RADIUS、TACACS+、LDAP、RSA、SAML、OAuth 2、DUO

この章は、次の項で構成されています。

概要

この記事では、RADIUS、TACACS+、LDAP、RSA、DUO、SAML、OAuth 2 ユーザーが APIC にアクセスできるようにする方法について、順を追って説明します。読者が *Cisco* プリケーション セントリック インフラストラクチャの基礎マニュアル、特にユーザー アクセス権、認証、アカウンティングの章を十分に利害していると仮定しています。

Cisco APIC リリース 6.0(1) から、**[管理（Admin）]** > **[AAA]** のパスの APIC GUI が変更されました。詳細については、Cisco APIC GUI の機能強化を参照してください。

（注） クラスタ内の 1 つを除くすべての APIC が失われるなどの障害シナリオの場合、APIC はリモート認証を無効にします。このシナリオでは、ローカル管理者アカウントのみがファブリック デバイスにログインできます。

（注） セキュリティ上の理由により、AAA 認証に shell:domains=all/read-all/ を使用するリモートユーザは、ファブリック内のリーフ スイッチおよびスパイン スイッチにアクセスすることはできません。このことは、4.0(1h) までのすべてのバージョンに当てはまります。

APIC Bash シェルのユーザ ID

APIC での Linux シェル用のユーザ ID は、ローカル ユーザ用に APIC 内で生成されます。認証クレデンシャルが外部サーバで管理されているユーザは、Linux シェル用のユーザ ID を cisco-av-pair で指定できます。上記の cisco-av-pair の（16001）を省略することは、リモートユーザがデフォルトの Linux ユーザ ID 23999 を取得すれば可能です。Linux ユーザ ID がバッシュ セッション中に使用され、標準の Linux 権限が適用されます。また、ユーザが作成するすべての管理対象オブジェクトは、そのユーザの Linux ユーザ ID によって作成されたとマークされます。

次に、APIC Bash シェルに表示されるユーザ ID の例を示します。

```
admin@ifav17-ifc1:~> touch myfile
admin@ifav17-ifc1:~> ls -l myfile
-rw-rw-r-- 1 admin admin 0 Apr 13 21:43 myfile
admin@ifav17-ifc1:~> ls -ln myfile
-rw-rw-r-- 1 15374 15374 0 Apr 13 21:43 myfile
admin@ifav17-ifc1:~> id
uid=15374(admin) gid=15374(admin) groups=15374(admin)
```

外部認証サーバの AV ペア

Cisco APIC では、管理者が外部認証サーバで Cisco AV ペアを設定する必要があります。Cisco AV ペアは、ユーザの RBAC ロールおよび権限に必要な APIC を指定します。Cisco AV ペアの形式は、RADIUS、LDAP、または TACACS+ のものと同じです。

外部認証サーバで Cisco AV ペアを設定するには、管理者が既存のユーザ レコードに Cisco AV ペアを追加します。Cisco AV ペアの形式は次のとおりです。

```
shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,
domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2
shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,
domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2(16003)
```

Cisco APIC リリース 2.1 より、AV ペアで UNIX ID が指定されていない場合は、APIC が固有の UNIX ユーザー ID を内部的に割り当てます。

（注） APIC の Cisco AV ペアの形式は互換性があり、他の Cisco AV ペアの形式と共存できます。APIC はすべての AV ペアから最初に一致した AV ペアを選択します。

リリース 3.1(x) 以降、AV Pair shell:domains=all//admin を使用すると、ユーザに読み取り専用権限を割り当て、スイッチにアクセスしてコマンドを実行できます。

APIC は、次の正規表現をサポートしています。

```
shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?)(,\\S+?/\\S*?/\\S*?){0,31})(\\(\\d+\\))$
shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?)(,\\S+?/\\S*?/\\S*?){0,31})$
```

例：

- 例 1：writeRoles のみを持つ単一のセキュリティ ドメインを含む Cisco AV ペア：

```
shell:domains=domainA/writeRole1|writeRole2/
```

- 例 2：readRoles のみを持つ単一のセキュリティ ドメインを含む Cisco AV ペア：

```
shell:domains=domainA//readRole1|readRole2
```

（注） 「/」文字は、セキュリティ ドメインごとの writeRoles と readRoles の間の区切り文字であり、1 つのタイプのロールのみを使用する場合でも必要です。

Cisco AV ペアの文字列は、大文字と小文字が区別されます。エラーが表示されなくても、使用する大文字と小文字がドメイン名またはロールに一致していない場合は、予期しない権限が付与されることがあります。

オープン RADIUS サーバ（/etc/raddb/users）の設定例は次のとおりです。

```
aaa-network-admin Cleartext-Password := "<password>"
Cisco-avpair = "shell:domains = all/aaa/read-all(16001)"
```

AV ペアを割り当てるためのベスト プラクティス

ベスト プラクティスとして、

Cisco は、bash シェルでユーザに割り当てられる AV ペアには 16000 ～ 23999 の範囲の一意の UNIX ユーザ ID を割り当てることを推奨します（SSH、Telnet または Serial/KVM のコンソールを使用）。Cisco AV ペアが UNIX ユーザ ID を提供しない状況が発生すると、そのユーザにはユーザ ID 23999 または範囲内の類似した番号が割り当てられます。これにより、そのユー

ザのホーム ディレクトリ、ファイル、およびプロセスに UNIX ID 23999 を持つリモート ユーザがアクセスできるようになってしまいます。

リモート認証サーバがその av ペアを cisco 応答 UNIX ID を明示的に指定していないことを確認するには、(リモート ユーザ アカウントを使用) は、管理者として、APIC とログインへの SSH セッションを開きます。ログインすると、次のコマンド (置換」ユーザ id「ログに記録するユーザ名と) を実行します。

```
admin@apic1:remoteuser-userid> cd /mit/uni/userext/remoteuser-userid
admin@apic1:remoteuser-userid> cat summary
```

Cisco AV ペアの文字列は、大文字と小文字が区別されます。エラーが表示されなくても、使用する大文字と小文字がドメイン名またはロールに一致していない場合は、予期しない権限が付与されることがあります。

外部認証サーバの AV ペアの設定

属性/値（AV）のペア文字列のカッコ内の数字は、セキュア シェル（SSH）または Telnet を使用してログインしたユーザの UNIX ユーザ ID として使用されます。

手順の概要

1. 外部認証サーバの AV ペアを設定します。

手順の詳細

外部認証サーバの AV ペアを設定します。

Cisco AV ペアの定義は次のとおりです（シスコは、UNIX ユーザ ID が指定されているかどうかにかかわらず AV ペアをサポートします）

例：

```
shell:domains = domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2
shell:domains =
domainA/writeRole1|writeRole2|writeRole3/readRole1|readRole2,domainB/writeRole1|writeRole2|writeRole3/readRole1|readRole2(8101)

These are the boost regexes supported by APIC:
uid_regex("shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?)(,\\S+?/\\S*?/\\S*?){0,31})(\\(\\d+\\))$");
regex("shell:domains\\s*[=:]\\s*((\\S+?/\\S*?/\\S*?),\\S+?/\\S*?/\\S*?){0,31})$");
```

次に、例を示します。

```
shell:domains = coke/tenant-admin/read-all,pepsi//read-all(16001)
```

リモート ユーザの設定

ローカル ユーザを設定する代わりに、APIC を一元化された企業クレデンシャルのデータセンターに向けることができます。APIC は、Lightweight Directory Access Protocol（LDAP）、Active Directory、RADIUS、および TACACS+ をサポートしています。

（注） APIC が少数側である（クラスタから切断されている）場合、ACI は分散システムであり、ユーザ情報が APICS に分散されるため、リモート ログインは失敗する可能性があります。ただし、ローカル ログインは APIC に対してローカルであるため、この場合も機能します。

3.1 (1) のリリース以降、**サーバ モニタリング** は RADIUS、TACACS +、LDAP、および RSA を介して設定され、個別の AAA サーバがアクティブかを判断できます。サーバ モニタリング機能は、サーバがアクティブかどうか確認するためそれぞれのプロトコルのログインを使用します。たとえば、LDAP サーバは ldap 1ログインを使用し、Radius サーバはサーバがアクティブか判断するサーバ モニタリング機能を持つ radius のログインを使用します。

外部認証プロバイダーを通じて認証されたリモートユーザを設定するには、次の前提条件を満たす必要があります。

- DNS 設定は、RADIUS サーバのホスト名ですでに名前解決されている必要があります。
- 管理サブネットを設定する必要があります。

NX-OS スタイル CLI を使用したリモート ユーザの設定

ローカル ユーザを設定する代わりに、APIC を一元化された企業クレデンシャルのデータセンターに向けることができます。APIC は、Lightweight Directory Access Protocol（LDAP）、Active Directory、RADIUS、および TACACS+ をサポートしています。

外部認証プロバイダーを通じて認証されたリモートユーザを設定するには、次の前提条件を満たす必要があります。

- DNS 設定は、RADIUS サーバのホスト名ですでに名前解決されている必要があります。
- 管理サブネットを設定する必要があります。

Cisco AV ペアが欠落しているか不良であるリモート ユーザのデフォルトの動作の変更

ステップ 1 メニュー バーで、**[管理（Admin）] > [認証（Authentication）] > [AAA] > [ポリシー（Policy）]** タブを選択します。

ステップ 2 **[リモート ユーザー ログイン ポリシー（Remote user login policy）]** ドロップダウン リストから、**[デフォルト ロールの割り当て（Assign Default Role）]** を選択します。

デフォルト値は [No Login] です。[Assign Default Role] オプションは、Cisco AV ペアが欠落しているか不良であるユーザに最小限の読み取り専用権限を割り当てます。不正な AV ペアは、解析ルール適用時に問題があった AV ペアです。

NX-OS スタイル CLI を使用した欠落または不良 Cisco AV ペアを持つリモート ユーザのデフォルトの動作の変更

Cisco APIC では、管理者が外部認証サーバで Cisco AV ペアを設定する必要があります。これを行うには、管理者は既存のユーザ レコードに Cisco AV ペアを追加します。Cisco AV ペアは、ユーザの RBAC ロールおよび権限に必要な APIC を指定します。Cisco AV ペアの形式は、RADIUS、LDAP、または TACACS+ のものと同じです。AV ペアの形式には Cisco UNIX ユーザ ID が含まれるものと含まれないものがあります。すべてのリモート ユーザが同じロールを持ち、相互ファイル アクセスが許可される場合はどちらの形式でも問題ありません。UNIX ユーザ ID を指定しないと、APIC システムによって ID 23999 が適用され、AV ペア ユーザに対して複数のロールまたは読み取り権限が指定されます。これは、グループ設定で設定された権限より高いかまたは低い権限がユーザに付与される原因になることがあります。このトピックでは、許可されない動作を変更する方法について説明します。

NX-OS スタイル CLI を使用して欠落または不良 Cisco AV ペアを持つリモート ユーザのデフォルトの動作を変更するには、次の手順を実行します。

ステップ 1 NX-OS CLI で、コンフィギュレーション モードで開始します。

例：

```
apic1#
apic1# configure
```

ステップ 2 aaa ユーザ デフォルト ロールを設定します。

例：

```
apic1(config)# aaa user default-role
 assign-default-role  assign-default-role
 no-login             no-login
```

ステップ 3 aaa 認証ログイン メソッドを設定します。

例：

```
apic1(config)# aaa authentication
 login  Configure methods for login

apic1(config)# aaa authentication login
 console  Configure console methods
```

```
 default  Configure default methods
 domain   Configure domain methods

apic1(config)# aaa authentication login console
 <CR>

apic1(config)# aaa authentication login domain
 WORD      Login domain name
 fallback
```

プロバイダーを作成する

この手順に従って、認証/承認プロトコルのプロバイダーを作成します。

始める前に

認証/承認プロトコルのプロバイダーを作成する前の関連する前提条件については、関連するプロトコルのセクションで説明します。

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

ステップ 2 ナビゲーションウィンドウで、[**認証（Authentication**）] を選択します。

ステップ 3 作業ペインで、[**プロバイダー（Providers**）] を選択します。

ステップ 4 [**アクション（Actions**）] > [**プロバイダーの作成（Create Provider**）] をクリックします。

ステップ 5 表示された **[プロバイダーの作成（Create Provider）]** 画面で、**[ホスト名/IP アドレス（Hostname/ IP Address）]**、**[説明（Description）]** を入力し、ドロップダウンリストから **[レルム（Realm）]** を選択します。**[レルム（Realm）]** で使用できるオプションは次のとおりです。

- RADIUS
- TACACS+
- LDAP
- SAML
- RSA
- OAuth 2

プロバイダーを構成するためのオプションは動的であり、選択した**レルム**に応じて変化します。各**レルム**で使用できるオプションについては、以降の手順で詳しく説明します。

ステップ 6 （任意） RADIUS にのみ適用可能：レルム サブタイプを選択します。**[レルム サブタイプ（Realm Subtype）]** を選択します。オプションは、**[デフォルト（Default）]** または **[デュオ（Duo）]** です。次に、以下を指定します。

- RADIUS サーバーのパスワード：確認のためにもう一度パスワードを入力してください。

- **[到達可能 EPG の選択（Select Reachability EPG）]** をクリックして、エンドポイント グループを選択します。
- RADIUS のサービスポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 1812 です。
- 認証プロトコルのオプションは、**[PAP]**、**[CHAP]**、**[MS-CHAP]** です。このオプションは、**[デフォルト（Default）]** を **[レルム サブタイプ（Realm Subtype）]** として選択した場合にのみ、表示されます。
- RADIUS サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です（レルム サブタイプ：デフォルトの場合）。デフォルトは 30 秒です（レルム サブタイプ：Duo）。
- RADIUS エンドポイントに接続する際の再試行回数。
- 定期的なサーバー監視を有効にするには、**[有効（Enabled）]** チェックボックスをオンにして、同じユーザ名とパスワードを入力します。

この手順は、RADIUS プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 7 （オプションの手順で TACACS+ にのみ適用）次を指定します。

- TACACS+ サーバーのパスワード：確認のためにもう一度パスワードを入力してください。
- **[到達可能 EPG の選択（Select Reachability EPG）]** をクリックして、エンドポイントグループを選択します。
- TACACS+ のサービス ポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 49 です。
- 認証プロトコルのオプションは、PAP、CHAP、MS-CHAP です。
- TACACS+ サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- TACACS+ エンドポイントに接続する際の再試行回数。
- 定期的なサーバー監視を有効にするには、**[有効（Enabled）]** チェックボックスをオンにして、同じユーザー名とパスワードを入力します。

この手順は、TACACS+ プロバイダーの設定用です。これで、手順 12 に進むことができます。

ステップ 8 （オプションの手順でLDAPにのみ適用）レルム サブタイプを選択します。オプションは、**[デフォルト（Default）]** または **[デュオ（Duo）]** です。次に、以下を指定します。

- LDAP ディレクトリのルート識別名（DN）。
- LDAP ベース DN：APIC がリモートユーザーアカウントを検索する LDAP サーバー内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、APIC が *Cisco AVPair* に使用するために要求している属性を見つけます。
- LDAP サーバーのパスワード。確認のためにもう一度パスワードを入力してください。
- LDAP のサービスポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 389 です。
- **[到達可能 EPG の選択（Select Reachability EPG）]** をクリックして、エンドポイントグループを選択します。

- LDAP サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 30 秒です。
- LDAP エンドポイントに接続する際の再試行回数。
- **[有効（Enable）]** チェック ボックスをオンにして、SSL を有効にします。
- SSL 証明書の検証レベル。次のオプションがあります。
  - 許容（Permissive）：DUO LDAP SSL 証明書の問題の診断に役立つデバッグノブ。
  - 厳格（Strict）：実稼働環境で使用するレベル。
- LDAP 属性。
- 認証方式。次のオプションがあります。
  - LDAPバインド
  - パスワード比較
- フィルタ タイプフィルタは、検索要求のエントリの識別に使用される条件を定義する、主要なエレメントです。例：（cn=*）。これは、1 つ以上の *cn* 値を含むエントリを意味します。次のオプションがあります。
  - デフォルト
  - Microsoft Active Directory
  - カスタム（Custom）
- LDAP フィルタこのフィールドは、選択したフィルタ タイプに基づいて自動入力されます（カスタム オプションの [フィルタ タイプ（Filter Type）] を選択した場合を除く）。デフォルトを選択した場合、フィルタは `cn=Suserid` です。 Microsoft Active Directory を選択した場合、フィルタは `sAMAccountName=Suserid` です。
- 定期的なサーバー監視を有効にするには、**[有効（Enabled）]** チェックボックスをオンにして、同じユーザー名とパスワードを入力します。

この手順は、LDAP プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 9 （オプションの手順で RSA にのみ適用）次を指定します。

- RSA サーバーのパスワード：確認のためにもう一度パスワードを入力してください。
- **[到達可能 EPG の選択（Select Reachability EPG）]** をクリックして、エンドポイントグループを選択します。
- RSA のサービスポート番号。指定できる範囲は 1 ～ 65535 です。デフォルト値は 1812 です。
- RSA サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- RSA エンドポイントに接続する際の再試行回数。

- 定期的なサーバー監視を有効にするには、[**有効（Enabled**）] チェックボックスをオンにして、同じユーザー名とパスワードを入力します。

この手順は、RSA プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 10 （オプションの手順で SAML にのみ適用）以下を指定します。

- ID プロバイダー（IdP）オプションは、ADFS、OKTA、PING IDENTITY です。
- IDP が提供するメタデータ URL。

  ADFS の場合、IdP メタデータ URL は *https://<FQDN of ADFS>/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 サーバーから対応する SAML アプリケーションの [サインオン（Sign On）] セクションで、アイデンティティ プロバイダーメタデータ URL のリンクをコピーします。

  Ping ID については、Ping ID サーバーの構成セクション（SAML アプリケーションの下）メタデータ URL 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。
- IdP がプライベート CA によって署名されている場合は、[**認証局の選択（Select Certificate Authority**）] をクリックして認証局を選択します。
- GUI リダイレクトバナー。これは URL またはメッセージが可能です。この情報は、認証のためにユーザーが ID プロバイダーのログインページにリダイレクトされる前に表示されます。
- SAML サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- ドロップダウンリストから [署名アルゴリズム（Signature Algorithm）] を選択します。
- [**有効（Enabled**）] チェックボックスをオンにして、暗号化された SAML アサーション、SAML 応答の署名アサーション、SAML 署名要求、SAML 応答メッセージの署名のすべてまたは一部を有効にできます。

この手順は、SAML プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 11 （オプションの手順で OAuth 2 にのみ適用）以下を指定します。

- クライアント ID：IdP 上の APIC アプリケーションのクライアント識別子。
- APIC アプリケーションのクライアント シークレット。確認のため、もう一度クライアント シークレットを入力します。
- ユーザー名要求。トークンのユーザー名属性。例：メール、サブ。
- 範囲。OAuth 2 範囲のリスト。例：「openid プロファイル」。ユーザー グループ情報を受信するには、IdP プロバイダーで構成された対応するスコープを追加します。例：「openid プロファイル グループ」。
- OIDC プロトコルの **[有効化（Enable）]** または **[無効化（Disable）]** を選択します。
- **[有効化（Enabled）]** チェックボックスをオンにして、トークンの署名を検証します。

- JWKS エンドポイント。トークンを検証するための JSON Web キーセット（JWKS）。このフィールドは、トークン署名の検証を有効にしている場合にのみ表示されます。
- 認証エンドポイント。IdP エンドポイント認証 URL。IdP サーバーから認可エンドポイントを取得します。このフィールドは、OIDC プロトコルが無効な場合にのみ表示されます。
- トークンエンドポイント。IdP エンドポイントトークンの URL。IdP サーバーからトークン エンドポイントを取得します。このフィールドは、OIDC プロトコルが無効な場合にのみ表示されます。
- 発行元 URL IdP サーバーから発行者の URL を取得します。このフィールドは、OIDC プロトコルが有効な場合にのみ表示されます。
- IdP がプライベート CA によって署名されている場合は、[**認証局の選択（Select Certificate Authority）**] をクリックして、認証局を選択します。
- [**到達可能 EPG の選択（Select Reachability EPG**）] をクリックして、エンドポイントグループを選択します。
- OAuth 2 サーバーとの通信タイムアウト。有効な範囲は 0 ～ 60 秒です。デフォルトは 5 秒です。
- GUI リダイレクトバナー。これは URL またはメッセージが可能です。この情報は、認証のためにユーザーが ID プロバイダーのログインページにリダイレクトされる前に表示されます。

この手順は、OAuth 2 プロバイダー構成用です。これで、手順 12 に進むことができます。

ステップ 12 **[保存（Save）]** をクリックします。

ログイン ドメイン

ログイン ドメインは、ユーザの認証ドメインを定義します。ログイン ドメインは、ローカル、LDAP、RADIUS、TACACS+、DUO、SAML、RSA、または OAuth 2 認証メカニズムを設定できます。REST、CLI、または GUI からシステムにアクセスすると、APIC によりユーザは正しい認証ドメインを選択できます。

たとえば、REST シナリオでは、完全なログイン ユーザ名が次のように表示されるようにユーザ名の頭に文字列が付きます。

```
apic:<domain>\<username>
```

システムに GUI からアクセスする場合は、APIC により選択するユーザのドメインのドロップダウン リストが提供されます。`apic: domain` が指定されない場合は、デフォルトの認証ドメイン サーバがユーザ名の検索に使用されます。

ACI バージョン 1.0(2x) 以降、APIC のログイン ドメイン フォールバックのデフォルトはローカルになっています。デフォルト認証とコンソール認証方法がどちらも非ローカルの方法に設定されており、両方の非ローカル方法がローカル認証に自動的にフォールバックしない場合でも、APIC にはローカル認証を使用してアクセスすることができます。

APIC フォールバック ローカル認証にアクセスするには、次の文字列を使用します。

- GUI からは、*apic:fallback\\username* を使用します。
- REST API からは、*apic#fallback\\username* を使用します。

（注） フォールバック ログイン ドメインは変更しないでください。変更すると、システムからロックアウトされる可能性があります。

GUI を使用してローカル ドメインを作成する

SAML および OAuth 2 の外部サーバーによる認証は、標準の CiscoAVPair ベースの認証に加え、ユーザーグループのマップルール情報に基づいて行われるようになりました。

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックが設置され、Application Policy Infrastructure Controller（APIC）がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- ログインドメイン名、レルム、リモートサーバープロバイダーは、ユーザーに対して認証ドメインを定義できます。

ステップ 1 メニュー バーで、**[管理（Admin）]** > **[AAA]** の順に選択します。
ステップ 2 ナビゲーションウィンドウで、[**認証（Authentication**）] を選択します。
ステップ 3 作業ペインで、[**ログインドメイン（Login Domains**）] タブを選択します。
ステップ 4 [**アクション（Actions**）] ボタン > [**ログインドメインの作成（Create Login Domain**）] の順に選択します。
ステップ 5 [**ログインドメインの作成（Create Login Domain**）] 画面の [**一般（General**）] ペインで、次を指定します。

- ユーザーが構成したドメイン名。
- ログインドメインの説明。
- ファブリックデバイスにアクセスするエンティティ（個人またはデバイス）の ID を確認するためのレルムです。[**レルム（Realm**）] ドロップダウンリストにあるオプションは、以下で説明されています。

1. 認証用 RADIUS プロトコルをサポートするリモートサーバーグループに対する RADIUS プロバイダーグループ。
2. 認証に TACACS+ プロトコルをサポートするリモートサーバーグループの TACACS+ プロバイダーグループ。
3. 認証用 LDAP プロトコルをサポートするリモートサーバーのグループに対する LDAP プロバイダーグループ。
4. 認証用 RSA プロトコルをサポートするリモートサーバーのグループに対する RSA プロバイダーグループ。

5. 認証用の SAML プロトコルをサポートする SAML プロバイダー リモートサーバー。
6. 認証用 OAuth 2 プロトコルをサポートする OAuth 2 プロバイダー リモートサーバー

（注） LDAP、RADIUS、TACACS+ がデフォルトのセキュリティメソッドとして指定されており、このダイアログで指定された関連するプロバイダー グループがユーザ ログイン中に使用できない場合、特にそうするように構成されていない限り、Cisco APIC サーバーではフォールバック ローカル認証は実行されません。

Cisco APIC が ID プロバイダーに到達するためにプロキシサーバーを必要とする場合は、対応するプロキシ アドレスを構成します。プロキシ設定の構成は、**[システム（System）]**> > **[システム設定（System Setting）]**> > **[プロキシ ポリシー（Proxy Policy）]**の下にあります。**[プロキシ ポリシー（ Proxy Policy）]** ペインで、必要な URL を **[HTTP URL]** または **[HTTPS URL]** フィールドに入力します。

ステップ 6 表示されたオプションの詳細を入力します。表示されるオプションは動的で、選択した**レルム**に基づいています。

選択した**レルム**が RADIUS または LDAP の場合、次のオプションが表示されます。

- **レルムサブタイプ**として [**デフォルト（Default）**] または [**デュオ（Duo）**] を選択します。
- **[設定（Settings）]** ペインで、**[RADIUS (または LDAP) プロバイダーの追加（ Add RADIUS (or LDAP) Provider）]** をクリックしてプロバイダーを選択または作成します（上記の **[デフォルト（Default）]** オプションを選択した場合）。[**デュオ（Duo）**] オプションを選択した場合は、[**RADIUS (または LDAP) プロバイダーの追加（Add RADIUS (or LDAP) Provider**）] をクリックしてプロバイダーを選択または作成します。

選択した**レルム**が TACACS+ または RSA の場合、次のオプションが表示されます。

- [**設定（Settings**）] ペインで、[**RSA（または TACACS+） プロバイダーの追加（Add RSA（or TACACS+）Provider**）] をクリックして、プロバイダーを選択または作成します。

選択した**レルム**が SAML または OAuth 2 の場合、次のオプションが表示されます。

- [**設定（Settings**）] ペインで、[**SAML (または OAuth 2) プロバイダーの選択（Select SAML (or OAuth 2) Provider**）] をクリックして、プロバイダーを選択または作成します。
- [**SAML (または OAuth 2) 認証の選択（SAML (or OAuth 2) Authorization Choice**）] には、**CiscoAVPair** または **GroupMap** のいずれかを選択します。
  - **CiscoAVPair** を選択した場合、外部認証サーバーで設定された CiscoAVpair の値/文字列に基づいて承認されます。外部 IDP から CiscoAVPair の値を受信すると、それに応じて Cisco APIC ではリモートユーザに権限を割り当てます。
  - **GroupMap** を選択した場合、外部認証サーバーで構成されたグループ情報に基づいて承認されます。Cisco APIC では、外部 IDP からユーザーグループ情報を受信すると、 Cisco APIC に構成されたユーザーグループ名と照合し、それに応じてリモート ユーザ権限を割り当てます。

GroupMap を使用した承認には、次の 2 つの追加パラメータが必要です。

- [**グループ属性（Group Attribute**）] を入力します。ここで入力するグループ属性は、外部認証サーバーのグループ属性と一致している必要があります。SAML の場合、グループ属性は、SAML IdP サーバーによって送信される応答のグループ アサーションの名前と一致する必要があります。OAuth2 の場合、グループ属性は、OAuth2 サーバーによって送信される JWT（JSON Web トークン）のグループ要求と一致する必要があります。

  `Example: memberOf (used in Active directory), Groups or groups (used in ping ID/Okta)`

  また、OAuth2 の場合、IDP からグループ情報を適切に受信するには、対応するスコープが OAuth2 プロバイダー構成で構成されていることを確認してください。例：`openid profile groups`

- **[ユーザー グループ マップ ルール（User Group Map Rule）]** を、**[ユーザー グループ マップ ルールの追加（ Add User Group Map Rule）]** をクリックして、追加します。

  [**ユーザーグループ マップルールの作成（Create User Group Map Rule**）] 画面で、次の詳細を入力します。

  1. [**名前（Name**）] フィールドにユーザーグループ マップルールの名前を入力します。
  2. **[説明（Description）]** フィールドに、説明を入力します。
  3. [**グループ名（Group Name**）] フィールドに、ユーザーが属するユーザーグループの名前を入力します。

     ここで入力したユーザーグループが、外部サーバーのユーザーグループと一致していることを確認してください。これは、外部サーバーから受信した認証情報を検証するために Cisco APIC によって使用されます。権限は、ユーザーが属するユーザーグループに基づいて設定されます。
  4. **[ユーザー権限（User Privilegles）]** を設定するには、**[ユーザー権限の追加（Add User Privileges）]**をクリックします。
  5. セキュリティ ドメインを追加するには、**[セキュリティ ドメインの選択（Select Security Domain）]** をクリックして、表示されたリストからセキュリティ ドメインを選択します。
  6. **[ロールの選択（Select Role）]** をクリックしてロールを選択し、権限タイプ（読み取りまたは書き込み）を関連付け、チェックマークをクリックして、権限をロールに関連付けます。

     さらにロールを追加するには、**[ロールの追加（Add Role）]** をクリックし、権限を関連付けます。
  7. **[ユーザ権限の追加（Add User Privileges）]** ウィンドウで、**[追加（Add）]** をクリックします。
  8. **[ユーザーグループ マップ ルールの追加（Add User Group Map Rule）]** ウィンドウで、**[適用（Apply）]** をクリックします。

ステップ 7 [**ログインドメインの作成（Create Login Domain 画面**）] で、 [**保存（Save**）] をクリックします。

RADIUS 認証

Remote Authentication Dial-In User Service（RADIUS）は、ネットワーク サービスに接続し使用するユーザー向けに、一元化された認証、認可、およびアカウンティング(AAA)管理を提供するネットワーキング プロトコルです。

RADIUS サーバーでユーザーを設定するには、APIC 管理者は `cisco-av-pair` 属性を使用して必要な属性（`shell:domains`）を設定する必要があります。デフォルトのユーザ ロールは、network-operator です。

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。これらのオプションが `cisco-av-pair` 属性で指定されていない場合は、MD5 および DES がデフォルトの認証プロトコルとなります。

たとえば、SNMPv3 認証とプライバシー プロトコルの属性は次のように指定できます。

```
snmpv3:auth=SHA priv=AES-128
```

同様に、ドメインのリストは次のとおりです。

```
shell:domains="domainA domainB …"
```

RADIUS アクセス用の APIC の設定

始める前に

- ACI ファブリックが設置され、Application Policy Infrastructure Controller (APIC) がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- RADIUS サーバのホスト名または IP アドレス、ポート、認証プロトコル、およびキーを使用できること。
- APIC 管理エンドポイント グループを使用できること。

ステップ 1 APIC で、RADIUS プロバイダーを作成します。

RADIUS プロバイダーの設定については、プロバイダーを作成する （7 ページ）を参照してください。

APIC GUI のインバンドまたはアウトオブバンド管理のトグル：

ナビゲーションウィンドウで、[**システム（System）**] > [**システム設定（System Settings）**] > [**APIC 接続設定（APIC Connectivity Preferences）**] の順に選択します。作業ペインで、[**インバンド（inband）**] または [**アウトオブバンド（ooband）**] のいずれかを選択します。

ステップ 2 RADIUS の**ログインドメイン**を作成します。

手順については、GUI を使用してローカル ドメインを作成する （12 ページ）を参照してください。

次のタスク

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

REST API を使用して APIC 内の RADIUS を設定する

```
HTTP POST to https://{{apichost}}/api/node/mo/.xml
<aaaRadiusProvider authPort="1812" authProtocol="pap" descr="myradius"
    monitorServer="disabled"
    name="server.radius.local" key="mykey"
    retries="1" timeout="5"/>
```

REST API を使用して RADIUS のログイン ドメインを設定するには：

```
HTTP POST to https://{{apichost}}/api/node/mo/.xml
<aaaUserEp  descr="" dn="uni/userext"  name=""  pwdStrengthCheck="yes" rn=""
status="modified">
    <aaaLoginDomain descr="" name="RadDom" rn="logindomain-RadDom" status="created">
        <aaaDomainAuth name="" providerGroup="RadDom" realm="radius" rn="domainauth"
status="created"/>
    </aaaLoginDomain>
   <aaaRadiusEp descr="" name="" retries="1" rn="radiusext" status="modified" timeout="5">

       <aaaRadiusProviderGroup descr=""  name="RadDom"  rn="radiusprovidergroup-RadDom"
  status="created">
           <aaaProviderRef descr="acs" name="radius1.server.com" order="1"
               rn="providerref-radius.server.com" status="created" />
           <aaaProviderRef descr="acs" name="radius2.server.com" order="2"
               rn="providerref-radius2.server.com" status="created" />
        </aaaRadiusProviderGroup>
    </aaaRadiusEp>
</aaaUserEp>
```

TACACS+ 認証

Terminal Access Controller Access Control device Plus（TACACS+）は、シスコのシステムでサポートされている、もう 1 つのリモート AAA プロトコルです。TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。たとえば、Cisco Application Policy Infrastructure Controller（APIC）は、認証を行わずにアクセスを許可できます。
- AAA クライアントとサーバー間のデータ送信に TCP を使用しているため、コネクション型プロトコルで確実に転送されます。
- スイッチと AAA サーバー間でプロトコルペイロード全体が暗号化されるため、高いデータ機密性が確保されます。RADIUS ではパスワードしか暗号化されません。
- 構文と設定が RADIUS と異なる av-pairs を使用しますが、Cisco APIC は `shell:domains` をサポートします。

次の XML の例では、IP アドレス 10.193.208.9 の TACACS+ プロバイダーと連携するように Cisco Application Centric Infrastructure（ACI）ファブリックを設定しています。

```
<aaaTacacsPlusProvider name="10.193.208.9"
           key="test123"
           authProtocol="pap"/>
```

（注） この例では IPv4 アドレスを使用していますが、IPv6 アドレスも使用できます。

TACACS+: を使用するときには、次の制約事項および使用上のガイドラインが適用されます。

- TACACS サーバおよび TACAC ポートは、ping で到達可能である必要があります。
- 優先順位が最も高い TACACS サーバーが、最初にプライマリ サーバーと見なされます。

TACACS+ アクセス用の APIC の設定

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックが設置され、Application Policy Infrastructure Controller（APIC）がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 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。
- APIC 管理エンドポイント グループを使用できること。

ステップ 1 APIC で、TACACS+ プロバイダーを作成します。

TACACS+ プロバイダーの設定については、プロバイダーを作成する （7 ページ） を参照してください。

APIC GUI のインバンドまたはアウトオブバンド管理のトグル：

ナビゲーションウィンドウで、[**システム（System）**] > [**システム設定（System Settings）**] > [**APIC 接続設定（APIC Connectivity Preferences）**] の順に選択します。作業ペインで、[**インバンド（inband）**] または [**アウトオブバンド（ooband）**] のいずれかを選択します。

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

手順については、GUI を使用してローカル ドメインを作成する （12 ページ）を参照してください。

次のタスク

これで、APIC TACACS+ 設定手順は完了です。次に、RAIDUS サーバも使用する場合は、RADIUS 用の APIC の設定も行います。TACACS+ サーバのみを使用する場合は、次の ACS サーバ設定に関するトピックに進みます。

REST API を使用して APIC の TACACS を設定する

```
HTTP POST to https://{{apichost}}/api/node/mo/.xml
<aaaTacacsPlusProvider name="server.tacacs.local"
    authProtocol="pap"
    monitorServer="enabled" monitoringUser="user1" monitoringPassword="mypwd"
    port="49" retries="1" key="mykey" timeout="15" />
```

REST API を使用して TACACS のログイン ドメインを設定するには:

```
HTTP POST to https://{{apichost}}/api/node/mo/.xml
<aaaUserEp  descr="" dn="uni/userext"  name=""  pwdStrengthCheck="yes" rn=""
status="modified">
    <aaaLoginDomain  descr=""  name="Tacacs" nameAlias=""  rn="logindomain-Tacacs"
status="created,modified">
        <aaaDomainAuth  descr="" name="" nameAlias=""  providerGroup="Tacacs"
            realm="tacacs" rn="domainauth" status="created,modified"/>
    </aaaLoginDomain>
    <aaaTacacsPlusEp  descr="" name="" nameAlias=""  retries="1" rn="tacacsext"
status="created,modified" timeout="5">
        <aaaTacacsPlusProviderGroup  descr="" name="Tacacs" nameAlias=""
            rn="tacacsplusprovidergroup-Tacacs" status="created,modified">
          <aaaProviderRef descr="testing" name="tacacs.server.com" nameAlias="" order="1"

              rn="providerref-tacacs.server.com"  status="created,modified" />
            <aaaProviderRef descr="testing" name="tacacs2.server.com" nameAlias=""
order="2"
              rn="providerref-tacacs2.server.com"  status="created,modified" />
        </aaaTacacsPlusProviderGroup>
    </aaaTacacsPlusEp>
</aaaUserEp>
```

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

始める前に

- Cisco Secure Access Control Server (ACS) バージョン 5.5 がインストールされ、オンラインになっていること。

（注） ここでは手順の説明に ACS v5.5 が使用されています。ACS の他のバージョンでもこのタスクを実行できる可能性がありますが、GUI の手順はバージョンによって異なる場合があります。

- Cisco Application Policy Infrastructure Controller (Cisco APIC) の RADIUS キーまたは TACACS+ キーを使用できること (両方を設定する場合は両方のキー) 。
- APIC が設置されオンラインになっており、APIC クラスタが形成されて正常に動作していること。

• RADIUS または TACACS+ のポート、認証プロトコル、およびキーを使用できること。

ステップ 1 APIC をクライアントとして設定するには、ACS サーバにログインします。

a) **[Network Resources]** > **[Network Devices Groups]** > **[Network Devices and AAA Clients]** に移動します。

b) クライアント名、APIC インバンド IP アドレスを指定し、TACACS + または RADIUS（または両方）の認証オプションを選択します。

（注） RADIUS または TACACS+ のみの認証が必要な場合は、必要なオプションのみを選択します。

c) 共有秘密 (キー) や認証オプションに適したポートなど、認証の詳細を指定します。

（注） **[共有秘密（Shared Secret）]** は **[プロバイダ（Provider）]** キーと一致する必要があります。

ステップ 2 ID グループを作成します。

a) **[Users and Identity Stores]** > **[Internal Groups]** オプションに移動します。

b) 必要に応じて、**[Name]** と **[Parent Group]** を指定します。

ステップ 3 ユーザを ID グループにマッピングします。

a) **[Navigation]** ペインで、**[Users and Identity Stores]** > **[Internal Identity Stores]** > **[Users]** オプションをクリックします。

b) 必要に応じて、ユーザの **[Name]** と **[Identity Group]** を指定します。

ステップ 4 ポリシー要素を作成します。

a) **[Policy Elements]** オプションに移動します。

b) RADIUS の場合、[Authorization and Permissions] > [Network Access] > [Authorization Profiles **Name]** を指定します。TACACS+ の場合、必要に応じて、[Authorization and Permissions] > [Device Administration] > [Shell Profile **Name]** を指定します。

c) RADIUS の場合、必要に応じて、**[Attribute]** には「`cisco-av-pair`」、**[Type]** には「string」、**[Value]** には「**`shell:domains = <domain>/<role>/,<domain>// role`**」と指定します。TACACS+ の場合、必要に応じて、**[Attribute]** には「`cisco-av-pair`」、**[Requirement]** には「Mandatory」、**[Value]** には「**`shell:domains = <domain>/<role>/,<domain>// role`**」と指定します。

[値（Value）] フィールドの構文は、書き込み権限を付与するかどうかを決定します。

- 読み取り/書き込み権限の場合、構文は `shell:domains = <domain>/<role>/` です。
- 読み取り専用権限の場合、構文は `shell:domains = <domain>// <role>` です。

たとえば、*cisco-av-pair* の値が `shell:domains = solar/admin/,common// read-all` である場合、`solar` はセキュリティ ドメイン、`admin` は `solar` というセキュリティ ドメインに対する書き込み権限をこのユーザに付与するロールであり、`common` はテナント共通であり `read-all` はテナント共通のすべてに対する読み取り権限をこのユーザに付与するロールです。

ステップ 5 サービス選択ルールを作成します。

a) RADIUS の場合、サービス選択ルールを作成して ID グループをポリシー要素に関連付けるには、**[Access Policies]** > **[Default Device Network Access Identity]** > **[Authorization]** に移動し、ルールの [Name]、

[Status]、および [Conditions] を指定し、必要に応じて「`Internal Users:UserIdentityGroup in ALL Groups:<identity group name>`」を追加します。

b) TACACS+ の場合、サービス選択ルールを作成して ID グループをシェル プロファイルに関連付けるには、**[Access Policies]** > **[Default Device Admin Identity]** > **[Authorization]** に移動します。ルールの [Name] と [Conditions] を指定し、必要に応じて [Shell Profile] を選択します。

次のタスク

新しく作成した RADIUS および TACACS + ユーザを使用して APIC にログインします。割り当てられた RBAC のロールと権限に従って、ユーザが正しい APIC セキュリティ ドメインにアクセスできることを確認します。ユーザは、明示的に許可されていない項目にアクセスできてはなりません。読み取り/書き込みアクセス権が、そのユーザに設定されたものと一致している必要があります。

LDAP/Active Directory の認証

RADIUS および TACACS+ と同様、LDAP により、ネットワーク要素はユーザを認証し、特定のアクションの実行を許可するために使用できる AAA クレデンシャルを取得できます。追加された認証局の設定は管理者によって実行でき、LDAPS（SSL 経由の LDAP）の信頼性をイネーブルにし、中間者攻撃を防ぐことができます。

次に示す XML の例では、ACI ファブリックが IP アドレス 10.30.12.128 の LDAP プロバイダーを使用するように設定しています。

（注） この例では IPv4 アドレスを使用していますが、IPv6 アドレスも使用できます。

```
<aaaLdapProvider name="10.30.12.128"
          rootdn="CN=Manager,DC=ifc,DC=com"
          basedn="DC=ifc,DC=com"
          SSLValidationLevel="strict"
          attribute="CiscoAVPair"
          enableSSL="yes"
     key="myldappwd"
          filter="cn=$userid"
          port="636" />
```

（注） LDAP 設定のベスト プラクティスは、属性文字列として **CiscoAVPair** を使用することです。顧客がオブジェクト ID 1.3.6.1.4.1.9.22.1 を使用して問題が発生した場合、その他のオブジェクト ID 1.3.6.1.4.1.9.2742.1-5 が LDAPサーバにも使用できます。

Cisco AVPair を設定する代わりに、APIC で LDAP グループ マップを作成するオプションがあります。

LDAP の設定

LDAP 設定には 2 つのオプションがあります。Cisco AVPair を設定したり、APIC 内で LDAP グループマップを設定したりできます。このセクションには、両方の設定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 2012 LDAP の設定

始める前に

- 最初に LDAP サーバを設定し、次に Cisco Application Policy Infrastructure Controller（Cisco APIC）を LDAP アクセス用に設定する。
- Microsoft Windows Server 2012 がインストールされ、オンラインになっていること。
- Microsoft Windows Server 2012 サーバ マネージャの ADSI Edit ツールがインストールされていること。ADSI Edit をインストールするには、Windows Server 2012 サーバ マネージャのヘルプに記載されている手順に従ってください。
- `CiscoAVPair` の属性の指定：Common Name = **`CiscoAVPair`**, LDAP Display Name = **`CiscoAVPair`**, Unique X500 Object ID = 1.3.6.1.4.1.9.22.1, Description = **`CiscoAVPair`**, Syntax = **`Case Sensitive String`**。

（注） LDAP 設定のベスト プラクティスは、属性文字列として **`CiscoAVPair`** を使用することです。顧客がオブジェクト ID 1.3.6.1.4.1.9.22.1 を使用して問題が発生した場合、その他のオブジェクト ID 1.3.6.1.4.1.9.2742.1-5 が LDAPサーバにも使用できます。

- 以下を行うことができる Microsoft Windows Server 2012 ユーザ アカウントを使用できること。
  - ADSI Edit を実行して `CiscoAVPair` 属性を Active Directory（AD）スキーマに追加します。
  - `CiscoAVPair` 属性パラメータに対するアクセス許可を持つように Active Directory LDAP ユーザーを設定します。
- ポート 636 は、SSll/TLS と LDAP の連携設定に必要です。

ステップ 1 ドメイン管理者として Active Directory（AD）サーバにログインします。

ステップ 2 AD スキーマに `CiscoAVPair` 属性を追加します。

a) **[Start]** > **[Run]** に移動し、「**`mmc`**」と入力し、Enter を押します。
Microsoft Management Console（MMC）が開きます。

b) **[File]** > **[Add/Remove Sanp-in]** > **[Add]** に移動します。
c) [Add Standalonee Snap-in] ダイアログボックスで、[Active Directory Schema] を選択し、[Add] をクリックします。
MMC コンソールが開きます。
d) **[属性]** フォルダを右クリックし、**[属性の作成]** オプションを選択します。
[Create New Attribute] ダイアログボックスが開きます。
e) **[共通名]** に「**CiscoAVPair**」、**[LDAP 表示名]** に「**CiscoAVPair**」、[Unique X500 Object ID] に「**1.3.6.1.4.1.9.22.1**」と入力し、**[構文]**で「**Case Sensitive String**」を選択します。
f) [OK] をクリックして、属性を保存します。

ステップ 3 [User Properties] クラスを [CiscoAVPair] 属性が含まれるように更新します。

a) MMC コンソールで、[Classes] フォルダを展開し、[user] クラスを右クリックし、[Properties] を選択します。
[user Properties] ダイアログボックスが開きます。
b) **[属性]** タブをクリックし、**[追加]** をクリックして **[スキーマのオブジェクトを選択する]** ウィンドウを開きます。
c) [Select a schema object:] リストで、「**CiscoAVPair**」を選択し、[Apply] をクリックします。
d) MMC コンソールで、[Active Directory Schema] を右クリックし、[Reload the Schema] を選択します。

ステップ 4 **CiscoAVPair** 属性のアクセス許可を設定します。

LDAP には **CiscoAVPair** 属性が含まれているため、LDAP ユーザーに Cisco APIC RBAC ロールを割り当てることにより Cisco APIC アクセス許可を付与する必要があります。

a) [ADSI Edit] ダイアログ ボックスで、Cisco APIC にアクセスする必要があるユーザを見つけます。
b) ユーザ名を右クリックし、[Properties] を選択します。
[<user> Properties] ダイアログボックスが開きます。
c) **[属性エディタ]** タブをクリックし、「*CiscoAVPair*」属性を選択し、*[値]* に「 **shell:domains = <domain>/<role>/,<domain>// role**」と入力します。

たとえば、*CiscoAVPair* の値が `shell:domains = solar/admin/,common// read-all(16001)` である場合、`solar` はセキュリティ ドメイン、`admin` は `solar` というセキュリティ ドメインに対する書き込み権限をこのユーザーに付与するロールであり、`common` は Cisco Application Centric Infrastructure（Cisco ACI）テナント共通であり `read-all(16001)` は Cisco ACI テナント共通のすべてに対する読み取り権限をこのユーザーに付与するロールです。

d) [OK] をクリックして変更を保存し、[<user> Properties] ダイアログボックスを閉じます。

LDAP サーバは Cisco APIC にアクセスするように設定されます。

次のタスク

Cisco APIC を LDAP アクセス用に設定します。

LDAP アクセス用の APIC の設定

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックがインストールされていて、Application Policy Infrastructure コントローラがオンラインになっており、APIC クラスタが形成されていて正常に動作していること。
- 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。
- APIC 管理エンドポイント グループを使用できること。

ステップ 1 APIC で、LDAP プロバイダーを設定します。

LDAP プロバイダーの設定については、プロバイダーを作成する （7 ページ）を参照してください。

APIC GUI のインバンドまたはアウトオブバンド管理のトグル：

ナビゲーションウィンドウで、[**システム（System）**] > [**システム設定（System Settings）**] > [**APIC 接続設定（APIC Connectivity Preferences）**] の順に選択します。作業ペインで、[**インバンド（inband）**] または [**アウトオブバンド（ooband）**] のいずれかを選択します。

ステップ 2 LDAP の **ログイン ドメイン** を作成します。

手順については、GUI を使用してローカル ドメインを作成する （12 ページ）を参照してください。

次のタスク

これで、APIC LDAP 設定手順は完了です。次に、APIC LDAP ログイン アクセスをテストします。

Cisco APIC での LDAP グループ マップ ルールの設定

Cisco APIC での LDAP グループ マップの設定には、作成の最初の LDAP グループ マップ ルールが必要です。このセクションでは、LDAP グループ マップ ルールを作成する方法について説明します。

始める前に

LDAPサーバが設定されているグループのマッピングを実行しています。

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

ステップ 2 ナビゲーションウィンドウで、[**認証（Authentication）**] を選択します。

ステップ 3 作業ペインで、[**LADP グループマップ（LDAP Group Maps）**] > [**LDAP グループマップルール（LDAP Group Map Rules）**] を選択します。

ステップ 4 **[アクション（Actions）]** ボタン > **[LDAP グループ マップ ルールの作成（Create LDAP Group Map Rule）]** をクリックします。

ステップ 5 表示されている [**LDAP グループマップルールの作成（Create LDAP Group Map Rule**）] 画面で、タイプ、グループマップルール名、説明（オプション）、グループ DN を指定します。

ステップ 6 [セキュリティドメイン（Security Domains）] ペインで、[**セキュリティドメインの追加（Add Security Domain**）] をクリックします。[セキュリティドメイン（Security Domains）] ポップアップウィンドウで、次の詳細を入力します。

a) [**セキュリティドメインの選択（Select Security Domain**）] をクリックし、セキュリティドメインを選択します。

b) [**ロールの追加（Add Role**）] をクリックしてロールを追加し、ドロップダウンリストから権限を選択します。チェックマークをクリックして、選択した権限をロールに割り当てます。この手順を繰り返して、複数のロールをセキュリティドメインに追加します。

c) [セキュリティドメイン（Security Domains）] ウィンドウで **[追加（Add**）] をクリックします。

ステップ 7 [LDAP グループマップルールの作成（Create LDAP Group Map Rule）] 画面で **[保存（Save**）] をクリックします。

次のタスク

LDAP グループ マップ ルールを指定した後に、LDAP グループ マップを作成します。

Cisco APIC での LDAP グループ マップの設定

このセクションでは、LDAP グループ マップを作成する方法について説明します。

始める前に

- 実行中の LDAPサーバは、グループ マッピングで設定されます。

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

ステップ 2 ナビゲーションウィンドウで、[**認証（Authentication**）] を選択します。

ステップ 3 作業ペインで、[**LADP グループマップ（LDAP Group Maps**）] > [**LDAP グループマップ（LDAP Group Map**）] の順に選択します。

ステップ 4 [**アクション（Actions**）]>[**LDAP グループマップの作成（Create LDAP Group Map**）] の順に選択します。

ステップ 5 表示されている [**LDAP グループマップの作成（Create LDAP Group Map**）] 画面で、[**LDAP グループマップルールの追加（Add LDAP Group Map Rule**）] をクリックして、[タイプ（Type）]、[グループマップ名（Group Map Name）]、[説明（オプション）（Description）]、[グループマップルール（LDAP Group Map Rule）] を指定します。

LDAP グループマップルールが使用できない場合は、[**LDAP グループマップルールの作成（Create LDAP Group Map Rule**）] をクリックします。LDAP グループ マップ ルール作成のための詳細な手順については、*LDAP* グループ マップ ルールの構成の手順を参照してください。

ステップ 6 [保存（Save）] をクリックします。

DUO による多要素認証

Cisco APIC は、Duo セキュリティによる多要素認証をサポートしています。Duo セキュリティ自体は、ユーザー ID のリポジトリとして機能しません。オンプレミスまたはクラウドベースの組織の既存の認証に加えて、2 要素（2F）認証を提供します。Duo による 2 要素認証は、ユーザーが組織のプライマリ認証ソースでの認証を完了すると発生します。

プライマリ認証ソースで認証を完了した後、Duo は 3 種類の 2F 認証方法をサポートします。

- スマートフォンの Duo モバイル アプリを使用したモバイルでの通知プッシュ。
- 登録済みの電話または携帯電話での通話。
- Duo モバイル アプリで生成されるパスコード。

ユーザーは、次のサーバーを使用して認証されます。

- Duo プロキシ RADIUS サーバーは、Cisco APIC の多要素認証を使用して、RADIUS PAP プライマリ認証方式を使用して分散クライアント/サーバー システムを認証します。
- Duo プロキシ LDAP サーバーは、Cisco APIC の多要素認証を使用して、Cisco AVPair または Group Maps 認証方法を使用してリモート サーバーを認証します。

DUO RADIUS プロバイダーまたは DUO LDAP プロバイダーの作成については、プロバイダーを作成する （7 ページ） の手順を参照してください。

REST API を使用して DUO プロキシを設定する

```
The URL for all XML data :
POST  https://{{apichost}}/api/node/mo/.xml
```

以下は、プロキシ RADIUS およびプロキシ LDAP サーバーを使用した Duo の設定例です。

RADIUS の設定

- DUO RADIUS プロバイダーを追加します。

```
<aaaRadiusProvider authPort="1812" authProtocol="pap" descr="duoradius"
       dn="uni/userext/duoext/radiusprovider-duoproxy.host.com"
       monitorServer="disabled" monitoringUser=""
       name="duoproxy.host.com"  key="mypasswd"
       retries="1" status="created" timeout="30"/>
```

- DUO RADIUS プロキシ プロバイダーを使用してログイン ドメインを追加します。

```
<aaaUserEp  descr="" dn="uni/userext"  name="" pwdStrengthCheck="yes" rn=""
status="modified">
    <aaaLoginDomain descr="" name="DuoRadDom" rn="logindomain-DuoRadDom"
status="created">
        <aaaDomainAuth descr="" name="" providerGroup="DuoRadDom" realm="radius"
realmSubType="duo" rn="domainauth" status="created"/>
```

```
    </aaaLoginDomain>
    <aaaDuoEp descr="" name="" retries="1" rn="duoext" status="modified" timeout="40">

        <aaaDuoProviderGroup name="DuoRadDom" providerType="radius"
secFacAuthMethods="auto,push"
             rn="duoprovidergroup-DuoRadDom" status="created">
            <aaaProviderRef descr="duoradproxy" name="duoproxy.host.com" order="1"
               rn="providerref-duoproxy.host.com" status="created" />
        </aaaDuoProviderGroup>
    </aaaDuoEp>
</aaaUserEp>
```

LDAP 設定

- 属性 `Cisco AVPair` を持つ DUO LDAP プロキシ プロバイダーを追加します。

```
<aaaLdapProvider name="duoproxy.host.com"
    SSLValidationLevel="strict"
    attribute="CiscoAvPair"
    basedn="CN=Users,DC=host,DC=com"
    dn="uni/userext/duoext/ldapprovider-duoproxy.host.com" enableSSL="no"
filter="cn=$userid"
    monitorServer="disabled"
    port="389" retries="1"
    rootdn="CN=admin,CN=Users,DC=host,DC=com"
    timeout="60"
    key="12345"/>
```

- 属性 `memberOf` を持つ DUO LDAP プロキシ プロバイダーを追加します。

```
<aaaLdapProvider name="duoproxy.host.com"
    SSLValidationLevel="strict"
    attribute="memberOf"
    basedn="CN=Users,DC=host,DC=com"
    dn="uni/userext/duoext/ldapprovider-duoproxy.host.com" enableSSL="no"
filter="cn=$userid"
    monitorServer="disabled"
    port="389" retries="1"
    rootdn="CN=admin,CN=Users,DC=host,DC=com"
    timeout="60"
    key="12345"/>
```

- LDAP GroupMap ルールを追加します。

```
<aaaLdapGroupMapRule name="DuoEmpRule"
dn="uni/userext/duoext/ldapgroupmaprule-DuoEmpRule"
       groupdn="CN=Employee,CN=Users,DC=host,DC=com" status="created">
       <aaaUserDomain name="all" rn="userdomain-all" status="created,modified">
         <aaaUserRole name="fabric-admin" privType="writePriv" rn="role-fabric-admin"
 status="created,modified"/>
       </aaaUserDomain>
</aaaLdapGroupMapRule>
```

- LDAP GroupMap ルールを追加します。

```
<aaaLdapGroupMap name="DuoEmpGroupMap"
dn="uni/userext/duoext/ldapgroupmap-DuoEmpGroupMap"  status="created">
    <aaaLdapGroupMapRuleRef name="DuoEmpRule" rn="ldapgroupmapruleref-DuoEmpRule"
status="created"/>
</aaaLdapGroupMap>
```

- GroupMap を使用して DUO LDAP ログイン ドメインを追加します。

```
<polUni>
   <aaaUserEp dn="uni/userext" name="" pwdStrengthCheck="yes" rn="" status="modified">
```

```
            <aaaDuoEp attribute="memberOf" basedn="" filter="sAMAccountName=$userid"
                name="" retries="1" rn="duoext" status="modified" timeout="30">
                <aaaDuoProviderGroup name="DuoLdapDom" authChoice="LdapGroupMap"
    providerType="ldap"
                     rn="duoprovidergroup-DuoLdapDom" ldapGroupMapRef="DuoEmpGroupMap"
    secFacAuthMethods="auto,push" status="modified">
                    <aaaProviderRef name="duoproxy.host.com" order="1"
                        rn="providerref-duoproxy.host.com" status="modified"/>
                </aaaDuoProviderGroup>
            </aaaDuoEp>
            <aaaLoginDomain name="DuoLdapDom" rn="logindomain-DuoLdapDom"
    status="modified">
                <aaaDomainAuth name="" providerGroup="DuoLdapDom" realm="ldap"
    realmSubType="duo" rn="domainauth" status="modified"/>
            </aaaLoginDomain>
        </aaaUserEp>
    </polUni>
```

GUI のログイン ドメインを取得する

ログイン ドメインの GET URL:

```
GET https://apic.host.com/api/aaaListDomains.json
```

```
{   "totalCount": "5",
    "imdata": [{
            "name": "DuoRadDom",
            "type": "DUO",
            "secAuths": "auto,push"
        }, {
            "name": "DuoLdapDom",
            "type": "DUO",
            "secAuths": "auto,push"
        }, {
            "name": "RadDom",
            "type": "OTHER"
        }, {
            "name": "LdapDom",
            "type": "OTHER"
        }, {
            "name": "DefaultAuth",
            "guiBanner": "",
            "type": "OTHER"
        }
    ] }
```

RSA Secure ID 認証

RSA認証は、使用できる組み合わせで固定キーを使用して、パスワードを作成するさまざまな方法でトークンを提供します。これは、ハードウェア トークンとソフトウェア トークンの両方をサポートします。

GUI を使用して、RSA アクセス用の APIC の設定

始める前に

- ACI ファブリックが設置され、Application Policy Infrastructure Controller（APIC）がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- RSA サーバのホスト名または IP アドレス、ポート、認証プロトコル、およびキーを使用できること。
- APIC 管理エンドポイント グループを使用できること。

ステップ 1 APIC で、RSA プロバイダを作成します。

RSA プロバイダーの構成については、「プロバイダーを作成する （7 ページ）」を参照してください。

ステップ 2 RSA の **[ログイン ドメイン（Login Domain）]** を作成します。

詳細な手順については、「GUI を使用してローカル ドメインを作成する （12 ページ）」 を参照してください。

次のタスク

これで、APIC RSA 設定手順は完了です。次に、RSA サーバを設定します。

SAML 認証

SAML は XML ベースのオープン規格のデータ形式であり、いずれかのアプリケーションにサインインした後に、管理者は定義された一連のシスコのコラボレーション アプリケーションにシームレスにアクセスできます。SAML では、信頼できるビジネス パートナー間で、セキュリティに関連した情報交換を記述します。これは、サービス プロバイダーによってユーザーの認証に使用される認証プロトコルです。SAML により、ID プロバイダー（IdP）とサービス プロバイダーの間で、セキュリティ認証情報を交換できます。

SAML SSO は SAML 2.0 プロトコルを使用して、シスコのコラボレーション ソリューションのドメイン間と製品間で、シングル サインオンを実現しています。SAML 2.0 は、Cisco アプリケーション全体で SSO を有効にし、Cisco アプリケーションと IdP 間でフェデレーションを有効にします。SAML 2.0 では、高度なセキュリティ レベルを維持しながら、シスコの管理ユーザが安全なウェブ ドメインにアクセスして、IdP とサービス プロバイダーの間でユーザ認証と承認データを交換できます。この機能が安全なメカニズムを提供していることで、さまざまなアプリケーションにわたり、共通の資格情報や関連情報を使用します。

SAML SSO の管理者権限は、シスコのコラボレーション アプリケーションでローカルに設定されたロールベース アクセス コントロール（RBAC）に基づき認証されます。

SAML SSO は、IdP とサービス プロバイダーの間のプロビジョニング プロセスの一部として、メタデータと証明書を交換することで信頼の輪（CoT）を確立します。サービス プロバイダーは IdP のユーザ情報を信頼しており、さまざまなサービスやアプリケーションにアクセスできるようにします。

（注） サービス プロバイダーが認証にかかわることはありません。SAML 2.0 では、サービス プロバイダーではなく、IdP に認証を委任します。

クライアントは IdP に対する認証を行い、IdP はクライアントにアサーションを与えます。クライアントはサービス プロバイダーにアサーションを示します。CoT が確立されているため、サービス プロバイダーはアサーションを信頼し、クライアントにアクセス権を与えます。

SAML SSO を有効にすると、次のようないくつかの利点が得られます。

- 異なるユーザー名とパスワードの組み合わせを入力する必要がなくなるため、パスワードの劣化が軽減します。
- アプリケーションをホストしているお使いのシステムからサードパーティのシステムに、認証を転送します。SAML SSO を使用することで、IdP とサービス プロバイダーの間で信頼の輪を作成できます。サービス プロバイダーは IdP 信頼して、ユーザを認証します。
- 認証情報を保護し、安全に保ちます。暗号化機能により、IdP、サービス プロバイダー、ユーザの間で認証情報を保護します。SAML SSO では、IdP とサービス プロバイダー間で転送される認証メッセージを外部ユーザから保護することもできます。
- 同じ ID に資格情報を再入力する時間が省けるため、生産性が向上します。
- パスワードをリセットするためのヘルプデスクへの問い合わせが減るため、コスト削減につながります。

SAML の基本要素

- クライアント（ユーザのクライアント）：これは、認証用にブラウザインスタンスを活用できる、ブラウザベースのクライアントまたはクライアントです。システム管理者のブラウザはその一例です。
- サービス プロバイダー：これは、クライアントがアクセスを試みるアプリケーションまたはサービスです。
- ID プロバイダー（IdP）サーバ：これは、ユーザ資格情報を認証し、SAML アサーションを発行するエンティティです。
- Lightweight Directory Access Protocol（LDAP）ユーザ：これらのユーザは、Microsoft Active Directory や OpenLDAP などの LDAP ディレクトリと統合されます。非 LDAP ユーザは、Unified Communications サーバ上にローカルに存在します。
- SAML アサーション：これは、ユーザ認証のために、IdP からサービス プロバイダーに転送されるセキュリティ情報で構成されます。アサーションは、ユーザ名や権限などのサブ

ジェクトに関する信頼されたステートメントを含む、XML ドキュメントです。通常では、信頼性を確保するために、SAML アサーションはデジタル署名されます。

- SAML 要求：これは、Unified Communications アプリケーションにより生成される認証要求です。LDAP ユーザを認証するために、Unified Communications アプリケーションは認証要求を IdP に委任します。
- 信頼の輪（CoT）：これは、共同で 1 つの IdP に対して共有と認証を行うさまざまなサービス プロバイダーで構成されます。
- メタデータ：これは、IdP と同様に ACI アプリケーションによって生成された、XML ファイルです。SAML メタデータの交換により、IdP とサービス プロバイダーの間に信頼関係が確立します。
- Assertion Consumer Service（ACS）URL：この URL は、アサーションをポストする場所を IdP に指示します。ACS URL は、最終的な SAML 応答を特定の URL にポストすることを IdP に指示します。

（注） 認証が必要なすべてのインスコープ サービスでは、SSO のメカニズムとして SAML 2.0 を使用します。

サポートされている IdPs および SAML コンポーネント

サポートされる IdP

ID プロバイダー（IdP）は、ユーザ、システム、サービスの ID 情報を作成、維持、管理する認証モジュールです。また、分散ネットワーク内のその他のアプリケーションやサービス プロバイダーに対して認証も行います。

SAML SSO で、IdPs はユーザーのロールまたは各 Cisco コラボレーション アプリケーションのログイン オプションに基づいて、認証オプションを提供します。IdP は、ユーザ資格情報を保管、検証し、ユーザがサービス プロバイダーの保護リソースにアクセスできる SAML 応答を生成します。

（注） IdP サービスを十分理解している必要があります。現在インストールされていて、操作可能であることを確認してください。

APIC の SAML SSO 機能は、次の IdP でテストされています。

- https://technet.microsoft.com/en-us/library/cc772128(WS.10).aspx
- Okta シングル サインオン： https://www.okta.com/products/single-sign-on/
- PingFederate： https://documentation.pingidentity.com/pingfederate/pf90/index.shtml#gettingStartedGuide/concept/gettingStarted.html

SAML のコンポーネント

SAML SSO ソリューションは、特定のアサーション、プロトコル、バインディング、プロファイルの組み合わせに基づきます。さまざまなアサーションは、プロトコルやバインディングを使用しているアプリケーション間やサイト間で交換され、これらのアサーションによりサイト間でユーザを認証します。SAML のコンポーネントは次のとおりです。

- SAML アサーション：これは、IdP からサービス プロバイダーに転送される情報の構造と内容を定義します。セキュリティ情報のパケットで構成され、さまざまなレベルのアクセス コントロール決定にサービス プロバイダの用途があることを示す文書が含まれます。SAML SSO は次の種類の文書を提供します。
  - 認証ステートメント：これらのステートメントは、IdP とブラウザの間で特定の時間に行う認証の方法について、サービス プロバイダーにアサートします。
  - 属性ステートメント：これらのステートメントは、ユーザに関連付ける特定の属性（名前と値のペア）についてアサートします。属性アサーションには、ユーザに関する具体的な情報が含まれます。サービスプロバイダーは、属性を使用してアクセス制御の決定を行います。
- SAML プロトコル：SAML プロトコルは、SAML がアサーションをどのように要求し、取得するかを定義します。このプロトコルは、特定の SAML エレメントまたはアサーションで構成されている、SAML 要求と応答エレメントに対応します。SAML 2.0 には次のプロトコルがあります。
  - アサーション クエリと要求のプロトコル
  - 認証要求のプロトコル
- SAML バインディング：SAML バインディングは、SOAP 交換のような、標準メッセージング形式または通信プロトコルとの SAML アサーションまたはプロトコル メッセージ（またはその両方）の交換のマッピングを指定します。ACI は次の SAML 2.0 バインディングをサポートしています。
  - HTTP Redirect（GET）バインディング
  - HTTP POST バインディング
- SAML プロファイル：SAML プロファイルでは、明確に定義された使用事例をサポートするために、SAML アサーション、プロトコル、およびバインディングの組み合わせについて詳細に説明しています。

NTP の設定

SAML SSO で、Network Time Protocol（NTP）では APIC および IdP 間のクロック同期が可能です。SAML は時間的な制約のあるプロトコルであり、IdP は SAML アサーションが有効であることを時間ベースで判断します。IdP および APIC クロックが同期されていない場合、アサーションが無効になり SAML SSO 機能が停止します。IdP および APIC の間で許可される最大時差は 3 秒です。

（注） SAML SSO を動作させるには、NTP 設定を正しくインストールする必要があり、IdP と APIC アプリケーション間の時間差が 3 秒を超えていないことを確認する必要があります。IdP および APIC クロックが同期されていない場合、ユーザーは IdP で認証に成功した後でも APIC のログイン ページにリダイレクトされます。

DNS の設定

Domain Name System（DNS）により、ホスト名とネットワーク サービスをネットワーク（複数可）内の IP アドレスにマッピングできるようになります。ネットワーク内に配置された DNS サーバは、ネットワーク サービスをホスト名にマッピングし、次にホスト名を IP アドレスにマッピングするデータベースを備えています。ネットワーク上のデバイスは、DNS サーバに照会して、ネットワークにある他のデバイスの IP アドレスを受信できます。そのため、ネットワーク デバイス間の通信が容易になります。

まとめると、APIC および Idp は互いの完全修飾ドメイン名を IP アドレスに対して解消でき、クライアントによって解消される必要があります。

Certificate Authority：認証局

シスコは、次のいずれかの種類の認証局（CA）により署名されるサーバ証明書を使用することを推奨します。

- **パブリック CA**：サードパーティ企業が、サーバーの識別情報を確認し、信頼できる証明書を発行します。
- **プライベート CA**：自身でローカルの CA を作成および管理し、信頼できる証明書を発行します。

署名プロセスは製品ごとに異なり、サーバのバージョン間でも異なる場合があります。各サーバのすべてのバージョンに関する詳細な手順については、このマニュアルの範囲外になります。CA により署名された証明書を取得する方法の詳細な手順については、該当するサーバのマニュアルを参照してください。

パブリック CA により署名されたサーバ証明書を取得する場合、パブリック CA は、クライアント コンピュータの信頼ストアで、ルート証明書をあらかじめ提示しておくようにします。この場合、クライアント コンピュータでルート証明書をインポートする必要はありません。プライベート CA など、CA により署名される証明書が信頼ストアにまだ存在しない場合は、ルート証明書をインポートしてください。SAML SSO では、CN または SAN での正しいドメインが記載された CA 署名付き証明書が、IdP およびサービス プロバイダーに必要になります。正しい CA 証明書が検証されない場合、ブラウザはポップ アップ警告を出します。

APIC の信頼ストアに IdP のルート証明書が含まれていない場合は、新しい証明機関を作成する必要があります。APIC で SAML プロバイダを設定する際は、この認証機関を後で使用する必要があります。

SAML アクセス用の APIC の設定

（注） SAML ベースの認証と CLI/REST の APIC GUI でのみです。また、リーフ スイッチと背表紙には適用されません。APIC CLI では、SAML 設定を行うことはできません。

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックが設置され、Application Policy Infrastructure Controller（APIC）がオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- SAML サーバ 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。
- APIC 管理エンドポイント グループを使用できること。
- 次の設定を行います。
  - 時刻同期と 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。
  - 拡張 GUI を使用した DNS プロバイダーと接続するための DNS サービス ポリシーの設定：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。
  - GUI を使用した Cisco ACI HTTPS アクセス用カスタム証明書の設定：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 APIC で、SAML プロバイダーを作成します。

プロバイダーを作成するには、「プロバイダーを作成する （7 ページ）」を参照してください。

ステップ 2 SAML の**ログイン ドメイン**を作成します。

詳細な手順については、「GUI を使用してローカル ドメインを作成する （12 ページ）」 を参照してください。

REST API を使用して APIC で SAML を設定する

REST API を使用して SAML を構成するには、以下に示すように、最初に SAML プロバイダーを作成します。

```
<aaaSamlProvider name="cisco729224.okta.com"
dn="uni/userext/samlext/samlprovider-cisco729224.okta.com"
  entityId="http://www.okta.com/exk7j6qjvxgk8hwy0696"
  guiBannerMessage=""
  idP="okta"
  metadataUrl="https://cisco729224.okta.com/app/exk7j6qjvxgk8hwy0696/sso/saml/metadata"
monitorServer="disabled" retries="1" timeout="5"
  tp="oktacert"
  wantAssertionsEncrypted="no" wantAssertionsSigned="yes" wantRequestsSigned="yes"
wantResponseSigned="yes"
sigAlg="SIG_RSA_SHA256"
status="created,modified" />
```

次に、ログイン ドメインを作成します。認証には、CiscoAVPair またはグループ マップのいずれかを使用できます。

```
Authentication using CiscoAVPair
<aaaUserEp dn="uni/userext" status="created,modified">
<aaaLoginDomain dn="uni/userext/logindomain-TestSAML" name="TestSAML"
status="created,modified">
<aaaDomainAuth dn="uni/userext/logindomain-TestSAML/domainauth" providerGroup="TestSAML"
 realm="saml" realmSubType="default" status="created,modified"/>
</aaaLoginDomain>
<aaaSamlEp rn="samlext" status="modified">
<aaaSamlProviderGroup dn="uni/userext/samlext/samlprovidergroup-TestSAML" name="TestSAML"
 authChoice="CiscoAVPair" status="created,modified">
<aaaProviderRef
dn="uni/userext/samlext/samlprovidergroup-TestSAML/providerref-cisco729224.okta.com"
name="cisco729224.okta.com" order="1" status="created,modified"/>
</aaaSamlProviderGroup>
</aaaSamlEp>
</aaaUserEp>

Authentication using Group Map
<aaaUserEp dn="uni/userext" status="created,modified">
<aaaLoginDomain dn="uni/userext/logindomain-TestSAML" name="TestSAML"
status="created,modified">
<aaaDomainAuth dn="uni/userext/logindomain-TestSAML/domainauth" providerGroup="TestSAML"
 realm="saml" realmSubType="default" status="created,modified"/>
</aaaLoginDomain>
<aaaSamlEp rn="samlext" status="modified">
<aaaSamlProviderGroup dn="uni/userext/samlext/samlprovidergroup-TestSAML" name="TestSAML"
 authChoice="LdapGroupMap" groupAttribute="memberOf" status="created,modified">
<aaaUserGroupMapRule name="AdminRule" userGroup="CN=Domain
Admins,CN=Users,DC=insaaadev,DC=net" status="created,modified">
<aaaUserDomain name="all" rn="userdomain-all" status="created,modified">
<aaaUserRole name="fabric-admin" privType="writePriv" rn="role-fabric-admin"
status="created,modified"/>
</aaaUserDomain>
<aaaUserDomain name="mgmt" rn="userdomain-mgmt" status="created,modified">
<aaaUserRole name="access-admin" privType="writePriv" rn="role-access-admin"
status="created,modified"/>
<aaaUserRole name="nw-svc-policy" privType="writePriv" rn="role-nw-svc-policy"
status="created,modified"/>
</aaaUserDomain>
</aaaUserGroupMapRule>

<aaaUserGroupMapRule name="EmpRule" userGroup="CN=Employee,CN=Users,DC=insaaadev,DC=net"
 status="created,modified">
<aaaUserDomain name="mgmt" rn="userdomain-mgmt" status="created,modified">
<aaaUserRole name="ops" privType="writePriv" rn="role-ops" status="created,modified"/>
</aaaUserDomain>
</aaaUserGroupMapRule>
```

```
<aaaProviderRef
dn="uni/userext/samlext/samlprovidergroup-TestSAML/providerref-cisco729224.okta.com"
name="cisco729224.okta.com" order="1" status="created,modified"/>
</aaaSamlProviderGroup>
</aaaSamlEp>
</aaaUserEp>
```

Okta で SAML アプリケーションの設定

Okta で SAML を設定するには、管理者特権を持つユーザーとして Okta 組織にログインします。

（注） Okta 組織をお持ちでない場合、空の Okta を作成できます。

https://www.okta.com/start-with-okta/

ステップ 1 Okta で、青色の **[管理者]** ボタンをクリックします。

ステップ 2 **[アプリケーションの追加]** ショートカットをクリックします。

ステップ 3 緑色の **[新しいアプリケーションの作成]** ボタンをクリックし、次の操作を行います。

a) **[新しいアプリケーションの作成]** ダイアログ ボックスで、**[SAML 2.0]** オプションを選択し、緑色の **[作成]** ボタンをクリックします。

b) **[全般設定]** ボックスで、**[例 SAML アプリケーション]** を、 **[アプリケーション名]** フィールドに入力し、緑色の **[次へ]** ボタンをクリックします。

c) **[SAML の設定]** セクション A **[SAML 設定]** フィールドで、**[シングル サインオン URL]**、**[受信者 URL]**、**[対象者の制限]** フィールドに SAML URL を貼り付けます。

このフィールドは次の形式にする必要があります。

- https://<APIC_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name> </Login_domain_name> </APIC_hostname>
- 要求可能な SSO URL を使用して APIC のクラスタを設定します。
  - https://<APIC1_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name> </Login_domain_name> </APIC1_hostname>
  - https://<APIC2_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name> </Login_domain_name> </APIC2_hostname>
  - https://<APIC3_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name> </Login_domain_name> </APIC3_hostname>
- 名前 ID 形式：Transient
- 応答：署名済み
- アサーション署名: 署名

- アサーション暗号化: 暗号化されていません。
- SAML シングル ログアウト: Disabled
- authnContextClassRef: PasswordProtectedTransport
- SAML 発行者 ID: http://www.okta.com/$ {org.externalKey}

d) **[Attribute Statements]** セクションで、**[FirstName]**、**[LastName]**、**[Email]**、**[CiscoAvpair]** フィールドに情報を追加して、**[次へ]** をクリックします。

（注） **CiscoAvpair** と呼ばれるカスタム属性は **[プロファイル エディタ]** で Okta ユーザーを作成する必要があります。CiscoAvpair の詳細は、外部認証サーバの AV ペア （2 ページ） を参照してください。

e) **[フィードバック]** ボックスで、**[私は内部アプリケーションを追加する Okta 顧客です]** および **[これは私が作成した内部アプリケーションです]** を選択して、**[終了]** をクリックします。

ステップ 4 新しく作成した **[例 SAML アプリケーション]** アプリケーションの **[サインオン]** が表示されます。このページを保存し、別のタブまたはブラウザウィンドウで開きます。SAML 設定の **[ID プロバイダー メタデータ]** をコピーするには、後でこのページに戻ります。

（注） メタデータのリンクをコピーするには、**[ID プロバイダー メタデータ]** リンクを右クリックして **[コピー]** を選択します。

AD FS で Relying Party Trust の設定

AD FS 管理コンソールで信頼当事者証明を追加します。

ステップ 1 証明書利用者信頼を追加します。

a) AD FS サーバの AD FS 管理コンソールにログインし、**ADFS** > **Trust Relationships** > **Relying Party Trusts** の順に移動して、 [Add Relying Party Trust] を右クリックしてから [Start] をクリックします。

b) APIC 内で、対応するログイン ドメイン設定で利用できる [Download SAML Metadata] オプションを使用して生成されたメタデータ ファイルをインポートすることによって、 [Enter data about the relying party manually] または [Import data about relying party from a file (skip the steps d, e, f and g)] を選択します。

c) [Display Name] に信頼当事者証明の任意の表示名を入力し、[Next] をクリックします。

d) AD FS プロファイルを選択し、[Next] をクリックします。

e) もう一度 [Next] をクリックします。

f) [Enable support for the SAML 2.0 Web SSO Protocol] を選択し、**信頼当事者 SAML2.0 SSO サービス の URL** として *https://<APIC_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name>* と入力し、[Next] をクリックします。

g) **信頼当事者証明の識別子**として *https://<APIC_hostname>/api/aaaLoginSSO.json* 入力します。

h) [I do not want to configure multi-factor authentication settings for this relying party trust at this time] を選択し、[Next] をクリックします。

i) [Permit all users to access this relying party] を選択し、[Next] をクリックします。

j) [Open the Edit Claim Rules dialog for this relying party trust when the wizard closes] を選択し、[Close] をクリックします。

ステップ 2 次の**クレーム** ルールを追加します。

a) LDAP 属性をクレームとして送信します。

- [Edit Claim Rules] ウィンドウで、[Add Rule] をクリックします。
- [Claim Rule Template] で [Send LDAP attributes as Claims] を選択し、[Next] をクリックします。
- [Rule_Name] を入力し、[Attribute Store] として [Active Directory] を選択します。
- CiscoAvpair を格納するための予約済みユーザ属性を選択します（たとえば、[LDAP attribute type] として [Department] を選択し、それを [Outgoing Claim Manually Type] の [CiscoAvpair] にマッピングします）。
- [LDAP Attribute] で [E-Mail-Addresses] を選択し、それを [Outgoing Claim Type] の [E-mail Address] にマッピングして、[Finish] をクリックします。

b) 着信要求を変換します。

- [Edit Claim Rules] ウィンドウで再度 [Add Rule] をクリックし、[Transform an Incoming Claim as Claim Rule Template] を選択して、[Next] をクリックします。
- [Incoming claim type] として [E-Mail Address] を選択 します。
- [Outgoing claim type] として [Name ID] を選択します。
- [Outgoing name ID format] として [Transient Identifier] を選択します。

ステップ 3 APICのクラスタを追加するには、複数の**信頼当事者証明**をセットアップするか、または1つの**信頼当事者証明**をセットアップしてから複数の**信頼当事者識別子** および **SAML アサーション コンシューマ エンドポイント** をそれに追加することができます。

a) 上記で作成した同じ信頼当事者証明を持つクラスタ内に、他の APIC を追加する。

1. **ADFS Management Console** > **ADFS** > **Trust Relationships** > **Relying Party Trusts** と移動して、**CiscoAPIC** > **Properties** の順に右クリックします。
2. [Identifiers] タブをクリックし、クラスタ内に他の APIC を次のとおりに追加します：*https://<APIC2_hostname>/api/aaaLoginSSO.json*、*https://<APIC3_hostname>/api/aaaLoginSSO.json*
3. [Endpoints] タブをクリックし、[Add SAML] をクリックすることによって他の 2 つの APIC を追加します。[Add SAML Post Binding] 、[Index] を 1 として、信頼されている URL に *https://<APIC2_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name>* のように入力します。そして、[Add SAML Post Binding] に *https://<APIC3_hostname>/api/aaaLoginSSO.json?name=<Login_domain_name* のように入力します。

ステップ 4 メッセージとアサーションは、ADFS サーバ内の powershell から ADFS で署名する必要があります。ADFS サーバーでメッセージおよびアサーションを署名するには：

a) Windows Powershell を開き（管理者として実行する必要があります）、次のコマンドを実行します。
b) Set AdfsRelyingPartyTrust TargetName **RelyingpartytrustnameOfCiscoAPIC** - SamlResponseSignature **MessageAndAssertion** 。

OAuth 2 / OIDC 認証

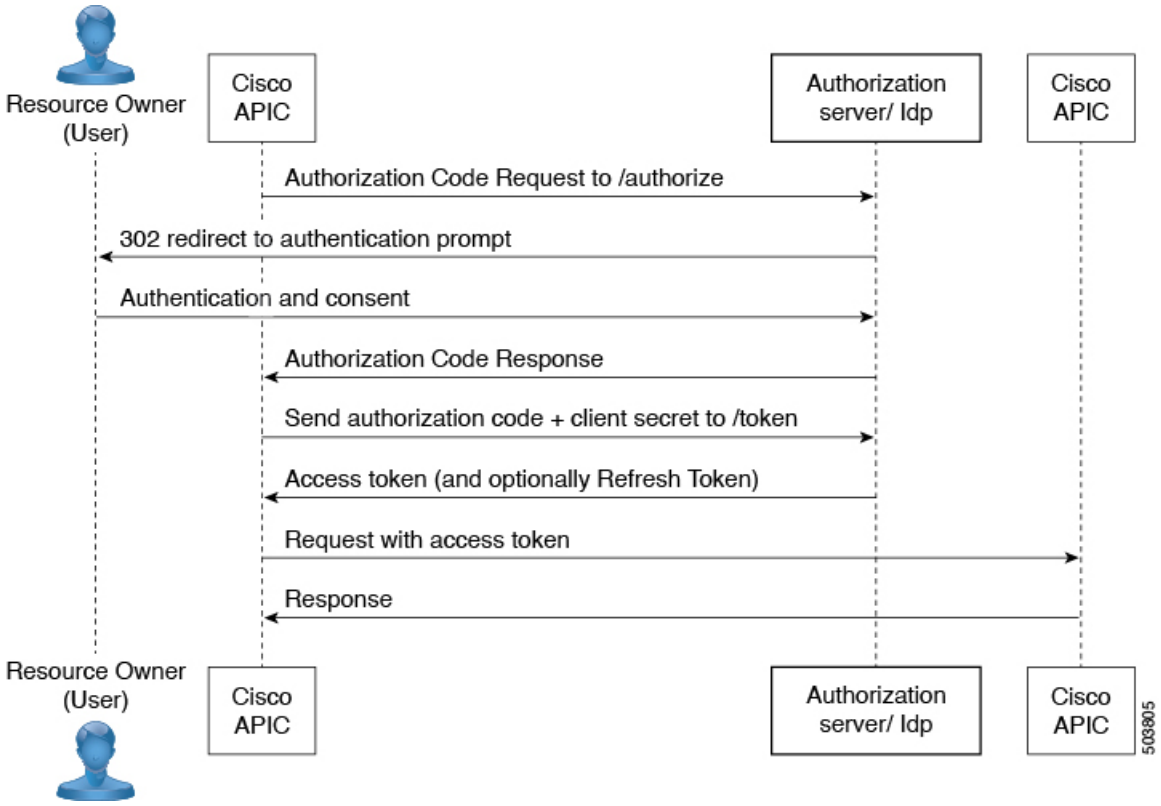
Open Authorization (OAuth) 2.0 は、オープン標準の認証プロトコルです。OAuth 2.0 を使用すると、ID プロバイダー (IdP) によって信頼または承認されたアプリケーション（サービスプロバイダー、すなわち SP）にアクセスできます。OAuth 2.0 は、承認トークンを使用して、コンシューマー アプリケーションに ID と承認請求を提供します。

OAuth 2.0 の詳細については、*RFC 6749* を参照してください。

OAuth 2.0 は、サービスプロバイダー アプリケーションから REST API を使用するさまざまなクライアントタイプをサポートするように設計されています。これには、企業内の Web サービスにアクセスするブラウザアプリケーションと、顧客のモバイルデバイスで実行されるアプリケーションの両方が含まれます。OAuthプロトコルでは、認証トークンを取得するための複数のメカニズムを定義し、さまざまなメカニズムがクライアントタイプの制約を認識します。単純な OAuth の例は、「https://service.example.com」などの Web サイトにログインしようとすると、ソーシャルメディアプラットフォームのログインまたは電子メールログインを使用して自分自身を識別するように求められる場合があります。これらの ID プロバイダーにログインしている場合は、何度もログインする必要はありません。いずれかのオプションを選択するとすぐに、「https://service.example.com」にログインすることが（OAuth を使用して）許可されます。

Cisco ACI での OAuth 2.0 認証

ACI で使用される OAuth のタイプは、承認付与フローです。この方法では、Cisco APIC は最初に認証されたユーザーによる承認付与を要求し、APIC は次に承認付与を使用して、承認情報を持つアクセス トークンを取得します。フローを次の図に示します。



OAuth の要素

- リソース所有者（ユーザー）— データ所有者
- Web アプリケーション — APIC（または Cloud APIC ）
- 承認サーバー（AS）または ID プロバイダー（IdP）サーバー - ユーザーを認証および承認します。
- リソース サーバー — APIC

（注） 承認サーバーが ID トークンとアクセス トークンの両方を提供する場合、ID トークンは、ユーザー名と CiscoAvpair クレームのアクセス トークンよりも優先されます。ID トークンで CiscoAvpair が利用できない場合、ユーザー名と CiscoAvpair の両方の要求がアクセス トークンから取得されます（利用可能な場合）。APIC は、両方のトークンからのユーザー名と CiscoAvpair クレームを結合しません。つまり、ID トークンからのユーザー名とアクセス トークンからの CiscoAvpair は考慮しません。また、その逆も考慮しません。どのトークンにも CiscoAvpair 要求がない場合、ID トークンからのユーザー名が取得され、設定されている場合はデフォルトの認証が試行されます。

Cisco APIC で OAuth を設定する

この手順を使用して、Cisco APIC で OAuth を設定します。

前提条件

Okta（またはその他の認証サーバー）で次のアクションを実行します。

- APIC 用の OAuth アプリケーションを作成します。クライアント ID とシークレットを書き留めます。
- APIC へのアクセスを許可する許可ポリシーが設定されていることを確認します。
- ACI で使用される承認エンドポイントとトークン エンドポイントに注意してください。
- APIC を使用するアプリケーションにユーザーを割り当てます。
- *CiscoAvpair* が、ACI での認証のためにユーザーに対して正しく設定されていることを確認します。
- トークン URL の証明書チェーンを保存します。

ID プロバイダーでの OAuth 2.0 アプリケーションの設定の詳細については、関連するドキュメントを参照してください。

OAuth 2 アクセス用の APIC の設定

この手順を使用して、OAuth 2 プロバイダーを作成し、ログインドメインを関連付けます。

ステップ 1 APIC で、OAuth 2 プロバイダーを作成します。

OAuth 2 プロバイダーの構成については、「プロバイダーを作成する （7 ページ）」 を参照してください。

ステップ 2 OAuth 2 の [**ログイン ドメイン（Login Domain）**] を作成します。

詳細な手順については、「GUI を使用してローカル ドメインを作成する （12 ページ）」 を参照してください。

認証局を作成する

トークン URL に使用される証明書チェーンを使用して認証局を作成するには、この手順を使用します。

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

ステップ 2 ナビゲーション ウィンドウで、[**セキュリティ（Security）**] を選択します。

ステップ 3 作業ペインで、[**認証局（Certificate Authorities）**] を選択します。

ステップ 4 [アクション（**Actions**）] > [認証局の作成（**Create Certificate Authority**）] をクリックします。

ステップ 5 名前、説明、および**証明書チェーン**を入力します。

以下の手順で**証明書チェーン**を取得してください。

a) Okta/承認サーバーからトークン URL を選択します。
b) ブラウザ ウィンドウで、トークン URL を入力します。
c) 右クリックして、**[詳細情報（More Information）]** を選択します。
d) 表示されたポップアップ ウィンドウから、**[新しい証明書（New Certificate）]** ボタンをクリックします。
e) 証明書画面が表示されます。**PEM（チェーン）** 証明書をダウンロードします。
f) 適切なプログラムを選択してファイルを開きます。
g) 表示された証明書のチェーンから必要な証明書を選択します。

（注） 最大 8 つの認証局を作成できます。

ステップ 6 **[保存（Save）]** をクリックします。

OAuth を使用したユーザー ログイン

OAuth 用に作成されたログイン ドメインを使用して APIC にログインしようとすると、認可サーバーのログインページにリダイレクトされます（まだ認証されていない場合）。ユーザーが認証されると、Web ブラウザを介して認可サーバーから APIC に認可コードが送信されます。APIC は、APIC アプリケーションのクライアント ID とシークレットを使用して、IdP からのアクセス トークンとこのコードを交換します。アクセス トークンには、*CiscoAvpair* のユーザー名と認証の詳細があります。その後、APIC にログインします。APIC では、ログインしているユーザーがそれに応じて示されます。

REST API を使用して APIC で OAuth を設定する

この手順を使用して、REST API を使用し APIC で OAuth を設定します。

ステップ 1 OAuth プロバイダーを作成します。

```
<aaaOauthProvider name="cisco729224.okta.com"
dn="uni/userext/oauthext/oauthprovider-cisco729224.okta.com"
status="created,modified"
timeout="5"
key="vCnIq1EGCTPfqMU"
oidcEnabled="no"
verifyEnabled="yes"
baseUrl="https://cisco729224.okta.com/oauth2/default"
clientId="0oa9g25h1cE7yZZ0t696"
usernameAttribute="EmailId"
scope="openid groups"
tp="oktacert"/>
```

ステップ 2 OAuth ログイン ドメインを作成します。認証には、CiscoAVPair またはグループ マップのいずれかを使用できます。

```
Authentication using CiscoAVPair
<aaaUserEp dn="uni/userext" status="created,modified">
<aaaLoginDomain dn="uni/userext/logindomain-TOAUTH" name="TOAUTH" status="created,modified">
<aaaDomainAuth dn="uni/userext/logindomain-TOAUTH/domainauth" providerGroup="TOAUTH" realm="oauth"
 realmSubType="default" status="created,modified"/>
</aaaLoginDomain>
<aaaOauthEp rn="oauthext" status="modified">
<aaaOauthProviderGroup dn="uni/userext/oauthext/oauthprovidergroup-TOAUTH" name="TOAUTH"
authChoice="CiscoAVPair" status="created,modified">
<aaaProviderRef dn="uni/userext/oauthext/oauthprovidergroup-TOAUTH/providerref-cisco729224.okta.com"
 name="cisco729224.okta.com" order="1" status="created,modified"/>
</aaaOauthProviderGroup>
</aaaOauthEp>
</aaaUserEp>
```

```
Authentication using Group Map
<aaaUserEp dn="uni/userext" status="created,modified">
<aaaLoginDomain dn="uni/userext/logindomain-TOAUTH" name="TOAUTH" status="created,modified">
<aaaDomainAuth dn="uni/userext/logindomain-TOAUTH/domainauth" providerGroup="TOAUTH" realm="oauth"
 realmSubType="default" status="created,modified"/>
</aaaLoginDomain>
<aaaOauthEp rn="oauthext" status="modified">
<aaaOauthProviderGroup dn="uni/userext/oauthext/oauthprovidergroup-TOAUTH" name="TOAUTH"
authChoice="LdapGroupMap" groupAttribute="memberOf" status="created,modified">
<aaaUserGroupMapRule name="AdminRule" userGroup="Domain Admins" status="created,modified">
<aaaUserDomain name="all" rn="userdomain-all" status="created,modified">
<aaaUserRole name="fabric-admin" privType="writePriv" rn="role-fabric-admin"
status="created,modified"/>
</aaaUserDomain>
<aaaUserDomain name="mgmt" rn="userdomain-mgmt" status="created,modified">
<aaaUserRole name="access-admin" privType="writePriv" rn="role-access-admin"
status="created,modified"/>
<aaaUserRole name="nw-svc-policy" privType="writePriv" rn="role-nw-svc-policy"
status="created,modified"/>
</aaaUserDomain>
</aaaUserGroupMapRule>
<aaaUserGroupMapRule name="EmpRule" userGroup="Employee" status="created,modified">
<aaaUserDomain name="mgmt" rn="userdomain-mgmt" status="created,modified">
<aaaUserRole name="ops" privType="writePriv" rn="role-ops" status="created,modified"/>
</aaaUserDomain>
</aaaUserGroupMapRule>
<aaaProviderRef dn="uni/userext/oauthext/oauthprovidergroup-TOAUTH/providerref-cisco729224.okta.com"
 name="cisco729224.okta.com" order="1" status="created,modified"/>
</aaaOauthProviderGroup>
</aaaOauthEp>
</aaaUserEp>
```

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。