Kenntnis der internen Services der ISE-Zertifizierungsstelle

Inhalt

Einleitung

Dieses Dokument beschreibt den CA-Service und den EST-Service (Enrollment over Secure Transport), der in der Cisco Identity Services Engine (ISE) vorhanden ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ISE
- Zertifikate und Public Key Infrastructure (PKI)
- Simple Certificate Enrollment Protocol (SCEP)

- Online Certificate Status Protocol (OCSP)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Identity Services Engine 3.0.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Zertifizierungsstellendienst (Certificate Authority, CA)

Zertifikate können selbstsigniert oder von einer externen Zertifizierungsstelle digital signiert werden. Die Cisco ISE Internal Certificate Authority (ISE CA) erstellt und verwaltet digitale Zertifikate für Endgeräte über eine zentrale Konsole, damit Mitarbeiter ihre privaten Geräte im Unternehmensnetzwerk nutzen können. Ein von einer Zertifizierungsstelle signiertes digitales Zertifikat gilt als Industriestandard und ist sicherer. Der primäre Policy Administration Node (PAN) ist die Root-CA. Die Policy Service Nodes (PSNs) sind dem primären PAN untergeordnete CAs.

ISE CA-Funktionalität

Die ISE-Zertifizierungsstelle bietet folgende Funktionen:

- Zertifikatausstellung: Validiert und signiert CSRs (Certificate Signing Requests) für Endpunkte, die eine Verbindung mit dem Netzwerk herstellen.
- Schlüsselverwaltung: Generiert und speichert Schlüssel und Zertifikate auf PAN- und PSN-Knoten.
- Zertifikatsspeicher: Speichert Zertifikate, die für Benutzer und Geräte ausgestellt werden.
- Online Certificate Status Protocol (OCSP)-Unterstützung: Bietet einen OCSP-Responder zur Überprüfung der Gültigkeit von Zertifikaten.

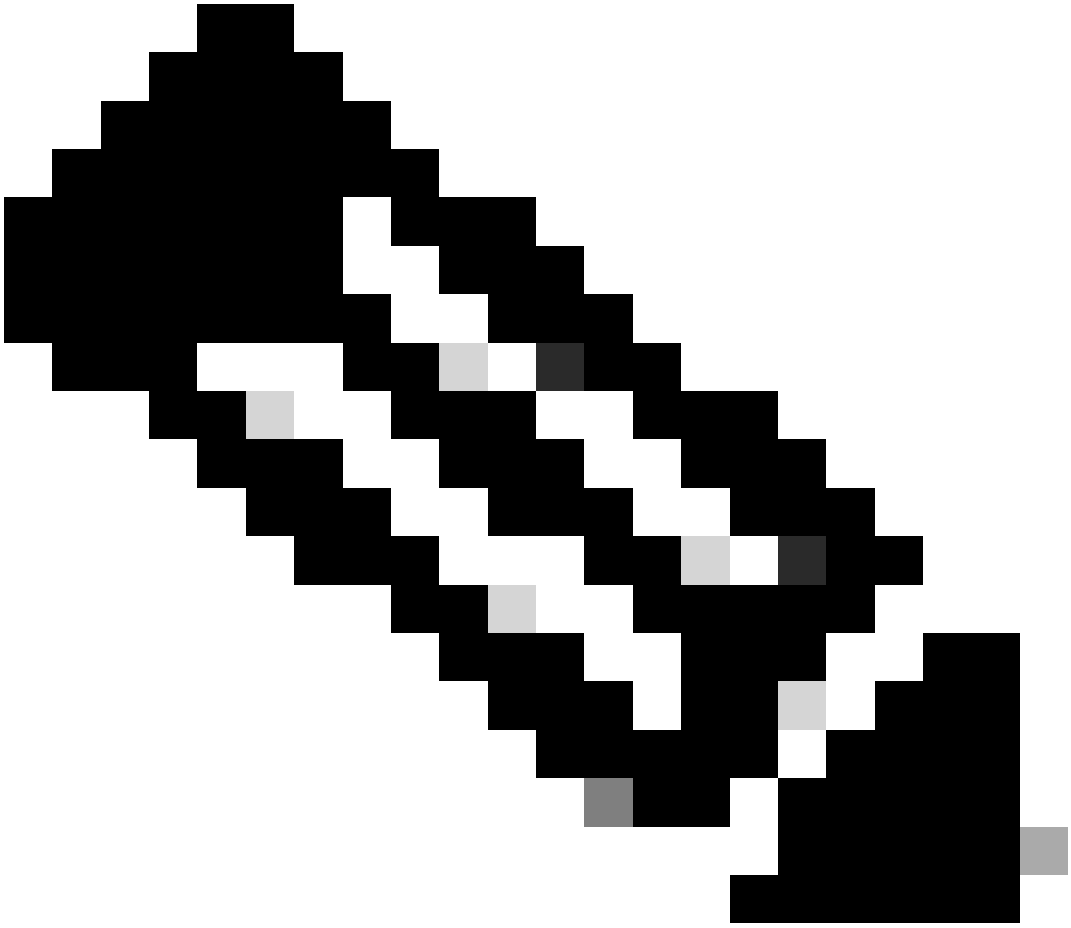
ISE-Zertifizierungsstellenzertifikate, die für Administrations- und Richtliniendienstknoten bereitgestellt werden

Nach der Installation wird ein Cisco ISE-Knoten mit einem Zertifikat der Stammzertifizierungsstelle und einem Zertifikat der Knotenzertifizierungsstelle bereitgestellt, um Zertifikate für Endpunkte zu verwalten.

Wenn eine Bereitstellung eingerichtet wird, wird der Knoten, der als primärer Administrationsknoten (PAN) festgelegt ist, zur Root-CA. Der PAN verfügt über ein Zertifikat der Stammzertifizierungsstelle und ein Zertifikat der Knotenzertifizierungsstelle, das von der Stammzertifizierungsstelle signiert wird.

Wenn ein sekundärer Administrationsknoten (SAN) beim PAN registriert wird, wird ein Zertifikat der Node-CA generiert und von der Root-CA auf dem primären Administrationsknoten signiert.

Jeder Policy Service Node (PSN), der beim PAN registriert ist, erhält eine Endpunkt-CA und ein OCSP-Zertifikat, das von der Knoten-CA des PAN signiert wird. Die Policy Service Nodes (PSNs) sind dem PAN untergeordnete CAs. Bei Verwendung der ISE-CA gibt die Endpunkt-CA auf dem PSN die Zertifikate an die Endpunkte aus, die auf das Netzwerk zugreifen.



Hinweis: Ab ISE 3.1 Patch 2 und ISE 3.2 FCS wurde die OCSP-Zertifikathierarchie geändert.

Gemäß RFC 6960:

"Ein Zertifikataussteller MUSS einen der folgenden Schritte ausführen:

- die OCSP-Antworten selbst zu unterzeichnen oder

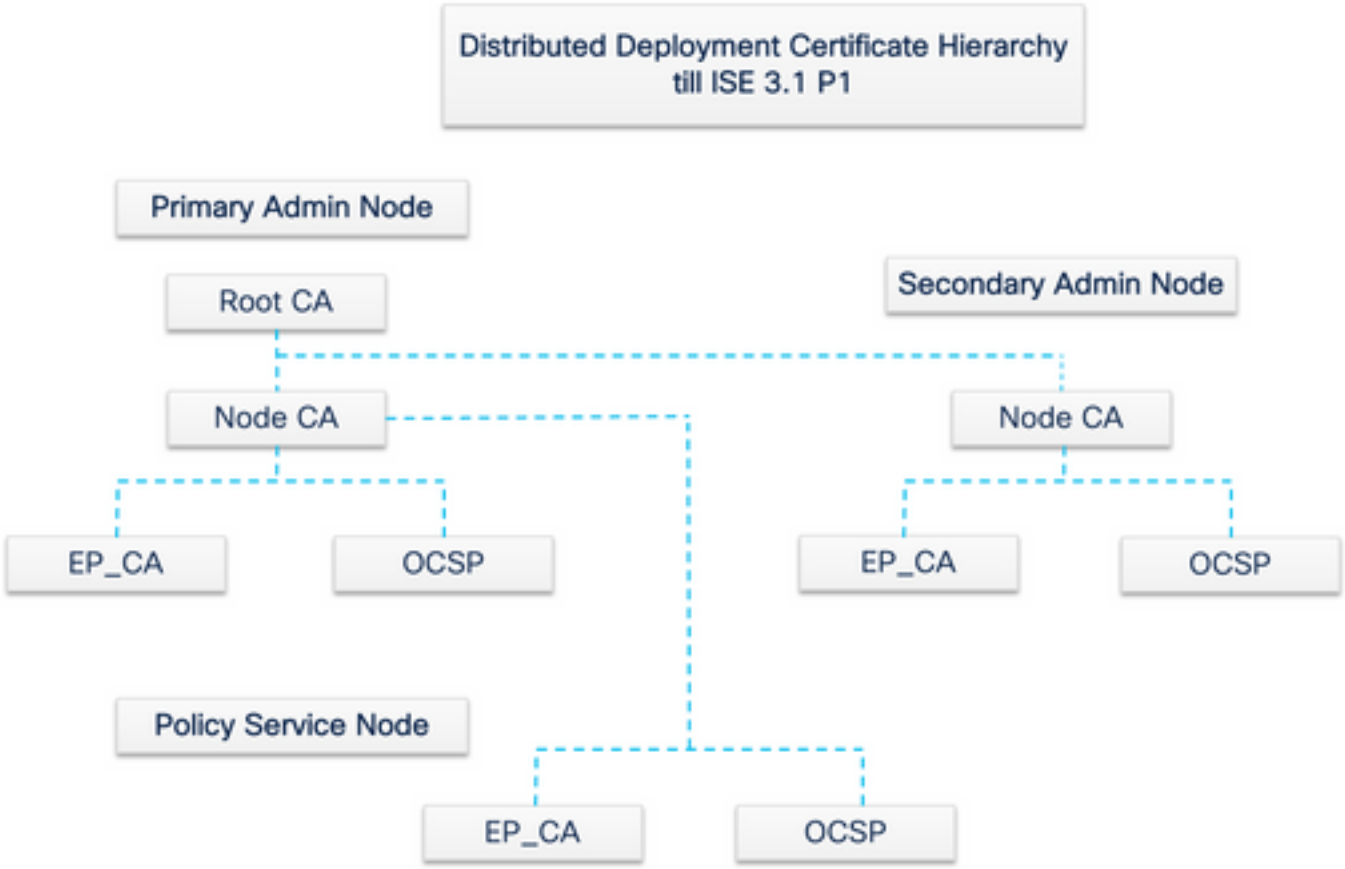
- diese Behörde ausdrücklich einer anderen Stelle zuweisen".

"Das OCSP-Antwortsignaturzertifikat MUSS direkt von der Zertifizierungsstelle ausgestellt werden, die in der Anforderung identifiziert wurde. "

"Das System (vertraut) auf OCSP-Antworten MUSS ein Delegationszertifikat erkennen, das von der Zertifizierungsstelle ausgestellt wurde, die das betreffende Zertifikat ausgestellt hat, nur, wenn

das Delegationszertifikat und das (die) auf Widerruf überprüfte (n) Zertifikat mit demselben Schlüssel signiert wurden."

Um den zuvor genannten RFC-Standard zu erfüllen, wird die Zertifikathierarchie für das OCSP-Responder-Zertifikat in der ISE geändert. Das OCSP-Responder-Zertifikat wird jetzt von der Endpunkt-Sub-CA desselben Knotens anstatt von der Knoten-CA in PAN ausgestellt.



Registrierung über den Secure Transport (EST)-Service

Das Konzept der Public-Key-Infrastruktur (PKI) besteht schon seit langem. Die PKI authentifiziert die Identität von Benutzern und Geräten mittels signierter Public-Key-Paare in Form digitaler Zertifikate. Die Registrierung für Secure Transport (EST) ist ein Protokoll, das diese Zertifikate bereitstellt. Der EST-Dienst definiert, wie die Zertifikatsregistrierung für Clients durchgeführt wird, die die Zertifikatsverwaltung über die kryptografische Nachrichtensyntax (Certificate Management over Cryptographic Message Syntax, CMC) über eine sichere Übertragung verwenden. Laut IETF beschreibt "EST ein einfaches, aber funktionelles Zertifikatsverwaltungsprotokoll, das auf Public Key Infrastructure (PKI)-Clients abzielt, die Client-Zertifikate und zugehörige Zertifizierungsstellen (Certification Authority, CA)-Zertifikate erwerben müssen. Sie unterstützt auch clientgenerierte öffentliche/private Schlüsselpaare sowie von der Zertifizierungsstelle generierte Schlüsselpaare."

EST-Anwendungsfälle

Das EST-Protokoll kann verwendet werden:

- Registrierung von Netzwerkgeräten mittels sicherer, eindeutiger Geräteidentität
- Für BYOD-Lösungen

Warum EST?

Sowohl das EST- als auch das SCEP-Protokoll adressieren die Zertifikatbereitstellung. EST ist ein Nachfolger des Simple Certificate Enrollment Protocol (SCEP). Aufgrund seiner Einfachheit ist SCEP seit vielen Jahren das De-facto-Protokoll bei der Zertifikatbereitstellung. Die Verwendung von EST über SCEP wird jedoch aus folgenden Gründen empfohlen:

- Verwendung von TLS für den sicheren Transport von Zertifikaten und Nachrichten - In EST kann die Zertifikatsanforderung (Certificate Signing Request, CSR) an einen Anforderer gebunden werden, der bereits vertrauenswürdig und mit TLS authentifiziert ist. Clients können nur für sich selbst ein Zertifikat erhalten. In SCEP wird der CSR durch einen gemeinsamen geheimen Schlüssel zwischen dem Client und der Zertifizierungsstelle authentifiziert. Dies führt zu Sicherheitsbedenken, da Personen mit Zugriff auf den gemeinsamen geheimen Schlüssel Zertifikate für andere Einheiten generieren können.
- Unterstützung für die Registrierung von ECC-signierten Zertifikaten - EST bietet kryptografische Flexibilität. Es unterstützt die elliptische Kurvenkryptographie (ECC). SCEP unterstützt ECC nicht und ist von RSA-Verschlüsselung abhängig. ECC bietet mehr Sicherheit und bessere Leistung als andere kryptographische Algorithmen wie RSA, auch wenn es eine viel kleinere Schlüssellänge verwendet.
- EST unterstützt die automatische Zertifikatneuregistrierung.

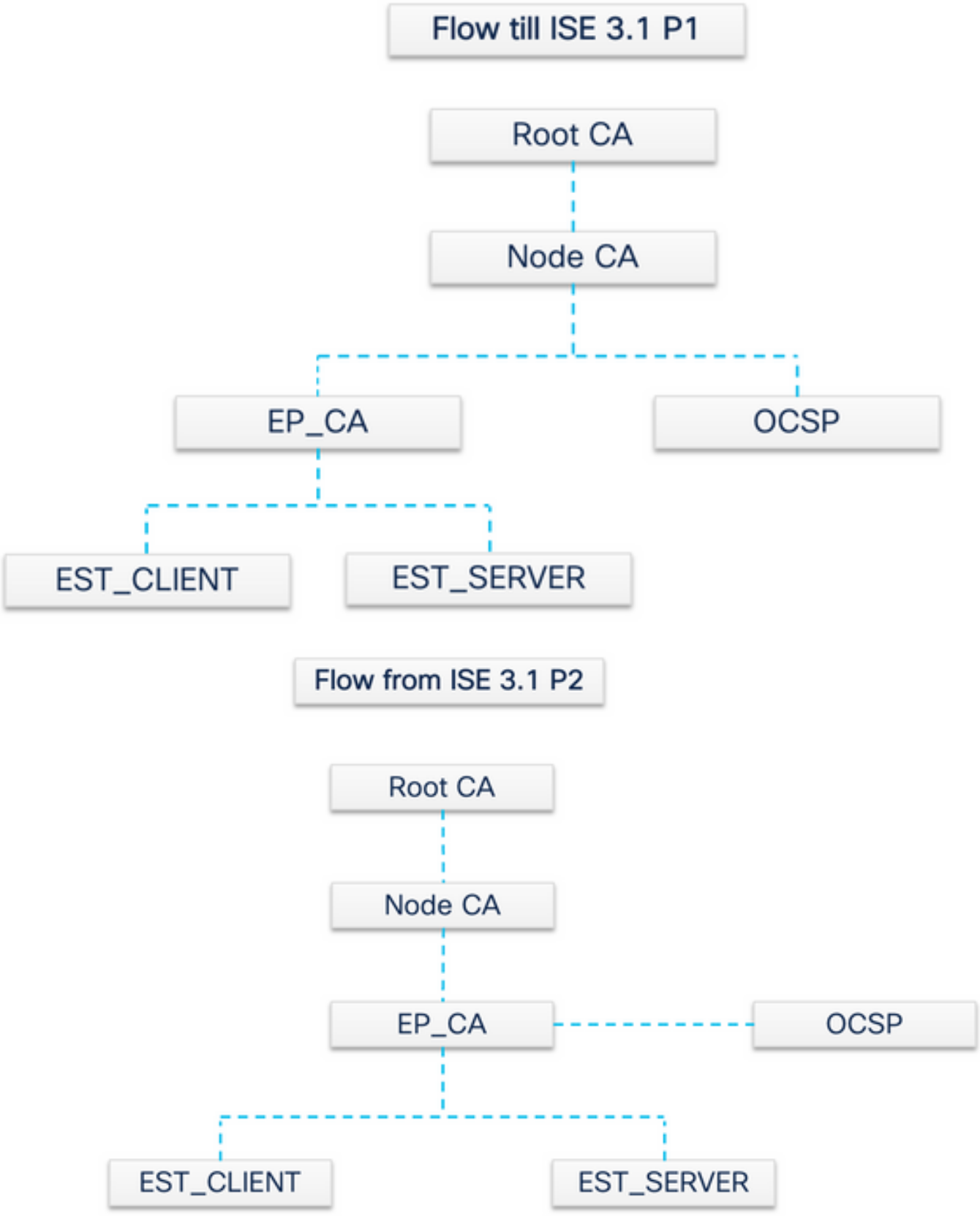
Die bewährte Sicherheit von TLS und die kontinuierliche Verbesserung stellen sicher, dass EST-Transaktionen einen kryptographischen Schutz bieten. Die enge SCEP-Integration mit RSA zum Schutz von Daten führt zu Sicherheitsbedenken im Zuge des technologischen Fortschritts.

EST in der ISE

Um dieses Protokoll zu implementieren, werden ein Client- und ein Servermodul benötigt:

- EST-Client - eingebettet in die reguläre ISE-Tomcat
- EST Server - wird auf einem Open-Source-Webserver namens NGINX bereitgestellt. Dies wird als separater Prozess ausgeführt und hört auf Port 8084 zu.

Die zertifikatbasierte Client- und Serverauthentifizierung wird von EST unterstützt. Die Endpunktzertifizierungsstelle stellt das Zertifikat für den EST-Client und den EST-Server aus. Die EST-Client- und Server-Zertifikate und ihre jeweiligen Schlüssel werden in der NSS DB der ISE-Zertifizierungsstelle gespeichert.



Arten von Anforderungen in ISE EST

Bei jedem Start des EST-Servers erhält er die neueste Kopie aller Zertifizierungsstellenzertifikate vom Zertifizierungsstellenserver und speichert sie. Anschließend kann der EST-Client eine CA-Zertifikatanforderung durchführen, um die gesamte Kette von diesem EST-Server abzurufen. Bevor ein EST-Client eine einfache Registrierungsanforderung stellt, muss er zuerst die

Zertifizierungsstellenzertifikatanforderung ausstellen.

CA Certificates Request (basierend auf RFC 7030)

1. Der EST-Client fordert eine Kopie der aktuellen Zertifizierungsstellenzertifikate an.
2. HTTPS-GET-Nachricht mit dem Betriebspfadwert von /cacerts.

- Dieser Vorgang wird vor allen anderen EST-Anforderungen ausgeführt.
- Alle 5 Minuten wird eine Anforderung gestellt, eine Kopie der aktuellsten Zertifizierungsstellenzertifikate zu erhalten.
- Der EST-Server darf keine Client-Authentifizierung erfordern.

Bei der zweiten Anforderung handelt es sich um eine einfache Registrierungsanforderung, für die eine Authentifizierung zwischen dem EST-Client und dem EST-Server erforderlich ist. Dies geschieht jedes Mal, wenn ein Endpunkt eine Verbindung mit der ISE herstellt und eine Zertifikatsanforderung erstellt.

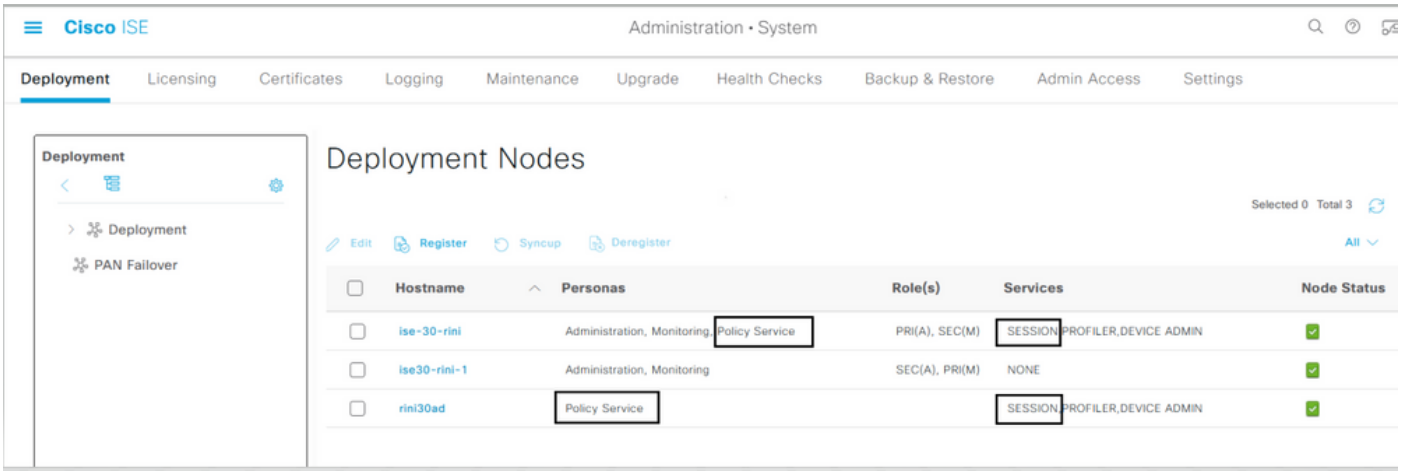
Einfache Registrierungsanfrage (basierend auf RFC 7030)

1. Der EST-Client fordert ein Zertifikat vom EST-Server an.
2. HTTPS-POST-Nachricht mit dem Betriebspfadwert /simpleenroll.

- Der EST-Client bettet die PKCS#10-Anforderung in diesen Anruf ein, der an die ISE gesendet wird.
- Der EST-Server muss den Client authentifizieren.

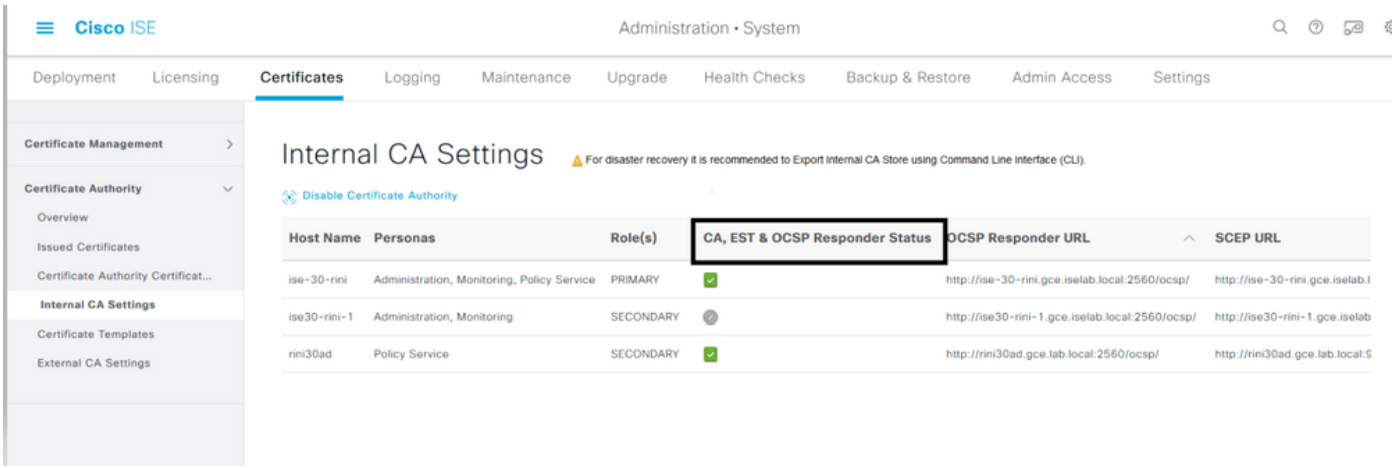
EST- und CA-Dienststatus

CA- und EST-Dienste können nur auf einem Richtliniendienstknoten ausgeführt werden, auf dem Sitzungsdienste aktiviert sind. Um Sitzungsdienste auf einem Knoten zu aktivieren, navigieren Sie zu Administration > System > Deployment . Wählen Sie den Serverhostnamen aus, auf dem die Sitzungsdienste aktiviert werden sollen, und klicken Sie auf Edit . Aktivieren Sie das **Enable Session Services** Kontrollkästchen unter "Policy Service persona".



Auf GUI angezeigter Status

Der EST-Dienststatus ist an den ISE-CA-Dienststatus auf der ISE gebunden. Wenn der CA-Dienst aktiv ist, ist der EST-Dienst aktiv, und wenn der CA-Dienst inaktiv ist, ist auch der EST-Dienst inaktiv.



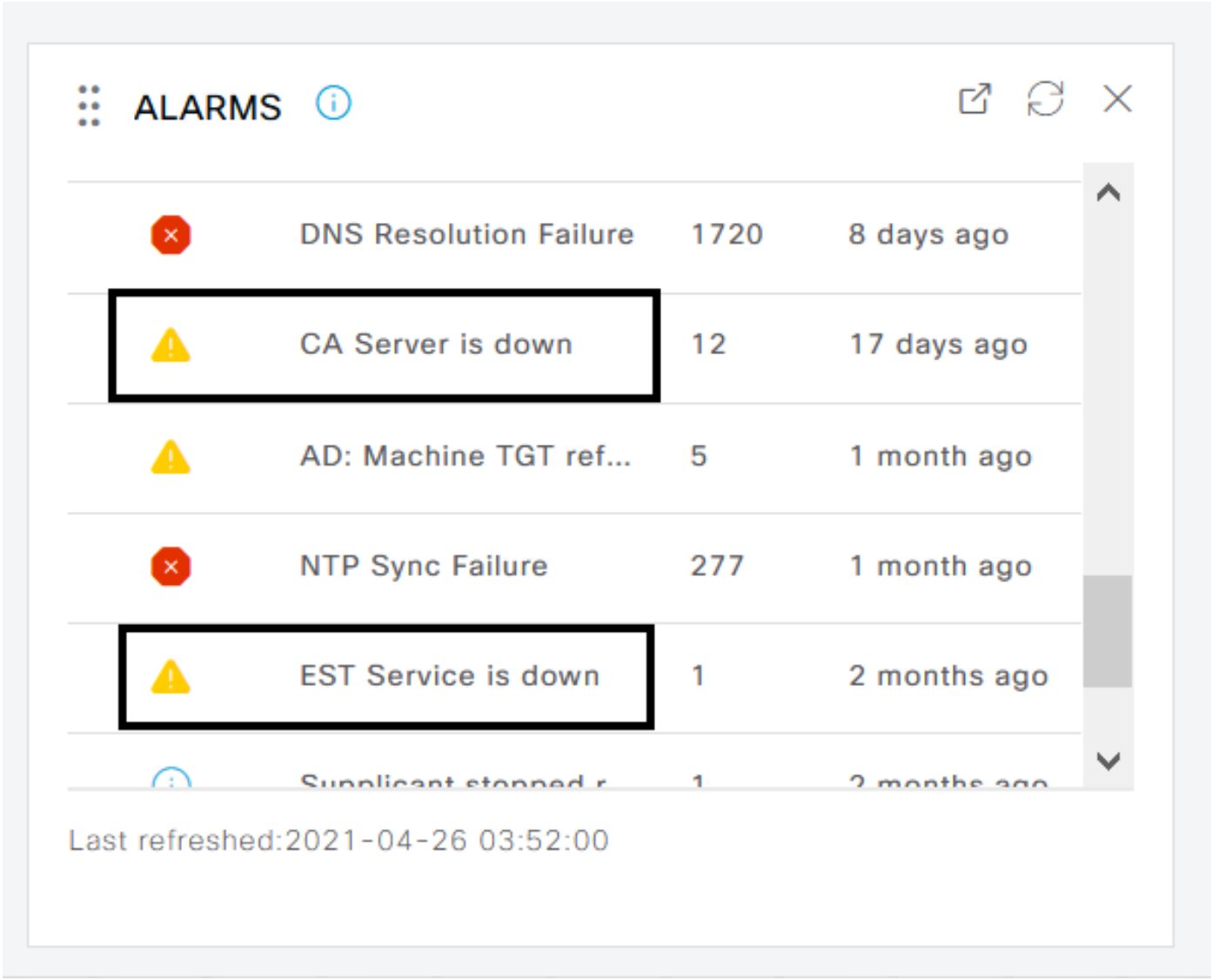
Auf CLI angezeigter Status

```
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
```

Alarme auf Dashboard

Der Alarm wird im ISE-Dashboard angezeigt, wenn die EST- und CA-Services ausfallen.



Auswirkungen, wenn CA- und EST-Services nicht ausgeführt werden

- EST-Client/cacerts-Anruffehler kann auftreten, wenn EST Server ausfällt. Der /cacerts Anruffehler kann auch auftreten, wenn die Zertifikatzertifizierungskette der EST-Zertifizierungsstelle unvollständig ist.

-

  Anmeldungsanforderungen für ECC-basierte Endpunktzertifikate sind fehlgeschlagen.

- Wenn einer der beiden vorherigen Fehler auftritt, wird der BYOD-Fluss unterbrochen.
- Es können Warnmeldungen zu Verbindungsfehlern in der Warteschlange generiert werden.

Fehlerbehebung

Wenn der BYOD-Fluss mit dem EST-Protokoll nicht ordnungsgemäß funktioniert, überprüfen Sie die folgenden Bedingungen:

- Zertifikatskette der Zertifizierungsstellenunterzertifizierung für Zertifikatdienste-Endpunkt ist abgeschlossen. So überprüfen Sie, ob die Zertifikatskette vollständig ist:

  1. Navigieren Sie zu Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates .

     - Aktivieren Sie das Kontrollkästchen neben dem Zertifikat, und klicken Sie auf **Anzeigen**, um ein bestimmtes Zertifikat zu überprüfen.

- Stellen Sie sicher, dass die CA- und EST-Dienste betriebsbereit sind. Wenn die Dienste nicht ausgeführt werden, navigieren Sie zu Administration > System > Certificates > Certificate Authority > Internal CA Settings, um den CA-Dienst zu aktivieren.

- Wenn ein Upgrade durchgeführt wurde, ersetzen Sie nach dem Upgrade die ISE-Stammzertifizierungsstellenkette. Gehen Sie dazu folgendermaßen vor:

  1. Wählen Sie Administration > System > Certificates > Certificate Management > Certificate Signing Requests .

- Klicken Sie auf .Generate Certificate Signing Requests (CSR)

- Wählen Sie ISE Root CA in derCertificate(s) will be used for Dropdown-Liste eine Option aus.

- Klicken Sie auf .Replace ISE Root CA Certificate Chain

- Hilfreiches Debugging, das aktiviert werden kann, um die Protokolle zu überprüfen: est , provisioning , ca-service und ca-service-cert . Weitere Informationen finden Sie unter ise-psc.log , catalina.out , caservice.log , und error.log in den Dateien.

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.