要监控的常规用户帐户。	
在特定 Active Directory 容器中，授予对 Tenable 服务帐户的访问权限。	
如果您要启用此功能，请授予特权分析使用权限。	
使用 AD 域用户帐户登录： • 格式：用户主体名称，例如“tenablead@domain.example.com”（出于 Kerberos 兼容性原因而推荐）；或者 NetBIOS，例如“DomainNetBIOSName\SamAccountName”。	
利用客户的 PKI 为 Tenable Identity Exposure 的 Web 门户颁发的 TLS 证书 • 否则，请通知 Tenable 使用自签名证书。	
要创建的 Tenable Identity Exposure 用户帐户列表： • 必填信息：名字和姓氏、电子邮件地址以及所需的登录信息。	
要激活的可选配置列表（电子邮件通知、Syslog 事件转发等）	
已确定且有空的项目协调员需要与 Tenable 员工开展合作。	
技术人员负责解决潜在的技术问题，例如网络筛选问题和无法访问 PDCe。	

另请参阅：

- 资源规格
- 硬件要求
- 网络要求
- Web 门户要求
- 与 Active Directory 域集成

资源规格

Tenable Identity Exposure 组件(**存储管理器**、**安全引擎节点**、**安全中继**和**目录侦听器**)需要拥有一定的内存量和计算能力才能正常运行。

- 这些所需的资源因您监控的 Active Directory (AD) 基础设施的大小而异。
- Tenable Identity Exposure 使用活跃用户数作为计算规格要求的指标,其中包括应用程序使用的常规用户帐户和服务帐户。

计算 AD 量:

- 在每个要监控的 Active Directory 域上运行以下 PowerShell 命令行:

```
Import-Module ActiveDirectory
(Get-ADUser -Server "dc.domain.com" -Filter 'enabled -eq $true').Count
```

其中:

- `-Server` 指定要连接的 Active Directory 域服务 (ADDS) 实例。
- `dc.domain.com` 指要用于计数的域控制器的完全限定域名 (FQDN)。

规格要求

计算要监控的活跃用户数后,请参阅以下部分以了解相应的规格要求:

- **安全中继**是一种将 Active Directory 数据从网络传输到 Tenable Identity Exposure 的模式。

托管安全中继的系统所需满足的规格要求:

客户规模	Tenable Identity Exposure 服务	需要的实例	vCPU (每个实例)	内存 (每个实例)	可用磁盘空间 (每个实例)	磁盘拓扑
任意尺寸	• `tenable_Relay` • `tenable_envoy`	1	2 个 vCPU	8 GB RAM	30 GB	独立于系统分区的

						日志分区

- **目录侦听器**接收实时 Active Directory 流。

托管目录侦听器组件的系统所需满足的规格要求：

目录侦听器				
活跃 AD 用户	需要的实例	vCPU（每个实例）	内存（每个实例）	磁盘空间（每个实例）
1 - 25,000	1 台虚拟机	2 核，2 个插槽	16 GB RAM	30 GB（银）
25,001 - 50,000	1 台虚拟机	4 核，2 个插槽	16 GB RAM	30 GB（银）
50,001 - 75,000	1 台虚拟机	4 核，2 个插槽	32 GB RAM	30 GB（银）
75,001 - 100,000	1 台虚拟机	4 核，2 个插槽	32 GB RAM	30 GB（银）
100,001 - 150,000	1 台虚拟机	8 核，2 个插槽	64 GB RAM	30 GB（银）
150,001 - 300,000	1 台虚拟机	8 核，2 个插槽	64 GB RAM	30 GB（银）
300,001 - 500,001+	1 台虚拟机	8 核，2 个插槽	64 GB RAM	30 GB（银）

- **安全引擎节点**为 Tenable Identity Exposure 的安全引擎、存储服务和最终用户提供支持。

> **注意**：如果将 SEN 服务分布在多台计算机上，请参阅“Split Security Engine Node (SEN) Services”以了解详细的资源大小调整。

托管安全引擎节点组件的系统所需满足的规格要求：

安全引擎节点				
活跃 AD 用户	需要的实例	vCPU（每个实例）	内存（每个实例）	磁盘空间（每个实例）
1 - 25,000	1 台虚拟机	8 核，2 个插槽	16 GB RAM	200 GB（金）
25,001 - 50,000	1 台虚拟	8 核，2 个插槽	32 GB RAM	300 GB（金）

	机			
50,001 - 75,000	1 台虚拟机	10 核 , 3 个插槽	32 GB RAM	300 GB(金)
75,001 - 100,000	1 台虚拟机	12 核 , 4 个插槽	64 GB RAM	400 GB(金)
100,001 - 150,000	1 台虚拟机	16 核 , 4 个插槽	96 GB RAM	400 GB(金)
拆分安全引擎节点				
150,001 - 300,000	5 台虚拟机	VM1:8 核 , 2 个插槽	VM1:16 GB RAM	VM1:1 TB
		VM2:8 核 , 4 个插槽	VM2:16 GB RAM	VM2:300 GB
		VM3:16 核 , 4 个插槽	VM3:32 GB RAM	VM3:100 GB
		VM4:16 核 , 4 个插槽	VM4:16 GB RAM	VM4:100 GB
		VM5:16 核 , 4 个插槽	VM5:48 GB RAM	VM5:100 GB
300,001 - 500,001+	5 台虚拟机	VM1:8 核 , 2 个插槽	VM1:16 GB RAM	VM1:1 TB
		VM2:8 核 , 4 个插槽	VM2:16 GB RAM	VM2:300 GB
		VM3:12 核 , 4 个插槽	VM3:32 GB RAM	VM3:100 GB
		VM4:16 核 , 4 个插槽	VM4:32 GB RAM	VM4:100 GB

		VM5：16 核，4 个插槽	VM5：64 GB RAM	VM5：100 GB

- **存储管理器**可为目录侦听器和安全节点服务提供热存储和冷存储支持。

托管存储管理器组件的系统所需满足的规格要求：

存储管理器				
活跃 AD 用户	需要的实例	vCPU（每个实例）	内存（每个实例）	磁盘空间（每个实例）
1 - 25,000	1 台虚拟机	8 核，2 个插槽	16 GB RAM	600 GB
25,001 - 50,000	1 台虚拟机	8 核，2 个插槽	16 GB RAM	800 GB
50,001 - 75,000	1 台虚拟机	12 核，4 个插槽	32 GB RAM	1.2 TB
75,001 - 100,000	1 台虚拟机	12 核，4 个插槽	32 GB RAM	2 TB
100,001 - 150,000	1 台虚拟机	12 核，4 个插槽	64 GB RAM	4 TB
150,001 - 300,000	1 台虚拟机	16 核，4 个插槽	64 GB RAM	6 TB
300,001 - 500,001+	1 台虚拟机	16 核，4 个插槽	128 GB RAM	8 TB

有关磁盘性能的信息，请参阅“存储管理器磁盘要求”。

存储策略管理

基于性能、可靠性和成本，存储服务可划分为三个不同的层级或级别：金、银和铜。定义可能因提供商而异。

- 金为最高层级，有着最佳性能和可靠性，适用于关键工作负载。
- 银是一个在性能和成本之间取得平衡的中端选项。
- 铜为较低层级，性能和可靠性较低，通常用于不太重要的工作负载。

规格示例

由三个 Active Directory 域组成的信息系统的规格如下。

域	活跃 AD 用户数
域 A	45,000
域 B	15,000
域 C	150
总计：	**60,150**

根据规格矩阵，此项 Tenable Identity Exposure 部署所需的资源如下。

Tenable Identity Exposure 服务	需要的实例	vCPU（每个实例）	内存（每个实例）	磁盘空间（每个实例）
目录侦听器	1	4 核，至少 2.6 GHz	32 GB RAM	30 GB
安全引擎节点	1	10 核，至少 2.6 GHz	32 GB RAM	300 GB
存储管理器	1	12 核，至少 2.6 GHz	32 GB RAM	• 1.2 TB（10,000 IOP） • 要升级：至少需要 20 GB 的可用空间

存储管理器磁盘要求

作为安全分析的一部分，Tenable Identity Exposure 会通过 AD 数据库或 SYSVOL 网络共享存储每项 Active Directory (AD) 变更的差异。

存储管理器组件使用以下内容来监控这些事件的存储情况：

- 攻击相关事件的事件日志存储
- 所有其他事件的 Microsoft SQL 服务器实例

Tenable 根据 Active Directory 活动提供最低和建议的硬件要求：

- 最低的规格配置，可满足在大多数基础设施中启动和运行平台的需求。
- 建议的规格配置，可满足大多数事件密集型 AD 基础设施的需求。

Tenable Identity Exposure 也需要实施特定的磁盘布局，以存储不同的数据库文件并确保 I/O 性能与其活动兼容。

鉴于所处理的 Active Directory 数据量，Tenable Identity Exposure 属于磁盘密集型应用程序。为避免存储（磁盘或 SAN）带来任何瓶颈问题，Tenable Identity Exposure 提供了最低配置和建议配置。

- 与规格一样，最低磁盘性能通常可以满足大多数基础设施的需求。
- 建议的基础设施可提供更好的大型或活动 AD 基础设施使用体验。

支持和建议的磁盘布局

某些特定环境要求拆分不同磁盘上的数据库文件：

- 一个数据文件磁盘
- 一个临时数据库磁盘
- 一个日志文件磁盘
- （可选）1 个备份磁盘

最小和建议的磁盘规格

下表介绍了在 Tenable Identity Exposure 中存储 6 个月的 Active Directory 事件所需满足的最小和建议磁盘规格要求。

存储管理器：磁盘规格矩阵				
活跃 AD 用户	磁盘空间（每个	数据文件磁盘空间	日志文件磁盘空间	临时数据库磁盘空间

实例)		最小值	建议值	最小值	建议值	最小值	建议值
1 - 25,000	600 GB	340 GB	375 GB	100 GB	200 GB	10 GB	25 GB
25,001 - 50,000	800 GB	400 GB	500 GB	125 GB	250 GB	25 GB	50 GB
50,001 - 75,000	1.2 TB	600 GB	775 GB	150 GB	350 GB	50 GB	75 GB
75,001 - 100,000	2 TB	725 GB	1.3 TB	200 GB	600 GB	75 GB	100 GB
100,001 - 150,000	4 TB	1.6 TB	3 TB	300 GB	800 GB	100 GB	200 GB
150,001 - 300,000	6 TB	2.45 TB	4.7 TB	400 GB	1 TB	150 GB	300 GB
300,001 - 500,001+	8 TB	3.3 TB	6.4 TB	500 GB	1.2 TB	200 GB	400 GB

最低和建议磁盘性能

数据库的限制因素通常是基础磁盘性能。磁盘吞吐量/IOPS 越大，Tenable Identity Exposure 的整体性能就越好。低延迟也是必要条件 (< 5 ms)。

存储管理器：磁盘性能矩阵				
活跃 AD 用户	最低磁盘性能		建议磁盘性能	
	吞吐量 (MB/sec)	IOP(读取/写入)	吞吐量 (MB/sec)	IOP(读取/写入)
1 - 25,000	150	2,500	300	5,000
25,001 - 50,000	200	5,000	400	10,000
50,001 - 75,000	200	5,000	400	10,000

75,001 - 100,000	200	5,000	400	10,000
100,001 - 150,000	250	7,500	500	15,000
150,001 - 300,000	250	7,500	500	15,000
300,001 - 500,001+	500	16,000	1,000	32,000

硬件要求

Tenable Identity Exposure 需要使用以下硬件：

- 支持的 Microsoft Windows 操作系统
  - Windows Server 2016
  - Windows Server 2019
  - Windows Server 2022
  - Windows Server 2025
- 规格部分所述的要求旨在让 Tenable Identity Exposure 的平台正常运行；不包括部署应用程序包需满足的操作系统要求。
- CPU 速度必须至少为 2.6 GHz。
- Tenable Identity Exposure 的平台支持采用 Intel Turbo Boost Technology 2.0 的 x86-64 处理器架构（至少为 Sandy Bridge 或 Piledriver）。
- 所需的网络接口：您可以出于管理、监控或任何其他原因添加其他网络接口。

网络要求

Tenable Identity Exposure 需要访问 Active Directory 基础设施才能启动安全监控。您必须允许不同 Tenable Identity Exposure 服务之间的网络流，如“网络流矩阵”中所述。

带宽

作为监控平台，Tenable Identity Exposure 会持续接收 Active Directory 事件。根据基础设施的尺寸，此过程会生成大量数据。

您必须分配适当的带宽，以保证在合理的时间内将数据传输到 Tenable Identity Exposure 进行分析。

根据被监控 AD 的大小，带宽规定如下表所示。

活跃 AD 用户	平均接收对象数(每分钟)	最小带宽	建议带宽
1 - 5,000	10	1 Mbps	2 Mbps
5,001 - 75,000	150	5 Mbps	10 Mbps
75,001 - 400,000	700	15 Mbps	30 Mbps

Microsoft API

要订阅并开始监控复制流，Tenable Identity Exposure 必须使用 Microsoft 的标准目录 API。Tenable Identity Exposure 仅要求使用常规用户帐户与主域控制器仿真器 (PDCe) 通信。您还必须部署新的组策略对象 (GPO) 才能激活攻击检测引擎。

与 AD 通信

对于本地安装，您需要在 Windows Server 环境中部署 Tenable Identity Exposure 软件包。Tenable Identity Exposure 必须与受监控的 Active Directory 通信。

Internet 访问

Tenable 提供持续集成流程，以支持定期发布新的检测功能。Tenable 建议您定期对 Tenable Identity Exposure 进行联网升级。

网络协议

利用特定的网络协议(如 Syslog、SMTP 或 HTTP)，Tenable Identity Exposure 可以提供本地警报功能、设计与安全信息和事件管理 (SIEM) 平台相关的特定分析流以及使用可集成到网络安全生态系统中的 REST API。

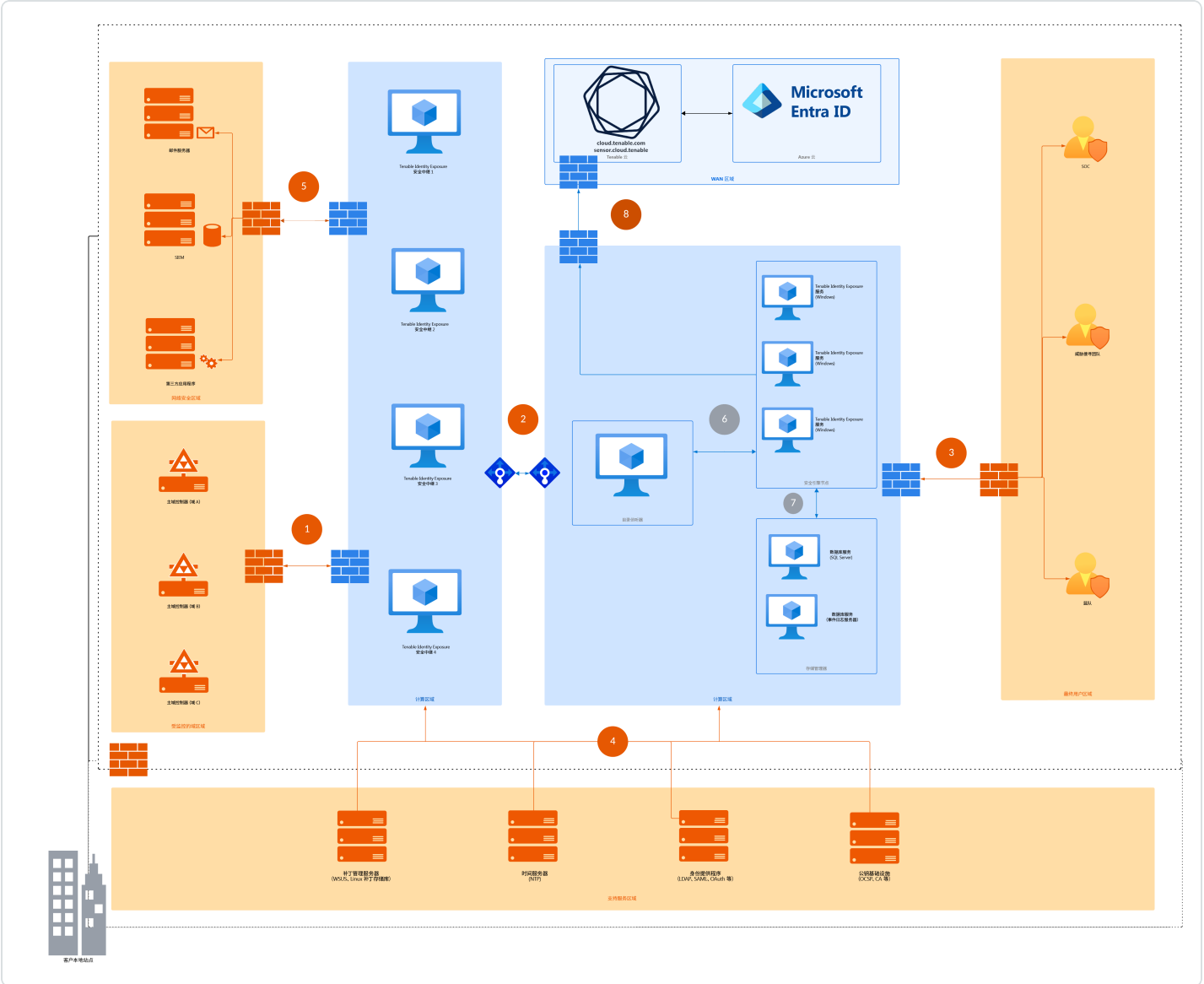
网络流矩阵

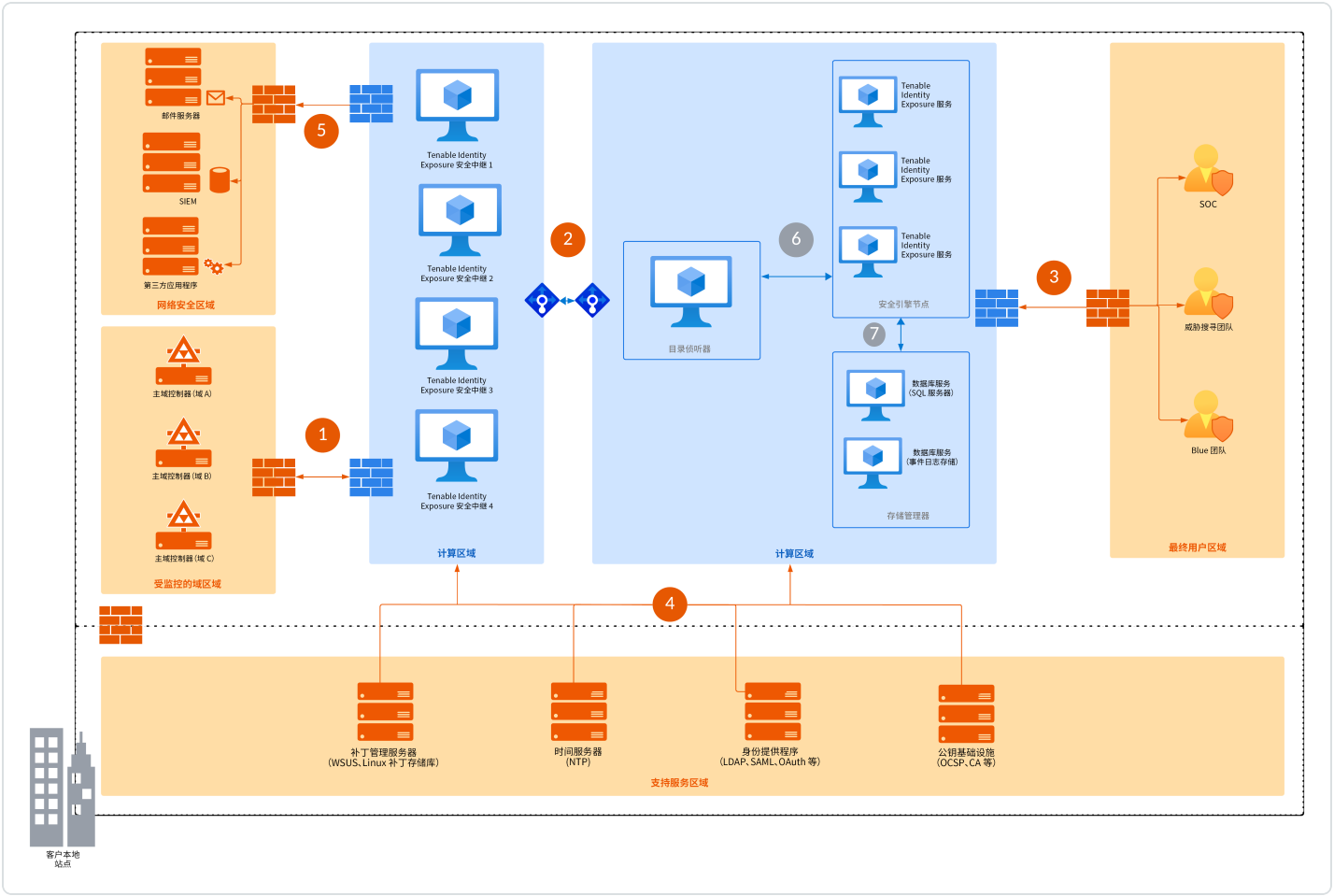
要执行安全监控，Tenable Identity Exposure 必须与每个域的主域控制器仿真器 (PDCe) 通信。您必须在每个 PDCe 上打开网络端口和传输协议，以确保有效监控。

除了这些网络流之外，您还必须考虑其他网络流，例如：

- 访问最终用户服务。
- Tenable Identity Exposure 服务之间传输的网络流。
- Tenable Identity Exposure 使用支持服务产生的网络流，例如更新管理基础设施和网络时间协议。

以下网络矩阵图提供了所涉及的不同服务的更多详细信息。





所需协议

在此图表的基础上，下表介绍了 Tenable Identity Exposure 需要使用的每个协议和端口。

网络流	从	至	Tenable Identity Exposure 的用法	流量类型	协议和端口
1.	Tenable Identity Exposure 的安全中继	域控制器	目录、复制、用户和计算机身份验证、组策略、信任	LDAP/LDAPS	TCP/389 和 TCP/636 ICMP/echo-request ICMP/echo-

					response

			复制、用户和计算机身份验证、组策略、信任	SMB、CIFS、SMB2、DFSN、LSARPC、NbtSS、NetLogonR、SamR、SrvSvc	TCP/445
			用户和计算机身份验证、林级信任	Kerberos	TCP/88、TCP/464 和 UDP/464
			用户和计算机身份验证、名称解析、信任	DNS	UDP/53 和 TCP/53
			复制、用户和计算机身份验证、组策略、信任	RPC、DCOM、EPM、DRSUAPI、NetLogonR、SamR、FRS	TCP 动态端口 (49152-65535) **注意**：从 Windows Vista 和 Windows Server 2008 开始，默认的动态端口范围为 49152-65535。这与早期版本所使用的端口 1025-5000 相比有所不同。
			目录、复制、用户和	全局目录	TCP/3268 和 TCP/3269

			计算机身份验证、组策略、信任		
			复制	RPC 端点映射程序	TCP/135
2.	Tenable Identity Exposure 的安全中继	Tenable Identity Exposure 的目录侦听器	Tenable Identity Exposure 的内部 API 流	HTTPS	TCP/443
			自动更新	HTTP	TCP/5049
3.	最终用户	Tenable Identity Exposure 的安全引擎节点	Tenable Identity Exposure 的最终用户服务(Web 门户、REST API 等)	HTTPS	TCP/443

4.	Tenable Identity Exposure	支持服务	时间同步	NTP	UDP/123
			更新基础设施 (例如，WSUS 或 SCCM)	HTTP/HTTPS	TCP/80 或 TCP/443
			PKI 基础设施	HTTP/HTTPS	TCP/80 或 TCP/443
			身份提供程序 SAML 服务器	HTTPS	TCP/443
			身份提供程序 LDAP	LDAP/LDAPS	TCP/389 和 TCP/636
			身份提供程序 OAuth	HTTPS	TCP/443

其他流

除了 Active Directory 协议之外，某些 Tenable Identity Exposure 配置还需要使用其他流。您必须打开 Tenable Identity Exposure 与目标服务之间的这些协议和端口。

网络流	从	至	Tenable Identity Exposure 的用法(可选)	流量类型	协议和端口
5.	Tenable Identity Exposure 的安	网络安全服务	电子邮件通知	SMTP	TCP/25、TCP/587、TCP/465、TCP/2525、

	全中继				TCP/25025 (取决于 SMTP 服务器的配置)
			Syslog 通知	Syslog	TCP/601、TCP/6515、UDP/514 (取决于事件日志服务器的配置)
		域控制器	特权分析	RPC 动态端口	TCP/49152-65535、UDP/49152-65535

内部端口

如果您将安全引擎节点和存储管理器拆分为两个不同的子网，Tenable Identity Exposure 需要拥有以下端口的访问权限。

注意：Tenable 不建议分隔不同网络上的安全引擎节点和存储管理器服务，以免发生性能问题。

网络流	从	至	Tenable Identity Exposure 的用法	流量类型	协议和端口
6.	Tenable Identity Exposure 的目录侦听器	Tenable Identity Exposure 的安全引擎节点	Tenable Identity Exposure 的通信总线	高级消息队列协议	TCP/5671 和 TCP/5672
			Tenable Identity Exposure 的内部 API 流	HTTP/HTTPS	TCP/80 或 TCP/443
7.	Tenable	Tenable Identity Exposure 的存储管理	MS SQL 服务器数据库访问	MS SQL 查询	TCP/1433

	Identity Exposure 的安全引擎节点	器			
			EventLogStorage 数据库访问	EventLogStorage 查询	TCP/4244
8.	Tenable Identity Exposure 的安全引擎节点	Tenable Cloud • cloud.tenable.com • sensor.cloud.tenable.com	Tenable Identity Exposure 云服务	HTTPS	TCP/443

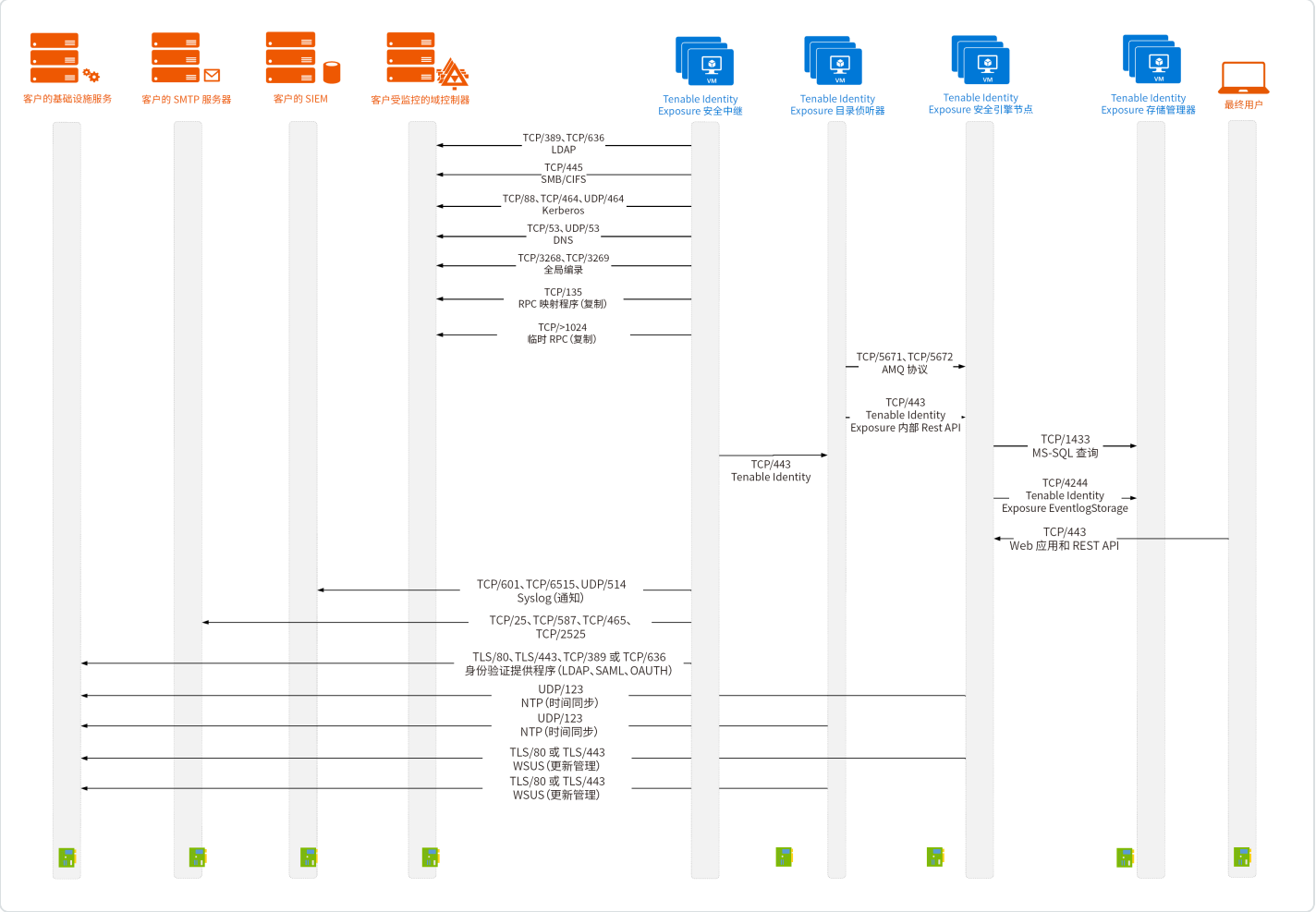
支持服务

支持服务通常因供应商而高度不同或视配置而定。例如，6.2 及更高版本的 WSUS 服务默认监听端口 TCP/8530，但其他版本的 WSUS 服务则监听 TCP/80。您可以将此端口重新配置为任何其他端口。

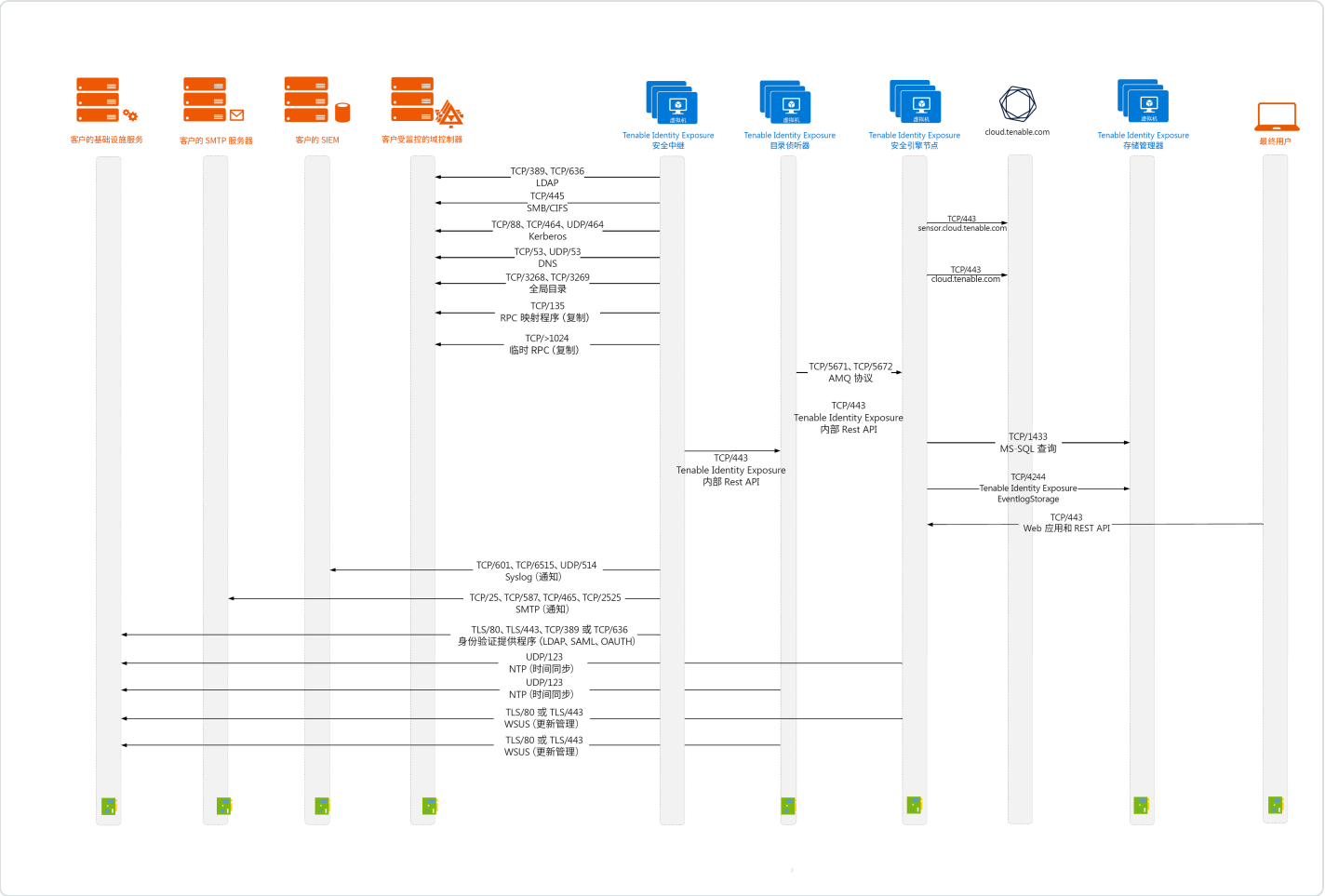
网络地址转换 (NAT) 支持

Tenable Identity Exposure 会启动所有网络连接，最终用户的网络连接除外。您可以通过网络互连，使用网络地址转换 (NAT) 连接到 Tenable Identity Exposure。

使用安全中继的本地平台



使用安全中继和代理的本地平台



Web 门户要求

Tenable Identity Exposure 不要求对客户端浏览器进行任何特定配置或安装插件。

支持的 Internet 浏览器

您必须使用最新版本的受支持的 Web 浏览器。

支持的 Web 浏览器(包括最低版本)	
Microsoft	Edge 版本 38.14393 或 Internet Explorer 11
Google	Chrome 版本 56.0.2924
Mozilla	Firefox 版本 52.7.3
Apple	Safari 版本 11.0

TLS 服务器证书

Tenable Identity Exposure 使用 SSL/TLS 加密机制访问应用程序。

Tenable 强烈建议使用您在安装期间提供的有效证书。

支持的 TLS 配置和版本

- TLS 1.1 至 TLS 1.3
- Tenable 提供的自签名证书
- 您的私有 PKI 颁发的证书
- 备用 TLS 证书

推荐的 TLS 配置和版本

- TLS 1.2
- 您的私有 PKI 颁发的证书

TLS 证书更新

如需在升级操作之外更改 TLS 证书，您可以更新 `Tenable\Tenable.ad\Certificates` 下的 CRT 和密钥文件并重新启动服务。

另请参阅：

- HTTPS for Tenable Identity Exposure Web Application

与 Active Directory 域集成

Tenable Identity Exposure 可在连接到 Active Directory (AD) 域的 Microsoft Server 操作系统上运行。以下指南关于是否将这些服务器连接到 AD 域。

- 由于 Tenable Identity Exposure 提供的安全信息较为敏感，**Tenable 不建议将其服务器加入任何 AD 域**。实际上，在隔离的环境中工作有助于明确区分受监控的边界和监控实体（即 Tenable Identity Exposure）。在此配置中，在受监控的域上拥有初始访问权限或有限权限的攻击者无法直接访问 Tenable Identity Exposure 及其安全分析结果。

- 如果有受信任的基础设施，您可以选择在域加入服务器上运行 Tenable Identity Exposure。此方法可以改进服务器管理，因为它是用于每个域加入服务器的常规流程的一部分。特别是，Tenable Identity Exposure 服务器应用的强化政策与其他公司服务器的强化政策相同。Tenable 建议仅在安全的 AD 环境中使用此架构，并且您必须考虑 AD 遭到入侵时带来的以下风险：
  - 拥有服务器管理权限的攻击者可以使用来自 Tenable Identity Exposure 的数据分析，收集有关入侵系统的方式的更多信息。
  - 对域加入服务器实施安全策略可禁止向 Tenable 支持团队或其认证合作伙伴授予管理员权限。
  - 攻击者可通过隐藏安全事件来破坏 Tenable Identity Exposure 的安全监控。

安装 Tenable Identity Exposure

所需用户角色:本地计算机上的管理员

Tenable Identity Exposure 的安装程序用于在不同的服务器上安装以下组件:

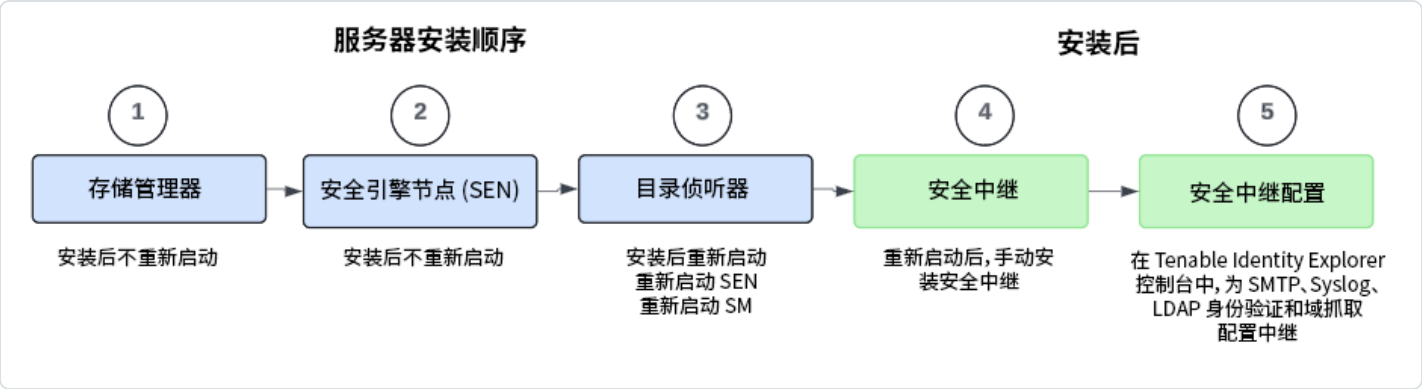
- **存储管理器** (SM), 用于托管基于 MSSQL 的所有数据。
- **目录侦听器** (DL), 以经过审核的域为目标。
- **安全引擎节点** (SEN), 用于执行安全分析和服务用户界面。

  有关如何在多台计算机上安装 SEN 的详细信息, 请参阅"Split Security Engine Node (SEN) Services"。
- **安全中继**(单独的安装程序), 允许您配置域, 以便安全中继从域中将数据转发到收集 AD 对象的数据侦听器组件。

所有计算机和安装的二进制文件都支持为底层操作系统应用任何安全更新(通过 Windows 服务器更新服务 (WSUS) 或系统中心配置管理器 (SCCM))。

安装顺序

要安装 **Tenable Identity Exposure** 3.77, 请按以下顺序操作:



事先说明

- 从 Tenable 的下载站点下载 **Tenable Identity Exposure** 和安全中继的可执行程序。
- **查看** 部署前要求。

注意：从 Tenable Identity Exposure **3.59.5** 版开始，请确保您的 **TLS 证书使用 OpenSSL 3.0.x**。

- **查看** 本地架构 并为您的平台**选择** TLS Installation Types。
- 安装 Tenable Identity Exposure 之前，请**保留以下资源** 并准备好相关信息：
  - 网络：私有 IP 地址。
  - 访问：用于访问 Tenable Identity Exposure 的 Web 门户的 DNS 名称。
  - 安全：确保安全访问 Web 门户的 TLS 证书及其相关私钥。

    有关更多信息，请参阅“网络要求”。
- **以本地用户或域用户(“本地管理员”组的成员)的身份运行安装程序**。
- **拥有帐户权限**：用于部署 Tenable Identity Exposure 的帐户必须拥有以下特定权限：`SeBackupPrivilege`、`SeDebugPrivilege` 和 `SeSecurityPrivilege`。
- **重新启动服务器**，然后再为每个组件启动 Tenable Identity Exposure 安装程序。

安装程序

请按照以下程序，使用“**带自动生成证书和自签名证书的 TLS(默认)**”安装 Tenable Identity Exposure 组件。有关更多信息，请参阅“TLS Installation Types”。

安装存储管理器：

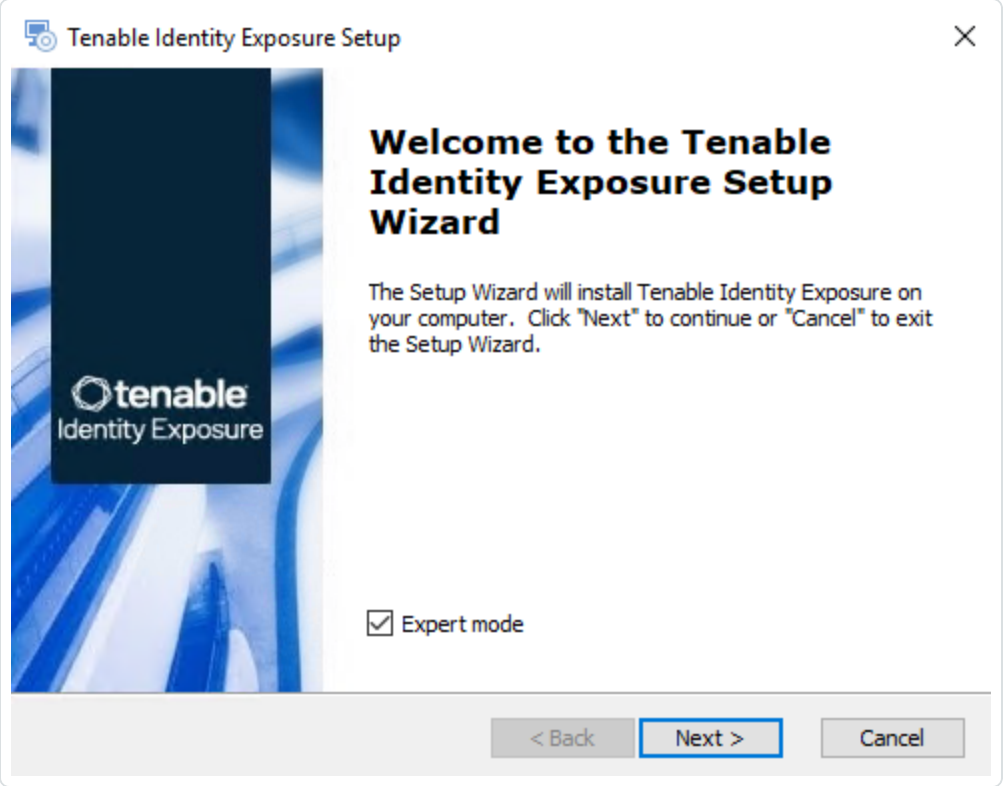
1. 在本地计算机上，运行 **Tenable Identity Exposure 3.77** 本地安装程序。

   出现“欢迎”屏幕。

2. 在设置语言框中，单击箭头即可选择要安装的语言，然后单击“**下一步**”。

   出现“**安装向导**”。

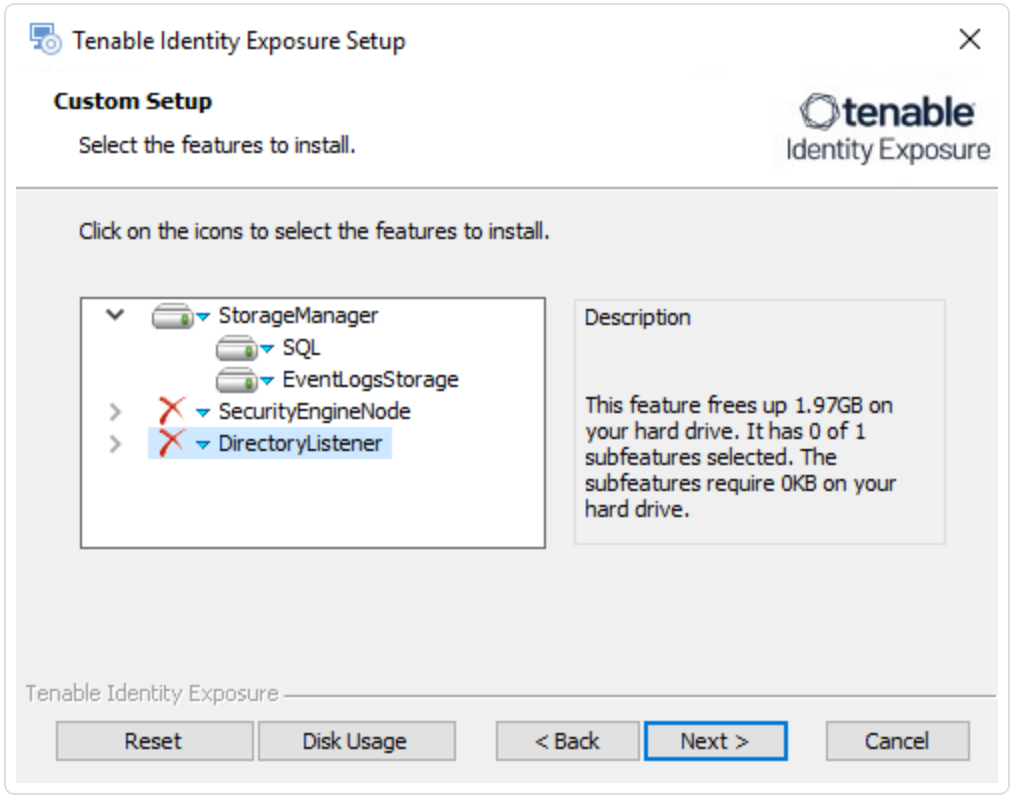
3. 选中“**专家模式**”复选框。



4. 单击“**下一步**”。

   出现“**自定义安装**”窗口。

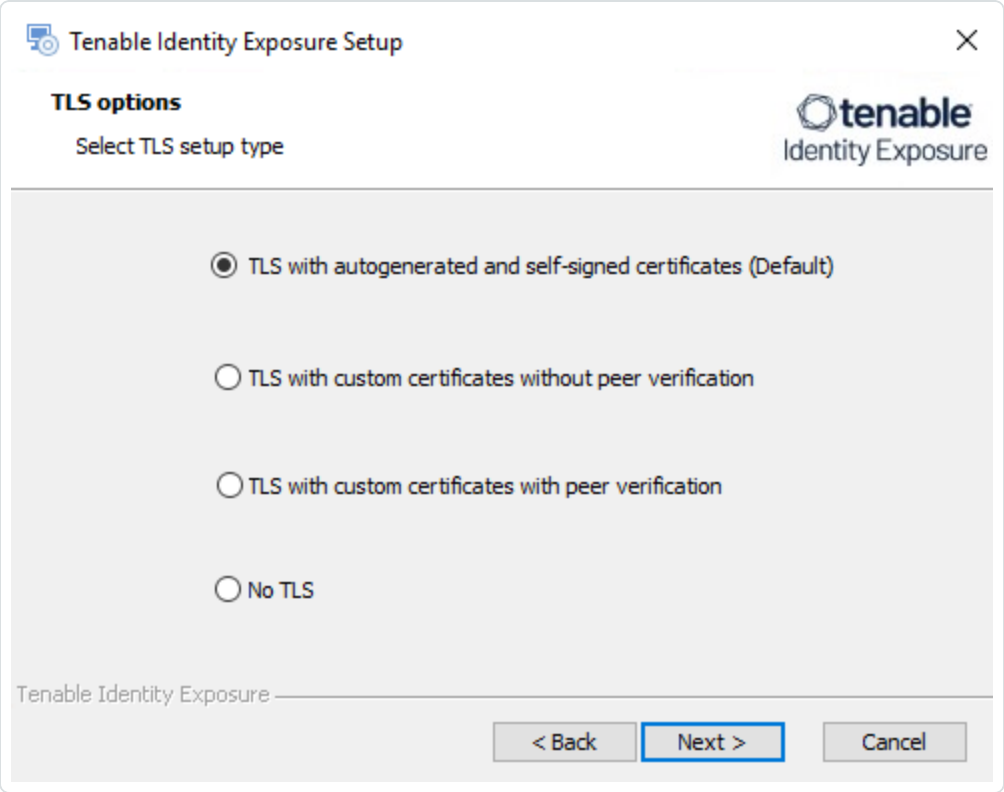
5. 取消选择*安全引擎节点*和*目录侦听器*组件。



6. 单击“**下一步**”。

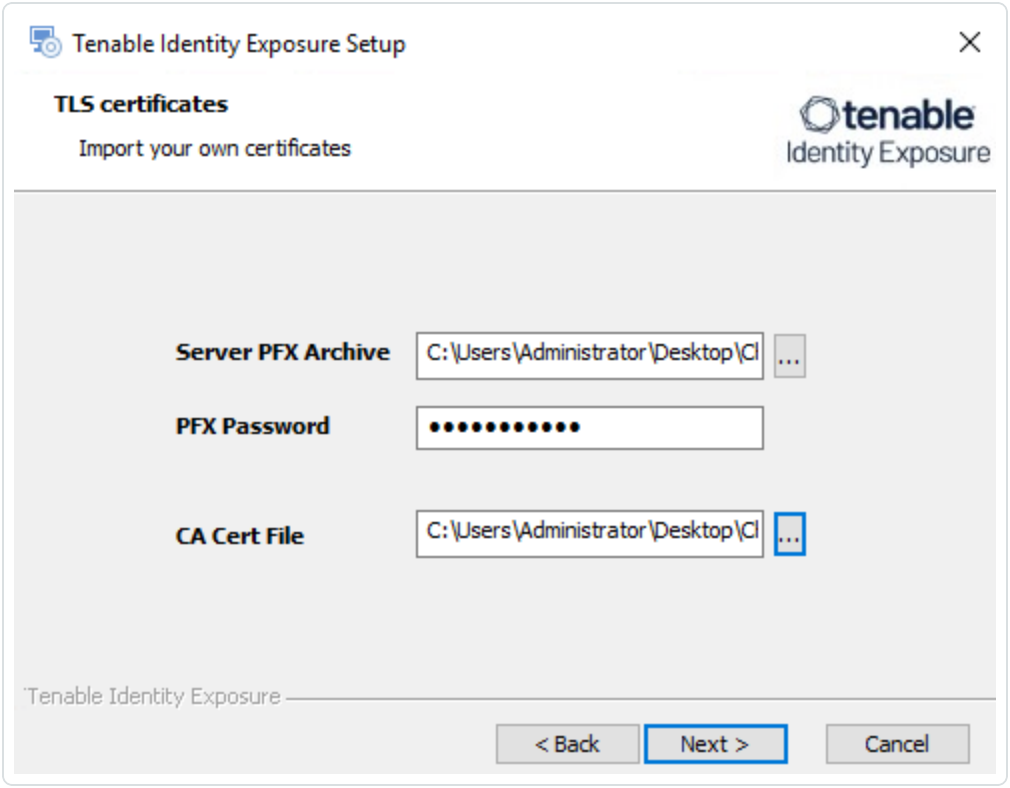
   出现“**TLS 选项**”窗口。

7. 选择“**带有自动生成证书和自签名证书的 TLS(默认)**”选项。



可选:如果您选择“**带有自定义证书的 TLS，无需对等验证**”或“**带有自定义证书的 TLS，需要对等验证**”，则下一个“**TLS 证书**”屏幕会要求您提供以下信息:

- 在“**服务器 PFX 存档**”框中，单击“**...**”以导航至“PFX 存档”。
- 在“**PFX 密码**”框中，输入 PFX 文件的密码。
- 在“**CA 证书文件**”框中，单击“**...**”以导航至 CA 证书文件。

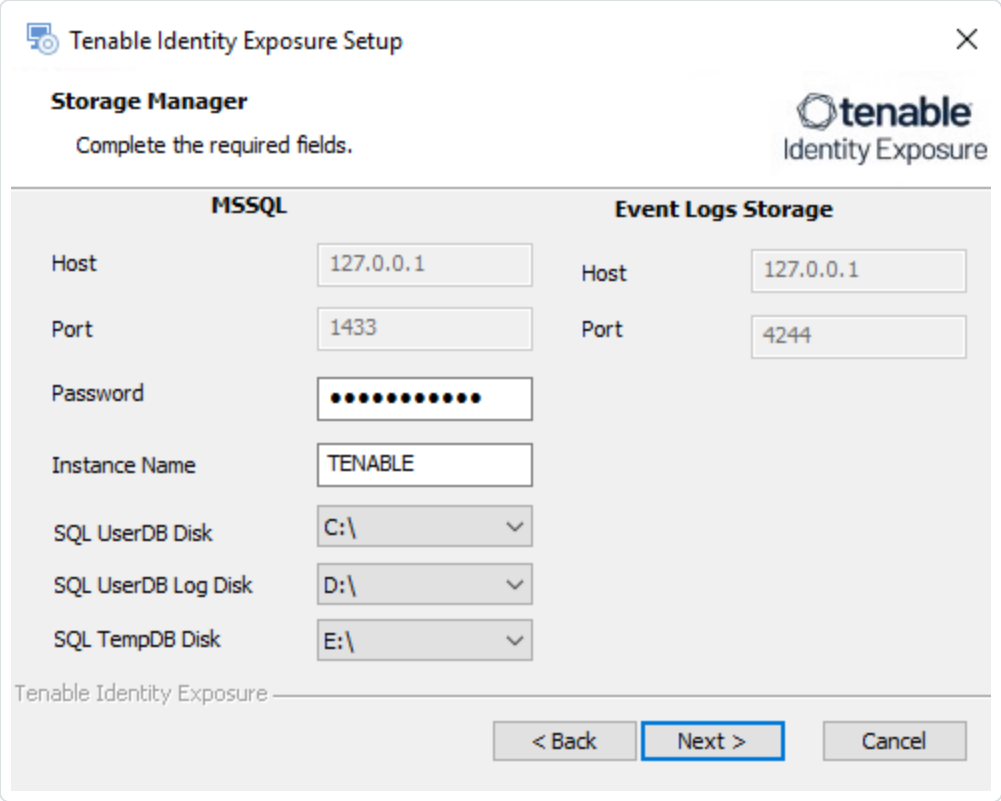


8. 单击“**下一步**”。

   出现“**存储管理器**”窗口。

9. 在“**密码**”框中，输入 MSSQL 数据库的密码。

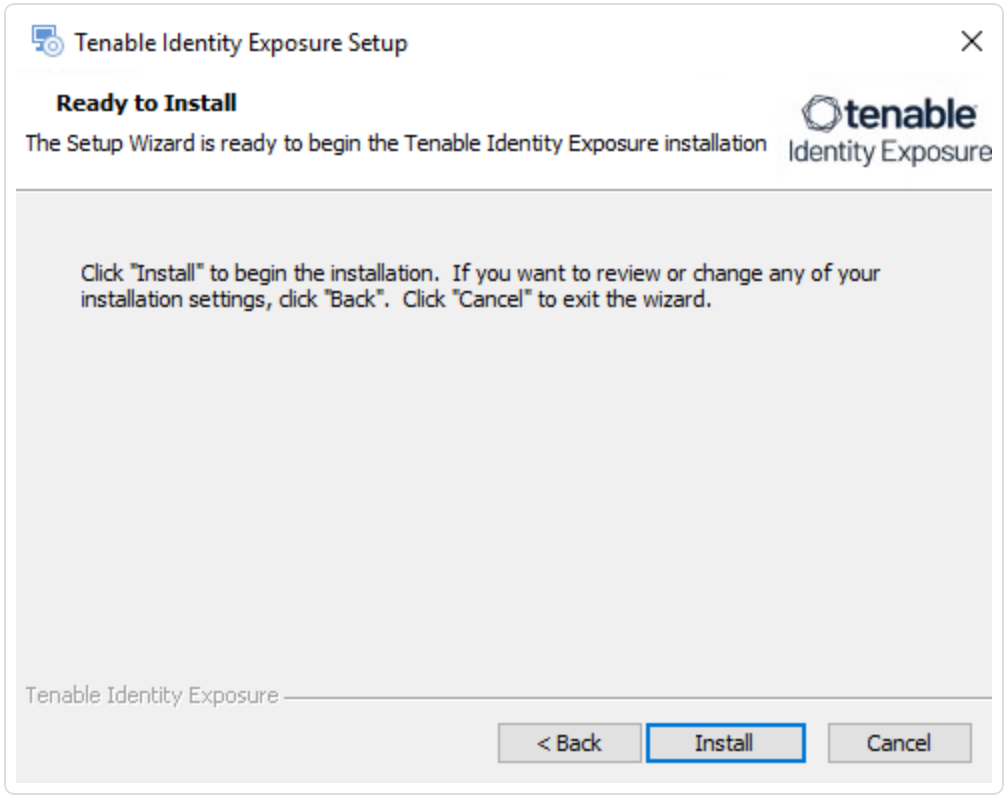
> **注意**：根据安装程序的要求，请遵循 SQL 服务器强密码中所述的语法规范设置 SA 密码。



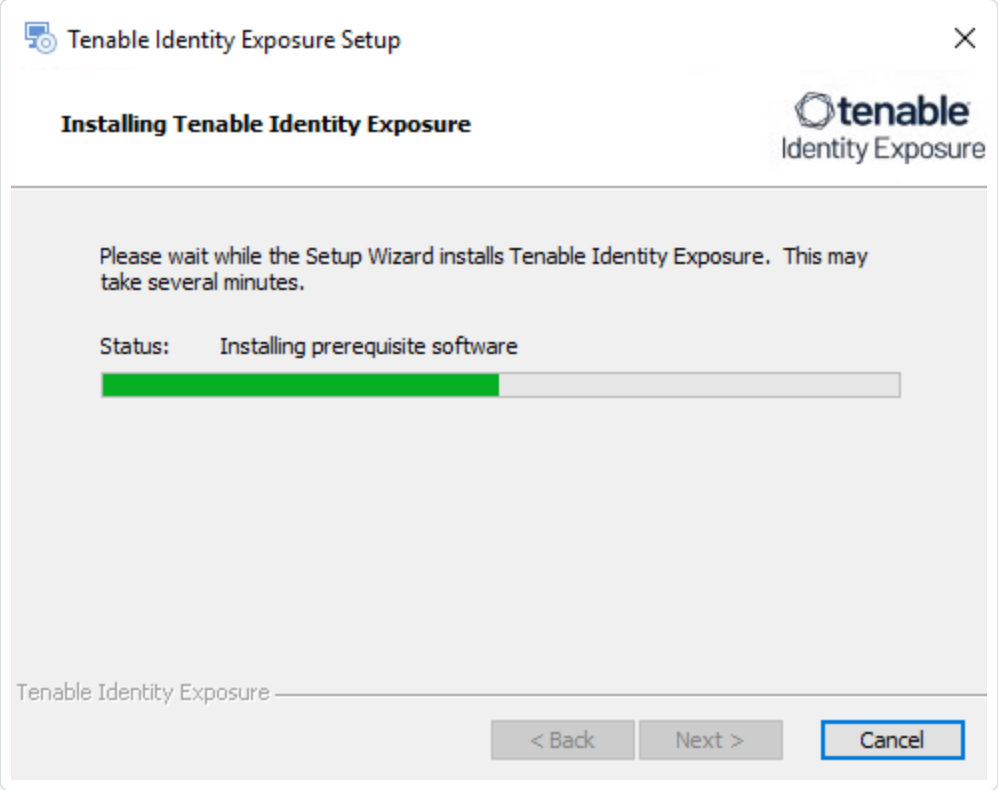
> **注意**：Tenable 强烈建议您保留默认的 Tenable 实例名称。

10. 单击“**下一步**”。

出现“**准备安装**”窗口。



11. 单击“**安装**”即可开始安装。



安装完成后，会出现“**正在完成 Tenable Identity Exposure 安装向导**”窗口。

12. 单击“**完成**”。

此时会出现一个对话框，询问是否要重新启动计算机。

13. 单击“**否**”。

> **注意**：暂时**不要**重新启动计算机。

14. 安装安全引擎节点。

安装安全引擎节点：

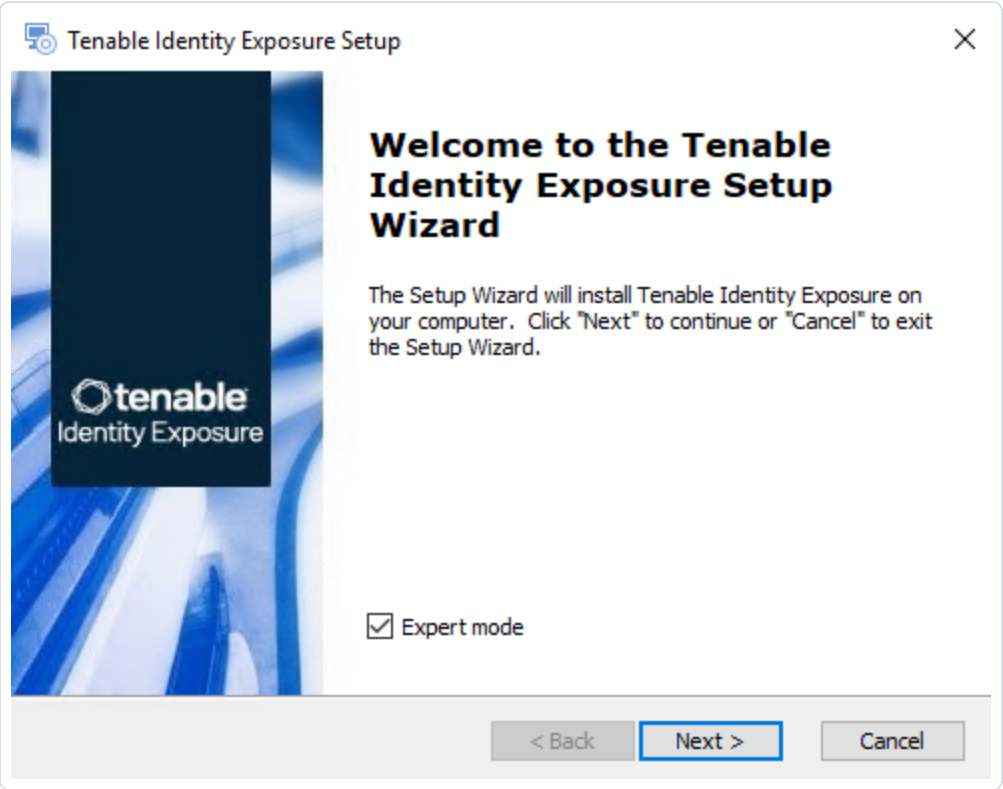
1. 在本地计算机上，运行 **Tenable Identity Exposure 3.77** 本地安装程序。

出现“欢迎”屏幕。

2. 在设置语言框中，单击箭头即可选择要安装的语言，然后单击“**下一步**”。

出现“**安装向导**”。

3. 选中“**专家模式**”复选框。

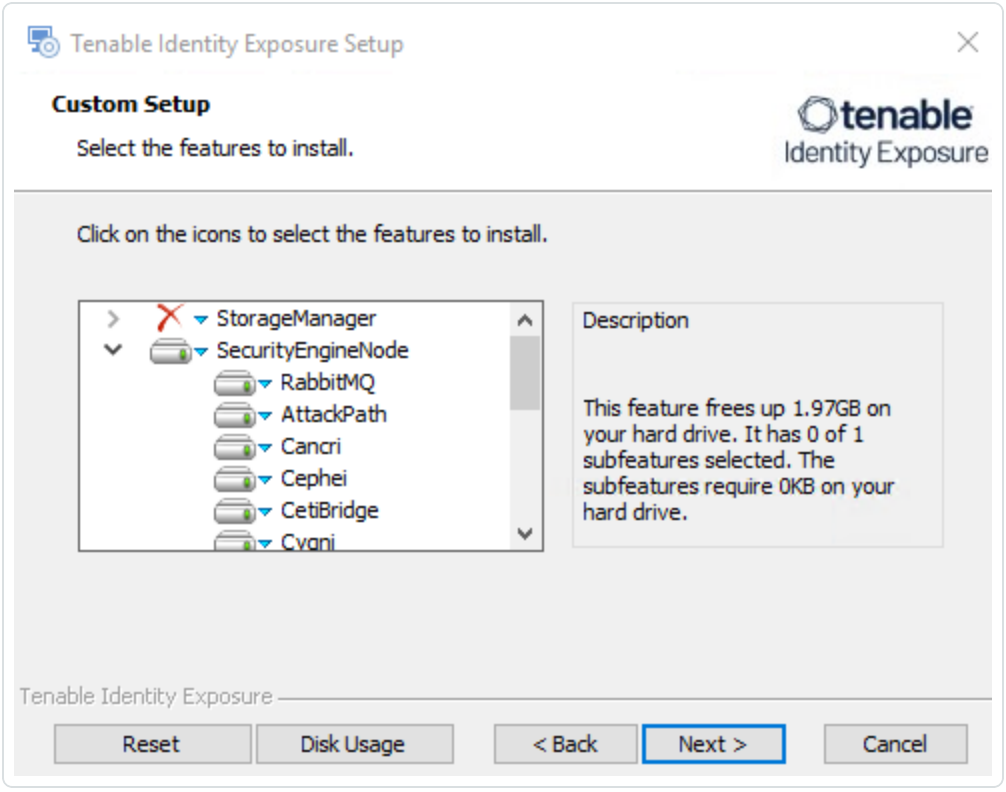


4. 单击“**下一步**”。

   出现“**自定义安装**”窗口。

5. 取消选择*存储管理器*和*目录侦听器*组件。

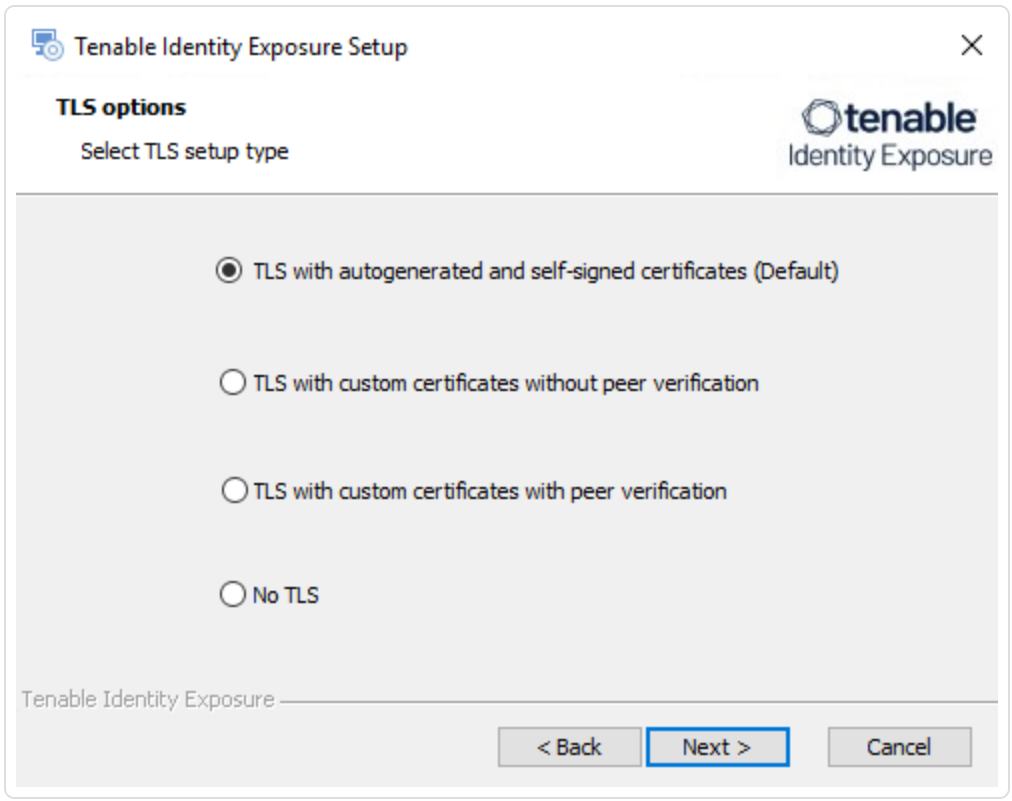
   注意：要在多台计算机上安装 SEN 服务，请参阅 Split Up SEN Services。



6. 单击“**下一步**”。

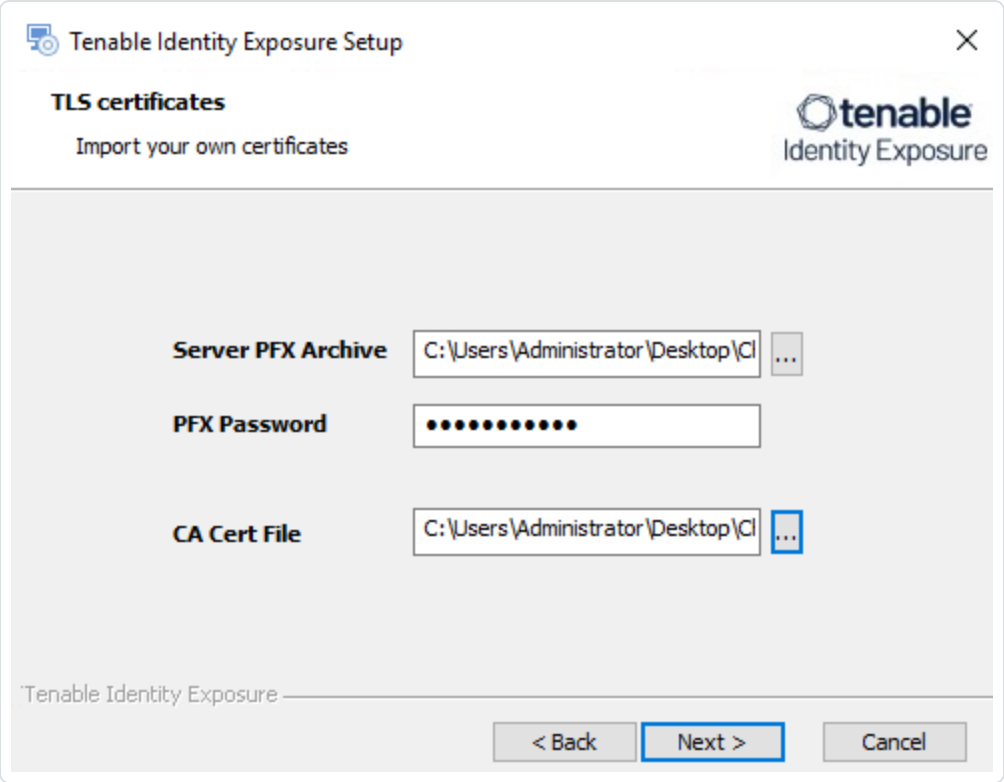
   出现“**TLS 选项**”窗口。

7. 选择“**带有自动生成证书和自签名证书的 TLS(默认)**”选项。



可选:如果您选择“**带有自定义证书的 TLS,无需对等验证**”或“**带有自定义证书的 TLS,需要对等验证**”,则下一个“**TLS 证书**”屏幕会要求您提供以下信息:

- 在“**服务器 PFX 存档**”框中,单击“**...**”以导航至“PFX 存档”。
- 在“**PFX 密码**”框中,输入 PFX 文件的密码。
- 在“**CA 证书文件**”框中,单击“**...**”以导航至 CA 证书文件。



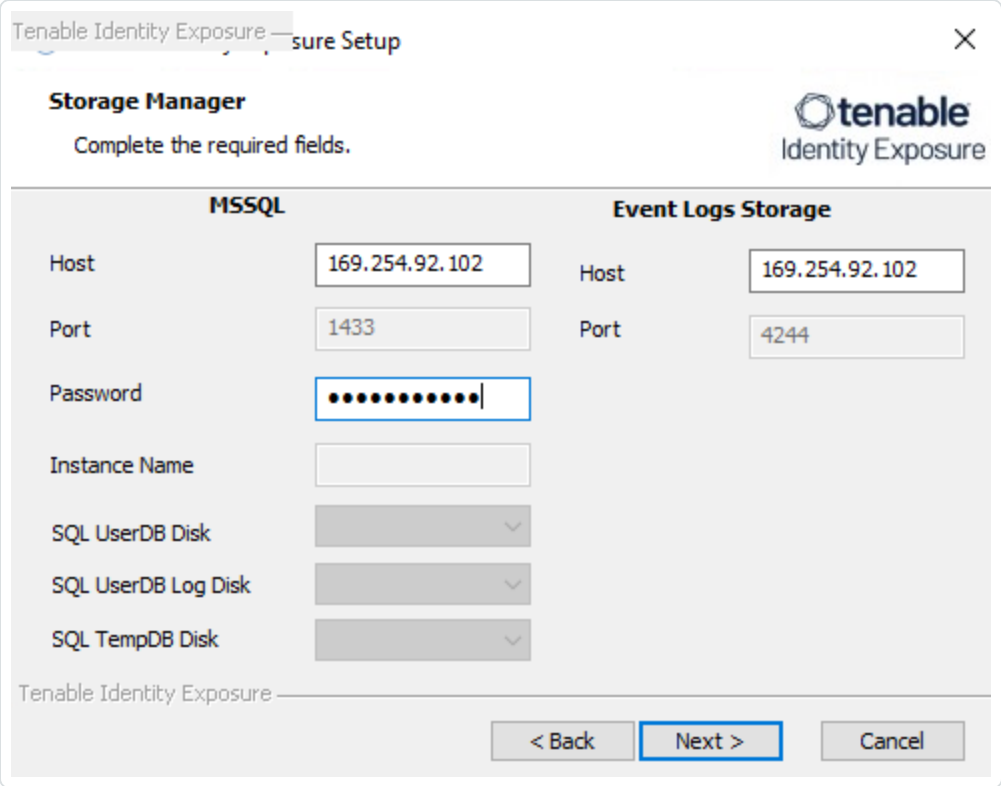
8. 单击“**下一步**”。

   出现“**存储管理器**”窗口。

9. 提供以下信息：

   - 在“**MSSQL**”和“**事件日志存储**”框中，输入存储管理器的 FQDN 或 IP 地址。
   - 在“**密码**”框中，为存储管理器安装设置中定义的 MSSQL 数据库输入服务帐户密码。

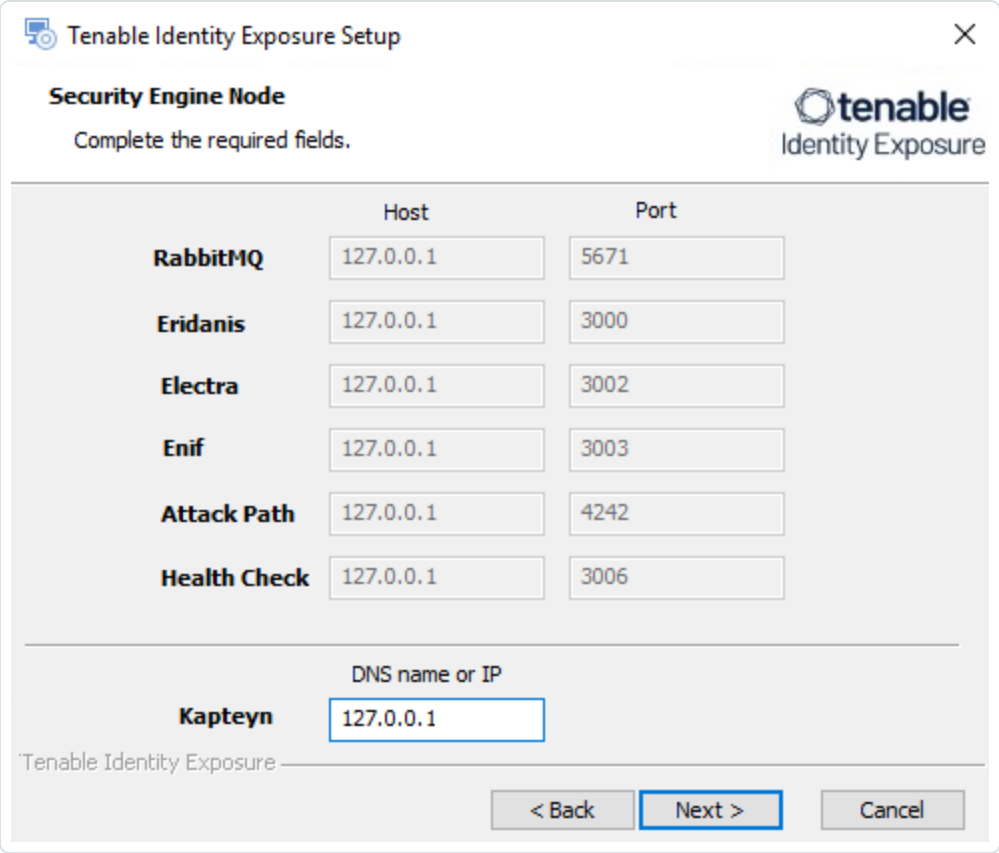
注意:根据安装程序的要求,请遵循 SQL 服务器强密码中所述的语法规范设置 SA 密码。



10. 单击“**下一步**”。

    出现“**安全引擎节点**”窗口。

11. 在“**主机**”框中,输入最终用户为了访问 Tenable Identity Exposure 而输入的 Web 服务器的 DNS 名称(首选)或 IP 地址。



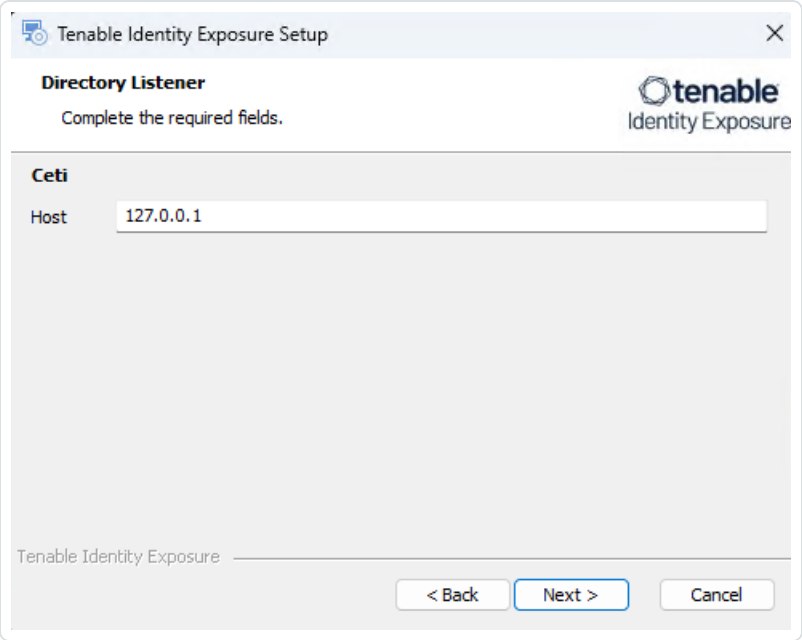
注意:默认情况下,在安装过程中,系统会使用您输入的 DNS 名称或 IP 地址创建自签名证书。有关更多信息,请参阅"Change the IIS Certificate"。

12. 单击"**下一步**"。

    出现"**目录侦听器**"窗口。

13. 在"**Ceti**"框中,输入目录侦听器计算机的 IP 地址或配置的 FQDN。

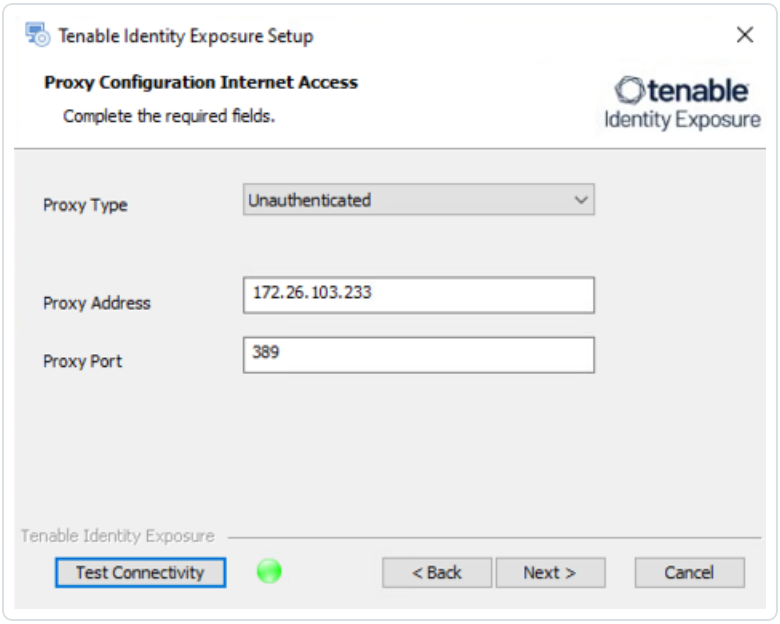
提示:如果计划在目录侦听器所在的同一计算机上安装安全中继,则必须在 SEN 上为 Ceti 保留默认 IP 地址"127.0.0.1"。如果计划在另一台计算机上安装安全中继,请在 SEN 上为 Ceti 输入目录侦听器的 IP 地址。



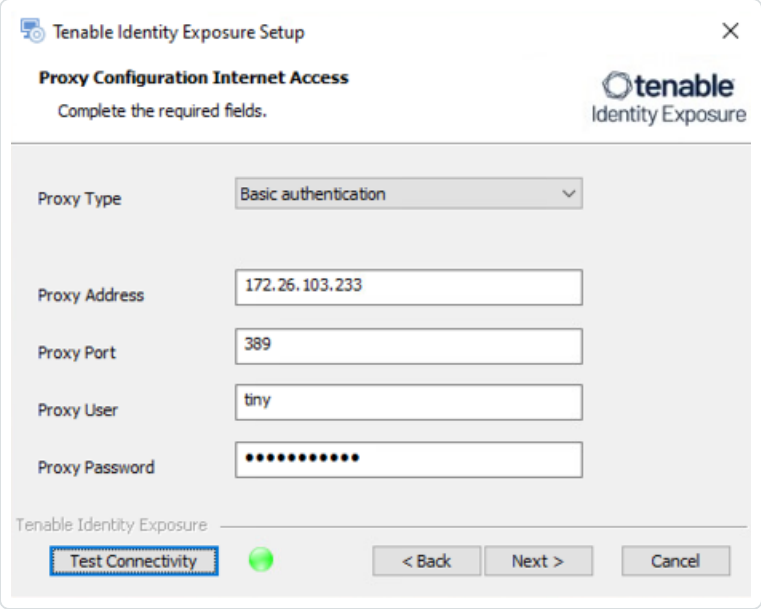
此时会出现“**代理配置**”窗口。

14. 有以下代理类型可供选择：

    - **无**：从下拉列表框中选择“无”，然后单击“**下一步**”。
    - **未经身份验证**：从下拉列表框中选择“未经身份验证”。
        - 在“**代理地址**”和“**代理端口**”框中，输入代理服务器的地址和端口。



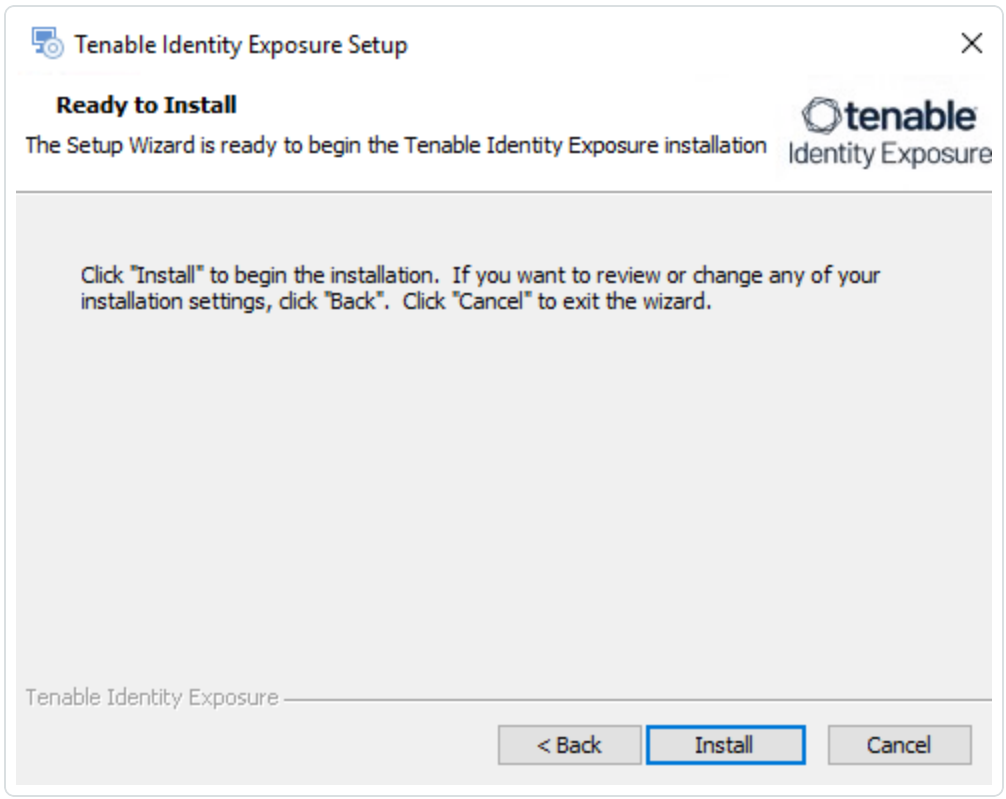
- **基本身份验证**：从下拉列表框中选择“基本身份验证”。
  - 在“**代理地址**”和“**代理端口**”框中，输入代理服务器的地址和端口。
  - 在“**代理用户**”和“**代理密码**”框中，输入被授权访问代理服务器的特定用户帐户的名称以及相关的凭据，以允许通过代理服务器发送请求。



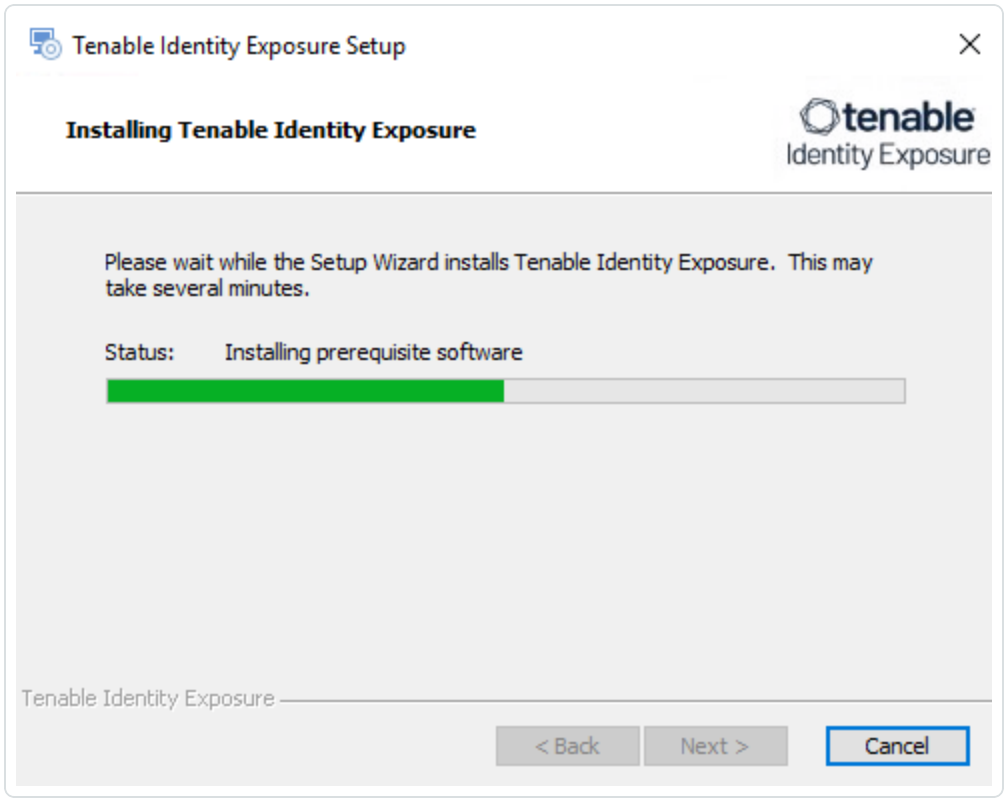
15. 单击“**测试连接**”。
16. 单击“**下一步**”。

    出现“**准备安装**”窗口。

17.



18. 单击“**安装**”即可开始安装。



安装完成后，会出现“**正在完成 Tenable Identity Exposure 安装向导**”窗口。

19. 单击“**完成**”。

    此时会出现一个对话框，询问是否要重新启动计算机。

20. 单击“**否**”。

    注意：暂时**不要**重新启动计算机。

21. 安装目录侦听器。

安装目录侦听器：

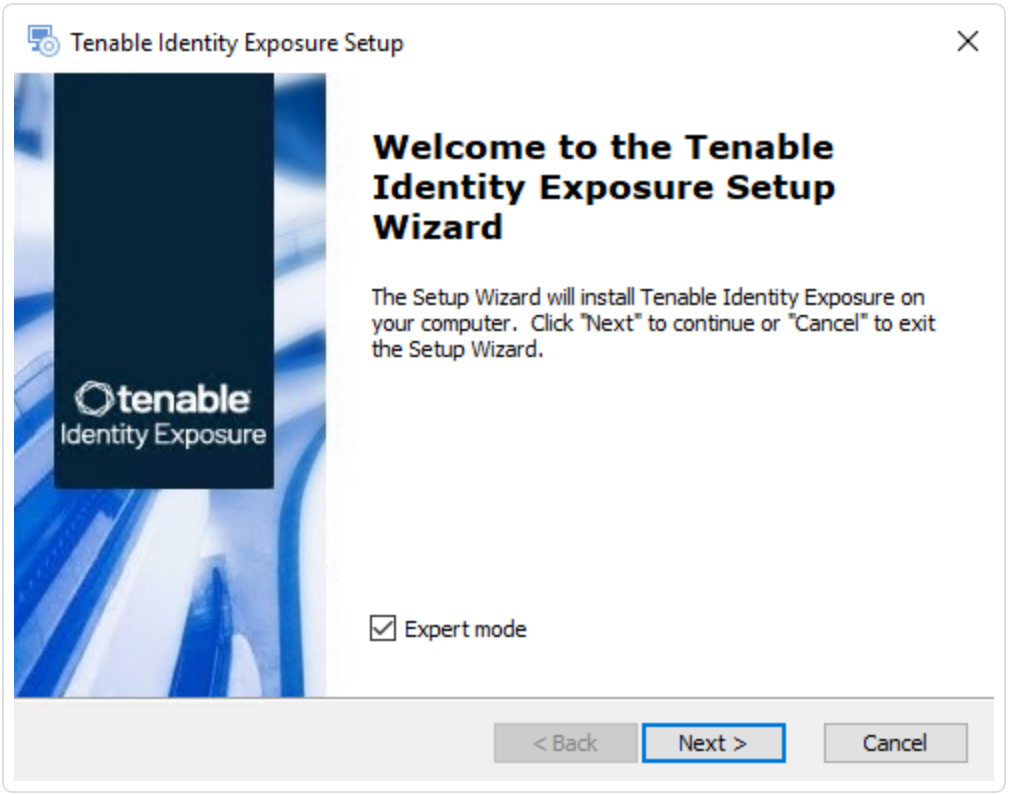
1. 在本地计算机上，运行 **Tenable Identity Exposure 3.77** 本地安装程序。

   出现“欢迎”屏幕。

2. 在设置语言框中，单击箭头即可选择要安装的语言，然后单击“**下一步**”。

   出现“**安装向导**”。

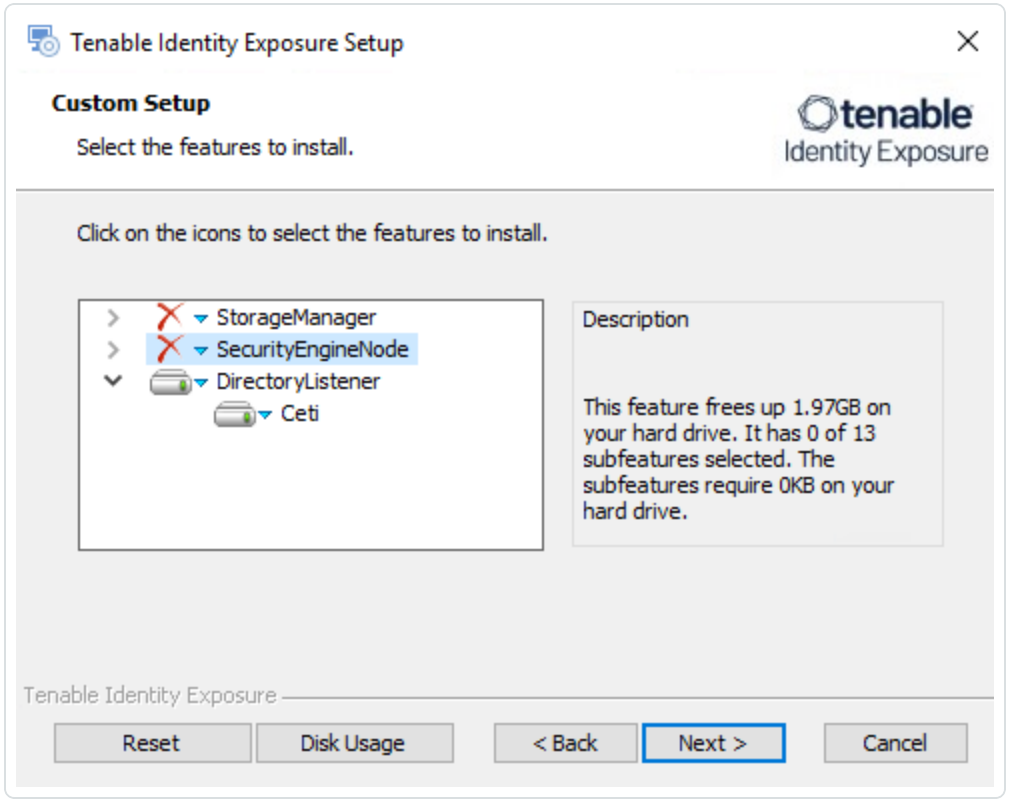
3. 选中“**专家模式**”复选框。



4. 单击“**下一步**”。

   出现“**自定义安装**”窗口。

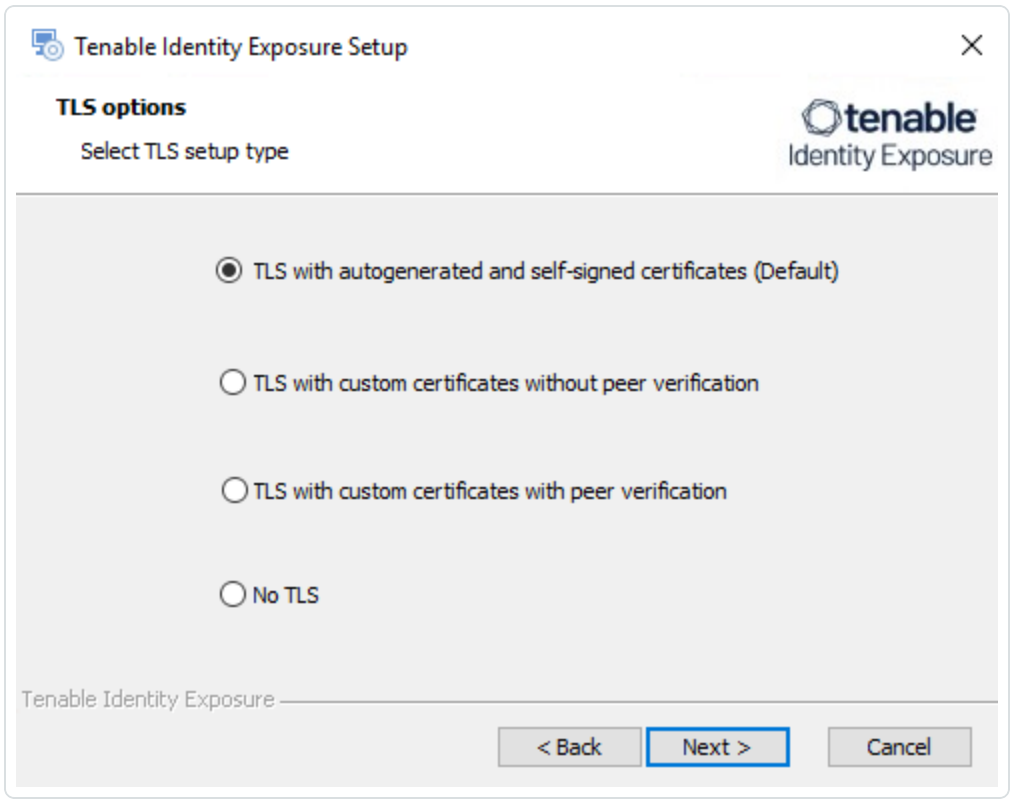
5. 取消选择*存储管理器*和*安全引擎节点*组件。



6. 单击“**下一步**”。

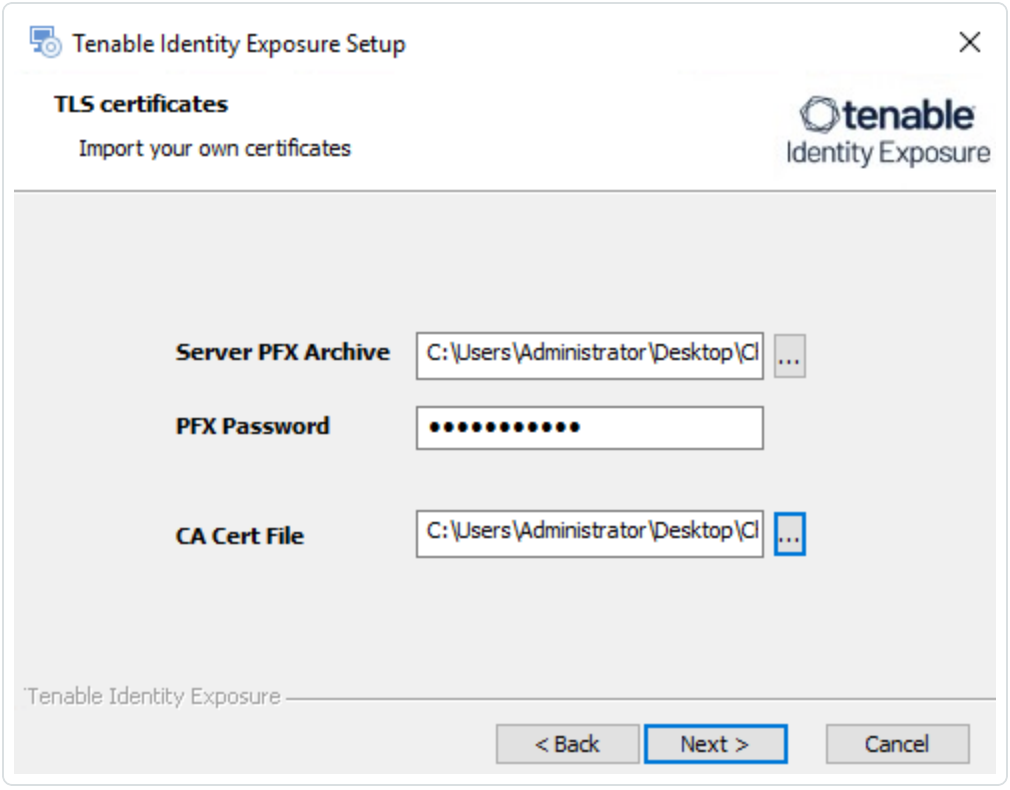
   出现“**TLS 选项**”窗口。

7. 选择“**带有自动生成证书和自签名证书的 TLS(默认)**”选项。



可选：如果您选择“**带有自定义证书的 TLS，无需对等验证**”或“**带有自定义证书的 TLS，需要对等验证**”，则下一个“**TLS 证书**”屏幕会要求您提供以下信息：

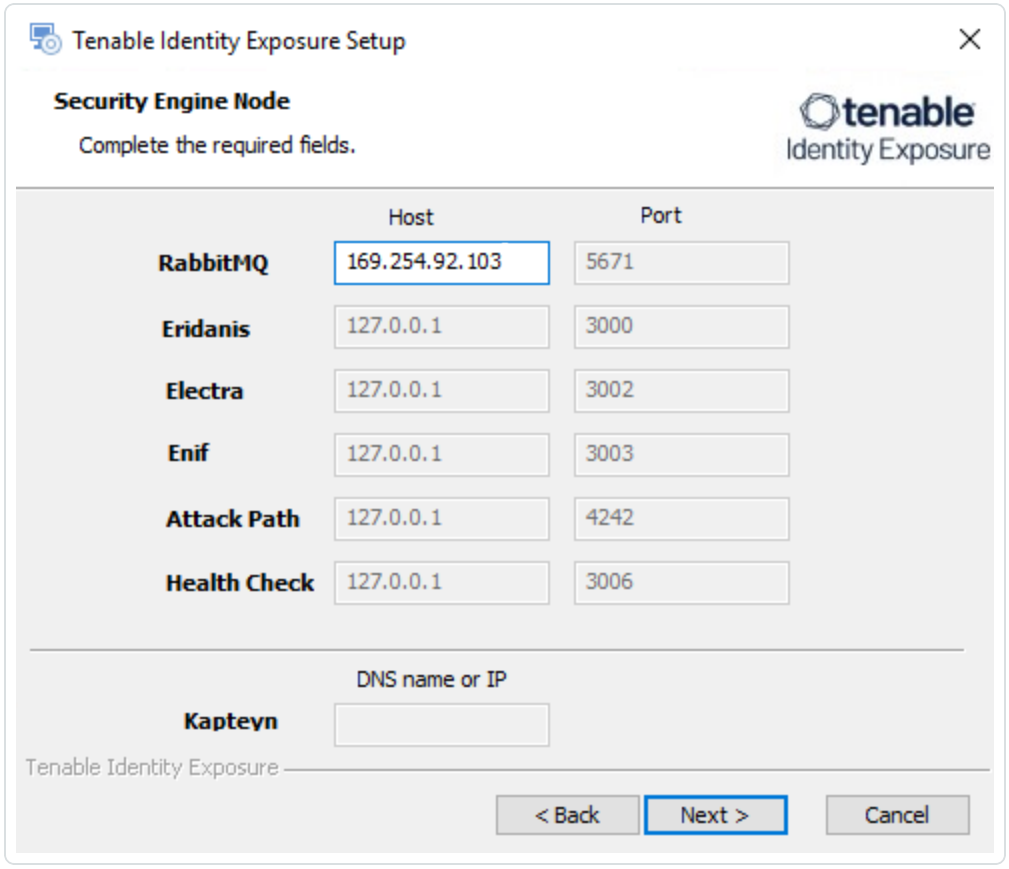
- 在“**服务器 PFX 存档**”框中，单击“**...**”以导航至“PFX 存档”。
- 在“**PFX 密码**”框中，输入 PFX 文件的密码。
- 在“**CA 证书文件**”框中，单击“**...**”以导航至 CA 证书文件。



8. 单击“**下一步**”。

   出现“**安全引擎节点**”窗口。

9. 在 RabbitMQ 的“**主机**”框中，输入托管 RabbitMQ 的安全引擎节点的地址。

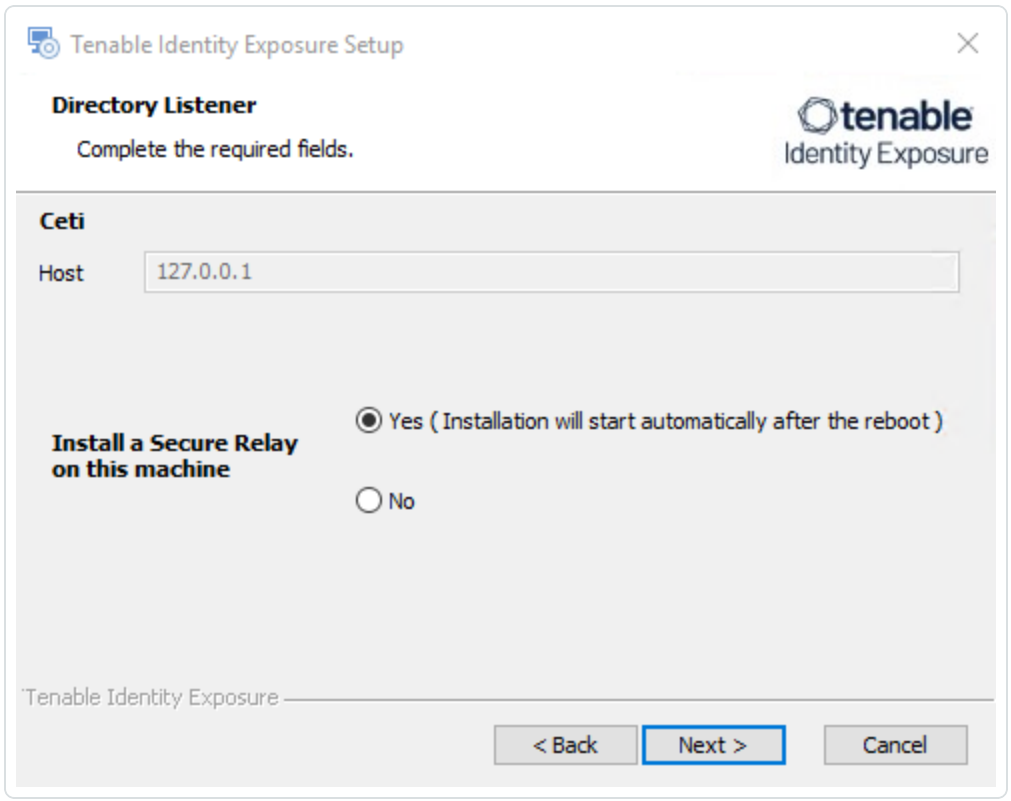


10. 单击“**下一步**”。

    出现“**目录侦听器**”窗口。

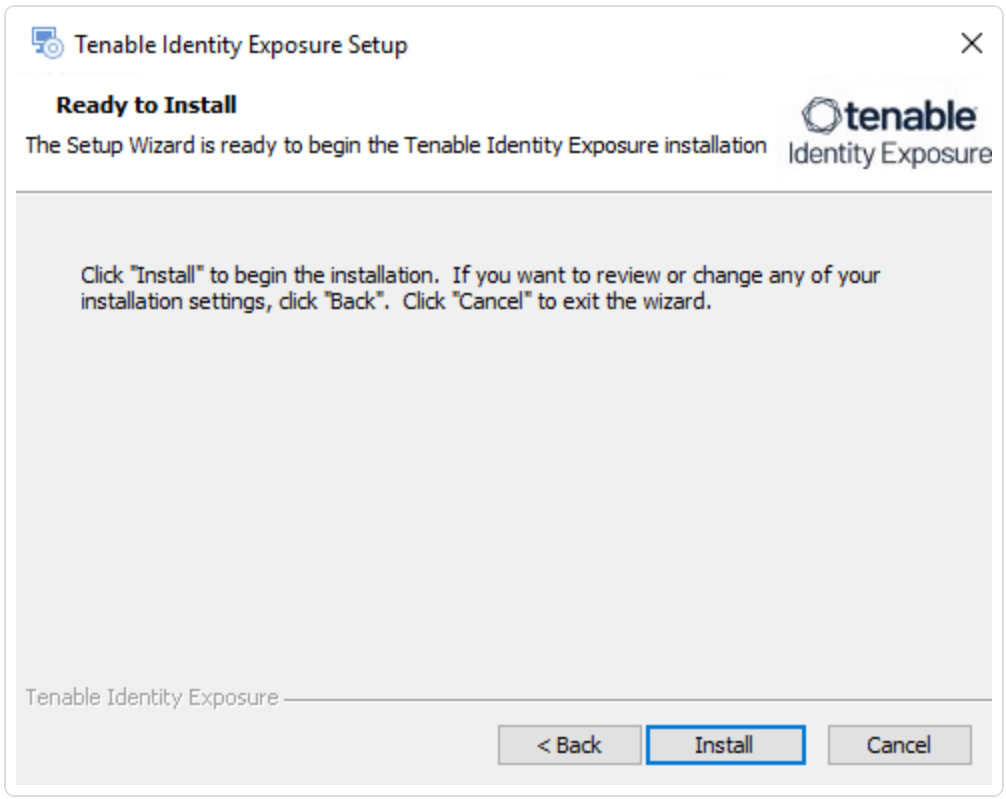
11. 有两个选项可供您选择是否在此目录侦听器上安装安全中继：

    - **是**：在此安装过程完成且目录侦听器重新启动后，安全中继安装程序便会启动。
    - **否**：您选择在以后**或在单独的服务器上**安装安全中继（请参阅“本地平台的安全中继架构”）。此时会出现一条消息，其中包含安全中继安装程序所在的位置。无论是在目录侦听器计算机还是单独的计算机上，您都**必须安装安全中继**。

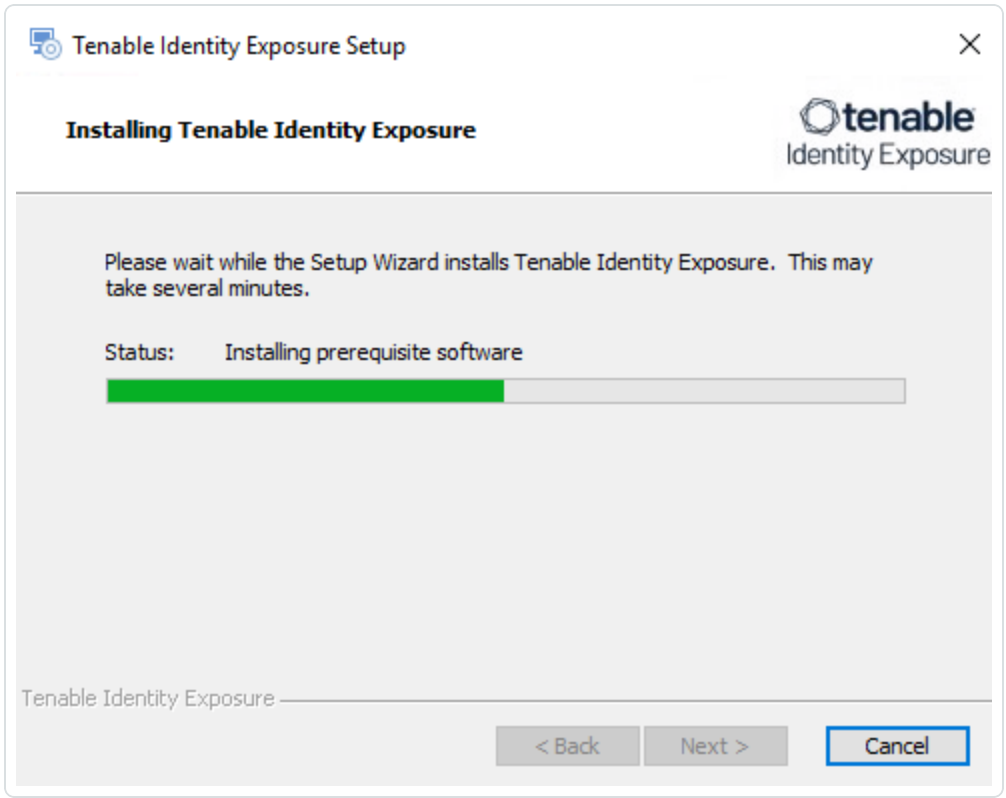


12. 单击“**下一步**”。

    出现“**准备安装**”窗口。



13. 单击“**安装**”即可开始安装。



安装完成后，会出现“**正在完成 Tenable Identity Exposure 安装向导**”窗口。

14. 单击“**完成**”。

    此时会出现一个对话框，询问是否要重新启动计算机。

15. 单击“**是**”。

    计算机重新启动。

16. 重新启动 SEN 计算机。

17. 重新启动存储管理器计算机。

18. 使用单独的安装程序安装 适用于 Tenable Identity Exposure 3.77 的安全中继。

若要登录 Tenable Identity Exposure：

1. Log in to Tenable Identity Exposure.

2. 输入您的初始凭据：用户名 `hello@tenable.ad`，密码是`verySecure1`。

若要安装安全中继，请执行以下操作：

1. 查看安全中继要求。

2. 选择 本地平台的安全中继架构。

3. 安装 适用于 Tenable Identity Exposure 3.77 的安全中继。

升级 Tenable Identity Exposure

所需用户角色：本地计算机上的管理员

从之前的版本升级到 Tenable Identity Exposure 版本 **3.77** 需要调整之前的架构，以包含安全中继组件。**升级之前，请仔细检查并了解以下部分中说明的变更**：

- 本地平台的安全中继架构 升级前 (3.42) 和升级后 3.77 之间的差异
- **在升级存储管理器、安全引擎节点和目录侦听器之后**，请使用单独的安装程序手动安装适用于 Tenable Identity Exposure 3.77 的安全中继。

注意：从 Tenable Identity Exposure **3.59.5** 版开始，请确保您的 **TLS 证书使用 OpenSSL 3.0.x**。有关更多信息，请参阅“部署前要求”。

升级路径

要升级到 Tenable Identity Exposure 的最新版本，您必须遵循以下安装路径中的一条：

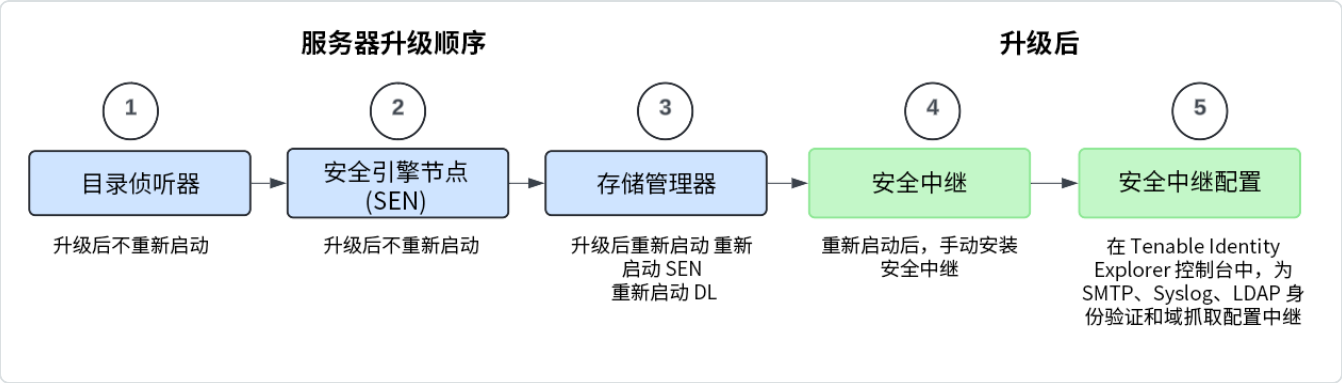
- 2.7 -> 3.1 -> 3.11 -> 3.19 -> 3.29 -> 3.42 -> 3.77。
- 3.x -> 3.59 -> 3.77。

  提示：如果您从 **v.3.59** 升级，系统会自动安装与配置安全中继。

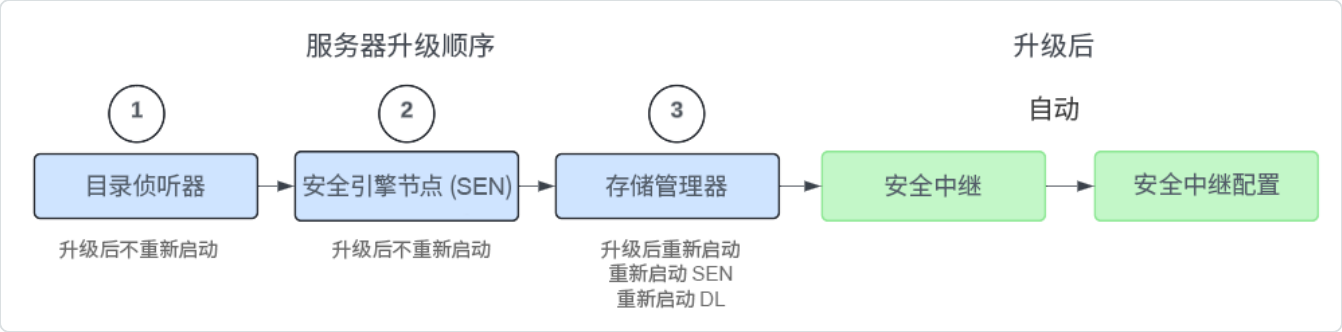
注意：您可以从任何次要版本升级到下一个主要版本。

升级顺序

- 要从 **Tenable Identity Exposure 3.42** 升级到 **3.77**，请按以下顺序操作：



- 要从 **Tenable Identity Exposure 3.59** 升级到 **3.77**，请按以下顺序操作：



事先说明

- **请确保您的 TLS 证书使用 OpenSSL 3.0.x**。有关更多信息，请参阅“部署前要求”。
- **在升级之前，为环境拍摄快照**。如果升级失败，Tenable Identity Exposure 支持部门无法执行回滚，而这会导致全新安装并造成您丢失之前的数据。请参阅“备份”，以获取完整信息。
- **备份和还原存储管理器**。Tenable 强烈建议您在升级之前备份存储管理器。有关如何备份或还原 MSSQL 的说明，请参阅 Microsoft 官方文档。
- **考虑停机时间**：根据您的环境和升级程度，停机时间从几分钟到几小时不等。请将此因素纳入您的日程安排和通信计划考虑范围中，并将计划的停机时间和可能发生的服务中断消息告知受影响的用户。

- 从 Tenable 的下载站点下载 **Tenable Identity Exposure** 和安全中继的可执行程序。
- **以本地用户或域用户(“本地管理员”组的成员)的身份运行安装程序**。
- **重新启动服务器**，然后再为每个组件启动 Tenable Identity Exposure 安装程序。

升级程序

请按照以下程序，使用“**带自动生成证书和自签名证书的 TLS(默认)**”升级 Tenable Identity Exposure 组件。有关更多信息，请参阅“TLS Installation Types”。

> **注意**：“无 TLS”的安装默认采用此模式。

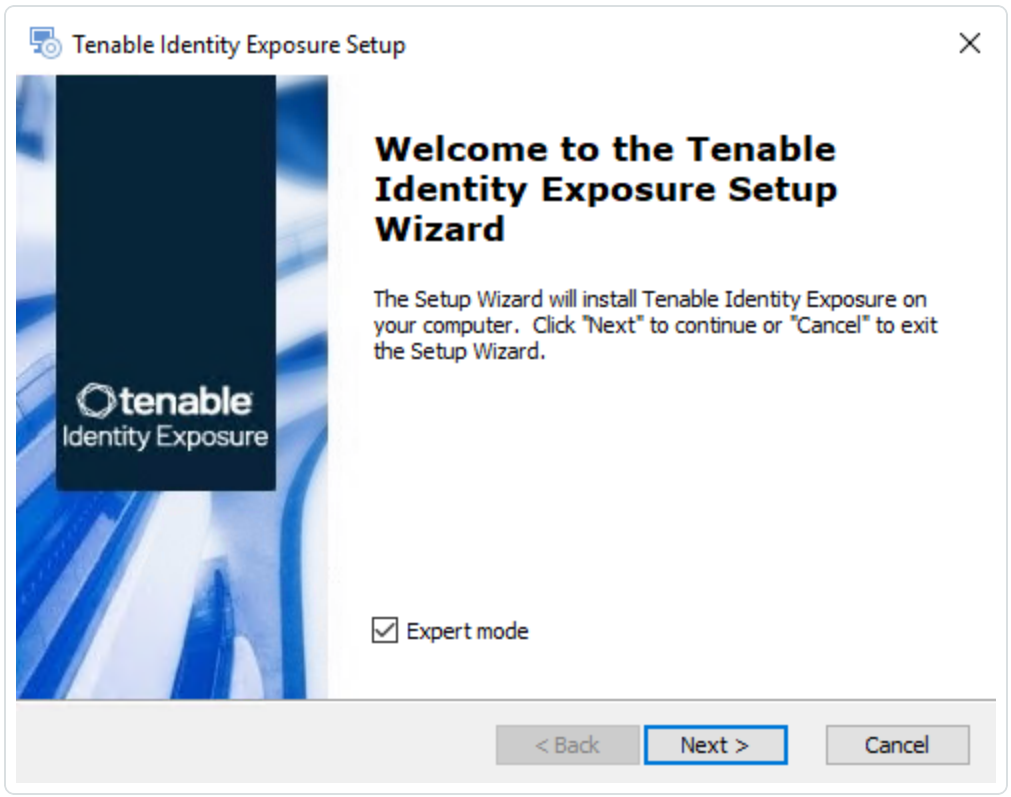
升级目录侦听器：

1. 在本地计算机上，重新启动服务器并运行 **Tenable Identity Exposure 3.77** 本地安装程序。

   出现“欢迎”屏幕。

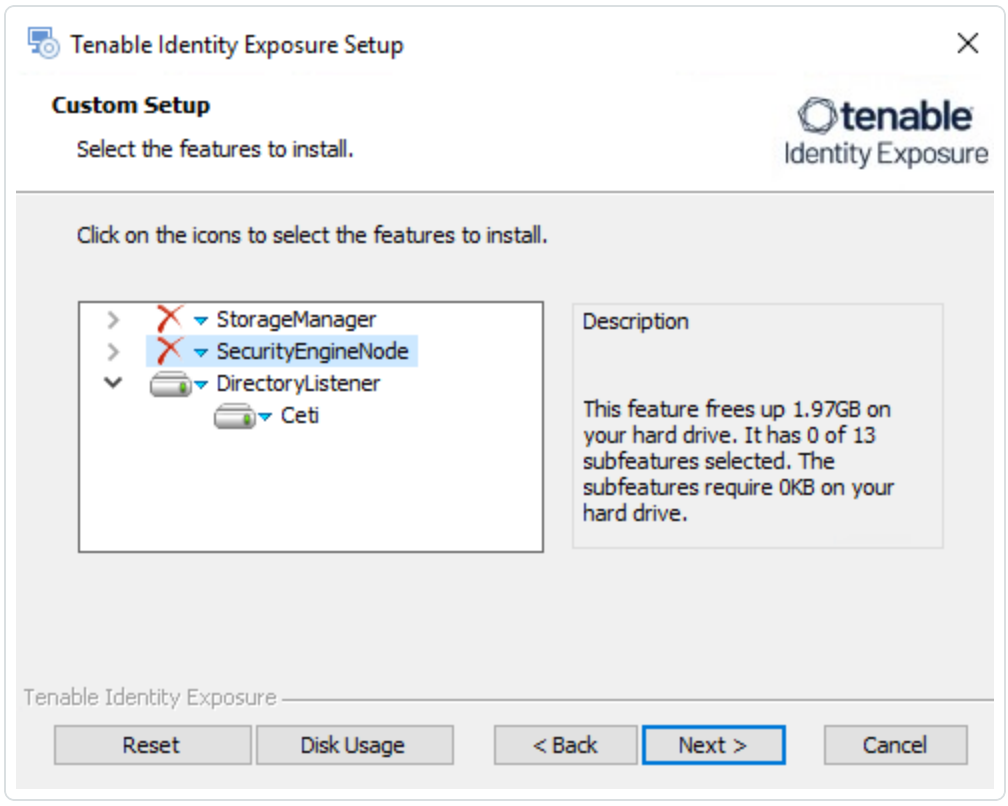
2. 在设置语言框中，从下拉列表中选择要安装的语言，然后单击“**下一步**”。

   出现“**安装向导**”。“**专家模式**”复选框为默认选中。



3. 单击“**下一步**”。

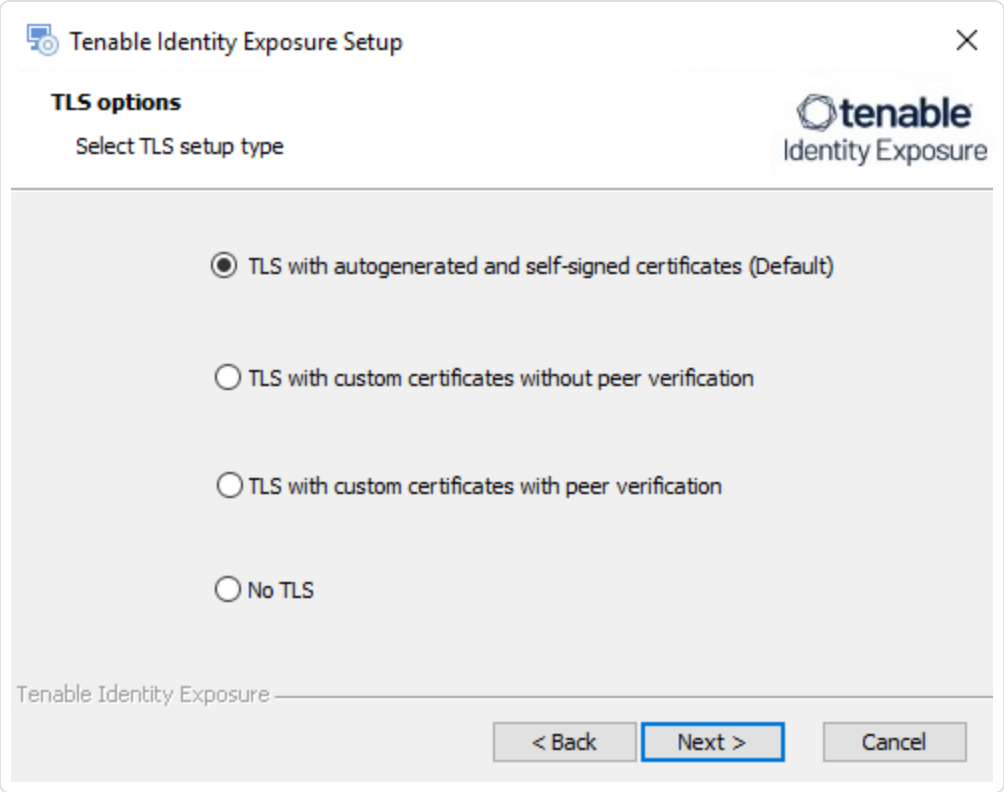
   出现“**自定义安装**”窗口。



4. 安装程序会根据之前的安装自动预选目录侦听器组件。单击“**下一步**”。

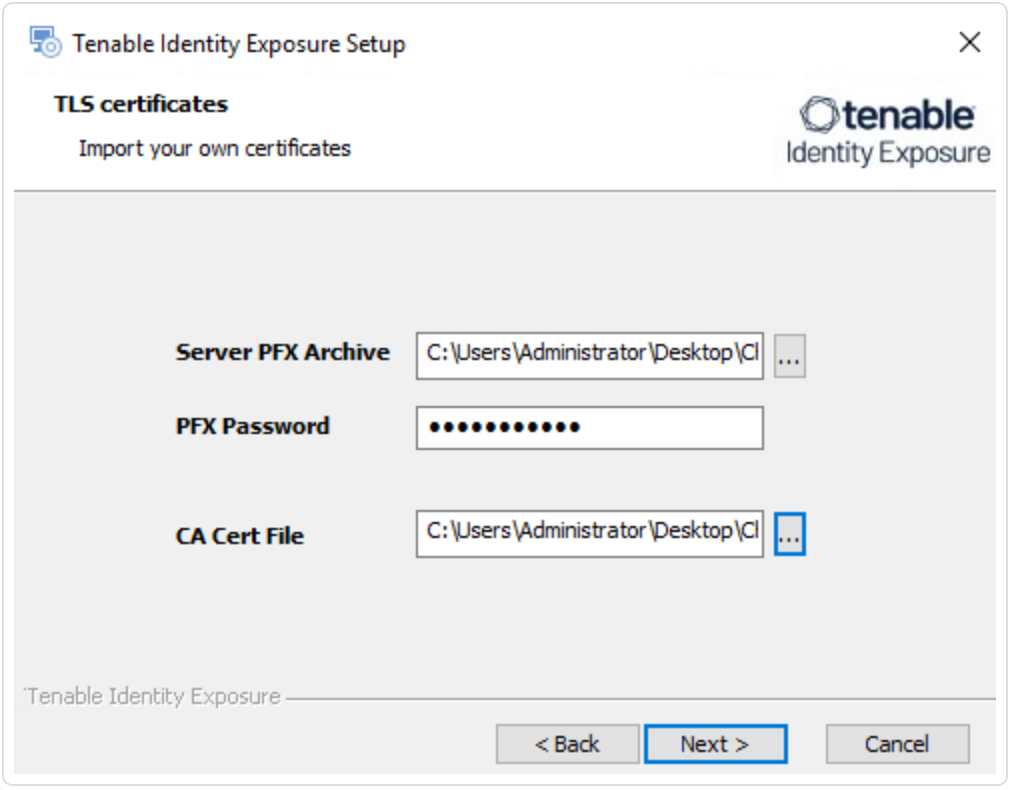
   出现“**TLS 选项**”窗口。

5. 选择“**带有自动生成证书和自签名证书的 TLS(默认)**”选项。



可选:如果您选择“**带有自定义证书的 TLS，无需对等验证**”或“**带有自定义证书的 TLS，需要对等验证**”，则下一个“**TLS 证书**”屏幕会要求您提供以下信息:

- 在“**服务器 PFX 存档**”框中，单击“**...**”以导航至“PFX 存档”。
- 在“**PFX 密码**”框中，输入 PFX 文件的密码。
- 在“**CA 证书文件**”框中，单击“**...**”以导航至 CA 证书文件。

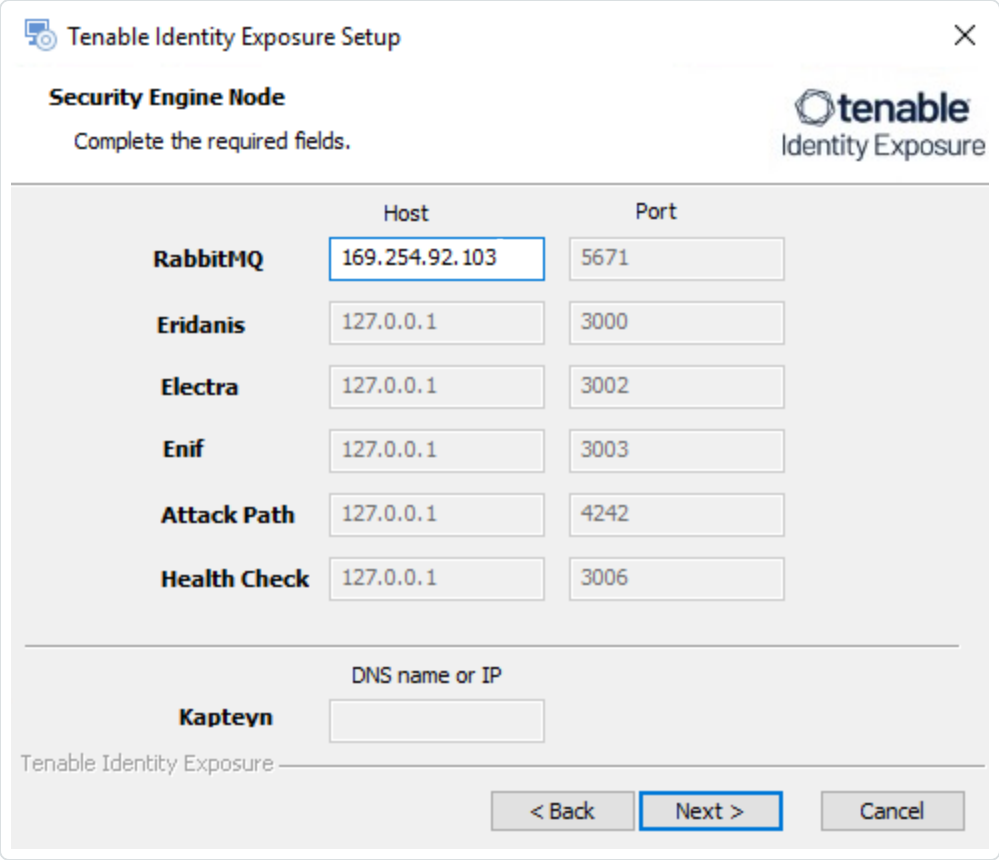


6. 单击“**下一步**”。

   出现“**安全引擎节点**”窗口。

7. 在 RabbitMQ 的“**主机**”框中，输入**安全引擎节点的 IP 地址**(或**托管 RabbitMQ 的安全引擎节点的 IP 地址**(如果使用拆分架构))。

注意:如果保留默认值"127.0.0.1"并单击"下一步",安装程序将失败并执行回滚。

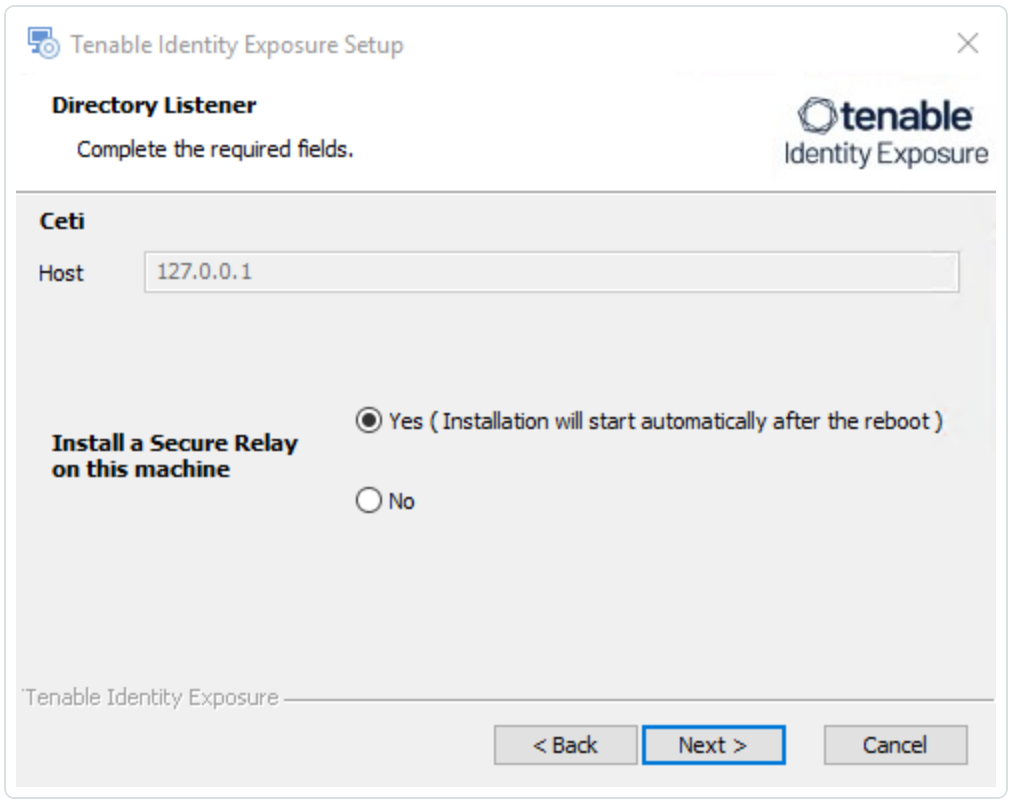


8. 单击"**下一步**"。

   出现"**目录侦听器**"窗口。

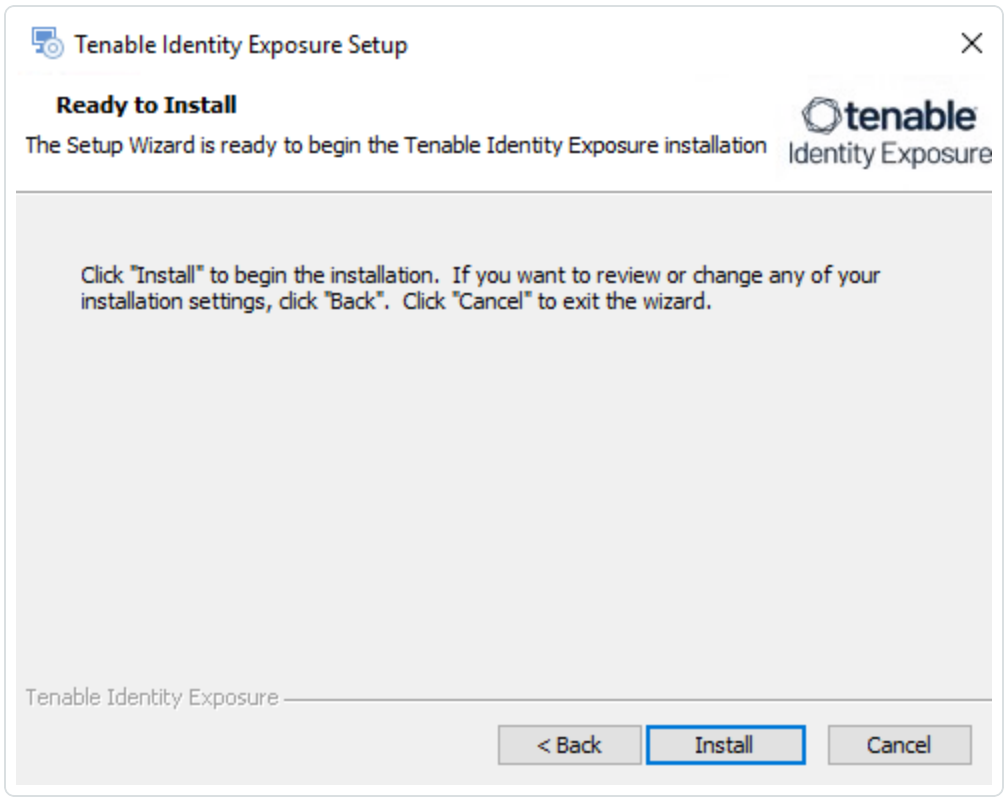
9. 有两个选项可供您选择是否在此目录侦听器上安装安全中继:

   - **是**:在此安装过程完成且目录侦听器重新启动后,安全中继安装程序便会启动。
   - **否**:您选择在以后**或在单独的服务器上**安装安全中继(请参阅"本地平台的安全中继架构")。此时会出现一条消息,其中包含安全中继安装程序所在的位置。无论是在目录侦听器计算机还是单独的计算机上,您都**必须安装安全中继**。

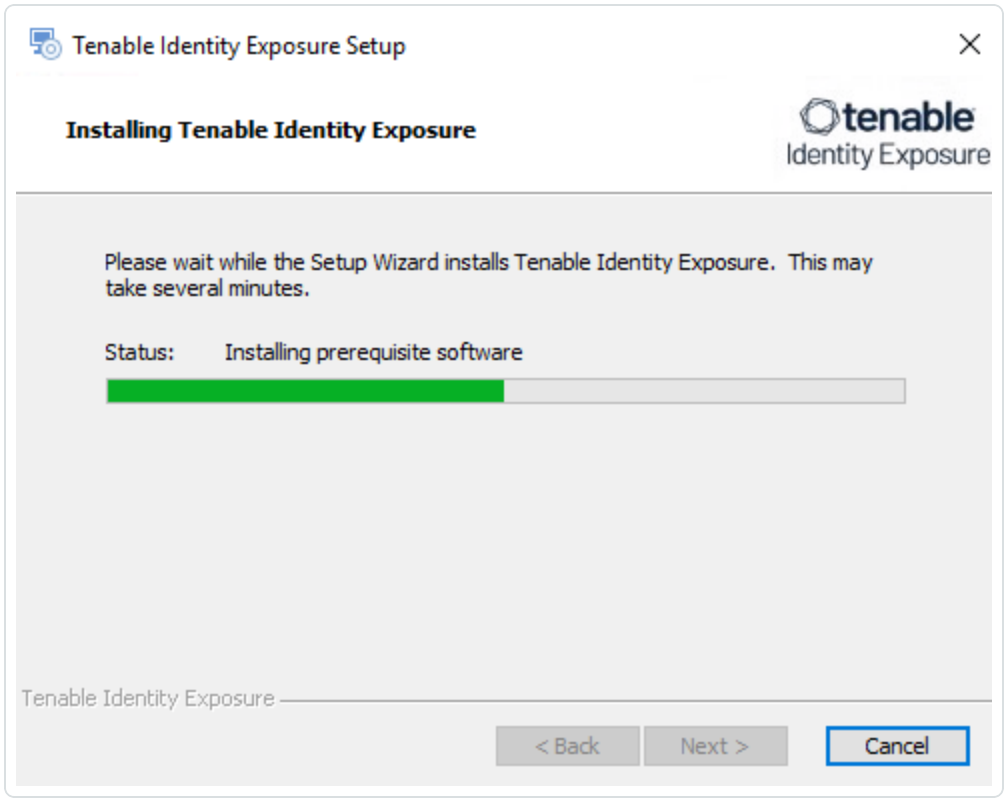


10. 单击“**下一步**”。

    出现“**准备安装**”窗口。



11. 单击“**安装**”即可开始升级。



升级完成后，会出现“**正在完成 Tenable Identity Exposure 安装向导**”窗口。

12. 单击“**完成**”。

    此时会出现一个对话框，询问是否要重新启动计算机。

13. 单击“**否**”。

    注意：暂时**不要**重新启动计算机。请在升级所有服务器后再重新启动计算机。

14. 升级安全引擎节点 (SEN)。

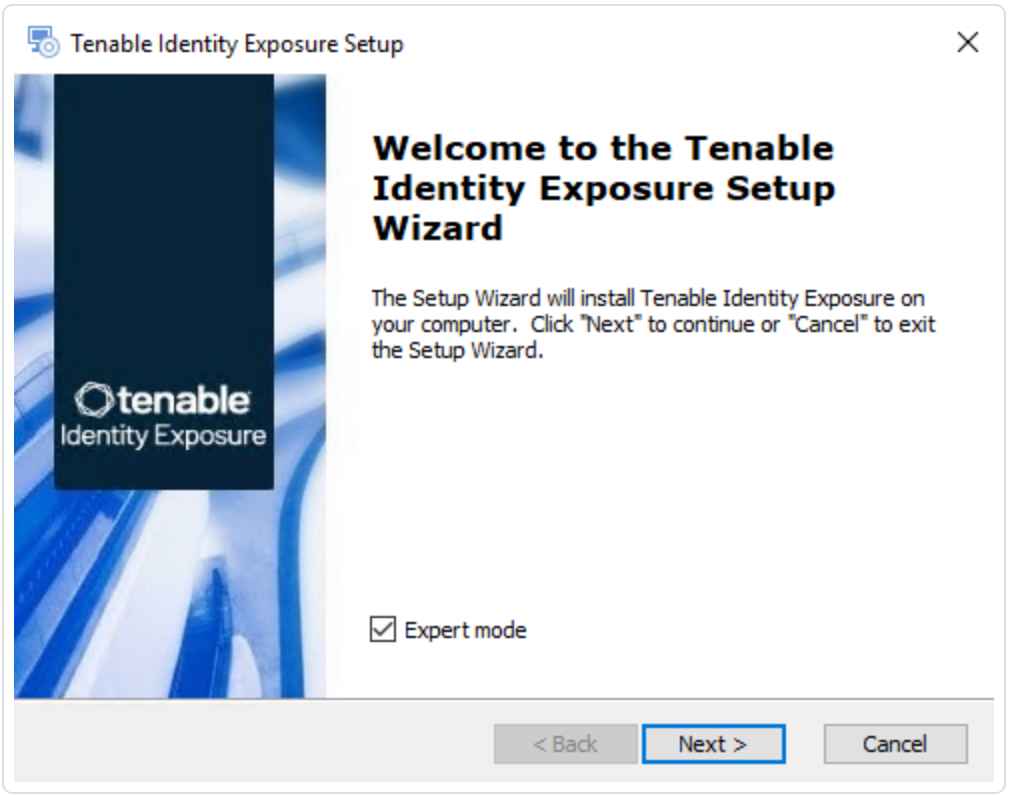
升级 SEN：

1. 在本地计算机上，重新启动服务器并运行 **Tenable Identity Exposure 3.77** 本地安装程序。

   出现“欢迎”屏幕。

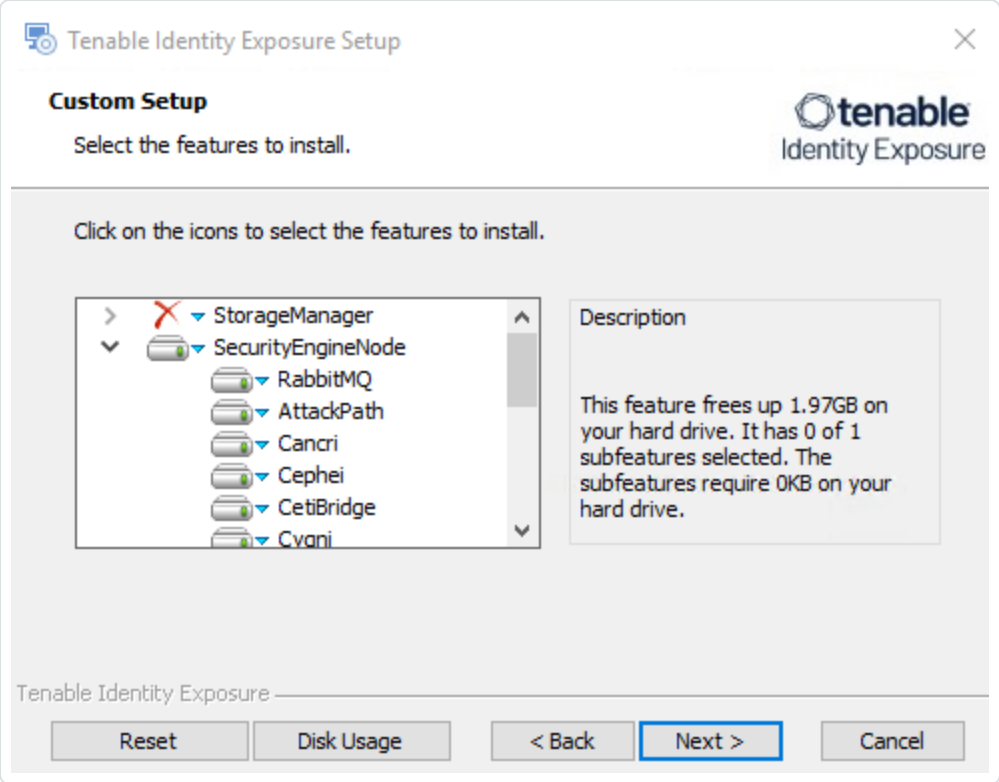
2. 在设置语言框中，单击箭头即可选择要安装的语言，然后单击“**下一步**”。

   出现“**安装向导**”。“**专家模式**”复选框为默认选中。



3. 单击“**下一步**”。

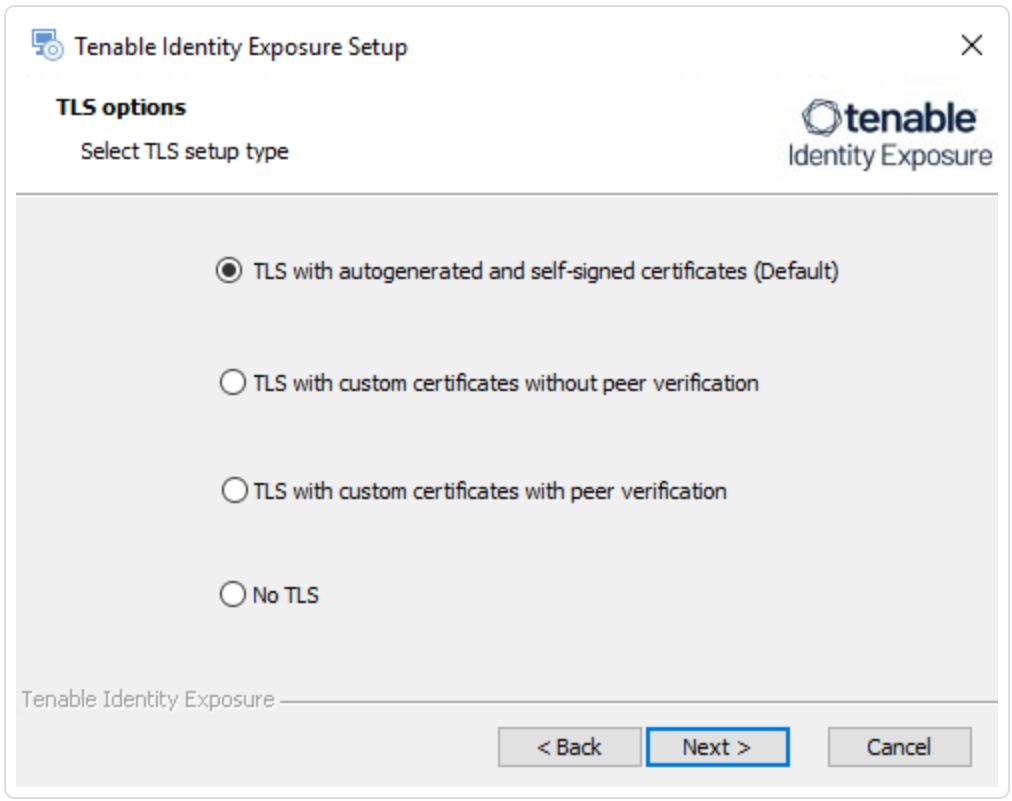
   出现“**自定义安装**”窗口。



4. 安装程序会根据之前的安装自动预选 SEN 组件。单击“**下一步**”。

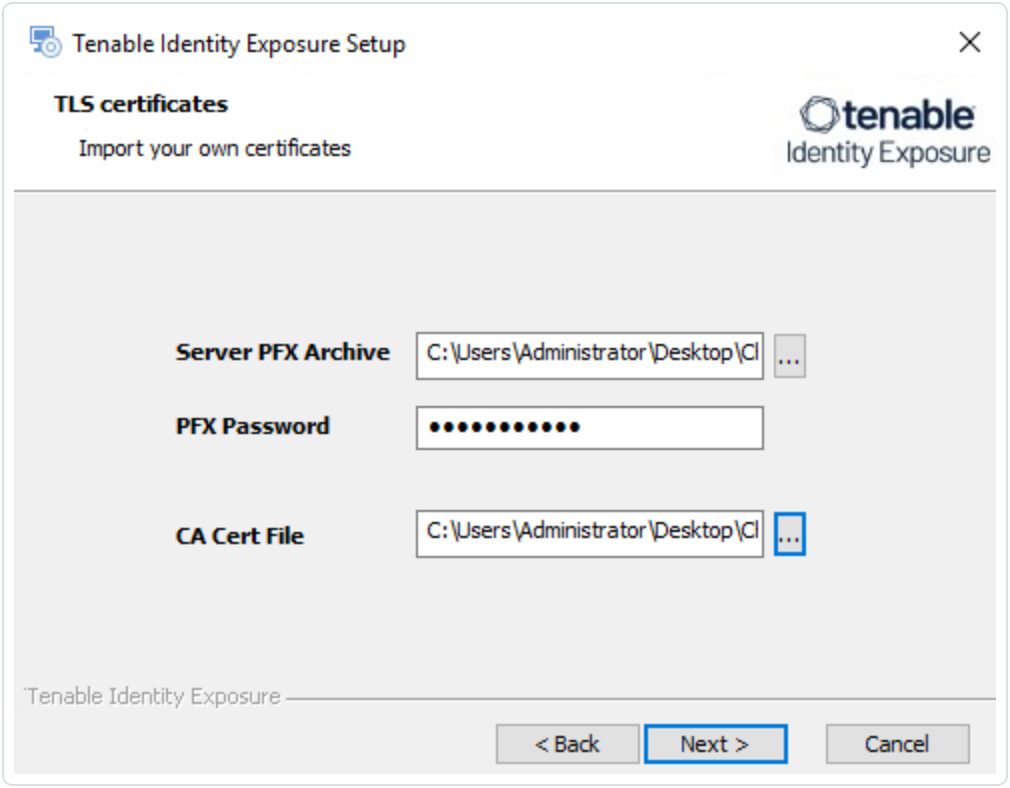
   出现“**TLS 选项**”窗口。

5. 选择“**带有自动生成证书和自签名证书的 TLS(默认)**”选项。



可选:如果您选择“**带有自定义证书的 TLS，无需对等验证**”或“**带有自定义证书的 TLS，需要对等验证**”，则下一个“**TLS 证书**”屏幕会要求您提供以下信息:

- 在“**服务器 PFX 存档**”框中，单击“**...**”以导航至“PFX 存档”。
- 在“**PFX 密码**”框中，输入 PFX 文件的密码。
- 在“**CA 证书文件**”框中，单击“**...**”以导航至 CA 证书文件。



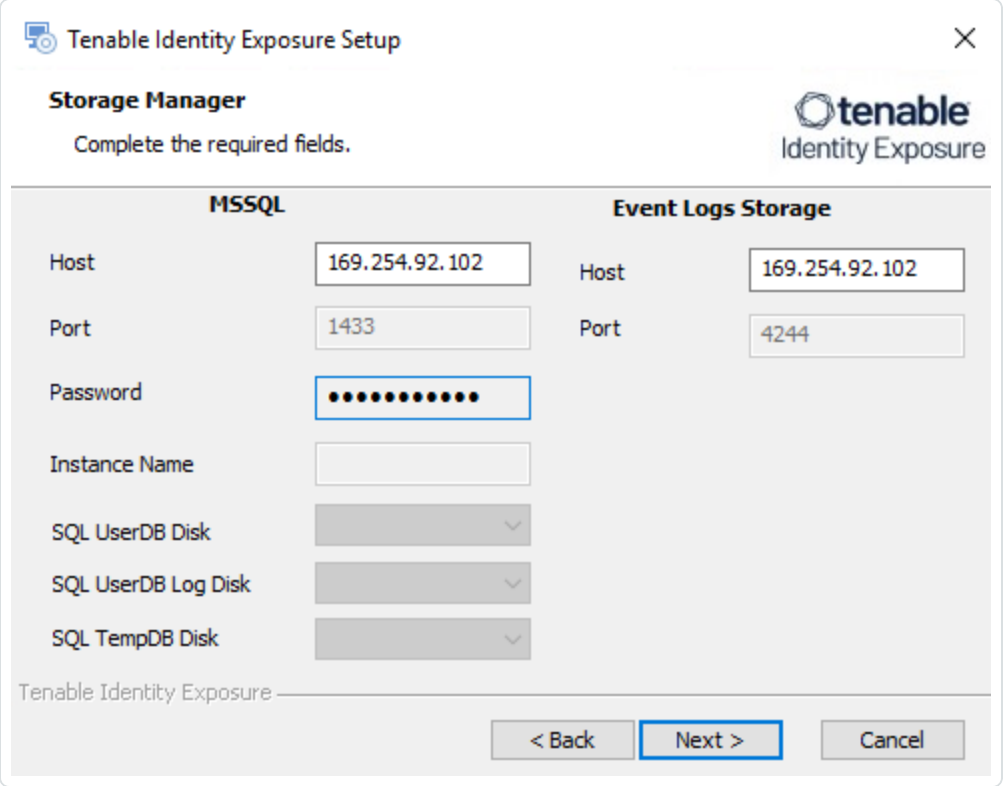
6. 单击“**下一步**”。

   出现“**存储管理器**”窗口。

7. 验证或输入以下信息：

   - 在“**主机**”框中，检查以前安装的 MSSQL 数据库的 FQDN 或 IP 地址是否仍然有效，并根据需要予以更正。
   - 在“**事件日志存储**”框中，输入存储事件日志的计算机的 IP 地址，该地址通常与 MSSQL 数据库的 IP 地址相同。

   注意：如果您在上次安装后更改了 SA 密码，则安装程序会要求您遵循 SQL 服务器强密码中所述的语法规范。

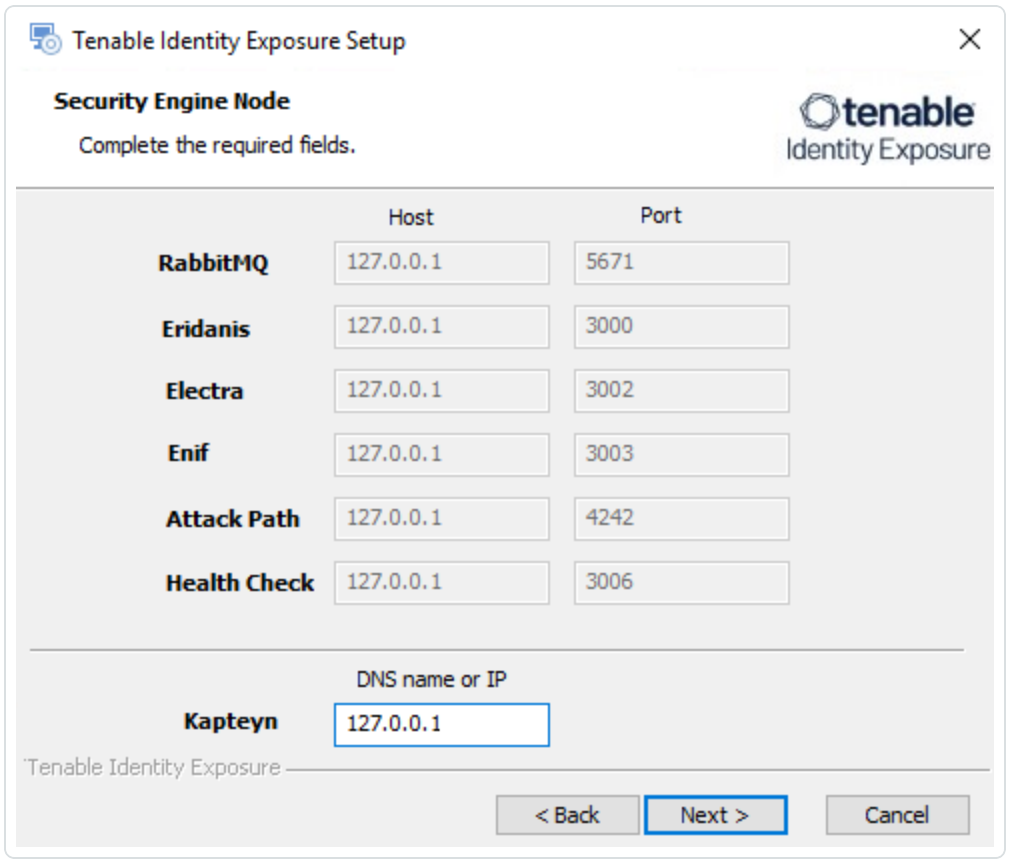


注意:切记在此步骤中更新事件日志存储 IP 或主机名地址,否则会导致攻击检测问题。如果您已成功完成此屏幕中的设置并升级了 SEN,则必须将 `TENABLE_CASSIOPEIA_CYGNI_Service__EventLogsStorage__Host` 和 `TENABLE_CASSIOPEIA_EVENT_LOGS_DECODER_Service__EventLogsStorage__Host` 的环境变量从**当前值**更新为 **<存储管理器主机名或 IP 地址>** 的准确值。有关更多信息,请参阅"故障排除知识库文章"。

8. 单击"**下一步**"。

   出现"**安全引擎节点**"窗口。

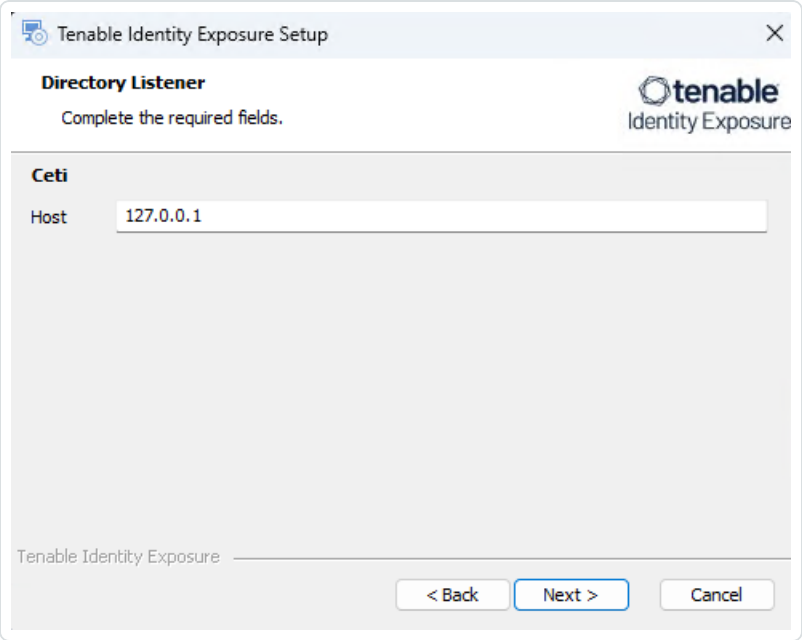
9. 在"**DNS 名称或 IP**"框中,安装程序会显示最终用户为了访问上次安装的 Tenable Identity Exposure 而输入的 Web 服务器的 DNS 名称(首选)或 IP 地址。如有必要,请检查名称或地址是否仍然正确有效。



10. 单击“**下一步**”。

    出现“**目录侦听器**”窗口。

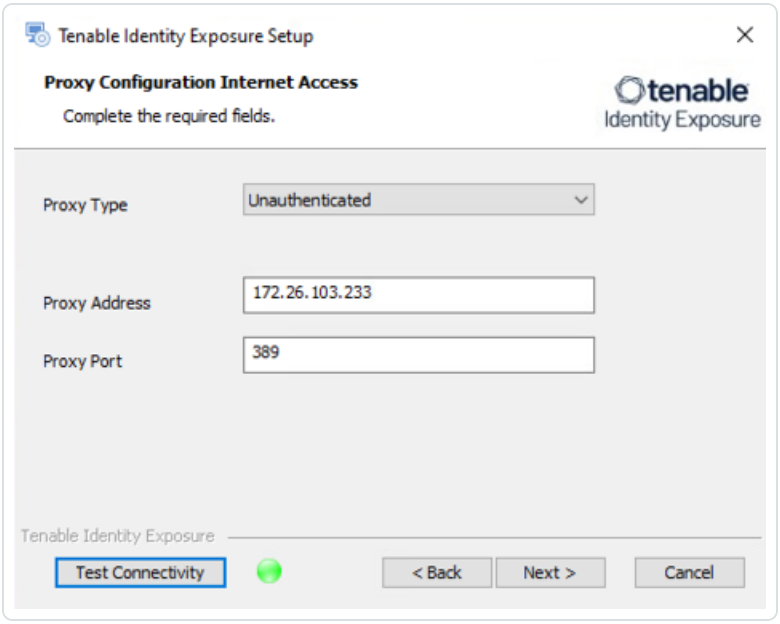
11. 在“**Ceti**”框中，输入**目录侦听器的 IP 地址**。



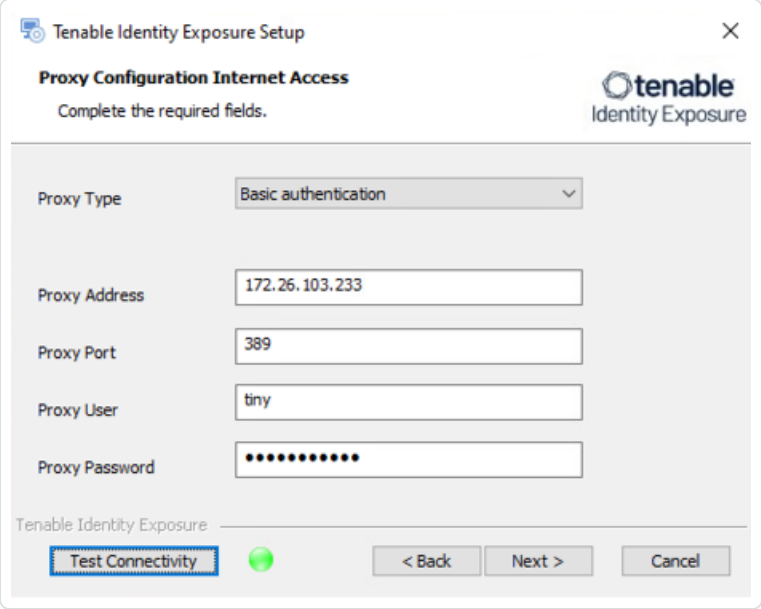
此时会出现“**代理配置**”窗口。

12. 有以下代理类型可供选择：

    - **无**：从下拉列表框中选择“无”，然后单击“**下一步**”。
    - **未经身份验证**：从下拉列表框中选择“未经身份验证”。
        - 在“**代理地址**”和“**代理端口**”框中，输入代理服务器的地址和端口。

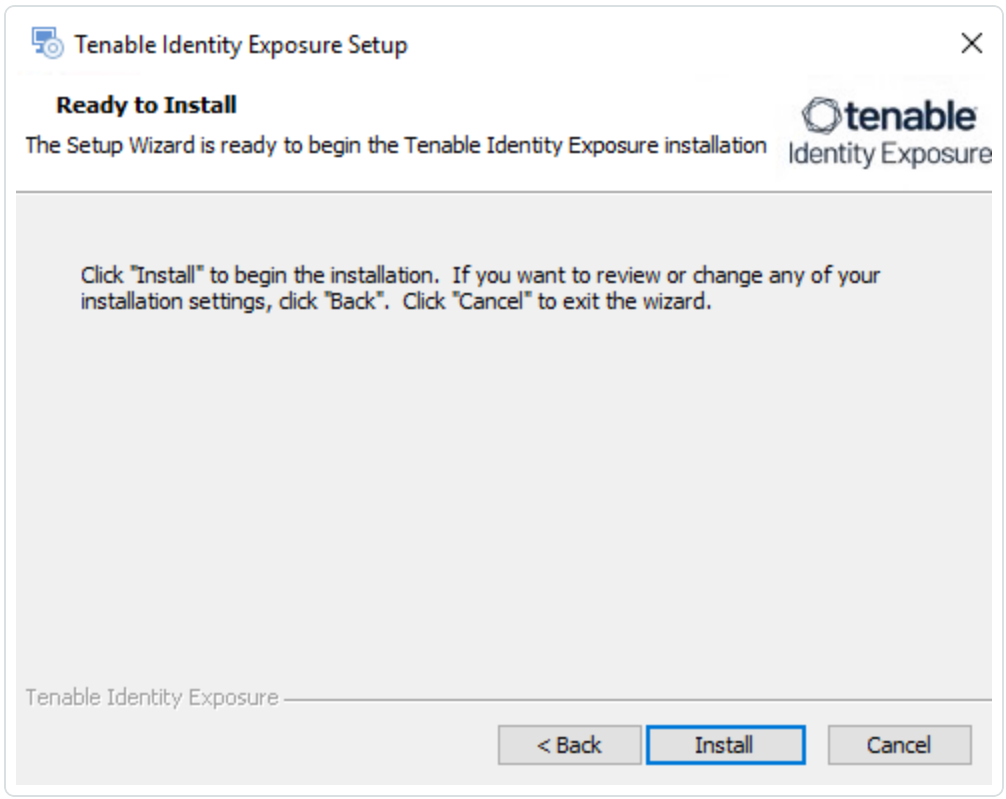


- **基本身份验证**：从下拉列表框中选择“基本身份验证”。
  - 在“**代理地址**”和“**代理端口**”框中，输入代理服务器的地址和端口。
  - 在“**代理用户**”和“**代理密码**”框中，输入被授权访问代理服务器的特定用户帐户的名称以及相关的凭据，以允许通过代理服务器发送请求。

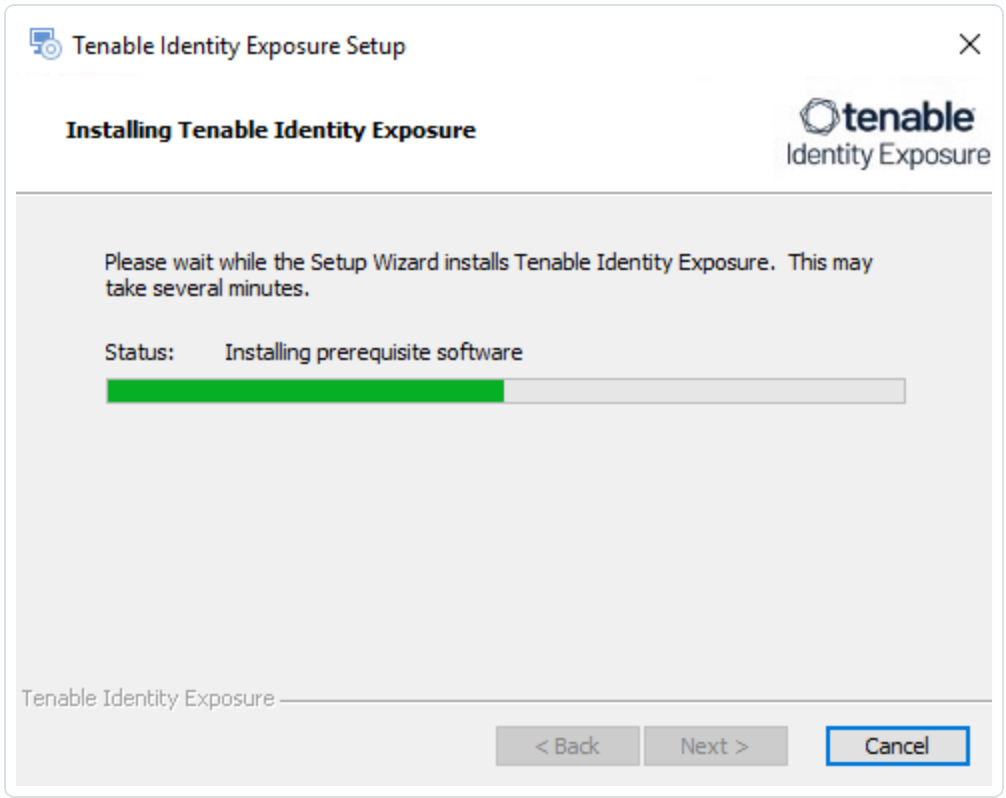


13. 单击“**测试连接**”。
14. 单击“**下一步**”。

    出现“**准备安装**”窗口。



15. 单击“**安装**”即可开始升级。



升级完成后，会出现“**正在完成 Tenable Identity Exposure 安装向导**”窗口。

16. 单击“**完成**”。

    此时会出现一个对话框，询问是否要重新启动计算机。

17. 单击“**否**”。

    注意：暂时**不要**重新启动服务器。请在升级所有服务器后再重新启动计算机。

18. 升级存储管理器。

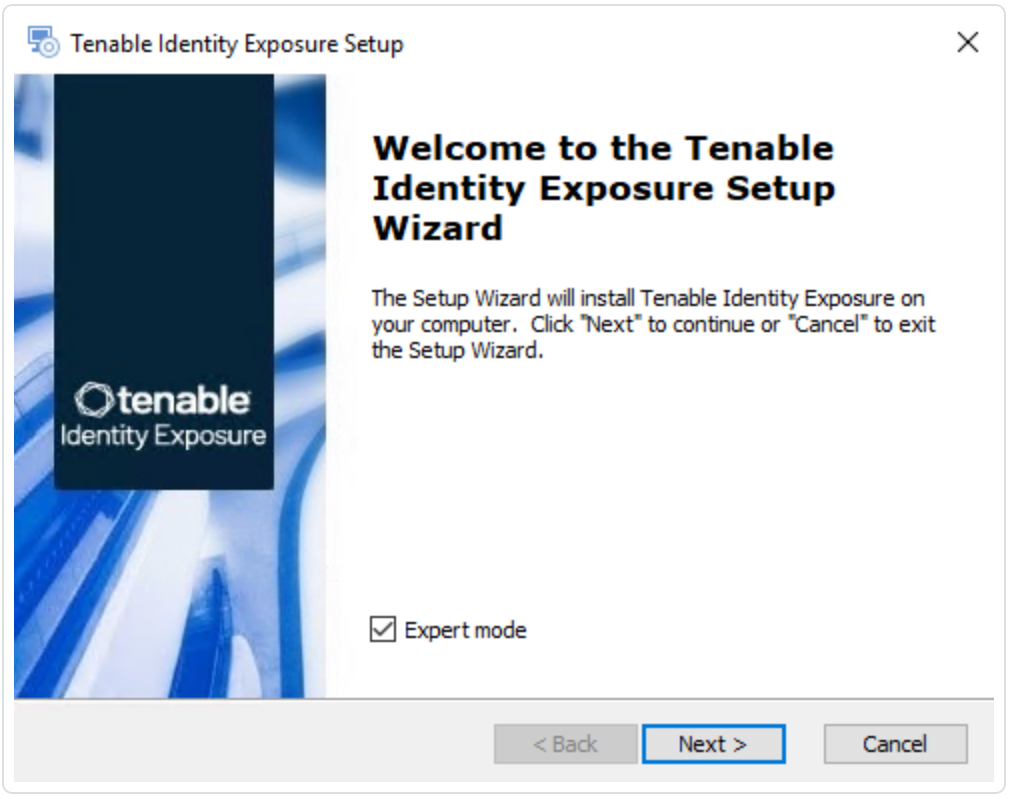
升级存储管理器：

1. 在本地计算机上，重新启动服务器并运行 **Tenable Identity Exposure 3.59** 本地安装程序。

   出现“欢迎”屏幕。

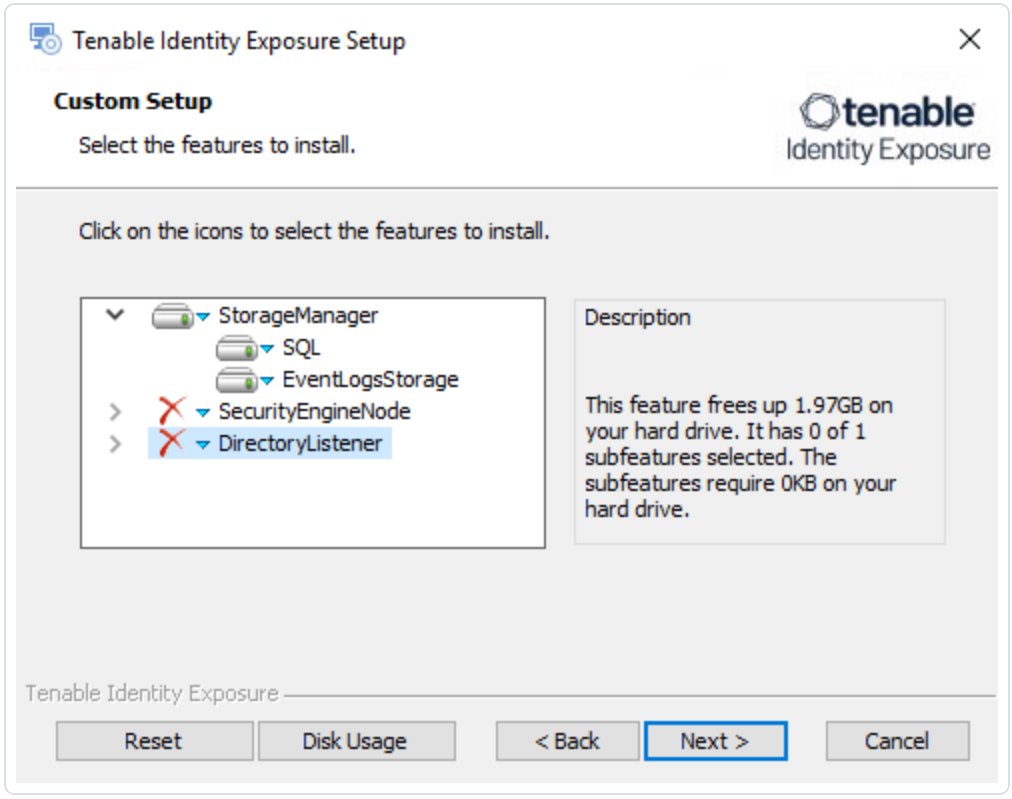
2. 在设置语言框中，单击箭头即可选择要安装的语言，然后单击“**下一步**”。

   出现“**安装向导**”。“**专家模式**”复选框为默认选中。



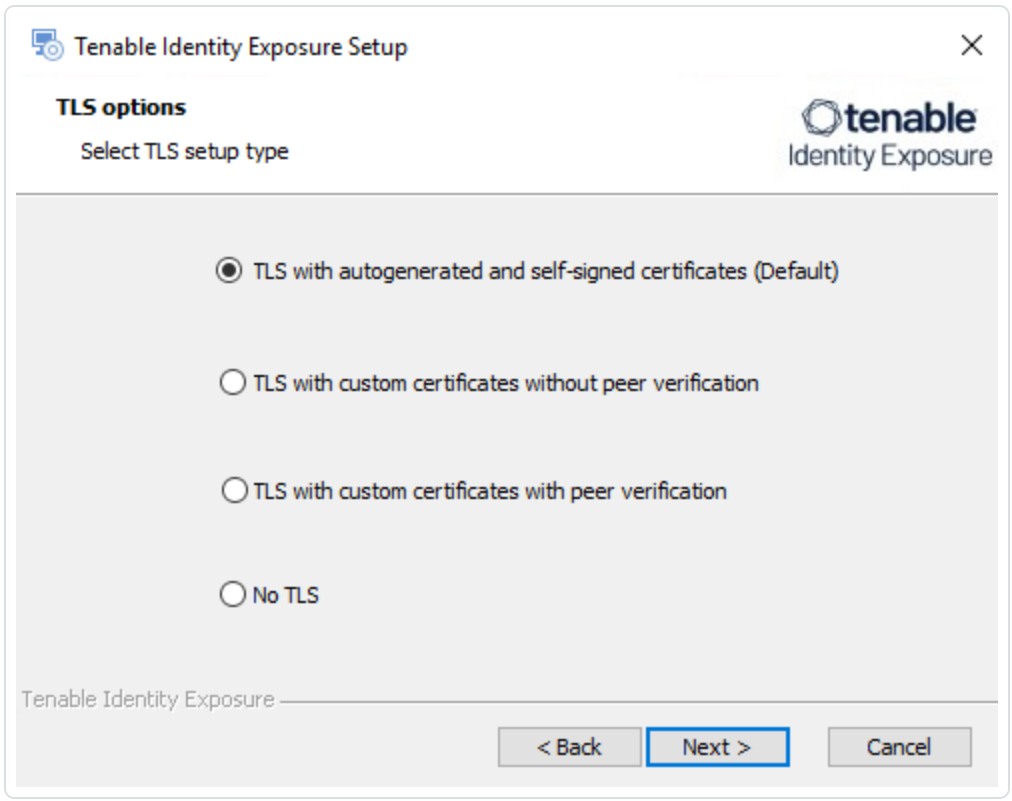
3. 单击“**下一步**”。

   出现“**自定义安装**”窗口。安装程序会根据之前的安装自动预选存储管理器组件。



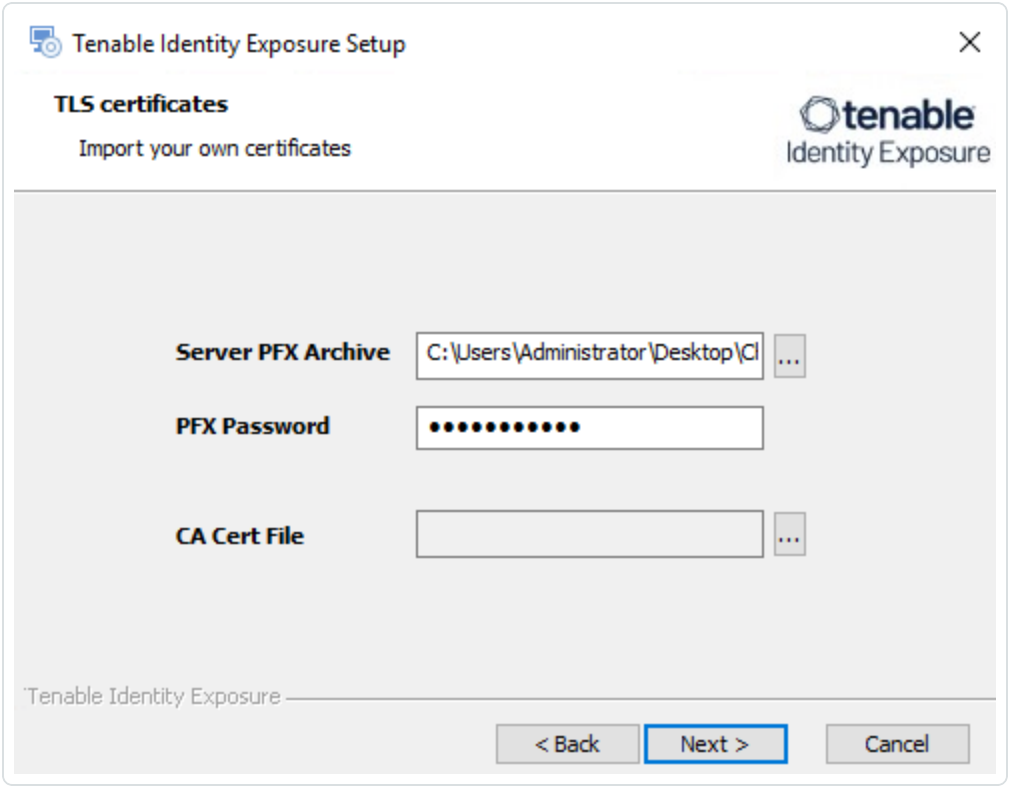
4. 单击“**下一步**”。
5. (可选)单击“**浏览**”,以更改安装文件夹位置。仅更改驱动器号。

   出现“**TLS 选项**”窗口。
6. 选择“**带有自动生成证书和自签名证书的 TLS(默认)**”选项。



可选：如果您选择“**带有自定义证书的 TLS，无需对等验证**”或“**带有自定义证书的 TLS，需要对等验证**”，则“**TLS 证书**”屏幕会要求您提供以下信息：

- 在“**服务器 PFX 存档**”框中，单击“**...**”以导航至“PFX 存档”。
- 在“**PFX 密码**”框中，输入 PFX 文件的密码。

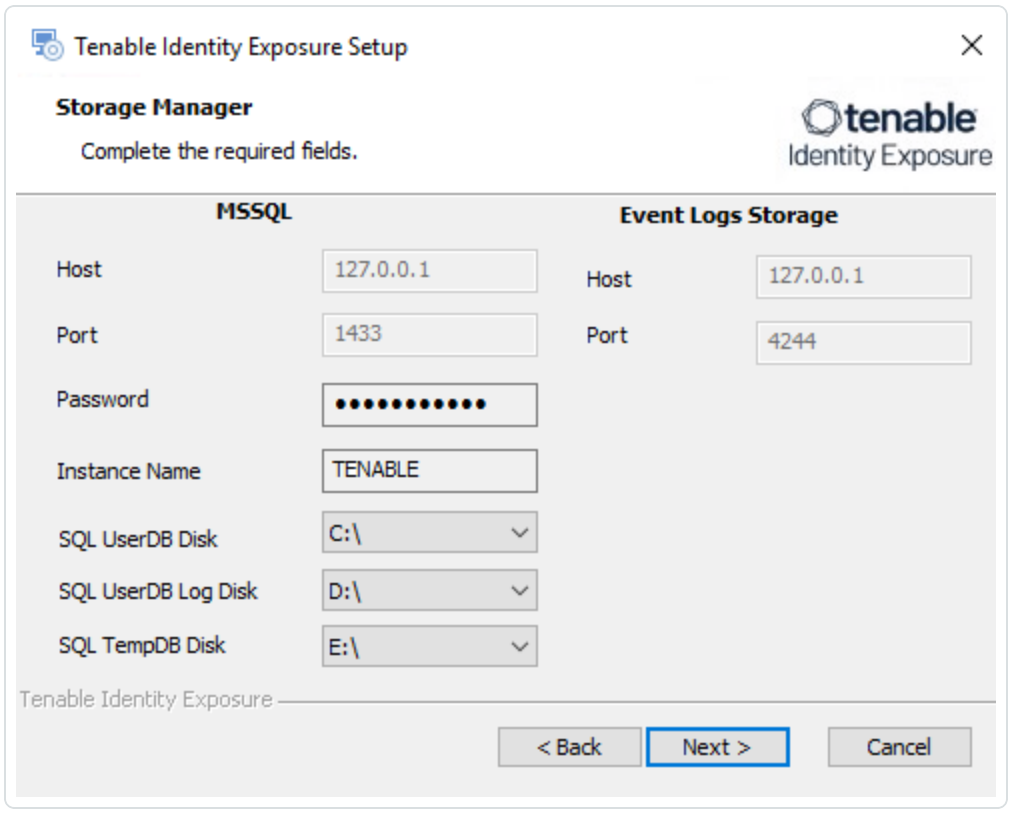


7. 单击“**下一步**”。

   出现“**存储管理器**”窗口。

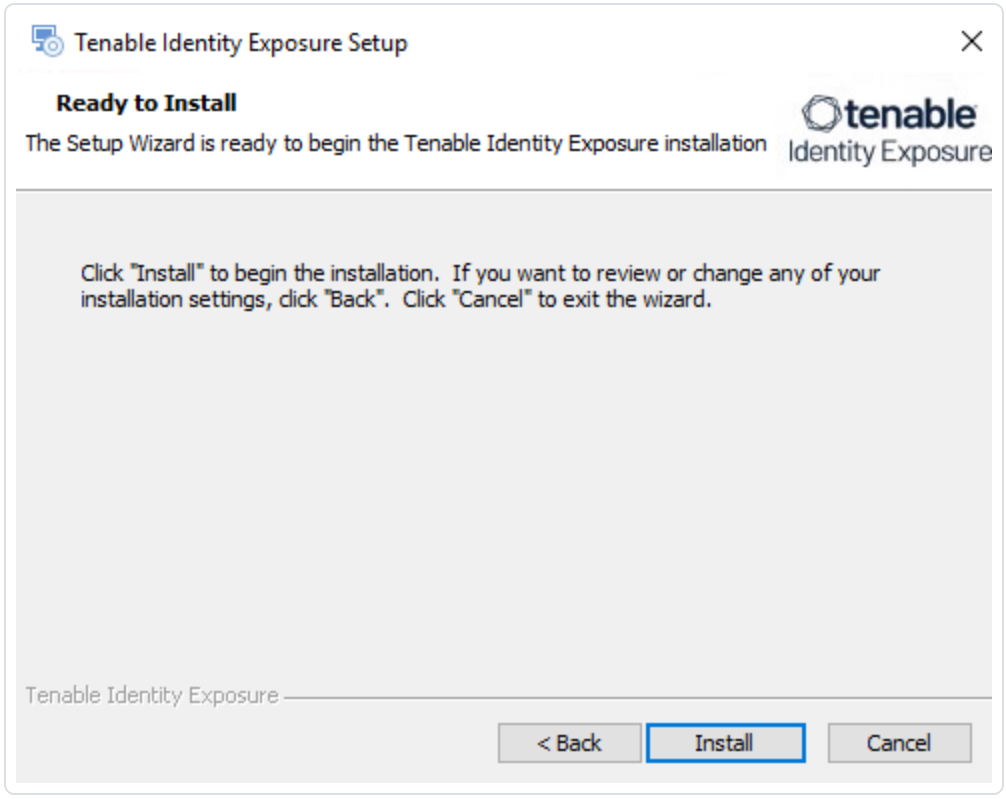
8. 安装程序会再次使用以前安装的信息。单击“**下一步**”。

   注意：如果您在上次安装后更改了 SA 密码，则安装程序会要求您遵循 SQL 服务器强密码中所述的语法规范。

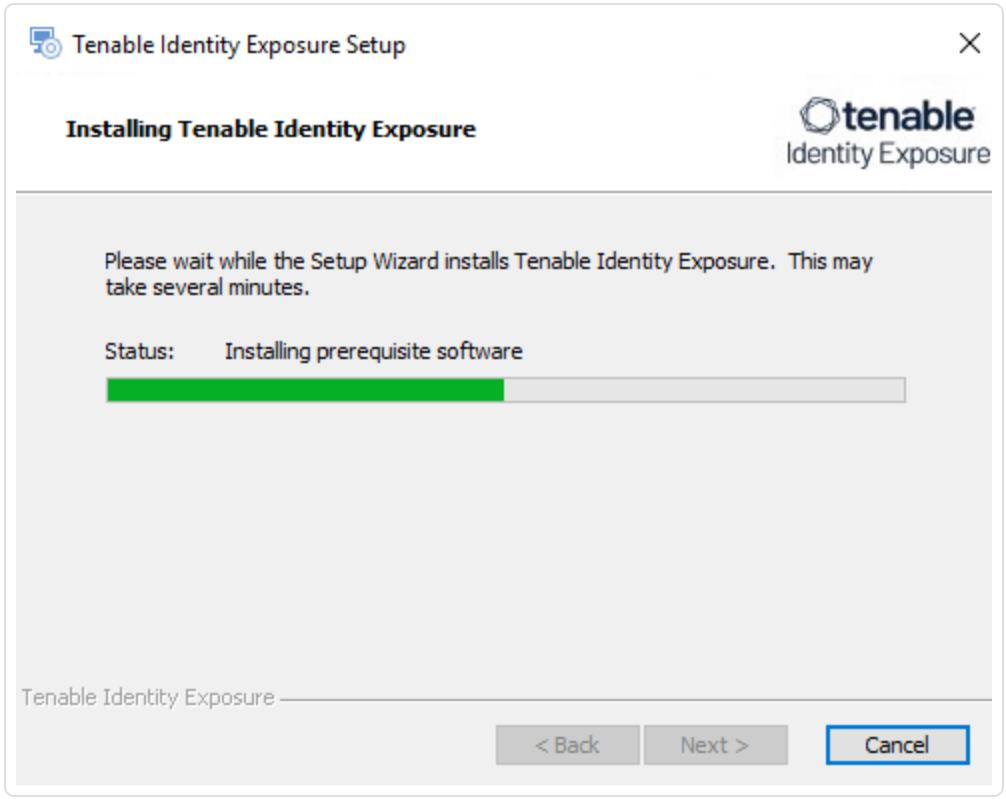

Tenable Identity Exposure Setup
Storage Manager
Complete the required fields.
tenable
Identity Exposure
MSSQL
Event Logs Storage
Host
127.0.0.1
Port
1433
Password
Instance Name
TENABLE
SQL UserDB Disk
C:\
SQL UserDB Log Disk
D:\
SQL TempDB Disk
E:\
Host
127.0.0.1
Port
4244
Tenable Identity Exposure
< Back
Next >
Cancel

9. 单击“**下一步**”。

   出现“**准备安装**”窗口。



10. 单击“**安装**”即可开始升级。



升级完成后，会出现“**正在完成 Tenable Identity Exposure 安装向导**”窗口。

11. 单击“**完成**”。

此时会出现一个对话框，询问是否要重新启动计算机。

12. 单击“**是**”。

计算机重新启动。

13. 重新启动 SEN。
14. 重新启动 DL。
15. 使用单独的安装程序安装 适用于 Tenable Identity Exposure 3.77 的安全中继。

若要安装安全中继，请执行以下操作：

1. 查看安全中继要求。
2. 选择 本地平台的安全中继架构。

3. 安装 适用于 Tenable Identity Exposure 3.77 的安全中继。

备份

定期且可靠的备份对于确保 Tenable Identity Exposure 应用程序内数据的可用性和完整性至关重要。

目的

- **缓解数据丢失**:在指定的场景中执行备份,以缓解升级、更新或系统更改期间的数据丢失风险。
- **确保顺利恢复**:如果在系统修改期间出现意外问题,拥有备份可确保恢复过程顺利。

> **提示**:定期监控备份过程,以确保其有效性;对还原过程执行定期测试,以确认备份数据的完整性及其促进系统成功恢复的作用。

> **提示**:执行备份时,无需停止应用程序服务。

备份类型

以下方法可确保备份策略安全、高效且符合组织政策。

- 将图像备份(快照)用作为您环境中的首选方法。
- 确保备份整个系统状态,包括应用程序配置、数据库和相关文件。

MSSQL 备份

请参阅 Microsoft 的说明文档。

备份频率

至少每个月执行一次常规备份,以捕获最新的数据更改和配置。

安排在非高峰时间进行备份,尽量减少对系统性能和用户体验的影响。

对于 MSSQL,至少每周执行一次常规备份,以捕获最新数据。

> **注意**:无需备份 SQL 日志。

备份场景

- **Tenable Identity Exposure 版本升级**：对 Identity Exposure 应用程序发起任何版本升级之前，请执行可靠的备份。
- **操作系统升级或重要更新**：执行任何操作系统升级或对主机系统应用重要更新之前，确保进行可靠的备份。
- **Tenable Identity Exposure 主机的硬件/操作系统发生变化**：对 Identity Exposure 主机的硬件或操作系统配置进行任何修改之前，请进行完整的备份。
- **Tenable 支持部门建议的修改**：在实施 Tenable 支持部门建议的任何更改或修改之前，请根据需要执行备份，以实现最佳系统性能。

重新启动服务

完成存储管理器、安全引擎节点和目录侦听器**安装或升级后**，您可以重新启动服务。

重新启动序列

服务的重新启动顺序视其是安装还是升级而异：

- **新安装**：目录侦听器 - 安全引擎节点 - 存储管理器
- **升级**：存储管理器 - 安全引擎节点 - 目录侦听器

存储管理器

重新启动存储管理器计算机：

1. 在安装程序出现提示时，单击“**是**”。
2. 检查这些存储管理器服务是否正在运行：
    - SQL 服务器 (Tenable)
    - SQL 服务器代理 (Tenable)
    - `tenable_EventlogStorage1`

安全引擎节点

数据库必须处于运行状态，然后您才能重新启动安全引擎节点 (SEN) 服务。

重新启动 SEN 计算机：

1. 在安装程序出现提示时，单击“**是**”。
2. 如果您有多台 SEN 计算器，请按以下顺序重新启动这些计算机：
    1. RabbitMQ
    2. 其他（Eridanis、Kapteyn 等）
    3. Cancri、EventLogsDecoder
    4. Cygni

3. 检查以下 SEN 服务是否正在运行：
    - tenable_AttackPath1
    - tenable_Cancri
    - tenable_Cephei
    - tenable_CetiBridge
    - tenable_Cygni
    - tenable_Electra
    - tenable_Eltanin
    - tenable_Enif
    - tenable_Eridanis
    - tenable_EventLogsDecoder1
    - tenable_HealthCheck
    - tenable_Kapteyn
    - Rabbitmq
    - 万维网出版服务

目录侦听器

数据库和安全引擎节点必须处于运行状态，然后您才能重新启动目录侦听器服务。

重新启动目录侦听器服务：

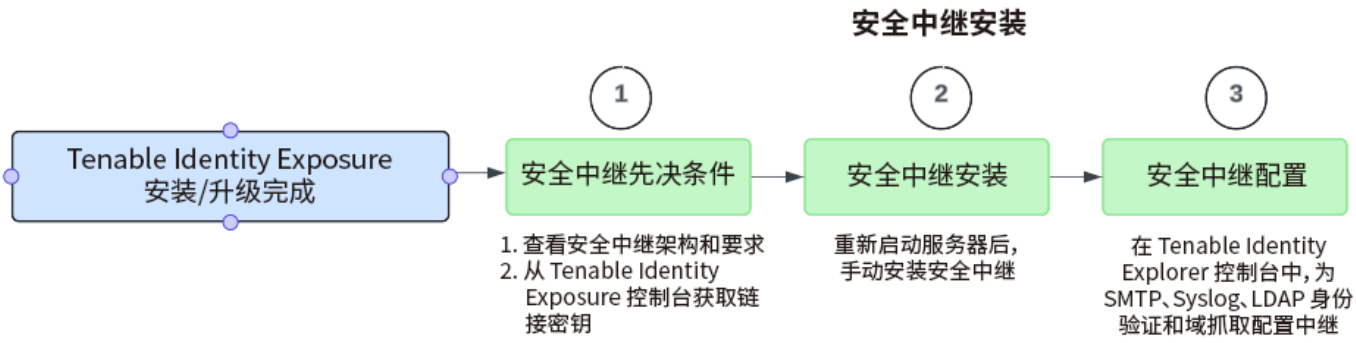
1. 在安装程序出现提示时，单击“**是**”。
2. 检查以下目录侦听器服务是否正在运行：
    - Tenable_ceti
    - tenable_envoy_server
    - tenable_envoy
    - tenable_relay

适用于 Tenable Identity Exposure 3.77 的安全中继

只有在安装或升级 Tenable Identity Exposure 之后，您才能安装安全中继组件。

自 3.59 版本起，**安全中继**组件将接管 Tenable Identity Exposure 平台中的指定任务：

- 允许您配置域，以便安全中继从域中将数据转发到收集 AD 对象的目录侦听器 (DL) 组件。
- 通过自动更新，促进大型基础设施设置和维护：不再需要使用要求同时升级的多个 DL。
- 充当单个 DL 和各种端点（例如，域控制器、SMTP 或 SYSLOG 服务器或者用于产品内身份验证的 LDAP 服务器）之间的桥梁。
- 绑定至一个或多个域。DL 可以管理数量不限的中继。
- 要求在 Tenable Identity Exposure 控制台中进行配置，例如命名和映射（域、SMTP、SYSLOG、LDAP 身份验证）。
- 支持**在 DL 服务器上安装安全中继**或**将安装中继与 DL 分开安装**的选项。
- 支持Split Security Engine Node (SEN) Services.



事先说明

请按照以下指南安装或升级含安全中继的 Tenable Identity Exposure 3.59：

1. 查看 本地平台的安全中继架构 和 Secure Relay Requirements。

2. 版本 3.59 **仅支持安装一个 DL**。升级目录侦听器 (DL) 时：

    - **仅保留一个 DL**，您可以选择在其中安装一个中继。如果选择此选项，请**同时满足 DL 和中继的必要资源要求**。有关更多信息，请参阅“资源规格”。
    - 您必须**至少拥有一个中继**。如果未在 DL 上安装中继，则必须配置新计算机以安装此中继。
    - 或者，如果您之前使用过多个 DL，请安装中继以替换其他 DL。

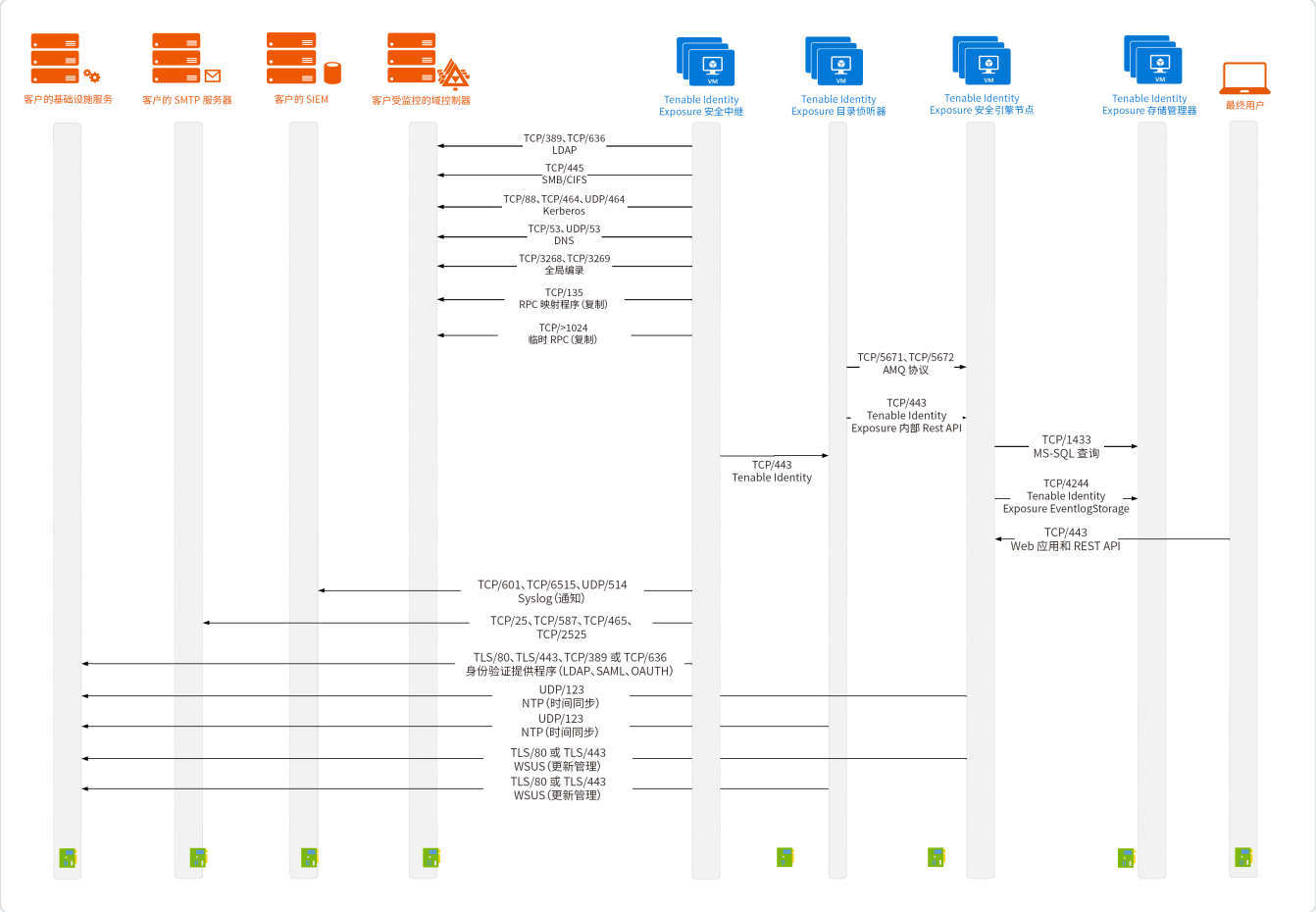
      有关更多信息，请参阅“本地平台的安全中继架构”。

3. **网络要求**：

    - 在之前和当前版本中，DL 均使用 AMQP(S) 协议直接与 SEN 通信。
    - 在版本 3.59 中，中继取代了多个 DL，通过 HTTPS 与唯一剩下的 DL 通信。
    - Envoy 是反向代理。

使用安全中继的本地平台的网络流

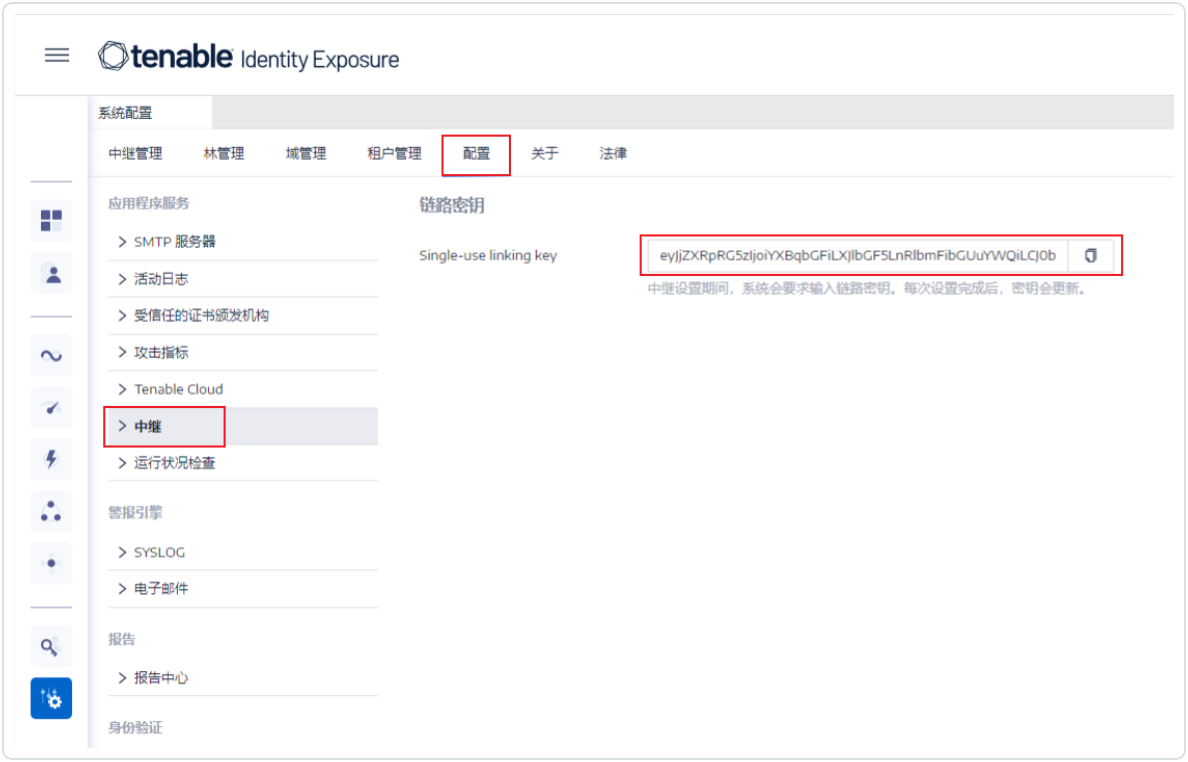
以下是使用安全中继的本地平台的网络流：



4. **链接密钥**:安装安全中继需要使用包含网络地址和身份验证令牌的一次性链接密钥。Tenable Identity Exposure 每次成功安装安全中继后都会重新生成新密钥。

   检索链接密钥:

   1. 在 Tenable Identity Exposure 控制台中,单击左侧菜单栏上的"**系统**",然后依次选择"**配置**"选项卡 >"**中继**"。



2. 单击 以复制链接密钥。

5. **角色权限**：您必须是拥有角色权限的用户才能配置中继。所需的权限如下：
   - **数据实体**：实体中继
   - **界面实体**：
     - 管理 > 系统 > 配置 > 应用程序服务 > 中继
     - 管理 > 系统 > 中继管理

   有关更多信息，请参阅“Set Permissions for a Role”。

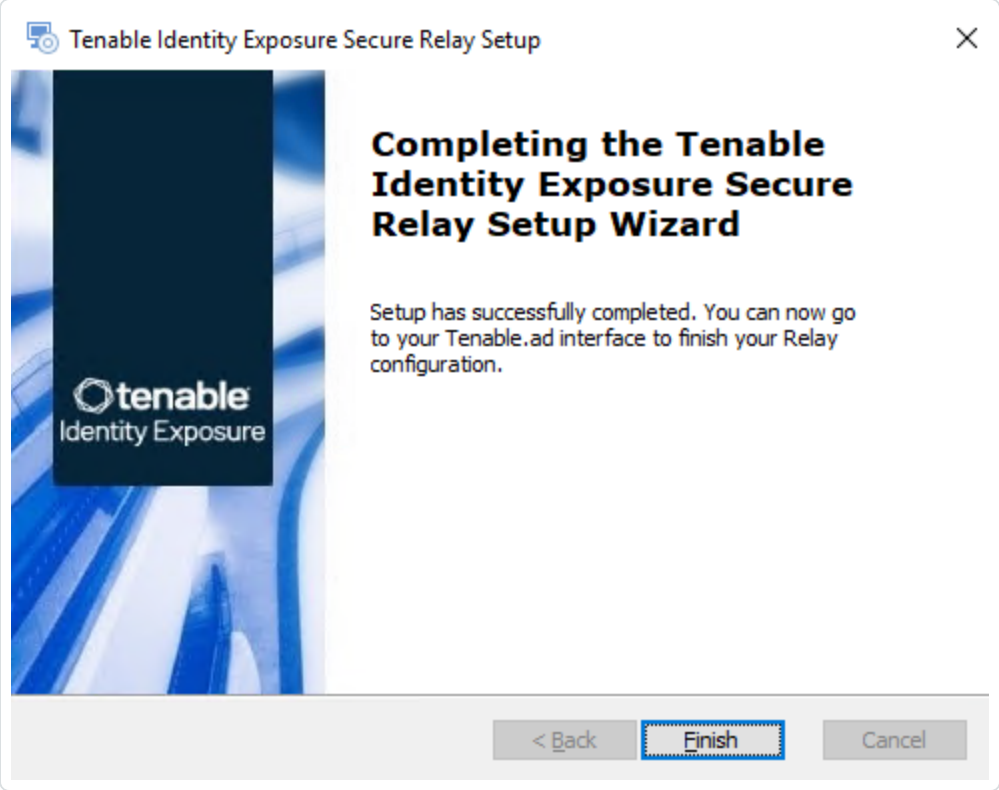
安装程序

所需用户角色：本地计算机上的管理员

若要安装安全中继，请执行以下操作：

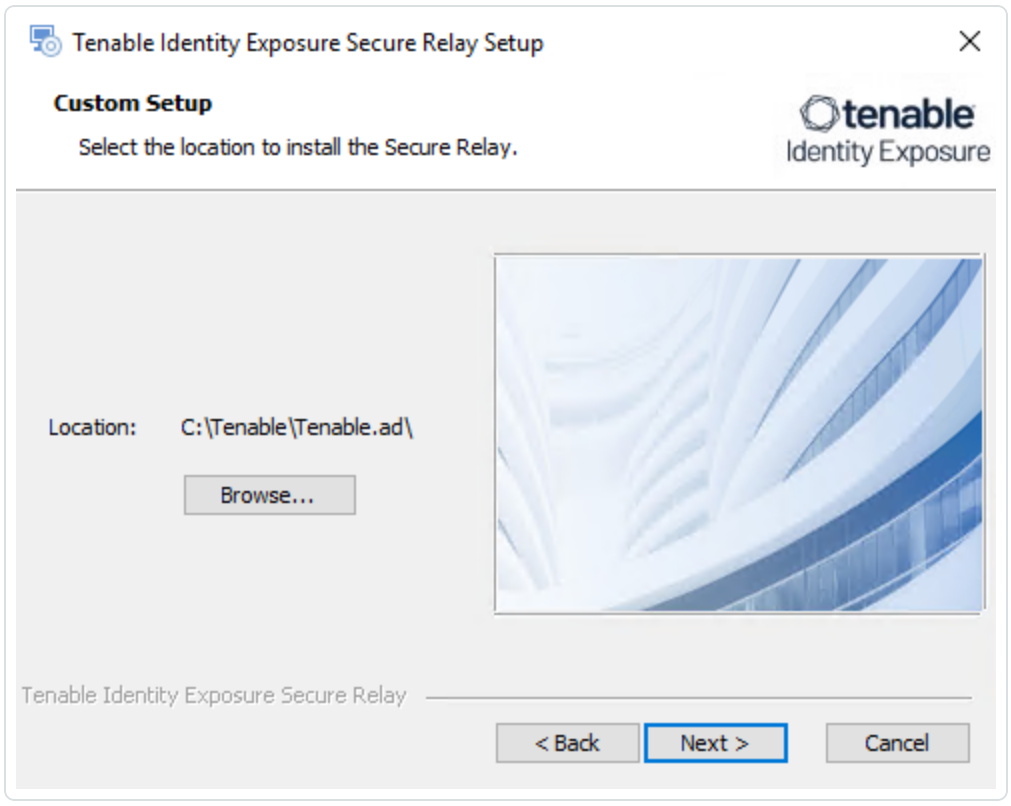
1. 从 Tenable 的下载站点下载安全中继的可执行程序。
2. 双击文件 `tenable.ad_SecureRelay_v3.xx.x` 以启动安装向导。

出现“**欢迎**”屏幕。



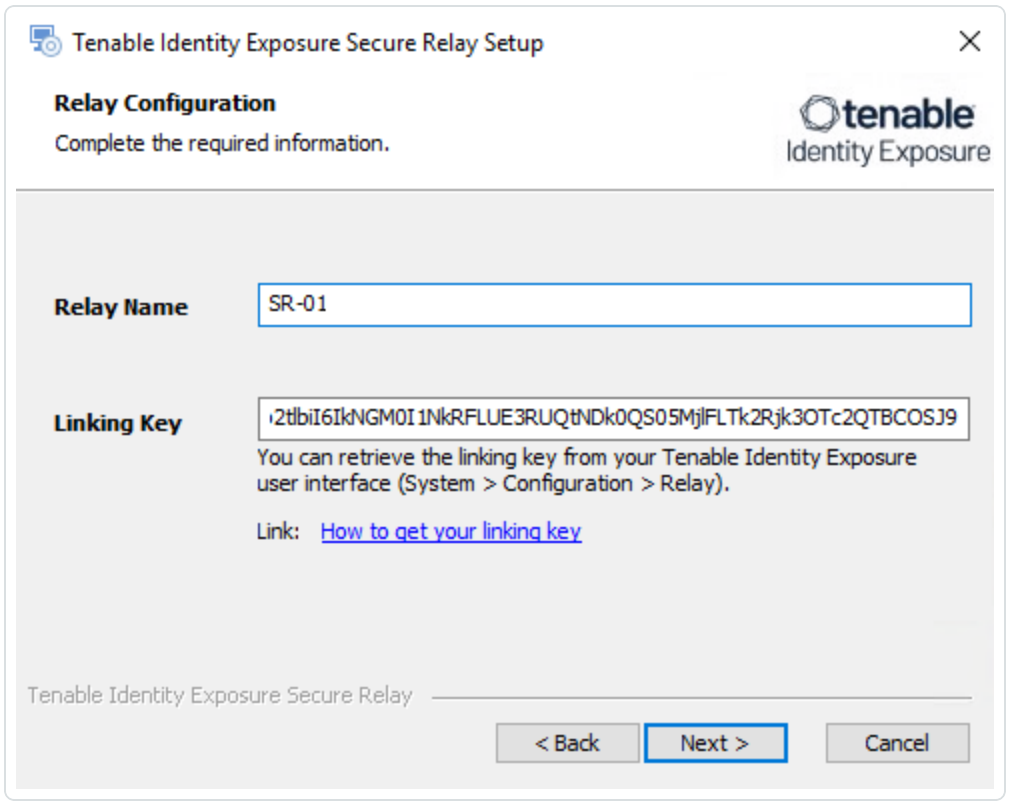
3. 单击“**下一步**”。

   出现“**自定义安装**”窗口。



4. 单击“**浏览**”以选择为安全中继保留的磁盘分区(独立于系统分区)。
5. 单击“**下一步**”。

   出现“**中继配置**”窗口。



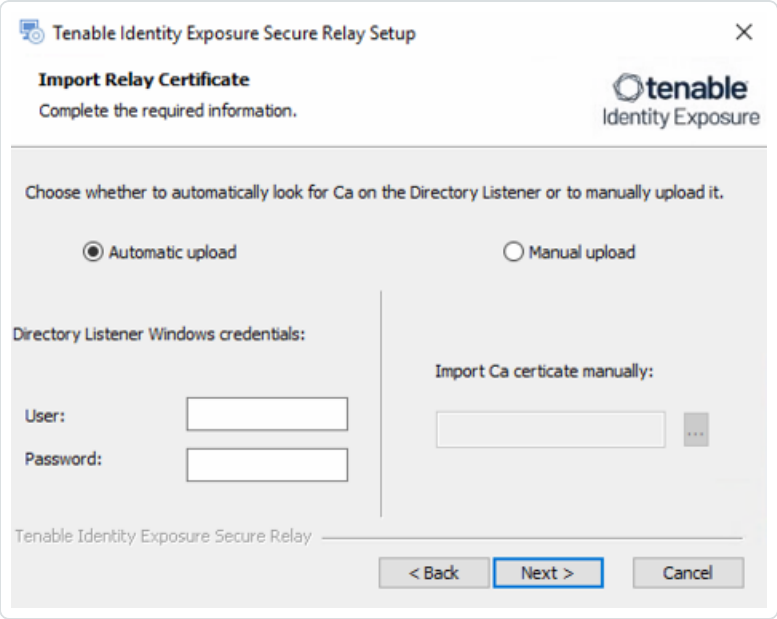
6. 提供以下信息：

   a. 在“**中继名称**”框中，输入安全中继的名称。

   b. 在“**链接密钥**”框中，粘贴从 Tenable Identity Exposure 门户检索的链接密钥。

   c. 如果选择使用代理服务器，请选择“**为中继调用使用 HTTP 代理**”选项并提供代理地址和端口号。

7. 如果您在与目录侦听器**不同的(独立)计算机**上安装中继，则会出现“**导入中继证书**”窗口：(如果您在同一台计算机上安装目录侦听器和中继，请转至下一步。)

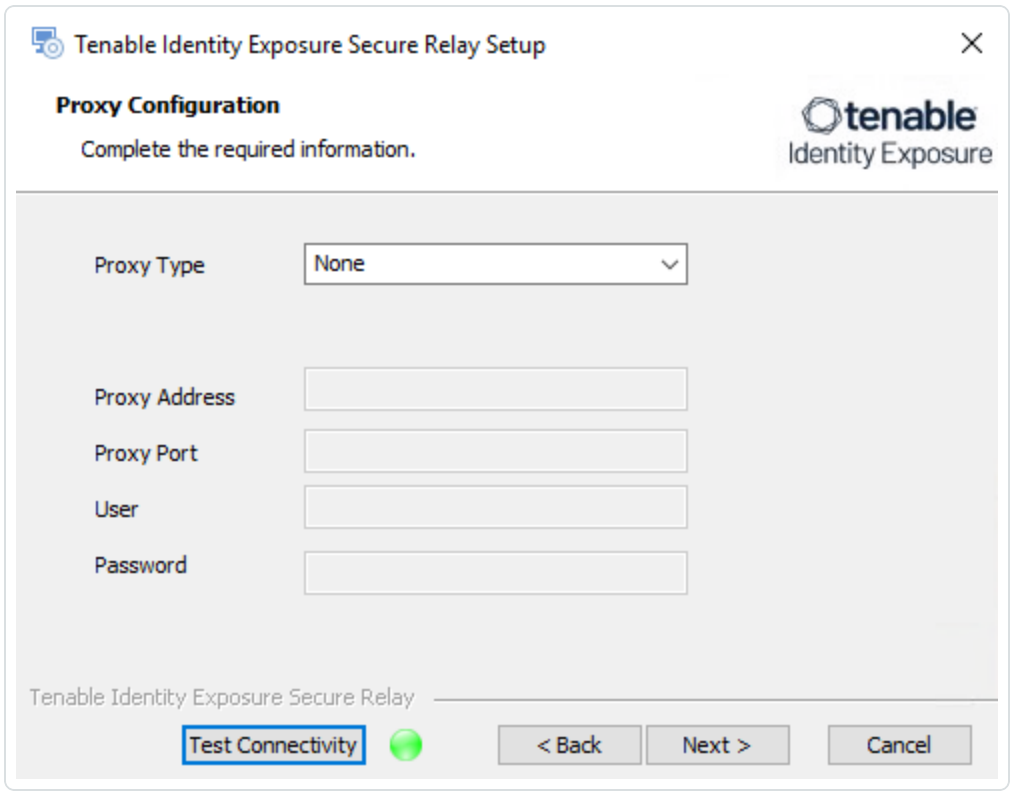


单击以下选项之一的单选按钮：

- **自动上传** – 从目录侦听器中自动检索 CA 证书：在“**目录侦听器 Windows 凭据**”下，输入用于访问目录侦听器服务的 Windows 帐户的用户名和密码。
- **手动上传** – 单击“**...**”以浏览目录侦听器使用的 CA 证书。

8. 单击“**下一步**”。

此时会出现“中继配置”窗口：



9. 请选择以下选项之一：

   a. **无**：不使用代理服务器。

   b. **未经身份验证**：输入代理服务器的地址和端口。

   c. **基本身份验证**：除了地址和端口，还要输入代理服务器的用户和密码。

   注意：若要使用“未经身份验证”或“基本身份验证”配置代理，中继仅支持 IPv4 地址（例如 `192.168.0.1`）或不带 `http://` 或 `https://` 的代理 URI（例如 `myproxy.mycompany.com`）。中继不支持 IPv6 地址（例如 `2001:0db8:85a3:0000:0000:8a2e:0370:7334`）。

10. 单击“**测试连接**”。可能出现以下情况：

    - **绿灯** - 连接成功。
    - **链接密钥无效** - 从 Tenable Identity Exposure 门户检索链接密钥。
    - **中继名称无效** - 此框不能为空。提供中继的名称。
    - **连接失败** - 检查您的互联网访问。

11. 单击“**下一步**”。

出现“**准备安装**”窗口。

12. 单击“**安装**”。
13. 安装完成后，单击“**完成**”。

安装后检查

完成安全中继安装后，检查以下项目：

Tenable Identity Exposure 中安装的中继列表

查看已安装的中继列表：

- 在 Tenable Identity Exposure 中，单击左侧菜单栏上的“**系统**”，然后选择“**中继管理**”选项卡。

  窗格中将显示列出安全中继及其所链接域的列表。

服务

安装成功后，系统将运行以下服务：

- `Tenable_Relay`
- `tenable_envoy`

  注意：您可以在 Tenable Identity Exposure 中的“**系统**”>“**法律**”>“**Envoy 许可证**”中找到 Envoy 许可证。

环境变量

安装过程还添加了 6 个与安全中继相关的新环境变量，其名称均以“ALSID_CASSIOPEIA_”开头。如果您选择使用代理服务器，则还会新增 2 个与代理 IP 和端口相关的环境变量。

故障排除日志

您可以在以下位置找到日志：

- **安装日志**：`C:\Users\<your user>\AppData\Local\Temp`
- **中继日志**：在安装时指定的文件夹中托管安全中继的 VM 上。

中继配置

- 配置中继

自动更新

在您安装安全中继后，Tenable Identity Exposure 会定期检查新版本。此过程完全自动完成，需要对您的域进行 HTTPS 访问 (TCP/443)。网络托盘中的图标会指示 Tenable Identity Exposure 正在更新安全中继。该进程完成后，Tenable Identity Exposure 服务会重新启动并恢复数据收集。

卸载

若要卸载安全中继，请执行以下操作：

1. 在 Windows 中，转至“**设置**”>“**应用程序和功能**”>“**Tenable Identity Exposure安全中继**”。
2. 单击“**卸载**”。

   卸载完成后，系统中将不再显示 Tenable Identity Exposure 安全中继的服务和环境变量。
3. 在 Tenable Identity Exposure 中，单击左侧菜单栏上的“**系统**”，然后选择“**中继管理**”选项卡。
4. 选择您刚卸载的中继，然后单击  ，将其从可用中继列表中删除。

另请参阅：

- Troubleshoot Secure Relay Installation
- 安全中继 - 常见问题

本地平台的安全中继架构

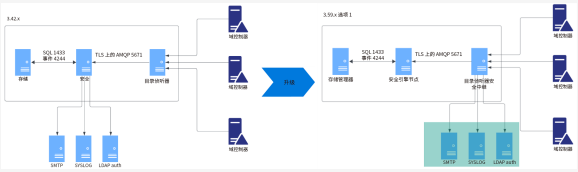
Tenable Identity Exposure 支持以下包含存储管理器 (SM)、安全引擎节点 (SEN)、目录侦听器 (DL) 和安全中继 (SR) 的架构：

- DL 和 SR 位于同一服务器上的标准 3 服务器架构
- DL 和 SR 位于单独服务器上的标准 3 服务器架构
- 多个 DL 转换为运行 SR 的单个 DL
- 多个 DL 转换为与 SR 通信的新 DL

DL 和 SR 位于同一服务器上的标准 3 服务器架构

此架构从标准 3 服务器架构(SM、SEN 和 DL)转换为 DL 和 SR 在同一服务器上运行的架构。

3.42	3.59 3.77
• 安全引擎节点具备以下功能: ◦ 发送电子邮件和 Syslog 警报 ◦ 提供 LDAP 身份验证	• 目录侦听器运行安全中继,该中继具备以下功能: • ◦ 发送电子邮件和 Syslog 警报 ◦ 提供 LDAP 身份验证

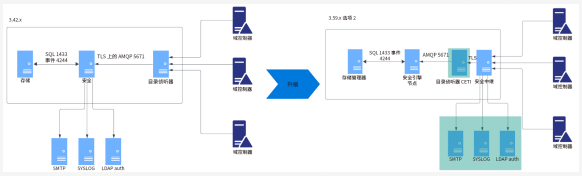


注意:此架构要求在一个虚拟机中同时包含 DL 和 SR 所需的资源。

DL 和 SR 位于单独服务器上的标准 3 服务器架构

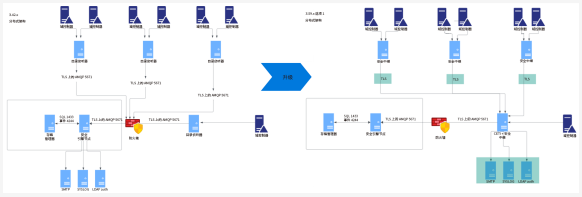
此架构从标准 3 服务器架构(SM、SEN 和 DL)转换为 DL 和 SR 在单独服务器上运行的架构。

3.42	3.59 3.77
• 安全引擎节点具备以下功能: ◦ 发送电子邮件和 Syslog 警报 ◦ 提供 LDAP 身份验证	• 需要使用**新的目录侦听器服务器** • 安全中继具备以下功能: ◦ 替换目录侦听器 ◦ 发送电子邮件和 Syslog 警报

	◦ 提供 LDAP 身份验证
	

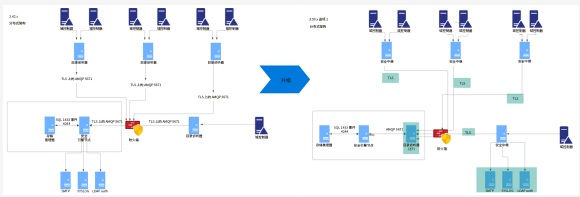
多个 DL 转换为运行 SR 的单个 DL

此架构从多个 DL 架构转换为利用单个 DL 运行 SR 的架构。

3.42	3.59 3.77
• 目录侦听器通过 TLS 使用 AMQP 与安全引擎通信 • 安全引擎节点具备以下功能： ◦ 发送电子邮件和 Syslog 警报 ◦ 提供 LDAP 身份验证	**第一个目录侦听器拥有安全中继**，充当所有已部署的安全中继的“集中器”(以前称为目录侦听器)，并使用 TLS 与这些中继通信。此安全中继具备以下功能： • 发送电子邮件和 Syslog 警报 • 提供 LDAP 身份验证
	

多个 DL 转换为与 SR 通信的新 DL

此架构从多个 DL 架构转换为利用新的 DL 与安全中继通信(替换旧的目录侦听器)的架构。

3.42	3.59 3.77
• 目录侦听器通过 TLS 使用 AMQP 与安全引擎通信 • 安全引擎节点具备以下功能： ◦ 发送电子邮件和 Syslog 警报 ◦ 提供 LDAP 身份验证	**新的目录侦听器服务器**充当所有已部署的安全中继的“集中器”(以前称为目录侦听器)，并使用 TLS 与目录侦听器通信。 安全中继具备以下功能： • 发送电子邮件和 Syslog 警报 • 提供 LDAP 身份验证
	

另请参阅：

[适用于 Tenable Identity Exposure 3.77 的安全中继]

配置中继

在完成安装和安装后检查之后，您可以在 Tenable Identity Exposure 中配置中继，以将其链接到域并设置警报。

◦ 域映射：将含多个 DL 的应用程序设置或网络环境变量替换为必要的域设置(编辑次数可能会有所不同)。

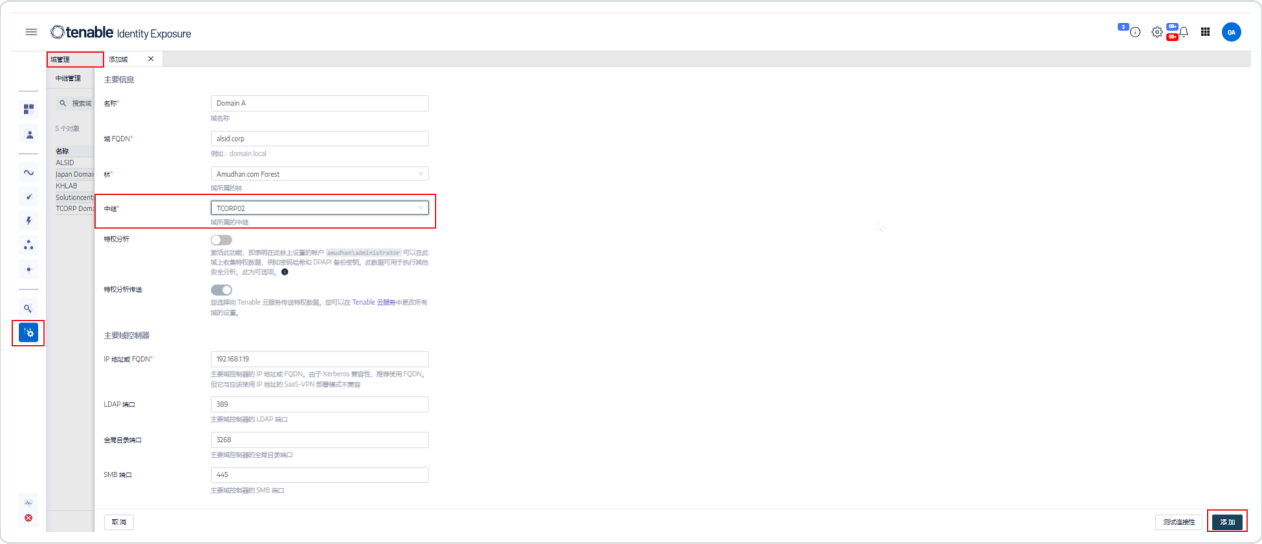
将域映射到安全中继：

1. 在 Tenable Identity Exposure 中，单击左侧菜单栏上的“**系统**”，然后选择“**域管理**”选项卡。

2. 在域列表中，选择要链接的域并单击该行末尾的 ✎。

   “**编辑域**”窗格随即打开。

3. 在“**中继**”框中，单击箭头以显示已安装中继的下拉列表，然后选择要链接到域的中继。



   单击“**编辑**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新域。SYSVOL 和 LDAP 将同步以包含所做修改。跟踪事件流开始接收新事件。

- 警报映射：
  - SMTP 配置：对 SMTP Server Configuration 进行必要的编辑。
  - Syslog 警报：配置 Syslog Alerts（编辑次数可能会有所不同）。
- LDAP 映射：实现 Authentication Using LDAP 。

另请参阅：

- 安全中继 - 常见问题

安全中继 - 常见问题

我以前有多个目录侦听器 (DL)。我是否仍然可以拥有多个 DL?

不，安全中继会取代多个 DL。Tenable Identity Exposure 现在**仅支持使用一个 DL**；使用多个 DL 会导致未知问题。

之前我只在计算机上安装了 DL，我能否在同一台计算机上同时安装 DL 和安全中继？

可以。但是，请确保同时满足 DL 和安全中继的资源要求。例如，如果 DL 的 RAM 要求为 5 GB，安全中继的 RAM 要求为 1 GB，则计算机的 RAM 必须为 6 GB (5 GB + 1 GB)。

您也可以在单独的虚拟机上安装安全中继，前提是该虚拟机可以支持 DL。

3.59 版本与之前的版本相比，网络流有哪些变化？

在 3.59 中，我们以最简单的方式在 Active Directory (AD) 和 DL 之间添加了一个安全中继。这意味着：

- AD 和安全中继之间的通信与之前 AD 和 DL 之间的通信相同。
- DL 与平台其余部分之间的通信与以前相同。
- 变化的地方在于，Tenable Identity Exposure 在一个或多个安全中继和 DL 之间使用 HTTPS 进行通信。您必须允许使用新的网络流。

我可以在哪里找到本地安全中继安装程序？

在文件夹 `C:\Tenable\Tenable.ad\DirectoryListener\Updates\` 中。

我应该使用 https://zh-cn.tenable.com/downloads 上提供的安全中继安装包，还是文件夹 C:\Tenable\Tenable.ad\DirectoryListener\Updates\ 中的安装包？

二者皆可，因为它们通常是相同的版本。利用 `C:\Tenable\Tenable.ad\DirectoryListener\Updates\` 文件夹中的安装包，您不需要登录即可访问二进制文件。

安装/升级 DL 时，被问到“是否在安装 DL 之后安装安全中继？”这个问题时，我选择了“是”，但却什么都没有安装。怎么回事呢？

安全中继会在 DL 服务器重新启动后开始安装；因此，请务必在安装/升级 DL 后重新启动服务器。

其他问题可能源于 AV/EDR 在重新启动后阻止安装过程运行。请务必查看完整的日志。

要在这些日志中查找的时间范围取决于阻止安装过程的 AV/EDR，因此请务必检查重新启动之前（DL 安装期间）和之后的某个时间。

如果中继安装失败，我应该收集哪些元素？

如果安装失败，您需要在尝试执行其他操作之前检索多个元素：

- 安装日志：发生故障时，从 MSI 对话框中提取这些内容。
- 中继日志：位于 `<install path>\SecureRelay\logs\Relay.log` 中。
- Envoy 日志：位于 `<install path>\SecureRelay\logs\envoy.logs` 中。
- `envoy.yaml` 配置文件：位于 `<install path>\SecureRelay\envoy.yaml` 中。如有必要，您可以编辑 API 密钥（尽管数据库中也有此密钥）。
- 环境变量：使用以下命令之一取得：

```
(cmd.exe) set
(powershell.exe) ls env: | fl
```

另请参阅：

- 对安装安全中继进行故障排除

故障排除日志

Tenable Identity Exposure 提供会调试日志，以便您进行故障排除和了解平台行为。

下面是一些常见的日志类型：

- 安装/升级日志
- 平台日志
- IoA 脚本安装/升级日志

安装/升级日志

如果无法使用安装程序在计算机上安装 Tenable Identity Exposure，您可以将日志文件转发给我们的支持团队 (https://community.tenable.com/s/)。

该日志文件位于 `%tmp%` 文件夹中，名称始终以“MSI”开头，接着是随机数字，例如 `MSI65931.LOG`。

要在其他位置生成日志文件（例如，如果您将安装程序放在桌面）：

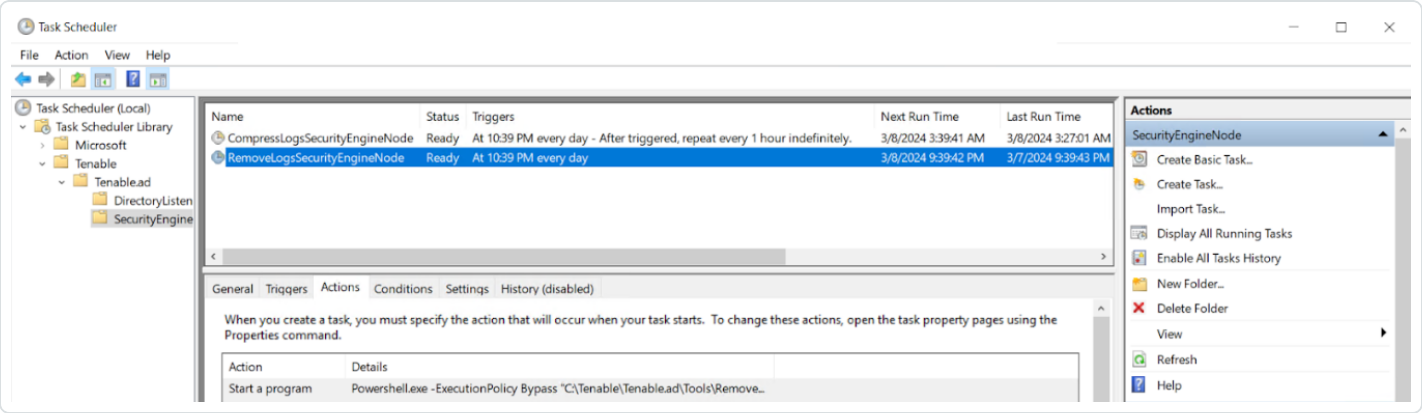
1. 在本地计算机的命令行中，输入 cd desktop。
2. 输入 .\installername.exe /LOGS "c:\<path>\logsmsi1.txt"。

平台日志

Tenable Identity Exposure 可为单独安装的各种服务生成日志文件。

- 在目录侦听器服务器中，位于以下位置：`<Installation Folder>\DirectoryListener\logs`
- 在安全引擎节点服务器中，位于以下位置：`<Installation Folder>\SecurityEngineNode\logs`
- 在存储管理器服务器中，位于以下位置：`<Installation Folder>\StorageManager\logs`
- 在目录侦听器服务器和/或独立的安全中继服务器中，位于以下位置：`<Installation Folder>\SecureRelay\logs`

如果每个文件的大小达到 100 MB 并且被压缩，默认平台日志文件会发生轮换。在 Windows 任务计划程序中，这些任务在安装期间自动生成。以下是安全引擎节点上的任务示例。



IoA 脚本安装/升级日志

攻击指标 (IoA) 脚本会在该脚本所在的位置中创建日志文件（例如 `Register-TenableIOA-xxxx.log`）。您可以检查安装期间是否发生任何错误或问题。

日志保留期

- **短期保留**：在调试日志生成后，予以短期保留，如 7 天。这样，您便可以诊断最近的问题，同时最大程度减少存储消耗。
- **长期存档**：出于合规性或故障排除目的，考虑延长调试日志子集的存档时间。您可以将它们存储到安全的位置，或者对其进行压缩以有效利用空间。

部署后任务

成功安装或升级 Tenable Identity Exposure 后，请完成以下检查，以

登录 Tenable Identity Exposure

您可以通过客户端 URL(如 `https://<SEN IP-address>` 或 `https://<SEN hostname>`)访问 Tenable Identity Exposure 的 Web 应用程序。

要登录 Tenable Identity Exposure，请选择以下选项之一：

- 使用 Tenable Identity Exposure 帐户
- 使用 LDAP 帐户
- 使用 SAML

> **注意**：您初始凭据的用户名“hello@tenable.ad”，密码是“verySecure1”。

请参阅“Log in to Tenable Identity Exposure”，以获取完整信息。

运行状况检查

使用“Health Checks”功能全面评估域和平台状态，以确保升级后的运行状况或状态相较于升级之前没有恶化。

功能检查

升级后，验证以下功能是否正常：

- **跟踪事件流**：检查“跟踪事件流”页面打开之后是否会正常显示事件列表。确保页面加载更新后的日期和时间戳。请参阅“Trail Flow”，以获取完整信息。
- **风险暴露指标** (IoE)：确保“风险暴露指标”窗格已打开。默认情况下，Tenable Identity Exposure 仅显示包含异常行为的 IoE。验证是否针对相应的异常行为正确加载了页面。请参阅“Indicators of Exposure”，以获取完整信息。
- **攻击指标** (IoA)：确保“攻击指标”窗格已打开。Tenable Identity Exposure 在单个窗格中实时显示时间线和影响 AD 的三大事件，以及攻击分布情况。如果可能，请对 IoA 执行示例测试(密码猜测)，以确认是否会触发警报。有关更多信息，请参阅“Indicators of Attack”。

术语表

此词汇表旨在让您熟悉 Tenable Identity Exposure 中的常用术语。

Cancri：计算 AD 对象之前状态与当前状态之间的差异的服务。它还会对事件排序，以便 Cygni 按顺序接收这些事件。

Cephei：计算仪表盘上可观察到的统计数据（小组件活跃用户计数、合规性分数、异常行为等）的服务。

Ceti：最先收集 AD 对象（抓取）并订阅复制流（出现的新事件：监听）的服务。当前检索到的 AD 对象有两个来源：LDAP 和 SYSVOL。

Cygni：此服务用于分析 AD 对象中的更改，以推断其是否涉及一个或多个风险，并汇总更改情况，以判断是否符合异常行为的标准。然后，此异常行为将被传输到数据库并在 Tenable Identity Exposure 中可见。

异常对象：风险暴露指标 (IoE) 标记的一组异常行为，指向其属性会触发相关 IoE 的对象。

目录侦听器：通过托管与受监控的域控制器密切配合的 Ceti 服务（本地环境），目录侦听器可以接收实时 Active Directory 流并应用多种处理方法来解码、隔离和关联安全更改。

Enif：此服务用于控制 Web 界面的身份验证。

Eridanis：API 服务，用于在 MS SQL 服务中存储业务数据（配置和 AD 对象、异常行为等）并为其他服务提供这些数据。

Kapteyn：托管 Tenable Identity Exposure Web 应用程序的服务。此实时应用程序使用 Javascript 技术开发而来，无需用户操作即可更新数据。

RabbitMQ：RabbitMQ 是一种第三方工具，供 Tenable Identity Exposure 用于在服务之间传输消息。在接收应用程序连接并从队列中移除消息之前，消息会一直保留在 RabbitMQ 队列管理器中。接收应用程序随后会处理该消息。

安全中继：一种使用传输层安全 (TLS) 而非 VPN 将 Active Directory 数据从网络传输到 Tenable Identity Exposure 的模式（不含 3.59 及更高版本）。

安全引擎节点：由于托管分析相关的服务，安全引擎节点可以为 Tenable Identity Exposure 安全引擎、内部通信总线和最终用户应用程序（如 Web 门户、REST API 或警报通知程序）提供支持。此组件基于被隔离的不同 Windows 服务构建而来。

存储管理器:存储管理器不仅提供热存储和冷存储支持,还能监控目录侦听器和安全引擎节点的服务数据。此组件是唯一必须持久保存信息的组件。在内部,它们使用 Microsoft MS SQL 服务器存储内部数据和配置。

跟踪事件流:“跟踪事件流”登录页面会显示影响 AD 基础设施的事件的实时监控和分析信息。“跟踪事件流”页面支持加载之前的事件,以返回到过去。您还可以使用此页面顶部的搜索功能执行威胁搜寻和检测恶意模式。

获取支持

如果客户在使用产品时遇到问题，Tenable 技术支持团队可以提供帮助。如需快速协助，请参阅以下文章，其中概述了提交支持案例的最佳实践：向技术支持团队提交案例：最佳实践。

Tenable 规定，客户通过 Tenable Community 创建技术支持案例时，可以指定相应的案例优先级。优先级范围在 P1 到 P4 之间，P1 代表最危急的问题，P4 代表无关紧要的问题。客户在分配案例优先级时应做出最佳判断，以确保案例得到及时处理；出于准确分类目的，技术支持团队保留提高或降低案例优先级的权利。我们强烈建议客户直接联系技术支持团队处理严重程度为 P1 的问题，以免因电子邮件通信造成任何延迟。以下是一些可帮助客户确定案例优先级的示例。

优先级	描述	示例
P1 - 严重	产品功能完全退化：对业务运营造成重大影响	• 产品（Nessus、Tenable Identity Exposure 等，不包括代理/客户端）服务将无法启动 • 所有用户均无法使用产品 • 升级失败：无法使用产品 • Nessus/Tenable Identity Exposure/Tenable.io 无法扫描（即所有扫描错误/无法启动）
P2 - 高危	产品功能严重退化：对业务运营造成严重影响	• 报告不会启动/生成（即所有报告均失败） • 无法查询漏洞/所有仪表盘/所有扫描结果 • 链接扫描程序/LCE/NNM 失败（不包括代理/客户端）
P3 - 中危	一般错误/问题：产品受损，但业务运营仍可正常进行	• 通常为默认优先级 • 误报/漏报 • 扫描/报告错误

		• 非核心功能错误:资产/目标列表、SMTP/LDAP 集成等。 • 插件更新失败 • 初始安装/设置问题 • 需要测试升级情况之后再安装到生产环境中
P4 - 信息性	有关 Tenable 产品的基本信息或协助:几乎不会影响业务运营	• 如何 [问题]? • 必须打开哪些端口才能使产品工作? • 是否有扫描“X”的插件? • 哪些 IP 会计入我的 Tenable Identity Exposure 许可证? 是否有“X”功能?