アクセスの制限

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権限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。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構成に対して、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。

たとえば、制限付きセキュリティ ドメインのユーザーがテナント A に関連付けられているとします。テナント A には、ユーザーが作成したアプリケーション プロファイル 1 と管理者が作成したアプリケーション プロファイル 2 の 2 つのアプリケーション プロファイルが含まれています。アプリケーションプロファイル2も同じテナントのものですが、ユーザーはアプリケーション プロファイル 1 しか表示できません。ユーザーが制限付きセキュリティ ドメインにいる場合、管理者によって作成されたプロファイルも表示されません。

上記の例では、アプリケーションプロファイル2は別のユーザー（管理者）によって作成されていますが、制限のないユーザー（制限付きのセキュリティドメインに属していないユーザー）は、アプリケーション プロファイル 1 とアプリケーション プロファイル 2 の両方を表示できます。

RBAC ルール

Cloud Application Policy Infrastructure Controller (cAPIC) では、ロールベース アクセス コントロール（RBAC）を介してユーザーのロールに従ってアクセスが提供されます。ファブリック ユーザーは以下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

Cloud APIC 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 cAPIC 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、 cAPIC 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。

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、cAPIC 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
- インフラ：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

Cisco Cloud APIC は、次の AAA ロールと権限をサポートしています。

特権	説明
ロール：管理	
admin	すべてのファブリックの機能へのフル アクセスを提供します。管理者権限は、その他のすべての権限を組み合わせたものとみなされます。
ロール：aaa	

特権	説明
aaa	ポリシーの認証、許可、アカウンティング、インポート/エクスポートの設定に使用されます。
Role: access-admin	
access-connectivity	インフラでのレイヤ 1 ～ 3 の構成、テナントの L3Out でのスタティックルート構成、管理インフラ ポリシー、テナント ERSPAN ポリシーに使用されます。
access-equipment	アクセス ポート設定に使用されます。
access-protocol	インフラストラクチャ、NTP、SNMP、DNS、およびイメージ管理用のファブリック全体のポリシー、およびクラスタポリシーやファームウェアポリシーなどの操作関連のアクセスポリシーでレイヤ 1 ～ 3 のプロトコル構成に使用されます。
access-qos	CoPP および QoS に関連するポリシーの変更に使用されます。
ロール：**fabric-admin**	
fabric-connectivity	ファブリック、ファームウェア、および導入ポリシーのレイヤ1～3の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーを生成します。
fabric-equipment	リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。
fabric-protocol	ファブリックでのレイヤ 1 ～ 3 のプロトコル構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPAN およびヘルススコアポリシー、およびファームウェア管理のトレースルートおよびエンドポイント トラッキングポリシーに使用されます。
ロール：**nw-svc-admin**	

特権	説明
nw-svc-policy	レイヤ 4 ～ レイヤ 7 ネットワークサービス オーケストレーションの管理に使用されます。
ロール： nw-svc-params	
nw-svc-params	レイヤ 4 ～ レイヤ 7 のサービス ポリシーの管理に使用されます。
Role: ops	
ops	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）。
ロール：port-mgmt	
port-mgmt	ノードをセキュリティドメインに割り当てるために使用されます。また、ノードルールを持つセキュリティドメインのユーザーは、`port-mgmt` のロールを持つドメイン `all` に割り当てる必要があります。
Role: tenant-admin	
aaa	ポリシーの認証、許可、アカウンティング、インポート/エクスポートの設定に使用されます。
access-connectivity	インフラでのレイヤ 1 ～ 3 の構成、テナントの L3Out でのスタティックルート構成、管理インフラ ポリシー、テナント ERSPAN ポリシーに使用されます。
access-equipment	アクセス ポート設定に使用されます。
access-protocol	インフラストラクチャ、NTP、SNMP、DNS、およびイメージ管理用のファブリック全体のポリシー、およびクラスタポリシーやファームウェアポリシーなどの操作関連のアクセスポリシーでレイヤ 1 ～ 3 のプロトコル構成に使用されます。
access-qos	CoPP および QoS に関連するポリシーの変更に使用されます。

特権	説明
fabric-connectivity	ファブリック、ファームウェア、および導入ポリシーのレイヤ1～3の構成に使用します。ポリシー導入の影響を推定するための警告、およびリーフスイッチとスパインスイッチのアトミックカウンタ、診断、およびイメージ管理ポリシーを生成します。
fabric-equipment	リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシーに使用されます。
fabric-protocol	ファブリックでのレイヤ 1 ～ 3 のプロトコル構成、NTP、SNMP、DNS、およびイメージ管理のファブリック全体のポリシー、ERSPAN およびヘルススコアポリシー、およびファームウェア管理のトレースルートおよびエンドポイント トラッキングポリシーに使用されます。
nw-svc-policy	レイヤ 4 ～ レイヤ 7 ネットワークサービス オーケストレーションの管理に使用されます。
tenant-network-profile	ネットワークプロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。
tenant-protocol	テナント下のレイヤ1～3プロトコルの構成、テナント トレース ルート ポリシー、およびファームウェア ポリシーの書き込みアクセスに使用されます。
tenant-qos	テナントの QoS に関連する設定に使用されます。
tenant-security	テナントのコントラクトに関連する設定に使用されます。
Role: tenant-ext-admin	

特権	説明
tenant-connectivity	ブリッジドメイン、サブネット、およびVRFなどの レイヤ 1 ～ 3 の接続変更に使用されます。これには、リーフ スイッチおよびスパイン スイッチのアトミック カウンタ、診断、およびイメージ管理ポリシー、テナントのインバンドおよびアウトオブバンド管理接続構成。アトミック カウンタやヘルス スコアなどのデバッグ/モニタリング ポリシーなどがあります。
tenant-epg	エンドポイント グループ、VRF、ブリッジ ドメインの削除/作成など、テナント設定の管理に使用されます。
tenant-ext-connectivity	書き込みアクセス ファームウェア ポリシーに使用されます。テナント L2Out および L3Out 設定の管理。デバッグ/モニタリング/オブザーバ ポリシー。
tenant-ext-protocol	BGP、OSPF、PIM、IGMP などのテナント外部レイヤ 1 ～ 3 プロトコルの管理、およびトレースルート、ping、oam、eptrk などのデバッグ/モニタリング/オブザーバ ポリシーに使用されます。通常、ファームウェア ポリシーの書き込みアクセスにのみ使用します。
tenant-network-profile	ネットワーク プロファイルの削除および作成、エンドポイント グループの削除および作成など、テナント設定の管理に使用されます。
tenant-protocol	テナント下のレイヤ1～3プロトコルの構成、テナント トレースルートポリシー、およびファームウェアポリシーの書き込みアクセスに使用されます。
tenant-qos	テナントの QoS に関連する設定に使用されます。
tenant-security	テナントのコントラクトに関連する設定に使用されます。

カスタム権限は、任意のMOクラスに割り当てることができます。22個のカスタム権限がCisco Cloud APIC GUIに表示されます。これらのカスタム権限のいずれかがクラスに割り当てられている場合、その MO のアクセスには新しく追加されたカスタム権限が含まれます。1 つのカスタム権限を 1 つ以上の MO クラスに関連付けることができます。

（注） カスタム権限はCisco Cloud APIC GUIで表示されますが、現在サポートされていません。

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。

RBACルール

RBAC ルールは、リソース（アプリケーション プロファイル、EPG、契約など）を、別のセキュリティ ドメインにいるためにアクセスできないユーザーに選択的に公開します。RBAC ルールは、アクセスされるオブジェクトを特定する識別名（DN）と、オブジェクトにアクセスするユーザーを含むセキュリティ ドメインの名前の 2 つの部分で構成されます。

RBAC ルールには 2 つのタイプがあります。

- 暗黙的 - ユーザーは、RBAC 階層に基づいてルールまたは権限を継承します
- 明示的 - ルールは特定のポリシーに基づいてユーザーに直接割り当てられます

制限付きおよび制限なしの両方のセキュリティ ドメインがサポートされています。

（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。

制限付きドメインの注意事項と制限事項

制限付きドメインのユーザーに対するガイドラインと制限は次のとおりです。

- あるセキュリティ ドメインのユーザーに別のセキュリティ ドメインが割り当てられている場合、そのユーザーは新しいドメインに関連付けられた構成にアクセスできます。

- ユーザーは、「制限付き」とマークされた1つ以上のセキュリティ ドメインの一部になることができます。
- 制限付きドメインユーザーは、システムで作成された構成への読み取り専用アクセス権を持っています。
- 複数のセキュリティ ドメインを持つユーザーの場合、すべてのセキュリティ ドメインを合わせた長さが 1024 文字を超えることはできません。長さが 1024 を超えると、ユーザーはポリシーの作成に問題が発生します。
- Cloud APIC の制限付きドメインは、クラウド リソースではサポートされていません。つまり、ある制限付きドメインのユーザーは、別の制限付きドメインのユーザーによって作成されたクラウド リソースを表示できます。

Cisco Cloud APIC GUI を使用した RBAC ルールの作成

このセクションでは、GUI を使用して RBAC ルールを作成する方法について説明します。

（注） RBAC ルールを構成できますが、Cloud APIC GUI は構成をサポートしていません。この手順（手順 4）を使用して構成された DN は、API を使用して照会できます。

始める前に

セキュリティ ドメインの作成詳細なタスクについては、「セキュリティ ドメインの作成」を参照してください。

ステップ 1 **インテント** アイコンをクリックします。**[インテント（Intent）]** メニューが表示されます。

ステップ 2 [Intent]検索ボックスの下にあるドロップダウン矢印をクリックし、[Administrative]を選択します。

[インテント（Intent）] メニューに**管理**オプションのリストが表示されます。

ステップ 3 **[インテント（Intent）]** メニューの **[管理（Administrative）]** リストから、**[セキュリティ（Security）]** > **[RBAC ルール（RBAC Rules）]** > **[RBAC ルールの作成（Create RBAC Rule）]** をクリックします。**[RBAC ルールの作成（Create RBAC Rule）]** ダイアログボックスが表示されます。

ステップ 4 **DN** フィールドに、ルールの DN を入力します。

明示的な RBAC ルールを作成するには、ObjectStore でアプリケーションの DN を見つけます。ここでその DN 値を使用します。

ステップ 5 セキュリティ ドメインを選択します。

a) **[セキュリティ ドメインの選択（Select Security Domain）]** をクリックします。**[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログ ボックスが表示されます。

b) **[セキュリティ ドメインの選択（Select Security Domain）]** ダイアログで、左側の列のセキュリティ ドメインをクリックして選択し、**[選択（Select）]** をクリックします。**[RBAC ルールの作成]** ダイアログボックスに戻ります。

ステップ 6 **[書き込みを許可]** フィールドで、**[はい]** をクリックして書き込みを許可するか、**[いいえ]** をクリックして書き込みを許可しません。

ステップ 7 設定が終わったら [Save] をクリックします。

（注） 明示的な RBAC ルールを作成した後、セキュリティ ドメインに割り当てられたユーザーは、以前に（ObjectStore から）定義されたアプリケーションとその子のみを表示できます。

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。