セキュリティ ドメインとノード ルールを使用したアクセスの制限

ドメイン別にアクセスを制限する

セキュリティドメインを使用すると、ファブリック管理者はリソースを選択的に一群のユーザーに公開し、それらのユーザーにそれらのリソースの読み取りと変更に必要なレベルの権限を提供できます。セキュリティドメインを使用することで、複数グループのユーザーに基盤となるインフラストラクチャを共有させながら、リソースへの管理アクセスを分離することができます。

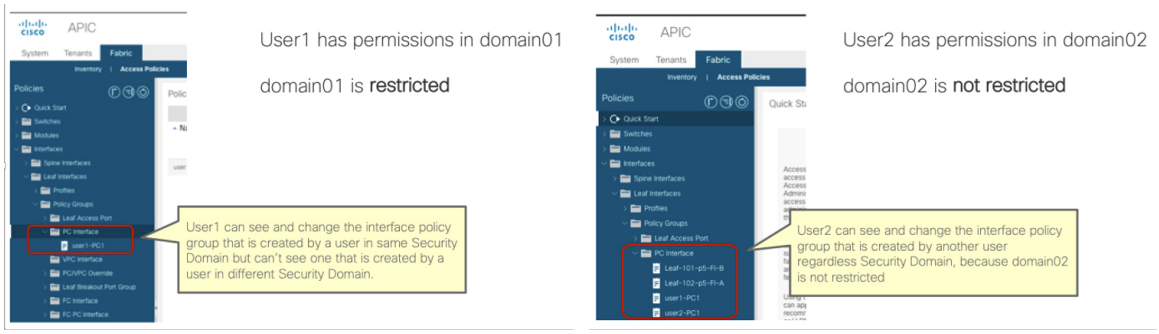
Cisco Application Policy Infrastructure Controller（APIC）リリース5.0(1) 以降では、セキュリティドメインを「制限あり」として構成できます。制限付きセキュリティドメインを使用すると、管理者は、両方のグループのユーザーに同じ特権が割り当てられている場合であっても、別のセキュリティドメインのユーザーグループによって作成されたオブジェクトを表示または変更できないようにすることができます。

たとえば、制限付きセキュリティドメイン `domainA` に関連付けられているユーザーは、セキュリティドメイン `domainB` に関連付けられているユーザーによって構成されたポリシー、プロファイル、またはユーザーを表示できません。`domainB` に関連付けられているユーザーは、`domainB` も制限付きとして構成されていない限り、 `domainA` に関連付けられているユーザーによって構成されたポリシー、プロファイル、またはユーザーを表示できます。ユーザーは、ユーザーが適切な権限を持っているシステムで作成された設定に対して、常に読み取り専用の可視性を持ちます。制限付きセキュリティドメインのユーザーには、そのドメイン内で幅広い

レベルの特権を与えることができます。ユーザーが別のテナントの物理環境に不注意で影響を与える心配はありません。

次の図は、制限付きセキュリティドメインの概念を示しています。

図 *1:* 制限付きセキュリティドメイン



制限付きセキュリティドメインは、アクセスポリシーなど、テナントレベル外のポリシーおよびプロファイルでマルチテナント機能を提供する上で重要な役割を果たします。アクセスポリシーがどのテナントにも属していない場合でも、テナントごとに分離された制限付きセキュリティドメインを使用すれば、各テナントのユーザーは、他のテナントのユーザーには表示されないアクセスポリシーを作成できます。

ノードをドメインに割り当てる

ファブリック管理者は、RBAC ノード ルールを使用して、リーフ スイッチなどの物理ノードをセキュリティ ドメインに割り当てることができます。このノード割り当てにより、そのセキュリティ ドメイン内のユーザーは、ノード ルールの一部として割り当てられたノードにアクセスして操作を実行できます。セキュリティドメイン内のノード管理権限を持つユーザーのみが、そのドメインに割り当てられたノードを設定できます。ユーザーは、セキュリティ ドメインの外部のノードにアクセスできず、他のセキュリティ ドメインのユーザーは、セキュリティ ドメインに割り当てられたノードにアクセスできません。セキュリティ ドメインに割り当てられたノードで構成を作成または変更するには、そのドメインのユーザもドメイン `all` に割り当てられていて、`port-mgmt` ロール（デフォルトで `custom-port-privilege` 権限を含むロール）か、または `custom-port-privilege` 権限を含むカスタム ロールを持っている必要があります。

（注） 割り当てられたノードのポートを管理するローカルユーザを構成するときは、ドメイン `all` のユーザにロールを付与し、ノードが割り当てられているセキュリティ ドメインには `admin` ロールを付与する必要があります。どちらの役割も、**[ロール権限タイプ（Role Privilege Type）]** が `[書き込み（Write）]` として設定されている必要があります。

セキュリティ ドメインおよびノードルールのガイドラインと制限事項

セキュリティドメインとノードルールを構成する際は、次の注意事項と制限事項に従ってください。このセクションで、「制限付きノードユーザー」とは、ノードが割り当てられている制限付きセキュリティ ドメイン内のユーザーのことです。

- Cisco Application Policy Infrastructure Controller（APIC）より前のリリースから 5.0 リリースにアップグレードする場合は、より詳細な以前の権限を使用するルール、ポリシー、ロールを再構成する必要があります。
- Cisco APIC 5.0 リリースからそれより前のリリースにダウングレードする場合は、デフォルトのロールを手動で編集して保持する必要があります。Cisco APIC 5.0 リリースで変更されたロールは保持されます。
- RBAC ノード ルールを使用してスパイン スイッチを割り当てることはできません。
- RBAC ノードルールを作成するときは、ノードを複数のセキュリティドメインに割り当てないでください。
- 制限付きノードユーザーは、ポリシーのみを構成できます。管理者ユーザーは、ノードの構成とトラブルシューティングを実行する必要があります。
- 制限付きノードユーザは、デフォルトのシステム作成の管理対象オブジェクトにアクセスできます。
- 制限付きノードユーザーは、障害ダッシュボードでファブリックレベルの障害数を表示できます。
- 制限付きノードユーザーは、AAA サーバー、NTP サーバー、DNS サーバーなどからのノードレベルの障害を表示できます。
- 管理者または非制限ドメインユーザーが関係ポリシーを制限ノードユーザーによって作成されたアクセス ポリシーに関連付ける場合、そのポリシーは制限ノード ユーザーに表示されます。
- CLI を使用して制限付きノード ユーザを構成することはできません。
- デフォルトでは、`port-mgmt` ロールには、事前定義されたアクセスポリシー管理オブジェクトを含む `custom-port-privilege` 権限があります。カスタム権限を設定する （6 ページ）の手順を使用して、さらに管理対象オブジェクトを追加できます。

セキュリティ ドメインの作成

この手順を使用して、セキュリティ ドメインを作成します。

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（Navigation）]** ペインで、**[セキュリティ（Security）]** をクリックします。

ステップ 3 **[作業（Work）]** ペインで、**[セキュリティ ドメイン（Security Domains）]** タブ > **[アクション（Actions）]** > **[セキュリティ ドメインの作成（Create Security Domain）]** を選択します。

ステップ 4 **[セキュリティ ドメインの作成（Create Security Domain）]**ダイアログボックスで、次の操作を実行します。

a) **[名前（Name）]** フィールドで、セキュリティ ドメインの名前を入力します。

b) [**説明（Description**）] を入力します。

c) セキュリティドメインを **[制限付き RBAC ドメイン（Restricted RBAC Domain）]** として設定するには、**[有効（Enabled）]** チェックボックスをオンにします。

セキュリティドメインを制限付きドメインとして構成した場合、このドメインに割り当てられたユーザーは、他のセキュリティドメインと関連付けられているユーザーが構成したポリシー、プロファイル、ユーザーを表示できません。

d) [保存（Save）] をクリックします。

ノードにアクセス権を割り当てるノードルールを作成する

この手順を使用して、リーフ スイッチなどの物理ノードをセキュリティ ドメインに割り当てる RBAC ノード ルールを設定します。

始める前に

ノードが割り当てられるセキュリティ ドメインを作成します。

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（Navigation）]** ペインで、**[セキュリティ（Security）]** をクリックします。

ステップ 3 **[作業（Work）]** ペインで、**[RBAC ルール（RBAC Rules）]** タブ > **[ノード ルール（Node Rules）]** サブタブ > **[アクション（Actions）]** > **[RBAC ノード ルールの作成（Create RBAC Node Rule）]** を選択します。

画面が表示されます。

ステップ 4 表示される **[ノードの RBAC ルールの作成（Create RBAC Rule for Node）]** 画面で、次の詳細を入力します。

a) [**ノード ID の選択（Select Node ID**）] をクリックして、ドロップダウンリストからノードを選択します。

b) **[ポートの RBAC ルール（RBAC Rule for Port ）]** を割り当てるには、**[ポートの RBAC ルールの追加（Add RBAC Rule for Port）]** をクリックして名前を入力し、**[ドメインの選択（Select Domain）]** をクリックしてドメインをルールに関連付けます。ドメインを選択したら、チェックマークをクリックします。

[ポートの RBAC ルールの追加（Add RBAC Rule for Port）] をクリックして、選択したポートに複数の RBAC ルールを割り当てることができます。

c) **[保存（Save）]** をクリックします。

次のタスク

セキュリティドメインに割り当てられたノードを管理するユーザーを割り当てます。

カスタムの役割と権限

カスタム権限を持つカスタム ロールの作成

この手順を使用して、ロールを作成し、一連の権限を選択します。

始める前に

カスタム ロールで使用できる権限を判断するには、AAA RBAC の役割および権限 にリストされている事前定義されたロールと権限のセットを参照してください。事前定義された特権で公開されていない管理対象オブジェクト（MO）への読み取りまたは書き込みアクセスが必要な場合は、カスタム権限を設定する （6 ページ） で説明されているように、カスタム権限を設定できます。

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（Navigation）]** ペインで、**[セキュリティ（Security）]** をクリックします。

ステップ 3 **[作業 (Work)]** ペインで、**[ロール（Roles）]** を選択します。

ステップ 4 **[作業 (Work)]** ペインで、[アクション（Actions）] アイコン ドロップダウン リストをクリックし、**[ロールの作成（Create Role）]** を選択します。

ステップ 5 [**ロールの作成（Create Role**）] 画面で、次の操作を実行します。

a) **[名前（Name）]** フィールドに、ロールの名前を入力します。

b) [**説明（Description**）] フィールドに、説明を入力します。
c) [**権限の追加（Add Privileges**）] をクリックします。表示されている [**権限の選択（Select Privileges**）] ウィンドウで、必要なチェックボックスを選択して、ロールに対する 1 つまたは複数の権限を選択します。
d) [権限の選択（Select Privileges）] ウィンドウで、[**選択（Select**）] をクリックします。

ステップ 6 **[保存（Save）]** をクリックします。

次のタスク

`custom-privilege-1` などのカスタム権限を選択した場合は、カスタム権限を設定する （6 ページ） の手順に従って、このカスタム権限で公開される管理対象オブジェクト (MO) を選択します。

カスタム権限を設定する

この手順を使用してカスタム権限を設定し、事前定義された権限で公開されていない 1 つ以上の管理対象オブジェクト（MO）への読み取りまたは読み取り/書き込みアクセス権を提供します。

管理対象オブジェクト クラスについては、『Cisco APIC 管理情報モデル リファレンス』で説明されています。MO クラスごとに、そのクラスの読み取りまたは読み取り/書き込み権限を持つ事前定義されたロールがリファレンスに記載されています。

事前定義された権限ごとに、Cisco APIC のロールと権限のマトリクスを使用して、MO クラスのリストと読み取り/書き込み権限を表示できます。

MO クラスへの読み取りまたは書き込みアクセス権限を持つカスタム権限を設定するには、APIC REST API を使用する必要があります。API を使用する場合は、『*Cisco APIC REST API* 設定ガイド』を参照してください。

手順

以下の形式で APIC REST API POST を作成して送信し、クラス `aaa:RbacClassPriv` のオブジェクトを作成します。

例：

```
POST https://<APIC-IP>/api/node/mo/uni/rbacdb/rbacclpriv-<moClassName>.json

{
    "aaaRbacClassPriv":
    {
        "attributes":
        {
            "name": "<moClasssName>",
            "wPriv": "<privilege>",
            "rPriv": "<privilege>"
```

```
        }
    }
}
```

URI の *moClassName* 値に、アクセスを設定するオブジェクト クラスの名前を含めます。

ペイロードで、次の属性を指定します。

- `name`：アクセスを設定するオブジェクト クラスの名前。
- `wPriv`：クラスのオブジェクトへの書き込みアクセスを含むカスタム権限の名前。
- `rPriv`：クラスのオブジェクトへの読み取りアクセスを含むカスタム権限の名前。

カスタム権限に読み取りおよび書き込みアクセスを割り当てるには、`wPriv` と `rPriv` の両方にカスタム権限の名前を入力します。

例

この例は、クラス `fabric:Pod` のオブジェクトへの読み取りアクセスと書き込みアクセスの両方を使用して、カスタム権限 `custom-privilege-1` を設定する方法を示しています。

```
POST https://apic-aci.cisco.com/api/node/mo/uni/rbacdb/rbacclpriv-fabricPod.json

{
    "aaaRbacClassPriv":
    {
        "attributes":
        {
            "name": "fabricPod",
            "wPriv": "custom-privilege-1",
            "rPriv": "custom-privilege-1"
        }
    }
}
```

次のタスク

カスタム権限を持つカスタム ロールの作成 （5 ページ） で説明されている手順を使用して、カスタム権限をカスタム ロールに追加します。

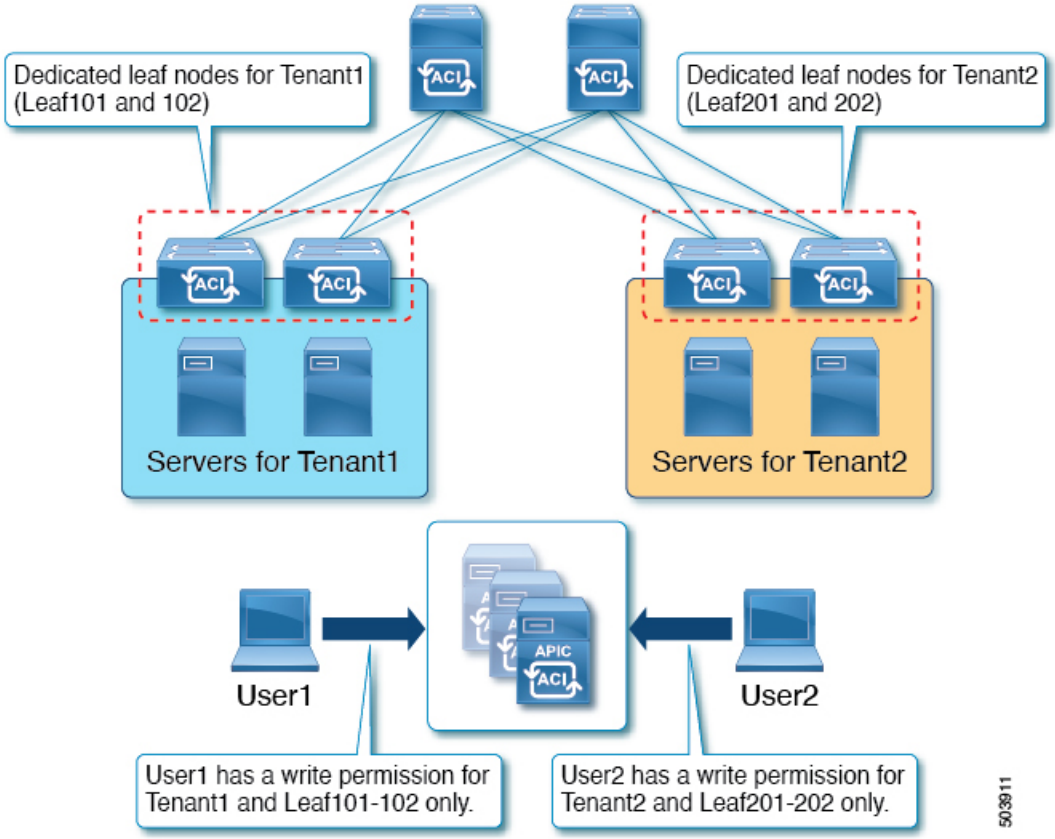
RBAC ノード ルールの設定の使用例

このセクションでは、このドキュメントで説明されている構成オプションが混在するユースケースについて説明します。各オプションの詳細については、このドキュメントの他の部分を参照してください。ユースケースは、次のシナリオに基づいています。

Cisco Application Centric Infrastructure (ACI) ファブリックに複数のテナントと複数のリーフノードがあるとします。マルチテナンシーの場合、ユーザーが特定のテナントと特定のリーフノードのセットのみを管理できるようにする必要があります。次に例を示します。

- User1 は Tenant1、リーフノード 101 と 102 のみを管理できます。
- User2 は Tenant2、リーフノード 201 および 202 のみを管理できます。

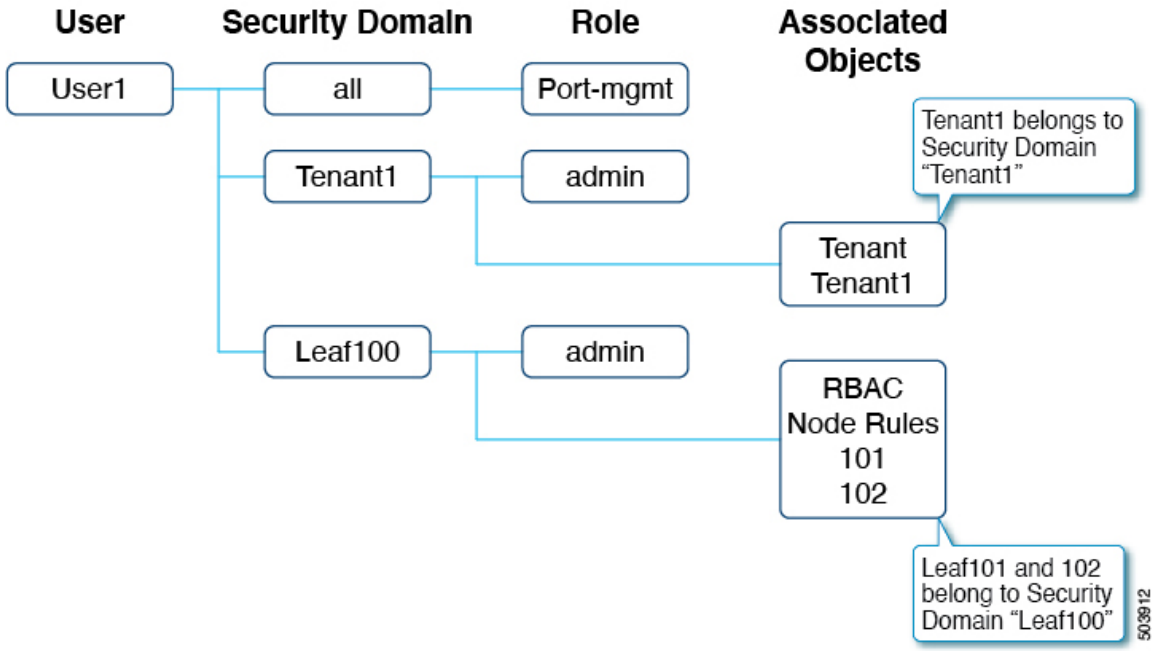
次の図では要件を説明しています。



これは、セキュリティドメインと RBAC ノードルールを使用して実現できます。高レベルでは、構成手順は次の通りです。

1. セキュリティドメインの作成
2. RBAC ノードルールの作成
3. ユーザーの作成

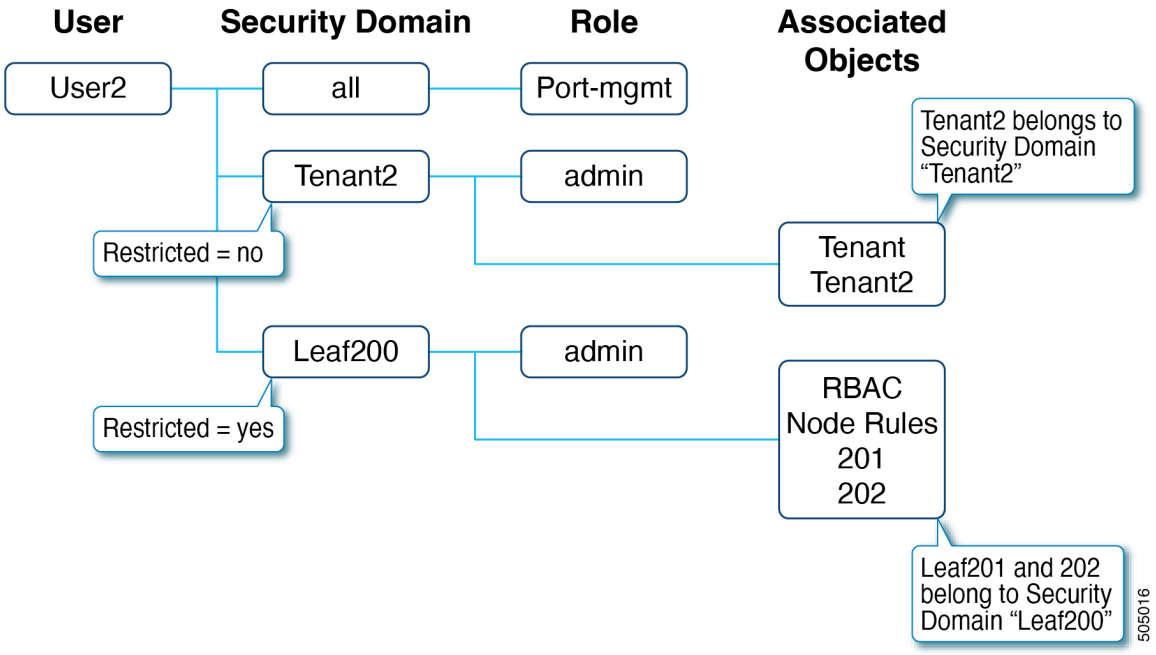
次の図は、この例の User1 の構成間の関係を示しています。



User1 には 3 つのセキュリティ ドメインがあります。

- `port-mgmt` ロールを持つすべてのドメイン ：User1 が割り当てられたリーフ ノードでポート関連の構成を管理できるようにします。
- `admin` ロールを持つドメイン `Tenant1`：User1 が Tenant1 を管理できるようにします。
- `admin` ロールを持つドメイン `Leaf100` ：User1 が Leaf101 と 102 を管理できるようにします。

次の図は、この例の User2 の構成間の関係を示しています。



User2 にも同様に 3 つのセキュリティドメインがあります。

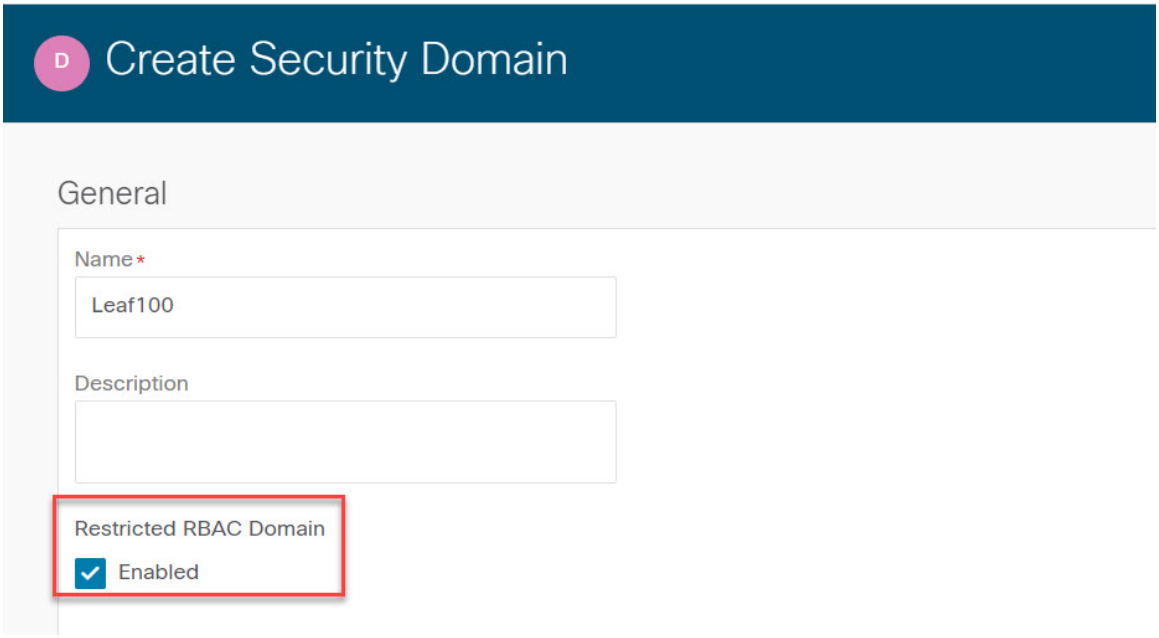
- `port-mgmt` ロールを持つすべてのドメイン ：User2 が割り当てられたリーフノードでポート関連の構成を管理できるようにします。
- `admin` ロールを持つドメイン `Tenant2`：User2 が Tenant2 を管理できるようにします。
- `admin` ロールを持つドメイン `Leaf200`：User2 が Leaf201 と 202 を管理できるようにします。

以降の項では、より詳細に構成手順について説明します。このセクションでは、User1 と Tenant1 の構成についてのみ説明します。User2 と Tenant2 の構成は、同じプロセスに従います。

手順 1：セキュリティドメインの作成

最初の手順は、セキュリティドメイン Tenant1 と Leaf100 を作成することです。これらのセキュリティドメインを組み合わせることができますが、この例では個別のセキュリティドメインを使用しています。

ドメインを作成するには、GUI で **[管理（Admin）]>>[AAA]>>[セキュリティ（Security）]>>[セキュリティドメイン（Security Domains）]> >[アクション（Actions）]>>[セキュリティ ドメインの作成（Create Security Domain）]**に移動します。



この例では、セキュリティドメイン Leaf100 の **[制限付き RBAC ドメイン（Restricted RBAC Domain）]** が有効になっています。そのため、User1 はインターフェイス ポリシー グループ、VLAN プール、および異なるセキュリティ ドメインの他のユーザによって作成された他のアクセスポリシーを表示できません。例外は、デフォルトのインターフェイスポリシーです。**[制限付き RBAC ドメイン（Restricted RBAC Domain）]** の構成に関係なく、デフォルトのインターフェイス ポリシーはリーフ RBAC ユーザに表示されます。つまり、**[制限付き RBAC ドメイン（Restricted RBAC Domain）]** が有効になっている場合、ユーザはデフォルト ポリシーの構成を変更できません。

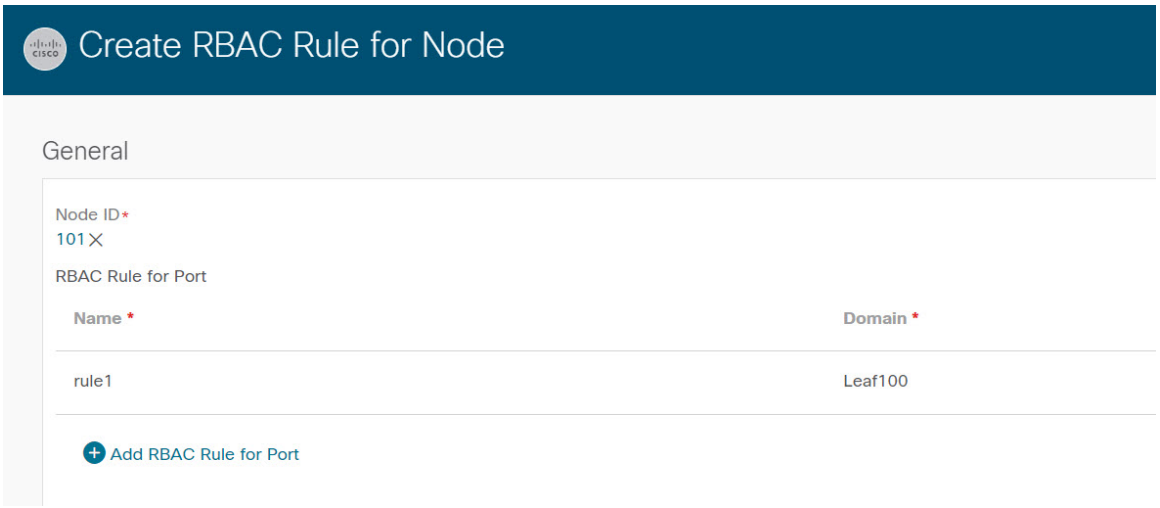
セキュリティドメイン Tenant1に対しては、**[制限付きRBACドメイン（Restricted RBAC Domain）]** を有効にしていません。テナントポリシーの場合、テナント自体が十分な管理の分離を提供するため、必須ではありません。テナント RBAC とノード RBAC の両方に同じセキュリティ ドメインを使用する場合は、**[制限付き RBAC ドメイン（Restricted RBAC Domain）]** を有効にする必要があります。

テナント RBAC の場合、テナントはセキュリティドメインに関連付けられている必要があります。この例では、Tenant1 をセキュリティドメイン「Tenant1」に関連付けます。ドメインを関連付けるには、GUI で、**[テナント（Tenant）]** > **[ポリシー（Policy）]** > **[セキュリティドメイン（Security Domains）]** に移動します。

手順 2: RBAC ノードルールを作成する

次の手順では、RBAC ノードルールを作成して、Leaf101 と Leaf102 をセキュリティドメイン Leaf100 に追加します。RBAC ノード ルールを作成するには、GUI で **[管理（Admin）]**> > **[AAA]**> > > **[セキュリティ（Security）]**> > **[RBAC ルール（RBAC Rules）]**> > **[ノード ルール（Node Rules）]**> > **[アクション（Actions）]**> > **[RBAC ノード ルールの作成（Create RBAC Node Rule）]**に移動します。

次の図は、ノード 101 の RBAC ルールを示しています。



ノード 102 に対して同じ構成を繰り返します。

手順 3：ユーザーを作成する

最後の手順は、ユーザー User1 を作成することです。ユーザを作成するには、GUI で **[管理（Admin）]> > [AAA]> > [ユーザ（Users）]> > [アクション（Actions）]> > [ローカル ユーザの作成（Create Local User）]** に移動します。

セキュリティと**ロール**の構成手順で、次のセキュリティドメインとロールを選択します。

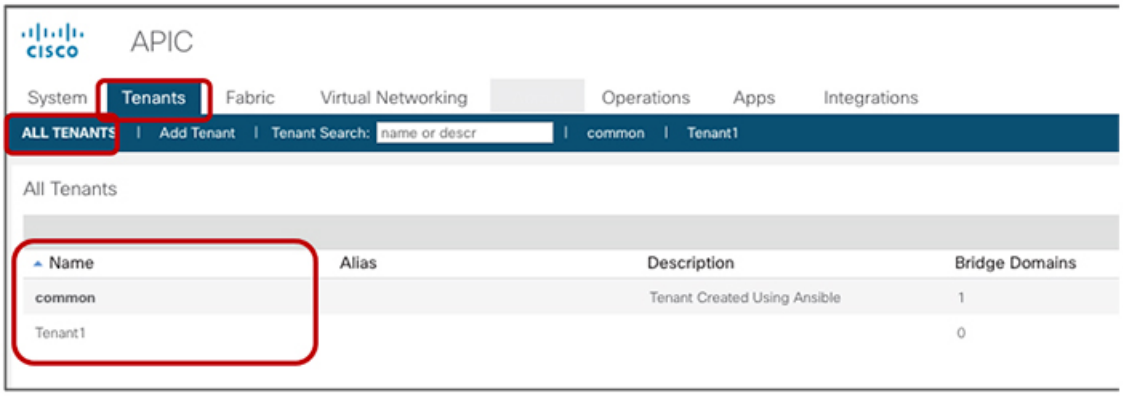
- all：書き込み権限を持つロール `port-mgmt`
- Leaf100：書き込み権限を持つロール `admin`
- Tenant1：書き込み権限を持つロール `admin`

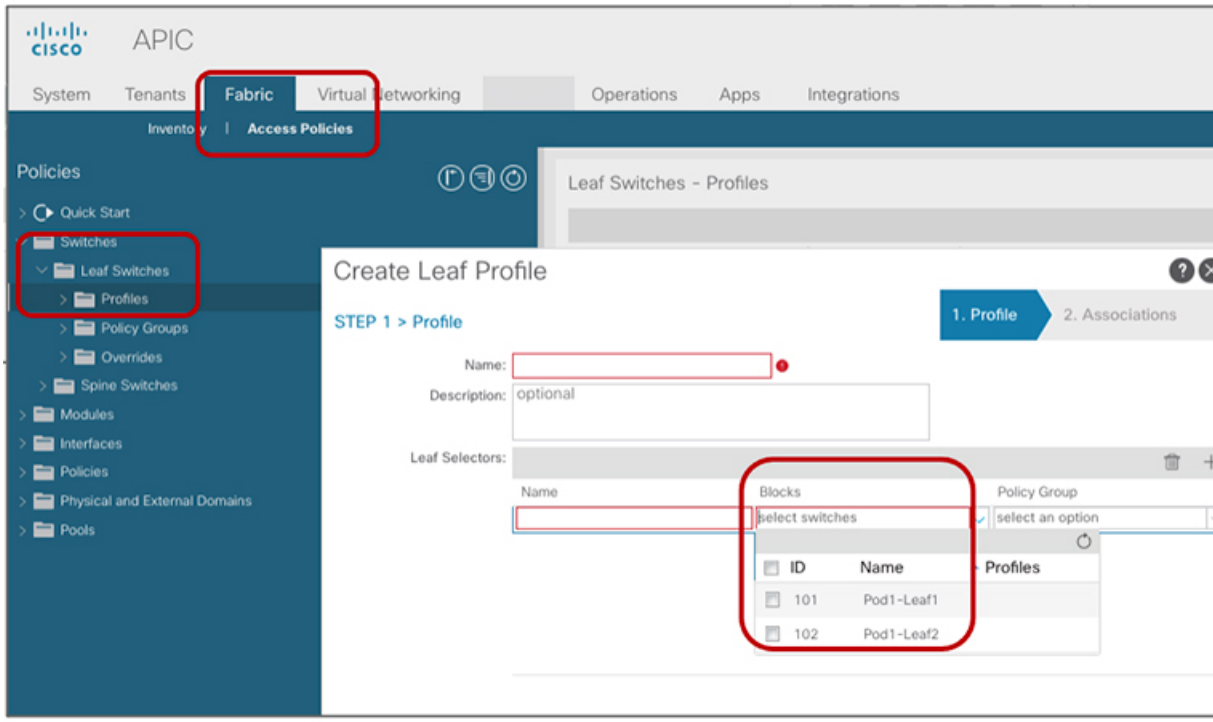
「RADIUS、 TACACS+、LDAP、RSA、SAML、OAuth 2、および DUO」の章で説明されている手順を使用して、Cisco AVPairs または LDAP グループ マップを使用して、リモート ユーザーに同じ設定を使用できます。

RBAC ノードルールの確認

User1 は Tenant1、Leaf 101 および 102 のみを管理できます。次に例を示します。

- User1 は、書き込み権限を持つ Tenant1 と読み出し権限を持つ共通テナント以外の他のテナントを参照することはできません。
- User1 は、**リーフセレクタ**で Leaf101 および 102 以外の他のリーフノードを表示できません。
- User1 は、同じセキュリティ ドメインに関連付けられたユーザーによって作成されたアクセスポリシー、またはシステムが作成したポリシー（読み取り専用）以外のアクセスポリシーを表示できません。


APIC
System
Tenants
Fabric
Virtual Networking
Operations
Apps
Integrations
ALL TENANTS
Add Tenant
Tenant Search:
name or descr
common
Tenant1
All Tenants
Name
Alias
Description
Bridge Domains
common
Tenant Created Using Ansible
1
Tenant1
0


APIC
System
Tenants
Fabric
Virtual Networking
Operations
Apps
Integrations
Inventory
Access Policies
Policies
Quick Start
Switches
Leaf Switches
Profiles
Policy Groups
Overrides
Spine Switches
Modules
Interfaces
Policies
Physical and External Domains
Pools
Leaf Switches - Profiles
Create Leaf Profile
STEP 1 > Profile
1. Profile
2. Associations
Name:
Description:
optional
Leaf Selectors:
Name
Blocks
Policy Group
select switches
select an option
ID
Name
Profiles
101
Pod1-Leaf1
102
Pod1-Leaf2

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。