Cisco ISE에서 SSL 디지털 인증서 설치, 갱신 및 문제 해결

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소
- 배경 정보

구성

- 시스템 인증서 가져오기
- 만료된 인증서 교체

일반적인 문제

- 시나리오 1: ISE 노드에서 만료되는 포털 인증서를 대체할 수 없습니다.
  - 오류
  - 솔루션
- 시나리오 2: 다중 사용 사용과 동일한 ISE 노드에 대해 2개의 CSR을 생성할 수 없습니다.
  - 오류
  - 솔루션
- 시나리오 3: 포털 사용을 위해 CA 서명 인증서를 바인딩할 수 없거나 포털 태그를 인증서에 할당할 수 없으며 오류가 발생합니다.
  - 오류
  - 솔루션
- 시나리오 4: 신뢰할 수 있는 인증서 저장소에서 만료된 기본 자체 서명 인증서를 삭제할 수 없습니다.
  - 오류
  - 솔루션
- 시나리오 5: CA 서명 pxGrid 인증서를 ISE 노드의 CSR과 바인딩할 수 없습니다.
  - 오류
  - 솔루션
- 시나리오 6: 기존 LDAP 또는 SCEP RA 프로파일 컨피그레이션으로 인해 만료된 기본 자체 서명 인증서를 신뢰할 수 있는 인증서 저장소에서 삭제할 수 없습니다.
  - 오류
  - 솔루션

추가 리소스

소개

이 문서에서는 SSL 인증서 설치, 갱신 및 Identity Services Engine에서 관찰되는 가장 일반적인 문제에 대한 솔루션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE(Identity Service Engine) GUI

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Cisco Identity Service Engine 2.7

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

배경 정보

이 문서에서는 트러블슈팅을 시작하고 Cisco 기술 지원에 문의하기 전에 확인하고 해결해야 할 일반적인 문제에 대한 권장 단계 및 체크리스트를 제공합니다.

인증서는 개인, 서버, 회사 또는 기타 엔터티를 식별하고 해당 엔터티를 공개 키와 연결하는 전자 문서입니다.

자체 서명 인증서는 자체 작성자가 서명합니다. 인증서는 외부 CA(Certificate Authority)에 의해 자체 서명되거나 디지털 서명될 수 있습니다.

CA 서명 디지털 인증서는 산업 표준으로 간주되며 더 안전합니다.

인증서는 네트워크에서 보안 액세스를 제공하는 데 사용됩니다.

Cisco ISE는 노드 간 통신 및 Syslog 서버, 피드 서버 및 모든 최종 사용자 포털(게스트, 스폰서 및 개인 디바이스 포털)과 같은 외부 서버와의 통신을 위해 인증서를 사용합니다.

인증서는 엔드 포인트에 대한 Cisco ISE 노드를 식별 하고 엔드 포인트와 Cisco ISE 노드 간의 통신을 보호 합니다.

인증서는 모든 HTTPS 통신 및 EAP(Extensible Authentication Protocol) 통신에 사용됩니다.

이 문서에서는 트러블슈팅을 시작하고 Cisco 기술 지원에 문의하기 전에 확인하고 해결해야 할 일반적인 문제에 대한 권장 단계 및 체크리스트를 제공합니다.

이러한 솔루션은 Cisco Technical Support가 해결한 서비스 요청에서 직접 제공됩니다. 네트워크가 가동 중인 경우 문제를 해결하기 위해 수행하는 단계가 미칠 수 있는 영향을 알고 있어야 합니다.

구성

다음 설명서에서는 인증서를 가져오고 교체하는 방법에 대해 설명합니다.

시스템 인증서 가져오기

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/workflow/html/b_basic_setup_2_7.html#ID547

만료된 인증서 교체

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116977-technote-ise-cert-00.html#anc5

일반적인 문제

시나리오 1: ISE 노드에서 만료되는 포털 인증서를 대체할 수 없습니다.

오류

CSR로 새 포털 인증서를 바인딩하는 동안 인증서 바인딩 프로세스가 실패하고 다음 오류가 표시됩니다.

내부 오류입니다. 자세한 내용은 로그를 확인하도록 ISE 관리자에게 요청하십시오

이 오류의 가장 일반적인 원인은 다음과 같습니다.

- 새 인증서의 주체 이름이 기존 인증서와 같습니다.

- 기존 인증서와 동일한 개인 키를 사용하는 갱신된 인증서 가져오기

솔루션

1. 같은 노드의 다른 인증서에 포털 사용을 임시로 할당
2. 만료되는 포털 인증서 삭제
3. 새 포털 인증서를 설치한 다음 포털 사용을 할당합니다

예를 들어 EAP 인증 사용이 있는 기존 인증서에 포털 사용을 일시적으로 할당하려면 다음 단계를 수행하십시오.

1단계. EAP 인증 사용이 있는 인증서를 선택 및 수정하고, 사용 아래에 포털 역할을 추가 하고 저장합니다

2단계. 만료되는 포털 인증서 삭제

3단계. (Usage 아래에서) 어떤 역할도 선택하지 않고 새 포털 인증서를 업로드하고 Submit(제출)

4단계. 새 포털 인증서를 선택 하고 편집 하고, 사용 및 저장에서 포털 역할을 할당 합니다

시나리오 2: 다중 사용 사용과 동일한 ISE 노드에 대해 2개의 CSR을 생성할 수 없습니다.

오류

다중 사용 사용과 동일한 노드에 대한 새 CSR 생성이 다음 오류와 함께 실패합니다.
같은 이름을 가진 다른 인증서가 이미 있습니다. 이름은 고유해야 합니다.

솔루션

CSR Friendly Names(CSR 친화적 이름)는 각 ISE 노드에 대해 하드코딩되므로 다중 사용 사용을 사용하는 동일한 노드에 대해 2개의 CSR을 생성할 수 없습니다. 활용 사례는 특정 노드에 있으며, 관리 및 EAP 인증 사용에 사용되는 CA 서명 인증서 하나와 SAML 및 포털 사용에 사용되는 또 다른 CA 서명 인증서가 있으며 두 인증서가 모두 만료됩니다.

이 시나리오에서:

1단계. 다중 사용 사용을 통해 첫 번째 CSR 생성

2단계. 첫 번째 CSR로 CA 서명 된 인증서를 바인딩 하고 관리 및 EAP 인증 역할을 할당 합니다

3단계. 다중 사용 사용을 통해 두 번째 CSR 생성

4단계. 두 번째 CSR로 CA 서명 인증서를 바인딩하고 SAML 및 포털 역할을 할당합니다.

시나리오 3: 포털 사용을 위해 CA 서명 인증서를 바인딩할 수 없거나 포털 태그를 인증서에 할당할 수 없으며 오류가 발생합니다.

오류

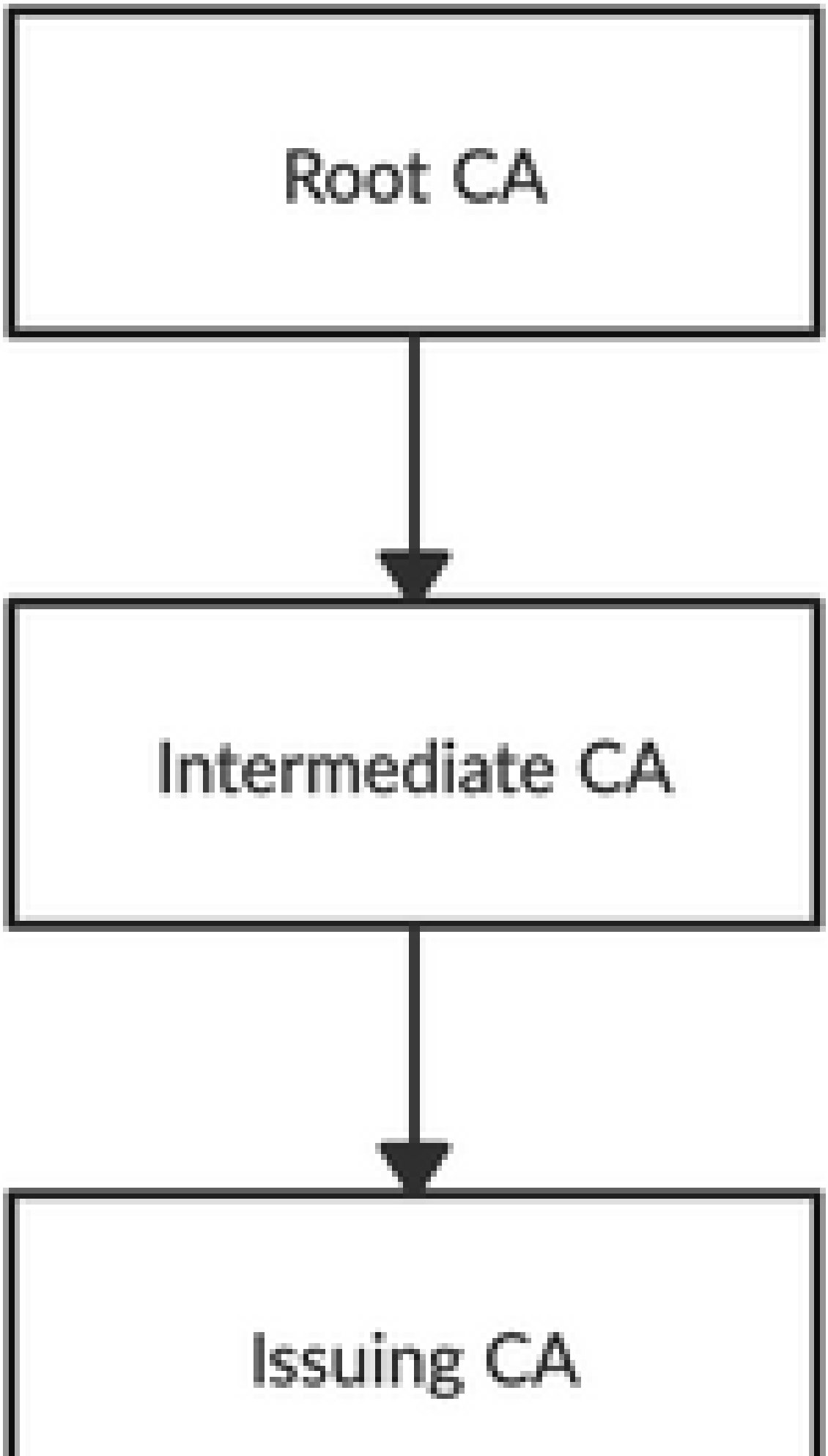
포털 사용을 위해 CA 서명 인증서를 바인딩하면 다음 오류가 발생합니다.

포털 시스템 인증서 체인의 일부이거나, 주체 이름이 같지만 일련 번호가 다른 인증서 기반 관리자 인증 역할로 선택된 하나 이상의 신뢰할 수 있는 인증서가 있습니다. 가져오기/업데이트가 중단되었습니다. 성공적으로 가져오기/업데이트하려면 중복된 신뢰할 수 있는 인증서에서 카트 기반 관리자 인증 역할을 사용하지 않도록 설정하거나 체인에 중복된 신뢰할 수 있는 인증서가 포함된 시스템 인증서에서 포털 역할을 변경해야 합니다.

솔루션

1단계. CA 서명 인증서의 인증서 체인을 확인하고(포털 사용) 신뢰할 수 있는 인증서 저장소에서 인증서 체인의 중복 인증서가 있는지 확인합니다.
2단계. 중복 인증서를 제거하거나 중복 인증서에서 인증서 기반 관리자 인증에 대한 Trust(신뢰) 확인란의 선택을 취소합니다.

예를 들어, CA 서명 된 포털 인증서는 다음과 같은 인증서 체인을 가지고 있습니다.


Root CA
Intermediate CA
Issuing CA

인증서 중 하나에 대해 중복된 인증서가 있는지 확인하고(만료된 인증서일 수 있음) 신뢰할 수 있는 인증서 저장소에서 중복된 인증서를 제거합니다.

시나리오 4: 신뢰할 수 있는 인증서 저장소에서 만료된 기본 자체 서명 인증서를 삭제할 수 없습니다.

오류

신뢰할 수 있는 인증서 저장소에서 만료된 기본 자체 서명 인증서를 삭제하면 다음 오류가 발생합니다.
Disable 또는 Delete 또는 Trust 인증서는 Remote Logging Targets(원격 로깅 대상) 아래의 System Certificates(시스템 인증서) 및/또는 Secure Syslog Target(보안 Syslog 대상)에서 참조되므로 허용되지 않습니다.

솔루션

1. 만료된 기본 자체 서명 인증서가 기존 원격 로깅 대상과 연결되어 있지 않은지 확인합니다. 이는 Administration(관리) > System(시스템) > Logging(로깅) > Remote Logging Targets(원격 로깅 대상) > Select and Edit SecureSyslogCollector(s)(SecureSyslogCollector 선택 및 수정)에서 확인할 수 있습니다
2. 만료된 기본 자체 서명 인증서가 특정 역할(사용)과 연결되어 있지 않은지 확인하십시오. 이 확인은 Administration(관리) > System(시스템) > Certificates(인증서) > System Certificates(시스템 인증서)에서 확인할 수 있습니다.

문제가 계속되면 TAC에 문의하십시오.

시나리오 5: CA 서명 pxGrid 인증서를 ISE 노드의 CSR과 바인딩할 수 없습니다.

오류

새 pxGrid 인증서를 CSR로 바인딩하는 동안 인증서 바인딩 프로세스가 실패하고 오류가 발생합니다.

pxGrid용 인증서는 EKU(Extended Key Usage) 확장에 클라이언트와 서버 인증을 모두 포함해야 합니다.

솔루션

CA 서명 pxGrid 인증서는 TLS 웹 서버 인증(1.3.6.1.5.5.7.3.1) 및 TLS 웹 클라이언트 인증(1.3.6.1.5.5.7.3.2) 확장 키 사용을 모두 포함해야 합니다. 이는 pxGrid 클라이언트와 서버 간의 통신을 보호하기 위해 클라이언트와 서버 인증에 모두 사용되기 때문입니다

참조 링크: https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

시나리오 6: 기존 LDAP 또는 SCEP RA 프로파일 컨피그레이션으로 인해 만료된 기본 자체 서명 인증서를 신뢰할 수 있는 인증서 저장소에서 삭제할 수 없습니다.

오류

신뢰할 수 있는 인증서 저장소에서 만료된 기본 자체 서명 인증서를 삭제하면 다음 오류가 발생합니다.

신뢰 인증서가 다른 곳에서 참조되고 있으므로 삭제할 수 없습니다. SCEP RA 프로필 또는 LDAP ID 소스에서 참조된 것일 수 있습니다.

* 기본 자체 서명 서버 인증서

인증서를 삭제하려면 SCEP RA 프로필을 삭제하거나 LDAP ID 소스를 편집하여 이 인증서를 사용하지 마십시오.

솔루션

1. Administration > Identity Management > External Identity Sources > LDAP > Server Name > Connection으로 이동합니다
2. LDAP 서버 루트 CA가 "기본 자체 서명 서버 인증서"를 사용하지 않는지 확인합니다.
3. LDAP 서버가 보안 연결에 필요한 인증서를 사용하지 않는 경우 Administration(관리) > System(시스템) > Certificates(인증서) > Certificate Authority(인증 기관) > External CA Settings(외부 CA 설정) > SCEP RA Profiles(SCEP RA 프로파일)로 이동합니다
4. SCEP RA 프로필이 기본 자체 서명 인증서를 사용하지 않는지 확인합니다

추가 리소스

와일드카드 인증서를 설치 하는 방법
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

ISE 인증서 관리
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

ISE에 서드파티 CA 인증서 설치
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html

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.