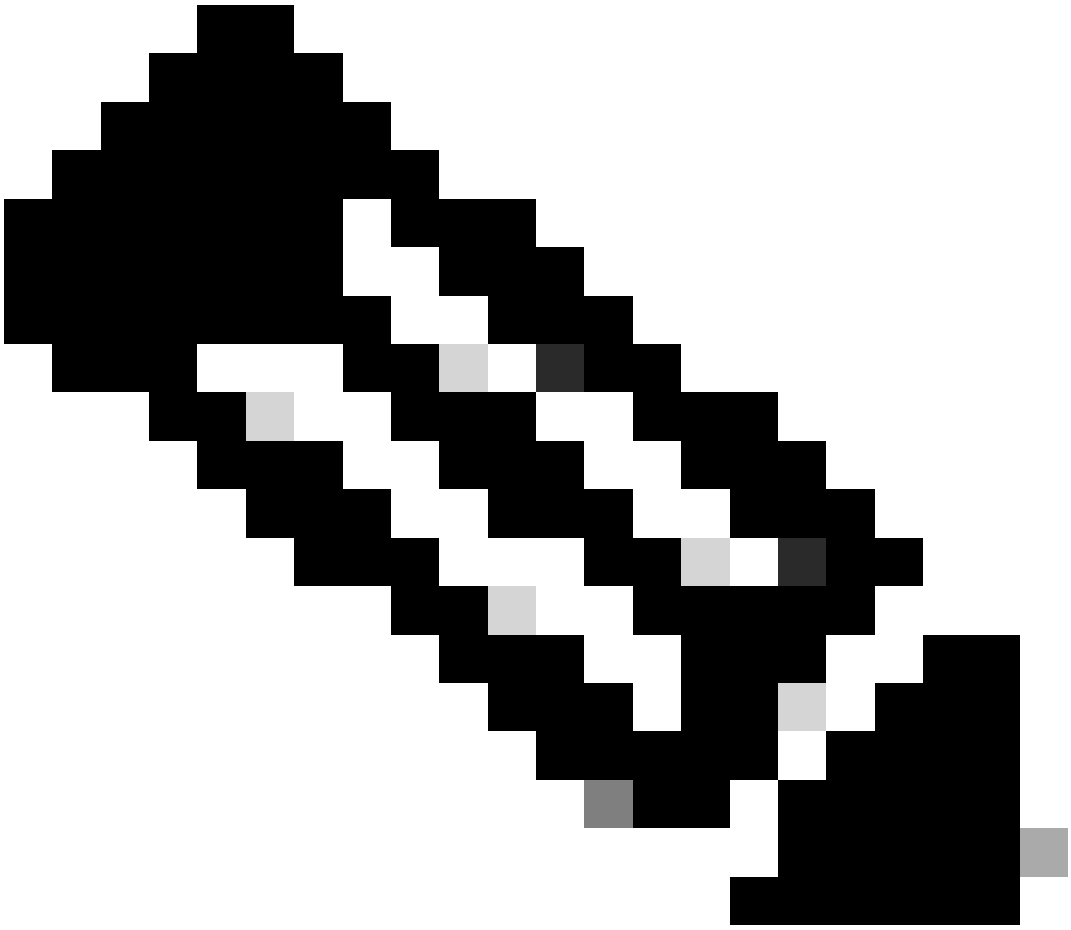
OpenDNS_Connector 사용자의 필수 권한 이해

목차

소개

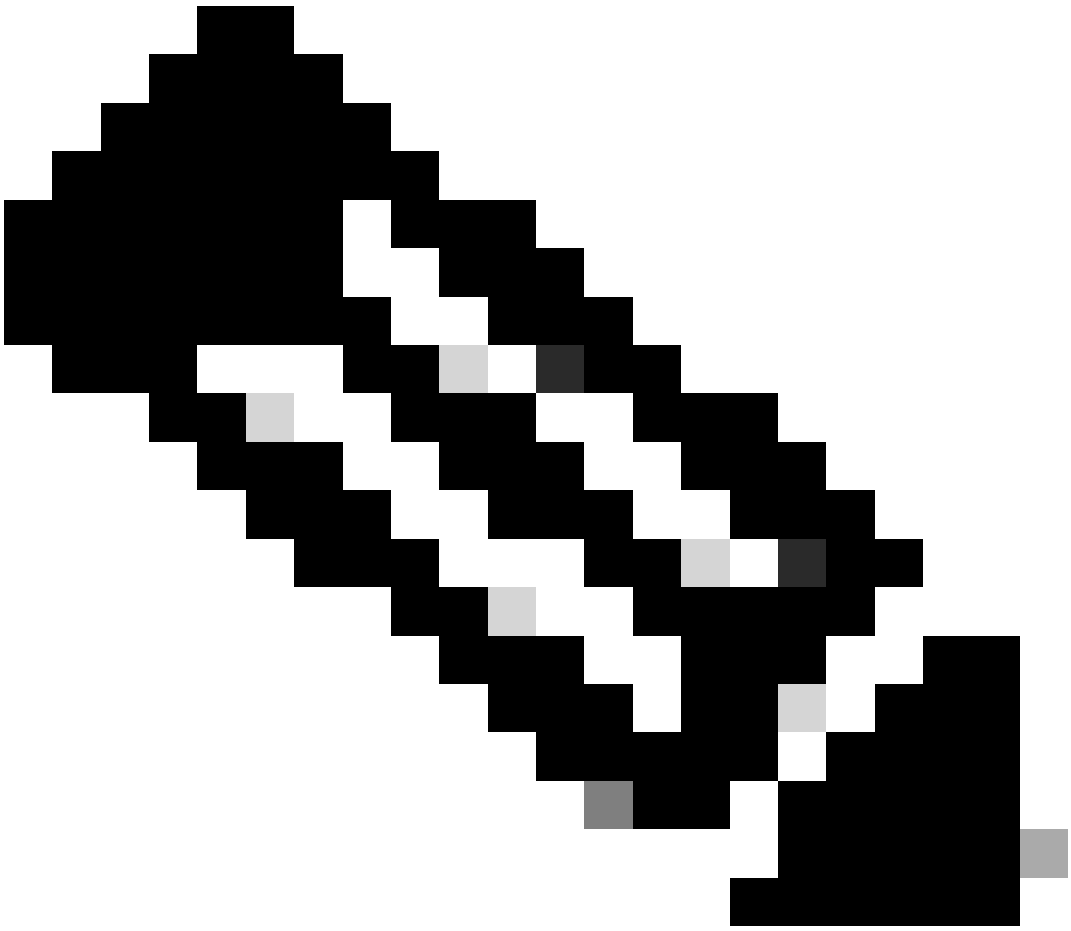
이 문서에서는 OpenDNS_Connector 사용자의 필수 권한에 대해 설명합니다.



참고: 브랜드 재지정 노력에 따라, 가정한 AD 사용자 이름 "OpenDNS_Connector"가 최근 "Cisco_Connector"로 대신 업데이트되었습니다.

개요

Windows Connector 스크립트는 일반적으로 Cisco_Connector 사용자에게 필요한 권한을 설정합니다. 그러나 엄격한 AD 환경에서는 일부 관리자가 도메인 컨트롤러에서 VB 스크립트를 실행할 수 없으므로 Windows 구성 스크립트의 작업을 수동으로 복제해야 합니다. 이 문서에서는 DC에 어떤 권한을 설정해야 하는지 자세히 설명합니다.



참고: 이 문서의 목적상 Cisco_Connector는 AD에서 Connector 계정의 sAMAccountName으로 간주됩니다. 사용자 지정 이름을 대신 사용하는 경우 Cisco_Connector 대신 커넥터 계정의 sAMAccountName에 동일한 지침을 사용하십시오.

Cisco_Connector 사용자에게 작동 권한이 충분하지 않은 경우, AD Connector는 대시보드에 경고 또는 오류 상태를 표시하며, 경고 위에 마우스를 올려놓으면 나열된 메시지는 등록

된 도메인 컨트롤러 중 하나에 대한 액세스 거부입니다.

Cisco_Connector 사용자가 AD 그룹의 멤버인지 확인합니다.

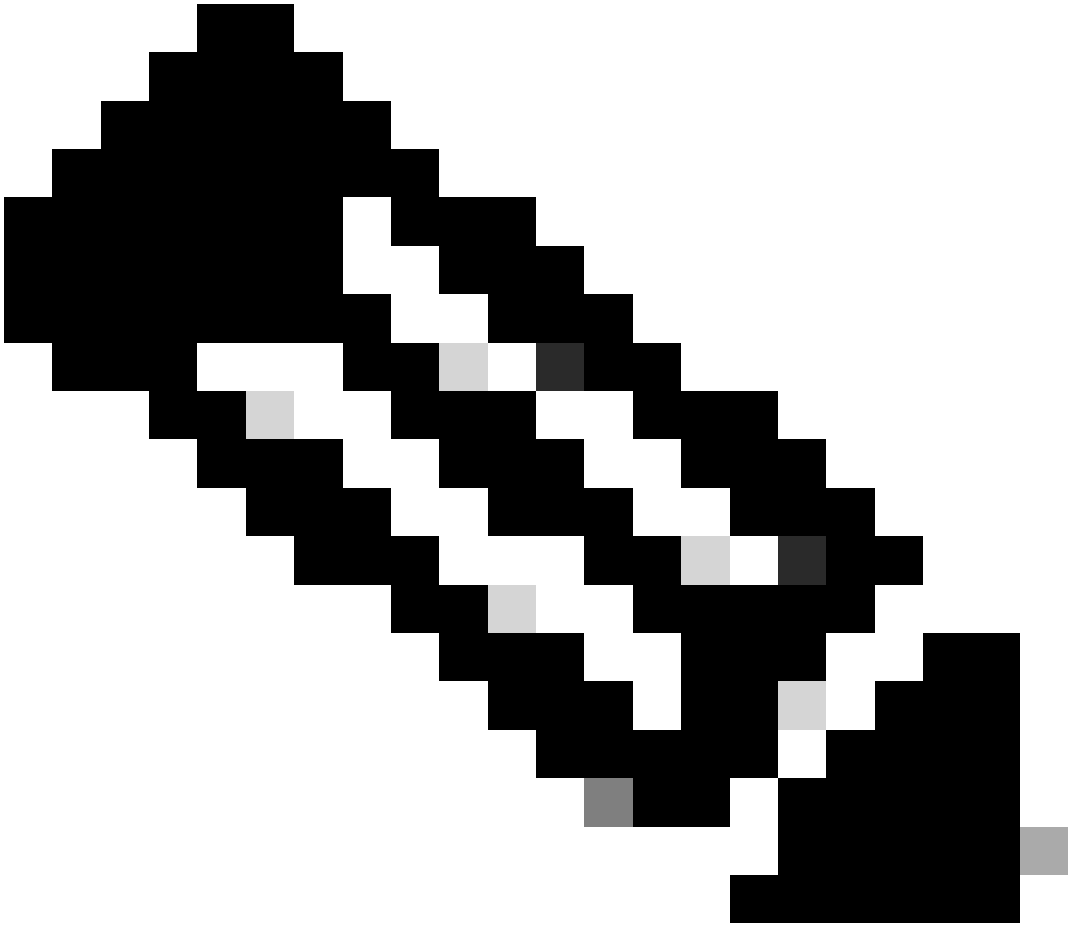
- 엔터프라이즈 읽기 전용 도메인 컨트롤러
- 이벤트 로그 판독기(구축에 가상 어플라이언스가 포함된 경우에만)

또한 Cisco_Connector 사용자는 "도메인 사용자" 및 "사용자" 그룹에 속해야 합니다. 다음 명령을 사용하여 Cisco_Connector 사용자의 그룹 멤버십을 확인할 수 있습니다.

dsquery user -samid Cisco_Connector | dsget user -memberof -expand

Umbrella AD Connector는 이러한 권한이 필요한 두 가지 기본 작업을 수행합니다. 먼저 AD 그룹을 기반으로 정책을 생성하고 Umbrella 대시보드에서 AD 사용자 이름 및 그룹 이름을 표시할 수 있도록 Active Directory에서 LDAP 정보를 가져옵니다. Replicate `Directory Changes` 권한은 이를 허용합니다.

둘째, 도메인 컨트롤러에서 로그인 이벤트를 수집하여 가상 어플라이언스에 전달합니다. 이를 통해 가상 어플라이언스는 IP-사용자 매핑을 생성하여 사용자를 식별할 수 있습니다. 모든 권한은 디렉터리 변경 복제 권한을 제외하고 여기에 적용됩니다. 이러한 권한은 배포에 도메인 컨트롤러와 동일한 Umbrella 사이트에 가상 어플라이언스가 포함된 경우에만 필요합니다.



참고: Cisco_Connector 사용자에 필요한 권한을 설정하는 것 외에도 Domain Controller Configuration 스크립트는 Umbrella에 API 호출을 실행하여 도메인 컨트롤러를 등록합니다. 컨피그레이션 스크립트를 사용하는 대신 수동으로 권한을 수정할 경우 이 등록도 수동으로 수행해야 합니다. Umbrella 대시보드에서 도메인 컨트롤러를 수동으로 추가하는 방법은 Umbrella 설명서를 참조하십시오.

필요한 권한

- 디렉토리 변경 복제
- 이벤트 로그 판독기
- 원격 관리자
- 감사 정책

디렉토리 변경 복제

이 권한을 통해 Cisco_Connector 사용자는 LDAP에 쿼리할 수 있습니다. 이는 일반적으로

"Enterprise Read-Only Domain Controllers" 그룹에 제공되는 필수 권한입니다. 이렇게 하면 Umbrella 대시보드에는 AD 객체의 이름을 표시하고 그룹 멤버십을 확인하는 데 필요한 정보가 제공됩니다. 커넥터는 다음 특성을 요청합니다.

`cn` - 일반 이름입니다.

`dn` - 고유 이름입니다.

`dNSHostName` - DNS에 등록된 디바이스 이름입니다.

`mail` - 사용자와 연결된 이메일 주소입니다.

`memberOf` - 사용자를 포함하는 그룹입니다.

`objectGUID` - 개체의 그룹 ID입니다. 이 속성은 Secure Access에 해시로 전송됩니다.

`primaryGroupId` - 사용자 및 그룹에 사용할 수 있는 기본 그룹 ID입니다.

`primaryGroupToken` - 그룹에 대해서만 사용할 수 있는 기본 그룹 토큰입니다. 비밀번호 또는 비밀번호 해시가 검색되지 않습니다. Secure Access는

액세스 정책 및 컨피그레이션 및 보고의 primaryGroupToken 데이터 이 데이터는 각 사용자 또는 컴퓨터별 필터링에도 필요합니다.

`sAMAccountName`—Cisco AD Connector에 로그인하는 데 사용하는 사용자 이름입니다.

`userPrincipalName` - 사용자의 사용자 이름입니다.

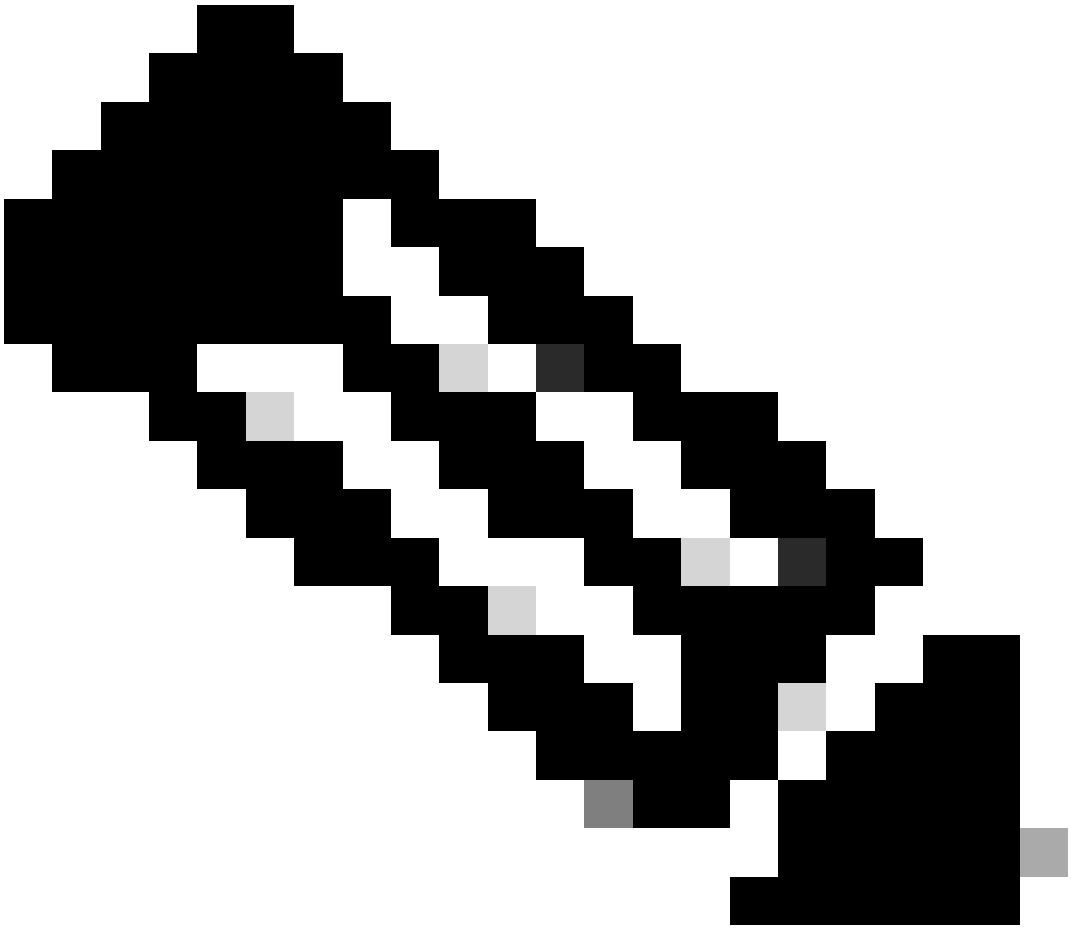
다음 objectClasses에서

```
(&(objectCategory=person)(objectClass=user))
(objectClass=organizationalunit)
(objectClass=computer)
(objectClass=group)
```

기본 제공 "Enterprise Read-only Domain Controllers" 그룹이 이 권한을 제공해야 하므로 Cisco_Connector 사용자가 이 그룹의 구성원이어야 합니다. 그룹의 권한을 확인하거나 Cisco_Connector 사용자에 대해 특별히 권한을 지정할 수 있습니다(그룹이 이러한 권한을 제공하지 않는 경우).

- Active Directory 사용자 및 컴퓨터 스냅인 열기
- 보기 메뉴에서 고급 기능을 클릭합니다.
- "company.com"과 같은 도메인 개체를 마우스 오른쪽 단추로 클릭한 다음 속성을 클릭합니다.
- Security(보안) 탭에서 "Enterprise Read-only Domain Controllers(엔터프라이즈 읽기 전용 도메인 컨트롤러)" 또는 "Cisco_Connector" 사용자를 선택합니다.
    - 필요한 경우 "추가"를 클릭하여 "Cisco_Connector" 사용자를 추가할 수 있습니다.
    - 사용자, 컴퓨터 또는 그룹 선택 대화 상자에서 원하는 사용자 계정을 선택한 다음 추가를 클릭합니다.

    - OK를 클릭하여 Properties 대화 상자로 돌아갑니다.
- 목록에서 Replicating Directory Changes and Read 확인란을 클릭하여 선택합니다.
- Apply(적용)를 클릭한 다음 OK(확인)를 클릭합니다.
- 스냅인을 닫습니다.



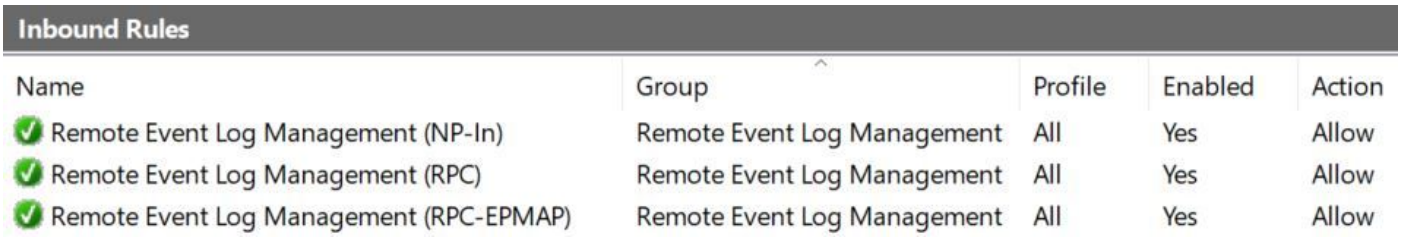
참고: 상위/하위 도메인 시나리오에서 "엔터프라이즈 읽기 전용 도메인 컨트롤러"는 상위 도메인에만 존재합니다. 이 경우 표시된 대로 Cisco_Connector에 대한 권한을 수동으로 추가해야 합니다.

이벤트 로그 판독기

이 변경은 구축에 도메인 컨트롤러와 동일한 Umbrella 사이트에 가상 어플라이언스가 포함된 경우에만 필요합니다. 이 그룹의 멤버십을 사용하면 Cisco_Connector 사용자가 이벤트 로그에서 로그온 이벤트를 읽을 수 있습니다.

도메인 컨트롤러 시스템의 Windows 고급 방화벽 설정에서 원격 이벤트 로그 관리(NP-In, RPC 및 RPC-EPMAP)에 대한 인바운드 규칙이 허용되는지 확인합니다. Umbrella AD Connector는 "RPC

서버를 사용할 수 없습니다"라는 오류를 로깅할 수 있으며, 이러한 규칙이 허용되지 않는 경우 로그인 이벤트를 읽지 못할 수 있습니다.



Inbound Rules

Name	Group	Profile	Enabled	Action
Remote Event Log Management (NP-In)	Remote Event Log Management	All	Yes	Allow
Remote Event Log Management (RPC)	Remote Event Log Management	All	Yes	Allow
Remote Event Log Management (RPC-EPMAP)	Remote Event Log Management	All	Yes	Allow

360090909832

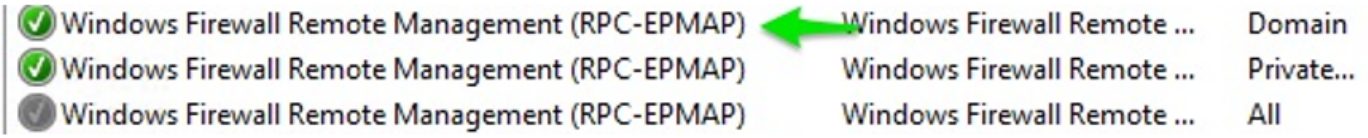
또한 다음 명령을 통해 이러한 규칙을 활성화할 수 있습니다. netsh advfirewall set rule group="Remote Event Log Management" new enable=yes

원격 관리자

커넥터가 도메인 컨트롤러에서 로그인 이벤트를 읽을 수 있도록 하려면 원격 관리가 필요합니다. 이 권한은 구축에 도메인 컨트롤러와 동일한 Umbrella 사이트에 가상 어플라이언스가 포함된 경우에만 필요합니다.

명령 프롬프트에서 다음 명령을 실행하십시오.

```
netsh advfirewall firewall set rule group="remote administration" new enable=yes
netsh advfirewall set currentprofile settings remotemanagement enable
```



Windows Firewall Remote Management (RPC-EPMAP)	Windows Firewall Remote ...	Domain
Windows Firewall Remote Management (RPC-EPMAP)	Windows Firewall Remote ...	Private...
Windows Firewall Remote Management (RPC-EPMAP)	Windows Firewall Remote ...	All

4413613529492

감사 정책

이 변경은 구축에 도메인 컨트롤러와 동일한 Umbrella 사이트에 가상 어플라이언스가 포함된 경우에만 필요합니다. 감사 정책은 도메인 컨트롤러의 이벤트 로그에 기록되는 이벤트를 정의합니다. Connector에서는 사용자가 IP 주소에 매핑될 수 있도록 성공한 로그온 이벤트를 기록해야 합니다.

일반적인 Windows Server 2008+ 환경에서는 레거시 "로그온 이벤트 감사" 설정을 구성해야 합니다. 특히 "로그온 이벤트 감사" 정책을 "성공"으로 설정해야 합니다. 명령 프롬프트에서 다음 명령을 실행하여 이를 확인할 수 있습니다.

```
GPRESULT /z
```

이 정책은 그룹 정책 개체로 정의됩니다. 이를 수정하려면 DC에 대한 적절한 그룹 정책(일반적으로 "기본 도메인 컨트롤러 정책")을 편집하고 "성공" 이벤트를 포함하도록 이 정책을 설정합니다.

```
Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy\Audit lo
```

이 변경을 수행한 후 DC에서 그룹 정책을 업데이트해야 합니다.

그러나 Windows Server 2008에는 고급 감사 정책 구성도 도입되었습니다. 레거시 Windows 감사 정책은 계속 사용할 수 있지만 고급 감사 정책이 정의된 경우 무시됩니다. 두 감사 정책이 상호 작용하는 방식을 알아보려면 Microsoft 설명서를 참조하십시오.

커넥터의 목적상, 고급 감사 정책(로그온과 특별히 관련이 없는 정책 포함)이 정의되어 있으면 고급 감사 정책을 사용해야 합니다.

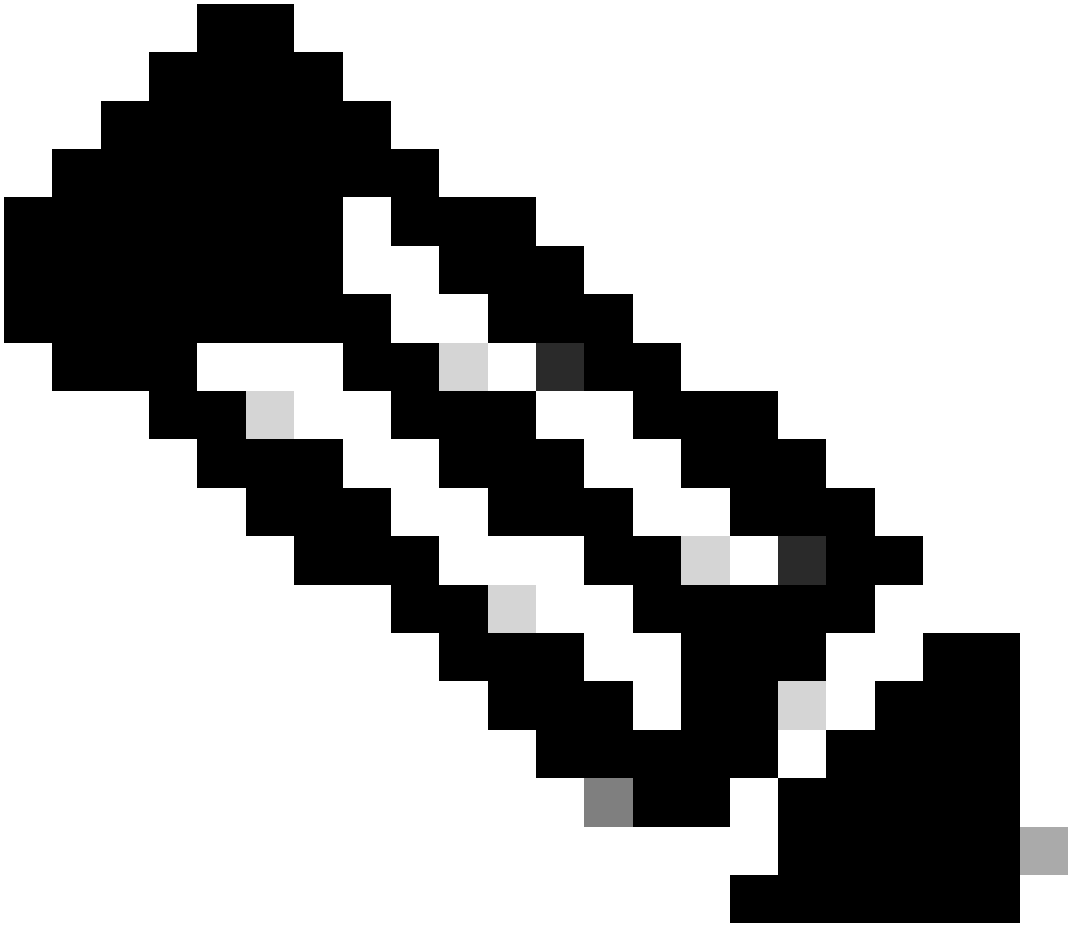
그룹 정책을 사용하는 모든 DC에 대해 고급 감사 정책을 설정해야 합니다. DC에 적합한 그룹 정책(일반적으로 "기본 도메인 컨트롤러 정책")을 편집하고 다음 섹션으로 이동합니다.

```
Computer Configuration\Policies\Windows Settings\Security Settings\Advanced Audit Policy Configuration\
```

이 섹션에서 "Success(성공)" 및 "Failure(실패)" 이벤트를 모두 포함하도록 다음 정책을 설정합니다
.

```
Audit Logon
Audit Logoff
Audit Other Logon/Logoff Events
```

이 변경을 수행한 후 DC에서 그룹 정책을 업데이트해야 합니다.



참고: AD Connector를 가상 어플라이언스와 함께 구축하는 경우 방화벽 규칙이 변경되고 Connector가 통신하는 도메인의 모든 도메인 컨트롤러에서 감사 정책 설정이 수행되어야 합니다.

앞서 언급한 설정을 확인/변경한 후에도 대시보드에 "액세스 거부" 메시지가 표시되면 이 문서에 설명된 대로 Umbrella Support에 커넥터 로그를 보내십시오. AD 커넥터 로그 지원

이 정보를 Support(지원팀)에 제공할 때 다음 두 명령의 출력을 포함합니다.

```
auditpol.exe /get /category:* > DCNAME_auditpol.txt
GPRESULT /H DC_NAME.htm
```

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.