ManageEngine
ADAudit Plus

最小权限

manageengine.cn/products/active-directory-audit/

目录

概述

要启动 ManageEngine ADAudit Plus 并开始审核您的 Active Directory (AD)、Azure AD、Windows 服务器、文件服务器、工作站和其他网络附加存储 (NAS) 设备，需要一定的最低权限。本指南将引导您完成这些先决条件以及如何设置具有所需权限的服务帐户。

1. 对于产品启动

1.1 安装文件夹权限

为了增强 ADAudit Plus 安装的安全性，从版本 7251 开始，对 ADAudit Plus 文件夹的默认访问权限仅限于用于安装的用户帐户。*系统*，*管理员*，和*域管理员*群组。但是，要允许其他用户启动 ADAudit Plus，您可以按照以下步骤操作。*为 ADAudit Plus 文件夹分配修改权限 对于开始使用产品的用户。*

如果您使用的是较早版本的 ADAudit Plus，或者您最近升级到了 7251 版本，则有两种方法可以保护 ADAudit Plus 文件夹免受未经授权的修改：

- 使用 SecureDeployment.exe
- 手动修改权限

1.2 使用 SecureDeployment.exe

SecureDeployment.exe 文件将通过以下方式自动增强 ADAudit Plus 安装的安全性：

- 阻止非管理组访问 ADAudit Plus 文件夹。
- 将“修改”权限分配给选定的用户帐户。
- 如果 ADAudit Plus 已安装为服务，则需要配置“登录”帐户凭据。

运行 SecureDeployment.exe 文件：

- 前往*<安装目录>|ADAudit Plus|bin*文件夹（如果您最近已升级到版本 7251）并找到*SecureDeployment.exe*文件。

> 笔记：如果您使用的是早期版本，下载 SecureDeployment 压缩文件，解压缩并将其内容复制到*<安装目录>|ADAudit Plus|bin*文件夹。

- 右键单击SecureDeployment.exe文件和选择以管理员身份运行。
- 输入“1”并继续删除非管理组的权限，即 *已验证用户、内置用户、创建者所有者、所有受限应用程序包、所有应用程序包、受信任的安装程序和所有人。*
- 权限移除后，按任意键打开选择用户或组对话框。
- 输入要授予启动 ADAudit Plus 权限的用户名称，然后单击 核对姓名确认选择。

> 笔记：如果您已使用“登录”帐户凭据将 ADAudit Plus 安装为服务，请输入与该帐户关联的用户名。

- 点击好的。

> 笔记：如果您想将启动 ADAudit Plus 的权限分配给多个用户，请按照以下步骤操作。*为启动产品的用户分配对 ADAudit Plus 文件夹的修改权限*。

1.3 手动修改权限

如果您不想使用*SecureDeployment.exe*为了加强 ADAudit Plus 安装的安全性，您可以确保以下几点：

禁用 ADAudit Plus 文件夹的继承。

- 转到<安装目录>\ManageEngine。
- 右键单击ADAudit Plus 文件夹并选择特性。
- 点击安全按下 Tab 键，然后点击先进的。
- 在*高级安全设置*点击窗口禁用继承。
- 点击好的。

从 ADAudit Plus 文件夹的访问控制列表中删除非管理组。

- 转到<安装目录>\ManageEngine。
- 右键单击ADAudit Plus 文件夹并选择特性。
- 点击安全按下 Tab 键，然后点击先进的。
- 在高级安全设置窗户下方权限条目，选择非管理用户和组，然后单击消除。
- 点击好的。

为域管理员、管理员和 SYSTEM 组分配完全控制权限。

- 转到<安装目录>\ManageEngine。
- 右键单击 ADAudit Plus 文件夹并选择特性。
- 点击安全按下 Tab 键，然后点击先进的。
- 在权限点击 Tab 键添加。
- 点击选择一位校长链接并添加*域管理员*、*管理员*， 和*系统*团体。
- 点击好的。
- 旁边类型，选择允许，旁边适用于，选择此文件夹、子文件夹和文件。
- 在下面基本权限检查完全控制盒子。
- 点击好的。

为启动该产品的用户分配对 ADAudit Plus 文件夹的修改权限。

- 转到<安装目录>\ManageEngine。
- 右键单击 ADAudit Plus 文件夹并选择特性。
- 点击安全按下 Tab 键，然后点击先进的。
- 在权限点击 Tab 键添加。
- 点击选择一位校长点击链接，输入要授予启动 ADAudit Plus 权限的用户名称，然后点击核对姓名确认选择。
- 点击好的。
- 旁边类型，选择允许旁边适用于，选择此文件夹、子文件夹和文件。
- 在下面基本权限检查调整盒子。
- 点击好的。

> 笔记：若产品以服务形式运行并配置了登录账户，请确保该账户拥有修改权限。

1.4 将 ADAudit Plus 从防病毒和终端保护中排除

为防止出现任何性能问题并避免对 ADAudit Plus 数据库（PostgreSQL）的运行造成潜在干扰，必须将某些目录从 ADAudit Plus 服务器上的防病毒软件和终端安全防护程序中排除。此排除操作至关重要，因为防病毒软件和终端安全防护程序有时会将 ADAudit Plus 安装目录中的数据库和其他文件错误地标记为威胁或漏洞。

由于防病毒软件和终端保护软件，您在使用 ADAudit Plus 时可能会遇到的性能问题包括：处理事件和警报时延迟高、向数据库或数据引擎添加数据时吞吐量低以及数据库文件损坏。

为获得最佳性能，建议您将 java.exe 和 postgres.exe 使用的目录从 ADAudit Plus 服务器上的防病毒和终端保护程序中排除。需要排除的目录如下所示：

<安装文件夹>\ManageEngine\ADAudit Plus\index <安装文件夹>\ManageEngine\ADAudit Plus\eventdata <安装文件夹>\ManageEngine\ADAudit Plus\alertdata <安装文件夹>\ManageEngine\ADAudit Plus\ehcache <安装文件夹>\ManageEngine\ADAudit Plus\apps\dataengine-xnode\data <安装文件夹>\ManageEngine\ADAudit Plus\pgsql

> 笔记：java.exe 和 postgres.exe 进程分别位于： *<安装目录>|ManageEngine|ADAudit Plus|jre|bin|java.exe <安装目录>|ManageEngine|ADAudit Plus|pgsql|bin|postgres.exe*

2. 对于数据引擎

2.1 引言

ADAudit Plus 中的 DataEngine 组件能够高效地存储和检索日志数据。它通过加快数据搜索和检索速度来增强可扩展性。

默认情况下，数据引擎将数据存储在 C:\Program Files (x86)\ManageEngine\ADAudit Plus\apps 目录下。该文件夹的大小取决于收集和存储的日志量。例如，每 100,000 条日志条目大约需要 15MB 的空间。因此，请务必在磁盘上分配足够的空间来存储日志数据。

> 笔记：误删此文件夹中的任何文件都可能导致数据丢失，因此强烈建议不要删除此文件夹中的任何文件。

数据引擎作为一项独立的服务运行，即：*ManageEngine ADAudit Plus - DataEngine XNode*此服务使用端口 29118 进行通信，为了 ADAudit Plus 的最佳运行，需要保持此服务运行。

您可以通过修改参数值来更改正在使用的端口。*xnode.connector.port*在以下文件中。请确保在以下两个文件中使用相同的值：

<安装目录>|apps|dataengine-xnode|conf|dataengine-xnode.conf <安装目录>|conf|DataEngine|engines|xnode|dataengine-xnode.conf

2.2 必要权限

启动 ManageEngine ADAudit Plus 服务的用户或服务帐户需要以下权限：

- 对产品安装文件夹拥有完全控制权。
- 拥有启动、安装和停止 ManageEngine ADAudit Plus - DataEngine XNode 服务的权限。

授予产品安装文件夹完全控制权限的步骤：

- 登录机器其中 ADAudit Plus 已安装，并具有域管理员权限。
- 导航至产品安装文件夹（C:\Program Files (x86)\ManageEngine\ADAudit Plus）。右键单击并选择属性 > 安全 > 编辑。选择用户帐户你想提供完全控制访问权限并点击添加。查看允许在下面完全控制访问。点击好的。

提供启动、安装和停止 DataEngine 服务所需权限的步骤
您可以将用户添加到本地管理员组，或者使用组策略授予其必要的权限。

A. 将用户添加到本地管理员组：

- 登录机器ADAudit Plus 已安装。
- 前往开始 > 控制面板 > 编辑本地用户和组 > 组。双击管理员。
- 在管理员中特性点击打开的窗口添加。
- 选择完整目录。选择所需用户并单击添加。
- 点击好的。

B. 使用组策略提供必要的权限：

- 使用域管理员凭据登录到任何具有以下权限的域控制器：活动目录用户和计算机。
- 前往开始 > Windows 管理工具 > Active Directory 用户和计算机。
- 右键单击领域点击您要将组织单元添加到的目录。新建 > 组织单元。
- 在*新对象 - 组织单元*在打开的窗口中，输入所需内容OU名称并移动电脑ADAudit Plus 服务在 OU 中运行的位置。
- 前往开始 > Windows 管理工具 > 组策略管理。

> 笔记：组策略管理控制台 (GPMC) 默认情况下不会安装在所有工作站和服务器上。您可以按照以下步骤操作：本页 在所需的成员服务器和工作站上安装 GPMC。

- 导航至最近创建的内容俄亥俄大学。右键单击俄亥俄大学并选择创建 GPO 并将其链接到此处。在*新GPO*在窗口中，输入所需内容姓名点击好的。
- 选择新创建的GPO，右键单击并选择编辑。在*组策略管理编辑器*去电脑配置 > 策略 > Windows 设置 > 安全设置 > 系统服务。右键单击ManageEngine ADAudit Plus - DataEngine XNode并选择特性。在新窗口中，检查定义此策略设置点击方框。编辑安全设置。
- 在*安全*在打开的标签页中，搜索并找到要授予必要权限的用户帐户。选择该用户帐户并授予权限。完全访问权限去它。
- 点击**好的**。
- 此组策略需 要在整个域中强制执行。为此，请转到：开始 > 命令提示符。输入gpupdate/force。

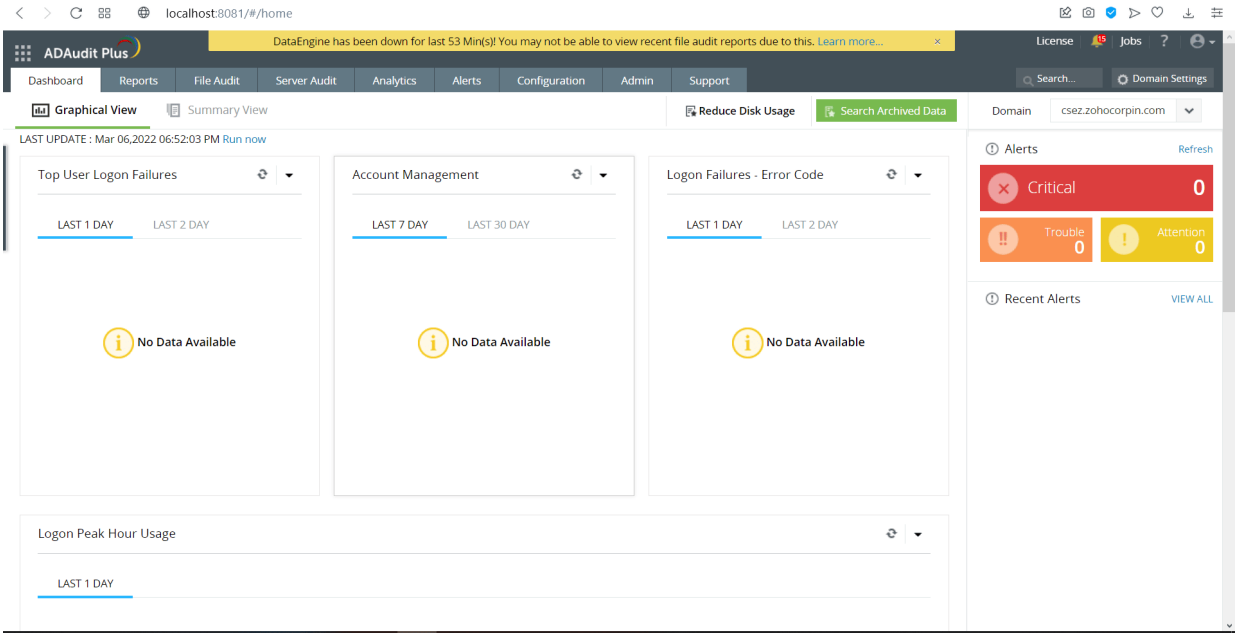
授予归档和恢复审计数据权限的步骤

- 要查找存档文件夹的位置：打开 ADAudit Plus → 管理 → 存档事件 → 向下滚动查看位置。
- 登录机器ADAudit Plus 已安装，并拥有域管理员权限。→ 找到存档文件夹 → 右键单击 该文件夹并选择属性 > 安全 > 编辑。选择用户帐户 你想提供完全控制访问权限并点击添加。查看允许在下面完全控制访问。点击好的。
- 如果存档文件夹是共享文件夹，请转到分享标签页 →高级共享… → 权限 → 选择用户帐户你想提供完全控制访问权限并点击添加。→ 检查允许 在下面完全控制访问。点击好的。

> 笔记：如果归档文件夹是共享文件夹，则务必确保用于运行 DataEngine 服务的服务帐户与用于运行 ADAudit Plus 服务的服务帐户相同，并且您已将完全控制权限分配给该服务帐户。

2.3 故障排除

1.数据引擎已宕机“x”分钟。因此，您可能无法查看最近的文件审核报告。



解决方案：

1. 打开 ADAudit Plus 日志文件夹中的 DataEngine.log 文件，即 <installation_dir>\logs。

2. 检查 DataEngine.log 文件中是否存在以下列出的错误：

- 无法安装 ManageEngine ADAudit Plus - DataEngine XNode 服务 - 访问被拒绝。
- 无法启动 ManageEngine ADAudit Plus - DataEngine XNode 服务 - 访问被拒绝。

```
[10:36:37:091]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: DE XNode START :: XNode is not running! Going to start it...|
[10:36:37:091]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: DE XNode START :: STARTING DataEngine XNode Service @ 127.0.0.1... |
[10:36:37:091]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: STARTING Local DataEngine XNode Service...|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #-----------------------------------------------|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # COMMAND : ..\apps\dataengine-xnode\bin\dataengine-xnode.bat -t|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # INPUT STREAM : |
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # --------------|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # |
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # ERROR STREAM : |
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # --------------|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # wrapperm | Unable to start the ManageEngine ADAudit Plus - DataEngine XNode service - Access is denied. (0x5)|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #-----------------------------------------------|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # STATE after start command : UNINSTALLED|
[10:36:37:154]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: INSTALLING Local DataEngine XNode Service...|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #-----------------------------------------------|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # COMMAND : ..\apps\dataengine-xnode\bin\dataengine-xnode.bat -i|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # INPUT STREAM : |
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # --------------|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # |
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # ERROR STREAM : |
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # --------------|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # wrapperm | Unable to install the ManageEngine ADAudit Plus - DataEngine XNode service - Access is denied. (0x5)|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #-----------------------------------------------|
[10:36:37:216]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]: CHECKING if Local DataEngine XNode service is installed...|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #-----------------------------------------------|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # COMMAND : ..\apps\dataengine-xnode\bin\dataengine-xnode.bat -q|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # INPUT STREAM : |
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # --------------|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # wrapperm | The ManageEngine ADAudit Plus - DataEngine XNode Service is installed.|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # ERROR STREAM : |
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # --------------|
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  # |
[10:36:37:279]|[01-07-2022]|[DataEngineLogger]|[INFO]|[25]:  #-----------------------------------------------|
```

2.1 如果文件中出现这些错误，则表示由于权限不足，DataEngine 服务不可用。要授予启动、安装和停止 DataEngine 服务所需的足够权限，请按照以下步骤操作。此处列出 。

2.2 如果这些内容不在文件中，那么联系我们的支持团队 他们将协助您调试 DataEngine 服务的问题。

3. 用于 AD、Windows Server 和工作站审核

3.1 概述

ADAudit Plus 在提供域管理员凭据后会立即开始审核活动。如果您不想提供域管理员凭据，请按照本指南中的步骤设置服务帐户，使其仅拥有审核环境所需的最低权限。

> 笔记：如果要在 ADAudit Plus 中配置多个域，我们建议为每个域创建单独的服务帐户。

3.2 创建新用户、组和 GPO

1. 创建新用户

我。使用域管理员权限登录到您的域控制器 → 打开“Active Directory 用户和计算机” → 右键单击 您的域 → 新建 → 用户 → 将用户命名为“*ADAudit Plus*“。”

2. 创建一个新组

我。使用域管理员权限登录到您的域控制器 → 打开“Active Directory 用户和计算机” → 右键单击 您的域 → 新建 → 组 → 将组命名为“*ADAudit Plus 权限组*“。”

二、将所有已审计的计算机添加为“成员”。*ADAudit Plus 权限组*：右键单击“*ADAudit Plus 权限组*

- “ → 属性 → 成员 → 添加所有要审核的域控制器、Windows 服务器和工作站。

3. 创建一个新的域级 GPO 并将其链接到所有已审核的计算机

由于在单个计算机上配置权限是一个复杂的过程，因此创建了一个域级 GPO 并将其应用于所有受监控的计算机。

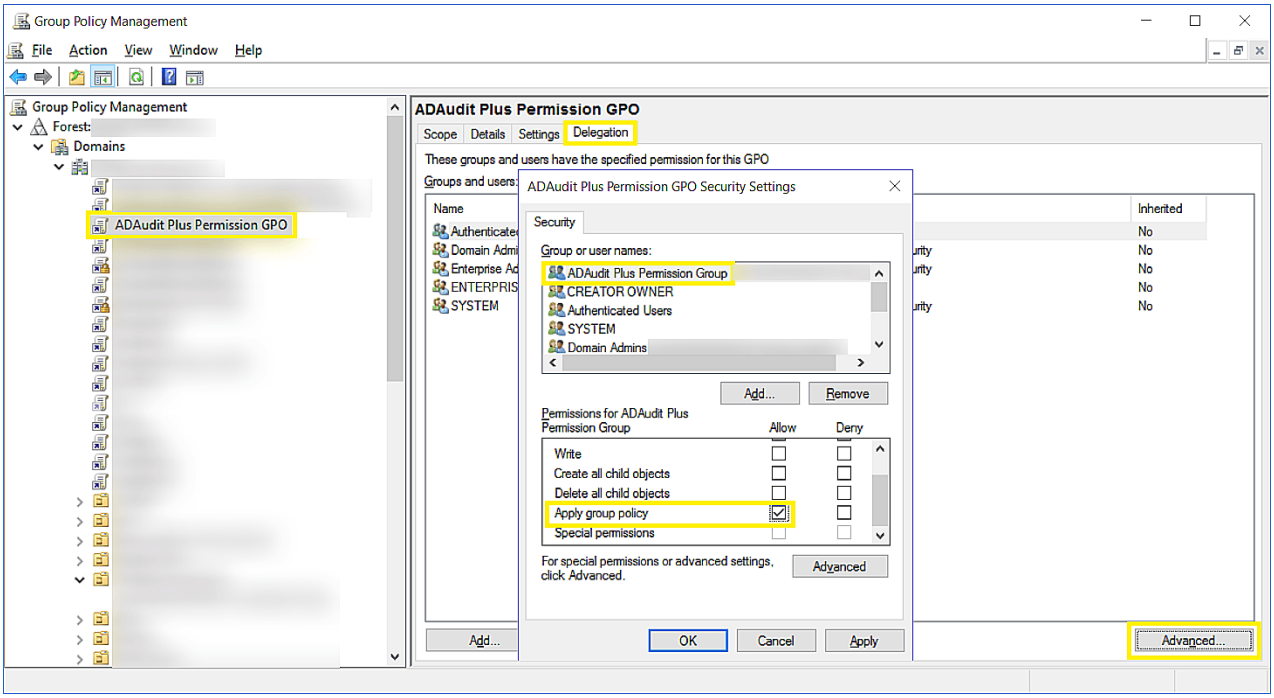
我。使用域管理员权限登录到您的域控制器。

ii. 创建新的域级 GPO：
打开组策略管理控制台 → 右键单击 您的域 → 在此域中创建一个 GPO 并将其链接到此处 → 将 GPO 命名为“*ADAudit Plus 权限 GPO*“

iii. 移除“已验证用户”组的“应用组策略”权限：
点击“ADAudit Plus 权限 GPO”→导航到右侧面板，点击“委派”选项卡→“高级”→点击“已验证用户”→删除“应用组策略”权限。

iv. 将“ADAudit Plus 权限组”添加到“ADAudit Plus 权限 GPO”的安全筛选器设置中：

打开组策略管理控制台 → 域 → 选择“ADAudit Plus 权限 GPO” → 导航到右侧面板，单击委派选项卡 → 高级 → 添加“ADAudit Plus 权限组” → 选中“应用组策略”。



3.3 事件日志收集所需的权限/许可

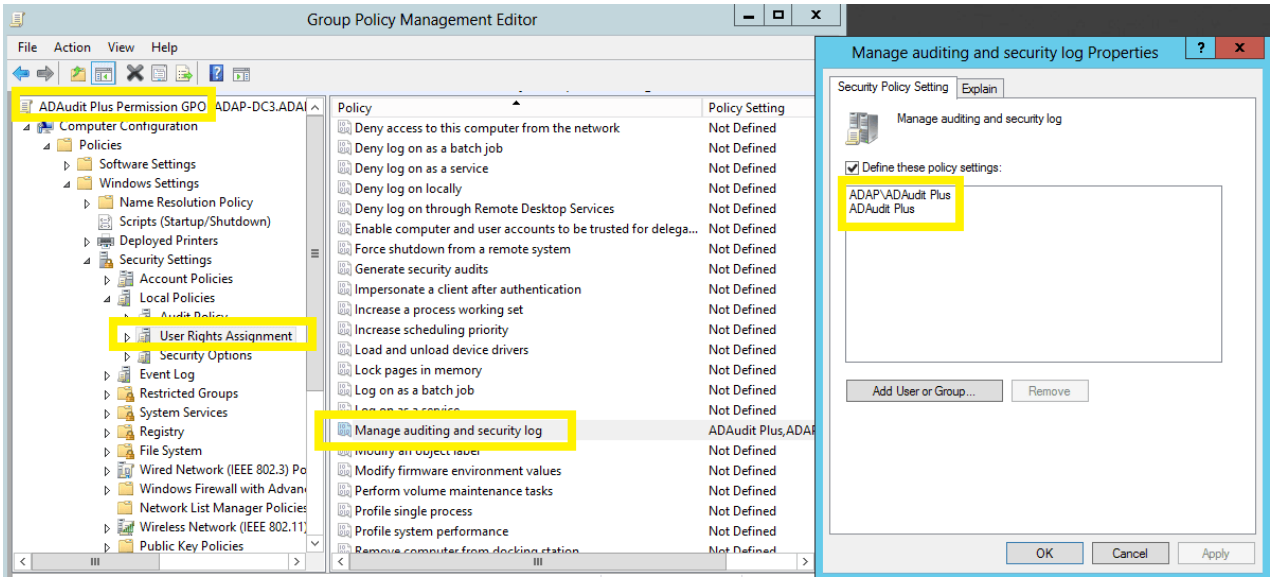
1. 授予用户“管理审计和安全日志”权限

“管理审计和安全日志”权限允许用户定义对象级别的审计。

i. 使用域管理员权限登录到您的域控制器→ 打开组策略管理控制台 → 右键单击 “ADAudit Plus 权限 GPO” → 编辑。

二、在组策略管理编辑器 → 计算机配置 → 策略 → Windows 设置 → 安全设置 → 本地策略 → 用户权限分配中。

三、导航至右侧面板，右键单击“管理审核和安全日志”→“属性”→添加“ADAudit Plus”用户。



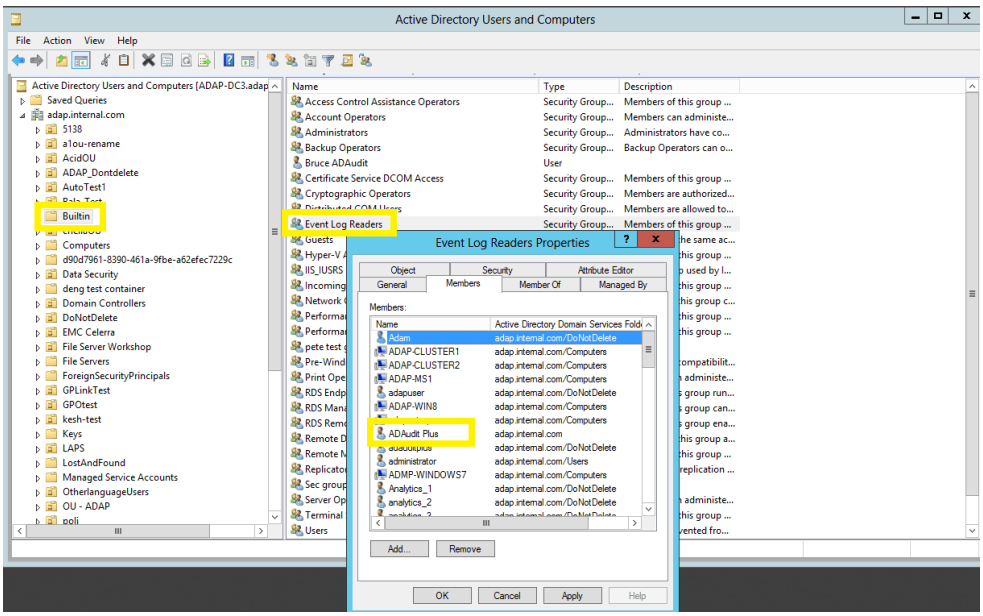
2. 将用户添加到事件日志读取者组

事件日志读取器组的成员将能够读取所有受审计计算机的事件日志。

i. 对于域控制器：

使用域管理员权限登录到您的域控制器→ 打开“Active Directory 用户和计算机”→ 内置容器 → 导航到右侧面板，右键单击“事件日志读取器”

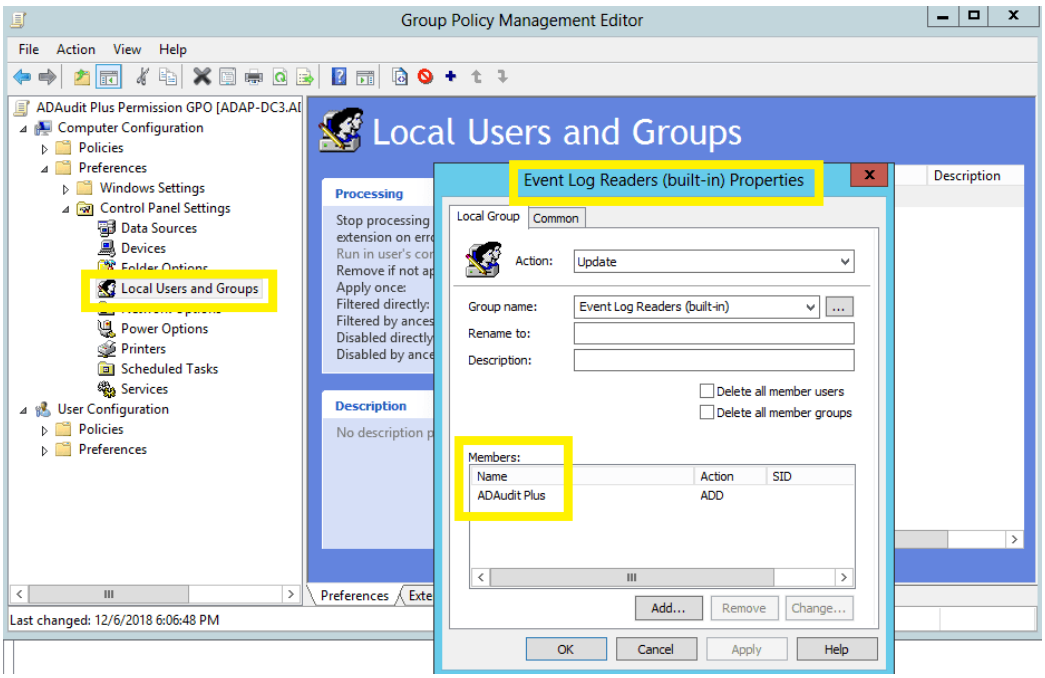
→ 物业 → 会员 →添加“ADAudit Plus”用户。



ii. 对于其他计算机（Windows 服务器和工作站）：

a. 使用域管理员权限登录到您的域控制器→ 打开组策略管理控制台 → 右键单击 “ADAudit Plus 权限 GPO” → 编辑。

b.在组策略管理编辑器中 → 计算机配置 → 首选项 → 控制面板设置 → 右键单击 “本地用户和组” → 新建 → 本地组 → 在组名称下选择“事件日志读取器”组 →添加“ADAudit Plus”用户。



笔记：要读取事件日志，您还需要授予“ADAudit Plus”用户读权限 HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security。

我。使用域管理员权限登录到域控制器 → 打开组策略管理控制台 → 右键单击 “ADAudit Plus 权限 GPO”→ 编辑。

二、在组策略管理编辑器中 → 计算机配置 → 策略 → Windows 设置 → 安全设置 → 右键单击 注册表 → 添加项。

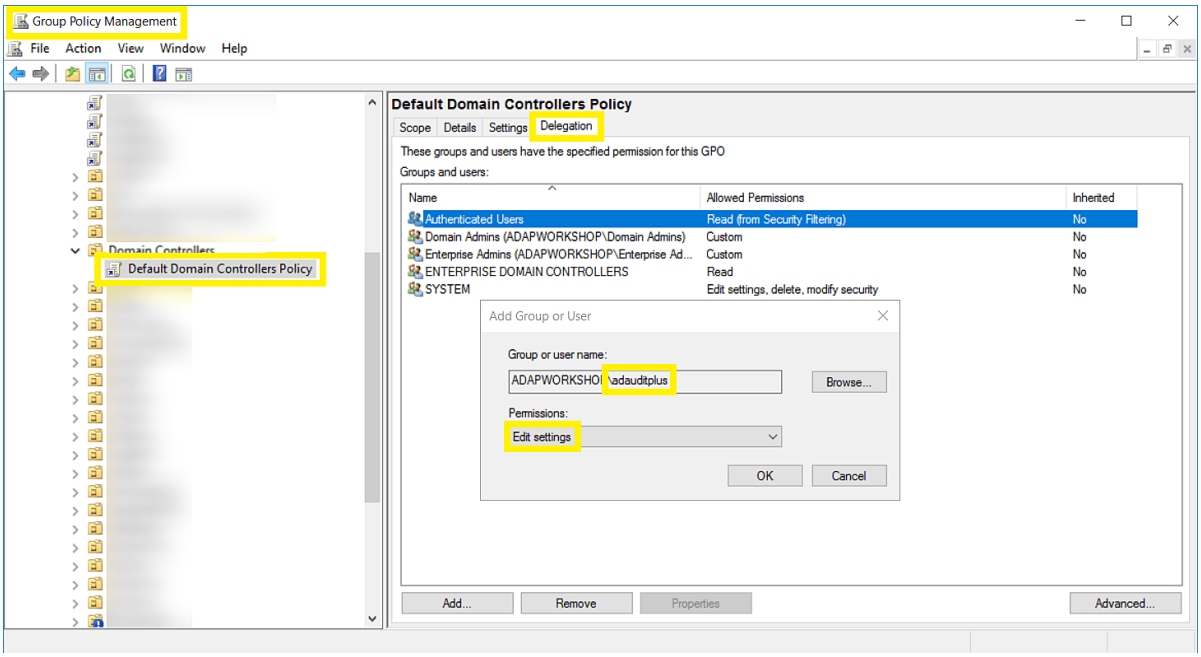
三、在“选择注册表项”窗口中，导航至“计算机”→“系统”→“当前控制集”→“服务”→“事件日志”→“安全”→单击“确定”→“授予”。读允许“ADAudit Plus”用户 → 点击“申请”。

四、在“添加对象”窗口中，选择配置此键，然后 → 将所有子键上的现有权限替换为可继承权限→ 点击确定。

3.4 自动审计策略和对象级审计配置所需的权限/许可

1. 域控制器审核配置所需的权限/许可 授予服务帐户以下权限后，ADAudit Plus 即可自动配置环境中所需的审核策略和对象级审核设置。ADAudit Plus 通过组策略对象 (GPO) 将所需设置推送至包含所有受监控计算机的组。

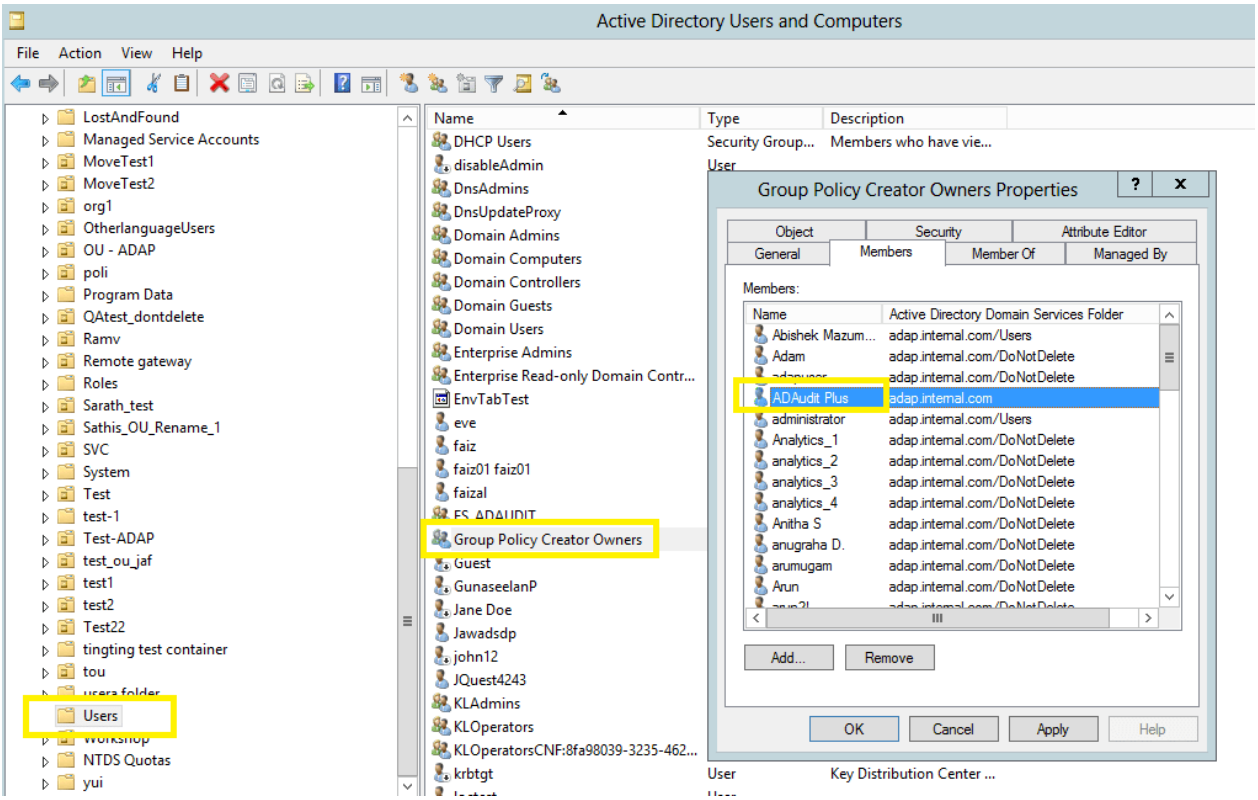
i. 使用域管理员权限登录到您的域控制器→ 打开组策略管理控制台 → 单击“默认域控制器策略” → 导航到右侧面板，单击“委派”选项卡 →添加 ADAudit Plus 使用r → 提供编辑设置的权限。



2. 成员服务器、工作站和文件服务器审计配置所需的权限/许可

2.1 将用户添加到“组策略创建者所有者”组

i. 使用域管理员权限登录到您的域控制器→ 打开“Active Directory 用户和计算机”→ 单击“用户”→ 导航到右侧面板，右键单击“组策略创建者所有者”组 →添加“ADAudit Plus”用户为成员。



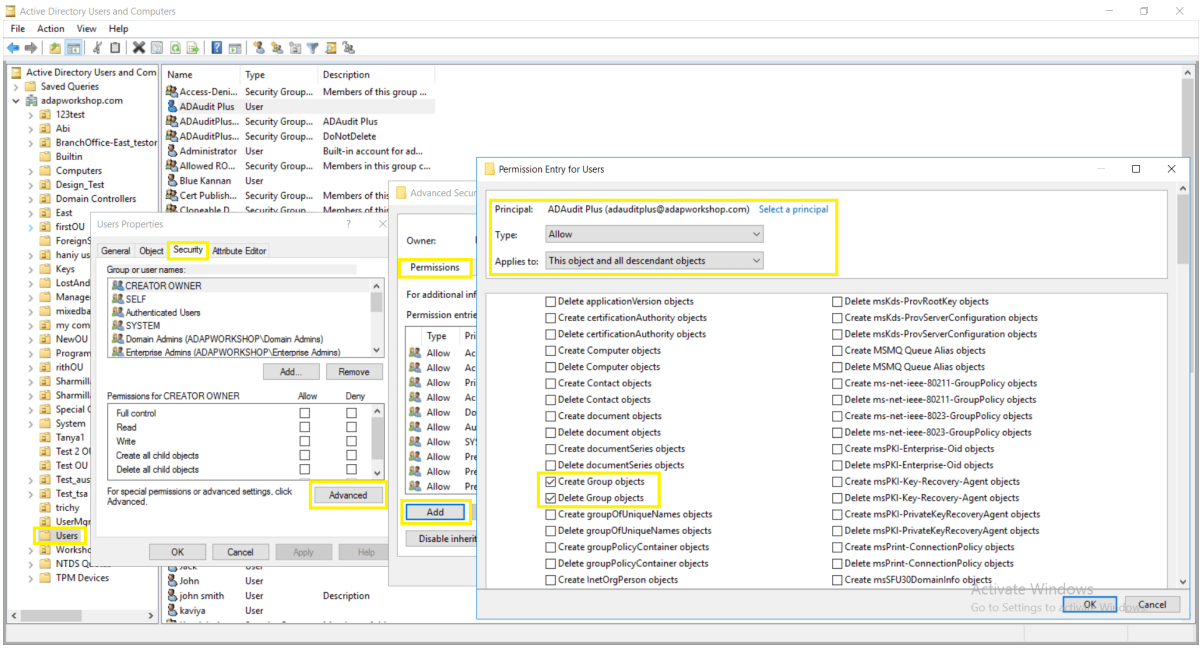
2.2 授予用户和组管理权限

i. 使用域管理员权限登录到您的域控制器→ 打开 Active Directory 用户和计算机。

点击“查看”，确保已启用“高级功能”。这将显示“Active Directory 用户和计算机”中选定对象的高级安全设置。

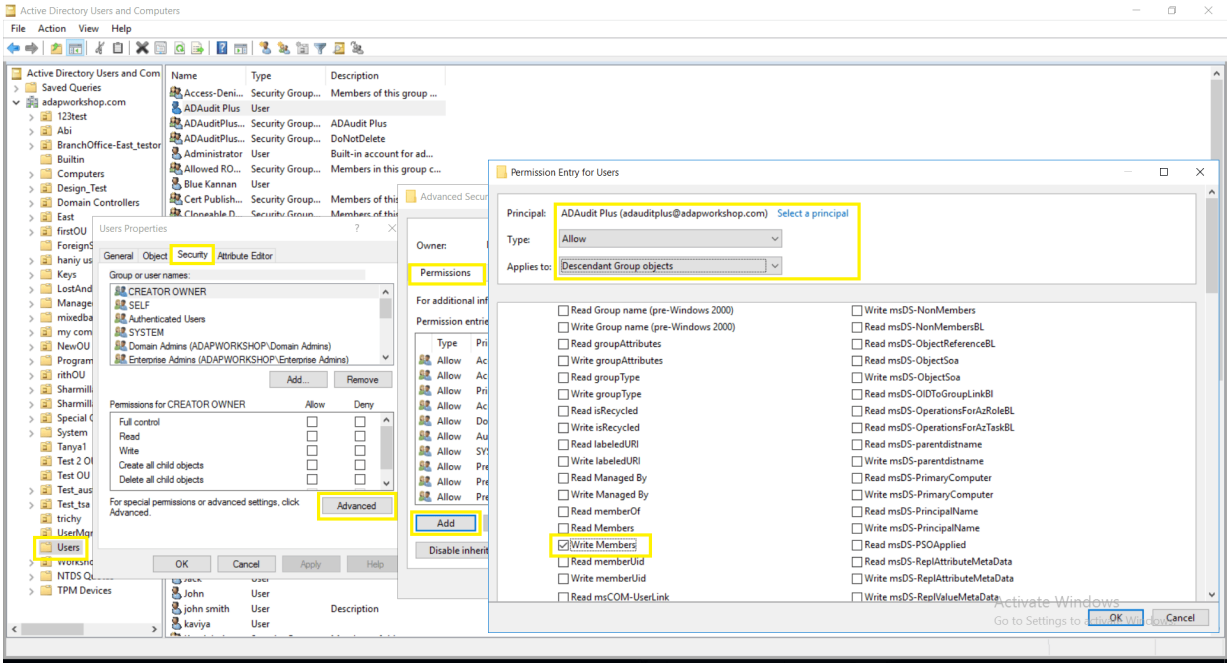
二、右键单击“用户”→“属性”→“安全”→“高级”→“权限”→“添加”→在“用户权限条目”窗口中，选择主体：ADAudit Plus 用户 → 类型：允许 → 应用于：此对象及其所有子对象 → 选择权限：创建组对象和删除组对象。

> 笔记：使用全部清除在选择上述权限之前，请先移除所有权限和属性。



三、从“Active Directory 用户和计算机”控制台 → 右键单击 “用户” → “属性” → “安全” → “高级” → “权限” → “添加” → 在“用户权限条目”窗口中 →选择主体：ADAudit Plus 用户 → 类型：允许 → 应用于：子组对象 → 选择属性：写入成员。

> 笔记：使用全部清除在选择所述属性之前，请先移除所有权限和属性。



4. 用于文件服务器审计

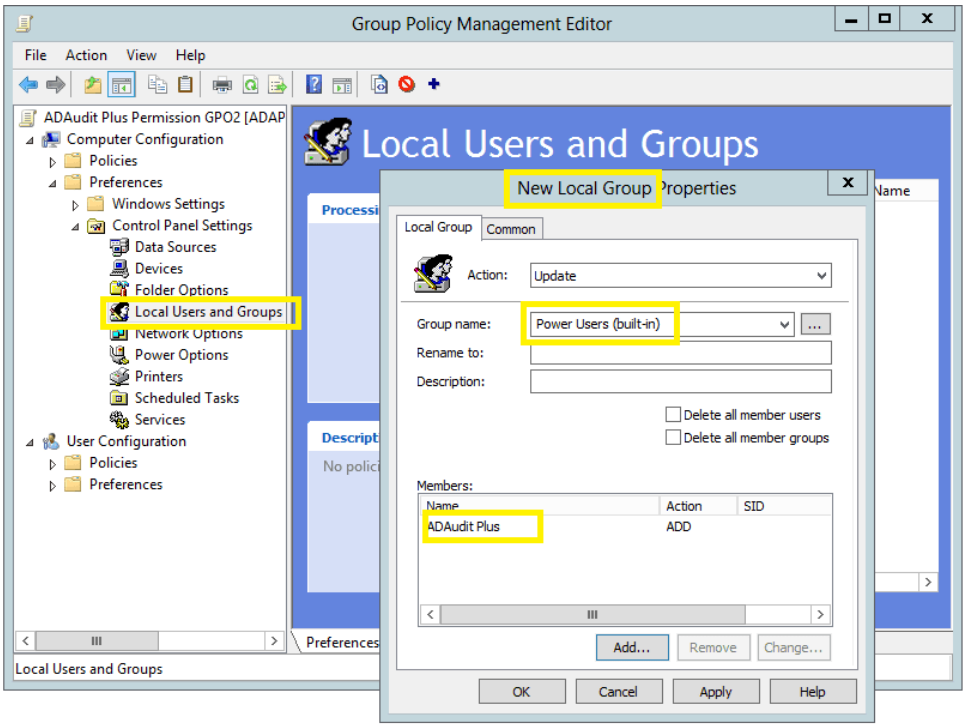
4.1 将用户添加到“高级用户”组

高级用户组成员将能够发现位于 Windows 文件服务器上的共享文件夹。

我。使用域管理员权限登录到您的域控制器 → 打开组策略管理控制台 → 右键单击 “ADAudit Plus Permission GPO” → 编辑。

二、在组策略管理编辑器中 → 计算机配置 → 首选项 → 控制面板设置 → 右键单击 本地用户和组 → 添加本地组。

三、在“新建本地组属性”向导中，选择“操作”下的“更新”→在组名称下选择“高级用户”组→添加“ADAudit Plus”用户。



4.2 授予用户对所有已审计份额的读取权限

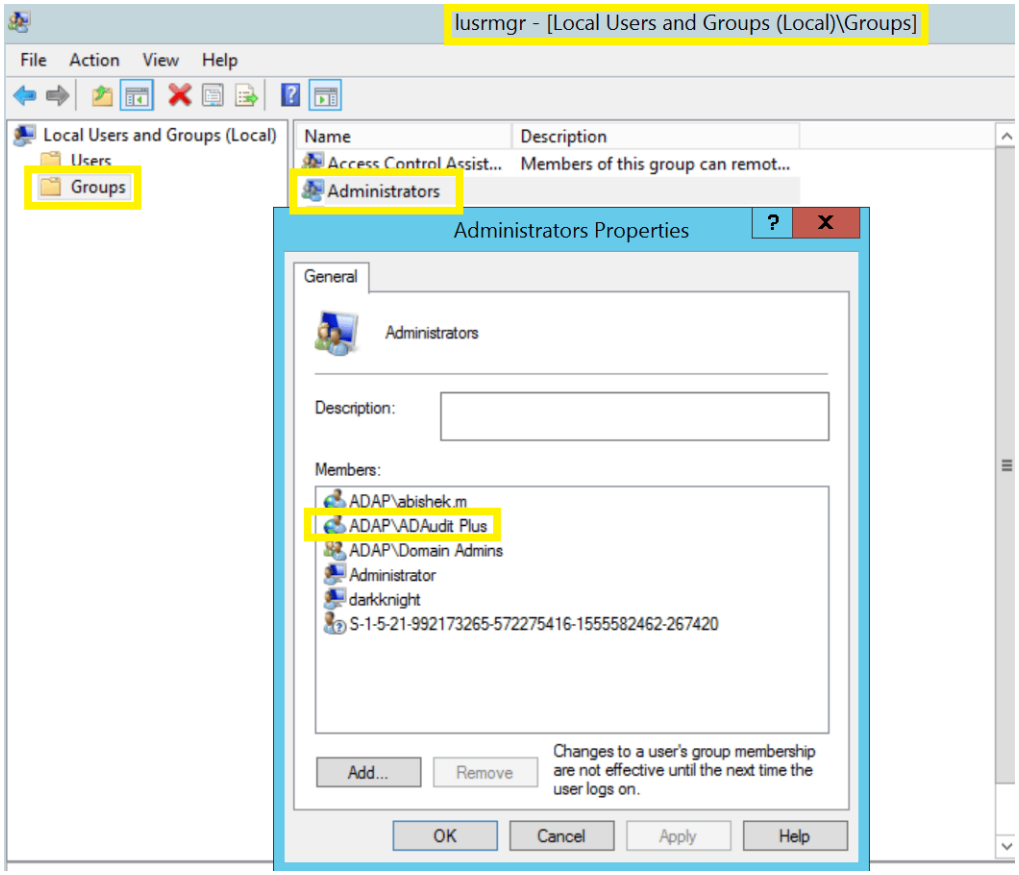
有两种方法可以授予用户对所有已审计共享的读取权限：

i. 将用户设为本地管理员组成员。

a. 使用域管理员权限登录任何计算机→ 打开 MMC 控制台 → 文件 → 添加/删除管理单元 → 选择本地用户和组 → 添加 → 另一台计算机 → 添加目标计算机

b.选择目标计算机 → 打开本地用户和组 → 选择组 → 右键单击 administrators → 属性 →添加“ADAudit Plus”用户。

c. 对每个已审核的 Windows 文件服务器/集群重复上述步骤。

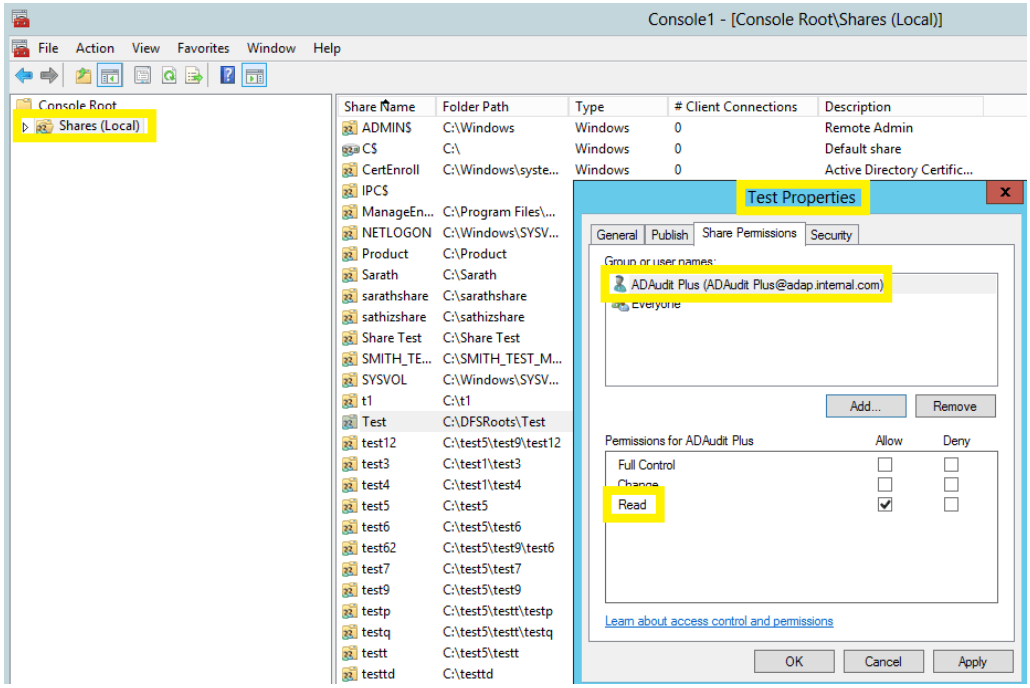


ii. 授予用户对每个已审核共享的共享和 NTFS 读取权限。

a. 使用域管理员权限登录任何计算机→ 打开 MMC 控制台 → 文件 → 添加/删除管理单元 → 选择共享文件夹 → 添加 → 另一台计算机 → 添加目标计算机

b.选择目标计算机 → 选择共享 → 右键单击 → 属性 → 安全 → 编辑 →添加“ADAudit Plus”用户 → 提供共享和 NTFS 读取权限。

c. 对每一股经审计的股份重复上述步骤。



4.3 授予用户 DCOM 和 WMI 权限

> 笔记：文件集群审核也需要 DCOM 和 WMI 权限。

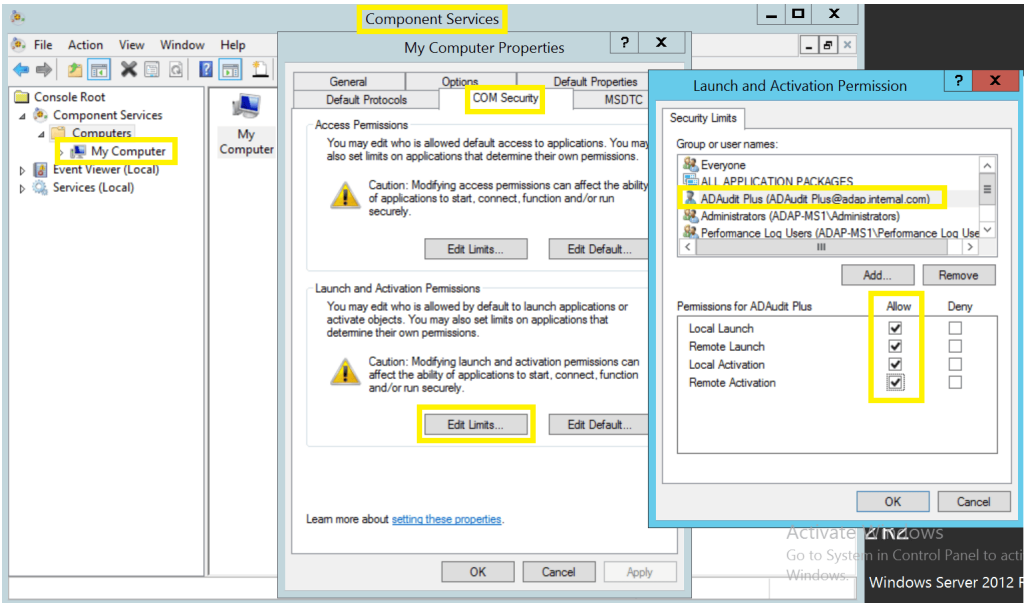
i. 授予 DCOM 权限：

a. 使用域管理员权限登录任何计算机→ 打开组件服务 → 连接到目标计算机 → 右键单击 目标计算机 → 属性 → COM 安全。

b.导航至“启动和激活权限”→“编辑限制”→“安全限制”→添加“ADAudit Plus”用户并授予以下权限：

- 本地发布
- 远程启动
- 局部激活
- 远程激活。

c.对每台被审核的计算机重复上述步骤。



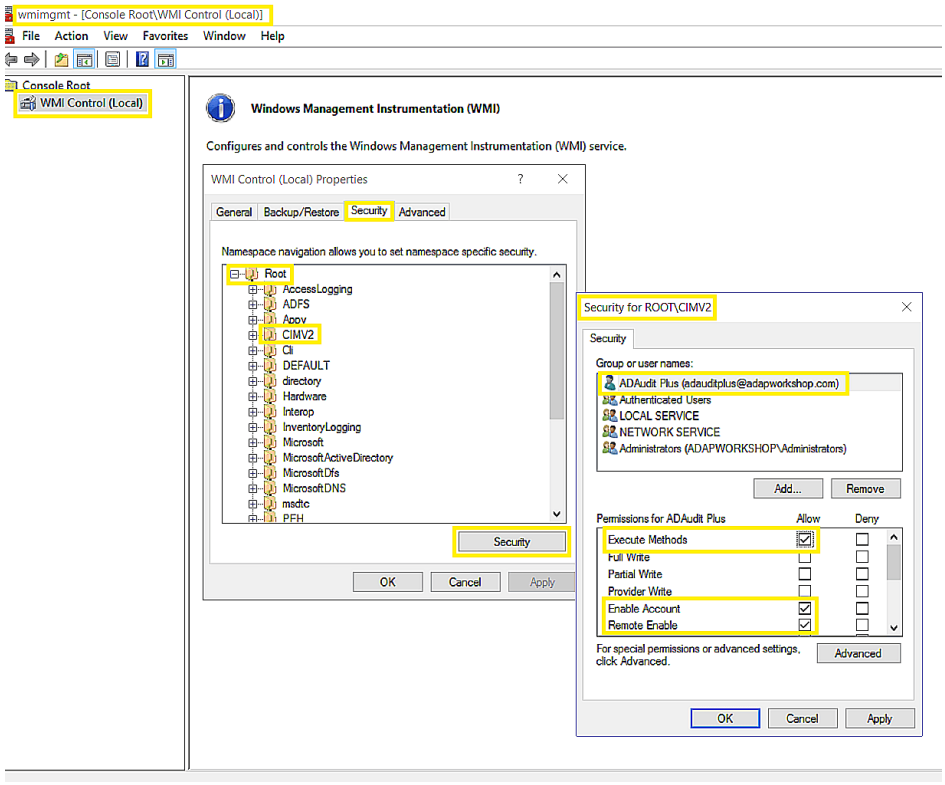
ii. 授予 WMI 权限：

a. 使用域管理员权限登录任何计算机→ 运行 wmimgmt.msc → 右键单击 WMI 控制（本地） → 连接到目标计算机。

b.右键单击 WMI 控制（目标计算机）→ 属性 → 安全 → +Root → CIMV2 → 安全 → 添加“ADAudit Plus”用户并授予以下权限：

- 执行方法
- 启用帐户
- 远程启用

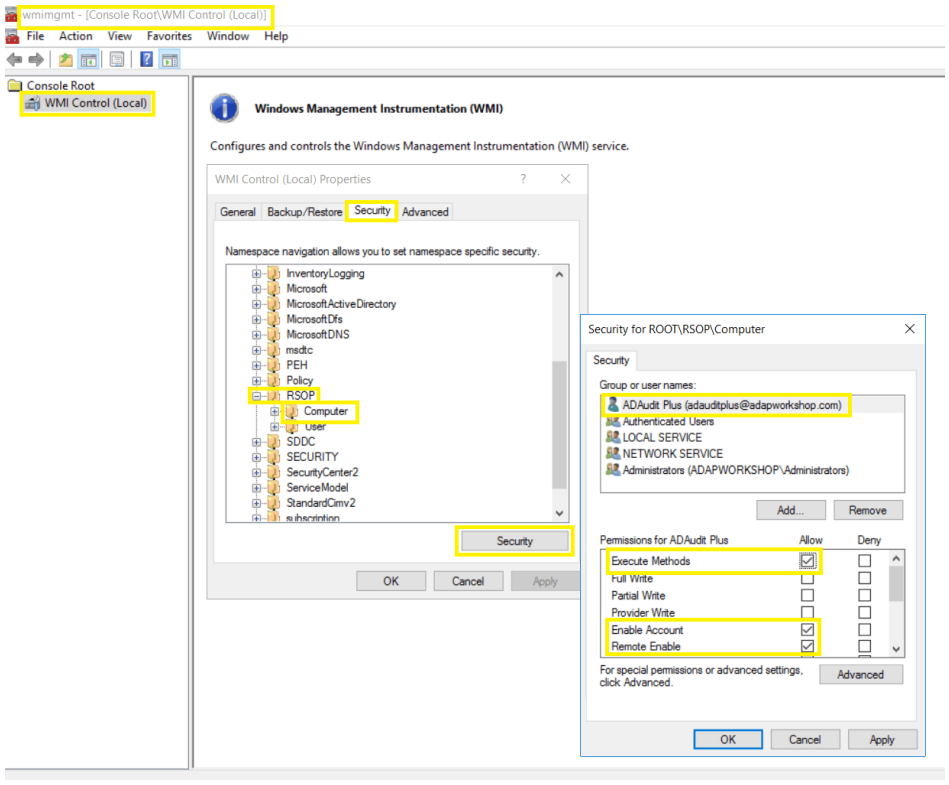
c.点击确定。



d.导航至 +Root → +RSOP → 计算机 → 安全 → 添加“ADAudit Plus”用户并授予以下权限：

- 执行方法
- 启用帐户
- 远程启用

e.点击确定。



f.对每台被审核的计算机重复上述步骤。

笔记：如果需要审核多台计算机，您可能更倾向于通过组策略运行脚本来自动执行上述过程。请联系我们。support@manageengine.cn更多详情请见下文。

4.4 授予用户对 c$ 共享的读取权限

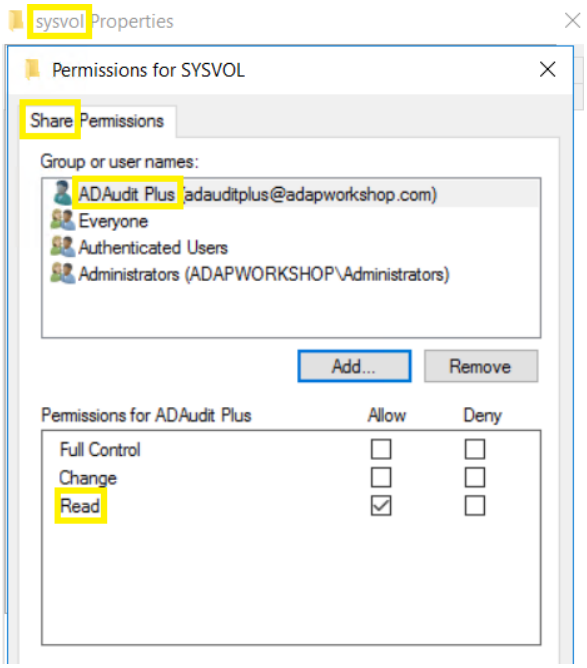
笔记：要访问 NetApp C-Mode 日志文件，需要对 C$ 共享 (\\server_name\C$) 具有读取权限。

5. 其他特权

i. 授予用户对 SYSVOL 文件夹的读取权限：
要进行 GPO 设置更改审核，需要对 SYSVOL 文件夹具有读取权限。

笔记：默认情况下，所有经过身份验证的用户都对 sysvol 文件夹具有读取权限；如果“ADAudit Plus”用户没有读取权限，则必须按照以下步骤提供读取权限。

导航到 sysvol 文件夹（C:\Windows\SYSVOL\sysvol)→ 右键单击 →属性 → 共享 → 高级共享 → 权限→ 添加“ADAudit Plus”用户 → 提供共享读取权限。



ii. 授予用户对产品安装文件夹的完全控制权限：

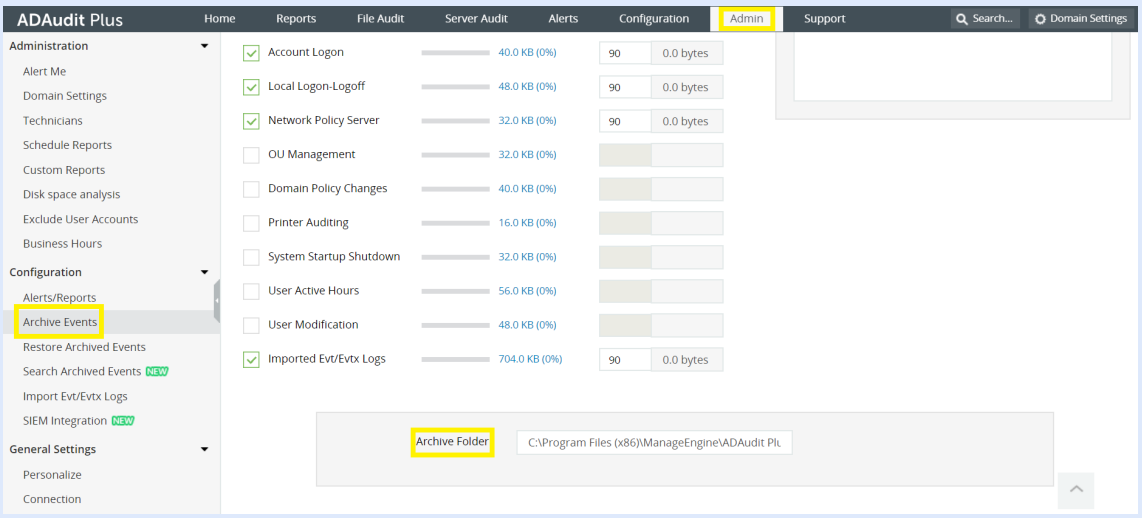
ADAudit Plus 需要对产品安装文件夹拥有完全控制权才能写入数据库。

a. 使用域管理员权限登录到安装了 ADAudit Plus 的计算机→ 找到产品安装文件夹 → 右键单击 → 属性 → 安全 → 编辑 →添加“ADAudit Plus”用户并授予完全控制权限。

iii. 授予用户对 ADAudit Plus 归档文件夹的完全控制权限：
要存储和检索数据库中的归档数据，需要对归档文件夹拥有完全控制权。

笔记：默认情况下，归档文件夹存储在安装文件夹（Installation_folder\ManageEngine\ADAudit Plus\archive）中。如果归档文件夹保存在其他位置，则需要按照以下步骤授予完全控制权限。

a. 查找存档文件夹的位置：打开 ADAudit Plus → 管理 → 存档事件 → 向下滚动查看位置。



b. 使用域管理员权限登录目标计算机→ 找到文件夹 → 右键单击 文件夹 → 属性 → 安全 → 编辑 →添加 ADAudit Plus 用户 → 提供 NTFS 完全控制权限。

c.如果存档文件夹是共享文件夹，请转到“共享”选项卡 → “高级共享…” → “权限” →添加 ADAudit Plus 用户 → 提供完全控制权限。

四、授予用户对所有 ADAudit Plus 计划报告文件夹的完全控制权限：
要将计划报告保存到指定位置，需要对计划报告文件夹拥有完全控制权。

ii. 授予用户对产品安装文件夹的完全控制权限：

ADAudit Plus 需要对产品安装文件夹拥有完全控制权才能写入数据库。

a. 使用域管理员权限登录到安装了 ADAudit Plus 的计算机→ 找到产品安装文件夹 → 右键单击 → 属性 → 安全 → 编辑 →添加“ADAudit Plus”用户并授予完全控制权限。

iii. 授予用户对 ADAudit Plus 归档文件夹的完全控制权限：
要存储和检索数据库中的归档数据，需要对归档文件夹拥有完全控制权。

笔记：默认情况下，“计划报告”文件夹存储在安装文件夹（Installation_folder\ManageEngine\ADAudit Plus）中。如果“计划报告”文件夹保存在其他位置，则需要按照以下步骤授予其 NTFS 完全控制权限。

a. 要查找计划报告文件夹的位置：打开 ADAudit Plus → 管理 → 计划报告 → 修改计划报告 → 向下滚动查看位置。

b. 使用域管理员权限登录目标计算机→ 找到文件夹 → 右键单击 文件夹 → 属性 → 安全 → 编辑 →添加 ADAudit Plus 用户 → 提供 NTFS 完全控制权限。

c. 对所有“计划报告”文件夹重复上述步骤。

五、授予用户对 ADAudit Plus 所有警报脚本文件夹的读取和执行权限： 触发警报后，需要对警报脚本文件夹具有读取和执行权限才能执行脚本文件。

笔记：默认情况下，“警报脚本”文件夹存储在安装文件夹（Installation_folder\ManageEngine\ADAudit Plus）中。如果“警报脚本”文件夹保存在其他位置，则需要按照以下步骤授予其 NTFS 读取和执行权限。

a. 查找文件夹位置：打开 ADAudit Plus → 配置 → 修改警报配置文件 → 向下滚动查看位置。

b. 使用域管理员权限登录目标计算机→ 找到文件夹 → 右键单击 文件夹 → 属性 → 安全 → 编辑 →添加 ADAudit Plus 用户 → 提供 NTFS 读取和执行权限。

c. 对所有 Alert Script 文件夹重复上述步骤。

六、授予用户 DCOM 和 WMI 权限：
对于域控制器、Windows 成员服务器和工作站，需要 DCOM 和 WMI 权限才能以 WMI 模式收集事件并显示 RSoP 数据。

一个。授予用户 DCOM 和 WMI 权限，请按照以下步骤操作 。

ManageEngine
ADAudit Plus

我们的产品

AD360 |Log360 | ADManager Plus | ADSelfService Plus

DataSecurity Plus | M365 Manager Plus

关于 ADAudit Plus

ADAudit Plus 是一款统一的审计解决方案，只需点击几下即可全面了解 Active Directory (AD)、Entra ID、文件服务器（Windows、NetApp、EMC 等）、Windows 服务器和工作站上的活动。ADAudit Plus 可帮助企业简化审计流程、证明合规性并增强身份威胁检测和响应能力，其功能包括实时变更审计、用户登录跟踪、帐户锁定分析、特权用户监控、文件审计、合规性报告、攻击面分析（适用于 AD、Azure、AWS 和 GCP）、用户行为分析 (UBA)、响应自动化以及 AD 备份和恢复。

有关 ADAudit Plus 的更多信息，请访问
www.manageengine.cn/products/active-directory-audit/。

$ 获取报价　下载