HTTPS アクセス

この章の内容は、次のとおりです。

概要

この記事は、Cisco ACI を使用する際の HTTPS アクセスのカスタム証明書を設定する方法の例を示します。

カスタム証明書の設定のガイドライン

- ワイルドカード証明書（*.cisco.com など。複数のデバイス間で使用）およびそれに関連する他の場所で生成される秘密キーは、APIC ではサポートされません。これは、APIC に秘密キーまたはパスワードを入力するためのサポートがないためです。また、ワイルドカード証明書などのいかなる証明書の秘密キーもエクスポートできません。
- 証明書署名要求（CSR）を生成する前に、公開中間証明書とルート CA 証明書をダウンロードしてインストールする必要があります。ルート CA 証明書は技術的には CSR を生成するために必要ではありませんが、シスコでは、対象とする CA 機関と CSR への署名に使用される実物の間の不一致を防ぐために、CSR を生成する前にルート CA 証明書が必要です。APIC は、送信された証明書が設定されている CA によって署名されていることを確認します。
- 更新された証明書の生成に同じ公開キーと秘密キーを使用するには、次のガイドラインを満たす必要があります。
    - 元の CSR にはキー リング内の秘密キーとペアになる公開キーが含まれているため、元の CSR を維持する必要があります。

- APIC で公開キーと秘密キーを再利用する場合は、元の証明書に使用されたものと同じ CSR を、更新された証明書に関して再送信する必要があります。
- 更新された証明書に同じ公開キーと秘密キーを使用する場合は、元のキーリングを削除しないでください。キーリングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

- マルチサイト、VCPlugin、VRA、および SCVMM は、証明書ベースの認証ではサポートされません。
- ポッドあたり 1 つの証明書ベースのルートのみをアクティブにすることができます。
- 任意のリリースからリリース 4.0(1) へのダウングレードを実行する場合は、事前に証明書ベースの認証を無効にしておく必要があります。
- 証明書ベースの認証セッションを終了するには、ユーザはログアウトして CAC カードを削除する必要があります。

GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

注意：ダウンタイムの可能性があるため、メンテナンス時間中にのみこのタスクを実行してください。ダウンタイムは外部ユーザまたはシステムからの APIC クラスタおよびスイッチへのアクセスには影響しますが、APIC とスイッチの接続には影響しません。スイッチ上の NGINX プロセスも影響を受けますが、外部接続のみでファブリックのデータプレーンには影響ありません。APIC、設定、管理、トラブルシューティングなどへのアクセスは影響を受けることになります。この操作中にファブリック内のすべての Web サーバの再起動が予期されます。

始める前に

適切な認証局を作成できるように、信頼できる証明書を取得する機関を決定します。

手順

ステップ 1 メニュー バーで、**[Admin]** > **[AAA]** の順に選択します。

ステップ 2 [Navigation] ペインで、[Security] を選択します。

ステップ 3 [Work] ペインで、**[Public Key Management]** > **[Certificate Authorities]** > **[Create Certificate Authority]** を選択します。

ステップ 4 [Create Certificate Authority] ダイアログボックスの [Name] フィールドに、認証局の名前を入力します。

ステップ 5 [Certificate Chain] フィールドに、Application Policy Infrastructure Controller（APIC）の証明書署名要求（CSR）に署名する認証局の中間証明書およびルート証明書をコピーします。

証明書は、Base64 エンコード X.509（CER）形式である必要があります。中間証明書はルート CA 証明書の前に配置されます。次の例のようになります。

```
-----BEGIN CERTIFICATE-----
<Intermediate Certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root CA Certificate>
-----END CERTIFICATE-----
```

ステップ 6 [Submit] をクリックします。

ステップ 7 [Navigation] ペインで、**[Public Key Management]** > **[Key Rings]** の順に選択します。

ステップ 8 [Work] ペインで、**[Actions]** > **[Create Key Ring]** の順に選択します。

ステップ 9 [Create Key Ring] ダイアログボックスで、[Name] フィールドに、名前を入力します。

ステップ 10 [Certificate] フィールドには、コンテンツを追加しないでください。

ステップ 11 [Modulus] フィールドで、目的のキー強度のラジオボタンをクリックします。

ステップ 12 [Certificate Authority] フィールドのドロップダウン リストから、前に作成した認証局を選択します。[Submit] をクリックします。

（注） キー リングは削除しないでください。キー リングを削除すると、CSR で使用されている関連秘密キーが自動的に削除されます。

[Work] ペインの [Key Rings] 領域では、作成したキー リングに対する [Admin State] に [Started] と表示されます。

ステップ 13 [Navigation] ペインで、**[Public Key Management]** > **[Key Rings]** > ***[key_ring_name]*** の順に選択します。

ステップ 14 [Work] ペインで、**[Actions]** > **[Create Certificate Request]** の順に選択します。

ステップ 15 [Subject] フィールドに、APIC の完全修飾ドメイン名（FQDN）を入力します。

ステップ 16 必要に応じて、残りのフィールドに入力します。

（注） 使用可能なパラメータの説明については、[Create Certificate Request] ダイアログボックスでオンライン ヘルプ情報を確認してください。

ステップ 17 [Submit] をクリックします。
[Navigation] ペインでは、前に作成したキー リングの下にオブジェクトが作成され、表示されます。[Navigation] ペインでそのオブジェクトをクリックすると、[Work] ペインの [Properties] 領域の [Request] フィールドにその CSR が表示されます。認証局に送信するコンテンツをフィールドからコピーします。

ステップ 18 [Navigation] ペインで、**[Public Key Management]** > **[Key Rings]** > ***[key_ring_name]*** の順に選択します。

ステップ 19 [Work] ペインの [Certificate] フィールドに、認証局から受信した署名付き証明書を貼り付けます。

ステップ 20 [Submit] をクリックします。

（注） CSR がキー リングで示されている認証局によって署名されていない場合、または証明書に MS-DOS 形式の行末が含まれている場合は、エラー メッセージが表示され、証明書は承認されません。MS-DOS 形式の行末を削除します。

キーが確認されて [Work] ペインの [Admin State] が [Completed] に変わり、HTTP ポリシーを使用できるようになります。

ステップ 21 メニュー バーで、**[Fabric]** > **[Fabric Policies]** の順に選択します。

ステップ 22 [Navigation] ペインで、**[Pod Policies]** > **[Policies]** > **[Management Access]** > **[default]** の順に選択します。

ステップ 23 [Work] ペインの [Admin Key Ring] ドロップダウン リストで目的のキー リングを選択します。

ステップ 24 （オプション）証明書ベースの認証では、[Client Certificate TP] ドロップダウン リストで、以前に作成したローカル ユーザ ポリシーを選択し、[Client Certificate Authentication state] の [Enabled] をクリックします。

ステップ 25 [Submit] をクリックします。
すべての Web サーバが再起動されます。証明書がアクティブになり、デフォルト以外のキーリングが HTTPS アクセスに関連付けられています。

次のタスク

証明書の失効日には注意しておき、期限切れになる前に対応する必要があります。更新された証明書に対して同じキーペアを維持するには、CSR を維持する必要があります。これは、CSR にはキーリング内の秘密キーとペアになる公開キーが含まれているためです。証明書が期限切れになる前に、同じ CSR を再送信する必要があります。キー リングを削除すると、APIC に内部的に保存されている秘密キーも削除されるため、新しいキー リングの削除または作成は行わないでください。

NX-OS CLI を使用した証明書ベースの認証の有効化

手順

証明書ベースの認証を有効にするには、次の手順を実行します。

例：

```
To enable CAC for https access:
  configure terminal
   comm-policy default
    https
     client-cert-ca <ca name>
     client-cert-state-enable
 To disable:
  configure terminal
   comm-policy default
    https
```

```
no client-cert-state-enable
no client-cert-ca
```