

도메인 이름 컨피그레이션이 없어 ISE 관리자 SAML 로그인 문제 해결 액세스가 거부됨

목차

문제

ISE(Identity Services Engine) 관리 SAML(Security Assertion Markup Language) 로그인이 Azure Entra 인증 성공 후 "액세스 거부" 오류와 함께 실패합니다. Azure Entra에서 성공적인 SAML 인증을 표시하지만 ISE는 관리 포털에 대한 액세스를 거부합니다. 또한 CSR(Certificate Signing Request) 생성에 실패하며 다음 오류가 발생합니다.

```
cpm.admin.caservice.utils.CAUtil -::admin::addLocalCert:- Error occurred managing certificates :::-CSR
```

ISE 로그는 내부 HTTPS 검증 중에 노드의 FQDN 및 SSL 핸드셰이크 예외에 대한 DNS 확인 실패를 보여줍니다.

```
SSLHandshakeException: No subject alternative names matching IP address 10.X.X.X found
```

또한 만료된 기본 자체 서명 인증서 및 RESTConf가 인증서 사용 불가로 인해 HTTP로 폴백되는 것에 대한 반복적인 경고가 표시됩니다.

환경

- Cisco ISE(Identity Services Engine) 버전 3.4 패치 3
- SAML ID 공급자로 구성된 Azure Entra(이전의 Azure AD)
- IP 주소 및 FQDN을 통해 액세스되는 ISE 관리
- ISE 3.3에서 3.4로 업그레이드된 환경

해결

1. 다음 명령을 실행하여 현재 ISE 노드 컨피그레이션 및 DNS 확인을 확인합니다.

```
show running-config | include domain
nslookup xxxxxxxxxx.internal
ping xxxxxxxxxx.internal
```



참고: 예상 결과에 따르면 DNS 오류 없이 올바른 IP 주소를 반환하는 성공적인 DNS 확인이 표시됩니다.

2. ISE CLI를 사용하여 ISE 노드 컨피그레이션에 도메인 이름을 다시 추가합니다.

```
device# config t
device(config)# ip domain-name xxxxxxxxxx.internal
```

3. ISE GUI에서 Administration > System > Certificates > Certificates로 이동하고 기본 자체 서명 인증서를 다시 생성합니다. 새 인증서에 FQDN 및 IP 주소가 모두 Subject Alternative Name (SAN) 필드에 포함되어 있는지 확인합니다.

4. 재생성된 인증서가 SAN 필드에 노드 IP 주소를 포함하고 관리 및 포털 서비스 모두에 올바르게 바인딩되어 있는지 확인합니다.

5. ISE 관리자 SAML 로그인을 테스트합니다. 이제 "액세스 거부" 오류 없이 인증에 성공해야 합니다.

원인

이 문제는 [Cisco 버그 ID CSCwm59777](#)에 의해 발생합니다. ISE 3.3에서 ISE 3.4로 업그레이드하는 동안 IP 도메인 이름 처리와 관련이 있습니다. 업그레이드 프로세스 중에 노드의 최상위 도메인 이름 컨피그레이션이 제거되어 ISE에서 자체 FQDN을 제대로 확인하지 못합니다. 이로 인해 두 가지 관련 문제가 발생합니다.

1. DNS 확인 실패: ISE는 자체 호스트 이름을 확인할 수 없으므로 SAML 인증 처리 중에 내부 HTTPS 호출이 호스트 이름 검증에 실패합니다.
2. 인증서 SAN 불일치: 기본 관리자 인증서는 SAN 필드에 노드 IP 주소를 포함하지 않으므로 ISE가 IP 주소를 대신 사용하여 내부 HTTPS 검증을 시도할 때 SSL 핸드셰이크 오류가 발생합니다.

이러한 문제를 함께 사용하면 Azure Entra SAML 인증이 성공한 다음 내부 인증서 유효성 검사 실패로 인해 ISE 액세스가 거부됩니다.

관련 콘텐츠

- [Cisco 버그 ID CSCwm59777](#)
- [Azure AD에서 SAML SSO를 통한 ISE 관리자 로그인 흐름 구성](#)
- [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.