# wevtutil을 사용하여 이벤트 로그 권한 확인

## 목차



## 소개

이 문서에서는 wevtutil을 사용하여 커넥터 로그온 이벤트 권한을 확인하는 방법에 대해 설명합니다
.

커넥터가 wbemtest를 사용하여 DC에서 로그온 이벤트를 읽을 수 있는지 테스트할 수 있습니다.

wbemtest가 실제로 연결하지 못할 경우 일반적으로 WMI/DCOM 권한 오류로 인해 발생하므로 다른 곳에서 도움말을 찾아보십시오.

그러나 경우에 따라 wbemtest가 연결되지만 이벤트가 표시되지 않습니다.

여기에는 두 가지 원인이 있습니다.

- 감사 정책이 잘못되어 DC에서 로그온 이벤트를 추적하지 않습니다. 감사 정책에 대한 도움을 구합니다.
- 이벤트가 DC에 기록되고 있지만 OpenDNS_Connector에는 보안 이벤트 로그를 읽을 수 있는 권한이 없습니다. 계속...

## 기본 - 이벤트 로그 판독기

대부분의 경우 OpenDNS_Connector 사용자를 Event Log Readers 그룹에 추가하는 것처럼 간단합니다. 이렇게 하면 이벤트 로그를 읽는 데 필요한 권한이 부여됩니다.

## wevtutil - 권한 확인

드문 경우이지만 Event Log Readers 그룹에 기본 권한이 없습니다. WebUtil을 사용하여 보안 이벤트 로그에 부여된 권한을 쉽게 확인할 수 있습니다.

간단히 실행:

```
wevtutil gl security
```

1. 출력은 다음과 같이 SDDL 구문을 사용하여 권한을 표시합니다.

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

2. 이벤트 로그 판독기의 SID는 S-1-5-32-573이거나 ER로 축약할 수 있습니다.
3. 16진수 값은 다음과 같은 권한에 사용됩니다.
    - 0x1 = 읽기
    - 0x2 = 쓰기
    - 0x3 = 읽기/쓰기\

# 수정 1 - 기본값으로 재설정

사용자 지정 SDDL 문자열을 포함하는 레지스트리 값을 삭제하여 권한을 기본값으로 재설정할 수 있습니다. 이는 빠른 해결책이지만 이벤트 로그에서 읽는 다른 소프트웨어에 영향을 미칠 수 있습니다(해당되는 경우).

HKLM\SYSTEM\CurrentControlSet\Services\Eventlog\Security에서 'CustomSD' 값을 삭제합니다.

# 수정 2 - wevtutil을 사용하여 SDDL 업데이트

드문 경우이지만 wevtutil을 사용하여 권한을 직접 할당할 수 있습니다.

1. 다음 명령을 사용하여 이전에 설명한 대로 현재 권한을 가져옵니다.

```
wevtutil gl security
```

2. 채널 액세스 문자열을 기록합니다. 예:

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

3. OpenDNS_Connector 사용자의 SID를 처리합니다.

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

4. 다음과 같이 기존 채널 액세스 문자열에 추가하여 OpenDNS_Connector에 대한 읽기 액세스 권한을 부여할 수 있습니다. <SID>를 OpenDNS_Connector SID로 바꿉니다.

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

참고로 Event Log Readers 그룹의 SID는 다음과 같습니다.

SID: S-1-5-32-573

이름: 기본 제공\이벤트 로그 판독기
설명: 기본 제공 로컬 그룹. 이 그룹의 구성원은 로컬 컴퓨터에서 이벤트 로그를 읽을 수 있습니다.

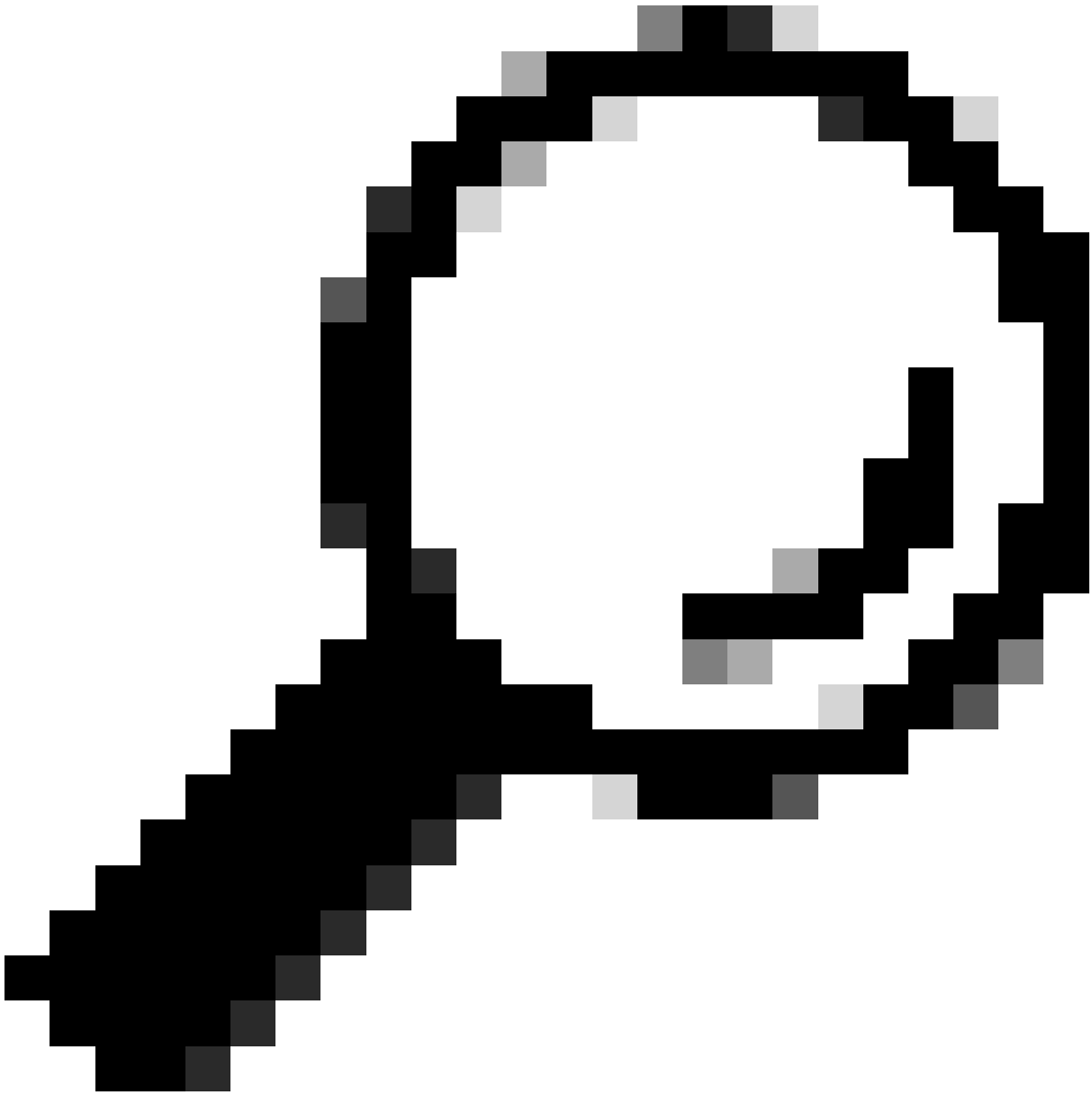
## 수정 3 - GPO

이 그룹 정책 설정을 사용하여 보안 이벤트 로그를 읽고 쓸 수 있는 권한을 OpenDNS 커넥터 계정에 부여할 수 있습니다.  이 설정은 기술적으로 필요한 것보다 많은 권한을 부여하지만 쉽게 변경할 수 있는 방법입니다.

컴퓨터 구성\정책\Windows 설정\보안 설정\로컬 정책\사용자 권한 할당\감사 및 보안 로그 관리

변경한 후 도메인 컨트롤러에서 'gpupdate /force'를 실행하십시오.

---



참고: Windows 2003/2003 기능 수준에서 Event Log Readers 그룹이 없을 수 있으므로 이

---

GPO는 OpenDNS 커넥터가 해당 플랫폼에 액세스할 수 있도록 하는 기본 방법입니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.