ユーザアクセス、認証およびアカウンティング

この章は、次の内容で構成されています。

アクセス権のワークフローの依存関係

Cisco Application Centric Infrastructure (ACI) RBAC のルールによって、ファブリック全体へのアクセスを有効にするか、一部へのアクセスに制限します。たとえば、ベア メタル サーバ アクセス用のリーフ スイッチを設定するには、ログインしている管理者が `infra` ドメインに対する権限を持っている必要があります。デフォルトでは、テナント管理者は `infra` ドメインに対する権限を持っていません。この場合、リーフ スイッチに接続されているベア メタル サーバの使用を計画しているテナント管理者は、そのために必要なすべての手順を実行することはできません。テナント管理者は、`infra` ドメインに対する権限を持っているファブリック管理者と連携する必要があります。ファブリック管理者は、テナント管理者が ACI リーフ スイッチに

接続されたベア メタル サーバを使用するアプリケーション ポリシーを導入するために使用するスイッチ設定ポリシーをセットアップします。

ユーザ アクセス、認可およびアカウンティング

Application Policy Infrastructure Controller（APIC）ポリシーは、Cisco Application Centric Infrastructure（ACI）ファブリックの認証、認可、およびアカウンティング（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、CLI、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。

マルチテナントのサポート

コア Application Policy Infrastructure Controller（APIC）の内部データ アクセス コントロール システムにより、マルチテナント分離が提供され、テナント間での個人情報の漏洩が防止されます。読み取り/書き込みの制約により、テナントによる他のテナントの設定、統計情報、障害、またはイベントデータの参照が防止されます。管理者によって読み取り権限が割り当てられない限り、テナントはファブリックの設定、ポリシー、統計情報、障害、またはイベントの読み取りが制限されます。

ユーザ アクセス：ロール、権限、セキュリティ ドメイン

APIC では、ロールベース アクセス コントロール (RBAC) を介してユーザのロールに従ってアクセスが提供されます。Cisco Application Centric Infrastructure (ACI) ファブリック ユーザは、次に関連付けられています。

- 事前定義またはカスタム ロール。ユーザに割り当てられた 1 つ以上の権限のセットです。
- 権限のセット。ユーザがアクセスできる管理対象オブジェクト（MO）を決定します。
- ロールごとの権限タイプ：アクセスなし、読み取り専用、または読み取り/書き込み
- ユーザがアクセスできる管理情報ツリー (MIT) の一部を識別する 1 つ以上のセキュリティ ドメイン タグ

ロールと権限

権限はシステム内の特定の機能に対するアクセス権を制御します。ACI ファブリックは、管理対象オブジェクト（MO）レベルでアクセス権限を管理します。すべてのオブジェクトは、読み取り可能な権限のリストと、書き込み可能な権限のリストを保持しています。特定の機能に

対応するすべてのオブジェクトには、その機能の読み取りまたは書き込みリストの権限が付与されます。オブジェクトは追加の機能に対応する場合があるため、そのリストには複数の権限が含まれている場合があります。権限を含むロールがユーザに割り当てられると、そのユーザには、読み取りリストが読み取りアクセスを指定する関連オブジェクトへの読み取りアクセス権が付与され、書き込みリストが書き込みアクセスを指定するオブジェクトへの書き込みアクセス権が付与されます。

たとえば、「fabric-equipment」は、物理ファブリック内の機器に対応するすべてのオブジェクトへのアクセスを制御する権限です。物理ファブリック内の機器に対応するオブジェクト（「eqptBoard」など）には、特権リストに「fabric-equipment」が含まれます。「eqptBoard」オブジェクトは、「fabric-equipment」権限の読み取り専用アクセスを許可します。「fabric-admin」などの権限「fabric-equipment」が割り当てられているユーザには、「eqptBoard」オブジェクトへの読み取り専用アクセスなど、これらの機器オブジェクトへのアクセス権が付与されます。

（注） 一部のロールには他のロールが含まれています。たとえば、テナント管理者、ファブリック管理者、アクセス管理者などの「-admin」ロールは、同じベース名を持つロールのグループです。たとえば、「access-admin」は「access-connectivity」、「access-equipment」、「access-protocol」、および「access-qos」のグループです。同様に、tenant-adminは「テナント」ベースのロールのグループで、fabric-adminは「ファブリック」ベースのロールのグループです。

「admin」ロールにはすべての権限が含まれます。

ロールと権限の詳細については、『APIC ロールと権限マトリクス』を参照してください。

セキュリティ ドメイン

セキュリティ ドメインは、ACI MIT オブジェクト階層の特定のサブツリーに関連付けられたタグです。たとえば、デフォルトのテナント「common」にはドメインタグ `common` が付いています。同様に、特殊なドメインタグ `all` の場合、MIT オブジェクトツリー全体が含まれます。管理者は、MIT オブジェクト階層にカスタム ドメイン タグを割り当てることができます。たとえば、管理者は「solar」という名前のテナントにドメインタグ「solar」を割り当てることができます。MIT 内では、特定のオブジェクトだけがセキュリティ ドメインとしてタグ付けできます。たとえば、テナントはセキュリティ ドメインとしてタグ付けすることができますが、テナント内のオブジェクトはできません。

（注） セキュリティドメインのパスワード強度パラメータは、**[Custom Conditions]** を作成するか、または提供されている **[Any Three Conditions]** を選択して設定できます。

ユーザを作成してロールを割り当てても、アクセス権は有効になりません。1 つ以上のセキュリティ ドメインにそのユーザを割り当てることも必要です。デフォルトでは、ACI ファブリックには事前作成された次の 2 つの特殊なドメインが含まれています。

- `All`：MIT 全体へのアクセスを許可

- `Infra`：ファブリック アクセス ポリシーなどの、ファブリック インフラストラクチャのオブジェクトおよびサブツリーへのアクセスを許可

（注） ユーザのクレデンシャルが許可しない管理対象オブジェクトの読み取り操作の場合、「DN/Class Unauthorized to read」ではなく「DN/Class Not Found」というエラーが返されます。ユーザのクレデンシャルが許可しない管理対象オブジェクトへの書き込み操作の場合、「HTTP 401 Unauthorized」というエラーが返されます。GUI では、ユーザのクレデンシャルが許可しないアクションの場合、表示されないか、またはグレー表示されます。

事前に定義された一連の管理対象オブジェクト クラスをドメインに関連付けることができます。これらのクラスがオーバーラップすることはできません。ドメインの関連付けをサポートするクラスの例：

- レイヤ 2 およびレイヤ 3 のネットワークで管理されたオブジェクト
- ネットワーク プロファイル (物理、レイヤ 2、レイヤ 3、管理など)
- Quality of Service（QoS）ポリシー

ドメインに関連付けることができるオブジェクトが作成されると、ユーザは、ユーザのアクセス権の範囲内でオブジェクトにドメインを割り当てる必要があります。ドメインの割り当てはいつでも変更できます。

仮想マシン管理 (VMM) ドメインがセキュリティ ドメインとしてタグ付けされている場合、セキュリティ ドメイン内のユーザは、対応するタグ付き VMM ドメインにアクセスできます。たとえば、solar という名前のテナントに sun というセキュリティ ドメインのタグが付いており、VMM ドメインにも sun というセキュリティ ドメインのタグが付いている場合、solar テナント内のユーザは各自のアクセス権限に従って VMM ドメインにアクセスできます。

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。

手順

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）]** をクリックします。

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。**[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のグループに対するRADIUS プロバイダー グループ。
2. 認証用 TACACS+ プロトコルをサポートするリモート サーバのグループに対する 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。

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。

手順

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。
  - 寛容：DUO LDAP SSL証明書の問題の診断に役立つデバッグノブ。
  - 厳密：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。

ローカル ユーザの設定

初期の設定スクリプトで、管理者アカウントが設定され、管理者はシステム起動時の唯一のユーザとなります。APIC は、きめ細かなロールベースのアクセス コントロール システムをサポートしており、そのシステムでは、権限が少ない管理者以外のユーザを含め、ユーザ アカウントをさまざまなロールで作成することができます。

GUI を使用したローカル ユーザの設定

始める前に

- ACI ファブリックが設置され、APIC 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正常に動作していること。
- 必要に応じて、ユーザがアクセスするセキュリティ ドメインが定義されていること。たとえば、新しいユーザ アカウントがテナントへのアクセスに制限される場合、テナント ドメインはそれに応じてタグ付けされます。
- 以下を行うことができる APIC ユーザ アカウントを使用できること。
  - TACACS+ プロバイダーの作成。
  - ターゲット セキュリティ ドメインでのローカル ユーザ アカウントの作成。ターゲット ドメインが `all` である場合、新しいローカル ユーザの作成に使用するログイン アカウントは、`all` にアクセスできるファブリック全体の管理者である必要があります。ターゲット ドメインがテナントである場合、新しいローカル ユーザの作成に使用するログイン アカウントは、ターゲット テナント ドメインに対する完全な読み取り/書き込みアクセス権を持つテナント管理者である必要があります。

手順

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 [Navigation] ペインで、[Users] をクリックします。

[Work] ペインで、[Local Users] タブを表示していることを確認します。

ステップ 3 **[作業（Work）]** ペインで、タスク アイコンのドロップダウン リストをクリックし、**[ローカル ユーザの作成（Create Local User）]** を選択します。

ステップ 4 **[ステップ 1 > ユーザ ID（STEP 1 > User Identity）]** ダイアログ ボックスで、次の操作を実行します。

a) [Login ID] フィールドで、ID を追加します。

ログイン ID は、次のガイドラインを満たしている必要があります。

- APIC 内で一意である必要があります。
- 先頭は英字にする必要があります。
- 1 ー 32 文字を使用できます。
- 英数字、アンダースコア、ハイフンを使用してください。

ユーザ アカウントの作成後は、ログイン ID を変更できません。ユーザ アカウントを削除し、新しいユーザ アカウントを作成する必要があります。

b) [Password] フィールドにパスワードを入力します。

ユーザがパスワードを設定する時点で、APIC によって以下の基準が検証されます。

- パスワードの最小長は 8 文字です。
- パスワードの最大長は 64 文字です。
- 連続して繰り返される文字は 3 文字未満です。
- 小文字、大文字、数字、記号の文字種のうち少なくとも 3 種類の文字が含まれている必要があります。
- 簡単に推測できるパスワードは使用しません。
- ユーザ名やユーザ名を逆にしたものは使用できません。
- cisco、isco、またはこれらの文字列の並べ替えを変化させたものや、それらの文字の大文字化の変更により取得される変形語であってはなりません。

c) [Confirm Password] フィールドで、パスワードを確認します。

d) （任意） 証明書ベースの認証の場合は、**[ユーザ証明書の属性（User Certificate Attribute）]** フィールドに、認証証明書からのユーザ ID を入力します。

e) **[次へ（Next）]** をクリックします。

ステップ 5 **[アカウント ステータス（Account Status）]** コントロールを使用してユーザ アカウントをアクティブまたは非アクティブにできます。また、**[アカウントの有効期限（Account Expires）]** コントロールを使用して有効期限を設定できます。

ステップ 6 **[ステップ 2 > セキュリティ（STEP 2 > Security）]** ダイアログ ボックスの **[セキュリティ ドメイン（Security Domain）]** で、ユーザの機能のセキュリティ ドメインを選択し、**[次へ（Next）]** をクリックします。

ステップ 7 **[ステップ 3 > ロール（STEP 3 > Roles）]** ダイアログ ボックスで、次のアクションを実行します。

a) **[+]** をクリックして、ユーザをドメインに関連付けます。

b) ドロップダウン リストから、ユーザの**ロール名**と**ロール権限タイプ**を選択します。
c) **[更新（Update）]** をクリックします。

読み取り専用または読み取り/書き込み権限を提供できます。

ステップ 8 **[完了（Finish）]** をクリックします。

GUI を使用した SSH 公開キー認証の設定

始める前に

- ターゲット セキュリティ ドメインでローカル ユーザ アカウントを作成します。ターゲット ドメインが `all` である場合、新しいローカル ユーザの作成に使用するログイン アカウントは、`all` にアクセスできるファブリック全体の管理者である必要があります。ターゲット ドメインがテナントである場合、新しいローカル ユーザの作成に使用するログイン アカウントは、ターゲット テナント ドメインに対する完全な読み取り/書き込みアクセス権を持つテナント管理者である必要があります。
- UNIX コマンド **ssh-keygen** を使用して公開キーを生成します。

  デフォルトのログイン ドメインは **local** に設定する必要があります。

手順

ステップ 1 メニューバーで、**[管理者（Admin）]** > **[ユーザー（Users）]** を選択し、**[ローカル（Local）]** タブが表示されていることを確認します。

ステップ 2 **作業**ペインで、事前に作成したユーザーの名前をクリックします。

ユーザーに関する情報を含むウィンドウが右側に表示されます。

ステップ 3 **[詳細（Details）]** アイコンをクリックすると、新しい画面に  およびユーザーの詳細が表示されます。

下方向にスクロールして SSH 認証の詳細を確認します。

ステップ 4 **[編集（Edit）]** アイコンをクリックすると、  、および **[ローカル ユーザーの編集（Edit Local User）]** 画面が表示されます。必要に応じて、SSH の詳細を変更できます。

（注） リモートロケーションにダウンロードするための SSH 秘密キーファイルを作成するには、メニューバーで、**[ファイル名（Firmware）]** > **[タスクのダウンロード（Download Tasks）]** を展開します。

ステップ 5 **[保存（Save）]** をクリックします。

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。

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

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)
```

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。

手順

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 （8 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 （5 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。

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。

手順

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 （8 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 （5 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。

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。

手順

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。

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。

手順

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。

手順

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 （8 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 （5 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 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

手順

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。

署名ベースのトランザクションについて

Cisco ACI ファブリックの APIC コントローラは、ユーザを認証するためにさまざまな方法を提供します。

主要な認証方式ではユーザ名とパスワードが使用され、APIC REST API は APIC に対するその後のアクセスに使用できる認証トークンを返します。これは、HTTPS が使用不可であるか有効でない状況では安全でないと見なされます。

提供されている別の認証形式では、トランザクションごとに計算される署名が活用されます。その署名の計算には秘密キーが使用され、そのキーは安全な場所に保管して秘密にしておく必要があります。APIC がトークン以外の署名が付いた要求を受信すると、APIC は X.509 証明書を活用して署名を確認します。署名ベースの認証では、APICに対するすべてのトランザクションに新しく計算された署名が必要です。これは、ユーザがトランザクションごとに手動で行うタスクではありません。理想的には、この機能は APIC と通信するスクリプトまたはアプリケーションで使用する必要があります。この方法では、攻撃者がユーザ クレデンシャルを偽装またはなりすますためには RSA/DSA キーを解読する必要があるため、最も安全です。

（注） また、リプレイ攻撃を防ぐためには HTTPS を使用する必要があります。

認証に X.509 証明書ベースの署名を使用する前に、次の必須タスクが完了していることを確認します。

1. OpenSSL または同様のツールを使用して X.509 証明書と秘密キーを作成します。

2. APIC のローカル ユーザを作成します（ローカル ユーザがすでに利用可能である場合、このタスクはオプションです）。
3. APIC のローカル ユーザに X.509 証明書を追加します。

ガイドラインと制約事項

次の注意事項と制約事項に従ってください。

- ローカル ユーザはサポートされます。リモート AAA ユーザはサポートされません。
- APIC GUI は証明書認証方式をサポートしません。
- WebSocket と eventchannel は X.509 要求では動作しません。
- サードパーティにより署名された証明書はサポートされません。自己署名証明書を使用します。

X.509 証明書と秘密キーの生成

手順

ステップ 1 OpenSSL コマンドを入力して、X.509 証明書と秘密キーを生成します。

例：

```
$ openssl req -new -newkey rsa:1024 -days 36500 -nodes -x509 -keyout userabc.key -out
userabc.crt -subj '/CN=User ABC/O=Cisco Systems/C=US'
```

（注）
- X.509 証明書が生成されると、APIC のユーザ プロファイルに追加され、署名の確認に使用されます。秘密キーは、署名を生成するためにクライアントによって使用されます。
- 証明書には公開キーは含まれていますが、秘密キーは含まれていません。公開キーは、計算された署名を確認するために APIC によって使用される主要な情報です。秘密キーが APIC に保存されることはありません。このキーを秘密にしておく必要があります。

ステップ 2 OpenSSL を使用して証明書のフィールドを表示します。

例：

```
$ openssl x509 -text -in userabc.crt
        Certificate:
            Data:
                Version: 3 (0x2)
                Serial Number:
                    c4:27:6c:4d:69:7c:d2:b6
                Signature Algorithm: sha1WithRSAEncryption
                Issuer: CN=User ABC, O=Cisco Systems, C=US
                Validity
```

```
            Not Before: Jan 12 16:36:14 2015 GMT
            Not After : Dec 19 16:36:14 2114 GMT
        Subject: CN=User ABC, O=Cisco Systems, C=US
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:92:35:12:cd:2b:78:ef:9d:ca:0e:11:77:77:3a:
                    99:d3:25:42:94:b5:3e:8a:32:55:ce:e9:21:2a:ff:
                    e0:e4:22:58:6d:40:98:b1:0d:42:21:db:cd:44:26:
                    50:77:e5:fa:b6:10:57:d1:ec:95:e9:86:d7:3c:99:
                    ce:c4:7f:61:1d:3c:9e:ae:d8:88:be:80:a0:4a:90:
                    d2:22:e9:1b:25:27:cd:7d:f3:a5:8f:cf:16:a8:e1:
                    3a:3f:68:0b:9c:7c:cb:70:b9:c7:3f:e8:db:85:d8:
                    98:f6:e3:70:4e:47:e2:59:03:49:01:83:8e:50:4a:
                    5f:bc:35:d2:b1:07:be:ec:e1
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                0B:E4:11:C7:23:46:10:4F:D1:10:4C:C1:58:C2:1E:18:E8:6D:85:34
            X509v3 Authority Key Identifier:
              keyid:0B:E4:11:C7:23:46:10:4F:D1:10:4C:C1:58:C2:1E:18:E8:6D:85:34

                DirName:/CN=User ABC/O=Cisco Systems/C=US
                serial:C4:27:6C:4D:69:7C:D2:B6

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha1WithRSAEncryption
        8f:c4:9f:84:06:30:59:0c:d2:8a:09:96:a2:69:3d:cf:ef:79:
        91:ea:cd:ae:80:16:df:16:31:3b:69:89:f7:5a:24:1f:fd:9f:
        d1:d9:b2:02:41:01:b9:e9:8d:da:a8:4c:1e:e5:9b:3e:1d:65:
        84:ff:e8:ad:55:3e:90:a0:a2:fb:3e:3e:ef:c2:11:3d:1b:e6:
        f4:5e:d2:92:e8:24:61:43:59:ec:ea:d2:bb:c9:9a:7a:04:91:
        8e:91:bb:9d:33:d4:28:b5:13:ce:dc:fe:c3:e5:33:97:5d:37:
        cc:5f:ad:af:5a:aa:f4:a3:a8:50:66:7d:f4:fb:78:72:9d:56:
        91:2c
[snip]
```

ローカル ユーザの設定

GUI を使用したローカル ユーザの作成とユーザ証明書の追加

手順

ステップ 1 メニュー バーで、**[ADMIN]** > **[AAA]** を選択します。

ステップ 2 [Navigation] ペインの [Work] ペインで、[Users] と [Local Users] をクリックします。

ステップ 3 [Work] ペインで、[Local Users] タブを表示していることを確認します。

デフォルトでは admin ユーザが存在します。

ステップ 4 [Work] ペインで、タスク アイコンのドロップダウン リストをクリックし、[Create Local User] を選択します。

ステップ 5 [Security] ダイアログボックスで、ユーザに必要なセキュリティ ドメインを選択し、[Next] をクリックします。

ステップ 6 [Roles] ダイアログボックスで、ユーザのロールを選択するためのオプション ボタンをクリックし、[Next] をクリックします。

読み取り専用または読み取り/書き込み権限を提供できます。

ステップ 7 [User Identity] ダイアログボックスで、次の操作を実行します。

a) [Login ID] フィールドで、ID を追加します。
b) [Password] フィールドにパスワードを入力します。
c) [Confirm Password] フィールドで、パスワードを確認します。
d) （オプション）証明書ベースの認証の場合は、[User Certificate Attribute] フィールドに、認証証明書からのユーザ ID を入力します。
e) [Finish] をクリックします。

ステップ 8 [Navigation] ペインで、作成したユーザの名前をクリックします。[Work] ペインで、[Security Domains] 領域のユーザの横にある [+] 記号を展開します。
ユーザのアクセス権限が表示されます。

ステップ 9 [Work] ペインの [User Certificates] 領域で、ユーザ証明書の [+] 記号をクリックし、[Create X509 Certificate] ダイアログ ボックスで次の操作を実行します。

a) [Name] フィールドに、証明書の名前を入力します。
b) [Data] フィールドに、ユーザ証明書の詳細を入力します。
c) **Submit** をクリックします。

X509 証明書がローカル ユーザ用に作成されます。

Python SDK を使用したローカル ユーザの作成

手順

ローカル ユーザを作成します。

例：

```
#!/usr/bin/env python
from cobra.model.pol import Uni as PolUni
from cobra.model.aaa import UserEp as AaaUserEp
from cobra.model.aaa import User as AaaUser
from cobra.model.aaa import UserCert as AaaUserCert
from cobra.model.aaa import UserDomain as AaaUserDomain
from cobra.model.aaa import UserRole as AaaUserRole
from cobra.mit.access import MoDirectory
from cobra.mit.session import LoginSession
from cobra.internal.codec.jsoncodec import toJSONStr

APIC = 'http://10.10.10.1'
username = 'admin'
password = 'p@$$w0rd'
```

```
session = LoginSession(APIC, username, password)
modir = MoDirectory(session)
modir.login()

def readFile(fileName=None, mode="r"):
   if fileName is None:
      return ""
   fileData = ""
   with open(fileName, mode) as aFile:
      fileData = aFile.read()
   return fileData

# Use a dictionary to define the domain and a list of tuples to define
# our aaaUserRoles (roleName, privType)
# This can further be abstracted by doing a query to get the valid
# roles, that is what the GUI does

userRoles = {'all': [
               ('aaa', 'writePriv'),
               ('access-admin', 'writePriv'),
               ('admin', 'writePriv'),
               ('fabric-admin', 'writePriv'),
               ('nw-svc-admin', 'writePriv'),
               ('ops', 'writePriv'),
               ('read-all', 'writePriv'),
               ('tenant-admin', 'writePriv'),
               ('tenant-ext-admin', 'writePriv'),
               ('vmm-admin', 'writePriv'),
           ],
}

uni = PolUni('') # '' is the Dn string for topRoot
aaaUserEp = AaaUserEp(uni)
aaaUser = AaaUser(aaaUserEp, 'userabc', firstName='Adam',
                  email='userabc@cisco.com')

aaaUser.lastName = 'BC'
aaaUser.phone = '555-111-2222'
aaaUserCert = AaaUserCert(aaaUser, 'userabc.crt')
aaaUserCert.data = readFile("/tmp/userabc.crt")
# Now add each aaaUserRole to the aaaUserDomains which are added to the
# aaaUserCert
for domain,roles in userRoles.items():
   aaaUserDomain = AaaUserDomain(aaaUser, domain)
   for roleName, privType in roles:
       aaaUserRole = AaaUserRole(aaaUserDomain, roleName,
                                 privType=privType)
print toJSONStr(aaaUser, prettyPrint=True)

cr = ConfigRequest()
cr.addMo(aaaUser)
modir.commit(cr)
# End of Script to create a user
```

秘密キーを使用した署名の計算

始める前に

次の情報が用意されている必要があります。

- HTTP メソッド：GET、POST、DELETE
- 要求される REST API URI（クエリ オプションを含む）
- POST 要求の場合、APIC に送信される実際のペイロード
- ユーザの X.509 証明書の生成に使用される秘密キー
- APIC のユーザ X.509 証明書の宛先名

手順

ステップ 1 HTTP メソッド、REST API URI、およびペイロードをこの順序で連結し、ファイルに保存します。

OpenSSL で署名を計算するには、この連結データをファイルに保存する必要があります。この例では、ファイル名 payload.txt を使用します。秘密キーは userabc.key というファイルにあることに注意してください。

例：

GET の例：

```
GET http://10.10.10.1/api/class/fvTenant.json?rsp-subtree=children
```

POST の例：

```
POST http://10.10.10.1/api/mo/tn-test.json{"fvTenant": {"attributes": {"status": "deleted",
 "name": "test"}}}
```

ステップ 2 payload.txt ファイルに正しい情報が含まれていることを確認します。

たとえば、前の手順で示したような取得例を使用します。

```
GET http://10.10.10.1/api/class/fvTenant.json?rsp-subtree=children
```

payload.txt ファイルには、次の情報のみ含める必要があります。

```
GET/api/class/fvTenant.json?rsp-subtree=children
```

ステップ 3 payload ファイルを作成するときに新しい行を間違って作成していないことを確認します。

例：

```
# cat –e payload.txt
```

次と同じように出力の最後に **$** 記号があるか確認します。

```
GET/api/class/fvTenant.json?rsp=subtree=children$
```

ある場合、Payload.ファイルを作成したときに新しい行が作成されたことを意味します。payload ファイルの生成時に新しい行が作成されることを防ぐには、次のようなコマンドを使用します。

```
echo -n "GET/api/class/fvTenant.json?rsp-subtree=children" >payload.txt
```

ステップ 4 OpenSSL を使用して、秘密キーとペイロード ファイルを使用して署名を計算します。

例：

```
openssl dgst -sha256 -sign userabc.key payload.txt > payload_sig.bin
```

生成されたファイルには、複数行に印字された署名があります。

ステップ 5 base64 形式に署名を変換します。

例：

```
openssl base64 -A -in payload_sig.bin -out payload_sig.base64
```

ステップ 6 Bash を使用して、署名から改行文字を取り除きます。

例：

```
$ tr -d '\n' < payload_sig.base64
P+OTqK0CeAZjl7+Gute2R1Ww8OGgtzE0wsLlx8fIXXl4V79Zl7
Ou8IdJH9CB4W6CEvdICXqkv3KaQszCIC0+Bn07o3qF//BsIplZmYChD6gCX3f7q
IcjGX+R6HAqGeK7k97cNhXlWEoobFPe/oajtPjOu3tdOjhf/9ujG6Jv6Ro=
```

（注） これは、この特定の要求に関して APIC に送信される署名です。その他の要求では、独自の署名を計算する必要があります。

ステップ 7 署名を文字列内に配置し、APIC が署名をペイロードと照合して確認できるようにします。

この完全な署名が、要求のヘッダー内のクッキーとして APIC に送信されます。

例：

```
APIC-Request-Signature=P+OTqK0CeAZjl7+Gute2R1Ww8OGgtzE0wsLlx8f
IXXl4V79Zl7Ou8IdJH9CB4W6CEvdICXqkv3KaQszCIC0+Bn07o3qF//BsIplZmYChD6gCX3f
7qIcjGX+R6HAqGeK7k97cNhXlWEoobFPe/oajtPjOu3tdOjhf/9ujG6Jv6Ro=;
APIC-Certificate-Algorithm=v1.0; APIC-Certificate-Fingerprint=fingerprint;
APIC-Certificate-DN=uni/userext/user-userabc/usercert-userabc.crt
```

（注） ここで使用される DN が、次のステップの x509 証明書を含むユーザ認定オブジェクトの DN に一致する必要があります。

ステップ 8 署名を使用して APIC と通信するには、Python SDK の CertSession クラスを使用します。

次のスクリプトは、ACI Python SDK の CertSession クラスを使用して、署名を使用して APIC に要求する方法の例です。

例：

```
#!/usr/bin/env python
# It is assumed the user has the X.509 certificate already added to
# their local user configuration on the APIC
from cobra.mit.session import CertSession
from cobra.mit.access import MoDirectory

def readFile(fileName=None, mode="r"):
```

```
    if fileName is None:
        return ""
    fileData = ""
    with open(fileName, mode) as aFile:
        fileData = aFile.read()
    return fileData

pkey = readFile("/tmp/userabc.key")
csession = CertSession("https://ApicIPOrHostname/",
                       "uni/userext/user-userabc/usercert-userabc", pkey)

modir = MoDirectory(csession)
resp = modir.lookupByDn('uni/fabric')
pring resp.dn
# End of script
```

（注） 前のステップで使用した DN が、このステップの x509 証明書を含むユーザ認定オブジェクトの DN に一致する必要があります。

アカウンティング

ACI ファブリック アカウンティングは、障害およびイベントと同じメカニズムで処理される以下の 2 つの管理対象オブジェクト（MO）によって処理されます。

- `aaaSessionLR` MO は、APIC およびスイッチでのユーザ アカウントのログイン/ログアウト セッション、およびトークン更新を追跡します。ACI ファブリック セッション アラート機能は、次のような情報を保存します。
  - ユーザ名
  - セッションを開始した IP アドレス
  - タイプ（telnet、https、REST など）
  - セッションの時間と長さ
  - トークン更新：ユーザ アカウントのログイン イベントは、ユーザ アカウントが ACI ファブリックの権利を行使するために必要な、有効なアクティブ トークンを生成します。

（注） トークンはログインに関係なく期限切れになります。ユーザはログアウトできますが、トークンは含まれているタイマー値の期間に従って期限切れになります。

- `aaaModLR` MO は、ユーザがオブジェクトに対して行う変更、およびいつ変更が発生したかを追跡します。

- AAA サーバが ping 可能でない場合は、使用不可としてマークされ、エラーが表示されます。

aaaSessionLR と aaaModLR の両方のイベント ログが、APIC シャードに保存されます。データがプリセットされているストレージ割り当てサイズを超えると、先入れ先出し方式でレコードを上書きします。

（注） APIC クラスタ ノードを破壊するディスク クラッシュや出火などの破壊的なイベントが発生した場合、イベント ログは失われ、イベント ログはクラスタ全体で複製されません。

aaaModLR MO と aaaSessionLR MO は、クラスまたは識別名（DN）でクエリできます。クラスのクエリは、ファブリック全体のすべてのログ レコードを提供します。ファブリック全体の aaaModLR レコードはすべて、GUI の **[Fabric]** > **[Inventory]** > **[POD]** > **[History]** > **[Audit Log]** セクションから入手できます。APIC GUI の **[History]** > **[Audit Log]** オプションを使用すると、GUI に示された特定のオブジェクトのイベント ログを表示できます。

標準の syslog、callhome、REST クエリ、および CLI エクスポート メカニズムは、aaaModLR MO と aaaSessionLR MO のクエリ データで完全にサポートされます。このデータをエクスポートするデフォルト ポリシーはありません。

APIC には、一連のオブジェクトまたはシステム全体のデータの集約を報告する、事前設定されたクエリはありません。ファブリック管理者は、aaaModLR および aaaSessionLR のクエリ データを定期的に syslog サーバにエクスポートするエクスポート ポリシーを設定できます。エクスポートされたデータを定期的にアーカイブし、システムの一部またはシステム ログ全体のカスタム レポートを生成するために使用できます。

共有サービスとしての外部ネットワークへのルーテッド接続の課金と統計情報

Cisco Application Policy Infrastructure Controller（APIC）は、共有サービスとして外部ネットワークへのルーテッド接続用に設定されたポートからバイト カウントおよびパケット カウント課金統計情報を収集するように設定できます。外部ネットワークは、Cisco Application Centric Infrastructure（ACI）内の外部 L3Out エンドポイント グループ（l3extInstP 管理対象オブジェクト）として表されます。任意のテナントの任意の EPG は、外部ネットワークへのルーテッド接続のために外部 L3Out EPG を共有できます。課金統計情報は、共有サービスとして外部 L3Out EPG を使用するテナントの各 EPG について収集できます。外部 L3Out EPG がプロビジョニングされているリーフスイッチは、課金統計情報を集約先である Cisco APIC に転送します。アカウンティング ポリシーは、これらの課金統計情報を定期的にサーバにエクスポートするように設定できます。

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。