Cisco ISEでのSSLデジタル証明書のインストール、更新、およびトラブルシューティング

内容

はじめに

このドキュメントでは、SSL証明書のインストール、更新、およびIdentity Services Engine(ISE)で見られる最も一般的な問題の解決策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。

- Identity Service EngineのGUI

使用するコンポーネント

この文書の情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Identity Service Engine 2.7

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。

背景説明

このドキュメントでは、トラブルシューティングを開始してシスコテクニカルサポートに問い合わせる前に、確認して対処する必要がある一般的な問題の推奨手順とチェックリストについて説明します。

証明書は、個人、サーバ、会社、またはその他のエンティティを識別し、そのエンティティを公開キーに関連付ける電子ドキュメントです。

自己署名証明書は、独自の作成者によって署名されます。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。

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見なされます。

証明書は、セキュアなアクセスを提供するためにネットワークで使用されます。

Cisco ISEは、ノード間の通信、およびSyslogサーバ、フィードサーバ、およびすべてのエンドユーザポータル（ゲスト、スポンサー、およびパーソナルデバイスポータル）などの外部サーバとの通信に証明書を使用します。

証明書は、エンドポイントに対してCisco ISEノードを識別し、そのエンドポイントとCisco ISEノード間の通信を保護します。

証明書は、すべてのHTTPS通信と拡張認証プロトコル(EAP)通信に使用されます。

このドキュメントでは、トラブルシューティングを開始してシスコテクニカルサポートに問い合わせる前に、確認して対処する必要がある一般的な問題の推奨手順とチェックリストについて説明します。

これらのソリューションは、シスコテクニカルサポートが解決したサービスリクエストから直接提供されます。 稼働中のネットワークで問題に対処する際には、実施する手順が及ぼす潜在的な

影響を十分に理解しておく必要があります。

設定

次のガイドでは、証明書をインポートおよび置換する方法について説明します。

システム証明書のインポート

https://www.cisco.com/c/en/us/td/docs/security/ise/2-7/admin_guide/workflow/html/b_basic_setup_2_7.html#ID547

期限切れの証明書の置き換え

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/116977-technote-ise-cert-00.html#anc5

一般的な問題

シナリオ1:ISEノードで期限切れのポータル証明書を置き換えることができない

エラー

新しいポータル証明書をCSRにバインドする際に、証明書のバインドプロセスが失敗し、次に示すエラーが表示されます。

Internal error.詳細については、ISE管理者にログの確認を依頼してください

このエラーの最も一般的な原因は次のとおりです。

– 新しい証明書のサブジェクト名が既存の証明書と同じである

– 既存の証明書と同じ秘密キーを使用している更新された証明書をインポートする

解決方法

1. ポータルの使用状況を同じノード上の別の証明書に一時的に割り当てる
2. 期限切れポータル証明書の削除
3. 新しいポータル証明書をインストールし、ポータルの使用状況を割り当てます

たとえば、EAP認証を使用する既存の証明書にポータルの使用を一時的に割り当てる場合は、次の手順を実行します。

ステップ 1：EAP認証を使用する証明書を選択して編集し、[Usage]にポータルロールを追加して[Save]をクリックします

ステップ 2：期限切れポータル証明書の削除

ステップ 3：ロールを選択せずに新しいポータル証明書をアップロードし（使用状況の下）、送信する

ステップ 4：新しいポータル証明書を選択して編集し、[Usage]の下でポータルロールを割り当てて保存します。

シナリオ2：複数回使用する同じISEノードに2つのCSRを生成できない

エラー

Multi-Useを使用する同じノードに対する新しいCSRの作成が失敗し、次のエラーが表示されます。
同じフレンドリ名の別の証明書が既に存在します。フレンドリ名は一意でなければなりません。

解決方法

CSRフレンドリ名はISEノードごとにハードコードされるため、同じノードに複数回使用する2つのCSRを作成することはできません。この使用例は特定のノードを対象としています。管理者とEAP認証に使用されるCA署名付き証明書と、SAMLとポータルに使用されるCA署名付き証明書が1つ存在し、両方の証明書の有効期限が切れます。

このシナリオでは次のようになっています。

ステップ 1：多用途で使用する最初のCSRの生成

ステップ 2：CA署名付き証明書を最初のCSRにバインドし、AdminおよびEAP認証ロールを割り当てます

ステップ 3：2つ目のCSRを多用途に使用して生成

ステップ 4：CA署名付き証明書を2番目のCSRにバインドし、SAMLおよびポータルロールを割り当てます

シナリオ3：ポータルを使用するためにCA署名付き証明書をバインドできない、または証明書にポータルタグを割り当てられず、エラーが発生する

エラー

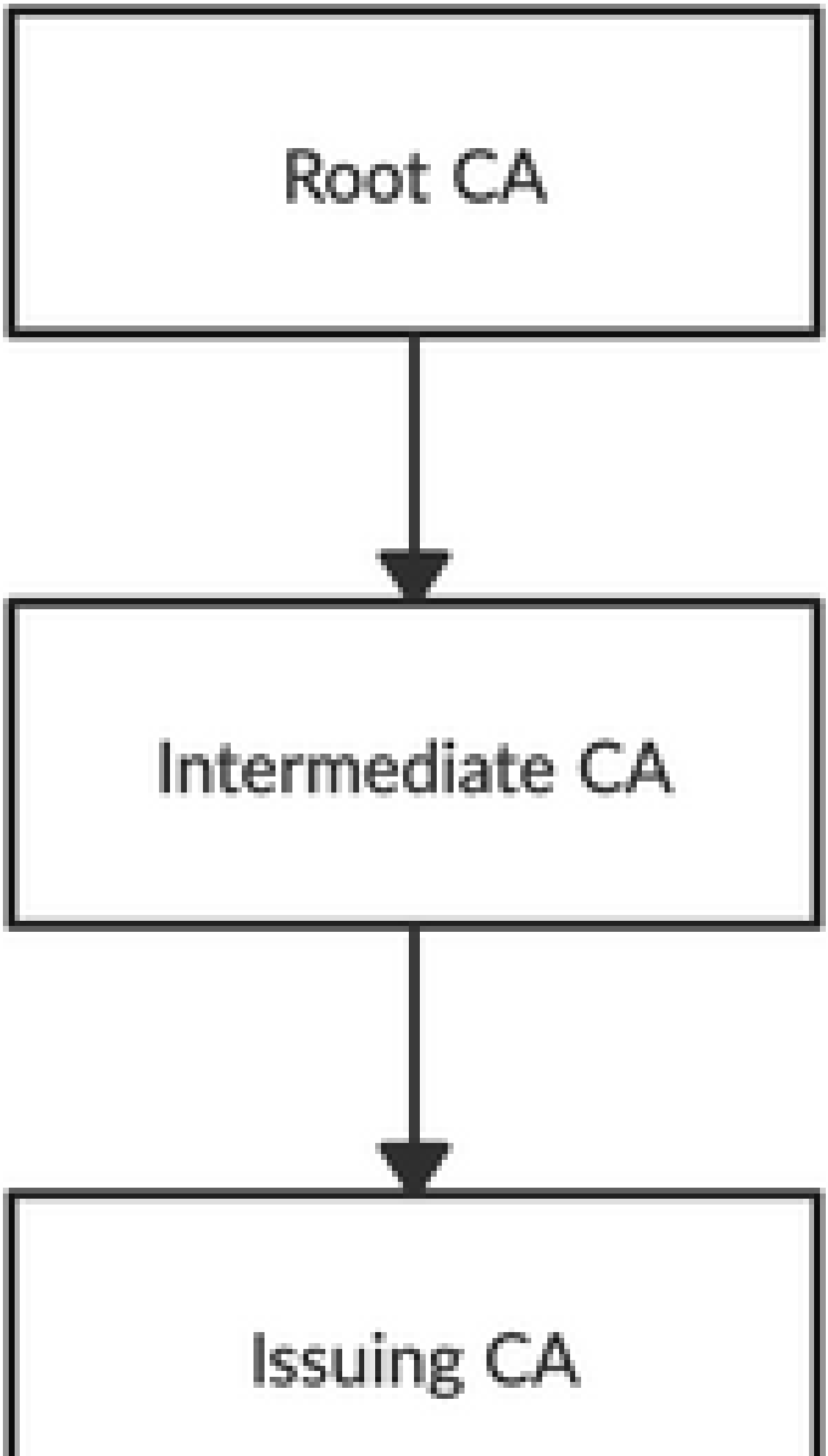
ポータルを使用するためのCA署名付き証明書のバインドで次のエラーがスローされます。

ポータルシステム証明書チェーンの一部であるか、同じサブジェクト名でシリアル番号が異なる証明書ベースの管理認証ロールを持つ、1つ以上の信頼された証明書があります。インポート/更新が中止されました。インポート/更新を正常に実行するには、カートベースの管理者認証ロールを重複した信頼できる証明書から無効にするか、またはチェーンに重複した信頼できる証明書を含むシステム証明書からポータルロールを変更する必要があります。

解決方法

ステップ 1：ポータルで使用するCA署名付き証明書の証明書チェーンを確認し、信頼できる証明書ストアで、証明書チェーンに重複する証明書がないか確認します。
ステップ 2：重複する証明書を削除するか、重複する証明書から証明書ベースの管理者認証の信頼チェックボックスをオフにします。

たとえば、CA署名付きポータル証明書には次の証明書チェーンがあります。


Root CA
Intermediate CA
Issuing CA

証明書の無効化、削除、または信頼は許可されません。これは、証明書がリモートログターゲットのシステム証明書またはセキュアSyslogターゲットのいずれかによって参照されているためです。

解決方法

1. 期限切れのデフォルトの自己署名証明書が、既存のリモートログターゲットに関連付けられていないことを確認します。これを確認するには、Administration > System > Logging > Remote Logging Targets > Select and Edit SecureSyslogCollector(s)
2. 期限切れのデフォルトの自己署名証明書が特定のロール（使用法）に関連付けられていないことを確認します。これは、Administration > System > Certificates > System Certificatesで確認できます。

それでも問題が解決しない場合は、TACにお問い合せください。

シナリオ5:CA署名付きpxGrid証明書をISEノードのCSRにバインドできない

エラー

新しいpxGrid証明書をCSRにバインドする際に、証明書のバインドプロセスがエラーで失敗します。

pxGridの証明書には、拡張キー使用法(EKU)拡張のクライアント認証とサーバ認証の両方が含まれている必要があります。

解決方法

CA署名付きpxGrid証明書は、クライアント認証とサーバ認証（pxGridクライアントとサーバ間の通信を保護するため）の両方に使用されるため、TLS Webサーバ認証(1.3.6.1.5.5.7.3.1)とTLS Webクライアント認証(1.3.6.1.5.5.7.3.2)の両方の拡張キー使用法を持っている必要があります

参照リンク：https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_011010.html

シナリオ6：既存のLDAPまたはSCEP RAプロファイル設定が原因で、期限切れのデフォルト自己署名証明書を信頼できる証明書ストアから削除できない

エラー

期限切れのデフォルトの自己署名証明書を信頼できる証明書ストアから削除すると、次のエラーが発生します。

信頼証明書は、SCEP RAプロファイルまたはLDAPアイデンティティソースから参照されている可能性があるため、削除できませんでした

*デフォルトの自己署名サーバ証明書

証明書を削除するには、SCEP RAプロファイルを削除するか、この証明書を使用しないようにLDAPアイデンティティソースを編集します。

解決方法

1. Administration > Identity Management > External Identity Sources > LDAP > Server Name > Connectionの順に移動します。
2. LDAPサーバのルートCAが「デフォルトの自己署名サーバ証明書」を使用していないことを確認します。
3. LDAPサーバがセキュア接続に必要な証明書を使用していない場合は、Administration > System > Certificates > Certificate Authority > External CA Settings > SCEP RA Profilesの順に移動します
4. SCEP RAプロファイルのいずれかがデフォルトの自己署名証明書を使用していないことを確認します

関連情報

ワイルドカード証明書をインストールする方法
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

ISE証明書の管理
https://www.cisco.com/c/en/us/td/docs/security/ise/2-6/admin_guide/b_ise_admin_guide_26/b_ise_admin_guide_26_chapter_0111.html

ISEへのサードパーティCA証明書のインストール
https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine-software/200295-Install-a-3rd-party-CA-certificate-in-IS.html

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。