Interne certificeringsinstantie van ISE begrijpen

Inhoud

- Inleiding
- Voorwaarden
  - Vereisten
  - Gebruikte componenten
- Service van certificeringsinstantie (CA)
  - ISE-CA-functionaliteit
  - ISE-AC-certificaten, provisioning voor beheer- en beleidsserviceknooppunten
- Inschrijving via Secure Transport (EST)-service
  - EST-gebruikscases
  - Waarom EST?
  - EST in ISE
  - Soorten verzoeken in ISE EST
    - CA-certificaataanvraag (op basis van RFC 7030)
    - Eenvoudige inschrijvingsaanvraag (gebaseerd op RFC 7030)
- EST- en CA-servicestatus
  - Status weergegeven op GUI
  - Status weergegeven op CLI
  - Alarmen op Dashboard
  - Impact als CA- en EST-services niet actief zijn
- Problemen oplossen
- Gerelateerde informatie

Inleiding

Dit document beschrijft de CA-service en de Enrollment over Secure Transport (EST)-service die aanwezig is in Cisco Identity Services Engine (ISE).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- ISE
- Certificaten en Public Key Infrastructure (PKI)
- Eenvoudig protocol voor certificaatinschrijving (SCEP)
- Online Certificate Status Protocol (OCSP)

Gebruikte componenten

De informatie in dit document is gebaseerd op Identity Services Engine 3.0.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Service van certificeringsinstantie (CA)

Certificaten kunnen zelfondertekend of digitaal ondertekend worden door een externe certificeringsinstantie (CA). De Cisco ISE Internal Certificate Authority (ISE-certificeringsinstantie) geeft digitale certificaten uit en beheert deze voor endpoints vanaf een gecentraliseerde console om werknemers in staat te stellen hun persoonlijke apparaten te gebruiken in het netwerk van het bedrijf. Een CA-ondertekend digitaal certificaat wordt beschouwd als een industriestandaard en veiliger. Het Primary Policy Administration Node (PAN) is de Root CA. De Policy Service Nodes (PSN's) zijn ondergeschikte CA's voor het primaire PAN.

ISE-CA-functionaliteit

De ISE CA biedt deze functionaliteit:

- Certificaatafgifte: valideert en ondertekent certificaatondertekeningsaanvragen (CSR's) voor endpoints die verbinding maken met het netwerk.
- Key Management: genereert en slaat veilig sleutels en certificaten op zowel PAN- als PSN-knooppunten op.
- Certificaatopslag: Hierop worden certificaten opgeslagen die worden afgegeven aan gebruikers en apparaten.
- Ondersteuning van Online Certificate Status Protocol (OCSP): Biedt een OCSP-responder om de geldigheid van certificaten te controleren.

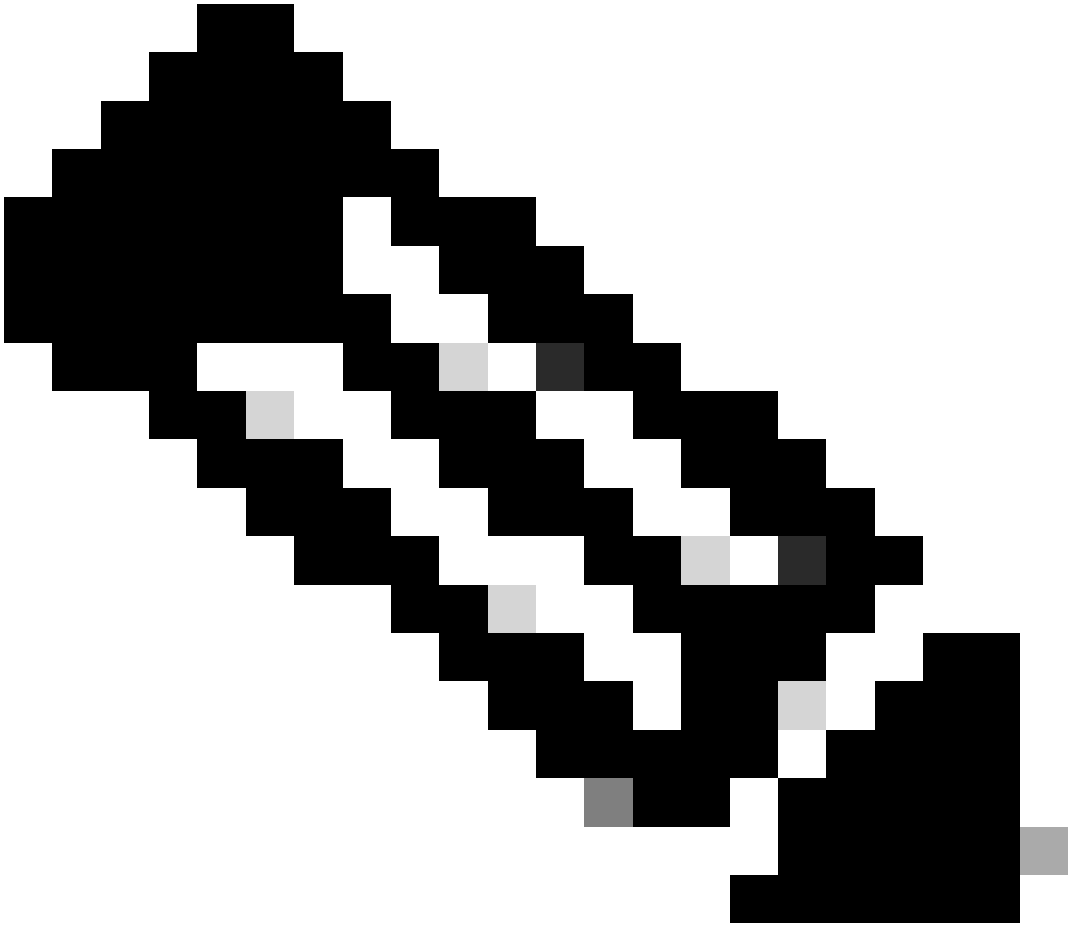
ISE-AC-certificaten, provisioning voor beheer- en beleidsserviceknooppunten

Na installatie is een Cisco ISE-knooppunt voorzien van een Root CA-certificaat en een Node CA-certificaat om certificaten voor endpoints te beheren.

Wanneer een implementatie is ingesteld, wordt het knooppunt dat is aangewezen als primair beheerknooppunt (PAN), de root-CA. De PAN heeft een Root CA-certificaat en een Node CA-certificaat dat is ondertekend door de Root CA.

Wanneer een secundair beheerknooppunt (SAN) is geregistreerd in het PAN, wordt een CA-certificaat voor knooppunt gegenereerd en ondertekend door de root-CA op het primaire beheerknooppunt.

Elk Policy Service Node (PSN) dat is geregistreerd in de PAN is voorzien van een Endpoint CA en een OCSP-certificaat dat is ondertekend door de Node CA van de PAN. De Policy Service Nodes (PSN's) zijn ondergeschikte CA's aan de PAN. Wanneer de ISE CA wordt gebruikt, geeft de Endpoint CA op de PSN de certificaten af aan de eindpunten die toegang hebben tot het netwerk.



Opmerking: van ISE 3.1 Patch 2 en ISE 3.2 FCS is de OCSP-certificaathiërarchie gewijzigd.

Conform RFC 6960:

"Een uitgevende instelling van certificaten MOET een van de volgende handelingen verrichten:

- de OCSP-antwoorden zelf ondertekenen, of

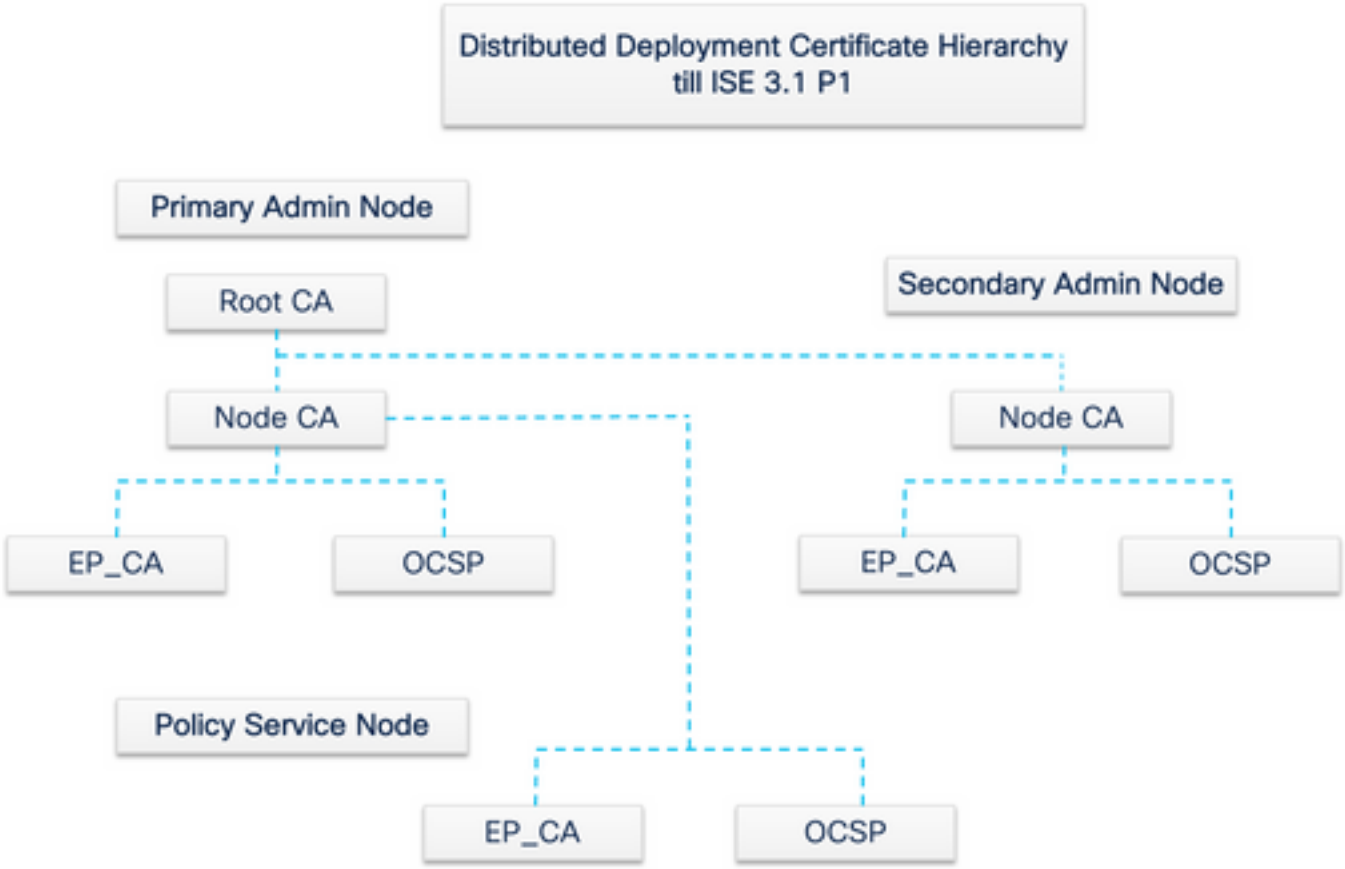
- deze instantie uitdrukkelijk aan een andere instantie aanwijzen."

"Het OCSP-bewijs van ondertekenaar MOET rechtstreeks worden afgegeven door de bevoegde instantie die in het verzoek wordt vermeld. "

"Het systeem (vertrouwt) op OCSP-antwoorden MOET een delegatiecertificaat erkennen zoals afgegeven door de CA die het certificaat in kwestie heeft afgegeven, alleen als het

delegatiecertificaat en het certificaat (wordt) gecontroleerd voor herroeping door dezelfde sleutel zijn ondertekend."

De certificaathiërarchie voor het OCSP-antwoordcertificaat wordt in ISE gewijzigd om aan de eerder genoemde RFC-standaard te voldoen. Het OCSP Responder Certificate wordt nu afgegeven door Endpoint Sub CA van hetzelfde knooppunt in plaats van Node CA in PAN.



Inschrijving via Secure Transport (EST)-service

Het concept public key infrastructure (PKI) bestaat al een hele tijd. De PKI verifieert de identiteit van gebruikers en apparaten door middel van ondertekende publieke sleutelparen in de vorm van digitale certificaten. Inschrijving via Secure Transport (EST) is een protocol om deze certificaten te leveren. EST-service bepaalt hoe u certificaatinschrijving uitvoert voor klanten die gebruik maken van Certificate Management via Cryptographic Message Syntax (CMC) via een beveiligd transport. In de IETF - "EST" wordt een eenvoudig, maar functioneel protocol voor certificaatbeheer beschreven dat zich richt op PKI-clients (Public Key Infrastructure) die clientcertificaten en bijbehorende CA-certificaten moeten aanschaffen. Het ondersteunt ook client-gegenereerde publiek/private toetsparen en toetsparen gegenereerd door de CA."

EST-gebruikscases

Het EST-protocol kan worden gebruikt:

- Netwerkapparaten inschrijven door middel van beveiligde unieke apparaatidentiteit
- Voor BYOD Solutions

Waarom EST?

Zowel EST- als SCEP-protocollen adresseren de provisioning van certificaten. EST is een opvolger van Simple Certificate Enrollment Protocol (SCEP). Wegens zijn eenvoud, is SCEP het de facto protocol in certificaatlevering vele jaren geweest. Het gebruik van EST over SCEP wordt echter om de volgende redenen aanbevolen:

- Gebruik van TLS voor veilig transport van certificaten en berichten - In EST kan het certificaat ondertekeningsverzoek (CSR) worden gekoppeld aan een aanvrager die al vertrouwd is en geauthenticeerd met TLS. Klanten kunnen alleen een certificaat krijgen voor zichzelf. In SCEP wordt de CSR geauthenticeerd door een gedeeld geheim tussen de klant en de CA. Dit brengt veiligheidszorgen met zich mee omdat iemand met toegang tot het gedeelde geheim certificaten kan genereren voor andere entiteiten dan zijzelf.
- Ondersteuning voor inschrijving van door ECC ondertekende certificaten - EST biedt cryptografische flexibiliteit. Het ondersteunt elliptische curve cryptografie (ECC). SCEP ondersteunt ECC niet en is afhankelijk van RSA-encryptie. ECC biedt meer veiligheid en betere prestaties dan andere cryptografische algoritmen zoals RSA zelfs terwijl het een veel kleinere sleutelgrootte gebruikt.
- EST is ontwikkeld om automatische herinschrijving van certificaten te ondersteunen.

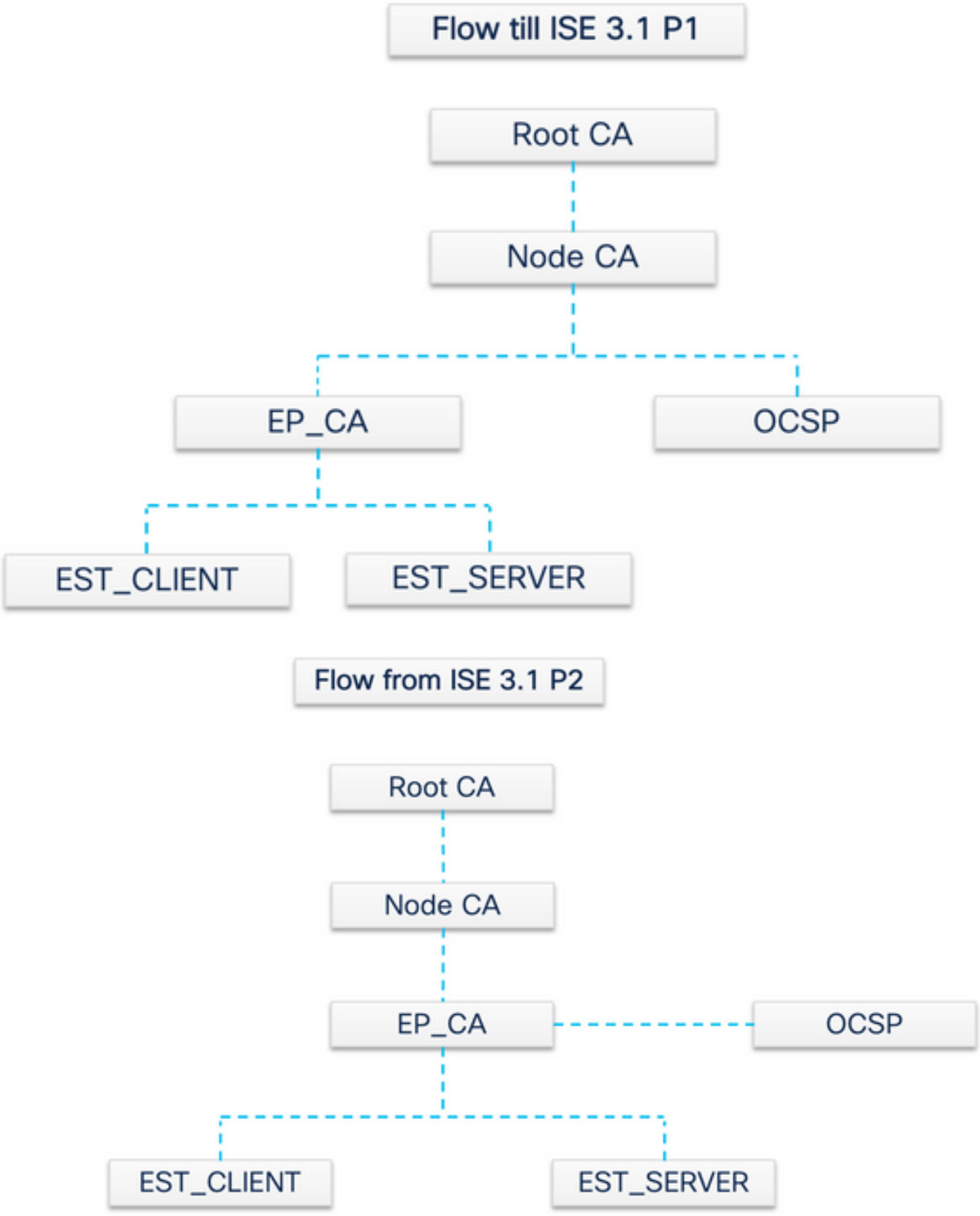
TLS bewezen beveiliging en continue verbetering helpen ervoor te zorgen dat EST-transacties veilig zijn in termen van cryptografische bescherming. SCEP strakke integratie met RSA om gegevens te beschermen introduceert beveiligingsproblemen naarmate de technologie zich verder ontwikkelt.

EST in ISE

Om dit protocol te implementeren zijn een client en een servermodule nodig:

- EST-client - ingesloten in de reguliere ISE-tomcat.
- EST-server - geïmplementeerd op een open-source webserver met de naam NGINX. Dit is een apart proces en het luistert op poort 8084.

Op certificaat gebaseerde client- en serververificatie wordt ondersteund door EST. Het eindpunt CA geeft het certificaat uit voor de EST-client en de EST-server. De EST-client- en servercertificaten en de bijbehorende sleutels worden opgeslagen in de NSS-database van ISE CA.



Soorten verzoeken in ISE EST

Wanneer de EST-server opduikt, krijgt deze de nieuwste kopie van alle CA-certificaten van de CA-server en slaat deze op. Vervolgens kan de EST-client een CA-certificaataanvraag indienen om de hele keten van deze EST-server te halen. Alvorens het een eenvoudig inschrijvingsverzoek doet, moet de EST-client eerst het CA-certificaatverzoek afgeven.

CA-certificaataanvraag (op basis van RFC 7030)

1. De EST-client vraagt een kopie van de huidige CA-certificaten.
2. HTTPS ONTVANG bericht met een waarde van het verrichtingspad van /cacerts.

- Deze handeling wordt uitgevoerd vóór andere EST-verzoeken.
- Er wordt om de 5 minuten een verzoek gedaan om een kopie te krijgen van de meest actuele CA-certificaten.
- Voor de EST-server is geen clientverificatie vereist.

Het tweede verzoek is een eenvoudig inschrijvingsverzoek en het heeft authenticatie tussen de EST-client en de EST-server nodig. Dit gebeurt elke keer dat een eindpunt verbinding maakt met ISE en een certificaataanvraag indient.

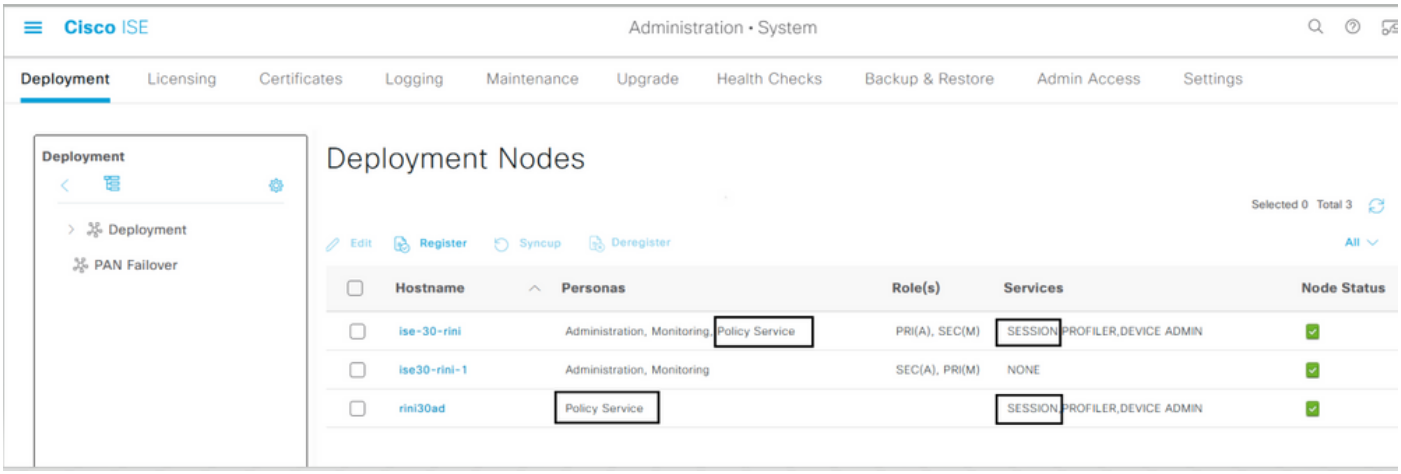
Eenvoudige inschrijvingsaanvraag (gebaseerd op RFC 7030)

1. De EST client vraagt een certificaat aan bij de EST server.
2. HTTPS-POST bericht met de waarde van het verrichtingspad van /simpleenroll.

- De EST-client sluit het PKCS#10-verzoek in binnen deze oproep die naar ISE wordt verzonden.
- De EST-server moet de client verifiëren.

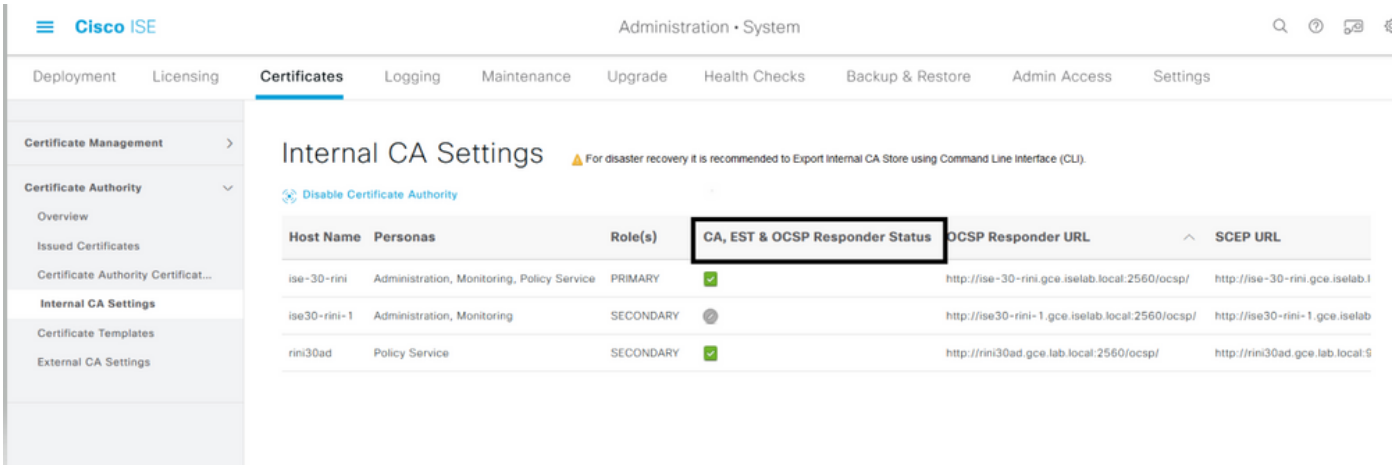
EST- en CA-servicestatus

CA- en EST-services kunnen alleen worden uitgevoerd op een Policy Service-knooppunt waarop sessieservices zijn ingeschakeld. Ga naar Administration > System > Deployment om sessieservices op een knooppunt in te schakelen. Selecteer de server hostname waarop de sessieservices moeten worden ingeschakeld en klik op Edit . Selecteer het **Enable Session Services** aankruisvakje onder Policy Service-persona.



Status weergegeven op GUI

EST-servicestatus is gekoppeld aan de ISE-servicestatus op ISE. Als de CA-dienst omhoog is, dan is de EST-dienst omhoog en als de CA-dienst is omlaag, is de EST-dienst ook omlaag.



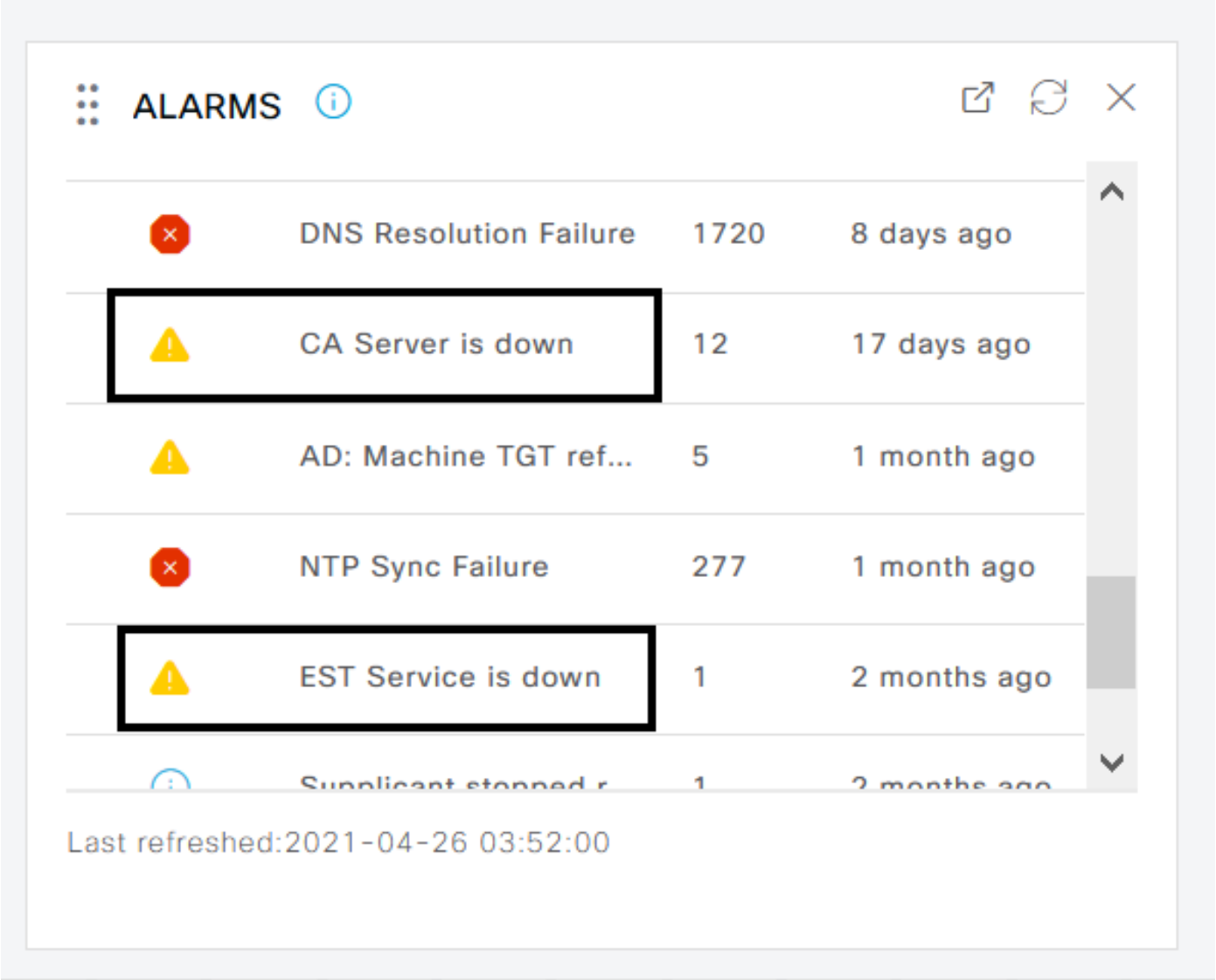
Status weergegeven op CLI

```
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
```

Alarmen op Dashboard

Het alarm wordt weergegeven op het ISE-dashboard als EST en CA-diensten niet beschikbaar zijn.



Impact als CA- en EST-services niet actief zijn

- EST-client /cacerts-aanroepuitval kan voorkomen wanneer EST-server niet actief is. De /cacerts call-uitval kan ook gebeuren als de EST CA-kettingcertificaat CA-keten onvolledig is.

-

  Aanvragen voor inschrijving van ECC-gebaseerde endpointcertificaten mislukken.

- De doorstroming van BYOD breekt als een van de twee voorgaande storingen optreedt.
- Er kunnen alarmen worden gegenereerd voor Queue Link Error.

Problemen oplossen

Als de BYOD-stroom met EST-protocol niet goed werkt, controleer dan deze omstandigheden:

- Certificaatservices Endpoint Sub CA certificaatketen is compleet. Om na te gaan of de certificaatketen volledig is:

  1. Navigeer naar Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates .

     - Selecteer het aanvinkvakje naast het certificaat en klik op **Weergeven** om een bepaald certificaat te controleren.

- Zorg ervoor dat de CA- en EST-services actief zijn. Als de services niet actief zijn, navigeer dan naar Administration > System > Certificates > Certificate Authority > Internal CA Settings om de CA-service in te schakelen.

- Als er een upgrade is uitgevoerd, vervangt u de ISE Root CA-certificaatketen na de upgrade. Dit doet u zo:

  1. Kies Administration > System > Certificates > Certificate Management > Certificate Signing Requests.

     -

Klik op de knop .Generate Certificate Signing Requests (CSR)

-

Selecteer dit ISE Root CA in Certificate(s) will be used for de vervolgkeuzelijst

-

Klik op de knop .Replace ISE Root CA Certificate Chain

- Handige debug die kan worden ingeschakeld om de logbestanden te controleren zoals est , provisioning , ca-service en ca-service-cert . Raadpleeg ise-psc.log , catalina.out caservice.log , en error.logbestanden.

Gerelateerde informatie

- **Cisco Technical Support en downloads**

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.