

Active Directory 가입 중 Cisco ISE 트러블슈팅 (&N) > 도메인 컨트롤러 검색 프로세스(&N)

목차

문제

Cisco ISE(Identity Services Engine)가 DC(Domain Controller)를 검색할 수 없으며 ISE AD(Active Directory) 가입이 실패합니다.

환경

- Cisco ISE(Identity Services Engine) - 3.x 이상
- Microsoft AD(Active Directory) - 2016 이상
- DNS(Domain Name System) - UDP/TCP 53
- LDAP(Lightweight Directory Access Protocol) - TCP 389; TCP 636(보안 LDAP(LDAPS)가 사용되는 경우)
- CLDAP(Connectionless Lightweight Directory Access Protocol) - UDP 389

해결

Cisco ISE는 AD 조인 프로세스 중에 DC를 검색하고 여러 기준을 사용하여 선택할 DC를 결정합니다.

DNS 검색:

- ISE는 DNS 서비스(SRV) 레코드 쿼리를 사용하여 사용 가능한 DC, GC(글로벌 카탈로그) 및 KDC(키 배포 센터)를 검색합니다. DNS 서버가 사용 가능한 DC, GC 및 KDC 목록을 반환합니다
- ISE가 이 정보를 수신하지 못하면 AD 조인 프로세스를 계속할 수 없으며 DNS 관련 오류를 보고합니다.
- ISE CLI에서 다음을 사용하여 AD SRV 레코드를 확인합니다.

`nslookup`

- 예:

`nslookup ldap.tcp.example.com querytype SRV`

`nslookup kerberos.tcp.example.com querytype SRV`

`nslookup ldap.tcp.dc._msdcs.example.com querytype SRV`

- 쿼리는 유효한 DC 호스트 이름을 반환해야 합니다. 그런 다음 반환된 DC 호스트 이름이 올바른 IP 주소로 확인되는지 확인합니다.

`nslookup dc01.example.com`

- ISE 실행 컨피그레이션에 구성된 DNS 서버가 사용 가능한 서버 목록을 반환합니다.
- 이 명령을 실행하여 ISE DNS 서버 구성을 확인합니다

`show running-config`

```
amysorea-36-san/admin#show running-config
interface GigabitEthernet 0
 ip address [REDACTED] 255.255.255.0
 ipv6 enable
 ipv6 address autoconfig
 !
 ntp server [REDACTED]
 repository local
 url disk: /
 !
 hostname amysorea-36-san
 icmp echo on
 ip domain-name amysorea.iselab.local
 ip default-gateway [REDACTED]
 ip name-server [REDACTED] ←
 ipv6 enable
 logging loglevel 6
```

- CLDAP의 경우 AD 조인을 수행하거나 관련 AD 진단을 실행하는 동안 ISE에서 패킷 캡처를 사용합니다.
- 예를 들어, ISE와 DC 간의 트래픽을 캡처하고 다음을 확인합니다.

```
ISE → DC01 : UDP/389 CLDAP Request
DC01 → ISE : UDP/389 CLDAP Response
```

- 응답은 연결 가능한 각 DC에서 수신되어야 합니다. ISE가 CLDAP 요청을 전송하지만 응답을 받지 못한 경우 ISE와 DC 간의 방화벽/ACL 규칙, 라우팅 및 UDP 389 연결을 확인합니다.

사이트 ID

- ISE는 CLDAP 정보를 사용하여 가능하면 동일한 Active Directory 사이트에 있는 DC를 식별하고 선호합니다.
- ISE 서브넷이 올바른 AD 사이트에 속하는지 확인합니다. 또한 예상 DC가 동일한 AD 사이트에 속하는지 확인합니다.

연결 모니터링

- ISE는 정기적으로 CLDAP를 사용하여 DC 가용성을 모니터링합니다.
- 패킷 캡처를 사용하여 ISE와 DC 간의 간헐적인 UDP 389 연결, 패킷 손실 또는 지연된 CLDAP 응답을 확인합니다.
- 2.5초 이상 걸리는 CLDAP 응답은 경고를 생성합니다. DC가 응답하지 않으면 AD 조인이 실패합니다.

원인

- ISE에서 DC를 검색할 수 없습니다.
- DNS는 필수 AD 레코드를 반환하지 않습니다.
- ISE에서 검색된 DC에 연결할 수 없습니다.
- DC는 CLDAP 요청에 응답하지 않습니다.
- ISE 서브넷이 잘못된 AD 사이트에 매핑됩니다.
- 선택한 DC가 LDAP 연결을 허용하지 않습니다.

관련 콘텐츠

- [ISE\(Identity Service Engine\) 및 Active Directory 통합 설명서](#)
- [Cisco 기술 지원 및 다운로드](#)

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.