Verwenden von wevtutil zum Überprüfen der Ereignisprotokollberechtigungen

Inhalt

Einleitung

In diesem Dokument wird die Verwendung von wevtutil zum Überprüfen von Connector-Anmeldeereignisberechtigungen beschrieben.

Mit wbemtest können Sie testen, ob der Connector Anmeldeereignisse aus einem Rechenzentrum lesen kann.

Wenn wbemtest die Verbindung nicht herstellen kann, wird dies normalerweise durch einen Fehler bei den WMI/DCOM-Berechtigungen verursacht. Suchen Sie deshalb anderswo nach Hilfe.

In einigen Fällen stellt wbemtest jedoch eine Verbindung her, zeigt aber keine Ereignisse an.

Hierfür gibt es zwei Ursachen:

- Die Überwachungsrichtlinie ist falsch, sodass Anmeldeereignisse im Rechenzentrum nicht nachverfolgt werden. Hilfe bei der Überwachungsrichtlinie einholen.
- Ereignisse werden auf dem Domänencontroller protokolliert, aber OpenDNS_Connector verfügt nicht über die Berechtigung zum Lesen aus dem Sicherheitsereignisprotokoll. Fortsetzung...

Grundlagen - Ereignisprotokollleser

In den meisten Fällen ist dies so einfach wie das Hinzufügen des OpenDNS_Connector-Benutzers zur Gruppe Ereignisprotokollleser. Dadurch erhält er die Berechtigungen, die er zum Lesen des Ereignisprotokolls benötigt.

wevtutil - Berechtigungen überprüfen

In seltenen Fällen verfügt die Gruppe Ereignisprotokollleser nicht über die Standardberechtigungen. Wir können wevtutil verwenden, um die Berechtigungen, die dem

Sicherheitsereignisprotokoll erteilt wurden, auf einfache Weise zu überprüfen.

Einfach ausführen:

```
wevtutil gl security
```

1. In der Ausgabe werden die Berechtigungen unter Verwendung der SDDL-Syntax wie folgt angezeigt:

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

2. Die SID für Ereignisprotokollleser lautet S-1-5-32-573 oder kann in ER abgekürzt werden.
3. Der Hexadezimalwert ist für Berechtigungen wie:
   - 0x1 = Lesen
   - 0x2 = Schreiben
   - 0x3 = Lesen/Schreiben\

Fix 1 - Auf Standard zurücksetzen

Berechtigungen können auf den Standardwert zurückgesetzt werden, indem ein Registrierungswert gelöscht wird, der die benutzerdefinierte SDDL-Zeichenfolge enthält. Dies ist eine schnelle Behebung, kann jedoch andere Software beeinträchtigen, die aus dem Ereignisprotokoll liest (falls zutreffend).

Löschen Sie den CustomSD-Wert aus HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security

Korrektur 2 - SDDL mit wevtutil aktualisieren

In seltenen Fällen können wir die Berechtigungen direkt mit wevtutil zuweisen.

1. Rufen Sie die aktuellen Berechtigungen wie oben beschrieben ab, und verwenden Sie den folgenden Befehl:

   ```
   wevtutil gl security
   ```

2. Notieren Sie sich die Kanalzugriffszeichenfolge. Beispiel:

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

3. Ermitteln Sie die SID für den OpenDNS_Connector-Benutzer:

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

4. Sie können OpenDNS_Connector Lesezugriff gewähren, indem Sie ihn wie folgt an die bestehende Kanalzugriffszeichenfolge anhängen. Ersetzen Sie <SID> durch die 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>)
```

Als Referenz sehen Sie hier die SID der Gruppe Ereignisprotokollleser.

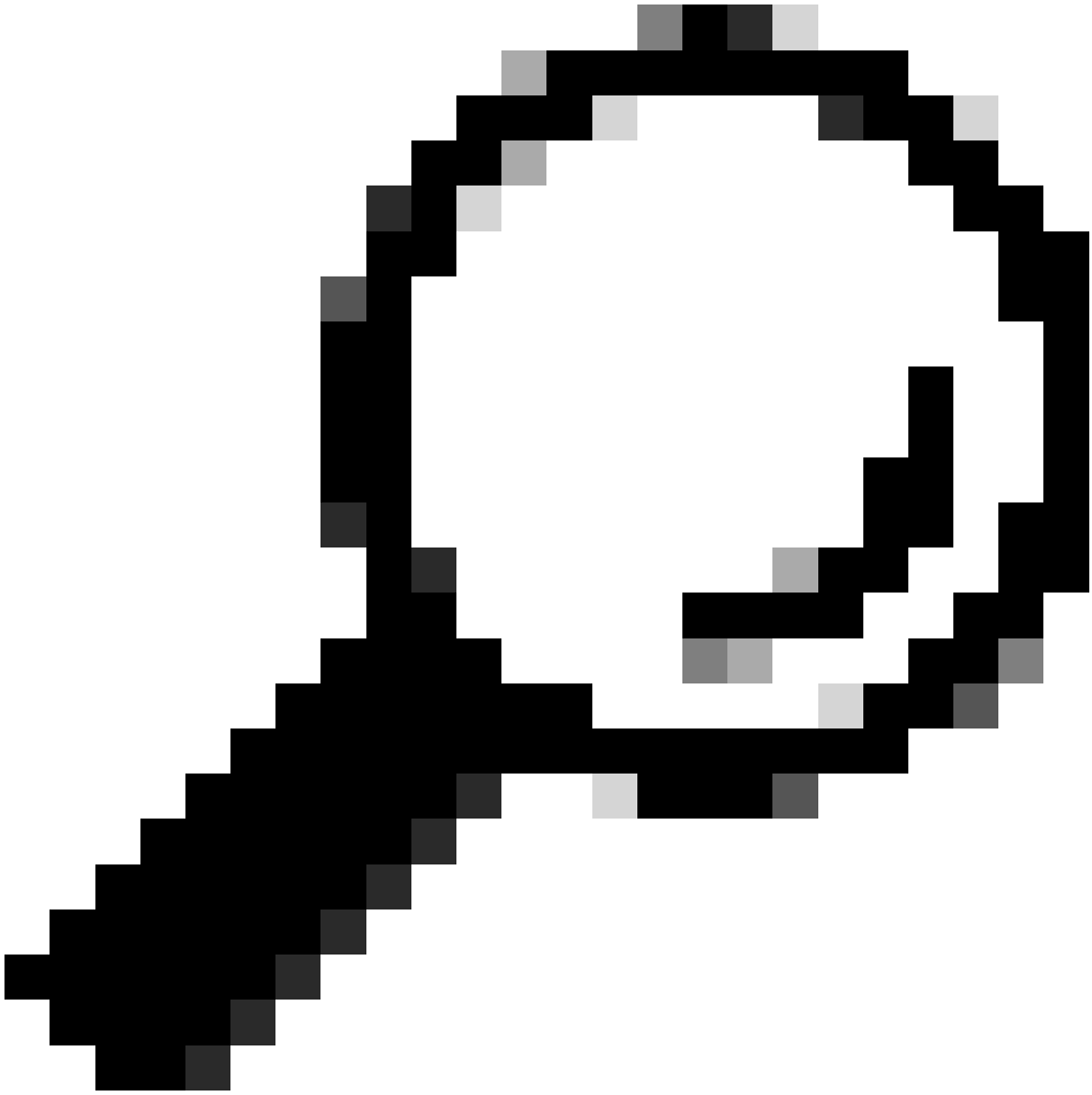
SID: S-1-5-32-573
Name: BUILTIN\Ereignisprotokollleser
Beschreibung: Eine integrierte lokale Gruppe. Mitglieder dieser Gruppe können Ereignisprotokolle vom lokalen Computer lesen.

Fix 3 - Gruppenrichtlinienobjekt

Das OpenDNS Connector-Konto kann mithilfe dieser Gruppenrichtlinieneinstellung die Berechtigung zum Lesen (und Schreiben!) des Sicherheitsereignisprotokolls erhalten. Diese Einstellung bietet technisch mehr Berechtigungen als erforderlich, ist jedoch eine einfache Möglichkeit, die Änderung vorzunehmen.

Computerkonfiguration\Richtlinien\Windows-Einstellungen\Sicherheitseinstellungen\Lokale Richtlinien\Zuweisung von Benutzerrechten\Überwachungs- und Sicherheitsprotokolle verwalten

Führen Sie nach der Änderung bitte 'gpupdate /force' auf dem/den Domänencontroller(n) aus.



Anmerkung: Auf Windows 2003/2003-Funktionsebene ist die Gruppe "Ereignisprotokollleser" möglicherweise nicht vorhanden. Daher ist dieses Gruppenrichtlinienobjekt die primäre Methode, um dem OpenDNS-Connector den Zugriff auf diese Plattformen zu ermöglichen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.