了解ISE内部证书颁发机构服务

目录

简介

本文档介绍CA服务和思科身份服务引擎(ISE)中存在的安全传输注册(EST)服务。

先决条件

要求

Cisco 建议您了解以下主题：

- ISE
- 证书和公钥基础设施(PKI)
- 简单证书注册协议 (SCEP)
- 在线证书状态协议(OCSP)

使用的组件

本文档中的信息基于身份服务引擎3.0。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

证书颁发机构(CA)服务

证书可以由外部证书颁发机构(CA)自签名或数字签名。思科ISE内部证书颁发机构(ISE CA)从集中控制台颁发和管理终端的数字证书，以允许员工在公司网络上使用其个人设备。 CA签名的数字证书被视为行业标准，并且更加安全。主策略管理节点(PAN)是根CA。策略服务节点(PSN)是从属CA到主PAN。

ISE CA功能

ISE CA提供以下功能：

- 证书颁发：验证和签署连接到网络的终端的证书签名请求(CSR)。
- 密钥管理：在PAN和PSN节点上生成并安全存储密钥和证书。
- 证书存储(Certificate Storage)：存储颁发给用户和设备的证书。
- 在线证书状态协议(OCSP)支持：提供OCSP响应器以检查证书的有效性。

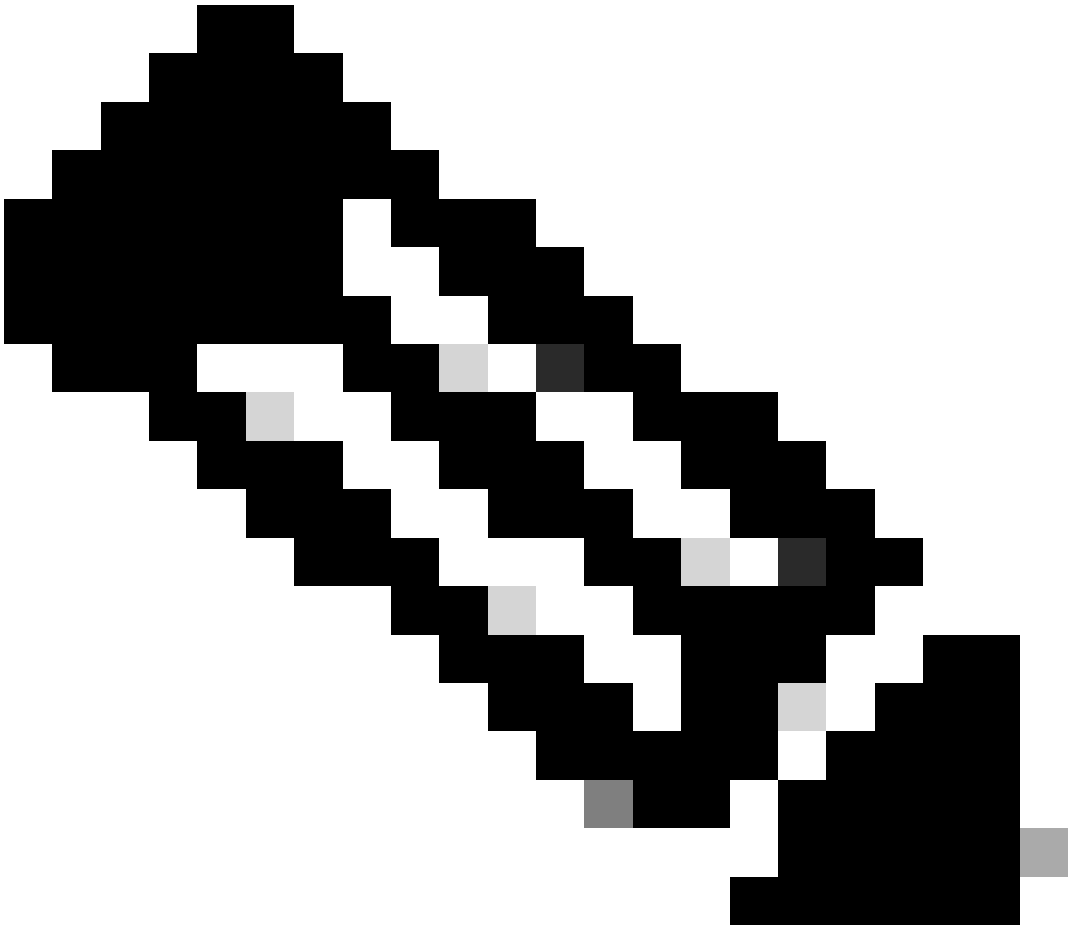
在管理和策略服务节点调配的ISE CA证书

安装后，思科ISE节点调配了根CA证书和节点CA证书来管理终端的证书。

设置部署后，指定为主要管理节点(PAN)的节点成为根CA。PAN有一个根CA证书和一个由根CA签名的节点CA证书。

当辅助管理节点(SAN)注册到PAN时，将生成节点CA证书，并由主管理节点上的根CA进行签名。

向PAN注册的所有策略服务节点(PSN)调配终端CA和由PAN的节点CA签名的OCSP证书。策略服务节点(PSN)是从CA到PAN。使用ISE CA时，PSN上的终端CA会向访问网络的终端颁发证书。



注意：从ISE 3.1补丁2和ISE 3.2 FCS中，OCSP证书层次结构已更改。

根据RFC 6960：

“证书颁发者必须执行以下操作之一：

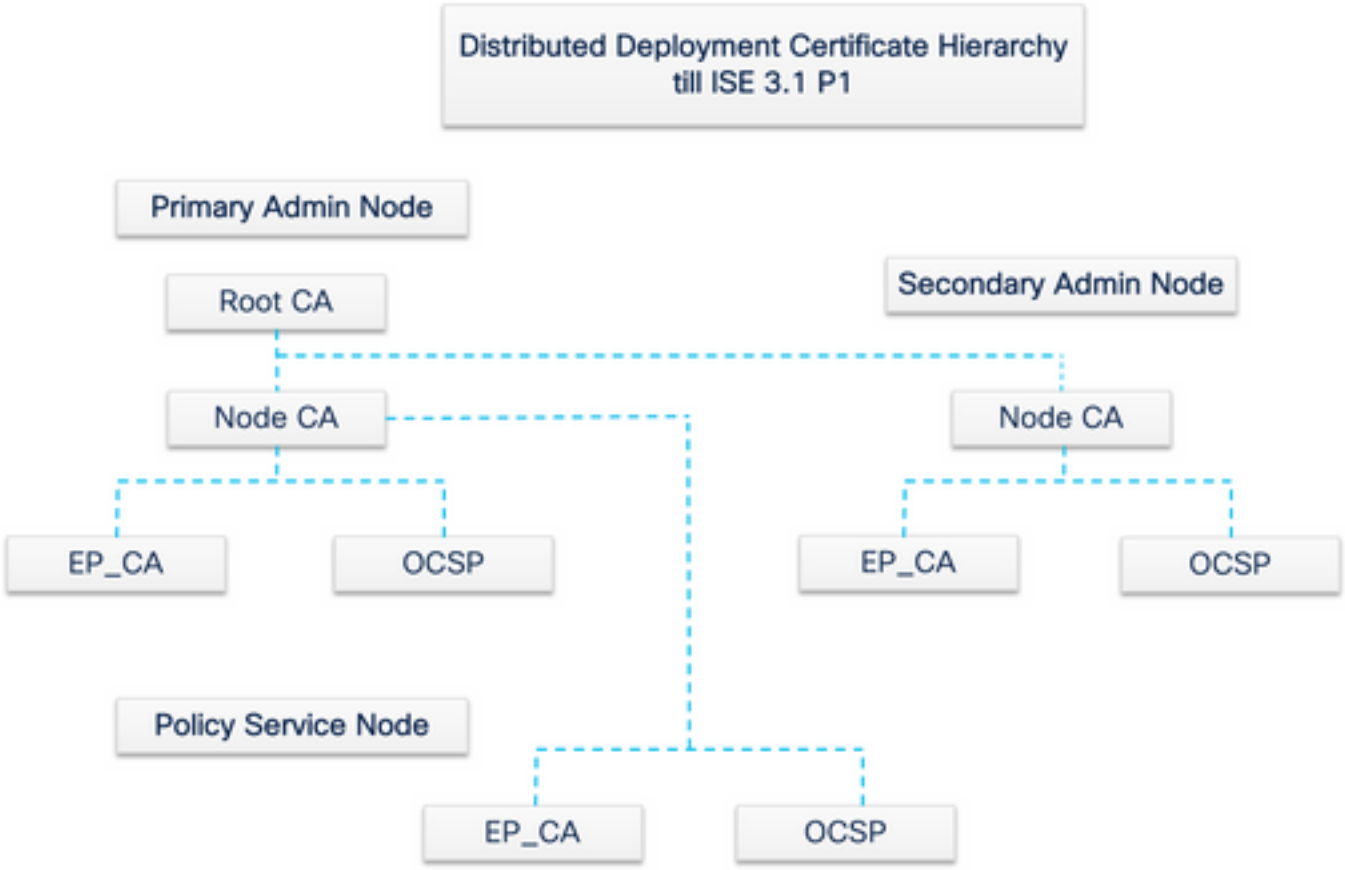
- 签署OCSP响应本身，或

- 明确将该机构指定给另一个实体”

“OCSP响应签名者证书必须由请求中确定的CA直接颁发。 "

“系统（依靠）的OCSP响应必须识别由签发相关证书的CA颁发的授权证书，前提是委派证书和检查撤销的证书(is)由同一密钥签名。”

为了符合前面提到的RFC标准，ISE中更改了OCSP响应器证书的证书层次结构。OCSP响应方证书现在由同一节点的终端子CA颁发，而不是PAN中的节点CA。



通过安全传输(EST)服务注册

公钥基础设施(PKI)的概念由来已久。PKI通过数字证书形式的签名公钥对来验证用户和设备的身份。通过安全传输注册(EST)是提供这些证书的协议。EST服务定义如何对使用加密消息语法(CMC)证书管理的客户端通过安全传输执行证书注册。根据IETF -“EST描述了一个简单但实用的证书管理协议，它面向需要获取客户端证书和相关证书颁发机构(CA)证书的公钥基础设施(PKI)客户端。它还支持客户端生成的公钥/私钥对，以及CA生成的密钥对。"

EST使用案例

可以使用EST协议：

- 通过安全的唯一设备身份注册网络设备
- 自带设备解决方案

为什么选择EST？

EST和SCEP协议都处理证书调配。EST是简单证书注册协议(SCEP)的后继协议。由于其简单性，SCEP多年来一直是证书调配中的实际协议。但是，出于以下原因，建议使用EST over SCEP：

- 使用TLS安全传输证书和邮件-在EST中，证书签名请求(CSR)可以与已受信任并使用TLS进行身份验证的请求方关联。客户端只能获得自己的证书，而不能获得证书。在SCEP中，CSR通过客户端和CA之间的共享密钥进行身份验证。这会带来安全问题，因为有权访问共享密钥的人员可以为除自己之外的实体生成证书。
- 支持ECC签名证书的注册- EST提供加密灵活性。它支持椭圆曲线加密(ECC)。SCEP不支持ECC并依赖于RSA加密。ECC比RSA等其它加密算法提供了更高的安全性和更好的性能，即使它使用的密钥大小要小得多。
- EST旨在支持自动证书重新注册。

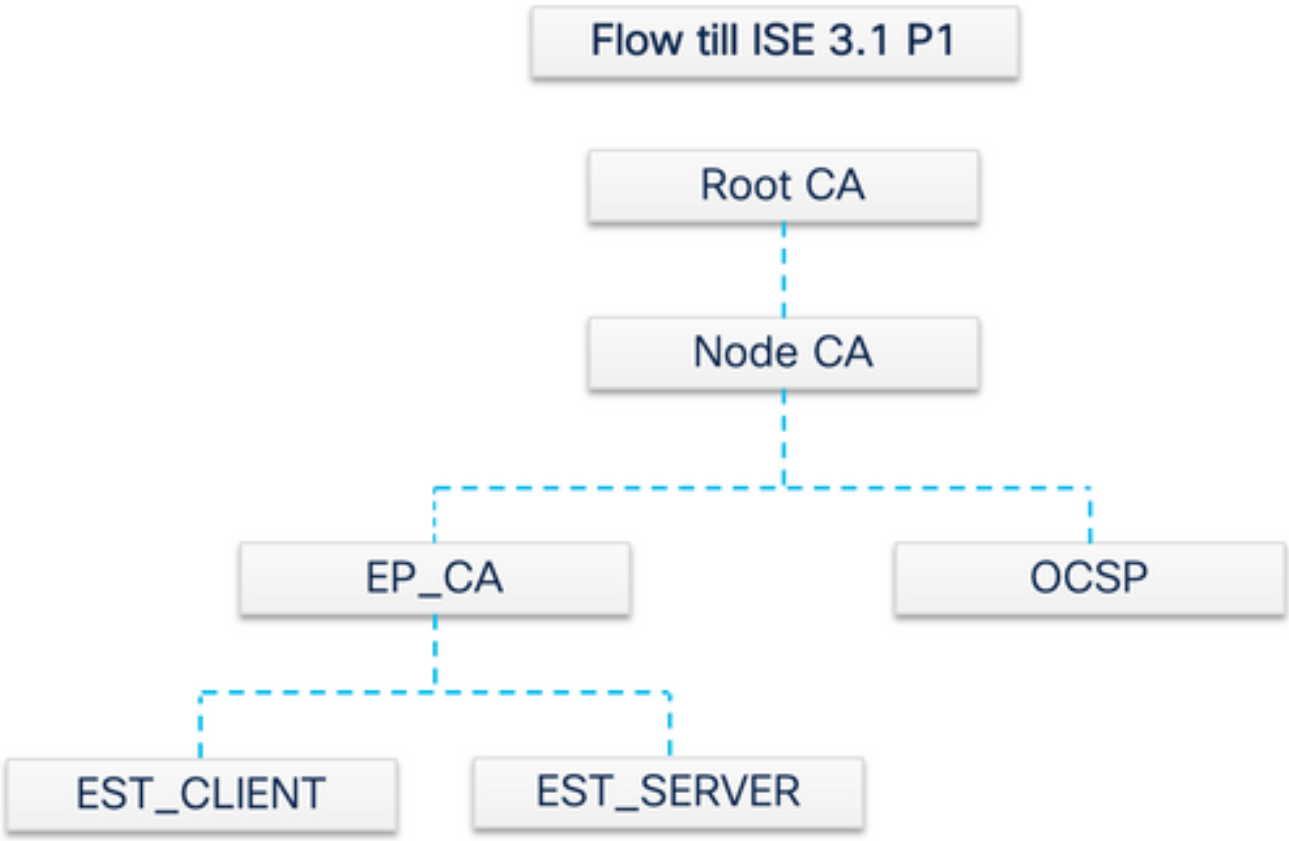
TLS经过验证的安全性和持续改进有助于确保EST事务在加密保护方面是安全的。SCEP与RSA紧密集成以保护数据，随着技术的进步带来了安全问题。

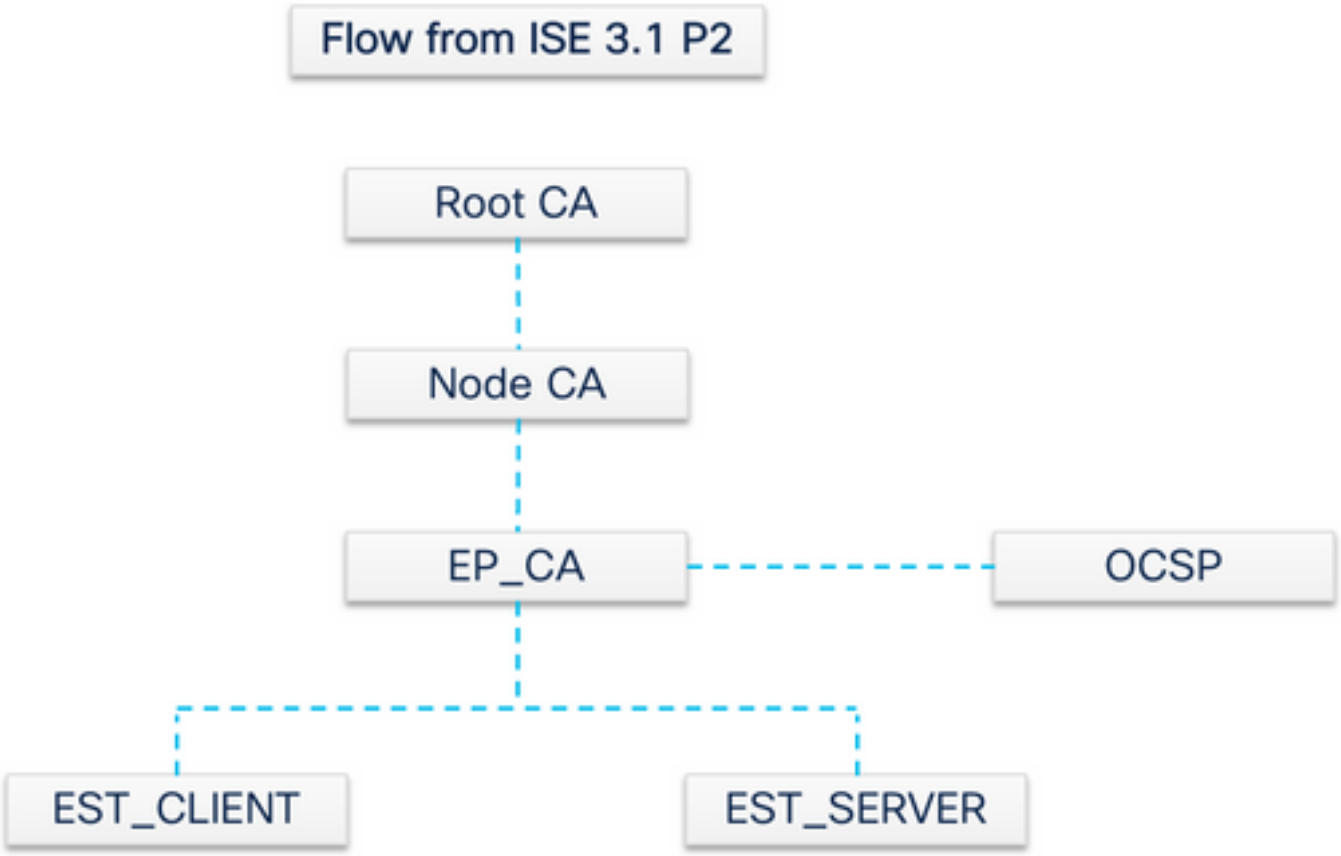
ISE中的EST

要实施此协议，需要客户端和服务器模块：

- EST客户端-嵌入在常规ISE tomcat中。
- EST服务器-部署在称为NGINX的开源Web服务器上。该进程作为单独的进程运行，并在端口8084上侦听。

EST支持基于证书的客户端和服务器身份验证。终端CA为EST客户端和EST服务器颁发证书。EST客户端和服务器证书及其各自的密钥存储在ISE CA的NSS数据库中。





ISE EST中的请求类型

每当EST服务器启动时，它从CA服务器获取所有CA证书的最新副本并将其存储。然后，EST客户端可以发出CA证书请求，从此EST服务器获取整个证书链。在发出简单注册请求之前，EST客户端必须首先发出CA证书请求。

CA证书请求（基于RFC 7030）

1. EST客户端请求当前CA证书的副本。
2. 操作路径值为HTTPS GET消息 /cacerts.

- 该操作在任何其他EST请求之前执行。
- 每5分钟发送一次请求以获取最新CA证书的副本。
- EST服务器不得要求客户端身份验证。

第二个请求是一个简单的注册请求，它需要在EST客户端和EST服务器之间进行身份验证。每次终端连接到ISE并发出证书请求时，都会发生这种情况。

简单注册请求（基于RFC 7030）

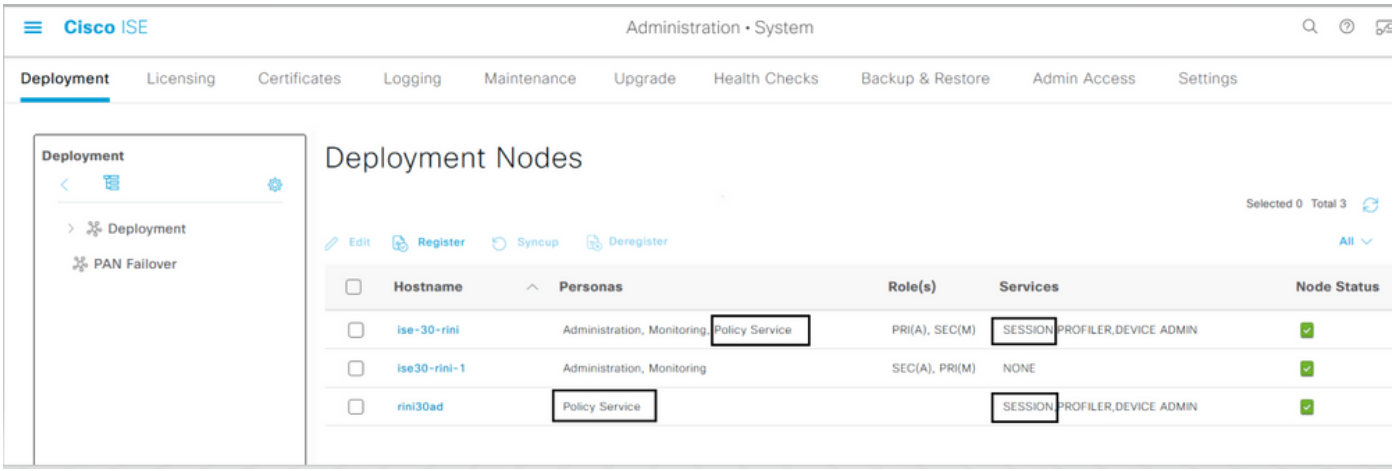
1. EST客户端向EST服务器请求证书。

2. 操作路径值为/simpleenroll的HTTPS POST消息。

- EST客户端在此呼叫中嵌入PKCS#10请求，该呼叫将发送到ISE。
- EST服务器必须对客户端进行身份验证。

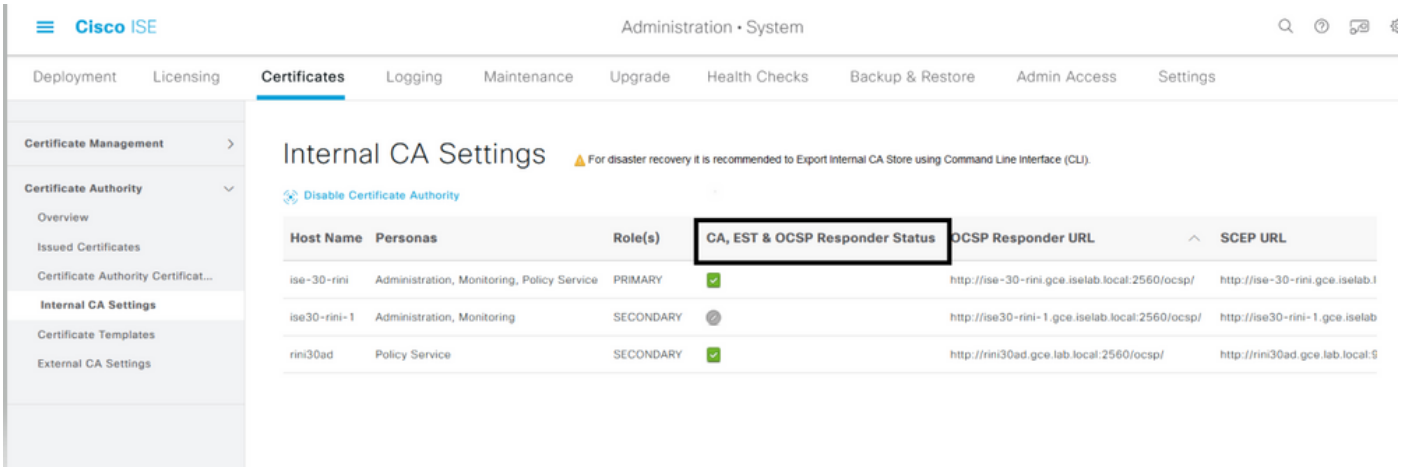
EST和CA服务状态

CA和EST服务只能在启用了会话服务的策略服务节点上运行。要在节点上启用会话服务，请导航到Administration > System > Deployment。选择需要启用会话服务的服务器主机名，然后单击Edit。选中Policy Service persona下的 **Enable Session Services** 复选框。



GUI上显示的状态

EST服务状态与ISE上的ISE CA服务状态关联。如果CA服务启动，则EST服务启动；如果CA服务关闭，则EST服务也关闭。



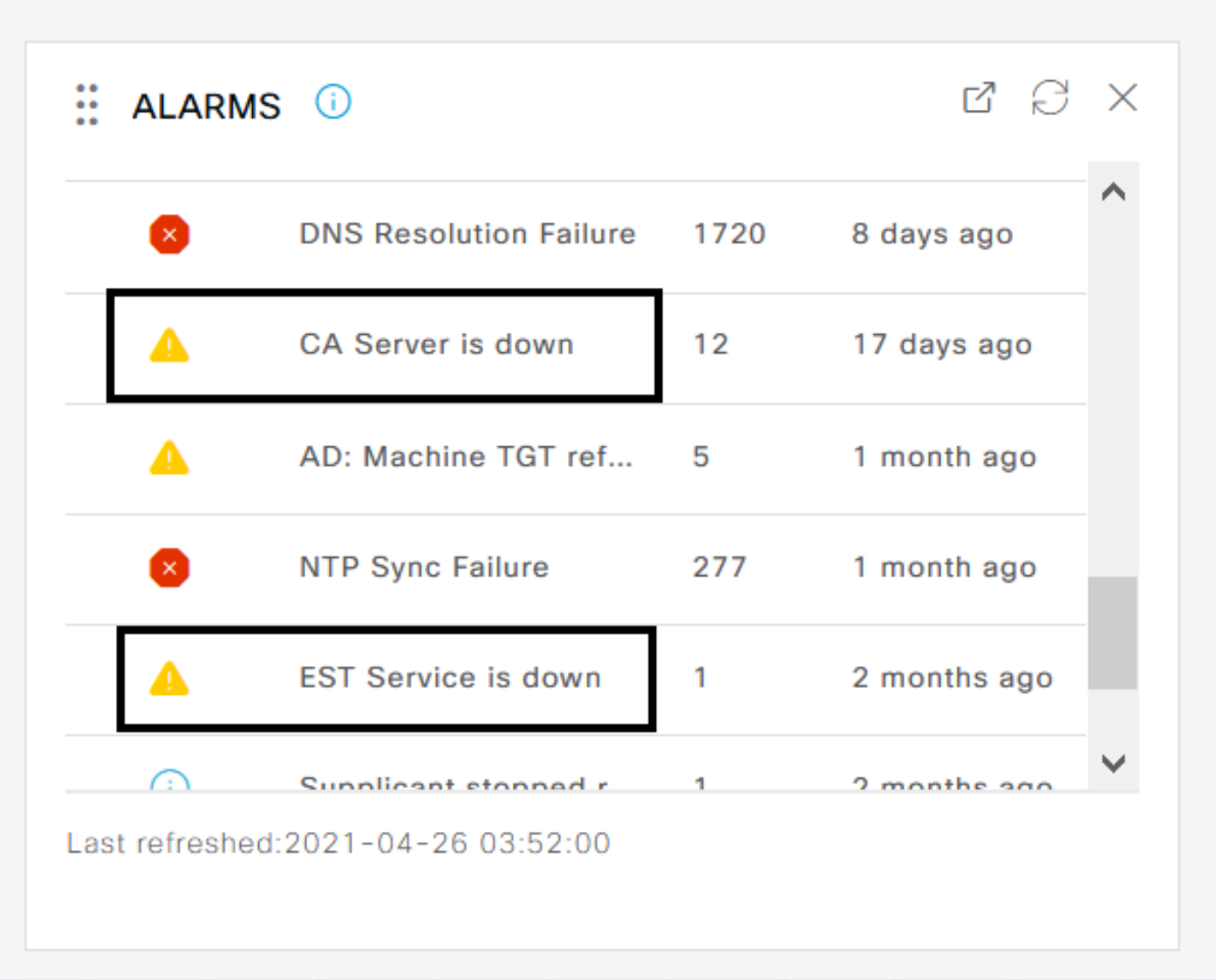
CLI上显示的状态

```
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
```

控制面板上的警报

如果EST和CA服务关闭，警报会显示在ISE控制面板上。



如果CA和EST服务未运行，将产生影响

- EST客户端/cacerts呼叫失败会在EST服务器发生故障时发生。如果EST CA链证书CA链不完整，/cacerts呼叫失败也会发生。
- 基于ECC的终端证书注册请求失败。
- 如果发生前两次故障之一，BYOD流程会中断。
- 可以生成队列链路错误警报。

故障排除

如果使用EST协议的BYOD流程无法正常工作，请检查以下条件：

- 证书服务终结点子CA证书链已完成。要检查证书链是否完整，请执行以下操作：

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

     - 选中证书旁边的复选框并单击**View**以检查特定证书。

- 确保CA和EST服务已启动并正在运行。如果服务未运行，请导航到Administration > System > Certificates > Certificate Authority > Internal CA Settings以启用CA服务。

- 如果已执行升级，请在升级后替换ISE根CA证书链。为此，请执行以下操作：

  1. 选择 。Administration > System > Certificates > Certificate Management > Certificate Signing Requests

     - 单击。Generate Certificate Signing Requests (CSR)

     - 在下拉列表中选择ISE Root CACertificate(s) will be used for

-

单击。Replace ISE Root CA Certificate Chain

- 能够启用来检查日志的有用调试包括est、provisioning、ca-service和ca-service-cert。请参阅ise-psc.log、catalina.out、caservice.log , 和error.log文件。

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。