ユーザ アクセス、認証およびアカウンティング

この章の内容は、次のとおりです。

ユーザ アクセス、認証およびアカウンティング

APIC ポリシーは、Cisco ACI ファブリックのアクセス、認証、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、管理者は非常に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。

マルチテナントのサポート

コア APIC 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。 ACI ファブリック ユーザは、次に関連付けられています。

- ロールのセット
- 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

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。 権限は、システム内の特定の機能に対するアクセスを許可または制限する MO です。 たとえば、ファブリック機器は権限ビットです。 このビットは、物理ファブリックの機器に対応するすべてのオブジェクト上で APIC によって設定されます。

ロールは権限ビットの集合です。 たとえば、「管理者」ロールが「ファブリック機器」と「テナント セキュリティ」に対する権限ビットに設定されていると、「管理者」ロールにはファブリックの機器とテナント セキュリティに対応するすべてのオブジェクトへのアクセス権があります。

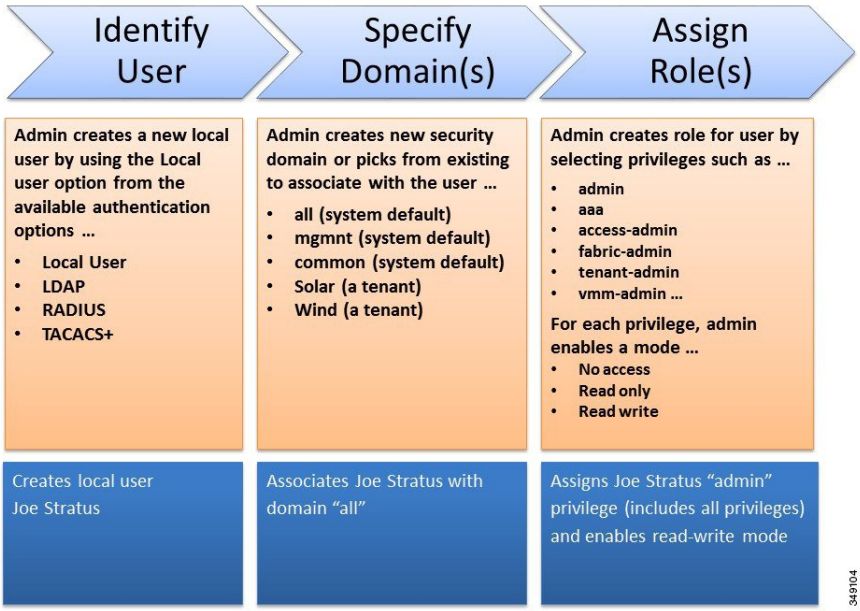
セキュリティ ドメインは、ACI MIT オブジェクト階層の特定のサブツリーに関連付けられたタグです。 たとえば、デフォルトのテナント「common」には、ドメイン タグ「common」があります。同様に、特別なドメイン タグ「all」には、MIT オブジェクト ツリー全体が含まれます。 管理ユーザは、MIT オブジェクト階層にカスタム ドメイン タグを割り当てることができます。 たとえば、「solar」ドメイン タグはテナント solar に割り当てられます。 MIT 内では、特定のオブジェクトだけがセキュリティ ドメインとしてタグ付けできます。たとえば、テナントはセキュリティ ドメインとし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。

APIC ローカル ユーザ

管理者は、外部 AAA サーバを使用しないことを選択し、APIC 自体でユーザを設定することができます。 これらのユーザは、APIC ローカル ユーザと呼ばれます。 また 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、または TACACS+ 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、APIC に同時にログインできます。

次の図は、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 APIC 認証データベース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。

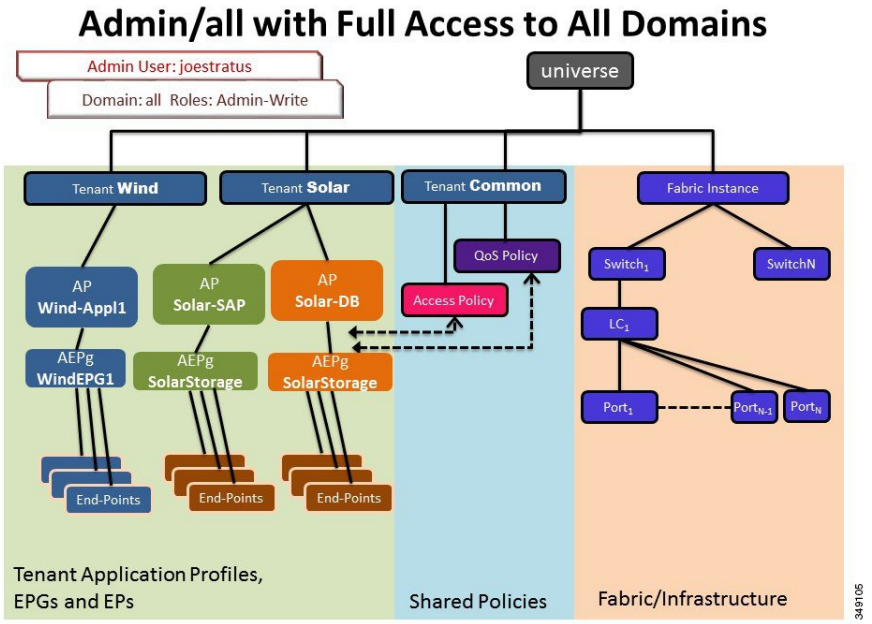
図 *1*：*APIC* ローカル ユーザの設定プロセス



（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 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

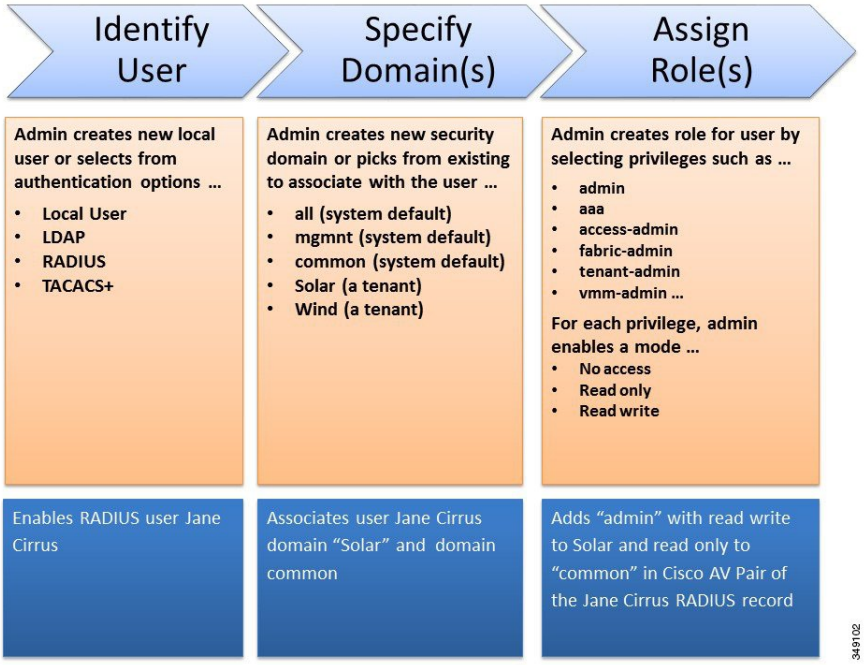


読み取り/書き込み「管理者」権限を持つユーザ Joe Stratus は、ドメイン「all」に割り当てられ、システム全体へのフル アクセス権が与えられます。

外部管理されている認証サーバのユーザ

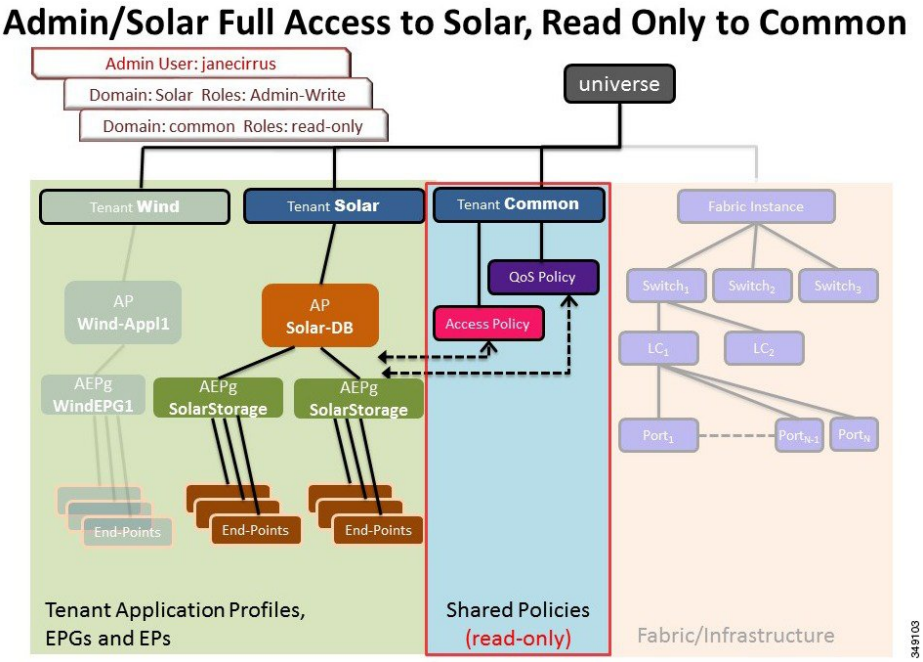
次の図は、テナント Solar へのフル アクセス権がある外部 RADIUS サーバ内の管理ユーザを設定するプロセスがどのように動作するかを示します。

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 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。

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)
```

最初の AV ペアの形式には UNIX ユーザ ID がなく、2 番目のものにはあります。 どちらも正しいです。

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})$
```

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:roles および shell:domains）を設定する必要があります。

ロール オプションが cisco-av-pair 属性で指定されていない場合は、デフォルトのユーザ ロールは network-operator になります。 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。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

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。 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を実行します。
- 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。
- RADIUS とは構文および設定の点で異なる av-pairs を使用しますが、APIC は同一の文字列のリストをサポートします（`shell:roles` および `shell:domains`）。

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。

RADIUS/TACACS+ と LDAP の唯一の相違点は、LDAP グループが APIC 内で `shell:roles` をマッピングするために使用できるという点です。 AAA LDAP クライアントは、ローカル ノードにマップされる LDAP プロバイダーのグループを検索します。 リモート ユーザが検出されると、AAA は、関連付けられた LDAP グループ マップで、その LDAP グループに定義されるユーザ ロールとロケールを割り当てます。 この機能はオプションです。 Active Directory には、再帰トラバーサルと呼ばれる機能があり、ユーザはユーザ グループの先祖をすべて取得し、ロールを適用できます。 この機能は、Active Directory がネストされたグループをサポートしているので可能になります。

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、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。