

Informazioni sui servizi ISE Internal Certificate Authority

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Servizio CA \(Certification Authority\)](#)

[Funzionalità ISE CA](#)

[Provisioning dei certificati CA ISE sui nodi dei servizi di amministrazione e policy](#)

[Servizio di registrazione su trasporto sicuro \(EST\)](#)

[Casi di utilizzo EST](#)

[Perché EST?](#)

[EST in ISE](#)

[Tipi di richieste in ISE EST](#)

[Richiesta certificati CA \(in base a RFC 7030\)](#)

[Richiesta di registrazione semplice \(basata su RFC 7030\)](#)

[Stato servizio EST e CA](#)

[Stato visualizzato sulla GUI](#)

[Stato visualizzato sulla CLI](#)

[Avvisi nel dashboard](#)

[Impatto se i servizi CA ed EST non sono in esecuzione](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive il servizio CA e il servizio Enrollment over Secure Transport (EST) presente in Cisco Identity Services Engine (ISE).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE
- Certificati e infrastruttura a chiave pubblica (PKI)
- Protocollo SCEP (Simple Certificate Enrollment Protocol)
- Protocollo OCSP (Online Certificate Status Protocol)

Componenti usati

Le informazioni fornite in questo documento si basano su Identity Services Engine 3.0.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Servizio CA (Certification Authority)

I certificati possono essere autofirmati o firmati digitalmente da un'Autorità di certificazione (CA) esterna. Cisco ISE Internal Certificate Authority (ISE CA) rilascia e gestisce i certificati digitali per gli endpoint da una console centralizzata per consentire ai dipendenti di usare i propri dispositivi personali sulla rete aziendale. Un certificato digitale firmato da CA è considerato uno standard del settore e più sicuro. Il nodo PAN (Policy Administration Node) primario è la CA radice. I PSN (Policy Service Nodes) sono CA subordinate alla PAN primaria.

Funzionalità ISE CA

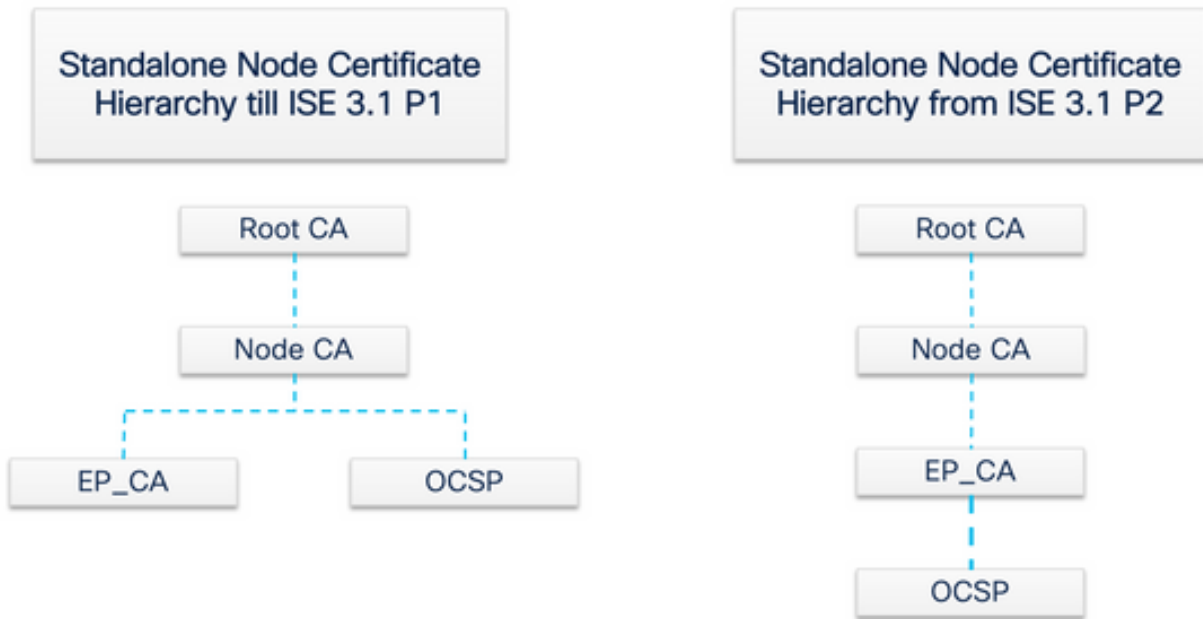
L'ISE CA offre questa funzionalità:

- Rilascio certificato: convalida e firma le richieste di firma del certificato (CSR) per gli endpoint che si connettono alla rete.
- Gestione chiavi: genera e archivia in modo sicuro chiavi e certificati su nodi PAN e PSN.
- Archiviazione certificati: archivia i certificati rilasciati a utenti e dispositivi.
- Supporto OCSP (Online Certificate Status Protocol): fornisce un risponditore OCSP per controllare la validità dei certificati.

Provisioning dei certificati CA ISE sui nodi dei servizi di amministrazione e policy

Dopo l'installazione, a un nodo Cisco ISE vengono forniti un certificato CA radice e un certificato CA nodo per gestire i certificati per gli endpoint.

Quando viene impostata una distribuzione, il nodo designato come PAN (Primary Administration Node) diventa la CA radice. La PAN ha un certificato CA radice e un certificato CA nodo firmato dalla CA radice.



Quando un nodo di amministrazione secondario (SAN) viene registrato nella rete PAN, viene generato un certificato CA del nodo che viene firmato dalla CA radice sul nodo di amministrazione principale.

A qualsiasi PSN (Policy Service Node) registrato con la PAN vengono forniti un'autorità di certificazione dell'endpoint e un certificato OCSP firmato dalla CA del nodo della PAN. I PSN (Policy Service Nodes) sono CA subordinate alla PAN. Quando si utilizza l'autorità di certificazione ISE, l'autorità di certificazione dell'endpoint nel PSN rilascia i certificati agli endpoint che accedono alla rete.



Nota: da ISE 3.1 Patch 2 e ISE 3.2 FCS, OCSP Certificate Hierarchy è stato modificato.

Come da RFC 6960:

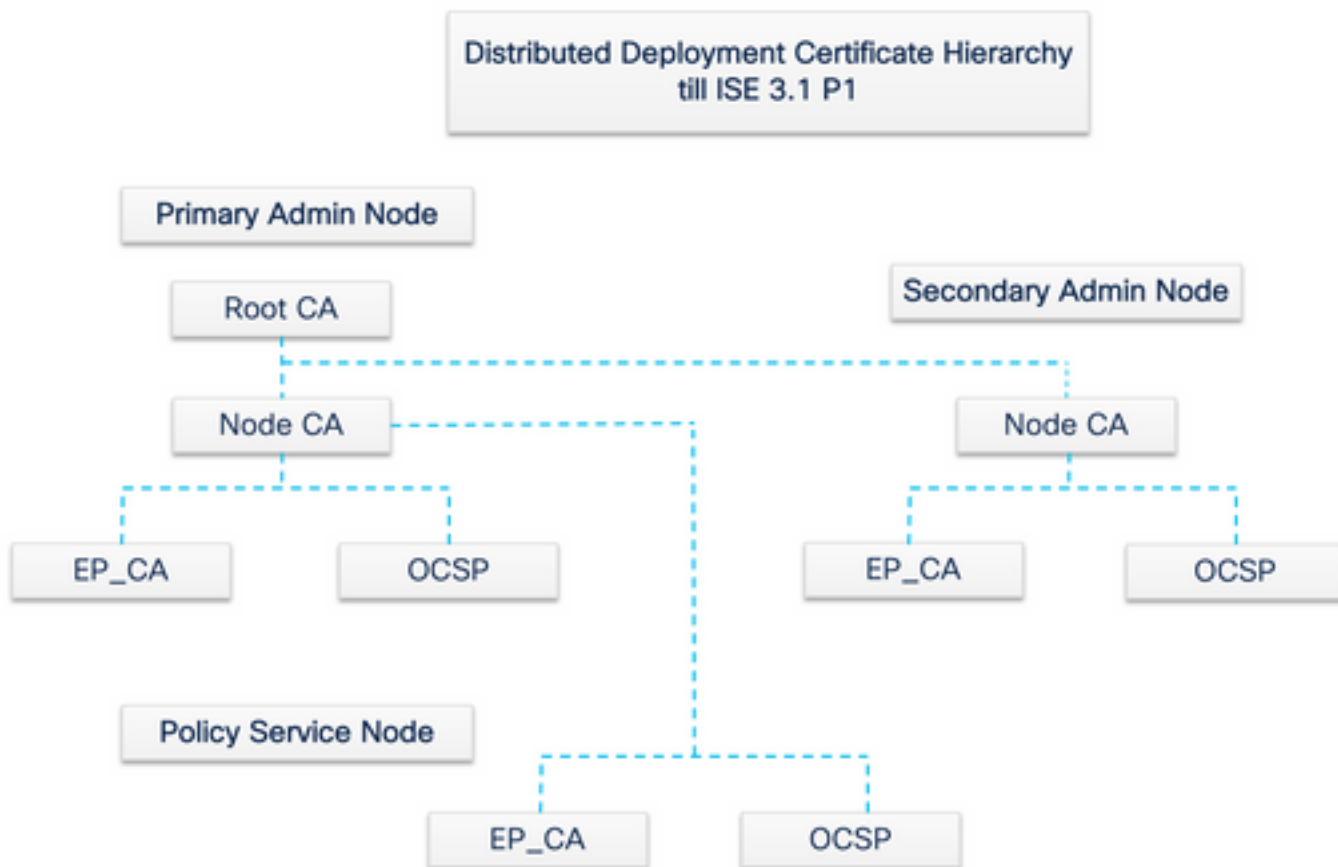
"L'emittente del certificato DEVE effettuare una delle seguenti operazioni:

- firmare le risposte OCSP, oppure
- designare esplicitamente tale autorità ad un altro soggetto"

"Il certificato del firmatario della risposta OCSP DEVE essere rilasciato direttamente dalla CA identificata nella richiesta. "

"Il sistema (si basa) sulle risposte OCSP DEVE riconoscere un certificato di delega come rilasciato dalla CA che ha emesso il certificato in questione solo se il certificato di delega e il certificato (è) controllato per la revoca sono stati firmati dalla stessa chiave."

Per essere conforme allo standard RFC sopra indicato, la gerarchia dei certificati per il certificato risponditore OCSP viene modificata in ISE. Il certificato del risponditore OCSP è ora rilasciato dalla CA secondaria dell'endpoint dello stesso nodo anziché dalla CA del nodo nella rete PAN.



Servizio di registrazione su trasporto sicuro (EST)

Il concetto di infrastruttura a chiave pubblica (PKI) esiste da molto tempo. La PKI autentica l'identità di utenti e dispositivi tramite coppie di chiavi pubbliche firmate sotto forma di certificati digitali. Enrollment over Secure Transport (EST) è un protocollo per fornire questi certificati. Il servizio EST definisce come eseguire la registrazione dei certificati per i client che utilizzano il servizio CMC (Certificate Management over Cryptographic Message Syntax) su un trasporto protetto. In base all'IETF - "EST descrive un protocollo di gestione dei certificati semplice ma funzionale destinato ai client PKI (Public Key Infrastructure) che devono acquisire certificati client e certificati CA (Certification Authority) associati. Supporta inoltre coppie di chiavi pubbliche/private generate dal client, nonché coppie di chiavi generate dalla CA."

Casi di utilizzo EST

Il protocollo EST può essere utilizzato:

- Registrazione di dispositivi di rete tramite Secure Unique Device Identity
- Per soluzioni BYOD

Perché EST?

Sia il protocollo EST che il protocollo SCEP indirizzano il provisioning dei certificati. EST è un successore del protocollo SCEP (Simple Certificate Enrollment Protocol). Grazie alla sua semplicità, SCEP è stato per molti anni il protocollo di fatto per il provisioning dei certificati. Tuttavia, si raccomanda l'uso di EST over SCEP per i seguenti motivi:

- Utilizzo di TLS per il trasporto sicuro di certificati e messaggi - In EST, la richiesta di firma del certificato (CSR) può essere associata a un richiedente già considerato attendibile e autenticato con TLS. I client non possono ottenere un certificato per nessuno tranne se stessi. In SCEP, il CSR viene autenticato da un segreto condiviso tra il client e la CA. Ciò comporta problemi di protezione in quanto gli utenti che hanno accesso al segreto condiviso possono generare certificati per entità diverse da se stessi.
- Supporto per la registrazione di certificati con firma ECC - EST offre agilità di crittografia. Supporta la crittografia a curva ellittica (ECC). SCEP non supporta ECC e dipende dalla crittografia RSA. ECC offre maggiore sicurezza e migliori prestazioni rispetto ad altri algoritmi di crittografia come RSA, anche se utilizza una chiave di dimensioni molto inferiori.
- EST è progettato per supportare la registrazione automatica dei certificati.

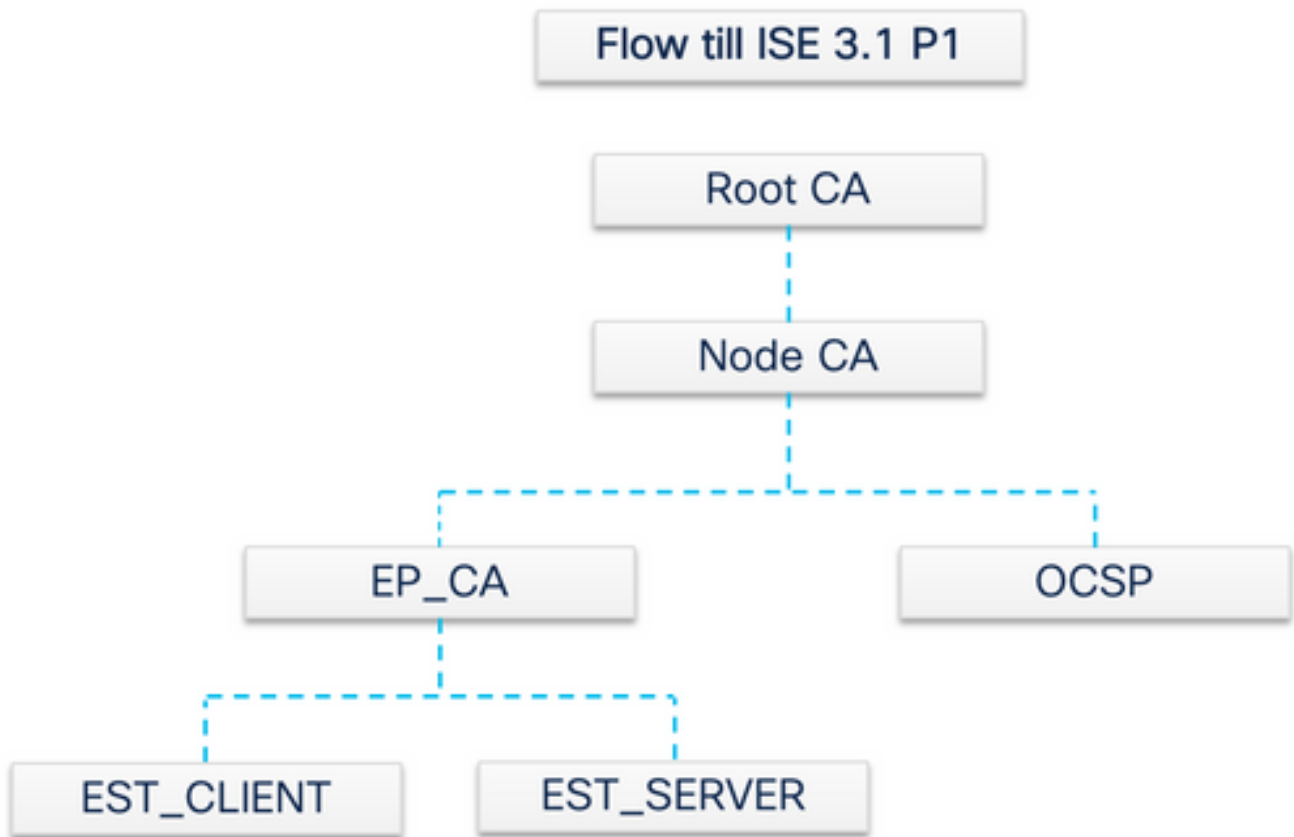
La sicurezza TLS e il continuo miglioramento garantiscono la sicurezza delle transazioni EST in termini di protezione crittografica. La stretta integrazione di SCEP con RSA per la protezione dei dati introduce problemi di sicurezza man mano che la tecnologia avanza.

EST in ISE

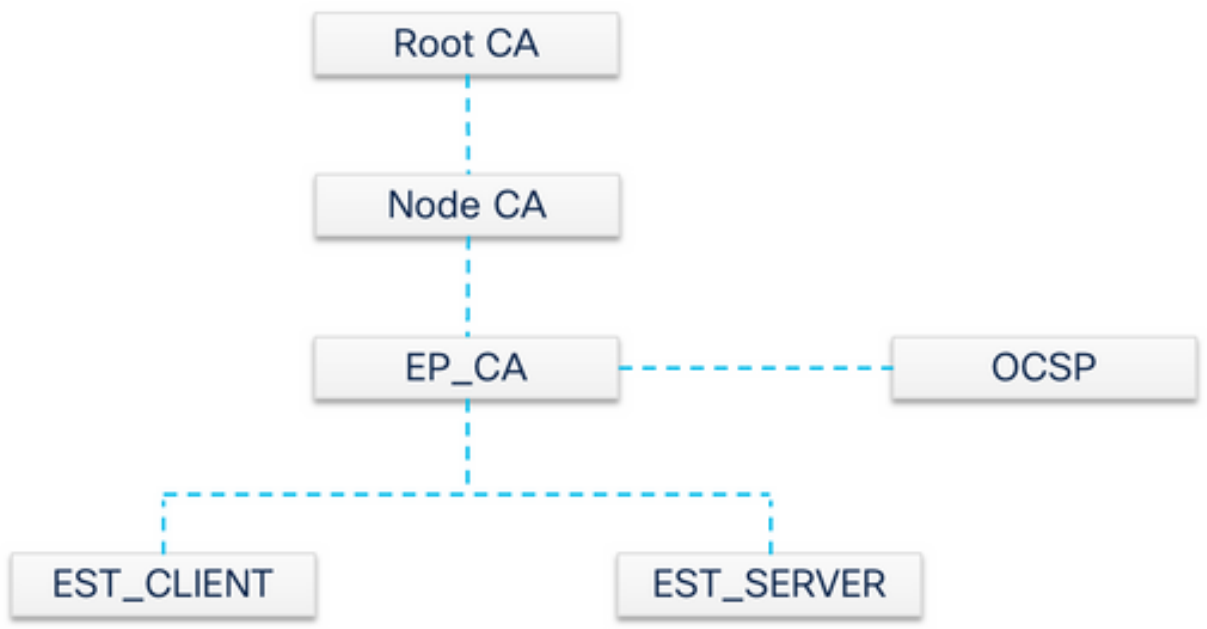
Per implementare questo protocollo, sono necessari un client e un modulo server:

- EST Client: integrato nel tradizionale gatto maschio ISE.
- Server EST: distribuito su un server Web open source denominato NGINX. Viene eseguito come processo separato e resta in ascolto sulla porta 8084.

L'autenticazione client e server basata su certificati è supportata da EST. L'autorità di certificazione dell'endpoint rilascia il certificato per il client EST e il server EST. I certificati EST Client e Server e le rispettive chiavi sono archiviati nel database NSS di ISE CA.



Flow from ISE 3.1 P2



Tipi di richieste in ISE EST

Ogni volta che il server EST viene attivato, ottiene la copia più recente di tutti i certificati CA dal server CA e la archivia. Il client EST può quindi effettuare una richiesta di certificato CA per ottenere l'intera catena da questo server EST. Prima di effettuare una semplice richiesta di registrazione, il client EST deve emettere la richiesta del certificato CA.

Richiesta certificati CA (in base a RFC 7030)

1. Il client EST richiede una copia dei certificati CA correnti.
2. Messaggio GET HTTPS con un valore del percorso operazione di /cacerts.

- Questa operazione viene eseguita prima di qualsiasi altra richiesta EST.
- Ogni 5 minuti viene effettuata una richiesta per ottenere una copia dei certificati CA più aggiornati.
- Il server EST non deve richiedere l'autenticazione del client.

La seconda richiesta è una semplice richiesta di registrazione e richiede l'autenticazione tra il client EST e il server EST. Questo si verifica ogni volta che un endpoint si connette ad ISE ed effettua una richiesta di certificato.

Richiesta di registrazione semplice (basata su RFC 7030)

1. Il client EST richiede un certificato al server EST.
 2. Messaggio HTTPS POST con il valore del percorso dell'operazione /simpleenroll.
- Il client EST incorpora la richiesta PKCS#10 in questa chiamata che viene inviata ad ISE.
 - Il server EST deve autenticare il client.

Stato servizio EST e CA

I servizi CA e EST possono essere eseguiti solo in un nodo di servizio criteri in cui sono abilitati i servizi di sessione. Per abilitare i servizi di sessione in un nodo, passare a Administration > System > Deployment . Selezionare il nome host del server su cui abilitare i servizi di sessione e fare clic su Edit . Selezionare la **Enable Session Services** casella di controllo in Personalità servizio criteri.

The screenshot shows the Cisco ISE Administration console. The 'Deployment' menu is selected, and the 'Deployment Nodes' page is displayed. A table lists three nodes: 'ise-30-rini', 'ise30-rini-1', and 'rini30ad'. The 'Policy Service' and 'SESSION PROFILER, DEVICE ADMIN' services are highlighted with red boxes for each node. The 'Node Status' column shows green checkmarks for all nodes.

Hostname	Personas	Role(s)	Services	Node Status
ise-30-rini	Administration, Monitoring, Policy Service	PRI(A), SEC(M)	SESSION PROFILER, DEVICE ADMIN	✓
ise30-rini-1	Administration, Monitoring	SEC(A), PRI(M)	NONE	✓
rini30ad	Policy Service		SESSION PROFILER, DEVICE ADMIN	✓

Stato visualizzato sulla GUI

Lo stato del servizio EST è collegato allo stato del servizio ISE CA su ISE. Se il servizio CA è attivo, il servizio EST è attivo e se il servizio CA è inattivo, anche il servizio EST è inattivo.

The screenshot shows the 'Internal CA Settings' page in the Cisco ISE Administration console. A table lists three nodes: 'ise-30-rini', 'ise30-rini-1', and 'rini30ad'. The 'CA, EST & OCSP Responder Status' column shows green checkmarks for 'ise-30-rini' and 'rini30ad', and a grey circle with a slash for 'ise30-rini-1'. The 'OCSP Responder URL' and 'SCEP URL' columns are also visible.

Host Name	Personas	Role(s)	CA, EST & OCSP Responder Status	OCSP Responder URL	SCEP URL
ise-30-rini	Administration, Monitoring, Policy Service	PRIMARY	✓	http://ise-30-rini.gce.iselab.local:2560/ocsp/	http://ise-30-rini.gce.iselab.l
ise30-rini-1	Administration, Monitoring	SECONDARY	⊘	http://ise30-rini-1.gce.iselab.local:2560/ocsp/	http://ise30-rini-1.gce.iselab
rini30ad	Policy Service	SECONDARY	✓	http://rini30ad.gce.lab.local:2560/ocsp/	http://rini30ad.gce.lab.local:5

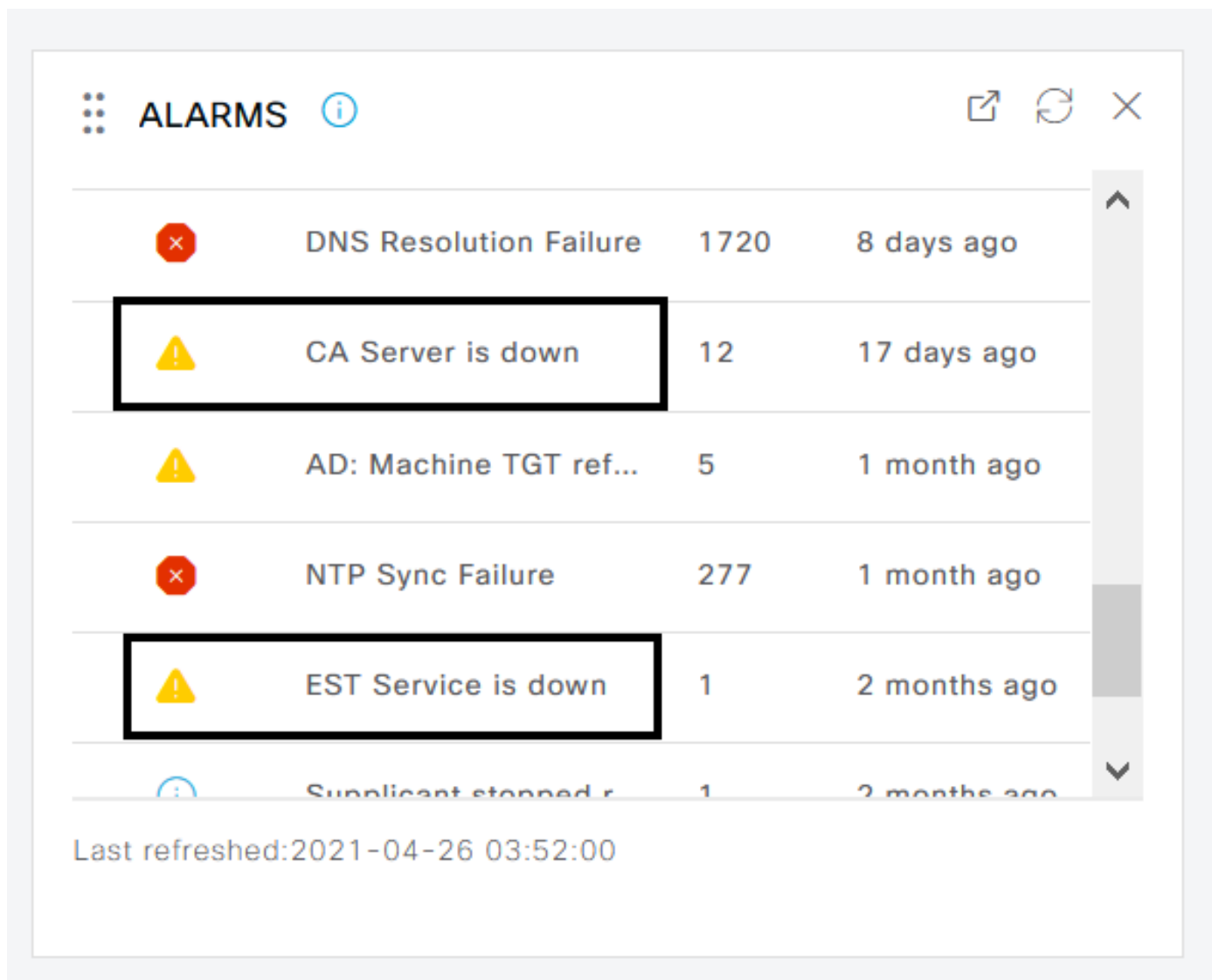
Stato visualizzato sulla CLI

```
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	

Avvisi nel dashboard

L'allarme viene visualizzato sul dashboard ISE se i servizi EST e CA non sono attivi.



The screenshot shows the 'ALARMS' section of the ISE dashboard. It contains a table of active alarms with the following data:

Icon	Alarm Name	Count	Time
✖	DNS Resolution Failure	1720	8 days ago
⚠	CA Server is down	12	17 days ago
⚠	AD: Machine TGT ref...	5	1 month ago
✖	NTP Sync Failure	277	1 month ago
⚠	EST Service is down	1	2 months ago
ⓘ	Suppliment stopped r	1	2 months ago

At the bottom of the dashboard, it states: 'Last refreshed: 2021-04-26 03:52:00'.

Impatto se i servizi CA ed EST non sono in esecuzione

- L'errore di chiamata al client/cacerts EST può verificarsi quando il server EST non è attivo. L'errore della/cacerts chiamata può inoltre verificarsi se la catena di certificati CA della catena di CA EST è incompleta.

•

Richieste di registrazione certificato endpoint basato su ECC non riuscite.

- Il flusso BYOD si interrompe se si verifica uno dei due errori precedenti.
- È possibile generare avvisi di errore di collegamento coda.

Risoluzione dei problemi

Se il flusso BYOD con il protocollo EST non funziona correttamente, verificare le seguenti condizioni:

-

Catena di certificati CA secondaria endpoint Servizi certificati completata. Per verificare se la catena di certificati è completa:

- 1.

Passare a Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates .

-

Selezionare la casella di controllo accanto al certificato e fare clic su **Visualizza** per controllare un determinato certificato.

-

Verificare che i servizi CA ed EST siano attivi e in esecuzione. Se i servizi non sono in esecuzione, passare a Administration > System > Certificates > Certificate Authority > Internal CA Settings per abilitare il servizio CA.

-

Se è stato eseguito un aggiornamento, sostituire la catena di certificati della CA radice ISE dopo l'aggiornamento. A tal fine:

- 1.

Scegliere Administration > System > Certificates > Certificate Management > Certificate Signing Requests .

-

Fare clic su `.Generate Certificate Signing Requests (CSR)`

-

Selezionare ISE Root CA nell'elenco a discesa Certificate(s) will be used for

-

Fare clic su `.Replace ISE Root CA Certificate Chain`

- Il debug che può essere abilitato per controllare i log include `est` , `provisioning ca-service` e `ca-service-cert` . Fare riferimento ai file `ise-psc.log` , `catalina.out` , `caservice.log` , `error.log` .

Informazioni correlate

- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).