Utilizar wevtutil para comprobar los permisos del registro de eventos

Contenido

Introducción

En este documento se describe el uso de wevtutil para comprobar los permisos de eventos de inicio de sesión del conector.

Puede probar si Connector puede leer eventos de inicio de sesión de un DC mediante wbemtest.

Si wbemtest no puede conectarse, normalmente se debe a un error de permisos de WMI/DCOM, por lo que debe buscar ayuda en otro lugar.

Sin embargo, en algunas circunstancias wbemtest se conecta pero no muestra ningún evento.

Hay dos causas para esto:

- La directiva de auditoría es incorrecta, por lo que no se está realizando un seguimiento de los eventos de inicio de sesión en el DC. Busque ayuda con la directiva de auditoría.
- Los eventos se registran en el DC, pero OpenDNS_Connector no tiene permiso para leer el registro de eventos de seguridad. Continuar en...

Conceptos básicos - Lectores de registros de eventos

En la mayoría de los casos esto es tan simple como agregar el usuario OpenDNS_Connector al grupo Event Log Readers. Esto le otorga los permisos que necesita para leer el registro de eventos.

wevtutil - Comprobar permisos

En casos excepcionales, el grupo Lectores del registro de eventos no tiene los permisos predeterminados. Podemos utilizar wevtutil para verificar fácilmente los permisos otorgados al registro de eventos de seguridad.

Simplemente ejecute:

```
wevtutil gl security
```

1. El resultado muestra los permisos que utilizan la sintaxis SDDL de la siguiente manera:

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

2. El SID para los lectores del registro de eventos es S-1-5-32-573 o se puede abreviar como ER.
3. El valor hexadecimal corresponde a los permisos, como:
   - 0x1 = Lectura
   - 0x2 = Escritura
   - 0x3 = Lectura/escritura\

Corregir 1: restablecer el valor predeterminado

Los permisos se pueden restablecer a los valores predeterminados eliminando un valor del Registro que contenga la cadena SDDL personalizada. Esta es una solución rápida, pero puede afectar a otro software que se lee del registro de eventos (si corresponde).

Elimine el valor 'CustomSD' de HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security

Corrección 2: actualización de SDDL mediante wevtutil

En raras circunstancias, podemos asignar directamente los permisos mediante wevtutil.

1. Obtenga los permisos actuales como se describió anteriormente, usando este comando:

   ```
   wevtutil gl security
   ```

2. Anote la cadena de acceso al canal. Por ejemplo:

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

3. Calcule el SID para el usuario de OpenDNS_Connector:

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

4. Puede dar acceso de lectura a OpenDNS_Connector anexándolo a la cadena de acceso al canal existente de la siguiente manera. Reemplace <SID> por el 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>)
```

A modo de referencia, aquí se muestra el SID del grupo Lectores del registro de eventos.

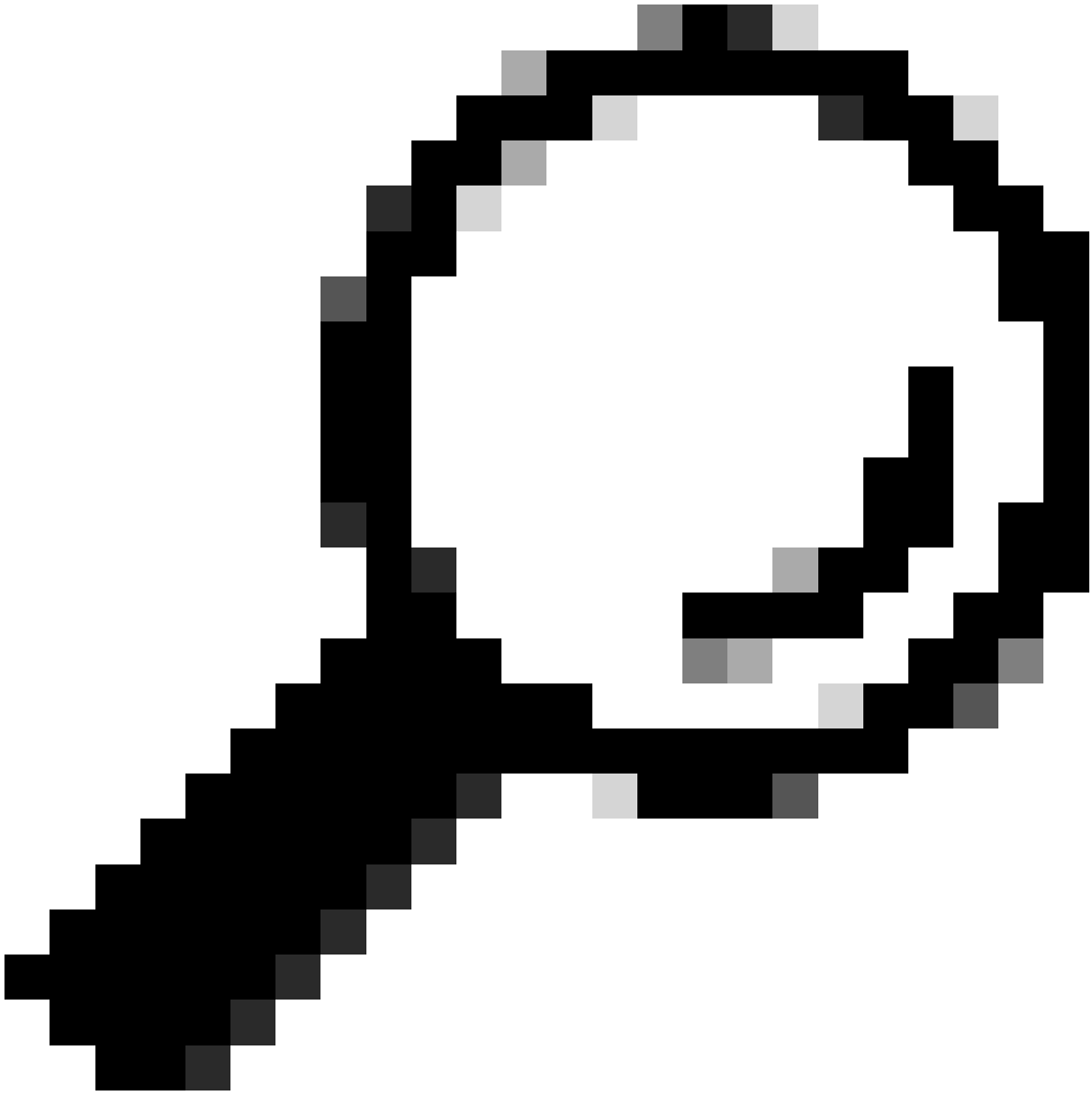
SID: S-1-5-32-573
Nombre: BUILTIN\Lectores de registro de eventos
Descripción: Un grupo local integrado. Los miembros de este grupo pueden leer los registros de eventos del equipo local.

Corrección 3: GPO

La cuenta del conector OpenDNS puede tener permiso para leer (y escribir) en el registro de eventos de seguridad con esta configuración de directiva de grupo. Técnicamente, esta configuración proporciona más permisos de los necesarios, pero es una forma fácil de realizar el cambio.

Configuración del equipo\Directivas\Configuración de Windows\Configuración de seguridad\Directivas locales\Asignación de derechos de usuario\Administrar registro de auditoría y seguridad

Después de realizar el cambio, ejecute 'gpupdate /force' en los controladores de dominio.



Nota: En el nivel funcional de Windows 2003 / 2003, es posible que el grupo Lectores de registro de eventos no exista, por lo tanto, este GPO es el método principal para permitir el acceso del conector OpenDNS en esas plataformas.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).