使用wevtutil检查事件日志权限

目录

简介

本文档介绍如何使用wevtutil检查连接器登录事件权限。

您可以使用wbemtest测试连接器是否可以从DC读取登录事件。

如果wbemtest实际上无法连接，这通常是由于WMI/DCOM权限错误造成的，因此请在其他位置寻求帮助。

但是，在某些情况下，连接最紧密，但没有显示任何事件。

导致此问题的原因有两个：

- 审核策略不正确，因此不会在DC上跟踪登录事件。 寻求有关审计策略的帮助。
- 事件在DC上记录，但OpenDNS_Connector没有从安全事件日志读取的权限。 继续……

基础知识 — 事件日志读取器

在大多数情况下，这只需将OpenDNS_Connector用户添加到Event Log Readers组。这赋予它读取事件日志所需的权限。

wevtutil — 检查权限

在极少数情况下，事件日志读取器组没有默认权限。我们可以使用wevtutil轻松检查授予安全事件日志的权限。

只需运行：

```
wevtutil gl security
```

1. 输出显示使用SDDL语法的权限，如下所示：

```
channelAccess: O:BAG:SYD:(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;S-1-5-573)
```

2. 事件日志读取器的SID为S-1-5-32-573，或者可以缩写为ER。
3. 十六进制值用于权限，例如：
    - 0x1 =读取
    - 0x2 =写入
    - 0x3 =读/写\

修复1 — 重置为默认值

通过删除包含自定义SDDL字符串的注册表值，可将权限重置为默认值。 这是一个快速修复程序，但可能会影响从事件日志读取的其他软件（如适用）。

从HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security删除“CustomSD”值

修复2 — 使用wevtutil更新SDDL

在极少数情况下，我们可以使用wevtutil直接分配权限。

1. 使用以下命令获取当前权限（如前所述）：

```
wevtutil gl security
```

2. 记下信道访问字符串。 例如：

```
/ca:O:BAG:SYD:(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)
```

3. 计算OpenDNS_Connector用户的SID:

```
wmic useraccount where name='OpenDNS_Connector' get sid
```

4. 您可以通过将OpenDNS_Connector附加到现有通道访问字符串来授予其读取访问权限，如下所示。 用OpenDNS_Connector SID替换<SID>。

```
wevtutil sl security /ca:O:BAG:SYD:(A;;0x3;;;S-1-5-3)(A;;0x3;;;S-1-5-33)(A;;0x1;;;<SID>)
```

供参考，这是Event Log Readers组的SID。

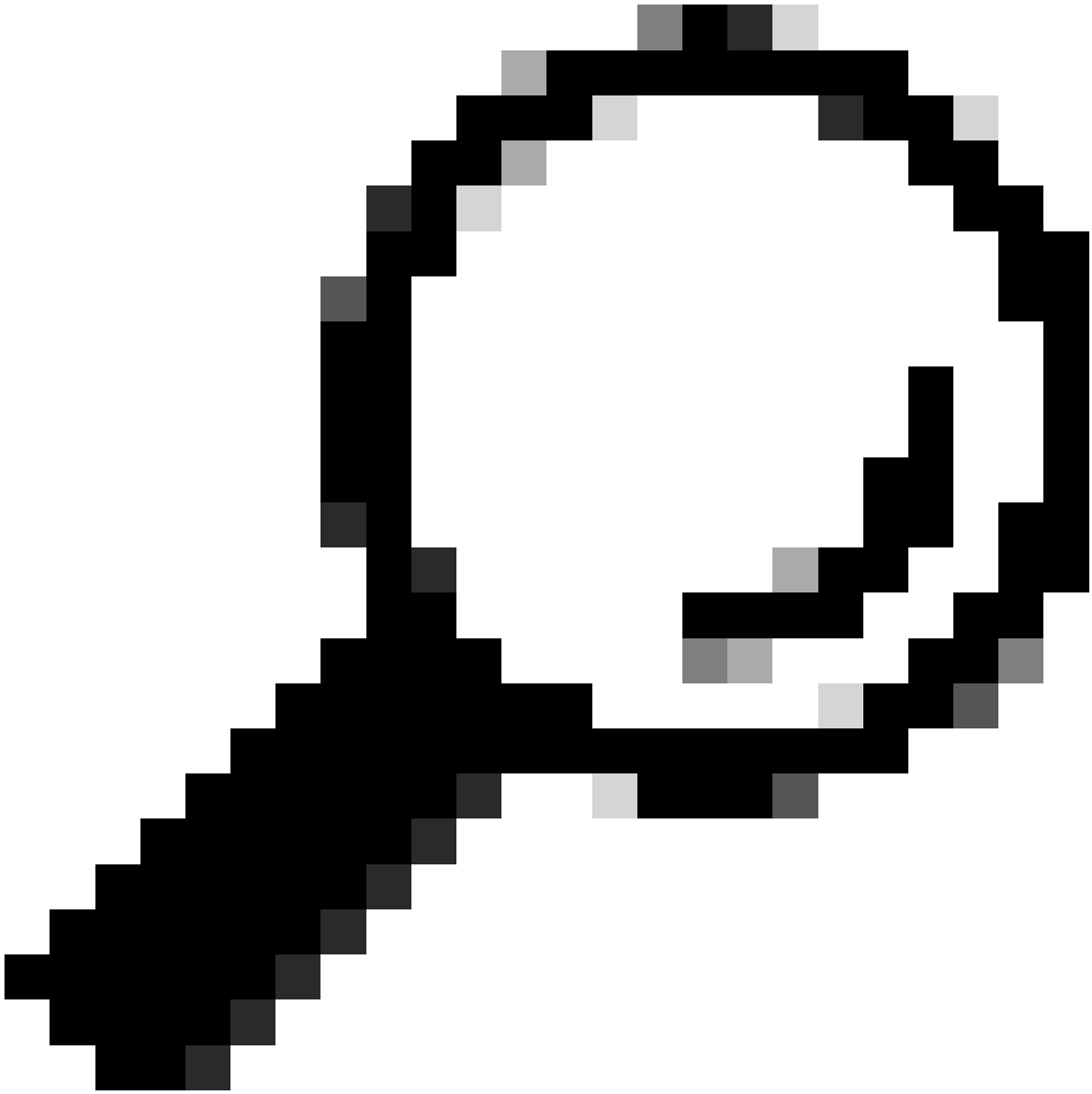
SID:S -1-5-32-573
名称：BUILTIN\事件日志读取器
描述:一个内置本地组。此组的成员可以从本地计算机读取事件日志。

修复3 - GPO

可以使用此组策略设置授予OpenDNS Connector帐户读取（和写入！）到安全事件日志的权限。从技术上讲，此设置提供的权限比所需的权限多，但这是进行更改的简单方法。

计算机配置\策略\Windows设置\安全设置\本地策略\用户权限分配\管理审核和安全日志

进行更改后，请在域控制器上运行“gpupdate /force”。



注意：在Windows 2003 / 2003功能级别上，事件日志读取器组可能不存在，因此此GPO是允许OpenDNS连接器访问这些平台的主要方法。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。