Utilizzare wevtutil per controllare le autorizzazioni del registro eventi

Sommario

Introduzione

In questo documento viene descritto l'utilizzo di wevtutil per controllare le autorizzazioni degli eventi di accesso del connettore.

È possibile verificare se il Connettore è in grado di leggere gli eventi di accesso da un controller di dominio utilizzando wbemtest.

Se la connessione a wbemtest non riesce, in genere ciò è causato da un errore di autorizzazioni WMI/DCOM. Per ulteriori informazioni, vedere altrove.

In alcune circostanze, tuttavia, wbemtest si connette ma non visualizza alcun evento.

Le cause sono due:

- I criteri di controllo non sono corretti, pertanto gli eventi di accesso non vengono rilevati nel controller di dominio. Cercare informazioni sui criteri di controllo.
- È in corso la registrazione di eventi nel controller di dominio, ma OpenDNS_Connector non dispone dell'autorizzazione per la lettura dal registro eventi di protezione. Continua...

Nozioni di base - Lettori del registro eventi

Nella maggior parte dei casi si tratta di aggiungere l'utente OpenDNS_Connector al gruppo Event Log Readers. In questo modo dispone delle autorizzazioni necessarie per leggere il registro eventi.

wevtutil - Controlla autorizzazioni

In rari casi il gruppo Lettori registro eventi non dispone delle autorizzazioni predefinite. È possibile utilizzare wevtutil per controllare facilmente le autorizzazioni concesse al registro eventi di protezione.

Esecuzione semplice:

```
wevtutil gl security
```

1. L'output mostra le autorizzazioni che utilizzano la sintassi SDDL come segue:

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

2. Il SID per i lettori di log eventi è S-1-5-32-573 o può essere abbreviato in ER.
3. Il valore esadecimale viene utilizzato per le autorizzazioni, ad esempio:
   - 0x1 = Lettura
   - 0x2 = Scrittura
   - 0x3 = Lettura/Scrittura\

Correzione 1 - Ripristino dei valori predefiniti

È possibile ripristinare le autorizzazioni predefinite eliminando un valore del Registro di sistema contenente la stringa SDDL personalizzata. Si tratta di una correzione rapida, ma può influire su altri software che leggono dal registro eventi (se applicabile).

Eliminare il valore 'CustomSD' da HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security

Correzione 2 - Aggiornare SDDL utilizzando wevtutil

In rari casi è possibile assegnare direttamente le autorizzazioni utilizzando wevtutil.

1. Ottenere le autorizzazioni correnti come descritto in precedenza utilizzando questo comando:

   ```
   wevtutil gl security
   ```

2. Prendere nota della stringa di accesso al canale. Esempio:

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

3. Elaborare il SID per l'utente OpenDNS_Connector:

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

4. È possibile concedere l'accesso in lettura a OpenDNS_Connector aggiungendolo alla stringa di accesso al canale esistente come indicato di seguito. Sostituire <SID> con il SID

OpenDNS_Connector.

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

Per riferimento, di seguito è riportato il SID del gruppo Event Log Readers.

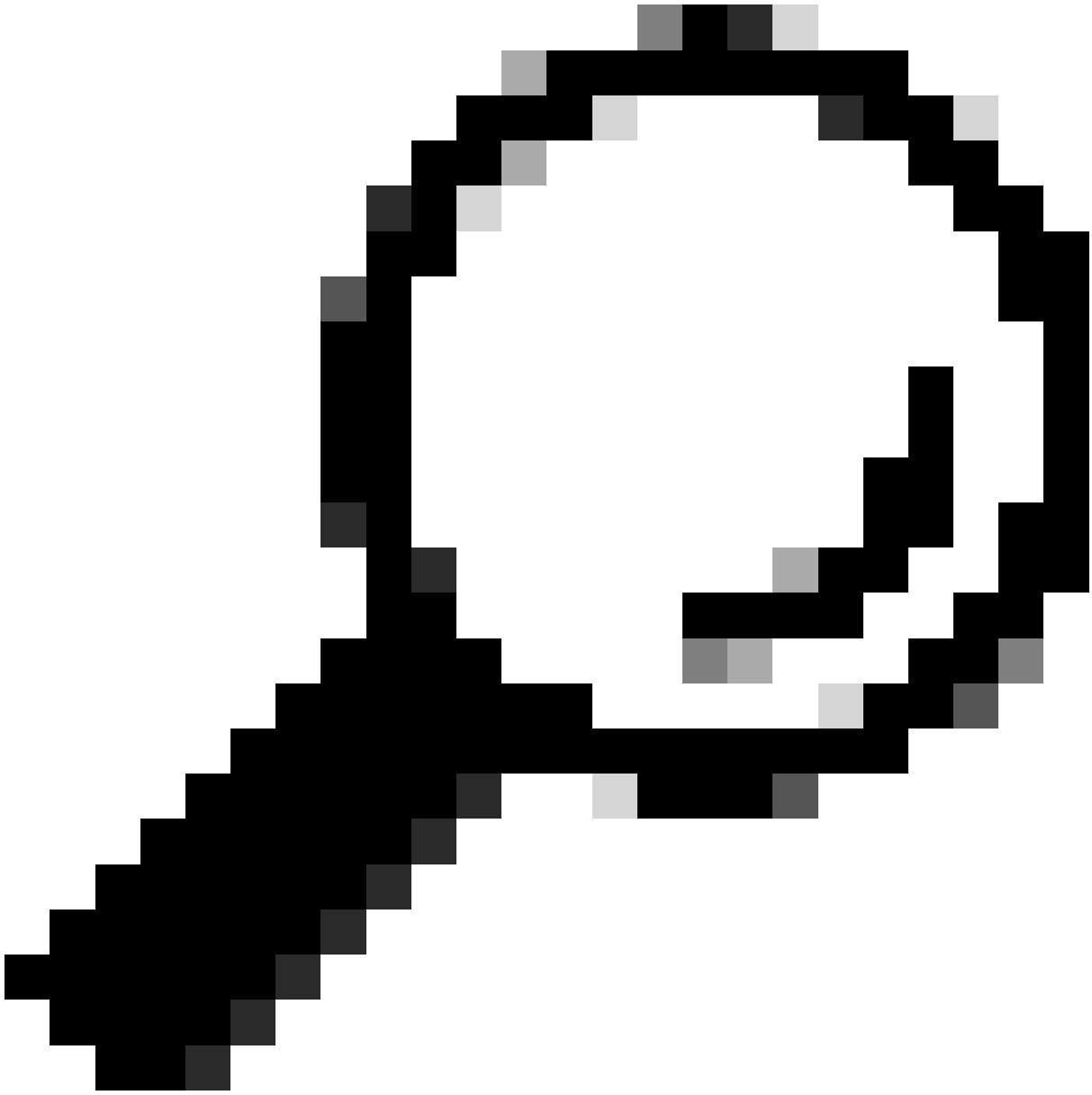
SID: S-1-5-32-573
Nome: BUILTIN\Lettori registro eventi
Descrizione: Gruppo locale incorporato. I membri di questo gruppo possono leggere i registri eventi dal computer locale.

Correzione 3 - Oggetto Criteri di gruppo

Tramite questa impostazione di Criteri di gruppo è possibile concedere all'account OpenDNS Connector l'autorizzazione di lettura e scrittura nel registro eventi di protezione. Tecnicamente, questa impostazione offre più autorizzazioni di quante siano necessarie, ma è un modo semplice per apportare la modifica.

Configurazione computer\Criteri\Impostazioni di Windows\Impostazioni protezione\Criteri locali\Assegnazione diritti utente\Gestisci registro di controllo e di protezione

Dopo aver apportato la modifica, eseguire 'gpupdate /force' nei controller di dominio.



Nota: A livello di funzionalità di Windows 2003 / 2003 il gruppo Event Log Readers potrebbe non esistere, pertanto questo oggetto Criteri di gruppo è il metodo principale per consentire al connettore OpenDNS di accedere a tali piattaforme.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).