Cisco Cloud Network Controller のセキュリティ

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、アカウンティング（AAA）機能を管理します。管理者は、ユーザ権限、ロール、ドメインとアクセス権限の継承機能を組み合わせることで、管理対象オブジェクトレベルで細かく AAA 機能を設定できます。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。

設定

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ーとなります。

ローカル ユーザの設定

Cisco Cloud Network Controller 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、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

次のトピックでは、Cloud APIC の TACACS+、RADIUS、LDAP、および SAML アクセスを設定する方法について説明します。

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 Network Controller 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、[Cisco Cloud Network Controller セキュリティ構成ガイド（Cisco Cloud Network Controller Security Configuration Guide）] を参照してください。

。

Configuring Cloud APIC for TACACS+ Access

Before you begin

- The Cloud Application Policy Infrastructure Controller (Cloud APIC) is online.
- The TACACS+ server host name or IP address, port, and key are available.
- The Cloud APIC management endpoint group is available.

ステップ 1 In the Cloud APIC, create the **TACACS+ Provider**.

a) On the menu bar, choose **Administrative** > **Authentication**.
b) In the Work pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.

The **Create Provider** dialog box appears.

c) In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.
d) In the **Description** field, enter a description of the provider.
e) Click the **Type** drop-down list and choose **TACACS+**.
f) In **Settings** section, specify the **Key**, **Port**, **Authentication Protocol**, **Timeout**, **Retries**, **Management EPG**. Select either **Enabled** or **Disabled** for **Server Monitoring**.

ステップ 2 Create the **Login Domain** for TACACS+.

a) Click the **Intent** icon.

The **Intent** menu appears.

b) Click the drop-down arrow below the **Intent** search box and choose **Administrative**.

A list of **Administrative** options appear in the **Intent** menu.

c) From the **Administrative** list in the **Intent** menu, click **Create Login Domain**.

The **Create Login Domain** dialog box appears.

d) Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

Properties	Description
General	
Name	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
Settings	
Realm	Choose **TACACS+** from the dropdown menu
Providers	To choose a Provider(s): **1.** Click **Add Providers**. The **Select Providers** dialog appears. **2.** Click to choose a provider(s) in the column on the left. **3.** Click **Select**. You return to the **Create Login Domain** dialog box.

e) Click **Save** to save the configuration.

What to do next

This completes the APIC TACACS+ configuration steps. Next, if a RADIUS server will also be used, configure the APIC for RADIUS.

Configuring Cloud APIC for RADIUS Access

Before you begin

- The Cloud Application Policy Infrastructure Controller (Cloud APIC) is online.
- The RADIUS server host name or IP address, port, and key are available.
- The Cloud APIC management endpoint group is available.

ステップ 1 In the Cloud APIC, create the **RADIUS Provider**.

a) On the menu bar, choose **Administrative** > **Authentication**.

b) In the Work pane, click on **Providers** tab and then click on the **Actions** drop-down and select **Create Provider**.

The **Create Provider** dialog box appears.

c) In the **Host Name/IP Address** field, enter the Host Name/IP Address of the provider.

d) In the **Description** field, enter a description of the provider.

e) Click the **Type** drop-down list and choose **RADIUS**.

f) In the **Settings** section, specify the **Key**, **Port**, **Authentication Protocol**, **Timeout**, **Retries**, **Management EPG**. Select either **Enabled** or **Disabled** for **Server Monitoring**.

ステップ 2 Create the **Login Domain** for **RADIUS**.

a) Click the **Intent** icon.

The **Intent** menu appears.

b) Click the drop-down arrow below the **Intent** search box and choose **Administrative**

A list of **Administrative** options appear in the **Intent** menu.

c) From the **Administrative** list in the **Intent** menu, click **Create Login Domain**.

The **Create Login Domain** dialog box appears.

d) Enter the appropriate values in each field as listed in the following *Create Login Domain Dialog Box Fields* table then continue.

Properties	Description
General	
Name	Enter the name of the Login Domain
Description	Enter the description of the Login Domain.
Settings	
Realm	Choose **RADIUS** from the dropdown menu
Providers	To choose a Provider(s): **1.** Click **Add Providers**. The **Select Providers** dialog appears. **2.** Click to choose a provider(s) in the column on the left. **3.** Click **Select**. You return to the **Create Login Domain** dialog box.

e) Click **Save** to save the configuration.

What to do next

This completes the Cloud APIC RADIUS configuration steps. Next, configure the RADIUS server.

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
- クラウド APIC での LDAP グループ マップの設定

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

Cisco Cloud Network Controller Security Configuration Guideの*[Cisco AVPair を使用した APIC アクセスのための Windows Server 2008 LDAP の設定（Configuring Windows Server 2008 LDAP for APIC Access with Cisco AVPair）]*セクションを参照してください。

Cloud APIC for LDAP 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。
- 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。
- 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、**LDAP 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、Cloud APIC が LDAP サーバーにログインするために使用する文字列です。Cloud APIC 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、Cloud APIC がリモート ユーザー アカウントを検索する LDAP サーバー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、Cloud APIC 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、Cloud APIC 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。Cloud APIC 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作成のフィールド（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。
[設定（Settings）]	
レルム	ドロップダウン メニューから **[LDAP]** 選択します。

[プロパティ（Properties）]	説明
プロバイダー	プロバイダーを選択するには、次の手順を実行します。 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. 左側の列でプロバイダーをクリックして選択します。 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。

認証タイプ（Authentication Type）	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。
	    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。

SAML Access 用の APIC の設定

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

Cisco Cloud Network Controller Security Configuration Guideの*[SAML について（About SAML）]*セクションを参照してください。

SAML の基本要素

Cisco Cloud Network Controller Security Configuration Guideの*[SAML のベーシック エレメント（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

Cisco Cloud Network Controller Security Configuration Guideの*[サポートされている IdPs and SAML コンポーネント（Supported IdPs and SAML Components）]*セクションを参照してください。

Configuring APIC for SAML Access

Note SAML based Authentication is only for APIC GUI and not for CLI/REST. Also, not applicable for LEAF Switches and SPINEs. SAML configuration cannot be done via APIC CLI.

Before you begin

- The Cisco Application Centric Infrastructure (ACI) fabric is installed, Application Policy Infrastructure Controllers (APICs) are online, and the APIC cluster is formed and healthy.
- The SAML server host name or IP address, and the IdP's metadata URL are available..
- The APIC management endpoint group is available.
- Set up the following:
  - Time Synchronization and NTP: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3-x/basic_config/b_APIC_Basic_Config_Guide_3_x/b_APIC_Basic_Config_Guide_3_x_chapter_011.html#concept_9CE11B84AD78486AA7D83A7DE1CE2A77.
  - Configuring a DNS Service Policy to Connect with DNS Providers Using the Advanced GUI: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3-x/basic_config/b_APIC_Basic_Config_Guide_3_x/b_APIC_Basic_Config_Guide_3_x_chapter_011.html#task_750E077676704BFBB5B0FE74628D821E.

- Configuring a Custom Certificate for Cisco ACI HTTPS Access Using the GUI: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3-x/basic_config/b_APIC_Basic_Config_Guide_3_x/b_APIC_Basic_Config_Guide_3_x_chapter_011.html#task_F037F1B75FF74ED1BCA4F3C75A16C0FA.

ステップ 1 In the APIC, create the SAML provider.

ステップ 2 Create the **Login Domain** for SAML.

Okta で SAML アプリケーションの設定

Cisco Cloud Network Controller Security Configuration Guide の *[Okta のSAML アプリケーションの設定（Setting Up a SAML Application in Okta）]*セクション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。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。