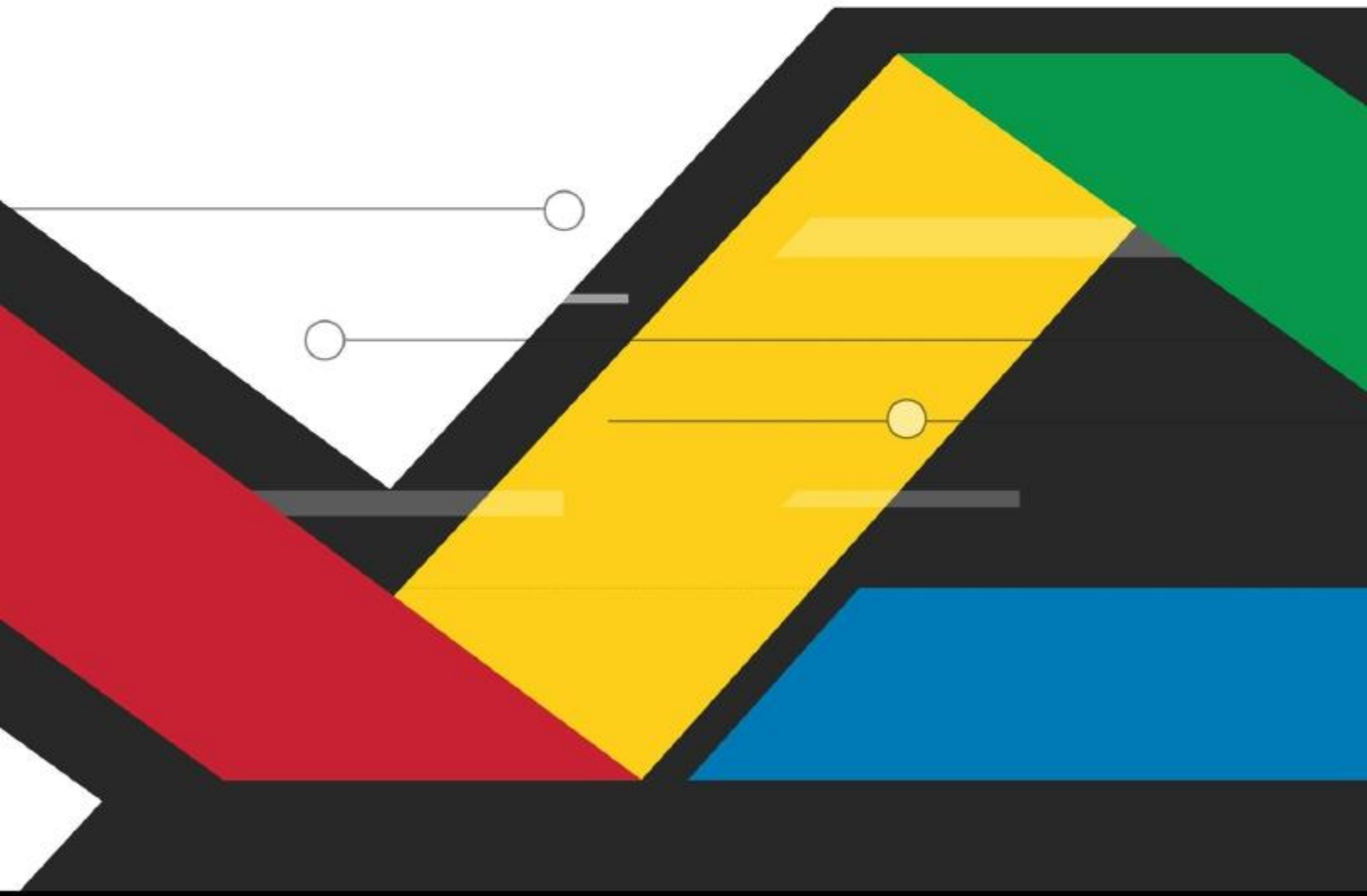


非管理员域用户的 WMI 日志收集



本文档介绍了如何创建一个非管理员域用户，而该用户具有从域控制器收集 WMI 日志的必要权限。

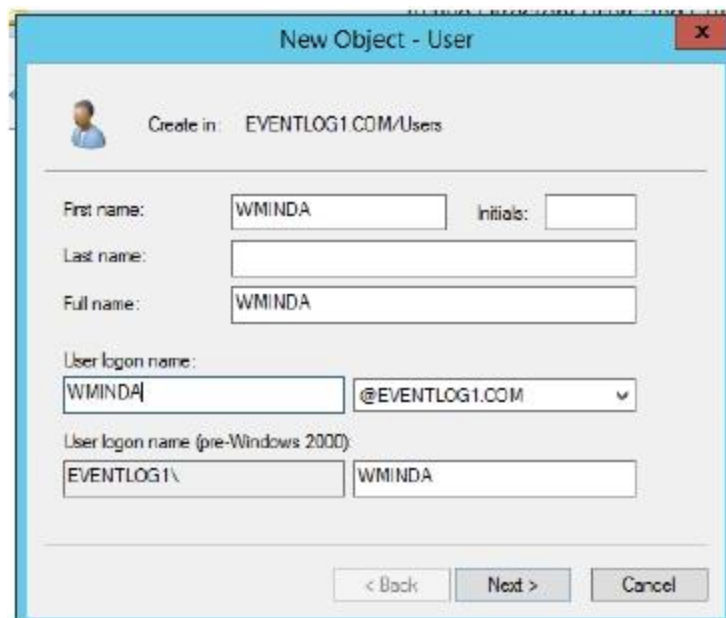
概要

1. 在 **Active Directory** 中创建一个非管理员域用户。
2. 将创建的用户添加到必要的 **AD** 用户组。
3. 在组策略管理控制台中创建一个新的组策略。
4. 指派权限给创建的用户。
5. 强制创建的组策略。
6. 在 **WMI** 客户端和服务端中更新组策略。
7. 授予 **WMI** 命名空间安全权限给创建的用户。
8. 授予 **COM** 权限给创建的用户。
9. 在 **EventLog Analyzer** 的 **web** 控制台使用该非管理域用户的凭证进行日志收集。

步骤

1. 在 **Active Directory** 中创建一个非管理员用户

- a. 打开 **Active Directory** 用户和计算机。
- b. 点击 **用户 > 新建 > 用户**。
- c. 在弹出的窗口中输入指定的详细信息，并创建用户。

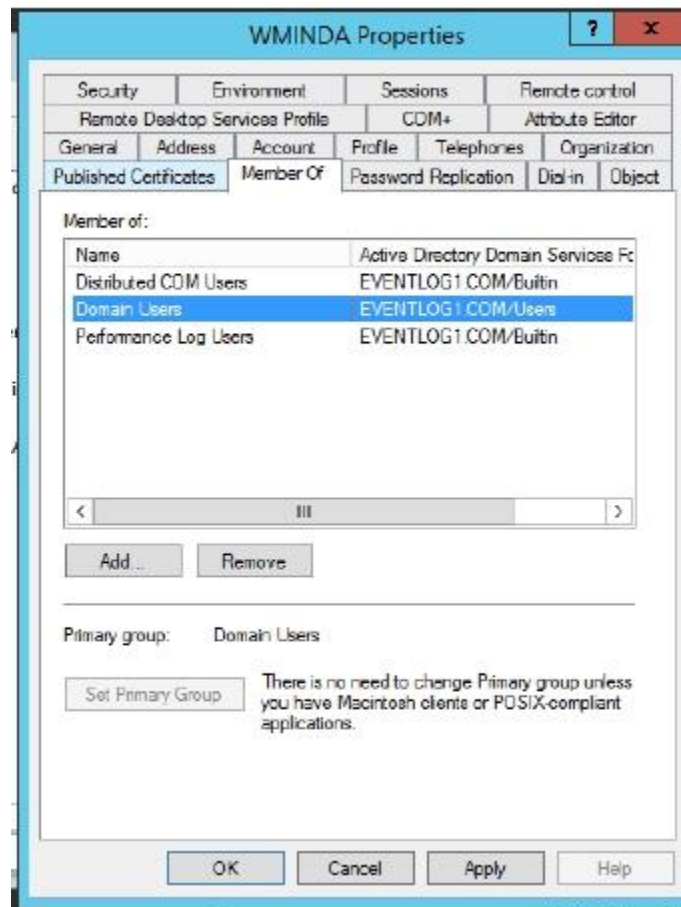


The screenshot shows the 'New Object - User' dialog box in Active Directory. The 'Create in' field is set to 'EVENTLOG1.COM/Users'. The 'First name' field contains 'WMINDA'. The 'Last name' field is empty. The 'Full name' field contains 'WMINDA'. The 'User logon name' field contains 'WMINDA' and the domain dropdown is set to '@EVENTLOG1.COM'. The 'User logon name (pre-Windows 2000)' field contains 'EVENTLOG1\WMINDA'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'.

2. 将创建的用户添加到必要的 AD 用户组

在创建的用户上点击右键并选择**添加到组**。用户需要添加到以下组中。

- Performance Log Users
- Distributed COM Users



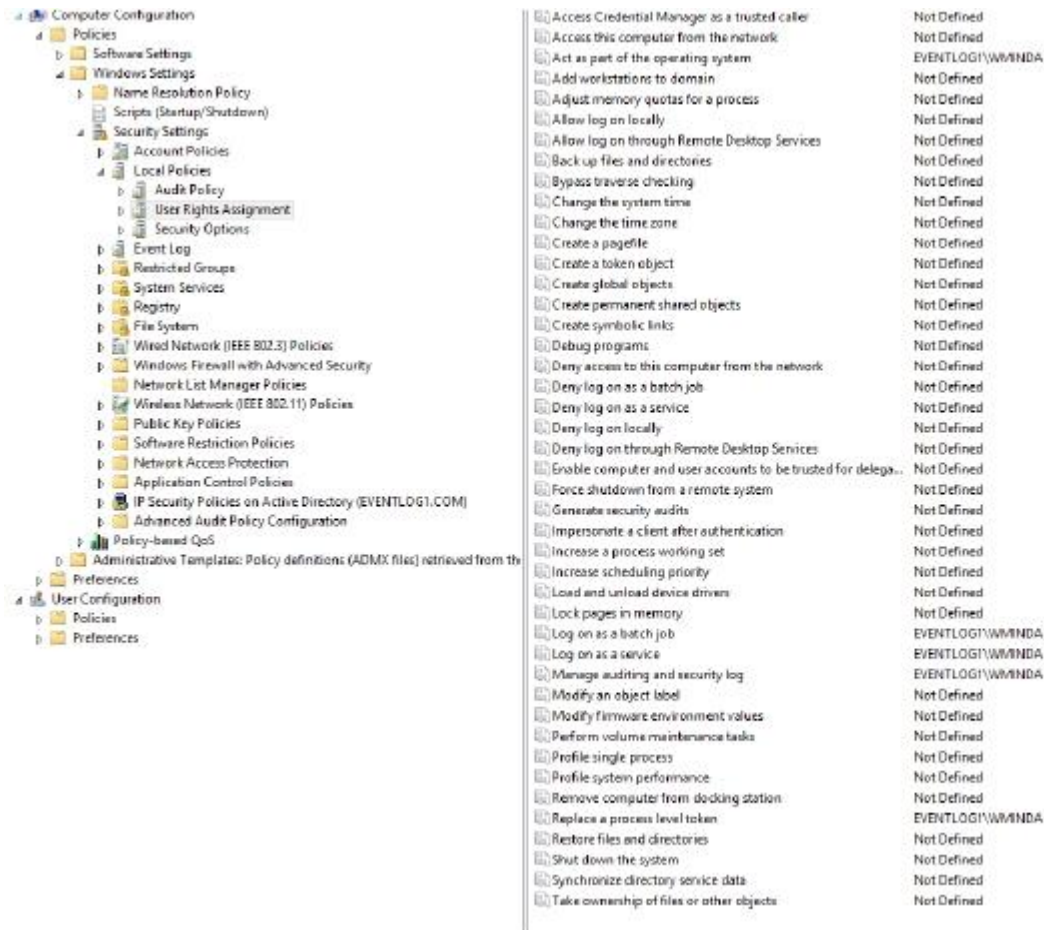
3. 在组策略管理控制台中创建一个组策略。

4. 指派权限给创建的用户

- 右键点击创建的组策略，然后点击**编辑**。
- 打开组策略管理编辑器，打开计算机配置 > 策略 > **Windows 设置** > 安全设置 > 本地策略 > 用户权限分配。
- 右键点击指定的权限然后点击**属性**，授予创建的用户以下权限。
- 启用定义这些策略设置，点击 **添加用户和组**，选择创建的用户然后点击应用权限。

权限

- 以操作系统的方式执行
- 作为批处理作业登录
- 作为服务登录
- 替换一个进程级令牌
- 管理审核和安全日志



5. 强制创建的组策略

在左窗格中，右键单击创建的组策略并单击**强制**。

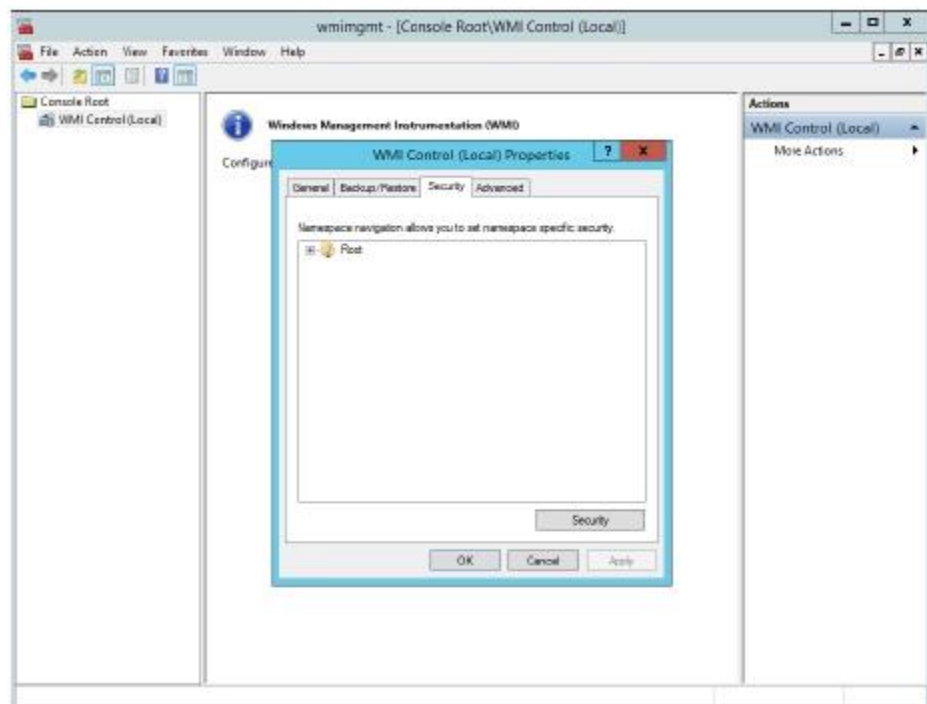
6. 在 WMI 客户端和服务端中更新组策略

在客户端和服务端中以管理员的方式打开**命令提示符**，并运行以下命令。

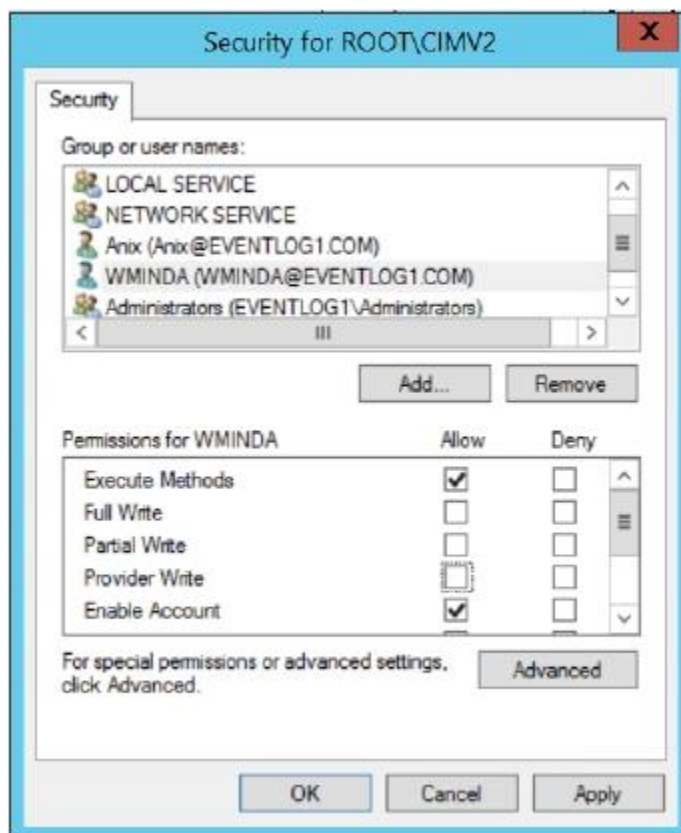


7. 授予 WMI 命名空间安全权限给创建的用户

- a. 在要收集日志的域控制器中，打开 **WIN+R**，输入 **wmimgmt.msc** 打开 **WMI 管理控制台**。



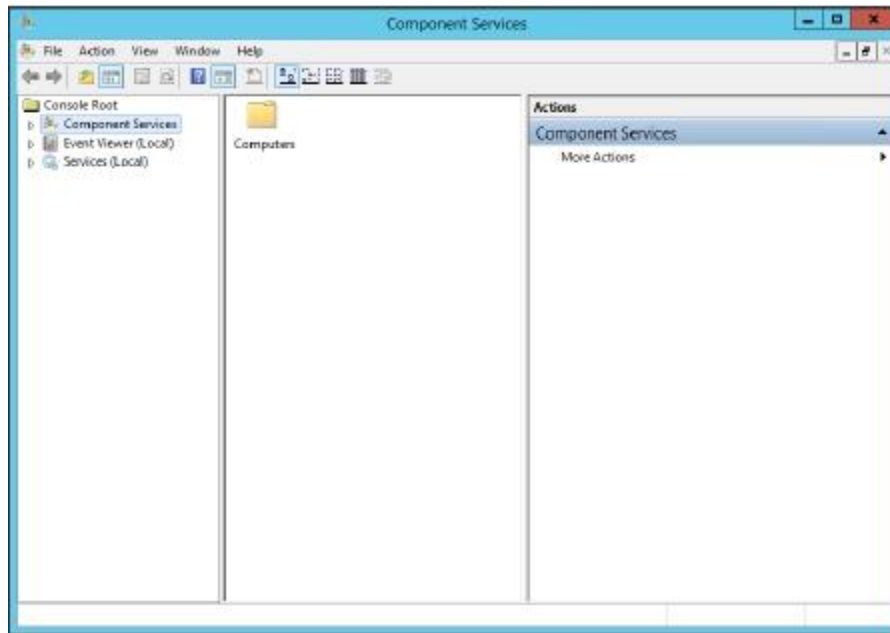
- b. 右击 **WMI 控件(本地)**，点击属性。
- c. 在 **WMI 控件属性**窗口中，点击安全页签。
- d. 在安全页签中，展开 **Root** 命名空间，选择 **CIMV2** 命名空间。



- e. 点击右下角的**安全设置**按钮，打开 ROOT\CIMV2 的安全设置。
- f. 点击**添加**并选择创建的用户。
- g. 用户现在需要被授予权限。点击用户，勾选以下权限的**允许**选框。
 - i. 执行方法
 - ii. 启用账户
 - iii. 远程启用
 - iv. 读取
- h. **应用变更**并点击**确定**，退出 WMI 管理控制台。

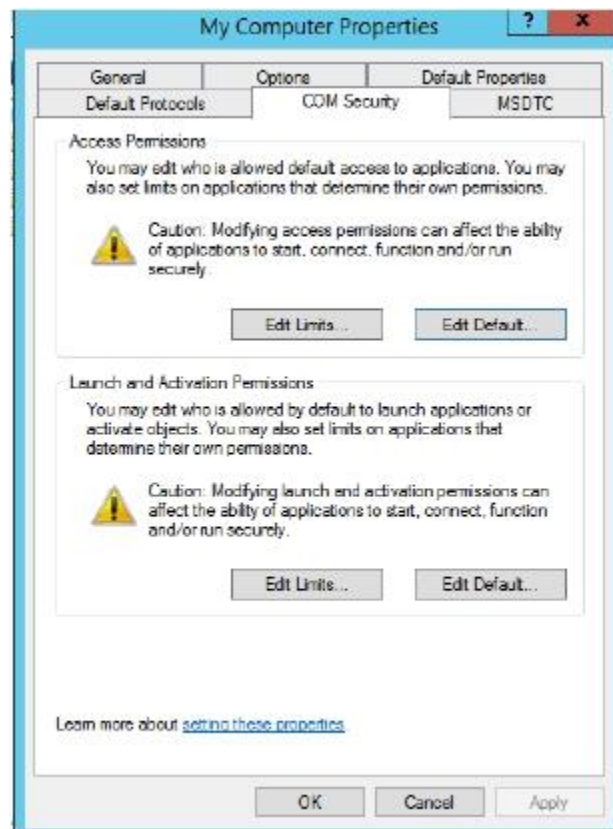
8. 授予 **COM** 权限给创建的用户

- a. 在要收集日志的域控制器中，打开**开始 > 管理工具 > 组件服务**。

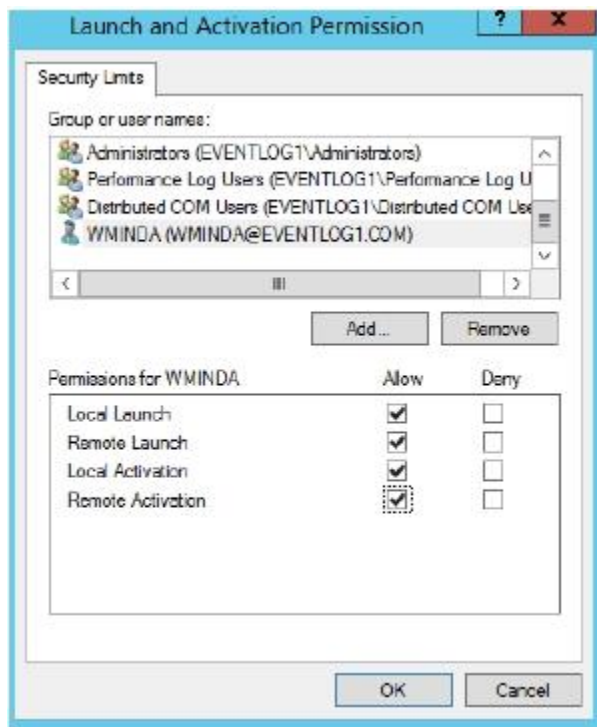


b. 打开计算机文件夹；进入我的电脑> 属性> **COM 安全**。

- 在访问权限中，点击编辑限制，点击添加，添加创建的用户。授予所有的权限，然后点击确定。



- 在启用和激活权限， 点击编辑限制， 点击添加， 添加创建的用户。 授予所有的权限， 然后点击确定。



您授予上述所有权限之后，创建的非管理员用户就能够从域控制器中收集日志了。

9. 在 **EventLog Analyzer** 的 web 控制台使用该非管理域用户的凭证进行日志收集。