Use wevtutil to Check Event Log Permissions

Contents

Introduction

Basics - Event Log Readers

wevtutil - Check permissions

Fix 1 - Reset to default

Fix 2 - Update SDDL using wevtutil

Fix 3 - GPO

Introduction

This document describes using wevtutil to check Connector logon event permissions.

You can test whether the Connector can read logon events from a DC using wbemtest.

If wbemtest actually fails to connect this is usually caused by a WMI/DCOM permissions error, so seek help elsewhere.

However, in some circumstances wbemtest connects but shows no events.

There are two causes for this:

- The audit policy is incorrect, so logon events are not being tracked on the DC. Seek help with the audit policy.
- Events are being logged on the DC but OpenDNS_Connector does not have permission to read from the Security event log. Continue on...

Basics - Event Log Readers

In most cases this as simple as adding the OpenDNS_Connector user to the **Event Log Readers** group. This gives it the permissions it needs to read the event log.

wevtutil - Check permissions

In rare cases the Event Log Readers group does not have the default permissions. We can use wevtutil to easily check the permissions granted to the Security Event log.

Simply run:

```
wevtutil gl security
```

1. The output shows you the permissions using SDDL syntax as follows:

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

2. The SID for Event Log readers is **S-1-5-32-573** or can be abbreviated to **ER**.
3. The hexadecimal value is for permissions, such as:
    - 0x1 = Read
    - 0x2 = Write
    - 0x3 = Read/Write\

Fix 1 - Reset to default

Permissions can be reset to default by deleting a registry value which contains the custom SDDL string. This is a quick fix, but may affect other software that reads from the event log (if applicable).

Delete the '*CustomSD'* value from *HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security*

Fix 2 - Update SDDL using wevtutil

In rare circumstances we can directly assign the permissions using wevtutil.

1. Get the current permissions as described previously, using this command:

    ```
    wevtutil gl security
    ```

2. Make a note of the channel access string. Eg:

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

3. Work out the SID for the OpenDNS_Connector user:

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

4. You can give read access to OpenDNS_Connector by appending it to the existing channel access string as follows. Replace <SID> with the 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>)
    ```

For reference, here is the SID of the Event Log Readers group.

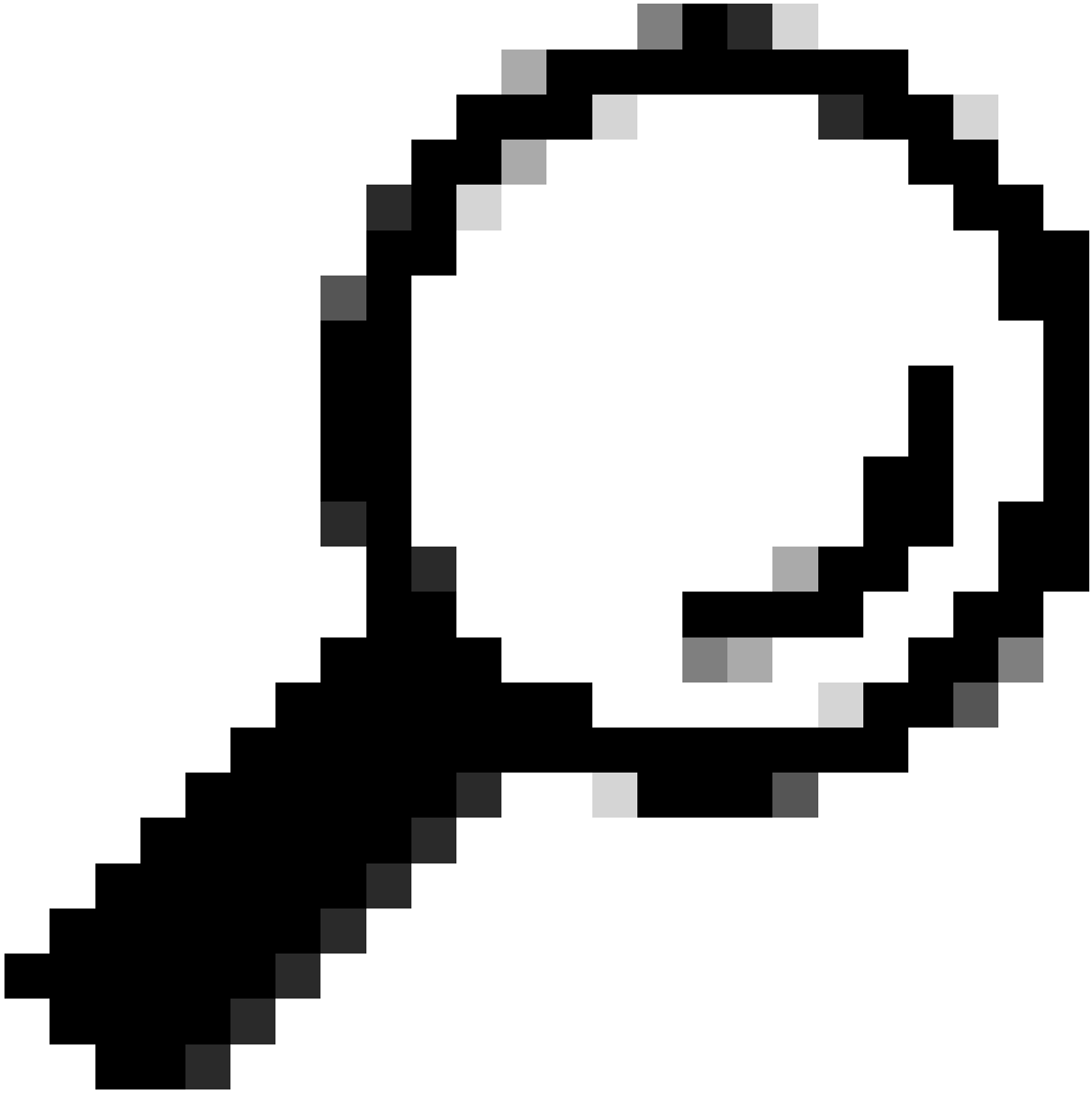
SID: S-1-5-32-573
Name: BUILTIN\Event Log Readers
Description: A Builtin Local group. Members of this group can read event logs from local machine.

Fix 3 - GPO

The OpenDNS Connector account can be given permission to read (and write!) to the security event log using this group policy setting. This setting technically gives more permissions than are needed, but is an easy way to make the change.

Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Manage auditing and security log

After making the change, please runb 'gpupdate /force' on the domain controller(s).



Note: On Windows 2003 / 2003 functional level the Event Log Readers group may not exist, therefore this GPO is the primary method to allow the OpenDNS Connector access ion those platforms.
