Cisco ACI でのマイクロセグメンテーション

この章の内容は、次のとおりです。

• Cisco ACI でのマイクロセグメンテーション （1 ページ）

Cisco ACI でのマイクロセグメンテーション

シスコ アプリケーション セントリック インフラストラクチャ（ACI）を使用したマイクロセグメンテーションを使用すると、エンドポイントをエンドポイント グループ（EPG）と呼ばれる論理セキュリティ ゾーンに自動的に割り当てることができます。これらの EPG はさまざまなネットワーク ベースまたは仮想マシン (VM) ベースの属性に基づいています。この章には、Cisco ACI とマイクロセグメンテーションのコンセプトについての情報と、 マイクロセグメント (uSeg) EPG の設定の手順が含まれています。

Cisco ACI のマイクロセグメンテーションは、以下のものにアタッチされた仮想エンドポイントをサポートしています:

- Cisco ACI Virtual Edge

（注） Cisco ACI によるマイクロセグメンテーションは、Cisco ACI Virtual Edge が Cisco ACI Virtual Pod（vPod）の一部ではない場合に、Cisco ACI Virtual Edge に対してサポートされます。

- Cisco Application Virtual Switch（AVS）
- Microsoft Hyper-V 仮想スイッチ
- VMware vSphere 分散スイッチ (VDS)

ネットワーク ベースの属性を持つマイクロセグメンテーションは、ベアメタル環境もサポートしています。『*Cisco APIC の基本的なコンフィギュレーション ガイド リリース 3.x*』の、「ネッ

トワークベースの属性を持つマイクロセグメンテーションのベア メタルでの使用」の項を参照してください。

Cisco ACI のマイクロセグメンテーションは、IP ベースの属性を持つ EPG を使用して、物理エンドポイントもサポートします。

（注） Cisco ACI のマイクロセグメンテーションは物理および仮想エンドポイントに合わせて設定することができ、同じ EPG を物理および仮想エンドポイントの両方と共有することができます。

（注） Cisco ACI Virtual Edge、 Cisco AVS、または Microsoft Hyper-V 仮想スイッチを使用する場合には、次の制限に注意してください: MAC ベースの EPG と、仮想エンドポイントの IP 以外の属性を使用する場合には、VDS VMM ドメインの物理エンドポイントまたは仮想エンドポイントに対し、オーバーラップのある IP 属性フィルタを設定しないでください。これに従わないと、Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチでは、マイクロセグメンテーション EPG の分類が上書きされます。

Cisco Application Policy Infrastructure Controller（APIC）は、Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、および Microsoft Hyper-V 仮想スイッチが使用するマイクロセグメンテーションポリシーを管理します。ファブリックはポリシーを適用します。このセクションでは、EPG、テナント、契約、および Cisco ACI ポリシーに関連するその他の主要な概念に精通していることを想定しています。詳細については、『*Cisco Application Centric Infrastructure Fundamentals*』を参照してください。

Cisco APIC リリース 3.2(1) 以降では、マイクロセグメント EPG 同士の間、およびマイクロセグメント EPG と通常の EPG の間の契約で、レイヤ 4 ～ レイヤ 7 のサービス グラフがサポートされます。詳細な情報と設定の手順については、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』 を参照してください。Cisco.com から入手できます。

Cisco ACI でのマイクロセグメンテーションの利点

テナント内の仮想マシン（VM）をグループ化してフィルタリングおよび転送ポリシーを適用するには、エンドポイント グループ（EPG）を使用します。Cisco ACI でのマイクロセグメンテーションは、既存のアプリケーション EPG 内のエンドポイントを新しいマイクロセグメント (uSeg) EPG にグループ化し、ネットワークまたは VM ベースの属性をこれらの uSeg EPG に合わせて構成する能力を付与します。これにより、これらの属性をフィルタリングして、より動的なポリシーを適用することができます。Cisco ACI でのマイクロセグメンテーションにより、テナント内の任意のエンドポイントにポリシーを割り当てることもできます。

例：単一 EPG または同じテナント内の複数の EPG における Cisco ACI でのマイクロセグメンテーション

EPG に Web サーバを割り当て、類似したポリシーを適用できるようにすることができます。デフォルトでは、EPG 内のすべてのエンドポイントが自由に相互に通信できます。ただし、こ

の Web EPG に実稼働 Web サーバと開発用 Web サーバが混在する場合は、これらの異なるタイプの Web サーバ間の通信を許可したくない場合があります。Cisco ACI でのマイクロセグメンテーションを使用すると、新しい EPG を作成し、「Prod-xxxx」や「Dev-xxx」などの VM 名属性に基づいてエンドポイントを自動的に割り当てることができます。

例：エンドポイント検疫のためのマイクロセグメンテーション

Web サーバおよびデータベース サーバに個別の EPG があり、それぞれに Windows VM と Linux VM の両方が含まれているとします。Windows のみに影響するウィルスがネットワークに脅威を与えている場合は、たとえば「Windows-Quarantine」という新しい EPG を作成し、VM ベースのオペレーティング システム属性を適用してすべての Windows ベースのエンドポイントをフィルタリングで除去することにより、すべての EPG にわたって Windows VM を分離することができます。この検疫 EPG には、さらに制限された通信ポリシーを適用できます（許可されるプロトコルの制限や、コントラクトを持たないことによるその他の EPG との通信の防御など）。マイクロセグメント EPG は、コントラクトを持っていてもコントラクトを持っていなくてもかまいません。

Cisco ACI を使用するマイクロセグメンテーションの仕組み

Cisco ACI を使用するマイクロセグメンテーションには、Cisco APIC、vCenter または Microsoft System Center Virtual Machine Manager（SCVMM）、およびリーフ スイッチが含まれます。このセクションでは、Cisco ACI Virtual Edge, Cisco AVS、VMware VDS、Microsoft Hyper-V 仮想スイッチを使用するマイクロセグメンテーションのワークフローを説明します。

Cisco APIC

1. ユーザーは、Cisco APIC の Cisco ACI Virtual Edge、Cisco APIC、VMware VDS、Microsoft Hyper-V 仮想スイッチの VMM ドメインを設定します。
2. Cisco APIC は vCenter または SCVMM に接続し、以下を実行します。
    1. Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、または Microsoft Hyper-V 仮想スイッチのインスタンスを作成します。
    2. VM と、関連付けられた VMware vCenter または Microsoft SCVMM からのハイパーバイザのインベントリ情報をプルします。
3. ユーザーはアプリケーション EPG を作成し、vCenter/SCVMM ドメインに関連付けます。各 vCenter/SCVMM ドメインでは、新しいカプセル化がこのアプリケーション EPG に割り当てられます。アプリケーション EPG に属性はありません。

    vCenter/SCVMM 管理者は、マイクロセグメンテーション（uSeg）EPG ではなく、このアプリケーション EPG に仮想エンドポイントを割り当てます。ポート グループとして vCenter/SCVMM に表示されるのはこのアプリケーション EPG です。
4. ユーザは uSeg EPG を作成して VMM ドメインに関連付けます。

    uSeg EPG はポート グループとして vCenter/SCVMM に表示されません。これには特別な機能があります。uSeg EPG には、フィルタ条件と一致する VM ベースの属性があります。

uSeg EPG VM 属性と VM の間に一致がある場合、Cisco APIC はその VM を uSeg EPG に動的に割り当てます。

エンドポイントはアプリケーション EPG から uSeg EPG に転送されます。uSeg EPG が削除されると、エンドポイントは再びアプリケーション EPG に割り当てられます。

Seg EPG を有効にするには、uSeg EPG を VMM ドメインに割り当てる必要があります。uSeg EPG を VMM ドメインに関連付けると、条件はその VMM ドメインにのみ適用されます。VMware VDS がある場合、アプリケーション EPG として同じブリッジ ドメインに uSeg EPG を割り当てる必要があります。

VMware VDS の場合、条件はその VMM ドメインとブリッジ ドメインに適用されます。

リーフ スイッチおよび Cisco ACI Virtual Edge、Cisco AVS、Microsoft Hyper-V 仮想スイッチ

1. 物理リーフ スイッチは Cisco APIC から属性ポリシーを取得します。
2. VM が Cisco ACI Virtual Edge、Cisco AVS、Microsoft Hyper-V 仮想スイッチに接続するとき、OpFlex プロトコルを使用して Cisco ACI Virtual Edge,、Cisco AVS、Microsoft Hyper-V 仮想スイッチは物理リーフ スイッチに VM 接続メッセージを送信します。
3. 物理リーフ スイッチは、テナントに設定された属性ポリシーと VM を照合します。
4. VM が設定された VM 属性と一致する場合、物理リーフ スイッチは、uSeg EPG を対応するカプセル化とともに 、Cisco ACI Virtual Edge、Cisco AVS または Microsoft Hyper-V 仮想スイッチにプッシュします。

   この操作では、vCenter/SCVMM での VM に対する元のポート グループ割り当ては変更されません。

Cisco ACI Virtual Edge、Cisco AVS、Microsoft Hyper-V 仮想スイッチへのパケット転送

1. VM がデータ パケットを送信すると、Cisco ACI Virtual Edge、Cisco AVS または Microsoft Hyper-V 仮想スイッチは、アプリケーション EPG ではなく、uSeg EPG に対応するカプセル化を使用して、それらのパケットにタグ付けします。
2. 物理リーフのハードウェアは、属性ベースのカプセル化された VM パケットを確認して、設定されたポリシーと照合します。

   VM は uSeg EPG に動的に割り当てられ、パケットは、その特定の uSeg EPG に定義されたポリシーに基づいて転送されます。

Cisco ACI でのマイクロセグメンテーションの属性

uSeg EPG に属性を適用すると、属性なしで EPG にポリシーを適用する場合よりも高い精度の転送ポリシーおよびセキュリティ ポリシーを EPG に適用できます。属性はテナント内で固有です。

uSeg EPG に適用可能な属性には、ネットワーク ベースの属性と VM ベースの属性の 2 つのタイプがあります。

ネットワークベースの属性

ネットワーク ベースの属性は、IP（IP アドレス フィルタ）と MAC（MAC アドレス フィルタ）です。uSeg EPG に、1 個以上の MAC アドレスまたは IP アドレスを適用できます。

IP アドレスには単にアドレスまたはサブネットを指定し、MAC アドレスには単にアドレスを指定します。

（注） ネットワークベースの属性を使用し、同じサブネット内のIPアドレスを分類する場合は、MAC ベースのネットワークの属性を使用する必要があります。IP ベースのマイクロセグメンテーション EPG は、同じサブネット内の IP アドレスの分類をサポートしていません。IP ベースのマイクロセグメンテーション EPG は、トラフィックでレイヤ 3 ルーティングが必要な場合にのみサポートされます。トラフィックがブリッジされた場合、マイクロセグメンテーションポリシーは適用できません。

VM ベースの属性

VMware VDS、Cisco AVS、または Cisco ACI Virtual Edge uSeg EPG に複数の VM ベースの属性を適用できます。VM ベースの属性は、VMM ドメイン、オペレーティング システム、ハイパーバイザ ID、データセンタ、VM ID、VM 名、VNic Dn（vNIC ドメイン名）、カスタム属性、タグです。

（注） 属性データセンタは、Microsoft Hyper-V 仮想スイッチのクラウドに対応します。

（注） 属性 VM フォルダは、GUI にも表示されます。この機能はベータ テスト版のみであり、実稼働環境で展開しないでください。

VM ベースの属性を作成する場合、属性に名前を付けるほかに、以下を実行する必要があります。

1. [VM Name] や [Hypervisor Identifier] などの属性タイプを指定します。
2. [Equals] や [Starts With] などの演算子を指定します。
3. 特定の vNIC またはオペレーティング システムの名前などの値を指定します。

カスタム属性およびタグ属性

このカスタム属性およびタグ属性により、他の属性で使用されていない条件に基づいて属性を定義できます。たとえば、vCenter で「セキュリティ ゾーン」というカスタム属性を定義し、「DMZ」や「境界」など値を使用してこの属性を 1 つ以上の VM に関連付けることができます。APIC 管理者は、その VM カスタム属性に基づいて、uSeg EPG を作成できます。

カスタム属性およびタグ属性が、VM の属性として APIC GUI で表示されます。

- カスタム属性
  - VMware vCenter で設定された VM 属性として Cisco ACI Virtual Edge, Cisco AVS、VMware VDS で利用可能です
  - Microsoft SCVMM で設定されているカスタム プロパティとして Microsoft Hyper-V 仮想スイッチで利用可能です
- 属性のタグ：Cisco ACI Virtual Edge 、Cisco AV、VMware VDS のみで利用可能です

Cisco ACI Virtual Edge。Cisco AVS、VMware VDS のカスタム属性またはタグ属性を使用する場合、VMware vSphere Web クライアントにも追加される必要があります。Microsoft Hyper-V の仮想スイッチのカスタム属性を使用する場合は、Microsoft SCVMM のカスタム プロパティとして追加する必要があります。USeg EPG を設定する前に行うことをお勧めします。これにより、Cisco APIC で"マイクロセグメンテーション ポリシーを設定する際、ドロップダウンリストでカスタム属性またはタグ属性を選択することができます。

Cisco APIC で uSeg EPG を設定した後、vSphere Web クライアントまたは SCVMM でカスタム属性またはタグ属性を追加できます。ただし実行する場合、テキストボックスにカスタム属性またはタグ属性の名前を入力可能でも、Cisco APIC のドロップダウンリストでカスタム属性またはタグ属性が表示されません。

vSphere Web クライアントでカスタム属性またはタグ属性を追加する手順については、VMware vSphere ESXi および vCenter Server のマニュアルを参照してください。SCVMM でカスタム属性を追加するための手順については、Microsoft のマニュアルを参照してください。

ただし、カスタム属性と同様に、一部でタグ属性とは異なります。

- タグ属性はホストまたはデータセンタなどの vCenter 内のオブジェクトに適用できます。カスタム属性は VM および ESXi にのみ適用できます。ただし、VM のタグ属性のみがマイクロセグメンテーションに関連します。
- カスタム属性と同様に、タグ属性には名前と値がありません。タグはオブジェクトに適用されるか否かのみラベリングしています。
- カスタム属性を設定するため、演算子や値と同じく、コントローラおよびVMに関する詳細を説明します。タグ属性を設定するには、属性タイプ、カテゴリ、演算子、タグ名を提供します。

（注） VCenter が vSphere 6 以降を実行している場合にのみ、uSeg EPG のタグ属性を定義できます。

テナント内の属性の一意性

属性はテナント内で一意である必要があります。一意性は属性の値によって異なります。

たとえば、ネットワーク ベースの属性については、テナント内の属性 IP アドレスのフィルタを使用できます。その場合、使用されるたびに属性が異なる値の IP アドレスを持つことがで

きます。したがって、アドレス 192.168.33.77 の IP アドレス フィルタ属性は複数回使用できません。ただし、IP アドレスが異なるのであれば（たとえば 192.168.33.78）、IP アドレス フィルタ属性を 2 回使用できます。

uSeg EPG での VM のフィルタリングの方法

複数の属性を持つ uSeg EPG を設定することができます。ただし、VM が所属できるのは 1 つの uSeg EPG だけです。VM がテナントの複数の uSeg EPG に一致する属性を持っている場合には、Cisco APIC はフィルタリング規則に基づいて VM を uSeg EPG に配置します。

属性を定義する方法に応じて、次のような、さまざまなフィルタリング規則を使用できます:

- **任意の属性に一致する**—任意の属性との照合を行えます。Cisco APIC は、VM がどの uSeg に参加する を決定するために、属性間のデフォルトの優先順位に従います。

  詳細については、このガイドの任意の属性に一致した場合の VM フィルタ リング （7 ページ）を参照してください。

- **すべての属性に一致する** —uSeg EPG 用に定義された VM ベースのすべての属性との照合を行えます。複数のネットワーク ベースの属性をすべて照合することはできません。

  詳細については、このガイドのすべての属性に一致するときに VM をフィルタリング （10 ページ）を参照してください。

- **単純な、またはブロック文を使用する** — 複数の属性をフィルタ リングする複数の文を作成することができます。またはブロック構造の、またはネストした文を作成して、正確なフィルタリングを行うルールを作成できます。

  詳細については、このガイドのシンプル ステートメントまたはブロック ステートメントを使用する場合の VM フィルタ （10 ページ）を参照してください。

- **既存のルールをオーバーライドする** — : uSeg EPG を作成する際には、優先順位を設定して、他のルールをオーバーライドできます。任意の属性に一致するか、すべての属性に一致したときの優先順位を設定できます。テナントの EPG 全体での同順位を避けるために、一致の優先順位を設定する必要があります。すべての属性に一致させることにして、一致の優先順位を設定しないこともできます。ただし、そのような場合、同じ属性を持つ uSeg EPG があると、VM が任意の uSeg EPG に一致することになります。

  詳細については、このガイドのEPG 一致の優先順位を使用するときの VM フィルタ リング （11 ページ）を参照してください。

任意の属性に一致した場合の VM フィルタ リング

uSeg EPG のために定義された属性への一致が、デフォルト設定です。

複数の属性があり、任意のものに一致する場合、Cisco APIC は、任意の属性に一致した VM のフィルタリングを行います。VM がテナント内の他の EPG に一致した場合には、属性の優先順位に基づいて uSeg EPG に入れます。

属性の優先順位のルールが適用される方法

次の表に、uSeg EPG に指定できる属性のリストを示します。

属性	タイプ	優先順位	例
MAC	ネットワーク	1- Cisco ACI Virtual Edge/Cisco AVS/Microsoft Hyper-V Virtual Switch 2 - VMware VDS	5c:01:23:ab:cd:ef
IP	ネットワーク	1 - VMware VDS 2- Cisco ACI Virtual Edge/Cisco AVS/Microsoft Hyper-V Virtual Switch	192.168.33.77 10.1.0.0/16
VNic Dn（vNIC ドメイン名）	VM	3	a1:23:45:67:89:0b
VM ID	VM	4	VM-598
VM Name	VM	5	HR_VDI_VM1
ハイパーバイザ ID	VM	6	ホスト - 25
VMM ドメイン	VM	7	AVS-SJC-DC1
データセンター	VM	8	SJC-DC1
カスタム属性	VM	9	SG_DMZ
オペレーティングシステム	VM	10	Windows 2008。
タグ (Cisco ACI Virtual Edge、Cisco AVS、および VMware VDS のみ)	VM	11	Linux

属性	タイプ	優先順位	例
VM のフォルダ (Cisco ACI Virtual Edge、Cisco AVS、および VMware VDS のみ) （注） VM フォルダ属性がベータ試験のためだけの機能です。実稼働環境には展開しないでください。この機能の詳細については Cisco にお問い合わせください。	VM	12	VM_Folder_1

（注） MAC ベースの属性と IP ベースの属性の優先順位は VMware VDS と Cisco ACI Virtual Edge、および Microsoft Hyper-V の仮想スイッチでは異なっています。

優先順位のルールの適用方法についての例

同じ VMと一致する属性を含む 4 つの uSeg EPG があり、それぞれの uSeg EPG は異なるネットワークまたはVM属性を持つものとします。オペレーティング システム、ハイパーバイザ ID、IP、MAC アドレス フィルタです。

Cisco AVS と Microsoft Hyper-V 仮想スイッチのための規則は、MAC、IP、ハイパーバイザ ID、およびオペレーティング システムの順に適用されます。ルールは MAC に適用され、後続のルールはスキップされます。ただし、MAC 属性を持つ uSeg EPG が削除された場合、ルールは IP アドレス フィルタに適用され、後続のルールはスキップされます（他の属性も同様です）。

VMware VDS のルールは、IP アドレス フィルタ、MAC アドレス フィルタ、ハイパーバイザ ID、オペレーティング システムの順序で適用されます。ルールは IP に適用され、後続のルールはスキップされます。ただし、IP 属性を持つ uSeg EPG が削除された場合、ルールは MAC に適用され、後続のルールはスキップされます（他の属性も同様です）。

別のケースとして、同じ VM を含む uSeg EPG があり、それぞれの uSeg EPG には VMM ドメイン、データセンター、カスタム属性および VNic Dn という異なる VM 属性があるとします。

ルールは VNic Dn に適用され、後続のルールはスキップされます。ただし、VNic Dn 属性を持つ uSeg EPG が削除された場合、ルールは VMM ドメインに適用され、後続のルールはスキップされます（他の属性も同様です）。

すべての属性に一致するときに VM をフィルタリング

uSeg EPG では、定義されているすべての VM ベースの属性に一致することを条件としたフィルタ処理を行えます。これは、APIC GUI のドロップダウンリストから **Match All** を選択するか、NX-OS CLI または REST API で一致条件を指定することによって行えます。

すべての属性を一致させる場合、uSeg EPG のために定義されているすべての属性に一致しない限り、Cisco APIC は VM を uSeg EPG に配置しません。

たとえば、ハイパーバイザが存在するハイパーバイザ識別子は host-25 であり、VM 名には「vm」が含まれており、そしてオペレーティング システムは Linux であるという属性を持つ uSeg EPG があるとします。Cisco APIC は、ハイパーバイザが host-25 であり、VM 名に「vm」が含まれており、そしてオペレーティング システム Linux である VM だけを uSeg EPG に配置します。最初の 2 つの属性が一致していても、オペレーティング システムが Microsoft である VM は uSeg EPG に配置しません。

（注） すべての属性の一致では、VMベースの属性のみをサポートします。ネットワーク ベースの属性では、[Match All] を選択することはできません。

すべての VM ベースの属性を一致させる場合には、uSeg EPG を作成する際に、EPG の一致の優先順位を設定しておくとよいでしょう。これにより、どの uSeg EPG が他の uSeg Epg をオーバーライドする必要があるかを決定できます。ただし、EPG の一致の優先順位では、任意の属性またはすべての属性のどちらにするかを設定できます。詳細については、このガイドのEPG 一致の優先順位を使用するときの VM フィルタ リング （11 ページ）を参照してください。

（注） Microsoft Hyper-V の仮想スイッチを使用していて、より新しいリリースから APIC リリース 2.3(1) へダウン グレードする必要がある場合には、まず [Match All] フィルタで設定された uSegs を削除する必要があります。APIC リリース 3.0(1) 以降では、Microsoft での [Match All] フィルタがサポートされています。

シンプル ステートメントまたはブロック ステートメントを使用する場合の VM フィルタ

uSeg EPG の属性を定義するときは、シンプル ステートメントまたはブロック ステートメントで複数の属性を定義できます。単純文とブロック ステートメントを組み合わせて、複雑な属性フィルタを作成することができます。

シンプルなステートメントには単一の属性が含まれています。uSeg EPG ごとに、必要な数だけシンプルなステートメントを作成できます。すべての属性またはすべての属性に一致させることができます。

ブロック ステートメントには、階層内の異なるレベルに複数の属性が含まれています。ブロック ステートメント内には 2 つのサブレベルしか存在できません。ブロック ステートメントの各レベルの任意の属性またはすべての属性を一致させることができます。

（注） ネットワーク ベースの属性をブロック ステートメントのサブレベルに入れることはできません。ただし、ネットワーク ベースの属性がブロック ステートメントの最上位にある場合は、ネットワーク ベースの属性のサブレベルを作成できます。

ブロック ステートメントがある場合、Cisco APIC は最初に最上位で定義された属性をフィルタリングします。次に、次に高いレベルをフィルタリングし、その次に高いレベルをフィルタリングします。

APIC GUI、NX-OS CLI、および REST API でシンプル ステートメントとブロック ステートメントを作成できます。

ブロック ステートメントの使用例

いくつかの VMをuSeg EPG に入れて、Linux をアップデートすることができます。VM は単一のデータセンター内にありますが、更新を 2 つの VMM ドメイン内の VM に限定する必要があります。ブロック ステートメントを使用して、それらの VM のフィルタリングを設定できます。

Linux を実行し、単一のデータセンターにある VM をフィルタリングするので、2 つのシンプル ステートメントを作成します。1 つは Linux の値を持つオペレーティング システム属性用で、もう 1 つは [datacenter3] の値を持つ属性データセンター用です。これらのステートメントでは、Linux を実行し、[datacenter3] に属しているテナント内のすべての VM をキャプチャしたいので、[Match All] を選択します。

ただし、Linux を実行し、[datacenter3] に属している VM では、VMM ドメイン mininet2 または mininet4 にのみ属する VM を取得する必要があります。2 つのシンプル ステートメントのサブレベルとしてブロック ステートメントを作成します。ブロック ステートメントには、2つの属性、1 つは属性 VMM ドメインの値 (mininet 2 の値)、1 つは属性 VMM ドメインの値 (mininet 4 の値) が含まれます。いずれかの VMM ドメインにある VM をキャプチャする必要があるため、ブロック ステートメントに [match any] を選択します。

属性を定義すると、Cisco APIC は最初に Linux を実行し、 [datacenter3] にある VM をフィルタリングします。次に、それらの VM の中から、mininet2 または mininet4 のいずれかに属する VM を検索します。

EPG 一致の優先順位を使用するときの VM フィルタ リング

EPG一致の優先順位を使用すると、VMベースの属性をフィルタリングするときに、uSeg EPG のデフォルト優先順位ルールをオーバーライドすることができます。これは、GUI、NX-OS CLI または REST API で uSeg EPG を作成する時に設定します。

EPG一致の優先順位は、任意の属性またはすべての属性のマッチングを行うときにはオプションです。ただし、すべての属性のマッチングを行い、複数の属性でフィルタリングを行う場

合、優先順位を設定すると、Cisco APIC は uSeg EPG 間の結合を切ることができるようになります。

（注） ネットワーク ベースの属性をフィルタリングする場合は、EPG 一致の優先順位を使用することはできません。これを行うと、エラー メッセージが表示されます。

EPG 一致の優先順位を設定するときには、uSeg EPG に整数値を与えます。数値が大きいほど優先順位が高くなります。優先順位は、ほぼ 43 億 (2^{32}) のレベルに設定できます。デフォルトでは 0 で、優先順位が設定されていないことを示します。

たとえば、それぞれ 1 つだけの属性を持つ 2 つの uSeg EPG があるとします。一方は属性として VM 名を持ち、もう一方はオペレーティング システムを持ちます。ある VM が両方の uSeg EPG と一致する可能性があるとします。デフォルトでは、Cisco APIC はその VM を VM 名属性を持つ uSeg EPG に割り当てます。この属性は、オペレーティング システム属性よりも高い優先順位を持つからです。

ただし、オペレーティング システム属性を持つ uSeg EPG に優先順位 10 を与え、VM 名属性を持つ uSeg EPG に優先順位 7 を与えると、 Cisco APIC は両方の uSeg EPG にマッチした VM をオペレーティング システム属性を持つ uSeg EPG に与えます。

オペレータの優先順位

テナント内で uSeg EPG の属性に基づいてフィルタリング ルールを適用するほかに、Cisco APIC では演算子タイプに基づいて VM ベースの属性内でフィルタリング ルールを適用します。

VM ベースの属性でマイクロセグメントを設定する際、Contains、Ends With、Equals、Starts With の 4 つの演算子のうち 1 つを選択します。各演算子は、特定の属性の文字列または値の一致を指定します。

たとえば、VM 名属性でマイクロセグメントを作成し、「HR_VM」で始まる名前の VM、または名前のどこかに「HR」を含む VM をフィルタリングできます。または、特定の VM に対してマイクロセグメントを設定し、名前「HR_VM_01」をフィルタリングできます。

演算子の優先順位のルールの適用方法

テナント内の特定の VM 属性の演算子により、マイクロセグメントに VM ベース属性を適用する順序が決まります。また、同じ属性および重複する値を共有するマイクロセグメント グループ内での、演算子の優先順位も決定されます。次の表に、Cisco AVS と Microsoft Hyper-V Virtual Switch のデフォルトの演算子の優先順位 Cisco ACI Virtual Edge を示します。

演算子タイプ	優先順位
Equals	1
記載内容	2
Starts With	3

演算子タイプ	優先順位
Ends With	4

優先順位のルールの適用方法についての例

データセンター クラスタで同じテナントの下に VM_01_HR_DEV、VM_01_HR_TEST および VM_01_HR_PROD という 3 つの人事 VM マシンがあります。VM 名属性に基づいて、2 つのマイクロセグメント化された EPG を作成しました。

Criterion	CONTAIN-HR マイクロセグメント	HR-VM-01-PROD マイクロセグメント
属性タイプ。	VM Name	VM Name
演算子タイプ	記載内容	Equals
値	VM_01_HR	VM_01_HR_PROD

演算子タイプ Equals は演算子タイプ Contains よりも優先順位が高いため、値 VM_01_HR の前に値 VM_01_HR_PROD が一致します。したがって、VM 名は両方のマイクロセグメントに当てはまりますが、完全な条件一致であるため、および演算子 Equals は演算子 Contains よりも優先順位が高いため、VM_01_HR_PROD という名前の VM はマイクロセグメント HR-VM-01-PROD に配置されます。他の 2 つの VM は、マイクロセグメント CONTAIN-HR に配置されます。

Cisco ACI でマイクロセグメンテーションを使用するシナリオ

ここでは、ネットワークでマイクロセグメンテーションが役立つ状況の例を示します。

単一アプリケーション EPG 内の VM における Cisco ACI でのマイクロセグメンテーションの使用

Cisco ACI でのマイクロセグメンテーションを使用すると、新しい uSeg EPG を作成して単一アプリケーション EPG の VM を含めることができます。デフォルトでは、アプリケーション EPG 内の各 VM は相互に通信できます。ただし、VMS が強制モードになっていて、uSeg EPG 間にコントラクトがない場合は VM グループ間での通信を防止することができます。

EPG 内の VM 間の通信を制御する EPG 間分離ノブの詳細については、VMware VDS または Microsoft Hyper-V 仮想スイッチの EPG 分離 を参照してください。

例：同じアプリケーション EPG 内の VM をマイクロセグメント化された EPG に配置

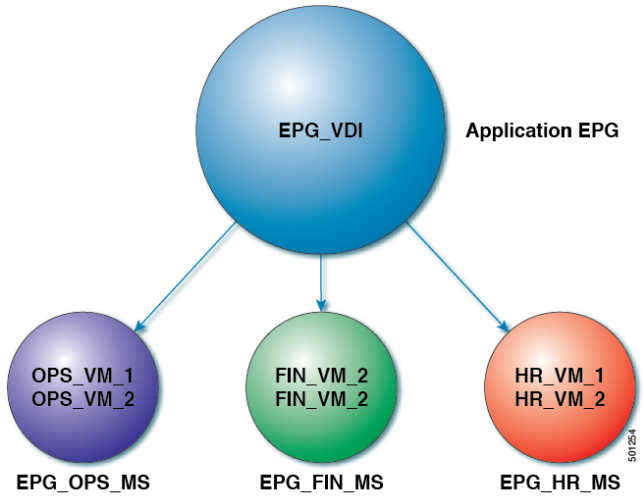
企業が、人事、経理、および業務の各部門に仮想デスクトップインフラストラクチャ（VDI）を導入します。VDI 仮想デスクトップ VM は、EPG_VDI と呼ばれる単一アプリケーション EPG の一部であり、アプリケーション EPG の他の部分とアクセス要件は同じです。

EPG-VDI がインターネット リソースと内部リソースにアクセスできるようにサービス コントラクトが作成されます。ただし、それと同時に、各グループ（人事、経理、および業務）は同じアプリケーション EPG（EPG_VDI）に属していますが、企業は各 VM グループが他のグループにアクセスできないようにする必要があります。

この要件を満たすには、アプリケーション EPG_VDI 内の VM の名前を確認するフィルタを Cisco APIC で作成します。値「HR_VM」を使用してフィルタを作成すると、Cisco APIC はすべての人事 VM 用の uSeg EPG（マイクロセグメント）を作成します。一致する VM を 1 つの EPG にグループ化したいのですが、Cisco APIC はテナント内のすべての EPG 内で一致する値を検索します。したがって、VM を作成する際には、テナント内で一意な名前を選択することを推奨します。

同様に、キーワードとして経理仮想デスクトップ用の「FIN_VMs」および業務仮想デスクトップ用の「OPS_VMs」を使用してフィルタを作成できます。これらの uSeg EPG は、Cisco APIC ポリシー モデル内の新しい EPG として表されます。その後、各 VM グループは同じアプリケーション EPG に属しているのですが、コントラクトとフィルタを適用して VM グループ間のアクセスを制御できます。

図 *1* : 単一アプリケーション *EPG* の *VM* における *Cisco ACI* でのマイクロセグメンテーション



上の図では、人事、経理、および業務の各グループのすべての仮想デスクトップ VM は、アプリケーション EPG（EPG_VDI）から新しい uSeg EPG（EPG_OPS_MS、EP_FIN_MS、および EPG_HR_MS）に移動しています。各 uSeg EPG は、VM の名前の主要な部分に一致する値を使用した属性タイプ VM 名を持っています。EPG_OPS_MS は値 OPS_VM を持っているため、名前に OPS_VM が含まれるテナント内のすべての VM が EPG_OPS_MS に含まれるようになります。その他の uSeg EPG も対応する値を持っており、一致する名前を持つテナント内の VM が uSeg EPG に移動されます。

別のアプリケーション EPG 内の VM における Cisco ACI でのマイクロセグメンテーションの使用

Cisco ACI でマイクロセグメンテーションを設定して、異なるマイクロセグメンテーション EPG に属する VM を新しい uSeg EPG に配置できます。これを実行することで、異なるアプリケーション EPG に属するものの、特定の特性を共有する VM にポリシーを適用できます。

例：異なるアプリケーション EPG に属する VM を新しい uSeg EPG に配置する

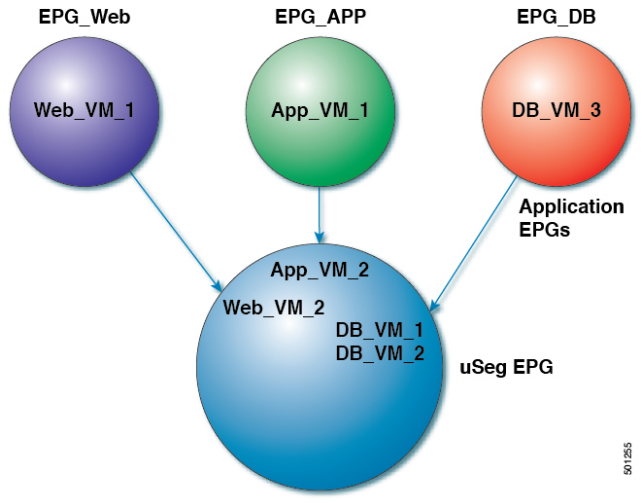
企業で、3 層 Web アプリケーションを導入するとします。アプリケーションは、異なるオペレーティング システムおよび同じオペレーティング システムの異なるバージョンを実行する VM 上に構築されます。たとえば、VM は Linux、Windows 2008 および Windows 2008 R2 を実行する可能性があります。アプリケーションは分散型であり、企業は VM を 3 つの異なる EPG（EPG_Web、EPG_App、EPG_DB）に分割しました。

Windows 2008 オペレーティング システムの脆弱性のため、企業のセキュリティ チームは VM が危険にさらされた場合に備えて、Windows 2008 を実行する VM を隔離することを決定しました。セキュリティ チームはさらに、すべての Windows 2008 VM を Windows 2012 にアップグレードすることにしました。また、すべての EPG ですべての本番 VM をマイクロセグメント化し、これらの VM への外部接続を制限したいと考えています。

この要件を満たすために、Cisco APIC で uSeg EPG を設定できます。属性はオペレーティング システムで、属性の値は Windows 2008 です。

これで、Windows 2008 を実行する VM を隔離し、Windows 2012 にアップグレードできます。アップグレードが完了すると、VM は、Windows 2008 を実行する VM に作成した uSeg EPG の一部ではなくなります。この変更は、Cisco APIC に動的に反映され、それらの仮想マシンは元の EPG に戻ります。

図 *2 :* 異なるアプリケーション *EPG* の *Cisco ACI* でのマイクロセグメンテーション



EPG Windows with attribute type **Operating System** and value **Windows**

上の図では、新しい uSeg EPG EPG_Windows は、属性タイプ「オペレーティング システム」と値「Windows」を持ちます。VM App_VM_2、DB_VM_1、DB_VM_2 および Web_VM_2 はオペレーティング システムとして Windows を実行するため、新しい uSeg EPG EPG_Windows に移動されました。ただし、VM App_VM_1、DB_VM_3 および Web_VM_1 は Linux を実行するため、それらのアプリケーション EPG に残ります。

ネットワーク ベースの属性を使用したマイクロセグメンテーションの使用

Cisco APIC を使用して Cisco ACI でのマイクロセグメンテーションを設定し、ネットワークベースの属性、MAC アドレス、または 1 つ以上の IP アドレスを使用した新しい uSeg EPG を作成できます。ネットワーク ベースの属性を使用して Cisco ACI でのマイクロセグメンテーションを設定し、単一のアプリケーション EPG 内の VM またはさまざまな EPG 内の VM を分離できます。

IP ベースの属性の使用

IP ベースのフィルタを使用して、単一 IP アドレス、サブネット、または多様な非連続 IP アドレスを分離できます。単一マイクロセグメントでの複数の IP アドレスの分離は、名前で VM を指定するより便利な場合があります。ファイアウォールの使用と同様に、セキュリティゾーンを作成するための迅速かつ簡単な方法として、IP アドレスに基づいて VM を分離できます。

MAC ベースの属性の使用

MAC ベースのフィルタを使用して、単一 MAC アドレスまたは複数の MAC アドレスを分離できます。ネットワークに不正なトラフィックを送信するサーバがある場合に、これを行うことができます。MAC ベースのフィルタを使用してマイクロセグメントを作成することにより、そのサーバを分離できます。

Cisco ACI でのマイクロセグメンテーションの設定

ここでは、Cisco APIC GUI および NX-OS スタイルの CLI を使用して、Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、または Microsoft Hyper-V 仮想スイッチによるマイクロセグメンテーションを設定する手順を説明します。この手順は、ネットワークの特定のニーズに合わせて調整できます。

（注） VMware vCenter のドメイン プロファイルで VXLAN ロード バランシングが有効の場合、Cisco ACI によるマイクロセグメンテーションはドメインでサポートされません。

Cisco ACI でのマイクロセグメンテーションを設定するための前提条件

Cisco ACI for Cisco ACI Virtual Edge、Cisco AVS、VMware VDS または Microsoft Hyper-V 仮想スイッチでマイクロセグメンテーションを設定する前に、以下の前提条件を満たす必要があります。

- マイクロセグメンテーションのハードウェア要件を満たしていることを確認します:

表 *1:* マイクロセグメンテーションのハードウェア サポート

	Cisco Nexus 9332PQ、9372PX、9372TX、9396PX、9396TX、93120TX、および 93128TX スイッチ	**Cisco Nexus 9372PX-E および 9372TX-E スイッチ**	**Cisco Nexus 93108TC-EX、93180YC-EX、および 93180LC-EX スイッチ**	**Cisco Nexus 93180YC-FX、93108TC-FX、および 9348GC-FXP スイッチ**
Cisco ACI Virtual Edge uSeg (VM、IP、MAC)	○	○	○	○
Microsoft uSeg (VM、IP、MAC)	○	○	○	○
VDS uSeg (VM、IP、MAC)	なし	なし	○	○
ベアメタル (IP-EPG)	なし	○	○	○
ベアメタル (MAC-EPG)	該当なし	○	○	○

（注） Cisco AVS マイクロセグメンテーションがすべてのハードウェアで動作すること。

- uSeg EPG を作成するときに使用するフィルタで使用できる名前を持つ VM がすでに存在している必要があります。

  使用できる名前を持つVMが存在しない場合、手順を進めてuSeg EPGを作成し、その後、フィルタで使用できるVM名に変更できます。Cisco APICは、自動的にそれらのVMを新しいuSeg EPGに含めます。

- すでにアプリケーション EPG が存在している必要があります。
- 対応するブリッジ ドメインには、IP サブネットが定義されている必要があります。そうしないと、VM は通信できません。
- 独自の属性、名前、および値が選択済みである必要があります。

  前にシナリオで使用されている属性、名前、および値は、例として提供されているものです。

- コントラクトにEPGを関連付ける場合は、1つ以上の属性を使用してマイクロセグメントを作成する前にコントラクトを作成する必要があります。
- Cisco ACI Virtual Edge、Cisco AVS または VMware VDS があるときに VM カスタム属性を使用する場合は、その属性を VMware vSphere Web クライアントに追加する必要があります。Microsoft Hyper-V 仮想スイッチがあり、VM カスタム属性を使用する必要がある場合には、それを Microsoft SCVMM に追加する必要もあります。

  カスタム属性は、Cisco APIC でマイクロセグメンテーションを設定する前に、VMware vSphere Web クライアントまたは Microsoft SCVMM に追加することを推奨します。これにより、Cisco APIC GUI でマイクロセグメントを設定する際、ドロップダウンリストからカスタム属性を選択できるようになります。

  vSphere Web クライアントでカスタム属性を追加する手順については、VMware vSphere ESXi および vCenter Server のマニュアルを参照してください。SCVMM でカスタム属性を追加するための手順については、Microsoft のマニュアルを参照してください。
- Microsoft Hyper-V 仮想スイッチ ベースのマイクロセグメンテーションでは、次のいずれかが必要です:
  - SCVMM 2012 R2 ビルド 3.2.8145.0 またはそれ以降
  - SCVMM 2016 ビルド 4.0.1662.0 またはそれ以降

  これらのビルドには、「仮想マシン上の vNIC でのダイナミック VLAN の有効化」という機能が含まれています。この機能は Cisco SCVMM エージェントによって自動的に有効になり、ACI でのマイクロセグメンテーションを利用する仮想マシンのライブ マイグレーションを可能にします。詳細については、Microsoft のマニュアルを参照してください:https://support.microsoft.com
- VMware VDS またはベアメタル サーバがある場合は場合に、VRF ポリシーの適用方向が [ingress] になっていることを確認します。そうしないとエラーが発生します。
- VMware VDS がある場合には、ブレードスイッチで PVLAN がセットアップされていることを確認します。また、VLAN の使用率が一貫したものになるように、静的 VLAN が展開されていることを確認します。

Cisco ACI でのマイクロセグメンテーションを設定するためのワークフロー

ここでは、Cisco ACI でのマイクロセグメンテーションを設定するために実行する必要があるタスクの概要を示します。

1	uSeg EPG の作成：新しい uSeg EPG に名前とブリッジ ドメインを指定し、EPG にネットワーク ベースの属性か VM ベースの属性を選択します。 （注） VMware VDS の場合、アプリケーション EPG が使用する新しい uSeg EPG のものと同じブリッジ ドメインを選択する必要があります。そうしないと、VDS uSeg が VM 属性に一致しない、または VM が uSeg EPG に配置されることになります。

2	新しい uSeg EPG を VMM ドメイン プロファイルに関連付けます。アプリケーション EPG で使用されている同じ VMM ドメイン プロファイルと関連付ける必要があります。
3	uSeg EPG の属性を設定します。
4	エンドポイントが アプライアンス EPG から uSeg EPG に移動したことを確認します。

Cisco ACI でのマイクロセグメンテーションの設定 （16 ページ）という項に記載されている手順に従ってください。

GUI を使用して、Cisco ACI とともにマイクロセグメンテーションを設定する

Cisco ACI での Cisco APIC のマイクロセグメンテーションの設定は、異なる複数のアプリケーション EPG または同一の EPG に属する VM を新しい uSeg EPG に配置するために使用できます。タスクは基本的に、Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、および Microsoft Hyper-V 仮想スイッチで同じですが、手順の若干の違いを次に示します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Tenants** を選択し、マイクロセグメントを作成するテナントを選択します。

ステップ 3 テナントのナビゲーション ウィンドウで、テナント フォルダ、**Application Profiles** フォルダ、および ***profile*** フォルダを展開します。

ステップ 4 次のいずれかの操作を実行します。

- Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチを使用している場合には、次の手順をスキップし、ステップ 5 に進みます。
- VMware VDS を使用している場合は、次の手順を実行します。

a) **Application EPGs** フォルダと、アプリケーション EPG のフォルダを展開します。

b) フォルダ **Domains (VMs and Bare-Metals)** を右クリックします。

c) **Add VMM Domain Association** ダイアログボックスで、VMM ドメインを選択してから、**Allow Micro-Segmentation** チェック ボックスをオンにします。

VMware VDS を使用している場合は、必要なすべてのパラメータも設定する必要があります。

d) [Submit] をクリックします。

ステップ 5 テナントのナビゲーション ウィンドウで、**uSeg EPGs** フォルダを右クリックし、**Create Useg EPG** を選択します。

ステップ 6 **Create USeg EPG Step 1 > Identity** ダイアログボックスで、次の手順に従って、VM のグループのための uSeg EPG の作成を開始します:

a) **Name** フィールドに名前を入力します。

新しい uSeg ベースの EPG では、マイクロセグメントであることを示す名前を選択することを推奨します。

b) [intra-EPG isolation] フィールドで **enforced** または **unenforced** を選択します。

enforced を選択した場合は、Cisco ACI によってこの uSeg EPG 内のエンドポイント デバイス間のすべての通信が防止されます。

c) **Bridge Domain** エリアで、ドロップダウン リストからブリッジ ドメインを選択します。

（注） VMware VDS の場合、アプリケーション EPG が使用しているのと同じブリッジ ドメインを選択する必要があります。そうしないと、VM 属性が一致しないため、VDS uSeg は VM を uSeg EPG に入れません。

d) (オプション) **Epg Match Precedence** フィールドで、他の VM ベース属性 uSeg EPG との間での優先順位を設定する整数を選択して、デフォルトのルールをオーバーライドします。

整数の値が大きいほど、優先順位は高くなります。

e) [Next] をクリックします。

ステップ 7 **Create USeg EPG Step 2 > Domains** で、uSeg EPG を VMM ドメインに関連付けるため、次の手順を実行します。

a) ダイアログボックスの右側にある、+ (プラス) のアイコンをクリックします。

b) **Domain Profile** ドロップダウン リストから、プロファイルを選択します。

Cisco ACI Virtual Edge,、Cisco AVS、または VMware VDS がある場合には、VMware ドメインを選択します。Microsoft Hyper-V 仮想スイッチがある場合には、Microsoft ドメインを選択します。

（注） アプリケーション EPG が使用しているのと同じドメインを選択する必要があります。

c) **Deploy Immediacy** ドロップダウンリストでデフォルトの **On Demand** を選択するのは、Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチがある場合です。VMware VDS がある場合には、**Immediate** を選択します。

d) **Resolution Immediacy** ドロップダウンリストでは、デフォルトの **Immediate** のままにします。

e) **Encap Mode** ドロップダウンリストでは、デフォルトの **Auto** にままにします。

f) **Port Encap (or Secondary VLAN for Micro-Seg)** フィールドでは、VMware VDS を使用している場合にはデフォルトの値のままにします。Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチを使用している場合には、デフォルト値のままにします。

g) Cisco ACI Virtual Edge がある場合には、**Switching Mode** ドロップダウンリストで、モードを選択します。

AVE は、Cisco ACI Virtual Edge を通して uSeg EPG を切り替える場合に選択します。VMware VDS を通して uSeg EPG を切り替える場合には **native** を選択します。

h) **Update** をクリックし、**Finish** をクリックします。

ステップ 8 テナントのナビゲーション ページで、作成した uSeg EPG のフォルダを開きます。

ステップ 9 **uSeg Attributes** フォルダをクリックします。
[uSeg Attributes] 作業ウィンドウが表示されます。ここでは、uSeg EPG に入れる VM をフィルタリングするための属性を設定できます。

ステップ 10 (オプション) VM ベースの属性用いてフィルタリングを行う場合には、**uSeg Attributes** 作業ウィンドウで、**Match Any** または **Match All** を選択します。

一致機能を使えば、uSeg EPG の VM をフィルタリングするために、複数の属性を使用できます。デフォルトは **Match Any** です。すべての特徴を一致させる機能がサポートされているのは、VM ベースの属性だけです。『*Cisco ACI Virtualization Guide*』のマイクロセグメントの章に記されている、「いずれかの属性に一致したときに VM のフィルタリング」と「すべての属性に一致したときに VM のフィルタリング」について説明したセクションを参照してください。

ステップ 11 + または **+(** アイコンをクリックして、フィルタリングのステートメントを追加します。

+ アイコンを使えば、1 つの属性に対するフィルタを作成する、シンプルなステートメントを作成できます。複数の属性に対するフィルタリングを行うには、このシンプルなステートメントを順次追加します。**+(** アイコンを使えば、ブロックの、または入れ子になったステートメントを作成できます。これにより、階層構造になった属性を設定して、最上位の属性で最初にフィルタリングし、その後で下位の属性でフィルタリングすることができます。詳細については、このガイドのシンプル ステートメントまたはブロック ステートメントを使用する場合の VM フィルタ （10 ページ）のセクションを参照してください。

ステップ 12 フィルタを設定するには、次のいずれかの一連の手順を実行します。

項目	結果
IP ベースの属性	1. **Select a type...** ドロップダウンリストから、**IP** を選択します。 2. **Use EPG Subnet?** ドロップダウンリストで、**Yes** または **No** を選択します。 **Yes** を選択すると、前に定義したサブネットを IP 属性のフィルタとして使用することができます。 **No** を選択した場合には、**Use EPG Subnet?** ドロップダウンリストの右側にあるフィールドに、VM の IP アドレス、または適切なサブネットマスクを持つサブネットを入力します。 3. （オプション）ステップ a から c を繰り返して、2 番目の IP アドレス フィルタを作成します。 マイクロセグメントに不連続な IP アドレスを含めるために、2 番目の IP アドレス フィルタを作成するのが望ましい場合もあるでしょう。 4. [Submit] をクリックします。
MAC ベースの属性	1. **Select a type...** ドロップダウンリストから、**MAC** を選択します。 2. 右側のフィールドに VM の MAC アドレスを入力します。

項目	結果
	3. [Submit] をクリックします。
VM ベースのカスタム属性	**1.** **Select a type...** ドロップダウンリストから、**VM - Custom Attribute** を選択します。 **2.** **Select a type...** ドロップダウンリストの右側にあるフィールドの検索アイコンをクリックします。 **3.** **Select Custom Attribute** ダイアログボックスで、**Controller** ドロップダウン リストからコントローラを選択します。 **4.** **VM** ドロップダウンリストから VM を選択します。 **5.** **Attribute Name** ドロップダウンリストで名前を選択し、**Select** をクリックします。 **6.** 演算子ドロップダウンリストから、演算子を選択し、ロップダウンリストの右側の フィールドに値を入力します。 **7.** [Submit] をクリックします。
VM ベースのタグ属性 (Cisco ACI Virtual Edge, Cisco AVS および VMware VDS のみ)	**1.** **Select a type...** ドロップダウンリストから、**VM - Tag** を選択します。 **2.** **Category** フィールドの隣にある虫眼鏡アイコンをクリックし、**Select VM Category** ダイアログボックスで、**Category Name** ドロップダウンリストを選択し、**Select** をクリックします。 入力したカテゴリは、VMware vCenter で以前にタグに割り当てたものと同じである必要があります。 **3.** 演算子のドロップダウンリストから適切な演算子を選択します、 **4.** 右側のフィールドの隣にある虫眼鏡アイコンをクリックし、**Select VM Tag** ダイアログボックスで、**Tag Name** ドロップダウンリストからタグを選択して、**Select** をクリックします。 **5.** [Submit] をクリックします。
その他の VM ベースの属性	**1.** **Select a type...** ドロップダウンリストから、VM の属性を選択します。 **2.** 演算子のドロップダウンリストから適切な演算子を選択します、 **3.** 次のいずれかの手順を実行します。 • **Datacenter** VM ベース属性を選択した場合、演算子のドロップダウンリストの右側のフィールドに、データセンターの名前を入力します。 • それ以外の VM ベース属性を選択した場合、演算子のドロップダウンリストの右側にあるフィールドの検索アイコンをクリックし

項目	結果
	て、**Select VM Identifier** ダイアログボックスから属性に適切な値を入力し、**Select** をクリックします。 **4.** [Submit] をクリックします。

ステップ 13 + または +(アイコンをクリックして、uSeg EPG に付加的な属性を追加します。

ステップ 14 ステップ 2 および 13 の操作を繰り返して、追加の uSeg EPG を作成します。

次のタスク

uSeg EPG が正しく作成されたことを確認します。

VM ベースの属性を設定する場合は、次の手順を実行します。

1. Cisco APIC の [Navigation] ペインで、新しいマイクロセグメントをクリックします。
2. 作業ウィンドウで、**Operational** タブをクリックし、**Client End-Points** タブがアクティブであることを確認します。
3. 作業ウィンドウで、アプリケーション EPG から移行する VM が新しい uSeg ベースの EPG のエンドポイントとして表示されていることを確認します。

IP または MAC ベースの属性を設定する場合は、トラフィックが、新しいマイクロセグメントに配置した VM で動作していることを確認します。

NX-OS スタイル CLI を使用した Cisco ACI でのマイクロセグメンテーションの設定

このセクションでは、アプリケーション EPG 内で VM ベースの属性を使用して Cisco ACI for Cisco ACI Virtual Edge、Cisco AVS, VMware VDS、または Microsoft Hyper-V でマイクロセグメンテーションを設定する方法について説明します。

手順

ステップ 1 CLI で、コンフィギュレーション モードに入ります。

例：

```
apic1# configure
apic1(config)#
```

ステップ 2 USeg EPG を作成します。

例：

この例は、アプリケーション EPG のためのものです。

（注） 次の例のマイクロセグメンテーションを許可するコマンドが VMware VDS にのみ必要です。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-baseEPG1
apic1(config-tenant-app-epg)# bridge-domain member cli-bd1
apic1(config-tenant-app-epg)# vmware-domain member cli-vmm1 allow-micro-segmentation
```

例：

（オプション）この例の設定は、uSeg EPG の EPG の優先順位と一致します。:

```
apic1(config)# tenant Coke
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# match-precedence 10
```

例：

この例では、属性 VM 名に基づいてフィルタを使用します。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# attribute-logical-expression 'vm-name contains <cos1>'
```

例：

この例では、IP アドレスに基づいてフィルタを使用します。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# attribute-logical-expression 'ip equals <FF:FF:FF:FF:FF:FF>'
```

例：

この例では、MAC アドレスに基づいてフィルタを使用します。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# attribute-logical-expression 'mac equals
<FF-FF-FF-FF-FF-FF>'
```

例：

この例では、演算子 AND を使用してすべての属性を一致させるか、演算子 OR を使用してすべての属性を一致させます。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# attribute-logical-expression 'hv equals host-123 OR
(guest-os equals "Ubuntu Linux (64-bit)" AND domain contains fex)'
```

例：

この例では、属性 VM カスタム属性に基づいてフィルタを使用します。

```
apic1(config)# tenant cli-ten1
apic1(config-tenant)# application cli-a1
apic1(config-tenant-app)# epg cli-uepg1 type micro-segmented
apic1(config-tenant-app-uepg)# bridge-domain member cli-bd1
apic1(config-tenant-app-uepg)# attribute-logical-expression 'custom <Custom Attribute
Name> equals <Custom Attribute value>'
```

ステップ 3 (Cisco ACI Virtual Edge のみ）：uSeg EPG を Cisco ACI Virtual Edge VMM ドメインに接続し、スイッチングおよびカプセル化モードを指定します。

例：

```
vmware-domain member AVE-CISCO
    switching-mode AVE
    encap-mode vxlan
    exit
```

ステップ 4 USeg EPG の作成を確認します。

例：

次の例は、VM 名属性フィルタを持つ uSeg EPG のためのものです。

```
apic1(config-tenant-app-uepg)# show running-config
# Command: show running-config tenant cli-ten1 application cli-a1 epg cli-uepg1 type
micro-segmented # Time: Thu Oct 8 11:54:32 2015
  tenant cli-ten1
    application cli-a1
      epg cli-uepg1 type micro-segmented
        bridge-domain cli-bd1
        attribute-logical-expression 'vm-name contains cos1 force'
        {vmware-domain | microsoft-domain} member cli-vmm1
        exit
     exit
exit
```

REST API を使用した Cisco ACI でのマイクロセグメンテーションの設定

ここでは、REST API を使用して Cisco ACI for Cisco ACI Virtual Edge、Cisco AVS、VMware VDS、または Microsoft vSwitch でマイクロセグメンテーションを設定する方法について説明します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 `Https://apic-ip-address/api/node/mo/.xml.`*`apic-ip-address`*`/api/node/mo/.xml.` にポリシーをポストします。

例：

この例では、すべての属性と EPG 一致設定 1 と一致する状態で、「vm」を含む属性 VM 名と「CentOS」および「Linux」の値を含むオペレーティング システム属性を持つ uSeg EPG を設定します。

```
<fvAEPg name="Security" isAttrBasedEPg="yes" pcEnfPref="unenforced" status="">
      <fvRsBd tnFvBDName="BD1" />
      <fvRsDomAtt tDn="uni/vmmp-VMware/dom-mininet”/>
       <fvCrtrn name="default" match=“all” prec=“1”>
                  <fvVmAttr name="foo" type="vm-name" operator="contains" value="vm"/>
               <fvSCrtrn name="sub-def" match=“any”>
                        <fvVmAttr name="foo1" type="guest-os" operator="contains"
value="CentOS"/>
                        <fvVmAttr name="foo2" type="guest-os" operator="contains"
value="Linux"/>
                    </fvSCrtrn>
       </fvCrtrn>
 </fvAEPg>
```

例：

この例では、アプリケーション EPG のマイクロセグメンテーションが有効になっています。

```
<polUni>
  <fvTenant dn="uni/tn-User-T1" name="User-T1">
      <fvAp dn="uni/tn-User-T1/ap-Application-EPG" name="Application-EPG">
          <fvAEPg dn="uni/tn-User-T1/ap-Application-EPG/applicationEPG”
name=“applicationEPG” pcEnfPref="enforced” >
               <fvRsBd tnFvBDName="BD1" />
               <fvRsDomAtt tDn="uni/vmmp-VMware/dom-cli-vmm1" classPref=“useg”/>
           </fvAEPg>
        </fvAp>
   </fvTenant>
</polUni>
```

上記の例では、文字列 `<fvRsDomAtt tDn="uni/vmmp-VMware/dom-cli-vmm1" classPref=“useg”/>` は VMware VDS とのみ関連しており、 Cisco ACI Virtual Edge、Cisco AVS、または Microsoft Hyper-V 仮想スイッチとは関連していません。

例：

この例では、uSeg EPG を Cisco ACI Virtual Edge VMM ドメインにアタッチし、スイッチングモードを追加します。

```
<fvRsDomAtt resImedcy="immediate" instrImedcy="immediate" switchingMode="AVE"
encapMode="auto" tDn="uni/vmmp-VMware/dom-AVE-CISCO" primaryEncapInner=""
secondaryEncapInner=""/>
```