Tenable Identity Exposure 3.x 用户和管理员指南

上次修订日期：2024 年 4 月 5 日

目录

欢迎使用 Tenable Identity Exposure **8**

浏览 Tenable Identity Exposure 10

登录 Tenable Identity Exposure 13

访问 Workspace 18

用户首选项 21

通知 24

仪表盘 26

小组件 28

Identity Explorer 32

跟踪事件流 34

"跟踪事件流"表 36

使用向导搜索"跟踪事件流" 38

手动搜索"跟踪事件流" 40

自定义跟踪事件流查询 42

书签查询 45

查询历史记录 48

显示异常事件 50

事件详细信息 52

属性更改 55

跟踪事件流用例 58

风险暴露指标 62

风险暴露指标详细信息 65

异常对象 68

搜索异常对象 71
忽略异常对象 75
危害认定属性 77
基于 RSoP 的风险暴露指标 79
与 Microsoft Entra ID 相关的风险暴露指标 80
根据风险暴露指标修复异常对象 81
标准用户中设置了 AdminCount 属性 82
存在风险的 Kerberos 委派 85
确保 SDProp 一致性 91
攻击指标 95
攻击指标详情 98
攻击指标事件 101
拓扑 106
信任关系 108
危险的信任 111
攻击路径 113
攻击关系 118
添加密钥凭据 120
添加成员 122
允许行动 124
允许委派 127
属于 GPO 130
DCSync 132
允许行动的授权 134

有 SID 历史记录 136
隐式接管 138
继承 GPO 140
链接的 GPO 142
成员归属 144
拥有 146
重置密码 148
RODC 管理 150
写入 DACL 152
写入所有者 154
识别第 0 层资产 156
有攻击路径的帐户 158
攻击路径节点类型 160
活动日志 163
Tenable Identity Exposure 管理员指南 165
Active Directory 配置 167
访问 AD 对象或容器 168
特权分析的访问权限 169
安全中继 175
网络流 176
TLS 要求 177
事先说明 180
允许的文件和进程 182
链接密钥 184

安装 185
卸载 186
自动更新 187
另请参阅： 188
安装安全中继 (GUI) 189
安装安全中继 (Tenable Nessus Agent) 193
安装后检查 196
配置中继 198
攻击指标部署 199
安装攻击指标 202
攻击指标安装脚本 209
技术变更与潜在影响 217
攻击场景 (< v. 3.36) 219
安装 Microsoft Sysmon 224
卸载攻击指标 229
对攻击指标进行故障排除 230
防病毒检测 231
高级审核策略配置优先级 233
事件日志侦听器验证 235
Tenable Identity Exposure 日志文件 237
DFS 复制问题缓解措施 244
身份验证 246
使用 Tenable One 进行身份验证 247
使用 Tenable Identity Exposure 帐户进行身份验证 248

使用 LDAP 进行身份验证 252
使用 SAML 进行身份验证 254
用户帐户 257
创建用户 258
编辑用户 260
停用用户 261
删除用户 262
安全配置文件 263
定制指标 265
完善指标的定制 267
用户角色 269
管理角色 270
设置角色的权限 271
设置用户界面实体的权限(示例) 275
林 278
管理林 279
保护服务帐户 280
域 281
强制在域上执行数据刷新 285
Honey Account 286
Kerberos 身份验证 289
警报 296
SMTP 服务器配置 297
电子邮件警报 299

Syslog 警报 303
Syslog 和电子邮件警报详细信息 307
运行状况检查 313
报告中心 319
Microsoft Entra ID 支持 322
Tenable Cloud 数据收集 331
特权分析 332
活动日志 333
Tenable Identity Exposure 公共 API 336
数据管理 338
部署区域 339
Tenable Identity Exposure 许可 341
管理许可证 343
故障排除 Tenable Identity Exposure 347
Tenable Identity Exposure 诊断工具 348
SYSVOL 强化干扰 Tenable Identity Exposure 350

欢迎使用 Tenable Identity Exposure

上次更新日期：2024/4/30

Tenable Identity Exposure(原名 Tenable.ad) 可以预测威胁、检测入侵并对事件和攻击做出响应，从而保护您的基础设施。我们提供直观的仪表盘实时监控 Active Directory，您可以一目了然地看到最严重的漏洞，获取修正过程建议。Tenable Identity Exposure 的攻击指标和风险暴露指标可帮助您发现影响 Active Directory 的潜在问题，识别危险的信任关系，并深入分析攻击的详细信息。

> 是否可用攻击指标和风险暴露指标取决于您购买的许可证。

如要开始使用，请参阅《Tenable Identity Exposure 入门》。

> **注意：**Tenable Identity Exposure 可单独购买，也可随 Tenable One 程序包一起购买。有关更多信息，请参阅Tenable One。

> **提示：***《Tenable Identity Exposure 用户指南》*提供英语、日语、德语、韩语、简体中文和繁体中文版本。*Tenable Identity Exposure* 用户界面提供英语、日语、德语、韩语、简体中文和繁体中文版本。要更改用户界面语言，请参阅"用户首选项"。

有关 Tenable Identity Exposure 的更多信息，请查看以下客户教育材料：

- Tenable Identity Exposure 自助指南
- Tenable Identity Exposure 简介 (Tenable University)

Tenable One 风险暴露管理平台

Tenable One 是一款风险暴露管理平台，可帮助组织洞察现代攻击面，集中精力防范可能的攻击，并准确传达网络安全风险，以支持组织达到最佳业务绩效。

该平台结合了涵盖 IT 资产、云资源、容器、Web 应用程序和身份系统的最广泛的漏洞覆盖范围，以 Tenable Research 的速度和广泛的漏洞覆盖范围为基础，并增加了全面的分析，以对操作进行优先级分析和传达网络安全风险。Tenable One 可让组织：

- 获得对现代攻击面的全面可见性
- 预测威胁并对操作进行优先级分析以防止攻击
- 传达网络安全风险以做出更好的决策

Tenable Identity Exposure 是一款单独的产品，但也可以随 Tenable One 风险暴露管理平台一起购买。

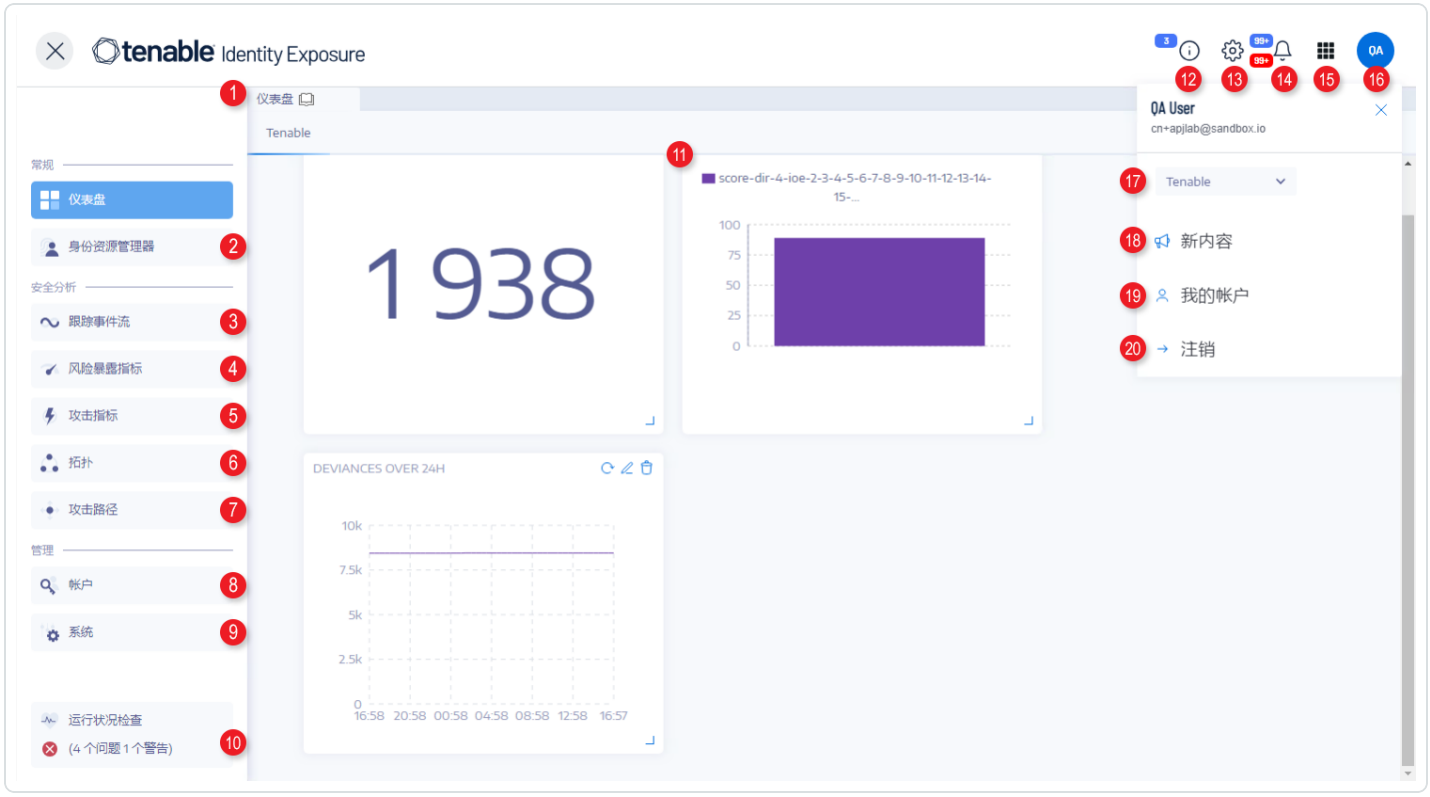
提示：有关 Tenable One 产品的更多入门信息，请查看《Tenable One 部署指南》。

浏览 Tenable Identity Exposure

登录到 Tenable Identity Exposure 后，主页随即打开，如此例中所示。

若要展开或折叠侧边导航栏：

- 展开：点击窗口左上角的 ☰ 菜单。
- 折叠：点击窗口左上角的 **X**。



#	名称	功能
1	仪表盘	“仪表盘”让您可以通过可视化的方式有效管理和监控 Active Directory 基础设施中的安全性。
2	Identity Explorer	Tenable Identity Exposure 的身份资源管理器视图统一了 Active Directory 和 Microsoft Entra ID 中的标识。此视图显示每个列出资产的标识风险评分(测试版) 以及标识遭

		到破坏的潜在范围。
3	跟踪事件流	“跟踪事件流”显示影响 Active Directory 的事件的实时监控和分析。
4	风险暴露指标	Tenable Identity Exposure 使用风险暴露指标 (IoE) 衡量 Active Directory 的安全成熟度，并为其监控和分析的事件流分配严重程度（“严重”、“高危”、“中危”或“低危”）。
5	攻击指标	Tenable Identity Exposure 可以借助攻击指标实时检测攻击。
6	Topology	“拓扑”页面以交互式图形方式显示 Active Directory。该页面显示林、域以及它们之间存在的信任关系。
7	攻击路径	“攻击路径”页面以图形方式展示 Active Directory 关系： • 爆炸半径：通过可能遭到入侵的资产评估 AD 中的横向移动。 • 攻击路径：预测从某个进入点访问资产的特权提升技术。 • 资产风险暴露：使用资产风险暴露可视化来衡量资产的漏洞，并解决所有特权提升路径。
8, 9	管理 **所需用户角色**：具有适当权限的组织用户。	在此部分，您可以配置以下内容： • 帐户：用户帐户、角色和安全配置文件。 • 系统：林和域、应用程序服

		务、警报和身份验证。 有关更多信息，请参阅 Tenable Identity Exposure 管理员指南。
10	运行状况检查	运行状况检查使您可以在一个综合视图中实时了解域和服务帐户的配置，以深入了解更详细的信息。
11	小组件	“小组件”是仪表盘显示的可定制数据集。它们可能包含条形图、折线图和计数器。
12	产品更新	有关最新产品功能的信息。
13	设置	访问系统配置、林和域管理、许可证、用户和角色管理、配置文件和活动日志的权限。
14	通知(铃铛)	铃铛图标和计数牌可以通知您等待确认的攻击警报和/或风险暴露警报。
15	应用程序切换器	单击此图标可在 Tenable 工作区的应用程序之间切换。
16, 19	用户配置文件图标 (用户首选项)	点击此图标可访问安全配置文件、发行说明、活动日志、首选项或注销的子菜单。
17	安全配置文件	“安全配置文件”允许不同类型的用户从不同报告角度查看安全分析。
18	新增功能	点击可打开 Tenable Identity Exposure 最新版本的发行说明。
20	注销	点击以注销 Tenable Identity Exposure。

登录 Tenable Identity Exposure

您可以通过客户端 URL 访问 Tenable Identity Exposure 的 Web 应用程序。

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

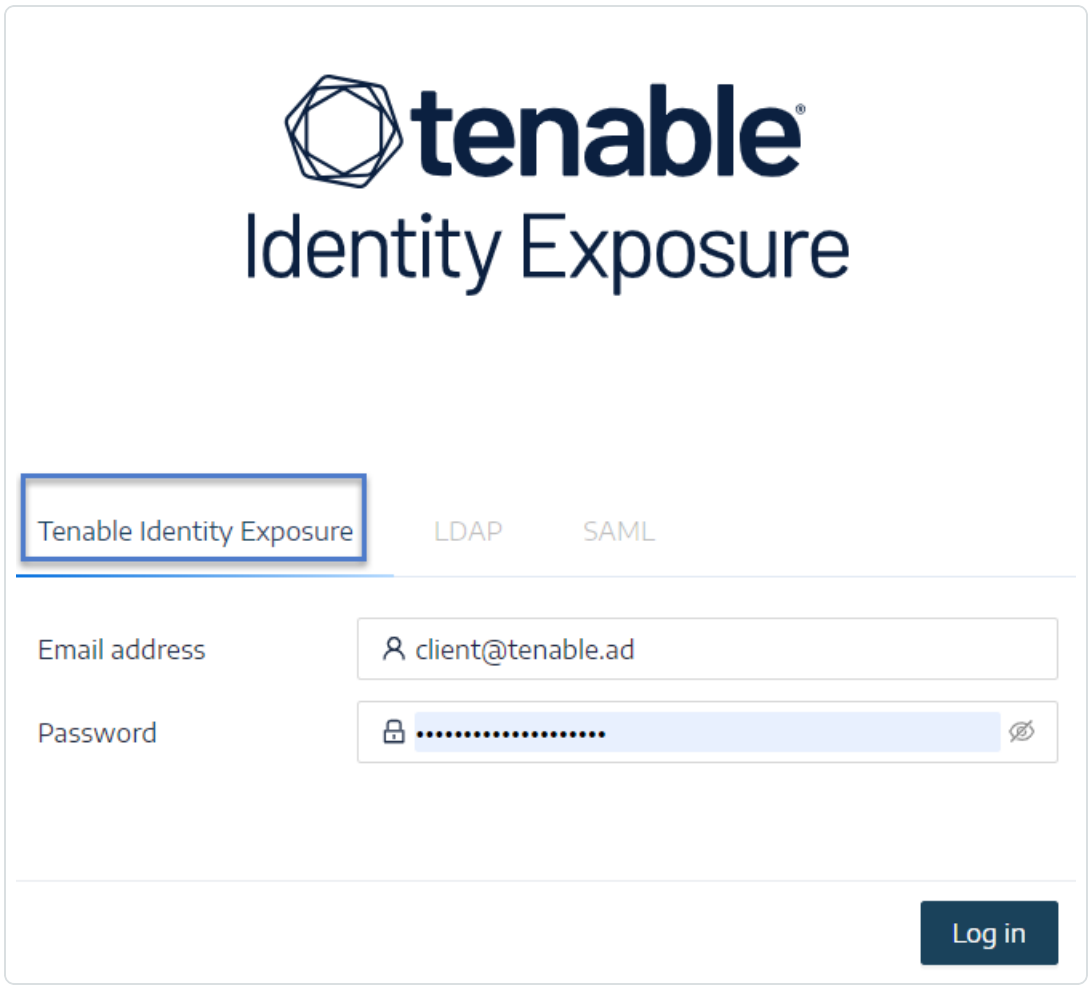
- ◦ 使用 Tenable Identity Exposure 帐户
  ◦ 使用 LDAP 帐户
  ◦ 使用 SAML

使用 Tenable Identity Exposure 帐户

使用 Tenable Identity Exposure 帐户登录：

1. 在任意浏览器的地址栏中，输入客户端 URL（例如：client.tenable.ad）。

   此时会出现“**登录**”窗口。



2. 点击 **Tenable Identity Exposure** 选项卡。
3. 输入您的电子邮件地址。
4. 输入密码。
5. 点击“**登录**”。

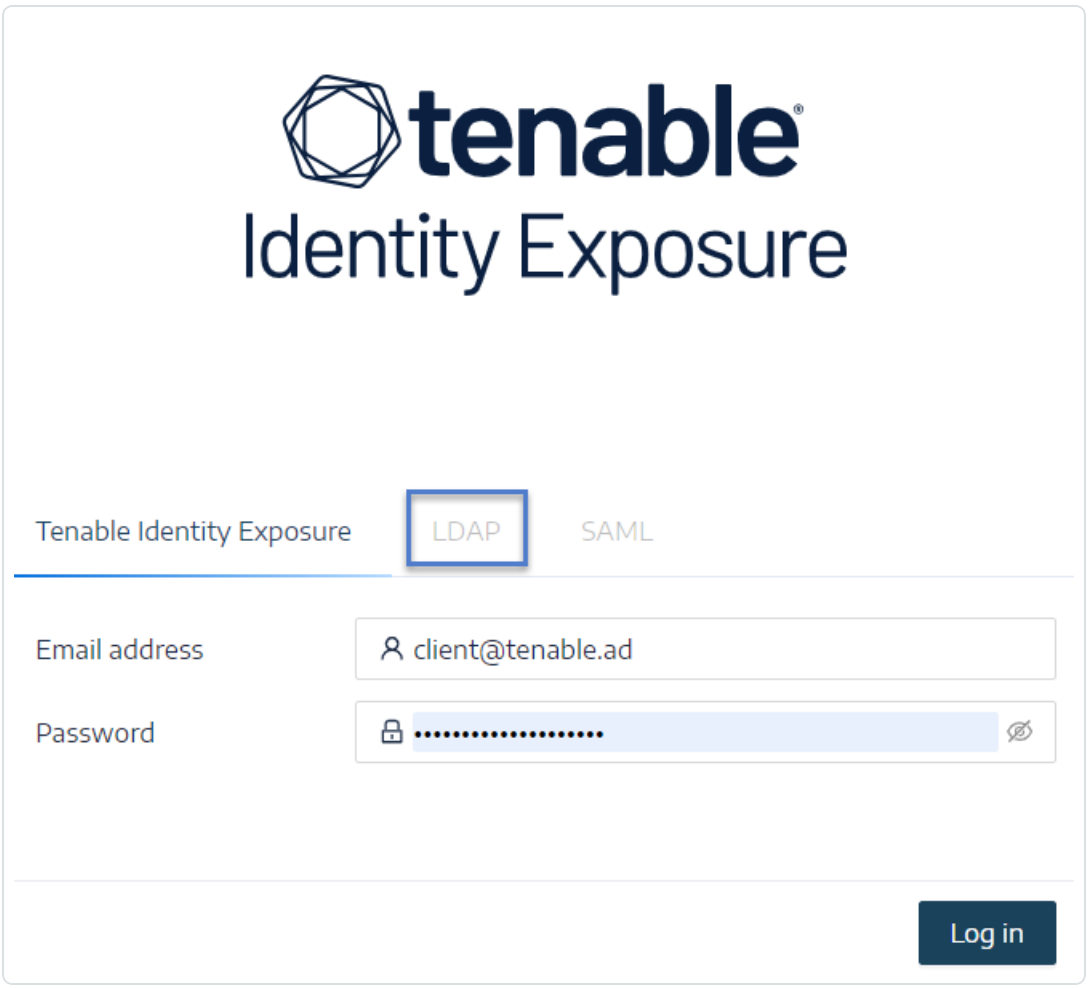
   此时 Tenable Identity Exposure 页面会打开。

使用 LDAP 帐户

使用 LDAP 登录的步骤：

1. 在任意浏览器的地址栏中，输入客户端 URL(例如：client.tenable.ad) 。

   此时会出现“**登录**”窗口。



2. 点击“**LDAP**”选项卡。
3. 输入 LDAP 帐户名称。
4. 输入 LDAP 密码。
5. 点击“**登录**”。

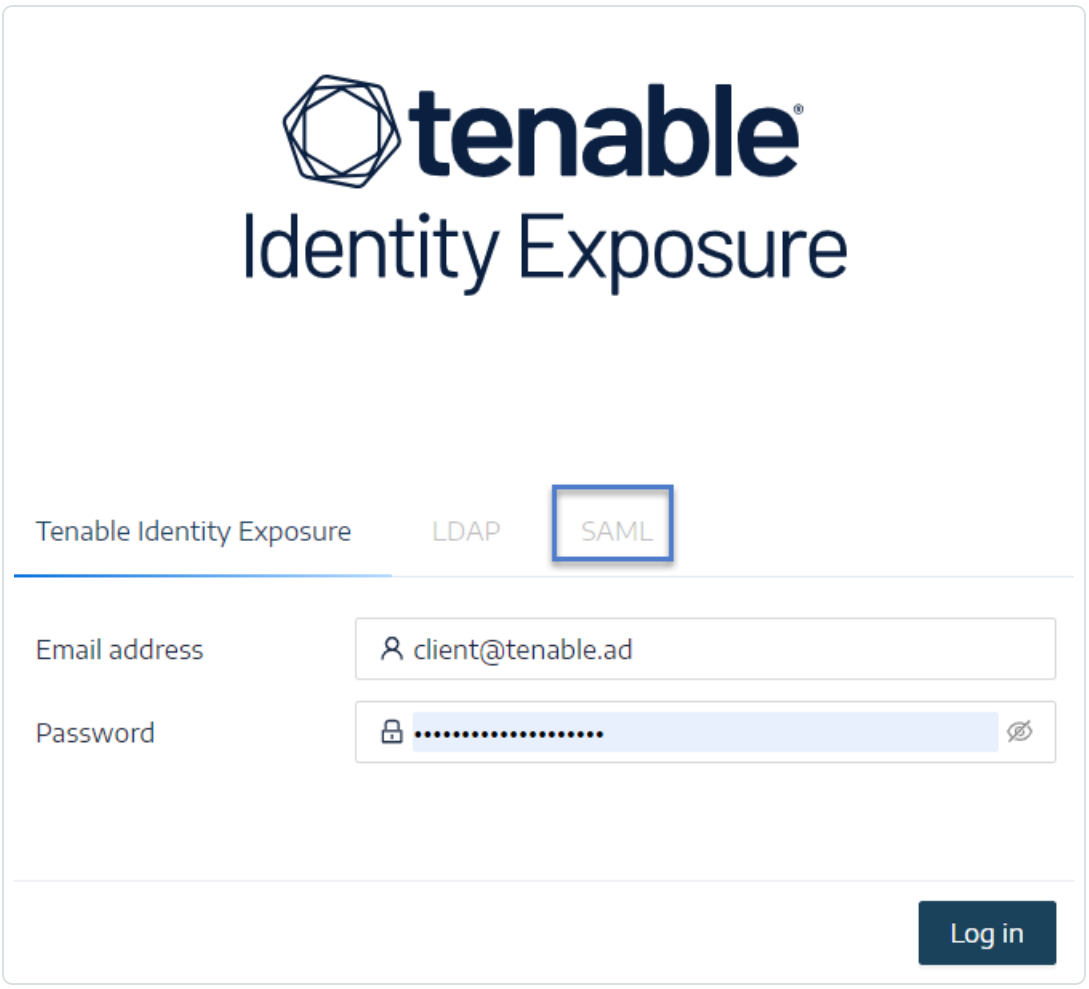
   此时 Tenable Identity Exposure 页面会打开。

使用 SAML

使用 SAML 登录的步骤：

1. 在任意浏览器的地址栏中，输入客户端 URL(例如：client.tenable.ad) 。

   此时会出现“**登录**”窗口。



2. 点击"**SAML**"选项卡。
3. 单击身份提供程序 (IDP) 的链接。

   Tenable Identity Exposure 会将您重定向到 SAML 服务器进行身份验证。
4. 在 IDP 上输入公司凭据。

   您将以登录用户的身份重定向到 Tenable Identity Exposure。

注意:如果您反复登录失败,Tenable Identity Exposure 将锁定您的帐户。此时请联系管理员。

注销 Tenable Identity Exposure 的步骤:

1. 在 Tenable Identity Exposure 中的单击您的用户图标。

   此时会出现一个子菜单。

2. 点击“**注销**”。

   Tenable Identity Exposure 会返回至登录页面。

访问 Workspace

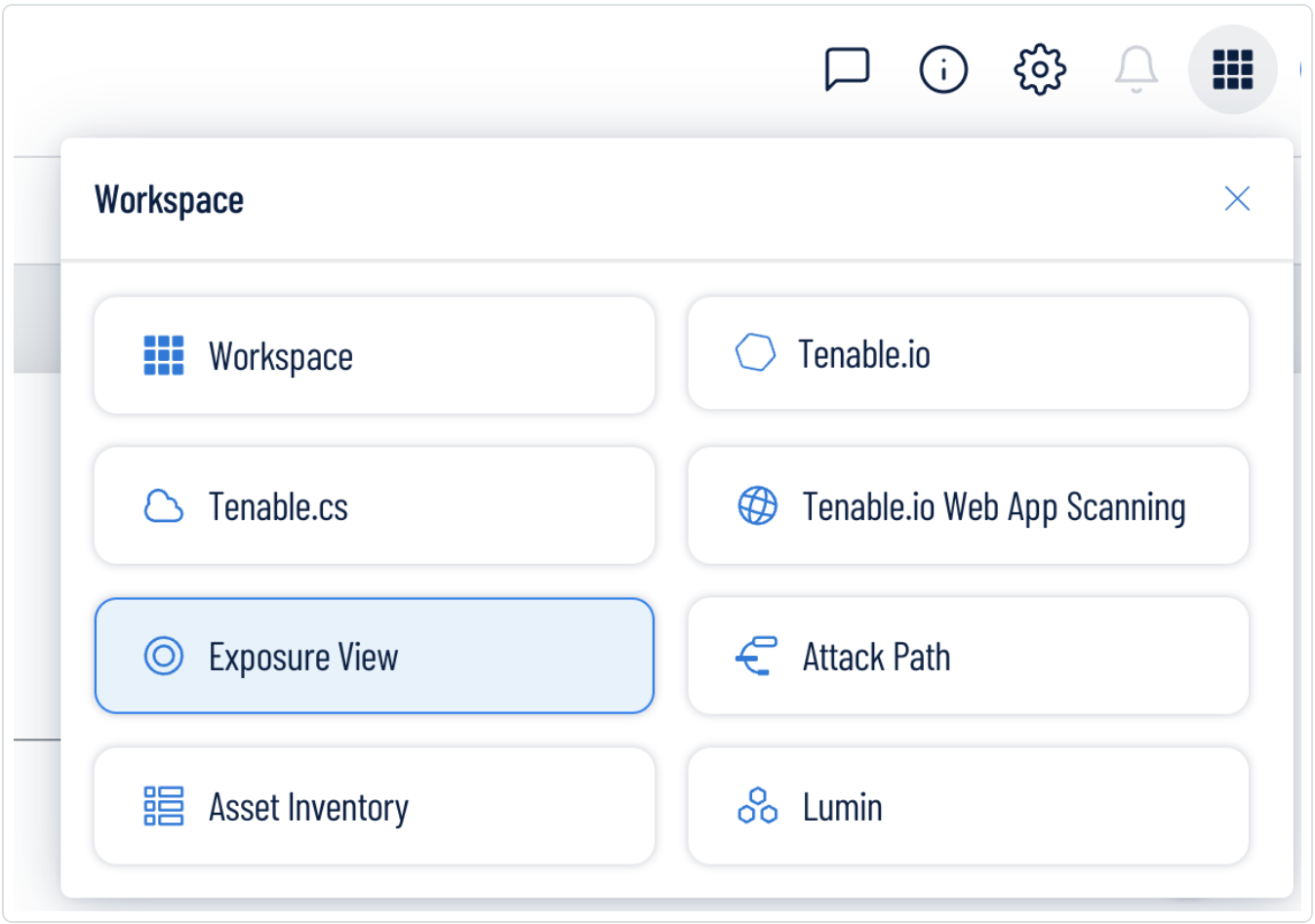
当您登录 Tenable 时，默认显示“**Workspace**”页面。在“**Workspace**”页面上，您可以在 Tenable 应用程序之间进行切换，或设置默认应用程序以在将来跳过“**Workspace**”页面。您也可以通过顶部导航栏中的“**Workspace**”菜单在应用程序之间进行切换。

打开“Workspace”菜单

若要打开“**Workspace**”菜单，请执行以下操作：

1. 在任意 Tenable 应用的右上角，点击 按钮。

   此时会出现“**Workspace**”菜单。



2. 单击应用程序磁贴将其打开。

查看“Workspace”页面

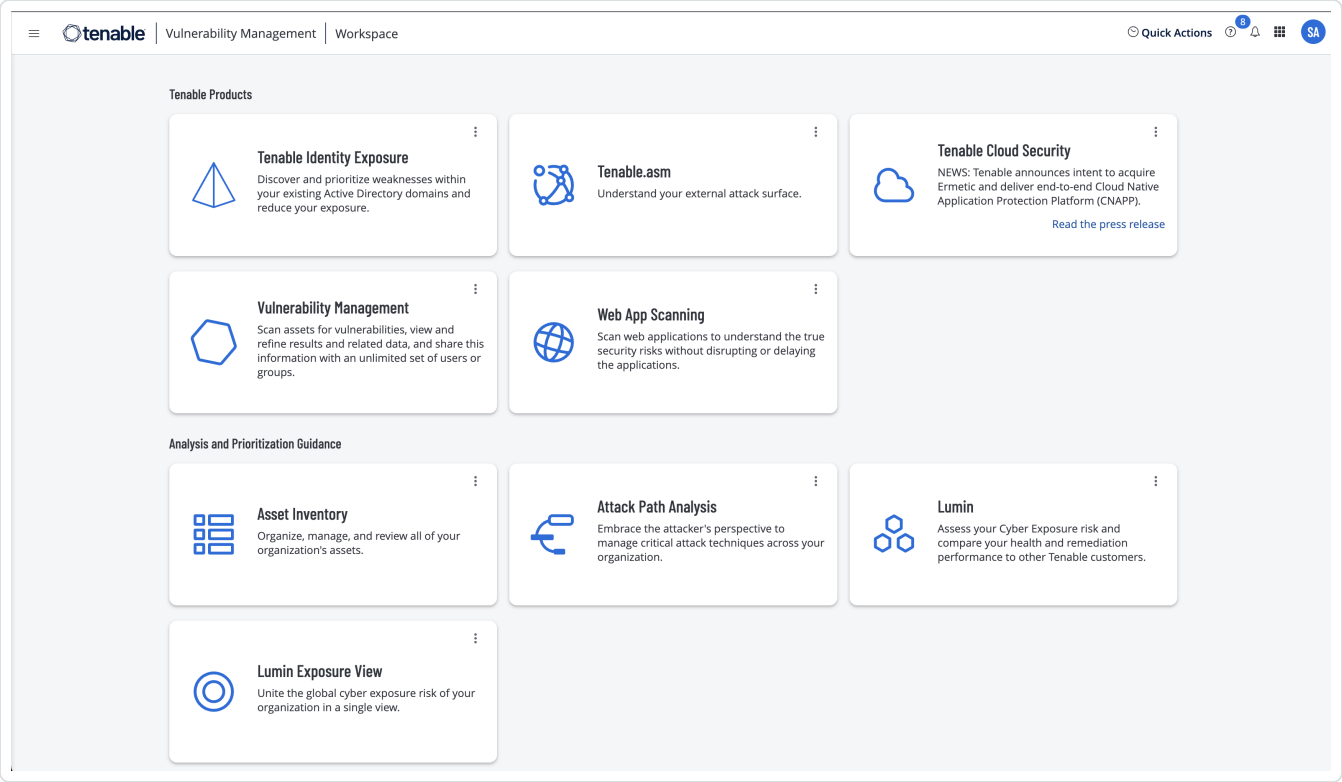
若要查看“Workspace”页面，请执行以下操作：

1. 在任意 Tenable 应用的右上角，点击 按钮。

   此时会出现“**Workspace**”菜单。

2. 在“**Workspace**”菜单中，单击“**Workspace**”。

   此时会出现“**Workspace**”页面。



设置默认应用程序

当您登录 Tenable 时，默认显示“**Workspace**”页面。但您可以设置默认应用程序以在将来跳过“**Workspace**”页面。

> 默认情况下，具有**管理员**、**扫描管理员**、**扫描操作员**、**标准**和**基本**角色的用户可以设置默认应用程序。如果您是其他角色，请联系您的管理员并在“**我的帐户**”下请求“**管理**”权限。有关更多信息，请参阅“自定义角色”。

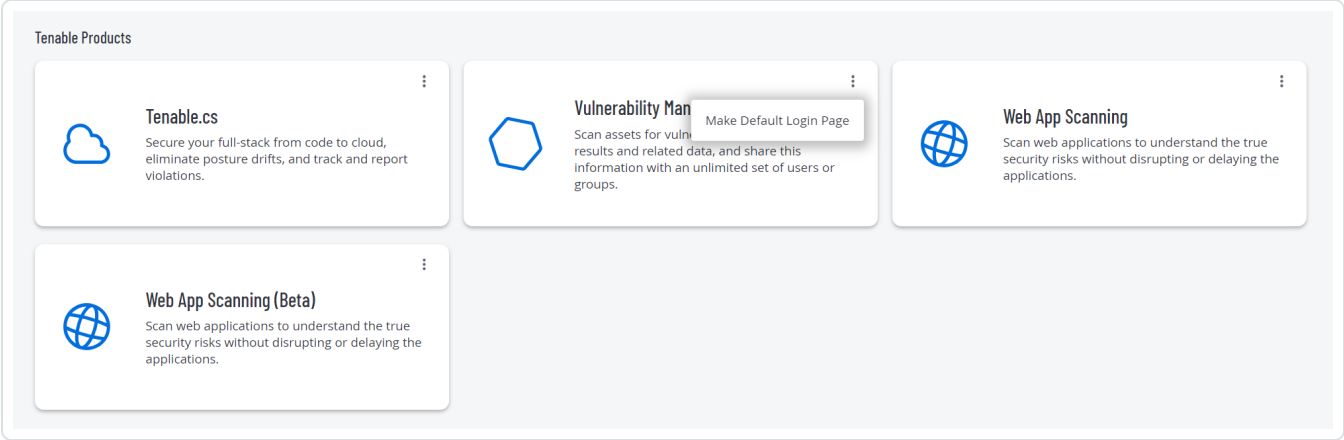
若要设置默认登录应用程序，请执行以下操作：

1. 登录 Tenable。

   此时会出现“**Workspace**”页面。

2. 在要选择的应用程序右上角，单击 ⋮ 按钮。

   此时会出现菜单。



3. 在菜单中，单击“**设为默认登录页面**”。

   现在当您登录时，会出现此应用程序。

移除默认应用程序

若要移除默认登录应用程序，请执行以下操作：

1. 登录 Tenable。

   此时会出现“**Workspace**”页面。

2. 在要移除的应用程序右上角，单击 ⋮ 按钮。

   此时会出现菜单。

3. 单击“**移除默认登录页面**”。

   现在当您登录时，将显示**“Workspace”**页面。

用户首选项

您可以在 Tenable Identity Exposure 中设置用户首选项。

- 选择语言的步骤：
- 选择配置文件的步骤：
- 更改密码的步骤：
- 选择配置文件的步骤：

设置首选项的步骤：

1. 在 Tenable Identity Exposure 中，点击右上角的用户配置文件图标。

   此时会出现一个子菜单。

2. 选择“**我的帐户**”。

   出现“**首选项**”页面。

选择语言的步骤：

a. 在“**语言**”中，点击下拉列表的箭头，选择您想要使用的语言。

b. 单击“**保存**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新您的首选项。随后，用户界面会显示您选择的语言。

选择配置文件的步骤：

从一个安全配置文件切换到另一个配置文件会改变在仪表盘、小组件和跟踪事件流上 Tenable Identity Exposure 显示的指标配置和数据表示形式的方式。

a. 在“**首选项**”下，点击“**配置文件**”。

b. 连接到 Tenable Identity Exposure 后，在“**首选配置文件**”中点击下拉箭头，选择默认配置文件。

c. 单击“**保存**”。

此时会出现一条消息，确认 Tenable Identity Exposure 已更新您的首选项。

有关更多信息，请参阅“安全配置文件”。

更改密码的步骤：

> **注意**：如果您拥有 Tenable One 许可证，则无法使用密码信息，在这种情况下，Tenable Vulnerability Management 会管理您的所有身份验证设置。有关更多信息，请参阅《Tenable Vulnerability Management 用户指南》中的访问控制。

a. 在“**首选项**”下，点击“**凭据**”。

b. 提供以下内容：

- 您的旧密码。
- 您的新密码。

c. 在“**新密码确认**”框中，重新输入新密码。

d. 单击“**保存**”。

此时会出现一条消息，确认 Tenable Identity Exposure 已更改您的密码。

> **注意**：在 Tenable Identity Exposure 中，无法更改通过 LDAP 或 SAML 等外部提供程序连接的帐户的密码。

管理 API 密钥的步骤：

a. 在“**首选项**”下，点击“**API 密钥**”。

   此时您的访问令牌会出现在“**当前 API 密钥**”框中。

b. 您可以执行以下操作：

c. 点击 图标，API 密钥复制到剪贴板，根据需要使用。

d. 点击“**刷新 API 密钥**”，生成新的访问令牌。

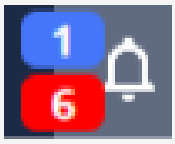
   此时会显示一条消息，要求您确认。

   > **注意**：刷新 API 密钥会导致 Tenable Identity Exposure 停用当前令牌。

更多详细信息，请参阅"使用公共 API"。

通知

在 Tenable Identity Exposure 主页的右上角，铃铛图标及其计数牌可以通知等待确认的攻击警报和/或风险暴露警报。在收到新的警报时，Tenable Identity Exposure 会增加通知计数牌中的数字。

	**蓝色**	风险暴露警报
	红色	攻击警报

若要显示警报，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击铃铛图标。

   “**警报**”窗格随即打开。

2. 请执行下列操作之一：
   - 点击“**风险暴露警报**”选项卡可显示风险暴露警报。
   - 点击“**攻击警报**”选项卡可显示攻击警报。

     关联警报列表随即出现。

若要查看与警报关联的事件，请执行以下操作：

1. 从列表中选择一个警报，然后点击“**操作**”>“**查看异常行为**”。

   “事件详细信息”窗格随即打开，其中包含以下信息：
   - 源(事件收集器)
   - 对象类型
   - 文件
   - 路径
   - 受影响的域
   - 日期
   - 具有事件发生时的值和当前值的属性列表

2. 点击“**异常行为**”选项卡。

   “**异常行为**”窗格随即打开，其中包含与该事件相关的异常行为列表。

3. 点击“**n/n 个指标**”可显示触发警报的风险暴露指标的窗格。
4. 点击“**n/n 个原因**”可显示警报原因。
5. 点击箭头可展开或折叠警报信息。
6. 点击指标名称可显示“指标详细信息”页面。

若要存档警报，请执行以下操作：

查看警报后，可以对其进行存档。

1. 在“**警报**”窗格中的警报列表中，选中要存档的警报的复选框。
   - 或者，可以点击窗格底部的“**已选 n/n 个对象**”的复选框来批量选择所有警报。
2. 在窗格底部，点击“**选择操作**”>“**存档**”。
3. 单击“**确定**”。

仪表盘

仪表盘允许将影响 Active Directory 安全性的数据和趋势可视化。可以使用小组件对其进行定制，以便根据个人要求显示图表和计数器。

Tenable Identity Exposure 提供仪表盘模板，您可以使用这些模板重点关注与贵组织有关的优先级问题，模板如下：

- **AD 合规性和首要风险**：合规性分数、演变和风险严重程度合规性
- **AD Risk 360**：异常行为演变和按风险暴露指标严重程度分类的问题
- **密码管理风险**：与密码相关的问题
- **用户监控**：AD 用户演变、用户类别计数
- **本机管理员监控**：管理帐户指标

若要使用模板创建新仪表盘，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“  ”或“**仪表盘**”。（此页面默认也会在 Tenable Identity Exposure 中打开。）
2. 您可以执行以下任一操作：
    - 如果窗格为空：点击“**添加仪表盘**”。
    - 如果窗格已包含至少一个仪表盘：点击右上角的“  ”>“**添加新仪表盘**”。

      此时会打开“**配置仪表盘模板**”窗格。
3. 选择要添加的仪表盘。
4. 点击“**添加仪表盘**”。
5. 此时会出现一条消息，确认 Tenable Identity Exposure 已创建仪表盘和小组件。新仪表盘会在“**仪表盘**”窗格的选项卡下显示。

若要添加自定义仪表盘，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“  ”或“**仪表盘**”。（此页面默认也会在 Tenable Identity Exposure 中打开。）
2. 点击右上角的“  ”>“**添加新仪表盘**”。

   此时会打开“**配置仪表盘模板**”窗格。
3. 在底部选择“**自定义仪表盘**”模板。
4. 为仪表盘输入名称。
5. 点击“**添加仪表盘**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已创建仪表盘。新仪表盘会在“**仪表盘**”窗格的选项卡下显示。
6. 请参阅“小组件”以了解如何将小组件添加至仪表盘。

若要重命名仪表盘，请执行以下操作：

1. 在“**仪表盘**”窗格中，选择要重命名的仪表盘的选项卡。
2. 点击右上角的“”>“**编辑名称**”。

   “**配置仪表盘**”窗格随即打开。
3. 在“**名称**”框中，为仪表盘输入另一名称。
4. 单击“**编辑**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新仪表盘。

若要删除仪表盘，请执行以下操作：

1. 在“**仪表盘**”窗格中，选择要删除的仪表盘的选项卡。
2. 点击右上角的“”>“**删除仪表盘**”。

   “**删除仪表盘**”窗格随即打开，并要求您确认删除。
3. 点击“**删除**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已删除仪表盘。

小组件

仪表盘中的小组件能以条形图、折线图和计数器的形式将 Active Directory 数据可视化。可以定制小组件以显示特定信息。拖动小组件可以将其放置在仪表盘上的不同位置。

可以向新建的仪表盘或现有仪表盘添加小组件。

若要向仪表盘添加小组件，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“  ”或“**仪表盘**”。（此页面默认也会在 Tenable Identity Exposure 中打开。）
2. 在“仪表盘”窗格中，选择“仪表盘”选项卡。
3. 您可以执行以下操作之一：
   - 如果仪表盘为空：点击“**添加小组件**”。
   - 如果仪表盘已包含小组件：点击右上角的“  ”>“**向当前仪表盘添加小组件**”。

     此时会打开“**添加小组件**”窗格。
4. 点击某个磁贴以选择下列选项之一：
   - 条形图
   - 线形图
   - 计数器
5. 在“**小组件名称**”框中，输入该小组件的名称
6. 在“**小组件配置**”下的“**数据类型**”框中，点击下拉列表上的箭头，以选择下列选项之一：
   - 用户计数：域的活动用户数量。
   - 异常行为计数：检测到的异常行为数量或安全漏洞数量。
   - 合规性分数：0-100 分，由 Tenable Identity Exposure 通过核算检测到的异常行为数量及其严重性而计算得出。
   - 持续时间（适用于折线图）：点击下拉列表上的箭头以选择要显示的持续时间。

7. 在“**数据集配置**”下：

数据集配置	
状态(用户计数)	选择“活动”、“非活动”或“全部”。
指标	a. 点击“**指标**”以选择一个或多个指标。 此时会打开“**风险暴露指标**”窗格。 b. 从列表中选择一个或多个指标。或者还可以： ■ 在搜索框中输入指标名称。 ■ 选择所有指标。 ■ 选择某个严重程度(“严重”、“高危”、“中危”或“低危”)的所有指标。 c. 单击“**按所选结果筛选**”。
域	a. 点击“**域**”以选择一个或多个域。 此时会打开“**林和域**”窗格。 b. 从列表中选择一个域。或者还可以： ■ 在搜索框中输入域名。 ■ 选择所有域。 c. 单击“**按所选结果筛选**”。

8. 在“**数据集的名称**”中，输入该数据集的名称。
9. 选择小组件的域。

   或者，在搜索框中输入域名。
10. 单击“**按所选结果筛选**”。
11. 或者，可以点击“**添加新数据集**”，以为小组件添加另外一个含不同选项的数据集。
12. 点击“**添加**”。

    此时会出现一条消息，确认 Tenable Identity Exposure 已添加小组件。

若要修改小组件，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“**仪表盘**”。
2. 选择包含要修改的小组件的仪表盘。
3. 选择该小组件。
4. 点击小组件右上角的 图标。

   此时会打开“**修改小组件**”窗格。
5. 根据需要进行修改。
6. 单击“**编辑**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新小组件。

若要刷新小组件，请执行以下操作：

1. 选择该小组件。
2. 点击小组件右上角的 图标。

   小组件随即刷新。

若要删除小组件，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“**仪表盘**”。
2. 选择包含要删除的小组件的仪表盘。
3. 选择该小组件。
4. 点击 图标。

   “删除小组件”窗格随即打开。此时会显示一条消息，要求您确认删除。
5. 点击“**确定**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已从仪表盘删除小组件。

另请参阅：

- 仪表盘

Identity Explorer

权限：如要访问 Microsoft Entra ID 的配置和数据可视化，您的用户角色必须具有相应的权限。有关更多信息，请参阅"设置角色的权限"。

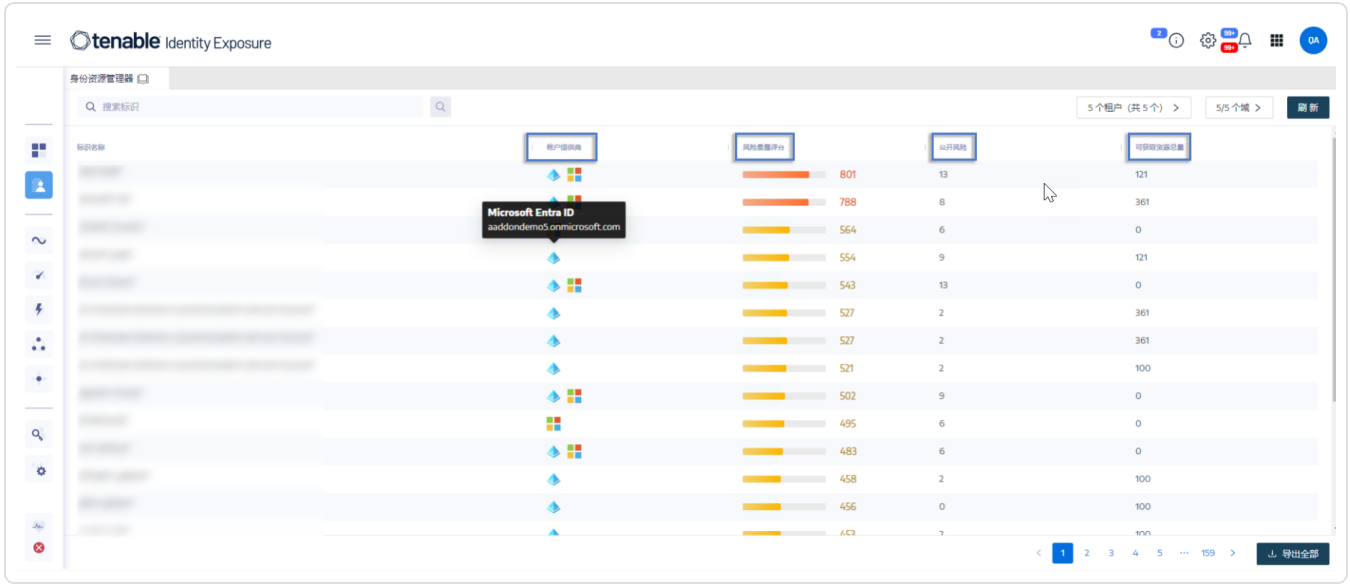
Tenable Identity Exposure 的 Identity Explorer 视图统一了 Active Directory 和 Microsoft Entra ID 中的标识。此视图显示每个列出资产的标识风险评分(测试版)以及标识遭到破坏的潜在范围。

若要访问 Identity Explorer，请执行以下操作：

注意：仅当使用 Microsoft Entra ID 功能时，Identity Explorer 才可见。有关更多信息，请参阅"Microsoft Entra ID 支持"。

- 在 Tenable Identity Exposure 中，点击左侧导航栏中的"Identity Explorer"图标 。

  "**Identity Explorer**"窗格随即打开。



"**Identity Explorer**"窗格显示所有可访问资源的以下信息：

- **标识名称** - 标识提供程序下的用户帐户名称。
- **帐户提供程序** - 标识提供程序。

- **风险暴露评分** - Tenable Identity Exposure 通过为每个标识提供程序评估资产或标识及其漏洞的重要性来计算此指标，并将其汇总以提供给定标识的总体风险暴露评分。

  注意：Tenable Identity Exposure 仅在您拥有 Tenable One 许可证时才显示风险暴露评分。

- **未化解的风险**：Microsoft Entra ID 风险暴露指标在扫描资产时检测到的结果数量。有关更多信息，请参阅"与 Microsoft Entra ID 相关的风险暴露指标"。
- **可访问资源总数** - 此资产可访问（读取、写入等）的任何类型的资源数量

如要搜索标识，请执行以下操作：

1. 在"**Identity Explorer**"窗格的**搜索**框中，键入用户或帐户的名称。
2. 点击 图标。

   Tenable Identity Exposure 显示匹配结果。

如要导出标识，请执行以下操作：

1. 在"**Identity Explorer**"窗格的底部，点击"**导出全部**"。

   "**导出标识**"窗格随即打开。

2. 点击"**导出全部**"。

   Tenable Identity Exposure 将文件下载到本地计算机。

跟踪事件流

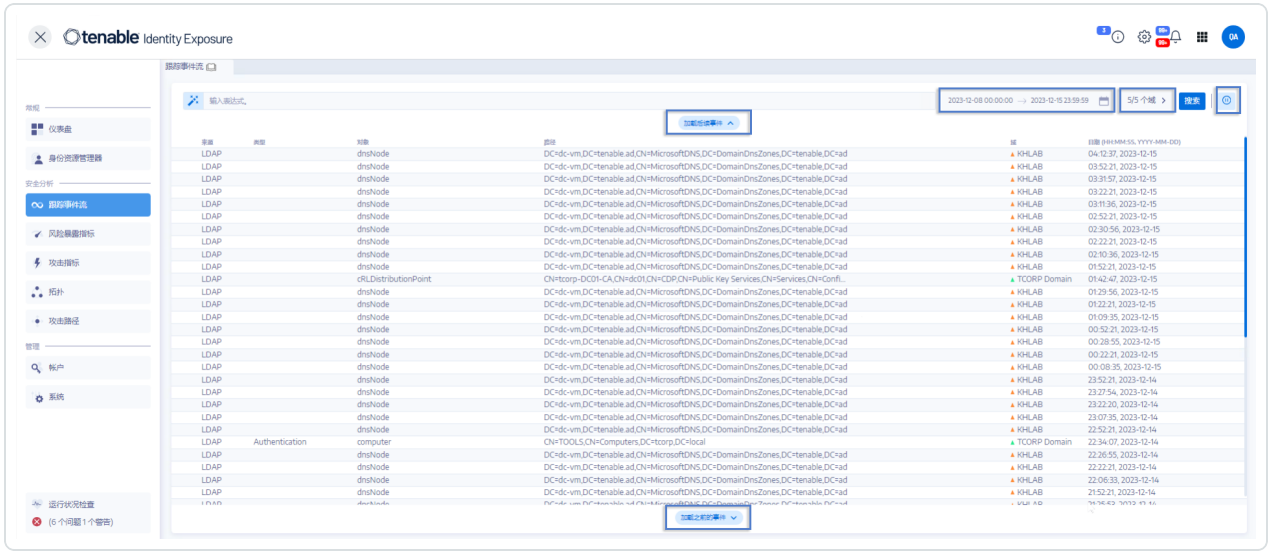
Tenable Identity Exposure 的“跟踪事件流”显示影响 AD 基础设施的事件的实时监控和分析。它允许您识别危急漏洞及其建议的修复过程。

可以使用“**跟踪事件流**”页面，返回到过去并加载以前的事件或搜索特定事件。还可以使用此页面顶部的搜索框搜索威胁和检测恶意模式。

若要访问“跟踪事件流”，请执行以下步骤：

- 在 Tenable Identity Exposure 中，点击左侧导航栏中的“**跟踪事件流**”。

  “跟踪事件流”页面随即打开，其中包含事件列表。有关更多信息，请参阅““跟踪事件流”表”。



若要选择时间范围，请执行以下操作：

1. 在“**跟踪事件流**”页面顶部，点击日历框。
2. 选择开始日期和结束日期。
3. 点击“**搜索**”。

   Tenable Identity Exposure 使用所选时间范围更新“跟踪事件流”表。

若要选择域，请执行以下操作：

1. 在“**跟踪事件流**”页面的顶部，点击“**n/n 个域 >**”。

   “**林和域**”窗格随即打开。

2. 选择林和域。

3. 单击“**按所选结果筛选**”。

   Tenable Identity Exposure 使用所选林和域的信息更新“跟踪事件流”表。

若要查看事件，请执行以下操作：

- 在“跟踪事件流”表中，点击包含要了解的事件的行。

  “事件详细信息”窗格随即打开。有关更多信息，请参阅“事件详细信息”。

若要暂停和重新启动“跟踪事件流”，请执行以下操作：

- 请执行下列操作之一：
  - 点击 ⏸ 图标可暂停“跟踪事件流”。

    暂停“跟踪事件流”会停止最近事件的自动垂直滚动，同时分析会在后台继续运行，并允许针对事件进行搜索。
  - 点击 ▶ 图标可重新启动“跟踪事件流”。

若要加载后面的或以前的事件，请执行以下操作：

- 在“跟踪事件流”页面中，执行下列操作之一：
  - 点击“加载后面的事件”
  - 点击“加载以前的事件”

“跟踪事件流”表

Tenable Identity Exposure 会在事件发生时，在“跟踪事件流”表中持续列出 Active Directory 中的事件。它包含以下信息：

信息	说明
源	指示 AD 基础设施中任何与安全相关的更改的源。 有两个可能的来源： • 用于与 AD 基础设施通信的轻型目录访问协议 (LDAP)。 • 用于共享文件、打印机等内容的服务器消息块 (SMB) 协议。 **Tenable Identity Exposure** 会彻底分析网络上的 LDAP 和 SMB 流量，以检测异常情况和潜在威胁。 **注意**：Active Directory (AD) 允许管理员创建组策略，以控制在用户和计算机帐户上部署的设置。组策略对象 (GPO) 可存储这些控制设置。Sysvol 文件夹会在域控制器上存储 GPO 文件。为了 AD 的安全性，监控 GPO 的内容非常重要，因为每个域成员都可以高级特权应用或执行这些内容。
类型	显示事件的特征元素，如： • 已更改 ACL • 已更改 SPN • 已删除成员 • 新成员 • 新的信任 • 添加了未知文件类型 • 新对象 • 已删除对象 • 已更改密码 • 已更改 UAC

	• 链接了新的 GPO • 已删除 GPO 链接 • 所有者更改 • 已重命名文件 • 已创建 SPN • 身份验证重设失败 • 身份验证失败
对象	指示与 AD 对象关联的类或文件扩展名。可以搜索目录对象(用户、计算机等) 或具有特定文件扩展名 (ini、xml、csv) 的文件。
路径	指示 AD 对象的完整路径，以在 AD 中标识此对象的唯一位置。
目录	指示 AD 基础设施中的更改来自哪个目录。
日期	指示事件的时间。

使用向导搜索"跟踪事件流"

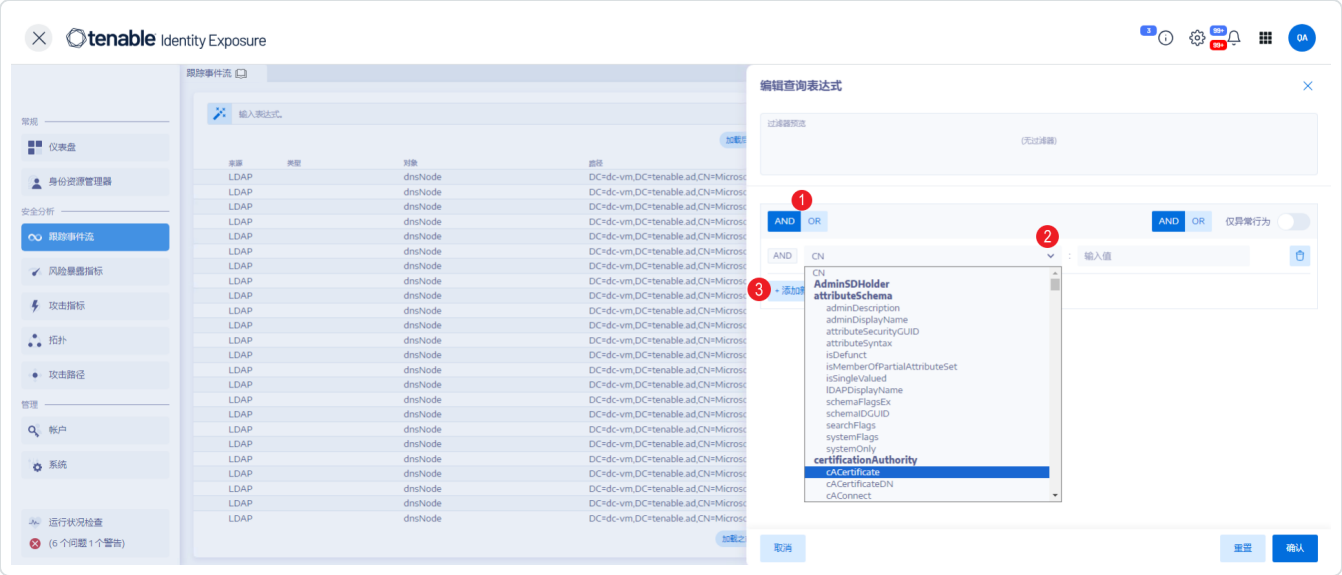
搜索向导允许创建和合并查询表达式。

- 在搜索框中使用常用表达式时，可以将其添加到书签列表，以供以后使用。
- 在搜索框中输入表达式时，Tenable Identity Exposure 会在其"历史记录"窗格中保存此表达式，以供重复使用。

若要使用向导搜索，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击"**跟踪事件流**"以打开"跟踪事件流"页面。
2. 点击 图标。

   "**编辑查询表达式**"窗格随即打开。有关更多信息，请参阅"自定义跟踪事件流查询"。



3. 要在面板中定义查询表达式，请点击要应用于第一个条件的 **AND** 或 **OR** 运算符按钮 (1)。
4. 从下拉菜单中选择属性，然后输入其值 (2)。
5. 执行以下任一操作：
   - 要添加属性，请点击"**+ 添加新规则**"(3)。
   - 要添加其他条件，请点击"**添加新条件**"**+AND** 或 **+OR** 运算符。从下拉菜单中选择属性，然后输入其值。

- 要将搜索限制为异常对象，请点击“**仅异常**”开关以允许这样做。选择 **+AND** 或 **+OR** 运算符以向查询添加条件。
- 要删除条件或规则，请点击 图标。

6. 点击“**验证**”运行搜索，或点击“**重置**”修改查询表达式。

另请参阅：

- 手动搜索“跟踪事件流”
- 使用向导搜索“跟踪事件流”
- 自定义跟踪事件流查询
- 书签查询
- 查询历史记录

手动搜索"跟踪事件流"

若要过滤与特定字符串或模式匹配的事件，可以在搜索框中输入表达式，以使用布尔运算符 ***、AND** 和 **OR** 优化结果。可以将 **OR** 语句放在括号中，以便修改搜索优先级。搜索操作会查找 Active Directory 属性中的任何特定值。

若要手动搜索跟踪事件流，请执行以下操作：

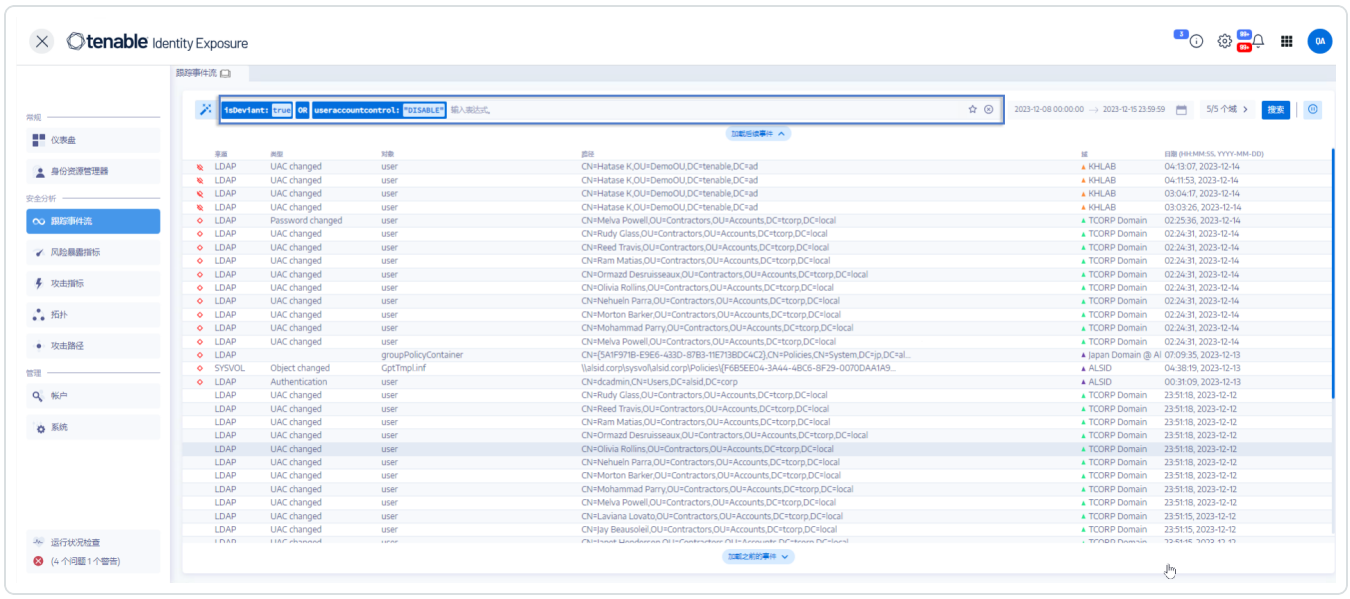
1. 在 Tenable Identity Exposure 中，点击"**跟踪事件流**"以打开"跟踪事件流"页面。
2. 在搜索框中，输入查询表达式。
3. 可以按如下方式过滤搜索结果：
    - 点击"**日历**"框以选择开始日期和结束日期。
    - 点击"**n/n 个域**"以选择林和域。
4. 点击"**搜索**"。

    Tenable Identity Exposure 使用与搜索条件匹配的结果更新列表。

示例：

以下示例可搜索：

- 可危及受监控 AD 基础设施的已停用的用户帐户。
- 可疑活动和异常帐户使用。



语法和句法

手动查询表达式会使用以下语法和句法：

- 语法：`EXPRESSION [OPERATOR EXPRESSION]*`
- 句法：`__KEY__ __SELECTOR__ __VALUE__`

  其中：

  - `__KEY__` 指的是要搜索的 AD 对象属性（如 `CN`、`userAccountControl`、`members` 等）。
  - `__SELECTOR__` 指运算符 `:`、`>`、`<`、`>=`、`<=`。
  - `__VALUE__` 指要搜索的值。

    可以使用更多键来查找特定内容：

  - `isDeviant` 可查找造成异常行为的事件。

可以使用 **AND** 和 **OR** 运算符组合多个跟踪事件流查询表达式。

示例：

- 在通用名称属性中查找包含字符串 `alice` 的所有对象：`cn:"alice"`
- 在通用名称属性中查找每个包含字符串 `alice` 且创建了特定异常行为的所有对象：`isDeviant:"true" and cn:"alice"`
- 查找 GPO 命名的默认域政策：`objectClass:"groupPolicyContainer" and displayname:"Default Domain Policy"`
- 查找 SID 中包含 S-1-5-21 的所有已停用帐户：`userAccountControl:"DISABLE"` 和 `objectSid:"S-1-5-21"`
- 在 Sysvol 中查找所有 `script.ini` 文件：`globalpath:"sysvol" and types:"SCRIPTSini"`

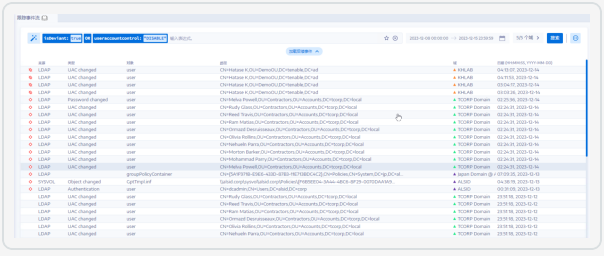
  > **注意**：此处，`types` 是指对象属性，而不是列标头。

自定义跟踪事件流查询

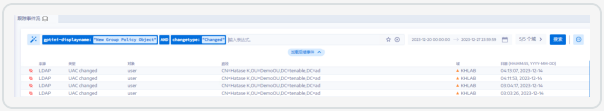
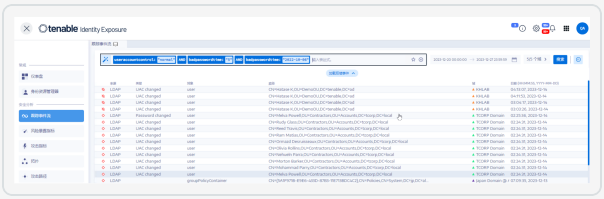
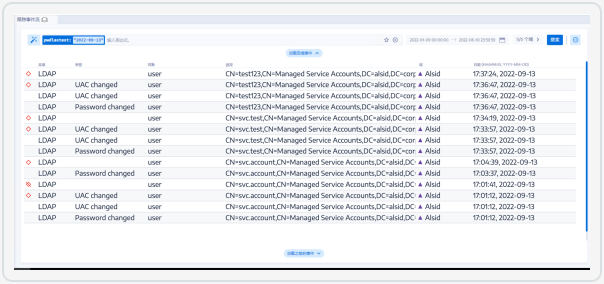
跟踪事件流支持将 Tenable Identity Exposure 功能扩展到风险暴露指标和攻击指标的默认监控之外。您可以创建自定义查询以快速检索数据，并将查询用作 Tenable Identity Exposure 可发送到您的安全信息和事件管理 (SIEM) 的自定义警报。

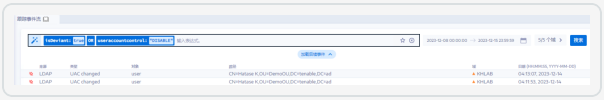
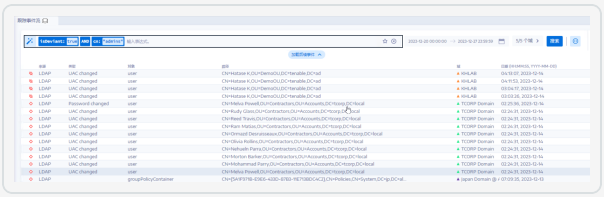
以下示例显示了 Tenable Identity Exposure 中的实际自定义查询。

用例	描述

GPO 启动和关机二进制文件以及全局 SYSVOL 路径监控	监控引导启动路径和/或全局 SYSVOL 复制路径中的脚本。攻击者经常使用这些脚本滥用本机 AD 服务，以便在整个环境中快速传播勒索软件。
	• **启动路径查询中的脚本：**
	`"sysvol" AND types: "Scriptsini"`
	注意：此处，types 指的是对象属性而非列标头。
	• **SYSVOL 监控查询**：
	`globalpath:"sysvol" AND (globalpath:".ps1" OR globalpath:".msi" OR globalpath:".bat" OR globalpath:".exe")`
	 

GPO 配置的修改	监控 GPO 配置的修改。攻击者经常使用此方法降级安全设置，以协助持久性和/或帐户接管。 • **GPO 监控查询：** `gptini-displayname:"New Group Policy`

	Object" AND changetype:"Changed" 
身份验证和密码重设失败	监控导致锁定的多次失败身份验证尝试，这可作为暴力破解尝试的早期警告标记。 **注意**：您必须设置锁定策略和日期/时间变量。有关更多信息，请参阅“使用 Tenable Identity Exposure 帐户进行身份验证”。 • **身份验证查询失败：** useraccountcontrol:"Normal" AND badpwdcount:"<ACCOUNT_LOCKOUT_THRESHOLD>“ AND badpasswordtime:”<DATE_TIME_STAMP>“  • **密码重置查询：** pwdlastset:"<DATE_TIME_STAMP" 
添加、删除或更改对象权限	监控对 ACL 权限和相关对象权限集的未经授权的修

	改。攻击者滥用此方法来提升权限。 **注意**:您必须提供日期/时间变量。 • **对象权限查询:** `ntsecuritydescriptor:0 AND whenchanged:"DATE_TIME_STAMP"` 
导致异常行为的管理员变更	内置管理群组和自定义群组是敏感群组,需要密切监控可引入风险的异常行为或配置变更。此查询可让您快速查看最近可能对 admins 组内的安全设置产生负面影响的更改。 • **对管理员查询的变更:** `isDeviant:true AND cn:"admins"` 

另请参阅:

- 手动搜索"跟踪事件流"
- 使用向导搜索"跟踪事件流"
- 书签查询
- 查询历史记录
- 跟踪事件流用例

书签查询

使用常见查询表达式时，可以将其添加到定制书签列表，以供再次使用。

若要为查询表达式添加书签，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“**跟踪事件流**”以打开“跟踪事件流”页面。
2. 点击搜索框旁的 图标。

   “**编辑查询表达式**”窗格随即打开。
3. 在搜索框中输入查询表达式。
4. 点击搜索框右侧的 ☆ 图标。

   “**添加到书签**”框随即出现。
5. 在“**选择文件夹**”框中，点击下拉箭头，从列表中选择一个文件夹。
6. （可选）点击以将“**新建文件夹**”开关切换为“**是**”。在“**文件夹名称**”框中，输入书签文件夹的名称。
7. 在“**书签名称**”框中，输入书签的名称。
8. 点击“**添加**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已将书签添加到列表。

若要使用加过书签的查询表达式，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“**跟踪事件流**”以打开“跟踪事件流”页面。
2. 点击搜索框内部。

   “**历史记录**”和“**书签**”选项卡出现在搜索框下方。
3. 点击“**书签**”选项卡。

   书签列表随即出现。
4. 点击书签以将其选中。

   Tenable Identity Exposure 加载查询表达式并运行搜索。

若要管理书签，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“**跟踪事件流**”以打开“跟踪事件流”页面。
2. 点击搜索框内部。

   “**历史记录**”和“**书签**”选项卡出现在搜索框下方。
3. 点击“**书签**”选项卡。

   书签列表随即出现。
4. 点击“**管理书签**”。

   “**书签**”窗格随即打开。
5. 执行以下任一操作：
   - 搜索书签：
     a. 在搜索框中键入书签名称。
     b. 从下拉列表中选择一个文件夹。
   - 编辑书签或书签文件夹的名称：
     a. 点击书签或书签文件夹的 图标。
     b. 在“**书签名称**”框或“**文件夹名称**”框中，输入书签或书签文件夹的新名称。
     c. 单击“**编辑**”。

        此时会出现一条消息，确认 Tenable Identity Exposure 已更新书签或书签文件夹名称。
   - 删除书签文件夹的书签：
     - 点击书签或书签文件夹对应的 图标。

另请参阅：

- 手动搜索“跟踪事件流”
- 使用向导搜索“跟踪事件流”
- 自定义跟踪事件流查询

- 查询历史记录
- 跟踪事件流用例

查询历史记录

在搜索框中输入表达式时，Tenable Identity Exposure 会在其"历史记录"窗格中保存此表达式，以供重用。

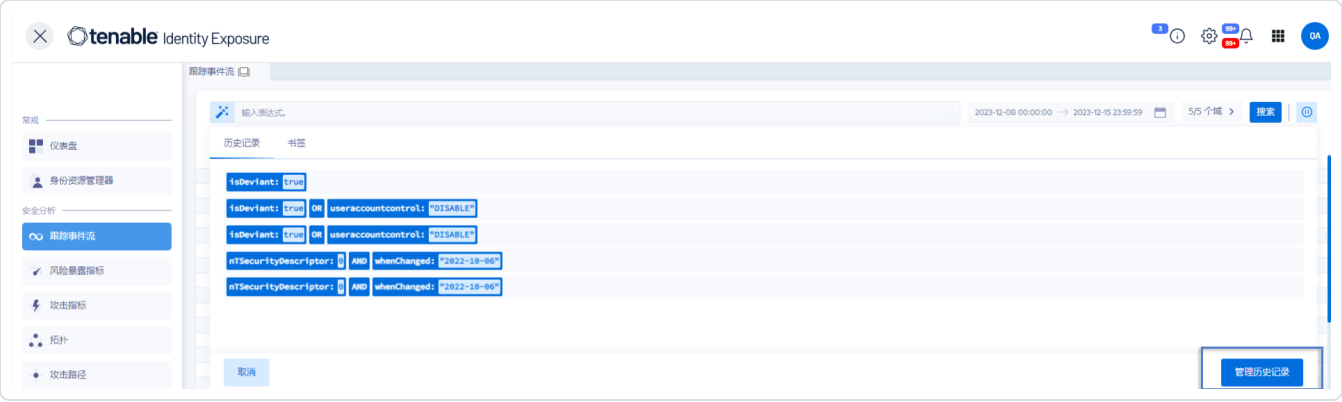
若要使用历史记录中的查询表达式，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击"**跟踪事件流**"以打开"跟踪事件流"页面。
2. 点击搜索框内部。

   "**历史记录**"和"**书签**"选项卡出现在搜索框下方。
3. 点击"**历史记录**"选项卡。

   查询表达式列表随即出现。
4. 点击以选择要使用的查询表达式。

   Tenable Identity Exposure 加载查询表达式并运行搜索。



若要管理查询表达式历史记录，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击"**跟踪事件流**"以打开"跟踪事件流"页面。
2. 点击搜索框内部。

   "**历史记录**"和"**书签**"选项卡出现在搜索框下方。
3. 点击"**历史记录**"选项卡。

   查询表达式列表随即出现。
4. 点击"**管理历史记录**"。

"**历史记录**"窗格随即打开。

5. 执行以下任一操作：

- 搜索查询表达式：
  a. 在搜索框中输入查询表达式。
  b. 点击"日历"框以选择开始日期和结束日期。
  c. 点击"**搜索**"。
- 若要从历史记录中删除查询表达式，请执行以下操作：
  - 点击 图标。
- 若要清除历史记录中的所有查询表达式，请执行以下操作：
  a. 点击"**清除选择**"。

     此时会显示一条消息，要求您确认删除。
  b. 点击"**确认**"。

另请参阅：

- 手动搜索"跟踪事件流"
- 使用向导搜索"跟踪事件流"
- 自定义跟踪事件流查询
- 书签查询
- 跟踪事件流用例

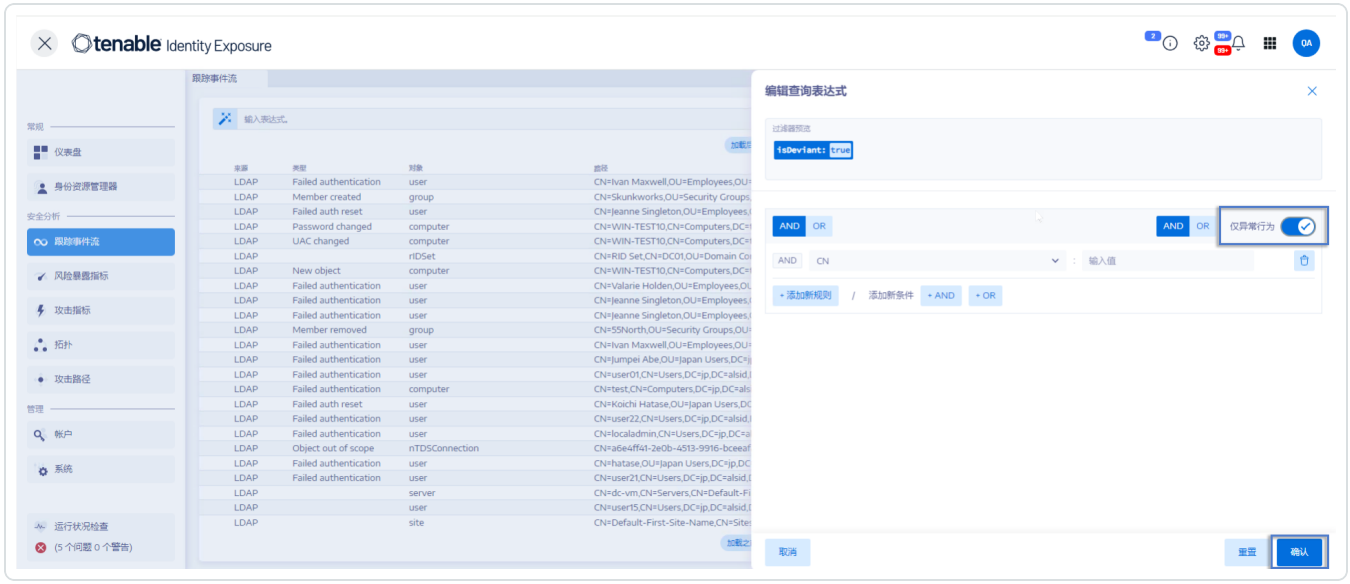
显示异常事件

可以直接将“跟踪事件流”表中的异常事件清零。

若要显示异常事件，请执行以下操作：

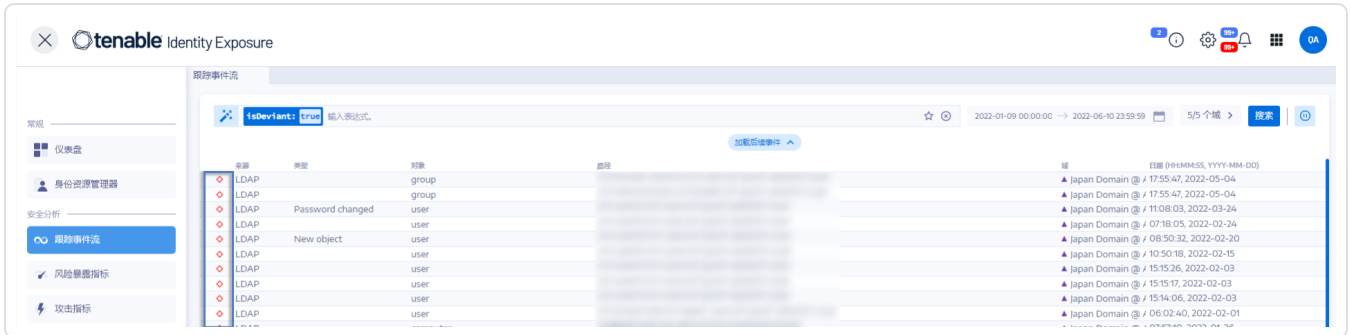
1. 在 Tenable Identity Exposure 中，点击“**跟踪事件流**”以打开“跟踪事件流”页面。
2. 点击搜索框旁的 图标。

   “**编辑查询表达式**”窗格随即打开。



3. 点击将“**仅异常行为**”开关切换为“允许”。
4. 点击“**验证**”。

   Tenable Identity Exposure 使用来源旁带有红色菱形的事件列表更新“跟踪事件流”表。



其中：

- ◇“跟踪事件流”在 Tenable Identity Exposure 安全配置文件中检测到异常行为。
- ◆“跟踪事件流”在其他安全配置文件中检测到异常行为。
- 显示更改解决了异常行为。

事件详细信息

Tenable Identity Exposure 中的"跟踪事件流"可提供有关影响 Active Directory (AD) 的每个事件的详细信息。可以在特定事件的详细信息中查看技术信息，并采取风险暴露指标 (IoE) 的严重程度所需的修复措施。

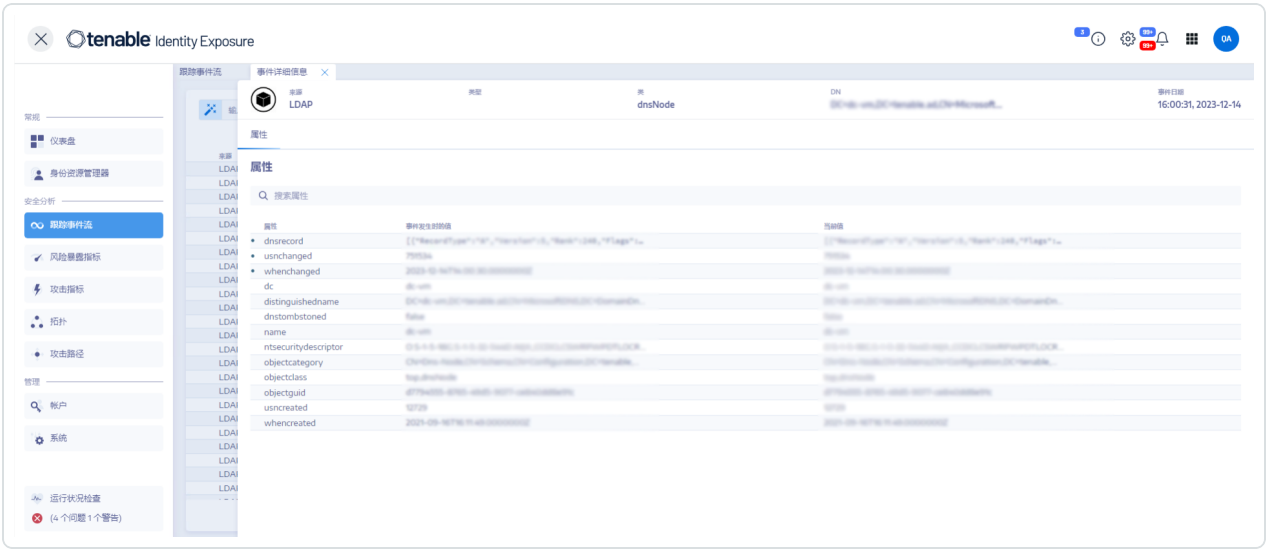
若要查看事件详细信息，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击"**跟踪事件流**"以打开"跟踪事件流"页面。
2. 点击以选择"跟踪事件流"表中的一个条目。

   "**事件详细信息**"窗格随即打开。

IoE、事件和异常对象

- **风险暴露指标** (IoE) 描述的是一种影响 AD 的威胁。Tenable Identity Exposure 的 IoE 可在收到事件后实时评估安全级别。IoE 可能包含数个技术漏洞。IoE 可针对检测到的漏洞、关联的异常对象和修复措施建议提供相关信息。
- "**事件**"表示与 AD 中出现的安全功能相关的变更。该变更可能是密码更改、用户创建、新 GPO 或修改后的 GPO、新的委派权限等。事件可将 IoE 的合规性状态从合规变为不合规。
- **异常对象**是一种技术元素，既可单独使用，亦可与另一个异常对象关联，以便 IoE 的攻击向量有效。



属性表

"属性"表包含以下列:

列	说明
属性	指示与已在"跟踪事件流"表中选择的事件关联的 AD 对象的属性。属性描述对象特性。多种属性可描述单个 AD 对象。
事件发生时的值	指示事件发生时的属性值。
当前值	指示用户查看 AD 时其中的属性值。

提示:若要显示事件发生前的属性值,请将鼠标悬停在左侧的蓝点上(如有)。

若要搜索属性,请执行以下操作:

- 在"**事件详细信息**"窗格的搜索框中输入字符串。

  Tenable Identity Exposure 将列表缩小到与搜索字符串匹配的属性。

有关更多信息,请参阅"属性更改"。

异常行为

如果"跟踪事件流"中的某个事件包含异常行为,"事件详细信息"窗格也会显示这些异常行为,以便深入了解问题根源。

若要显示异常行为,请执行以下操作:

1. 在 Tenable Identity Exposure 中,点击"**跟踪事件流**"以打开"跟踪事件流"页面。
2. 点击以选择"跟踪事件流"表中的一个条目。

   "**事件详细信息**"窗格随即打开。
3. 选择"**异常行为**"选项卡。

Tenable Identity Exposure 显示异常行为及触发此类行为的 IoE 的列表。

若要深入了解 IoE 的详细信息，请执行以下操作：

1. 在“**异常行为**”选项卡中，点击异常行为原因下方的 IoE 磁贴。

   “**指标详细信息**”窗格随即打开，其中包含异常对象列表和以下信息：

   - IoE 的名称
   - IoE 的严重程度（严重、高危、中危、低危）
   - IoE 状态
   - 最新检测的时间戳

2. 点击以下任一选项卡：

   - “**信息**”：包含关于此 IoE 的内部和外部资源。
   - “**漏洞详细信息**”：包括对在 AD 中检测到的漏洞的说明。
   - “**异常对象**”：包括技术详细信息和用于过滤对象的搜索框。
   - “**建议**”：有关如何解决此问题的提示。

属性更改

属性值更改后，“跟踪事件流”会在“**属性**”列前面显示一个蓝点。

若要显示属性更改，请执行以下操作：

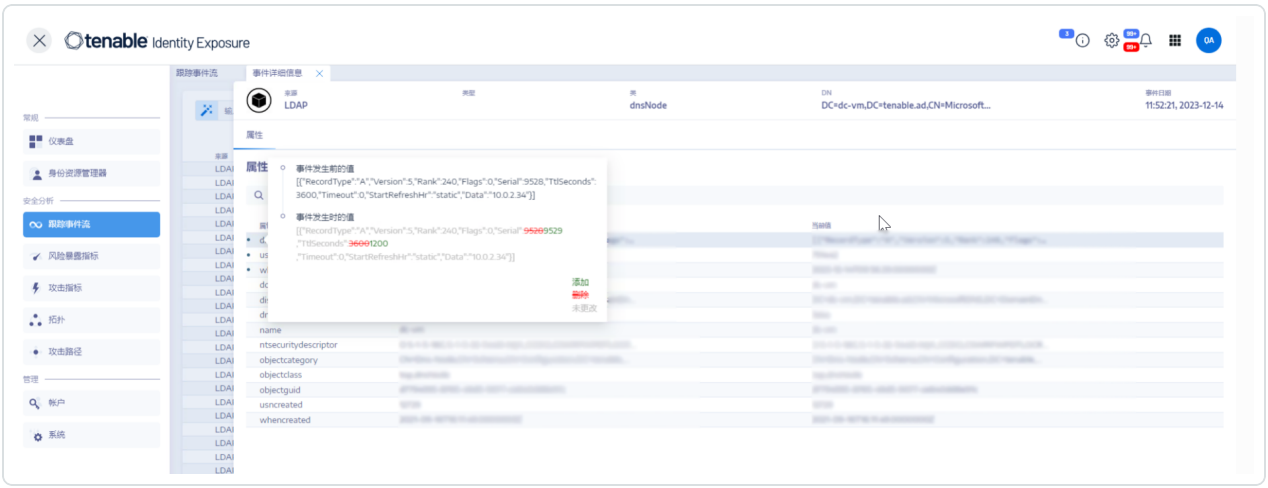
1. 在 Tenable Identity Exposure 中，点击左侧导航栏中的“**跟踪事件流**”。

   “**跟踪事件流**”页面随即打开，其中包含事件列表

2. 将鼠标悬停在事件行前面的蓝点上，即可显示更改。

   事件发生时的值标签的不同颜色表示应用到属性的不同更改：

   - 绿色：**添加**
   - 红色：**删除**
   - 灰色：**未更改**



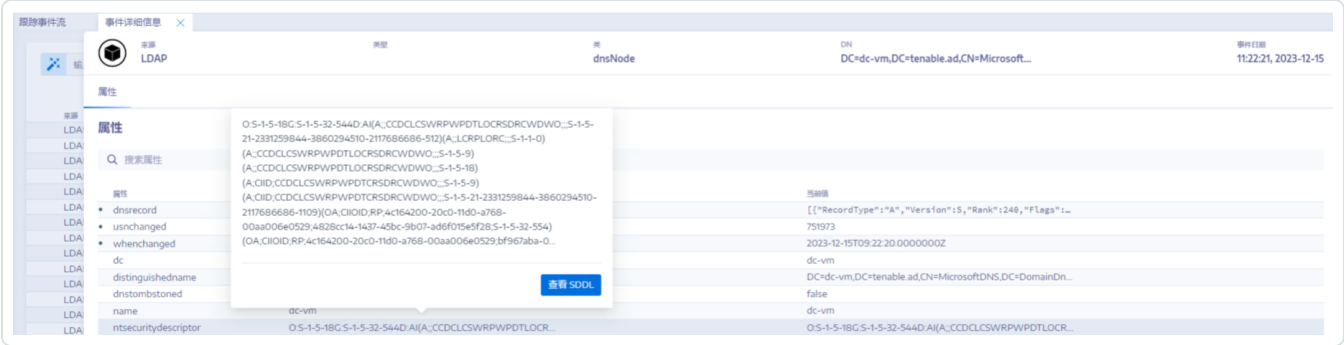
“ntsecuritydescriptor”属性

安全描述符是一种数据结构，包含有关 AD 对象的安全信息，例如其所有权和权限。更多详细信息，请参阅 Microsoft 的在线文档。

若要显示对象安全描述符的详细信息，请执行以下操作：

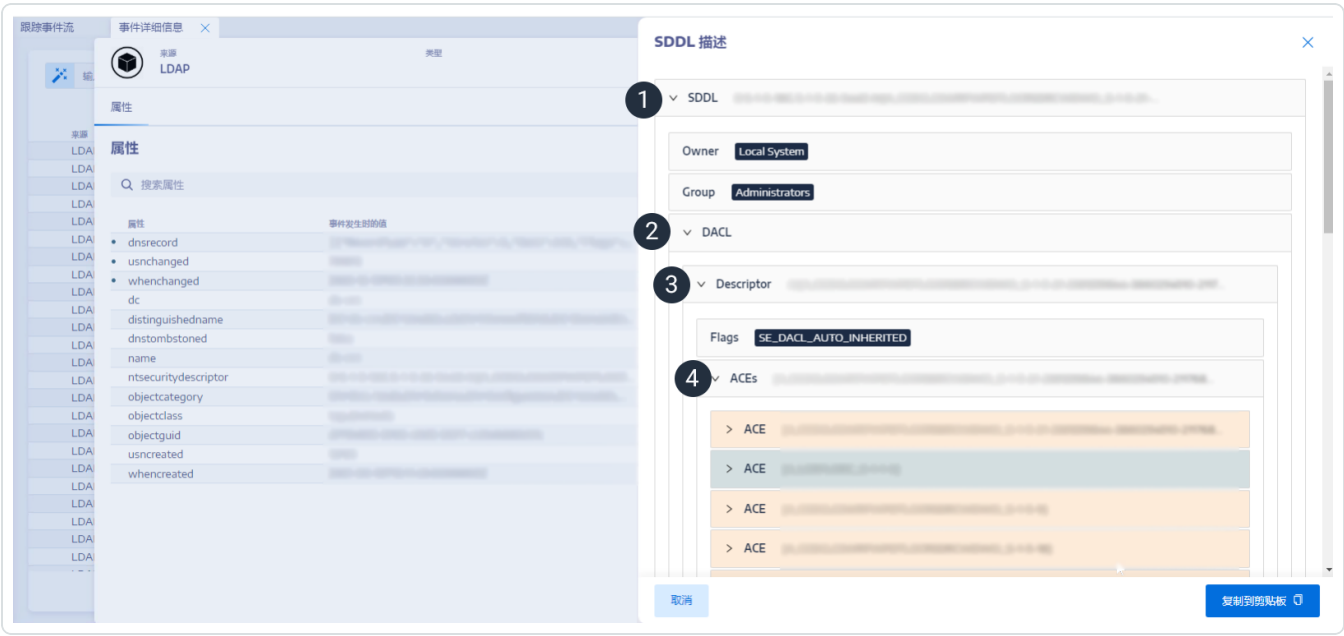
1. 在 Tenable Identity Exposure 中，点击“**跟踪事件流**”以打开“跟踪事件流”页面。
2. 点击以选择“跟踪事件流”表中的一个条目。

   “**事件详细信息**”窗格随即打开。
3. 将鼠标悬停在 `ntsecuritydescriptor` 属性条目（“事件发生时的值”或“当前值”列）上**。



4. 点击“**查看 SDDL 描述**”。

   “**SDDL 描述**”窗格随即打开。
5. 点击 SDDL (1)、DACL (2) 和描述符 (3) 左侧的箭头，以展开描述：



6. 找到以彩色突出显示的访问控制条目 (ACE)(4)，其中会显示对象的访问权限。颜色代码表示：

- **红色**:为用户分配了危险权限,但他们不得拥有对象的访问权限。
- **橙色**:将危险权限分配给了通常允许拥有此类权限的特权用户(例如:域管理员)。
- **绿色**:无危险权限。

7. 若要复制 SDDL 描述,请点击"**复制到剪贴板**"。

跟踪事件流用例

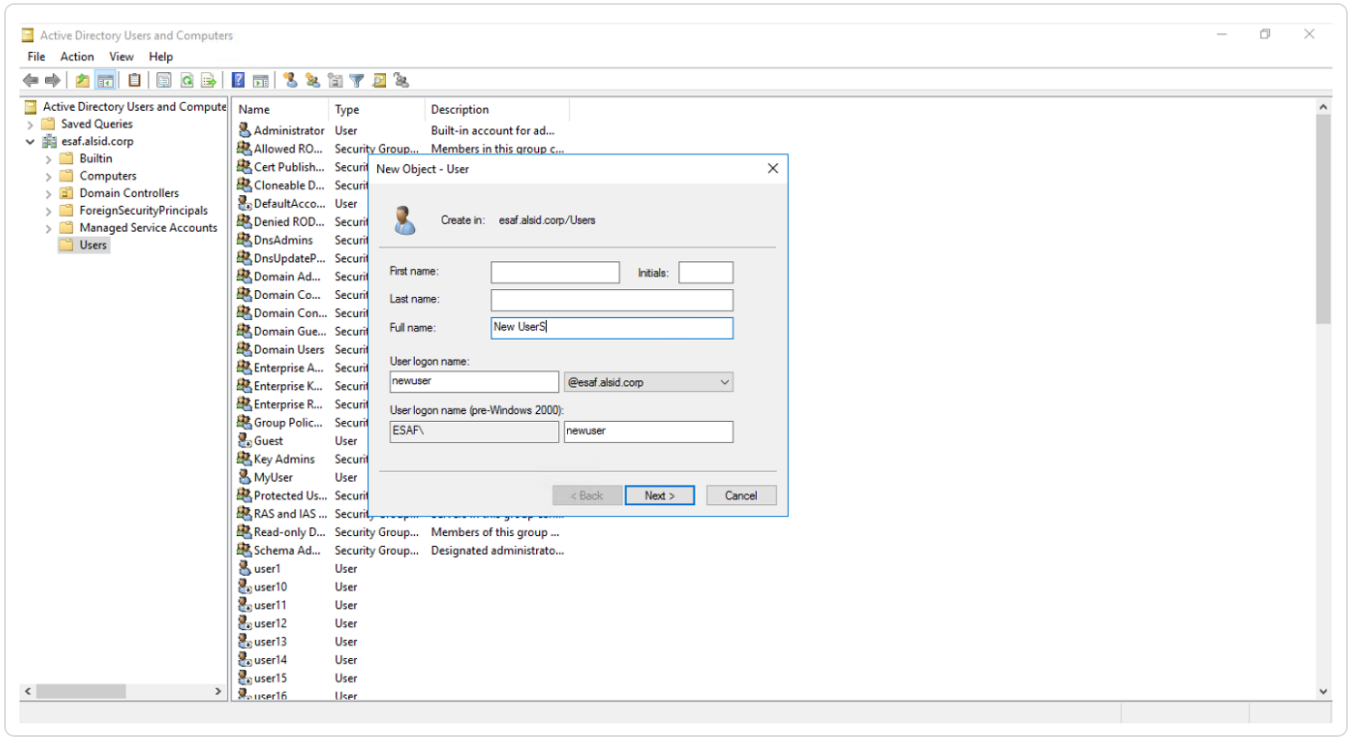
要了解“跟踪事件流”行为，有两个示例可以说明在 Active Directory (AD) 界面中执行的操作如何反映在“跟踪事件流”页面中。

每个示例都会将管理员端（在 AD 界面中）的数据与最终用户端（在 Tenable Identity Exposure 中）的数据进行比较。无论使用应用程序、API 还是服务对 AD 执行操作，“跟踪事件流”上的结果均相同。

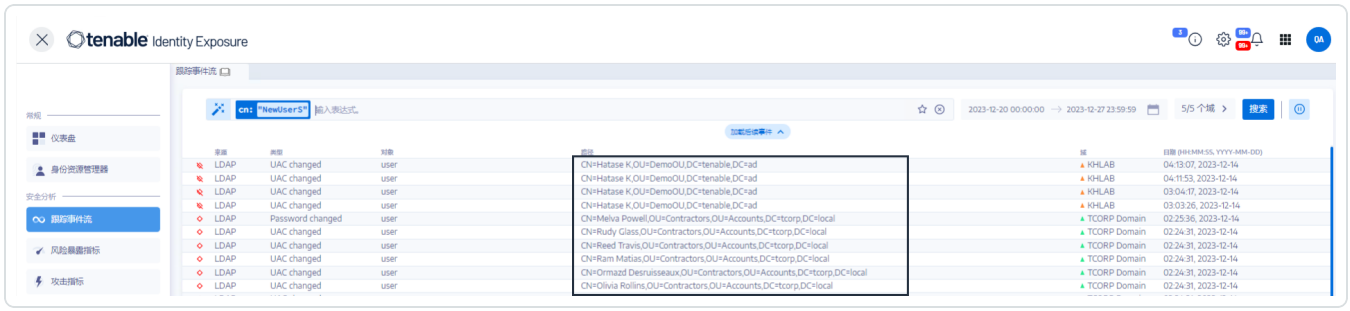
注意：这些示例并非详尽无遗，无法涵盖所有可能的情况。

创建新的 AD 用户帐户时，跟踪事件流中会发生什么情况？

- 在管理员端，输入有关新用户帐户的各种信息。

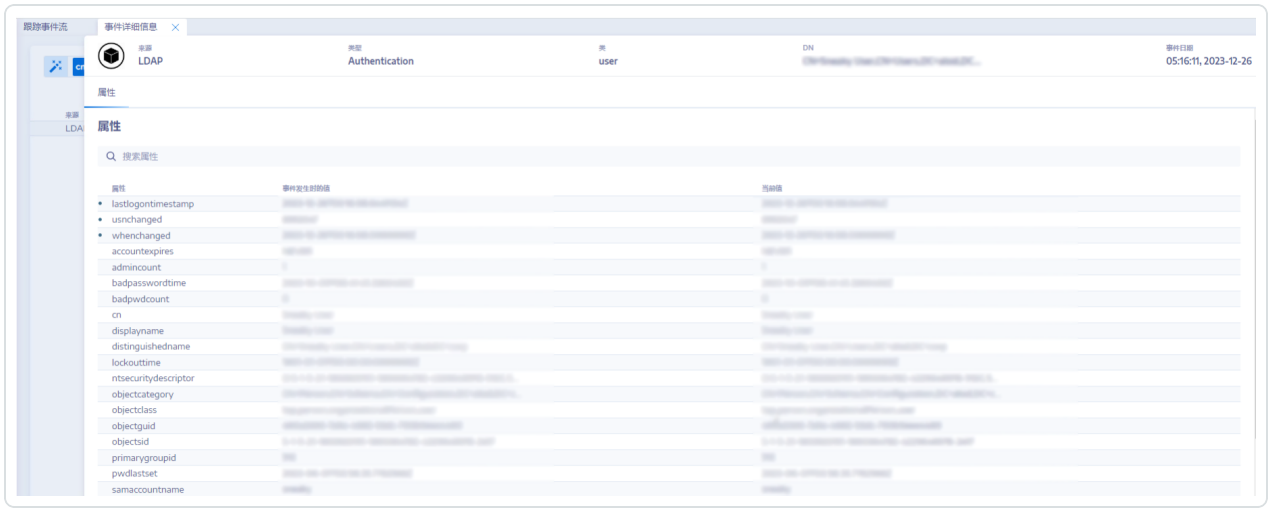


- 在最终用户端，Tenable Identity Exposure 可更新“**跟踪事件流**”页面。请参阅指示*新对象*的“**类型**”列。



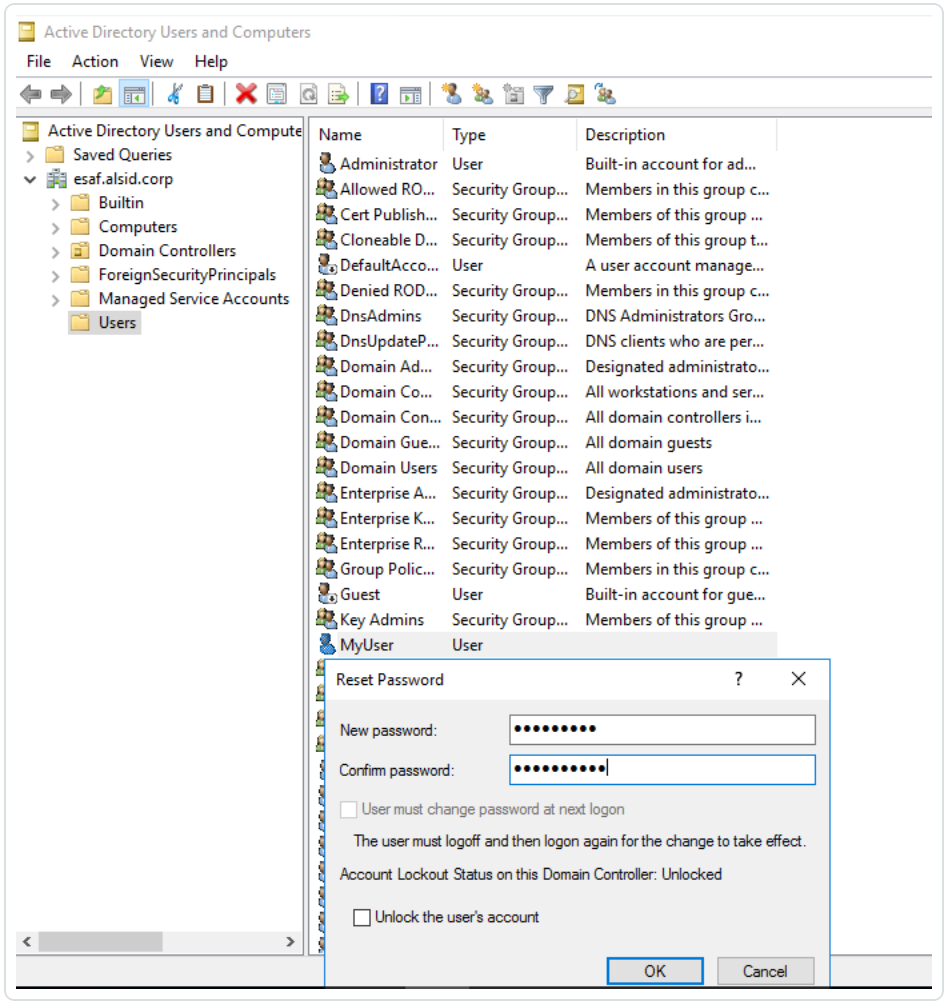
- “**事件详细信息**”页面也会反映此更改。属性名称左侧的蓝点表示发生了更新。

  有关属性的更多详细信息，请参阅查看事件详细信息。



更改 AD 用户的密码时，跟踪事件流中会发生什么情况？

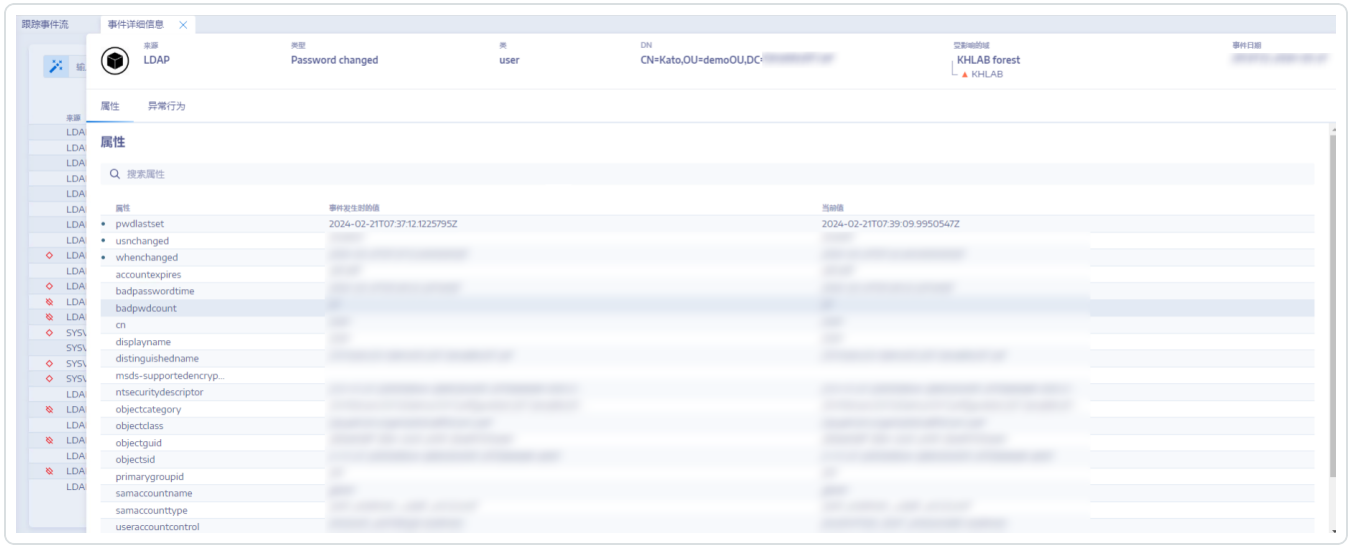
- 在管理员端，输入用于重置用户密码的各种信息。



- 在最终用户端，Tenable Identity Exposure 可更新“**跟踪事件流**”页面。请参阅指示“密码已更改”的“**类型**”列。

- “**事件详细信息**”页面还通过 whenchanged 属性左侧的蓝点反映此更改。

  有关“属性”的更多详细信息，请参阅 事件详细信息。



另请参阅：

- 手动搜索“跟踪事件流”
- 使用向导搜索“跟踪事件流”
- 自定义跟踪事件流查询
- 书签查询
- 查询历史记录

风险暴露指标

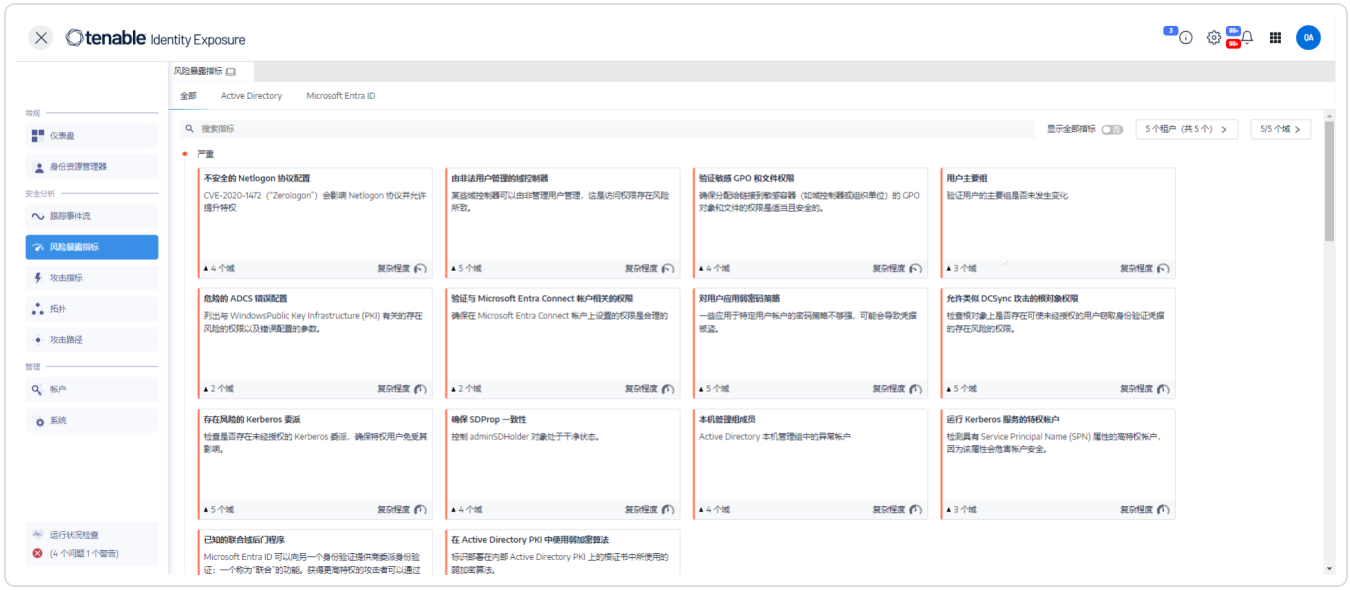
Tenable Identity Exposure 通过风险暴露指标 (IoE) 衡量 AD 基础设施的安全成熟度，并为监控和分析的事件流分配严重程度。Tenable Identity Exposure 在检测到安全回退时触发警报。

若要显示 IoE，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击导航窗格中的“**风险暴露指标**”。

   此时会打开“**风险暴露指标**”窗格。默认情况下，Tenable Identity Exposure 仅显示包含异常行为的 IoE。

2. (可选) 要显示所有 IoE，点击以将“**显示全部指标**”开关切换为“**是**”。



若要搜索 IoE，请执行以下操作：

1. 在“**风险暴露指标**”页面的顶部，在搜索框中输入一个字符串。该字符串可以是与 IoE 相关的任何术语，如密码、用户、登录等。

2. 按 Enter。

   IoE 页面会随与搜索词关联的指标更新。

若要过滤特定林或域的 IoE，请执行以下操作：

1. 点击“**n/n 个域**”。

   “**林和域**”窗格随即打开。

2. 选择林或域。

3. 单击“**按所选结果筛选**”。

严重程度

严重程度允许评估检测到的漏洞的严重程度，并确定修复措施的优先级。

“**风险暴露指标**”窗格按照如下方式显示 IoE：

- 使用颜色代码按严重程度显示。
- 垂直方向：从最严重到最不严重（红色表示优先级最高，蓝色表示优先级最低）。
- 水平方向：从最复杂到最不复杂。Tenable Identity Exposure 可动态计算复杂程度指标，以指示修复异常 IoE 的难易程度。

严重程度	说明
危急：红色	显示如何防止某些非特权用户对 Active Directory 的攻击和危害。
高危：橙色	处理后渗透利用技术攻击（导致凭据窃取或安全绕过），或者处理需要链接才能带来危险的渗透利用技术。
中危 - 黄色	表示 Active Directory 基础设施的风险有限。
低危 - 蓝色	显示良好的安全实践。某些业务环境可能会导致低影响异常行为，但不一定影响会 AD 安全。仅当管理员做出错误行为（例如激活不活动帐户）时，这些异常行为才会对 AD 产生影响。

另请参阅：

- 风险暴露指标详细信息
- 异常对象
- 搜索异常对象

- 忽略异常对象
- 危害认定属性

风险暴露指标详细信息

通过特定风险暴露指标的详细信息，可以查看有关已检测到的漏洞、关联的异常对象和修复建议的技术信息。

若要显示风险暴露指标详细信息，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击导航窗格中的“**风险暴露指标**”。

   此时会打开“**风险暴露指标**”窗格。默认情况下，Tenable Identity Exposure 仅显示包含异常行为的 IoE。

2. （可选）要显示所有 IoE，点击以将“**显示全部指标**”开关切换为“**是**”。

3. 点击页面上的任何“**风险暴露指标**”磁贴。

   “**指标详细信息**”窗格随即打开。

“**指标详细信息**”窗格顶部汇总了“跟踪事件流”表中已经提供的信息：

- IoE 的**名称**。
- 其**严重程度**（严重、高危、中危或低危）。
- 其合规性**状态**，以 Tenable Identity Exposure 运行的上次分析的结果为基础。
- “**上次检测时间**”，指出 Tenable Identity Exposure 上次运行分析的时间。

4. 点击以下任一选项卡，提供 IoE 的更多详细信息：

选项卡	说明
信息	包括关于 IoE 的内部和外部资源，如： • 执行摘要：概述问题，以协助做出适当决策。 • 文档：链接到 IoE 上的外部资源。 • 攻击者已知工具：入侵工具的名称。 • 受影响的域的树状结构。
漏洞详细信息	提供对在 AD 中检测到的漏洞的解释，以及不采取修复措施时对 Active Directory (AD) 造成的风险。
异常对象	异常对象会揭示 AD 中的缺陷或潜在的危险行为。可以对异常对象应用过滤条件，以查明危急问题。 当 IoE 状态不合规且包含异常对象时，可以采取修复措施来纠正 Tenable Identity Exposure 检测到的安全缺陷。有关更多信息，请参阅“异常对象”。
建议	有关如何恢复安全要求合规性和提高 AD 安全性的提示： • 执行摘要概述 Tenable Identity Exposure 建议的解决方案。 • “详细信息”子部分提供有关如何实施行动计划的建议，并帮助管理人员启动对其 AD 基础设施的必要更改。 • “文档”子部分提供关于当前建议的解决方案或威胁的外部资源的链接。

另请参阅：

- 风险暴露指标
- 异常对象
- 搜索异常对象

- 忽略异常对象
- 危害认定属性

异常对象

Tenable Identity Exposure 的风险暴露指标 (IoE) 可标记揭示 Active Directory (AD) 中的漏洞或潜在危险行为的异常对象。关注这些异常对象有助于查明危急问题并对其进行修复。可以执行以下任一操作：

- 搜索异常对象。
- 忽略一段时间内的异常对象。
- 选择林和域以搜索异常对象。
- 获取有关影响 IoE 且会造成危害的属性的说明。
- 下载显示所有异常对象的报告。

若要显示异常对象，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击导航窗格中的“**风险暴露指标**”。

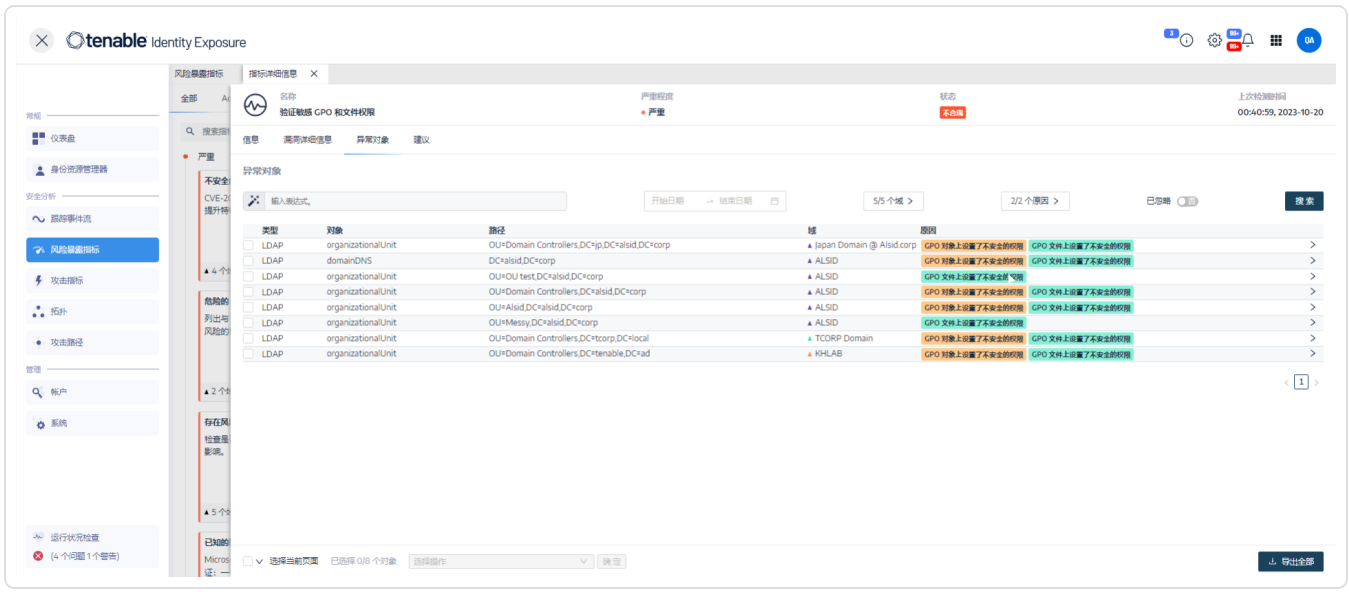
   “**风险暴露指标**”页面随即打开。默认情况下，Tenable Identity Exposure 仅显示包含异常行为的 IoE。

2. 点击页面上的任何“**风险暴露指标**”磁贴。

   “**指标详细信息**”窗格随即打开。

3. 点击“**异常对象**”选项卡。

   与 IoE 关联的异常对象列表随即出现。



异常对象表包括以下信息：

- **类型**：指示 AD(LDAP 或 SMB 协议) 中任何与安全相关的更改的来源。
- **对象**：指示与 AD 对象关联的类或文件扩展名。
- **路径**：指示 AD 对象的完整路径，以在 AD 中标识此对象的唯一位置。
- **域**：指示 AD 中的更改来自哪个域。
- **原因**：列出影响异常对象的危害认定属性。

若要导出异常对象报告，请执行以下操作：

1. 在“**异常对象**”页面底部，点击“**导出全部**”。

   “**导出异常对象**”窗格随即出现。

2. 在“**导出格式**”框中，点击下拉箭头以选择格式。
3. 点击“**导出全部**”。

   Tenable Identity Exposure 将异常对象报告下载到您的计算机中。

另请参阅：

- 风险暴露指标
- 风险暴露指标详细信息
- 搜索异常对象
- 忽略异常对象
- 危害认定属性

搜索异常对象

可以手动或使用向导搜索异常对象。

向导搜索

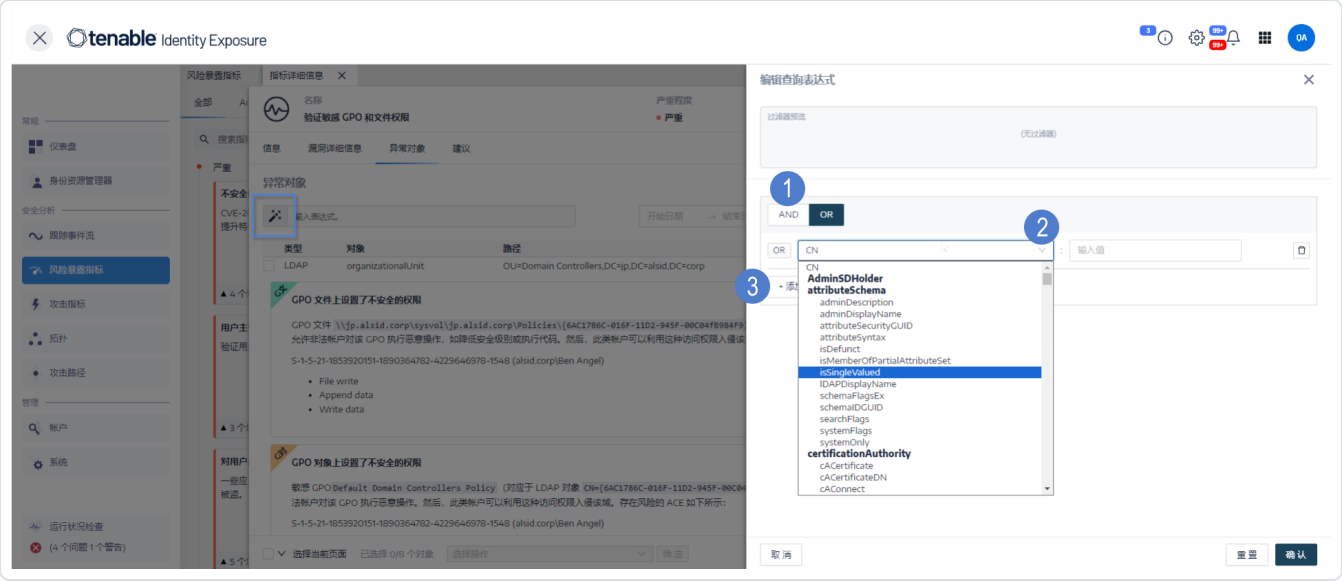
搜索向导允许创建查询表达式。

- 在搜索框中使用常用表达式时，可以将其添加到书签列表，以供以后使用。
- 在搜索框中输入表达式时，Tenable Identity Exposure 会在其“历史记录”窗格中保存此表达式，以供重复使用。

若要使用向导搜索异常对象，请执行以下操作：

1. 显示 异常对象 的列表。
2. 点击 图标。

   “**编辑查询表达式**”窗格随即打开。



3. 要在面板中定义查询表达式，请点击要应用于第一个条件的 **AND** 或 **OR** 运算符按钮 (1)。
4. 从下拉菜单中选择属性，然后输入其值 (2)。
5. 执行以下任一操作：

- 要添加属性，请点击“**+ 添加新规则**”(3)。
- 要添加其他条件，请点击“**添加新条件**”**+AND** 或 **+OR** 运算符。从下拉菜单中选择属性，然后输入其值。
- 要将搜索限制为异常对象，请点击“**仅异常**”开关以允许这样做。选择 **+AND** 或 **+OR** 运算符以向查询添加条件。
- 要删除条件或规则，请点击 图标。

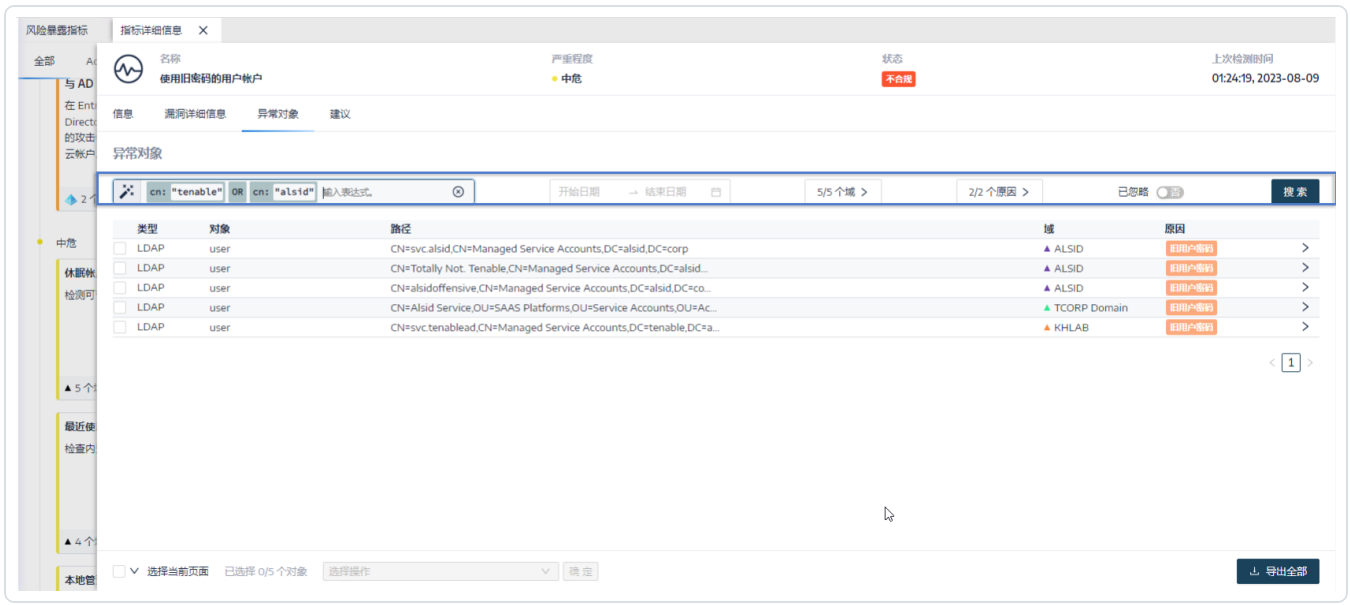
6. 点击“**验证**”运行搜索，或点击“**重置**”修改查询表达式。

手动搜索

若要过滤与特定字符串或模式匹配的异常对象，可以在搜索框中输入表达式，以使用布尔运算符 ***、**AND** 和 **OR** 优化结果。可以将 **OR** 语句放在括号中，以便修改搜索优先级。搜索操作会查找 Active Directory 属性中的任何特定值。若要手动搜索跟踪事件流，请执行以下操作：

若要手动搜索异常对象，请执行以下操作：

1. 显示 异常对象 的列表。



2. 在搜索框中，输入查询表达式。
3. 可以按如下方式过滤搜索结果：

- 点击“**日历**”框以选择开始日期和结束日期。
- 点击“**n/n 个域**”以选择林和域。

4. 点击“**搜索**”。

   Tenable Identity Exposure 使用与搜索条件匹配的结果更新列表。

语法和句法

手动查询表达式会使用以下语法和句法：

- 语法：`EXPRESSION [OPERATOR EXPRESSION]*`
- 句法：`__KEY__ __SELECTOR__ __VALUE__`

  其中：

  - `__KEY__` 指的是要搜索的 AD 对象属性（如 `CN`、`userAccountControl`、`members` 等）。
  - `__SELECTOR__` 指运算符 `:`、`>`、`<`、`>=`、`<=`。
  - `__VALUE__` 指要搜索的值。

    可以使用更多键来查找特定内容：

  - `isDeviant` 可查找造成异常行为的事件。

可以使用 **AND** 和 **OR** 运算符组合多个跟踪事件流查询表达式。

示例：

- 在通用名称属性中查找包含字符串 `alice` 的所有对象：`cn:"alice"`
- 在通用名称属性中查找每个包含字符串 `alice` 且创建了特定异常行为的所有对象：`isDeviant:"true" and cn:"alice"`
- 查找 GPO 命名的默认域政策：`objectClass:"groupPolicyContainer" and displayname:"Default Domain Policy"`
- 查找 SID 中包含 S-1-5-21 的所有已停用帐户： `userAccountControl:"DISABLE"` 和 `objectSid:"S-1-5-21"`

- 在 Sysvol 中查找所有 script.ini 文件：globalpath:"sysvol" and types:"SCRIPTSini"

> **注意**：此处，types 是指对象属性，而不是列标头。

另请参阅：

- 风险暴露指标
- 风险暴露指标详细信息
- 异常对象
- 忽略异常对象
- 危害认定属性

忽略异常对象

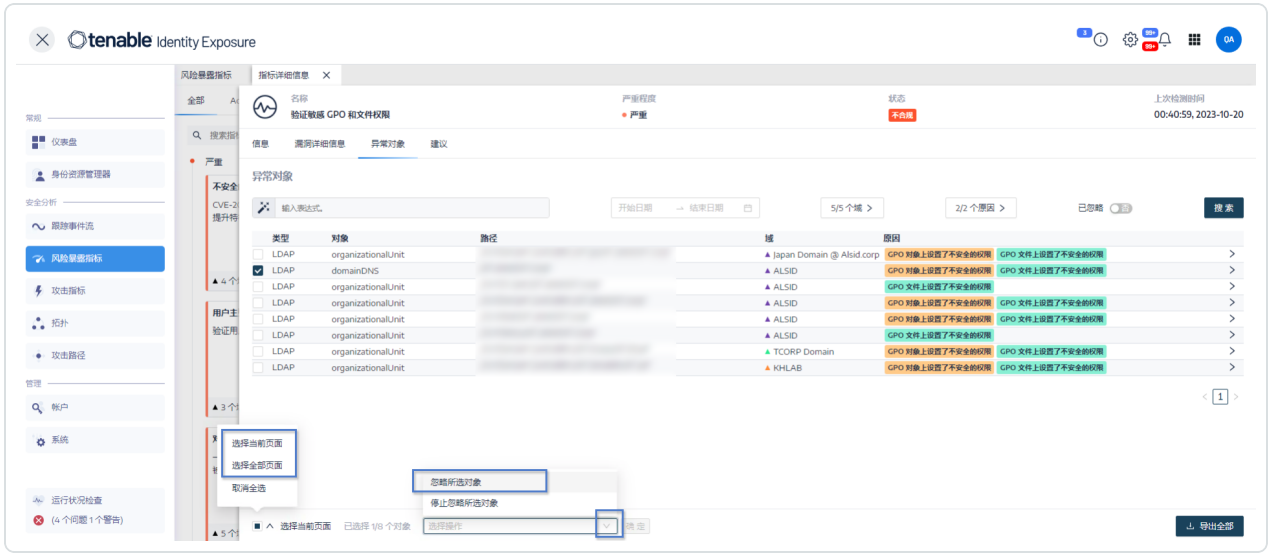
出于调查或报告目的，为防止屏幕内容杂乱，可以通过强制 Tenable Identity Exposure 在选定时间段内忽略某些异常对象来过滤掉它们。您可以选择忽略一个或多个异常对象。可以立即应用自定义过滤条件，也可以指定激活该过滤条件的时间范围。

注意：忽略对象后，对象便无法在 Tenable Identity Exposure 中解析。

若要忽略异常对象，请执行以下操作：

1. 在 Tenable Identity Exposure 中显示 异常对象 的列表。
2. 选中要忽略的异常对象前的复选框。
3. 或者还可以过滤要忽略的异常对象：
   - 点击“**日历**”框以选择开始日期和结束日期。
   - 点击“**n/n 个域**”以选择林和域。

提示：要加快选择速度，可以选中页面底部的“**选择全部页面**”或“**选择当前页面**”框。



4. 从页面底部的下拉列表中选择“**忽略所选对象**”。
5. 点击“**确定**”。

   “**忽略所选对象**”窗格将随即出现。

6. 点击“**在此日期之前忽略**”框以显示日历，然后选择 Tenable Identity Exposure 必须在此前忽略异常对象的日期。
7. 点击“**确定**”。

   Tenable Identity Exposure 显示一则确认消息，并更新剩余异常对象的列表。

若要显示已忽略的异常对象，请执行以下操作：

1. 点击以将“**已忽略**”开关切换为“**是**”。
2. 在页面底部点击“**选择全部页面**”。
3. 从下拉列表中选择“**停止忽略所选对象**”。
4. 点击“**确定**”。

   “确认”窗格随即出现。
5. 点击“**确定**”验证您的更改。

   Tenable Identity Exposure 显示被忽略的异常对象。

另请参阅：

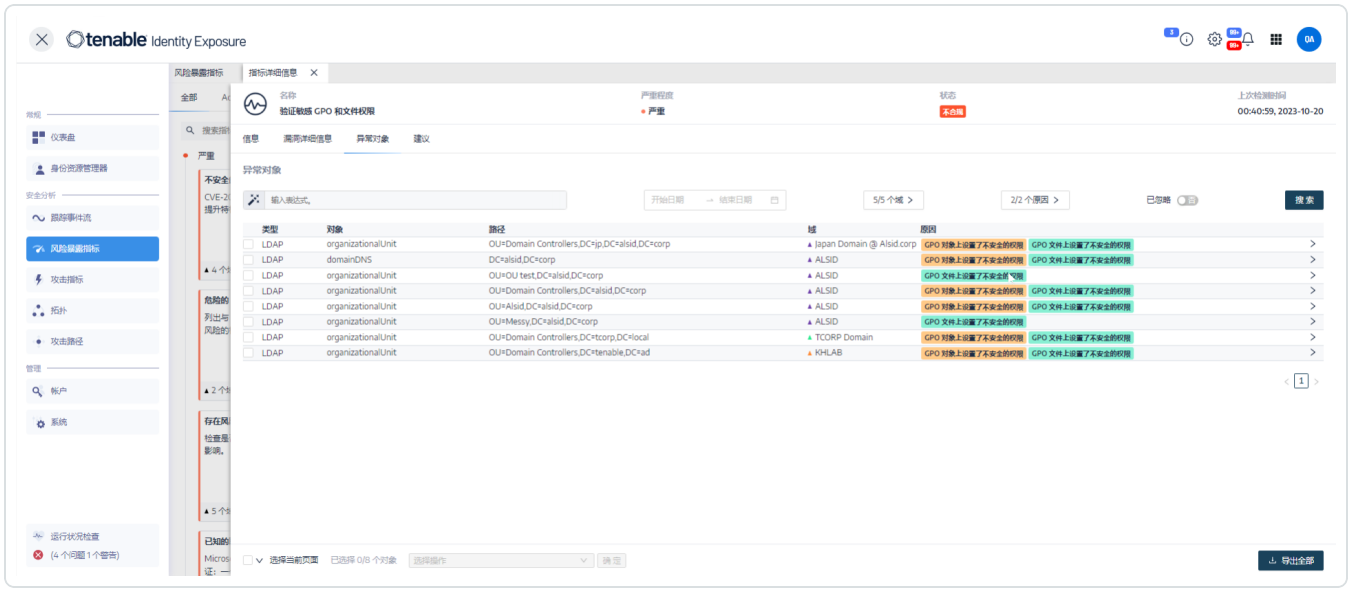
- 风险暴露指标
- 风险暴露指标详细信息
- 异常对象
- 搜索异常对象
- 危害认定属性

危害认定属性

Tenable Identity Exposure 在风险暴露指标 (IoE) 中显示可触发异常对象的危害认定属性，并给出相应理由，以帮助了解异常行为并对其进行修复。

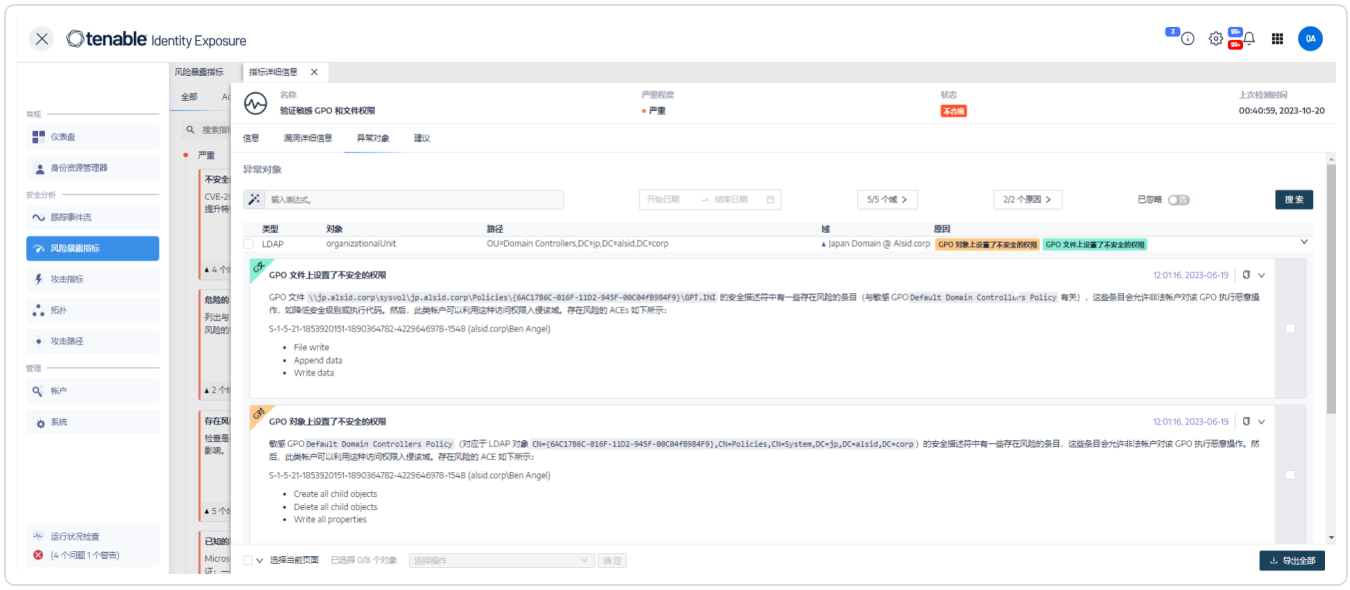
若要查看危害认定属性，请执行以下操作：

1. 显示 异常对象 的列表：



2. 点击异常对象列表中的一个条目。

   Tenable Identity Exposure 显示该异常对象的危害认定属性：



该列表包含以下信息：

- **使用颜色编码的标签**，用于区分多种原因。
- 值：
  - ?- 表示异常行为的缺失（空）属性值。
  - 没有关于此异常行为的说明：此检测可追溯至 2.6 版，且 Tenable Identity Exposure 不再管理此属性。

若要复制危害认定属性，请执行以下操作：

- 选择该属性并点击 图标。

另请参阅：

- 风险暴露指标
- 风险暴露指标详细信息
- 异常对象
- 搜索异常对象
- 忽略异常对象

基于 RSoP 的风险暴露指标

Tenable Identity Exposure 使用一组基于 RSoP（策略结果集）的风险暴露指标 (IoE) 评估并确保各个方面的安全性与合规性。此部分深入剖析了特定 RSoP IoE 当前的行为，以及 Tenable Identity Exposure 如何解决与其计算相关的性能问题。

以下依赖于 RSoP 的 IoE 在 Tenable Identity Exposure 的安全框架中发挥作用：

- 特权用户登录限制
- 存在风险的敏感特权
- 对用户应用弱密码策略
- 针对勒索软件的加固不足
- 不安全的 Netlogon 协议配置

这些 IoE 依赖于在需要时初始化的 RSoP 计算结果缓存，以计算应请求而添加的值，而不依赖于预先存在的值。以前，`AdObjects` 的更改会触发缓存失效，导致在 IoE 的 RSoP 执行期间频繁进行重新计算。

现在，Tenable Identity Exposure 解决了与 RSoP 计算相关的性能影响，具体如下所示：

1. **对可能过时的数据进行实时 IoE 分析**：即使用于处理的数据可能并非最新数据，依赖于 RSoP 的 IoE 在其发生时仍会实时进行计算（输入/输出事件）。可能会使 RSoP 缓存失效的缓冲事件会保持存储状态，直到事件满足提示预期计算的特定条件。
2. **计划的 RSoP 失效**：当满足重新计算的条件时，系统会考虑到缓冲事件而在无效化过程中使 RSoP 缓存失效。
3. **使用最新缓存重新执行 IoE**：缓存失效后，IoE 使用从缓存获取的 `AdObject` 最新版本，并结合缓冲事件进行重新执行。Tenable Identity Exposure 单独计算每个缓冲事件的每个 IoE。

出于这些原因，依赖于 RSoP 结果的 IoE 优化计算时长会导致与 RSoP 相关的异常行为计算变慢。

与 Microsoft Entra ID 相关的风险暴露指标

特定于 Microsoft Entra ID 的暴露指标

Tenable Identity Exposure 具有针对 Microsoft Entra ID 中资产的潜在漏洞发出警报的专用风险暴露指标 (IoE)。

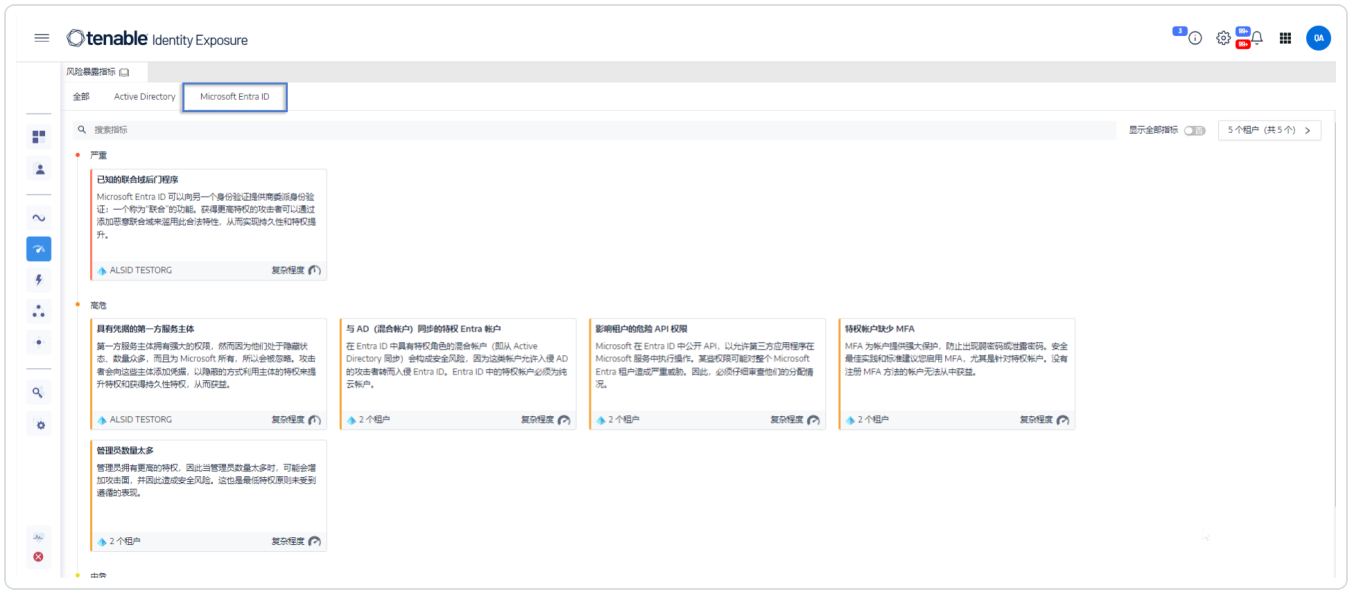
若要显示 Microsoft Entra ID IoE，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击左侧导航栏中的 IoE 图标 。

   此时会打开“IoE”窗格。

2. 点击“**Microsoft Entra ID**”选项卡。

   Tenable Identity Exposure 显示与触发了结果的 Microsoft Entra ID 相关的 IoE。



3. 点击包含您想要调查的 IoE 的磁贴。

4. “标识指标详细信息”窗格随即打开，其中包含以下信息：

   - **漏洞信息**：暴露于潜在攻击的方式。
   - **结果**：有关标识提供程序类型的详细信息和风险描述。
   - **建议**：修复该威胁的步骤。

根据风险暴露指标修复异常对象

Tenable Identity Exposure 会在风险暴露指标 (IoE) 遇到需要修复的异常对象时触发警报。

以下示例显示了如何对三个特定 IoE 执行修复程序。

- 标准用户中设置了 AdminCount 属性
- 存在风险的 Kerberos 委派
- 确保 SDProp 一致性

有关 IoE 的完整信息，请参阅 Tenable Identity Exposure 用户界面中提供的文档。

标准用户中设置了 AdminCount 属性

用户帐户的 adminCount 属性表示管理组中过去的成员资格，并且该属性在帐户离开管理组后不会重置。因此，即使是旧的管理帐户也设有此属性，这会阻止 Active Directory 权限的继承。虽然该属性的初衷是保护管理员，但却可能引发棘手的权限问题。

此中等级别 IoE 仅报告具有此属性的活动用户帐户和组，不包括合法成员的 adminCount 属性设为 1 的特权组。

若要修复"**标准用户中设置了 AdminCount 属性**"IoE 中的异常对象，请执行以下操作：

1. 在 Tenable Identity Exposure 中，单击导航窗格中的"**风险暴露指标**"以将其打开。

   默认情况下，Tenable Identity Exposure 仅显示包含异常对象的 IoE。

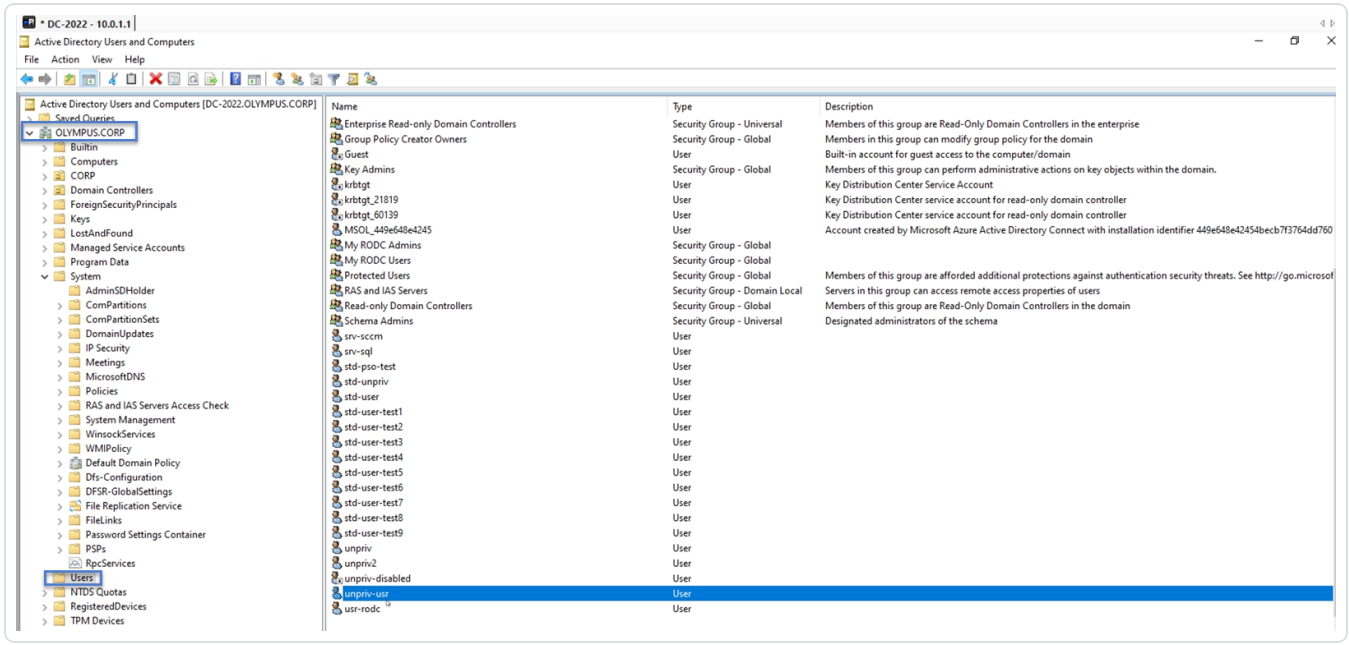
2. 单击"**标准用户中设置了 AdminCount 属性**"IoE 的磁贴。

   "**指标详细信息**"窗格随即打开。

3. 将鼠标悬停在异常对象上并单击以查看详细信息，同时记下域名和帐户。(在此示例中：域名 = OLYMPUS.CORP，标准帐户为 unpriv-usr)

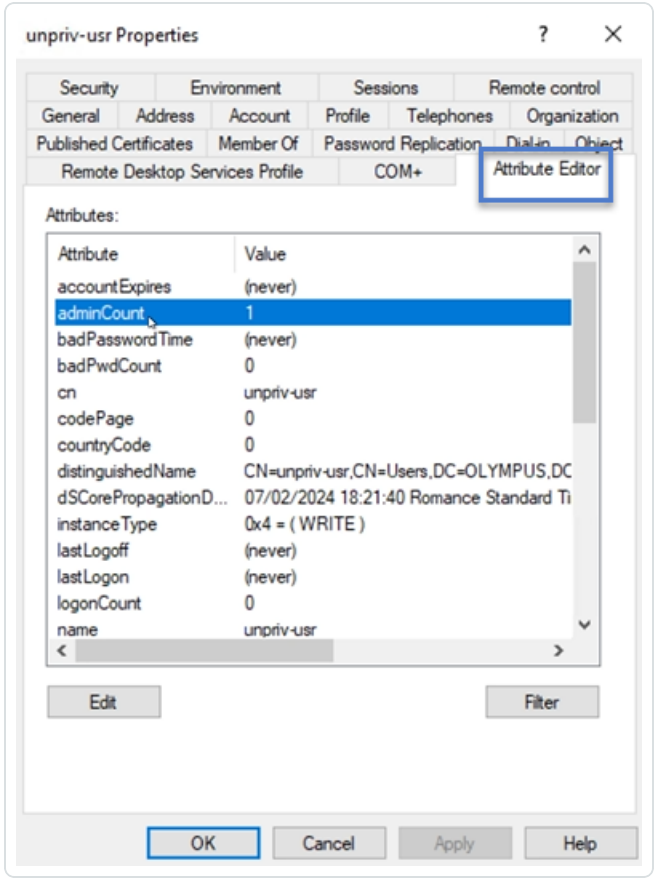
4. 在远程桌面管理器(或类似工具)中,找到该域名并导航到"**用户**"和 Tenable Identity Exposure 标记的帐户。

> **所需权限**:必须拥有域管理员帐户,才能执行该过程。

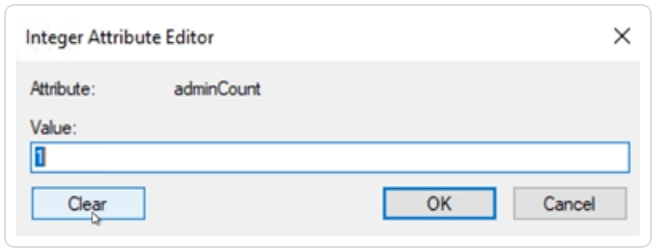


5. 单击帐户名称以打开"**属性**"对话框,然后选择"**属性编辑器**"选项卡。

6. 在属性列表中,单击"adminCount"以打开"**整数属性编辑器**"对话框。



7. 在对话框中，先后单击“**清除**”和“**确定**”。



8. 在 Tenable Identity Exposure 中，返回“指标详细信息”窗格并刷新页面。

   异常对象不再显示在列表中。

存在风险的 Kerberos 委派

Kerberos 协议对 Active Directory 的安全至关重要，该协议允许某些服务器重复使用用户凭据。如果攻击者入侵其中一台服务器，他们就可以窃取这些凭证，并使用凭证在其他资源上进行身份验证。

此严重程度的 IoE 会报告所有具有委派属性的帐户，并排除已禁用的帐户。特权用户不应配置委派属性。若要保护这些用户帐户，请将其添加到“Protected Users”组或将其标记为“敏感帐户，无法委派”。

若要将帐户添加到“受保护的组”，请执行以下操作：

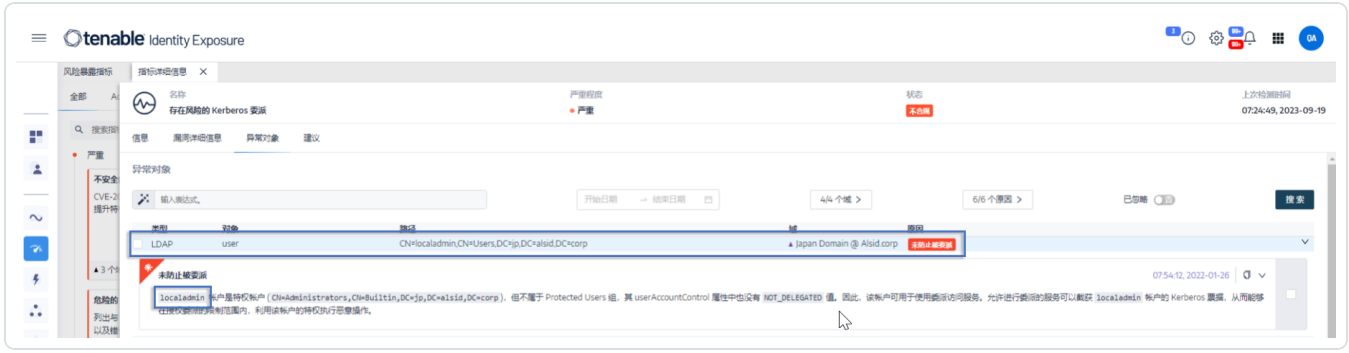
1. 在 Tenable Identity Exposure 中，单击导航窗格中的“**风险暴露指标**”以将其打开。

   默认情况下，Tenable Identity Exposure 仅显示包含异常对象的 IoE。

2. 单击“**存在风险的 Kerberos 委派**”IoE 的磁贴。

   “**指标详细信息**”窗格随即打开。

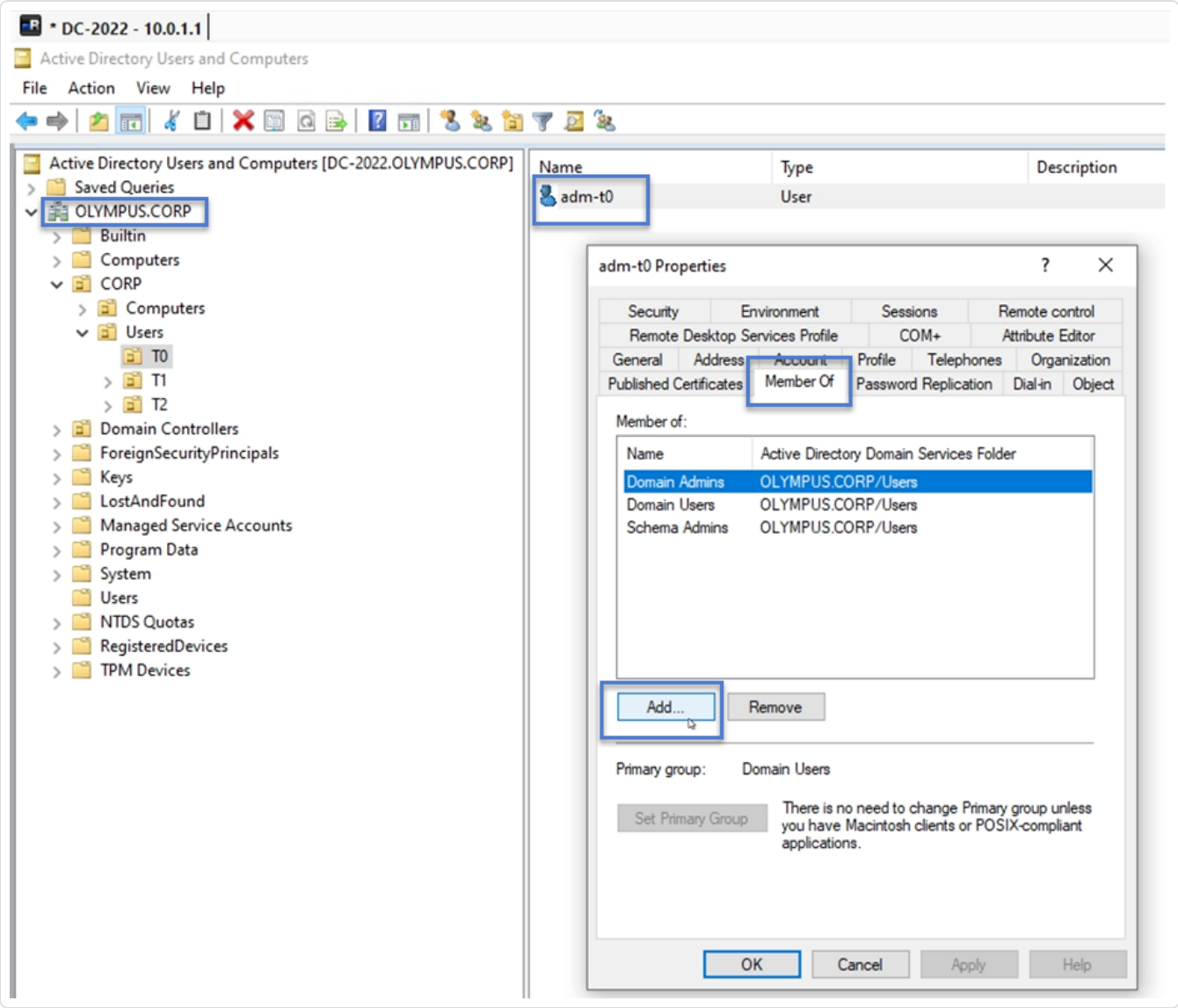
3. 将鼠标悬停在异常对象上并单击以查看详细信息，同时记下域名和帐户。(在此示例中：域名 = OLYMPUS.CORP，帐户 = `adm-t0`)



4. 在远程桌面管理器(或类似工具)中,找到该域名并导航到 Tenable Identity Exposure 标记的域和帐户。

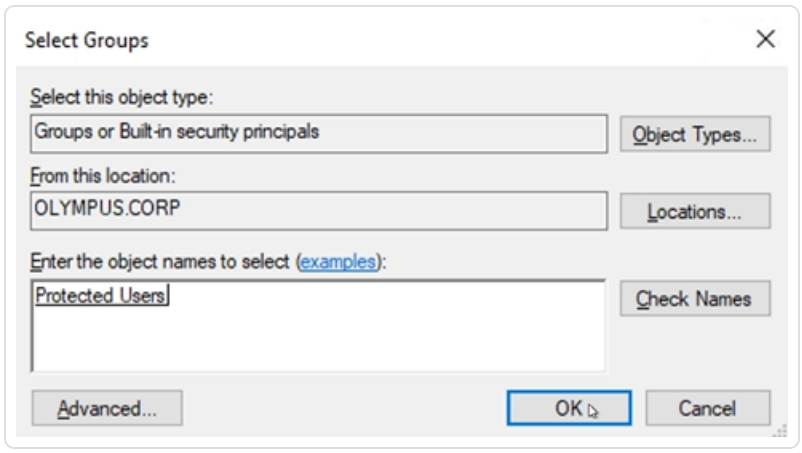
> **所需权限**:必须拥有域管理员帐户,才能执行该过程。

5. 单击帐户名称以打开"**属性**"对话框,然后选择"**成员归属**"选项卡。
6. 在成员列表中,单击"**添加**"。



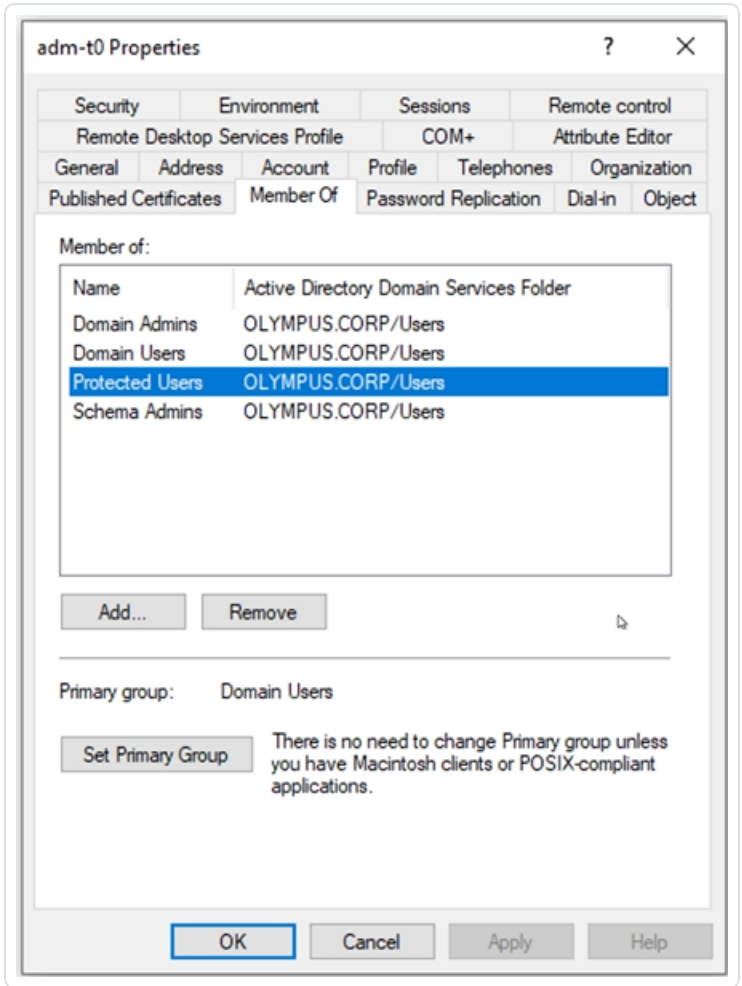
"**选择组**"对话框随即出现。

7. 输入对象名称"Protected Users"，然后单击"**检查名称**"。



8. 单击“**确定**”以关闭对话框。
9. 在“**属性**”对话框中，单击“**应用**”。

   此时，新组会出现在成员列表中。



10. 单击"**确定**"以关闭对话框。
11. 在 Tenable Identity Exposure 中，返回"指标详细信息"窗格并刷新页面。

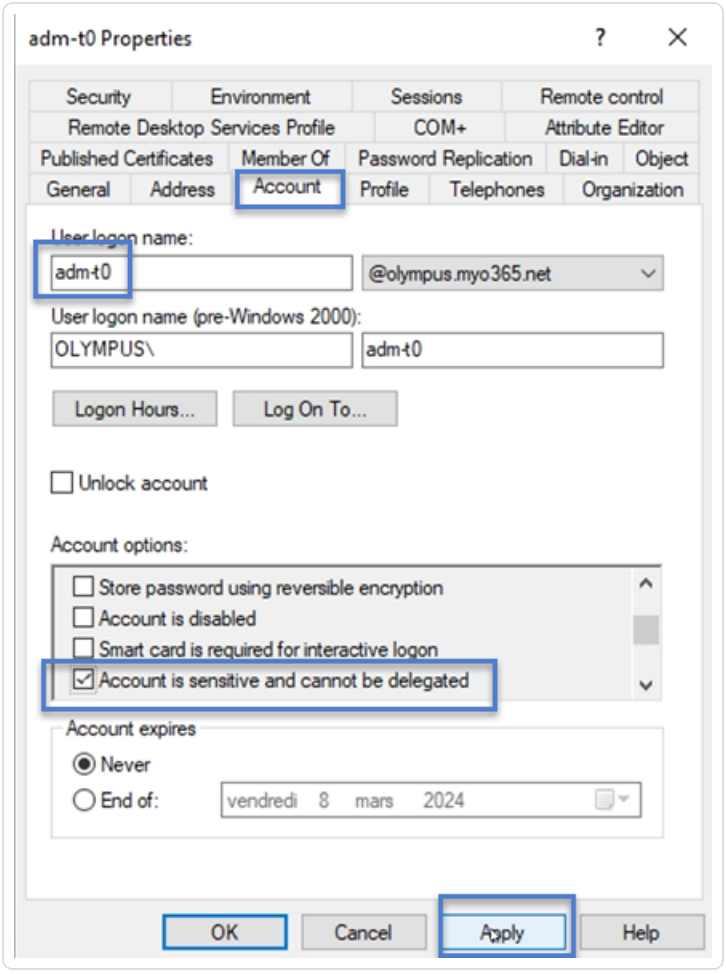
    异常对象不再显示在列表中。

若要将帐户设置为"无法委派"，请执行以下操作：

1. 在远程桌面管理器中，找到该域名并导航到 Tenable Identity Exposure 标记的域和帐户。

   所需权限：必须拥有域管理员帐户，才能执行该过程。

2. 单击帐户名称以打开"**属性**"对话框，然后选择"**帐户**"选项卡。
3. 在帐户选项列表中，选择"敏感帐户，无法委派"，然后单击"**应用**"。



4. 单击"**确定**"以关闭对话框。

5. 在 Tenable Identity Exposure 中，返回“指标详细信息”窗格并刷新页面。

   异常对象不再显示在列表中。

确保 SDProp 一致性

攻击者在破坏 Active Directory 域时，通常会修改 `adminSDHolder` 对象的 ACL，并且他们添加到 ACL 的任何权限都会被特权用户复制。这样一来，攻击者就很容易设置后门程序。

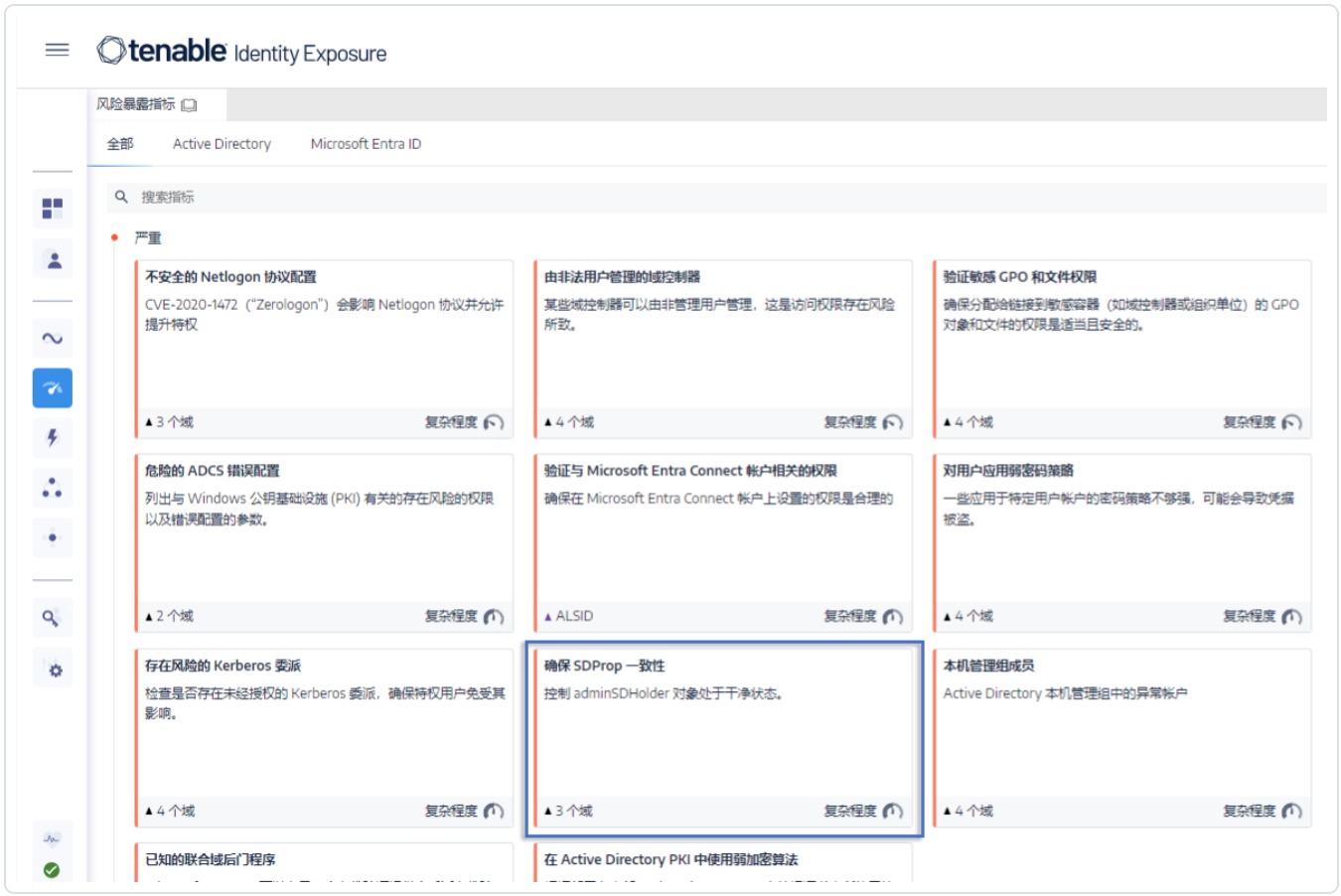
此严重程度的 IoE 会检查 `adminSDHolder` 对象上设置的权限是否只允许特权帐户访问管理帐户。

若要修复"**确保 SDProp 一致性**"IoE 中的异常对象，请执行以下操作：

1. 在 Tenable Identity Exposure 中，单击导航窗格中的"**风险暴露指标**"以将其打开。

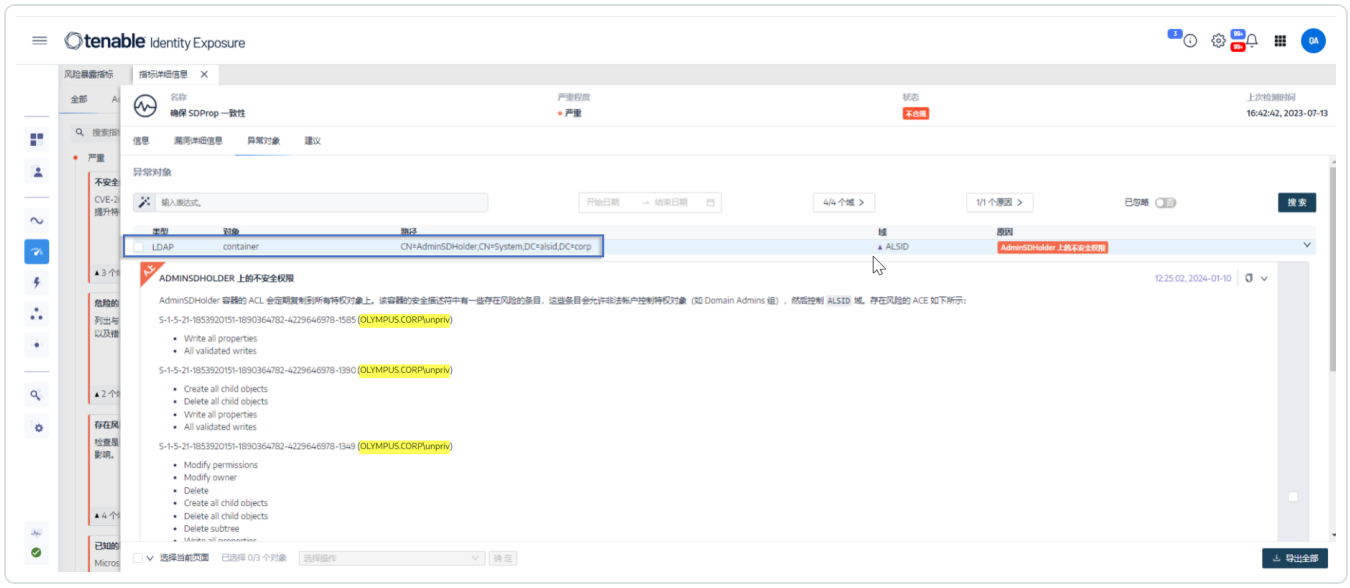
   默认情况下，Tenable Identity Exposure 仅显示包含异常对象的 IoE。

2. 单击"**确保 SDProp 一致性**"IoE 的磁贴。



"**指标详细信息**"窗格随即打开。

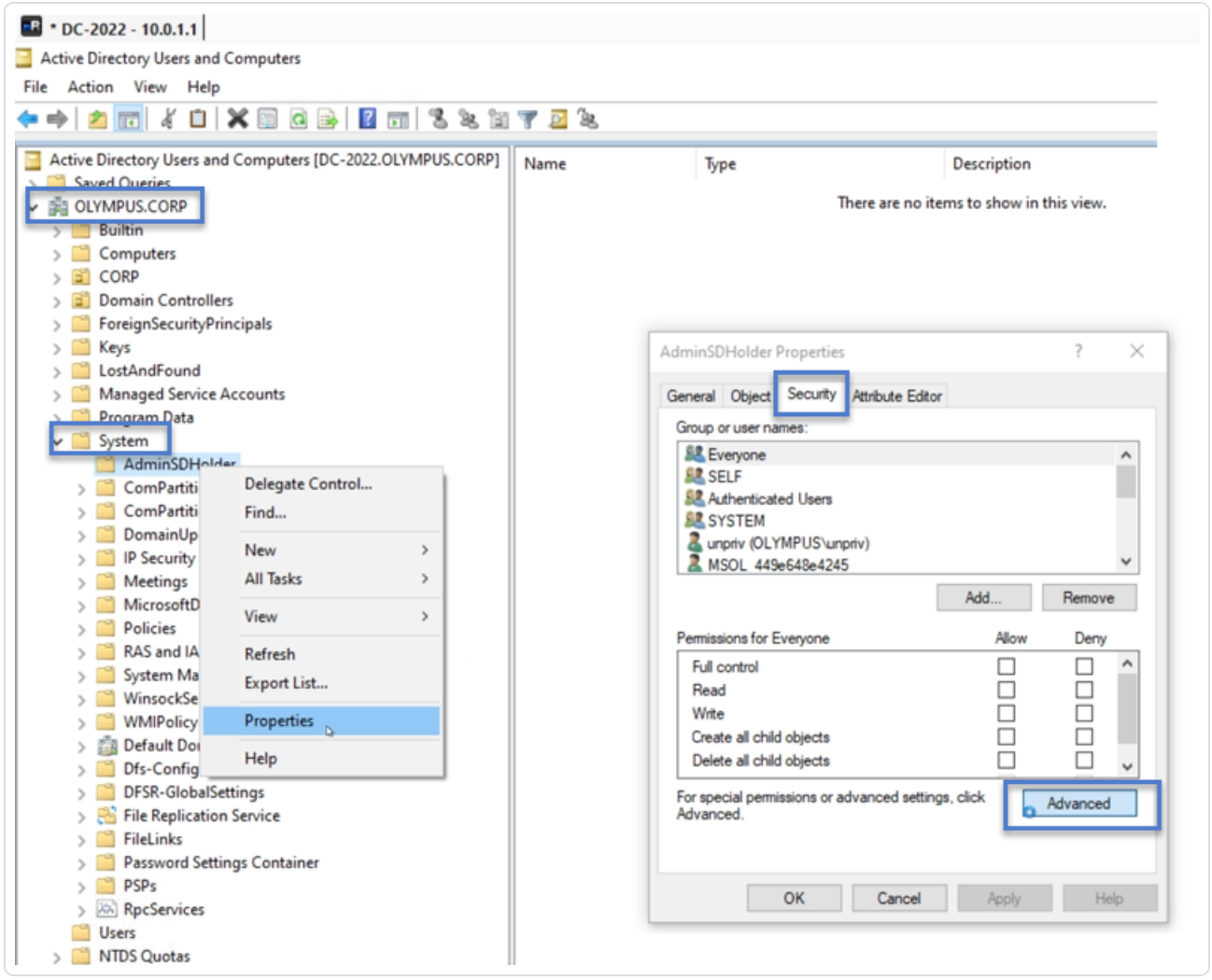
3. 将鼠标悬停在异常对象上并单击以查看详细信息。记下 Tenable Identity Exposure 标记的域名和相关权限。(在此示例中为 `OLYMPUS.CORP .\unpriv`)



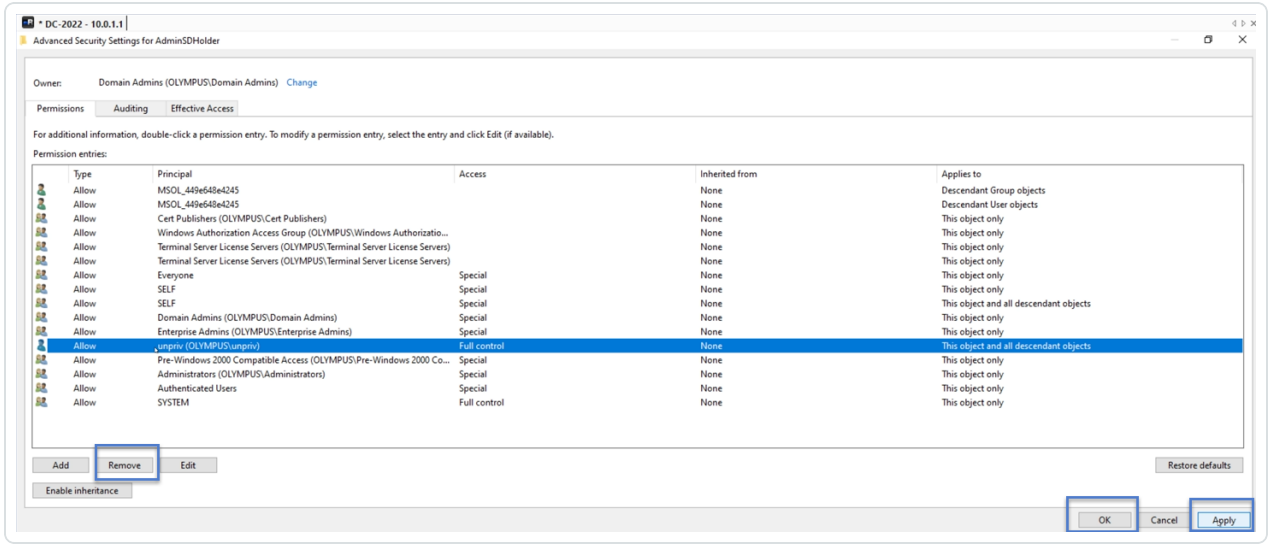
4. 在远程桌面管理器(或类似工具) 中，找到该域名并导航到“**系统**”>“**AdminSDHolder**”。

> **所需权限**：必须拥有域管理员帐户，才能执行该过程。

5. 右键单击“**AdminSDHolder**”并从上下文菜单中选择“**属性**”。



6. 在“**属性**”对话框中，选择“**安全**”选项卡，然后单击“**高级**”。
7. 在“**高级安全设置**”窗口的“**权限**”选项卡中，从权限条目列表中选择引起警报的权限。
8. 单击“**删除**”。
9. 依次单击“**应用**”和“**确定**”，关闭设置窗口。
10. 单击“**确定**”，关闭“**属性**”窗口。



11. 在 Tenable Identity Exposure 中，返回“指标详细信息”窗格并刷新页面。

    异常对象不再显示在列表中。

攻击指标

所需许可证：攻击指标

Tenable Identity Exposure 的**攻击指标** (IoA) 功能让您能够检测针对 Active Directory (AD) 的攻击。

攻击指标的合并视图在单个窗格中显示时间线、实时影响 AD 的前 3 个事件以及攻击分布情况。您可以执行以下操作：

- 从准确的攻击时间线对每个威胁进行可视化。
- 深入分析有关 AD 攻击的详细信息。
- 直接从检测到的事件探索 MITRE ATT&CK 描述。

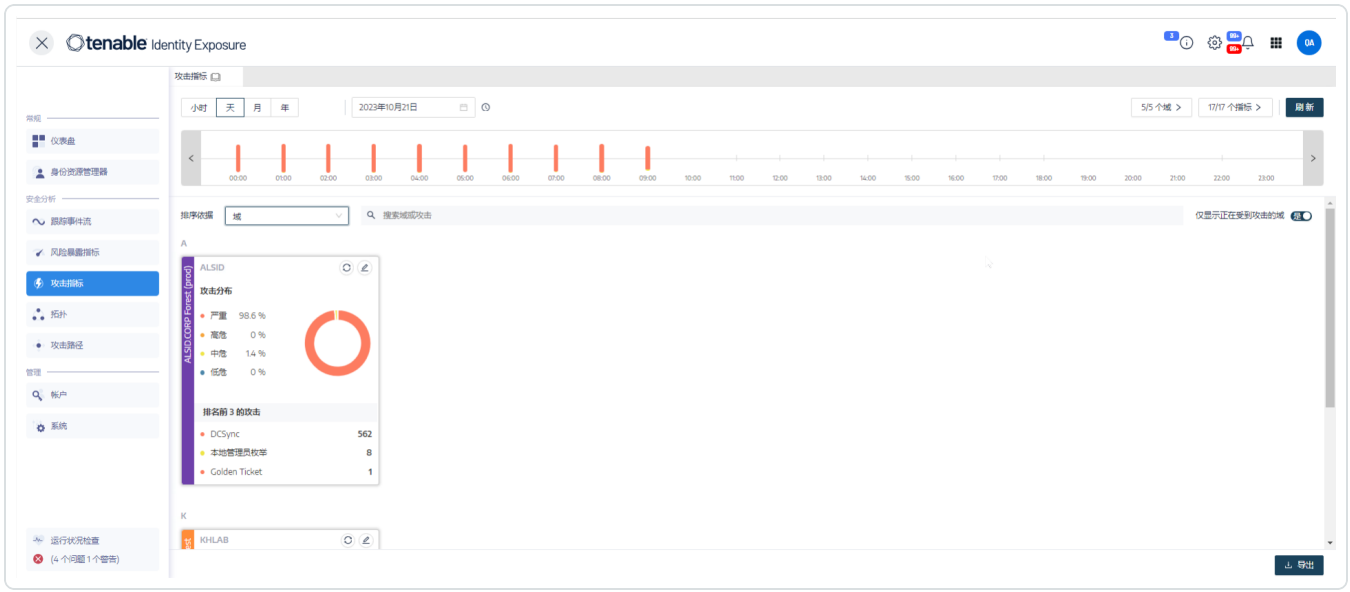
有关特定 IoA 的更多信息，请参阅 Indicators of Attack and the Active Directory。

注意：如果您发现检测到了大量攻击，请与您的管理员确认是否通过应用各种 IoA 选项的建议值来正确调整攻击指标。如需了解更多信息，请参阅调整 IoA。

若要显示攻击指标，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击导航窗格中的“**攻击指标**”。

   “**攻击指标**”窗格随即打开。



2. 默认情况下，Tenable Identity Exposure 显示所有 AD 林和域。若要调整此视图，请执行以下任一操作：

   - 选择要显示的时间段 - 点击“**小时**”、“**日**”（默认）、“**月**”或“**年**”。
   - 沿时间线移动 - 点击向左或向右箭头，可在时间线上前进或后退。
   - 选择特定时间 - 点击日期选择器以选择小时、日、月或年。
   - 返回到当前日期和时间 - 点击日期选择器旁的 图标。
   - 选择域 - 点击“**n/n 个域**”。

     a. 在“**林和域**”窗格中，选择域。

     b. 单击“**按所选结果筛选**”。

     Tenable Identity Exposure 更新视图。
   - 选择 IoA - 点击“**n/n 个指标**”。

     a. 在“攻击指标”窗格中，选择 IoA。

     b. 单击“**按所选结果筛选**”。

     Tenable Identity Exposure 更新视图。
   - 对 IoA 磁贴进行排序 - 在“**排序方式**”框中，点击箭头以显示包含以下选项的下拉列表：**域**、**重要性**或**林**。
   - 搜索域或攻击 - 在**搜索**框中键入域名或攻击。
   - 仅显示受攻击的域 - 点击“**仅显示受攻击的域**”，切换为“**是**”。
   - 导出攻击报告 - 点击“**导出**”。

     出现“**导出卡**”窗格。

     a. 在“**导出格式**”框中，点击下拉列表箭头以选择格式：**PDF**、**CSV** 或 **PPTX**。

     b. 点击“**导出**”。

     Tenable Identity Exposure 将报告下载到本地计算机。

严重程度

Tenable Identity Exposure 检测攻击并为其分配严重程度：

等级	描述
严重 - 红色	检测到经证实的后渗透利用攻击，攻击者需要先控制域才能实施该攻击。
高危 - 橙色	检测到允许攻击者控制域的重大攻击。
中危 - 黄色	IoA 与可导致危险的特权提升或允许访问敏感资源的攻击有关。
低危 - 蓝色	通过警报提醒存在与侦察操作或低影响事件相关的可疑行为。

另请参阅：

- 攻击指标详情
- 攻击指标事件

攻击指标详情

Tenable Identity Exposure 的"攻击指标"窗格显示有关 Active Directory 中所发生攻击的信息。

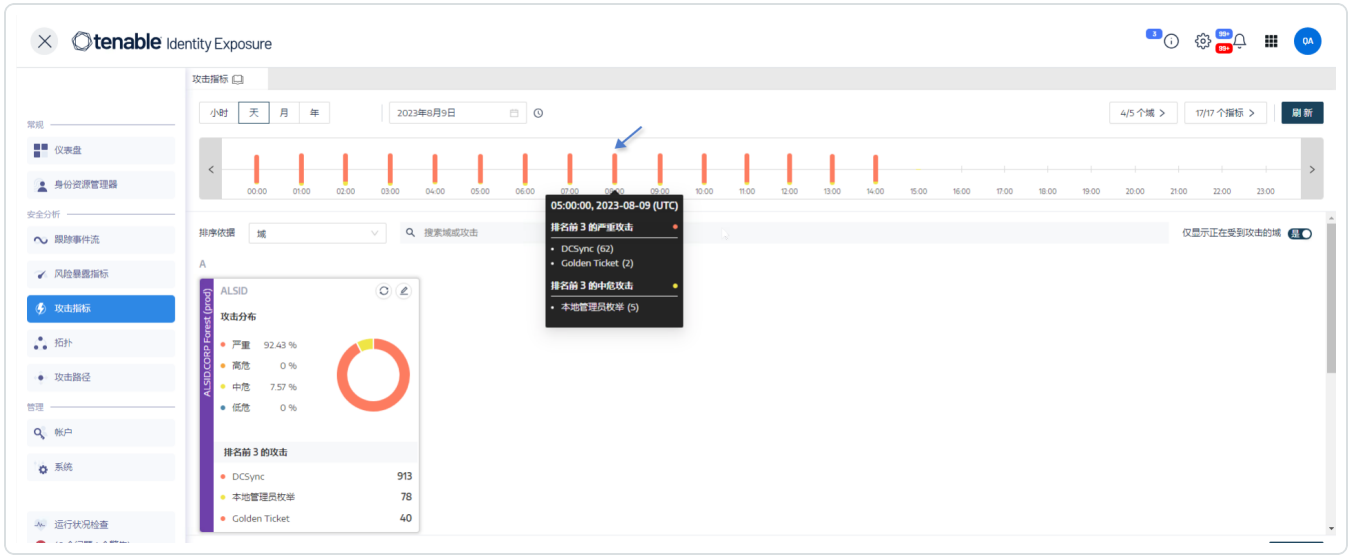
若要查看攻击指标：

- 在 Tenable Identity Exposure 中，点击导航窗格中的"**攻击指标**"。

  "**攻击指标**"窗格随即打开。

若要在时间线上显示攻击信息：

- 点击时间线上的任意事件以显示：
  - 事件检测日期和时间。
  - 排名前 3 的攻击的严重程度。
  - 在此日期和时间检测到的攻击总数。



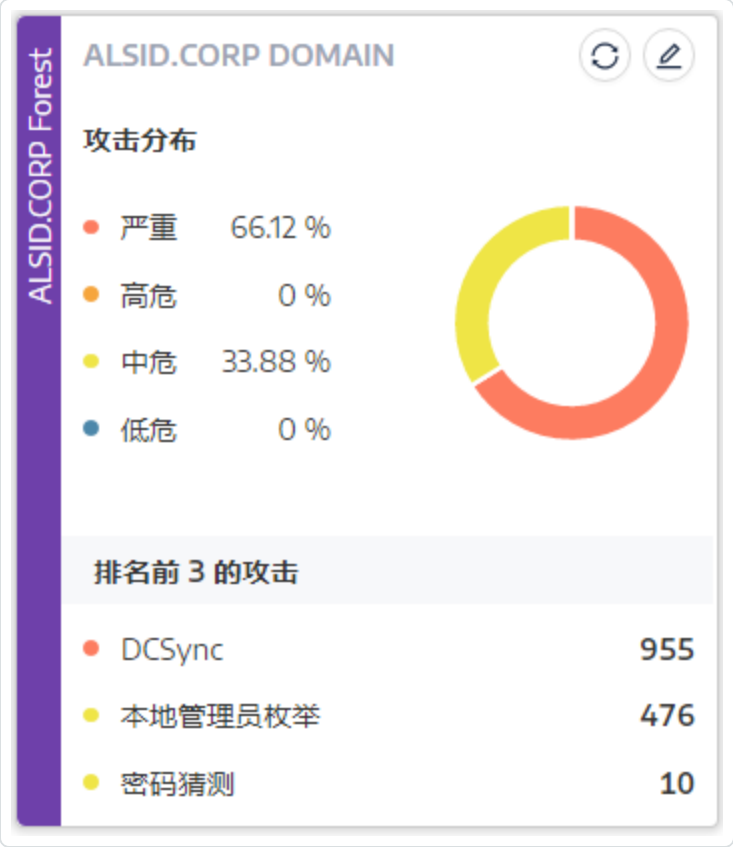
若要更改图表类型：

1. 点击 ✎ 图标可编辑域磁贴。

   此时会出现"**编辑卡信息**"窗格。

2. 选择图表类型：

- **攻击分布**:显示攻击严重性的分布情况。



- **事件数:** 显示前 3 位攻击及其发生次数。

3. 单击"**保存**"。

   Tenable Identity Exposure 更新图表。

另请参阅：

- 攻击指标
- 攻击指标事件

攻击指标事件

事件的攻击指标 (IoA) 列表提供有关针对 Active Directory (AD) 的特定攻击的详细信息。这让您可以根据 IoA 的严重性级别采取所需的操作。

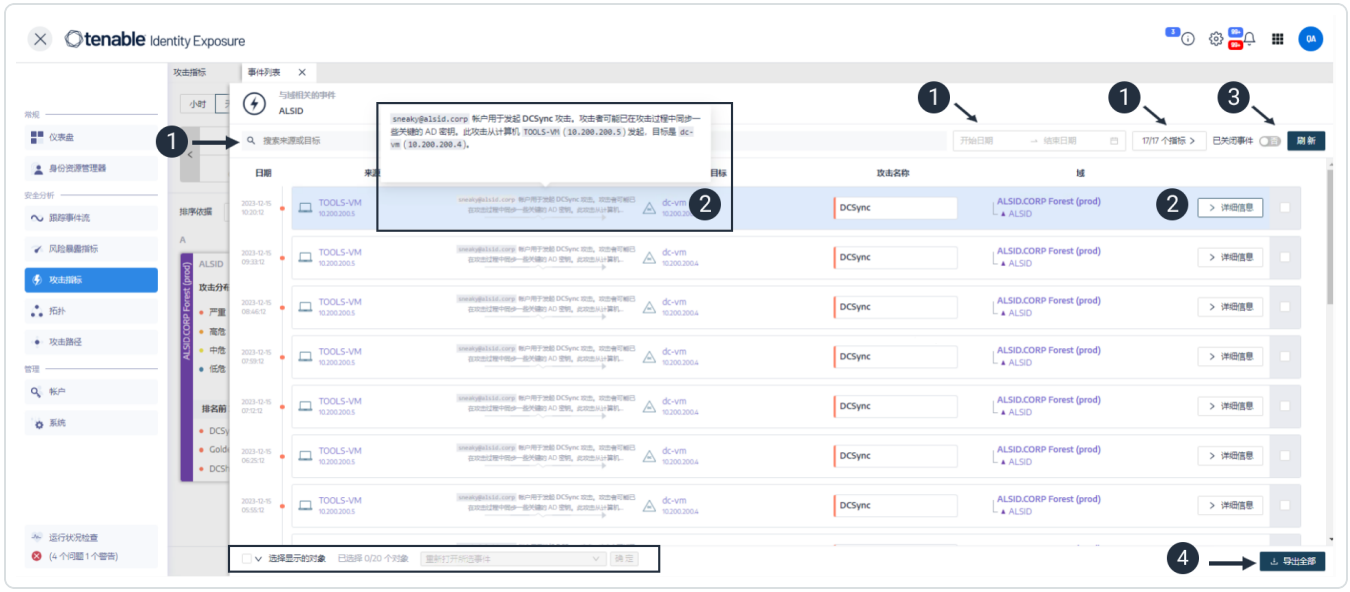
若要查看攻击事件：

1. 在 Tenable Identity Exposure 中，点击导航窗格中的“**攻击指标**”。

   “**攻击指标**”窗格随即打开。

2. 点击任意域磁贴。

   “**事件列表**”窗格随即出现，其中包含域中所发生事件的列表。



3. 在此列表中，您可以执行以下任一操作：

   - 定义搜索条件以搜索特定的事件❶。
   - 查看对影响 AD 的攻击的详细说明❷。
   - 关闭或重新打开事件❸。
   - 下载显示所有事件的报告❹。

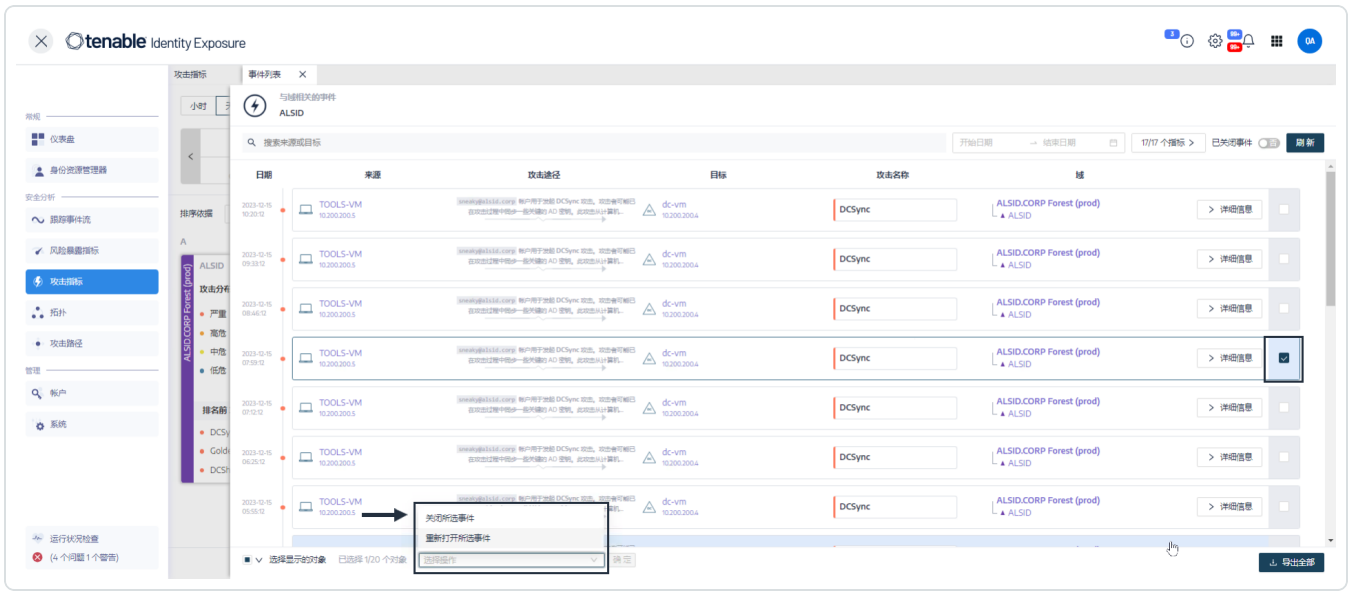
若要搜索事件：

1. 在**搜索**框中，键入来源或目标的名称。
2. 点击日期选择器，以选择事件的开始日期和结束日期。
3. 点击"**n/n 个指标**"以选择相关指标。
4. 点击"**已关闭事件**"，切换至"**是**"以将搜索范围限制为已关闭的事件。
5. 点击"**刷新**"。

   Tenable Identity Exposure 使用匹配的事件更新列表。

若要关闭事件：

1. 从事件列表中选择要关闭或重新打开的事件。



2. 在窗格底部，点击下拉菜单并选择"**关闭所选事件**"。
3. 点击"**确定**"。

   此时会显示一条消息，要求您确认关闭。

4. 点击“**确认**”。

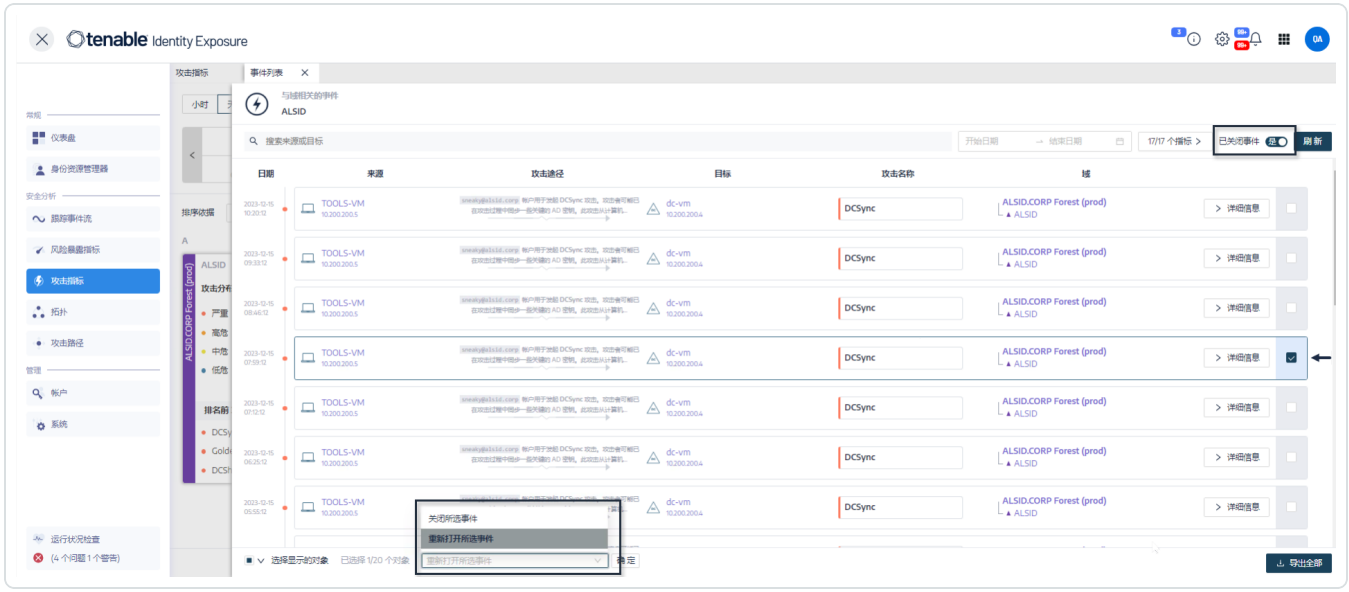
   一条消息确认 Tenable Identity Exposure 已关闭该事件，且不再显示该事件。

若要重新打开事件：

1. 在“**事件列表**”窗格中，点击“**已关闭事件**”，切换为“**是**”。

   Tenable Identity Exposure 使用已关闭的事件更新列表。

2. 选择要重新打开的事件。



3. 在窗格底部，点击下拉菜单并选择“**重新打开所选事件**”。

4. 点击“**确定**”。

   一条消息确认 Tenable Identity Exposure 已重新打开事件。

提示：您可以批量关闭或重新打开事件。在窗格底部，点击“**选择显示的对象**”。

事件详细信息

事件列表中的每个条目都显示以下信息：

- **日期** - 触发 IoA 的事件发生的日期。Tenable Identity Exposure 在时间线顶部显示最近的事件。
- **来源** - 发起攻击的来源及其 IP 地址。

- **攻击向量** – 解释攻击期间发生的情况。

  提示:将鼠标悬停在攻击向量上可查看有关 IoA 的更多信息。

- **目标** - 攻击的目标及其 IP 地址。
- **攻击名称** - 攻击的专业名称。
- **域** - 攻击影响的范围。

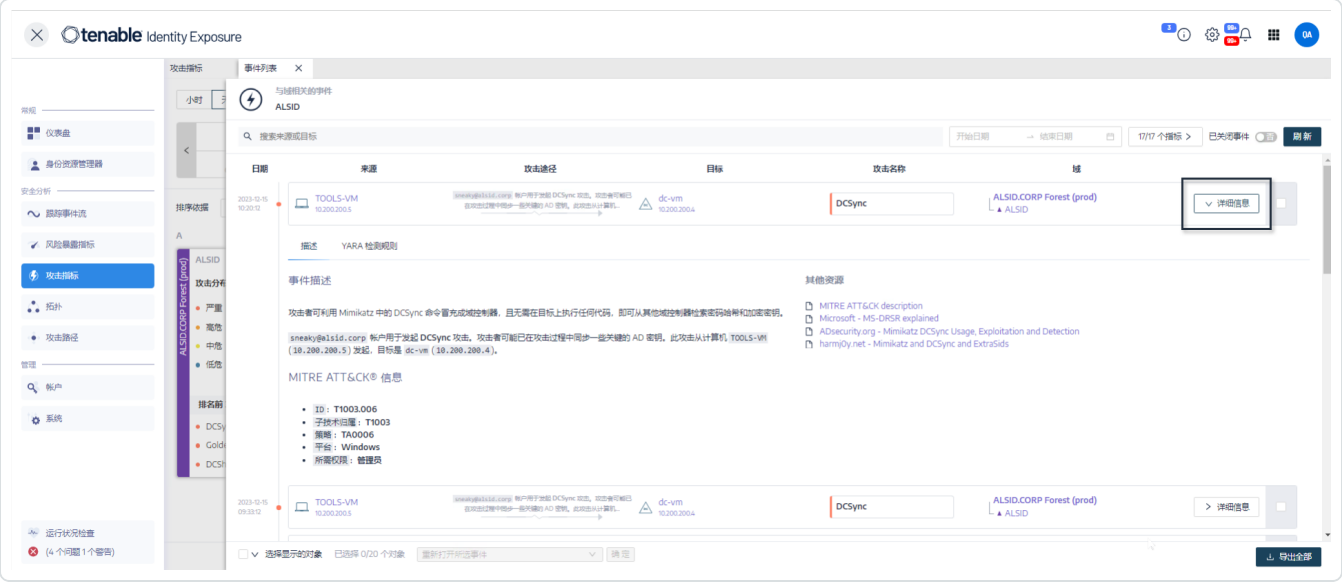
  提示:当您点击**事件列表**中的多个交互式元素(链接、操作按钮等)时,Tenable Identity Exposure 最多可显示五个窗格。若要同时关闭所有窗格,请点击页面上的任意位置。

攻击详细信息

从事件列表中,您可以深入了解特定攻击并采取必要的操作进行修复。

若要显示攻击详细信息:

1. 从事件列表中选择要深入了解哪个事件的详细信息。
2. 点击"**详细信息**"。



Tenable Identity Exposure 将显示与该攻击相关的详细信息:

描述

"**描述选项卡**"包含以下部分：

- **事件描述** - 提供对攻击的简短描述。
- **MITRE ATT&CK 信息** - 显示从 MITRE ATT&CK(对抗性策略、技术和通用知识) 知识库检索的技术信息。Mitre Att&ck 框架用于对攻击进行分类并描述攻击者在入侵网络后所采取的操作。它还提供安全漏洞的标准标识符，以确保网络安全社区能够达成共识。
- **其他资源** - 提供一些网站、文章和白皮书的链接，便于您获取有关此攻击的更深入信息。

YARA 检测规则

YARA 检测规则选项卡描述 Tenable Identity Exposure 在网络级别检测 AD 攻击时使用的 YARA 规则，用来增强 Tenable Identity Exposure 的检测链。

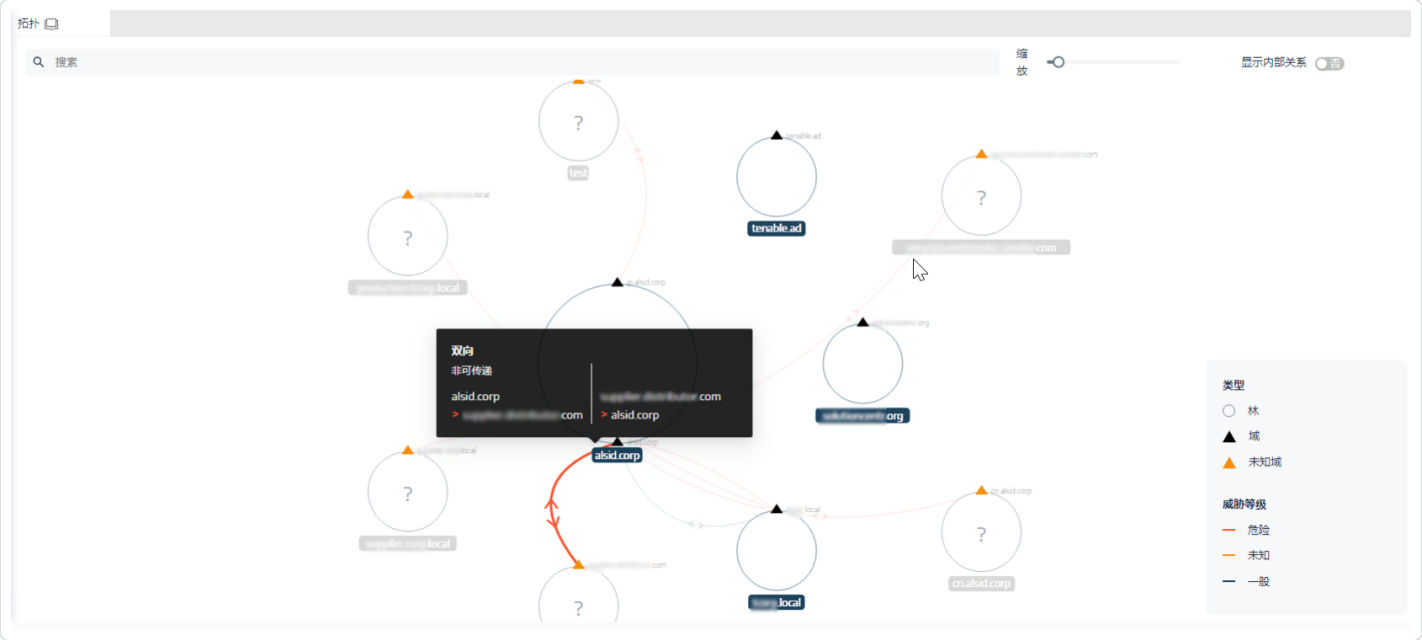
> **注意**：YARA 是一种工具，主要用于恶意软件研究和检测。它是一种基于规则的方法，用于基于文本或二进制模式创建对恶意软件系列的描述。一项描述本质上是一个 YARA 规则名称，这些规则由多组字符串和一个布尔表达式组成(来源：wikipedia.org) 。

另请参阅：

- 攻击指标
- 攻击指标详情

拓扑

“拓扑”页面以交互式图形方式显示 Active Directory。“**拓扑结构图**”显示林、域以及它们之间存在的信任关系。



若要打开“拓扑”页面，请执行以下操作：

- 在 Tenable Identity Exposure 中，点击左侧导航菜单上的“**拓扑**”。

  “拓扑”窗格随即打开，并以图形方式展示 AD。

若要搜索域，请执行以下操作：

- 在“**拓扑**”中，在**搜索**框中输入域名。

  Tenable Identity Exposure 突出显示该域。

若要放大图形，请执行以下操作：

- 在“**拓扑**”窗格中，点击“**缩放**”滑块可调整图形大小。

若要显示两个域之间的链接，请执行以下操作：

- 在“**拓扑**”窗格中，点击以将“**显示内部关系**”开关切换为“**是**”。

若要显示有关域的详细信息，请执行以下操作：

- 在“**拓扑**”窗格中，点击域名的 ▲。

  “**域详细信息**”窗格随即打开，其中包含检测到的风险暴露指标 (IoE) 和域的合规性分数。可以点击 IoE 磁贴，以深入了解更多信息。

另请参阅：

- 信任关系
- 危险的信任

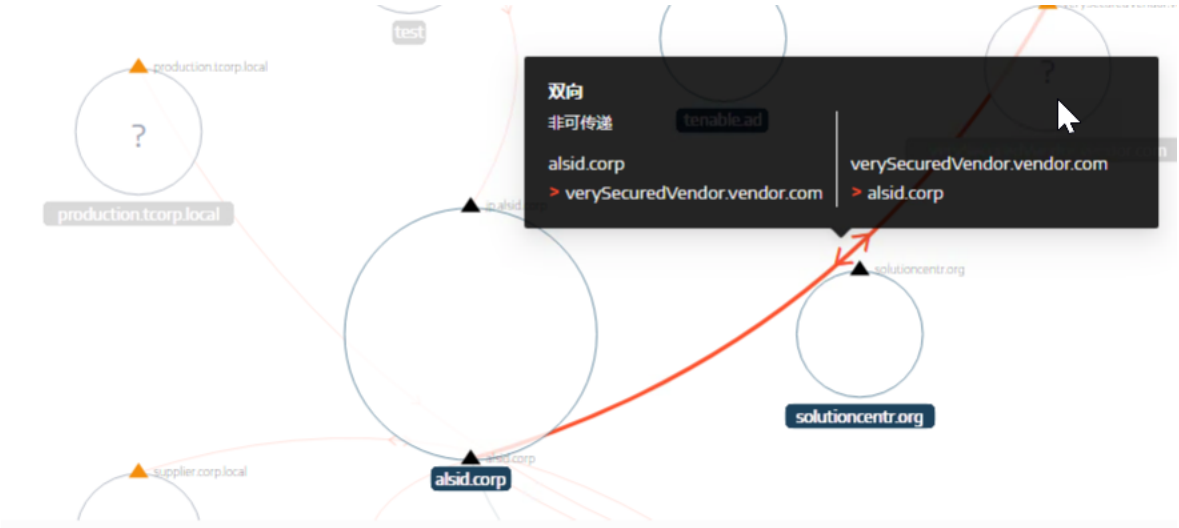
信任关系

拓扑图上的域之间的曲线箭头代表信任关系。

若要显示信任关系，请执行以下操作：

- 在拓扑图上，将鼠标悬停在曲线箭头上。

  Tenable Identity Exposure 通过显示两个实体之间的特定属性显示信任关系。



信任关系的颜色表示威胁等级：

- **红色**表示危险的信任
- **橙色**表示一般信任
- **蓝色**表示未知信任

有关更多信息，请参阅“危险的信任”。

信任属性信息将信任方向表示为“**单向**”或“**双向**”（传入/传出），并显示下列值之一：

值	说明
不可传递	默认情况下，林内信任是可传递信任。Tenable Identity Exposure 使用此标记将它们转换为不可传递信任。另一方面，默认情况下林间信任是不可传递的，因此存在林可传递标记。如果存在林内域间信任，则 Tenable Identity Exposure 显示此值。该信任不授予林以外的互连域访问权限，也不授予其他任何权限。

林可传递	表示两个林之间存在可传递信任。授予其他域的信任可传递至受信任的林。
林内	表示同一林内存在域间信任。如果 `WITHIN_FOREST` 和 `QUARANTINED_DOMAIN` 都存在，则信任被称为 **QuarantinedWithinForest**。
仅限较新版本	表示只有运行 Windows 2000 及更新版本操作系统的客户端可以使用此信任。
视为外部	(仅当 `FOREST_TRANSITIVE` 应用时)表示信任为外部类型。Tenable Identity Exposure 会修改按信任过滤的安全标识符 (SID)，并授权其相对标识符 (RID) 大于或等于 1000 的 SID 通过林。
隔离	表示 Tenable Identity Exposure 已为信任启用 SID 过滤(其 RID 大于或等于 1000)。默认情况下，Tenable Identity Exposure 仅对外部信任启用该功能，但它也可应用于父/子信任或林信任 。
跨组织身份验证	表示 Tenable Identity Exposure 已启用选择性身份验证并可跨域或林信任使用该功能。
选择性身份验证	请参阅跨组织身份验证。
跨组织未启用 TGT 委派	如果完全禁用受信任域中的委派(从不设置已发布的服务票据中的 ok-as-delegate 选项)，则显示此信息。
RC4 加密：	表示该信任支持用于 Kerberos 交换的 RC4 加密密钥。仅当 `trustType` 应用于 `TRUST_TYPE_MIT` 时才存在此标记。
AES 密钥	表示该信任支持用于 Kerberos 交换的 AES 加密密钥。
PIM 信任	如果 `FOREST_TRANSITIVE` 和 `TREAT_AS_EXTERNAL` 标记适用，但尚未启用 `QUARANTINED_DOMAIN` 标记，则 PIM 信任标志表示受信任的林管理与 SID 过滤(本地 SID 可跨此信任传递)有关的特权身份(特权身份管理)。PIM 信任用于实

	现堡垒林。
无属性	表示外部信任没有特定属性。

危险的信任

信任关系的颜色表示威胁等级：

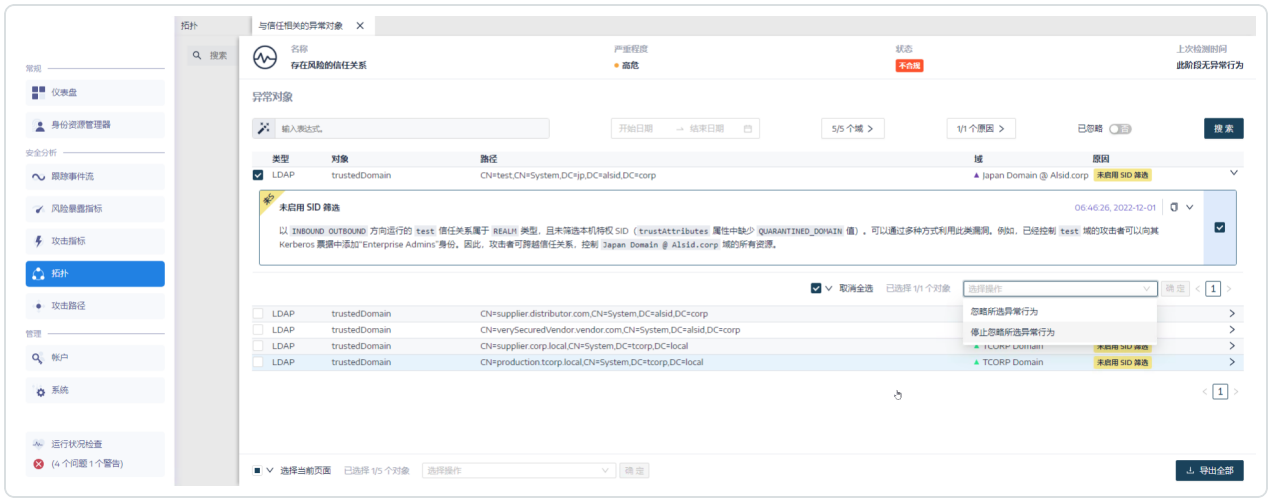
- **红色**表示危险的信任
- **橙色**表示一般信任
- **蓝色**表示未知信任

若要调查危险的信任，请执行以下操作：

1. 在拓扑图中，点击曲线箭头。

   “**与信任相关的异常对象**”窗格随即打开。

   > **提示**：此“危险信任关系”窗格中显示的事件详细信息均链接到“**危险信任关系**”风险暴露指标（也可以从“**风险暴露指标**”导航菜单访问）。



2. 悬停鼠标并点击列表中的异常对象，以显示详细信息。

若要导出异常对象，请执行以下操作：

1. 在拓扑图中，点击曲线箭头。

   “**与信任相关的异常对象**”窗格随即打开。

2. 点击“**导出全部**”。

   “**导出异常对象**”窗格随即打开。

3. 在“**导出格式**”框中，点击下拉箭头以选择格式。
4. 点击“**导出全部**”。

   Tenable Identity Exposure 以所选格式将文件下载到计算机。
5. 点击 **X** 关闭窗格。

攻击路径

Tenable Identity Exposure 提供多种方式来通过图形展示方式可视化业务资产的潜在漏洞。

- **攻击路径**：显示攻击者可从进入点危害资产的路径。
- **爆炸半径**：显示从任何资产到 Active Directory 可能的横向移动。
- **资产风险**：显示可能控制某项资产的所有路径。

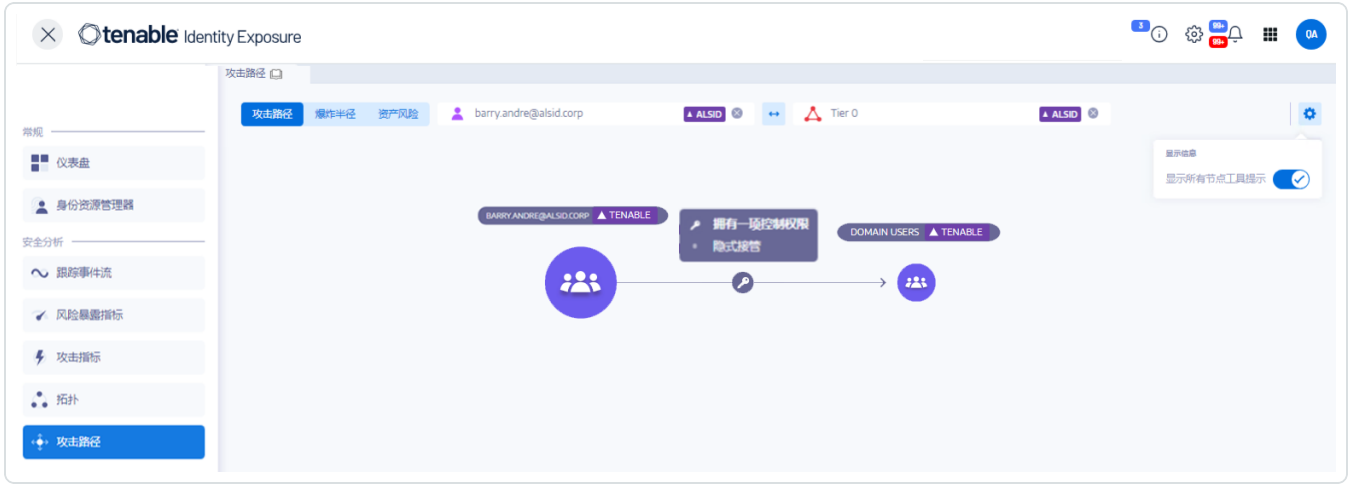
若要显示攻击路径，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击侧边栏菜单上的“**攻击路径**”。

   “**攻击路径**”窗格随即出现。

2. 在标题栏中，点击“**攻击路径**”。
3. 在“**起点**”框中，输入进入点的资产。
4. 在“**终点**”框中，输入路径末端的资产。
5. 点击  图标。

   Tenable Identity Exposure 显示两个资产之间的攻击路径。



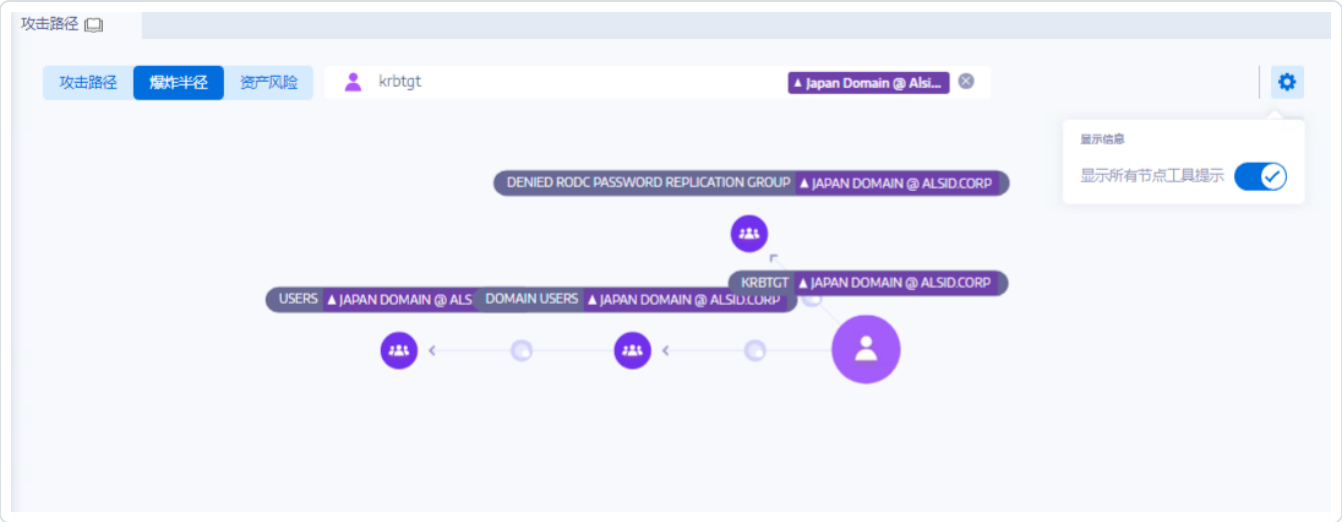
6. 或者，可以点击  图标来执行以下操作：
    - 点击“**缩放**”滑块以调整图形的放大倍数。
    - 点击“**显示所有节点工具提示**”开关，以显示有关资产的信息。

若要显示爆炸半径，请执行以下操作：

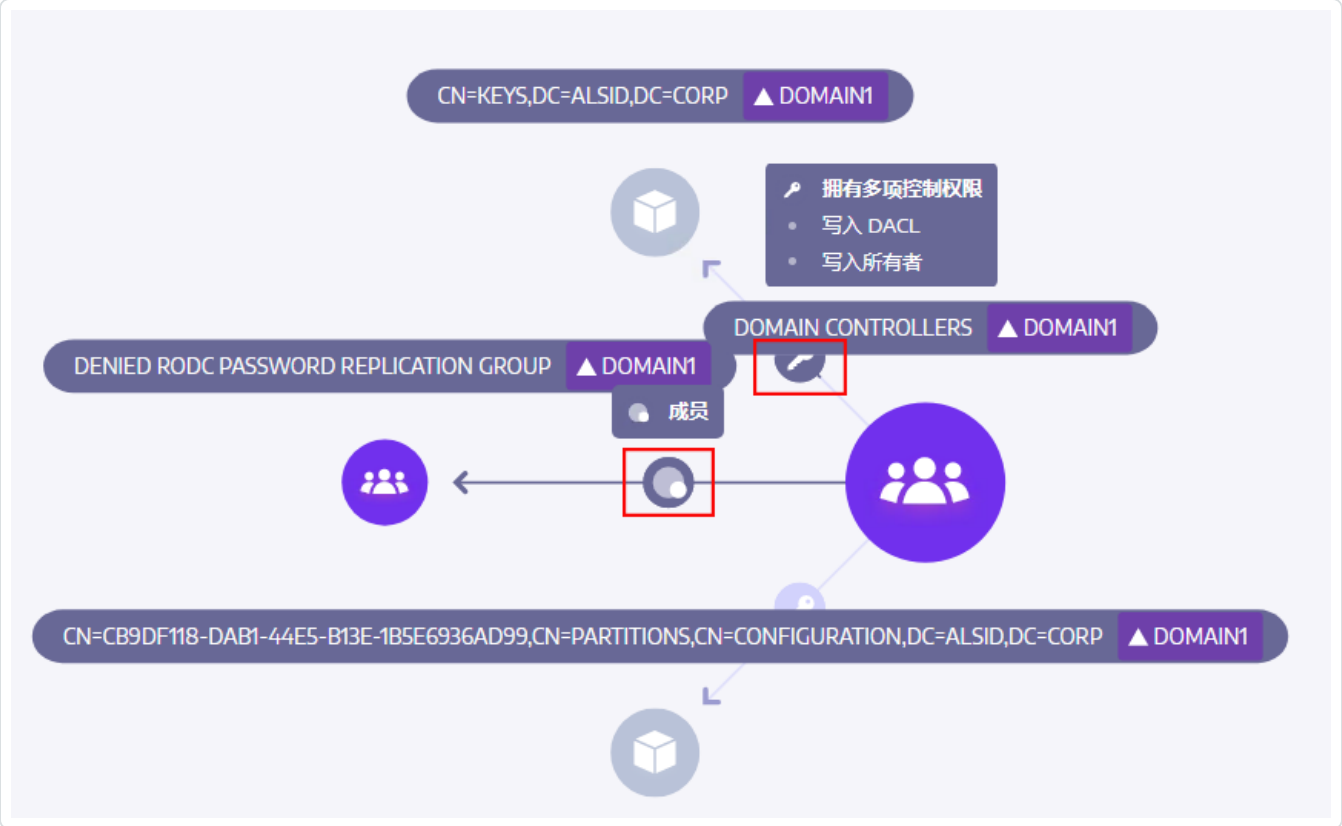
1. 在 Tenable Identity Exposure 中，点击侧边栏菜单上的“**攻击路径**”。

   “**攻击路径**”窗格随即出现。
2. 在标题栏中，点击“**爆炸半径**”。
3. 在“**搜索对象**”框中，输入资产的名称。
4. 点击  图标。

   Tenable Identity Exposure 显示该资产辐射的横向连接：



5. 点击资产之间的箭头上的图标，以显示它们之间的关系。



若要显示资产风险暴露，请执行以下操作：

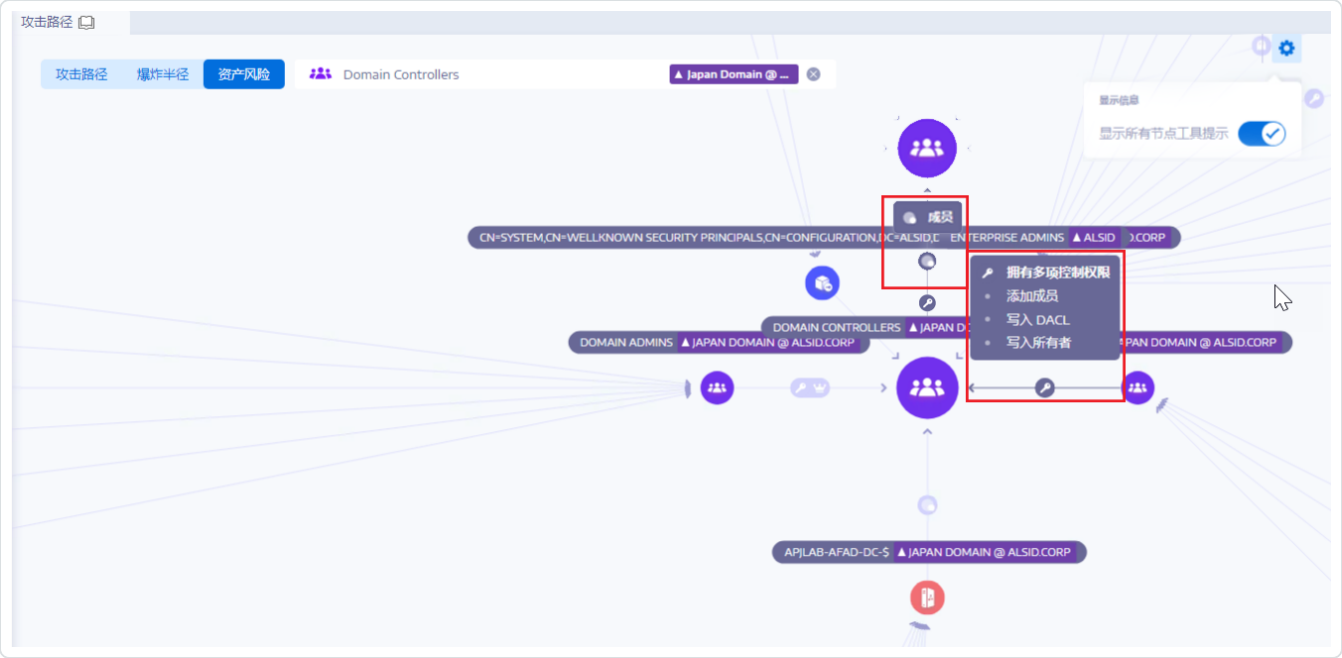
1. 若要显示爆炸半径，请执行以下操作：
2. 在 Tenable Identity Exposure 中，点击侧边栏菜单上的“**攻击路径**”。

"**攻击路径**"窗格随即出现。

3. 在标题栏中，点击"**资产风险**"。
4. 在"**搜索对象**"框中，输入资产的名称。
5. 点击 图标。

   Tenable Identity Exposure 显示通向资产的路径以及资产之间的关系。

6. 点击资产之间的箭头上的图标，以显示它们之间的关系。



若要固定攻击路径：

1. 在攻击路径上点击要突出显示的节点。

   Tenable Identity Exposure 将在屏幕上固定该攻击路径。

2. 若要取消固定攻击路径，请点击 图标或其他攻击路径上的其他节点。

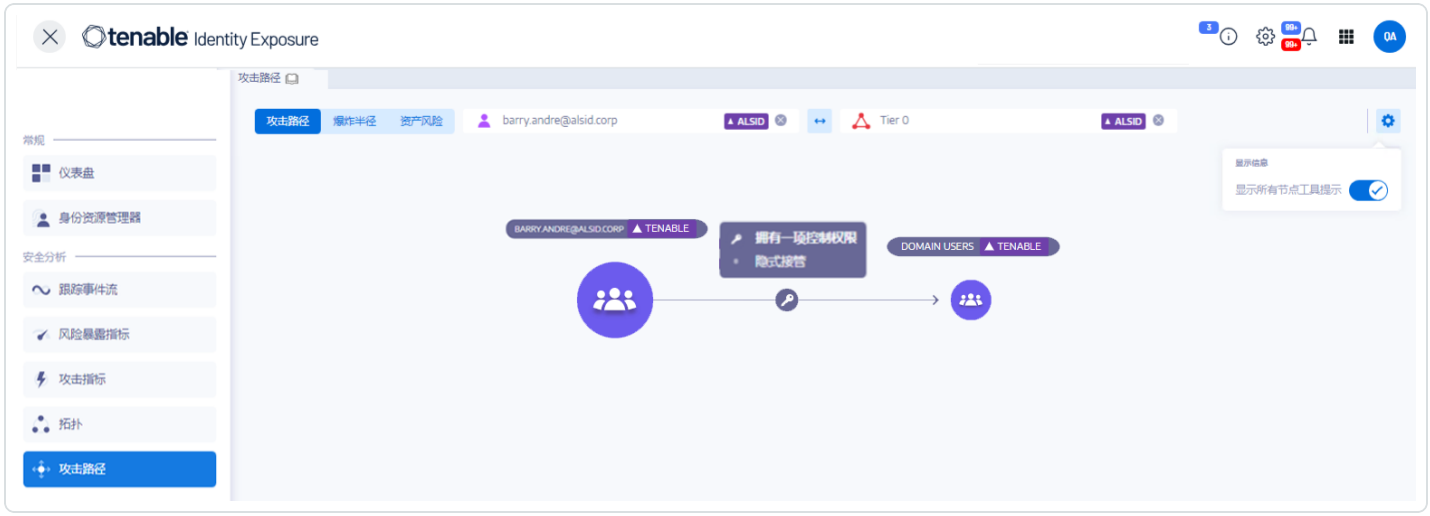

攻击路径
攻击路径
爆炸半径
资产风险
Account Operators
Japan Domain @ ...
CN=SYSTEM,CN=WELL-KNOWN SECURITY PRINCIPALS,CN=CONFIGURATION,DC=ALSID,C
ENTERPRISE ADMINS
ALSID
CORP
ACCOUNT OPERATORS
JAPAN DOMAIN @ ALSID.CORP
DOMAIN ADMINS
JAPAN DOMAIN @ ALSID.CORP
ADMINISTRATORS
JAPAN DOMAIN @ ALSID.CORP

另请参阅：

- 攻击关系

攻击关系

从源节点到目标节点的攻击关系为单向关系。由于关系可传递，攻击者可以将其链接在一起，创建"攻击路径"：



Tenable Identity Exposure 具有下列攻击关系：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属

- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

添加密钥凭据

说明

源安全主体可通过利用密钥信任帐户映射(也称为密钥凭据或"影子凭据")假冒目标。

这之所以可能实现是因为源有权编辑目标的 `msDS-KeyCredentialLink` 属性。

Windows Hello for Business (WHfB) 通常会使用此功能,但即使未使用该功能,攻击者也可加以利用。

渗透利用

危害源安全主体的攻击者必须使用 Whisker 或 DSInternals 等专门的黑客工具来编辑目标计算机的 `msDS-KeyCredentialLink` 属性。

攻击者的目标是向此目标的属性添加他们拥有其私钥的新证书。然后,他们会使用 Kerberos PKINIT 协议,通过已知私钥作为目标进行身份验证,从而获得 TGT。此协议还允许攻击者获取目标的 NTLM 哈希。

修复

多个本机特权安全主体在默认情况下拥有此权限,即 Account Operators、Administrators、Domain Admins、Enterprise Admins、Enterprise Key Admins、Key Admins 和 SYSTEM。这些合法的安全主体无需修复。

对于无修改此属性的合理需求的源安全主体,必须删除此权限。搜索"写入所有属性"、"写入 msDS-AllowedToActOnBehalfOfOtherIdentity"、"完全控制"等权限。

另请参阅:

- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync

- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

添加成员

说明

源安全主体可将其自身(经过验证的写入权限)或任何人(写入属性权限)添加至目标组的成员,并从授予该组的访问权限中受益。

执行此操作的恶意安全主体将会创建"成员归属"攻击关系。

渗透利用

危害源安全主体的攻击者只需通过"net group/domain"等本机 Windows 命令、"Add-ADGroupMember"等 PowerShell、"Active Directory 用户和计算机"等管理工具或 PowerSploit 等专用黑客工具来编辑目标组的"members"属性。

修复

如果源安全主体不需要向目标组添加成员的权限,则必须删除此权限。

若要修改目标组的安全描述符,请执行以下操作:

1. 在"Active Directory 用户和计算机"中,右键点击"**属性**">"**安全性**"。
2. 删除"写入成员"、"写入所有属性"、"完全控制"、"所有经过验证的写入"、"添加/删除自身作为成员"等权限。

注意:组可以继承 Active Directory 树中更高级别对象的权限。

另请参阅:

- 添加密钥凭据
- 允许行动
- 允许委派
- 属于 GPO
- DCSync

- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

允许行动

说明

源安全主体可以在目标计算机上执行基于 Kerberos 资源的约束委派。这意味着该主体可以在使用 Kerberos 对在目标计算机上运行的任何服务进行身份验证时，假冒目标计算机。

因此，它通常会导致目标计算机遭到全面入侵。

此攻击也称为基于资源的约束委派 (RBCD)、基于 Kerberos 资源的约束委派 (KRBCD)、基于资源的 Kerberos 约束委派 (RBKCD), 以及"允许代表其他身份行动"。

渗透利用

危害源安全主体的攻击者可以使用 Rubeus 等专用黑客工具，利用合法的 Kerberos 协议扩展 (S4U2self 和 S4U2proxy) ，来伪造 Kerberos 服务票据并假冒目标用户。攻击者将有可能选择假冒特权用户来获得特权访问权限。

攻击者伪造服务票据后，便可使用任何本机管理工具或与 Kerberos 兼容的专用黑客工具执行远程任意命令。

成功的漏洞利用尝试必须满足以下限制：

- 源和目标安全主体必须具有 ServicePrincipalName。如果不具备此条件，Tenable Identity Exposure 不会创建此攻击关系。
- 被锁定为欺骗目标的帐户既不能标记为"敏感且无法委派"(UserAccountControl 中的 `ADS_UF_NOT_DELEGATED`) ，也不能是"Protected Users"组成员，原因是 Active Directory 会保护此类帐户免受委派攻击。

修复

如果源安全主体无需可在目标计算机上执行基于 Kerberos 资源的约束委派 (RBCD) 的权限，则必须将其删除。必须在目标端进行修改，这与"允许委派"委派攻击关系相反。

不能使用"Active Directory 用户和计算机"等现有图形管理工具管理 RBCD。必须改用 PowerShell 来修改 `msDS-AllowedToActOnBehalfOfOtherIdentity` 属性的内容。

使用以下命令列出允许对目标执行操作的源安全主体(位于"Access:"部分) ：

```
Get-ADComputer target -Properties msDS-AllowedToActOnBehalfOfOtherIdentity | Select-Object -
ExpandProperty msDS-AllowedToActOnBehalfOfOtherIdentity | Format-List
```

如果不需要列出的任何安全主体，可以使用以下命令清除所有安全主体：

```
Set-ADComputer target -Clear "msDS-AllowedToActOnBehalfOfOtherIdentity"
```

如果只需从列表中删除一个安全主体，很遗憾，Microsoft 不提供直接命令。必须使用去除要删除的主体的相同列表覆盖该属性。例如，如果“sourceA”、“sourceB”和“sourceC”均受支持，但您只想删除“sourceB”，请运行以下命令：

```
Set-ADComputer target -PrincipalsAllowedToDelegateToAccount (Get-ADUser sourceA),(Get-ADUser sourceC)
```

最后我们一般会建议，为了限制敏感特权帐户遭到此类委派攻击，Tenable Identity Exposure 建议将此类帐户标记为“敏感且无法委派”(ADS_UF_NOT_DELEGATED)，或在仔细验证相关操作影响之后，将其添加到“Protected Users”组。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属

- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

允许委派

说明

源安全主体可以在目标计算机上，使用协议转换执行 Kerberos 约束委派 (KCD)。这意味着该主体可以在使用 Kerberos 对在目标计算机上运行的任何服务进行身份验证时，假冒目标计算机。

因此，它通常会导致目标计算机遭到全面入侵。

渗透利用

危害源安全主体的攻击者可以使用 Rubeus 等专用黑客工具，利用合法的 Kerberos 协议扩展（S4U2self 和 S4U2proxy），来伪造 Kerberos 服务票据并假冒目标用户。攻击者可能会选择假冒特权用户来获得特权访问权限。

攻击者伪造服务票据后，便可使用任何本机管理工具或与 Kerberos 兼容的专用黑客工具执行远程任意命令。

成功的漏洞利用尝试必须满足以下限制：

- 必须为协议转换启用源安全主体（UserAccountControl 中的 `ADS_UF_TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION`/Delegation GUI 中的“使用任何身份验证协议”）。更准确地说，攻击无需协议转换（在 Delegation GUI 中“仅使用 Kerberos”）即可奏效，但攻击者必须首先对源安全主体进行目标用户 Kerberos 身份验证，这一点会加大攻击难度。因此，Tenable Identity Exposure 在此情况下不会创建攻击关系。
- 源和目标安全主体必须具有 ServicePrincipalName。如果不具备此条件，Tenable Identity Exposure 不会创建此攻击关系。
- 被锁定为欺骗目标的帐户既不能标记为“敏感且无法委派”（UserAccountControl 中的 `ADS_UF_NOT_DELEGATED`），也不能是“Protected Users”组成员，原因是 Active Directory 会保护此类帐户免受委派攻击

相反，支持委派的目标计算机可由服务主体名称 (SPN) 指定，因此包含带“cifs/host.example.net”的 SMB、带“http/host.example.net”的 HTTP 等特定服务。但是，攻击者实际上可以使用“sname 替换攻击”，瞄准在相同目标帐户下运行的任何其他 SPN 和服务。因此，这不是限制。

修复

如果源安全主体不需要可在目标计算机上执行基于 Kerberos 的约束委派 (KCD) 的权限，则必须将其删除。必须在源端进行修改，这与“允许行动”委派攻击关系相反。

若要删除源安全主体，请执行以下操作：

1. 在“Active Directory 用户和计算机”管理 GUI 中，转至源对象的“**属性**”>“**委派**”选项卡。
2. 删除与目标对应的服务主体名称。
3. 如果不需要来自此源的任何委派，请删除所有 SPN，然后选择“不信任此计算机进行委派”。

或者，可以使用 PowerShell 修改源的“msDS-AllowedToDelegateTo”属性的内容。

- 例如，在 Powershell 中，运行此命令即可替换所有值：

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Replace @{ "msDS-
AllowedToDelegateTo" = @("cifs/desiredTarget.example.net") }
```

- 如果不需要来自此源的任何委派，请运行以下命令以清除该属性：

```
Set-ADObject -Identity "CN=Source,OU=corp,DC=example,DC=net" -Clear "msDS-
AllowedToDelegateTo"
```

还可以通过禁用协议转换来降低风险，同时不完全关闭此攻击路径。这要求所有安全主体仅使用 Kerberos(而非 NTLM) 连接到源。

若要禁用协议转换，请执行以下操作：

1. 在“Active Directory 用户和计算机”管理 GUI 中，转至源对象的“**属性**”>“**委派**”选项卡。
2. 选择“仅使用 Kerberos”，而非“使用任何身份验证协议”。

或者，可以在 PowerShell 中运行以下命令来禁用协议转换：

```
Set-ADAccountControl -Identity "CN=Source,OU=corp,DC=example,DC=net" -TrustedToAuthForDelegation
$false
```

最后我们一般会建议，为了限制敏感特权帐户遭到此类委派攻击，Tenable Identity Exposure 建议将此类帐户标记为“敏感且无法委派”(ADS_UF_NOT_DELEGATED)，或在仔细验证相关操作影响之后，将其添加到“Protected Users”组。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 属于 GPO
- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

属于 GPO

说明

SYSVOL 共享中的源 GPO 文件或文件夹属于目标 GPC (GPO), 这意味着它定义 GPO 应用的设置或程序/脚本。

渗透利用

攻击者不会单独使用这种攻击关系。但作为示例，它可以显示完整的攻击路径，其中控制属于 GPO 的 GPO 文件/文件夹的攻击者可在攻击路径末端对用户/计算机强制执行任意设置或启动脚本。

修复

此关系显示了在 SYSVOL 中找到的 GPO 文件和文件夹如何与相应的 GPC (GPO) 对象相关联。这是正常现象，也是设计使然。

因此无需修复。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO

- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

DCSync

说明

DCSync 是域控制器仅用于复制更改的合法 Active Directory 功能，但非法安全主体也可以使用该功能。

源安全主体可以使用 DCSync 功能请求目标域的敏感机密（密码哈希、Kerberos 密钥等），最终导致域遭到全面破坏。

提取密码需要两个安全权限，即“Replicating Directory Changes”(`DS Replication Get Changes`)和“Replicating Directory Changes All”(`DS Replication Get Changes All`)。仅当直接或通过嵌套组成员身份将这些权限同时授予源时，才会出现该关系。

渗透利用

危害源安全主体的攻击者可使用 *mimikatz* 或 *impacket* 等专用黑客工具获取密码。

- **黄金票据**：通过获取“krbtgt”帐户的密码哈希可以伪造 Kerberos TGT，并允许在任何计算机/服务上假冒任何人。这将特别授予域中任何计算机的管理权限。
- **白银票据**：通过获取计算机/服务帐户的密码哈希可以伪造 Kerberos TGT，并允许在指定计算机/服务上假冒任何人。

修复

默认情况下，可以利用 DCSync 的合法安全主体是：

- 管理员
- 域管理员
- 企业管理员
- 系统

此外，Microsoft Entra ID Connect 配置允许其密码哈希同步服务帐户 (MSOL_...) 以利用 DCSync。

最后，可以发现某些安全工具的服务帐户，尤其是密码审核解决方案。与负责人员一同验证其合法性。

对于无执行 DCSync 的合理需求的源安全主体，必须删除此权限。

若要修改目标域的安全描述符，请执行以下操作：

1. 在“Active Directory 用户和计算机”中，右键点击域名，然后选择“属性”>“安全性”。
2. 删除非法安全主体的“复制目录变更”和“复制目录变更 - 全部”权限。

注意：DCSync 关系可通过来自嵌套组成员身份的权限产生。因此，根据具体情况，必须删除组本身或仅删除其中的部分成员。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

允许行动的授权

说明

允许源安全主体授予自己或他人与目标计算机的 允许行动 关系。这种关系通常会通过 Kerberos RBCD 委派攻击导致目标计算机遭到全面破坏。

这之所以可能实现是因为源有权编辑目标的“msDS-AllowedToActOnBehalfOfOtherIdentity”属性。

执行此操作的恶意安全主体会创建“允许行动”攻击关系。

渗透利用

危害源安全主体的攻击者必须使用 PowerShell 编辑目标计算机的 `msDS-AllowedToActOnBehalfOfOtherIdentity`(例如“Set-ADComputer<target> -PrincipalsAllowedToDelegateToAccount ...”) 。

修复

多个本机特权安全主体在默认情况下拥有此权限，即 Account Operators、Administrators、Domain Admins、Enterprise Admins 和 SYSTEM。这些安全主体合法，且无需修复。

Kerberos RBCD 的设计目的是使计算机的管理员可以将在计算机上执行委派的权限授予任何需要的人员。这与需要域管理员级别权限的其他 Kerberos 委派模式有所差异。这允许较低级别的管理员自行管理这些安全设置，此原则也称为委派。在这种情况下，该关系是合法的。

但是，如果源安全主体不是目标计算机的合法管理员，则该关系不合法，并且必须删除此权限。

若要修改目标计算机的安全描述符，请执行以下操作：

1. 在“Active Directory 用户和计算机”中，右键点击“**属性**”>“**安全性**”。
2. 删除提供给源安全主体的权限。搜索“写入 msDS-AllowedToActOnBehalfOfOtherIdentity”、“写入所有属性”、“写入帐户限制”、“完全控制”等权限。

注意：源安全主体可以继承 Active Directory 树中更高级别对象的权限。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

有 SID 历史记录

说明

源安全主体在其 SIDHistory 属性中具有目标安全主体的 SID，这意味着源与目标具有相同的权限。

SID 历史记录是一个在域之间迁移安全主体时使用的合法机制，目的在于保持所有授权参考其之前的 SID 功能。

但是，这也是攻击者使用的持久性机制，因为它允许谨慎的后门帐户具有与所需目标（例如管理员帐户）相同的权限。

渗透利用

危害源安全主体的攻击者可直接作为目标安全主体进行身份验证，因为目标的 SID 显然已添加到 Active Directory 身份验证机制生成的令牌中（NTLM 和 Kerberos）。

修复

如果源和目标安全主体与经过批准的域迁移有关，则可将此关系视为合法关系，并且无需执行任何操作。此关系仍然可做作为潜在攻击路径提示显示。

如果原始域在迁移后被删除，或者未在 Tenable Identity Exposure 中进行配置，则目标安全主体将被标记为未解析。由于风险存在于目标中而该目标不存在，因此不存在风险，无需修复。

相反，与本机特权用户或组的 SID 历史记录关系很可能是恶意的，因为 Active Directory 阻止此类关系的创建。这意味着此类关系很可能是使用“DCShadow”攻击等黑客技术创建的。也可以在与“SID 历史记录”相关的 IoE 中找到这些案例。

如果是这样，Tenable Identity Exposure 建议对整个 Active Directory 林进行取证检查。原因是攻击者必须已经获得高特权（域管理员或同等特权），才能恶意编辑源的 SID 历史记录。取证检查有助于通过相应的修复指南分析攻击，并确定要删除的潜在后门程序。

最后，Microsoft 建议修改所有服务（SMB 共享、Exchange 等）中的所有访问权限，以便在此迁移完成后使用新的 SID，同时删除不必要的 SIDHistory 值。这是内务处理的最佳做法，但详尽无遗地识别并修复所有 ACL 非常困难。

有权编辑源对象本身上的 SIDHistory 属性的用户可以删除 SIDHistory 值。与创建相反，此操作无需域管理员权限。

为此，只能使用 PowerShell，原因是 Active Directory 用户和计算机等图形工具将会失败。示例：

```
Set-ADUser -Identity <user> -Remove @{sidhistory="S-1-..."}
```

注意：虽然删除 SIDHistory 值十分容易，但恢复此操作却非常复杂。这是因为必须重新创建 SIDHistory 值，而这要求存在可能已停用的其他域。因此，Microsoft 还建议准备快照或备份。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

隐式接管

说明

源是 Tier0 安全主体。Tier0 是在域中拥有最高特权的 Active Directory 对象集，例如 Domain Admins 或 Domain Controllers 组的成员。即使没有明确的其他关系，所有 Tier0 资产亦可隐式危害域中的任何其他对象。

此关系让对内置到 Active Directory 中的隐式权限建模成为可能。这些权限源于设计且记录在案，因此均属攻击者已知范畴。但是，Tenable Identity Exposure 无法通过标准途径获得这些权限。此外，此关系简化了攻击路径图，因为一旦攻击者破坏 Tier0 节点，他们便可直接攻击任何其他对象，且不会遇到其他显式关系。

总而言之，源 Tier0 资产被视为与图表中的任何目标节点都具有"隐式接管"关系。

渗透利用

具体的渗透利用方法取决于锁定的源 Tier0 资产的类型，但这些方法均属于有据可查的技术，便于攻击者有效掌握。

修复

此关系源自设计，无法修复。几乎无法阻止访问 Tier0 资产的攻击者进行进一步攻击。

修复措施必须以攻击路径中的上游关系为重点。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权

- 有 SID 历史记录
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

继承 GPO

说明

组织单位 (OU) 或域(而非站点) 等源可链接容器包含 LDAP 树中的目标 OU、用户、设备、DC 或只读域控制器 (RODC)。这是因为可链接容器的子对象继承了与之链接的 GPO(请参阅"链接的 GPO"关系) 。

Tenable Identity Exposure 会将 OU 阻止继承的所有情况考虑在内。

渗透利用

只要攻击者设法破坏攻击路径上游的 GPO, 他们便没有必要利用这种关系。按照设计, 该关系适用于可链接的容器及其中的对象, 正如继承 GPO 关系所示。

修复

在大多数情况下, 将 GPO 应用到来自其父容器的可链接子容器属于正常且合法的行为。但是, 此链接会暴露其他攻击路径。

因此, 为了降低风险, 应尽可能将 GPO 链接到组织单位层次结构中的最低级别。

此外, GPO 需要防止攻击者在未经授权的情况下进行修改, 以免将其暴露给其他攻击关系。

最后, OU 可通过其"阻止继承"选项禁用更高级别的 GPO 继承。但是, 请仅将此选项用作最后手段, 因为它会阻止所有 GPO, 包括在最高域级别定义的潜在安全强化 GPO。它还会加大对已应用 GPO 进行推理的难度。

另请参阅 :

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync

- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

链接的 GPO

说明

源 GPO 链接到域或组织单位 (OU) 等目标可链接容器。这意味着源 GPO 可以在目标中包含的设备和用户上分配设置和运行程序。源 GPO 还可通过“继承 GPO”关系应用到其下面的容器中的对象。

最终，GPO 会破坏它应用到的设备和用户。

渗透利用

攻击者必须首先通过另一个攻击关系破坏源 GPO。

然后，他们会采用多种技术，对目标及其中的设备和用户执行恶意操作。示例如下：

- 滥用合法的“即时计划任务”在设备上执行任意脚本。
- 在所有设备上添加具有管理权限的新本地用户
- 安装 MSI 程序
- 禁用防火墙或杀毒软件
- 授予更多权限
- 等

攻击者可以使用“组策略管理”等管理工具或 PowerSploit 等专用黑客工具，通过手动编辑 GPO 的内容对其进行修改。

修复

在大多数情况下，将 GPO 链接到可链接容器属于正常且合法的行为。但是，此链接会扩大其出现位置及其所属容器中的攻击面。

因此，为了降低风险，应尽可能将 GPO 链接到组织单位层次结构中的最低级别。

此外，GPO 需要防止攻击者在未经授权的情况下进行修改，以免将其暴露给其他攻击关系。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

成员归属

说明

源安全主体是目标组的成员。因此，该主体可通过组拥有的所有访问权限受益，例如访问文件共享、在业务应用程序中担任角色等。

渗透利用

攻击者无需执行任何操作即可利用此攻击关系。它们只需作为源安全主体进行身份验证，即可获取其本地或远程安全标令牌或 Kerberos 票据中的目标组。

修复

如果源安全主体是目标组的非法成员，则必须将其删除。

您可以使用"Active Directory 用户和计算机"等任何标准 Active Directory 管理工具 或 Remove-ADGroupMember 等 PowerShell。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO

- 拥有
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

拥有

说明

源安全主体是目标对象声明的所有者，因为它可能是该目标对象的创建者。所有者具有隐式权限（“读取控制”和“写入 DACL”），可让他们为自己或他人获取更多权限，并最终危害目标对象。

渗透利用

危害源安全主体的攻击者只需通过“dsacls”等本机 Windows 命令、“Set-ACL”等 PowerShell、“Active Directory 用户和计算机”等管理工具或 PowerSploit 等专用黑客工具来编辑目标对象的安全描述符。

创建对象时存在特权提升的风险，前提是该对象由低权限用户创建并因此拥有（例如标准帮助台技术人员），随后该对象被提升为更高特权（例如管理员）。原始所有者仍然存在，并且现在可以破坏新特权对象，以利用其权限。

修复

如果源安全主体不是目标对象的合法所有者，则必须对其进行更改。

若要更改目标对象的所有者，请执行以下操作：

1. 在“Active Directory 用户和计算机”中，右键点击“**属性**”>“**安全性**”>“**高级**”。
2. 在顶部的“**所有者**”行上点击“**更改**”。

大多数敏感 Active Directory 对象在默认情况下使用的 Safe Target 对象所有者为：

- 域分区中的对象：“管理员”或“域管理员”
- 配置分区中的对象：“企业管理员”
- Schema 分区中的对象：“Schema 管理员”

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 重置密码
- RODC 管理
- 写入 DACL
- 写入所有者

重置密码

说明

源安全主体可重置目标的密码，从而使其能够使用新的属性密码对目标进行身份验证，并通过目标的特权受益。

重置密码与更改密码不同，更改密码操作可由知道当前密码的任何人执行。密码过期时，通常需要更改密码。

渗透利用

危害源安全主体的攻击者只需通过使用“net user /domain”等本机 Windows 命令、“Set-ADAccountPassword -Reset”等 PowerShell、“Active Directory 用户和计算机”等管理工具或 PowerSploit 等专用黑客工具来重设目标的密码。

此后，攻击者只需使用合法的身份验证方法，以其新选择的密码对 Active Directory 或目标资源进行身份验证，即可完全假冒目标。

但是，攻击者通常不知道要在攻击后恢复为以前的密码。因此，攻击通常对目标背后的合法人员可见，甚至会造成拒绝服务，对于服务帐户更是如此。

修复

IT 管理员和服务台工作人员可以依法重置密码。但您必须建立适当的委派，以便他们仅在其允许的范围内执行此操作。

此外，根据分层模型，必须确保普通用户服务台等较低级别的工作人员无法重置较高级别帐户（例如域管理员）的密码，因为这是一个可以提升特权的机会。

若要修改目标的安全描述符并删除非法权限，请执行以下操作：

1. 在“Active Directory 用户和计算机”中，右键点击“属性”>“安全性”。
2. 删除源安全主体的“重置密码”权限。

> **注意**：请勿将此权限与“更改密码”混淆。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- RODC 管理
- 写入 DACL
- 写入所有者

RODC 管理

说明

源安全主体可在目标只读域控制器 (RODC) 的“ManagedBy”属性中找到。这意味着源对目标 RODC 具有管理权限。

> **注意**：其他 Active Directory 对象类型仅出于参考目的使用相同的“ManagedBy”属性，且不为声明的管理器提供任何管理权限。因此，此关系仅适用于 RODC 类型的目标节点。

RODC 的敏感程度低于更常见的可写入域控制器，但对于攻击者而言，此类控制器仍然是极具价值的目标，因为它们可以从 RODC 窃取凭据，以便进一步攻击其他系统。这取决于 RODC 配置中的强化级别，例如，具有可同步密钥的对象的数量。

渗透利用

渗透利用方法与“AdminTo”关系相同。

危害源安全主体的攻击者可使用其身份进行远程连接，并使用管理权限在目标 RODC 上执行命令。它们可利用可用的本机协议，例如具有管理共享的服务器消息块 (SMB)、远程桌面协议 (RDP)、Windows Management Instrumentation (WMI)、远程过程调用 (RPC)、Windows 远程管理 (WinRM) 等。

攻击者可使用本机远程管理工具，如 PsExec、services、scheduled Tasks、Invoke-Command 等，或专门的黑客工具，如 wmiexec、smbexec、Invoke-DCOM、SharpRDP 等。

攻击的最终目标既可以是危害目标 RODC，也可以是使用凭据转储工具（例如 mimikatz）获取更多凭据和密码，以便攻击其他计算机。

修复

如果源安全主体不是目标只读域控制器 (RODC) 的合法管理员，则必须将其替换为适当的管理员。

请注意，域管理员通常不会管理 RODC，因此请使用专用的“管理者”设置。这是因为 RODC 的信任级别较低，而高权限的域管理员不应通过对其进行身份验证来暴露其凭据。

因此，必须根据 Active Directory RODC 规则为 RODC 选择适当的“中级”管理员，例如，为其所在组织的本地分支选择 IT 管理员。

若要更改“ManagedBy”属性，请执行以下操作：

1. 在“Active Directory 用户和计算机”中，选择“RODC”>“**属性**”>“**ManagedBy**”选项卡。
2. 点击“**更改**”。

也可以在 PowerShell 中运行以下命令：

```
Set-ADComputer <rodc> -ManagedBy (Get-ADUser <rodc_admin>)
```

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- 写入 DACL
- 写入所有者

写入 DACL

说明

源安全主体有权更改自主访问控制列表 (DACL) 中的目标对象的权限。这允许源为自己获取或授予他人额外的权限，并最终危害目标对象。

渗透利用

危害源安全主体的攻击者只需通过“dsacls”等本机 Windows 命令、“Set-ACL”等 PowerShell、“Active Directory 用户和计算机”等管理工具或 PowerSploit 等专用黑客工具来编辑目标对象的安全描述符。

修复

如果源安全主体没有合法权限来更改目标对象的权限，则必须删除此权限。

若要修改目标对象的安全描述符，请执行以下操作：

1. 在“Active Directory 用户和计算机”中，右键点击该对象，然后点击“**属性**”>“**安全性**”>“**高级**”。
2. 删除源安全主体的权限“修改权限”权限。

注意：对象可以继承 Active Directory 树中更高级别对象的此权限。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO
- DCSync
- 允许行动的授权

- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入所有者

写入所有者

说明

源安全主体有权更改目标对象的所有者，包括将自己分配为所有者。所有者具有隐式权限，即“读取控制”和“写入 DACL”，可让他们为自己或他人获取更多权限，并最终危害目标对象。

有关更多信息，请参阅 拥有 关系。

渗透利用

危害源安全主体的攻击者只需使用“dsacls /takeownership”等本机 Windows 命令、“Set-ACL”等 PowerShell、“Active Directory 用户和计算机”等管理工具或 PowerSploit 等专用黑客工具来分配自己作为目标的所有者。

然后，他们可以使用类似方法编辑目标对象的安全描述符。

修复

如果源安全主体没有合法权限来更改目标对象的所有者，则必须删除此权限。

若要修改目标对象的安全描述符，请执行以下操作：

1. 在“Active Directory 用户和计算机”中，右键点击该对象，然后选择“**属性**”>“**安全性**”>“**高级**”。
2. 删除源安全主体的权限“修改所有者”权限。

> **注意**：对象可以继承 Active Directory 树中更高级别对象的此权限。

另请参阅：

- 添加密钥凭据
- 添加成员
- 允许行动
- 允许委派
- 属于 GPO

- DCSync
- 允许行动的授权
- 有 SID 历史记录
- 隐式接管
- 继承 GPO
- 链接的 GPO
- 成员归属
- 拥有
- 重置密码
- RODC 管理
- 写入 DACL

识别第 0 层资产

第 0 层资产包括对 Active Directory 林和域具有直接或间接管理控制权的帐户、组和其他资产。

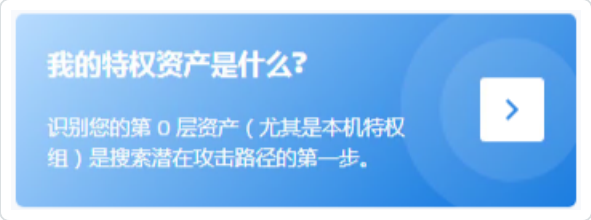
Tenable Identity Exposure 列出您的第 0 层资产和帐户，以及通向该资产的潜在攻击路径。

如要列出第 0 层资产：

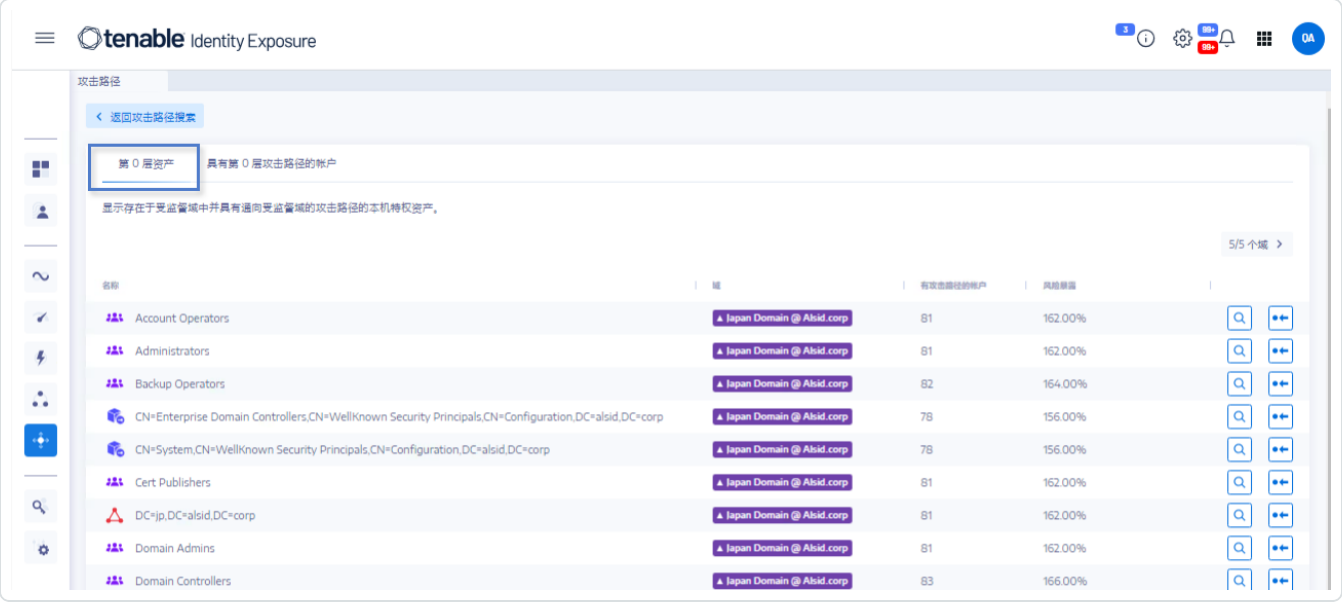
1. 在 Tenable Identity Exposure 中，单击左侧导航栏中的攻击路径图标 。

   “**攻击路径**”窗格随即打开。

2. 单击“**我的特权资产是什么？**”磁贴。

   Tenable Identity Exposure 显示 AD 中的第 0 层资产列表。

   每一行都给出了**资产名称**、其**域**和以下信息：

- **具有攻击路径的帐户**:具有通向第 0 层资产的攻击路径的资产数量。
- **风险暴露**:具有通向第 0 层资产的攻击路径的帐户占域中帐户总数的百分比。

如要过滤任何特定域的资产:

1. 单击"**n/n**"按钮。

   "**林和域**"窗格随即打开。您可以执行以下任一操作:

   - 在**搜索**框中,输入林或域名。
   - 选择"**全部展开**"框并选择所需的林或域。

2. 单击"**按所选结果筛选**"。

   Tenable Identity Exposure 更新资产列表。

如要列出包含通向第 0 层资产的攻击路径的资产:

- 在第 0 层资产名称的行末,单击  图标。

  Tenable Identity Exposure 显示包含通向第 0 层资产的攻击路径的资产列表。

要查看第 0 层资产的资产风险暴露情况,请执行以下操作:

- 在具有第 0 层资产名称的行末,单击  图标。

  Tenable Identity Exposure 打开该第 0 层资产的"资产风险暴露"页面。有关更多信息,请参阅攻击关系

有攻击路径的帐户

Tenable Identity Exposure 显示具有通向第 0 层资产的攻击路径的帐户，以便为您提供潜在安全威胁的全面视图，因为用户和计算机帐户可通过各种攻击关系获得特权。

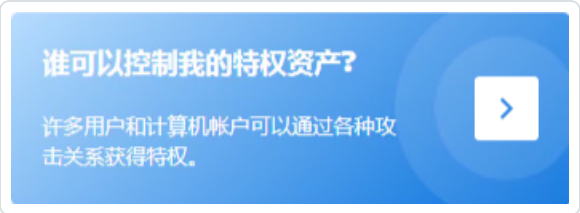
有关更多信息，请参阅“识别第 0 层资产”。

显示带有攻击路径的资产：

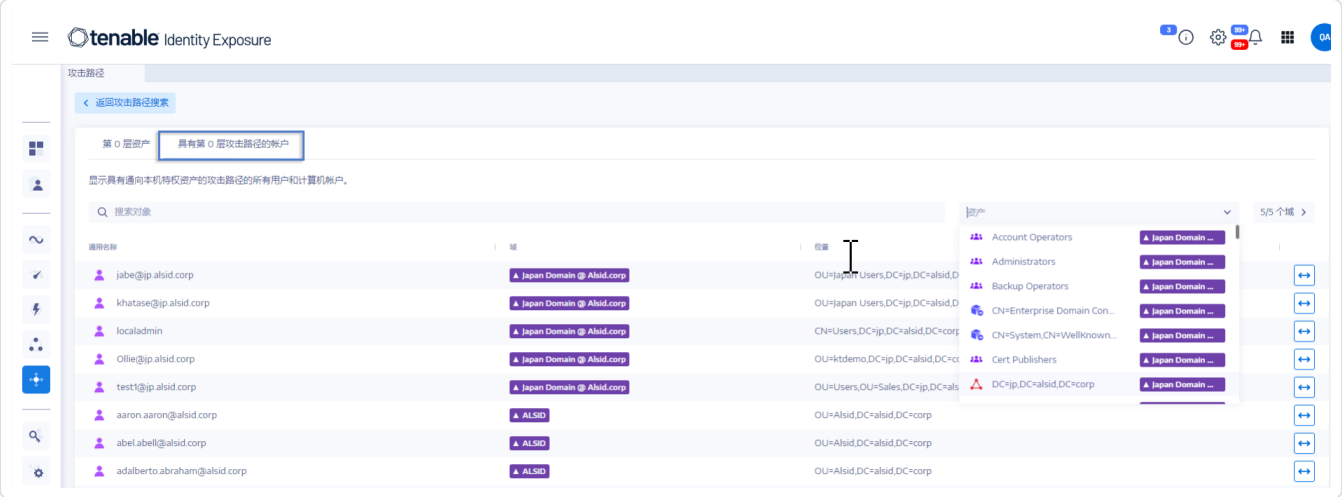
1. 在 Tenable Identity Exposure 中，单击左侧导航栏中的攻击路径图标 。

   “**攻击路径**”窗格随即打开。

2. 单击“**谁有权控制我的特权资产？**”磁贴。

   Tenable Identity Exposure 显示具有通向第 0 层资产的攻击路径的所有用户和计算机帐户。

如要搜索特定资产：

1. 在**搜索**框中，输入资产的名称。
2. 在"**资产**"框中，单击箭头 **>** 以显示第 0 层资产的下拉列表并选择一个资产。

   Tenable Identity Exposure 使用匹配的结果更新列表。

如要过滤任何特定域的资产：

1. 单击"**n/n**"按钮。

   "**林和域**"窗格随即打开。您可以执行以下任一操作：

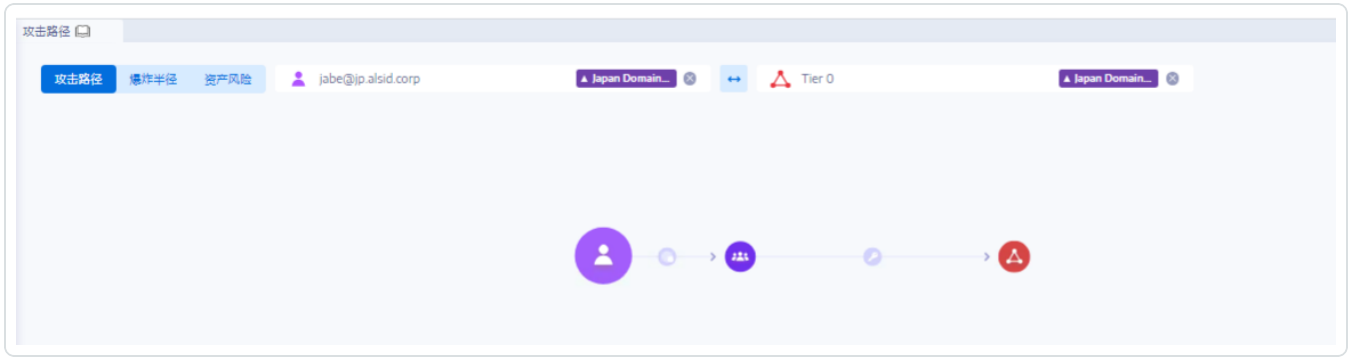
   - 在**搜索**框中，输入林或域名。
   - 选择"**全部展开**"框并选择所需的林或域。
2. 单击"**按所选结果筛选**"。

   Tenable Identity Exposure 更新资产列表。

如要探索攻击路径：

- 在资产名称的行末，单击  图标。

  Tenable Identity Exposure 打开从该资产到所有第 0 层资产的"攻击路径"页面。有关更多信息，请参阅攻击路径和攻击关系。



攻击路径节点类型

Tenable Identity Exposure 中的攻击路径功能会以图表形式显示对 Active Directory 环境中的攻击者开放的攻击路径。该图表包含表示攻击关系的**边**和表示 Active Directory (LDAP/SYSVOL) 对象的**节点**。

以下列表介绍了您可在攻击路径图中看到的所有可能的节点类型。

节点类型	位置	图标	说明
用户	LDAP		LDAP 对象，其“objectClass”属性包含“user”类，而非“computer”类。
组	LDAP		LDAP 对象，其“objectClass”属性包含“class”组。
设备	LDAP		LDAP 对象，其“objectClass”属性包含“computer”类，而非“msDS-GroupManagedServiceAccount”类。 其“primaryGroupID”属性不等于 516 (DC) 或 521 (RODC)。 **注意**：为与 Tenable 产品加以区分，此类别称为“设备”而非“计算机”，以便更通用。
组织单位 (OU)	LDAP		LDAP 对象，其“objectClass”属性包含“organizationalUnit”类。避免将“container”类的对象与任何 Active Directory (AD) 对象均可充当容器以允许其包含其他对象这一事实混淆。
域	LDAP		LDAP 对象，其“objectClass”属性包含“domainDNS”类和特定属性。
域控制器 (DC)	LDAP		LDAP 对象，其“objectClass”属性包含“computer”类，其“primaryGroupID”属性等于 516(因此不是 RODC) 。
只读域控制器 (RODC)	LDAP		LDAP 对象，其“objectClass”属性包含“computer”类，其“primaryGroupID”属性等于 521(因此不是正常 DC) 。

组策略(GPC)	LDAP		LDAP 对象，其“objectClass”属性包含“groupPolicyContainer”类。
GPO 文件	SYSVOL		在特定 GPO 的 SYSVOL 共享中发现的文件(例如“\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\{Machine,User}\Preferences\ScheduledTasks\ScheduledTasks.xml”)
GPO 文件夹	SYSVOL		在特定 GPO 的 SYSVOL 共享中发现的文件夹。每个 GPO 都有一个文件夹(例如“\\example.net\sysvol\example.net\Policies\{A8370D7F-8AC0-452E-A875-2A6A52E9D392}\Machine\Scripts\Startup”)
组托管服务帐户(gMSA)	LDAP		LDAP 对象，其“objectClass”属性包含“msDS-GroupManagedServiceAccount”类。
企业级 NtAuth 存储	LDAP		LDAP 对象，其“objectClass”属性包含“certificationAuthority”类。
PKI 证书模板	LDAP		LDAP 对象，其“objectClass”属性包含“pKICertificateTemplate”类。
未解析的安全主体	LDAP		LDAP 对象的“objectSid”或“DistinguishedName”属性在构建关系时的某个时间点被使用了，但是没有找到对应的 LDAP 安全主体对象(“未解析的 SID”的典型情况)。 亦缺少与之相关的特定安全主体类型(用户、计算机、组等)的信息；仅其 SID/DN 为已知信息。
特殊身份	LDAP		Windows 和 Active Directory 在内部使用已知身份。这些身份的功能类似于组，但 AD 并没有将它们声明为组。有关更多信息，请参阅特殊身份组。

其他			当前不属于上述类别的所有 AD/SYSVOL 对象。

活动日志

在 Tenable Identity Exposure 的活动日志中，可以查看 Tenable Identity Exposure 平台上发生的所有活动的跟踪信息，包括具体的 IP 地址、用户或操作等。

注意：由于技术限制，目前无法查看与租户管理（包括添加、编辑或删除）等特定视图相关的活动日志。

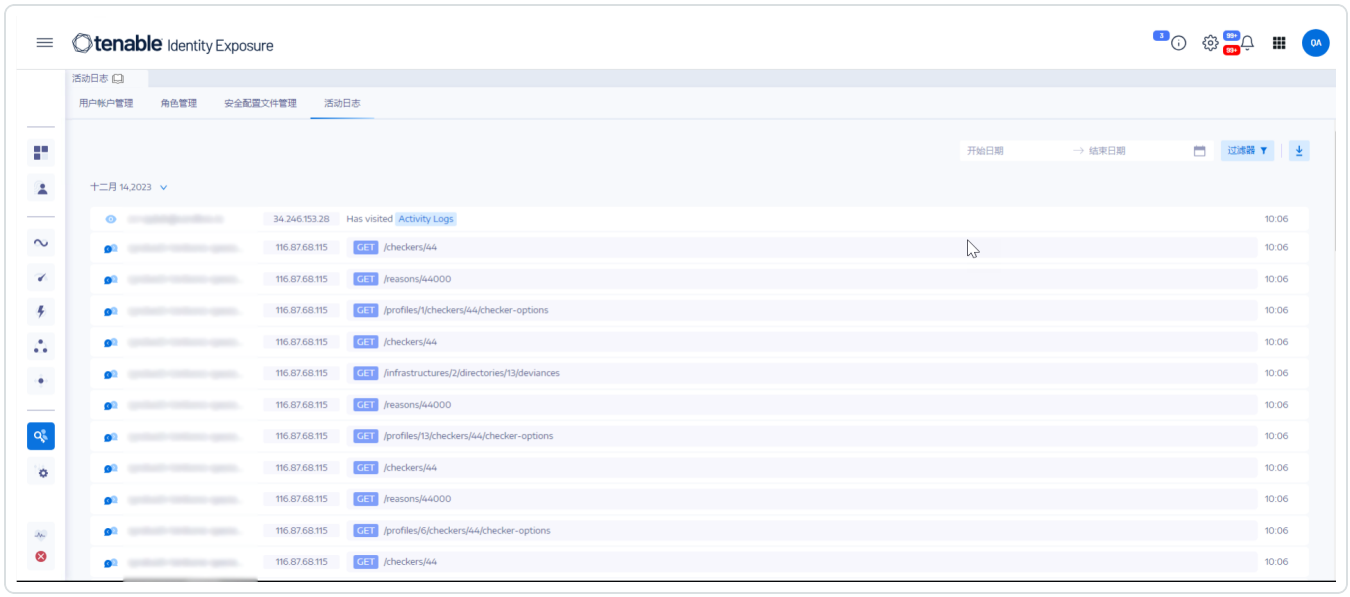
若要查看活动日志，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击左侧导航菜单中的**帐户**图标  。

   此时会出现“**用户帐户管理**”窗格。

2. 选择“**活动日志**”选项卡。

   “活动日志”窗格随即打开。



若要显示特定时间范围的活动日志：

1. 在“活动日志”窗格顶部，点击日期选择器。
2. 为所需时间段选择开始日期和结束日期。
3. （可选）使用滚动条选择时间（默认：当前时间）

4. 点击“**确定**”。

   Tenable Identity Exposure 显示该时间段的活动日志。

若要筛选活动日志：

1. 在“活动日志”窗格顶部，点击 Filters 按钮。

   “**筛选器**”窗格随即显示。

2. 点击以下框中的“>”：
   - IP 地址
   - 用户
   - 操作

3. 点击“**验证**”。

   Tenable Identity Exposure 显示您定义的筛选器的活动日志。

若要清除筛选器：

- 在“**筛选器**”窗格底部，点击“**清除筛选器**”。

  Tenable Identity Exposure 显示未筛选的活动日志。

若要导出活动日志：

- 在“活动日志”窗格顶部，点击 图标。

  Tenable Identity Exposure 将 CSV 格式的活动日志下载到您的计算机。

Tenable Identity Exposure 管理员指南

上次更新日期：2024 四月 30

管理员指南提供了有关 Tenable Identity Exposure(原名 Tenable.ad) 的管理任务的信息。

Tenable 建议您在 Tenable Identity Exposure 中以管理员身份完成以下操作以开始使用：

- 准备和安装
- 配置配置文件和用户
- 检测和监控

提示：有关 Tenable Identity Exposure 的更多信息，请查看以下客户教育材料：

- Tenable Identity Exposure 自助指南
- Tenable Identity Exposure 简介 (Tenable University)

准备和安装

准备并完成 Tenable Identity Exposure 安装：

- 按照 *Tenable Identity Exposure 安装指南*中的说明安装 Tenable Identity Exposure。
- 连接并登录 Tenable Identity Exposure。

配置配置文件和用户

接下来，我们建议与以下内容交互以配置和浏览 Tenable Identity Exposure 界面：

- 设置配置文件首选项：配置默认语言、更改密码以及为配置文件设置其他首选项
- 创建用户并将其添加到 Tenable Identity Exposure 实例。
- 配置基于角色的访问控制 (RBAC) 来保护对其数据的访问权限以及您组织内的功能。

检测和监控

根据业务需求对 Tenable Identity Exposure 进行配置和调整后，即可开始使用数据：

- 部署攻击指标模块。
- 使用 Tenable Identity Exposure 门户管理和接收有关受监控基础设施安全状态的信息。
- 通过为 Tenable Identity Exposure 选择要在特定域上监控的攻击类型来定义攻击场景。

注意：Tenable Identity Exposure 可单独购买，也可随 Tenable One 程序包一起购买。有关更多信息，请参阅Tenable One。

Tenable One 风险暴露管理平台

Tenable One 是一款风险暴露管理平台，可帮助组织洞察现代攻击面，集中精力防范可能的攻击，并准确传达网络安全风险，以支持组织达到最佳业务绩效。

该平台结合了涵盖 IT 资产、云资源、容器、Web 应用程序和身份系统的最广泛的漏洞覆盖范围，以 Tenable Research 的速度和广泛的漏洞覆盖范围为基础，并增加了全面的分析，以对操作进行优先级分析和传达网络安全风险。Tenable One 可让组织：

- 获得对现代攻击面的全面可见性
- 预测威胁并对操作进行优先级分析以防止攻击
- 传达网络安全风险以做出更好的决策

Tenable Identity Exposure 是一款单独的产品，但也可以随 Tenable One 风险暴露管理平台一起购买。

> **提示：**有关 Tenable One 产品的更多入门信息，请查看《enable One 部署指南》。

有关更多信息，请参阅以下内容：

Active Directory 配置

Tenable Identity Exposure 需要在受监控的 Active Directory 上进行某些配置，才能允许某些功能运行：

- 访问 AD 对象或容器
- 特权分析的访问权限
- 攻击指标部署

访问 AD 对象或容器

注意:此部分仅适用于风险暴露指标模块的 Tenable Identity Exposure 许可证。

Tenable Identity Exposure 不需要管理权限即可实现安全监控。

此方法依赖于 Tenable Identity Exposure 读取域中存储的所有 Active Directory 对象(包括用户帐户、组织单位、组等)时所用用户帐户的能力。

默认情况下,大多数对象对 Tenable Identity Exposure 服务帐户使用的组 Domain Users 具有读取访问权限。但是,您必须手动配置某些容器以允许 Tenable Identity Exposure 用户帐户进行读取访问。

下表详细说明了需要手动配置以便在 Tenable Identity Exposure 监控的每个域上进行读取访问的 Active Directory 对象和容器。

容器的位置	描述
`CN=Deleted Objects,DC=<DOMAIN> ,DC=<TLD>`	托管已删除对象的容器。
`CN=Password Settings Container,CN=System, DC=<DOMAIN> ,DC=<TLD>`	(可选)托管密码设置对象的容器。

若要授予对 AD 对象或容器的访问权限:

- 在域控制器的命令行界面中,运行以下命令以授予对 Active Directory 对象或容器的访问权限:

  注意:您必须在 Tenable Identity Exposure 监控的每个域上运行此命令。

  ```
  dsacls "<__CONTAINER__>" /takeownership
  dsacls "<__CONTAINER__>" /g <__SERVICE_ACCOUNT__>:LCRP /I:T
  ```

  其中:

  - `<__CONTAINER__>` 指的是需要访问权限的容器。
  - `<__SERVICE_ACCOUNT__>` 指的是 Tenable Identity Exposure 使用的服务帐户。

特权分析的访问权限

可选的特权分析功能需要管理权限。您必须为 Tenable Identity Exposure 使用的服务帐户分配权限。

有关更多信息，请参阅“特权分析”。

注意：您必须在每个启用了特权分析的域上分配权限。

若要使用以下命令行分配权限：

要求：若要分配权限，您需要具有域管理员权限或同等权限的帐户。

- 在域控制器的命令行界面中，运行以下命令以添加两项权限：

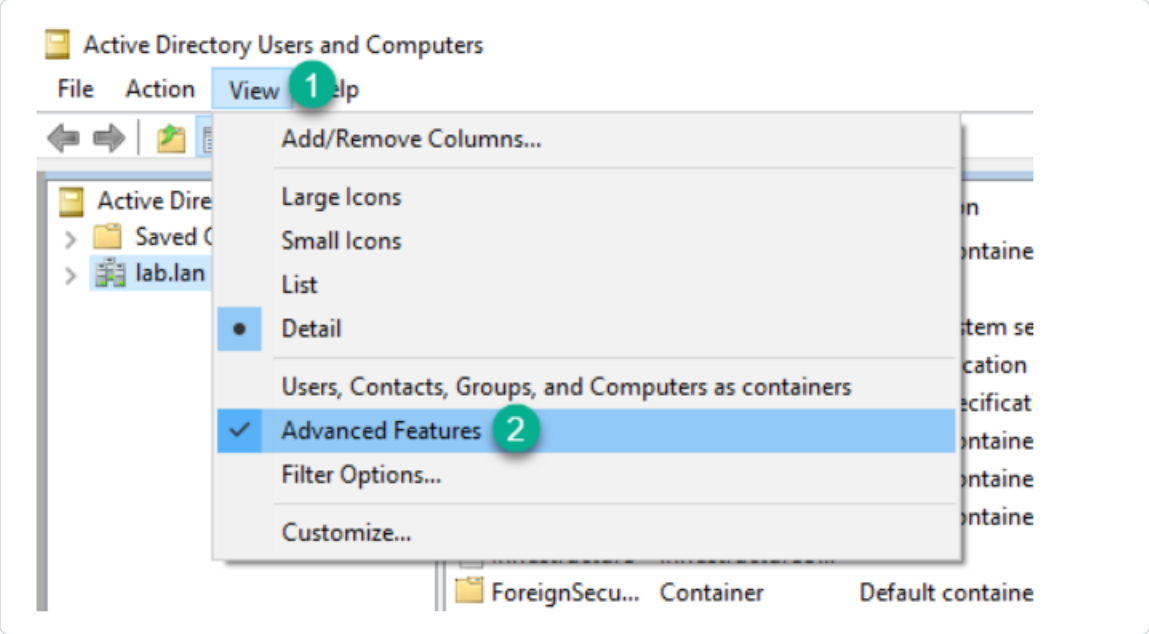
```
dsacls "<__DOMAIN_ROOT__>"  /g "<__SERVICE_ACCOUNT__>:CA;Replicating Directory Changes" "<__
SERVICE_ACCOUNT__>:CA;Replicating Directory Changes All"
```

  其中：

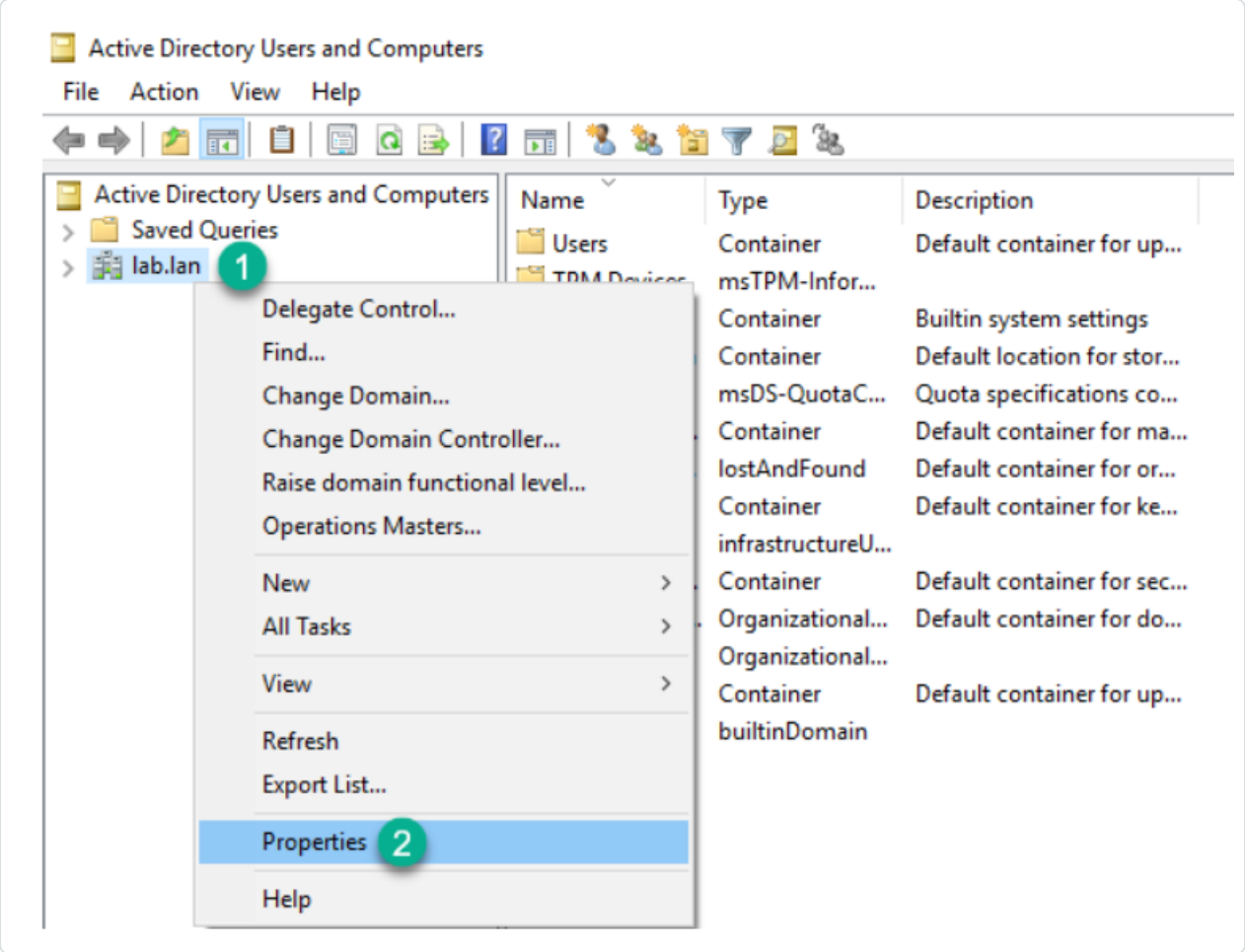
  - `<__DOMAIN_ROOT__>` 指的是域根的标识名。示例：“DC=<DOMAIN>,DC=<TLD>”
  - `<__SERVICE_ACCOUNT__>` 指的是 Tenable Identity Exposure 使用的服务帐户。示例：“DOMAIN\tenablead”。

若要使用图形用户界面分配权限：

1. 从 Windows 的“**开始**”菜单中，打开“**Active Directory 用户和计算机**”。
2. 从“**视图**”菜单中，选择“**高级功能**”。

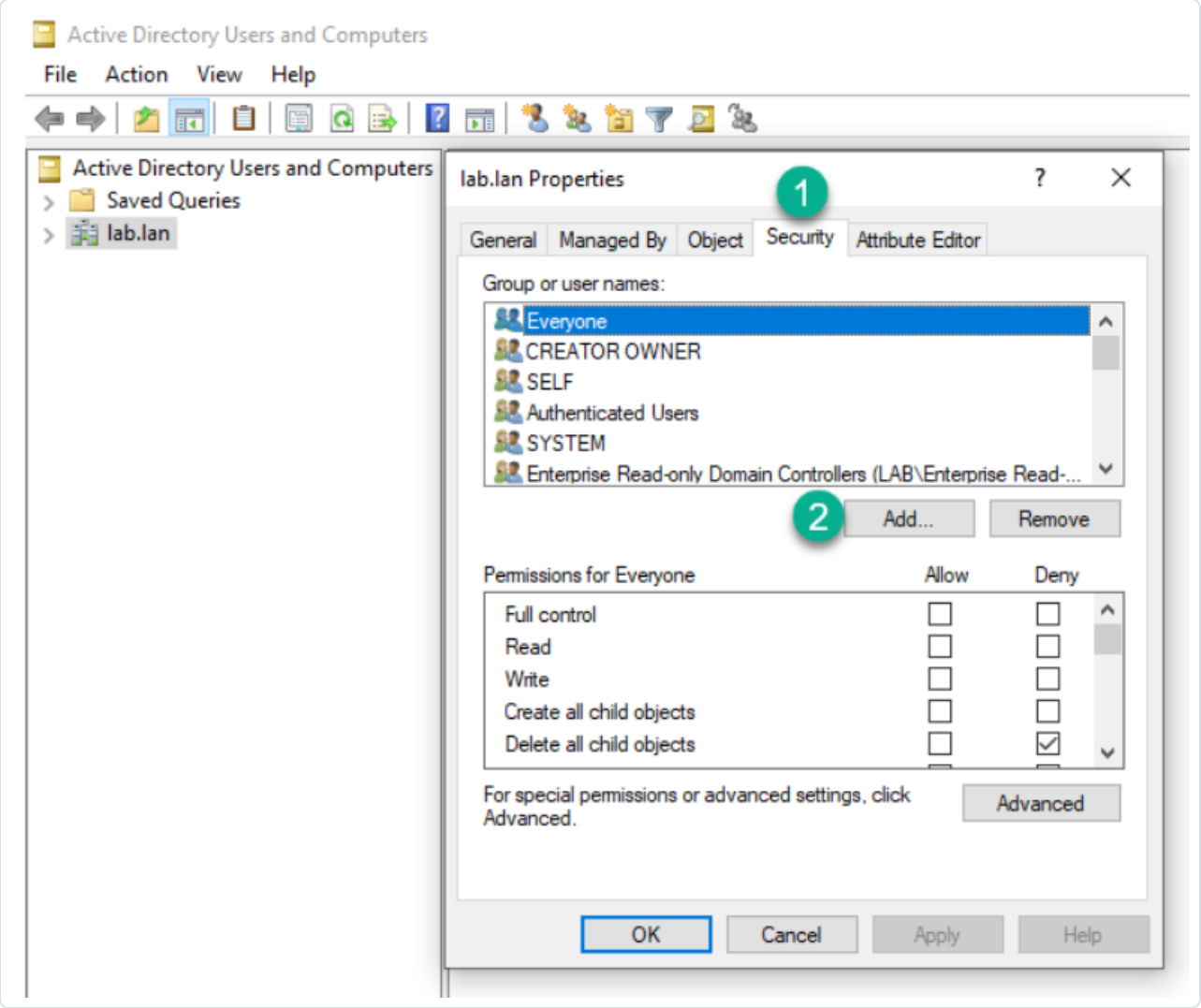


3. 右键点击域根，并选择“**属性**”。



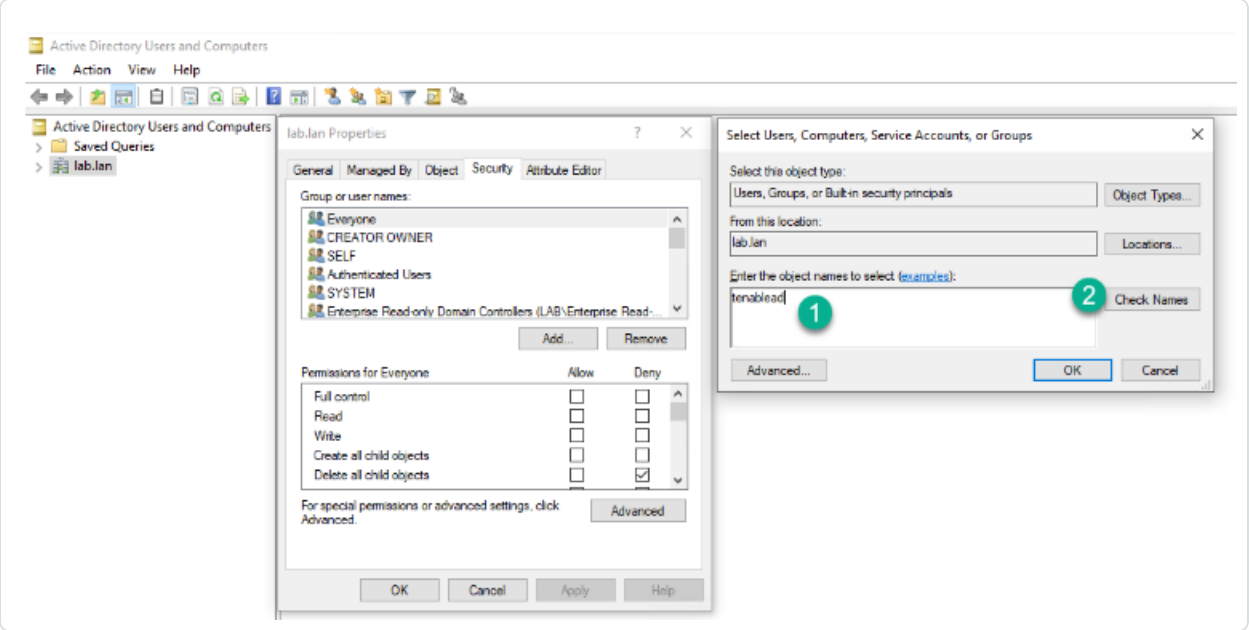
域根的属性窗格随即打开。

4. 点击“**安全**”选项卡，然后单击“**添加**”。



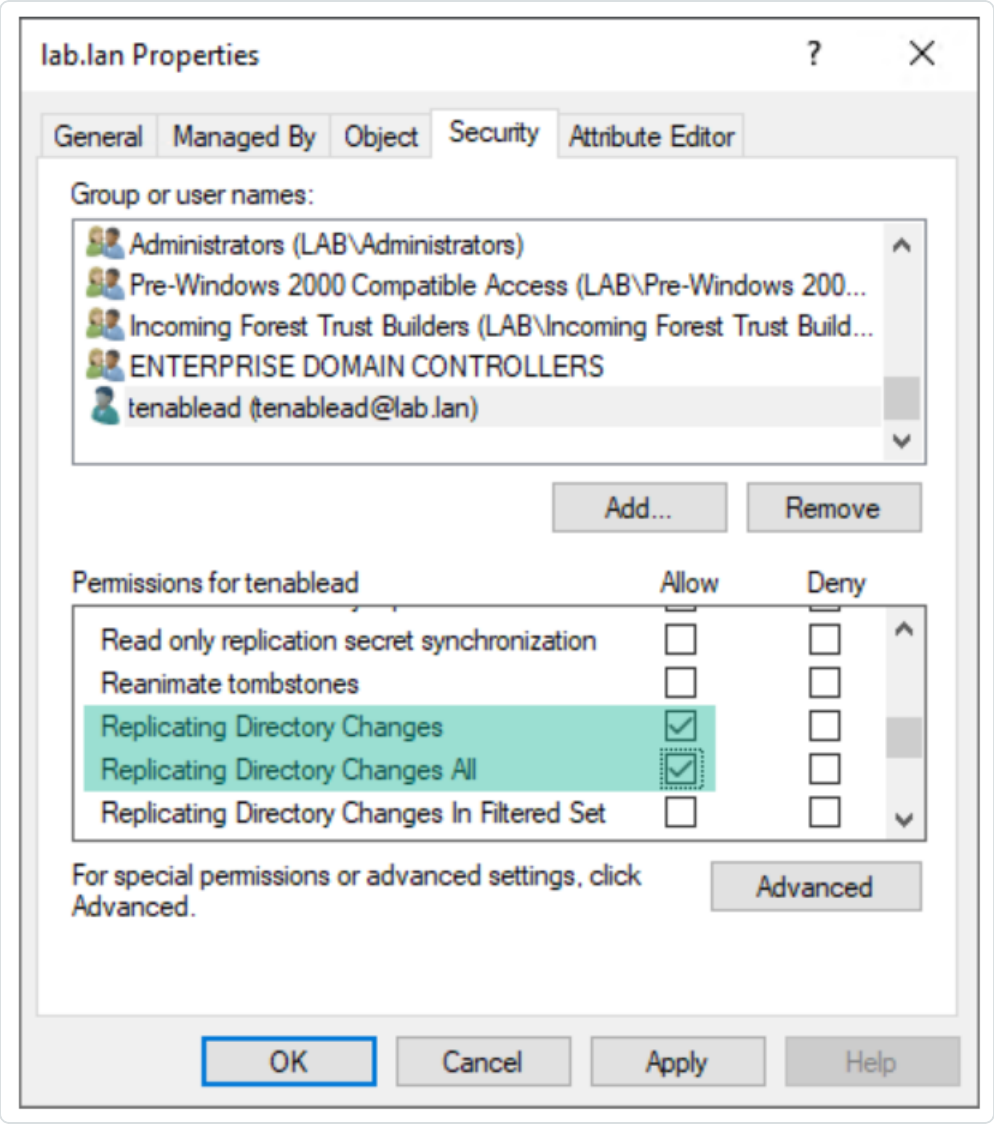
5. 找到 Tenable Identity Exposure 服务帐户：

> **注意**：在具有多个域环境的林中，服务帐户可能位于不同的 Active Directory 域中。



6. 向下滚动列表，并取消选择默认设置的所有权限。

7. 在“**允许**”列中，同时为“*复制目录更改*”和“*复制目录更改所有项*”选择权限。



8. 点击“**确定**”。

重要说明

Tenable Identity Exposure 中每个林仅需要一个服务帐户，因此当您在域中分配权限时，可能需要**从另一个域搜索该服务帐户**。

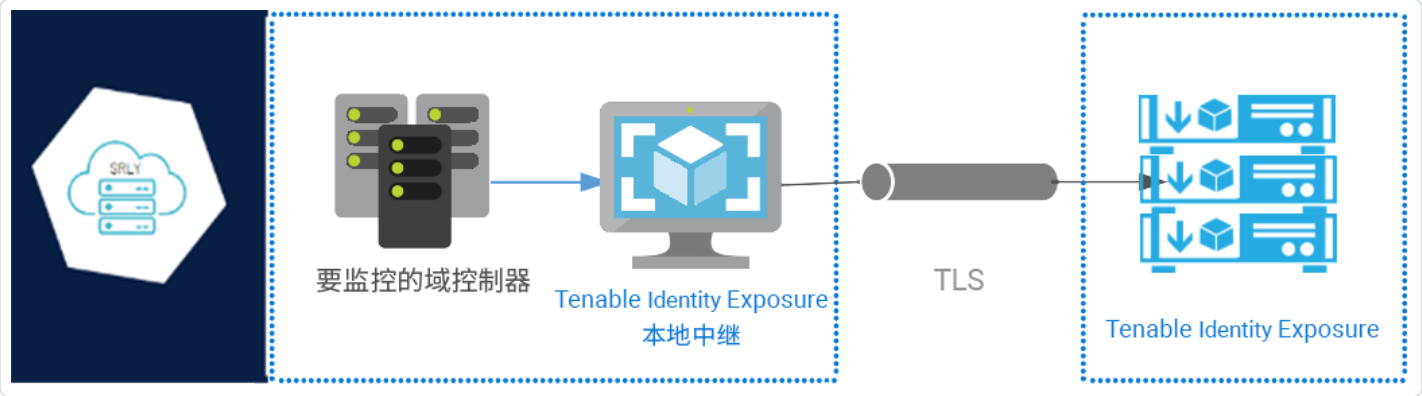
您必须**在域根级别**分配其他权限。Active Directory 不支持分配给某个组织单位或特定用户的权限（例如将特权分析限制为 OU 或用户），因此不会产生任何影响。

这些权限授予 Tenable Identity Exposure 服务帐户更多的 Active Directory 域权限。然后，您必须将其视为**特权帐户（第 0 层）**并像保护域管理员帐户一样加以保护。有关完整程序，请参阅“保护服务帐户”。

安全中继

安全中继是一种使用传输层安全 (TLS) 代替 VPN 将 Active Directory 数据从网络传输到 Tenable Identity Exposure 的新模式(如该图表中所示) 。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。

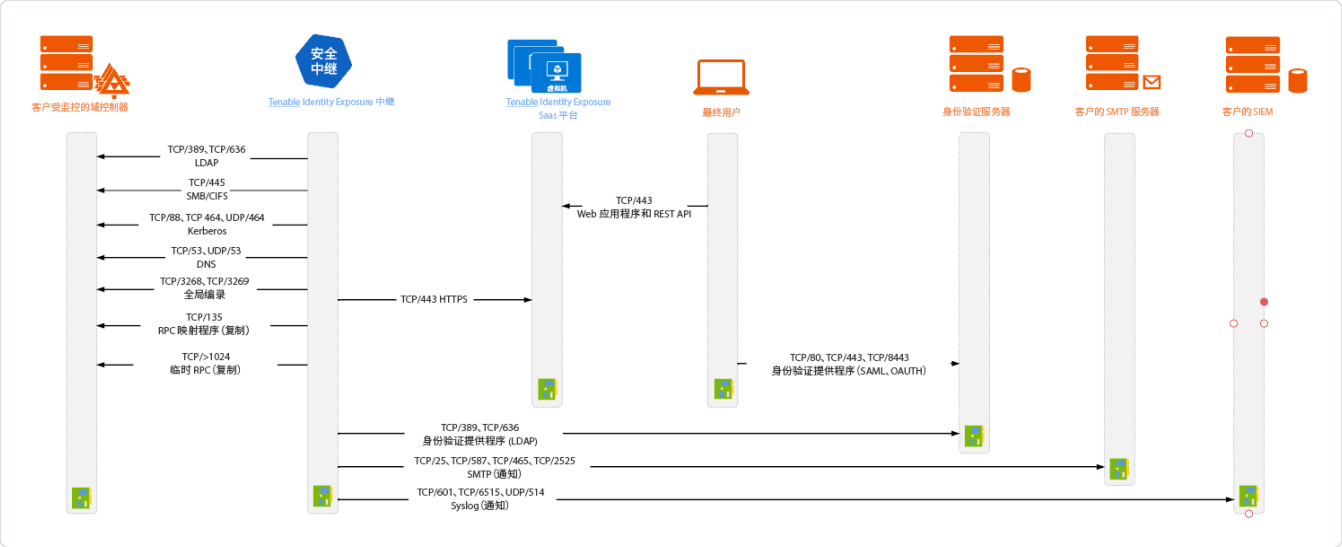


注意: 安全中继功能目前仅在 Tenable Identity Exposure 对平台进行安全中继使用配置后才适用。您无法手动将配置从 VPN 切换到安全中继。如需有关将平台从 VPN 迁移到安全中继的帮助, 请联系 Tenable Identity Exposure 客户支持代表。

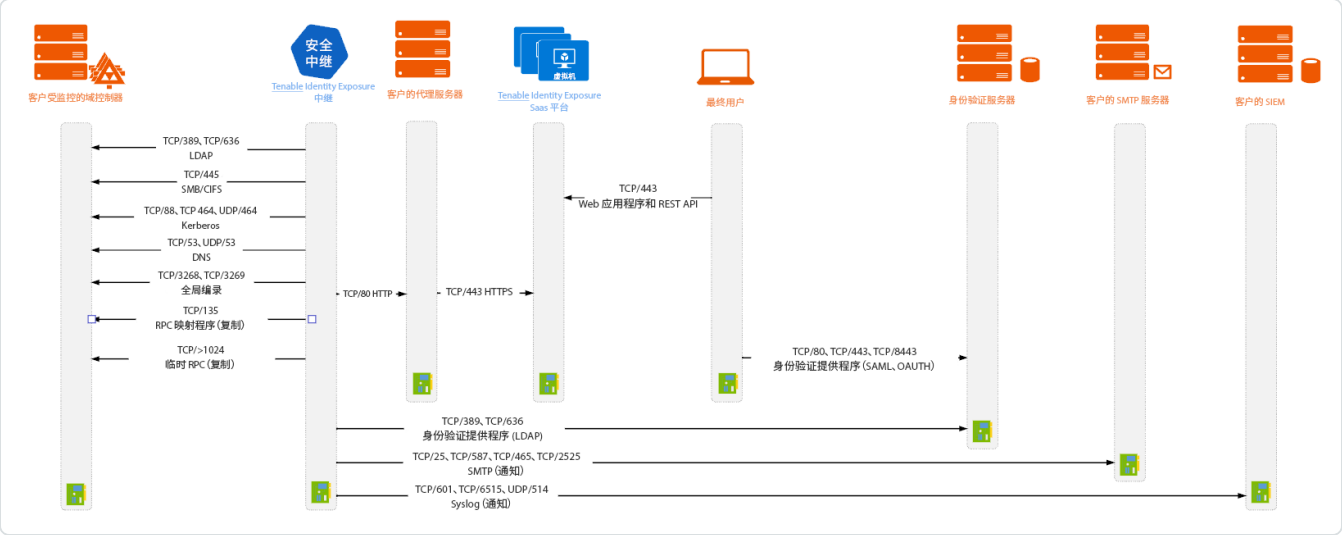
网络流

安全中继所需的端口

- 对于**没有代理服务器**的经典设置，中继需要以下端口：



- 对于**使用代理服务器**的设置，中继需要以下端口：



TLS 要求

截至 2024 年 1 月 24 日，若要使用 TLS 1.2，中继服务器必须至少支持以下一种加密套件：

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256

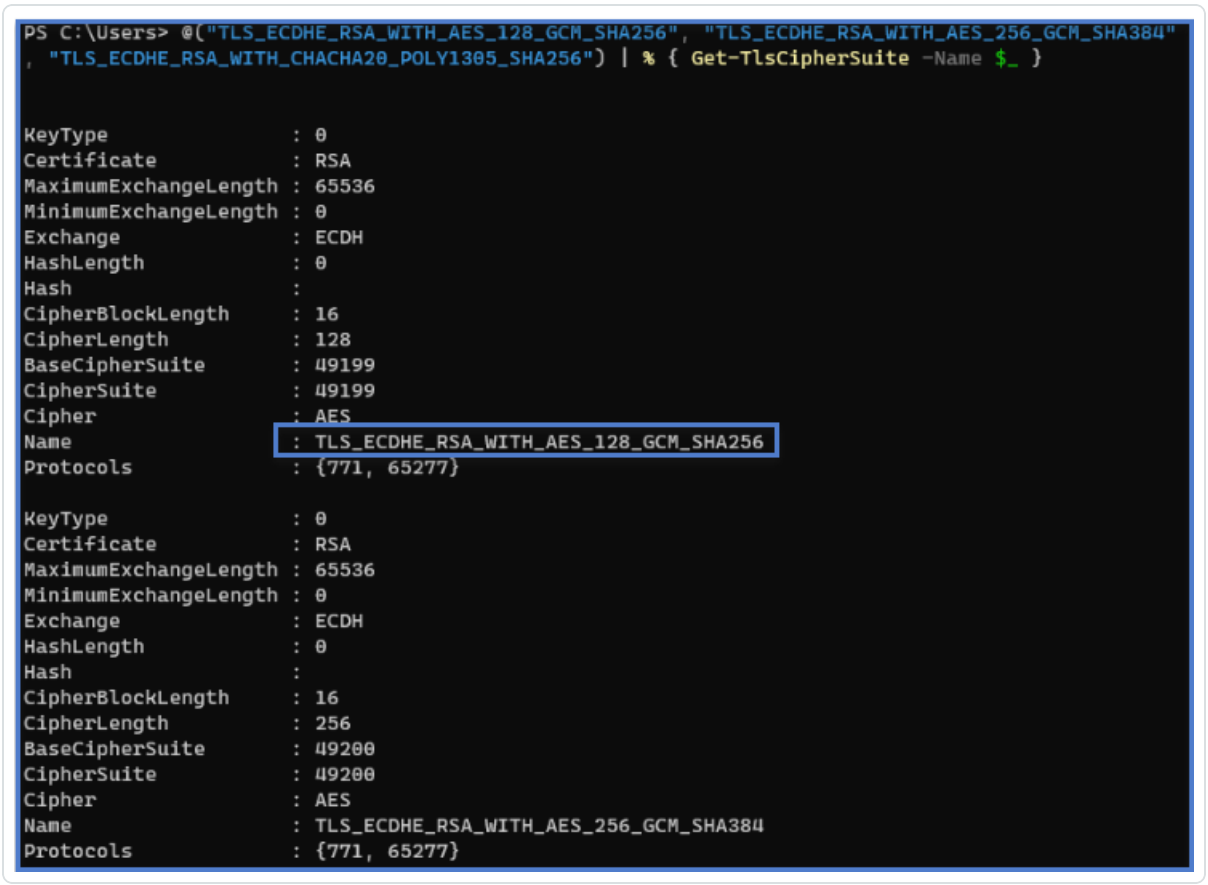
此外，请确保您的 Windows 配置与指定的加密套件一致，以与中继功能兼容。

若要检查加密套件，请执行以下操作：

1. 在 PowerShell 中运行以下命令：

```
@("TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256", "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384", "TLS_ECDHE_
RSA_WITH_CHACHA20_POLY1305_SHA256") | % { Get-TlsCipherSuite -Name $_ }
```

2. 检查输出：TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256。



3. 若输出为空，则表示未为中继的 TLS 连接启用任何必要的加密套件。启用至少一个加密套件。
4. 验证中继服务器中的椭圆曲线加密 (ECC) 曲线。若要使用椭圆曲线临时 Diffie-Hellman（Elliptic Curve Diffie-Hellman Ephemeral，简称 ECDHE）加密套件，则必须进行此验证。在 PowerShell 中运行以下命令：

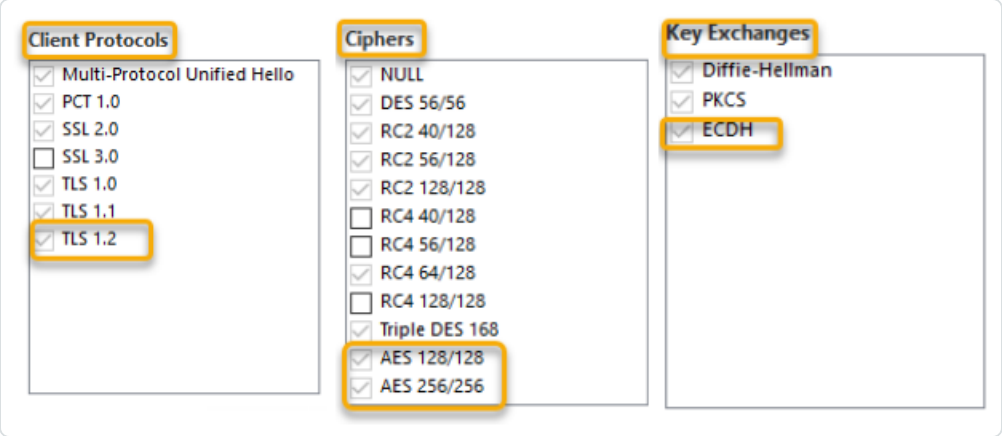
```
Get-TlsEccCurve
```

5. 检查您是否有曲线 **25519**。如果没有，请启用。

```
PS C:\Users> Get-TlsEccCurve
curve25519
NistP256
NistP384
```

若要验证 Windows 加密设置，请执行以下操作：

1. 在 IIS Crypto 工具中，检查您是否启用了以下选项：
   - 客户端协议：**TLS 1.2**
   - 加密：**AES 128/128** 和 **AES 256/256**
   - 密钥交换：**ECDH**



2. 修改加密设置后，请重新启动计算机。

注意：修改 Windows 加密设置会影响计算机上运行的所有应用程序，并使用 Windows TLS 库（即“Schannel”）。因此，请确保您进行的任何调整不会造成意外的副作用。验证所选配置是否符合组织的总体强化目标或合规性要求。

事先说明

先决条件

虚拟机

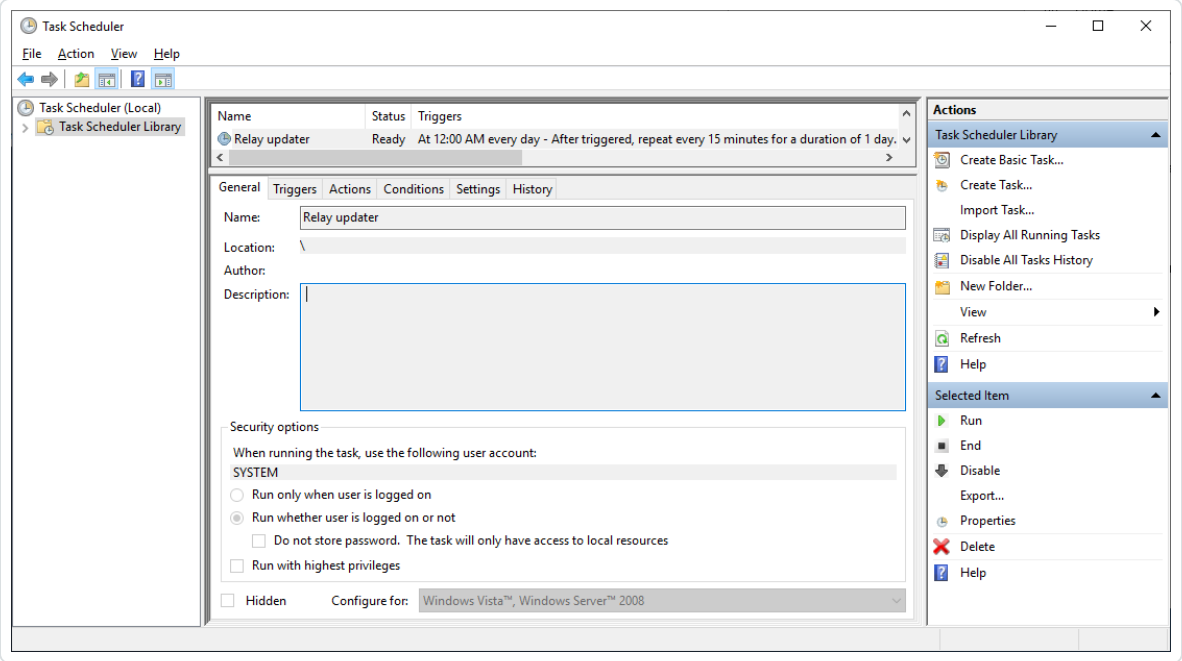
托管安全中继的虚拟机 (VM) 须符合如下要求：

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

VM 还必须具有：

- Windows Server 2016+ 操作系统（无 Linux）
- 解决了至少适用于 `cloud.tenable.com` 和 `*.tenable.ad` (TLS 1.2) 的互联网 DNS 查询和互联网访问。
- 本地管理员特权
- EDR、杀毒软件和 GPO 配置：
  - VM 上剩余足够的 CPU - 例如，Windows Defender Real-Time 功能会消耗大量 CPU 并可使计算机饱和。
  - 自动更新：
    - 允许调用 `*.tenable.ad`，以便自动更新功能可以下载中继可执行文件。
    - 检查确认没有组策略对象 (GPO) 阻止自动更新功能。

- 不删除或变更“中继更新程序”计划任务：



角色权限

用户必须具有可配置中继的基于角色的权限。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“设置角色的权限”。

允许的文件和进程

为使中继顺利运行，允许第三方安全工具（例如防病毒工具和/或 EDR（端点检测和响应）与 XDR（扩展检测和响应））的特定文件和进程。

允许以下文件和进程：

注意：将 C:\ 路径调整为指向中继安装驱动器。

Windows
文件
C:\Tenable*
C:\tools*
C:\ProgramData\Tenable*
进程
nssm.exe --> 路径：C:\tools\nssm.exe
Tenable.Relay.exe --> 路径：C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
envoy.exe --> 路径：C:\Tenable\Tenable.ad\SecureRelay\Tenable.Relay.exe
updater.exe --> 路径：C:\Tenable\Tenable.ad\updater.exe
powershell.exe --> 路径：C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe（可能因 OS 版本而不同）
计划的任务
C:\Windows\System32\Tasks\Relay updater
C:\Windows\System32\Tasks\Manual Renew Apikey
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\CompressLogsSecureRelay
C:\Windows\System32\Tasks\Tenable\Tenable.ad\SecureRelay\RemoveLogsSecureRelay
注册表项

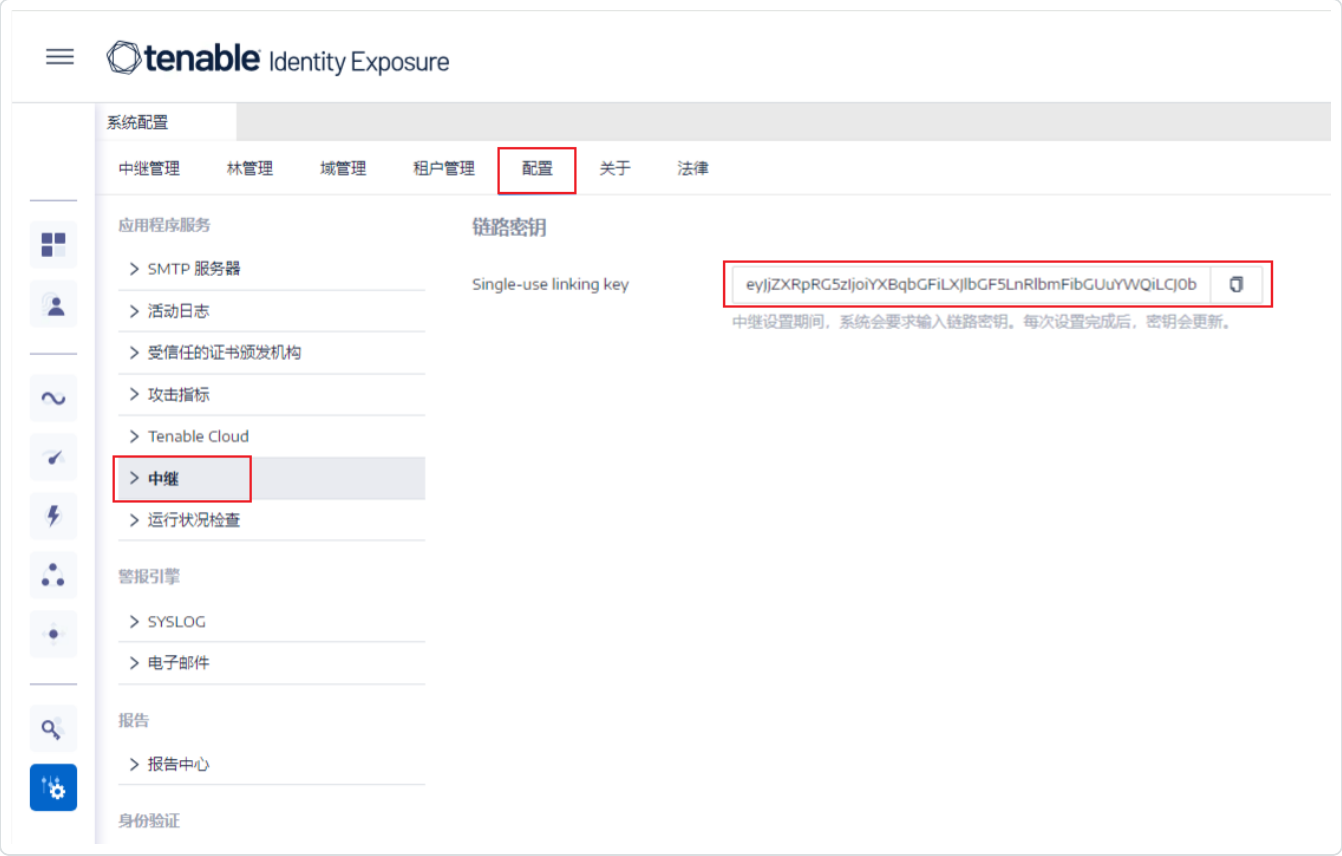
```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Tenable\Tenable.ad Secure Relay
```

链接密钥

安装安全中继时需要使用包含网络地址和身份验证标记的一次性链接密钥。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 中，点击左侧菜单栏上的“**系统**”，然后选择“**配置**”选项卡 >“**中继**”。



2. 单击 以复制链接密钥。

安装

若要安装安全中继，请执行以下操作：

- 选择安装方法：
  - 安装安全中继 (GUI)
  - 安装安全中继 (Tenable Nessus Agent)

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。

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。

另请参阅：

有关安全中继的完整信息，请参阅《Tenable Identity Exposure 管理员指南》中的“安全中继”一节。

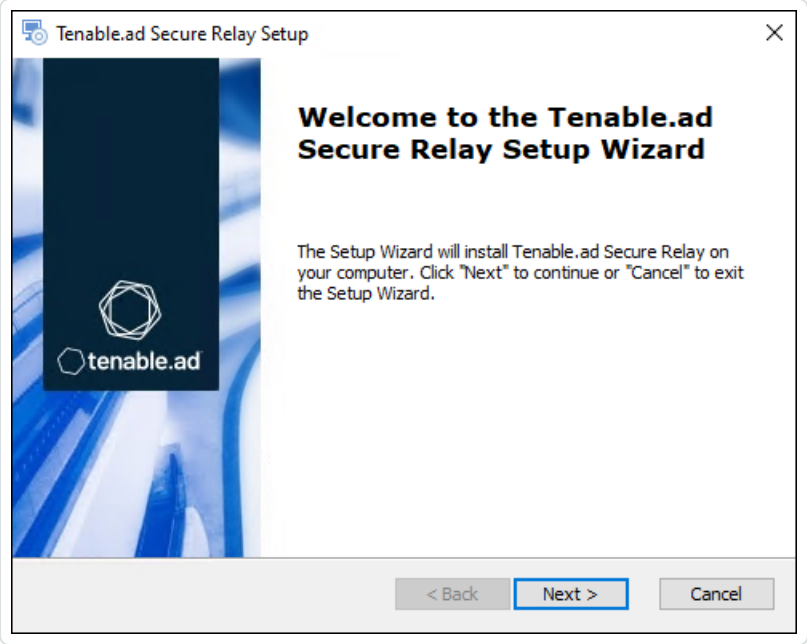
安装安全中继 (GUI)

以下过程使用 Windows 安装程序安装安全中继。开始安装之前，请检查您是否具备 安全中继 中所述的必要先决条件和**必需的链路密钥**

若要安装安全中继，请执行以下操作：

1. 将安装程序从 Tenable Identity Exposure 下载门户 下载到虚拟机。
2. 双击文件 `tenable.ad_SecureRelay_v3.xx.x` 以启动安装向导。

   出现“**欢迎**”屏幕。



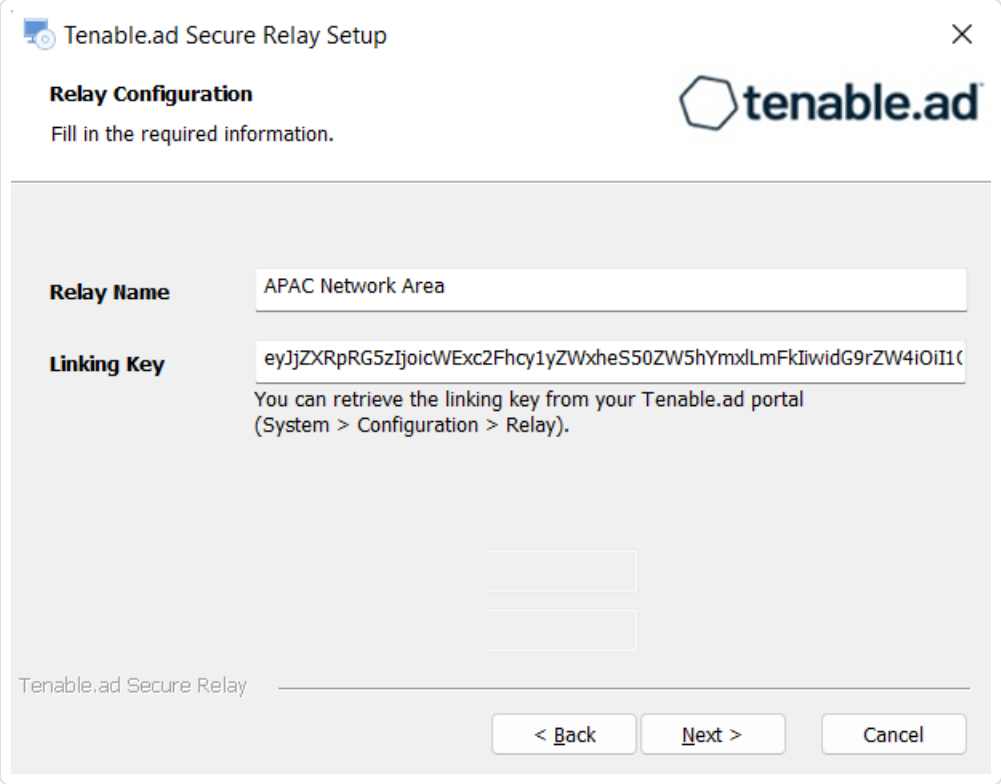
3. 单击“**下一步**”。

   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：

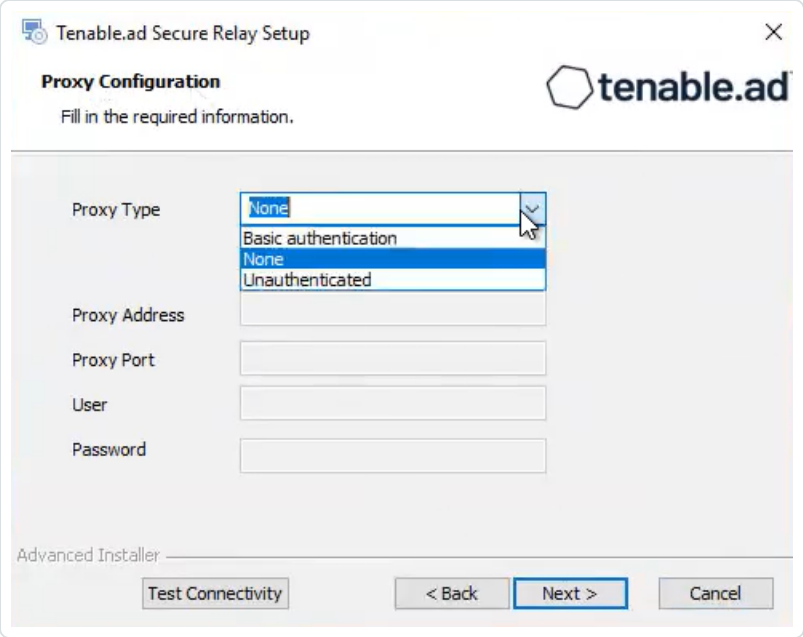
   a. 在“**中继名称**”框中，输入安全中继的名称。

   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. 单击“**下一步**”。

   此时会出现“中继配置”窗口：



8. 请选择以下选项之一：

   a. **没有**：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，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`）。

9. 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。

10. 单击“**下一步**”。

    出现“**准备安装**”窗口。

11. 单击“**安装**”。

12. 安装完成后，单击“**完成**”。

后续操作

- 安装后检查

另请参阅：

- 安全中继
- 安装安全中继 (Tenable Nessus Agent)
- 安装后检查
- 配置中继

安装安全中继 (Tenable Nessus Agent)

以下过程使用 Tenable Nessus Agent 安装安全中继。

事先说明

- 检查是否已下载并安装 Tenable Nessus Agent。

  注意：Tenable Nessus Agent 安装程序要求提供代理密钥。安全中继功能**不需要**此密钥。

- 满足必要的先决条件并具有安全中继中所列出的**必要链接密钥**。

若要安装安全中继，请执行以下操作：

1. 在托管 Tenable Nessus Agent 并充当中继的计算机上，在 Tenable Nessus Agent 目录 (`c:\Program Files\Tenable\Nessus Agent`) 中打开管理员命令提示窗口并输入以下命令：

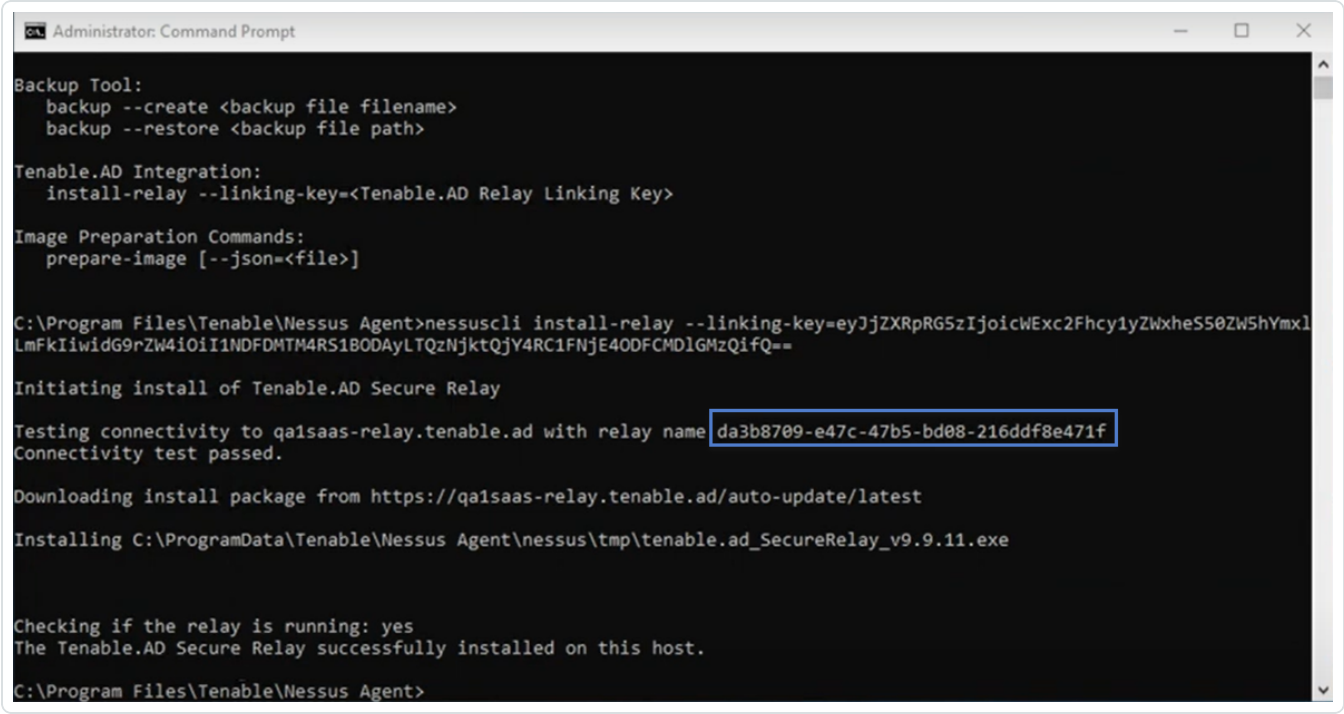
   安全中继安装

   ```
   nessuscli install-relay --linking-key=<Relay Linking Key> --proxy-host=<Customer Proxy IP or DNS> --proxy-port=<Customer Proxy Port>
   ```

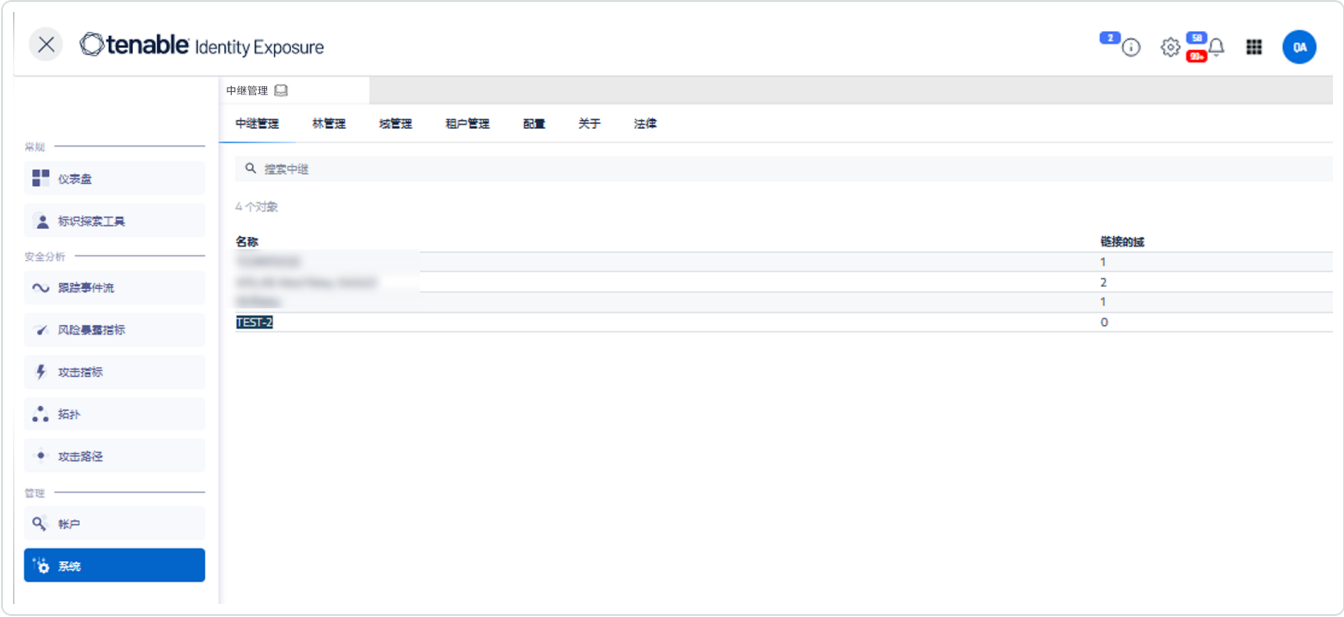
2. 将 <Tenable Identity Exposure 中继链接密钥> 替换为之前从 Tenable Identity Exposure 实例复制的值，并且如果您使用代理服务器，请提供代理地址和端口号。

   随即开始安装。运行连接检查和安装过程需要花费几分钟时间。

   安装成功完成后，页面会显示一则消息，表示中继正在主机上运行。



3. 在 Tenable Identity Exposure 中，点击“**系统**”>“**中继管理**”。新安装的中继会出现在中继列表中，其标识符会显示在安装窗口中。



后续操作

- 安装后检查

另请参阅：

- 安全中继
- 安装安全中继 (GUI)
- 安装后检查
- 配置中继

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

该安装还添加了 4 个与安全中继相关并且名称以“ALSID”开头的新环境变量。如果选择使用代理服务器，还会添加另外两个与代理 IP 和端口相关的变量。

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。

后续操作

- 配置中继

另请参阅：

- 安全中继
- 安装安全中继 (GUI)
- 安装安全中继 (Tenable Nessus Agent)

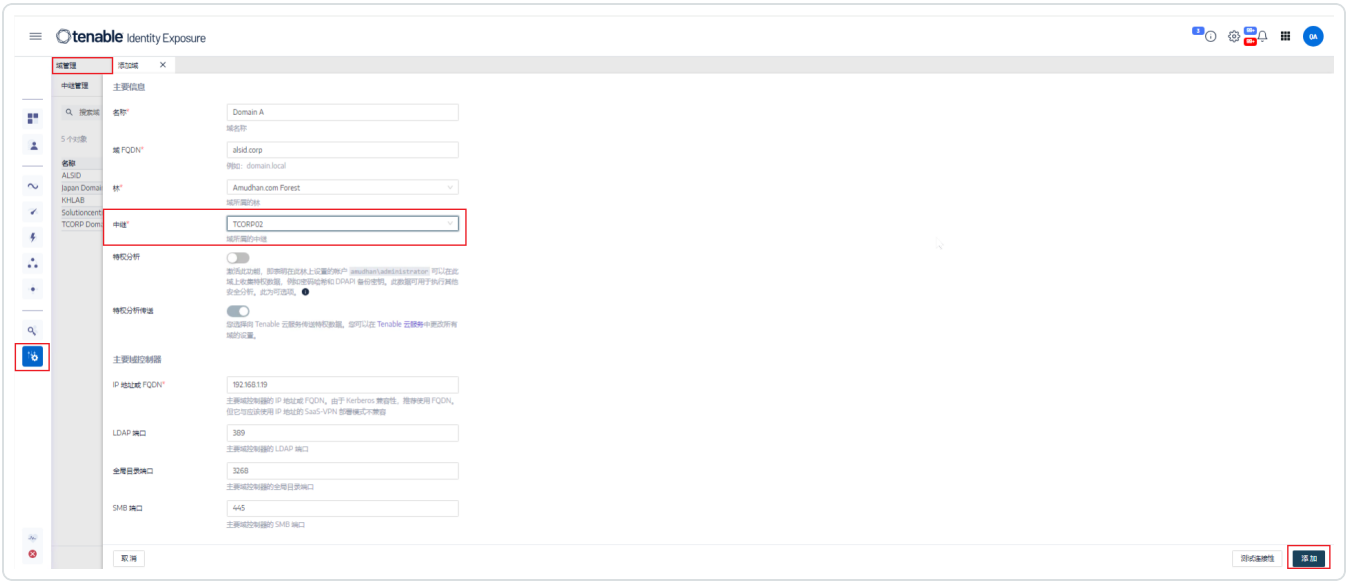
配置中继

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。

将域链接到安全中继：

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。



4. 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。

另请参阅：

- 安全中继
- 安装安全中继 (GUI)
- 安装安全中继 (Tenable Nessus Agent)
- 安装后检查

攻击指标部署

注意:此信息仅适用于可使用攻击指标模块的许可证。

Tenable Identity Exposure 的**攻击指标** (IoA) 功能让您能够检测针对 Active Directory (AD) 的攻击。每个 IoA 都需要安装脚本自动启用的特定审核策略。有关 Tenable Identity Exposure IoA 及其实现的完整列表,请参阅 Tenable 下载门户中的《Tenable Identity Exposure 攻击指标参考指南》。

攻击指标和 Active Directory

Tenable Identity Exposure 作为监控 Active Directory 基础设施的非侵入式解决方案,无需部署代理,且对环境的配置更改最少。

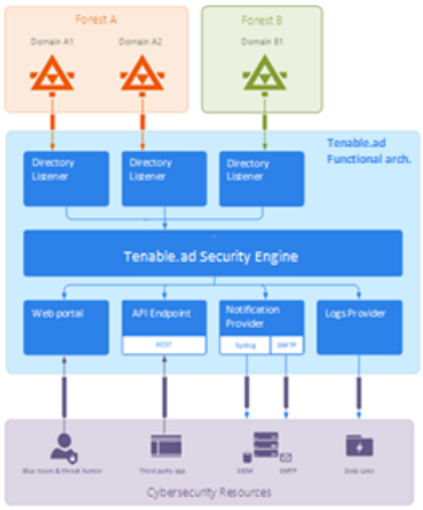
Tenable Identity Exposure 使用没有管理权限的常规用户帐户连接到其安全监控功能的标准 API。

Tenable Identity Exposure 利用 Active Directory 复制机制检索相关信息,这仅在每个域的 PDC 和 Tenable Identity Exposure 的目录侦听器之间产生有限的带宽成本。

为使用攻击指标有效地检测安全事件,Tenable Identity Exposure 使用了 Windows 事件跟踪 (ETW) 信息和每个域控制器上可用的复制机制。若要收集这组信息,请依照 安装攻击指标 中所述,使用 Tenable Identity Exposure 中的脚本部署专用的组策略对象 (GPO)。

此 GPO 会在所有写入系统卷 (SYSVOL) 的域控制器上激活使用 Windows EvtSubscribe API 的事件日志监听器,以便从 AD 复制引擎和 Tenable Identity Exposure 监听 SYSVOL 事件的功能中受益。GPO 在 SYSVOL 中为每个域控制器创建一个文件,并定期刷新其内容。

若要启动安全监控,Tenable Identity Exposure 必须联系 Microsoft 的标准目录 API。



域控制器

Tenable Identity Exposure 仅需要使用网络流矩阵中所述的网络协议与主域控制器仿真器 (PDCe) 通信。

如果存在多个受监控的域或林，则 Tenable Identity Exposure 必须到达每个域的 PDCe。为获得最佳性能，Tenable 建议您在要监控的 PDCe 附近的物理网络上托管 Tenable Identity Exposure。

用户帐户

Tenable Identity Exposure 使用非管理员用户帐户对受监控的基础设施进行身份验证，以访问复制流。

一个普通 Tenable Identity Exposure 用户可以访问收集的所有数据。Tenable Identity Exposure 不访问机密属性，例如凭据、密码哈希或 Kerberos 密钥。

Tenable 建议您创建一个作为"Domain Users"组成员的服务帐户，如下所示：

- 此服务帐户位于主要受监控的域中。
- 此服务帐户位于任何组织单位 (OU) 中，最好是您创建其他安全服务帐户的组织单位。
- 此服务帐户具有标准用户组成员资格（例如 Domain Users AD 默认组的成员）。

开始之前

- 查看安装 IoA 的限制和潜在影响，如 技术变更与潜在影响 中所述。
- 检查 DC 是否已安装 Active Directory 和 GroupPolicy 的 PowerShell 模块并可用。
- 检查 DC 是否启用了分布式文件系统工具功能 RSAT-DFS-Mgmt-Con，以便部署脚本可以检查复制状态，因为它在 DC 复制时无法创建 GPO。
- Tenable Identity Exposure 建议您在非高峰时间安装/升级 IoA，以减少平台中断情况。
- 检查权限 - 要安装 IoA，您必须拥有具有以下权限的用户角色：
  - 在“**数据实体**”中，对以下项目的“读取”权限：
    - 所有攻击指标
    - 所有域
  - 在“**界面实体**”中，对以下内容的访问权限：
    - 管理 > 系统 > 配置
    - 管理 > 系统 > 配置 > 应用程序服务 > 攻击指标
    - 管理 > 系统 > 配置 > 应用程序服务 > 攻击指标 > 下载安装文件

  有关基于角色的权限的更多信息，请参阅 设置角色的权限。

另请参阅：

- 安装攻击指标
- 攻击指标安装脚本
- 技术变更与潜在影响
- 安装 Microsoft Sysmon 是一个 Windows 系统工具，Tenable Identity Exposure 的有些攻击指标需要使用该工具来获取相关系统数据。
- 对攻击指标进行故障排除

安装攻击指标

所需用户角色：Tenable Identity Exposure 中具有修改攻击指标配置权限的组织用户。有关更多信息，请参阅"设置角色的权限"。

Tenable Identity Exposure 的攻击指标 (IoA) 模块要求以能够创建新的组策略对象 (GPO) 并将其链接到组织单位 (OU) 的管理帐户运行 PowerShell 安装脚本。您可以从加入了 Tenable Identity Exposure 监控的 Active Directory 域并可通过网络访问域控制器的任何计算机上运行此脚本。

您只需在每个 AD 域中执行此安装脚本一次：因为自动创建的 GPO 会将事件监听器部署至所有现有和新的域控制器 (DC) 上。

此外，启用"自动更新"选项可以避免必须重新执行安装脚本，即使在更改了 IoA 配置的情况下也是如此。

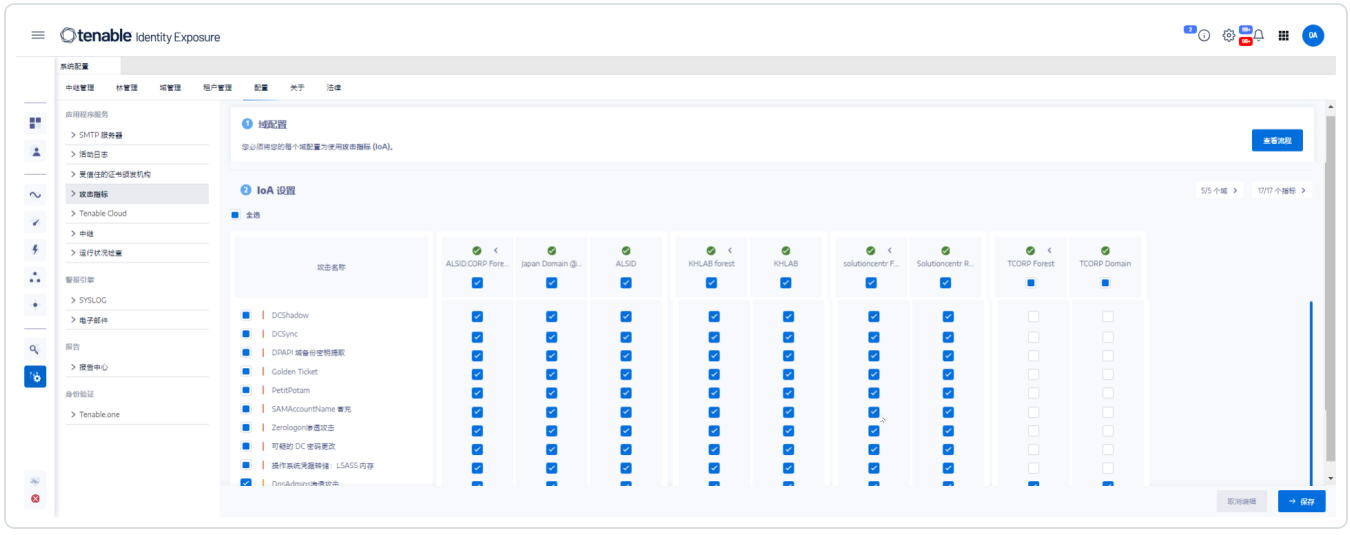
为 IoA 配置域：

1. 在 Tenable Identity Exposure 中，单击左侧菜单栏上的"**系统**"，然后单击"**配置**"选项卡。

   配置窗格随即显示。

2. 点击"**攻击指标**"。

   IoA 配置窗格随即显示。



3. 在 **(1) 域配置**中，单击"**查看流程**"。

   程序窗口随即打开。

4. 在"**未来自动更新?** "下面：
   - 默认选项"**启用**"允许 Tenable Identity Exposure 日后根据您在 Tenable Identity Exposure 中所做修改自动更新 IoA 配置。这也可确保持续的安全分析。
   - 如果您关闭此选项，系统会显示一条消息，要求您将其打开以获取未来的自动更新。单击"**查看程序**"并切换为"**启用**"。
5. 单击"**下载**"以下载要为每个域运行的脚本 (`Register-TenableIOA.ps1`)。
6. 单击"**下载**"以下载域的配置文件 (`TadIoaConfig-AllDomains.json`)。
7. 单击 以复制 Powershell 命令，然后配置域。

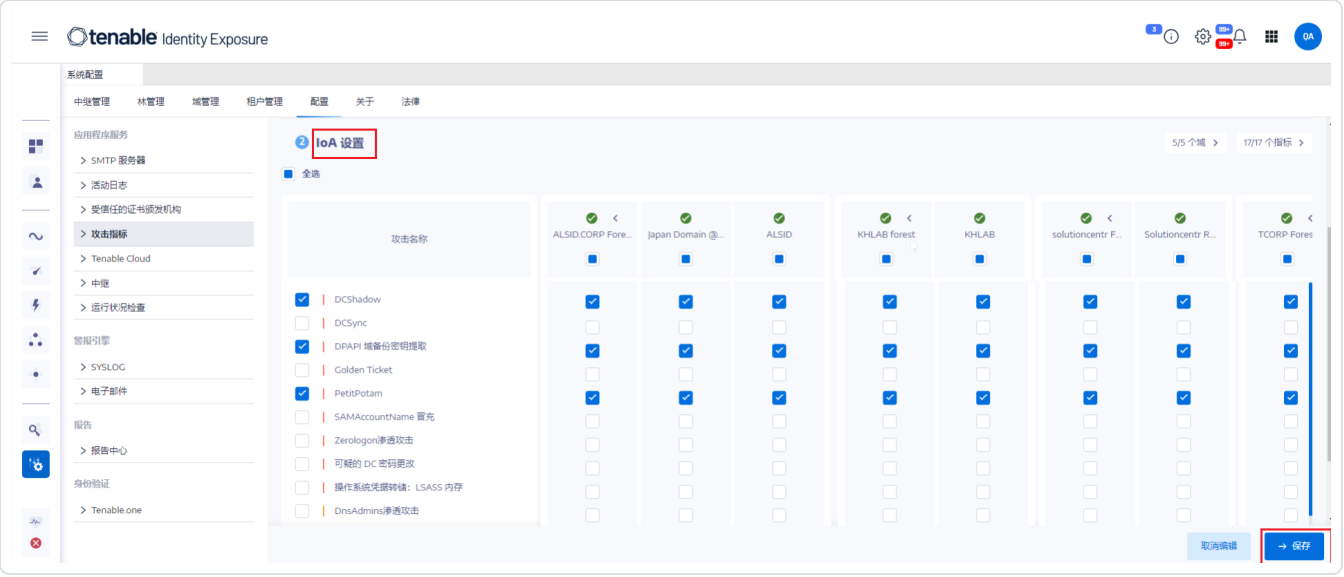
8. 在程序窗口外部单击以将其关闭。

9. 使用管理权限打开 PowerShell 终端并运行命令，以针对 IoA 配置域控制器。

> **注意**：用于安装 IoA 和查询域的服务帐户必须具有 Tenable Identity Exposure（原名 Tenable.ad）中的写入权限。安装脚本会自动添加此权限。如果删除此权限，Tenable Identity Exposure 将显示错误消息，并且自动更新不再有效。有关更多信息，请参阅"攻击指标安装脚本"。

设置 IoA：

1. 在 IoA 配置窗格的"**IoA 设置**"下选择配置中所需的 IoA。



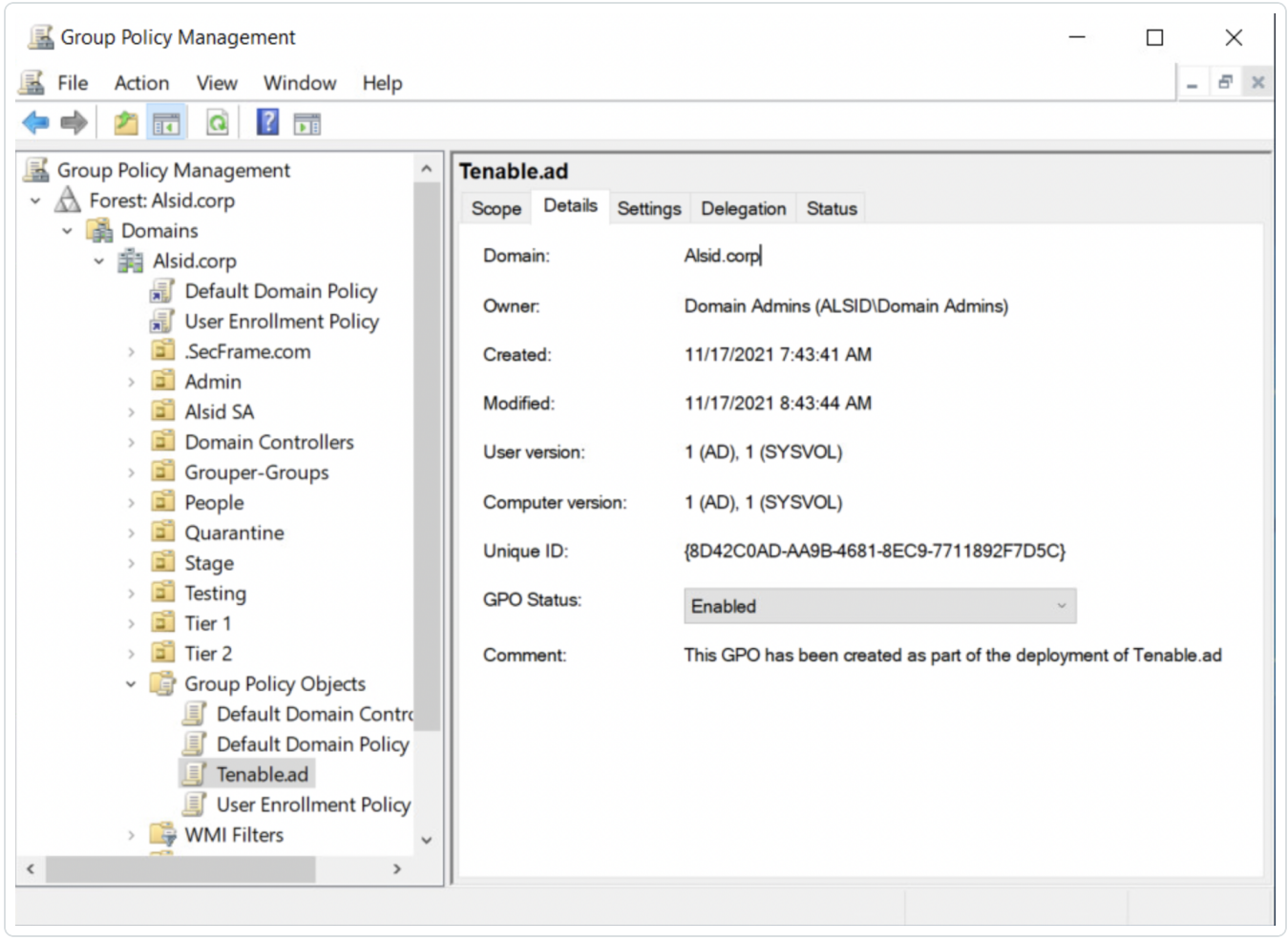
> **提示**：**Zerologon 漏洞利用**攻击指标 (IoA) 可以追溯到 2020 年。如果您的所有域控制器 (DC) 在过去三年内进行了更新，则它们将免受此漏洞的影响。若要确定保护 DC 免受此漏洞影响所需的补丁，请参阅 Microsoft 的"Netlogon 特权提升漏洞"中的信息。确认 DC 安全后，您可以安全地停用此 IoA 以避免引发不必要的警报。

2. 单击"**保存**"。

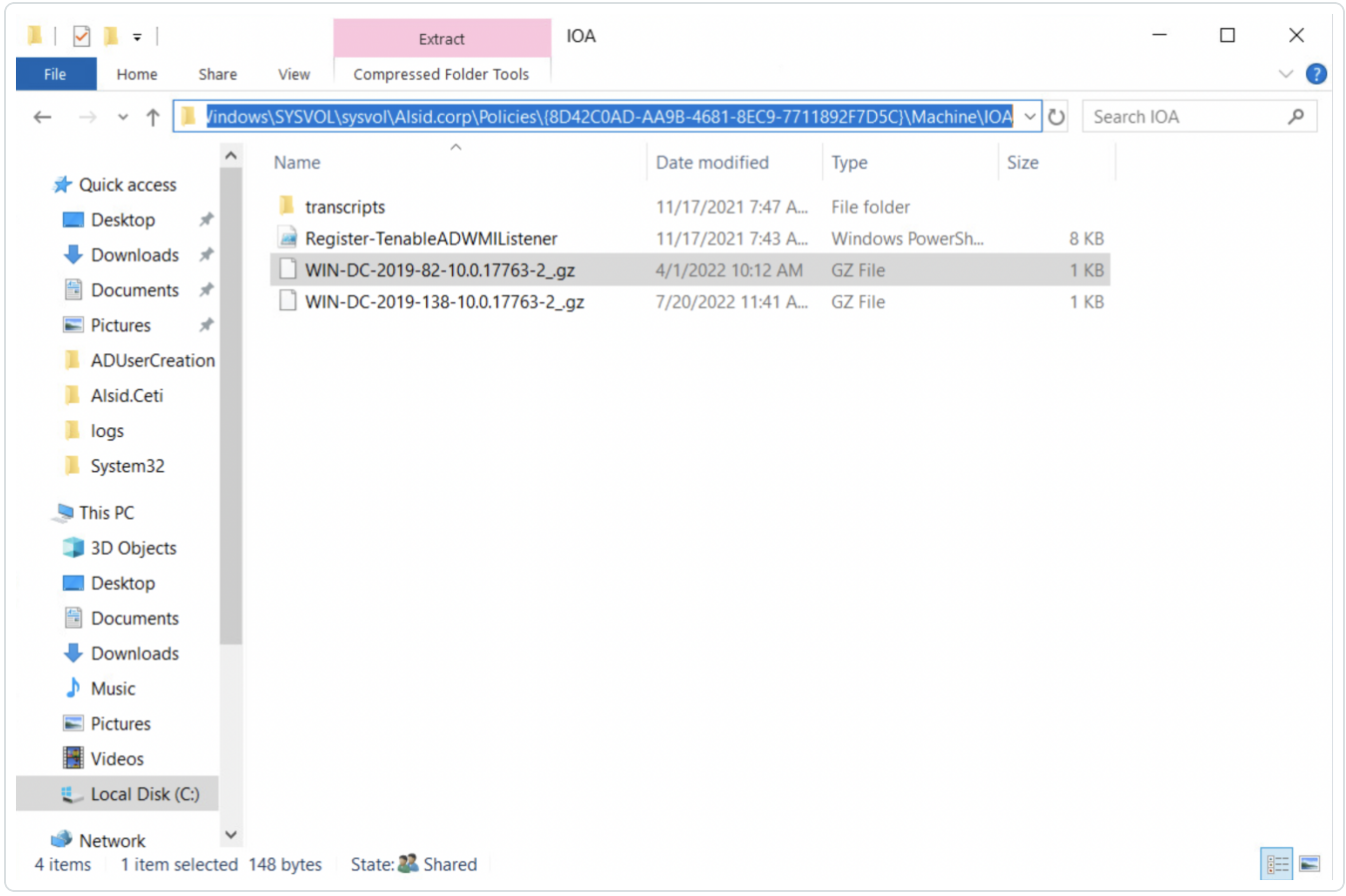
   - 如果启用了"**未来自动更新**"，Tenable Identity Exposure 将保存并自动更新您的新配置。等待几分钟以使此更新生效。
   - 如果未启用"**未来自动更新**"，则会出现一个程序窗口指导您 为 IoA 配置域：

检查 IoA 安装：

1. 在"组策略管理"中，检查新 Tenable Identity Exposure GPO 是否存在以及其是否链接至域控制器 OU：



2. 测试 IoA 之前，请转至 `C:\Windows\SYSVOL\sysvol\alsid.corp\Policies\{GUID}\Machine\IOA` 并检查**所有域控制器**中是否存在 `.gz` 文件：



若要检查 Tenable Identity Exposure 服务帐户的"写入"权限，请执行以下操作：

1. 在文件资源管理器中，转至 `\\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\Machine\`。
2. 右键点击"IOA"文件夹，并选择"**属性**"。
3. 选择"**安全**"选项卡，然后单击"**高级**"。
4. 单击"**有效访问**"选项卡。
5. 单击"**选择用户**"。
6. 输入 `<TENABLE-SERVICE-ACCOUNT-NAME>` 并单击"**确定**"。
7. 点击"**查看有效访问**"。
8. 检查"写入"权限是否已激活。

或者，您可以使用 Powershell 执行操作：

- 运行以下命令：

```
Install-Module -Name NTFSSecurity -RequiredVersion 4.2.3
```

```
Get-NTFSEffectiveAccess -Path \\<DNS-NAME>\sysvol\<DNS-NAME>\Policies\{<GPO-ID>}\IOA\ -
Account <TENABLE-SERVICE-ACCOUNT-NAME>
```

调整 IoA

为避免误报攻击或缺少对合法攻击的检测，您必须根据您的环境来调整 IoA，即通过使其适应 Active Directory 的大小、将已知工具列入白名单等操作来进行调整。

1. 请参阅《Tenable Identity Exposure 攻击指标参考指南》，了解有关要选择的选项和建议值的信息。
2. 在安全配置文件中，如 定制指标 中所述，将选项和值应用于每个 IoA。

故障排除

部署期间可能出现以下错误消息：

消息	修复
“Tenable Identity Exposure 无法写入配置文件，因为目标文件夹<targetFolder>不存在。这表示 IoA 模块部署可能已失败。”	卸载脚本并单击“查看程序”，以获取有关重新安装脚本的说明。
“Tenable Identity Exposure 无法写入位于<targetFile>的配置文件对其进行更新。这可能是由于另一个进程锁定了文件或权限变更。”	• 确保除 IoA 模块外没有其他进程在使用此配置文件。 • 检查服务帐户是否具有修改文件内容的权限。 • 如果您不想向服务帐户授予权限，请禁用“自动更新”切换开关，然后单击“查看程序”以获取有关在修改 IoA 配置时如何执行手动更新的说明。

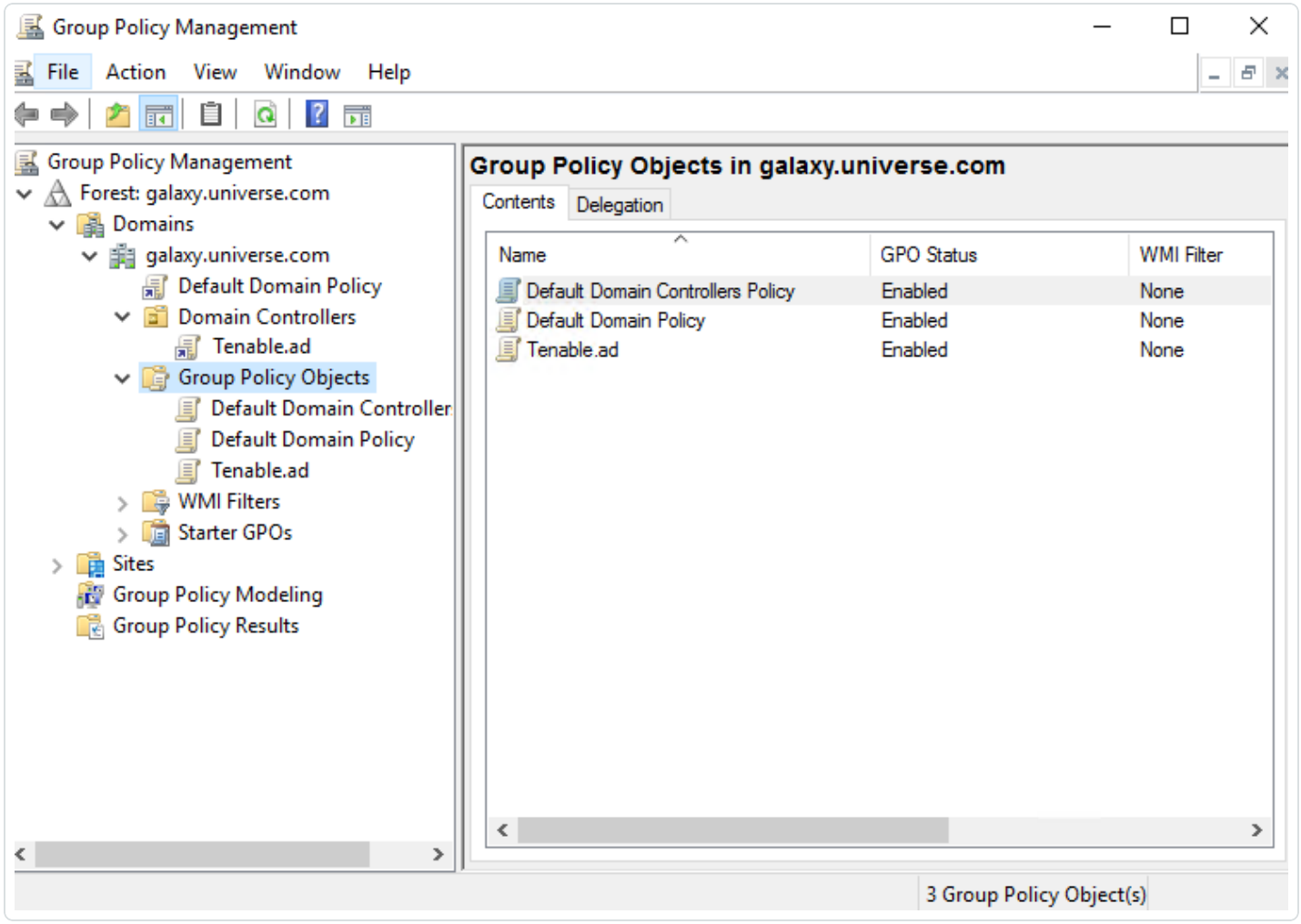
“目标文件夹<targetFolder>包含无法运行自动更新的 Tenable Identity Exposure 版本。”	当前安装的脚本是使用 WMI 的旧版本。卸载当前版本，然后下载新的安装脚本，并运行此脚本。
“配置文件部署遇到意外错误。”	卸载脚本并单击“查看程序”，以获取有关重新安装脚本的说明。如果这不起作用，请联系您的客户支持代表。

有关更多信息，请参阅：

- 攻击指标安装脚本
- 技术变更与潜在影响
- 防病毒检测
- 高级审核策略配置优先级

攻击指标安装脚本

下载并运行攻击指标 (IoA) 安装文件后，IoA 脚本会在 Active Directory (AD) 数据库中创建一个默认命名为 `Tenable.ad` 的新组策略对象 (GPO)。系统仅将 Tenable Identity Exposure GPO 链接到包含所有域控制器 (DC) 的域控制器组织单位 (OU)。新策略会使用 GPO 机制在所有 DC 之间自动复制。



安装脚本 (Tenable Identity Exposure v. 3.29)

GPO 包含所有 DC 在本地执行以收集相关数据的 PowerShell 脚本，如下所示：

- 该脚本使用 Windows EvtSubscribe API 在每个域控制器上配置一个事件日志监听器。该脚本通过提交请求和由 EvtSubscribe 触发的针对每个匹配事件日志的回调，为 `TenableADEventsListenerConfiguration.json` 中指定的每个必要事件日志通道进行

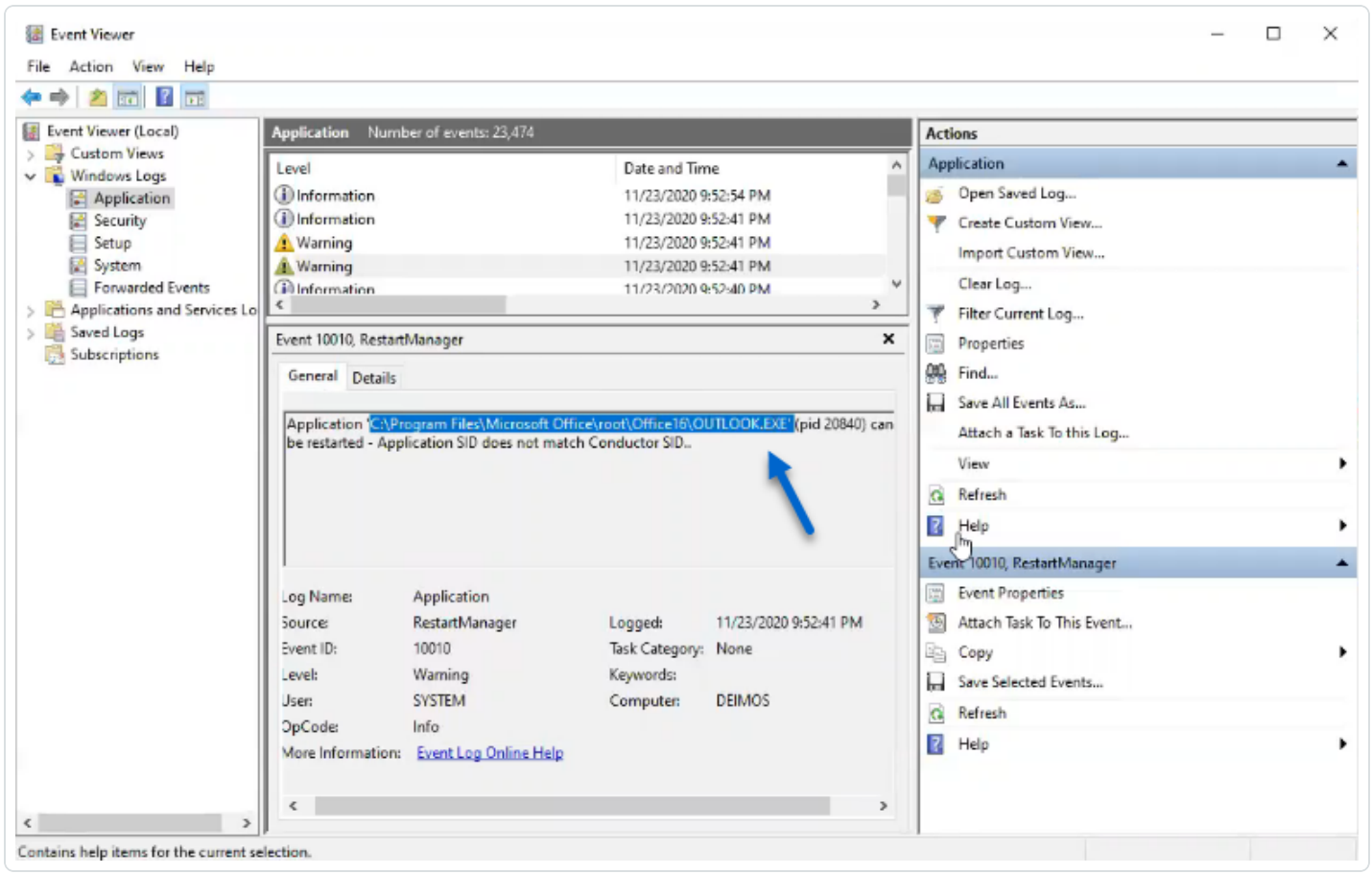
订阅。

- 事件监听器接收事件日志并对其进行缓冲，然后定期将其刷新到网络共享区中名为 Sysvol 的文件。每个 DC 都刷新到单个 Sysvol 文件，该文件存储收集的事件并将其复制到其他域控制器。
- 该脚本还创建了一个 WMI 使用者，通过在 DC 重新启动时重新注册事件订阅者来确保此机制持续存在。每次 DC 重新启动时，WMI 都会通知使用者，以允许使用者再次注册事件监听器。
- 此时，分布式文件系统 (DFS) 复制开始并在域控制器之间自动同步文件。Tenable Identity Exposure 的平台监听传入的 DFS 复制流量，并使用此数据收集事件、运行安全分析，然后生成 IoA 警报。

本地数据检索

Windows 事件日志记录操作系统及其应用程序中发生的所有事件。事件日志依赖于 Windows 中集成的组件框架。

Tenable Identity Exposure IoA 事件日志侦听器使用 EvtSubscribe API，仅以插入字符串的形式收集从事件日志中提取的有用的事件日志数据段。Tenable Identity Exposure 将这些插入字符串写入 Sysvol 文件夹中存储的文件中，并通过 DFS 引擎进行复制。这样，Tenable Identity Exposure 就可以从事件日志收集正确数量的安全数据，以运行安全分析和检测攻击。



IoA 脚本摘要

下表概述了 Tenable Identity Exposure 脚本部署。

步骤	描述	涉及的组件	技术操作
1	注册 Tenable Identity Exposure的 IoA 部署	GPO 管理	创建 `Tenable.ad`(默认名称) GPO 并将其链接到域控制器 OU。
2	在 DC	DC 本	每个 DC 都会检测要应用的新 GPO, 具体取决于 AD 复制和组

	上启动 Tenable Identity Exposure 的 IoA 部署	地系统	策略刷新间隔。
3	控制高级日志记录策略状态	DC 本地系统	系统通过设置注册表项 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy` 来激活高级日志记录策略。
4	更新本地日志记录策略	DC 本地系统	根据要检测的 IoA，Tenable Identity Exposure 会动态生成并激活特定审核策略。此策略不会停用任何现有的日志记录策略，而仅会在必要时加以丰富。如果检测到冲突，GPO 安装脚本将停止并显示消息“Tenable Identity Exposure 需要审核策略 '...'，但当前 AD 配置阻止其使用。”
5	注册事件监听器和 WMI 生产者	DC 本地系统	系统注册并执行 GPO 中包含的脚本。此脚本运行 PowerShell 进程以使用 EvtSubscribe API 订阅事件日志，并出于持久性目的创建 `ActiveScriptEventConsumer` 实例。Tenable Identity Exposure 使用这些对象接收和存储事件日志内容。
6	收集事件日志消息	DC 本地系统	Tenable Identity Exposure 捕获相关事件日志消息，定期对其进行缓冲，然后保存到与 Tenable Identity Exposure GPO (`...{GPO_GUID}\Machine\IOA<DC_name>`) 相关联的 Sysvol 文件夹中存储的文件（每个 DC 一个文件）。
7	将文件复制到声明的 DC SYSVOL 文件夹	Active Directory	AD 使用 DFS 跨域复制文件，特别是在已声明的 DC 中。Tenable Identity Exposure 平台获取每个文件的通知并读取其内容。

8	覆盖这些文件	Active Directory	每个 DC 都会自动且连续地将定期缓冲的事件写入同一个文件中。

安装脚本(Tenable Identity Exposure v. 3.19.11 及更早版本)

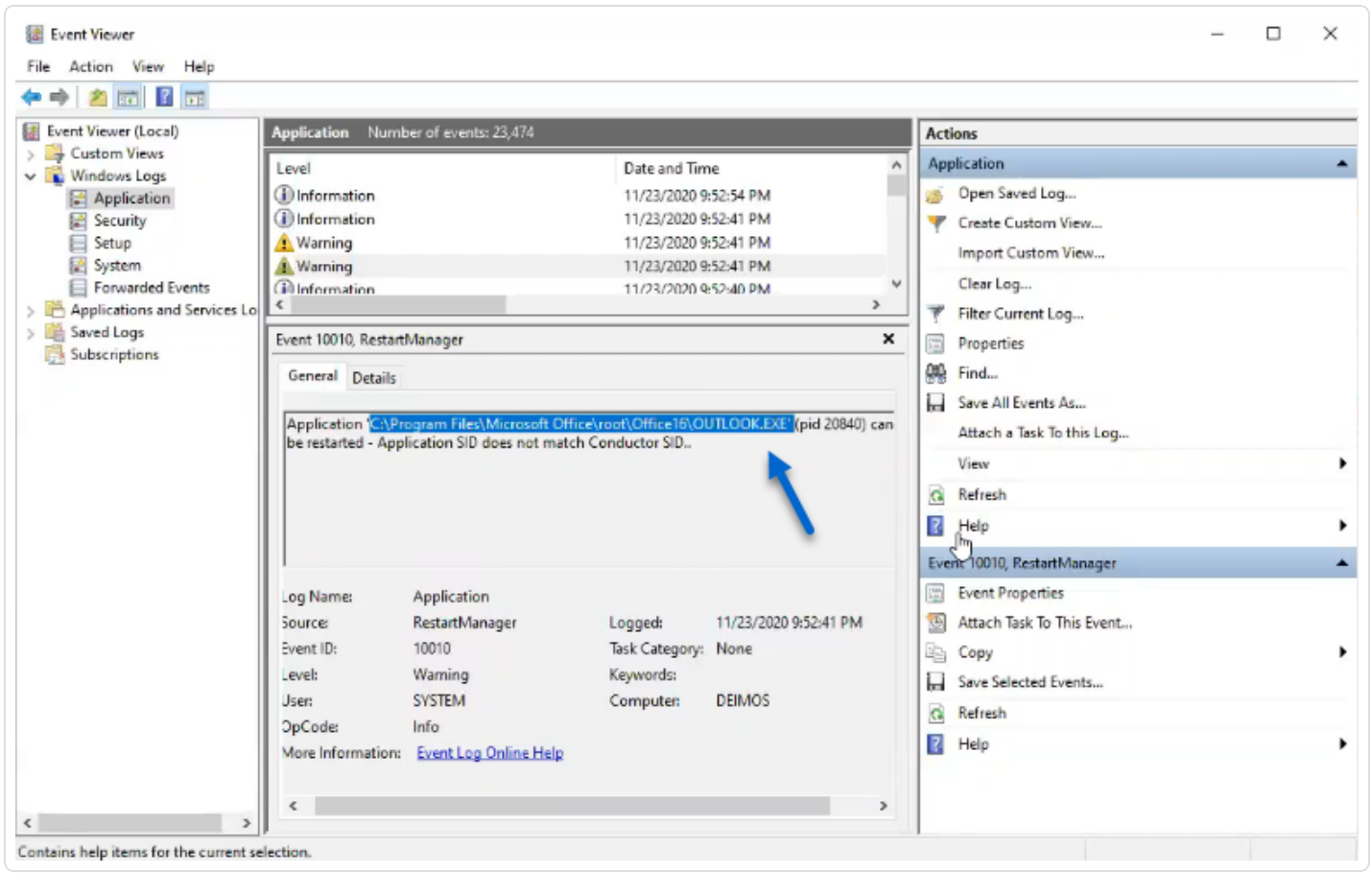
GPO 包含所有 DC 在本地执行以收集相关数据的 PowerShell 脚本，如下所示：

- 这些脚本在计算机内存中配置事件观察程序和 Windows Management Instrumentation (WMI) 生产者/使用者。WMI 是一个 Windows 组件，为您提供有关本地或远程计算机系统状态的信息。
- 事件观察程序接收事件日志并定期对其进行缓冲，然后将其刷新到网络共享区中名为 Sysvol 的文件。每个 DC 都刷新到单个 Sysvol 文件，该文件存储收集的事件并将其复制到其他域控制器。
- WMI 使用者在 DC 重新启动时再次注册事件观察程序，通过这种方式使此机制持续运作。每次 DC 重新启动时，生产者都会唤醒并通知使用者。因此，使用者会再次注册事件观察程序。
- 此时，分布式文件系统或 DFS 复制开始并在域控制器之间自动同步文件。Tenable Identity Exposure 的平台监听传入的 DFS 复制流量，并使用此数据收集事件、运行安全分析，然后生成 IoA 警报。

本地数据检索

Windows 事件日志记录操作系统及其应用程序中发生的所有事件。名为 Event Tracing for Windows (ETW) 的事件日志依赖于 Windows 中集成的组件框架。ETW 在内核中运行，产生的数据存储在 DC 本地，AD 协议不会复制这些数据。

Tenable Identity Exposure 使用 WMI 引擎，仅以插入字符串的形式收集从事件日志中提取的有用的 ETW 数据段。Tenable Identity Exposure 将这些插入字符串写入 Sysvol 文件夹中存储的文件中，并通过 DFS 引擎进行复制。这样，Tenable Identity Exposure 就可以从 ETW 收集正确数量的安全数据，以运行安全分析和检测攻击。



IoA 脚本摘要

下表概述了 Tenable Identity Exposure 脚本部署。

步骤	描述	涉及的组件	技术操作
1	注册 Tenable Identity Exposure的 IoA 部署	GPO 管理	创建 `Tenable.ad`(默认名称) GPO 并将其链接到域控制器 OU。
2	在 DC	DC 本	每个 DC 都会检测要应用的新 GPO, 具体取决于 AD 复制和组

	上启动 Tenable Identity Exposure 的 IoA 部署	地系统	策略刷新间隔。
3	注册事件观察程序和 WMI 生产者/使用者	DC 本地系统	系统注册并执行即时任务。此任务运行 PowerShell 进程，以创建以下类的实例：`ManagementEventWatcher` 和 `ActiveScriptEventConsumer`。Tenable Identity Exposure 使用这些对象接收和存储 ETW 消息。
4	控制高级日志记录策略状态	DC 本地系统	系统通过设置注册表项 `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\SCENoApplyLegacyAuditPolicy` 来激活高级日志记录策略。
5	更新本地日志记录策略	DC 本地系统	根据要检测的 IoA，Tenable Identity Exposure 会动态生成并激活高级日志记录策略。此策略不会停用任何现有的日志记录策略，而仅会在必要时加以丰富。如果检测到冲突，GPO 安装脚本将停止并显示消息“Tenable Identity Exposure 需要审核策略 '...'，但当前 AD 配置阻止其使用。”
6	收集 ETW 消息	DC 本地系统	Tenable Identity Exposure 捕获相关 ETW 消息，定期对其进行缓冲，然后保存到与 Tenable Identity Exposure GPO (`...{GPO_GUID}\Machine\IOA<DC_name>`) 相关联的 Sysvol 文件夹中存储的文件（每个 DC 一个文件）。
7	将文件复制到 Tenable Identity Exposu	Active Directory	AD 使用 DFS 跨域复制文件。Tenable Identity Exposure 平台也接收文件。

	re 平台		
8	覆盖这些文件	Active Directory	每个 DC 都会自动且连续地将定期缓冲的事件写入同一个文件中。

另请参阅：

- Indicators of Attack and the Active Directory
- 安装攻击指标
- 技术变更与潜在影响

技术变更与潜在影响

攻击指标 (IoA) 模块的安装脚本会创建一个 GPO，以在受监控的 DC 上透明地应用以下更改：

- 默认情况下，名为“Tenable.ad”的新 GPO 链接到域控制器的组织单位 (OU)。
- 修改注册表项，以激活 Microsoft Advanced 日志记录策略。
- 激活新的事件日志策略，以强制域控制器生成 IoA 所需的 ETW 信息。

  注意：事件日志策略是必需项，这样 ETW 引擎才可以生成 Tenable Identity Exposure 所需的插入字符串。此策略不会禁用任何现有的日志记录策略，而是会向其中添加内容。如果存在冲突，部署脚本将停止并显示错误消息。

- 为 Tenable Identity Exposure 服务帐户添加了写入权限，以允许对 GPO 文件夹中存储的 IoA 配置进行“自动更新”。

限制和潜在影响

攻击指标 (IoA) 模块可造成以下限制：

- IoA 模块依赖于 ETW 数据，并在 Microsoft 定义的限制内运行。
- 安装的 GPO 必须在整个域中进行复制，并且必须经过 GPO 刷新间隔才能完成安装过程。在复制期间，可能会发生误报和漏报。即使 Tenable Identity Exposure 会通过不立即启动攻击指标引擎中的检查来最大程度地减少此影响，仍会有此情形发生。
- Tenable 使用 SYSVOL 文件共享来从域控制器检索 ETW 信息。当 SYSVOL 复制到域中的每个域控制器时，在 Active Directory 活动的高峰期间会出现复制活动显着增加。
- 在域控制器和 Tenable Identity Exposure 之间复制文件也会消耗一些网络带宽。Tenable Identity Exposure 通过自动删除其收集的文件来控制这些影响，同时会限制这些文件的大小(默认情况下最大为 500 MB) 。
- 与分布式文件系统 (DFS) 复制缓慢或损坏相关的问题。有关更多信息，请参阅“DFS 复制问题缓解措施”。

另请参阅：

- Indicators of Attack and the Active Directory
- 安装攻击指标
- 攻击指标安装脚本
- 对攻击指标进行故障排除

攻击场景 (< v. 3.36)

注意:攻击指标的此配置更新功能不再适用于 Tenable Identity Exposure 3.36 以上版本。

所需用户角色:具有修改攻击指标配置权限的组织用户。

您可以通过为 Tenable Identity Exposure 选择要在特定域上监控的攻击类型来定义攻击场景。

开始之前

要修改攻击场景,您必须拥有具有以下权限的用户角色:

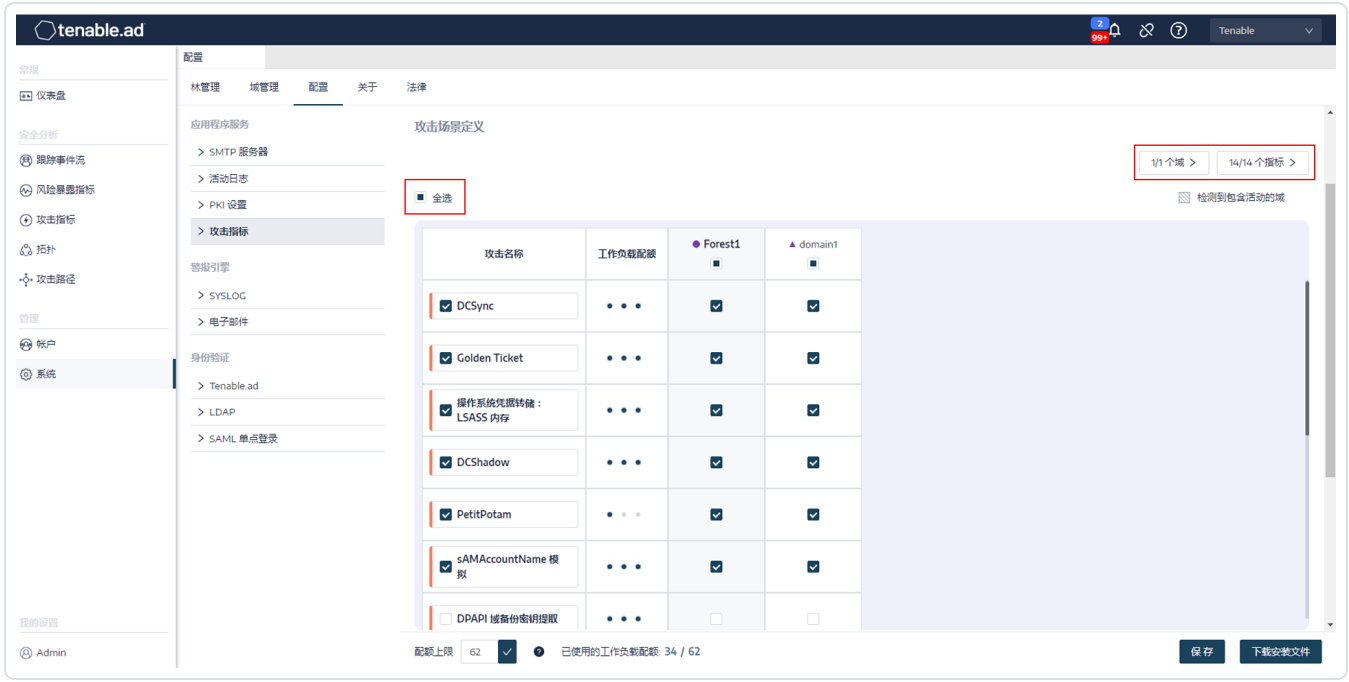
- 在"**数据实体**"中,对以下内容的"读取"权限:
  - 所有攻击指标
  - 所有域
- 在"**界面实体**"中,对以下内容的访问权限:
  - 管理 > 系统 > 配置
  - 管理 > 系统 > 配置 > 应用程序服务 > 攻击指标
  - 管理 > 系统 > 配置 > 应用程序服务 > 攻击指标 > 下载安装文件

有关基于角色的权限的更多信息,请参阅 设置角色的权限。

定义攻击场景的步骤:

1. 在 Tenable Identity Exposure 中,点击"**系统**">"**配置**">"**攻击指标**"。

   此时"**攻击场景定义**"窗格会打开。



2. 在“**攻击名称**”下，选择要监控的攻击。
3. 选择要在其上针对所选攻击进行监控的域。
4. 您可以选择执行以下操作之一：
    - 点击“**全选**”以监控所有域上的所有攻击。
    - 点击“**n/n 个域**”或“**n/n 个指标**”以筛选要在其上监控特定攻击的特定域。
5. 单击“**保存**”。

    此时会出现一条确认消息，通知您 Tenable Identity Exposure 会在您保存配置后清除每个攻击的活动状态。
6. 点击“**确认**”。

    此时会出现一条消息，确认 Tenable Identity Exposure 已更新攻击指标配置。
7. 点击“**下载安装文件**”。
8. 为使新的攻击配置生效，请运行安装文件：
    a. 将下载的安装文件复制并粘贴到受监控域中的 DC。
    b. 使用管理权限打开 PowerShell 终端。

c. 在 Tenable Identity Exposure 中，复制窗口底部“攻击指标”部分下面的命令。

d. 在 PowerShell 窗口中，粘贴命令以运行脚本。

工作负载配额

注意：工作负载配额功能不再适用于 Tenable Identity Exposure 3.36 以上版本。

所需用户角色：具有编辑工作负载配额权限的组织用户。

Tenable Identity Exposure 中的每个攻击指标都有一个相关联的工作负载配额，此配额考虑了分析攻击数据所需的资源。

Tenable Identity Exposure 计算工作负载配额以限制同时运行的攻击指标 (IoA) 的数量，该数量会影响域控制器上用于生成事件的带宽和 CPU 使用率。

修改工作负载配额限制后，请执行以下操作：

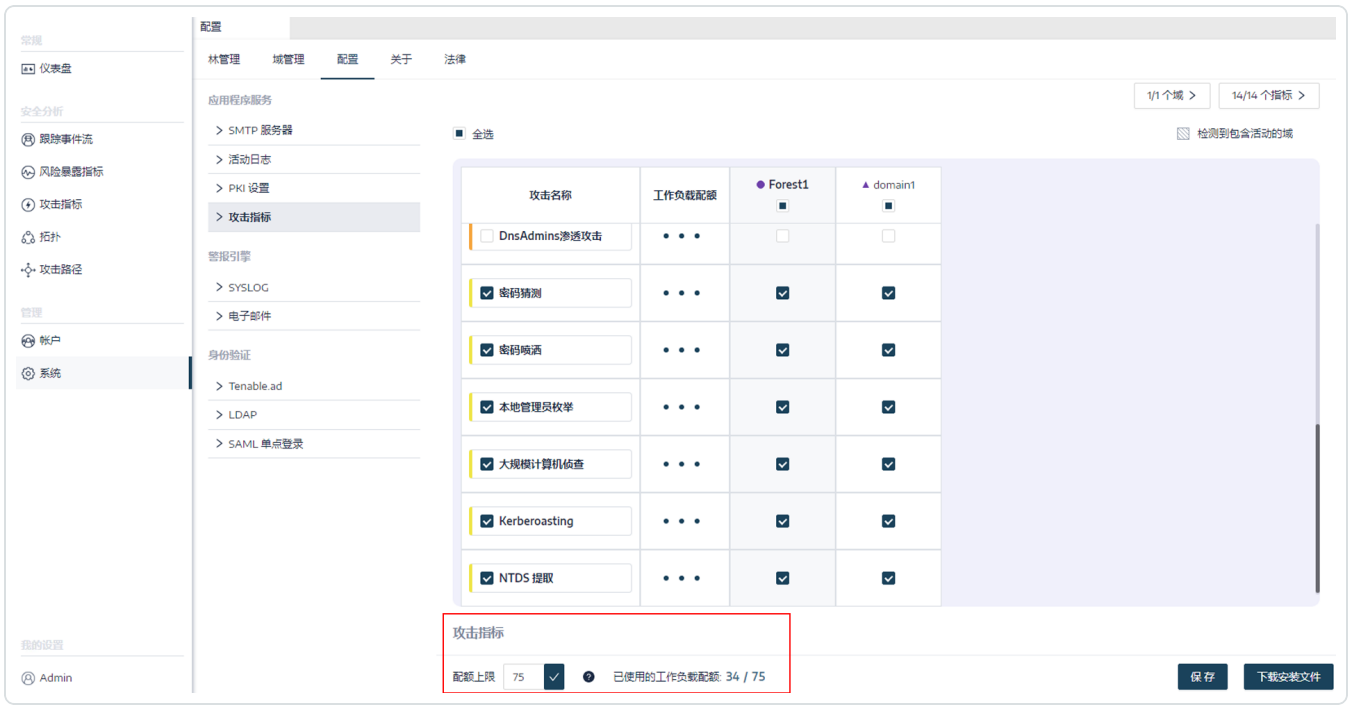
- 增加：监控增加后的统计数据以确保合理的余量。
- 减少：停用某些 IoA，使其数量保持在此配额以下，从而减少针对攻击的安全范围。

修改工作负载配额的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”>“**攻击指标**”。

   “**IoA 配置**”窗格随即打开。

2. 为配置选择所需的 IoA。
3. 在“**攻击指标**”下的“**配额上限**”框中，键入工作负载配额限制的值。



4. 点击您输入的值旁边的复选标记。

   此时会出现一条消息，通知您此修改对 Tenable Identity Exposure 造成的影响。

   注意：如果输入的配额最大限制小于当前攻击配置的要求，则必须调整活动攻击指标的数量或提高限制。

5. 点击“**确认**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新配额最大限制。

6. 单击“**保存**”。

   此时会出现一条确认消息，通知您 Tenable Identity Exposure 会在您保存配置后清除每个攻击的活动状态。

7. 点击“**确认**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新攻击指标配置。

8. 点击“**下载安装文件**”。

9. 为使新的攻击配置生效，请运行安装文件：

a. 将下载的安装文件复制并粘贴到受监控域中的 DC。

b. 使用管理权限打开 PowerShell 终端。

c. 在 Tenable Identity Exposure 中，复制窗口底部“攻击指标”部分下面的命令。

d. 在 PowerShell 窗口中，粘贴命令以运行脚本。

安装 Microsoft Sysmon

某些 Tenable Identity Exposure 的攻击指标 (IoA) 需要激活 Microsoft System Monitor (Sysmon) 服务。

Sysmon 监控系统活动并将其记录到 Windows 事件日志中，以便在 Event Tracing for Windows (ETW) 基础设施中提供更多面向安全的信息。

因为安装其他 Windows 服务和驱动程序可能会影响托管 Active Directory 基础设施的域控制器的性能，因此，Tenable 不会自动部署 Microsoft Sysmon。您必须手动安装或使用专用 GPO。

以下 IoA 需要 Microsoft Sysmon。

名称	原因
OS 凭据转储：LSASS 内存	检测进程注入

注意：如果您选择安装 Sysmon，则必须在所有域控制器上安装它，而不仅仅是在 PDC 上安装，这样才能收集所有必要的事件。

注意：在完全部署 Tenable Identity Exposure 之前，请测试您的 Sysmon 安装文件是否存在兼容性问题。

提示：确保在安装后定期更新 Sysmon，以利用修补程序解决可能的漏洞。与 Tenable Identity Exposure 兼容的最旧版本为 Sysmon 12.0。

如要安装 Sysmon，请执行以下操作：

1. 从 Microsoft 网站下载 Sysmon。
2. 在命令行界面中，运行以下命令以在本地计算机上安装 Microsoft Sysmon：

```
.\Sysmon64.exe -accepteula -i C:\TenableSysmonConfigFile.xml
```

注意：有关配置说明，请参阅带注释的 Sysmon 配置文件。

3. 运行以下命令以添加注册表项，以指示 WMI 筛选器已安装 Sysmon：

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

若要卸载 Sysmon：

1. 打开 PowerShell 终端。
2. 浏览到包含 `Sysmon64.exe` 的文件夹。
3. 键入以下命令：

```
PS C:\> .\Sysmon64.exe -u
```

若要删除注册表项：

- 在命令行界面中，在运行 Sysmon 的所有计算机上输入以下命令：

```
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog\Microsoft-Windows-Sysmon/Operational"
```

Sysmon 配置文件

注意：
- 使用前，请复制 Sysmon 配置文件并将其另存为 XML 文件。万一出错，也可在此处直接下载配置文件。
- 运行该文件之前，先在文件属性中取消阻止该文件。

```
<Sysmon schemaversion="4.40">
  <EventFiltering>

    <!--SYSMON EVENT ID 1 : PROCESS CREATION [ProcessCreate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessCreate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 2 : FILE CREATION TIME RETROACTIVELY CHANGED IN THE FILESYSTEM [FileCreateTime]-->
```

```
    <RuleGroup name="" groupRelation="or">
      <FileCreateTime onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateTime>
    </RuleGroup>

    <!--SYSMON EVENT ID 3 : NETWORK CONNECTION INITIATED [NetworkConnect]-->
    <RuleGroup name="" groupRelation="or">
      <NetworkConnect onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </NetworkConnect>
    </RuleGroup>

    <!--SYSMON EVENT ID 4 : RESERVED FOR SYSMON SERVICE STATUS MESSAGES-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 5 : PROCESS ENDED [ProcessTerminate]-->
    <RuleGroup name="" groupRelation="or">
      <ProcessTerminate onmatch="exclude">
        <!--NOTE: Using "exclude" with no rules means everything in this section will be logged-->
      </ProcessTerminate>
    </RuleGroup>

    <!--SYSMON EVENT ID 6 : DRIVER LOADED INTO KERNEL [DriverLoad]-->
    <RuleGroup name="" groupRelation="or">
      <DriverLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DriverLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 7 : DLL (IMAGE) LOADED BY PROCESS [ImageLoad]-->
    <RuleGroup name="" groupRelation="or">
      <ImageLoad onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </ImageLoad>
    </RuleGroup>

    <!--SYSMON EVENT ID 8 : REMOTE THREAD CREATED [CreateRemoteThread]-->
    <RuleGroup name="" groupRelation="or">
      <CreateRemoteThread onmatch="include">
        <TargetImage name="lsass" condition="is">C:\Windows\system32\lsass.exe</TargetImage>
      </CreateRemoteThread>
    </RuleGroup>

    <!--SYSMON EVENT ID 9 : RAW DISK ACCESS [RawAccessRead]-->
    <RuleGroup name="" groupRelation="or">
      <RawAccessRead onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RawAccessRead>
    </RuleGroup>

    <!--SYSMON EVENT ID 10 : INTER-PROCESS ACCESS [ProcessAccess]-->
    <RuleGroup name="" groupRelation="or">
        <ProcessAccess onmatch="include">
          <!-- Detect Access to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
```

```
            <GrantedAccess>0x1FFFFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1F1FFF</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x1010</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x143A</GrantedAccess>
          </Rule>

          <!-- Detect process hollowing to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0800</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1003,technique_name=Credential Dumping"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x800</GrantedAccess>
          </Rule>

          <!-- Detect process process injection to LSASS-->
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x0820</GrantedAccess>
          </Rule>
          <Rule groupRelation="and">
            <TargetImage name="technique_id=T1055,technique_name=Process Injection"
condition="is">C:\Windows\system32\lsass.exe</TargetImage>
            <GrantedAccess>0x820</GrantedAccess>
          </Rule>
        </ProcessAccess>
    </RuleGroup>

    <!--SYSMON EVENT ID 11 : FILE CREATED [FileCreate]-->
    <RuleGroup name="" groupRelation="or">
      <FileCreate onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreate>
    </RuleGroup>

    <!--SYSMON EVENT ID 12 & 13 & 14 : REGISTRY MODIFICATION [RegistryEvent]-->
    <RuleGroup name="" groupRelation="or">
      <RegistryEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </RegistryEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 15 : ALTERNATE DATA STREAM CREATED [FileCreateStreamHash]-->
```

```
    <RuleGroup name="" groupRelation="or">
      <FileCreateStreamHash onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileCreateStreamHash>
    </RuleGroup>

    <!--SYSMON EVENT ID 16 : SYSMON CONFIGURATION CHANGE-->
      <!--Cannot be filtered.-->

    <!--SYSMON EVENT ID 17 & 18 : PIPE CREATED / PIPE CONNECTED [PipeEvent]-->
    <RuleGroup name="" groupRelation="or">
      <PipeEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </PipeEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 19 & 20 & 21 : WMI EVENT MONITORING [WmiEvent]-->
    <RuleGroup name="" groupRelation="or">
      <WmiEvent onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </WmiEvent>
    </RuleGroup>

    <!--SYSMON EVENT ID 22 : DNS QUERY [DnsQuery]-->
    <RuleGroup name="" groupRelation="or">
      <DnsQuery onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </DnsQuery>
    </RuleGroup>

    <!--SYSMON EVENT ID 23 : FILE DELETED [FileDelete]-->
    <RuleGroup name="" groupRelation="or">
      <FileDelete onmatch="include">
        <!--NOTE: Using "include" with no rules means nothing in this section will be logged-->
      </FileDelete>
    </RuleGroup>

  </EventFiltering>
</Sysmon>
```

卸载攻击指标

所需角色:本地计算机上的管理员。

若要卸载攻击指标 (IoA) 模块,请运行创建 Tenable Identity Exposure cleaning 新组策略对象 (GPO) 的命令。

卸载进程默认使用此新 GPO 清除以前安装的 GPO 及其 SYSVOL 文件、注册表设置、高级日志记录策略和 WMI 筛选器。

注意:如果更改了初始 GPO 的名称,则必须将其传递给卸载程序,以便它知道要卸载哪个 GPO。若要传递新的 GPO 名称,请使用参数 `-GpoDisplayName`。

若要卸载 IoA 模块:

1. 在命令行界面中,运行以下命令以卸载 IoA 模块:

   ```
   Register-TenableIOA.ps1 -Uninstall
   ```

2. 在整个域中复制此新 GPO。该脚本强制执行 4 小时延迟以便完成复制。

3. 运行以下命令以删除 Cleaning GPO:

   ```
   Remove-GPO -Guid <GUID> -Domain "<DOMAIN>"
   ```

4. 可选:运行以下命令以验证 GPO 不再存在:

   ```
   (Get-ADDomainController -Filter *).Name | Foreach-Object {Get-GPO -Name "Tenable.ad cleaning"}
   | Select Displayname| measure
   ```

对攻击指标进行故障排除

- 高级审核策略配置优先级
- 防病毒检测
- Tenable Identity Exposure 日志文件
- 事件日志侦听器验证
- DFS 复制问题缓解措施

防病毒检测

Tenable 和 Microsoft 不建议在域控制器(或任何其他具有中央管理控制台的工具)上安装杀毒软件、端点防护平台 (EPP) 或端点检测与响应 (EDR) 软件。如果您选择这样做,您的杀毒软件/EPP/EDR 可能会检测甚至阻止或删除域控制器上攻击指标 (IoA) 事件集合所需的项目。

Tenable Identity Exposure 的攻击指标部署脚本不包含恶意代码,甚至未进行模糊化处理。但是,考虑到该脚本使用 PowerShell 和 WMI,并且其实现具有无代理性质,偶尔会进行检测。

如果您遇到如下问题:

- 安装期间的错误消息
- 检测中的误报或漏报

若要对安装脚本防病毒检测进行故障排除:

1. 检查防病毒软件/EPP/EDR 安全日志,以确认是否检测、阻止或删除 Tenable Identity Exposure 组件。防病毒软件/EPP/EDR 可影响下列组件:
    - 应用于域控制器的 Tenable Identity Exposure GPO 中的 `ScheduledTasks.xml` 文件。
    - 域控制器上用于启动 PowerShell.exe 的 Tenable Identity Exposure 计划任务。
    - Tenable Identity Exposure `Register-TenableADEventsListener.exe` 进程在域控制器上启动。
2. 在工具中为受影响的组件添加安全例外。
    - 特别是,Symantec Endpoint Protection 在 IoA 安装过程中会引发 `CL.Downloader!gen27` 检测。您可以将此特定已知风险添加到例外策略中。
    - 设置好任务计划程序后,运行 PowerShell 以启动 `Register-TenableADEventsListener.exe` 进程。杀毒/EPP/EDR 软件可能会阻碍此 PowerShell 脚本,从而阻碍攻击指标的正确执行。密切跟踪此进程并确保其在所有受监视的域控制器上仅运行一次。

杀毒/EPP/EDR 的文件路径排除示例：

```
Register-TenableADEventsListener.exe process
 "\\"domain"\sysvol\"domain"\Policies\{"GUID_Tenable.ad}\Machine\IOA\Register-
TenableADEventsListener.exe"
```

```
ScheduledTasks.xml file
    C:\Users\<User Name>\AppData\Local\Temp\4\Tenable.ad\
{GUID}\DomainSysvol\GPO\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    C:\Windows\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
    \\[DOMAIN.FQDN]\[SYSVOL]\POLICIES\
{[GUID]}\Machine\Preferences\ScheduledTasks\ScheduledTasks.xml
```

高级审核策略配置优先级

Tenable Identity Exposure 为启用所需事件日志记录而创建的组策略对象 (GPO) 链接到启用了强制模式的组织单元 (OU) 域控制器。

这为 GPO 提供了高优先级，但在更高级别（如域或站点）配置的强制 GPO 的优先级更高。

如果定义高级审核策略配置设置的较高优先级 GPO 与 Tenable Identity Exposure 的需求冲突，则 GPO 优先且 Tenable Identity Exposure 会错过攻击检测所需的事件。

由于 Windows 会合并 GPO 定义的高级审核策略配置设置，因此不同的 GPO 可定义不同的设置。

但是，在每个设置级别，它仅使用具有更高优先级的 GPO 定义的值。例如，Tenable Identity Exposure 需要“审核凭据验证”设置具有“Success and Failure”值。但是，如果具有更高优先级的 GPO 仅为审核凭据验证定义“Success”，则 Windows 仅会收集“Success”事件，而 Tenable Identity Exposure 会错过所需的“Failure”事件。

要检查 GPO 优先级，请执行以下操作：

1. 在命令行界面中，在域控制器上运行以下命令。

   它会在考虑所有 GPO 和优先级之后输出有效的高级审核策略配置。

   ```
   auditpol.exe /get /category:*
   ```

2. 将输出与 Tenable Identity Exposure 高级审核策略要求进行比较。对于 Tenable Identity Exposure 需要的每项设置，请检查有效策略是否也涵盖该设置。

   - 如果有效策略更详尽，则不是问题，例如当 Tenable Identity Exposure 需要“Success”或“Failure”，而设置为“Success and Failure”时。
   - 如果有效策略不充分，则表示优先级较高的 GPO 定义了冲突的设置。

若要修复 GPO 优先级：

1. 在定义高级审核策略配置的“强制”模式下查找链接到更高级别（域或站点）的 GPO。
2. 在命令行界面中，在域控制器上运行以下命令，以准确找到成功的 GPO：

   ```
   gpresult /scope:computer /h gpo.html
   ```

3. 修改 GPO 中相应的高级审核策略配置设置，以满足 Tenable Identity Exposure 的最低要求。例如：

    - 如果 Tenable Identity Exposure 需要“Success”，而更高优先级的 GPO 定义为“Failure”，则将设置修改为“Success and failure”。
    - 如果 Tenable Identity Exposure 需要“Success and Failure”，而更高优先级的 GPO 定义为“Success”，则将设置修改为“Success and Failure”。

4. 修改设置后，您可以等待更新后的 GPO 应用或使用 `gpupdate` 命令强制执行。
5. 重复程序 要检查 GPO 优先级，请执行以下操作： 以检查新的有效策略。

事件日志侦听器验证

攻击指标安装脚本在计算机内存中配置事件观察程序和 Windows Management Instrumentation (WMI) 生产者/使用者。WMI 是一个 Windows 组件，为您提供有关本地或远程计算机系统状态的信息。

若要检查 WMI 注册是否正确，请执行以下操作：

- 在 PowerShell 中运行以下命令：

```
Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter "Filter
= ""__EventFilter.name='AlsidForAD-Launcher'"""
```

- 如果至少存在一个使用者，您将获得以下类型的输出：

```
> Get-WmiObject -Class '__FilterToConsumerBinding' -Namespace 'root\subscription' -Filter
"Filter = ""__EventFilter.name='AlsidForAD-Launcher'"""


__GENUS                 : 2
__CLASS                 : __FilterToConsumerBinding
__SUPERCLASS            : __IndicationRelated
__DYNASTY               : __SystemClass
__RELPATH               : __
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name=\"AlsidForAD-Launcher\"",F
                          ilter="__EventFilter.Name=\"AlsidForAD-Launcher\""
__PROPERTY_COUNT        : 7
__DERIVATION            : {__IndicationRelated, __SystemClass}
__SERVER                : DC-999
__NAMESPACE             : ROOT\subscription
__PATH                  : \\DC-999\ROOT\subscription:__
FilterToConsumerBinding.Consumer="ActiveScriptEventConsumer.Name
                          =\"AlsidForAD-Launcher\"",Filter="__EventFilter.Name=\"AlsidForAD-
Launcher\""
Consumer                : ActiveScriptEventConsumer.Name="AlsidForAD-Launcher"
CreatorSID              : {1, 1, 0, 0...}
DeliverSynchronously    : False
DeliveryQoS             :
Filter                  : __EventFilter.Name="AlsidForAD-Launcher"
MaintainSecurityContext : False
SlowDownProviders       : False
PSComputerName          : DC-999
```

  - 如果没有已注册的 WMI 使用者，则该命令不返回任何内容。
  - 这是进程在 DC for WMI 上运行的先决条件。

若要检索 WMI 进程（针对不高于 3.19 的版本），请执行以下操作：

- 在 PowerShell 中运行以下命令：

```
gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}
```

- 有效结果示例：

```
> gcim win32_process | Where-Object { $_.CommandLine -match "TenableADWMIListener"}

ProcessId Name           HandleCount WorkingSetSize VirtualSize
--------- ----           ----------- -------------- -----------
952       powershell.exe 502         26513408       2199678185472
```

若要检索事件日志侦听器(针对不低于 3.29 的版本)，请执行以下操作：

- 在 PowerShell 中运行以下命令：

```
gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}
```

- 有效结果示例：

```
PS C:\IOAInstall> gcim win32_process | Where-Object { $_.CommandLine -match "Register-
TenableADEventsListener.exe"}

ProcessId Name                                HandleCount WorkingSetSize VirtualSize

5748      Register-TenableADEventsListener.exe 152         4096000        4384534528
```

Tenable Identity Exposure 日志文件

如果在验证 GPO 和 WMI 使用者之后仍然没有看到“攻击指标”警报，可以查看 Tenable Identity Exposure 的内部日志。

Ceti 日志

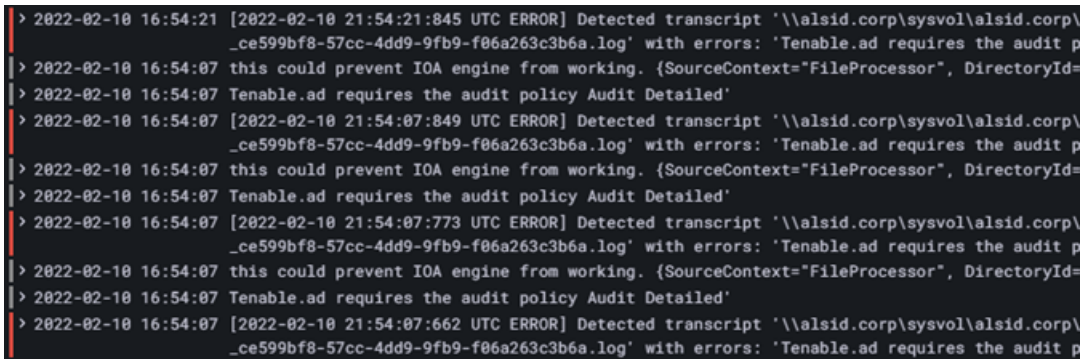
- 检查 CETI 日志中的以下错误消息：

```
[2022-02-22 22:23:27:570 UTC WARNING] Some domain controllers are not generating IOA
events: 'CORP-DC'. {SourceContext="DirectoryEventToCetiAdObjectMessageMapper",
DirectoryId=2, Dns="corp.bank.com", Host="10.10.20.10", Source=SYSVOL, Version="3.11.5"}
```

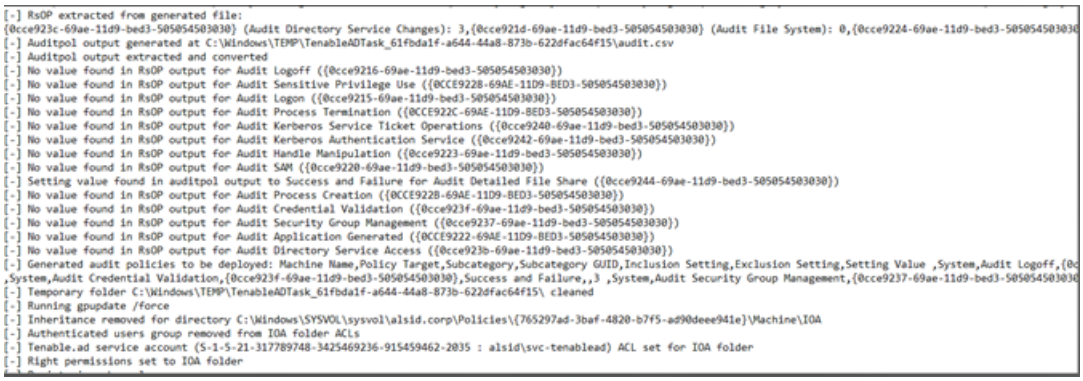
- 如果看到此消息，请验证上述错误消息中列出的域控制器 (DC) 上是否正在运行 GPO 设置和 WMI 使用者。

审核设置

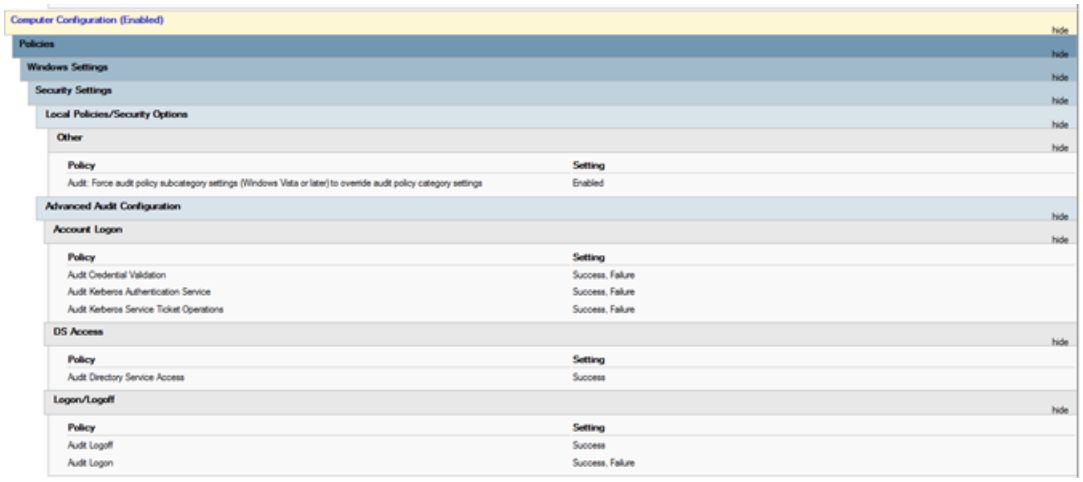
- 如果您看到类似于以下内容的错误：“Tenable Identity Exposure 要求审核策略...”，请检查现有 GPO 以确保没有将所需的审核策略设置为“不审核”。



- 如果收到指出“RSOP...”的错误：



- 检查审核策略并查看 Sysvol 文件夹中的脚本文件，以查看在安装过程中是否遇到任何问题。



Cygni 日志

Cygni 记录攻击并列出被 Tenable Identity Exposure 调用以生成警报的特定 `.gz` 文件。

I-DCSync

```
2022-03-15 11:39:31
[2022-03-15 15:39:30:759 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCSync' and Event '110052' {SourceContext="AttackEngine", CodeName="I-DCSync", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-GoldenTicket

```
2022-03-15 11:40:31
[2022-03-15 15:40:31:490 UTC INFORMATION] Anomaly 'Logon' has been raised for Indicator 'I-
GoldenTicket' and Event '110061' {SourceContext="AttackEngine", CodeName="I-GoldenTicket",
ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ProcessInjectionLsass

```
022-03-15 12:47:09
[2022-03-15 16:47:09:811 UTC INFORMATION] Anomaly 'ProcessAccess' has been raised for Indicator 'I-
ProcessInjectionLsass' and Event '115948' {SourceContext="AttackEngine", CodeName="I-
ProcessInjectionLsass", ProfileId=1, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-DCShadow

```
2022-03-15 11:30:30
[2022-03-15 15:30:30:657 UTC INFORMATION] Anomaly 'ControlAccess' has been raised for Indicator 'I-
DCShadow' and Event '109948' {SourceContext="AttackEngine", CodeName="I-DCShadow", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-BruteForce

```
2022-03-15 08:02:11
[2022-03-15 12:02:11:231 UTC INFORMATION] Anomaly 'An account failed to log on' has been raised for
Indicator 'I-BruteForce' and Event '109082' {SourceContext="AttackEngine", CodeName="I-BruteForce",
ProfileId=6, AdObjectId="3:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{765297AD-3BAF-4820-B7F5-
AD90DEEE941E}\\Machine\\IOA\\dc-vm-10.0.17763-8_.gz", Event.Id=0, Version="3.16.0"}
```

I-PasswordSpraying

```
2022-03-15 12:39:43
[2022-03-15 16:39:43:793 UTC INFORMATION] Anomaly 'An account failed to log on.' has been raised for
Indicator 'I-PasswordSpraying' and Event '115067' {SourceContext="AttackEngine", CodeName="I-
PasswordSpraying", ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\
{08D6D98F-7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0,
Version="3.16.0"}
```

I-PetitPodam

```
2022-03-15 12:43:02
[2022-03-15 16:43:02:737 UTC INFORMATION] Anomaly 'PetitPotamEFSError' has been raised for Indicator
'I-PetitPotam' and Event '115844' {SourceContext="AttackEngine", CodeName="I-PetitPotam",
ProfileId=4, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-ReconAdminsEnum

```
022-03-15 12:55:31
[2022-03-15 16:55:31:638 UTC INFORMATION] Anomaly 'LocalAdmin enumeration (BloodHound/SharpHound).
Version 2016+' has been raised for Indicator 'I-ReconAdminsEnum' and Event '116085'
{SourceContext="AttackEngine", CodeName="I-ReconAdminsEnum", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

Kerberoasting

```
022-03-15 12:51:30
[2022-03-15 16:51:30:236 UTC INFORMATION] Anomaly 'Kerberos TGS requested on honey account' has been
raised for Indicator 'I-Kerberoasting' and Event '116013' {SourceContext="AttackEngine", CodeName="I-
Kerberoasting", ProfileId=3, AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-
7455-464B-BBEC-23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

I-NtdsExtraction

```
2022-03-15 12:03:51
[2022-03-15 16:03:50:949 UTC INFORMATION] Anomaly 'Shadow copy created on 2012 and above' has been
raised for Indicator 'I-NtdsExtraction' and Event '111168' {SourceContext="AttackEngine",
CodeName="I-NtdsExtraction", ProfileId=4,
AdObjectId="5:\\\\alsid.corp\\sysvol\\alsid.corp\\Policies\\{08D6D98F-7455-464B-BBEC-
23DE4BDF856C}\\Machine\\IOA\\dc-vm-10.0.17763-16_.gz", Event.Id=0, Version="3.16.0"}
```

Cephei 日志

以下日志条目可确定 Cephei 正在写入攻击。密钥值是指定可用于与 Cygni 条目关联的攻击类型的 **attackTypeID**：

I-DCSync attackTypeID:1

```
2022-03-15 11:39:52
2022-03-15T15:39:52.037023041Z stdout F [2022-03-15 15:39:52:035 UTC INFORMATION] [Equuleus] POST
```

```
http://equuleus:3004/attacks/write responded 204 in 32.16 ms : Request Body=
{"timestamp":"1647358722449","directoryId":5,"profileId":4,"attackTypeId":1,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-GoldenTicket attackTypeID:2

```
2022-03-15 11:40:52
2022-03-15T15:40:52.084931986Z stdout F [2022-03-15 15:40:52:084 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.6607 ms : Request Body=
{"timestamp":"1647358773608","directoryId":5,"profileId":4,"attackTypeId":2,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ProcessInjectionLsass attackTypeID:3

```
2022-03-15 12:47:52
2022-03-15T16:47:52.29927328Z stdout F [2022-03-15 16:47:52:298 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 35.7532 ms : Request Body=
{"timestamp":"1647362812784","directoryId":5,"profileId":1,"attackTypeId":3,"count":2}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-DCShadow attackTypeID:4

```
2022-03-15 11:30:52
2022-03-15T15:30:51.949399295Z stdout F [2022-03-15 15:30:51:944 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 24.2605 ms : Request Body=
{"timestamp":"1647358182800","directoryId":5,"profileId":3,"attackTypeId":4,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-BruteForce attackTypeID:5

```
2022-03-15 08:02:54
2022-03-15T12:02:54.698814039Z stdout F [2022-03-15 12:02:54:698 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 30.7623 ms : Request Body=
{"timestamp":"1647345728023","directoryId":3,"profileId":6,"attackTypeId":5,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PasswordSpraying attackTypeID:6

```
2022-03-15 12:39:52
2022-03-15T16:39:52.187309945Z stdout F [2022-03-15 16:39:52:186 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.9422 ms : Request Body=
{"timestamp":"1647362356837","directoryId":5,"profileId":4,"attackTypeId":6,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-PetitPotam attackTypeID:7

```
022-03-15 12:43:52
2022-03-15T16:43:52.226125918Z stdout F [2022-03-15 16:43:52:223 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 15.8402 ms : Request Body=
{"timestamp":"1647362570534","directoryId":5,"profileId":1,"attackTypeId":7,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-ReconAdminsEnum attackTypeID:8

```
2022-03-15 12:55:52
2022-03-15T16:55:52.399889635Z stdout F [2022-03-15 16:55:52:399 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 40.6632 ms : Request Body=
{"timestamp":"1647363305295","directoryId":5,"profileId":4,"attackTypeId":8,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-Kerberoasting attackTypeID:10

```
2022-03-15 12:51:52
2022-03-15T16:51:52.352432644Z stdout F [2022-03-15 16:51:52:351 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 21.0547 ms : Request Body=
{"timestamp":"1647363026345","directoryId":5,"profileId":4,"attackTypeId":10,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

I-NtdsExtraction attackTypeID:11

```
022-03-15 12:03:52
2022-03-15T16:03:52.137547488Z stdout F [2022-03-15 16:03:52:137 UTC INFORMATION] [Equuleus] POST
http://equuleus:3004/attacks/write responded 204 in 13.0304 ms : Request Body=
{"timestamp":"1647360224606","directoryId":5,"profileId":4,"attackTypeId":11,"count":1}
{SourceContext="Equuleus", Version="3.16.0"}
```

Electra 日志

您应该会看到以下条目：

[2022-03-15T14:04:39.151Z] INFO: server/4016 on WIN-UFRSCEN0CI3: Message receive from MQ:attack-alert (namespace=electra)

```
[2022-03-15T14:04:39.151Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Message received from MQ: attack-
alert (namespace=electra)
[2022-03-15T14:04:39.168Z]  INFO: server/4016 on WIN-UQRSCEN0CI3: Sending ws message to listeners.
alertIoA (namespace=electra)
```

Eridanis 日志

您应该会看到以下条目：

```
022-03-15T14:04:39.150Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2010 200
122 - 7ms (namespace=hapi)
[2022-03-15T14:04:39.165Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: notifyAttackAndAttackAlertCreation
success { attackId: 2011 } (namespace=eridanis)
[2022-03-15T14:04:39.170Z]  INFO: server/4988 on WIN-UQRSCEN0CI3: KAPTEYN get /attack-alerts/2011 200
122 - 6ms (namespace=hapi)
```

DFS 复制问题缓解措施

攻击指标部署脚本中的附加参数 `-EventLogsFileWriteFrequency X` 有助于您解决可能遇到的分布式文件系统 (DFS) 复制缓慢或损坏的潜在问题。

此参数为可选参数，仅当您遇到 DFS 复制问题或自部署 IoA 脚本后注意到这些问题时，才建议使用该参数。在正常情况下，该参数保持默认值，您在运行脚本时无需将其包含在命令行中。

何时修改参数

参数 `-EventLogsFileWriteFrequency X` 的值 [X] 是 Tenable Identity Exposure 监听器在非 PDCe 域控制器 (DC) 上生成事件日志文件的频率。Tenable Identity Exposure 侦听器使用的默认建议值为 15 秒。但是，自定义值不适用于 PDCe DC，该控制器会保持其默认的 15 秒间隔，以确保攻击检测功能完全可操作。Tenable 建议仅当您的基础设施面临或容易受到 DFS 复制问题影响时，才使用此参数并将其值从默认的 15 秒值增加到 300 秒（5 分钟）。

建议

请注意，增加事件日志文件的写入频率会降低生成文件的频率，从而增加攻击检测的延迟（例如，文件可能会每 30 秒生成一次，而不是在非 PDCe DC 上所默认的 15 秒）。此外，在 技术变更与潜在影响 中定义的设定限制内，增加延迟会增加生成的事件日志文件的大小。因此，此参数仅用作缓解措施，而不能替代对 DFS 复制问题进行的适当调查。

如要应用参数，请执行以下操作：

1. 按照流程所述为 IoA 配置域。有关更多信息，请参阅“安装攻击指标”。

2. 使用管理权限打开 PowerShell 终端。
3. 运行脚本以配置 IoA 的域控制器并附加 `-EventLogsFileWriteFrequency X` 参数，其中 [X] 是要为事件日志文件频率设置的频率。

身份验证

可通过多种方式对 Tenable Identity Exposure 用户进行身份验证：

- 使用 Tenable Identity Exposure 帐户进行身份验证
- 使用 LDAP 进行身份验证
- 使用 SAML 进行身份验证

使用 Tenable One 进行身份验证

所需许可证：Tenable One

注意：使用 Tenable One 许可证时，您可以管理 Tenable Vulnerability Management 中的所有身份验证设置。有关更多信息，请参阅 *《Tenable Vulnerability Management 用户指南》*中的访问控制。

若要使用 Tenable One 配置身份验证，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”。

   此时会出现配置窗格。

2. 在“**身份验证**”部分下，点击“**Tenable One**”。

3. 在“**默认配置文件**”下拉框中，为用户选择配置文件。

4. 在“**默认角色**”框中，为用户选择角色。

   提示：Tenable One 中之前未连接到 Tenable Identity Exposure 且经过身份验证的用户在登录 Tenable Identity Exposure 时会自动拥有一个帐户。默认配置文件和默认角色会默认应用于该用户。**例外**：在 Tenable Vulnerability Management 中具有“管理员”角色的用户在 Tenable Identity Exposure 中也具有“全局管理员”角色。

5. 单击“**保存**”。

使用 Tenable Identity Exposure 帐户进行身份验证

最简单的身份验证方法是通过需要用户名和密码的 Tenable Identity Exposure 帐户。

此身份验证方法提供默认锁定策略，这是一种安全控制，旨在减少针对身份验证机制的暴力破解攻击。它会在登录尝试失败次数过多后锁定用户帐户。当帐户被锁定时，用户将无权访问 Tenable Identity Exposure API。

使用 Tenable Identity Exposure 帐户配置身份验证：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”。

   此时会出现配置窗格。

2. 在“**身份验证**”部分下，点击“**Tenable Identity Exposure**”。

3. 在“**默认配置文件**”下拉框中，为用户选择配置文件。

4. 在“**默认角色**”框中，为用户选择角色。

5. 配置锁定策略设置：

设置	描述	默认值
已启用	• **已启用** – Tenable Identity Exposure 在一定次数的登录尝试失败后会锁定该帐户。 • **已禁用** – Tenable Identity Exposure 在登录尝试失败后不会锁定该帐户。	已启用
锁定持续时间	Tenable Identity Exposure 锁定帐户并阻止其任何登录尝试的持续时间。在此时间过后，Tenable Identity Exposure 会自动解锁帐户，以允许用户再次尝试登录。 配置锁定持续时间： 1. 点击滑块可设置锁定持续时间。 2. 如果您不想在设定的持续时间后自动解锁帐户，请选择“**无限**”。 **注意**：如果“全局管理员”组内的所有帐户均被锁定，Tenable Identity Exposure 会在 10 秒后解锁默认管理帐户。	300 秒
锁定前的尝试次数	Tenable Identity Exposure 锁定帐户之前失败的登录尝试次数。	3
密码尝试期	在此期间，Tenable Identity Exposure 会计算失败登录尝试次数。在达到指定的登录尝试失败次数后，Tenable Identity Exposure 将锁定帐户。 设置密码尝试期的步骤： 1. 点击滑块，设置时间区间的长度。 2. 如果您不想设置在 Tenable Identity Exposure 锁定帐户之前计算不成功的登录尝试次数的时间区间，请选择“无限”。	900 秒

6. 单击“**保存**”。

禁用锁定策略的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”。

   此时会出现配置窗格。

2. 点击“**已启用**”切换开关以关闭锁定策略。

注意：如果禁用锁定策略，锁定的用户帐户可尝试重新连接。

查看锁定的帐户列表的步骤：

- 在 Tenable Identity Exposure 中，前往“**帐户**”>“**用户帐户管理**”。

  在用户列表中，Tenable Identity Exposure 显示带有红色挂锁图标的锁定帐户。Tenable Identity Exposure 向拥有锁定帐户的用户显示以下消息：“由于身份验证尝试失败次数过多，您的帐户被锁定。您必须联系管理员。”

解锁帐户的步骤：

您必须具有编辑用户的权限才能解锁帐户。

1. 在 Tenable Identity Exposure 中，点击“**帐户**”>“**用户帐户管理**”。

   此时会出现用户帐户管理窗格。

2. 在用户列表中，找到锁定的帐户。

3. 点击笔形图标可编辑锁定的用户帐户。

   此时会出现用户的信息窗格。

4. 点击“**解除锁定**”按钮。

向用户角色授予配置锁定策略的权限的步骤：

1. 在 Tenable Identity Exposure 中，点击“**帐户**”>“**角色管理**”。

   此时会出现“**角色管理**”窗格。

2. 点击角色名称旁的笔形图标可编辑该角色。

此时会出现“**编辑角色**”窗格。

3. 点击“**系统配置实体**”选项卡。
4. 在“**权限管理**”部分下，选中“**帐户锁定策略**”复选框。
5. 点击切换开关，切换至“**未授权**”或“**已授予**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新用户的权限。

   注意：Tenable Identity Exposure 对在此窗格中仅具有读取权限的用户禁用锁定策略设置。

使用 LDAP 进行身份验证

Tenable Identity Exposure 让您可以使用轻型目录访问协议 (LDAP) 进行身份验证。

要启用 LDAP 身份验证，您必须准备以下内容：

- 预配置的服务帐户，并且其用户名和密码可用于访问 Active Directory。
- 预配置的 Active Directory 组。

设置 LDAP 身份验证后，LDAP 选项会显示在登录页面的选项卡中。

配置 LDAP 身份验证的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”。

   此时会出现配置窗格。

2. 在“**身份验证**”部分下，点击“**LDAP**”。
3. 点击“**启用 LDAP 身份验证**”，切换至已启用状态。

   此时会出现一个 LDAP 信息表单。

4. 提供以下信息：

   - 在“**LDAP 服务器地址**”框中，键入以“`ldap://`”开头并以域名和端口号结尾的 LDAP 服务器 IP 地址。

     > **注意**：如果使用 LDAPS 服务器，请键入以“`ldaps://`”开头并以域名和端口号结尾的地址。请参阅 为 LDAPS 添加自定义受信任证书颁发机构 (CA) 证书的步骤： 步骤以完成 LDAPS 的配置。

   - 在“**用于查询 LDAP 服务器的服务帐户**”框中，键入用于访问 LDAP 服务器的标识名 (DN)、SamAccountName 或 UserPrincipalName。
   - 在“**服务帐户密码**”框中，键入此服务帐户的密码。
   - 在“**LDAP 搜索库**”框中，键入 Tenable Identity Exposure 用于搜索尝试连接的用户的 LDAP 目录，以“DC=”或“OU=”开头。这可以是根目录或特定的组织单位。
   - 在“**LDAP 搜索过滤器**”框中，键入 Tenable Identity Exposure 用于过滤用户的属

性。Active Directory 中用于身份验证的标准属性为 `samaccountname={{login}}`。登录的值是用户在身份验证期间提供的值。

5. 对于“**启用 SASL 绑定**”，执行下列操作之一：
   - 如果您为服务帐户使用 SamAccountName，请点击“**启用 SASL 绑定**”，切换至已启用状态。
   - 如果使用服务帐户的标识名或 UserPrincipalName，请将“**启用 SASL 绑定**”保持在已禁用状态。
6. 在“**默认配置文件和角色**”部分下，点击“**添加 LDAP 组**”，以便指定允许身份验证的组。

   此时会出现一个 LDAP 组信息表单。
   - 在“**LDAP 组名称**”框中，键入组的可分辨名称（例如：`CN=TAD_User,OU=Groups,DC=Tenable,DC=ad`）
   - 在“**默认配置文件**”下拉框中，为允许的组选择配置文件。
   - 在“**默认角色**”框中，为允许的组选择角色。
7. 如有必要，点击 ⊕ 图标，添加新的允许的组。
8. 单击“**保存**”。

为 LDAPS 添加自定义受信任证书颁发机构 (CA) 证书的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”。
2. 点击“**配置**”选项卡以显示配置窗格。
3. 在“**应用程序服务**”部分下，点击“**受信任的证书颁发机构**”。
4. 在“**其他 CA 证书**”框中，粘贴要供 Tenable Identity Exposure 使用的您公司的 PEM 编码可信 CA 证书。
5. 单击“**保存**”。

有关安全配置文件和角色的更多信息，请参阅：

- 安全配置文件
- 用户角色

使用 SAML 进行身份验证

您可以配置 SAML 身份验证，以便 Tenable Identity Exposure 用户在登录 Tenable Identity Exposure 时可以使用身份验证提供商发起的单点登录 (SSO)。

开始之前：

- 查看“Tenable SAML 配置快速参考”指南，了解有关如何配置 SAML 以与 Tenable Identity Exposure 一起使用的分步指南。
- 检查身份验证提供商 (IDP) 是否满足以下条件：
  - 仅限 SAML v2。
  - 已启用“断言加密”。
  - 具备 Tenable Identity Exposure 用于在 Tenable Identity Exposure Web 门户中授予访问权限的 IDP 组。
  - 拥有 SAML 服务器的 URL。
  - 以 PEM 编码格式签署 SAML 服务器证书的受信任证书颁发机构 (CA)，以“`-----BEGIN CERTIFICATE -----`”开头，以“`-----END CERTIFICATE -----`”结尾。

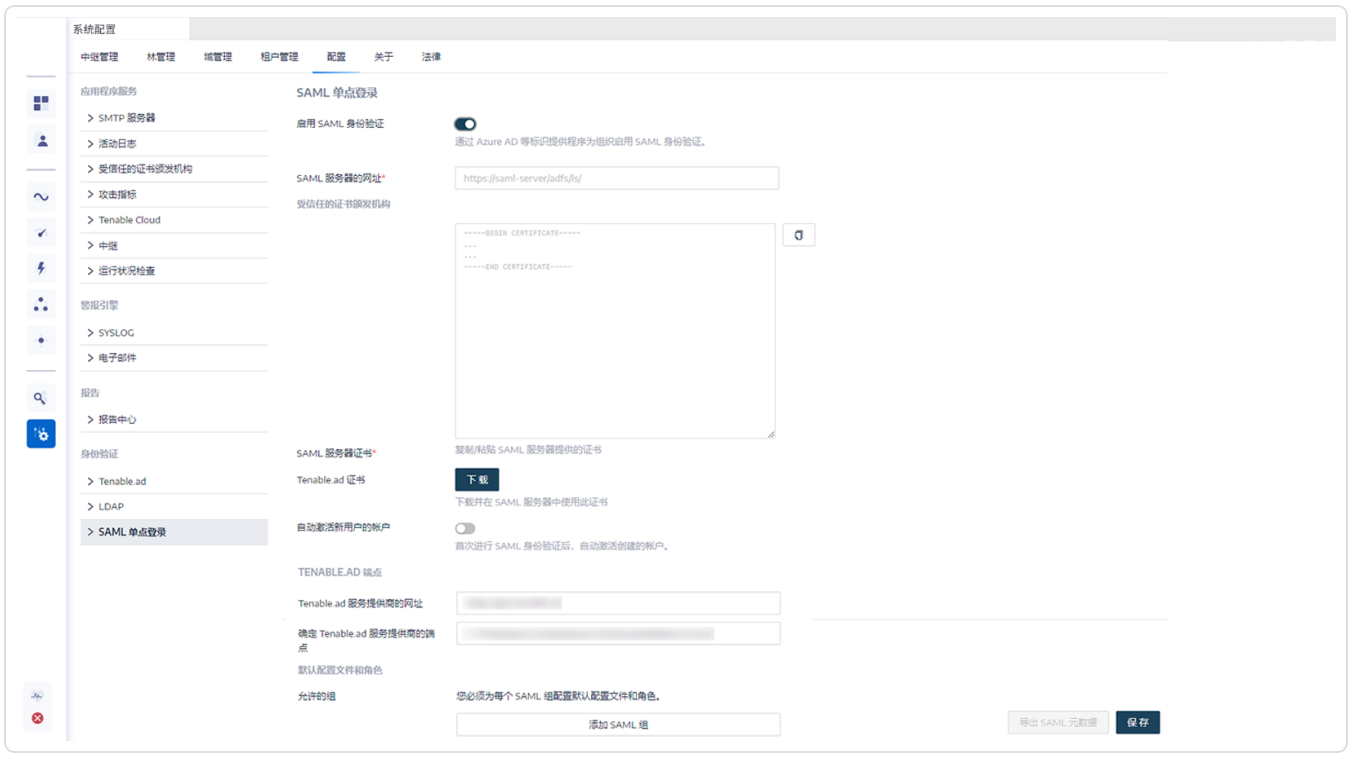
配置 SAML 身份验证的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”，

   此时会出现配置窗格。

2. 在“**身份验证**”部分下，点击“**SAML 单点登录**”。
3. 点击“**启用 SAML 身份验证**”切换开关。

   此时会出现一个 SAML 信息表单。



4. 提供以下信息：

   - 在“**SAML 服务器的 URL**”框中，输入 Tenable Identity Exposure 必须连接的 IDP SAML 服务器的完整 URL。
   - 在“**受信任的证书颁发机构**”框中，粘贴从 SAML 服务器签署证书的 CA。

5. 在“**Tenable Identity Exposure 证书**”框中，单击“**生成并下载**”。这会生成新的自签名证书、更新数据库中的 SAML 配置，并返回新证书以供下载。

   注意：当您单击此按钮时，它会中断 SAML 配置，因为 Tenable Identity Exposure 预期 IDP 会在 IDP 仍在使用以前的证书（如果存在）时立即使用最近生成的证书进行认证。如果生成新的 Tenable Identity Exposure 证书，则必须重新配置 IDP 以使用新证书。

6. 在首次登录 SAML 后，点击“**自动激活新用户帐户**”切换开关来激活新用户帐户。

7. 在 **Tenable Identity Exposure 端点**下，提供以下信息：

   - Tenable Identity Exposure 服务提供商的网址
   - 确定 Tenable Identity Exposure 服务提供商的端点

8. 在“**默认配置文件和角色**”部分下，点击“**添加 SAML 组**”，以便指定允许身份验证的组。

   此时会出现一个 SAML 组信息表单。

9. 提供以下信息：

   - 在“**SAML 组名**”框中，输入在 SAML 服务器中显示的允许的组的名称。
   - 在“**默认配置文件**”下拉框中，为允许的组选择配置文件。
   - 在“**默认角色**”框中，为允许的组选择角色。

10. 如有必要，点击 ⊕ 图标，添加新的允许的组。
11. 单击“**保存**”。

    设置 SAML 身份验证后，SAML 选项会显示在登录页面的选项卡中。

有关安全配置文件和角色的更多信息，请参阅：

- 安全配置文件
- 用户角色

用户帐户

“**用户帐户管理**”页面提供添加、编辑、删除或查看 Tenable Identity Exposure 用户帐户详细信息的功能。

用户有两类:

- 全局管理员 - 拥有所有权限的管理员角色。
- 用户 - 仅对业务数据具有只读权限的简单用户角色。

有关更多信息,请参阅:

- 创建用户
- 编辑用户
- 停用用户
- 删除用户

创建用户

所需用户角色：具有适当权限的管理员或组织用户。

注意：以下说明适用于 Tenable Identity Exposure 的独立实例。对于链接到 Tenable Vulnerability Management 的实例，您在 Tenable Vulnerability Management 中创建用户随后会传播至 Tenable Identity Exposure。

创建用户的步骤：

1. 在 Tenable Identity Exposure 中，点击“**帐户**”>“**用户帐户管理**”。

   此时会出现“**用户帐户管理**”窗格。

2. 点击右侧的“**创建用户**”按钮。

   此时会出现“**创建用户**”窗格。

3. 在“**主要信息**”部分下，输入关于用户的以下信息：

   - 名字
   - 姓名
   - 电子邮件
   - 密码：至少需要 12 个字符，且至少包含：1 个小写字母、1 个大写字母、1 个数字和 1 个特殊字符
   - 密码确认
   - 部门
   - 档案

4. 点击切换开关“**允许身份验证**”以激活用户。

5. 在“**角色管理**”部分下，选择要应用到用户的角色。

6. 点击“**创建**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已创建具有所选角色的用户。

另请参阅：

- 编辑用户
- 停用用户
- 删除用户

编辑用户

所需用户角色:具有适当权限的管理员或组织用户。

编辑用户的步骤:

1. 在 Tenable Identity Exposure 中,点击"**帐户**">"**用户帐户管理**"。

   此时会出现"**用户帐户管理**"窗格。

2. 在用户列表中,将鼠标悬停在显示用户名的行上,然后点击该行末尾的 ✎ 图标。

   此时会出现"**编辑用户**"窗格。

3. 在"**主要信息**"部分下,根据需要修改关于用户的以下信息:

   - 名字
   - 姓名
   - 电子邮件
   - 密码:至少需要 8 个字符
   - 密码确认
   - 部门
   - 档案

4. 在"**角色管理**"部分下,根据需要修改用户的角色。

5. 单击"**编辑**"。

   此时会出现一条消息,确认 Tenable Identity Exposure 更新了具有所选角色的用户。

另请参阅:

- 创建用户
- 停用用户
- 删除用户

停用用户

所需用户角色:具有适当权限的管理员或组织用户。

停用用户的步骤:

1. 在 Tenable Identity Exposure 中,点击"**帐户**">"**用户帐户管理**"。

   此时会出现"**用户帐户管理**"窗格。

2. 在用户列表中,将鼠标悬停在显示用户名的行上,然后点击该行末尾的 图标。

   此时会出现"**编辑用户**"窗格。

3. 点击切换开关"**允许身份验证**"以停用用户。

4. 单击"**编辑**"。

   此时会出现一条消息,确认 Tenable Identity Exposure 已更新用户。

另请参阅:

- 创建用户
- 编辑用户
- 删除用户

删除用户

所需用户角色:具有适当权限的管理员或组织用户。

若要删除用户,请执行以下操作:

1. 在 Tenable Identity Exposure 中,点击"**帐户**">"**用户帐户管理**"。

   此时会出现"**用户帐户管理**"窗格。

2. 在用户列表中,将鼠标悬停在显示要删除的用户名所在行上,然后点击该行末尾的 图标。

   此时会显示一条消息,要求您确认删除。

3. 点击"**删除**"。

   此时会出现一条消息,确认 Tenable Identity Exposure 已删除该用户。

另请参阅:

- 创建用户
- 编辑用户
- 停用用户

安全配置文件

所需用户角色:具有适当权限的管理员或组织用户。

配置文件可让您创建和定制影响 Active Directory 的风险视图。

每个配置文件都显示专门为使用该配置文件的用户配置的风险暴露和攻击情况。例如,IT 管理员的数据分析总体视图可能与安全团队的不同,后者显示 AD 基础设施面临的所有风险的综合视图。

应用安全配置文件后,不同类型的用户可以从该安全配置文件的指标定义的不同报告角度查看数据分析。

通过"安全配置文件管理"窗格,您可以维护可从不同报告角度查看安全分析的不同类型的用户。您可以通过安全配置文件定制风险暴露指标和攻击指标的行为。

注意:Tenable Identity Exposure 提供名为"Tenable"的默认安全配置文件。**您无法修改或删除 Tenable 配置文件**,但您可以将其用作模板,根据需要创建具有调整后设置的其他安全配置文件。

创建新安全配置文件的步骤:

1. 在 Tenable Identity Exposure 中,点击"**帐户**">"**安全配置文件管理**"。

   此时会出现"**安全配置文件管理**"窗格。

2. 点击右侧的"**创建配置文件**"按钮。

   此时会出现"**创建配置文件**"窗格。

3. 从"操作"下拉框中,您可以执行以下操作之一:

   - **创建新的配置文件**。
   - **复制**可用于创建新配置文件的现有安全配置文件。(例如"Tenable"配置文件)

4. 在"**新配置文件的名称**"框中,输入新配置文件的名称。

   注意: Tenable Identity Exposure仅接受字母数字字符和下划线。

5. 点击右下角的"**创建**"按钮。

此时会出现一条消息，显示 Tenable Identity Exposure 已创建配置文件。此时会出现“**配置文件配置**”窗格。

删除安全配置文件的步骤：

1. 在 Tenable Identity Exposure 中，点击“**帐户**”>“**安全配置文件管理**”。

   此时会出现“**安全配置文件管理**”窗格。

2. 在安全配置文件列表中，将鼠标悬停在要删除的安全配置文件上，然后点击该行末尾的 图标。

   此时会显示一条消息，要求您确认删除。

3. 单击“**删除**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已删除配置文件。

后续操作

要完成配置文件的创建，请参阅 定制指标 了解更多信息。

有关更多信息，请参阅：

- 定制指标
- 完善指标的定制

定制指标

所需用户角色:具有适当权限的管理员或组织用户。

您可以为安全配置文件定制风险暴露指标和攻击指标。

每个安全配置文件均独立运行,以确保一个配置文件不会影响另一个配置文件的结果。您应该仅使用"Tenable"配置文件作为参考,因为您无法定制该文件或使用该文件来将异常情况列入白名单。您必须创建专属的定制配置文件以满足特定要求。

"指标定制"窗格上的术语"全局定制"**适用于所有域**而不是所有配置文件。因此,应用于一个安全配置文件的"全局定制"的任何设置都不会影响"Tenable"配置文件或另一配置文件。

提示:如要查看"Tenable"安全配置文件的设置,请单击该行末尾的 图标。

若要定制指标,请执行以下操作:

1. 在 Tenable Identity Exposure 中,点击"**帐户**">"**安全配置文件管理**"。

   此时会出现"**安全配置文件管理**"窗格。

2. 在安全配置文件列表中,将鼠标悬停在包含要定制的指标的安全配置文件上。点击显示安全配置文件名称的行末尾的 图标。

   此时会出现"**配置文件配置**"窗格。

3. 选择"**风险暴露指标**"或"**攻击指标**"选项卡。

4. (可选)在"**搜索指标**"框中,输入指标名称。

5. 点击要定制的指标的名称。

   出现"**指标定制**"窗格。

6. 对指标进行必要的定制操作。

   注意:某些指标选项需要使用正则表达式 (Regex)。正则表达式为"包含"匹配项,不是"相等"匹配项。示例:当提供"`admin`"作为输入选项时,可以将具有"`samAccountName=admin`"的用户以及具有"`samAccountName=admintoto`"的用户列入白名单。
   - 要获得完全匹配,必须使用 Regex 特殊字符 ("`^...$`") 语法。
   - 使用 Regex 时,还必须使用反斜线对特殊字符进行转义。示例:若要声明"`domain\user`"和

CN=Vincent C (Test),DC=tenable,DC=corp”，请输入“domain\\user" and "CN=Vincent C. (Test\),DC=tenable,DC=corp”。

7. 点击“**另存为草稿**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已保存定制选项。

应用定制选项的步骤：

1. 您可以执行以下操作之一：

   - 在“**配置文件配置**”窗格中，点击右下角的“**应用待定定制**”，或
   - 在“**安全配置文件管理**”窗格中，点击显示安全配置文件名称的行末尾的 ✓ 图标。

   此时会显示一条消息，警告您应用定制后，系统会擦除其所有数据，并且需要对受监控的 Active Directory 进行完整分析，这可能需要一些时间。

2. 点击“**确定**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已应用定制选项。在“**安全配置文件管理**”表的“*安全分析*”列中，**正在等待**表示正在等待根据安全配置文件进行分析。

弃用定制选项的步骤：

- 您可以执行以下操作之一：
  - 在“**配置文件配置**”窗格中，点击左下角的“**还原待定定制**”，或
  - 在“**安全配置文件管理**”窗格中，点击显示安全配置文件名称的行末尾的 ↶ 图标。

  此时会出现一条消息，确认 Tenable Identity Exposure 已取消定制选项。

另请参阅：

- 完善指标的定制

完善指标的定制

所需用户角色:具有适当权限的管理员或组织用户。

您可以通过对安全配置文件的指标进行更多定制来为特定域选择指标选项。默认情况下,全局定制适用于所有域。

完善指标定制的步骤:

1. 在 Tenable Identity Exposure 中,点击"**帐户**">"**安全配置文件管理**"。

   此时会出现"**安全配置文件管理**"窗格。

2. 在安全配置文件列表中,将鼠标悬停在包含要定制的指标的安全配置文件上。点击显示安全配置文件名称的行末尾的 图标。

   此时会出现"**配置文件配置**"窗格。

3. 选择"**风险暴露指标**"或"**攻击指标**"选项卡。

4. (可选)在"**搜索指标**"框中,输入指标名称。

5. 点击要定制的指标的名称。

   出现"**指标定制**"窗格。

6. 在"**全局定制**"选项卡旁,点击 + 图标。

   此时会出现"**定制编号 1**"选项卡。

7. 点击"**应用于**"框。

   出现"**林和域**"窗格。

8. (可选)在搜索框中,键入林或域名。

9. 选择域。

10. 单击"**按所选结果筛选**"。

11. 根据需要对所选域的指标进行进一步定制。

12. 点击"**另存为草稿**"。

弃用完善定制选项的步骤：

1. 点击用于定制的选项卡。
2. 点击窗格底部的“**删除此配置**”。

另请参阅：

- 定制指标

用户角色

Tenable Identity Exposure 使用基于角色的访问控制 (RBAC) 来保护对其数据的访问权限以及您组织内的功能。角色确定用户可根据其角色从其帐户访问的信息类型。

具有适当权限的用户可根据其角色将权限分配给其他用户，以执行以下操作：

- 读取内容和菜单、系统以及风险暴露指标配置。
- 读取内容和菜单、系统以及攻击指标配置。
- 创建帐户、安全配置文件和角色。

另请参阅：

- 管理角色
- 设置角色的权限
- 设置用户界面实体的权限（示例）

管理角色

创建新角色的步骤：

1. 在 Tenable Identity Exposure 中，前往“**帐户**”>“**角色管理**”。
2. 点击右上角的“**创建角色**”按钮。

   此时会出现“**创建角色**”窗格。
3. 在“名称”框中，键入角色的名称。
4. 在“描述”框中，键入有关该角色的一些信息。
5. 点击右下角的“**添加**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已创建该角色。系统还会显示“**编辑角色**”窗格，您可以在其中设置该角色的权限。

注意：您不能修改 Tenable Identity Exposure 管理员角色（称为全局管理员）。点击 👁 图标可显示 Tenable Identity Exposure 角色设置。

删除角色的步骤：

1. 在 Tenable Identity Exposure 中，前往“**帐户**”>“**角色管理**”。
2. 在角色列表中，将鼠标悬停在要删除的角色上，然后点击右侧的 🗑 图标。

   此时会显示一条消息，要求您确认删除。
3. 点击“删除”。

   此时会出现一条消息，确认角色已删除。

另请参阅：

- 设置角色的权限

设置角色的权限

所需用户角色:具有适当权限的管理员或组织用户。

Tenable Identity Exposure 使用基于角色的访问控制 (RBAC) 来保护对其数据的访问权限。角色根据用户在组织中的功能角色来确定用户可以访问的信息类型。当您在 Tenable Identity Exposure 中创建新用户时,您将为该用户分配一个具有相关权限的特定角色。

设置角色权限的步骤:

1. 在 Tenable Identity Exposure 中,点击"**帐户**">"**角色管理**"。
2. 将鼠标悬停在要设置权限的角色上,然后点击右侧的 图标。

   此时会出现"**编辑角色**"窗格。
3. 在"**权限管理**"下,选择实体类型:
   - 数据实体
   - 用户实体
   - 系统配置实体
   - 界面实体
4. 在实体名称列表中,选择要设置权限的实体。
5. 在"**读取**"、"**编辑**"或"**创建**"列下,点击切换开关,切换至"已授予"或"未授权"。
6. 您可以执行以下操作之一:
   - 点击"应用"以应用权限,并保持"**编辑角色**"窗格打开,以进行进一步修改。
   - 点击"应用并关闭"以应用权限并关闭"**编辑角色**"窗格。

   此时会出现一条消息,确认 Tenable Identity Exposure 已更新角色。

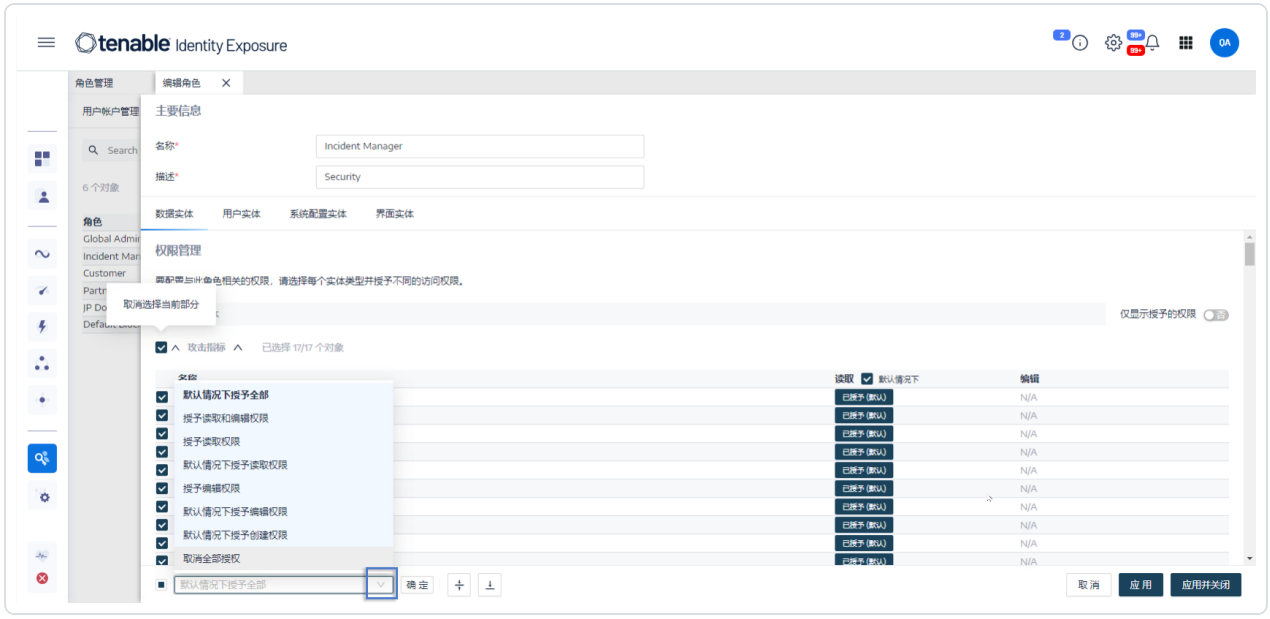
批量设置角色权限的步骤:

1. 在 Tenable Identity Exposure 中,点击"**帐户**">"**角色管理**"。
2. 将鼠标悬停在要设置权限的角色上,然后点击右侧的 图标。

   此时会出现"**编辑角色**"窗格。

3. 在“**权限管理**”下，选择实体类型。
4. 选择要对其设置权限的实体或实体部分（例如风险暴露指标）。
5. 在页面底部，点击下拉框上的箭头以显示权限列表。
6. 选择角色的权限。
7. 点击“**确定**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已设置实体上的权限。



权限类型

权限	描述
读取	查看对象或配置的权限。
编辑	修改对象或配置的权限。需要具备读取权限才能应用修改。
创建	创建对象或配置的权限。“**创建**”权限需要具备“**读取**”和“**编辑**”权限，才能对允许的资源执行允许的操作。

实体类型

Tenable Identity Exposure 中有四种类型的实体需要访问权限，您可以针对组织中的每个用户角色进行定制：

实体类型	包含	权限
数据实体		
此实体控制在 Tenable Identity Exposure 中设置受监控的 Active Directory 和配置数据分析的权限。	• 攻击指标 • 风险暴露指标 • 林 • 域 • 配置文件 • 用户 • 电子邮件发出的警报 • SYSLOG 发出的警报 • 角色 • 实体中继 • 报告	读取、编辑、创建
用户实体		
此实体控制用户配置 Tenable Identity Exposure 显示的信息以进行数据分析以及修改个人信息和首选项的能力。	• 首选项 • 仪表盘 • 小组件 • API 密钥 • 个人信息	编辑、创建
系统配置实体		
此实体控制对 Tenable Identity Exposure 平台和服务的访问权限。	• 应用程序服务(SMTP、日志、身份验证 Tenable Identity Exposure、攻击指标、受信任的证书颁发机构) • 通过公共 API 得到的分数	读取、编辑

	• 许可证 • LDAP 身份验证 • SAML 身份验证 **注意**：如果您拥有 Tenable Vulnerability Management 许可证，则 LDAP 和 SAML 身份验证的权限不可用。 • 拓扑 • 帐户锁定策略 • 重新抓取多个域 • 活动日志 • Tenable 云服务 (Tenable Cloud 数据收集) • Microsoft Entra ID 支持 • 运行状况检查 • 仅显示用户自己的跟踪信息	
界面实体		
此实体定义访问 Tenable Identity Exposure 用户界面和功能的特定部分的权限。	特定 Tenable Identity Exposure 功能的访问路径。有关更多信息，请参阅设置用户界面实体的权限(示例)	已授予、未授权

另请参阅：

- 用户帐户
- 用户角色

设置用户界面实体的权限(示例)

Tenable Identity Exposure 沿着用于访问特定用户界面功能的路径来应用权限。以下示例显示如何设置权限以允许配置 SYSLOG。

要访问 SYSLOG 参数,用户需要访问 Tenable Identity Exposure 中路径"**系统**">"**配置**">"**SYSLOG**"的权限:

- 系统配置:**管理** > **系统**
- 配置参数:**管理** > **系统** > **配置**
- SYSLOG 警报:**管理** > **系统** > **配置** > **警报引擎** > **SYSLOG**

设置 SYSLOG 配置的权限:

1. 在 Tenable Identity Exposure 中,点击"**帐户**">"**角色管理**"。
2. 将鼠标悬停在要设置权限的角色上,然后点击右侧的 图标。

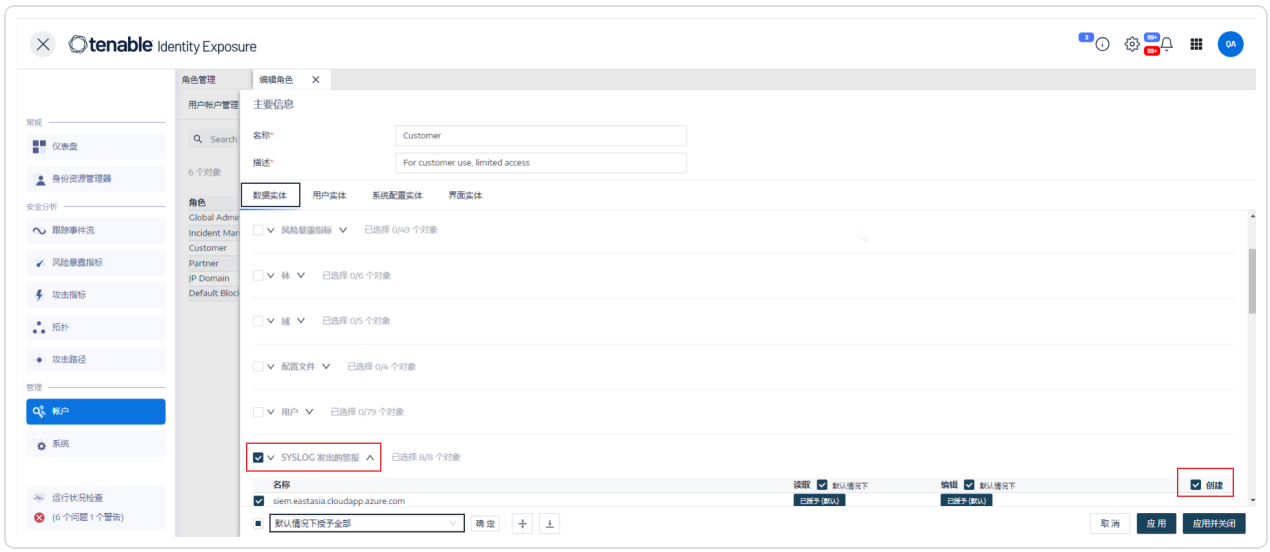
   此时会出现"**编辑角色**"窗格。
3. 在"**权限管理**"下,选择"**界面实体**"。
4. 在实体列表中,执行以下操作:
   - 选择"**管理**">"**系统**",并点击"访问"切换开关,切换至"**已授予**"。
   - 选择"**管理**">"**系统**">"**配置**",并点击"访问"切换开关,切换至**"已授予"**。
   - 选择"**管理**">"**系统**">"**配置**">"**警报引擎**">"**SYSLOG**",并点击"访问"切换开关,切换至**"已授予"**。
5. 点击"**应用**"。

   此时会出现一条消息,确认 Tenable Identity Exposure 已更新实体上的权限。

6. 在“**权限管理**”下，选择“**数据实体**”。
7. 在实体列表中，选择“**SYSLOG 发出的警报**”。
8. 选择“**创建**”（权限）。

   Tenable Identity Exposure 会隐式授予读取和编辑权限。
9. 点击“**应用并关闭**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新实体上的权限。


tenable Identity Exposure
角色管理
用户帐户管理
编辑角色
主要信息
名称*
Customer
描述*
For customer use, limited access
数据实体
用户实体
系统配置实体
界面实体
仪表盘
身份资源管理器
跟踪事件流
风险暴露指标
攻击指标
拓扑
攻击路径
帐户
系统
运行状况检查
(6 个问题 1 个警告)
SYSLOG 发出的警报
已选择 8/8 个对象
名称
siem.eastasia.cloudapp.azure.com
读取
编辑
创建
已授予 (默认)
默认情况下授予全部
确定
取消
应用
应用并关闭

林

Active Directory (AD) 林是共享通用方案、配置和信任关系的域的集合。该林提供用于管理和组织资源的分层结构，可跨组织内的多个域实现集中管理和安全的身份验证。

管理林

若要添加林，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**林管理**”。
2. 点击右侧的“**添加林**”。

   此时会出现“添加林”窗格。
3. 在“**名称**”框中，输入林的名称。
4. 在“**帐户**”部分，为 Tenable Identity Exposure 使用的服务帐户提供以下内容：
   - **登录**：输入服务帐户的名称。
     格式：用户主体名称，例如“`tenablead@domain.example.com`”（推荐此格式，因为其与 Kerberos 身份验证 兼容）；或 NetBIOS，例如“`DomainNetBIOSName\SamAccountName`”。
   - **密码**：输入服务帐户的密码。

   注意：如果您必须将 Tenable Identity Exposure 的 AD 服务帐户设置为 Protected Users 组成员，请确保您的 Tenable Identity Exposure 配置支持 Kerberos 身份验证，因为 Protected Users 无法使用 NTLM 验证。
5. 单击“**添加**”。

   此时会出现一条消息，确认已添加新的林。

编辑林：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**林管理**”。
2. 在林列表中，将鼠标悬停在要修改的林上，然后点击右侧的 ✎ 图标。

   此时会出现“**编辑林**”窗格。
3. 根据需要进行修改。
4. 单击“**编辑**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新林。

保护服务帐户

Tenable 建议保护服务帐户来维护安全性，方法是通过正确设置用户帐户控制 (UAC) 属性来防止委派、要求预身份验证、使用更强的加密、强制使密码过期和强制执行密码要求，以及允许经授权的密码更改。这些措施可降低未经授权访问和潜在安全漏洞的风险，从而确保组织系统和数据的完整性。

若要使用 Windows 策略编辑器修改设置，请执行以下操作：

您可以借助适当的管理权限，使用 Windows 的本地安全策略编辑器或组策略编辑器来修改用户帐户控制设置。

- 在编辑器中，导航到“**本地策略**”->“**安全选项**”，找到并配置以下设置：(设置可能因 Windows 版本而有所不同。)
  - *“网络访问：不允许存储密码和凭据以进行网络认证”*：将其设置为“**已启用**”。
  - *“帐户：不需要 Kerberos 预身份验证”*：并将其设置为“**已禁用**”。
  - *“网络安全：配置 Kerberos 允许的加密类型”*：确保**未**选择*“为此帐户使用 Kerberos DES 加密类型”*选项。
  - *“帐户：密码最长使用期限”*：设置密码到期期限(例如 30 天、60 天或 90 天，以使 “PasswordNeverExpires”属性为 FALSE)。
  - *“帐户：将本地帐户使用空白密码限制为仅限控制台登录”*：将其设置为“**已禁用**”。
  - *“交互式登录：要缓存的以前登录的次数(以防域控制器不可用)”*：设置所需值，例如 “10”，以允许用户更改其密码。

若要使用 Powershell 修改设置，请执行以下操作：

- 在托管 AD 的计算机上，使用适当的管理权限打开 PowerShell 并运行以下命令：

```
Set-ADAccountControl -Identity <AD_ACCOUNT> -AccountNotDelegated $true -UseDESKeyOnly
$false -DoesNotRequirePreAuth $false -PasswordNeverExpires $false -PasswordNotRequired
$false -CannotChangePassword $false
```

“<AD_ACCOUNT>”是您想要修改的 Active Directory 帐户的名称。

域

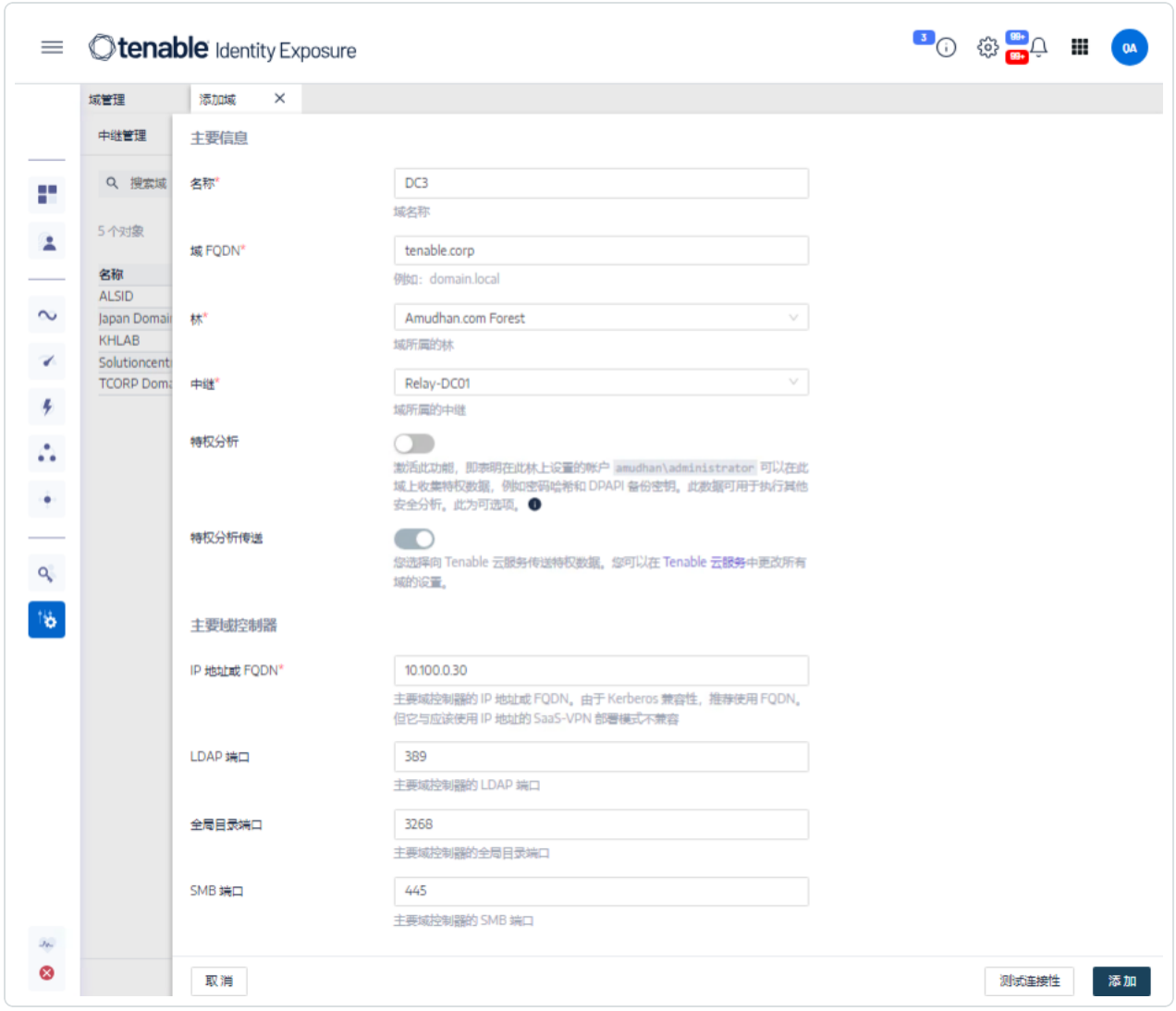
Tenable Identity Exposure 监控某些域，这些域对以一定逻辑方式共享通用设置的对象进行分组以进行集中管理。

添加域的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”。
2. 点击“**域管理**”选项卡。

   此时会出现“**域管理**”窗格。
3. 点击右上角的“**添加域**”。

   此时会出现“**添加域**”窗格。



4. 在“**主要信息**”部分，输入以下信息：
    - 在“**名称**”框中，输入域的名称。
    - 在“**域 FQDN**”框中，输入域的完全限定域名 (FQDN)。
    - 在“**林**”下拉框中，选择域所属的林。
5. **特权分析**（可选）：如果启用此开关，则允许此林中的“dcadmin”帐户收集此域上的特权数据以执行高级安全分析。
6. **特权分析传输**：有关此选项的更多信息，请参阅 Tenable Cloud 数据收集

7. 在“**主要域控制器**”部分，输入以下信息：

   - 在“**IP 地址或主机名**”框中，键入主域控制器的主机名（需要与 Kerberos 身份验证 兼容，但与 SaaS-VPN 部署模式不兼容）或 IP 地址。

     > Tenable Identity Exposure 不支持负载平衡器。

   - 在“**LDAP 端口**”框中，输入主要域控制器的 LDAP 端口。

     > **注意**：如果使用端口 TCP/636（LDAPS）连接域，Tenable Identity Exposure 必须有权访问 Active Directory 的证书颁发机构（CA）证书以验证 AD 证书，从而进行连接。在安全中继环境中，您可以在中继计算机上安装 CA 证书。无法在 VPN 环境中进行此配置。

   - 在“**全局目录端口**”框中，输入主要域控制器的全局目录端口。
   - 在“**SMB 端口**”框中，输入主要域控制器的 SMB 端口。

8. 点击“**添加**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已添加域。

编辑域的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”。
2. 点击“**域管理**”选项卡。

   此时会出现“**域管理**”窗格。

3. 将鼠标悬停在要编辑的域的名称上，以在右侧显示 ✎ 图标。
4. 点击 ✎ 图标。

   此时会出现“**编辑域**”窗格。

5. 编辑域的信息。
6. 单击“**编辑**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新域。

删除域的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”。
2. 点击“**域管理**”选项卡。

   此时会出现“**域管理**”窗格。
3. 将鼠标悬停在要删除的域的名称上，以显示 🗑 图标。
4. 点击 🗑 图标。

   此时会显示一条消息，要求您确认删除。
5. 点击“**删除**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已删除域。

另请参阅：

- 强制在域上执行数据刷新
- Honey Account
- Kerberos 身份验证

强制在域上执行数据刷新

强制在域上执行数据刷新的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”。
2. 点击“**域管理**”选项卡。

   此时会出现“**域管理**”窗格。
3. 将鼠标悬停在要强制执行数据刷新的域的名称上，以在右侧显示 图标。
4. 点击 图标。

   此时会出现一条消息，其中包含有关数据刷新操作的信息。
5. 点击“**确认**”。

另请参阅：

- Honey Account

Honey Account

所需用户角色：本地计算机上的管理员

Honey Account（蜜罐帐户）是一种诱饵帐户，专门用于检测尝试通过 Active Directory 入侵网络的攻击者。

Honey Account 是 Tenable Identity Exposure 的攻击指标检测 Kerberoasting 利用尝试的先决条件。Kerberoasting 通过请求和提取服务票据，然后离线破解服务帐户的凭据来获取对服务帐户的访问权限。当 Honey Account 收到登录尝试或票据请求时，Kerberoasting 攻击指标会发出警报。

您需要为每个域关联一个 Honey Account。Honey Account 与安全配置文件无关。

添加 Honey Account 的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**域管理**”。

   此时会出现“**域管理**”窗格。

2. 将鼠标悬停在要添加 Honey Account 的域上。

3. 在“**Honey Account 配置状态**”下，点击“**+**”。

   此时会出现“**添加 Honey Account**”窗格。

4. 在“**名称**”框中，为用户帐户输入要用作 Honey Account 的标识名 (DN)。

   提示：如果 Active Directory 中已存在该用户帐户，则您可输入任何字符串，Tenable Identity Exposure 会搜索该用户帐户名称并在下拉框中显示相匹配的名称。

5. 在“**部署**”部分，Tenable Identity Exposure 会生成一个具有适当设置的脚本，供您运行以便部署 Honey Account。点击 以复制此脚本。

6. 点击“**添加**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已添加 Honey Account。在“域管理”窗格中，所选域的“**Honey Account 配置状态**”会显示为橙色 (●)，表示您必须运行 Honey Account 部署脚本以将其激活。

注意：如果"**Honey Account 配置状态**"显示为红色 (🔴)，则表示 Tenable Identity Exposure 未在 Active Directory 中找到此用户帐户。您必须创建此用户帐户才能继续进行下一步。

7. 在具有 Active Directory 模块的计算机上的 Windows PowerShell 中，运行您复制的 Honey Account 部署脚本。

   在"**域管理**"窗格中，所选域的"**Honey Account 配置状态**"会显示为绿色 (🟢)，表示该域处于活动状态。

   注意：Tenable Identity Exposure 处理和激活 Honey Account 时可能需要一定时间。

编辑 Honey Account 的步骤：

1. 在 Tenable Identity Exposure 中，点击"**系统**">"**域管理**"。

   此时会出现"**域管理**"窗格。

2. 将鼠标悬停在要添加 Honey Account 的域上。

3. 在"**Honey Account 配置状态**"下，点击右侧的 图标。

   此时会出现"**编辑 Honey Account**"窗格。

4. 在"**名称**"框中，根据需要修改用户帐户。

5. 在"**部署**"部分，点击 以复制 Honey Account 部署脚本。

6. 单击"**编辑**"。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新 Honey Account。在"域管理"窗格中，所选域的"**Honey Account 配置状态**"会显示为橙色 (🟠)，表示您必须运行 Honey Account 部署脚本以将其激活。

   注意：如果"**Honey Account 配置状态**"显示为红色 (🔴)，则表示 Tenable Identity Exposure 未在 Active Directory 中找到此用户帐户。您必须创建此用户帐户才能继续进行下一步。

7. 在具有 Active Directory 模块的计算机上的 Windows PowerShell 中，运行您复制的 Honey Account 部署脚本。

   在"**域管理**"窗格中，所选域的"**Honey Account 配置状态**"会显示为绿色 (🟢)，表示该域已完成配置。

注意：Tenable Identity Exposure 处理和激活 Honey Account 时可能需要一定时间。

删除 Honey Account 的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**域管理**”。

   此时会出现“**域管理**”窗格。

2. 将鼠标悬停在要添加 Honey Account 的域上。

3. 在“**Honey Account 配置状态**”下，点击右侧的 图标。

   此时会出现“**编辑 Honey Account**”窗格。

4. 点击“**删除**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已删除 Honey Account。

另请参阅：

- 强制在域上执行数据刷新

Kerberos 身份验证

Tenable Identity Exposure 使用您提供的凭据向配置的域控制器进行身份验证。这些 DC 接受 NTLM 或 Kerberos 身份验证。NTLM 是一种存在已记录的安全问题的旧协议，Microsoft 和所有网络安全标准现在不鼓励使用。而 Kerberos 则是您应考虑的更可靠的协议。Windows 始终优先尝试 Kerberos，且仅在 Kerberos 不可用的情况下采用 NTLM。

在少数例外情况下，Tenable Identity Exposure 与 NTLM 和 Kerberos 兼容。当 Kerberos 满足所有必要条件时，Tenable Identity Exposure 将其作为首选协议。此部分内容会介绍要求并演示如何配置 Tenable Identity Exposure 以确保使用 Kerberos。

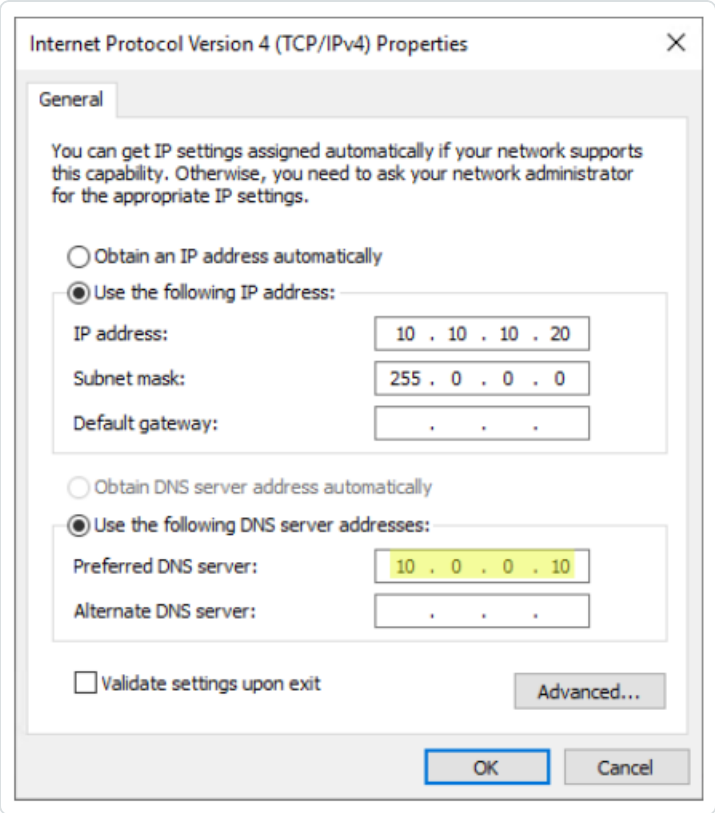
使用 NTLM 而不是 Kerberos 也是 SYSVOL 强化干扰 Tenable Identity Exposure 的原因。有关更多信息，请参阅"SYSVOL 强化干扰 Tenable Identity Exposure"。

与 Tenable Identity Exposure 部署模式的兼容性

部署模式	Kerberos 支持
本地	是
SaaS-TLS(旧版)	是
带 安全中继 的 SaaS	是
带 VPN 的 SaaS	否 - 必须将安装切换到 安全中继 部署模式。

技术要求

- **Tenable Identity Exposure 中配置的 AD 服务帐户必须具有 UserPrincipalName (UPN)**。请参阅 服务帐户和域配置 获取相关说明。
- **DNS 配置和 DNS 服务器必须允许解析所有必要的 DNS 条目** – 您必须将目录侦听器或中继计算机配置为使用知道域控制器的 DNS 服务器。如果目录侦听器或中继计算机已加入域(Tenable Identity Exposure 不建议这样做)，则您应已满足此要求。最简单的方法是将域控制器本身用作首选 DNS 服务器，因为它通常也运行 DNS。例如：



注意：如果目录侦听器或中继计算机连接到多个域，并且可能位于多个林中，请确保配置的 DNS 服务器可以解析所有域的所有必需 DNS 条目。否则，您需要设置多个目录侦听器或中继计算机。

- **Kerberos"服务器"的可访问性 (KDC)** – 这需要通过端口 TCP/88 从目录侦听器或中继到域控制器的网络连接。如果目录侦听器或中继已加入域(Tenable 不建议这样做)，则您应已满足此要求。每个配置的 Tenable Identity Exposure 林都要求 Kerberos 网络与包含服务帐户的相应域中的至少一个域控制器建立连接，并且每个连接的域中都至少有一个域控制器。

  有关要求的更多信息，请参阅"网络流矩阵"和"TLS 网络矩阵"。

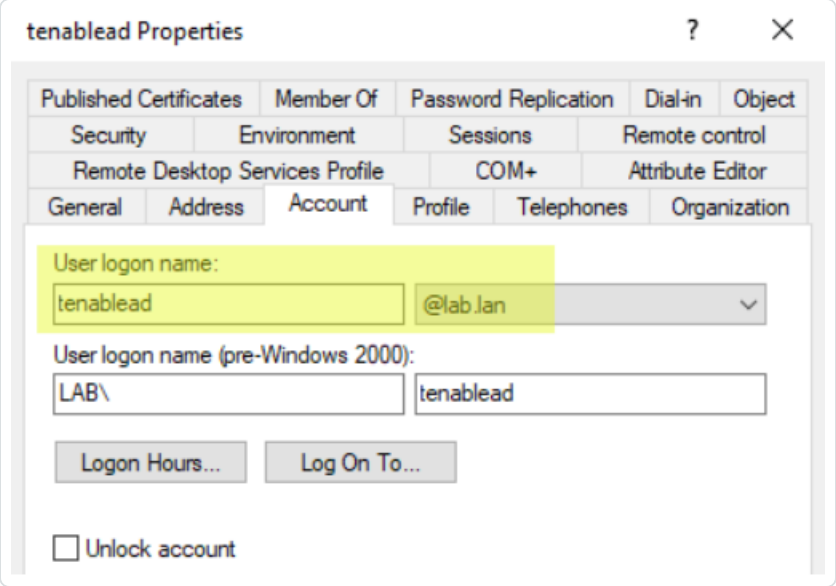
  注意：目录侦听器或中继计算机无需加入域即可使用 Kerberos。

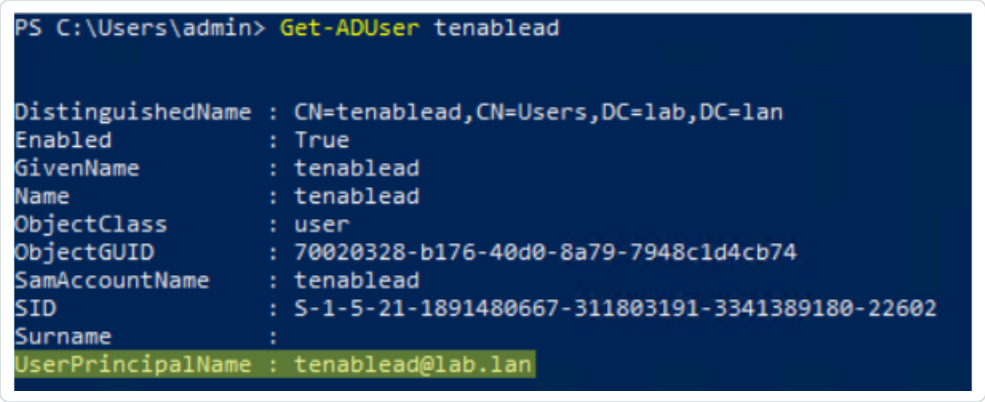
服务帐户和域配置

要在 Tenable Identity Exposure 中配置 AD 服务帐户和 AD 域以使用 Kerberos，请执行以下操作：

1. 使用 User PrincipalName (UPN) 格式登录。在此示例中，UPN 属性为“tenablead@lab.lan”。

    a. 在包含服务帐户的林的域中找到 UPN 属性，如下所示：

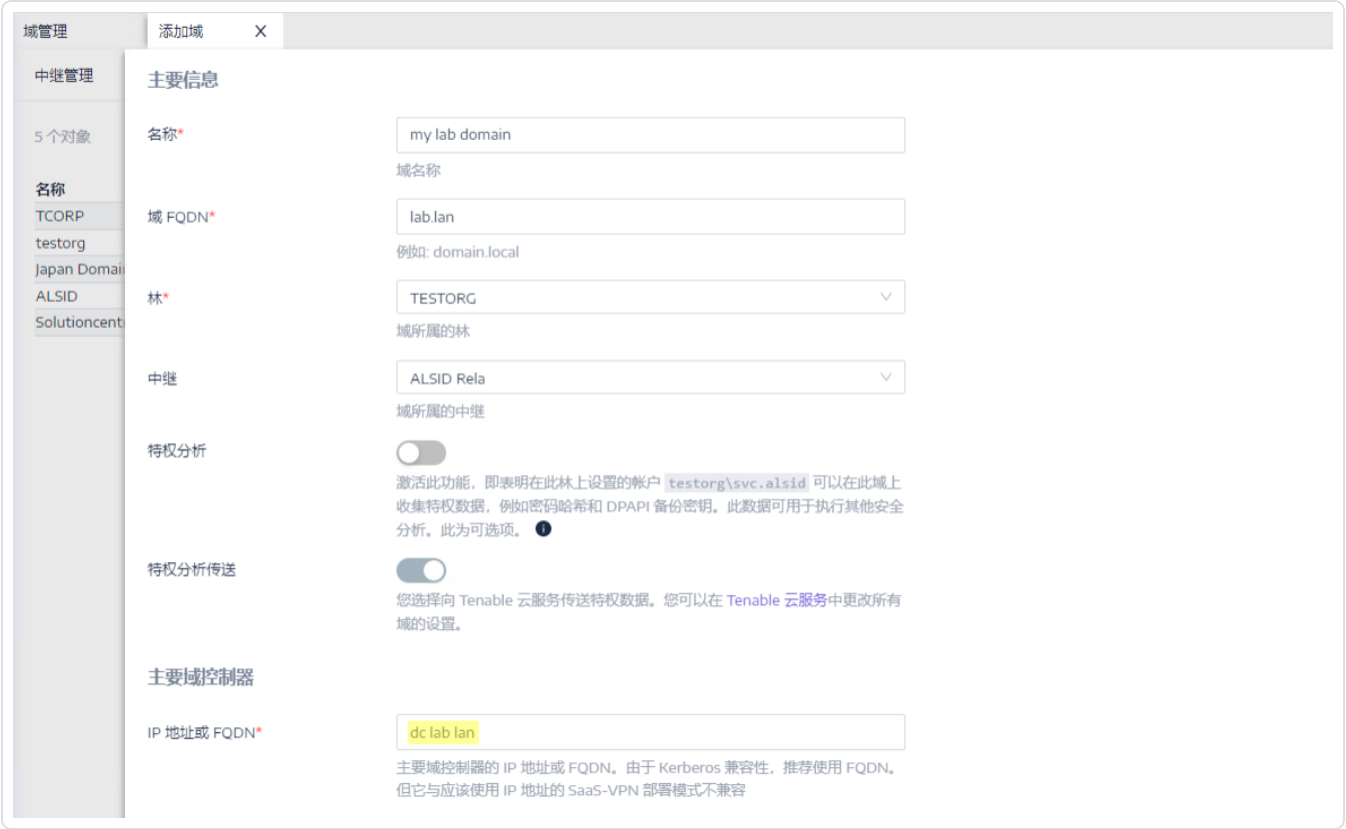




> **注意**：UPN 看起来像电子邮件地址，且经常（但不总是）与用户的电子邮件地址相同。

b. 在 Tenable Identity Exposure 的林配置部分中，设置此 UPN 而非设置短“用户名”格式或 NetBIOS“域/用户名”格式，如下所示：

2. 在 Tenable Identity Exposure 的域配置中使用完全限定域名 (FQDN), 为主域控制器 (PDC) 设置 FQDN, 而不是其 IP。

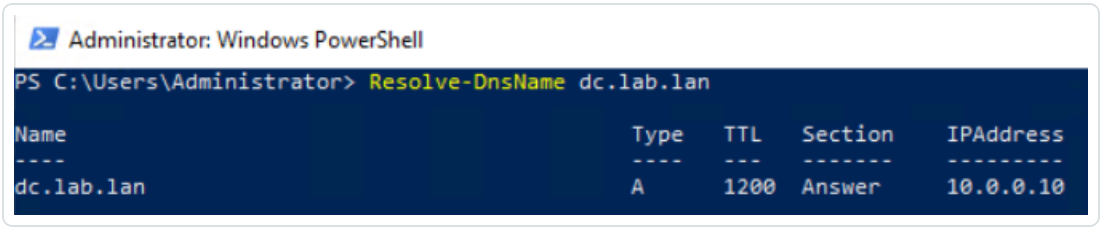


故障排除

Kerberos 需要执行多个配置步骤才能正常工作。否则, Windows 以及扩展程序 Tenable Identity Exposure 会静默转向使用 NTLM 身份验证。

DNS

确保目录侦听器或中继计算机上使用的 DNS 服务器可以解析提供的 PDC FQDN, 例如:



Kerberos

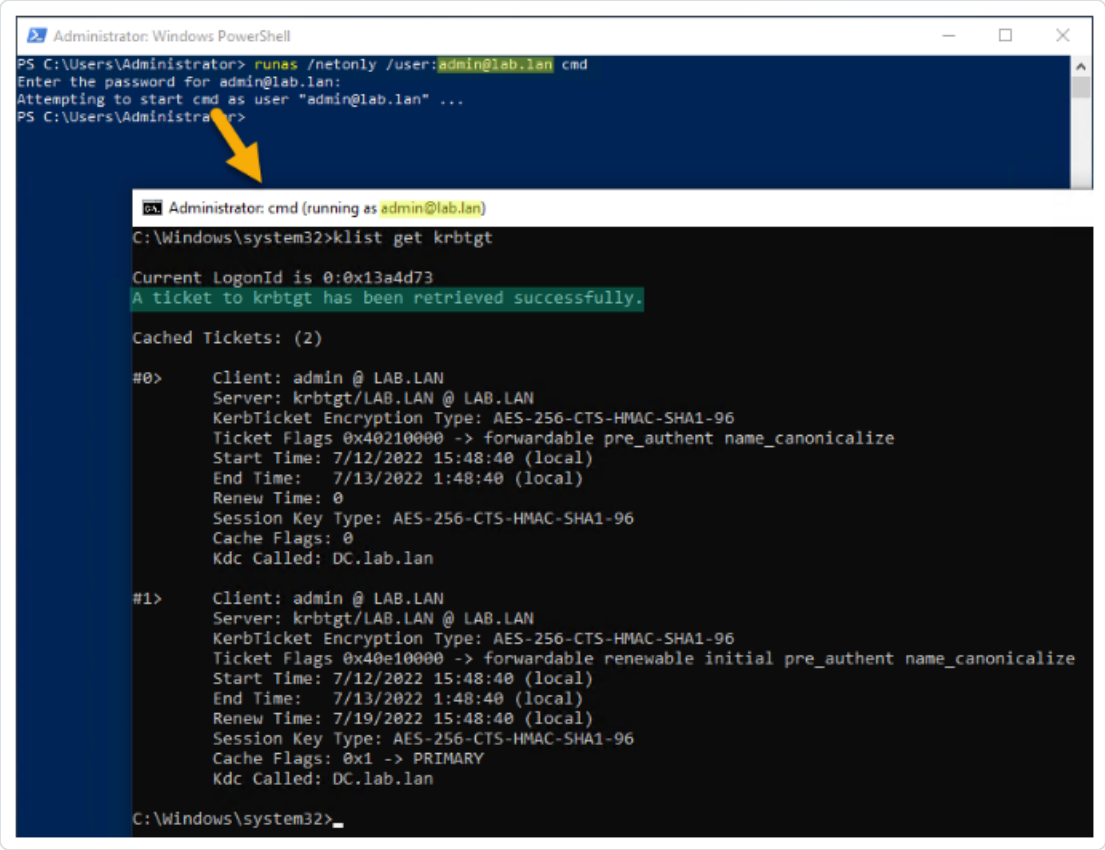
如要验证 Kerberos 是否使用您在目录侦听器或中继计算机上运行的命令，请执行以下操作：

1. 验证 Tenable Identity Exposure 中配置的 AD 服务帐户是否可获得 TGT：

   a. 在命令行或 PowerShell 中，运行“`runas /netonly /user:<UPN> cmd`”，然后输入密码。输入或粘贴密码时要格外小心，因为“`/netonly`”标记可导致无法验证。

   b. 在第二个命令提示中，运行“`klist get krbtgt`”以请求 TGT 票证。

   以下示例显示成功结果：



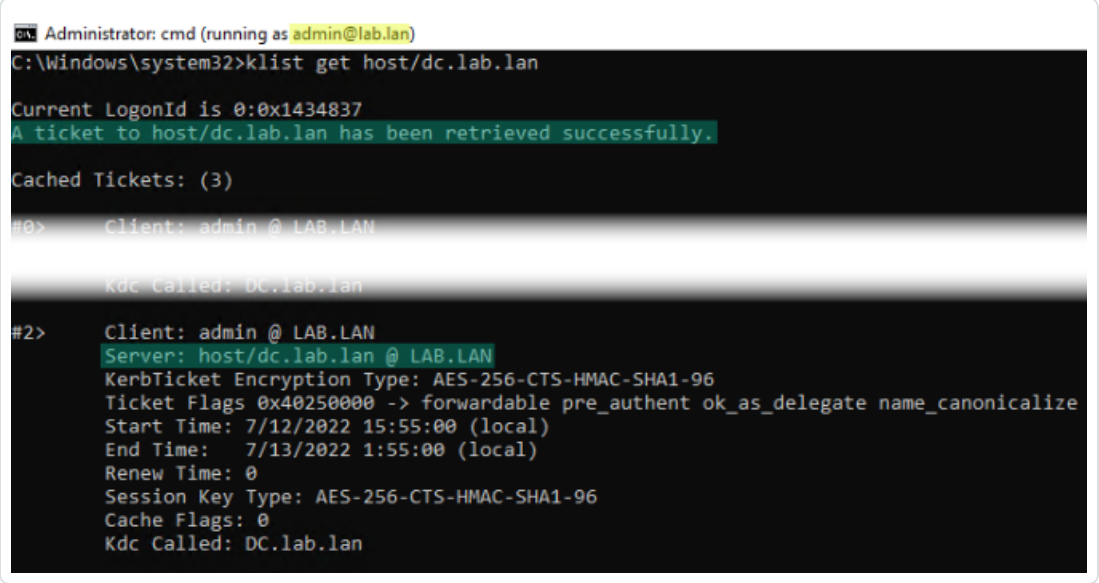
   以下是可能的错误代码：

   - `0xc0000064`:“用户使用拼写错误或错误的用户帐户登录”-> 检查登录信息(即 UPN 中“@”以前的部分)。
   - `0xc000006a`:“用户使用拼写错误或错误的密码登录”-> 检查密码。

- `0xc000005e`:“目前没有可用于登录请求服务的登录服务器。”-> 检查 DNS 解析是否运作，以及服务器是否可以联系返回的 KDC 等。
- 其他错误代码：请参阅与 4625 事件相关的 Microsoft 文档。

2. 验证在 Tenable Identity Exposure 中配置的域控制器是否可以获得服务票证。在相同的第二个命令提示符中，运行“`klist get host/<DC_FQDN>`”（替换“`<DC_FQDN>`”）。

   以下示例显示成功结果：



警报

所需许可证：根据要发送的警报的类型，您可能需要攻击指标或风险暴露指标的许可证。

Tenable Identity Exposure 的警报系统可帮助您识别对受监控 Active Directory 的安全回归和/或攻击。它通过电子邮件或 Syslog 通知实时推送有关漏洞和攻击的分析数据。

- SMTP 服务器配置
- 电子邮件警报
- Syslog 警报
- Syslog 和电子邮件警报详细信息

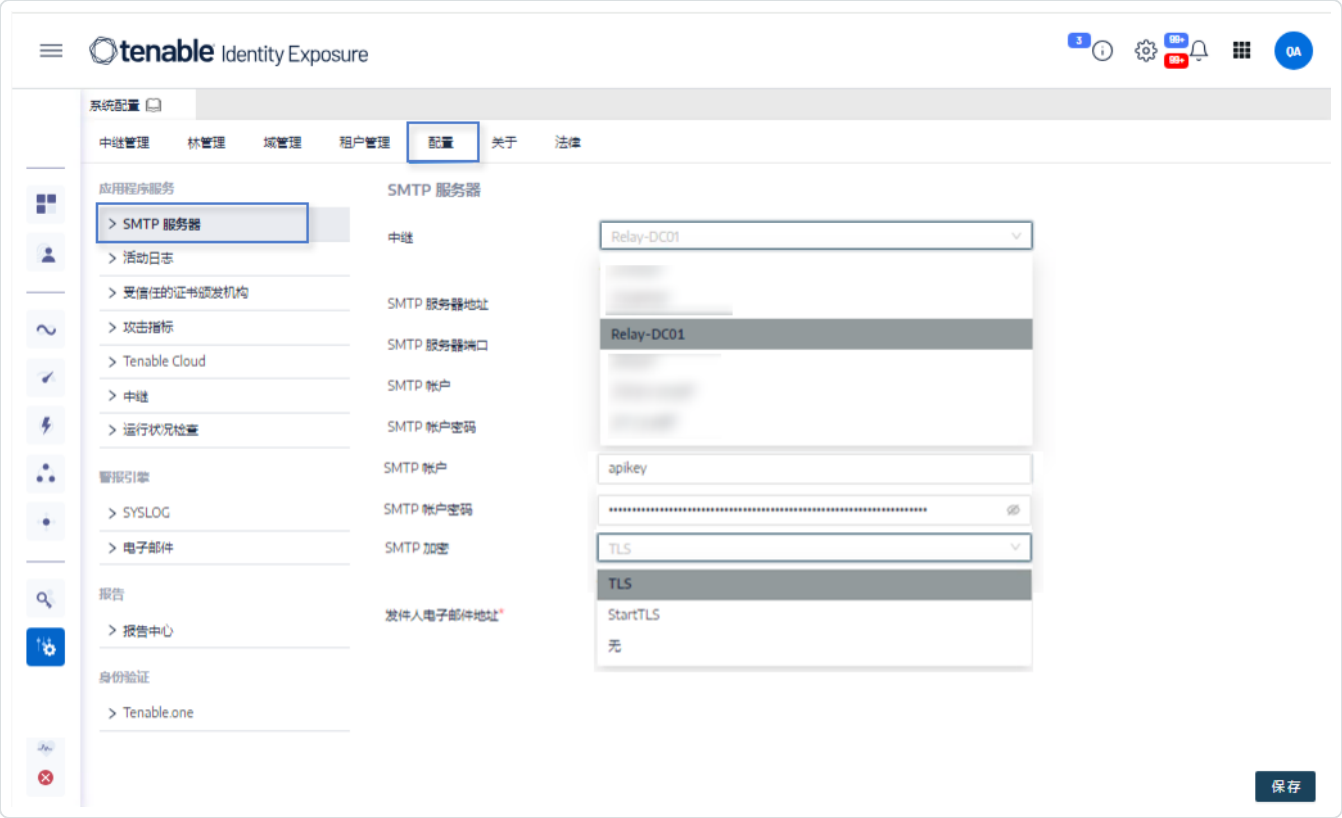
SMTP 服务器配置

Tenable Identity Exposure 需要简单邮件传输协议 (SMTP) 配置才能发出警报通知。

配置 SMTP 服务器的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”。
2. 在“**应用程序服务**”下，选择“**SMTP 服务器**”。

   此时“**SMTP 服务器**”窗格将打开。



3. **如果您的网络使用安全中继：**在“**中继**”框中，点击箭头以从下拉列表中选择一个与 SMTP 服务器进行通信的中继。
4. 提供以下信息：
   - SMTP 服务器地址
   - SMTP 服务器端口

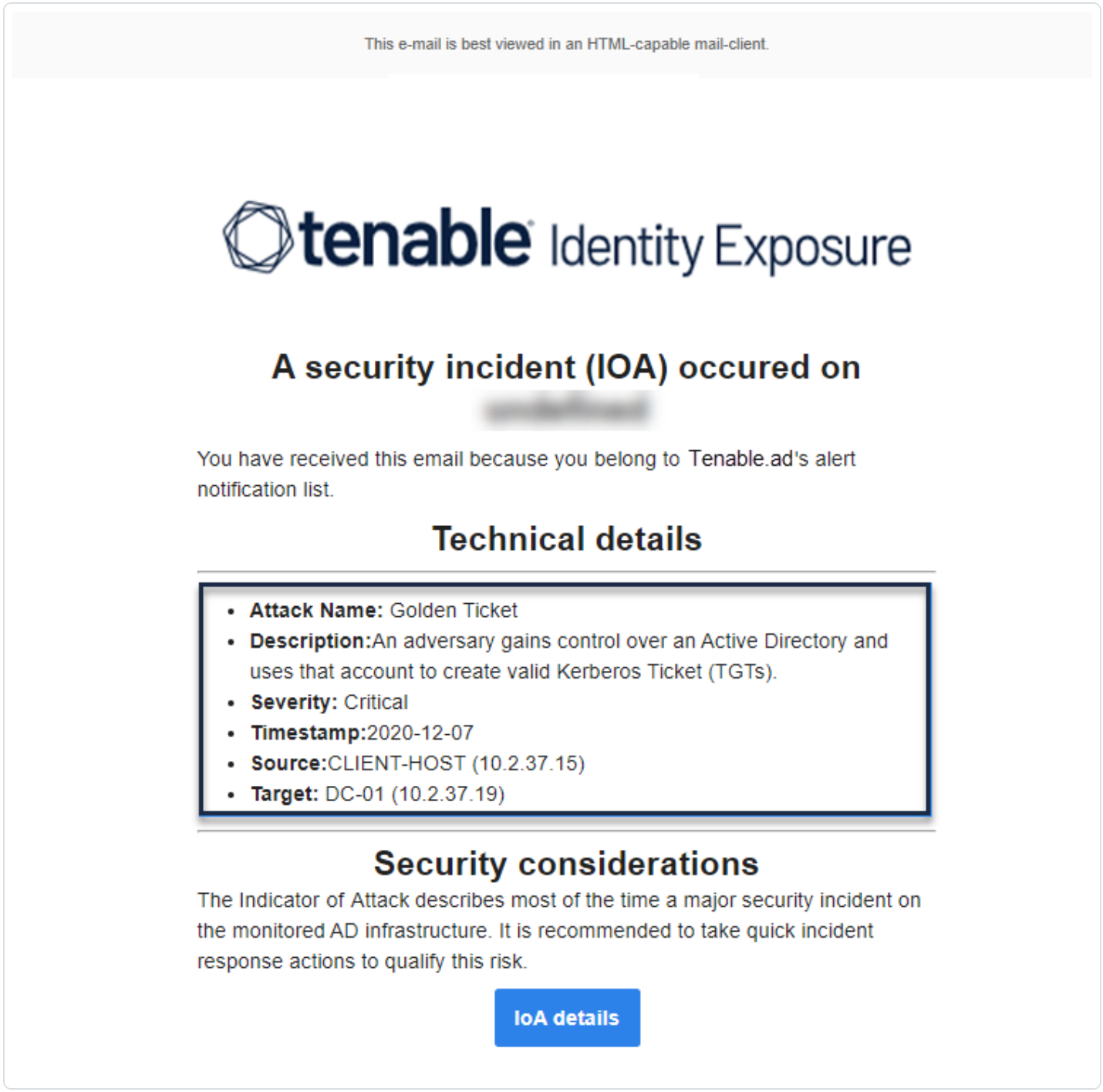
- SMTP 帐户
- SMTP 帐户密码

5. 在“SMTP 加密”框中，单击箭头以从下拉列表中选择加密方法。
6. 在“**发件人电子邮件地址**”框中，提供 Tenable Identity Exposure 发送电子邮件时要使用的电子邮件地址。
7. 单击“**保存**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新 SMTP 参数。

电子邮件警报

如果事件达到某个严重性阈值并需要采取修正操作，则 Tenable Identity Exposure 会自动发送电子邮件警报通知您。以下是电子邮件警报的示例：



添加电子邮件警报的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”>“**电子邮件**”。
2. 点击右侧的“**添加电子邮件警报**”按钮。

   此时会出现“**添加电子邮件警报**”窗格。
3. 在“**主要信息**”部分，提供以下信息：
   - 在“**电子邮件地址**”框中，输入收件人的电子邮件地址，以便他们接收通知。
   - 在“**描述**”框中，输入对收件人地址的描述。
4. 在“**触发警报**”下拉列表中，选择以下选项之一：
   - **每当出现异常行为时**：Tenable Identity Exposure 会针对每个异常 IoE 检测发出通知。
   - **每当出现攻击时**：Tenable Identity Exposure 会针对每个异常 IoA 检测发出通知。
   - **每当运行状况检查状态更改时**：Tenable Identity Exposure 会在运行状况检查状态发生更改时发出通知。
5. 在“**配置文件**”框中，点击以选择要用于此电子邮件警报的配置文件（如适用）。
6. **在初始分析阶段检测到异常行为时发送警报**：执行下列操作之一（如适用）：
   - 选中复选框：当系统重新启动触发警报时，Tenable Identity Exposure 会发出大量电子邮件通知。
   - 取消选中复选框：当系统重新启动触发警报时，Tenable Identity Exposure 不会发出电子邮件通知。
7. **严重性阈值**：点击下拉框的箭头以选择 Tenable Identity Exposure 发送警报的阈值（如适用）。
8. 根据您之前选择的警报触发器：
   - **风险暴露指标**：如果将警报设置为**每当出现异常行为时**触发，请点击每个严重程度旁边的箭头，展开风险暴露指标列表，并选择要为其发送警报的指标。
   - **攻击指标**：如果将警报设置为**每当出现攻击时**触发，请点击每个严重程度旁边的箭头，展开攻击指标列表，并选择要为其发送警报的指标。

- **运行状况检查状态更改**：点击“**运行状况检查**”，选择要触发警报的运行状况检查类型，然后点击“**按所选结果筛选**”。

9. 点击“**域**”框以选择 Tenable Identity Exposure 为其发出警报的域。

   出现“林和域”窗格。

   a. 选择林或域。

   b. 单击“**按所选结果筛选**”。

10. 点击“**测试配置**”。

    此时会出现一条消息，确认 Tenable Identity Exposure 已向服务器发送了电子邮件警报。

11. 点击“**添加**”。

    此时会出现一条消息，确认 Tenable Identity Exposure 已创建该电子邮件警报。

编辑电子邮件警报的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”>“**电子邮件**”。
2. 在电子邮件警报列表中，将鼠标悬停在要修改的警报上，然后点击行末的 图标。

   此时会出现“**编辑电子邮件警报**”窗格。
3. 按照步骤(添加电子邮件警报的步骤：) 进行必要的修改。
4. 单击“**编辑**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新警报。

删除电子邮件警报的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”>“**电子邮件**”。
2. 在电子邮件警报列表中，将鼠标悬停在要删除的警报上，然后点击行末的 图标。

   此时会显示一条消息，要求您确认删除。
3. 点击“**删除**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已删除警报。

另请参阅：

- SMTP 服务器配置
- Syslog 和电子邮件警报详细信息

Syslog 警报

一些组织使用 SIEM(安全信息和事件管理) 来收集有关潜在威胁和安全事件的日志。Tenable Identity Exposure 可将与 Active Directory 相关的安全信息推送到 SIEM Syslog 服务器以改进其警报机制。

添加新的 Syslog 警报的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”>“**配置**”>“**Syslog**”。
2. 点击右侧的“**添加 Syslog 警报**”按钮。

   此时会出现“**添加 Syslog 警报**”窗格。

3. 在“**主要信息**”部分，提供以下信息：

- **如果您的网络使用安全中继：**在“**中继**”框中，点击箭头以从下拉列表中选择一个与 SIEM 进行通信的中继。
- 在“**采集器 IP 地址或主机名**”框中，输入接收通知的服务器 IP 或主机名。
- 在“**端口**”框中，输入采集器的端口号。
- 在“**协议**”框中，点击箭头以选择 UDP 或 TCP。
  - 如果选择 TCP，并且要启用 TLS 安全协议以加密日志，请选中“**TLS**”选项的复选框。
- 在“**描述**”框中，输入对采集器的简要描述。

4. 在“**触发警报**”下拉列表中，选择以下选项之一：
   - **在变更时**：只要发生您指定的事件，Tenable Identity Exposure 就会发出通知。
   - **每当出现异常行为时**：Tenable Identity Exposure 会针对每个异常 IoE 检测发出通知。
   - **每当出现攻击时**：Tenable Identity Exposure 会针对每个异常 IoA 检测发出通知。
   - **每当运行状况检查状态更改时**：Tenable Identity Exposure 会在运行状况检查状态发生更改时发出通知。
5. 在“**配置文件**”框中，点击以选择要用于此 Syslog 警报的配置文件（如适用）。
6. **在初始分析阶段检测到异常行为时发送警报**：执行下列操作之一（如适用）：
   - 选中复选框：当系统重新启动触发警报时，Tenable Identity Exposure 会发出大量电子邮件通知。
   - 取消选中复选框：当系统重新启动触发警报时，Tenable Identity Exposure 不会发出电子邮件通知。
7. **严重性阈值**：点击下拉框的箭头以选择 Tenable Identity Exposure 发送警报的阈值（如适用）。
8. 根据您之前选择的警报触发器：
   - **事件变更**：如果将警报设置为“**在变更时**”触发，请输入表达式以触发事件通知。

     您可以点击 图标以使用搜索向导，也可以在搜索框中输入查询表达式并点击“**验证**”。有关更多信息，请参阅“自定义跟踪事件流查询”。

- **风险暴露指标**：如果将警报设置为**每当出现异常行为时**触发，请点击每个严重程度旁边的箭头，展开风险暴露指标列表，并选择要为其发送警报的指标。
- **攻击指标**：如果将警报设置为**每当出现攻击时**触发，请点击每个严重程度旁边的箭头，展开攻击指标列表，并选择要为其发送警报的指标。
- **运行状况检查状态更改**：点击"**运行状况检查**"，选择要触发警报的运行状况检查类型，然后点击"**按所选结果筛选**"。

9. 点击"**域**"框以选择 Tenable Identity Exposure 为其发出警报的域。

   出现"**林和域**"窗格。

   a. 选择林或域。

   b. 单击"**按所选结果筛选**"。

10. 点击"**测试配置**"。

    此时会出现一条消息，确认 Tenable Identity Exposure 已向服务器发送了 Syslog 警报。

11. 点击"**添加**"。

    此时会出现一条消息，确认 Tenable Identity Exposure 已创建 Syslog 警报。

编辑 Syslog 警报的步骤：

1. 在 Tenable Identity Exposure 中，点击"**系统**">"**配置**">"**Syslog**"。
2. 在 Syslog 警报列表中，将鼠标悬停在要修改的警报上，然后点击行末的 ✎ 图标。

   此时会出现"**编辑 Syslog 警报**"窗格。

3. 按照步骤(添加新的 Syslog 警报的步骤：)进行必要的修改。
4. 单击"**编辑**"。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新警报。

删除 Syslog 警报的步骤：

1. 在 Tenable Identity Exposure 中，点击"**系统**">"**配置**">"**Syslog**"。
2. 在 Syslog 警报列表中，将鼠标悬停在要删除的警报上，然后点击行末的 🗑 图标。

此时会显示一条消息，要求您确认删除。

3. 点击“**删除**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已删除警报。

另请参阅：

- Syslog 和电子邮件警报详细信息

Syslog 和电子邮件警报详细信息

当您启用 Syslog 或电子邮件警报时，Tenable Identity Exposure 在检测到异常行为、攻击或变更时会发出通知。

警报标头

Syslog 警报标头 (RFC-3164) 使用通用事件格式 (CEF)，这是集成安全信息和事件管理 (SIEM) 的解决方案中的通用格式。

风险暴露指标 (IoE) 的警报示例

IoE 警报标头

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "0" "1" "Alsid Forest" "emea.corp" "C-PASSWORD-DONT-EXPIRE" "medium" "CN=Gustavo Fring,OU=Los_Pollos_Hermanos,OU=Emea,DC=emea,DC=corp" "28" "1" "R-DONT-EXPIRE-SET" "2434" "TrusteeCn"="Gustavo Fring"
```

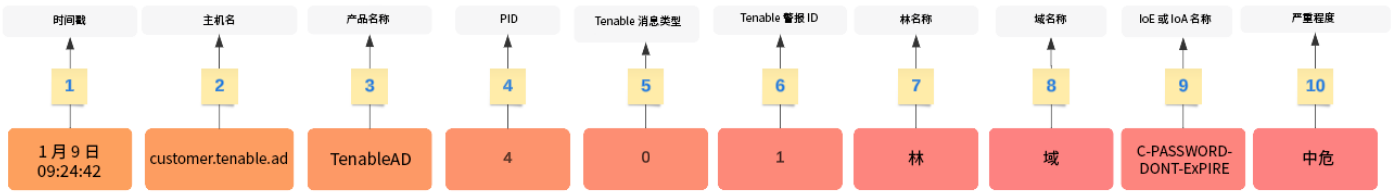
攻击指标 (IoA) 的警报示例

IoA 警报标头

```
<116>Jan  9 09:24:42 qradar.alsid.app AlsidForAD[4]: "2" "1337" "Alsid Forest" "emea.corp" "DC Sync" "medium" "yoda.alsid.corp" "10.0.0.1" "antoinex1x.alsid.corp" "10.1.0.1" "user"="Gustavo Fring" "dc_name"="MyDC"
```

警报信息

通用元素

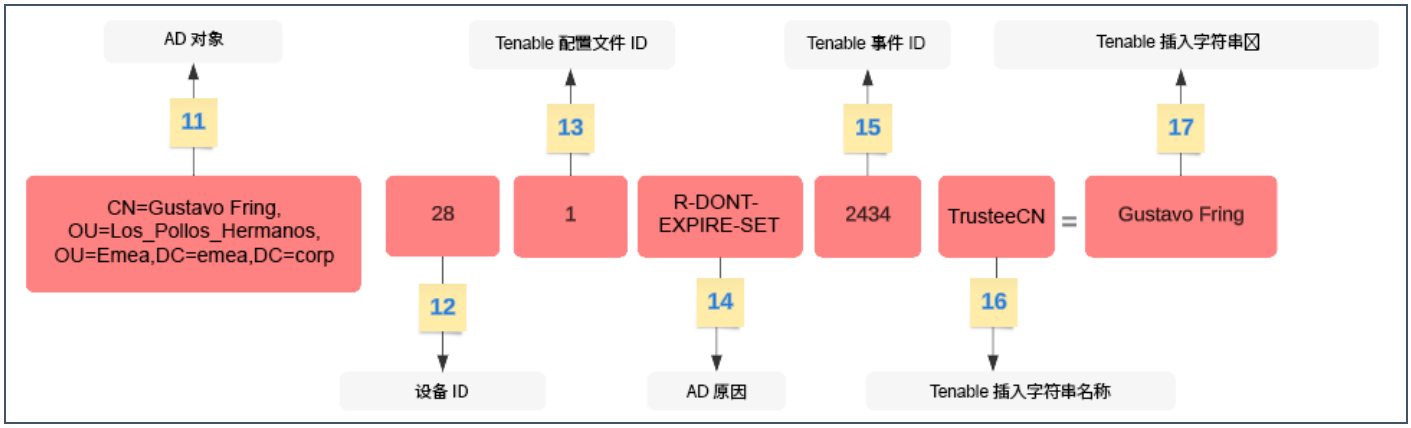


标头结构包括以下部分，如表中所述。

部分	描述
1	**“时间戳”**是检测日期。示例：“6 月 7 日 05:37:03”

2	**"主机名"**是应用程序的主机名。示例："customer.tenable.ad"
3	**"产品名"**是在其上触发了异常行为的产品的名称。示例："TenableAD"、"AnotherTenableADProduct"
4	**"PID"**是产品 (Tenable Identity Exposure) ID。示例：[4]
5	**"Tenable 消息类型"**是事件源的标识符。示例："0"(= 每当出现异常行为时)、"1"(= 在变更时)、"2"(= 每当出现攻击时)
6	**"Tenable 警报 ID"**是警报的唯一 ID。示例："0"、"132"
7	**"林名称"**是相关事件的林名称。示例："CorpForest"
8	**"域名"**为与事件相关的域名。示例："tenable.corp"、"zwx.com"
9	**"Tenable 代号"**是风险暴露指标 (IoE) 或攻击指标 (IoA) 的代号。示例："C-PASSWORD-DONT-EXPIRE"、"DC Sync"。
10	**"Tenable 严重程度"**是相关异常行为的严重性级别。示例："严重"、"高危"、"中危"

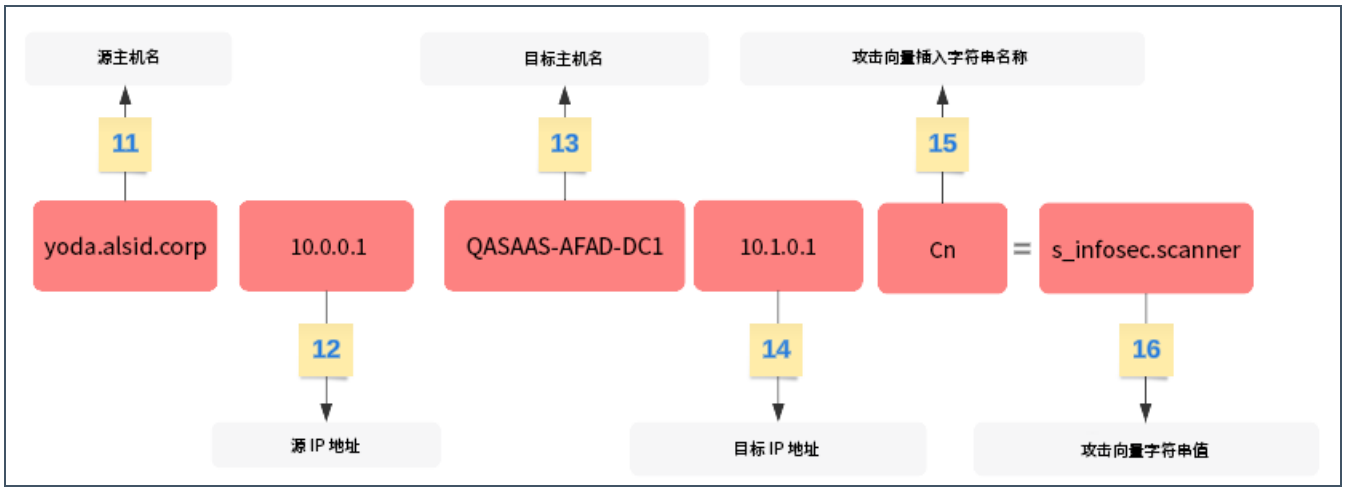
IoE 特定元素



部分	描述
11	**"AD 对象"**是异常对象的标识名。示例："CN=s_infosec.scanner,OU=ADManagers,DC=domain,DC=local"
12	**"Tenable 异常行为 ID"**是异常行为的 ID。示例："24980"、"132"、"28"
13	**"Tenable 配置文件 ID"**是 Tenable Identity Exposure 在其中触发了异常行为的配置

	文件的 ID。示例：“1”(Tenable)、“2”(sec_team)
14	**“AD 原因代号”**是异常行为原因的代号。示例：“R-DONT-EXPIRE-SET”、“R-UNCONST-DELEG”
15	**“Tenable 事件 ID”**是异常行为触发的事件的 ID。示例：“40667”、“28”
16	**“Tenable 插入字符串名称”**是异常行为对象触发的属性名称示例：“Cn”、“useraccountcontrol”、“member”、“pwdlastset”
17	**“Tenable 插入字符串值”**是异常行为对象触发的属性值。示例：“s_infosec.scanner”、“CN=Backup Operators,CN=Builtin,DC=domain,DC=local”

IoA 特定元素



部分	描述
11	**源主机名**是攻击主机的主机名。值也可以是“未知”。
12	**源 IP 地址**是攻击主机的 IP 地址。值可以是 IPv4 或 IPv6。
13	**目标主机名**是受攻击主机的主机名。
14	**目标 IP 地址**是受攻击主机的 IP 地址。值可以是 IPv4 或 IPv6。
15	**“攻击向量插入字符串名称”**是异常行为对象触发的属性名称。
16	**“攻击向量插入字符串值”**是异常行为对象触发的属性值。

示例

跟踪事件流事件详情

以下示例显示了跟踪事件流中包含以下内容的事件的详细信息：

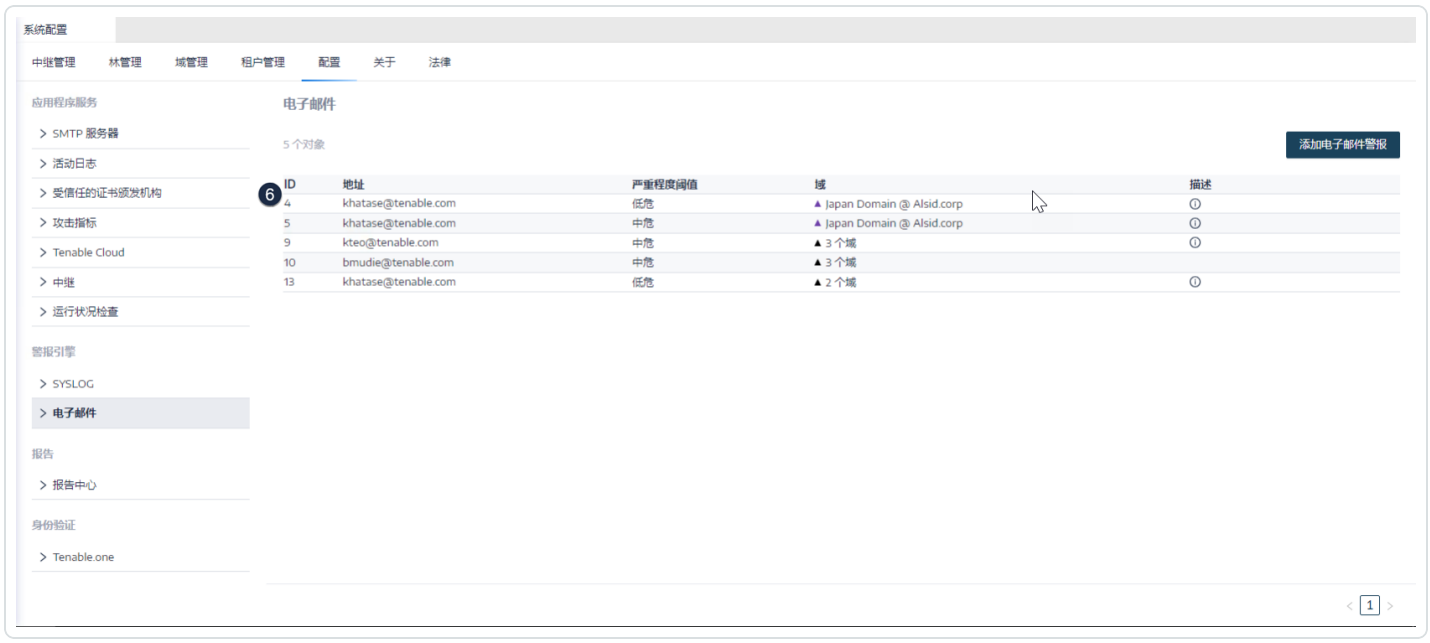
- 时间戳 (1)
- 异常对象名称 (11)
- 林 (7) 和域 (8) 名称
- 异常行为触发的属性名称 (17)

事件源

此示例显示事件 (5) 的来源。您在 Syslog 配置页面中设置此参数。有关更多信息，请参阅“Syslog 警报”。

警报 ID

此示例显示了警报的唯一 ID (6)，您可以在 Tenable Identity Exposure 的“**系统**”>“**配置**”>“**电子邮件**”中的已配置电子邮件地址列表中查看该 ID。


系统配置
中继管理
林管理
域管理
租户管理
配置
关于
法律
应用程序服务
SMTP 服务器
活动日志
受信任的证书颁发机构
攻击指标
Tenable Cloud
中继
运行状况检查
警报引擎
SYSLOG
电子邮件
报告
报告中心
身份验证
Tenable.one
电子邮件
5 个对象
添加电子邮件警报
6
ID
地址
严重程度阈值
域
描述
4 khatase@tenable.com 低危 Japan Domain @ Alsid.corp
5 khatase@tenable.com 中危 Japan Domain @ Alsid.corp
9 kteo@tenable.com 中危 3 个域
10 bmudie@tenable.com 中危 3 个域
13 khatase@tenable.com 低危 2 个域
1

运行状况检查

Tenable Identity Exposure 中的**运行状况检查**功能可让您在单一合并视图中实时查看域和服务帐户的配置情况，从而深入研究导致基础设施中出现连接问题或其他问题的任何配置异常。该功能会验证所有设置是否正确，以确保 Tenable Identity Exposure 的顺利运行，助您采取快速而准确的操作来修复问题，同时确保您的配置设置已经过优化，能够使 Tenable Identity Exposure 高效运行。

管理角色默认可查看运行状况检查，而对于某些用户角色，则需要获得相应的权限才能查看。您还可以根据运行状况检查状态的每次变更创建 Syslog 或电子邮件警报。

运行状况检查和 DC 同步攻击检测

运行状况检查提供有关 Tenable Identity Exposure 服务的状态和可用性的重要信息。该检查会验证服务帐户是否能够收集敏感信息，例如用于特权分析的密码哈希和 DPAPI 备份密钥。在运行状况检查报告中，Tenable 会尝试收集敏感数据以确定服务帐户是否正确配置了特权分析功能，如果未使用此功能，Tenable 实际不会收集任何信息。为防止在此过程中检测 DCSync 攻击，Tenable 会自动将为 DCSync 攻击指标提供的服务帐户列入白名单。

域状态

Tenable Identity Exposure 对每个域执行以下检查：

- AD 域的身份验证：LDAP 设置和状态、凭据以及 SMB 访问权限
- 域可访问性：与动态 RPC 端口的可正常工作连接、可访问的 SMB 服务器、可访问的域控制器 IP 地址或 FQDN、与 RPC 端口的可正常工作连接、可访问的 LDAP 服务器以及可访问的全局编录 LDAP 服务器。
- 权限：访问 AD 域数据和收集特权数据的能力。
- 链接到中继的域：域已正确关联到中继服务。

平台状态

Tenable Identity Exposure 对平台配置执行以下检查：

- 运行中继服务：中继配置是否正确，并提供关于故障排除的提示。
- 中继版本一致性：中继版本是否与 Tenable Identity Exposure 版本一致。

- 运行 AD 数据收集器服务：数据收集器服务、代理和收集器桥是否可操作，是否可将数据中继到其他服务。

若要访问运行状况检查，请执行以下操作：

1. 在 Tenable Identity Exposure 页面左下角，将鼠标悬停在  图标上，以查看基础设施的全局状态。
2. 点击图标可打开“**运行状况检查**”页面。在“**域状态**”或“**平台状态**”选项卡下，您会看到以下内容之一：
   - 显示已通过所有运行状况检查的信息
   - 特定状态的警告或问题列表：

	检查成功并显示正常结果。
	检查失败并发现一个问题。
	检查失败，但该问题不会妨碍 Tenable Identity Exposure 正常工作。 例如，如果服务帐户无法收集特权数据，则数据集合检查将失败，因为客户端的 Active Directory 配置错误。但该问题并不严重，出现此警告的原因是您尚未在 Tenable Identity Exposure 中在此域上激活特权分析功能。但是，如果您激活特权分析，检查将立即失败。
	检查显示未知结果，因为从属关系检查失败。例如，如果身份认证检查失败，则无法继续进行网络可访问性检查。

若要查看所有运行状况检查，请执行以下操作：

- 在右侧的运行状况检查列表上方，点击切换开关“**显示成功的检查**”以列出 Tenable Identity Exposure 执行的所有检查，其中包含以下信息：
  - 运行状况检查的名称
  - 状态（通过、失败、失败但无阻塞或未知）
  - 受影响的域及其关联的林（仅适用于域状态检查）

- 上次执行检查的时间
- 检查保持此状态的时间

若要刷新运行状况检查页面，请执行以下操作：

- 尽管 Tenable Identity Exposure 会定期执行运行状况检查，但并未借助结果实时更新页面。点击“  ”刷新结果列表。

若要按运行状况检查类型或域筛选结果，请执行以下操作：

1. 在右侧的运行状况检查列表上方，点击“**n/n 个运行状况检查**”或“**n/n 个域**”（仅适用于域状态）。

   此时会打开“**运行状况检查**”或“**林和域**”窗格。

2. 选择运行状况检查类型或林/域（如适用），然后点击“**按所选结果筛选**”。

若要深入了解有关每次运行状况检查的更多信息，请执行以下操作：

1. 在运行状况检查列表中，点击运行状况检查名称或行末的蓝色箭头 (→)。

   此时会打开“详细信息”窗格，并显示检查说明和相关详细信息列表。

运行状况检查的名称	类型	检查的描述	原因
域可访问性	域	与 AD 域建立连接的能力	• IP-UNREACHABLE R-LDAP-GLOBAL-CATALOG-UNREACHABLE • LDAP-SERVER-UNREACHABLE • SMB-SERVER-UNREACHABLE • DYNAMIC-RPC-CONNECTION-NOT-WORKING • RPC-CONNECTION-NOT-WORKING

AD 域身份验证	域	对 AD 域进行身份验证的能力	• INCORRECT-CREDENTIALS • LDAP-SERVER-BUSY • LDAP-SERVER-UNAVAILABLE • LDAP-SERVER-ACCESS-DENIED • SMB-SERVER-ACCESS-DENIED
收集 AD 域数据的权限	域	收集 AD 域数据的能力	• MISSING-PERMISSIONS-PRIVILEGED-DATA
访问 AD 容器的权限	域	访问 AD 容器的能力	• MISSING-PERMISSIONS-DELETED-OBJECTS-ACCESS • MISSING-PERMISSIONS-PASSWORD-SETTINGS-ACCESS
链接到中继的域	域	域已链接到中继	• LINKED-TO-RELAY-DOWN
中继服务启动	平台	中继按照预期工作	• RELAY-DOWN
中继服务版本	平台	中继版本与产品版本一致	• VERSION-MISMATCH
AD 数据收集器启动	平台	AD 数据收集器按预期工作	• DATA-COLLECTOR-SERVICE-DOWN • DATA-COLLECTOR-BRIDGE-DOWN • BROKER-DOWN

2. 点击详细信息行末尾的箭头以将其展开并显示有关结果的更多信息。

若要隐藏运行状况检查状态图标，请执行以下操作：

默认情况下，Tenable Identity Exposure 在屏幕左下角显示运行状况检查状态图标。

1. 在 Tenable Identity Exposure 中，转至左侧导航栏中的“**系统**”，然后选择“**配置**”选项卡。

   或者，您可以点击“运行状况检查”页面右上角的“ ”，然后选择“**配置**”。

2. 在“**应用程序服务**”下，选择“**运行状况检查**”。
3. 点击切换开关“**显示全局运行状况检查状态”**以禁用此功能。

   Tenable Identity Exposure 在屏幕左下角隐藏运行状况检查图标。

若要为用户角色分配运行状况检查权限，请执行以下操作：

1. 在 Tenable Identity Exposure 中，转至左侧导航栏中的“**帐户**”，然后选择“**角色管理**”选项卡。
2. 在角色列表中，选择用户角色并单击该行末尾的“ ”。

   此时会打开“**编辑角色**”窗格。
3. 选择“**系统配置实体**”选项卡。
4. 选择“**运行状况检查**”实体，然后点击权限切换按钮，将其从**未授权**状态切换为**已授权**状态。
5. 点击“**应用并关闭**”。

有关权限的更多信息，请参阅“设置角色的权限”。

若要设置运行状况检查状态变更警报，请执行以下操作：

1. 在 Tenable Identity Exposure 中，转至左侧导航栏中的“**系统**”，然后选择“**配置**”选项卡。

   或者，您可以点击“运行状况检查”页面右上角的“ ”，然后选择“**警报**”。

2. 在“**警报引擎**”下，选择“**Syslog**”或“ **电子邮件**”。
3. 点击“**添加 Syslog 警报**”或“**添加电子邮件警报**”。

   此时会打开一个新窗格。有关完整程序的信息，请参阅“警报”。

4. 在“**警报参数**”下的“**触发警报**”框中，从下拉菜单中选择“**每当运行状况检查状态更改时**”。
5. 点击“**健康状况检查**”框中的箭头，选择要触发警报的健康状况检查类型，然后点击“**按所选结果筛选**”。

6. 单击“**添加**”。

报告中心

Tenable Identity Exposure 中的**报告中心**拥有一个强大功能，可让您以报告形式向组织中的关键利益相关者导出重要数据。报告中心提供一种从预定义列表创建报告的方法，以确保过程高效且简化。

管理员可为不同的用户创建不同类型的报告，并灵活设置报告的时间范围，最长可以设置为一个季度。从 Tenable Identity Exposure 共享重要身份数据的能力增强了该组织主动缓解风险的能力以及识别基于身份的潜在攻击的能力。

如要下载报告，用户会收到一封电子邮件，其中包含页面的 URL，用户可在其中输入从管理员处收到的报告访问密钥。报告的下载期限为 30 天，过期后 Tenable Identity Exposure 将删除这些报告。用户必须尽快下载报告，因为 Tenable Identity Exposure 会针对指定的时间范围生成新的报告并覆盖旧报告。

若要访问报告中心，请执行以下操作：

1. 在 Tenable Identity Exposure 中，选择“**系统**”>“**配置**”。
2. 在“**报告**”下，点击“**报告中心**”。

   此时会打开一个窗格，其中包含已配置报告及其相关信息的列表，例如报告名称、类型、域、配置文件、时段、重复周期和收件人电子邮件。

若要创建报告，请执行以下操作：

1. 在“**报告中心**”窗格中，点击“**创建报告**”。

   此时会打开“**报告配置**”窗格。
2. 在“**报告类型**”下，填写以下信息：
   a. 在“**报告类型**”中，选择“**异常行为**”或“**攻击**”。
   b. 在“**指标**”中，点击“**n/n 个指标**”以选择“**风险暴露指标**”（用于异常行为）或“**攻击指标**”（用于攻击），然后点击“**按所选结果筛选**”。
   c. 在“**域**”中，点击“**n/n 个域**”，为报告选择林或域，然后点击“**按所选结果筛选**”。
   d. 在“**配置文件**”中，点击箭头以从下拉菜单中选择配置文件。

3. 在"**报告名称**"中，为报告输入名称。
4. 在"**生成参数**"下，选择以下设置：
   a. **数据的时间范围**：报告包含当前报告时间之前的时段，例如前一天、前一周、前一个月或前一个季度。
   b. **重复周期**：Tenable Identity Exposure 针对您定义的每个时间范围生成新的报告。您可点击箭头以从下拉菜单中选择相应的值。
   c. **时区**：与报告相关的时区。
5. 在"**收件人**"下，点击"**添加电子邮件**"，然后输入收件人的电子邮件地址。您可以根据需要添加任意数量的收件人。

   有关如何为报告收件人设置电子邮件的信息，请参阅"SMTP 服务器配置"
6. 点击"**创建报告**"。

若要允许用户下载报告，请执行以下操作：

- 在"**报告中心**"窗格顶部的"**报告访问密钥**"下，点击"⧉"进行复制。只有拥有此访问密钥，才能通过发送给收件人的电子邮件中的链接下载报告。所有用户和报告的访问密钥都是唯一的。
- 如有必要，点击"↻"以生成新的访问密钥。

  注意：生成新的访问密钥会使之前的访问密钥无法使用。只有使用新的访问密钥才能访问现有报告。

若要编辑报告配置，请执行以下操作：

1. 在报告列表中，选择一个报告并点击行末的"✎"以打开"**报告配置**"窗格。
2. 根据需要进行修改。
3. 单击"**保存**"。

若要删除报告，请执行以下操作：

1. 在报告列表中，选择一个报告并点击行末的“🗑”以删除报告。

   此时会显示一条消息，要求您确认删除。

2. 点击“**删除**”。

   最近生成的与此报告配置相关的报告不再可供下载。

若要向角色授予权限，请执行以下操作：

- 在“**权限管理**”中的“**数据实体**”>“**报告**”下，管理员可以向用户角色授予创建、读取或编辑所有或特定报告配置的权限。

  有关更多信息，请参阅“设置角色的权限”。

另请参阅：

- 小组件

Microsoft Entra ID 支持

除了 Active Directory 之外，Tenable Identity Exposure 还支持 Microsoft Entra ID（原名 Azure AD 或 AAD）以扩展组织中的标识范围。此功能利用专注于 Microsoft Entra ID 特定风险的新风险暴露指标。

若要将 Microsoft Entra ID 与 Tenable Identity Exposure 集成，请严格遵循指导流程：

1. 拥有 先决条件
2. 检查 权限
3. 配置 Microsoft Entra ID 设置
4. 激活 Microsoft Entra ID 支持
5. 启用租户扫描

先决条件

您必须拥有 **Tenable Vulnerability Management 帐户**才能使用 Microsoft Entra ID 支持功能。此帐户可让您为 Microsoft Entra ID 配置 Tenable 扫描并收集这些扫描的结果。

权限

Microsoft Entra ID 支持功能需要从 Microsoft Entra ID 收集数据，例如用户、组、应用程序、服务主体、角色、权限、策略、日志等。它使用 Microsoft Graph API 和遵循 Microsoft 建议的服务主体凭据收集此数据。

- 根据 Microsoft 的要求，您必须以**有权在租户范围内授予对 Microsoft Graph 的管理员同意**的用户身份登录到 Microsoft Entra ID，该身份必须具有全局管理员或特权角色管理员角色（或具有相应权限的任何自定义角色）。
- 如要访问 Microsoft Entra ID 的配置和数据可视化，您的 **Tenable Identity Exposure 用户角色**必须具有相应的权限。有关更多信息，请参阅“设置角色的权限”。

配置 Microsoft Entra ID 设置

通过以下过程（改编自 Microsoft 《快速入门：向 Microsoft 标识平台注册应用程序》文档），在 Microsoft Entra ID 中配置所有必需的设置。

1. **创建应用程序：**

   a. 在 Azure 管理员门户中，打开“应用程序注册”页面。

   b. 点击“**+ 新注册**”。

   c. 为应用程序命名（示例：“Tenable Identity Collector”）。对于其他选项，您可以保留默认值。

   d. 点击“**注册**”。

   e. 在此新创建应用程序的“概述”页面上，记录“应用程序（客户端）ID”和“目录（租户）ID”。

2. **向应用程序添加凭据：**

   a. 在 Azure 管理员门户中，打开“应用程序注册”页面。

   b. 点击已您创建的应用程序。

   c. 在左侧菜单中，点击“**证书和密钥**”。

   d. 点击“**+ 新客户端密钥**”。

   e. 在“**描述**”框中，为此密钥指定一个实用名称和一个符合您策略的**“到期”**值。请记住在接近到期日时更新此密钥。

   f. 请将密钥值保存在安全位置，因为 Azure 只会显示一次，如果丢失，必须重新创建。

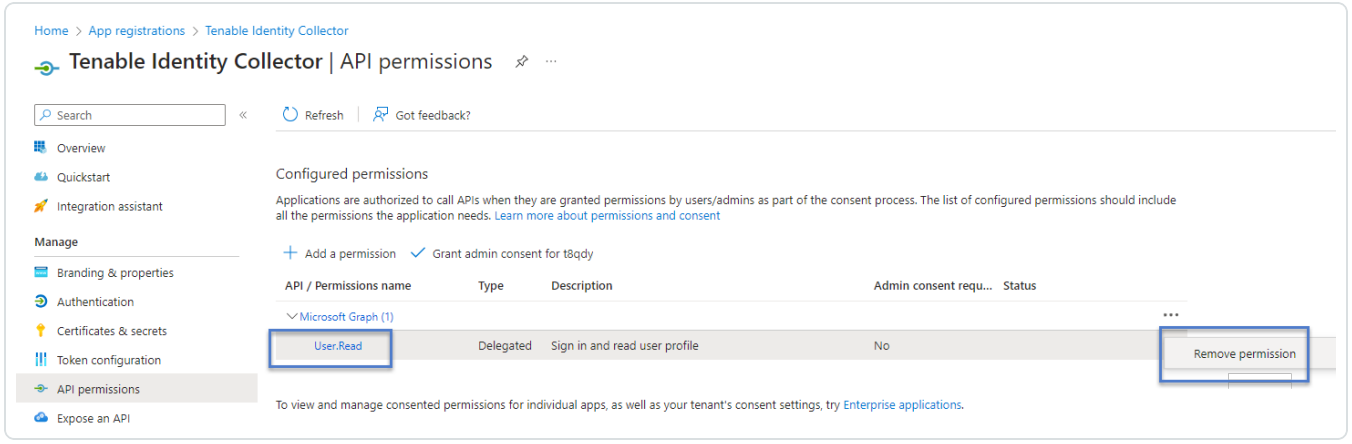
3. **为应用程序分配权限：**

   a. 在 Azure 管理员门户中，打开“应用程序注册”页面。

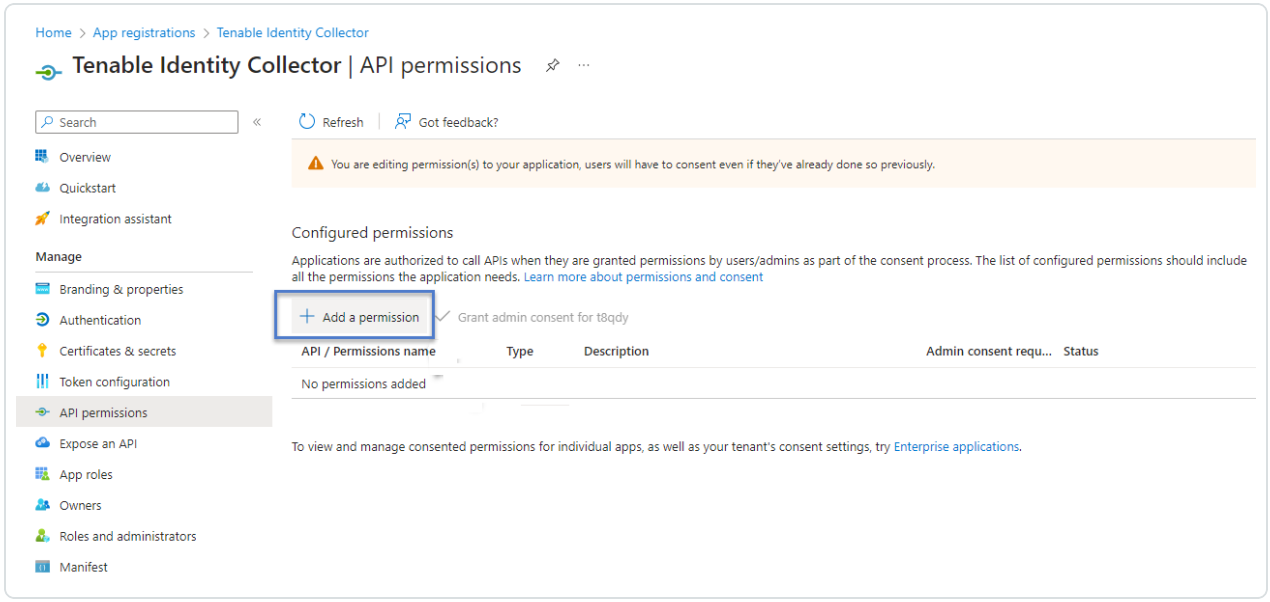
   b. 点击已您创建的应用程序。

   c. 在左侧菜单中，点击“**API 权限**”。

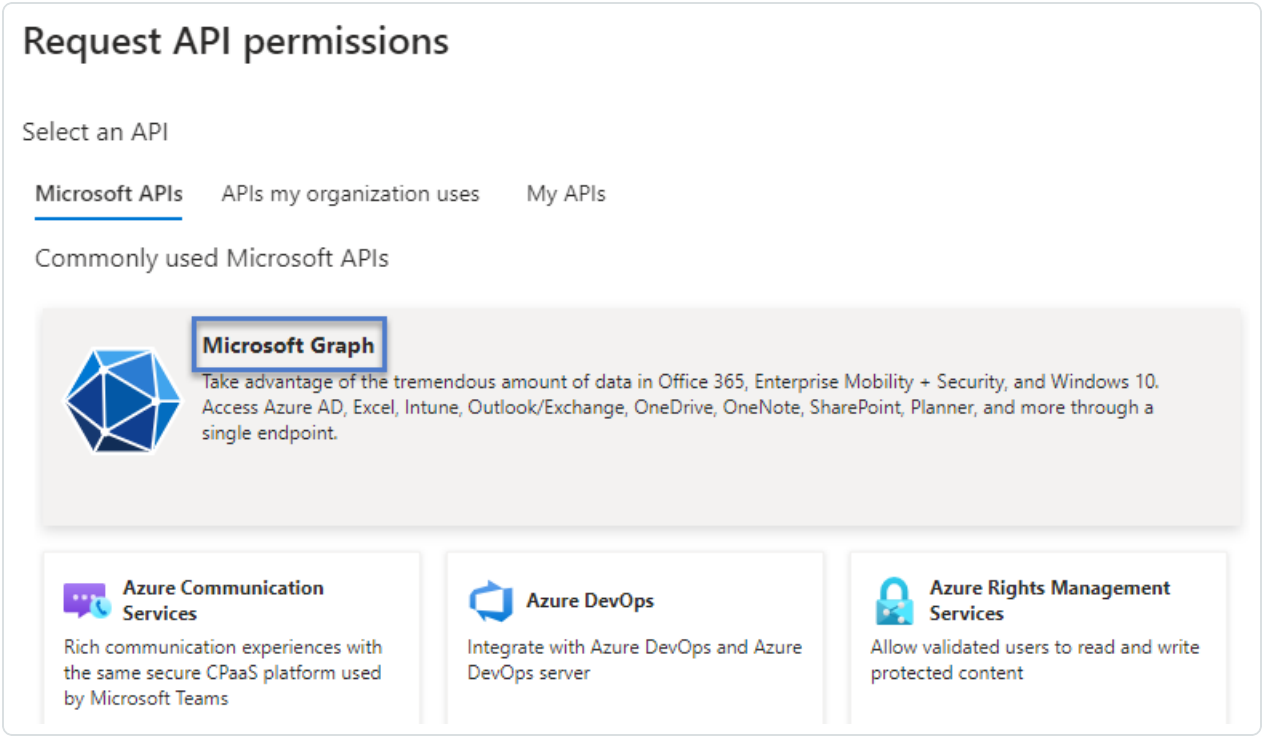
   d. 删除现有 `User.Read` 权限：



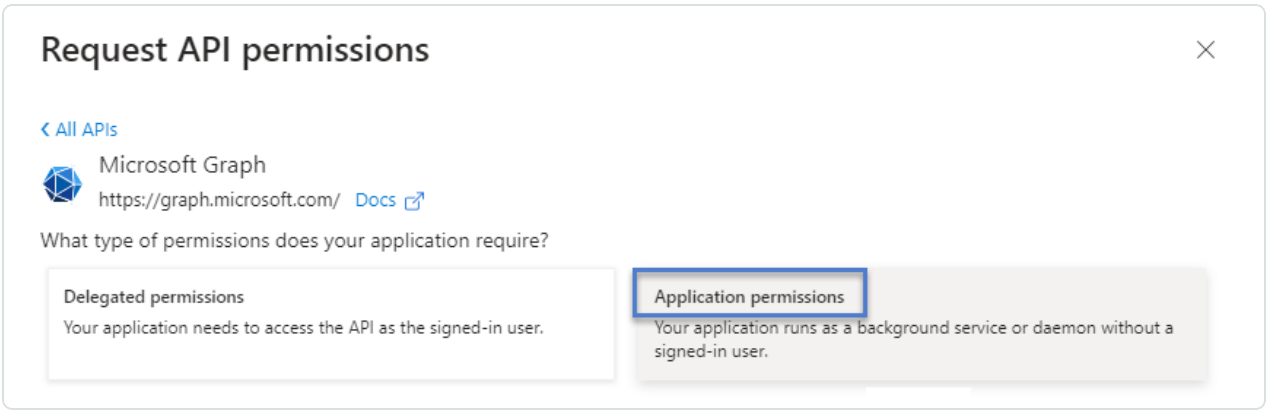
e. 点击“**+ 添加权限**”:



f. 选择“**Microsoft Graph**”:



g. 选择“**应用程序权限**”(非“委派权限”) 。



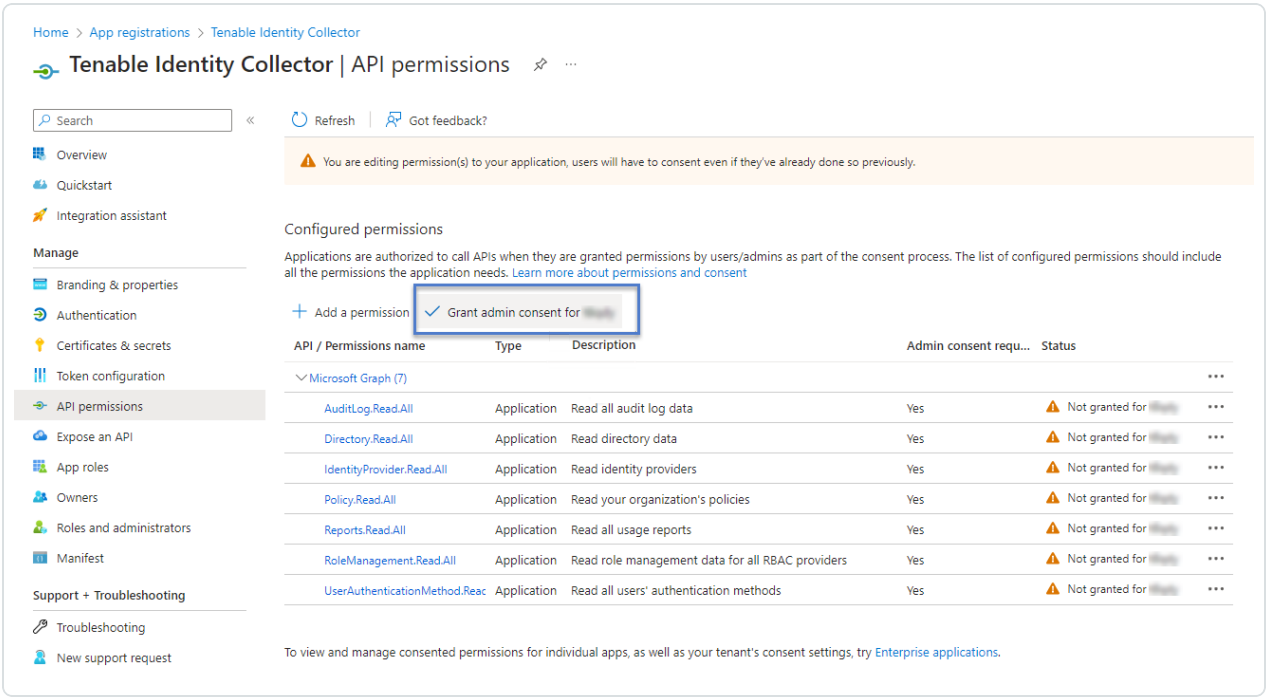
h. 使用列表或搜索栏查找并选择以下所有权限：

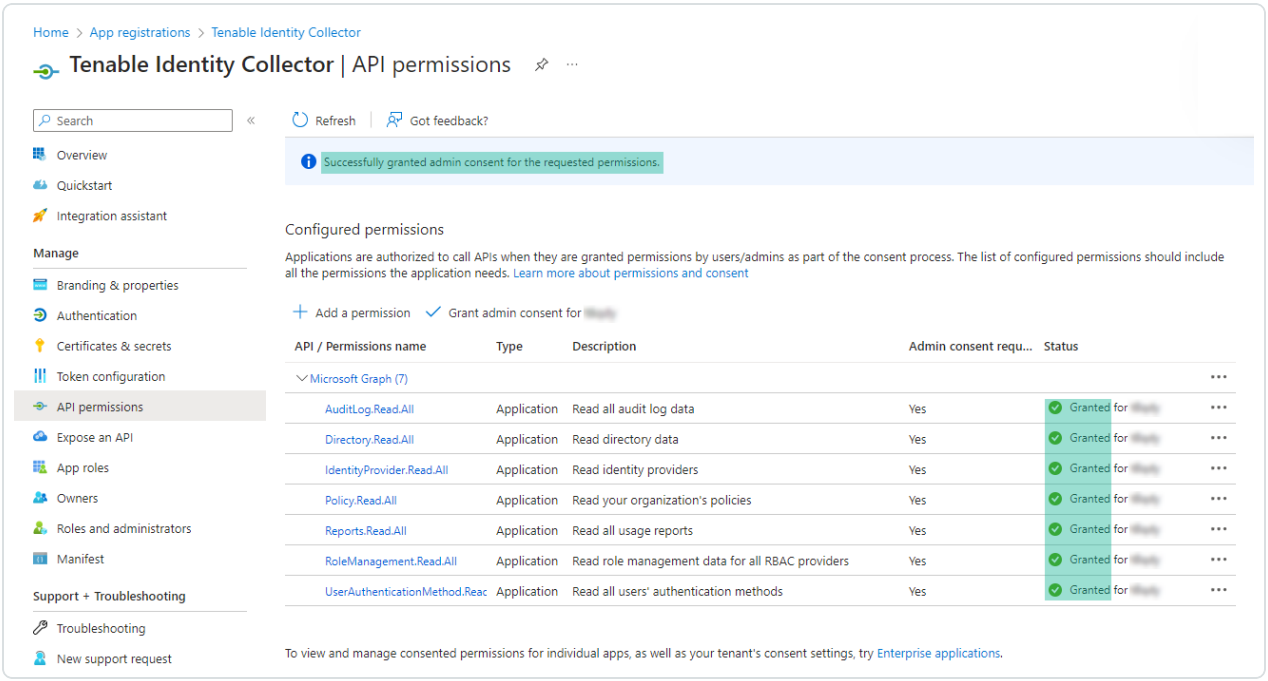
- `AuditLog.Read.All`
- `Directory.Read.All`
- `IdentityProvider.Read.All`
- `Policy.Read.All`
- `Reports.Read.All`

- `RoleManagement.Read.All`
- `UserAuthenticationMethod.Read.All`

i. 点击“**添加权限**”。

j. 点击“**为 <tenant name> 授予管理员同意**”并点击“**是**”以确认：





4. 在 Microsoft Entra ID 中配置所有必需的设置之后：

   a. 在 Tenable Vulnerability Management 中创建'Microsoft Azure'类型的新凭据。

   b. 选择"密钥"身份验证方法并输入在之前的流程中检索到的值：租户 ID、应用程序 ID 和客户端密码。

激活 Microsoft Entra ID 支持

若要激活 支持，请执行以下操作：

注意：为了成功激活此功能，创建了访问密钥和密钥的 Tenable Cloud 用户必须在 Tenable Identity Exposure 许可证引用的 Tenable Cloud 容器中拥有管理权限。有关更多信息，请参阅"Tenable Identity Exposure 许可"。

1. 在 Tenable Identity Exposure 中，点击左侧导航菜单中的系统图标  。
2. 点击"**配置**"选项卡。

   "**配置**"窗格随即打开。
3. 在"应用程序服务"部分下，点击"**Tenable Cloud**"。
4. 在"**激活 Microsoft Entra ID** 支持"中，点击以切换为启用。
5. 如果您之前未登录 Tenable Cloud，请点击链接以转至登录页面：

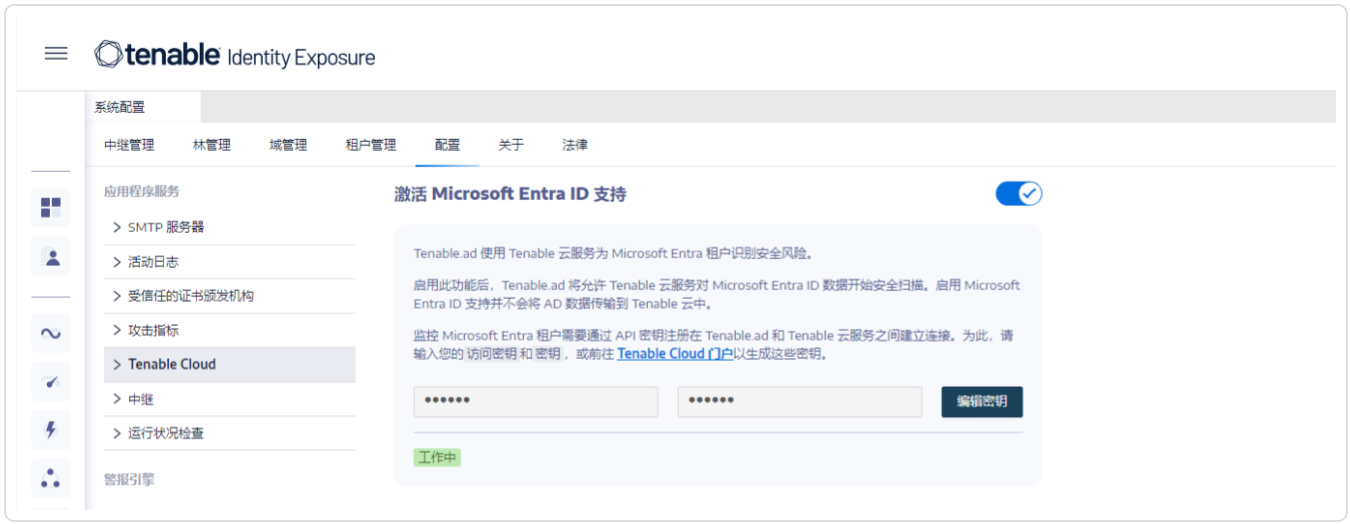
   a. 点击"**忘记密码？**"以请求重置密码。

   b. 键入与 Tenable Identity Exposure 许可证相关联的电子邮件地址，然后点击"**请求重置密码**"。

   Tenable 会向该地址发送一封电子邮件，其中包含用于重置密码的链接。

   注意：如果您的电子邮件地址与 Tenable Identity Exposure 许可证关联的电子邮件地址不同，请联系客户支持以获取帮助。
6. 登录 Tenable Vulnerability Management。
7. 如要在 Tenable Vulnerability Management 中生成 API 密钥，请转至"Tenable Vulnerability Management">"**设置**">"**我的帐户**">"**API 密钥**"。

8. 输入您的 Tenable Vulnerability Management“Admin”用户访问密钥和安全密钥，以在 Tenable Identity Exposure 和 Tenable 云服务之间建立连接。
9. 点击“**编辑密钥**”以提交 API 密钥。



Tenable Identity Exposure 显示一条消息，以确认其已更新 API 密钥。

启用租户扫描

如要添加新的 租户，请执行以下操作：

添加租户会将 Tenable Identity Exposure 与 Microsoft Entra ID 链接起来以对该租户执行扫描。

1. 在“配置”页面中，点击“**租户管理**”选项卡。

   “**租户管理**”页面随即打开。

2. 点击“**添加租户**”。

   “**添加租户**”页面随即打开。

3. 在"**租户名称**"框中，输入名称。
4. 在"**凭据**"框中，点击下拉列表以选择凭据。
5. 如果您的凭据未出现在列表中，您可以：
   - 在 Tenable Vulnerability Management 中创建一个（通过"Tenable Vulnerability Management">"**设置**">"**凭据**"）。有关更多信息，请参阅"在 Tenable Vulnerability Management 中创建 Azure 类型凭据的过程"。
   - 检查您是否在 Tenable Vulnerability Management 中具有凭据的"可使用"或"可编辑"权限。除非您拥有这些权限，否则 Tenable Identity Exposure 不会在下拉列表中显示凭据。
6. 点击"**刷新**"以更新凭据下拉列表。
7. 选择您已创建的凭据。

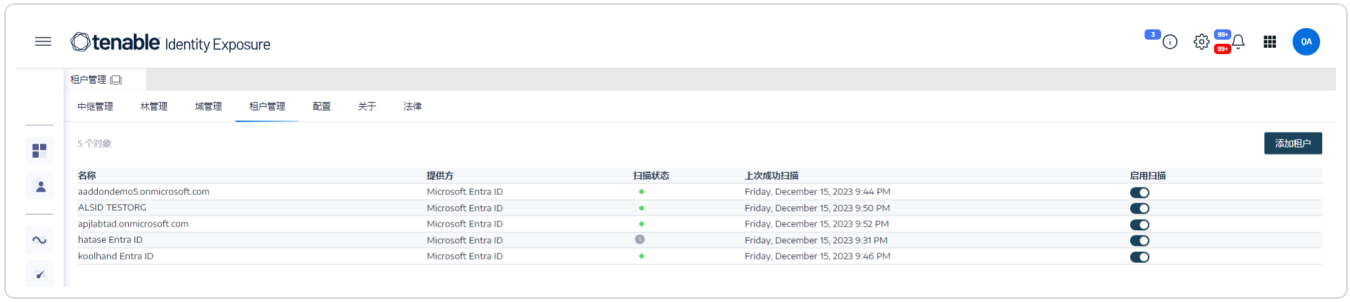
8. 单击“**添加**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 添加了租户，该租户现在显示在“租户管理”页面的列表中。

若要为租户启用扫描，请执行以下操作：

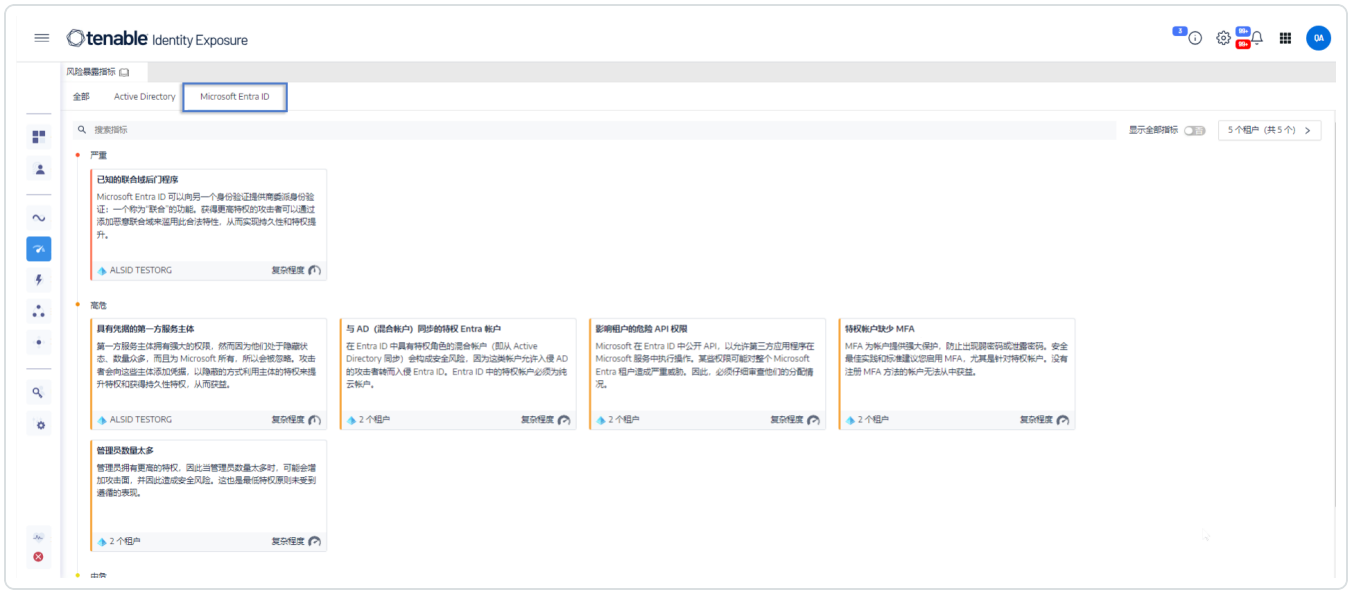
注意：租户扫描不会实时发生，且至少需要 45 分钟的时间才能在 Identity Explorer 中看到 Microsoft Entra ID 数据。

- 在列表中选择一个租户，然后点击以切换至“**已启用扫描**”。



Tenable Identity Exposure 请求对租户进行扫描，随后结果会显示在“风险暴露指标”页面中。

注意：两次扫描之间的强制性最短时间延迟为 **30 分钟**。



Tenable Cloud 数据收集

Tenable Cloud(Tenable Identity Exposure 中的数据收集功能) 会将您的信息传输到其私有云，以提供安全分析和服务。有关数据收集的更多信息，请参阅 Tenable 的信任与保证声明。

要使用 Tenable Cloud，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击侧边导航栏上的“**系统**”，然后点击“**系统**”。

   “**系统配置**”窗格随即打开。

2. 选择“**配置**”选项卡。

3. 在“**应用程序服务**”部分下，点击“**Tenable Cloud**”。

   “**Tenable Cloud**”窗格随即打开。

4. 点击“使用 Tenable Cloud 服务”，切换至“**启用**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新信息传输配置。

特权分析

特权分析是 Tenable Identity Exposure 中的可选功能，与其他功能相反，该功能需要更多权限以便获取本应受到保护的数据并提供更多安全分析。

数据获取

> 注意：特权分析功能需要更高的特权。请参阅 特权分析的访问权限。

特权分析功能一旦启用，它会额外获取以下数据：

- **密码哈希** - Tenable Identity Exposure 获取 LM 和 NT 哈希以进行密码分析。Tenable Identity Exposure 获取 LM 哈希只是为了在 LM 哈希使用旧的弱算法时警告其存在，并不会存储它们。哈希集合范围包括：
    - 所有已启用的用户帐户
    - 所有已启用的域控制器计算机帐户

数据保护

Active Directory (AD) 本身不直接存储用户密码，而是仅存储使用不允许恢复原始密码的 LM 或 NT 哈希算法的密码哈希。Tenable Identity Exposure 不存储 LM 哈希。

除了在 SAAS-VPN 平台中托管中继的客户端之外，密码永远不会离开客户端的基础设施，因为只有中继才能处理它们。中继不存储密码，而是在每次需要分析时检索用户的密码，仅将其临时保存在缓存中，通常仅保存几毫秒。然而，Tenable Identity Exposure 会保留最少位数的密码哈希数据。数据安全地存储在中继的 RAM 中，仅用于执行 K-anonymity 分析以检查具有相同密码的用户。

> **注意**：对于 SaaS-VPN 平台客户端，中继的行为方式是相同的，但托管您的中继的是 Tenable。

活动日志

在 Tenable Identity Exposure 的活动日志中，可以查看 Tenable Identity Exposure 平台上发生的所有活动的跟踪信息，包括具体的 IP 地址、用户或操作等。

若要配置活动日志：

1. 在 Tenable Identity Exposure 侧导航窗格中的“**管理**”下，点击“**系统**”。

   “**系统配置**”窗格随即打开。

2. 在“**应用程序服务**”部分下，点击“**活动日志**”。

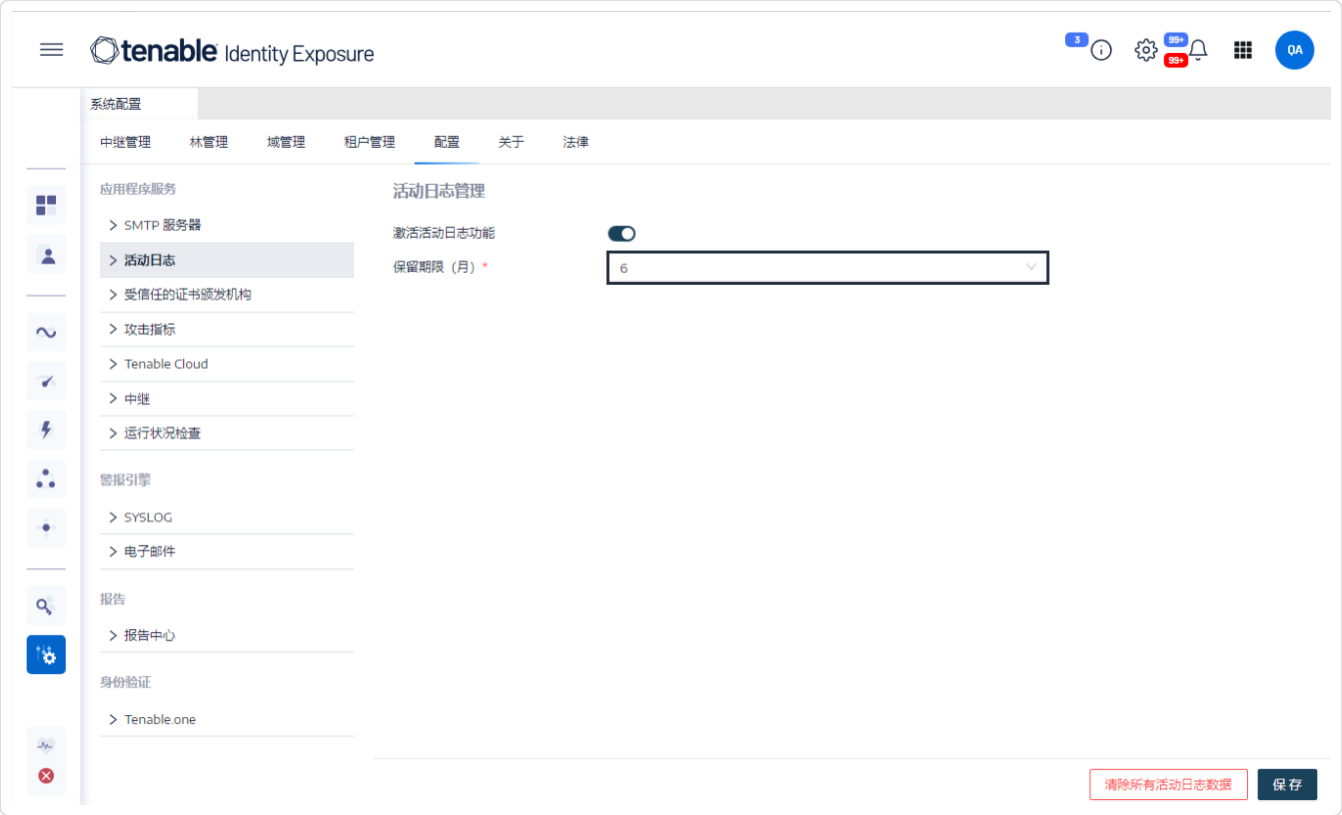
   “**活动日志管理**”窗格随即打开。

3. 若要激活活动日志功能，请点击切换为“**启用**”。

4. 在“保留期限（月）”框中，点击“**>**”以选择要记录活动的月数。

5. 单击“**保存**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新设置。



若要清除活动日志数据：

1. 在 Tenable Identity Exposure 侧导航窗格中的“**管理**”下，点击“**系统**”。

   “**系统配置**”窗格随即打开。

2. 在“**应用程序服务**”部分下，点击“**活动日志**”。

   “**活动日志管理**”窗格随即打开。

3. 在“**清除所有活动日志数据**”下，点击“**清除**”。

   此时会显示一条消息，要求您确认。

4. 点击“**确认**”。

   此时会出现一条消息，确认 Tenable Identity Exposure 已更新设置。

若要为用户自己的活动日志设置权限：

1. 在 Tenable Identity Exposure 侧导航窗格中的“**管理**”下，点击“**帐户**”。

   “**用户帐户管理**”窗格随即打开。

2. 选择“**角色管理**”选项卡。

3. 在角色列表中，将鼠标悬停在需要此权限的用户角色上，然后点击行末的 图标。

   此时会打开“**编辑角色**”窗格。

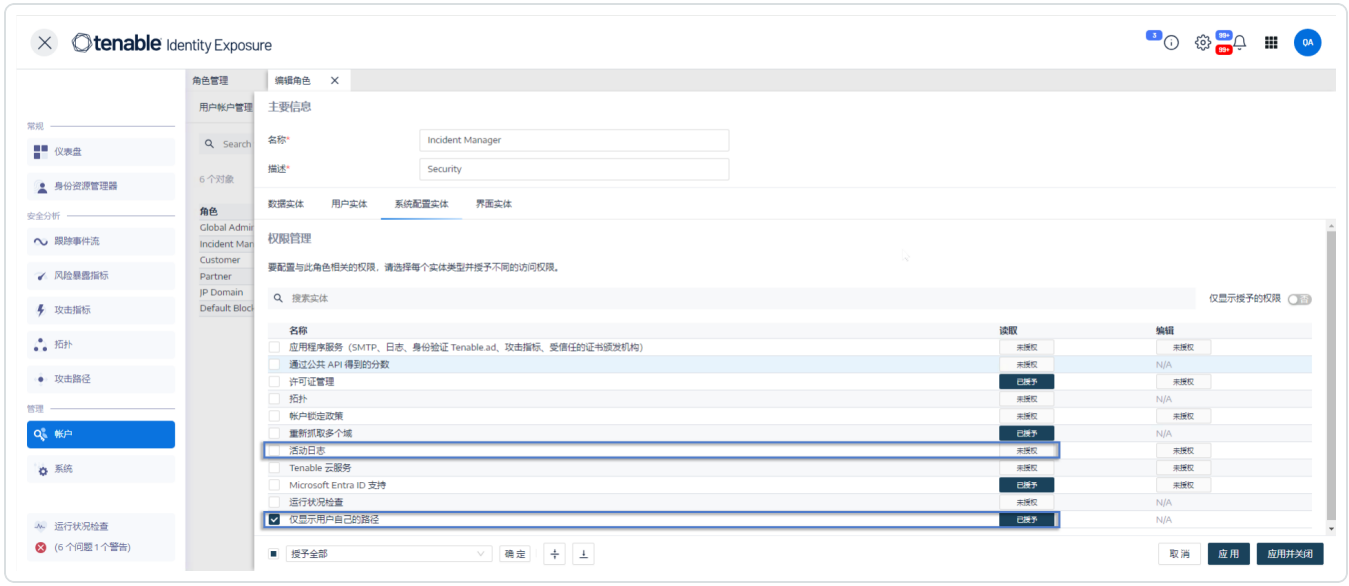
4. 在“**主要信息**”部分下，选择“**系统配置实体**”选项卡。

5. 在“**权限管理**”部分下，执行以下操作：

   - 取消选择“**活动日志**”权限，更改为“*未授权*”。
   - 选择“**仅显示用户自己的跟踪信息**”的权限，更改为“*已授权*”。

6. 点击“**应用并关闭**”。

此时会出现一条消息，确认 Tenable Identity Exposure 已更新用户角色。



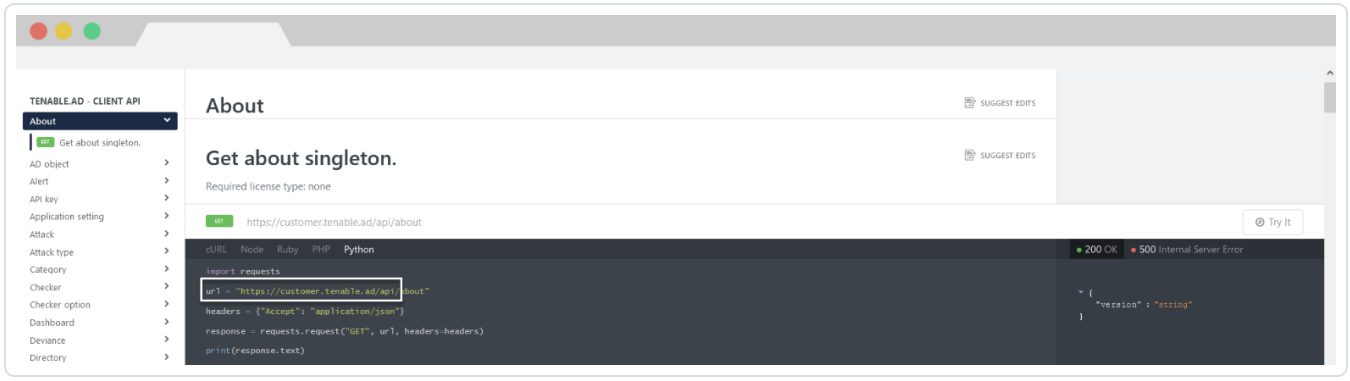
Tenable Identity Exposure 公共 API

Tenable Identity Exposure 的 API 允许您与其数据库服务通信。

包含 Tenable Identity Exposure 的 API 结构和资源的 OpenAPI 文件可在此处获得。

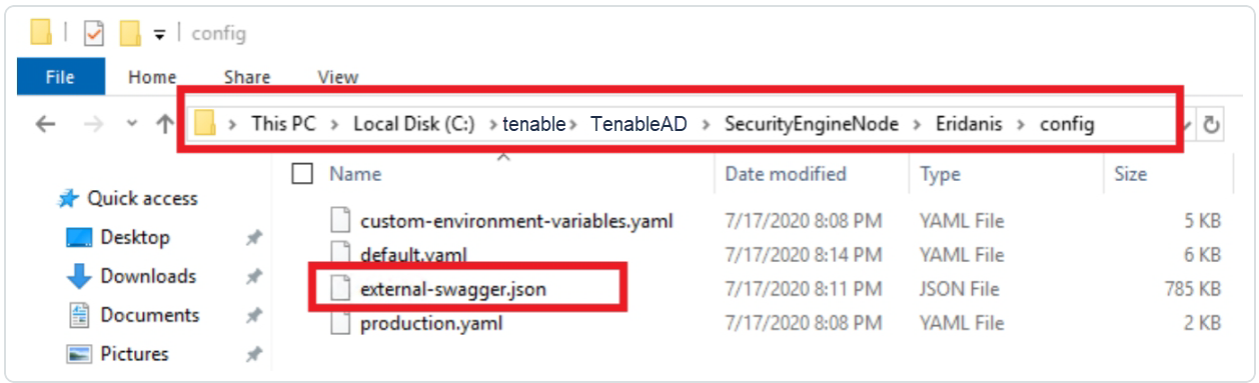
要访问 Tenable Identity Exposure 实例的 API，请执行以下操作：

- 在浏览器中打开此 URL：



下载 OpenAPI 文件：

- 对于本地安装，请使用通往此安全引擎节点的路径：



- 对于 SaaS 安装，请转至 Tenable Identity Exposure API Explorer。

要检索 API 密钥，请执行以下操作：

1. 在 Tenable Identity Exposure 中，点击您的用户配置文件图标并选择“**首选项**”。

   出现“首选项”窗格。

2. 从菜单中，选择“**API 密钥**”。

Tenable Identity Exposure 会显示您当前的 API 密钥。

3. 点击 图标，将 API 密钥复制到剪贴板。

要刷新 API 密钥，请执行以下操作：

如果单击“**刷新 API 密钥**”或者失去生成 API 密钥或访问令牌的权限，访问令牌将过期。到期与时间或 API 请求数量无关。生成或刷新 API 密钥仅与当前用户有关，不会干扰其他帐户 API 密钥。获取 API 密钥时，您还会收到一个刷新令牌。您可以使用此刷新令牌检索新的 API 密钥。

注意：刷新 API 密钥时，Tenable Identity Exposure 会停用当前的 API 密钥。您还会收到一个刷新令牌。

1. 单击“**刷新 API 密钥**”。

   此时会显示一条消息，要求您确认。

2. 点击“**确认**”。

数据管理

Tenable Identity Exposure 将数据保留 6 个月。此数据管理周期不可配置。

部署区域

Tenable Identity Exposure SaaS 当前部署在以下 Azure 区域中：

国家/地区	Azure 区域
美洲	
巴西 – 圣保罗	巴西南部
加拿大 – 魁北克市	加拿大东部
加拿大 – 多伦多市	加拿大中部
美国 – 加利福尼亚州	美国西部
美国 – 爱荷华州	美国中部
美国 – 弗吉尼亚州	美国东部 2
欧洲、中东及非洲	
法国 – 巴黎	法国中部
爱尔兰	北欧
荷兰	西欧
南非 – 约翰内斯堡	南非北部
瑞士 – 苏黎世	瑞士北部
阿拉伯联合酋长国 – 迪拜	阿联酋北部
英国 – 伦敦	英国南部
亚太地区	
澳大利亚 – 新南威尔士州	澳大利亚东部
澳大利亚 – 维多利亚州	澳大利亚东南部
中国香港	东亚
印度 – 浦那	印度中部

日本 – 大阪	日本西部
新加坡	东南亚

Tenable Identity Exposure 许可

本主题详细介绍了作为独立产品的 Tenable Identity Exposure 的许可流程，并解释了资产的计数方式，同时描述了许可证超额使用或到期时会发生什么。如要了解如何使用 Tenable Identity Exposure，请参阅《Tenable Identity Exposure 用户指南》。

Tenable Identity Exposure 许可

Tenable Identity Exposure 有两个版本：云版本和本地版本。在某些情况下，Tenable 还提供订阅定价。

如要使用 Tenable Identity Exposure，您需要根据组织的需求和环境详情购买许可证。Tenable Identity Exposure 随后会将这些许可证分配给您的资产：您目录服务中的已启用用户。

当您的环境扩展时，资产数量也会相应增加，因此您需要购买更多许可证以适应这种变化。Tenable 许可证采用递进定价方式，即购买数量越多，单价就越低。如需了解价格，请联系您的 Tenable 代表。

提示：如要查看当前的许可证数量和可用资产，请在 Tenable 顶部导航栏中点击“”，然后点击“**许可证信息**”。如要了解详情，请参阅许可证信息页面。

注意：Tenable 向托管安全服务提供商 (MSSP) 提供简化的定价方案。如要了解详情，请联系您的 Tenable 代表。

资产计数方式

您每购买一个 Tenable Identity Exposure 许可证，即表示您有权扫描一个唯一用户身份或其数字表示。Tenable 不会重复计算身份的数量。例如，同一个身份在 Microsoft Active Directory 和 Microsoft Entra ID 中启用的用户帐户被视为一个 Tenable 许可证。

Tenable Identity Exposure 组件

Tenable Identity Exposure 的两个版本都随附以下组件：

- 跟踪事件流视图
- 拓扑视图

- 风险暴露指标
- 攻击指标
- 攻击路径
- Identity Explorer
- Microsoft Entra ID 支持

回收许可证

购买许可证后，在合同有效期内，您的许可证总数保持不变，除非您购买更多许可证。但是，当您从环境的目录服务中删除已启用用户时，Tenable Identity Exposure 会实时回收许可证。

超出许可证限制

为应对因硬件更新、环境突然扩大或未预期威胁导致的用量高峰，Tenable 许可证具有弹性。但是，当扫描的资产数量超过许可数量时，Tenable 会明确通知您超额情况，随后分三个阶段缩减功能。

场景	结果
您拥有的已启用身份数量连续三天超出许可数量	Tenable Identity Exposure 中将显示一条消息。
您拥有的已启用身份数量超出许可数量已达 15 天及以上	Tenable Identity Exposure 中将显示有关功能缩减的消息和警告。
您拥有的已启用身份数量超出许可数量已达 45 天及以上	Tenable Identity Exposure 中将显示一条消息；导出功能遭禁用。

许可证已到期

您购买的 Tenable Identity Exposure 许可证在合同有效期内有效。在许可证到期前 30 天，用户界面中会显示警告。在此续约期间，请与您的 Tenable 代表合作，以添加或移除产品或更改许可证数量。

许可证到期后，您将无法再登录 Tenable 平台。

管理许可证

Tenable Identity Exposure 需要来自 Tenable 或通过授权企业合作伙伴提供的许可证文件。许可证用户计数涵盖所有启用的用户和服务帐户。

您必须上传许可证文件才能配置和使用 Tenable Identity Exposure。

Tenable Identity Exposure 许可证包括：

- 攻击指标
- 风险暴露指标
- 以上两者结合的许可证

若要查看许可证，请执行以下操作：

- 在“Tenable Identity Exposure”中，点击“**系统**  ”>“**关于**”选项卡。

  此时会出现许可证。

许可证使用

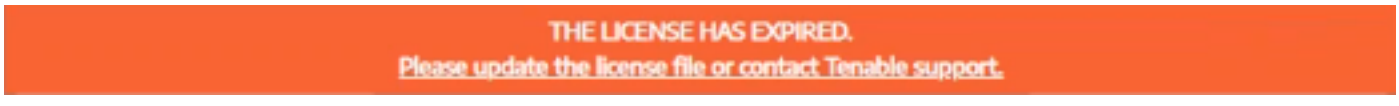
对于本地安装，Tenable Identity Exposure 会在有互联网连接时跟踪许可证使用情况。

许可证有效性

只要满足以下条件，Tenable Identity Exposure 许可证就会持续有效：

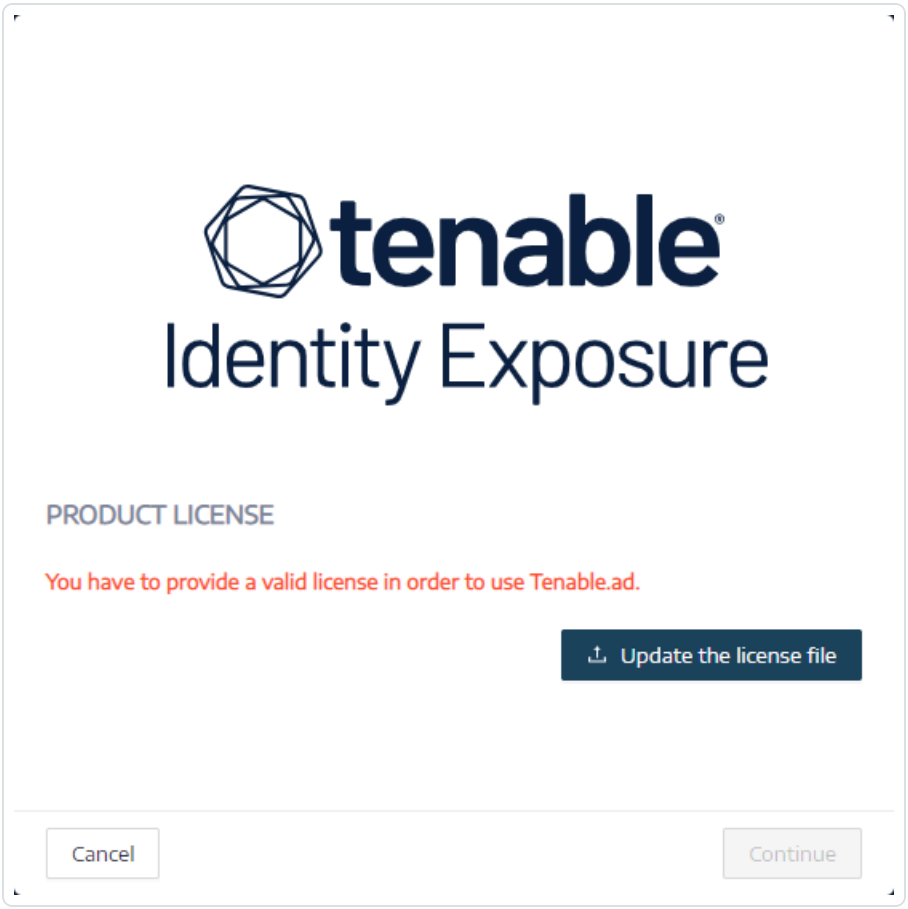
- 用户数量不超过许可证上授予的数量。
- 尚未到达到期日期。

如果不满足上述任一条件，Tenable Identity Exposure 会显示警告，提示您更新许可证：



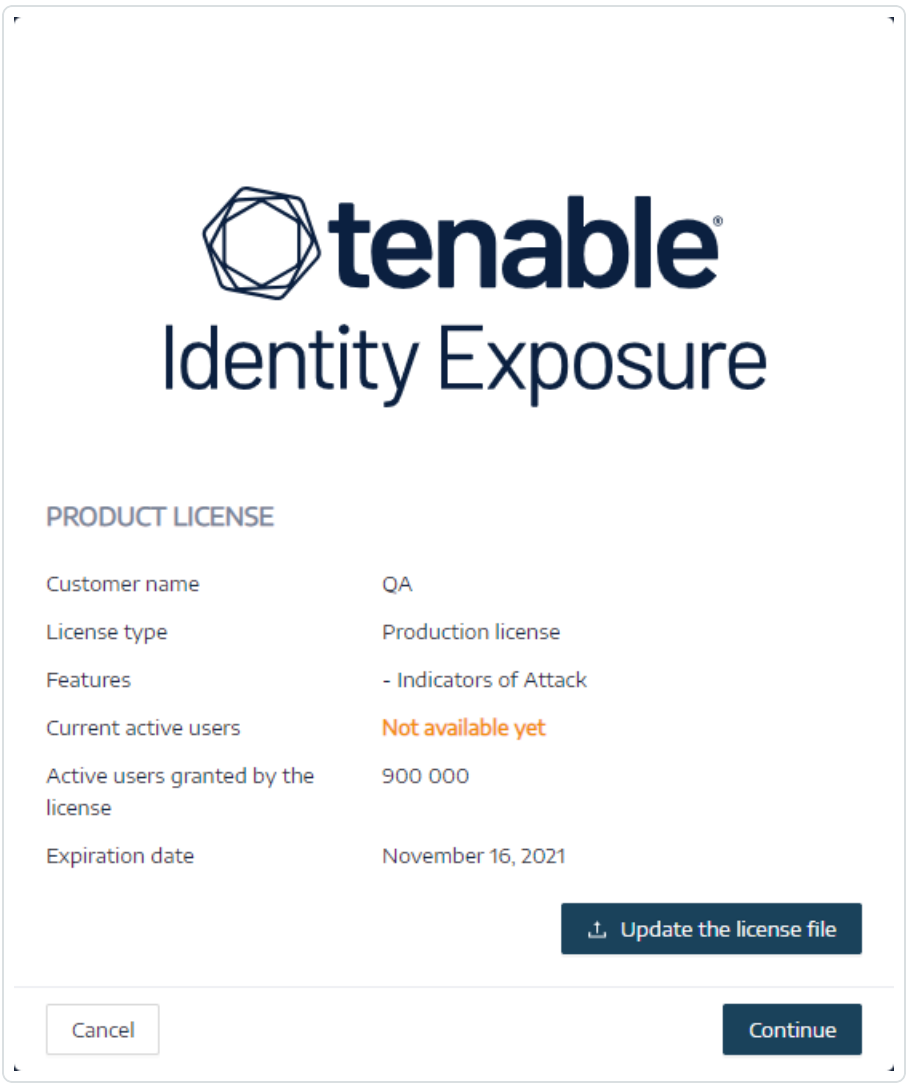
上传许可证文件的步骤：

1. 在登录窗口中，点击“**更新许可证文件**”。



2. 浏览到许可证文件所在的位置，然后点击“**打开**”。

   以下示例为已成功应用的许可证文件：



3. 点击“**继续**”，打开 Tenable Identity Exposure。

更新许可证文件的步骤：

1. 在 Tenable Identity Exposure 中，点击“**系统**”和“**关于**”。
2. 点击“**更新许可证文件**”。
3. 浏览到许可证文件所在的位置，然后点击“**打开**”。

   Tenable Identity Exposure 会更新许可证文件。如果许可证文件无效，请联系客户支持。

故障排除 Tenable Identity Exposure

以下主题可帮助您解决使用 Tenable Identity Exposure (原名 Tenable.ad) 时可能出现的问题:

- Tenable Identity Exposure 诊断工具
- SYSVOL 强化干扰 Tenable Identity Exposure

Tenable Identity Exposure 诊断工具

Tenable Identity Exposure 提供诊断工具，可让您检索与 Tenable Identity Exposure 安装相关的日志信息，以便客户支持可以分析任何问题并为您提供帮助。

您可以从 Tenable 下载门户下载此诊断工具。

注意：此诊断工具仅适用于 Tenable Identity Exposure 的**本地安装** 。

诊断工具具有下列功能：

- 确定当前计算机（已启动可执行文件的计算机）是托管存储管理器 (SM)、安全引擎节点 (SEN) 还是目录侦听器 (DL)。
- 扫描环境以查找网络上可用的其他 Tenable Identity Exposure 安装。
- 检测与 Tenable Identity Exposure 安装相关的日志源列表，以相应地测试和检索与这些安装有关的信息。
- 检索失败的 Tenable Identity Exposure 安装尝试中的 MSI 日志。

获得最佳结果的一些提示

- 在 SEN 上运行诊断工具。
- 以权限升级用户身份运行诊断工具以激活大部分或所有日志源。
- 如要检测 SM 或其他安装，请检查您是否具备以下条件：
  - 该配置允许在远程计算机上运行远程命令 (Invoke-Command cmdlet)。
  - 该配置允许对磁盘进行远程访问。
  - 当前用户帐户已启用并允许 WMI。

如要运行诊断工具，请执行以下操作：

1. 从 Tenable 下载门户下载文件 `TenableAdDiagnosticTool.OnPrem.Console.exe`。
2. 在 Tenable Identity Exposure 计算机（最好是托管 SEN 的计算机）上以管理员身份运行可执行文件。
3. 在出现提示时，输入下列任意一项选项：

- `E` – 所有日志(默认选项)
- `Msi` – 与 Tenable Identity Exposure 安装相关的日志
- `Tenable` – 与 Tenable Identity Exposure 有关的日志

4. 按 Enter。

   诊断工具会扫描您的安装。扫描完成后,将在当前目录中生成压缩文件输出。

5. 将此压缩文件发送给 Tenable Identity Exposure 客户支持。确保不以任何方式更改文件内容。

使用命令行运行诊断工具:

1. 在命令行中,以管理员身份在 Tenable Identity Exposure 计算机(最好是托管 SEN 的计算机)上运行可执行文件 `TenableAdDiagnosticTool.OnPrem.Console.exe`。

   诊断工具会扫描您的安装。扫描完成后,将在当前目录中生成压缩文件输出。

2. 将此压缩文件发送给 Tenable Identity Exposure 客户支持。确保不以任何方式更改文件内容。

其他选项

借助命令行,诊断工具还提供以下选项:

- `--` 帮助 – 诊断工具使用情况的简要说明。
- `--` 命令 – 用于测试计算机功能和扫描其他安装的 Powershell / WMI 查询列表。

SYSVOL 强化干扰 Tenable Identity Exposure

SYSVOL 是位于 Active Directory 域中每个域控制器 (DC) 的共享文件夹。它存储组策略 (GPO) 的文件夹和文件。SYSVOL 的内容会在所有 DC 中进行复制，且可通过通用命名约定 (UNC) 路径（例如 `\\<example.com>\SYSVOL` 或 `\\<DC_IP_or_FQDN>\SYSVOL`）进行访问 。

SYSVOL 强化是指使用 UNC 强化路径参数，也称为"UNC 强化访问"、"强化的 UNC 路径"、"UNC 路径强化"或"强化路径"等。此功能会响应组策略中的 MS15-011 (KB 3000483) 漏洞。许多网络安全标准（例如 CIS 基准测试）要求强制执行此功能。

当您在服务器消息块 (SMB) 客户端上应用此强化参数时，它实际上会提高已加入域的计算机的安全性，以确保从 SYSVOL 检索的 GPO 内容不会被网络上的攻击者篡改。但在某些情况下，此参数也会干扰 Tenable Identity Exposure 的操作。

如果您发现强化的 UNC 路径中断了 Tenable Identity Exposure 和 SYSVOL 共享之间的连接，请遵循此故障排除部分中的指南。

受影响的环境

以下 Tenable Identity Exposure 部署选项可能会遇到此问题：

- 本地
- 具有安全中继的 SaaS

此部署选项不受影响：

- 带 VPN 的 SaaS

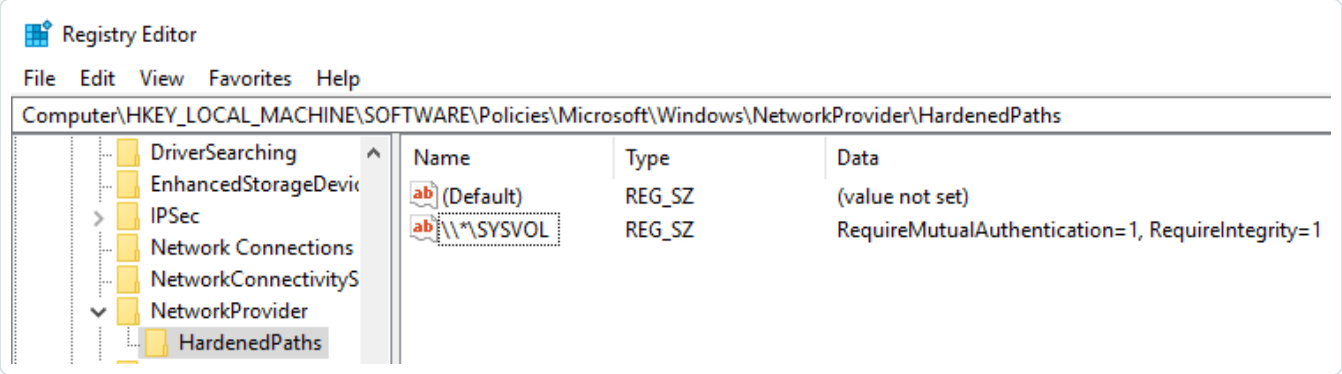
SYSVOL 强化是一个客户端参数，这意味着它在连接 SYSVOL 共享的计算机上运行，而不是在域控制器上运行。

Windows 默认启用此参数，且此参数会干扰 Tenable Identity Exposure。

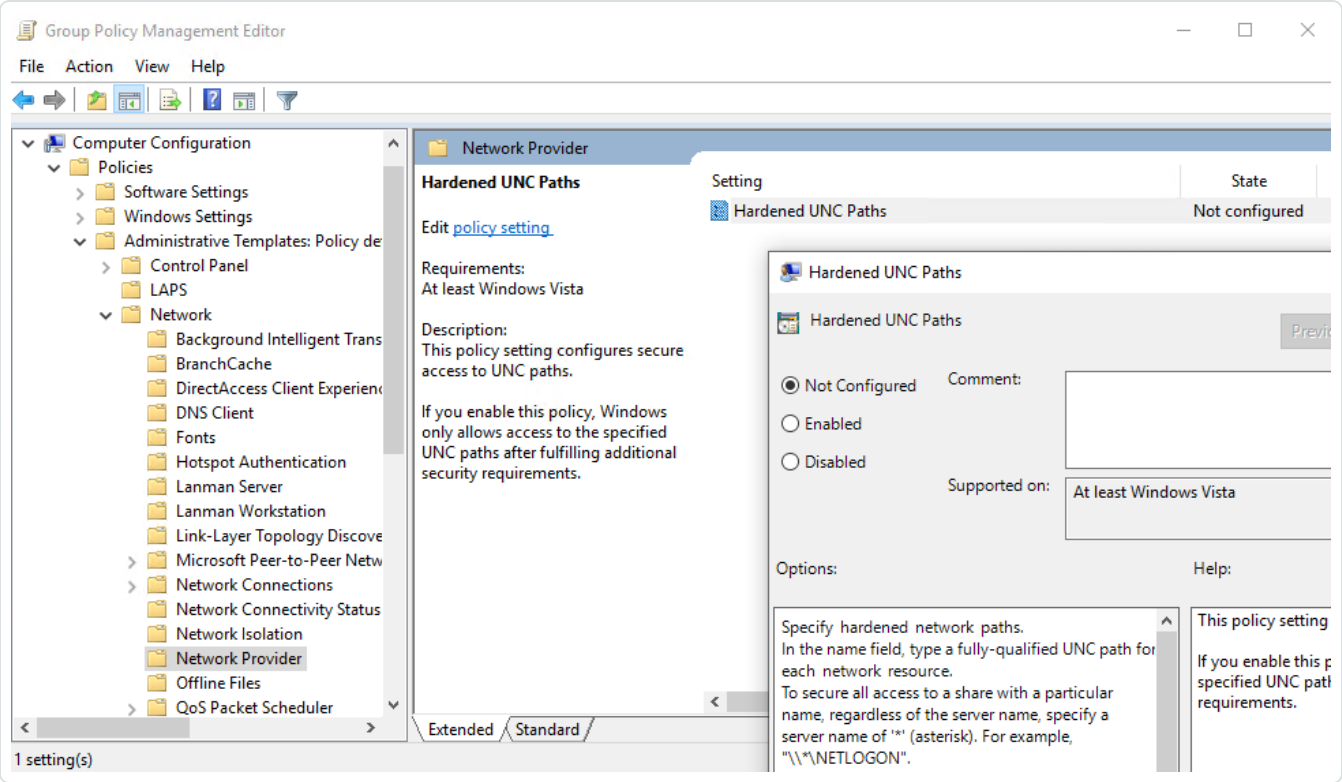
一些组织亦想确保激活此参数，并通过使用相关的 GPO 设置或直接设置相应的注册表项来强制执行。

- 您可以在"`HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths`"

下找到与 UNC 强化路径相关的注册表项：



- 您可以在“Computer Configuration/Administrative Templates/Network/Network Provider/Hardened UNC paths”下找到相应的 GPO 设置：



当引用 SYSVOL 的 UNC 路径(例如“*\SYSVOL”) 将参数“RequireMutualAuthentication”和“RequireIntegrity”设置为值“1”时，会强制执行 SYSVOL 强化。

SYSVOL 强化问题的迹象

当您怀疑存在与 Tenable Identity Exposure 相关的 SYSVOL 强化干扰时，请检查以下内容：

1. 在 Tenable Identity Exposure 中，转至“**系统**”>“**域管理**”以查看每个域的 LDAP 和 SYSVOL 初始化状态。

   具有正常连接的域会显示一个绿色指示符，而存在连接问题的域会显示一个持续尝试连接的指示符。

2. 在目录侦听器或中继计算机上，打开日志文件夹：`<Installation Folder>\DirectoryListener\logs`。

3. 打开 Ceti 日志文件并搜索字符串“SMB 映射创建已失败”或“访问被拒绝”。包含此短语的错误日志表示可能在目录侦听器或中继计算机上发生了 UNC 强化。

修复选项

有两个可能的修复选项：切换到 Kerberos 身份验证或禁用 SYSVOL 强化。

切换到 Kerberos 身份验证

此为首选选项，因为这样做可以避免禁用强化功能。

仅当使用 NTLM 身份验证连接受监控的域控制器时，SYSVOL 强化才会干扰 Tenable Identity Exposure。这是因为 NTLM 与“`RequireMutualAuthentication=1`”参数不兼容。Tenable Identity Exposure 也支持 Kerberos。如果正确配置和使用 Kerberos，则没有必要禁用 SYSVOL 强化。有关更多信息，请参阅Kerberos 身份验证

禁用 SYSVOL 强化

如果无法切换到 Kerberos 身份验证，您还可以选择禁用 SYSVOL 强化。

Windows 默认启用 SYSVOL 强化，因此仅删除注册表项或 GPO 设置是不够的。您必须明确禁用强化，并且仅在托管目录侦听器（本地）或中继（具有安全中继的 SaaS）的计算机上应用此更改。这样做不会影响其他计算机，并且您永远不需要在域控制器本身上禁用 SYSVOL 强化。

托管目录侦听器（本地）或中继（具有安全中继的 SaaS）的计算机上所使用的 Tenable Identity Exposure 安装程序已在本地禁用 SYSVOL 强化。但是，环境中的 GPO 或脚本可能会删除或覆盖注册表项。

有两种可能的情况：

- 如果目录侦听器或中继计算机**未加入域**，即您不能使用 GPO 配置计算机。您必须禁用注册表中的 SYSVOL 强化（请参阅 注册表 - GUI 或 注册表 - PowerShell）。
- 如果目录侦听器或中继计算机**已加入域**（Tenable Identity Exposure 不建议此做法），即您可以直接在注册表中应用设置（请参阅 注册表 - GUI 或 注册表 - PowerShell）或使用 GPO 应用设置。使用其中任何一种方法，您必须确保 GPO 或脚本不会覆盖注册表项。您可以通过以下任一方式执行此操作：
  - 仔细检查此计算机上适用的所有 GPO。
  - 应用更改并稍等片刻，或使用“`gpupdate /force`”强制应用 GPO，然后检查注册表项是否保留其值。

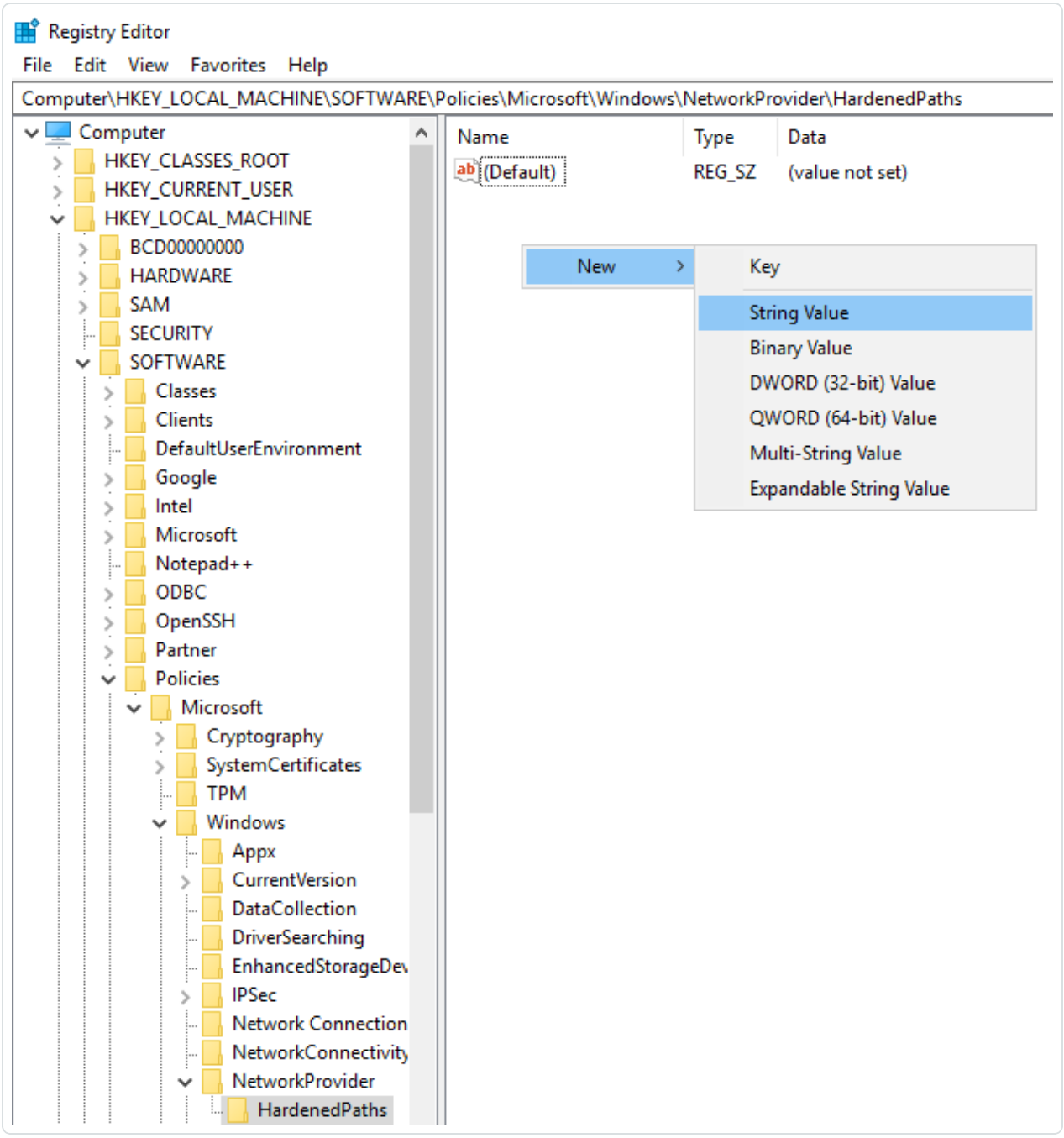
重新启动目录侦听器或中继计算机后，修改后的域上的抓取指示符应变为绿色指示符：

注册表 - GUI

使用 GUI 在注册表中禁用 SYSVOL 强化：

1. 以管理权限连接目录侦听器或中继计算机。
2. 打开注册表编辑器并导航至:HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths。
3. 创建名为“*\SYSVOL”的表项(如果尚不存在),操作如下所示:

a. 在右窗格中单击鼠标右键，然后选择“**新建**”>“**字符串值**”。



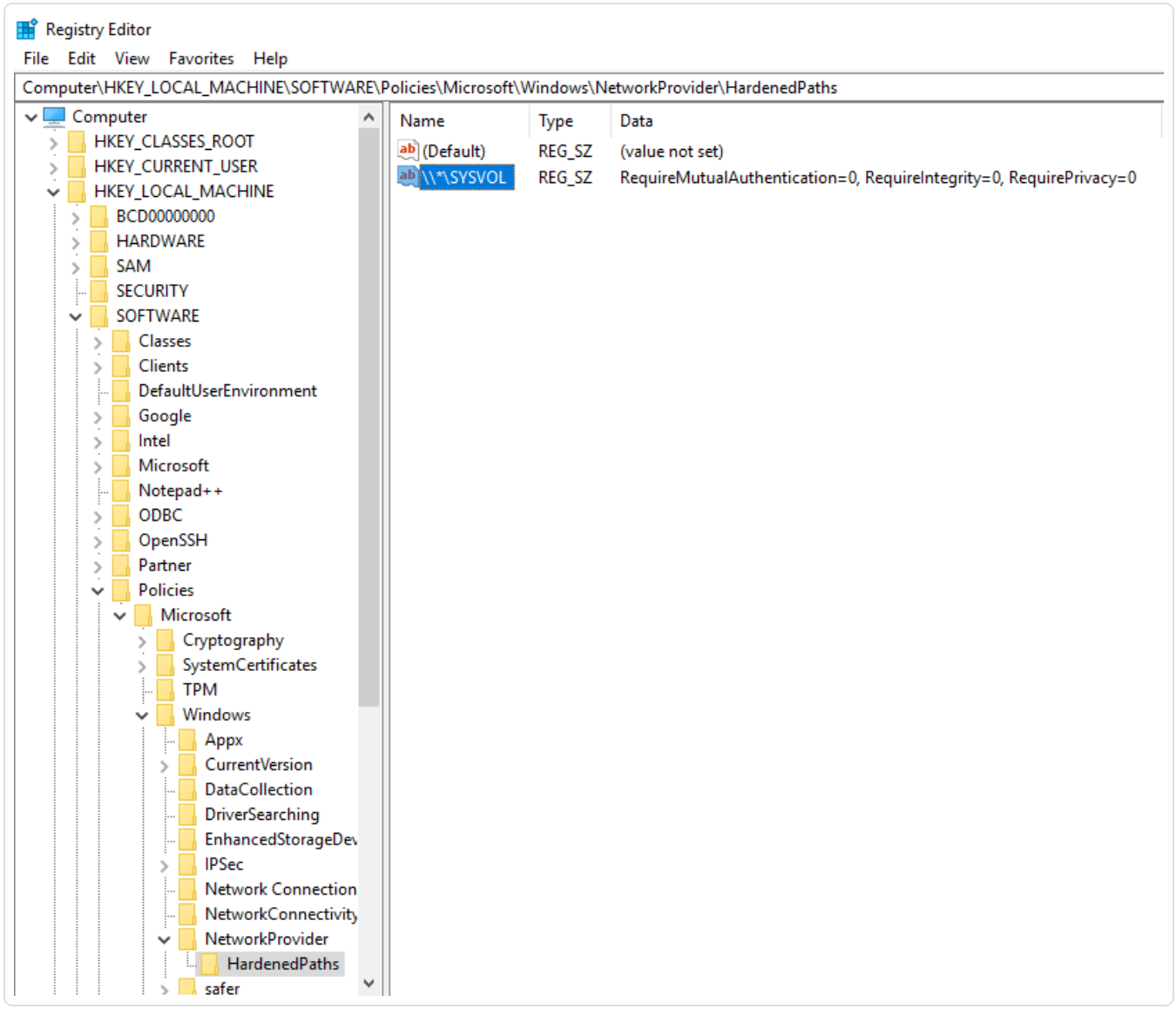
b. 在名称字段中，输入“*\SYSVOL”。

4. 双击“*\SYSVOL”表项（新创建的或以前存在的）以打开“**编辑字符串**”窗口。

5. 在“**值**”数据字段中，输入以下值：`RequireMutualAuthentication=0`，`RequireIntegrity=0`，`RequirePrivacy=0`

6. 单击“**保存**”。

   结果应如下所示：



7. 重新启动计算机。

注册表 - PowerShell

使用 PowerShell 在注册表中禁用 SYSVOL 强化：

1. 使用此 PowerShell 命令收集 UNC 强化路径注册表项的当前值以供参考：

```
Get-Item -Path "HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths"
```

2. 设置建议值：

```
New-ItemProperty -Path
"HKLM:\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\HardenedPaths" -Name "\\*\SYSVOL" -
Value "RequireMutualAuthentication=0, RequireIntegrity=0, RequirePrivacy=0"
```

3. 重新启动计算机。

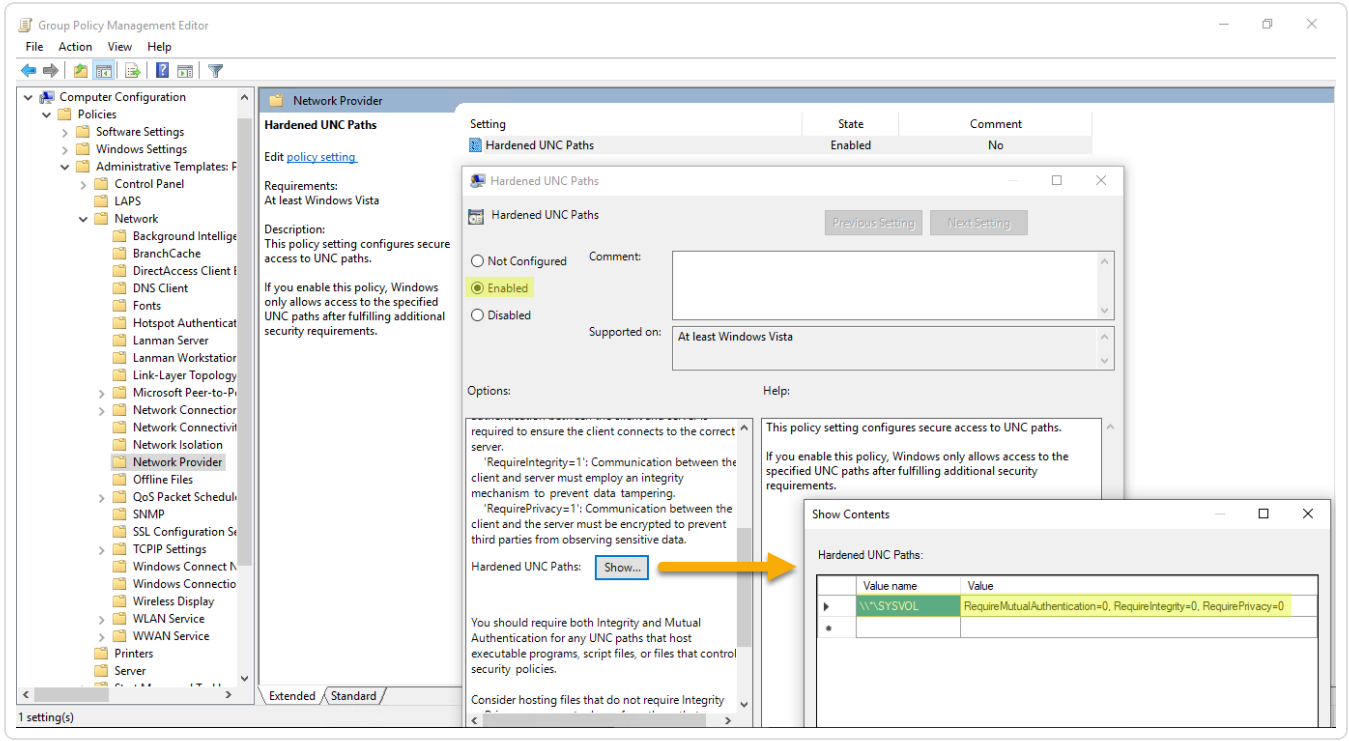
GPO

先决条件：您必须以 Active Directory 用户身份进行连接，该用户有权在域上创建 GPO 并将其链接到包含 Tenable Identity Exposure 目录侦听器或中继计算机的组织单位。

使用 GPO 禁用 SYSVOL 强化：

1. 打开组策略管理控制台。
2. 创建新的 GPO。
3. 编辑 GPO 并浏览到以下位置：`Computer Configuration/Administrative Templates/Network/Network Provider/Hardened UNC paths`。
4. 启用此设置并使用以下命令创建新的强化 UNC 路径：
   - 值名称 = `\\*\SYSVOL`
   - 值 = `RequireMutualAuthentication=0`、`RequireIntegrity=0`、`RequirePrivacy=0`

   结果应如下所示：



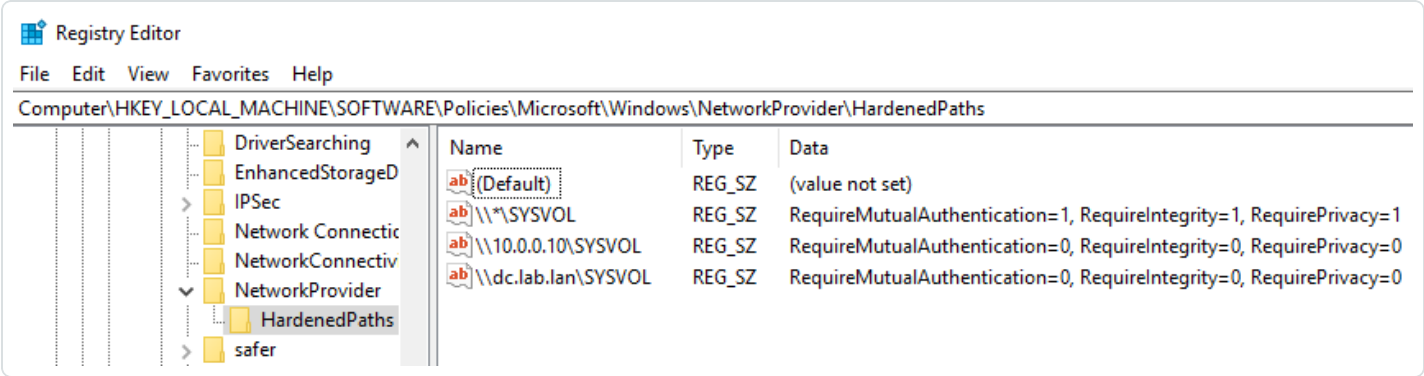
5. 点击“**确认**”以确认。

6. 将此 GPO 链接到包含 Tenable Identity Exposure 目录侦听器或中继计算机的组织单位。您还可以使用安全组筛选条件 GPO 功能确保此 GPO 仅适用于此计算机。

特定 UNC 路径例外情况

之前的过程使用通配符 UNC 路径 (“*\SYSVOL”) 禁用 SYSVOL 强化。您也可以仅针对特定 IP 地址或 FQDN 禁用强化。这意味着您可以对“*\SYSVOL”保持启用 UNC 强化路径设置(值“1”) , 并同时拥有与 Tenable Identity Exposure 中配置的域控制器的每个 IP 地址或 FQDN 相对应的例外情况。

下图显示为所有服务器(“*”) 启用的 SYSVOL 强化示例 , “10.0.0.10”和“dc.lab.lan”除外 , 它们是我们在 Tenable Identity Exposure 中配置的域控制器 :



您可以使用上述注册表或 GPO 方法添加这些附加设置。

注意：您必须指定在 Tenable Identity Exposure 中配置的确切值（例如，如果 Tenable Identity Exposure 配置使用 FQDN，则无法指定 IP 地址。）。此外，请记住在每次更改 Tenable Identity Exposure 域管理页面中的 IP 地址或 FQDN 时更新这些表项。

禁用 SYSVOL 强化的风险

SYSVOL 强化是一项安全功能，禁用它会引发可能的风险。

- 对于未加入域的计算机，禁用 SYSVOL 强化没有风险。由于这些计算机不应用 GPO，因此不会从 SYSVOL 共享获取内容以执行。
- 对于 Tenable Identity Exposure 不建议加入域的但已加入域的计算机（目录侦听器或中继计算机），如果在目录侦听器或中继计算机与域控制器之间存在使攻击者处于“中间人”情况的潜在风险，则禁用 SYSVOL 强化会不安全。在这种情况下，Tenable Identity Exposure 建议您切换为 Kerberos 身份验证。

此停用范围仅限于目录侦听器或中继计算机，而不包括其他域计算机，更绝不包括域控制器。