瞭解ISE內部證書頒發機構服務

目錄

簡介

本檔案介紹CA服務和思科身分識別服務引擎(ISE)中存在的透過安全傳輸(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
- 憑證與公開金鑰基礎架構(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身分識別服務引擎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。

證書頒發機構(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內部證書頒發機構(ISE CA)從集中控制檯頒發和管理終端的數位證書，以允許員工在公司網路上使用其個人裝置。 CA簽名的數位證書被視為行業標準，並且更安全。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：驗證和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節點上生成並安全儲存金鑰和證書。
- 證書儲存：儲存頒發給使用者和裝置的證書。
- 線上證書狀態協定(OCSP)支援：提供OCSP響應程式以檢查證書的有效性。

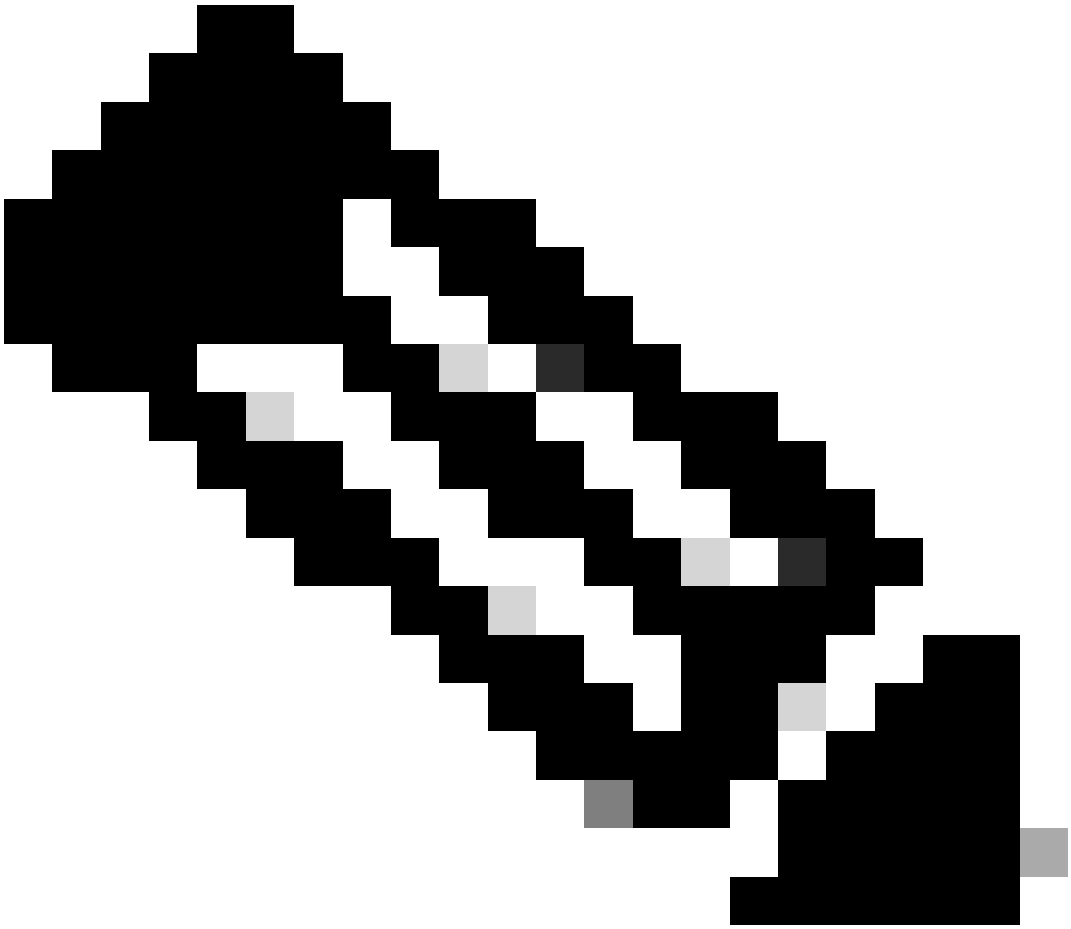
在管理和策略服務節點上調配的ISE CA證書

安裝後，思科ISE節點調配了根CA證書和節點CA證書來管理終端證書。

設定部署後，指定為主要管理節點(PAN)的節點將成為根CA。PAN具有根CA證書和由根CA簽名的節點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註冊的任何策略服務節點(PSN)都調配由終端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。



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

根據RFC 6960:

「證書頒發機構必須執行以下操作之一：

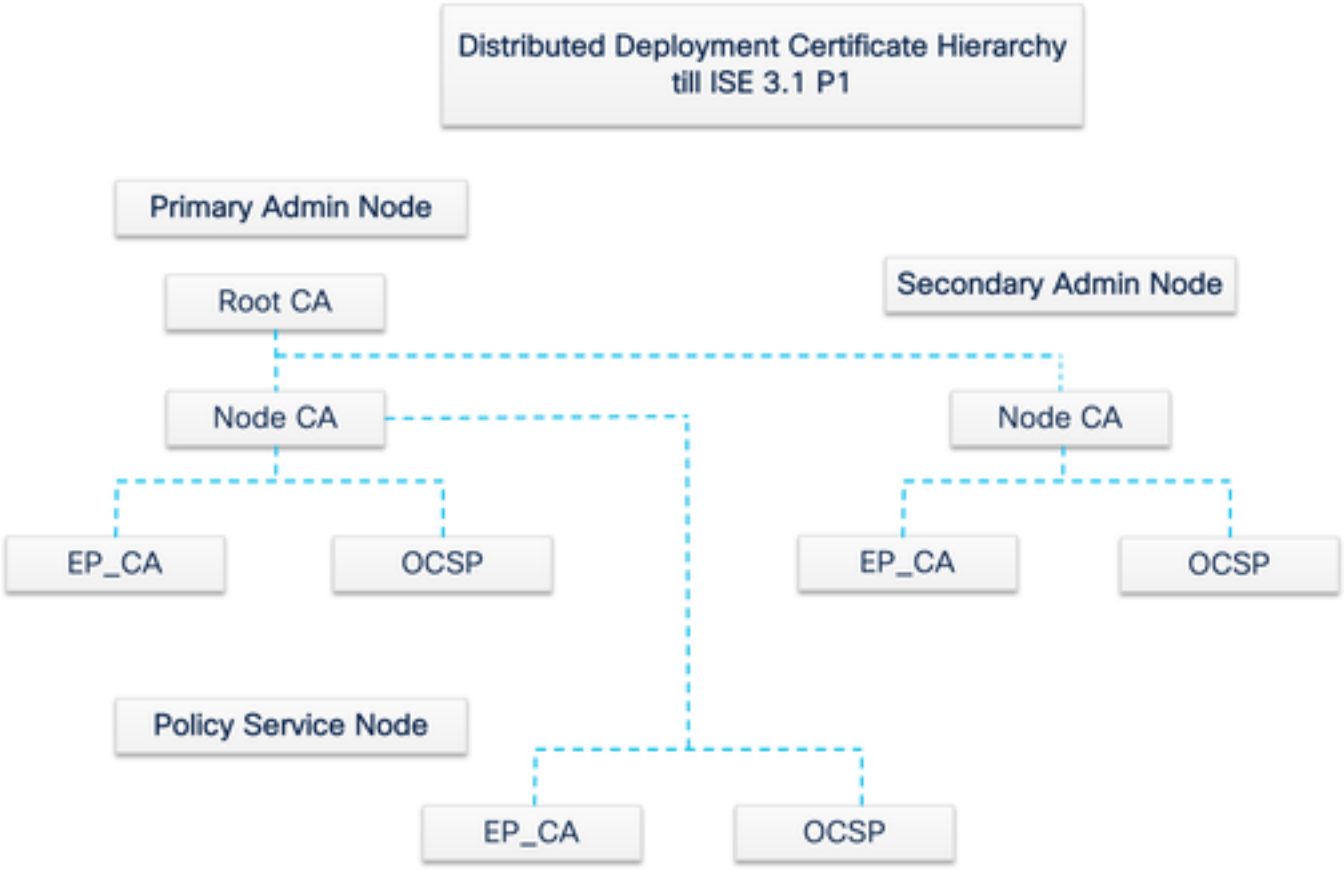
— 簽署OCSP響應本身，或

— 明確將該機構指定給另一個實體」

"OCSP響應簽名者證書必須由請求中決定的CA直接頒發。 "

"系統（依賴於）OCSP響應必須識別由頒發相關證書的CA頒發的委派證書，前提是委派證書和檢查撤銷的證書(is)由同一金鑰簽名。"

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。



通過安全傳輸(EST)服務註冊

公鑰基礎設施(PKI)的概念存在已久。PKI通過數位證書形式的簽名公鑰對來認證使用者和裝置的身份。透過安全傳輸註冊(EST)是提供這些憑證的通訊協定。EST服務定義如何對使用通過加密消息語法(CMC)進行證書管理(Certificate Management over Cryptographic Message Syntax， CMC)的客戶端在安全傳輸上執行證書註冊。根據IETF - 「EST描述了一個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：

- 通過安全唯一裝置標識註冊網路裝置
- 自帶裝置解決方案

為什麼EST

EST和SCEP協定都定址證書調配。EST是簡單憑證註冊通訊協定(SCEP)的後繼路由器。 由於SCEP的簡單性，多年來它一直是證書調配中的實際協定。但是，出於以下原因，建議使用EST over SCEP:

- 使用TLS安全傳輸證書和郵件 — 在EST中，證書簽名請求(CSR)可以與已信任並使用TLS進行身份驗證的請求者關聯。除了他們自己，客戶不能為任何人獲取證書。在SCEP中，CSR透過使用者端和CA之間的共用金鑰進行驗證。這會帶來安全隱患，因為有權訪問共用金鑰的人員可以為自身以外的實體生成證書。
- 支援註冊ECC簽名的證書 — 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。與RSA等其他加密演算法相比，ECC提供了更高的安全性和更好的效能，即使它使用的金鑰大小要小得多。
- EST旨在支援自動證書重新註冊。

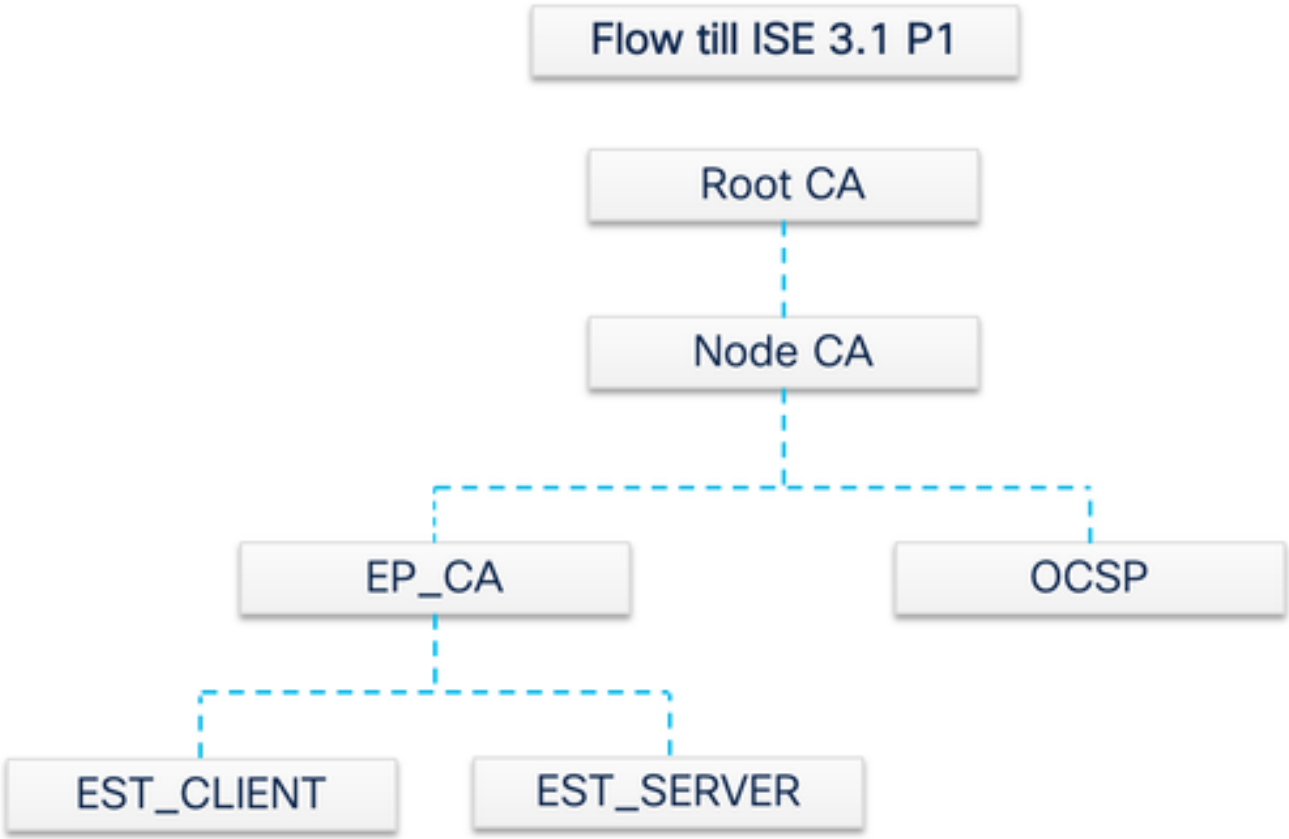
TLS經過驗證的安全性和持續改進有助於確保EST交易在加密保護方面是安全的。SCEP與RSA緊密整合以保護資料，隨著技術的進步，帶來了安全問題。

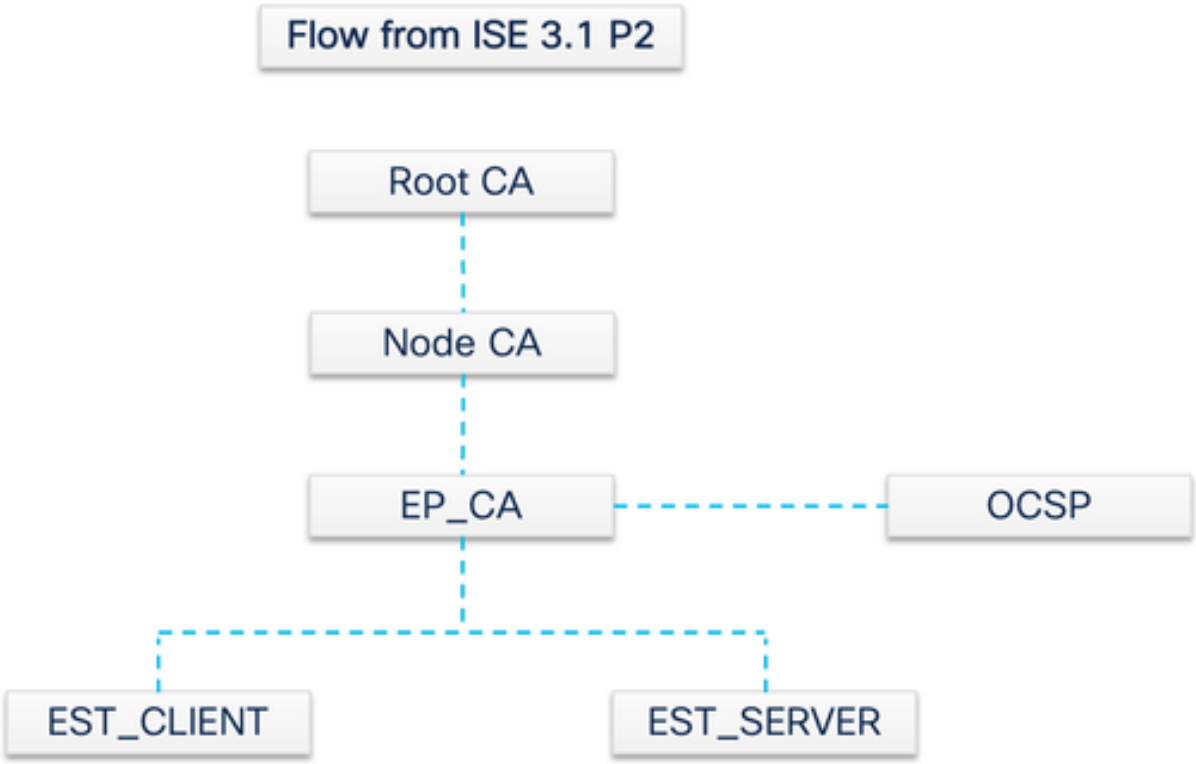
ISE中的EST

為了實施此協定，需要客戶端和伺服器模組：

- EST客戶端 — 嵌入到常規ISE tomcat中。
- EST伺服器 — 部署在稱為NGINX的開源Web伺服器上。此過程作為獨立進程運行，在埠8084上監聽。

EST支援基於證書的客戶端和伺服器身份驗證。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，它會從CA伺服器獲取所有CA證書的最新副本並儲存它。然後，EST客戶端可以發出一個CA證書請求，從該EST伺服器獲取整個證書鏈。在制定簡單註冊請求之前，EST客戶端必須首先發出CA證書請求。

CA憑證請求（基於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.
3. 此操作在任何其他的EST請求之前執行。
4. 每5分鐘進行一次請求，以獲取最新CA證書的副本。
5. 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。

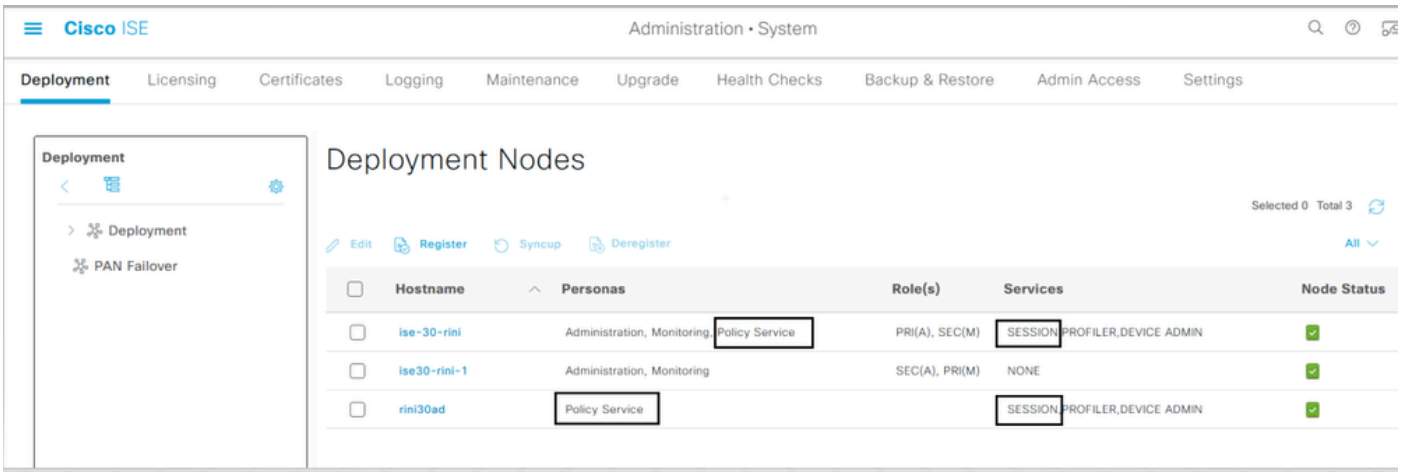
簡單註冊請求（基於RFC 7030）

1. EST客戶端向EST伺服器請求證書。
2. 操作路徑值為的HTTPS POST消息/simpleenroll。
3. EST客戶端在此呼叫中嵌入PKCS#10請求，該呼叫將傳送到ISE。
4. EST伺服器必須對客戶端進行身份驗證。

EST和CA服務狀態

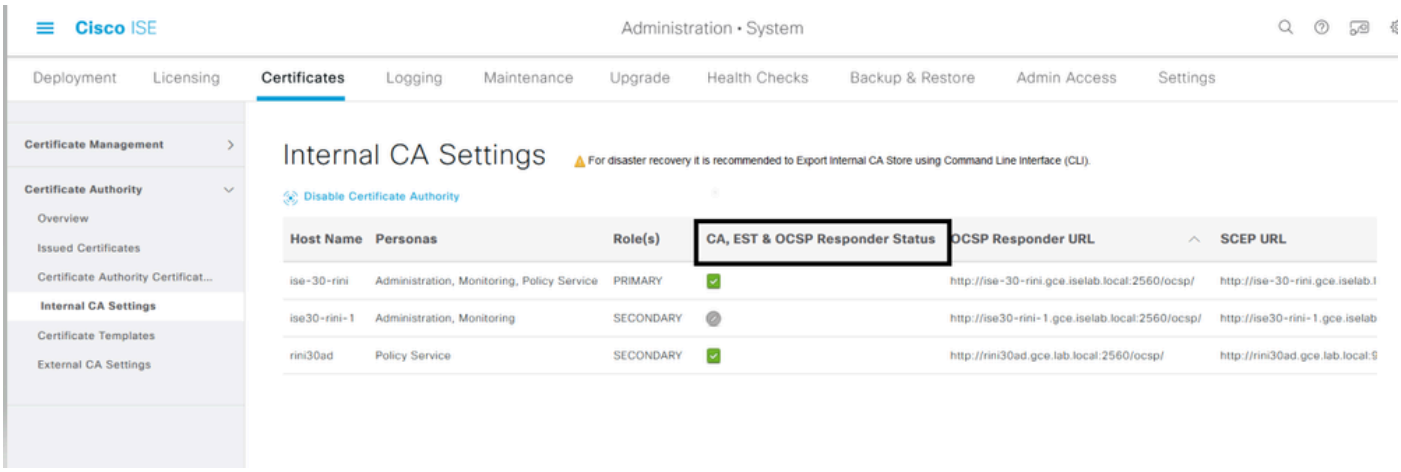
CA和EST服務只能在啟用了會話服務的策略服務節點上運行。要在節點上啟用會話服務，請導航到

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 **Enable Session Services**Service persona下的覈取方塊。



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，則EST服務也關閉。



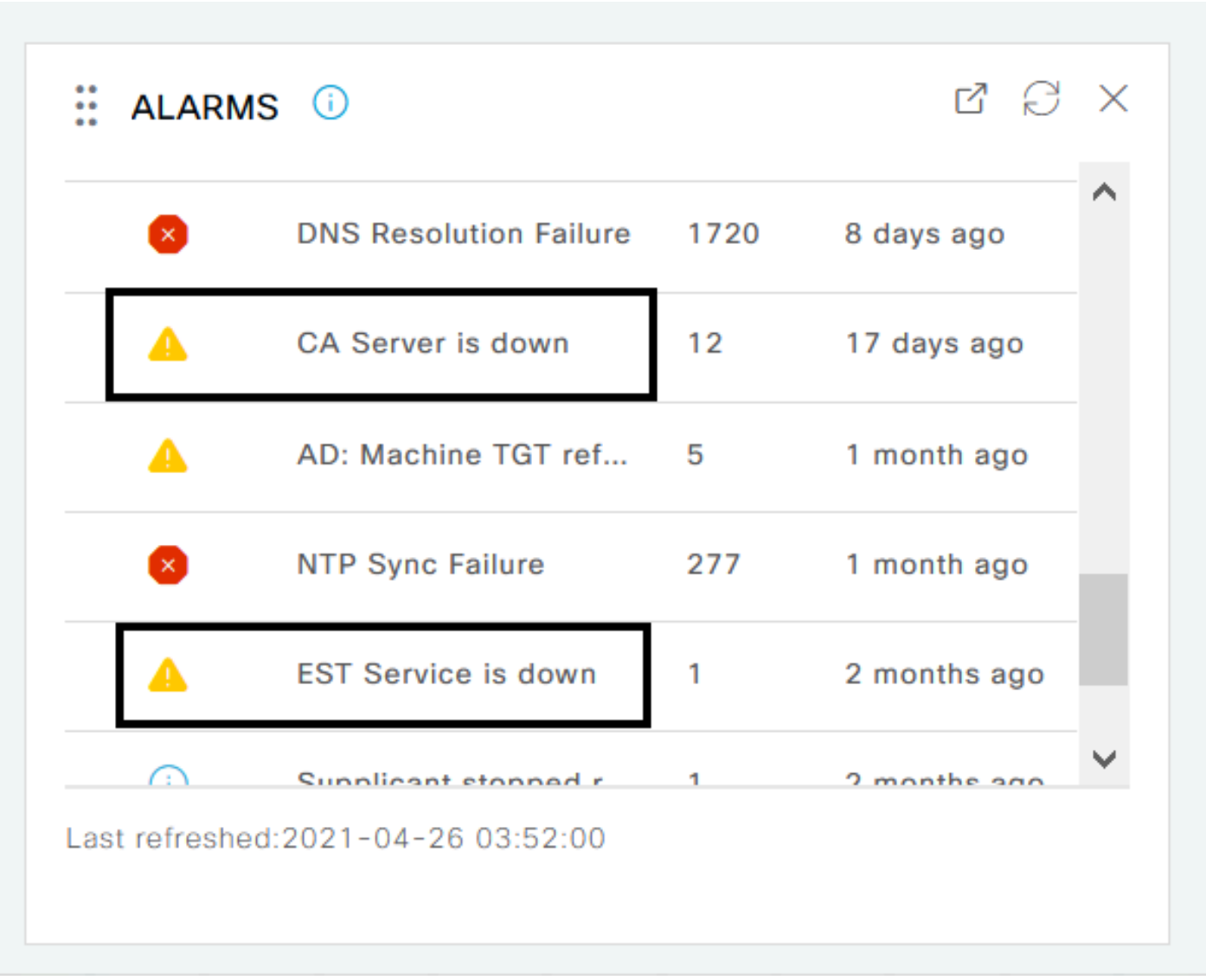
CLI上顯示的狀態

```
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控制面板上會顯示警報。



CA和EST服務未運行時的影響

- 當EST服務器關閉時/cacerts，可能會發生EST客戶端呼叫失敗。如果EST/cacerts CA鏈證書CA鏈不完整，也會發生呼叫失敗。
- 基於ECC的終端證書註冊請求失敗。
- 如果發生前兩次故障，BYOD流中斷。
- 可以生成隊列連結錯誤警報。

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：

- 證書服務終結點子CA證書鏈已完成。若要檢查憑證鏈結是否完整：
  1. 導航至Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates。
  2. 選擇憑證旁的覈取方塊，然後按一下「View」以檢查特定憑證。
- 確保CA和EST服務已啟動並正在運行。如果服務沒有運行，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
  2. 按一下Generate Certificate Signing Requests (CSR)。
  3. ISE Root CA 在Certificate(s) will be used for下拉選單中選擇
  4. 按一下Replace ISE Root CA Certificate Chain。
- 可用於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 ,和文error.log件。

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）。