瞭解ISE內部證書頒發機構服務

目錄

簡介

本文檔介紹思科身份服務引擎(ISE)中的CA服務和透過安全傳輸(EST)註冊(Enrollment over Secure Transport， EST)服務。

必要條件

需求

思科建議您瞭解以下主題：

- ISE
- 憑證和公開金鑰基礎架構(PKI)
- 簡單憑證註冊通訊協定(SCEP)
- 線上憑證狀態通訊協定(OCSP)

採用元件

本檔案中的資訊是根據Identity Services Engine 3.0。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

憑證授權單位(CA)服務

證書可以由外部證書頒發機構(CA)自簽名或數位簽章。思科ISE內部證書授權(ISE CA)從集中控制檯為終端頒發和管理數位證書，以允許員工在公司網路上使用其個人裝置。 CA簽署的數位憑證被認為是一種業界標準且更安全。主策略管理節點(PAN)是根CA。策略服務節點(PSN)是從屬CA到主PAN。

ISE CA功能

ISE CA提供以下功能：

- 證書頒發：驗證並簽署連線到網路的終端的證書簽名請求(CSR)。
- 金鑰管理：在PAN和PSN節點上生成並安全地儲存金鑰和證書。
- 憑證儲存：儲存發行給使用者和裝置的憑證。
- 線上憑證狀態通訊協定(OCSP)支援：提供OCSP回應方以檢查憑證的有效性。

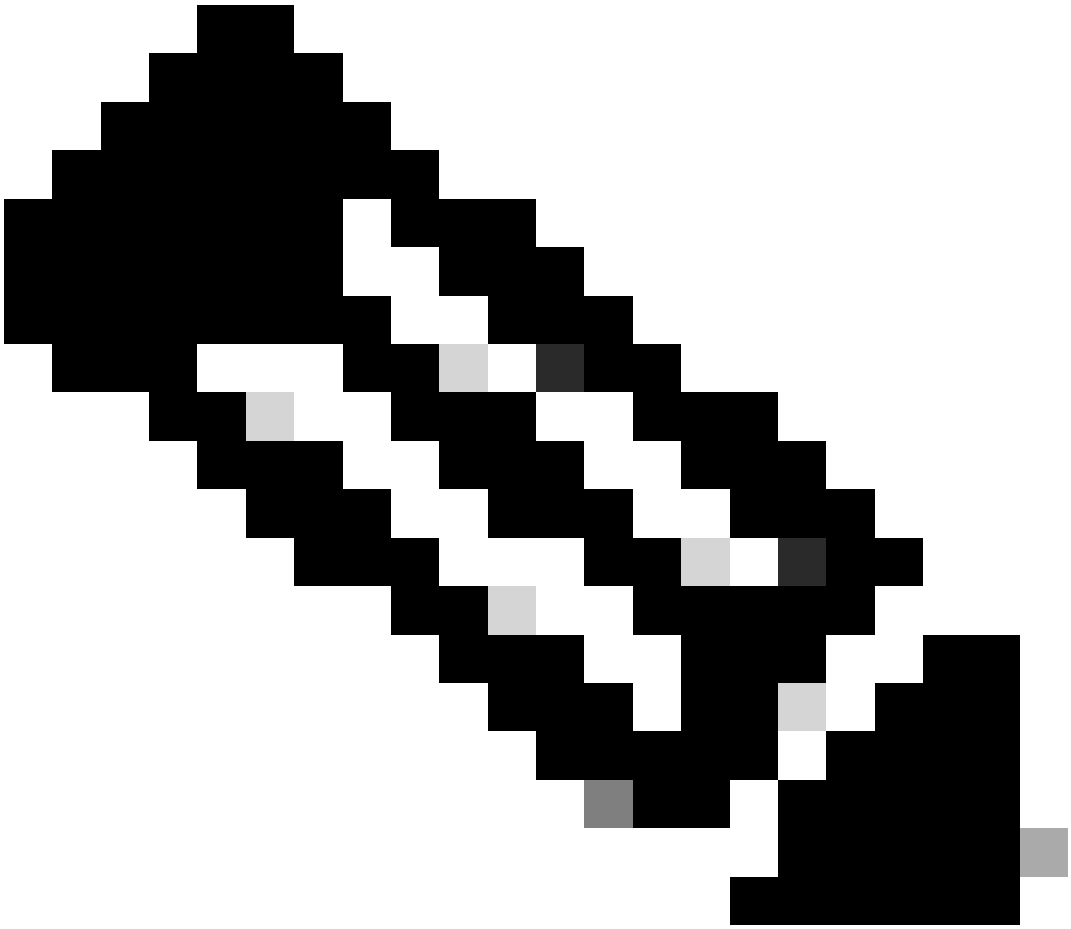
在管理和策略服務節點上調配的ISE CA證書

安裝後，思科ISE節點調配根CA證書和節點CA證書來管理終端的證書。

設定部署後，指定為主要管理節點(PAN)的節點會成為根CA。PAN具有根CA證書和根CA簽署的節點CA證書。

當輔助管理節點(SAN)註冊到PAN時，生成節點CA證書，並由主管理節點上的根CA簽名。

向PAN註冊的所有策略服務節點(PSN)都調配了終端CA和由PAN的節點CA簽名的OCSP證書。策略服務節點(PSN)是從CA到PAN。使用ISE CA時，PSN上的終端CA向訪問網路的終端頒發證書。



注意：從ISE 3.1修補2和ISE 3.2 FCS，OCSP證書層次結構已更改。

根據RFC 6960：

「證書頒發者必須執行以下操作之一：

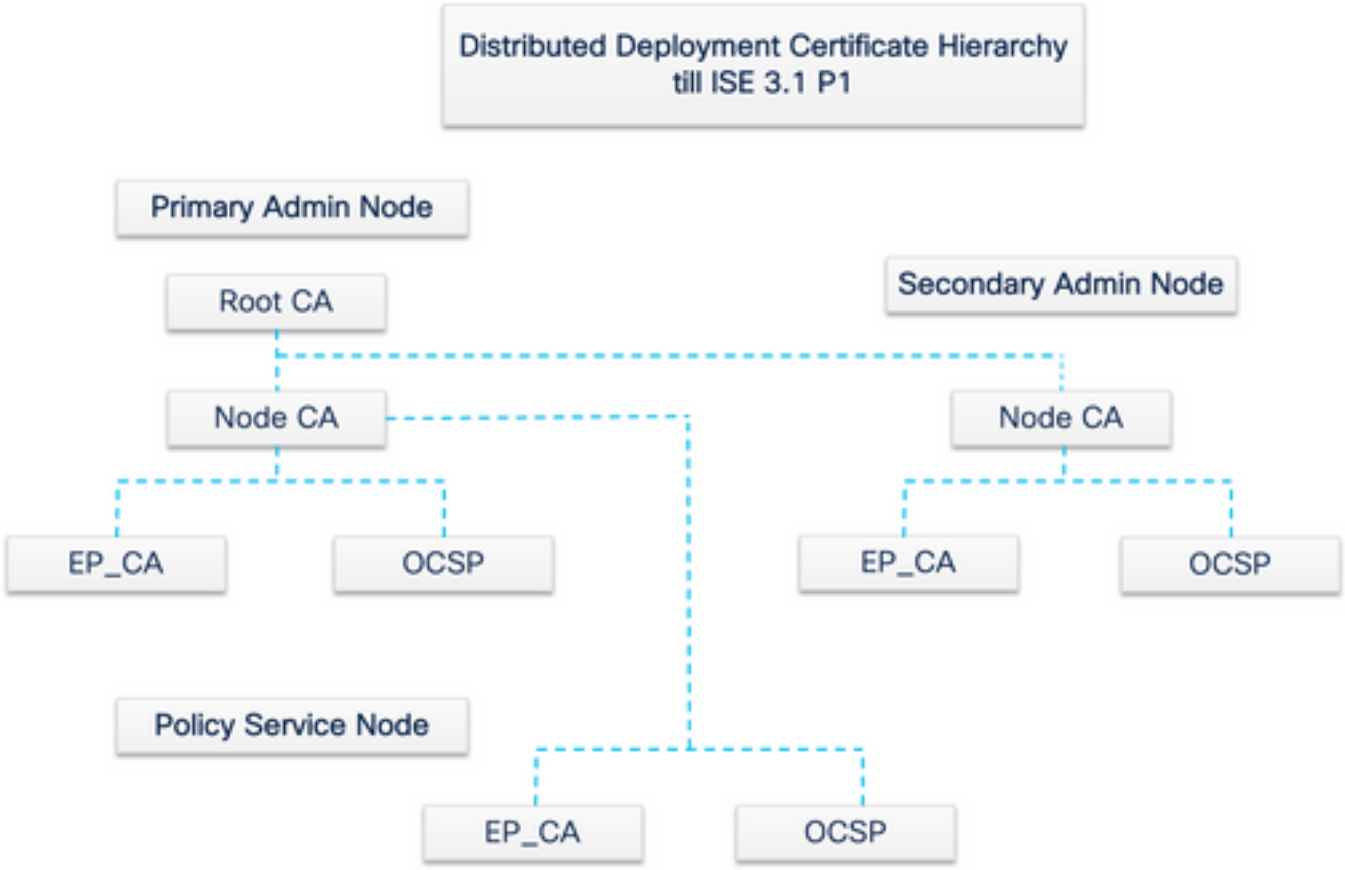
- 對OCSP響應本身進行簽名，或

- 明確指定這個許可權給另一個實體」

「OCSP響應簽名者證書必須由請求中標識的CA直接頒發。 "

系統（依賴）的OCSP響應必須辨識由簽發相關證書的CA頒發的委託證書，前提是委託證書和檢查撤銷的證書(is)由同一金鑰簽署。

為了符合前面提到的RFC標準，在ISE中更改OCSP響應方證書的證書層次結構。OCSP響應方證書現在由同一節點的終端子CA頒發，而不是PAN中的節點CA。



透過安全傳輸(EST)服務註冊

公開金鑰基礎架構(PKI)的概念已經存在很長時間了。PKI透過數位證書形式的簽名公鑰對來驗證使用者和裝置的身份。安全傳輸註冊(EST)是提供這些憑證的通訊協定。EST服務定義如何在安全傳輸上為使用加密消息語法(CMC)的證書管理的客戶端執行證書註冊。根據IETF -「EST描述的是一種簡單但功能正常的證書管理協定，它面向需要獲取客戶端證書和相關證書頒發機構(CA)證書的公鑰基礎設施(PKI)客戶端。它還支援客戶端生成的公鑰/私鑰對，以及CA生成的金鑰對。」

EST使用案例

可以使用EST協定：

- 透過安全唯一裝置身份註冊網路裝置
- 自帶裝置解決方案

為什麼選擇EST？

EST和SCEP協定都提供地址證書。EST是簡單證書註冊協定(SCEP)的後繼協定。由於其簡便性，SCEP多年來一直是證書調配的實際協定。但是，出於以下原因，建議使用EST over SCEP：

- 使用TLS安全傳輸憑證和訊息-在EST中，憑證簽署請求(CSR)可以繫結到已使用TLS信任和驗證的請求者。使用者端無法取得除了他們自己之外的任何人的憑證。在SCEP中，CSR透過客戶端和CA之間的共用金鑰進行身份驗證。這會帶來安全隱患，因為有權訪問共用金鑰的人可以為自身以外的實體生成證書。
- 支援ECC簽名證書的註冊- EST提供加密靈活性。它支援橢圓曲線加密(ECC)。SCEP不支援ECC並依賴RSA加密。ECC比RSA等其他密碼編譯演演算法提供更高的安全性和更佳的效能，即使它使用的金鑰大小要小得多。
- EST用於支援自動證書重新註冊。

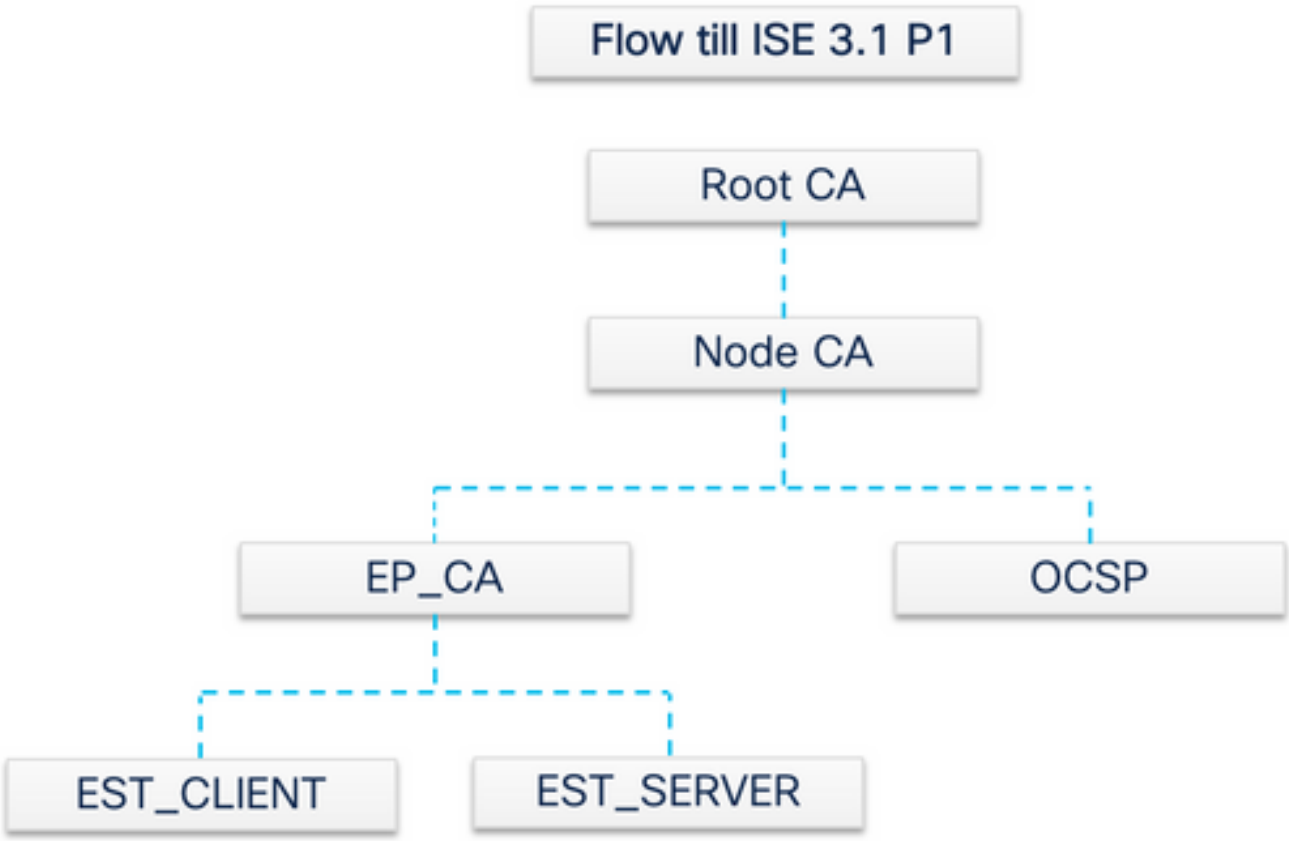
TLS經過驗證的安全性和持續改進有助於確保EST事務在加密保護方面是安全的。SCEP與RSA緊密整合以保護資料，隨著技術的進步，帶來了安全問題。

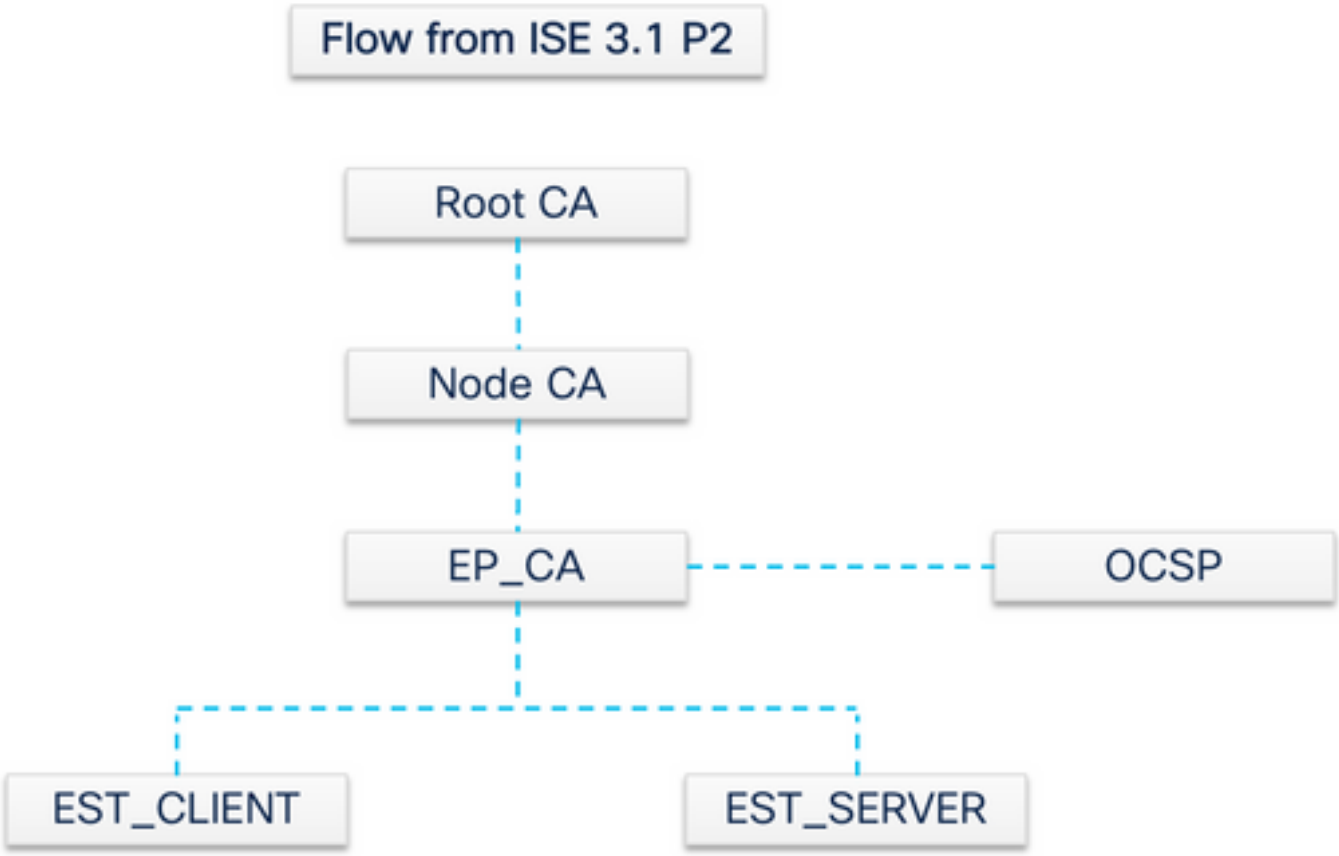
在ISE中設定

要實施此協定，需要客戶端和伺服器模組：

- EST客戶端-嵌入在常規ISE tomcat中。
- EST伺服器-部署在名為NGINX的開放源Web伺服器上。此進程作為單獨的進程運行，並在埠8084上偵聽。

EST支援憑證型使用者端和伺服器驗證。終端CA為EST客戶端和EST伺服器頒發證書。EST客戶端和伺服器證書及其各自的金鑰儲存在ISE CA的NSS DB中。





ISE EST中的請求型別

每當EST伺服器啟動時，它從CA伺服器獲取所有CA證書的最新副本並將其儲存。然後，EST客戶端可以發出CA證書請求，以從此EST伺服器獲取整個證書鏈。在發出簡單註冊請求之前，EST客戶端必須首先發出CA證書請求。

CA憑證要求（根據RFC 7030）

1. EST客戶端請求當前CA證書的副本。
2. 操作路徑值為HTTPS GET消息 /cacerts.

- 此作業會在任何其他EST要求之前執行。
- 每5分鐘會請求獲取最新CA證書的副本。
- EST伺服器不得要求客戶端身份驗證。

第二個請求是一個簡單的註冊請求，它需要在EST客戶端和EST伺服器之間進行身份驗證。每次終端連線到ISE並發出證書請求時都會發生這種情況。

簡單註冊請求（基於RFC 7030）

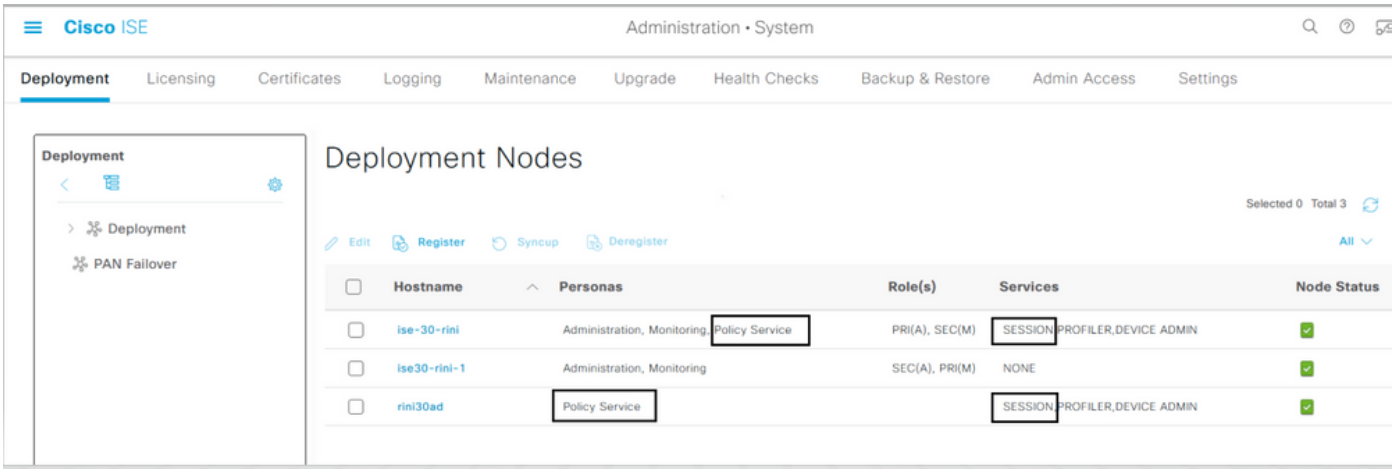
1. EST客戶端向EST伺服器請求證書。

2. 操作路徑值為/simpleenroll的HTTPS POST消息。

   - EST客戶端在此呼叫中嵌入PKCS#10請求，該呼叫將傳送到ISE。
   - EST伺服器必須對客戶端進行身份驗證。

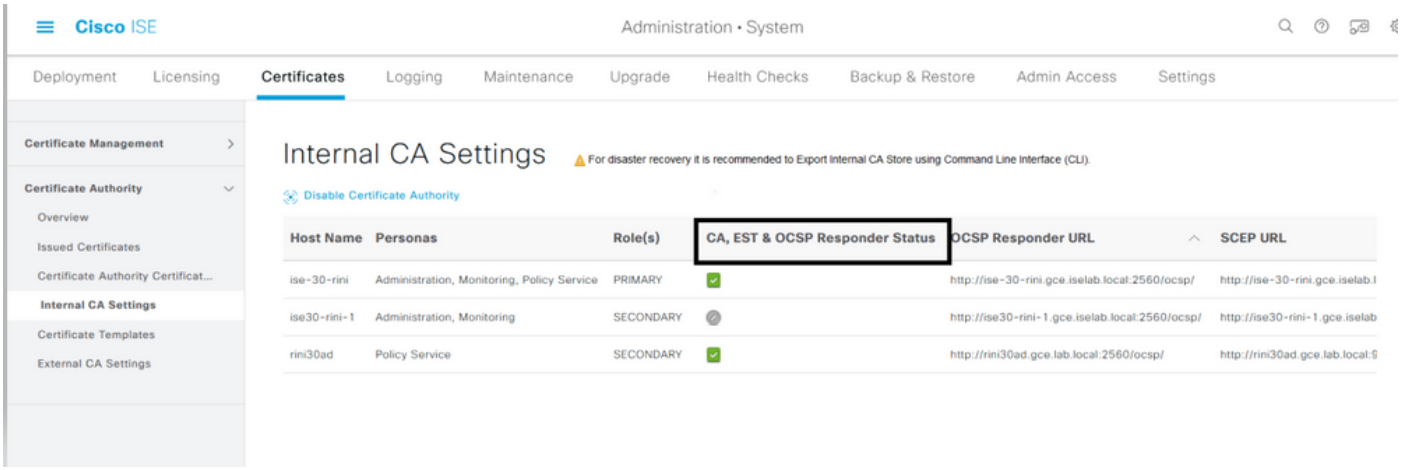
EST和CA服務狀態

CA和EST服務只能在啟用了會話服務的策略服務節點上運行。要在節點上啟用會話服務，請導航到Administration > System > Deployment。選擇需要啟用會話服務的伺服器主機名，然後按一下Edit。選中Policy Service persona下的 **Enable Session Services** 覈取方塊。



GUI上顯示的狀態

EST服務狀態與ISE上的ISE CA服務狀態關聯。如果CA服務啟動，則EST服務啟動；如果CA服務關閉，EST服務也關閉。



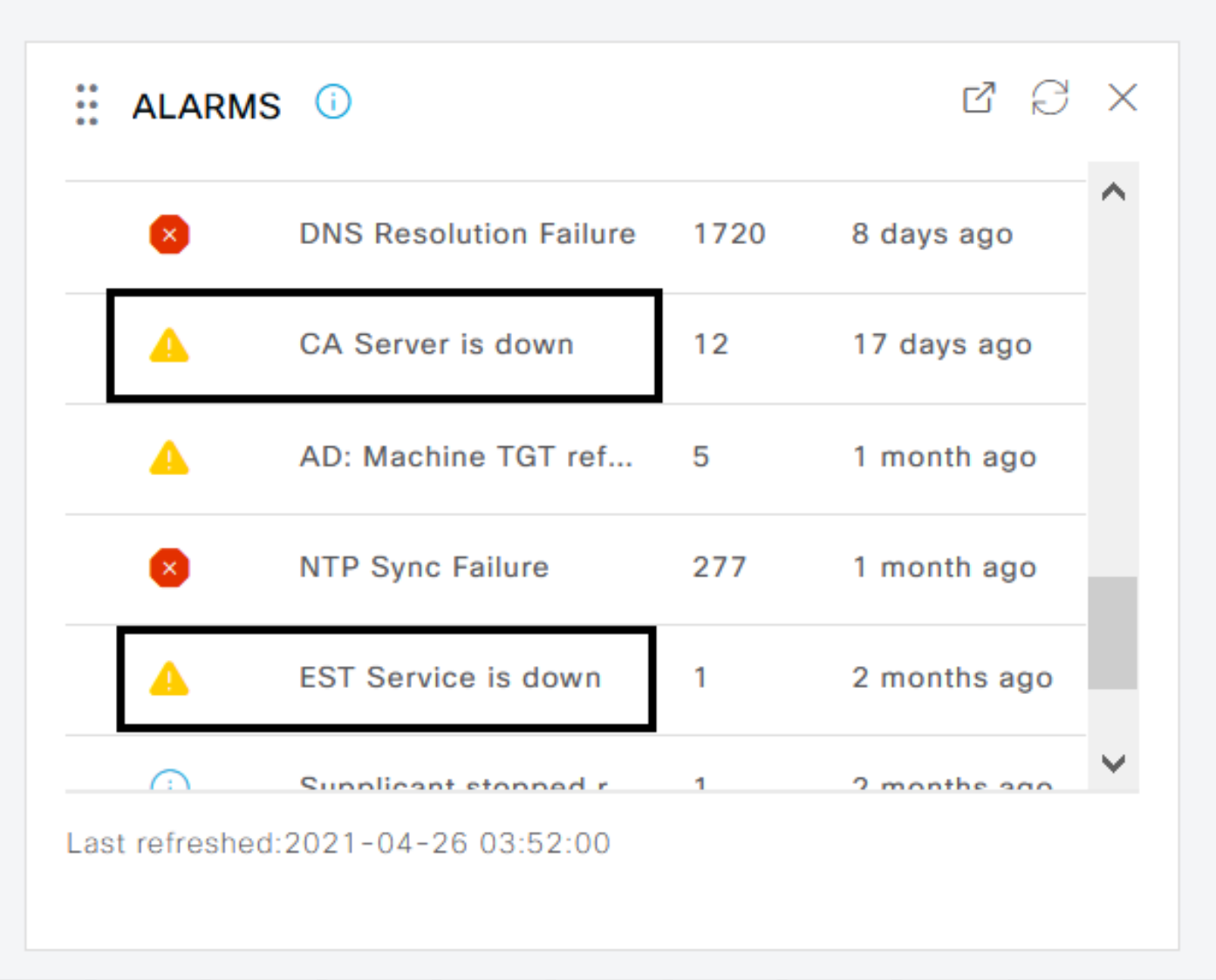
CLI上顯示的狀態

```
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
```

儀表板上的警報

如果EST和CA服務關閉，ISE控制台上將顯示警報。



如果CA和EST服務未運行的影響

- 當EST伺服器發生故障時，可能會發生EST Client/cacerts（使用者端）呼叫故障。如果EST CA鏈證書CA鏈不完整，/cacerts呼叫失敗也會發生。
- 基於ECC的端點證書註冊請求失敗。
- 如果發生前兩個故障之一，BYOD流將中斷。
- 可產生佇列連結錯誤警報。

疑難排解

如果使用EST協定的BYOD流無法正常工作，請檢查以下條件：

- 憑證服務端點子CA憑證鏈結已完成。若要檢查憑證鏈結是否完整：

  1. 導航到Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates。

     - 選中證書旁邊的覈取方塊並按一下**View**以檢查特定證書。

- 確保CA和EST服務已啟動並運行。如果服務未運行，請導航到Administration > System > Certificates > Certificate Authority > Internal CA Settings以啟用CA服務。

- 如果已執行升級，請在升級後替換ISE根CA證書鏈。為此：

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

     - 按一下Generate Certificate Signing Requests (CSR)。

-

在下拉選單中選擇ISE Root CACertificate(s) will be used for

-

按一下Replace ISE Root CA Certificate Chain。

- 可以啟用用來檢查日誌的有用調試包括est、provisioning、ca-service和ca-service-cert。請參閱ise-psc.log、catalina.out、caservice.log , 和error.log檔案。

相關資訊

- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。