TACACs +、RADIUS、LDAP、RSA、SAML

この章の内容は、次のとおりです。

概要

この記事は、RADIUS、TACACS＋、LDAP ユーザーが APIC にアクセスできるようにする手順を説明します。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。

（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。

RADIUS

RADIUS サーバでユーザを設定するには、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 …"
```

TACACS+ 認証

Terminal Access Controller Access Control device Plus（TACACS+）は、シスコ デバイスでサポートされる別のリモート 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、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による確実な転送が可能になります。
- スイッチと AAA サーバ間でプロトコル ペイロード全体を暗号化して、高度なデータ機密性を実現します。RADIUS はパスワードのみを暗号化します。
- 構文と設定が RADIUS と異なる av-pairs を使用しますが、APIC は `shell:domains` をサポートします。

（注） 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。

次に示す XML の例では、IP アドレス 10.193.208.9 の TACACS+ プロバイダーを ACI ファブリックに使用させるよう設定が行われています。

（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。

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

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)
```

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、または TACACS+ 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。

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"
          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。

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。

手順

ステップ 1 APIC で、RSA プロバイダを作成します。

a) メニュー バーで、**[Admin]** > **[AAA]** の順に選択します。
b) [Navigation] ペインで、**[RSA Managment]** > **[RSA Providers]** の順に選択します。
c) [Work] ペインで、**[Actions]** > **[Create RSA Provider]** の順に選択します。
d) RSA ホスト名（または IP アドレス）、ポート、プロトコル、および管理エンドポイント グループを指定します。

ステップ 2 RSA プロバイダー グループを作成します。

a) [Navigation] ペインで、**[RSA Managment]** > **[RSA ProviderGroups]** の順に選択します。
b) [Work] ペインで、**[Actions]** > **[Create RSA Provider Group]** を選択します。
c) 必要に応じて、RSA プロバイダ グループ名、説明、およびプロバイダを指定します。

ステップ 3 RSA のログイン ドメインを作成します。

a) [Navigation] ペインで、**[AAA Authentication]** > **[Login Domains]** の順に選択します。
b) [Work] ペインで、**[Actions]** > **[Create Login Domain]** の順に選択します。
c) 必要に応じて、ログイン ドメイン名、説明、レルム、およびプロバイダー グループを指定します。

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。

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 l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。

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：writeRole のみを持つ単一のログイン ドメインを含む Cisco AV ペア

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

- 例 2：readRole のみを持つ単一のログイン ドメインを含む Cisco AV ペア

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

（注） 文字「/」はログイン ドメインごとに writeRole と readRole の間を区切る記号で、使用するロールの種類が 1 つのみである場合も必要です。

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。

a) メニュー バーで、**[Admin]** > **[AAA]** の順に選択します。
b) [Navigation] ペインで、**[TACACS+ Managment]** > **[TACACS+ Providers]** の順に選択します。
c) [Work] ペインで、**[Actions]** > **[Create TACACS+ Provider]** の順に選択します。
d) TACACS+ ホスト名（または IP アドレス）、ポート、認証プロトコル、キー、および管理エンドポイント グループを指定します。

（注） APIC がインバンド管理に接続するために設定されている場合、アウトオブバンド管理は認証に機能しません。APIC リリース 2.1(1x) では、APIC サーバとその他の外部管理デバイス間のデフォルト管理接続として、インバンドおよびアウトオブ バンド間のグローバル トグルを設定できます。

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：

- リリース 2.2(1x) 以前、**[ナビゲーション]** ペインでは、**[ファブリック]** > **[ファブリック ポリシー]** > **[グローバル ポリシー]** > **[接続設定]** を選択します。**[作業ペイン]** で **[インバンド]** または **[アウトバウンド]** のどちらかを選択します。
- リリース 2.2(x) および 2.3(x): では、**[ナビゲーション]** ペインで、**[ファブリック]** > **[ファブリック ポリシー]** > **[グローバル ポリシー]** > **[APIC 接続設定]** を選択します。**[作業ペイン]** で **[インバンド]** または **[アウトバウンド]** のどちらかを選択します。
- リリース 3.0(1x) 以降、**[ナビゲーション]** ペインで、**[システム]** > **[システム設定]** > **[APIC 接続設定]** を選択します。**[作業ペイン]** で **[インバンド]** または **[アウトバウンド]** のどちらかを選択します。

ステップ 2 [TACACS+ Provider Group] を作成します。

a) [Navigation] ペインで、**[TACACS+ Managment]** > **[TACACS+ Provider Groups]** の順に選択します。
b) [Work] ペインで、**[Actions]** > **[Create TACACS+ Provider Group]** の順に選択します。
c) 必要に応じて、TACACS+ プロバイダー グループ名、説明、およびプロバイダーを指定します。

ステップ 3 TACACS+ の [Login Domain] を作成します。

a) [Navigation] ペインで、**[AAA Authentication]** > **[Login Domains]** の順に選択します。
b) [Work] ペインで、**[Actions]** > **[Create Login Domain]** の順に選択します。
c) 必要に応じて、ログイン ドメイン名、説明、レルム、およびプロバイダー グループを指定します。

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。

a) メニュー バーで、**[Admin]** > **[AAA]** の順に選択します。
b) [Navigation] ペインで、[Authentication] をクリックし、[RADIUS] タブをクリックします。
c) [Work] ペインで、**[Actions]** > **[Create RADIUS Provider]** の順に選択します。
d) RADIUS ホスト名 (または IP アドレス) 、ポート、プロトコル、および管理エンドポイント グループを指定します。

（注） APIC がインバンド管理接続用に設定されている場合、アウトバンド管理は認証のために機能しません。APIC リリース 2.1(1x) では、APIC サーバとその他の外部管理デバイス間のデフォルト管理接続として、インバンドおよびアウトオブバンド間のグローバル トグルを設定できます。

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：

- リリース 2.2(1x) 以前、**[ナビゲーション]** ペインでは、**[ファブリック]** > **[ファブリック ポリシー]** > **[グローバル ポリシー]** > **[接続設定]** を選択します。**[作業ペイン]** で **[インバンド]** または **[アウトバウンド]** のどちらかを選択します。
- リリース 2.2(x) および 2.3(x): では、**[ナビゲーション]** ペインで、**[ファブリック]** > **[ファブリック ポリシー]** > **[グローバル ポリシー]** > **[APIC 接続設定]** を選択します。**[作業ペイン]** で **[インバンド]** または **[アウトバウンド]** のどちらかを選択します。
- リリース 3.0(1x) 以降、**[ナビゲーション]** ペインで、**[システム]** > **[システム設定]** > **[APIC 接続設定]** を選択します。**[作業ペイン]** で **[インバンド]** または **[アウトバウンド]** のどちらかを選択します。

ステップ 2 RADIUS のログイン ドメインを作成します。

a) [Navigation] ペインで、**[AAA Authentication]** > **[Login Domains]** の順に選択します。
b) [Work] ペインで、**[Actions]** > **[Create Login Domain]** の順に選択します。

c) 必要に応じて、ログイン ドメイン名、説明、レルム、およびプロバイダー グループを指定します。

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) 。
- Cisco APIC がインストールされ、オンラインになっていること。Cisco 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 Cisco 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) クライアント名と Cisco 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） [Shared Secret] は Cisco APIC **[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。

   たとえば、*cisco-av-pair* 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に付与するロール、「`common`」はCisco Application Centric Infrastructure (Cisco ACI) テナント common、「`read-all(16001)`」は Cisco ACI テナント common 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

新しく作成された RADIUS および TACACS+ のユーザを使用して、Cisco APIC にログインします。割り当てられた RBAC ロールと権限に従って正しい Cisco 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 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 2008 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 2008 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 2008 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 2008 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 2008 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。

a) メニュー バーで、**[Admin]** > **[AAA]** の順に選択します。
b) [Navigation] ペインで、[Authentication] を選択し、[Work] ペインで [LDAP] タブをクリックします。
c) [Work] ペインで、**[Actions]** > **[Create LDAP Provider]** の順に選択します。
d) LDAP ホスト名（または IP アドレス）、ポート、バインド DN、ベース DN、パスワード、属性、および管理エンドポイント グループを指定します。

（注）
- バインド DN は、APIC が LDAP サーバにログインするために使用する文字列です。APIC は、ログインしようとするリモート ユーザの検証にこのアカウントを使用します。ベース DN は、APIC がリモート ユーザ アカウントを検索する LDAP サーバのコンテナ名とパスです。これはパスワードが検証される場所です。フィルタを使用して、APIC が *cisco-av-pair* に使用するために要求している属性を見つけます。これには、APIC で使用するユーザ認証と割り当て済み RBAC ロールが含まれます。APIC は、この属性を LDAP サーバから要求します。
- **[属性]** フィールド：次のうちいずれかを入力します。
  - LDAPサーバの設定では、Cisco AVPair、入力 **`CiscoAVPair`** 。
  - LDAP グループ マップ LDAPサーバ設定、入力 **`memberOf`** 。
- APICがインバンド管理接続用に設定されている場合、LDAPアクセス用にアウトオブバンド管理エンドポイントグループを選択しても有効にはなりません。また、インバンド管理エンドポイントグループ上のアウトオブバンドでLDAPサーバに接続することはできますが、LDAPサーバのスタティックルートの設定が必要です。本書の設定手順例では、APIC インバンド管理エンドポイント グループを使用します。

ステップ 2 APIC で、LDAP のログイン ドメインを設定します。

a) [Navigation] ペインで、**[Authentication]** > **[Login Domains]** を選択します。
b) **[Work]** ペインで、**[Actions]** > **[Create Login Domain]** の順に選択します。
c) 必要に応じて、ログイン ドメイン名、説明、レルム、およびプロバイダー グループを指定します。

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。

手順

ステップ 1 Cisco APIC GUI のメニュー バーで、**[Admin]** > **[AAA]** を選択します。

ステップ 2 [Navigation] ペインで、 [LDAP Managment] を展開し、[LDAP Group Map Rules] を右クリックして、 [Create LDAP Group Map Rule] をクリックします。[Create LDAP Group Map Rule: Security] ダイアログが表示されます。

ステップ 3 該当するフィールドにマップ ルールの名前、説明 (オプション)、グループの DN、およびセキュリティ ドメインを指定し、[Next] をクリックします。セキュリティ ドメイン オプションが表示された [Create LDAP Group Map Rule: Roles] ダイアログが表示されます。

ステップ 4 [+] をクリックして、[Role Name] および [Role Privilege Type] フィールドにアクセスします。

ステップ 5 [Role Name] ドロップダウン矢印をクリックして、ロール名を選択します。

ステップ 6 [Role Privilege Type] ドロップダウン矢印をクリックして、ロール権限のタイプを選択します ([Read] または [Write])。

ステップ 4 ～ 6 を繰り返して、LDAP グループ マップに他のロールを追加します。

ステップ 7 完了したら、[Finished] 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

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。
- LDAP グループ マップ ルールが設定されています。

手順

ステップ 1 Cisco APIC GUI のメニュー バーで、**[Admin]** > **[AAA]** を選択します。

ステップ 2 [Navigation] ペインで、 [LDAP Managment] を展開し、[LDAP Group Maps] を右クリックして、[Create LDAP Group Map] をクリックします。[Create LDAP Group Map] ダイアログが表示されます。

ステップ 3 マップの名前と説明（オプション）を指定します。

ステップ 4 [Rules] フィールドで、[+] をクリックしてから、 [Name] ドロップダウン矢印をクリックして、指定した LDAP グループ マップ ルールを選択し、[Update] をクリックします。

ステップ 4 を繰り返して、LDAP グループ マップに他のルールを追加します。

ステップ 5 完了したら、[送信（Submit）] をクリックします。

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

手順

ステップ 1 メニュー バーで、**[ADMIN]** > **[AAA]** の順にクリックします。

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

ステップ 3 [Work] ペインの [Remote Users] 領域で、[Remote user login policy] ドロップダウン リストから [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。

手順

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
```

SAML について

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、次のような利点が得られます。

- 別のユーザ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されます。
- 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。

手順

ステップ 1 APIC で、**SAML プロバイダー**を作成します。

a) メニュー バーで、**[Admin]** > **[AAA]** の順に選択します。
b) [Navigation] ペインで、**[SAML Management]** > **[SAML Providers]** を選択します。
c) [Work] ペインで、**[Actions]** > **[Create SAML Provider]** を選択します。
d) SAML ホスト名 (または IP アドレス) と IdP メタデータ URL を指定します。

- AD FS の場合、IdP メタデータ URL は *https://<ADFS の FQDN>/FederationMetadata/2007-06/FederationMetadata.xml* という形式になります。
- Okta の場合、IdP メタデータの URL を取得するには、Okta サーバから該当 SAML アプリケーションの [Sign On] セクションに、**アイデンティティ プロバイダー メタデータ**のリンクをコピーします。

e) SAML ベースのサービスの**エンティティ ID** を指定します。
f) IdP メタデータの URL にアクセスする必要がある場合は、Https プロキシを設定します。
g) IdP はプライベート CA によって署名された場合は、認証局を選択します。
h) ドロップダウン リストから、ユーザの要求の署名アルゴリズムの認証タイプを選択します。

ステップ 2 **SAML プロバイダー グループ**を作成します。

a) [Navigation] ペインで、**[SAML Management]** > **[SAML Providers Groups]** を選択します。
b) [Work] ペインで、**[Actions]** > **[Create SAML Provider Group]** を選択します。
c) 必要に応じて、SAML プロバイダー グループ名、説明、およびプロバイダーを指定します。

ステップ 3 SAML の**ログイン ドメイン**を作成します。

a) **[Navigation]** ペインで、**[AAA Authentication]** > **[Login Domains]** の順に選択します。
b) **[Work]** ペインで、**[Actions]** > **[Create Login Domain]** の順に選択します。
c) 必要に応じて、ログイン ドメイン名、説明、レルム、およびプロバイダー グループを指定します。

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/

手順

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（6 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 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 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。

手順

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** 。