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。

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。

アカウンティング

Cisco Application Centric Infrastructure（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によって処理されます。

- `aaaSessionLR` 管理対象オブジェクトは、Cisco Application Policy Infrastructure Controller（APIC）APIC およびスイッチでのユーザー 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。Cisco 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）

（注） 5.3(1) リリース以降、telnet はサポートされていません。

  - セッションの時間と長さ
  - トークン更新：ユーザー アカウントのログイン イベントは、ユーザー アカウントが Cisco 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 管理対象オブジェクト は、ユーザー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、Cisco 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、古いものから順にレコードが上書きされます。

（注） Cisco 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 管理対象オブジェクトは、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 **[ファブリック（Fabric）] > [インベントリ（Inventory）] > [POD] > [履歴（History）] > [監査ログ（Audit Log）]** セクションから入手できます。Cisco APIC GUI の **[履歴（History）] > [監査ログ（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 と aaaSessionLR 管理対象オブジェクトのクエリ 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。

Cisco 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。

カスタム RBAC 規則

RBAC 規則により、ファブリック全体の管理者は、本来はブロックされるはずのセキュリティドメイン間アクセスを許可することができます。RBAC 規則を使用して、別のセキュリティドメインにあるため他の方法ではアクセス不可能なサービスを共有したり物理リソースを公開したりできます。RBAC 規則では、ターゲット リソースへの読み取りアクセスのみ許可されます。GUI RBAC 規則ページは、[管理（Admin）] > [AAA] > [セキュリティ管理（Security Management）] の下にあります。RBAC 規則は、リソースが存在する前に作成できます。RBAC 規則、ロール、および権限（およびそれらの依存関係）の説明は、管理情報モデルのリファレンスに記載されています。

設定されているポリシーの表示に使用されます（ポリシーのトラブルシューティングなど）。

ops 規則は、新しいモニタリングポリシーおよびトラブルシューティング ポリシーの作成には使用できません。これらは、APIC の他のすべての構成と同様に、admin 権限を使用して行う必要があります。

複数のセキュリティ ドメイン間で物理リソースを選択的に公開する

ファブリック全体の管理者は、RBAC 規則を使用して、異なるセキュリティドメインにあるため他の方法ではアクセス不可能なユーザに対し、物理リソースを選択的に公開します。

たとえば、ソーラーというテナントのユーザが仮想マシン管理（VMM）ドメインへのアクセスを必要とする場合、ファブリック全体の管理者によって、これを許可する RBAC 規則を作成することができます。RBAC 規則は、次の 2 つの部分から構成されます。アクセス対象オブジェクトを検索する識別名（DN）と、オブジェクトにアクセスするユーザを含むセキュリティドメインの名前です。したがって、この例では、ソーラーというセキュリティドメイン内の指定ユーザがログインすると、このルールにより、VMM ドメインおよびツリーの内の子オブジェクトすべてへのアクセスが許可されます。VMM ドメインへのアクセスを複数のセキュリティドメイン内のユーザに許可するには、ファブリック全体の管理者は、セキュリティドメインそれぞれについて、VMM ドメインの DN とセキュリティ ドメインを含む RBAC 規則を作成します。

（注） 管理情報ツリー内の異なる部分に存在するユーザに対し、RBAC規則によりオブジェクトを公開することは可能ですが、CLIの使用によってツリーの構造を横断することでそのようなオブジェクトに移動することはできません。ただし、RBAC規則に含まれるオブジェクトのDNをユーザが把握していれば、ユーザはMO検索コマンドにより、CLIを使用してそれを見つけることができます。

複数のセキュリティ ドメイン間でのサービス共有を有効にする

ファブリック全体の管理者は、RBAC規則を使用して、テナント間の共有サービスを可能にするトランステナントEPG通信をプロビジョニングします。

APIC ローカル ユーザ

管理者は、外部 AAA サーバを使用せずに、Cisco Application Policy Infrastructure Controller（APIC）自体でユーザを構成することを選択できます。これらのユーザは、APIC ローカル ユーザと呼ばれます。

ユーザがパスワードを設定する時点で、Cisco 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。
- Cisco Application Centric Infrastructure （ACI）では、最大 100 名までの管理者ユーザがサポートされています。

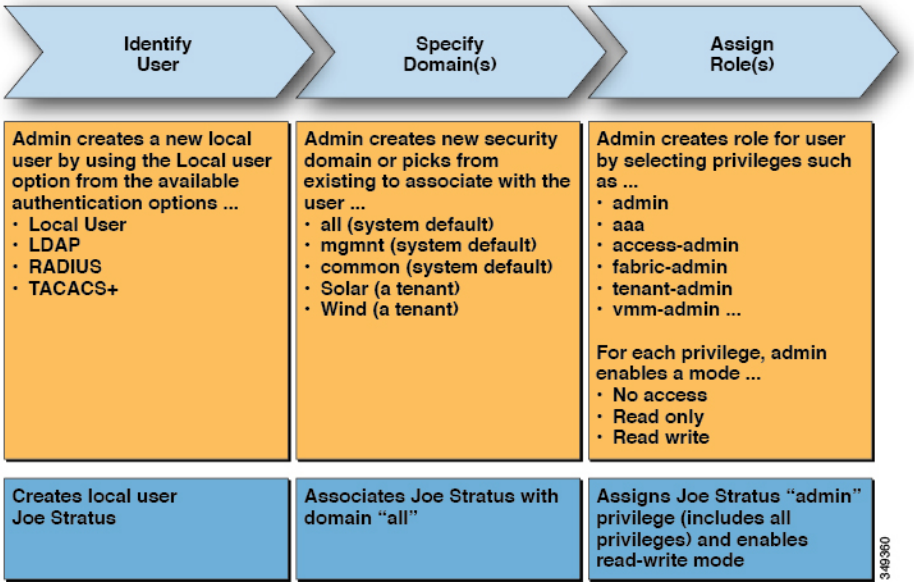
（注） 6.0(2) リリース以降、 Cisco APIC ベース OS が更新され、簡単に推測できるパスワードを検出するためのディクショナリが追加されました。その結果、以前のリリースで強力と見なされたパスワードのうち、現在では強力とは見なされなくなったものがあります。

Cisco ACI では、パスワードの保存に SHA256 一方向ハッシュを使用した暗号化ライブラリが使用されます。保管中のハッシュされたパスワードは、暗号化されたファイルシステムに保存されます。暗号化されたファイルシステムのキーは、Trusted Platform Module（TPM）を使用して保護されます。

また Cisco APIC により、管理者は、外部で管理されている認証 Lightweight Directory Access Protocol（LDAP）、RADIUS、TACACS+、または SAML サーバで設定されたユーザにアクセス権を付与できます。ユーザは、異なる認証システムに属し、Cisco APIC に同時にログインできます。

次の図は、Cisco ACI ファブリック全体へのフル アクセス権があるローカル Cisco APIC 認証データベース内の管理ユーザーを設定するプロセスがどのように動作するかを示しています。

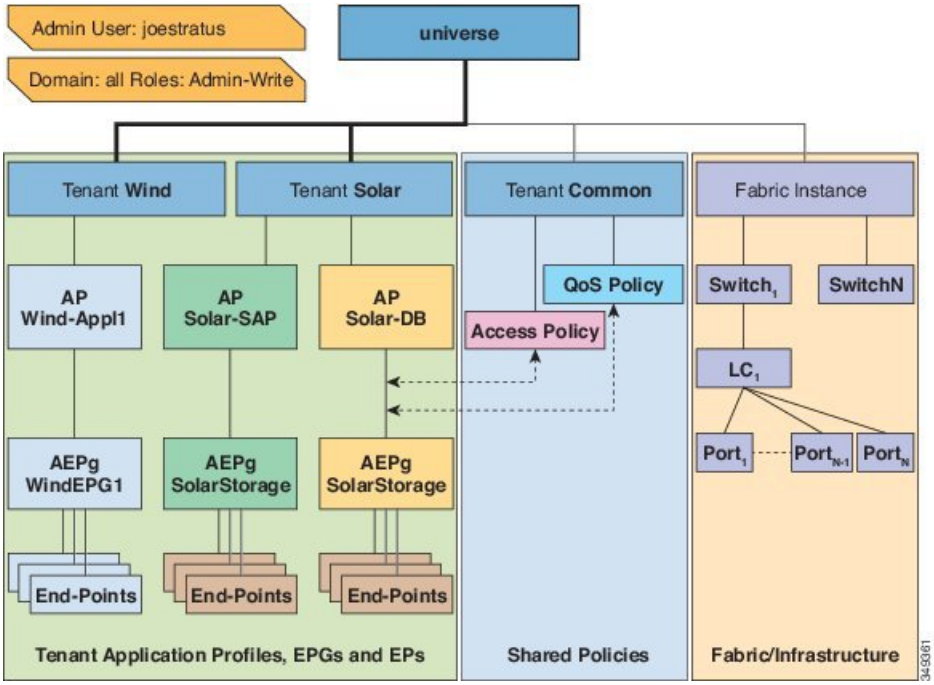
図 *1 : APIC* ローカル ユーザーの構成プロセス



（注） セキュリティ ドメイン「all」は、管理情報ツリー（MIT）全体を表します。このドメインには、システム内のすべてのポリシーと Cisco APIC よって管理されるすべてのノードが含まれます。テナント ドメインには、テナントのすべてのユーザおよび管理対象オブジェクトが含まれます。テナント管理者には、「all」ドメインへのアクセス権を付与しないでください。

次の図は、管理ユーザ Joe Stratus が持つシステムへのアクセス権を示します。

図 *2:*「*all*」ドメインへ管理ユーザを設定した結果

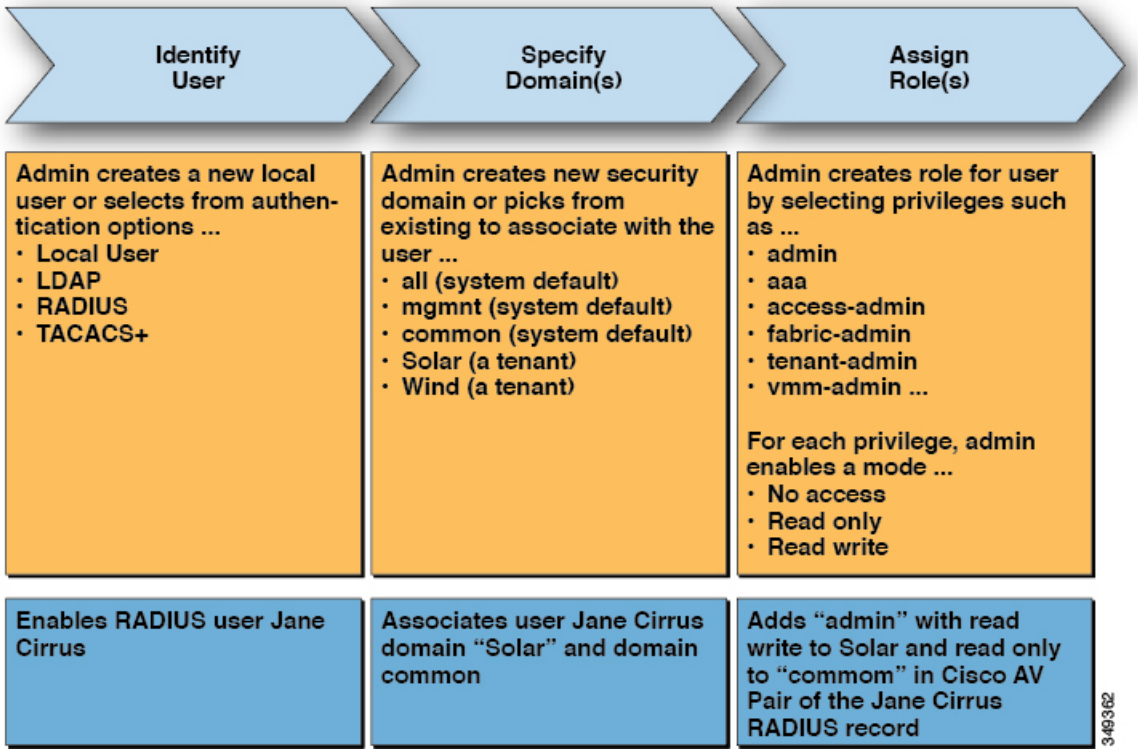


読み取り/書き込み「管理者」権限を持つユーザ Joe Stratus は、ドメイン「all」に割り当てられ、システム全体へのフル アクセス権が与えられます。

外部管理されている認証サーバのユーザ

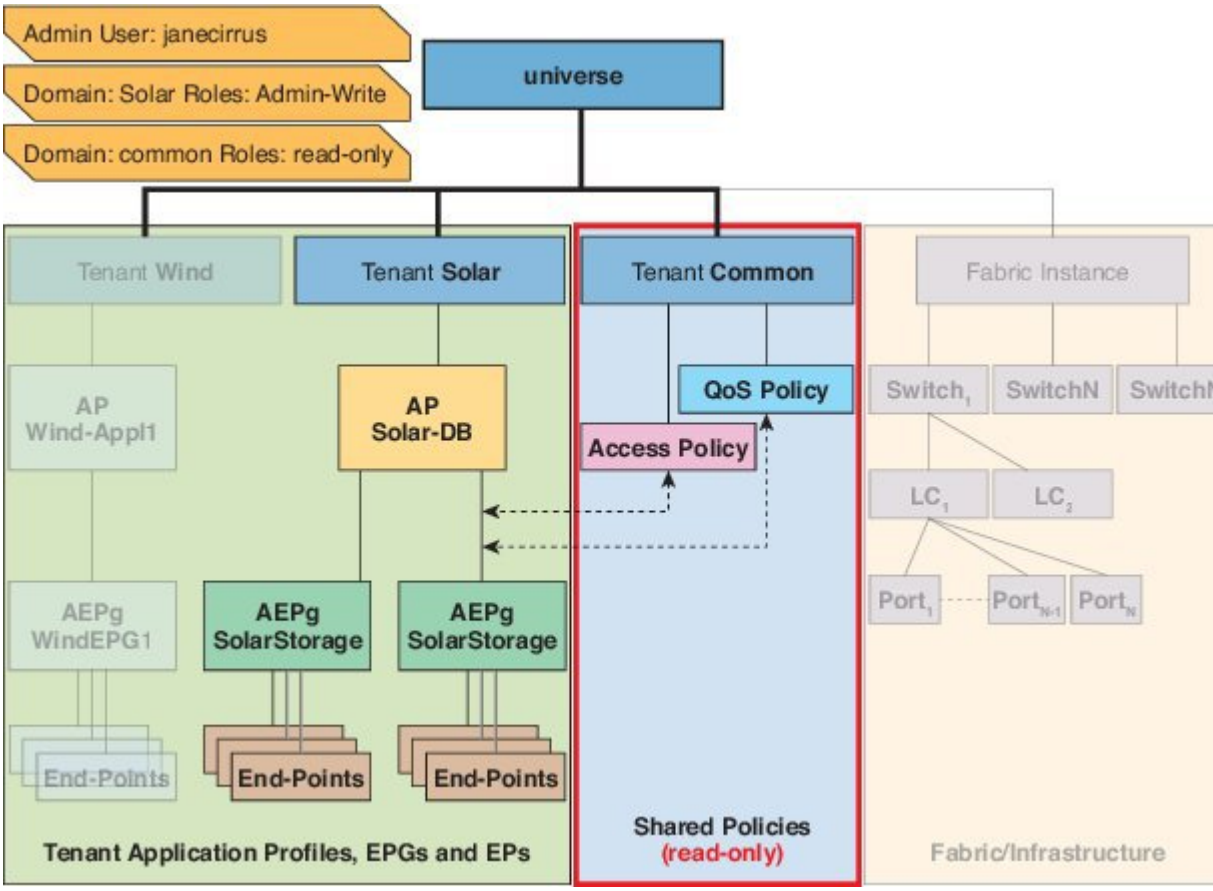
次の図は、テナント Solar へのフル アクセス権がある外部 RADIUS サーバ内の管理ユーザを設定するプロセスがどのように動作するかを示します。

図 *3*: 外部認証サーバでのユーザ設定のプロセス



次の図は、管理ユーザ Jane Cirrus が持つシステムへのアクセス権を示します。

図 *4 :* テナント ***Solar*** へ管理ユーザを設定した結果



この例では、Solar テナントの管理者には、Solar テナントに含まれるすべてのオブジェクトへのフル アクセス権と、テナント Common への読み取り専用アクセス権があります。テナント管理者 Jane Cirrus には、テナント Solar へのフル アクセス権があり、テナント Solar で新しいユーザを作成する機能などがあります。テナント ユーザは、自身が所有し制御する ACI ファブリックの設定パラメータを変更できます。また、エンドポイント、エンドポイント グループ（EPG）およびアプリケーション プロファイルなどの適用されるエンティティ（管理対象オブジェクト）の統計情報の読み取り、障害およびイベントのモニタもできます。

上記の例では、ユーザ Jane Cirrus は外部 RADIUS 認証サーバで設定されました。外部認証サーバで AV ペアを設定するには、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、APIC 上のユーザに対するロールベース アクセス コントロール（RBAC）のロールと権限を指定します。次に RADIUS サーバは、ユーザ権限を APIC コントローラに伝播します。

上記の例のオープン RADIUS サーバ（/etc/raddb/users）の設定は次のとおりです。

```
janecirrus Cleartext-Password := "<password>"
Cisco-avpair = "shell:domains = solar/admin/,common//read-all(16001)"
```

この例には、次の要素が含まれています。

- `janecirrus` はテナント管理者です。

- solar はテナントです。
- admin は書き込み権限があるロールです。
- common は、テナント共通サブツリーで、すべてのユーザがそのサブツリーへの読み取り専用アクセス権を持っています。
- read-all は、読み取り権限があるロールです。

Cisco AV ペアの形式

Cisco APIC は、管理者が外部認証サーバで Cisco AV ペアを設定し、1 個の AV ペアの文字列のみを検索することを要求しています。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。

AV ペア文字列を機能させるため、次の形式にする必要があります。

```
shell:domains =
ACI_Security_Domain_1/ACI_Write_Role_1|ACI_Write_Role_2|ACI_Write_Role_3/ACI_Read_Role_1|ACI_Read_Role_2,
ACI_Security_Domain_2/ACI_Write_Role_1|ACI_Write_Role_2|ACI_Write_Role_3/ACI_Read_Role_1|ACI_Read_Role_2,
ACI_Security_Domain_3/ACI_Write_Role_1|ACI_Write_Role_2|ACI_Write_Role_3/ACI_Read_Role_1|ACI_Read_Role_2
```

- **shell:domains=**：ACI が正常に文字列を読み取るために必要です。シェル文字列を常にプリペンドする必要があります。
- **ACI_Security_Domain_1//admin**：管理者にこのセキュリティ ドメインのテナントへの読み取り専用アクセス権を付与します。
- **ACI_Security_Domain_2/admin**：管理者にこのセキュリティ ドメインのテナントへの書き込みアクセス権を付与します。
- **ACI_Security_Domain_3/read-all**：このセキュリティ ドメインのテナントへの読み取り/書き込みすべてのアクセス権を付与します。

（注） **/** により区別される文字列のセキュリティ ドメイン、書き込み、読み取りセクション同じセキュリティ ドメイン内の **|** により区別される複数の書き込みまたは読み取り権限

（注） Cisco APIC リリース 2.1 より、AV ペアに UNIX ID が指定されていない場合、APIC は UNIX の固有ユーザー ID を内部的に割り当てます。

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=ACI_Security_Domain_1/Write_Role_1|Write_Role_2/
```

- 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=Security_Domain_1//Read_Role_1|Read_Role_2
```

（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。

AV ペア GUI の設定

セキュリティ ドメインは、 **[Admin]** > **[AAA]** > **[Security Management]** > **[Security Domains]** の ACI GUI で定義されており、**[テナント]** > **[Tenant_Name]** > **[ポリシー]** のテナントに割り当てられています。

セキュリティ ドメインには読み取りまたは書き込み権限のいずれかが必須です。これらの権限は、**[APIC]** > **[Admin]** > **[Security Management]** > **[Roles]** で定義されています。権限が書き込みセクションに入力される場合、ACI_Security_Domain_1/admin/admin/admin を使用する必要がないため、自動的に同じレベルの読み取り権限を付与します。

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 …"
```

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。

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。

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、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。

- APIC とスイッチの両方の REST API、GUI、および CLI で *apic#fallback\\username* 文字列を使用します。
- *apic:fallback\\username* 文字列は、REST API と GUI にのみ使用し、CLI インターフェイスには使用しません。

（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。

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。

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。