Usar wevtutil para Verificar Permissões do Log de Eventos

Contents

Introdução

Este documento descreve o uso do wevtutil para verificar as permissões de evento de logon do Connector.

Você pode testar se o Conector pode ler eventos de logon de um DC usando wbemtest.

Se o teste da Web falhar ao se conectar, isso geralmente é causado por um erro de permissões de WMI/DCOM; portanto, procure ajuda em outro lugar.

No entanto, em algumas circunstâncias, o wbemtest se conecta, mas não mostra eventos.

Há duas causas para isso:

- A diretiva de auditoria está incorreta, portanto, os eventos de logon não estão sendo rastreados no controlador de domínio. Procure ajuda com a política de auditoria.
- Os eventos estão sendo registrados no DC, mas o OpenDNS_Connector não tem permissão para ler no log de eventos de Segurança. Continuar em...

Conceitos Básicos - Leitores de Log de Eventos

Na maioria dos casos, isso é tão simples quanto adicionar o usuário do OpenDNS_Connector ao grupo Event Log Readers. Isso dá a ele as permissões necessárias para ler o log de eventos.

wevtutil - Verificar permissões

Em casos raros, o grupo Leitores de Log de Eventos não tem as permissões padrão. Podemos usar o wevtutil para verificar facilmente as permissões concedidas ao registro de Eventos de segurança.

Simplesmente execute:

```
wevtutil gl security
```

1. A saída mostra as permissões usando a sintaxe SDDL da seguinte maneira:

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

2. O SID para leitores de Log de Eventos é S-1-5-32-573 ou pode ser abreviado para ER.
3. O valor hexadecimal é para permissões, como:
    - 0x1 = Lida
    - 0x2 = Gravação
    - 0x3 = Leitura/Gravação\

Fix 1 - Redefinir para o padrão

As permissões podem ser redefinidas para o padrão excluindo um valor do Registro que contenha a cadeia de caracteres SDDL personalizada. Essa é uma correção rápida, mas pode afetar outros softwares que leem no registro de eventos (se aplicável).

Exclua o valor 'CustomSD' de HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security

Correção 2 - Atualizar SDDL usando wevtutil

Em raras circunstâncias, podemos atribuir diretamente as permissões usando wevtutil.

1. Obtenha as permissões atuais conforme descrito anteriormente, usando este comando:

```
wevtutil gl security
```

2. Anote a string de acesso ao canal. Por exemplo:

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

3. Calcule o SID do usuário do OpenDNS_Connector:

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

4. Você pode conceder acesso de leitura ao OpenDNS_Connector anexando-o à cadeia de caracteres de acesso de canal existente da seguinte maneira. Substitua <SID> pelo SID do OpenDNS_Connector.

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

Para referência, este é o SID do grupo de Leitores do Log de Eventos.

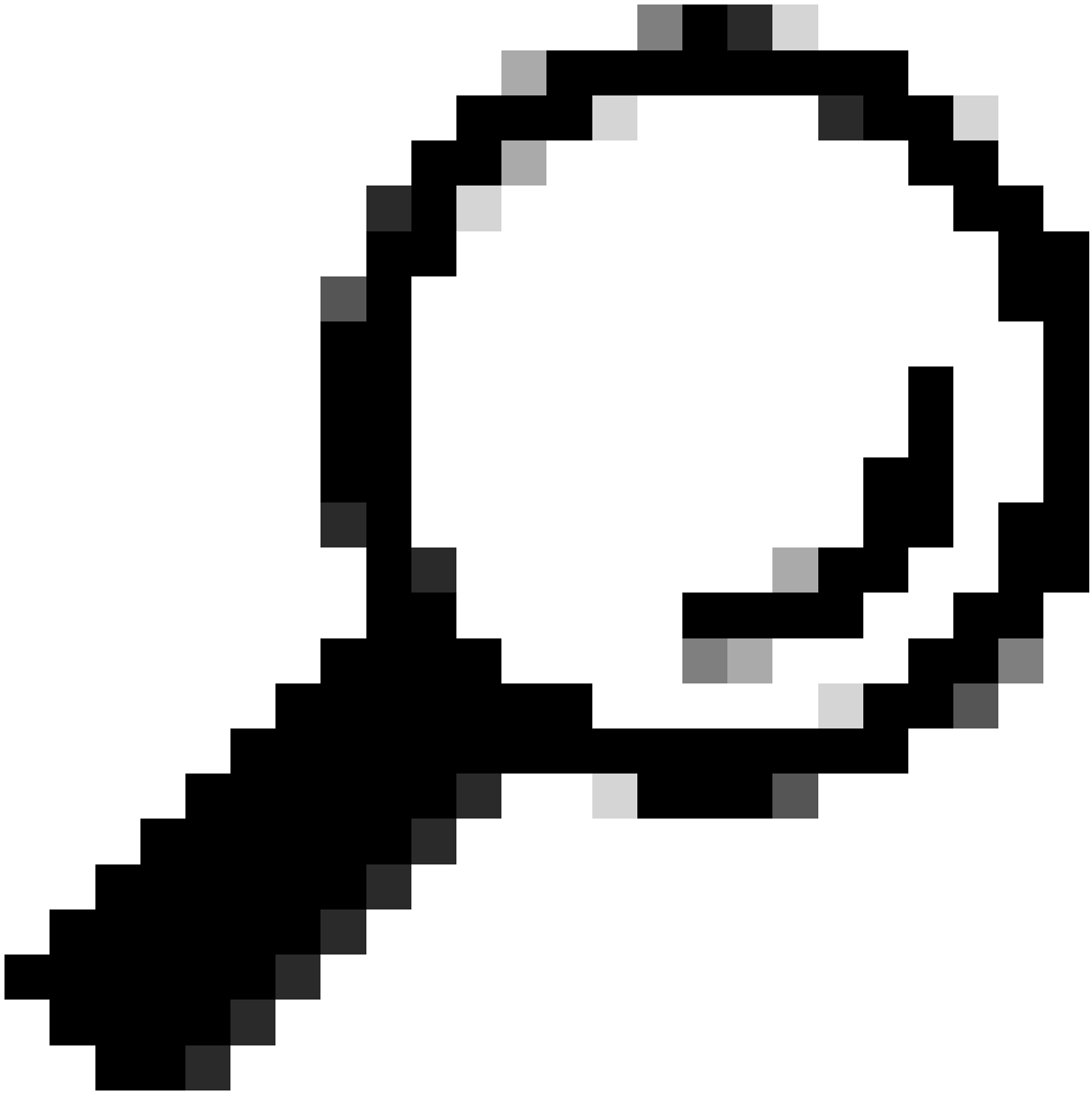
SID: S-1-5-32-573
Nome: BUILTIN\Leitores de Log de Eventos
Descrição: Um grupo Local Interno. Os membros deste grupo podem ler logs de eventos da máquina local.

Correção 3 - GPO

A conta do OpenDNS Connector pode ter permissão de leitura (e gravação!) no log de eventos de segurança usando esta configuração de política de grupo. Essa configuração tecnicamente dá mais permissões do que o necessário, mas é uma maneira fácil de fazer a alteração.

Configuração do Computador\Políticas\Configurações do Windows\Configurações de Segurança\Políticas Locais\Atribuição de Direitos do Usuário\Gerenciar a auditoria e o log de segurança

Após fazer a alteração, execute 'gpupdate /force' no(s) controlador(es) de domínio.



Note: No nível funcional do Windows 2003 / 2003, o grupo de Leitores de Log de Eventos pode não existir, portanto, este GPO é o principal método para permitir o acesso do OpenDNS Connector a essas plataformas.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.