



Cisco Cloud APIC セキュリティ

この章は、次の内容で構成されています。

- [アクセス、認証およびアカウントティング](#) (1 ページ)
- [TACACS+、RADIUS、LDAP、および SAML アクセスの構成](#) (2 ページ)
- [HTTPS Access の構成](#) (11 ページ)

アクセス、認証およびアカウントティング

Cisco Cloud Application Policy Infrastructure Controller (Cloud APIC) ポリシーは、認証、認可、アカウントティング (AAA) 機能を管理します。ユーザ権限、ロール、およびドメインとアクセス権限の継承を組み合わせることにより、管理者は細分化された方法で管理対象オブジェクトレベルで AAA 機能を設定することができます。これらの設定は、REST API または GUI を使用して実行できます。



- (注) ログインドメイン名に 32 文字を超えることはできないという既知の制限があります。また、ログインドメイン名とユーザ名を合わせた文字数は 64 文字を超えることはできません。

アクセス、認証、およびアカウント構成情報の詳細については、<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> の *Cisco APIC Security Configuration Guide, Release 4.0(1)* をお読みください。

構成

初期構成スクリプトで、管理者アカウントが構成され、管理者はシステム起動時の唯一のユーザとなります。

ローカル ユーザの設定

[Cisco Cloud APIC GUI を使用したローカル ユーザーの作成](#) を参照して、ローカル ユーザーを設定し、Cisco Cloud APIC GUI を使用して OTP、SSH 公開キー、および X.509 ユーザー証明書に関連付けます。

TACACS+、RADIUS、LDAP、および SAML アクセスの構成

次のトピックは、Cisco Cloud APIC の TACACS+、RADIUS、LDAP および SAML アクセスを構成する方法を説明します。

概要

このトピックでは、RADIUS、TACACS+、LDAP、および SAML ユーザー（ADFS、Okta、PingID など）の Cisco Cloud APIC へのアクセスを有効にする方法について、順を追って説明します。

TACACS+、RADIUS、LDAP、および SAML の詳細については、<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> の『Cisco APIC セキュリティ構成ガイド、リリース 4.0(1)』を参照してください。

Cloud APIC for TACACS+ Access の構成

始める前に

- Cloud Application Policy Infrastructure Controller (Cloud APIC) はオンラインになっています。
- TACACS+ サーバのホスト名または IP アドレス、ポート、およびキーを使用できること。
- Cloud APIC 管理エンドポイント グループが使用できます。

ステップ 1 クラウド APIC で、TACACS+ プロバイダーを作成します。

- メニューバーで、[管理 (Administrative)] > [認証 (Authentication)] を選択します。
- 作業ペインで、[プロバイダー (Providers)] タブをクリックして、[アクション (Actions)] ドロップダウンをクリックして、[プロバイダーの作成 (Create Provider)] を選択します。
[プロバイダーの作成 (Create Provider)] ダイアログボックスが表示されます。
- [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- [説明 (Description)] フィールドに、プロバイダーの説明を入力します。
- [タイプ (Type)] ドロップダウンリストをクリックし、[TACACS+] を選択します。
- [設定 (Settings)] セクションで、[キー (Key)]、[ポート (Port)]、[認証プロトコル (Authentication Protocol)]、[タイムアウト (Timeout)]、[再試行 (Retries)]、[管理 EPG (Management EPG)] を

指定します。有効化 (Enabled) または 無効化 (Disabled) のいずれかを [サーバー監視 (Server Monitoring)] に対して選択します。

ステップ 2 TACACS+ の [Login Domain] を作成します。

- a) インテント アイコンをクリックします。
[インテント (Intent)] メニューが表示されます。
- b) [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。
[Intent]メニューに管理オプションのリストが表示されます。
- c) [インテント (Intent)]メニューの[管理 (Administrative)]リストで、[ログインドメインの作成 (Create Login Domain)]をクリックします。
[ログインドメインの作成 (Create Login Domains)]ダイアログボックスが表示されます。
- d) 次の[ログインドメインダイアログボックスのフィールド (Login Domains Dialog Box Fields)]のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
Settings	
Realm	ドロップダウンメニューから TACACS+ を選択します。
プロバイダ (Providers)	<p>プロバイダーを選択するには :</p> <ol style="list-style-type: none"> 1. [プロバイダーの追加 (Add Providers)] をクリックします。[プロバイダーの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

- e) [保存 (Save)] をクリックして、設定を保存します。

次のタスク

これで、APIC TACACS+ 構成手順は完了です。次に、RADIUS サーバーも使用する場合は、RADIUS の APIC を設定します。

Cloud APIC for RADIUS Access の構成

始める前に

- Cloud Application Policy Infrastructure Controller (Cloud APIC) はオンラインになっています。
- RADIUS サーバーのホスト名または IP アドレス、ポート、およびキーを使用できること。
- Cloud APIC 管理エンドポイント グループが使用できます。

ステップ 1 Cloud APIC で、RADIUS プロバイダーを作成します。

- メニューバーで、[管理 (Administrative)] > [認証 (Authentication)] を選択します。
- 作業ペインで、[プロバイダー (Providers)] タブをクリックして、[アクション (Actions)] ドロップダウンをクリックして、[プロバイダーの作成 (Create Provider)] を選択します。
[プロバイダーの作成 (Create Provider)] ダイアログボックスが表示されます。
- [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- [説明 (Description)] フィールドに、プロバイダーの説明を入力します。
- [タイプ (Type)] ドロップダウンリストをクリックし、[RADIUS] を選択します。
- [設定 (Settings)] セクションで、[キー (Key)]、[ポート (Port)]、[認証プロトコル (Authentication Protocol)]、[タイムアウト (Timeout)]、[再試行 (Retries)]、[管理 EPG (Management EPG)] を指定します。有効化 (Enabled) または無効化 (Disabled) のいずれかを [サーバー監視 (Server Monitoring)] に対して選択します。

ステップ 2 RADIUS の [ログイン ドメイン] を作成します。

- intent アイコンをクリックします。
[intent (Intent)] メニューが表示されます。
- [intent (Intent)] 検索ボックスの下にあるドロップダウン矢印をクリックし、[管理 (Administrative)] を選択します。
[intent] メニューに管理オプションのリストが表示されます。
- [intent (Intent)] メニューの [管理 (Administrative)] リストで、[ログイン ドメインの作成 (Create Login Domain)] をクリックします。
[ログイン ドメインの作成 (Create Login Domains)] ダイアログボックスが表示されます。
- 次の [ログイン ドメインダイアログボックスのフィールド (Login Domains Dialog Box Fields)] のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
Settings	
Realm	ドロップダウンメニューから RADIUS を選択します。
プロバイダ (Providers)	<p>プロバイダーを選択するには：</p> <ol style="list-style-type: none"> 1. [プロバイダーの追加 (Add Providers)] をクリックします。[プロバイダーの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

e) [保存 (Save)] をクリックして、設定を保存します。

次のタスク

これで、Cloud APIC RADIUS 構成手順は完了です。次に、RADIUS サーバを設定します。

Cloud APIC への RADIUS および TACACS+ アクセス用の Cisco Secure Access Control Server の設定

『Cisco APIC Security Configuration Guide, Release 4.0 (1)』の「Configuring a Cisco Secure Access Control Server for RADIUS and TACACS + Access to the APIC」の項を </docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で参照してください。

LDAP Access の構成

LDAP 設定には 2 つのオプションがあります。

- Cisco AVPair の設定
- Cisco Cloud ネットワーク コントローラで LDAP グループ マップを構成する

次のセクションには、両方の構成オプションの手順が含まれています。

Cisco AVPair を使用した APIC アクセス用の Windows Server 2008 LDAP の設定

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-security/Cisco-APIC-Security-Configuration-Guide-401.html>にある『Cisco APIC Security Configuration Guide, Release 4.0(1)』の「Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair」を参照してください。

LDAP アクセスのための Cisco Cloud Network Controller の構成

始める前に

- Cisco Cloud Network Controller はオンラインです。
- LDAP サーバのホスト名または IP アドレス、ポート、バインド DN、ベース DN、およびパスワードを使用できること。
- Cisco Cloud Network Controller 管理エンドポイント グループが利用できます。

ステップ 1 Cisco Cloud Network Controller で、[LDAP プロバイダ (LDAP Provider)] を作成します。

- a) メニューバーで、[管理 (Administrative)] > [認証 (Authentication)] を選択します。
- b) 作業ペインで、[プロバイダー (Providers)] タブをクリックして、[アクション (Actions)] ドロップダウンをクリックして、[プロバイダーの作成 (Create Provider)] を選択します。

[プロバイダーの作成 (Create Provider)] ダイアログボックスが表示されます。

- c) [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- d) [説明 (Description)] フィールドに、プロバイダーの説明を入力します。
- e) [タイプ (Type)] ドロップダウンリストをクリックし、[LDAP] を選択します。
- f) バインド DN、ベース DN、パスワード、ポート、属性、フィルタタイプ、および管理 EPG を指定します。

- (注)
- バインド DN は、Cisco Cloud Network Controller が LDAP サーバにログインするために使用する文字列です。Cisco Cloud Network Controller は、ログインしようとするリモートユーザーの検証にこのアカウントを使用します。ベース DN は、Cisco Cloud Network Controller がリモートユーザー アカウントを検索する LDAP サーバのコンテナ名とパスです。これはパスワードが検証される場所です。フィルタを使用して、Cisco Cloud Network Controller が *cisco-av-pair* に使用するために要求している属性を見つけます。これには、Cisco Cloud Network Controller で使用するユーザー認証と割り当て済み RBAC ロールが含まれます。Cisco Cloud Network Controller は、この属性を LDAP サーバから要求します。
 - [属性] フィールド：次のうちいずれかを入力します。
 - LDAPサーバの設定では、Cisco AVPair、入力 **CiscoAVPair**。
 - LDAP グループ マップ LDAPサーバ設定、入力 **memberOf**。

ステップ 2 LDAP の ログイン ドメイン を作成します。

- a) メニュー バーで、[管理 (Administrative)] > [認証 (Authentication)] を選択します。
- b) [Work] ペインで、[Login Domains] タブをクリックし、[Actions] ドロップダウンをクリックして [Create Login Domain] を選択します。
- c) 次の [ログイン ドメイン ダイアログボックスのフィールド (Login Domains Dialog Box Fields)] のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
Settings	
Realm	ドロップダウンメニューから [LDAP] 選択します。
プロバイダ (Providers)	<p>プロバイダーを選択するには：</p> <ol style="list-style-type: none"> 1. [プロバイダーの追加 (Add Providers)] をクリックします。[プロバイダーの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

[プロパティ (Properties)]	説明
認証タイプ	<ol style="list-style-type: none"> 1. プロバイダーが属性として CiscoAVPair を使用して設定されている場合は、[Cisco AV ペア (Cisco AV Pairs)] を選択します。 2. プロバイダーが属性として memberOf で設定されている場合は、[LDAP Group Map Rules] を選択します。 <ol style="list-style-type: none"> 1. [LDAP グループ マップ ルールの追加 (Add LDAP Group Map Rule)] をクリックします。ダイアログボックスが表示されます。 2. マップの名前と説明 (オプション) および グループ DN を指定します。 3. [セキュリティ ドメインの追加 (Add Security Domain)] の横にある [+] をクリックします。ダイアログボックスが表示されます。 4. [+] をクリックして、[ロール (Role)] の名前およびロールの [権限 (Privilege)] タイプ (Read または Write) フィールドにアクセスします。チェックマークをクリックします。 5. さらにロールを追加するには、手順 4 を繰り返します。次に、[追加 (Add)] をクリックします。 6. 手順 3 を繰り返して、さらにセキュリティ ドメインを追加します。次に、[追加 (Add)] をクリックします。

- d) [ログイン ドメインの作成 (Create Login Domain)] ダイアログボックスで [**保存 (Save)**] をクリックします。

Cloud APIC for SAML Access の構成

次のセクションでは、SAML Access 用の Cloud APIC の設定について詳しく説明します。

SAML について

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0(1)』の「About SAML」セクションを参照してください。

SAML の基本要素

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0(1)』の「Basic Elements of SAML」セクションを参照してください。

サポートされている IdPs および SAML コンポーネント

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0(1)』の「Supported IdPs and SAML Components」セクションを参照してください。

Cloud APIC for SAML Access の構成



(注) SAML ベースの認証は Rest に対するものではなく、Cloud APIC GUI のみに対するものです。

始める前に

- SAML サーバー ホスト名または IP アドレスと、IdP メタデータの URL を使用できます。
- Cloud APIC 管理エンドポイント グループが使用できます。
- 次の設定を行います。
 - 時刻同期と NTP
 - GUI を使用した DNS プロバイダーの構成
 - GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定

ステップ 1 Cloud APIC で、SAML プロバイダーを作成します。

- a) メニューバーで、[管理 (Administrative)] > > [認証 (Authentication)] を選択します。
- b) [作業 (Work)] ペインで、[プロバイダー (Providers)] タブをクリックし、[アクション (Actions)] ドロップダウンをクリックして [プロバイダーの作成 (Create Provider)] を選択します。
- c) [ホスト名/IP アドレス (Host name/IP Address)] フィールドに、プロバイダーのホスト名/IP アドレスを入力します。
- d) [説明 (Description)] フィールドに、プロバイダーの説明を入力します。
- e) [タイプ (Type)] ドロップダウンリストをクリックし、[SAML] を選択します。

- f) [設定 (Settings)] ペインで、次の手順を実行します。
- IdP メタデータ URL を指定します。
 - AD FS の場合、IdP メタデータ URL は `https://<FQDN ofADFS>/FederationMetadata/2007-06/FederationMetadata.xml` という形式になります。
 - Okta の場合、IdP メタデータの URL を取得するには、Okta サーバから該当 SAML アプリケーションの [Sign On] セクションに、**アイデンティティ プロバイダー メタデータ** のリンクをコピーします。
 - SAML ベースのサービスの **エンティティ ID** を指定します。
 - IdP メタデータの URL にアクセスする必要がある場合は、**メタデータ URL の HTTPS プロキシ (HTTPS Proxy for Metadata URL)** を構成します。
 - IdP はプライベート CA によって署名された場合は、**[認証局 (Certificate Authority)]** を選択します。
 - ドロップダウン リストから、**[署名アルゴリズム認証ユーザー要求 (Signature Algorithm Authentication User Requests)]** を選択します。
 - **SAML 認証要求の署名、SAML 応答メッセージの署名、SAML 応答の署名アサーション、SAML アサーションの暗号化** を有効にするには、チェックボックスをオンにします。
- g) [保存 (Save)] をクリックして、設定を保存します。

ステップ 2 SAML のログインドメインを作成します。

- a) メニューバーで、**[管理 (Administrative)] > [認証 (Authentication)]** を選択します。
- b) 作業ペインで、**[ログインドメイン (Login Domains)]** タブをクリックして、**[アクション (Actions)]** ドロップダウンをクリックして、**[ログインドメインの作成 (Create Login Domains)]** を選択します。
- c) 次の **[ログインドメインダイアログボックスのフィールド (Login Domains Dialog Box Fields)]** のテーブルにリストされた各フィールドに適切な値を入力し、続行します。

[プロパティ (Properties)]	説明
全般	
名前	ログインドメインの名前を入力します
説明	ログインドメインの説明を入力します。
Settings	
Realm	ドロップダウンメニューから SAML を選択します。

[プロパティ (Properties)]	説明
プロバイダ (Providers)	プロバイダーを選択するには : <ol style="list-style-type: none"> 1. [プロバイダーの追加 (Add Providers)] をクリックします。[プロバイダーの選択 (Select Providers)] ダイアログが表示されます。 2. クリックして、左側の列のプロバイダーを選択します。 3. [選択 (Select)] をクリックします。[ログインドメインの作成] ダイアログボックスに戻ります。

d) [保存 (Save)] をクリックして、設定を保存します。

Okta で SAML アプリケーションの設定

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0(1)』のセクション「Setting Up a SAML Application」を参照してください。

AD FS で Relying Party Trust の設定

<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> で『Cisco APIC Security Configuration Guide、Release 4.0 (1)』の「Setting Up a Relying Party Trust in AD FS」セクションを参照してください。

HTTPS Access の構成

ここでは、HTTPS Access を構成する方法について説明します。

HTTPSアクセスについて

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。

詳細については、<https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/4-x/security/Cisco-APIC-Security-Configuration-Guide-401.html> の『*Cisco APIC Security Configuration Guide, Release 4.0(1)*』の「*HTTPS Access*」の項を参照してください。

カスタム証明書の構成のガイドライン

- 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、Cisco Cloud APIC ではサポートされません。これは、Cisco Cloud 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。Cisco Cloud APIC は、送信された証明書が設定された 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。
 - Cisco Cloud APIC で公開キーと秘密キーを再使用する場合は、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。
- 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。
- このリリースでは、クライアント証明書認証はサポートされていません。

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

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。

始める前に

注意：ダウンタイムの可能性があるので、メンテナンス時間中のみこのタスクを実行してください。この操作中に Cloud APIC のすべての Web サーバの再起動が予期されます。

ステップ 1 メニューバーで、[管理 (Administrative)] > セキュリティ (Security)] を選択します。

- ステップ 2 [作業 (Work)] ペインで、[証明書認証局 (Certificate Authorities)] タブをクリックし、[アクション (Actions)] ドロップダウンをクリックして [証明書認証局の作成 (Create Certificate Authorities)] を選択します。
- ステップ 3 [証明書認証局の作成 (Create Certificate Authority)] ダイアログボックスの [名前 (Name)] フィールドに、認証局の名前を入力します。
- ステップ 4 [用途 (Used for)] フィールドで [システム (System)] を選択します。
- ステップ 5 [証明書チェーン (Certificate Chain)] フィールドに、クラウドアプリケーション ポリシー インフラストラクチャコントローラー (APIC) の証明書署名要求 (CSR) に署名する認証局の中間証明書と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 [保存 (Save)] をクリックします。
- ステップ 7 メニューバーで、[管理 (Administrative)] > [セキュリティ (Security)] を選択します。
- ステップ 8 [作業 (Work)] ペインで、[キー リング (Key Rings)] タブをクリックし、[アクション (Actions)] ドロップダウンをクリックして [キー リングの作成 (Create Key Ring)] を選択します。
- ステップ 9 [キー リングの作成 (Create Key Ring)] ダイアログボックスで、[名前 (Name)] フィールドにキー リングの名前を入力し、[説明 (Description)] フィールドに説明を入力します。
- ステップ 10 [用途 (Used for)] フィールドで [システム (System)] を選択します。
- ステップ 11 [証明書認証局 (Certificate Authority)] フィールドで、[証明書認証局の選択 (Select Certificate Authority)] をクリックし、以前に作成した認証局を選択します。
- ステップ 12 [秘密キー (Private Key)] フィールドで、[新規キーの生成 (Generate New Key)] または [既存のキーのインポート (Import Existing Key)] を選択します。[既存のキーのインポート (Import Existing Key)] を選択した場合は、[秘密キー (Private Key)] テキスト ボックスに秘密キーを入力します。
- ステップ 13 [モジュラス (Modulus)] ドロップダウンからモジュラスを選択します。メニュー
- ステップ 14 [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 15 [保存 (Save)] をクリックします。
- [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 16 作成したキー リングをダブルクリックして、[作業 (Work)] ペインから [キー リング] [key\_ring\_name] ダイアログボックスを開きます。
- ステップ 17 [作業 (Work)] ペインで、[証明書要求の作成 (Create Certificate Request)] をクリックします。
- ステップ 18 [情報カテゴリ (Subject)] フィールドに、Cloud APIC の完全修飾ドメイン名 (FQDN) を入力します。
- ステップ 19 必要に応じて、残りのフィールドに入力します。
- ステップ 20 [保存 (Save)] をクリックします。
- [Key Ring] [key\_ring\_name] ダイアログボックスが表示されます。

- ステップ 21 フィールド [要求 (Request)] からコンテンツを署名するために証明書認証局 にコピーします。
- ステップ 22 [キー リング (Key Ring)] [key\_ring\_name] ダイアログボックスで、[編集 (Edit)] アイコンをクリックして [キー リング (Key Ring)] [key\_ring\_name] ダイアログボックスを表示します。
- ステップ 23 [証明書 (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 24 [保存 (Save)] をクリックして、[キー リング (Key Rings)] 作業ウィンドウに戻ります。
- キーが確認されて [作業 (Work)] ペインで [管理状態 (Admin State)] が [完了済み (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 25 [インフラストラクチャ (Infrastructure)] > [システム構成 (System Configuration)] に移動し、[管理アクセス (Management Access)] タブをクリックします。
- ステップ 26 [HTTPS] 作業ウィンドウの編集アイコンをクリックして、[HTTPS 設定 (HTTPS Settings)] ダイアログボックスを表示します。
- ステップ 27 [管理キー リング (Admin Key Ring)] をクリックし、以前に作成したキー リングを関連付けます。
- ステップ 28 [保存 (Save)] 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、Cloud 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。

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。