ISE内部認証局(CA)サービスについて

内容

はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)に存在するCAサービスとセキュアトランスポート(EST)での登録サービスについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ISE
- 証明書と Public Key Infrastructure（PKI）
- Simple Certificate Enrollment Protocol（SCEP）
- オンライン証明書ステータスプロトコル(OCSP)

使用するコンポーネント

このドキュメントの情報は、Identity Services Engine(ISE)3.0に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

認証局(CA)サービス

証明書は、自己署名することも、外部の認証局(CA)によってデジタル署名することもできます。Cisco ISE Internal Certificate Authority(ISE CA)は、従業員が会社のネットワーク上で個人デバイスを使用できるように、一元化されたコンソールからエンドポイントのデジタル証明書を発行および管理します。 CA署名付きデジタル証明書は、業界標準で安全性が高いと考えられています。プライマリポリシー管理ノード(PAN)はルートCAです。ポリシーサービスノード(PSN)は、プライマリPANの下位CAです。

ISE CAの機能

ISE CAは次の機能を提供します。

- 証明書の発行：ネットワークに接続するエンドポイントの証明書署名要求(CSR)を検証し、署名します。
- キー管理：PANノードとPSNノードの両方でキーと証明書を生成し、安全に保存します。
- 証明書ストレージ：ユーザとデバイスに発行される証明書を保存します。
- Online Certificate Status Protocol(OCSP)のサポート：OCSPレスポンダを使用して証明書の有効性をチェックできます。

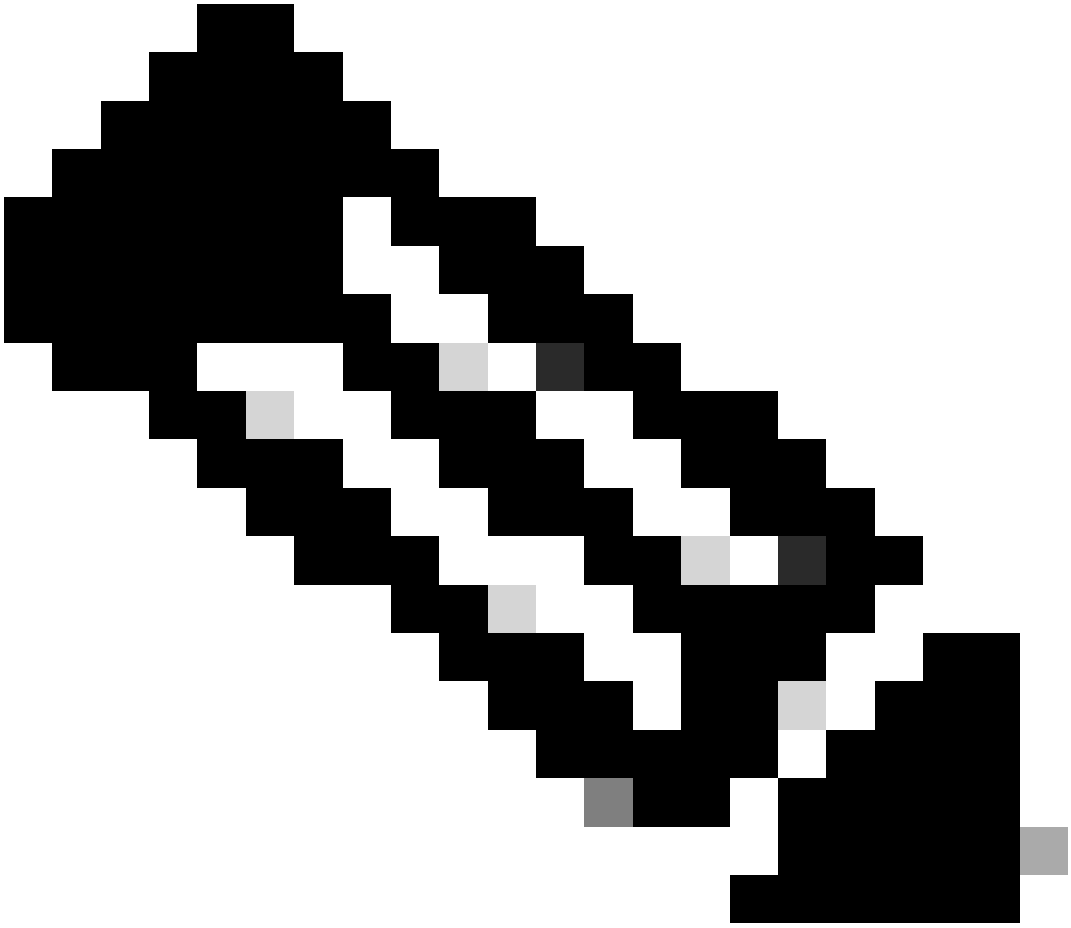
管理およびポリシーサービスノードでプロビジョニングされたISE CA証明書

インストール後、Cisco ISEノードはルートCA証明書とノードCA証明書を使用してプロビジョニングされ、エンドポイントの証明書を管理します。

展開をセットアップすると、プライマリ管理ノード(PAN)として指定されたノードがルートCAになります。PANには、ルートCA証明書と、ルートCAによって署名されたノードCA証明書があります。

セカンダリ管理ノード(SAN)がPANに登録されると、ノードCA証明書が生成され、プライマリ管理ノードのルートCAによって署名されます。

PANに登録されているポリシーサービスノード(PSN)は、エンドポイントCAと、PANのノードCAによって署名されたOCSP証明書としてプロビジョニングされます。ポリシーサービスノード(PSN)は、PANの下位CAです。ISE CAを使用すると、PSN上のエンドポイントCAが、ネットワークにアクセスするエンドポイントに証明書を発行します。



注:ISE 3.1パッチ2およびISE 3.2 FCSから、OCSP証明書階層が変更されました。

RFC 6960によると：

証明書発行者は、次のいずれかを行う必要があります。

- OCSP応答自体に署名する

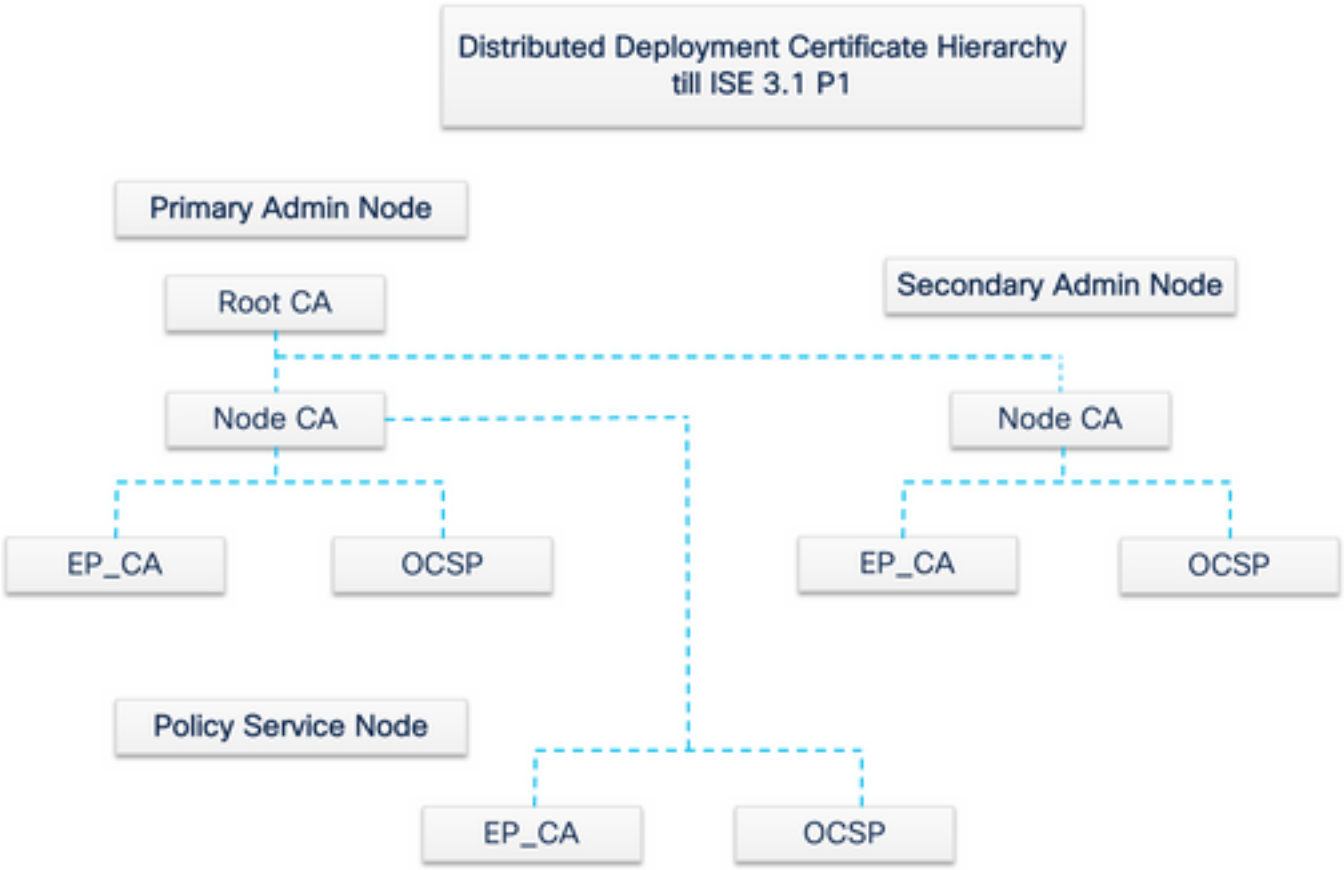
– この権限を別のエンティティに明示的に指定します。

「OCSP応答署名者証明書は、要求で特定されたCAから直接発行する必要があります。 "

「OCSP応答に依存するシステムは、委任証明書と失効が同じキーによって署名された場合にのみ、問題の証明書を発行したCAによって発行された委任証明書を認識する必要があります。」

前述のRFC標準に準拠するために、OCSPレスポンダ証明書の証明書階層がISEで変更されます。

OCSPレスポンダ証明書が、PANのノードCAではなく、同じノードのエンドポイントサブCAによって発行されるようになりました。



Secure Transport(EST)サービスを介した登録

公開キーインフラストラクチャ(PKI)の概念は長い間存在してきました。PKIは、デジタル証明書の形式の署名付き公開キーペアを使用して、ユーザとデバイスのアイデンティティを認証します。Enrollment over Secure Transport(EST)は、これらの証明書を提供するプロトコルです。ESTサービスは、セキュリティで保護されたトランスポートで、暗号化メッセージ構文(CMC)を介した証明書管理を使用するクライアントの証明書登録を実行する方法を定義します。IETFの「EST」によると、クライアント証明書および関連する認証局(CA)証明書を取得する必要がある公開キーインフラストラクチャ(PKI)クライアントを対象とする、シンプルでありながら機能する証明書管理プロトコルです。また、クライアントが生成した公開/秘密キーペアと、CAによって生成されたキーペアもサポートします」

ESTの使用例

ESTプロトコルは次のように使用できます。

- 一意のデバイスIDを使用してネットワークデバイスを登録する
- BYODソリューション

なぜESTなのか？

ESTプロトコルとSCEPプロトコルは両方とも、証明書のプロビジョニングに対応します。ESTは、Simple Certificate Enrollment Protocol(SCEP)の後継プロトコルです。SCEPは、そのシンプルさから、長年にわたって証明書プロビジョニングのデファクトプロトコルとなってきました。ただし、次の理由から、SCEPではなくESTを使用することを推奨します。

- 証明書およびメッセージの安全な転送のためのTLSの使用:ESTでは、証明書署名要求(CSR)を、TLSによってすでに信頼され認証されている要求元に関連付けることができます。クライアントは、自分以外のユーザの証明書を取得することはできません。SCEPでは、クライアントとCAの間の共有秘密によってCSRが認証されます。共有秘密にアクセスできるユーザが自分以外のエンティティの証明書を生成できるため、セキュリティ上の問題が生じます。
- ECC署名付き証明書の登録のサポート – ESTは暗号化の俊敏性を提供します。楕円曲線暗号(ECC)をサポートします。SCEPはECCをサポートしておらず、RSA暗号化に依存しています。ECCは、非常に小さいサイズの鍵を使用する場合でも、RSAなどの他の暗号化アルゴリズムよりも優れたセキュリティとパフォーマンスを提供します。
- ESTは、証明書の自動再登録をサポートするように構築されています。

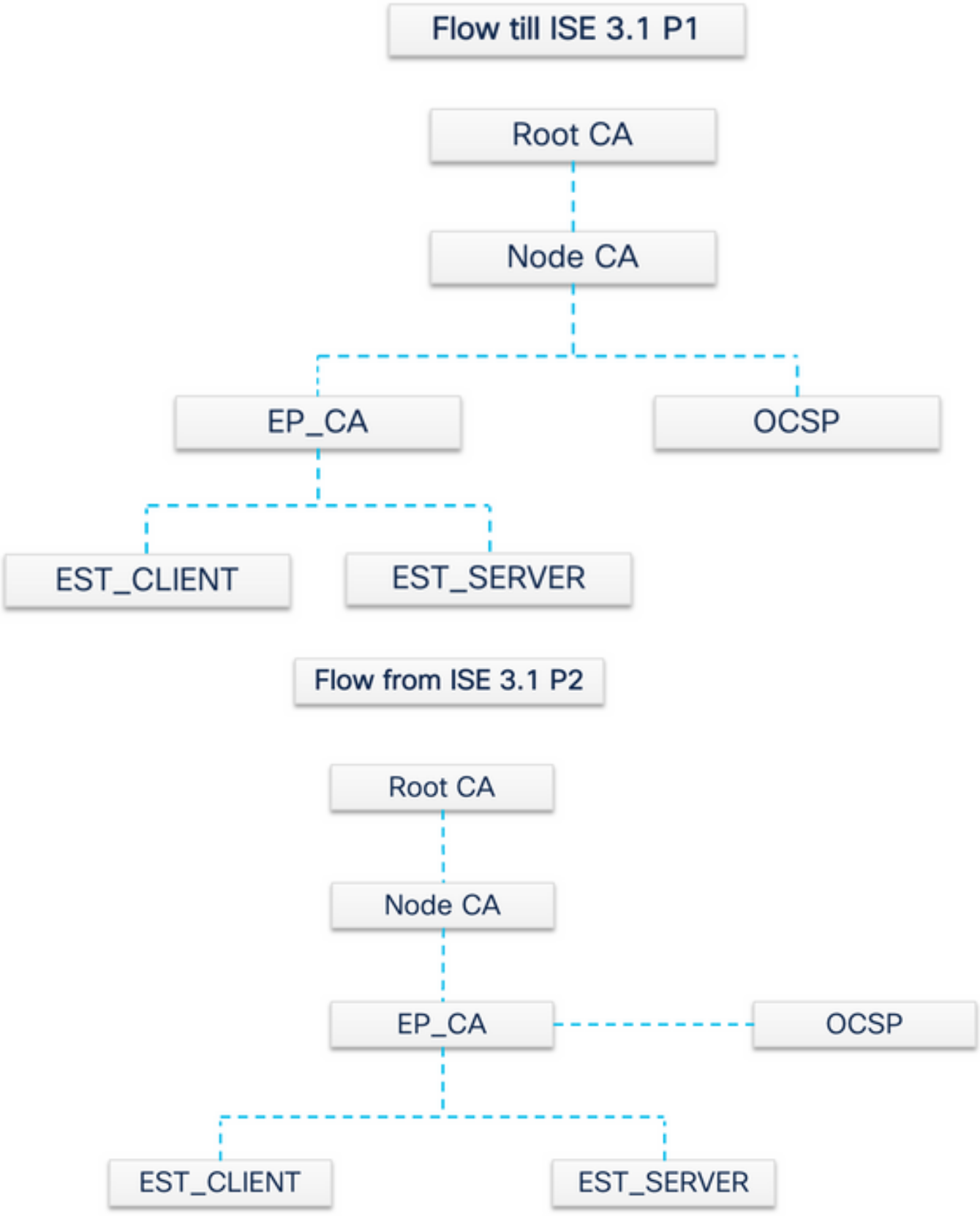
TLSの実績あるセキュリティと継続的な改善により、ESTトランザクションが暗号化保護の観点から安全であることが保証されます。SCEPとRSAの緊密な統合によるデータ保護は、テクノロジーの進歩に伴ってセキュリティ上の懸念をもたらします。

ISEでテスト

このプロトコルを実装するには、クライアントとサーバモジュールが必要です。

- ESTクライアント：通常のISE tomcatに組み込まれます。
- ESTサーバ：NGINXと呼ばれるオープンソースのWebサーバに導入されます。これは別のプロセスとして実行され、ポート8084でリッスンします。

証明書ベースのクライアントおよびサーバ認証は、ESTでサポートされています。エンドポイントCAは、ESTクライアントとESTサーバに対して証明書を発行します。ESTクライアント証明書とサーバ証明書、およびそれぞれのキーは、ISE CAのNSS DBに保存されます。



ISE ESTの要求のタイプ

ESTサーバは、起動するたびにCAサーバからすべてのCA証明書の最新のコピーを取得して保存します。次に、ESTクライアントは、このESTサーバからチェーン全体を取得するためにCA証明書要求を行うことができます。単純な登録要求を行う前に、ESTクライアントは最初にCA証明書要求を発行する必要があります。

CA証明書要求（RFC 7030に基づく）

1. ESTクライアントは、現在のCA証明書のコピーを要求します。
2. HTTPS GETメッセージの操作パス値は /cacerts.

- この操作は、他のEST要求の前に実行されます。
- 最新のCA証明書のコピーを取得するように5分ごとに要求されます。
- ESTサーバはクライアント認証を必要としません。

2番目の要求は単純な登録要求で、ESTクライアントとESTサーバ間の認証が必要です。これは、エンドポイントがISEに接続して証明書要求を行うたびに発生します。

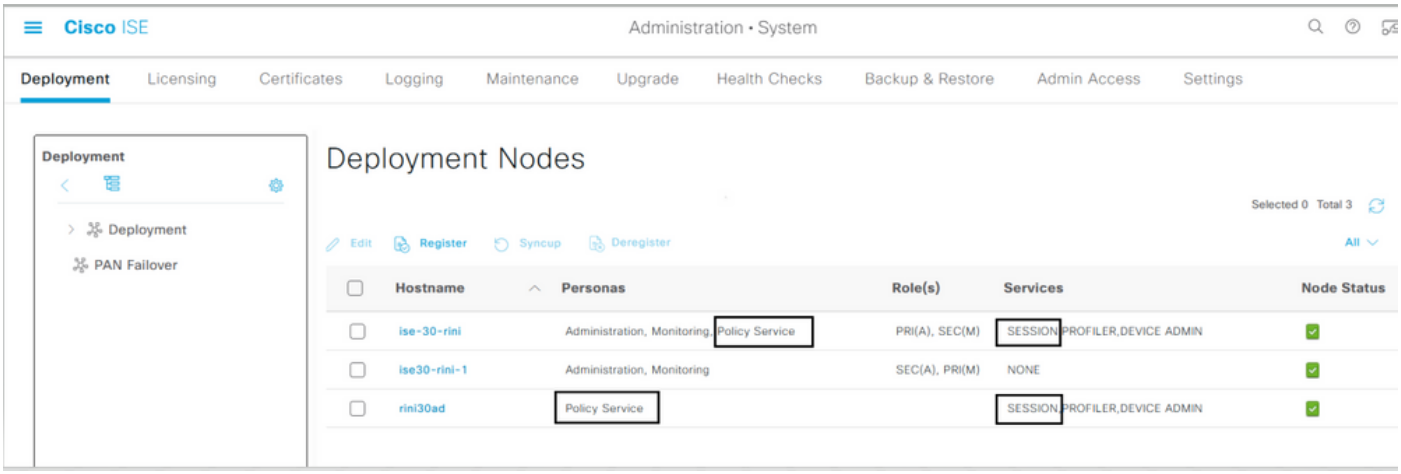
簡単な登録要求（RFC 7030に基づく）

1. ESTクライアントは、ESTサーバに証明書を要求します。
2. 操作パスの値が/simpleenrollのHTTPS POSTメッセージ。

- ESTクライアントは、ISEに送信されるこのコール内にPKCS#10要求を埋め込みます。
- ESTサーバはクライアントを認証する必要があります。

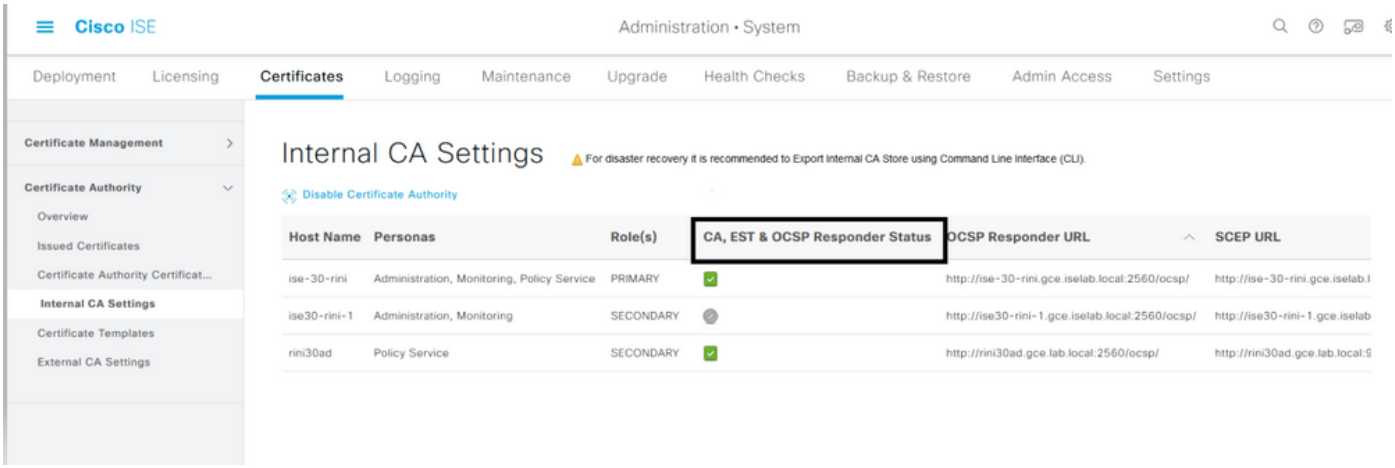
ESTおよびCAサービスステータス

CAおよびESTサービスは、セッションサービスが有効になっているポリシーサービスノードでのみ実行できます。ノードでセッションサービスを有効にするには、Administration > System > Deploymentに移動します。セッションサービスを有効にする必要があるサーバのホスト名を選択し、Editをクリックします。Policy Service personaの下の **Enable Session Services** チェックボックスをオンにします。



GUIに表示されるステータス

ESTサービスステータスは、ISEのISE CAサービスステータスに関連付けられます。CAサービスがアップ状態の場合はESTサービスがアップ状態であり、CAサービスがダウン状態の場合はESTサービスもダウン状態です。



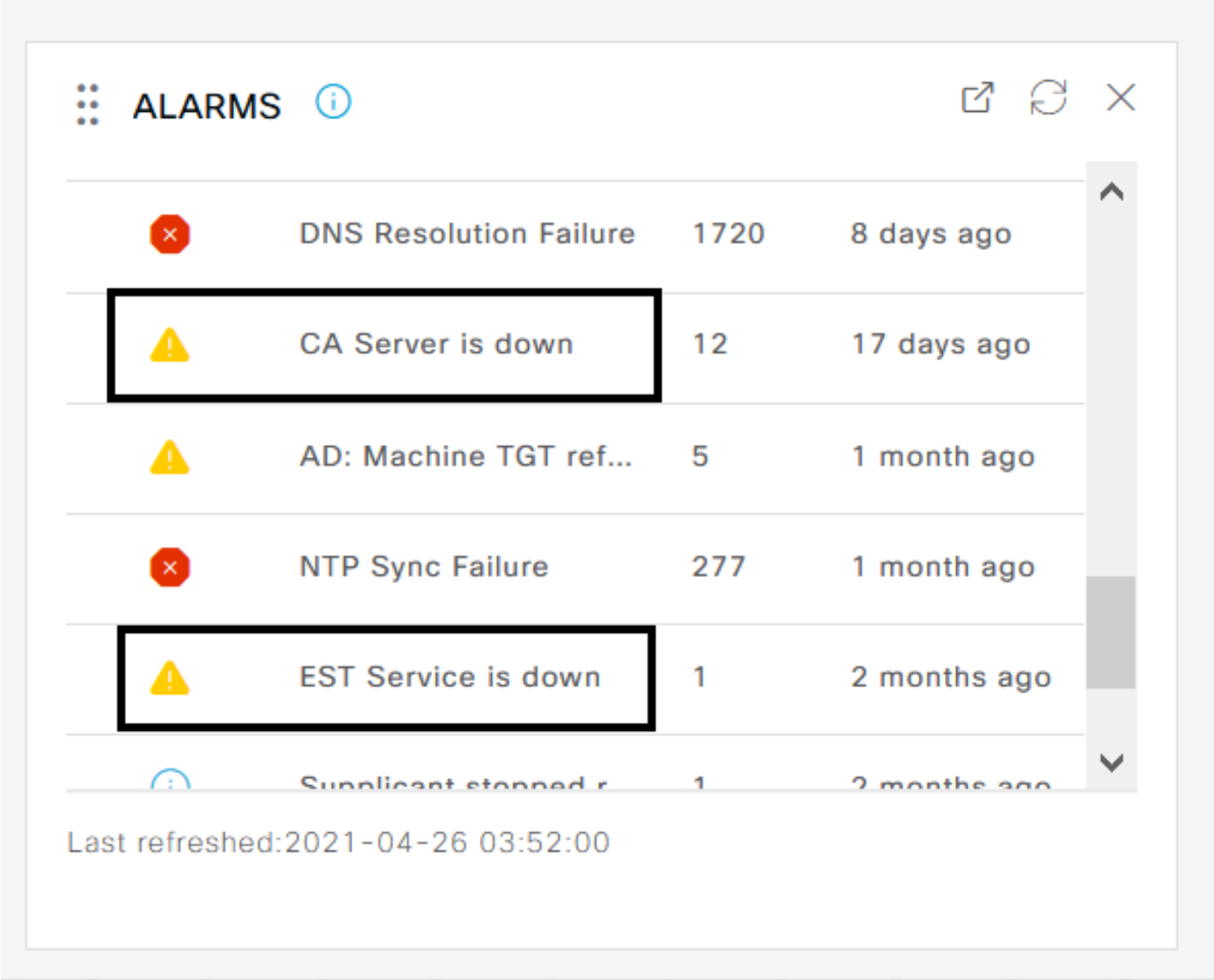
CLIに表示されるステータス

```
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
```

ダッシュボードのアラーム

ESTおよびCAサービスがダウンしている場合、アラームはISEダッシュボードに表示されます。



CAおよびESTサービスが実行されていない場合の影響

- ESTクライアント/cacertsのコール障害は、ESTサーバがダウンしている場合に発生する可能性があります。EST CAチェーン証明書CAチェーンが不完全な場合にも、/cacertsコールが失敗することがあります。

- ECCベースのエンドポイント証明書登録要求が失敗します。

- 前の2つの障害のいずれかが発生すると、BYODフローが中断します。
- キューリンクエラーアラームを生成できます。

トラブルシュート

ESTプロトコルを使用したBYODフローが正しく動作しない場合は、次の状態を確認します。

- 証明書サービスエンドポイントサブCA証明書チェーンが完了しました。証明書チェーンが完了しているかどうかを確認するには、次の手順を実行します。

  Administration > System > Certificates > Certificate Authority > Certificate Authority Certificates

  1. に移動します。
  2. 証明書の横にあるチェックボックスをオンにし、**View**をクリックして、特定の証明書をチェックします。

- CAおよびESTサービスが稼働していることを確認します。サービスが実行されていない場合は、Administration > System > Certificates > Certificate Authority > Internal CA Settingsに移動してCAサービスを有効にします。

- アップグレードを実行した場合は、アップグレード後にISEルートCA証明書チェーンを置き換えます。確認するには、次の手順を実行します。

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

-

をクリックします。Generate Certificate Signing Requests (CSR)

-

ドロップダウンリストでISE Root CACertificate(s) will be used for を選択します

-

をクリックします。Replace ISE Root CA Certificate Chain

- ログのチェックに有効にできる便利なデバッグには、est、provisioning、ca-service、ca-service-certがあります。ise-psc.log、catalina.out、caservice.log , error.logおよびファイルを参照してください。

関連情報

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。