ManageEngine
ADManager Plus

ADManager Plus 操作权限设置指南

www.admanagerplus.cn

目录

执行所需的 Active Directory (AD) 和 Microsoft 365 管理
以及报告操作，

必须为 ADManager Plus 授予必要的权限。这可以是……
通过输入已被授予权限的用户帐户凭据来完成
在 ADManager Plus 的“域设置”部分中需要授予必要的权限。
管理员选项卡。

要修改特权组，您需要使用具有以下身份的用户帐户登录：
管理员组成员。如果您不想使用域管理员。
账户，您可以使用已获得足够权限的用户账户登录。
执行必要操作的权限。

以下各节包含必须具备的最小权限。
分配给用户帐户以执行所需操作。

用户管理

本节详细说明了创建、修改和使用所需的权限。
删除用户帐户。

操作：创建用户

所需权限：
- 必须是账户运营组的成员，或者

- 必须对所需 OU 的所有用户对象拥有读取和写入权限。

授予创建用户帐户权限的步骤。

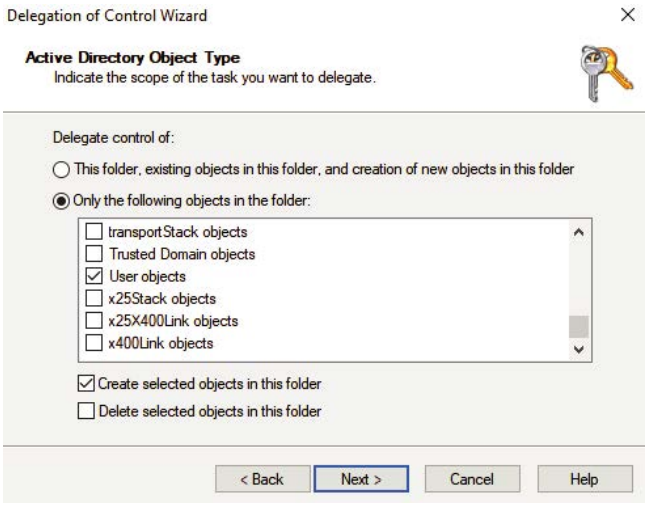
1. 登录到您的域控制器并启动**活动目录用户和计算机**。

2. 找到并右键单击要授予所需权限的域/组织单元，
   选择**委托控制**“委派控制权”向导将弹出。

3. 点击**下一个**添加所需的用户帐户并单击**下一个**。

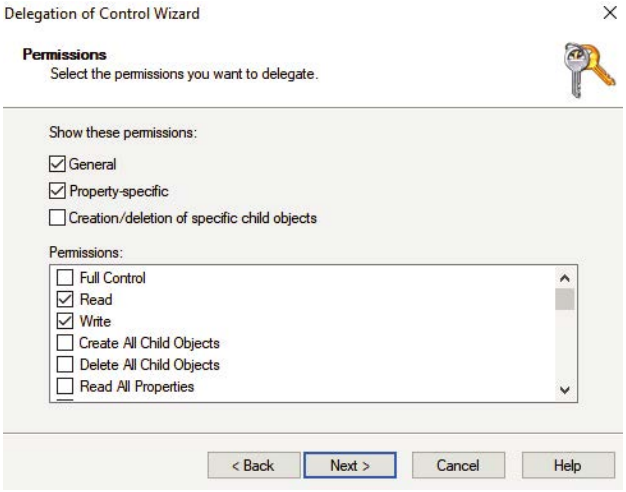
4. 选择**创建自定义任务**委托选项

5. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选中复选框。同时选中
   创建选定对象此文件夹选项如图所示。



6. 点击**下一个**在……之下**显示这些权限**部分，选择**一般的**和
   特定属性选项。

7. 在权限部分，选择**读**和**写**权限和点击
   下一个如下图所示。



8. 点击**结束**。

操作：修改用户

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需 OU 中的所有用户对象拥有读取、写入、读取所有属性和重置密码权限。

授予修改用户帐户权限的步骤。

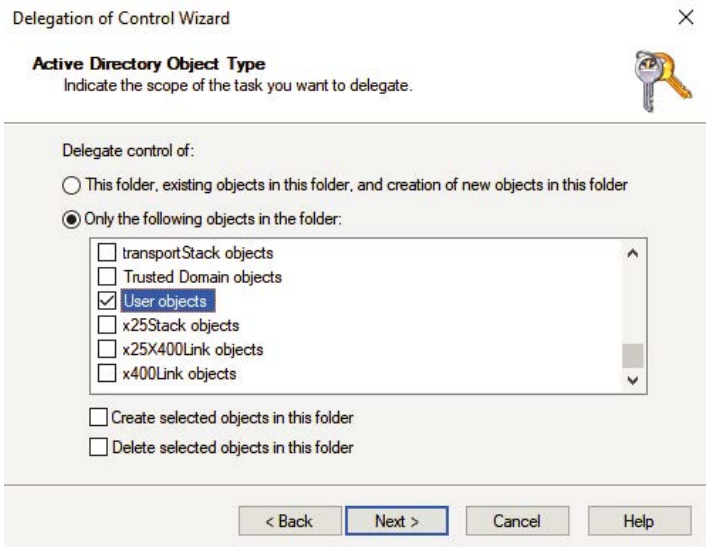
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个**添加所需的用户帐户并单击**下一个。**

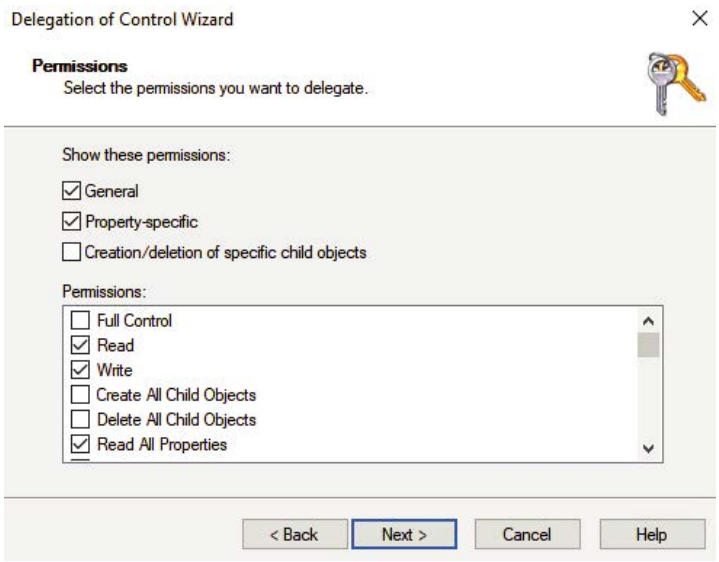
4. 选择**创建自定义任务以进行委派**选项

5. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项
   如图所示。



6. 点击**下一个。**在**显示这些权限**部分，选择**一般的**和
   特定属性选项。

7. 在权限部分，选择**阅读、写作、**和**阅读所有属性**权限
   点击**下一个**如下图所示。



8. 点击**结束**。

操作：删除用户

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需 OU 的所有用户对象拥有“删除所有子对象”权限。

授予删除用户帐户权限的步骤。

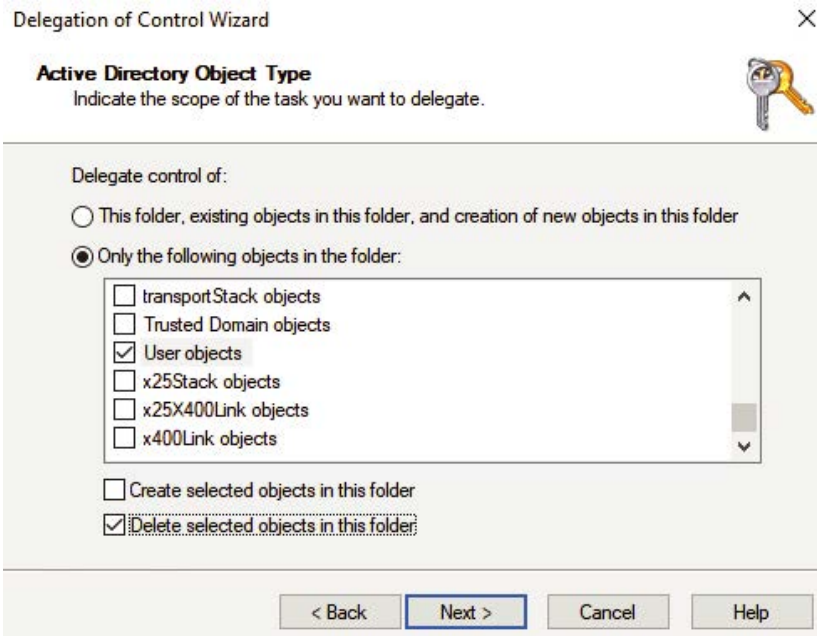
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个**添加所需的用户帐户并单击**下一个。**

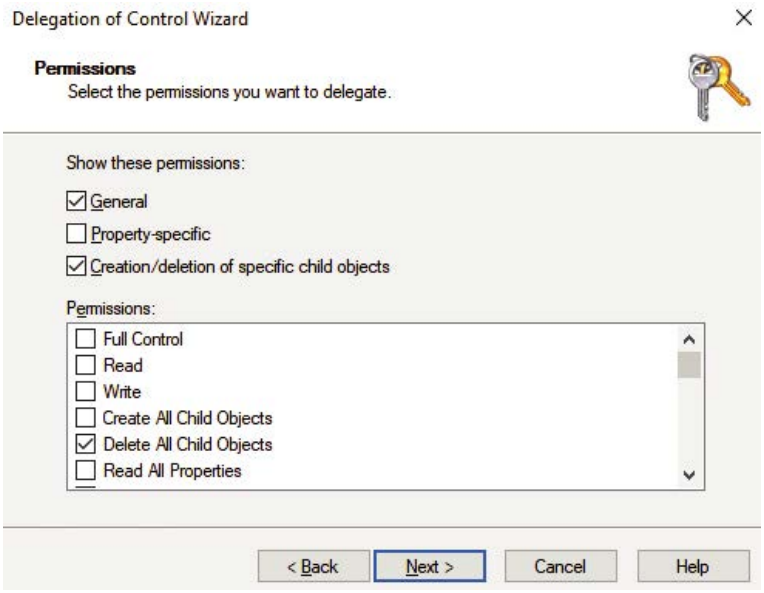
4. 选择**创建自定义任务以进行委派**选项

5. 选择**仅此文件夹中的对象选项**并选中“用户对象”复选框。
   同时选择**删除此文件夹中的选定对象**选项如下图所示。



6. 点击**下一个**在……之下**显示这些权限**部分，选择**一般的**和**创建/删除特定子对象**选项。

7. 在权限部分，选择**删除所有子对象**权限和点击**下一个，**如下图所示。



8. 点击**结束。**

操作：恢复用户

所需权限：

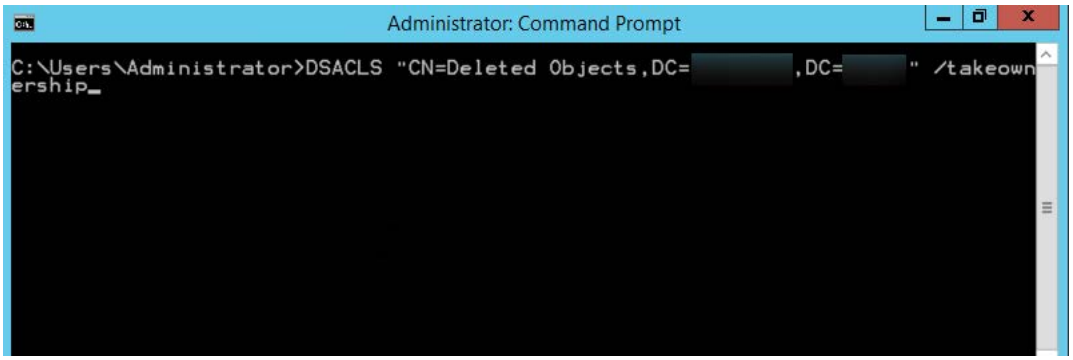
- 修改已删除对象容器权限的用户必须是成员
域管理员组，或
- 必须手动向所需的安全主体授予恢复 AD 用户的权限。
如下步骤所示。

授予恢复已删除 AD 用户所需权限的步骤

从 AD 中删除的任何对象都会存储在已删除对象容器中，并且可以恢复。
在其墓碑生命周期结束之前。要恢复已删除的 AD 对象，
非管理员用户必须拥有足够的权限才能访问此容器。
授予所需权限：

1. 登录到您的域控制器并以管理员身份启动命令提示符。

2. 指定以下格式的命令：dsacls "CN=已删除对象,DC=**admanagerplus**，
DC=**com**“使用 /takeownership 并以管理员身份运行该命令。

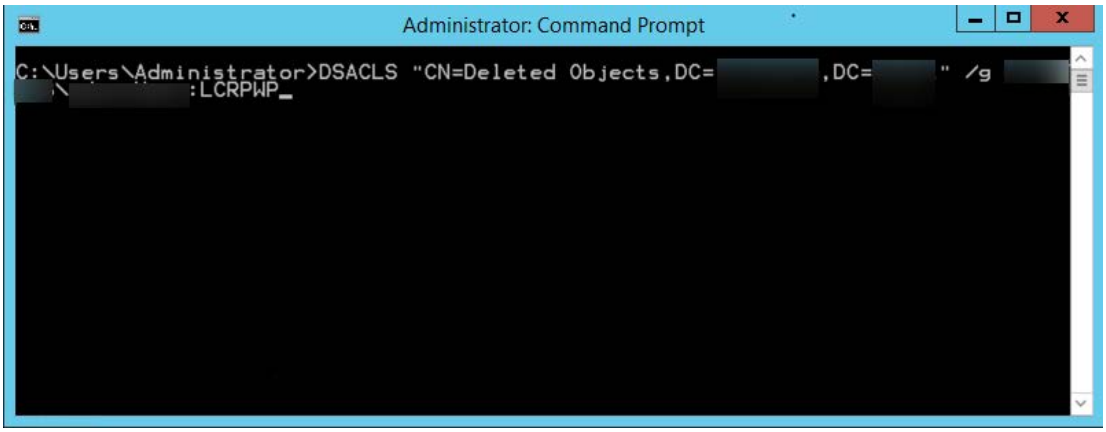


笔记：

- 林中的每个域都有自己的已删除对象容器，因此指定该容器至关重要。
您要修改权限的已删除对象容器的域名。

- 代替**admanagerplus**和**com**包含您的领域组件。

3. 要授予安全主体访问已删除对象OU的权限，请指定一个
命令格式如下：dsacls "CN=已删除对象,DC=admanagerplus,DC=com"
/g ADMANAGERPLUS\LukeJohnson:LCRPWP



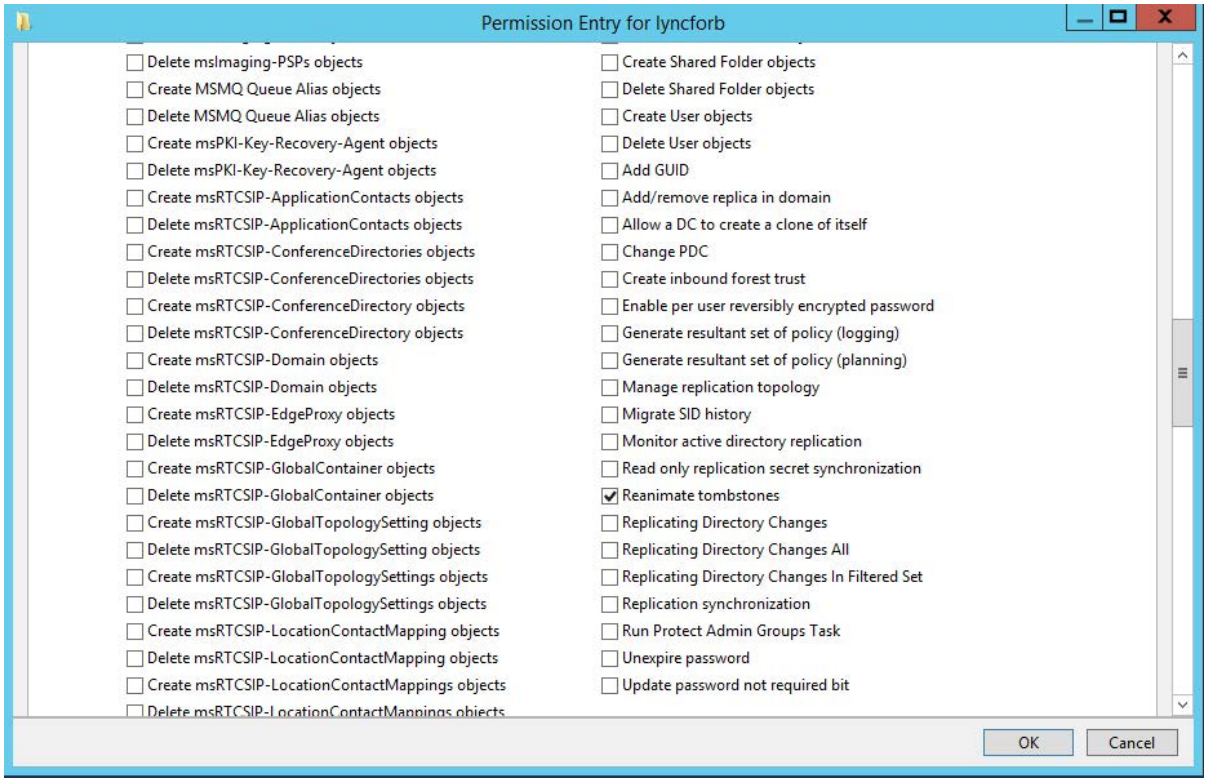
笔记：将“LukeJohnson”替换为您选择的安全负责人。

4. 接下来，连接到默认命名上下文，右键单击域根，然后选择**特性。**

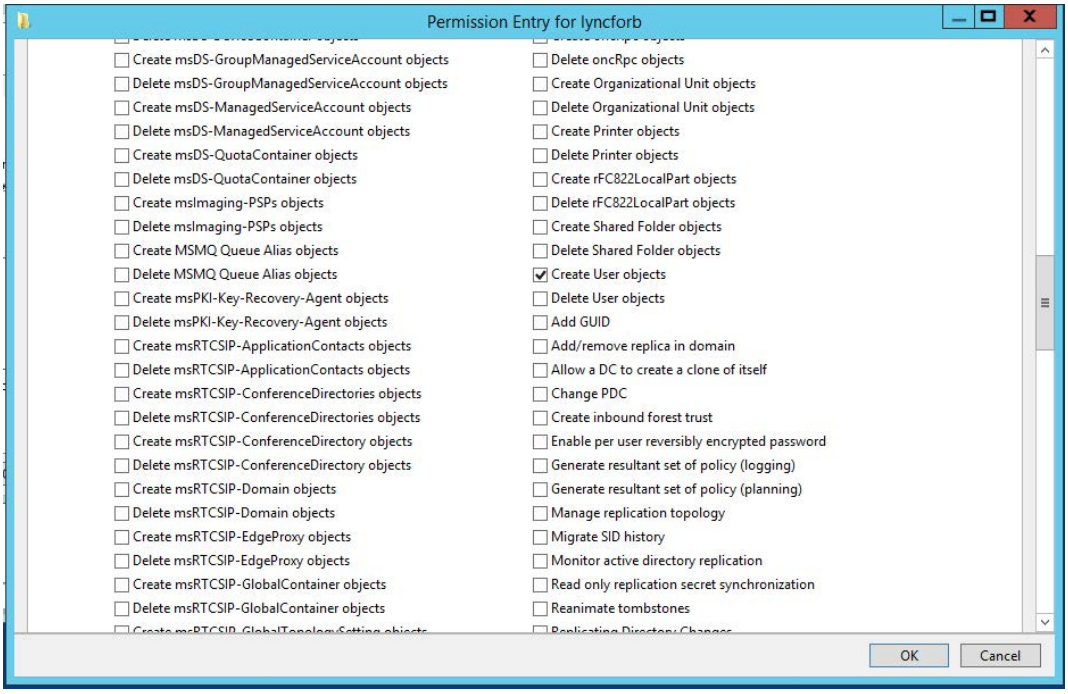
5. 在**安全选项卡中**点击 Tab 键**高级。**

6. 添加用户或组，并选择以下权限：

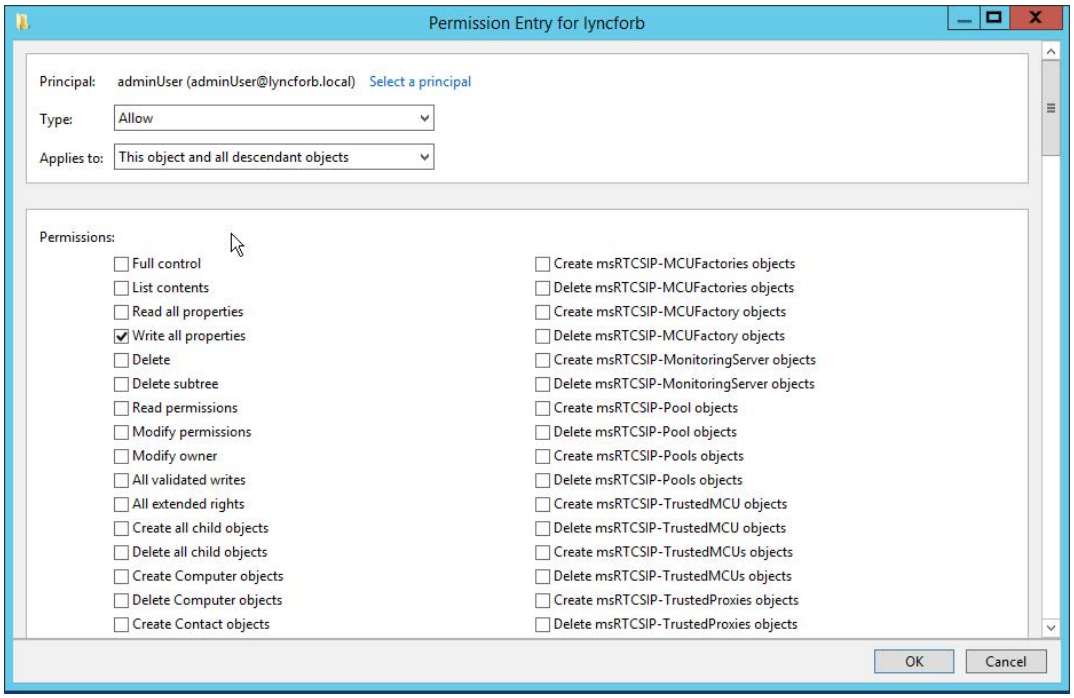
   a. 让墓碑复活



b. 创建用户对象



c. 写出所有属性



笔记：应用**恢复墓碑权利**对被保护的对象及其子对象。

7. 点击**好的**。

笔记：只有在委派上述权限之后删除的对象才能恢复。

操作：在 Active Directory 中重置用户密码

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 重置密码（右侧扩展）
  - 写入 nTSecurityDescriptor（以阻止用户更改密码）
  - 写入用户帐户控制（密码永不过期）
  - 写入 pwdLastSet（用户下次登录时必须更改密码）

授予重置用户密码权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加用于配置和验证域的用户帐户
   ADManager Plus，然后点击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*， 选择**一般的**和**特定于物业。**
8. 在*权限*请选择以下权限并单击**下一个：**
   - 重置密码
   - 写入 nTSecurityDescriptor
   - 写入用户帐户控制
   - 写入 pwdLastSet
9. 点击**结束。**

笔记：

- 这**重置密码（右侧扩展）**批量密码重置操作需要此功能，并且在创建用户时设置密码。

操作：修改 Active Directory 中用户帐户的组属性

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 读取主组 ID
  - 写入主组 ID

授予用户帐户修改组属性权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加所需的用户帐户并单击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*选择**特定于物业。**
8. 在*权限*，选择以下权限并单击**下一个：**
   - 读取主组 ID
   - 写入主组 ID
9. 点击**结束。**

笔记：

- 场景*初级组*操作需要**写入主组 ID**允许。

操作：在 Active Directory 中解锁用户帐户

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 写入锁定时间

授予解锁用户帐户权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加所需的用户帐户并单击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*选择**特定属性。**
8. 在*权限*，选择以下权限并单击**下一个：**
   - 写入锁定时间
9. 点击**结束。**

笔记：

- 解锁用户帐户会重置**锁定时间**属性值为零。

操作：在 Active Directory 中将用户帐户在组织单元 (OU) 之间移动

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 删除源 OU 上的用户对象
  - 删除源 OU 上的子对象
  - 在目标组织单元 (OU) 上创建用户对象
  - 在目标组织单元 (OU) 上创建子对象

授予用户帐户移动权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击要从中移动用户的源组织单元 (OU)，
   选择**委托控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加所需的用户帐户并单击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*选择**一般的。**
8. 在*权限*，选择以下权限并单击**下一个：**
   - 删除
9. 点击**结束。**
10. 在目标组织单元 (OU) 上重复上述步骤，并授予以下权限：
    - 创建用户对象

笔记：

- 在组织单元 (OU) 之间移动用户，在源 OU 中视为删除操作，在目标 OU 中视为创建操作。
  在目标组织单元中执行操作。

操作：在 Active Directory 中删除用户帐户

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 删除

授予删除用户帐户权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加所需的用户帐户并单击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*选择**常规。**
8. 在*权限*，选择以下权限并单击**下一个：**
   - 删除
9. 点击**结束。**

笔记：

- 委派**删除**OU 级别的权限仅允许帐户删除以下内容：
  该组织单元中的用户对象。
- 账户操作员组的成员可以删除域内的所有用户账户。
  受保护的系统帐户除外。

操作：恢复 Active Directory 中已删除的用户帐户

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 读/写 msDS-ExternalStdId
  - 读/写 isDeleted
  - 还原已删除对象

先决条件：

- 必须在域中启用 Active Directory 回收站。

授予恢复已删除用户帐户权限的步骤

1. 登录到您的域控制器并启动**Active Directory 管理中心。**
2. 点击域名并导航至**已删除对象**容器。
3. 右键单击 域名并选择**委托控制。**
4. 在*委派控制向导*点击弹出窗口**下一个。**
5. 添加所需的用户帐户并单击**下一个。**
6. 选择**创建自定义任务以进行委派**选项。
7. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
8. 点击**下一个**。 在下面*显示这些权限*选择**一般的**和**特定属性。**
9. 在*权限*，选择以下权限并单击**下一个：**
   - 读/写 msDS-ExternalStdId
   - 读/写 isDeleted
   - 还原已删除对象
10. 点击**结束。**

笔记：

- 恢复已删除的用户涉及重新激活已删除的对象，并将其属性写回 Active Directory。
- 如果未启用 Active Directory 回收站，则无法使用此操作恢复已删除的用户对象。
- 域管理员或企业管理员组的成员无需额外委派即可恢复已删除的用户。

操作：修改 Active Directory 中用户帐户的主文件夹和配置文件路径

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：

- 活动目录
  - 写入主目录
  - 写回 homeDrive
  - 写入配置文件路径

文件服务器

- 读
- 写
- 调整
- 删除

授予用户帐户修改主文件夹和配置文件路径权限的步骤

Active Directory 权限

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加所需的用户帐户并单击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*选择**特定属性。**
8. 在*权限*，选择以下权限并单击**下一个：**
   - 写入主目录
   - 写回 homeDrive
   - 写入配置文件路径
9. 点击**结束。**

文件服务器权限（必填）

除了 Active Directory 权限之外，委派帐户还必须拥有对 NTFS 文件系统的权限。
存储用户主文件夹和配置文件的文件服务器。

授予源文件夹和目标文件夹以下权限：

- 读
- 写
- 调整
- 删除

笔记：

- 移动主文件夹和移动配置文件路径操作需要对两者都具有写入权限。Active Directory 属性及其对应的文件系统路径。
- 删除主文件夹和删除配置文件操作需要文件服务器上的删除权限。
- 如果未授予所需的 NTFS 权限，Active Directory 属性可能会更新操作成功，但文件夹操作会失败。

操作：修改 Active Directory 中用户帐户的可继承权限

所需权限：
- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 读取权限
  - 修改权限
  - 写入 nTSecurityDescriptor

授予修改用户帐户可继承权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 来自**看法**菜单，启用**高级功能。**
3. 找到并右键单击要授予所需权限的域或组织单元 (OU)，然后选择**特性。**
4. 导航至**安全**Tab 键并单击**先进的。**
5. 确保**包含来自此对象父对象的可继承权限**已启用。
6. 添加所需的用户帐户，并授予用户对象以下权限：读取权限
   -
   - 修改权限
   - 写入 nTSecurityDescriptor
7. 点击**申请**进而**好的**保存更改。

笔记：

- 修改可继承权限需要访问以下权限：**安全**和**高级安全设置配置界面。**
- 对可继承权限的更改会影响组织单元 (OU) 内的所有子用户对象。
- 请在应用更改前仔细检查继承的权限，以避免意外访问。

操作：修改 Active Directory 中用户帐户的登录时间

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 阅读登录时间
  - 填写登录时间

授予修改用户帐户登录时间权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加所需的用户帐户并单击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*选择**特定属性。**
8. 在*权限*，选择以下权限并单击**下一个：**
   - 阅读登录时间
   - 填写登录时间
9. 点击**结束。**

笔记：

- 登录时间限制由域控制器在用户身份验证期间强制执行。
- 修改登录时间需要**写入登录时间**对用户对象的权限
  已委派的组织单元。

操作：修改 Active Directory 中用户帐户的用户工作站设置

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 读取用户工作站
  - 写入用户工作站

授予用户帐户修改用户工作站设置权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击**领域**或者**俄亥俄大学**您希望授予所需的权限
   并选择**委托控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加所需的用户帐户并单击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*选择**特定属性。**
8. 在*权限*，选择以下权限并单击**下一个：**
   - 读取用户工作站
   - 写入用户工作站
9. 点击**结束。**

笔记：

- 用户工作站设置限制用户可以登录的计算机。
- 修改此设置需要**写入用户工作站**用户对象的权限
  在已委派的组织单元内。

操作：管理 Active Directory 中用户帐户的照片

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 阅读缩略图照片
  - 写缩略图照片

授予用户帐户管理用户照片权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击**领域**或者**俄亥俄大学**您希望授予所需的权限并选择**委托控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加所需的用户帐户并单击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*选择**特定属性。**
8. 在*权限*，选择以下权限并单击**下一个：**
   - 阅读缩略图照片
   - 写缩略图照片
9. 点击**结束。**

操作：保护 Active Directory 中的用户对象免遭意外删除

所需权限：

- 必须是账户操作员组的成员，或者
- 必须对所需组织单元 (OU) 的所有用户对象拥有以下权限：
  - 修改权限
  - 删除
  - 删除子树

授予权限以防止用户对象被意外删除的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 来自**看法**菜单，启用**高级功能。**
3. 找到并右键单击要修改保护的用户对象，然后选择**特性。**
4. 导航至**安全选项卡**并单击**高级。**
5. 添加所需的用户帐户并授予必要的权限。
6. 点击**申请**进而**好的**保存更改。

笔记：

- 防止对象被意外删除的方法是修改对象的属性。
  安全权限。
- 被委派的帐户必须具有修改用户安全设置的权限。
  用于启用或禁用此选项的对象。
- 移除保护需要相同的权限。

操作：在 Active Directory 中修改用户属性

所需权限：

- 必须是账户操作员组的成员，或者

必须对所有用户对象的特定必需属性拥有写入权限。

必需的组织单元 (OU)，例如：

- 标题
- 部门
- 公司
- 经理
- 其他明确要求的属性

描述：

允许委派帐户修改 Active Directory 中的各种用户属性，包括：

- **账户属性：**启用/禁用、帐户过期、委托和安全选项
- **地址/组织属性：**职称、部门、公司、经理、地址信息
- **命名属性：**显示名称、名字、姓氏、登录名、员工标识符
- **个人资料属性：**配置文件路径、登录脚本、主文件夹
- **联系属性：**电话号码、电子邮件地址、办公详情
- **自定义属性：**已配置的自定义属性、附加属性和属性
  通过自定义脚本修改

授予修改用户属性权限的步骤

1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击需授予权限的域或组织单元
   并选择委派**控制。**
3. 在*委派控制向导*点击弹出窗口**下一个。**
4. 添加所需的用户帐户并单击**下一个。**
5. 选择**创建自定义任务以进行委派**选项。
6. 选择**此文件夹中仅包含对象**选项并选择**用户对象**选项。
7. 点击**下一个**。 在下面*显示这些权限*选择**一般的**和**特定属性。**
8. 在*权限*，选择**写**所有用户对象的特定必需属性的权限
   在所需的组织单元 (OU) 内（例如，职称、部门、公司和经理），然后单击**下一个。**
9. 点击**结束。**

笔记：

- 授予**写入所有属性**权限过高，除非必要，否则应避免授予过多权限。
  明确要求。
- 属性级委派可在确保运行成功的同时，提供最小权限访问。
- 应审查自定义脚本，以确定确切的属性依赖关系。
- 与配置文件相关的更改可能会引用外部资源（例如，主文件夹、配置文件路径）
  并且可能需要额外的文件系统权限（如适用）。

联系人管理

本节详细说明了创建、修改和创建所需的权限。

删除 AD 中的联系人。

操作：创建联系人

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需组织单元 (OU) 的所有联系人对象拥有读取和写入权限。

授予创建联系人帐户权限的步骤。

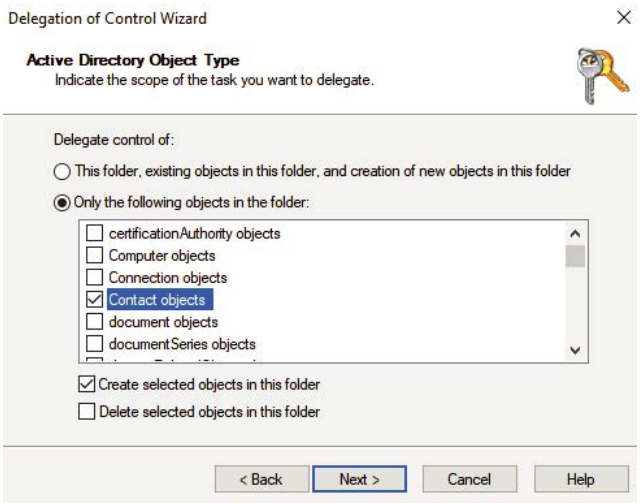
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域/组织单元，
   选择**委托控制**“委派控制权”向导将弹出。

3. 点击**下一个，**添加所需的用户帐户并单击**下一个。**

4. 选择**创建自定义任务以进行委派**选项

5. 选择**此文件夹中仅包含对象**然后选择“联系人对象”复选框。
   同时选择**在此文件夹中创建选定对象**如下图所示：



6. 点击**下一个**在……之下**显示这些权限**部分，选择**一般的**和
   特定属性选项。

7. 在权限部分，选择**读**和**写**权限并点击**下一个。**

8. 点击**结束。**

操作：修改联系人

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需 OU 的所有联系人对象拥有读取、写入和读取所有属性的权限。

授予修改联系人帐户权限的步骤。

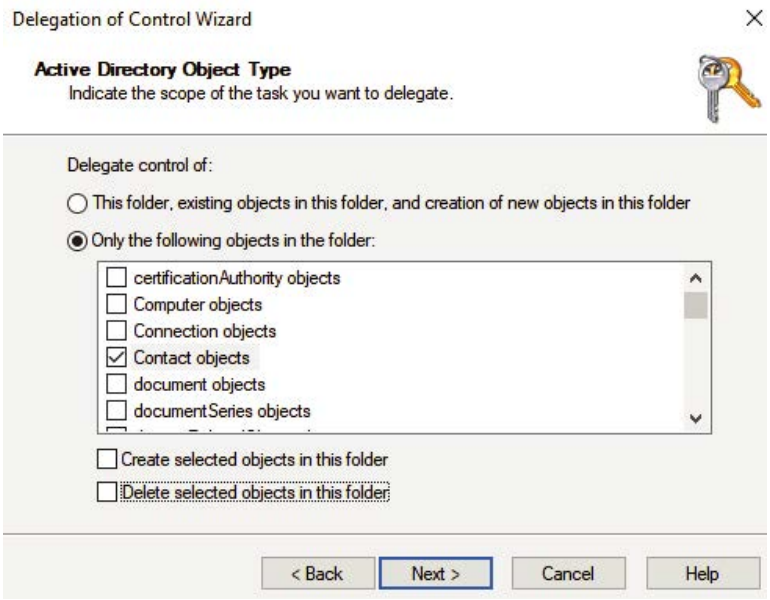
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个，**添加所需的用户帐户并单击**下一个。**

4. 选择**创建自定义任务以进行委派**选项

5. 选择**此文件夹中仅包含对象**选择“联系人对象”选项，然后选择“联系人对象”选项。
   如图所示。



6. 点击**下一个。**在**显示这些权限**部分，选择**一般的**和
   特定属性选项。

7. 在权限部分，选择**阅读，写作**和**阅读所有属性**
   权限和点击**下一个。**

8. 点击**结束。**

操作：删除联系人

所需权限：

- 必须是账户运营组的成员，或者

- 必须拥有对所需组织单元 (OU) 的所有联系人对象执行“删除所有子对象”的权限。

授予删除联系人帐户权限的步骤。

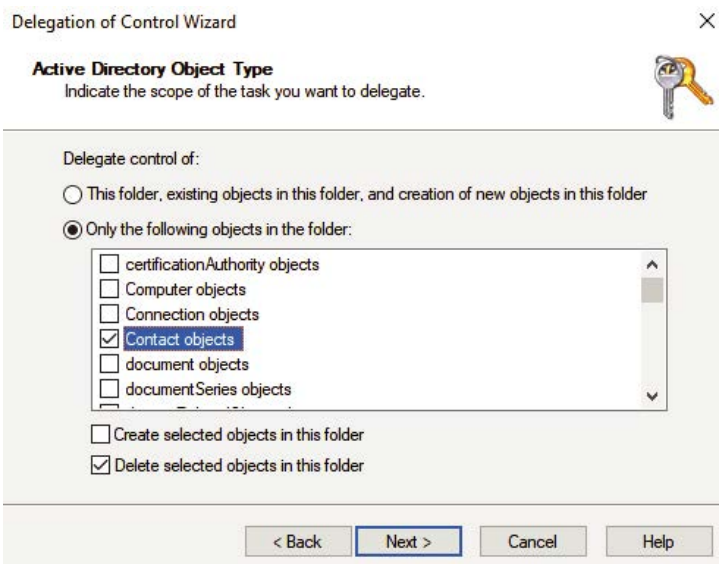
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个，**添加所需的用户帐户并单击**下一个。**

4. 选择**创建自定义任务以进行委派**选项。

5. 选择**此文件夹中仅包含对象**然后选择“联系人对象”复选框。
   同时选择**删除此文件夹中的选定对象**如下图所示：



6. 点击**下一个。**在**显示这些权限**部分，选择**一般的**和
   创建/删除特定子对象选项。

7. 在权限部分，选择**删除所有子对象**权限和点击**下一个。**

8. 点击**结束。**

操作：恢复联系人

所需权限：

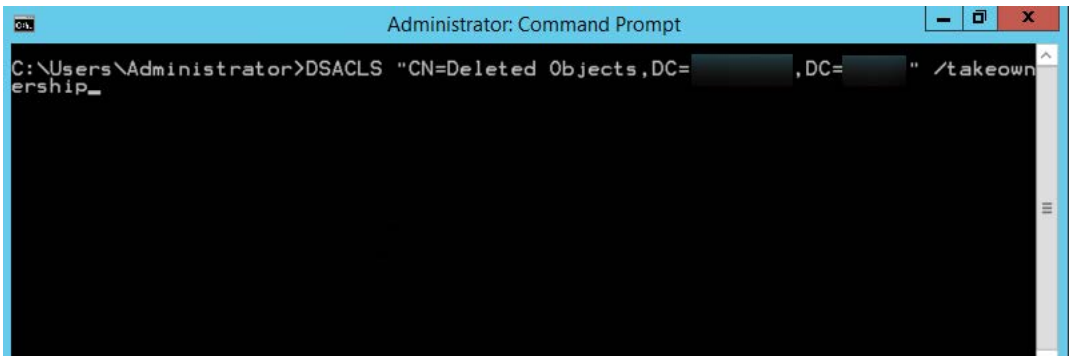
- 修改已删除对象容器权限的用户必须是成员
域管理员组，或
- 必须手动授予所需安全权限才能恢复 AD 联系人。
原理如下步骤所示。

授予恢复已删除 AD 联系人所需权限的步骤

从 AD 中删除的任何对象都会存储在已删除对象容器中，并且可以恢复。
在其生命周期结束之前。要恢复已删除的 AD 对象，
非管理员用户必须拥有足够的权限才能访问此容器。
授予所需权限：

1. 登录到您的域控制器并以管理员身份启动命令提示符。

2. 指定以下格式的命令：dsacls "CN=已删除对象,DC=**admanagerplus**,，
DC=**com**/接管

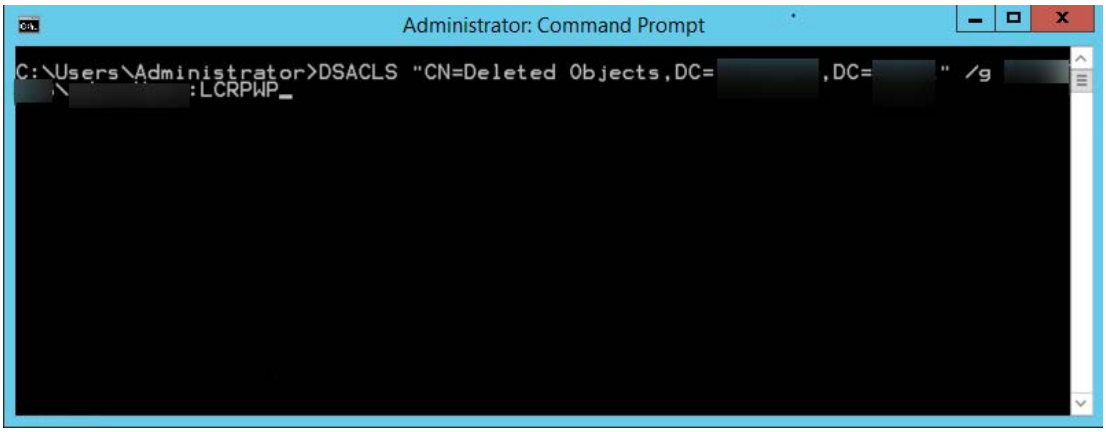


笔记：

- 林中的每个域都有自己的已删除对象容器，因此指定该容器至关重要。
您要修改权限的已删除对象容器的域名。

- 代替**admanagerplus**,和**com**包含您的领域组件。

3. 要授予安全主体访问已删除对象容器的权限，请指定一个
命令格式如下：dsacls "CN=已删除对象,DC=admanagerplus,DC=com"
/g ADMANAGERPLUS\LukeJohnson:LCRPWP



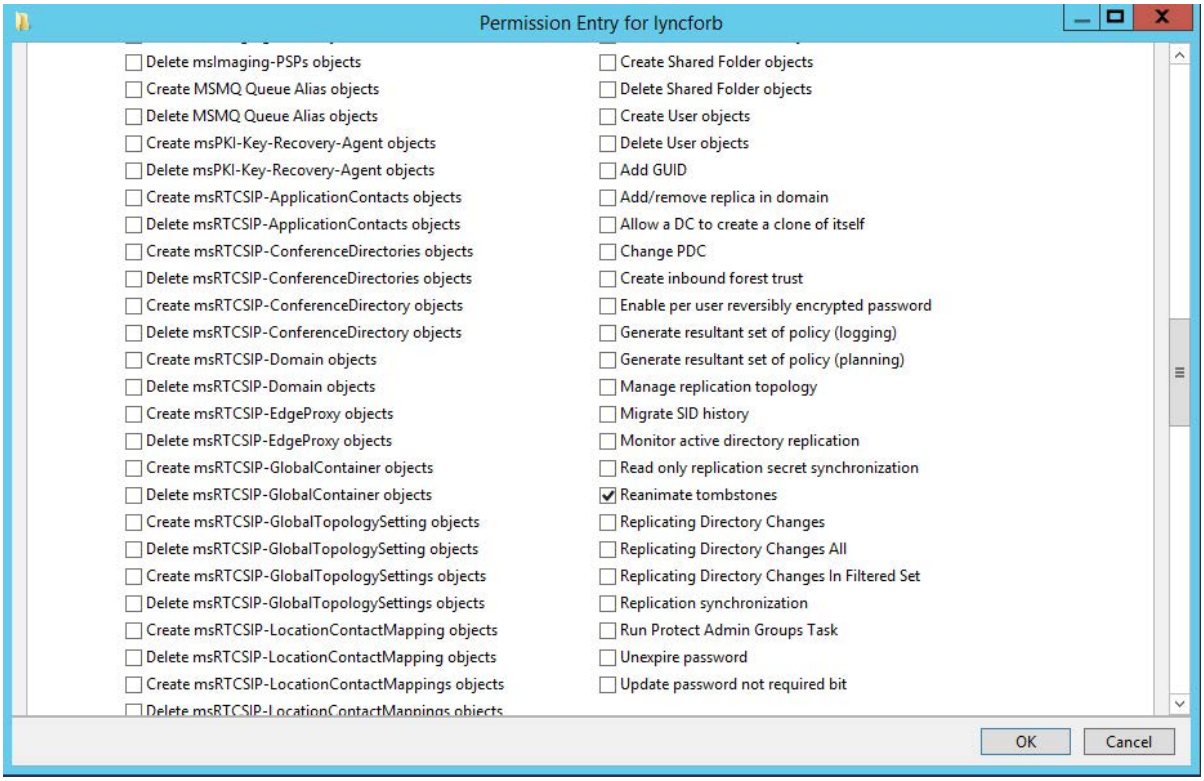
笔记：将“LukeJohnson”替换为您选择的安全负责人。

4. 接下来，连接到默认命名上下文，右键单击域根，然后选择**特性。**

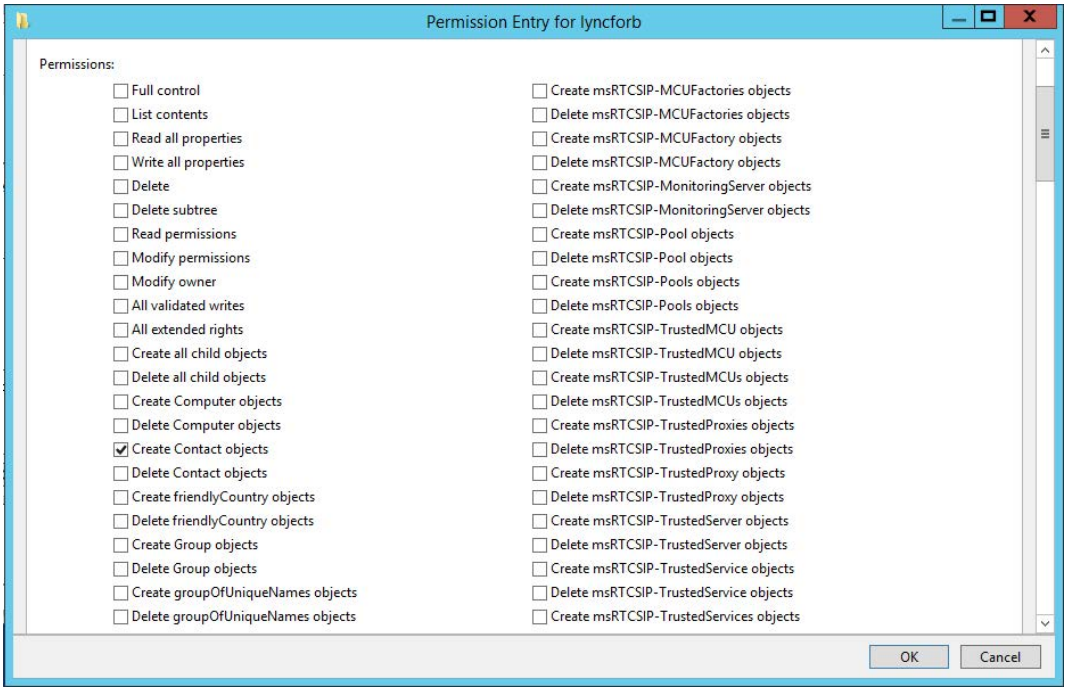
5. 在**安全选项卡**点击 Tab 键**高级。**

6. 添加用户或组，并选择以下权限：

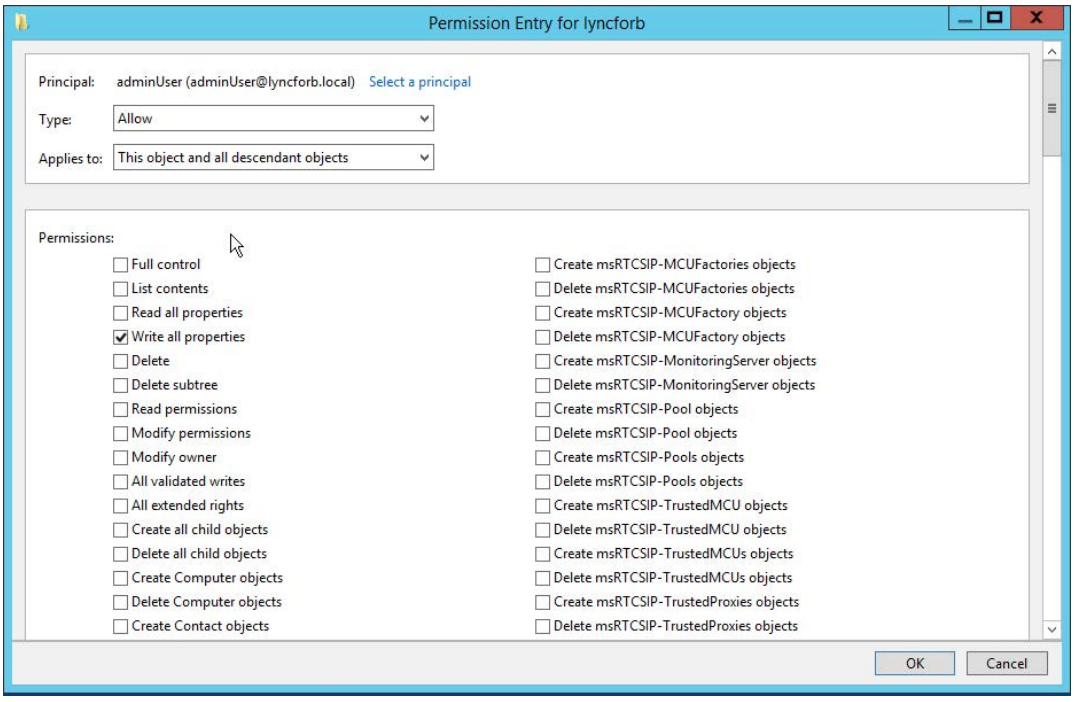
   a. 重新激活已删除对象



b. 创建联系人对象



c. 写出所有属性



笔记：应用**恢复已删除对象权利**对被保护的对象及其子对象。

7. 点击**好的**。

笔记：只有在委派上述权限之后删除的对象才能恢复。

计算机管理

本节详细说明了创建、修改和创建所需的权限。

删除 AD 中的计算机。

操作：创建计算机

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需组织单元 (OU) 的所有计算机对象具有读取和写入权限。

授予创建计算机帐户权限的步骤。

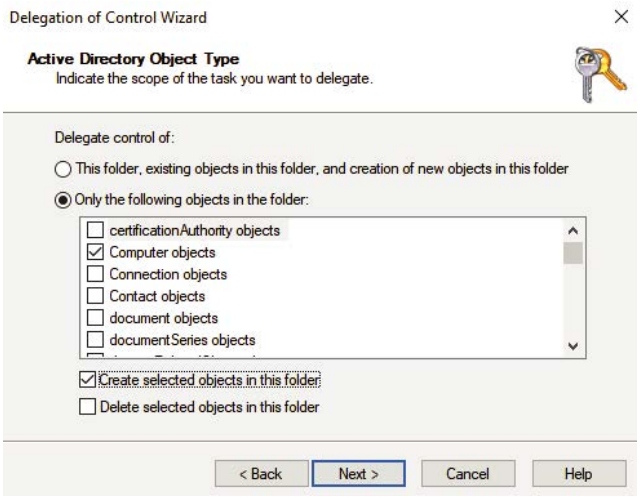
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个，**添加所需的用户帐户并单击**下一个。**

4. 选择**创建自定义任务以进行委派**选项

5. 选择**此文件夹中仅包含对象**然后选择“计算机对象”复选框。
   同时选择**在此文件夹中创建选定对象**选项如下图所示。



6. 点击**下一个。**在**显示这些权限**部分，选择**一般的**和
   特定属性选项。

7. 在权限部分，选择**读**和**写**权限并点击**下一个。**

8. 点击**结束。**

操作：计算机

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需 OU 的所有计算机对象拥有读取、写入和读取所有属性的权限。

授予修改计算机帐户权限的步骤。

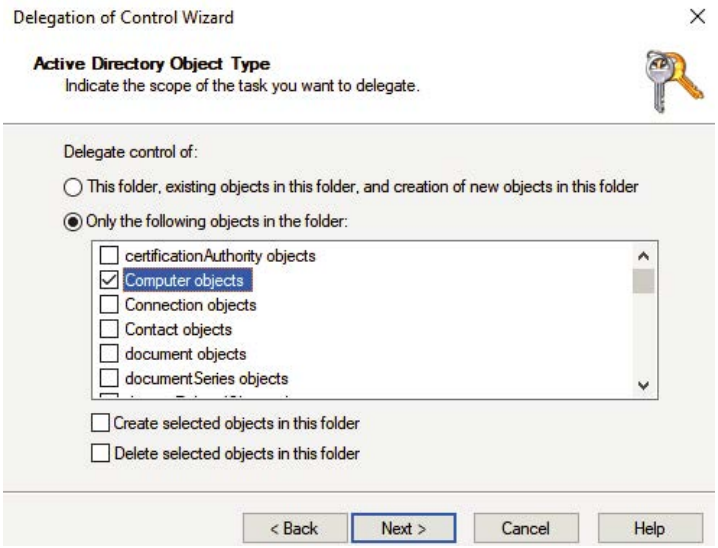
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个，**添加所需的用户帐户并单击**下一个。**

4. 选择**创建自定义任务以进行委派**选项

5. 选择**此文件夹中仅包含对象**选项并选择**计算机对象**复选框
   如下图所示：



6. 点击**下一个**在……之下**显示这些权限**部分，选择**一般的**和
   特定属性选项。

7. 在权限部分，选择**阅读，写作**和**阅读所有属性**
   权限和点击**下一个。**

8. 点击**结束。**

操作：删除计算机

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需组织单元 (OU) 的所有计算机对象拥有“删除所有子对象”权限。

授予删除计算机帐户权限的步骤。

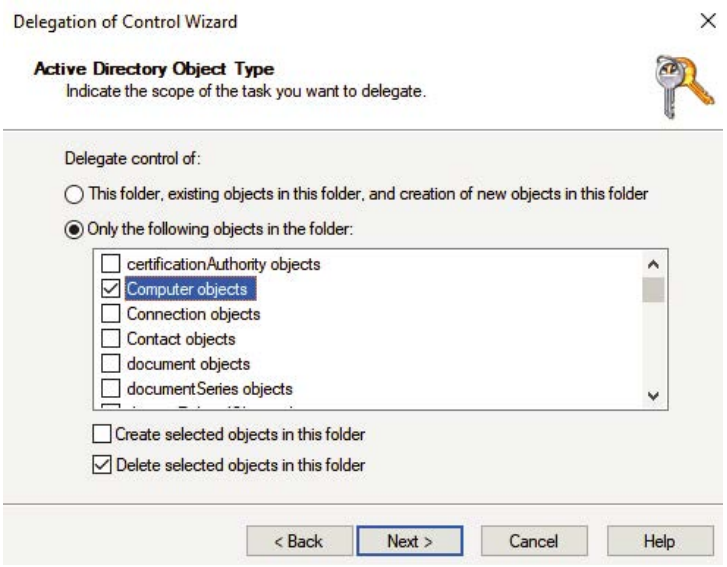
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个，**添加所需的用户帐户并单击**下一个。**

4. 选择**创建自定义任务以进行委派**选项

5. 选择**此文件夹中仅包含对象**选项并选择**计算机对象**复选框
   如下图所示：



6. 点击**下一个。**在“显示这些权限”部分下，选择**一般的**和
   创建/删除特定子对象选项。

7. 在权限部分，选择**删除所有子对象权限**点击**下一个。**

8. 点击**结束。**

操作：恢复计算机

所需权限：

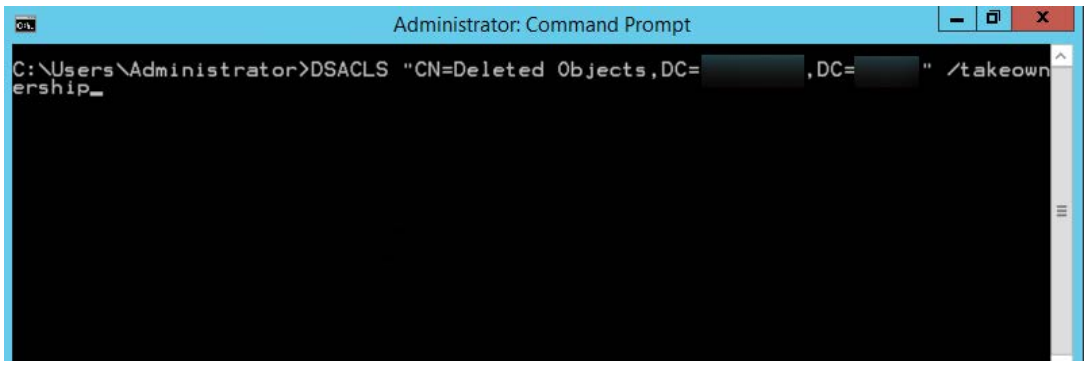
- 修改已删除对象容器权限的用户必须是成员
域管理员组，或
- 必须手动授予所需安全权限才能恢复 AD 计算机。
原理如下步骤所示。

授予恢复已删除 AD 计算机所需权限的步骤

从 AD 中删除的任何对象都会存储在已删除对象容器中，并且可以恢复。
在其墓碑生命周期结束之前。要恢复已删除的 AD 对象，
非管理员用户必须拥有足够的权限才能访问此容器。
授予所需权限：

1. 登录到您的域控制器并以管理员身份启动命令提示符。

2. 指定以下格式的命令：dsacls "CN=已删除对象,DC=**admanagerplus**,
CN=**com**/接管

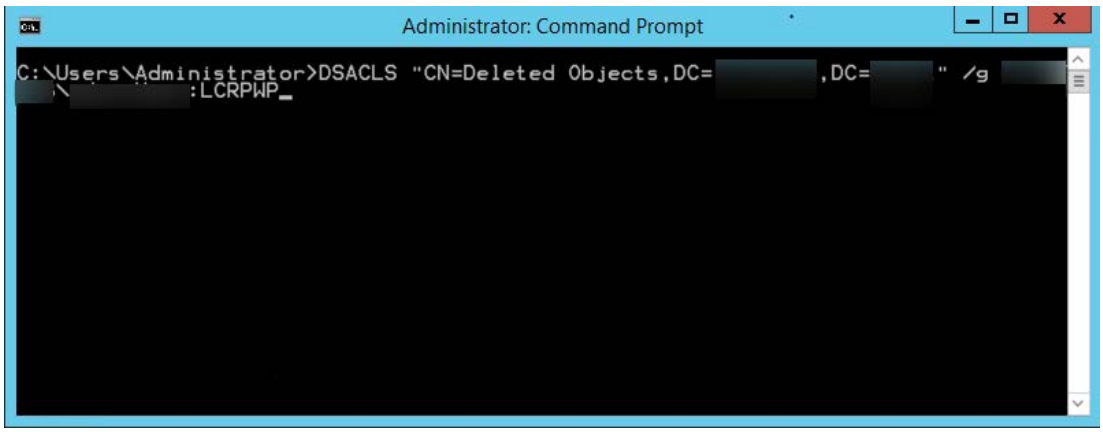


笔记：

- 林中的每个域都有自己的已删除对象容器，因此指定该容器至关重要。
您要修改权限的已删除对象容器的域名。

- 代替**admanagerplus**,和**com**包含您的领域组件。

3. 要授予安全主体访问已删除对象容器的权限，请指定一个
命令格式如下：dsacls "CN=已删除对象,DC=admanagerplus,DC=com"
/g ADMANAGERPLUS\LukeJohnson:LCRPWP



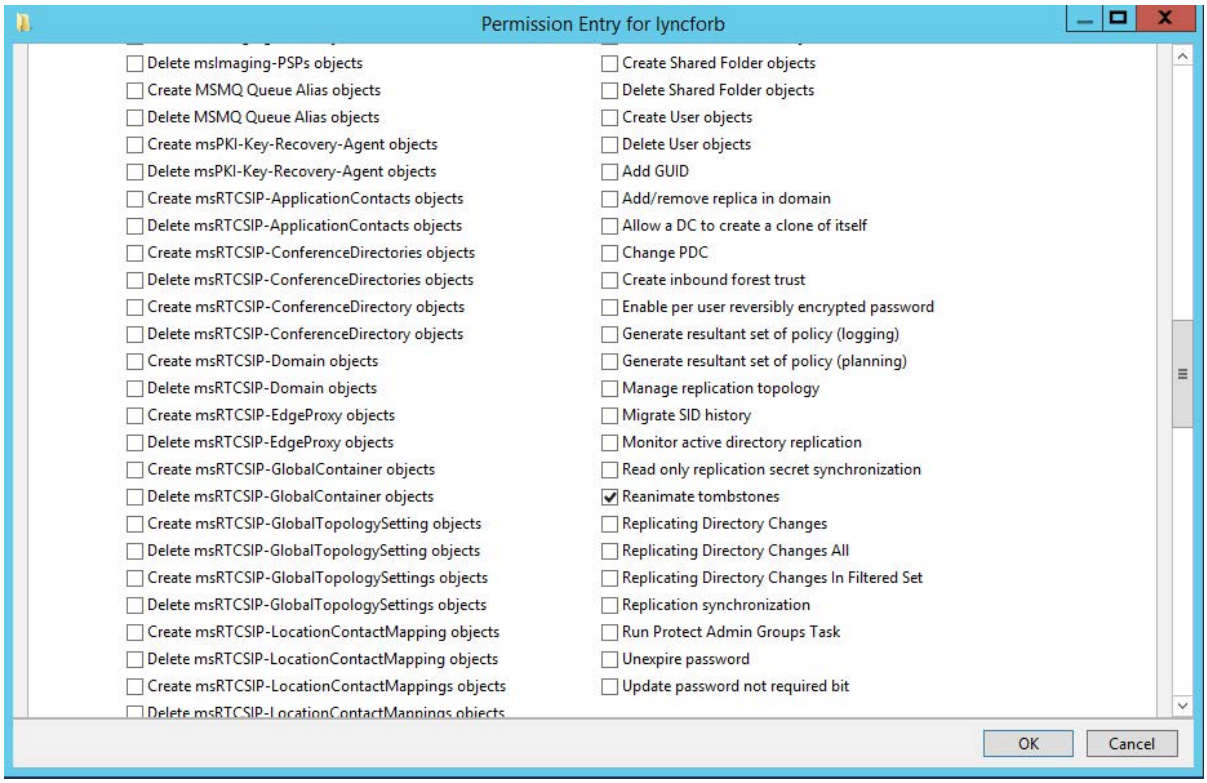
笔记：将“LukeJohnson”替换为您选择的安全负责人。

4. 接下来，连接到默认命名上下文，右键单击域根，然后选择**特性**。

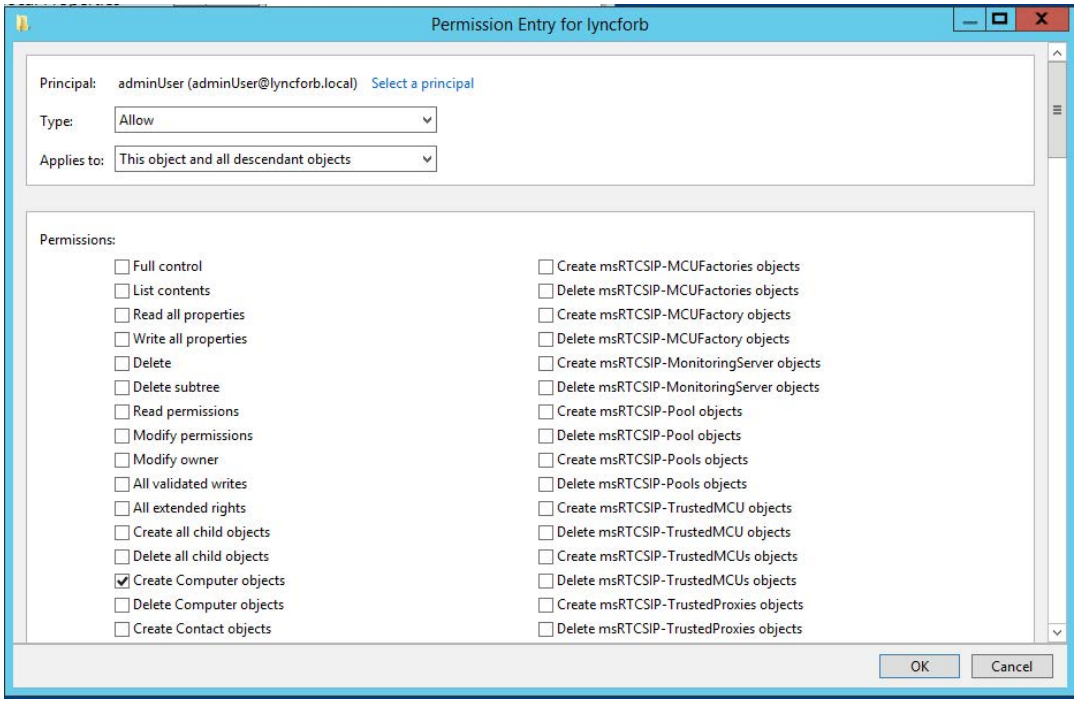
5. 在**安全**点击 Tab 键**高级**。

6. 添加用户或组，并选择以下权限：

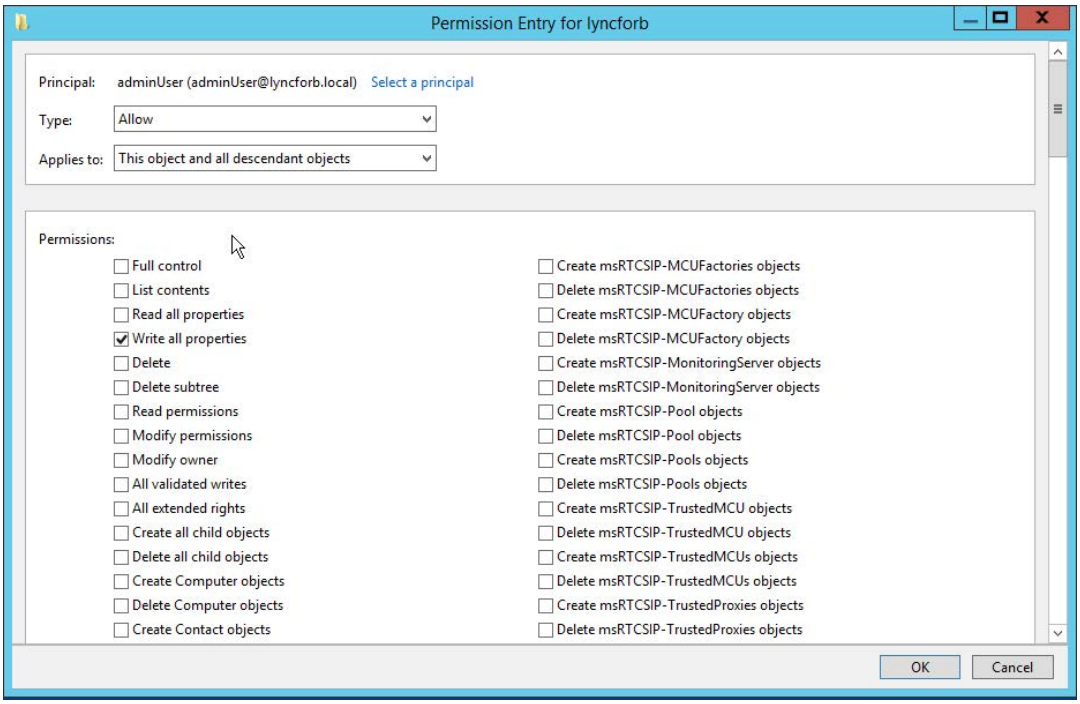
   a. 恢复已删除对象



b. 创建计算机对象



c. 写出所有属性



笔记：应用**恢复已删除对象权利**对被保护的对象及其子对象。

7. 点击**好的**。

笔记：只有在委派上述权限之后删除的对象才能恢复。

组管理

本节详细说明了创建、修改和创建所需的权限。

删除 AD 中的组。

操作：创建群组

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需 OU 的所有组对象拥有读取和写入权限。

授予创建群组权限的步骤。

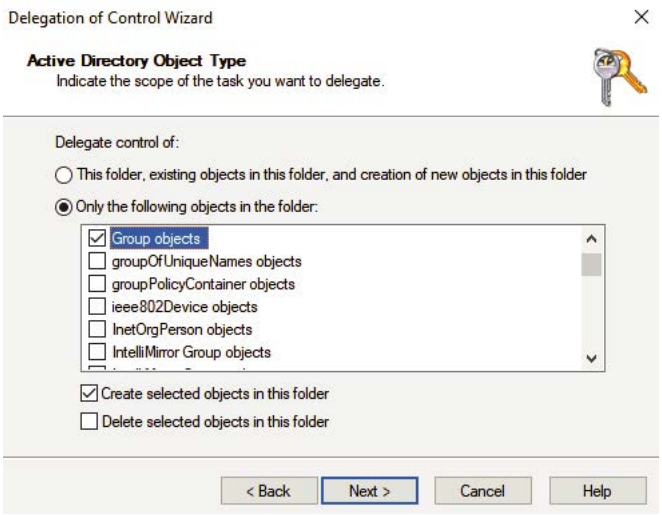
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个，**添加所需的用户帐户并单击**下一个。**

4. 选择**创建自定义任务以进行委派**选项

5. 选择**此文件夹中仅包含对象**然后选择“分组对象”复选框。
   同时选择**在此文件夹中创建选定对象**如下图所示。



6. 点击**下一个。**在**显示这些权限**部分，选择**一般的**和
   特定属性选项。

7. 在权限部分，选择**读**和**写**权限和点击**下一个。**

8. 点击**结束。**

操作：修改组

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需 OU 的所有组对象拥有读取、写入和读取所有属性的权限。

授予修改组权限的步骤。

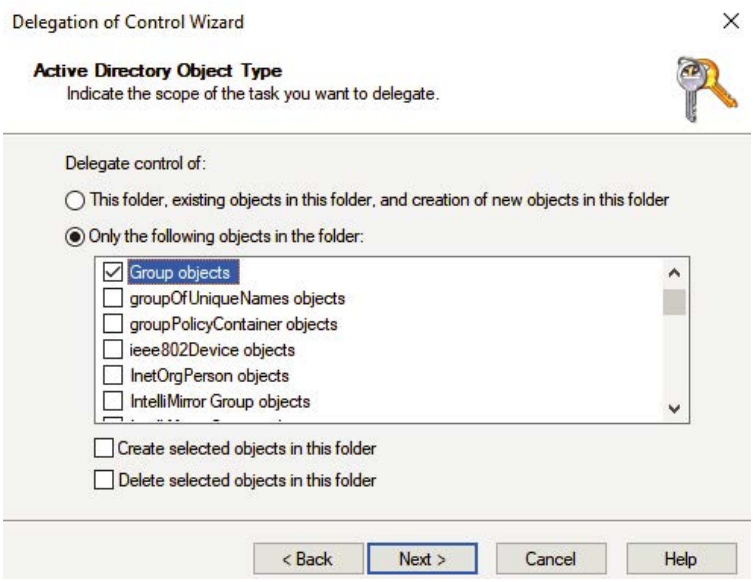
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个，**添加所需的用户帐户并单击**下一个。**

4. 选择**创建自定义任务以进行委派**选项

5. 选择**此文件夹中仅包含对象**选项并选择**组对象**复选框
   如图所示。



6. 点击**下一个。**在**显示这些权限**部分，选择**一般的**和
   特定属性选项。

7. 在权限部分，选择**阅读，写作**和**阅读全部**特性**权限**
   点击**下一个。**

8. 点击**结束。**

操作：删除群组

所需权限：

- 必须是账户运营组的成员，或者

- 必须对所需 OU 的所有组对象拥有“删除所有子对象”权限。

授予删除群组权限的步骤。

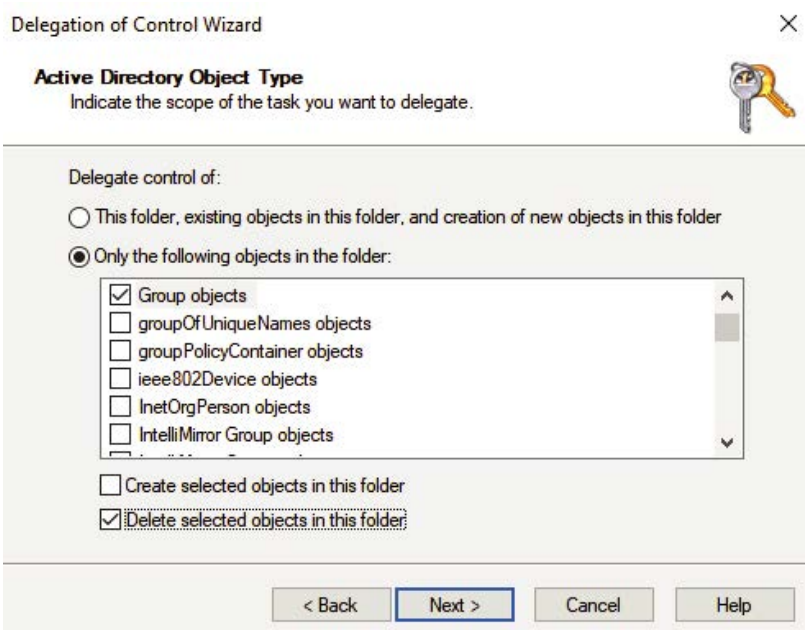
1. 登录到您的域控制器并启动**活动目录用户和计算机。**

2. 找到并右键单击要授予所需权限的域或组织单元 (OU)。
   并选择**委托控制。**“委派控制权”向导将弹出。

3. 点击**下一个，**添加所需的用户帐户并单击**下一个。**

4. 选择**创建自定义任务以进行委派**选项。

5. 选择**此文件夹中仅包含对象**然后选择“分组对象”复选框。
   同时选择**删除此文件夹中的选定对象**如下图所示：



6. 点击**下一个。**在**显示这些权限**部分，选择**一般的**和
   创建/删除特定子对象选项。

7. 在权限部分，选择**删除所有子对象权限**点击**下一个。**

8. 点击**结束。**

操作：恢复组

所需权限：

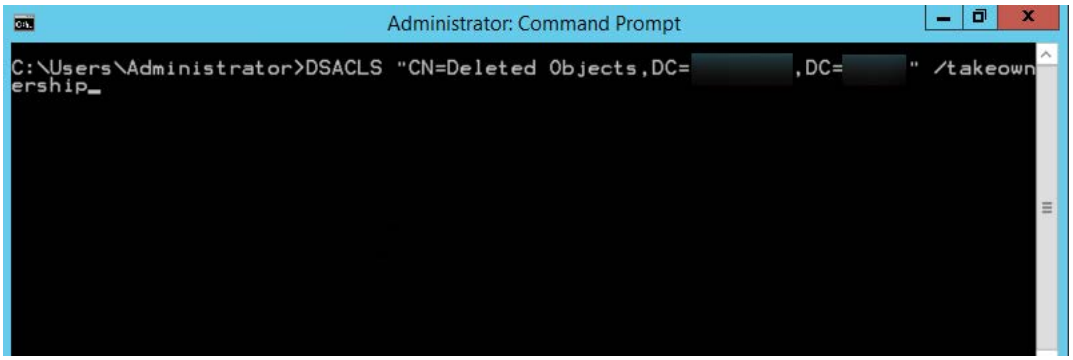
- 修改已删除对象容器权限的用户必须是成员
域管理员组，或
- 必须手动授予所需安全权限才能恢复 AD 组
遵循以下步骤所示的原则。

授予恢复已删除 AD 组所需权限的步骤

从 AD 中删除的任何对象都会存储在已删除对象容器中，并且可以恢复。
在其墓碑生命周期结束之前。要恢复已删除的 AD 对象，
非管理员用户必须拥有足够的权限才能访问此容器。
授予所需权限：

1. 登录到您的域控制器并以管理员身份启动命令提示符。

2. 指定以下格式的命令：dsacls "CN=已删除对象,DC=**admanagerplus**,
CN=**com**/接管

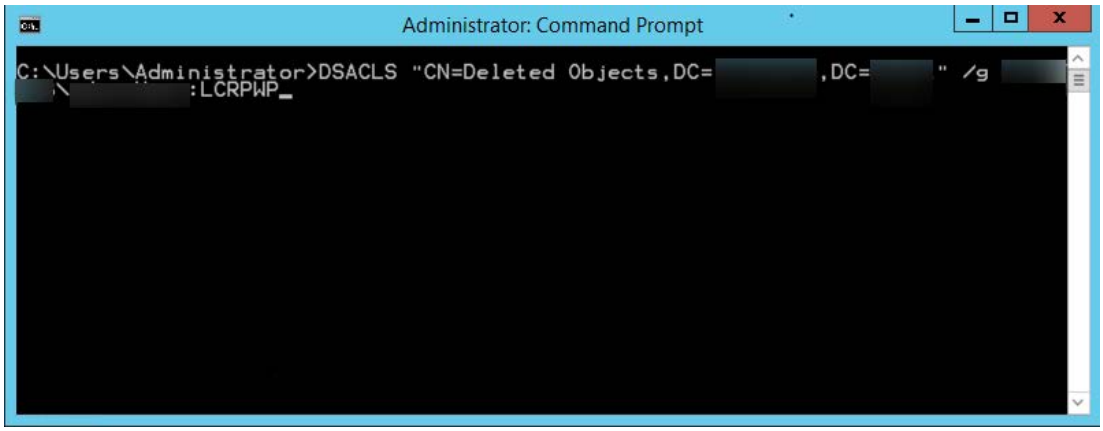


笔记：

- 林中的每个域都有自己的已删除对象容器，因此指定该容器至关重要。
您要修改权限的已删除对象容器的域名。

- 代替**admanagerplus**,和**com**包含您的领域组件。

3. 要授予安全主体访问已删除对象容器的权限，请指定一个
命令格式如下：dsacls "CN=已删除对象,DC=admanagerplus,DC=com"
/g ADMANAGERPLUS\LukeJohnson:LCRPWP



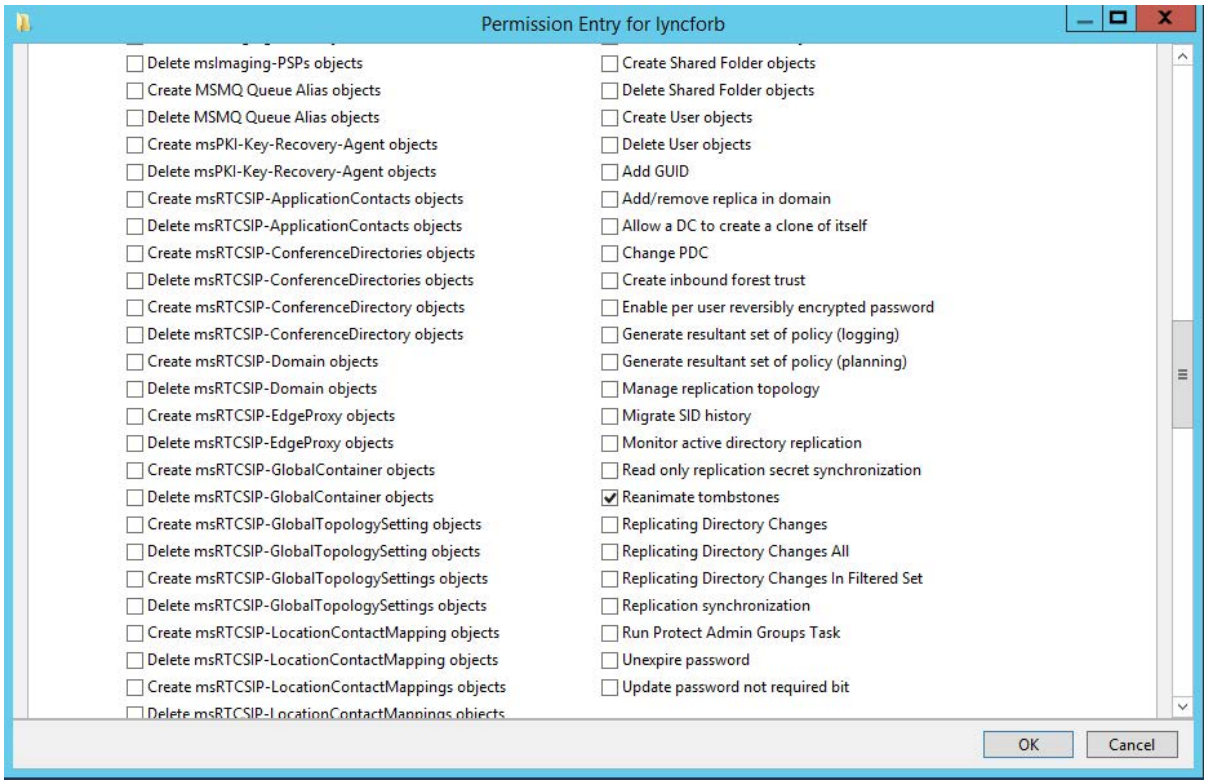
笔记：将“LukeJohnson”替换为您选择的安全负责人。

4. 接下来，连接到默认命名上下文，右键单击域根，然后选择**特性**。

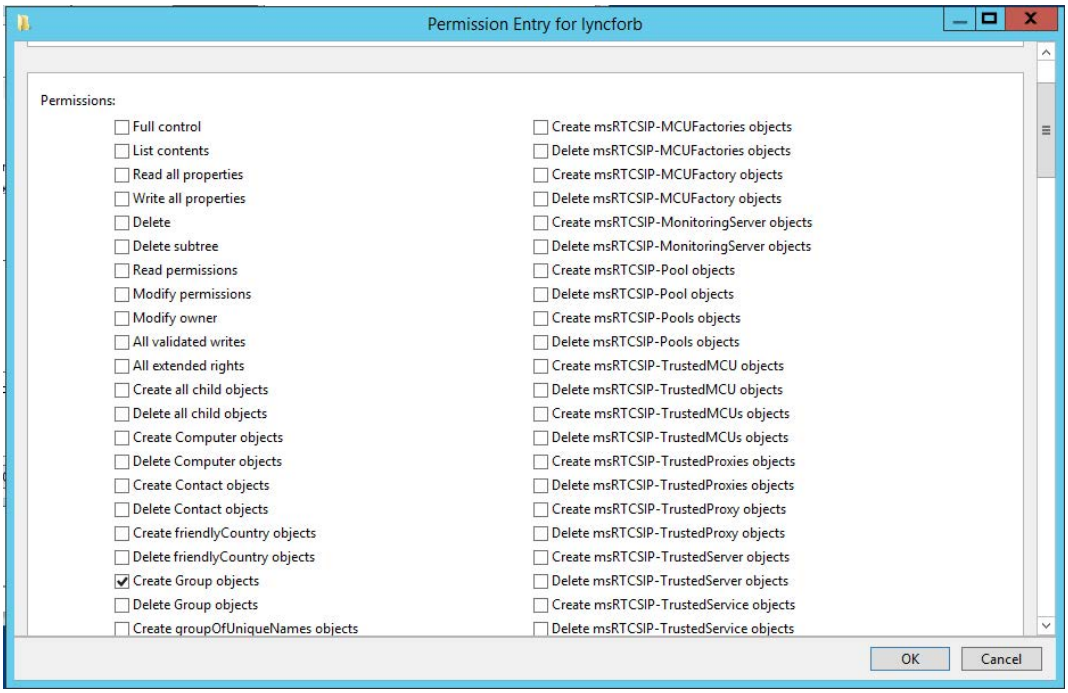
5. 在**安全**点击 Tab 键**高级**。

6. 添加用户或组，并选择以下权限：

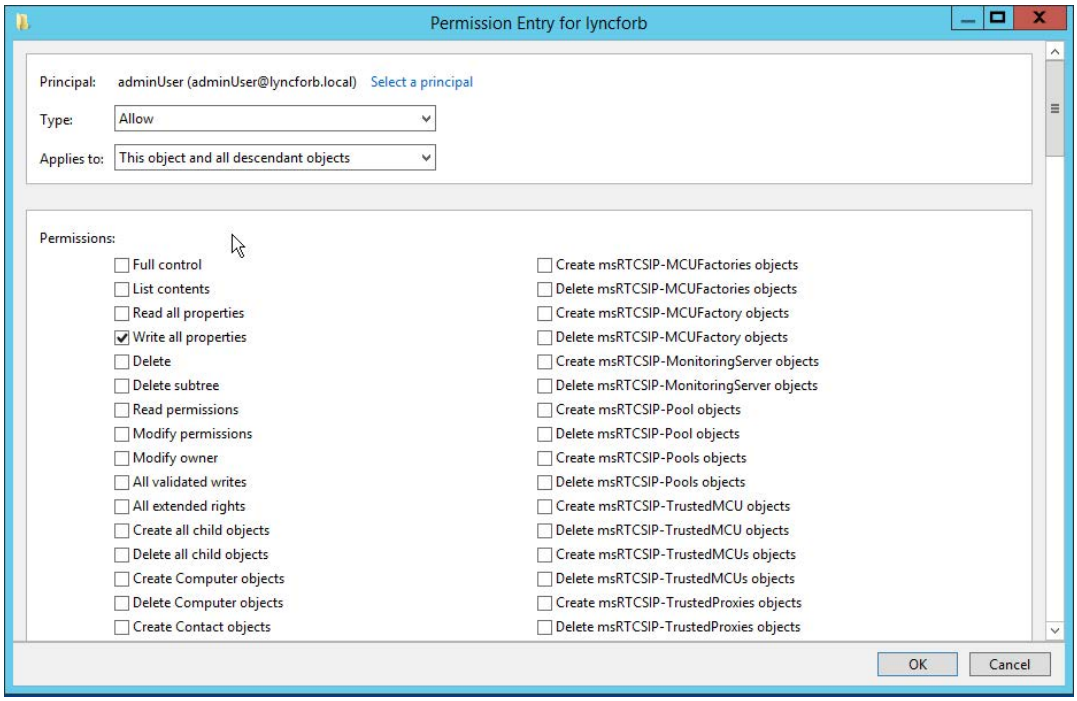
   a. 恢复已删除对象



b. 创建组对象



c. 写出所有属性



笔记：应用**恢复已删除对象权利**对被保护的对象及其子对象。

7. 点击**好的**。

笔记：只有在委派上述权限之后删除的对象才能恢复。

GPO管理和报告

操作	需要权限
创建组策略对象	- 必须是“组策略创建者所有者”组的成员
启用/禁用组策略对象	- 必备**编辑设置**已在组策略对象 (GPO) 中选择权限。 **笔记：**要了解如何将编辑设置权限委派给 GPO 中的组或用户，请参阅：本文档。
启用/禁用用户配置设置	- 必备**编辑设置**已在组策略对象 (GPO) 中选择权限。 **笔记：**要了解如何将权限委派给 GPO 中的组或用户，请参阅：本文档。
启用/禁用计算机配置设置	- 必备**编辑设置**已在组策略对象 (GPO) 中选择权限。 **笔记：**要了解如何将权限委派给 GPO 中的组或用户，请参阅：本文档。
启用/禁用/删除 GPO 链接	- 必须选择**链接 GPO**在**权限**下拉列表。 **笔记：**要了解如何委派权限以链接组策略对象，请参阅本文档。
编辑 GPO 设置	- 必须在 GPO 中选择“编辑设置”权限。 **笔记：**要了解如何将权限委派给 GPO 中的组或用户，请参阅：本文档。
强制执行 GPO 链接	- 必须选择**链接 GPO**在**权限**下拉列表。 **笔记：**要了解如何委派权限以链接组策略对象，请参阅本文档。
报告	- 必须对站点/域/OU 对象（在 gPlink 属性上）具有读取权限。 - 必须对站点/域/OU 对象（在 gPOptions 属性上）具有读取权限。 - 必须对 GPO 对象（标志、版本号、修改时间戳、创建时间戳属性）具有读取权限。 **笔记：**默认情况下，“域用户”组将拥有生成报告的权限。

报告	- 确保运行该产品的帐户（services.msc 或命令提示符上下文）具有建立与域的 DC 的远程 PowerShell 连接所需的权限。 **笔记：**请参阅此页面了解启用远程 PowerShell 连接的先决条件和配置。如果在建立连接过程中遇到任何问题，请查看此页面进行故障排除。

笔记：域管理员和企业管理员组的成员可以使用 ADManager Plus 执行上述所有 GPO 管理和报告操作。对于需要 PowerShell 远程处理的操作，必须满足指定的先决条件。

AD报告

运营	需要权限
生成所有 AD 报告	- 必须具备*看法*在所需的组织单元/域中拥有权限。
生成所有 NTFS 报告	- 必须具备*读*对相关文件夹的权限

笔记：除了上述权限之外，还有*复制目录更改*如果服务帐户没有域管理权限，则必须授予权限才能在 AD 和 ADManager Plus 之间进行有效的数据同步。

操作：生成 BitLocker 报告

所需权限：

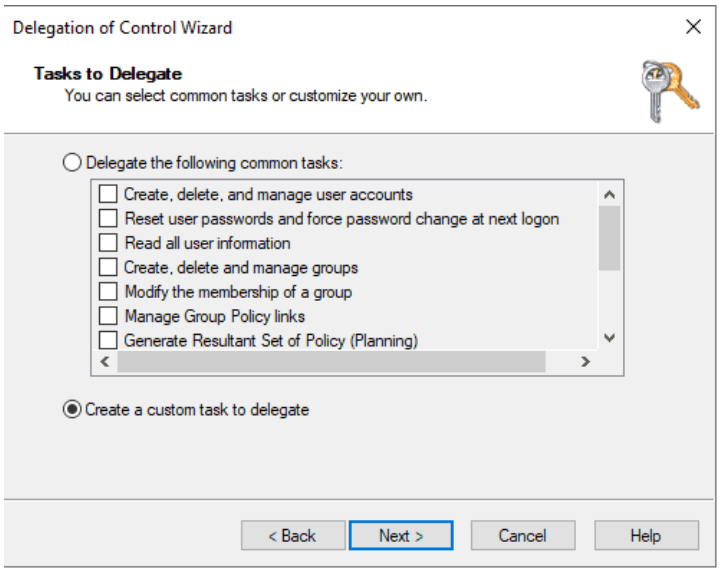
- 必须拥有目标组织单元和域的查看权限

授予查看 BitLocker 恢复密钥权限的步骤

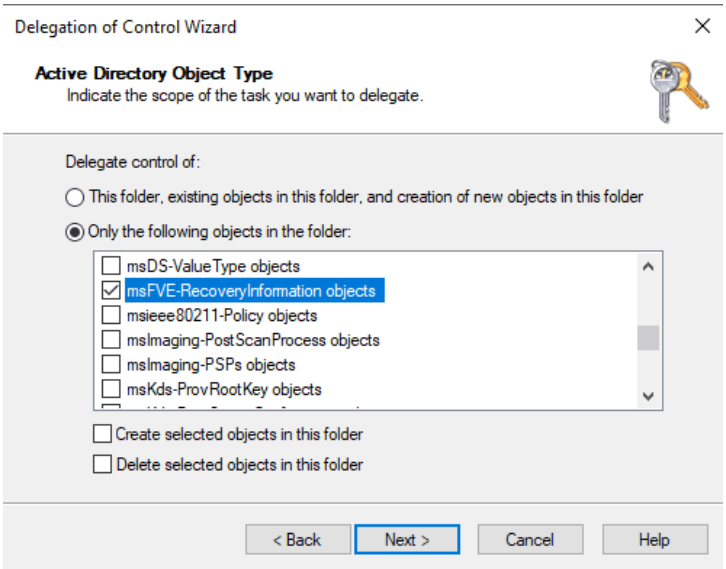
1. 登录到您的域控制器并启动**活动目录用户和计算机。**
2. 找到并右键单击需授予权限的域或组织单元
   并选择**委托控制**“委派控制权”向导将弹出。
3. 点击**下一个。**

4. 选择所需**用户帐户**或者OU然后点击**下一个**。

5. 选择**创建自定义任务以进行委派**点击**下一个**。

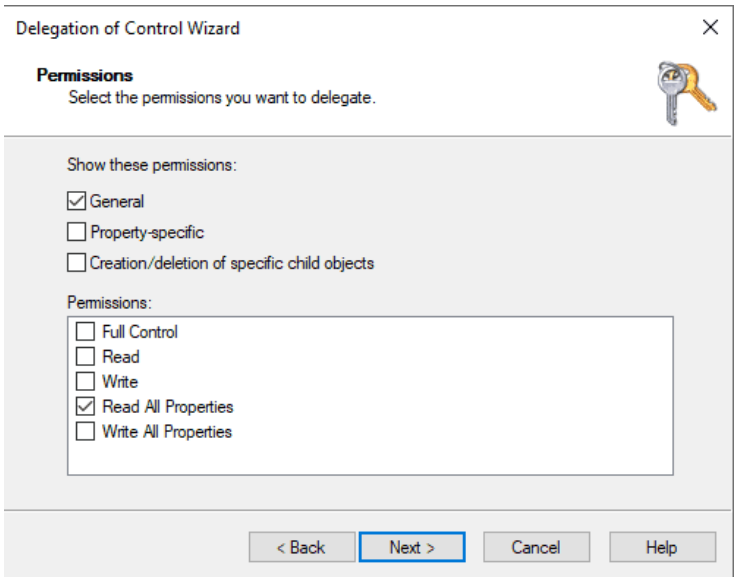


6. 选择**文件夹中只有以下对象**选项，检查毫秒**TPM 信息对象**
对象和**msFVE-恢复信息对象**然后点击**下一个**。

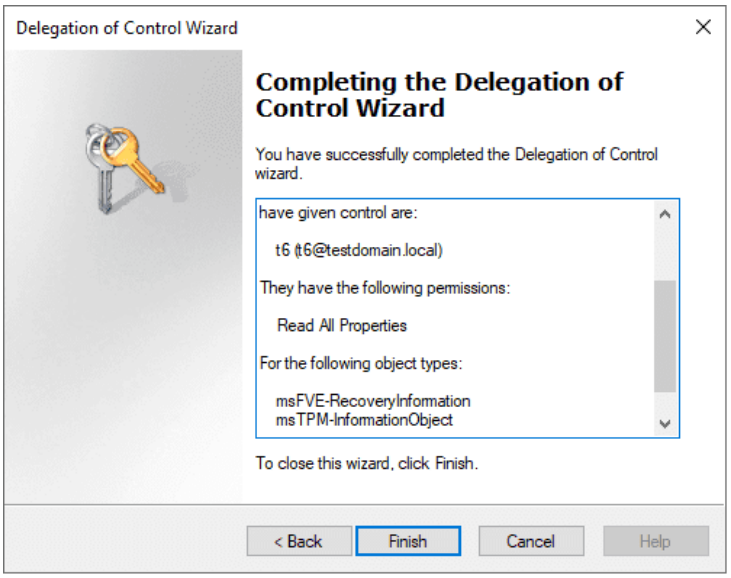


7. 在……之下*显示这些权限*部分，选择**一般的**和**特定属性**。

8. 在……之下*权限*在该部分中，选择**阅读，写作，** 和**阅读所有属性**权限
然后点击**下一个**。



9. 点击**结束**。



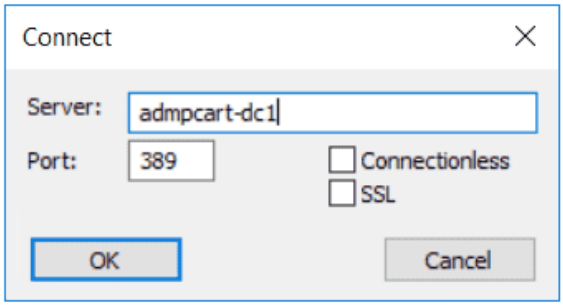
笔记：这些步骤仅启用读取级别权限。

使用 LDP 授予控制访问权限的步骤

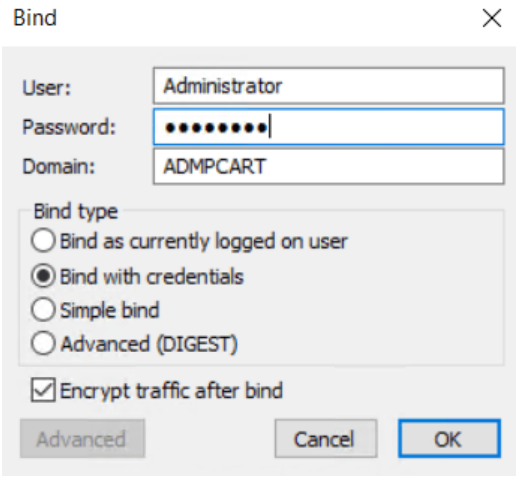
要启用控制访问权限，请以域管理员身份执行以下步骤：

1. 在域控制器上，启动**LDP.exe**。

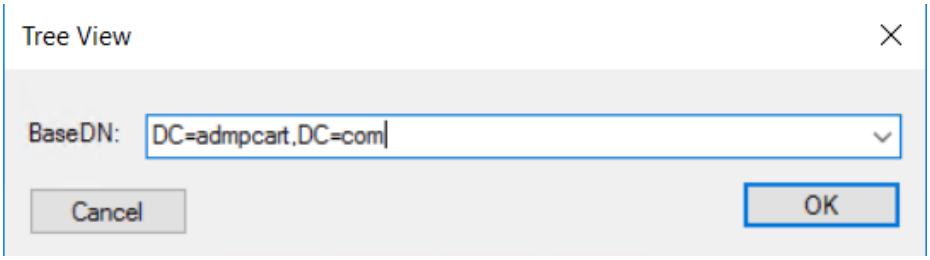
2. 导航至**连接 > 连接**，进入**服务器名称**和**端口号**点击**好的**。



3. 前往**连接 > 绑定**进入**用户名，密码，** 和**域名**选择
绑定类型然后点击**好的。**



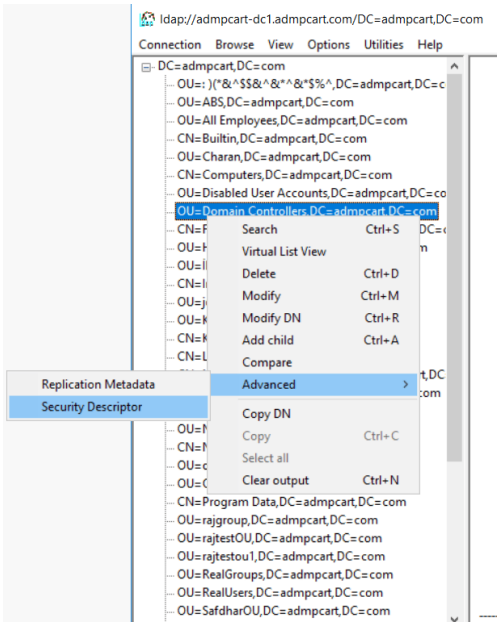
4. 选择**查看 > 树**进入**基本数字网络**然后点击**好的。**



5. 展开目录树并选择所需的组织单元 (OU)。

6. 右键单击 组织单元 (OU) 并导航至**高级 > 安全描述符。**

7. 进入**专有名称 (DN)**点击**好的。**



8. 在*安全描述符*点击对话框**添加**。

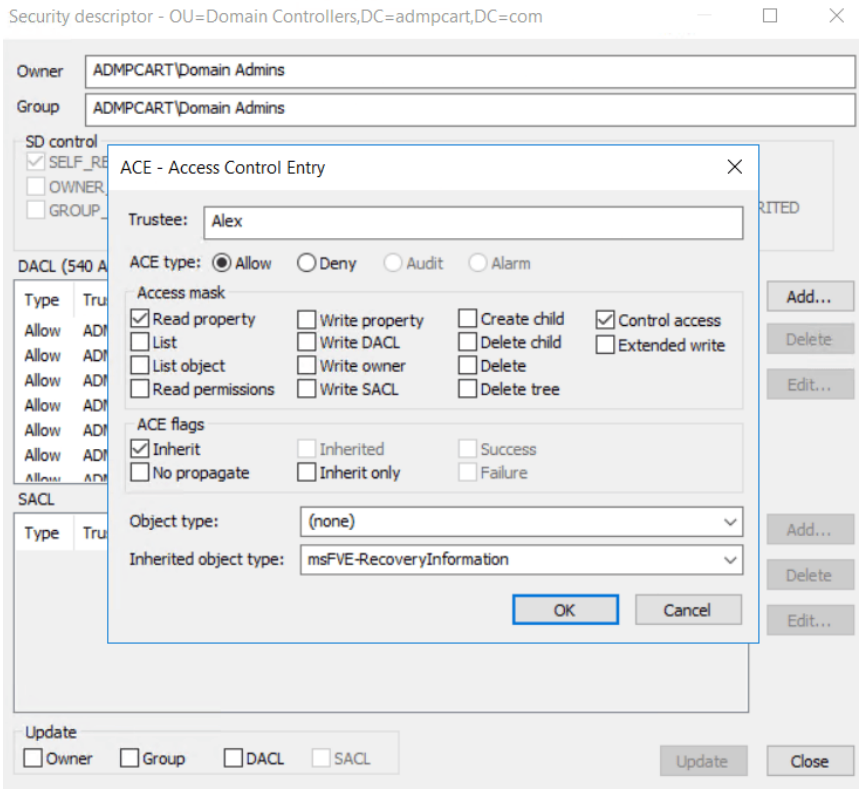
9. 在*门禁控制入口 (ACE)*对话：

   选择**阅读属性**和**控制访问权限**权限*访问掩码*。

   选择**继承**在下面*ACE旗帜*。

   选择**msFVE-恢复信息**作为继承的对象类型。

10. 点击**好的**应用这些权限。



文件权限管理

运营	需要权限
修改/删除 NTFS 权限	- 必须拥有相关文件夹的读取和写入权限
修改/移除共享权限	- 必须能够从安装了 ADManager Plus 的计算机访问该共享文件夹。

Exchange管理

运营	交换版本	需要权限
在 AD 中创建相应用户帐户的同时创建 Exchange 邮箱。	2007 年Exchange	- 必须具有 Exchange 收件人管理员角色和帐户操作员角色。
	2010 年Exchange及以上	- 必须是组织管理团队的一员
为现有 Active Directory 用户创建 Exchange 邮箱	2007 年Exchange	- 必须具有 Exchange 收件人管理员角色和帐户操作员角色。
	Exchange 2010 及以上	- 必须是组织管理团队的一员
设置邮箱权限	2007 年Exchange	- 必须拥有 Exchange 只读管理员角色、管理信息存储权限以及对邮箱所在邮箱存储的写入权限。
	Exchange 2010 及以上	- 必须是组织管理团队的一员
交易所报告	所有版本（2019年、2016年、2013年、2010年、2007年和2003年）	- 必须拥有 Exchange 只读管理员角色。

笔记：只有企业管理员才能执行跨林 Exchange 管理。

Microsoft 365 管理和报告

下面列出了在 ADManager Plus 中配置的服务帐户所需的角色和权限（最小范围）。

模块	角色名称	范围
管理	用户管理员	管理用户、联系人和群组。
	特权身份验证管理员	重置密码并阻止或解除阻止管理员。
	特权角色管理员	管理 Azure Active Directory 中的角色分配。
	Exchange 管理员	更新邮箱属性。
	Teams 服务管理员	管理 Microsoft Teams。
报告	全球读者	获取所有 Microsoft 365 服务的报告。
	安全读卡器	获取安全功能、登录报告和审计日志的只读访问权限。

下面列出了在 ADManager Plus 中配置的 Microsoft Entra ID 应用程序所需的角色和权限（最小范围）。

模块	API名称	允许	范围
管理	微软图形	用户.读写.全部	用户创建、修改、删除和恢复
		Group.ReadWrite.All	创建、修改、删除和恢复群组；添加或移除成员和所有者

报告	微软图形	用户读取全部	用户和群组成员报告
		群组读取全部	集团报告
		联系阅读	联系报告
		报告.阅读.全部	使用情况报告
		组织.阅读.全部	许可证详情报告
		审计日志读取全部	审计日志报告
	Azure Active 目录图	域.读取.全部	基于领域的报告

要了解在 ADManager Plus 中配置 Microsoft 365 帐户的先决条件，请单击这里。

Active Directory 迁移

运营	需要权限
用户迁移	域管理员

Google Workspace 管理和报告

运营	需要权限
管理	API作用域： https://www.googleapis.com/auth/admin.directory.user https://www.googleapis.com/auth/admin.directory.group https://www.googleapis.com/auth/admin.directory.orgunit https://www.googleapis.com/auth/admin.directory.domain.readonly
报告	API作用域： https://www.googleapis.com/auth/admin.directory.user

要了解在 ADManager Plus 中配置 Google Workspace 帐户的先决条件，点击这里。

高可用性先决条件

高可用性 (HA) 指的是旨在确保达到约定可用性级别的系统或组件。
在比正常情况下更长的时间内保持良好的运行性能。ADManager Plus 可以帮助管理员
为防止主服务器故障，保持备用服务器的高可用性。

ADManager Plus 通过采用高可用性架构来实现这一点，该架构指定了一个备份。
服务器充当主服务器的保护屏障。

- 两个服务器使用同一个数据库，并且在任何给定时间，只有一个服务器负责处理
  当一个用户处于非活动状态时，另一个用户会发出请求。

- 每当主服务器遇到计划外停机时，备用服务器就会接管。
  开始运行并接管组件的控制权。

先决条件：

- 主服务器和辅助服务器必须位于同一子网中。

- 两个服务中配置的用户帐户必须是域管理员组的成员。
  在 ADManager Plus 中配置高可用性时。

- 确保此用户帐户对主目录和共享目录都具有 NTFS 和共享权限。
  辅助服务器以及 C$(管理共享)。

笔记：配置高可用性时，用户帐户必须是域管理员组的成员。成功启用高可用性后，您可以将此用户帐户替换为具有运行 ADManager Plus 服务所需权限的最小权限用户帐户。这些步骤。

在 ADManager Plus 中配置高可用性的步骤：

要在 ADManager Plus 中启用高可用性：

1. 在主服务器上登录 ADManager Plus。
2. 导航至“管理”选项卡，然后单击**高可用性**。
3. 选择**启用高可用性**。
4. 在……之下**主服务器 URL**在此字段中，输入在主服务器上运行的 ADManager Plus 的 URL。
5. 在……之下**备用服务器**在本部分，输入：
   a. 备用服务器上运行的 ADManager Plus 的 URL 或 IP 地址。
   b. 备用服务器中的 ADManager Plus 内置管理员凭据。

6. 在……之下**虚拟 IP**输入以下部分：

   a. 可用于访问主服务器和备用服务器的 IP 地址。当此
   使用 IP 地址访问产品，数据通过当时可用的服务器进行路由。

   笔记：只有未使用的IP地址才能用作虚拟IP地址。要确保某个IP地址未使用，请尝试ping该IP地址。
   使用命令提示符。如果*请求超时*显示错误，该 IP 地址可能
   可用作虚拟IP地址。

   b.**虚拟主机名**这是分配给虚拟 IP 的别名。可以设置虚拟主机名。
   通过使用DNS服务器。

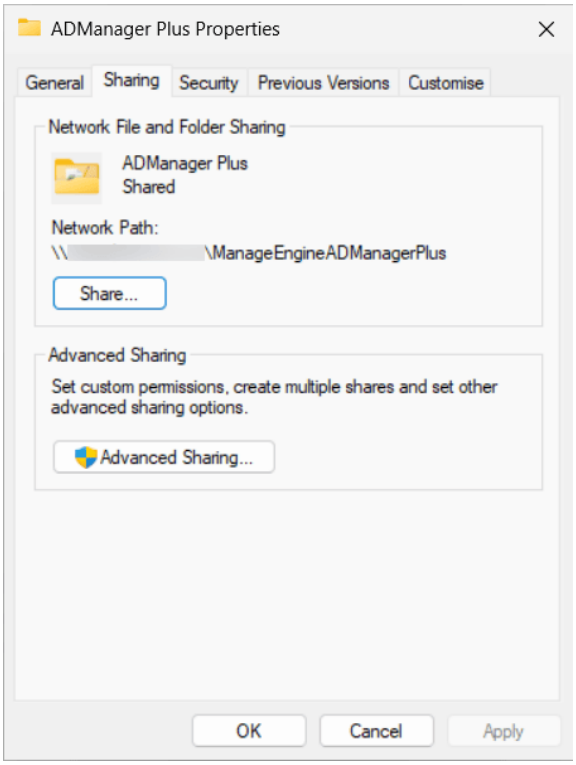
7. 点击**节省**。

笔记：
之后，您可以将此用户帐户从域管理员组中删除。

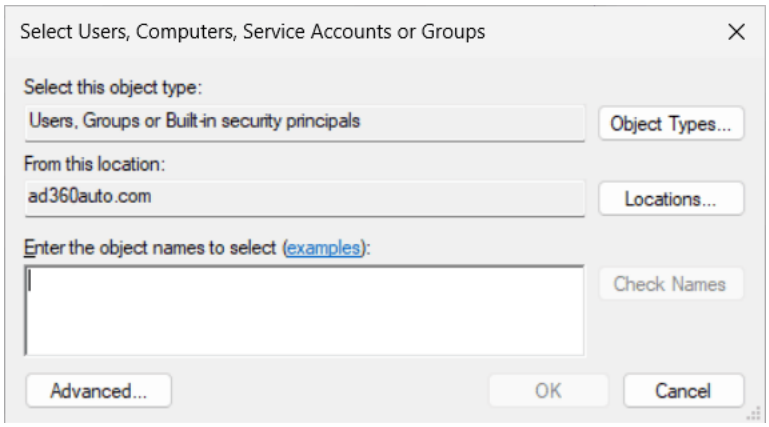
配置低权限用户以实现高可用性的步骤

使用域管理员帐户完成高可用性配置后，请按照以下步骤操作：
将该帐户替换为非域管理员的用户帐户。**services.msc**。

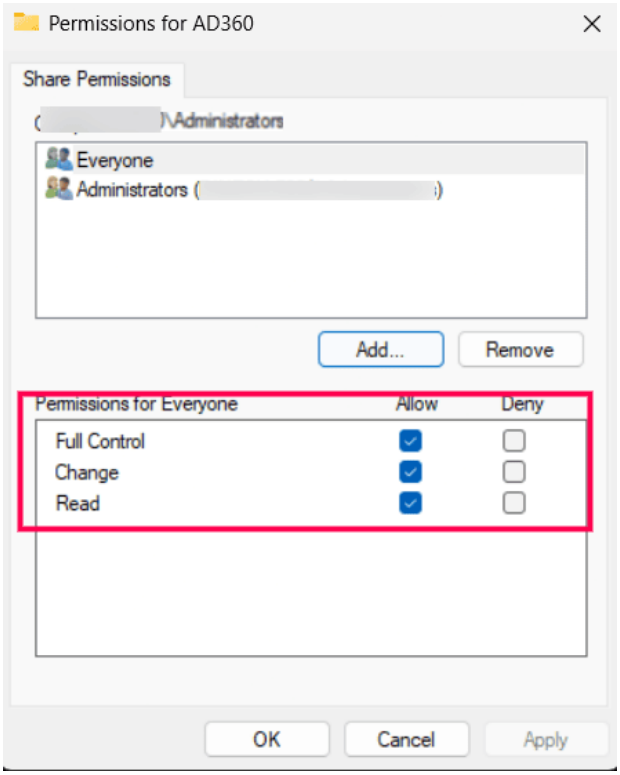
1. 创建一个域用户，用于在两台机器上运行 ADManager Plus 服务。
2. 授予该用户对两台机器上产品安装文件夹的完全权限：
   - 导航至 ADManager Plus 安装目录。
   - 右键单击**ADManager Plus**文件夹并打开**分享**标签。



   - 选择**高级共享 > 权限 > 添加。**



- 输入新创建的域用户并单击**好的**。
- 添加完成后，授予用户权限**完全控制**。



- 点击**申请**和**好的**保存更改。
- 在两台服务器上重复这些步骤。

3. 在两台机器上都为新创建的用户分配本地管理员权限，以确保虚拟IP功能。
   - 使用现有管理员帐户登录计算机。
   - 打开**跑步**对话框，输入**lusrmgr.msc**打开本地用户和组管理器。
   - 在左侧窗格中，选择OU。
   - 在右侧窗格中，双击“管理员”组。
   - 在*管理员属性*点击窗口**添加。**
   - 在*选择用户*点击窗口**地点**并选择您的域名。
   - 请按以下格式输入域名用户名**域名\用户名**或点击**高级 > 立即查找搜索**并选择用户。
   - 点击**好的**， 然后**申请，**和**好的**再次确认。
   - 域用户现已添加为该计算机的本地管理员。

   在主服务器和辅助服务器上重复这些步骤。
4. 打开**services.msc**在两台服务器上都进行更新**ManageEngine ADManager Plus**为使用新创建的用户帐户而不是域管理员帐户运行。
5. 按顺序重启 ADManager Plus 服务：
   - 首先重启**主服务器的**服务。
   - 然后重新启动**辅助服务器的**服务。
6. 无需更改域设置。更新服务登录用户**services.msc**就足够了。

如果您需要任何进一步的帮助或信息，请邮件至Support@manageengine.cn或致电我们**+86 400-660-8680。**

ManageEngine
ADManager Plus

我们的产品

AD360 |Log360 | ADAudit Plus| ADSelfService Plus

M365 Manager Plus | RecoveryManager Plus

关于 ADManager Plus

ADManager Plus 是一款身份治理与管理 (IGA) 解决方案，可简化身份管理、确保安全性并提升合规性。借助 ADManager Plus，您可以管理从配置到取消配置的用户生命周期，运行访问认证活动，协调跨企业应用程序的身份管理，并通过定期备份保护企业平台上的数据。利用 200 多个报告，深入了解身份及其访问权限。通过工作流、自动化和基于角色的访问控制策略，提高 IGA 操作效率。 ADManager Plus的Android和iOS应用程序有助于随时随地管理 AD和EntraID。

有关 ADManager Plus 的更多信息，请访问
manageengine.cn/products/ad-manager/。

$ 获取报价　⬇ 下载