ISE 내부 인증 기관 서비스 이해

목차

소개

이 문서에서는 Cisco ISE(Identity Services Engine)에 있는 CA 서비스 및 EST(Enrollment over Secure Transport) 서비스에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE
- 인증서 및 PKI(Public Key Infrastructure)
- SCEP(Simple Certificate Enrollment Protocol)
- OCSP(Online Certificate Status Protocol)

사용되는 구성 요소

이 문서의 정보는 Identity Services Engine 3.0을 기반으로 합니다.

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.

CA(인증 기관) 서비스

인증서는 외부 CA(Certificate Authority)에 의해 자체 서명되거나 디지털 서명될 수 있습니다. Cisco ISE ISE CA(Internal Certificate Authority)는 직원이 회사 네트워크에서 개인 디바이스를 사용할 수 있도록 중앙 집중식 콘솔에서 엔드포인트에 대한 디지털 인증서를 발급하고 관리합니다. CA 서명 디지털 인증서는 산업 표준으로 간주되며 더 안전합니다. 기본 PAN(Policy Administration Node)은 루트 CA입니다. PSN(Policy Service Node)은 기본 PAN의 하위 CA입니다.

ISE CA 기능

ISE CA는 다음 기능을 제공합니다.

- 인증서 발급: 네트워크에 연결하는 엔드포인트에 대한 CSR(Certificate Signing Request)을 확인하고 서명합니다.
- 키 관리: PAN 및 PSN 노드 모두에 키 및 인증서를 생성하고 안전하게 저장합니다.
- 인증서 저장: 사용자 및 장치에 발급된 인증서를 저장합니다.
- OCSP(Online Certificate Status Protocol) 지원: OCSP 응답자를 제공하여 인증서의 유효성을 검사합니다.

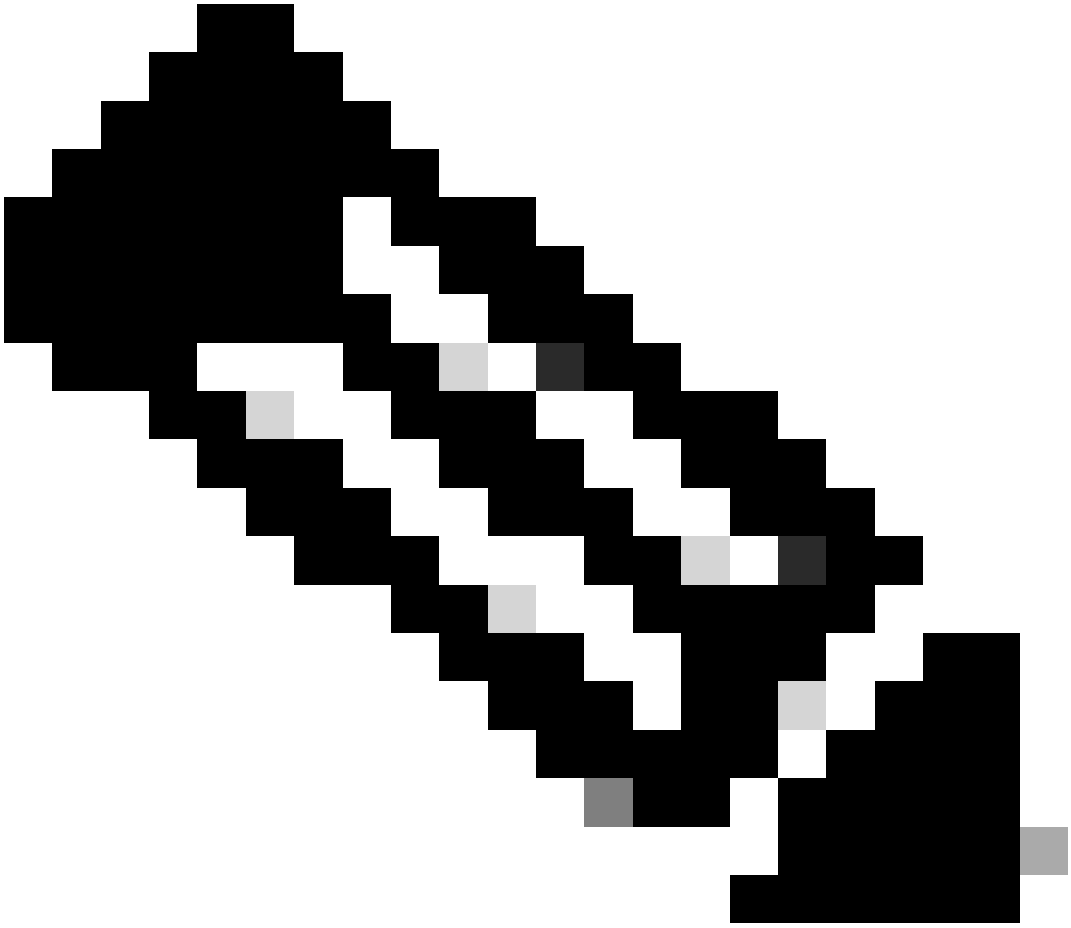
관리 및 정책 서비스 노드에 프로비저닝된 ISE CA 인증서

설치 후, Cisco ISE 노드는 엔드 포인트를 위한 인증서를 관리 하기 위해 루트 CA 인증서 및 노드 CA 인증서와 함께 프로비저닝 됩니다.

구축이 설정되면 PAN(Primary Administration Node)으로 지정된 노드가 루트 CA가 됩니다. PAN에는 루트 CA 인증서 및 루트 CA에서 서명한 노드 CA 인증서가 있습니다.

SAN(보조 관리 노드)이 PAN에 등록되면 노드 CA 인증서가 생성되고 기본 관리 노드의 루트 CA에 의해 서명됩니다.

PAN에 등록된 모든 PSN(Policy Service Node)은 엔드포인트 CA와 PAN의 노드 CA가 서명한 OCSP 인증서로 프로비저닝됩니다. PSN(Policy Service Node)은 PAN에 대한 하위 CA입니다. ISE CA가 사용될 때 PSN의 엔드포인트 CA는 네트워크에 액세스하는 엔드포인트에 인증서를 발급합니다.



참고: ISE 3.1 패치 2 및 ISE 3.2 FCS에서 OCSP 인증서 계층 구조가 변경되었습니다.

RFC 6960에 따르면:

"인증서 발급자는 다음 중 하나를 수행해야 합니다.

- OCSP 응답 자체에 서명 또는

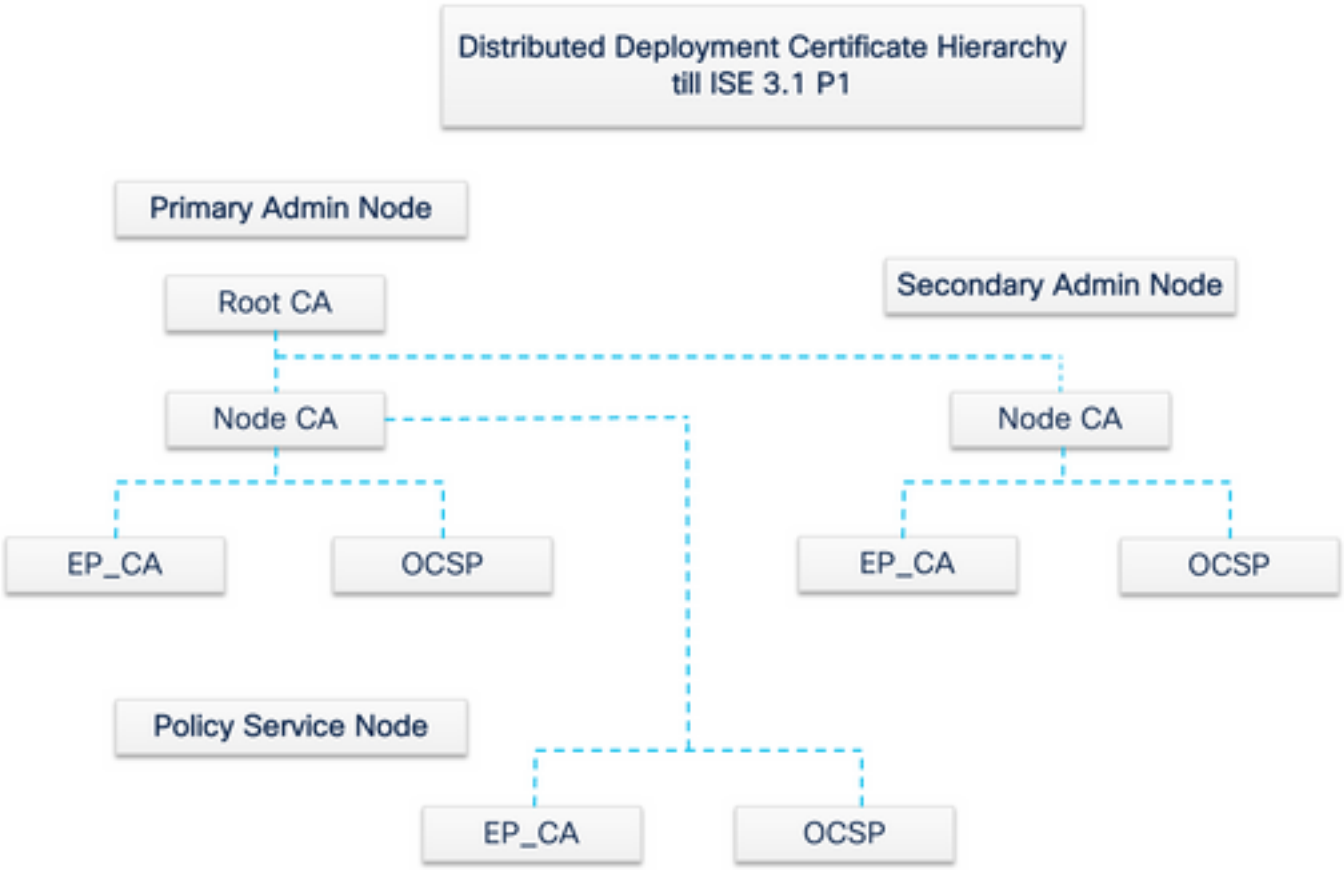
- 이 권한을 다른 엔터티에 명시적으로 지정"

"OCSP 응답 서명자 인증서는 요청에서 식별된 CA에서 직접 발급해야 합니다. "

"OCSP 응답에 의존하는 시스템은 위임 인증서와 폐기 검사를 받은 인증서(is)가 동일한 키로 서명된 경우에만 해당 인증서를 발급한 CA가 발급한 위임 인증서를 인식해야 합니다."

앞서 언급한 RFC 표준을 준수하기 위해 OCSP Responder Certificate의 인증서 계층 구조가 ISE에

서 변경됩니다. 이제 OCSP 응답자 인증서가 PAN의 노드 CA 대신 동일한 노드의 엔드포인트 하위 CA에 의해 발급됩니다.



EST(Enrollment over Secure Transport) 서비스

PKI(Public Key Infrastructure)의 개념은 오래전부터 존재해 왔습니다. PKI는 디지털 인증서 형태의 서명된 공개 키 쌍을 통해 사용자 및 디바이스의 ID를 인증합니다. EST(Enrollment over Secure Transport)는 이러한 인증서를 제공하는 프로토콜입니다. EST 서비스는 보안 전송을 통해 CMC(Certificate Management over Cryptographic Message Syntax)를 사용하는 클라이언트에 대해 인증서 등록을 수행하는 방법을 정의합니다. IETF에 따르면 - "EST는 클라이언트 인증서 및 관련 CA(Certification Authority) 인증서를 획득해야 하는 PKI(Public Key Infrastructure) 클라이언트를 대상으로 하는 간단하면서도 기능적인 인증서 관리 프로토콜을 설명합니다. 또한 클라이언트에서 생성한 공개/개인 키 쌍은 물론 CA에서 생성한 키 쌍도 지원합니다."

EST 활용 사례

EST 프로토콜을 사용할 수 있습니다.

- 보안 고유 장치 ID를 사용하여 네트워크 장치를 등록하려면
- BYOD 솔루션

왜 EST인가?

EST 및 SCEP 프로토콜 모두 인증서 프로비저닝을 다룹니다. EST는 SCEP(Simple Certificate Enrollment Protocol)의 후속 버전입니다. 단순성 때문에 SCEP는 수년 동안 인증서 프로비저닝에서 사실상의 프로토콜이었습니다. 그러나 다음과 같은 이유로 SCEP를 통한 EST를 사용하는 것이 좋습니다.

- 인증서 및 메시지의 안전한 전송을 위한 TLS 사용 - EST에서 CSR(Certificate Signing Request)은 이미 신뢰하고 TLS로 인증된 요청자에게 연결할 수 있습니다. 클라이언트는 자신을 제외한 다른 사람의 인증서를 가져올 수 없습니다. SCEP에서 CSR은 클라이언트와 CA 간의 공유 암호에 의해 인증됩니다. 이렇게 하면 공유 암호에 액세스할 수 있는 사용자가 자신이 아닌 다른 엔터티에 대해 인증서를 생성할 수 있으므로 보안 문제가 발생합니다.
- ECC 서명 인증서 등록 지원 - EST는 암호화 민첩성을 제공합니다. ECC(Elliptic Curve Cryptography)를 지원합니다. SCEP는 ECC를 지원하지 않으며 RSA 암호화에 따라 달라집니다. ECC는 훨씬 작은 키 크기를 사용하면서도 RSA와 같은 다른 암호화 알고리즘보다 더 우수한 보안 및 성능을 제공합니다.
- EST는 자동 인증서 재등록을 지원하도록 구축되었습니다.

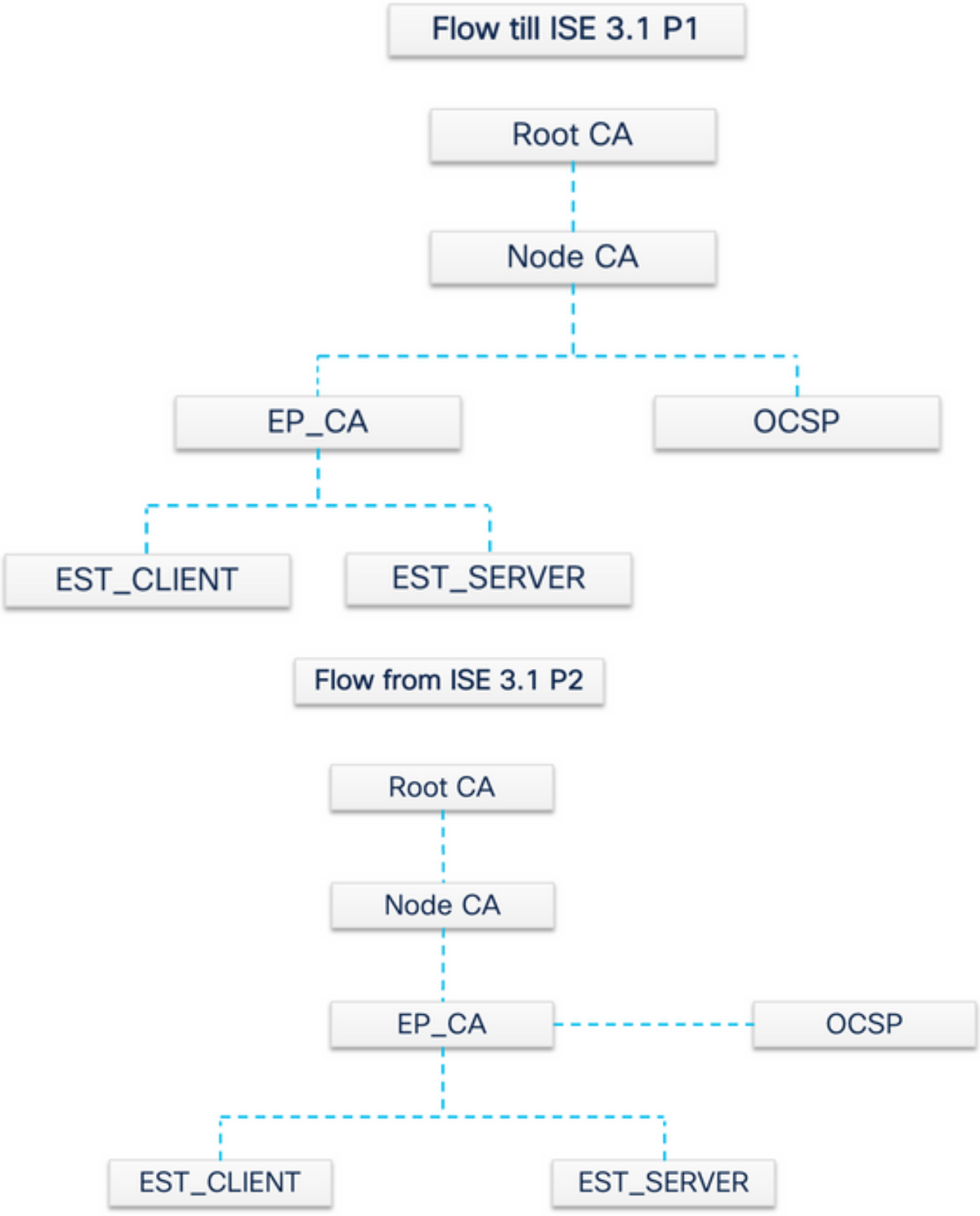
TLS의 검증된 보안과 지속적인 개선을 통해 EST 트랜잭션은 암호화 보호 측면에서 안전합니다. SCEP와 RSA의 긴밀한 통합으로 데이터 보호 기술 발전에 따른 보안 문제 발생

ISE의 EST

이 프로토콜을 구현하려면 클라이언트와 서버 모듈이 필요합니다.

- EST 클라이언트 - 일반 ISE tomcat에 포함됨
- EST 서버 - NGINX라는 오픈 소스 웹 서버에 구축됩니다. 이는 별도의 프로세스로 실행되며 포트 8084에서 수신됩니다.

인증서 기반 클라이언트 및 서버 인증은 EST에서 지원됩니다. 엔드포인트 CA는 EST 클라이언트 및 EST 서버에 대한 인증서를 발급합니다. EST 클라이언트 및 서버 인증서와 해당 키는 ISE CA의 NSS DB에 저장됩니다.



ISE EST의 요청 유형

EST 서버가 가동될 때마다 CA 서버에서 모든 CA 인증서의 최신 사본을 가져와 저장합니다. 그런 다음 EST 클라이언트는 CA 인증서 요청을 수행하여 이 EST 서버에서 전체 체인을 가져올 수 있습니다. 간단한 등록 요청을 하기 전에 EST 클라이언트는 먼저 CA 인증서 요청을 발행해야 합니다.

CA 인증서 요청(RFC 7030 기반)

1. EST 클라이언트는 현재 CA 인증서의 사본을 요청합니다.
2. 작업 경로 값이 인 HTTPS GET 메시지 /cacerts.

- 이 작업은 다른 EST 요청보다 먼저 수행됩니다.
- 최신 CA 인증서의 복사본을 가져오려면 5분마다 요청이 수행됩니다.
- EST 서버에는 클라이언트 인증이 필요하지 않아야 합니다.

두 번째 요청은 단순 등록 요청이며 EST 클라이언트와 EST 서버 간의 인증이 필요합니다. 이 작업은 엔드포인트가 ISE에 연결되어 인증서 요청을 수행할 때마다 수행됩니다.

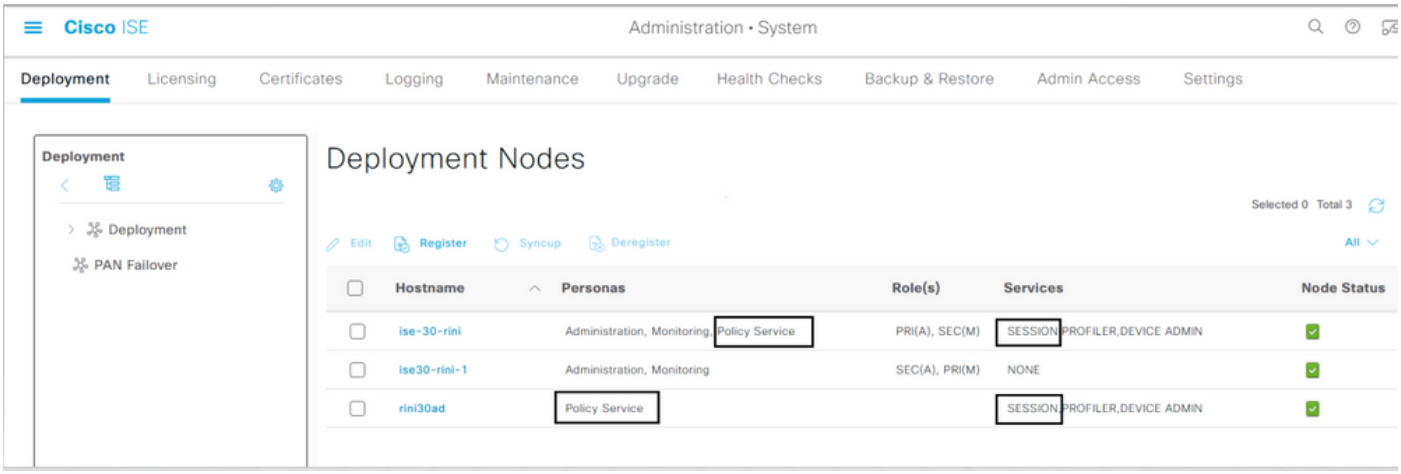
단순 등록 요청(RFC 7030 기반)

1. EST 클라이언트는 EST 서버로부터 인증서를 요청합니다.
2. 작업 경로 값이 인 HTTPS POST /simpleenroll 메시지

- EST 클라이언트는 ISE로 전송된 이 통화 내에 PKCS#10 요청을 포함합니다.
- EST 서버는 클라이언트를 인증해야 합니다.

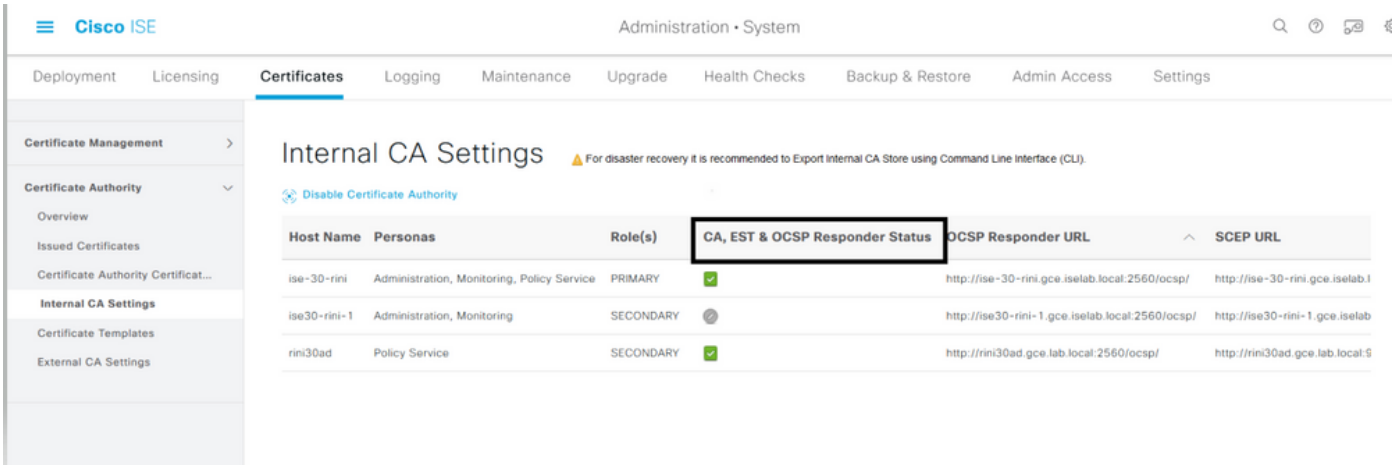
EST 및 CA 서비스 상태

CA 및 EST 서비스는 세션 서비스가 활성화된 정책 서비스 노드에서만 실행할 수 있습니다. 노드에서 세션 서비스를 활성화하려면 로 Administration > System > Deployment 이동합니다. 세션 서비스를 활성화해야 하는 서버 호스트 이름을 선택하고 를 클릭합니다Edit. Policy Service(정책 서비스) 페르소나 아래에서 **Enable Session Services** 확인란을 선택합니다.



GUI에 표시되는 상태

EST 서비스 상태는 ISE의 ISE CA 서비스 상태에 연결됩니다. CA 서비스가 작동 중이면 EST 서비스가 작동 중이고 CA 서비스가 작동 중이면 EST 서비스도 작동 중입니다.



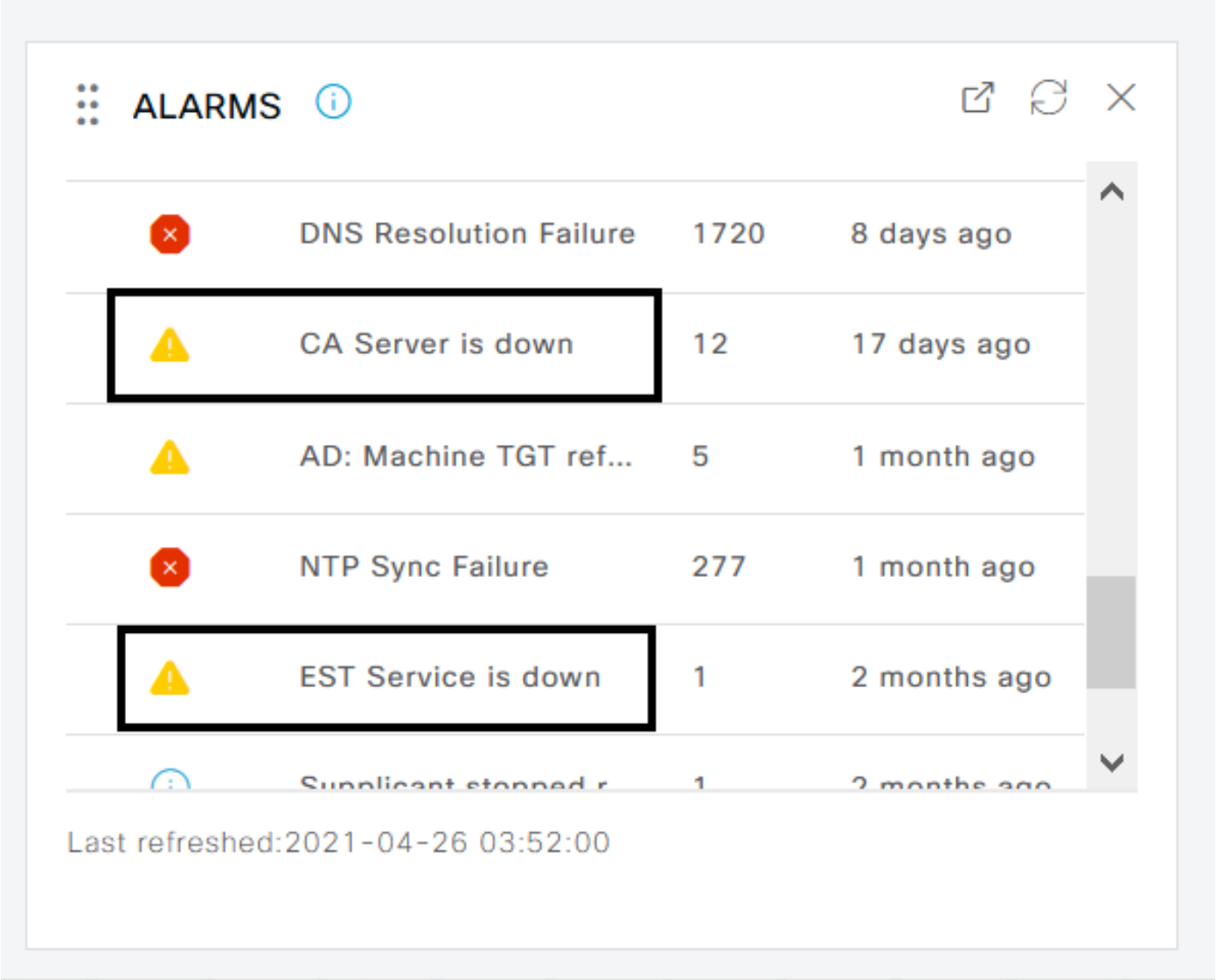
CLI에 표시되는 상태

```
ise-30-rini/admin# sh app status ise

ISE PROCESS NAME                       STATE            PROCESS ID
--------------------------------------------------------------------
Database Listener                      running          61993
Database Server                        running          159 PROCESSES
Application Server                     running          72240
Profiler Database                      running          68224
ISE Indexing Engine                    running          74972
AD Connector                           running          78912
M&T Session Database                   running          68007
M&T Log Processor                      running          70533
Certificate Authority Service          running          63090
EST Service                            running          64492
SXP Engine Service                     disabled
Docker Daemon                          running          64427
TC-NAC Service                         disabled
pxGrid Infrastructure Service          disabled
pxGrid Publisher Subscriber Service    disabled
pxGrid Connection Manager              disabled
```

대시보드의 경보

EST 및 CA 서비스가 다운된 경우 ISE 대시보드에 경보가 표시됩니다.



CA 및 EST 서비스가 실행되고 있지 않은 경우 영향

- EST 서버가 다운된 경우 EST 클라이언트 /cacerts호출 실패가 발생할 수 있습니다. EST CA 체인 인증서 CA 체인이 불완전한 경우에도 통화 실패가 발생할 수 있습니다/cacerts.

- ECC 기반 엔드포인트 인증서 등록 요청이 실패했습니다.

- 이전의 두 장애 중 하나가 발생하면 BYOD 흐름이 중단됩니다.
- 대기열 링크 오류 경보를 생성할 수 있습니다.

문제 해결

EST 프로토콜을 사용하는 BYOD 플로우가 제대로 작동하지 않을 경우 다음 조건을 확인하십시오.

- 인증서 서비스 엔드포인트 하위 CA 인증서 체인이 완료되었습니다. 인증서 체인이 완료되었는지 확인하려면 다음을 수행합니다.

  1. 로 Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates 이동합니다.

     - 특정 인증서를 확인 하려면 인증서 옆의 확인 란을 선택 하고 **보기** 를 클릭 합니다.

- CA 및 EST 서비스가 작동 및 실행 중인지 확인합니다. 서비스가 실행되고 있지 않으면 로 이동하여 Administration > System > Certificates > Certificate Authority > Internal CA Settings CA 서비스를 활성화합니다.

- 업그레이드가 수행된 경우 업그레이드 후 ISE 루트 CA 인증서 체인을 교체합니다. 이를 위해 다음을 수행합니다.

  1. 를 선택합니다Administration > System > Certificates > Certificate Management > Certificate Signing Requests.

-

를 Generate Certificate Signing Requests (CSR) 클릭합니다.

ISE Root CA

-

드롭다운 목록에서Certificate(s) will be used for 선택합니다

-

를 Replace ISE Root CA Certificate Chain 클릭합니다.

- 로그를 확인하기 위해 활성화할 수 있는 유용한 디버그est는 , provisioning 및ca-service 입니다ca-service-cert. , ise-psc.log, catalina.outerror.log 및 파일caservice.log , 을 참조하십시오.

관련 정보

- **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.