ISE 1.3 AD 인증 실패, "토큰 그룹 가져오기 권한 부족" 오류

목차

소개

이 문서에서는 ISE 시스템 계정 권한 부족으로 인해 발생한 오류 코드 "24371"로 인해 AD(Active Directory)에 대한 ISE(Identity Services Engine) 인증 실패 솔루션에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대한 기본적인 지식을 얻을 것을 권장합니다.

- ISE 구성 및 문제 해결
- Microsoft AD

사용된 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- ISE 버전 1.3.0.876
- Microsoft AD 버전 2008 R2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

"24371" 오류로 인해 AD 인증이 실패함

ISE 1.3 이상에서는 "24371" 오류로 인해 AD에 대해 인증이 실패할 수 있습니다. 오류에 대한 자세한 인증 보고서에는 다음과 유사한 단계가 있습니다.

```
24432     Looking up user in Active Directory - CISCO_LAB
24371     The ISE machine account does not have the required privileges to fetch groups. -
ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS
24371     The ISE machine account does not have the required privileges to fetch groups. -
CISCO_LAB 15048     Queried PIP - CISCO_LAB.ExternalGroups
```

AD 상태는 조인되고 연결되었으며 필요한 AD 그룹이 ISE 컨피그레이션에 올바르게 추가되었습니다.

솔루션

AD에서 ISE 머신 계정에 대한 권한 수정

세부 인증 보고서의 오류는 Active Directory에 있는 ISE의 시스템 계정에 토큰 그룹을 가져올 수 있는 충분한 권한이 없음을 의미합니다.

> **참고:**ISE 시스템 계정에 올바른 권한을 부여할 수 없으므로 AD 측에서 수정됩니다.AD에 대한 ISE의 연결을 끊거나 다시 연결해야 할 수 있습니다.

다음 예와 같이 시스템 계정의 현재 권한을 dsacls 명령으로 확인할 수 있습니다.

```
Open a command prompt on your AD with administrator privilege.
The dsquery command can be used to find the Fully Qualified Domain Name (FQDN) of the ISE.
C:\Users\admin> dsquery computer -name lab-ise1  //here lab-ise1 is the hostname of the ISE
"CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local"

The dsacls command can now be used to find the privileges assigned to the machine account
C:\Windows\system32> dsacls "CN=lab-ise1,CN=Computers,DC=ciscolab,DC=local" >>
C:\dsacl_output.txt
```

출력이 길어 메모장과 같은 텍스트 편집기**에서** 제대로 열리고 볼 수 있는 dsacl_output.txt 텍스트 파일로 리디렉션됩니다.

계정에 토큰 그룹을 읽을 수 있는 권한이 있는 경우 dsacl_**output.txt** 파일에 다음 항목이 있습니다.

```
Inherited to user
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                    SPECIAL ACCESS for tokenGroups   <Inherited from parent>
                                    READ PROPERTY Inherited to group
Allow NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS
                                    SPECIAL ACCESS for tokenGroups   <Inherited from parent>
                                    READ PROPERTY
```

권한이 없는 경우 다음 명령을 사용하여 추가할 수 있습니다.

```
C:\Windows\system32>dsacls "CN=Computers,DC=ciscolab,DC=local" /I:T /G "lab-
ise1$":rp;tokenGroups
```

FQDN 또는 정확한 그룹을 알 수 없는 경우 다음 명령에 따라 도메인 또는 OU(조직 구성 단위)에 대해 이 명령을 빠르게 실행할 수 있습니다.

```
C:\Windows\system32>dsacls "DC=ciscolab,DC=local" /I:T /G "lab-ise1$":rp;tokenGroups
C:\Windows\system32>dsacls "OU=ExampleOU,DC=ciscolab,DC=local" /I:T /G "lab-
ise1$":rp;tokenGroups
```

명령은 전체 도메인 또는 OU에서 각각 호스트 lab-ise1을 찾습니다.

명령의 그룹 및 호스트 이름 세부 정보를 구축의 해당 그룹 및 ISE 이름으로 바꿔야 합니다.이 명령은 ISE 시스템 계정에 토큰 그룹을 읽을 수 있는 권한을 부여합니다.한 도메인 컨트롤러에서만 실행해야 하며 다른 컨트롤러로 자동으로 복제해야 합니다.

문제를 즉시 해결할 수 있습니다.현재 ISE에 연결된 도메인 컨트롤러에서 명령을 실행합니다.

현재 도메인 컨트롤러를 보려면 Administration(관리) > Identity **Management(ID 관리) > External Identity Sources(외부 ID 소스) > Active Directory > Select AD join point(AD 가입 포인트 선택)로 이동합니다**.

관련 정보

- 다른 계정 권한에 대한 정보는 Active Directory Integration with Cisco ISE 1.3에서 찾을 수 있습니다.
- Microsoft Technet 링크
- **기술 지원 및 문서 – Cisco Systems**