wevtutilを使用してイベントログのアクセス許可を確認する

内容

はじめに

このドキュメントでは、wevtutilを使用してコネクタログオンイベントの権限を確認する方法について説明します。

wbemtestを使用して、コネクタがDCからログオンイベントを読み取ることができるかどうかをテストできます。

wbemtestが実際に接続に失敗する場合、通常はWMI/DCOMアクセス許可エラーが原因であるため、別の場所でヘルプを参照してください。

ただし、一部の環境ではwbemtestが接続してもイベントが表示されない場合があります。

これには2つの原因があります。

- 監査ポリシーが正しくないため、ログオンイベントはDCで追跡されません。監査ポリシーのヘルプを参照してください。
- DCにイベントが記録されていますが、OpenDNS_Connectorにセキュリティイベントログからの読み取りアクセス許可がありません。 続行…

基本 – イベントログリーダー

ほとんどの場合、これは単純で、OpenDNS_ConnectorユーザをEvent Log Readersグループに追加するだけです。これにより、イベントログの読み取りに必要なアクセス許可が付与されます。

wevtutil – アクセス許可を確認します

まれに、イベントログリーダーグループに既定のアクセス許可がない場合があります。wevtutilを使用すると、セキュリティイベントログに付与されている権限を簡単に確認できます。

単に実行：

```
wevtutil gl security
```

1. 出力には、SDDL構文を使用した権限が次のように表示されます。

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

2. イベントログリーダーのSIDはS-1-5-32-573で、短縮してERにすることができます。
3. 16進数値は、次のような権限に対するものです。
    - 0x1 =読み取り
    - 0x2 =書き込み
    - 0x3 =読み取り/書き込み

修正1 – デフォルトにリセット

カスタムSDDL文字列を含むレジストリ値を削除することで、アクセス許可をデフォルトにリセットできます。 これは迅速な修正ですが、イベントログから読み取る他のソフトウェアに影響を与える可能性があります（該当する場合）。

HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Securityから「CustomSD」値を削除します。

修正2 - wevtutilを使用したSDDLの更新

まれに、wevtutilを使用して権限を直接割り当てることができる場合があります。

1. 次のコマンドを使用して、前述のように現在の権限を取得します。

```
wevtutil gl security
```

2. チャネルアクセスストリングをメモします。 例：

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

3. OpenDNS_Connectorユーザの SIDを確認します。

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

4. OpenDNS_Connectorへの読み取りアクセス権を付与するには、次のように既存のチャネルアクセス文字列に追加します。 <SID>をOpenDNS_Connector SIDで置き換えます。

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

参考のために、イベントログリーダーグループのSIDを次に示します。

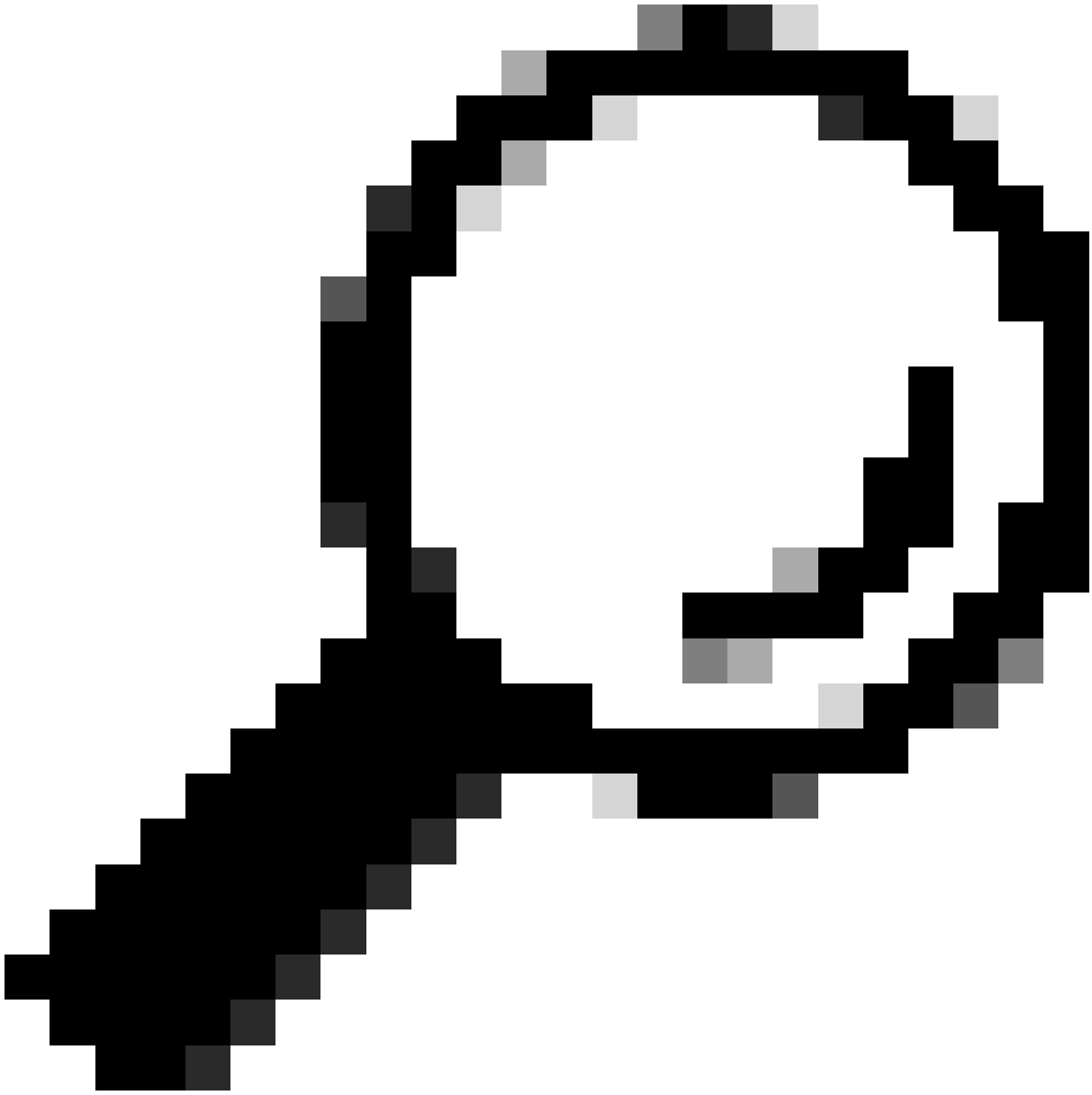
SID: S-1-5-32-573
名前： BUILTIN\Event Log Readers
説明：組み込みローカルグループ。このグループのメンバーは、ローカルコンピューターからイベントログを読み取ることができます。

修正3 - GPO

OpenDNSコネクタアカウントには、このグループポリシー設定を使用して、セキュリティイベントログの読み取り（および書き込み！）権限を付与できます。 この設定は、技術的には必要以上の権限を与えますが、変更を行う簡単な方法です。

コンピューターの構成\ポリシー\Windowsの設定\セキュリティの設定\ローカルポリシー\ユーザー権利の割り当て\監査とセキュリティログの管理

変更後、ドメインコントローラで'gpupdate /force'を実行してください。



注：Windows 2003/2003の機能レベルでは、Event Log Readersグループが存在しない可能性があります。したがって、このGPOは、これらのプラットフォームでOpenDNSコネクタのアクセスを許可する主要な方法です。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。