



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 \(1 ページ\)](#)
- [ノードをドメインに割り当てる \(1 ページ\)](#)
- [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 \(2 ページ\)](#)
- [セキュリティ ドメインの作成 \(3 ページ\)](#)
- [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 \(3 ページ\)](#)
- [カスタムの役割と権限 \(4 ページ\)](#)
- [RBAC ノード ルールの設定の使用例 \(7 ページ\)](#)

ドメイン別にアクセスを制限する

制限付きセキュリティ ドメインを使用すると、テナント A などのファブリック管理者は、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、あるユーザーグループがテナント B などの別のセキュリティ 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、テナント A の制限付きセキュリティ ドメインのテナント管理者は、テナント B のセキュリティ ドメインで設定されたポリシー、プロファイル、またはユーザーを表示できません。テナント B のセキュリティ ドメインも制限されていない限り、テナント B は、テナント A で設定されたポリシー、プロファイル、またはユーザーを表示できます。ユーザーが適切な権限を持つシステム作成の設定に対して、ユーザーは常に読み取り専用で閲覧可能であることに注意してください。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。

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ーもドメイン `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` のユーザーにロールを付与し、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ーは、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ー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 \(5 ページ\)](#) 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。

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が制限付きドメインとして構成されている場合、このドメインに割り当てられているユーザーは、他のセキュリティドメインで構成されたポリシー、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。

-
- 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。
- [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。
 - [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。
- [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 \(5 ページ\)](#) で説明されているように、カスタム権限を設定できます。

-
- 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 \(5 ページ\)](#) 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。

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 \(4 ページ\)](#) 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。

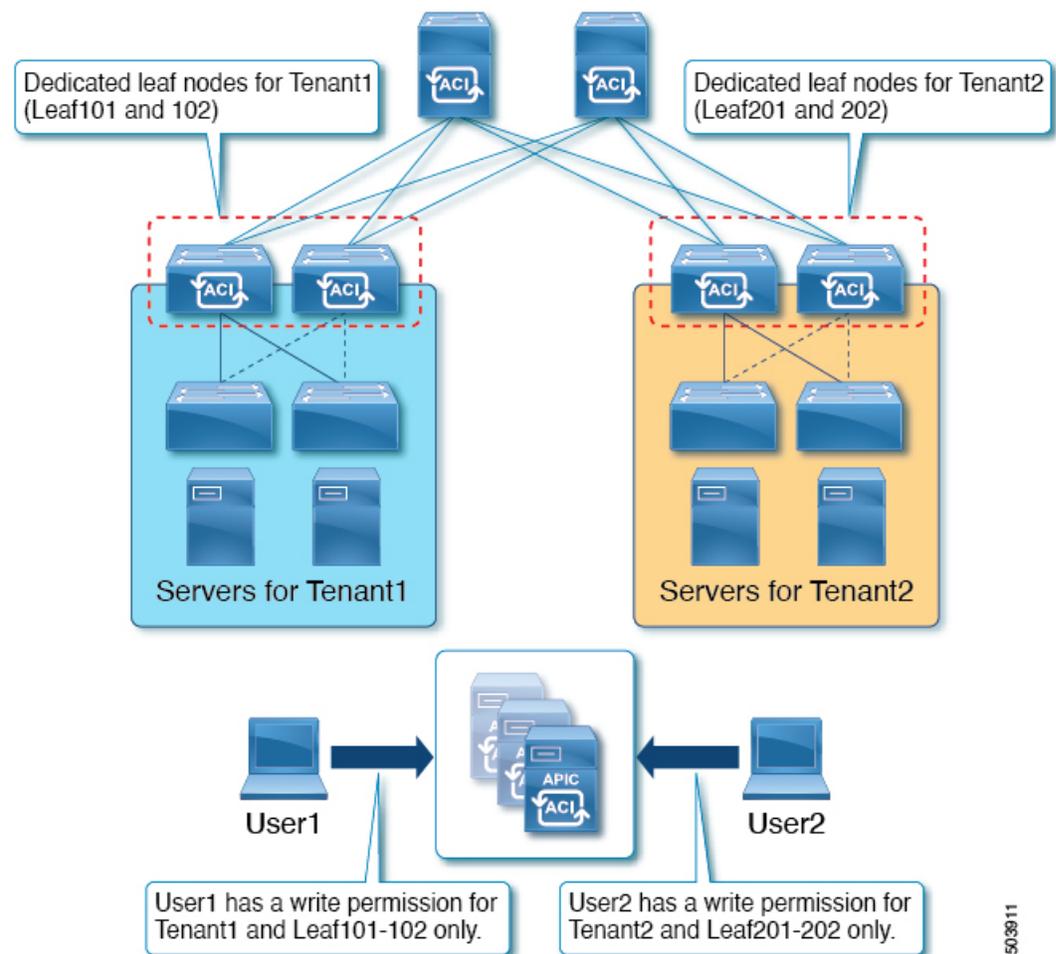
RBAC ノードルールの設定の使用例

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。

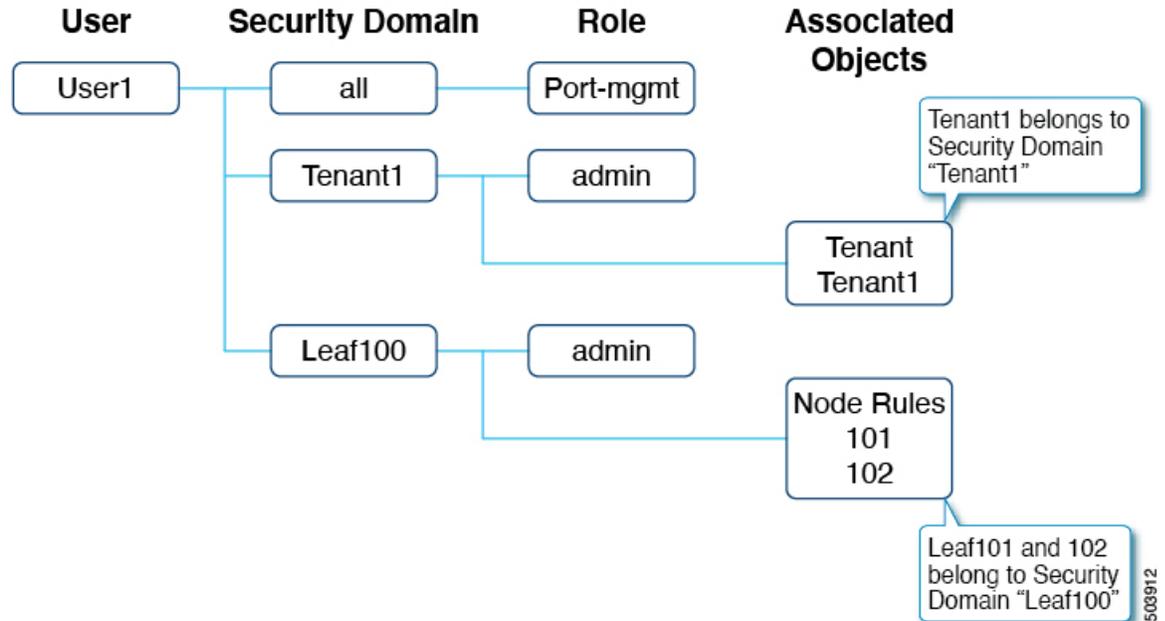
次の図では要件を説明しています。



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。

- すべての port-mgmt ロール : 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。デフォルトでは、port-mgmt ロールには custom-port-privilege 権限があります。custom-port-privilege 権限を含むお客様ロールを使用することもできます。
- admin ロールを持つ Tenant1 : User1 が Tenant1 を管理できるようにします。
- admin ロールを持つ Leaf100 : User1 が Leaf101 と 102 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。

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。

D Create Security Domain

General

Name*

Leaf100

Description

Restricted RBAC Domain

Enabled

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。

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。ドメインを作成するには、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。

Node ID*

101 X

RBAC Rule for Port

Name *	Domain *
rule1	Leaf100

+ Add RBAC Rule for Port

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。

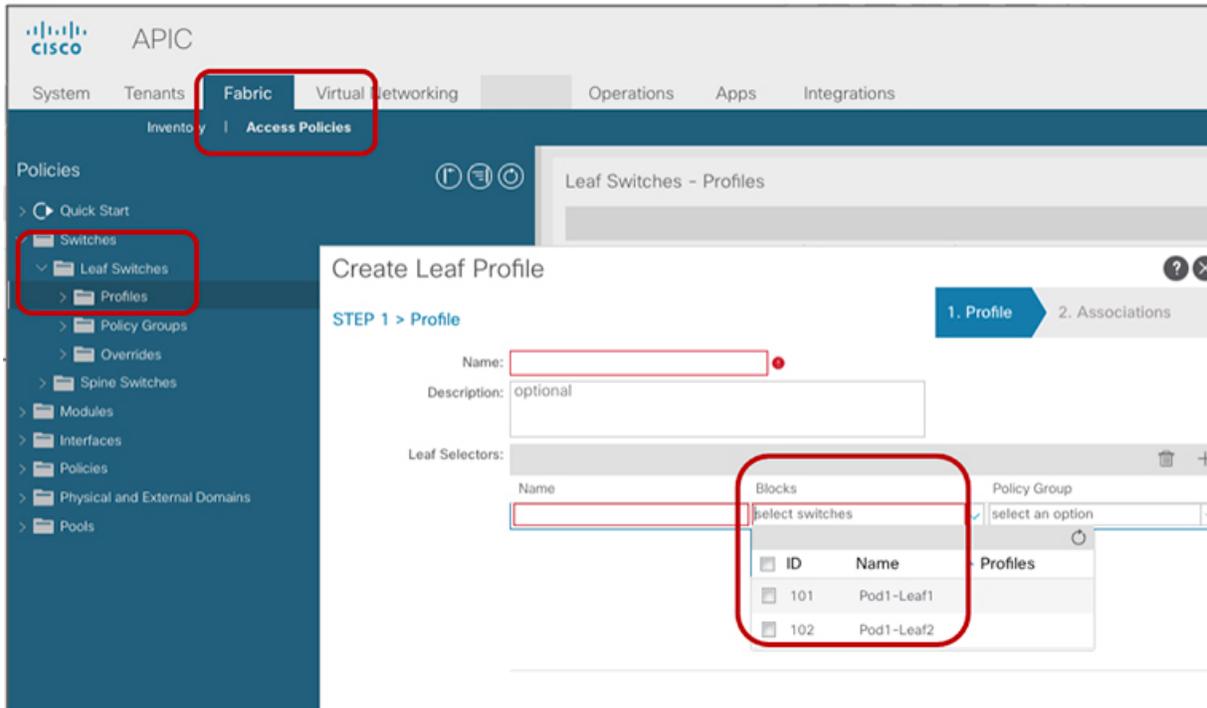
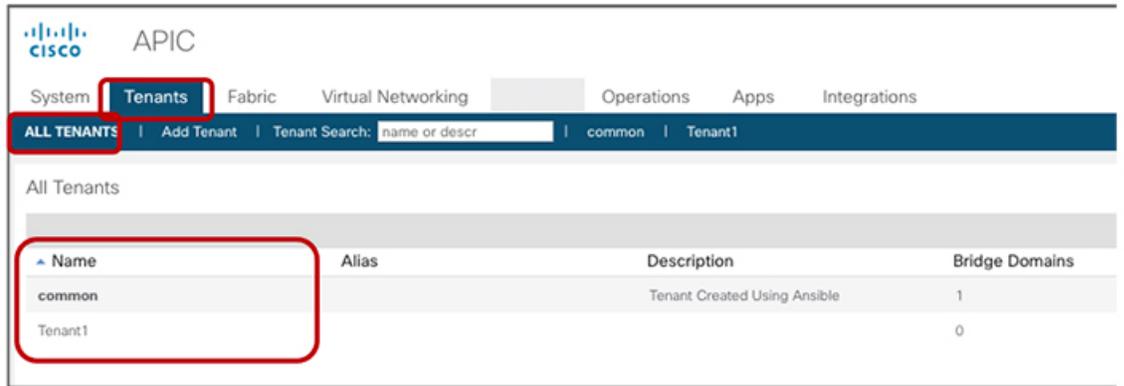
セキュリティとロールの構成手順で、次のセキュリティドメインとロールを選択します。

- 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

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。



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。