使用wevtutil檢查事件日誌許可權

目錄

簡介

本文檔介紹如何使用wevtutil檢查聯結器登入事件許可權。

您可以測試聯結器是否可以使用wbemtest從DC讀取登入事件。

如果wbemtest實際上無法連線，這通常是由於WMI/DCOM許可權錯誤導致的，因此請到其他位置尋求幫助。

但是，在某些情況下，連線最緊密，但沒有顯示任何事件。

造成這種情況的原因有兩個：

- 稽核策略不正確，因此不會在DC上跟蹤登入事件。 尋求有關審計策略的幫助。
- 事件在DC上記錄，但OpenDNS_Connector沒有從安全事件日誌讀取的許可權。 繼續……

基礎知識 — 事件日誌讀取器

在大多數情況下，這只需將OpenDNS_Connector使用者新增到「事件日誌讀取器」組即可。這樣，它就具有讀取事件日誌所需的許可權。

wevtutil — 檢查許可權

在極少數情況下，事件日誌讀取器組沒有預設許可權。我們可以使用wevtutil輕鬆地檢查授予安全事件日誌的許可權。

只需運行：

```
wevtutil gl security
```

1. 輸出顯示了使用SDDL語法的權限，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. 事件日誌讀取器的SID為S-1-5-32-573,或者可以縮寫為ER。
3. 十六進位制值用於許可權，例如：
    - 0x1 =讀取
    - 0x2 =寫入
    - 0x3 =讀/寫\

修復1 — 重置為預設值

通過刪除包含自定義SDDL字串的登錄檔值，可以將許可權重置為預設值。 這是一個快速修復程式，但是可能會影響從事件日誌讀取的其他軟體（如果適用）。

從HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security刪除「CustomSD」值

修復2 — 使用wevtutil更新SDDL

在極少數情況下，我們可以使用wevtutil直接分配許可權。

1. 使用以下命令獲取當前許可權（如前所述）：

```
wevtutil gl security
```

2. 記下通道訪問字串。 例如：

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

3. 計算OpenDNS_Connector使用者的SID:

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

4. 您可以通過將OpenDNS_Connector附加到現有通道訪問字串來授予其讀取訪問許可權，如下所示。 將<SID>替換為OpenDNS_Connector SID。

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

例如，以下是「事件日誌讀取器」組的SID。

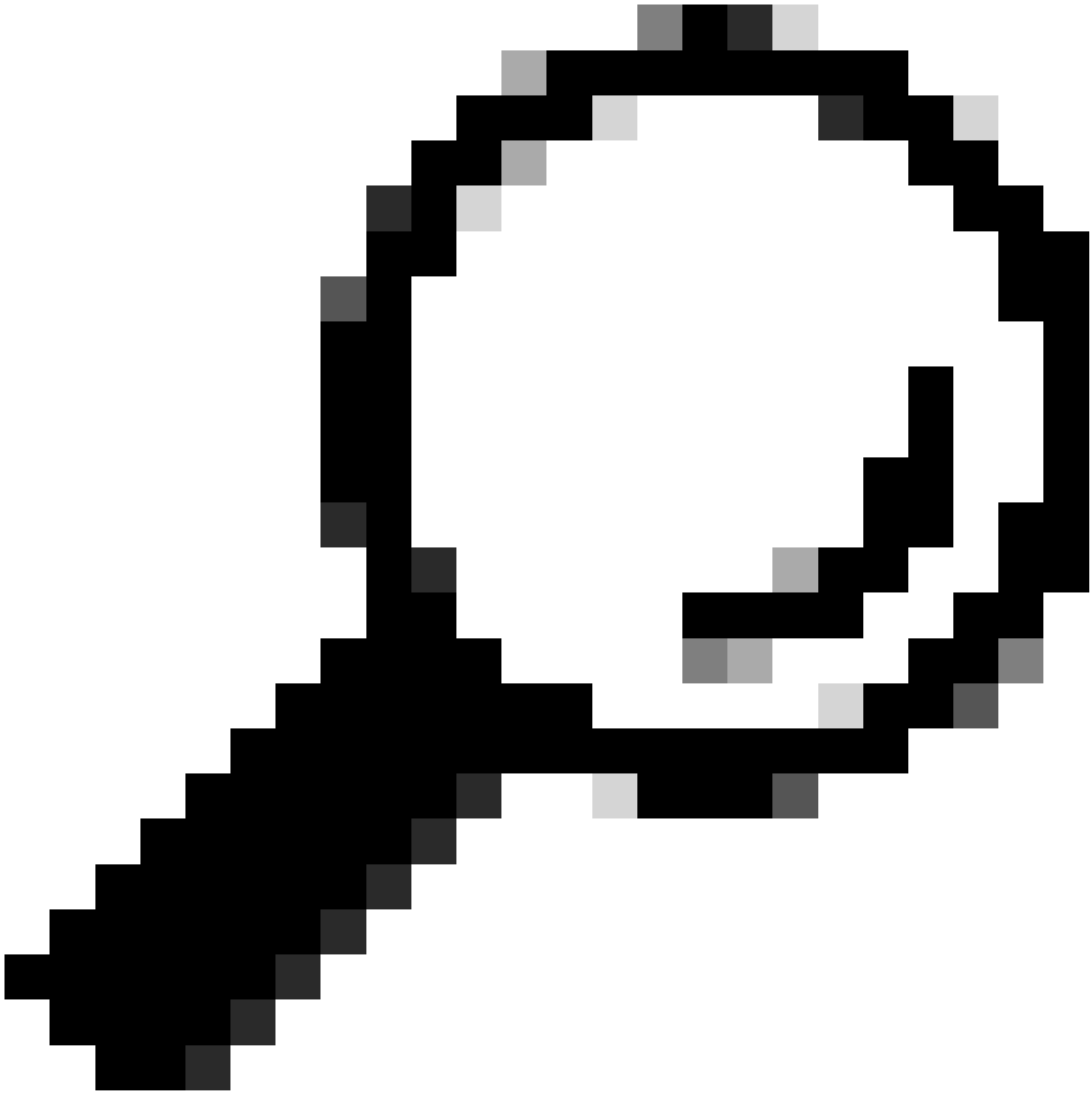
SID:S-1-5-32-573
名稱:BUILTIN\事件日誌讀取器
說明:Builtin本地組。此組的成員可以從本地電腦讀取事件日誌。

修復3 - GPO

使用此組策略設定，可以授予OpenDNS聯結器帳戶讀取（和寫入！）安全事件日誌的許可權。 從技術上講，此設定提供的許可權比所需的許可權多，但這是進行更改的一種簡單方法。

電腦配置\策略\Windows設定\安全設定\本地策略\使用者許可權分配\管理審計和安全日誌

進行更改後，請在域控制器上運行「gpupdate /force」。



附註：在Windows 2003/2003功能級別上，事件日誌讀取器組可能不存在，因此此GPO是允許OpenDNS聯結器訪問這些平台的主要方法。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。