



ポリシーの設定

- [ポリシーの概要 \(1 ページ\)](#)
- [グループベースのアクセス コントロール ポリシー \(1 ページ\)](#)
- [IP ベースのアクセス コントロール ポリシー \(12 ページ\)](#)
- [アプリケーションポリシー \(19 ページ\)](#)
- [トラフィック コピー ポリシー \(51 ページ\)](#)
- [仮想ネットワーク \(55 ページ\)](#)

ポリシーの概要

Cisco DNA Center を使用すると、ネットワークの特定の側面（ネットワークアクセスなど）に対する組織のビジネス目標を反映したポリシーを作成できます。Cisco DNA Center は、ポリシー内で収集された情報を取得し、お使いのネットワークデバイスのさまざまなタイプ、メーカー、モデル、オペレーティングシステム、ロール、およびリソースの制約によって必要とされる、ネットワーク固有およびデバイス固有の設定に変換します。

Cisco DNA Center を使用して、仮想ネットワーク、アクセス コントロール ポリシー、トラフィック コピー ポリシー、およびアプリケーション ポリシーを作成できます。

グループベースのアクセス コントロール ポリシー

Cisco DNA Center は、次の 2 つの方法で Software-Defined Access を実装します。

- 仮想ネットワーク (VN) は、マクロレベルのセグメンテーションを提供します。たとえば、企業のネットワークから IoT デバイスを分離します。
- グループベースのポリシーは、マイクロレベルのセグメンテーションを提供します。たとえば、エンジニアリンググループと HR グループの間で許可または拒否するネットワークトラフィックのタイプを制御します。

グループベースのアクセス コントロール ポリシー メニューを使用すると、スケーラブルなグループアクセスポリシーを監視および管理できます。それらのポリシーには、次の利点があります。

- ネットワークの自動化とアシュアランスの利点を備えた、豊富なアイデンティティベースのアクセス制御機能。
- きめ細かいアクセス制御。
- スケーラブルグループは、すべての仮想ネットワークに適用されるため、ポリシー管理が簡素化されます。
- ポリシービューは、全体的なポリシー構造を理解し、必要なアクセスコントロールポリシーを作成または更新するのに役立ちます。
- さまざまなアプリケーションを切り替えてスケーラブルグループを管理し、保護される資産を定義する必要がなくなります。
- エンタープライズ全体のアクセスコントロールポリシーを展開するための拡張機能を提供します。
- アイデンティティまたはネットワーク アドミッション コントロール (NAC) アプリケーションが配置される前に、ランサムウェアなどの脅威のラテラルムーブメントを制限します。
- サードパーティのアイデンティティ アプリケーションを使用しているが、Cisco ISE に移行したいユーザに対して、Cisco Identity Services Engine (Cisco ISE) への簡単な移行パスを提供します。

Cisco DNA Center での IP プール、サイト、および仮想ネットワークの作成方法については、『[Cisco Digital Network Architecture Center ユーザガイド](#)』[英語]を参照してください。

Cisco DNA Center for Cisco ISE のインストールと設定の詳細については [Cisco Digital Network Architecture Center 設置ガイド](#) [英語]を参照してください。

Cisco ISE for Cisco DNA Center の設定の詳細については、[Cisco Identity Services Engine 管理者ガイド](#) [英語]を参照してください。

まず、スケーラブルなグループと契約を定義してから、アクセスコントロールポリシーを作成します。アクセスコントロールポリシーは、送信元スケーラブルグループから宛先スケーラブルグループに渡すことができるネットワークトラフィックを定義します。

- **スケーラブルグループ**：ユーザ、ネットワークデバイス、またはリソースを割り当てることができる分類カテゴリ。スケーラブルグループは、アクセスコントロールポリシーで使用されます。組織のネットワーク設定、アクセス要件、および制限に基づいて、スケーラブルグループを仮想ネットワークに関連付けることができます。
- **契約**：アクセス契約は、送信元と宛先のスケーラブルグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。つまり、契約はトラフィックフィルタの定義です。アクセス契約は、トラフィックがネットワークアプリケーション、プロトコル、およびポートに一致したときに実行されるアクション（許可または拒否）を定義します。他のルールが一致しない場合、デフォルトアクションでは Catch All ルールが使用されます。

- **グループベースのアクセスコントロールポリシー**：グループベースのアクセスコントロールポリシーは、特定の送信元と宛先グループのペアを識別し、アクセス契約を関連付けます。アクセス契約は、送信元グループと宛先グループの間で許可または拒否されるトラフィックのタイプを指定します。これらのポリシーは単方向です。

スケーラブルグループおよびアクセス契約は、アクセスコントロールポリシーの基本的な構成要素です。アクセスコントロールポリシーを作成する際には、前に作成したスケーラブルグループと契約を使用したり、ポリシーの作成時に新しいスケーラブルグループと契約を作成したりできます。特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセスコントロールポリシーを作成できます。たとえば、「請負業者」送信元スケーラブルグループに関連付けられたユーザがアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成できます。「財務サーバ」宛先スケーラブルグループへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセスコントロールポリシーを作成できます。

送信元と宛先のスケーラブルグループの組み合わせにコントラクトが指定されていない場合に使用するデフォルトポリシーを指定できます。デフォルトポリシーは [Permit] です。必要に応じて、このポリシーを [Deny]、[Permit_IP_Log]、または [Deny_IP_Log] に変更できます。ネットワークタイプ、オープンネットワーク、またはクローズドネットワークに基づいて、デフォルトポリシーを設定できます。



(注) すべてのネットワーク インフラストラクチャ デバイスに必要なネットワークトラフィックを許可する明示的なポリシーを作成した場合のみ、デフォルトポリシーを [Permit] から [Deny] に変更することをお勧めします。そのようにしない場合、すべてのネットワーク接続が失われる可能性があります。

リスト ビュー

[Group-Based Access Control] ウィンドウの右上にある [List] アイコンをクリックして、[List] ビューを起動します。

- **[Source View]**：このビューには、送信元グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。
- **[Destination View]**：このビューには、宛先グループに基づいて編成された既存のポリシーのリストが表示されます。各行を展開して、特定の送信元と宛先のポリシーの詳細を表示できます。

特定の送信元グループから使用可能な宛先グループを確認するには、[Source] ビューを使用します。特定の宛先グループへのアクセスが許可されている送信元グループを確認するには、[Destination] ビューを使用します。たとえば、「請負業者」送信元スケーラブルグループの一部であるユーザが使用できる宛先グループを確認するには、[Source] ビューを使用します。「財務サーバ」宛先スケーラブルグループにアクセスできる送信元グループを確認するには、[Destination] ビューを使用します。

[Deploy] をクリックして、更新されたポリシーをネットワークデバイスに展開します。[Deploy] をクリックすると、Cisco DNA Center は Cisco Identity Services Engine (Cisco ISE) に、ポリシーの変更に関する通知をネットワークデバイスに送信するように要求します。

マトリクス ビュー

[Group-Based Access Control] ウィンドウの右上にある [Grid] アイコンをクリックして、[Matrix] ビューを起動します。[Matrix] ビューはコアポリシービューであり、すべてのスケーラブルグループに関するすべてのポリシーの概要を提供します（明示的またはデフォルトを問わない）。[Matrix] ビューを使用して、すべての送信元と宛先のポリシーを表示し、全体的なポリシー構造を理解できます。[Matrix] ビューからアクセスコントロールポリシーを表示、作成、および更新できます。

[Matrix] ビューには、次の 2 つの軸があります。

- 送信元軸：垂直軸にはすべての送信元スケーラブルグループがリストされます。
- 宛先軸：水平軸にはすべての宛先スケーラブルグループがリストされます。

特定の送信元スケーラブルグループと宛先スケーラブルグループのポリシーを表示するには、セルにカーソルを置きます。セルの色は、そのセルに適用されるポリシーに基づいています。次の色は、各セルに適用されるポリシーを示しています。

- [Permit]：緑色
- [Deny]：赤色
- [Custom]：金色
- [Default]：灰色

マトリクスの上部に表示される [Permit]、[Deny]、[Custom]、または [Default] アイコンにカーソルを置くと、そのポリシーが適用されているセルが表示されます。

セルをクリックすると、[Create Policy] または [Edit Policy] スライドインペインが開き、選択したセルのポリシーを作成または編集できます。[Create Policy] スライドインペインには、送信元と宛先のスケーラブルグループが読み取り専用フィールドとして表示されます。ポリシーのステータスとアクセス契約を更新できます。

[Filter] オプションを使用して、選択した一連の送信元および宛先グループのポリシーマトリクスのサブセットを表示できます。フィルタを作成して、関心のあるポリシーだけに絞り込むことができます。フィルタを作成するには、含める送信元および宛先グループを選択します。

カーソルでマトリックスコンテンツ領域をドラッグするか、または水平および垂直スクロールバーを使用して、マトリックス内を移動できます。ミニマップを使用して、マトリックス内を移動することもできます。ミニマップを使用すると、マトリックスのサイズが大きく、画面サイズを超えている場合に、マトリックス内を簡単に移動できます。ミニマップは、画面上の任意の場所に移動して配置できます。ミニマップにはマトリックスビュー全体が表示されます。ミニマップの薄い灰色の部分は、画面に現在表示されているマトリックスの部分を表します。この領域をドラッグして、マトリックスをスクロールできます。



(注) ミニマップはデフォルトで閉じられています。[Expand] アイコンをクリックして、ミニマップを展開して表示します。

セルを選択すると、[Matrix] ビューによってそのセルと対応する行（送信元スケーラブルグループ）およびカラム（宛先スケーラブルグループ）が強調表示されます。選択したセルの座標（送信元スケーラブルグループおよび宛先スケーラブルグループ）がマトリックスコンテンツ領域の近くに表示されます。

[Deploy] をクリックして、更新されたポリシーをネットワークデバイスに展開します。[Deploy] をクリックすると、Cisco DNA Center は Cisco ISE に、ポリシーの変更に関する通知をネットワークデバイスに送信するように要求します。

Cisco DNA Center と Cisco ISE を統合します。Cisco ISE は、Cisco DNA Center の代わりにネットワークデバイスにポリシーをダウンロードするためのランタイム ポリシー プラットフォームを提供します。ポリシーの同期の問題を防ぐために、セキュリティグループ、セキュリティグループアクセス コントロール リスト (SGACL)、およびイーグレスポリシーの [TrustSec Workcenter] ユーザインターフェイス画面が Cisco ISE に読み取り専用モードで表示されます。

ポリシー作成の概要

1. 組織の分類を定義するか、または最初に使用する組織の一部を定義します。
2. 特定した分類のスケーラブルグループを作成します。
3. 制御するネットワークトラフィックのタイプのアクセス契約を作成します。すべてのトラフィックを許可または拒否するためのサンプルアクセス契約が事前に定義されています。また、一部の契約例では、より具体的なトラフィックフィルタリングが示されています。特定のアプリケーション定義に基づいて、さらにきめ細かいアクセス契約を作成できます。
4. アプリケーションサーバや他のネットワークへの接続など、特定のネットワークリソースへのアクセスを必要とするネットワークユーザのカテゴリを決定します。
5. アクセスポリシーを作成し、送信元グループ、宛先グループ、およびアクセス契約を関連付け、送信元から宛先へのトラフィックのフローを許可する方法を定義します。

スケーラブルグループの作成

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

ステップ 1 [Policy] > [Group-Based Access Control] > [Scalable Groups] の順に選択します。 > >

ステップ 2 [Create Scalable Group] をクリックします。

[Create Scalable Group] スライドインペインが表示されます。

ステップ 3 [Create Scalable Group] スライドインペインで、スケーラブルグループの名前と説明（オプション）を入力します。

（注） [Name] フィールドでサポートされる文字は次のとおりです：

- 英数字
- アンダースコア (_)

スケーラブルグループ名は英字で開始する必要があります。

Cisco DNA Center タグ値を生成します。必要に応じて、この値を更新できます。指定した値が既存のスケーラブルグループによってすでに使用されている場合は、エラーメッセージが表示されます。有効な範囲は 2 ~ 65519 です。

ステップ 4 このスケーラブルグループに関連付ける**仮想ネットワーク**をドロップダウンリストから選択します。デフォルトでは、デフォルトの仮想ネットワーク (DEFAULT_VN) が選択されています。

ステップ 5 スケーラブルグループを Cisco Application Centric Infrastructure (ACI) に伝播する場合は、[Propagate to ACI] チェックボックスをオンにします。

ステップ 6 [Save] をクリックします。

[Scalable Groups] ウィンドウには、スケーラブルグループ名、タグ値、割り当てられた仮想ネットワーク、および関連付けられたポリシーが表示されます。このウィンドウでは、スケーラブルグループのサンプルを表示することもできます。それらのスケーラブルグループを使用または削除できます。

スケーラブルグループの [Policies] 列のリンクをクリックすると、そのスケーラブルグループとそれが属するポリシーを使用するアクセス制御ルールが表示されます。

Cisco ISE との同期が完了していない場合は、スケーラブルグループの横にオレンジ色の三角形のアイコンが表示されます。

スケーラブルグループは、[Scalable Groups] ウィンドウから編集または削除できます。ACI から学習したスケーラブルグループを編集または削除することはできません。スケーラブルグループが任意のアクセスポリシーで使用されている場合は、それを削除することはできません。

Cisco ISE は、内部エンドポイントグループ (IEPG) を同期し、Cisco ISE に関連付けられている読み取り専用スケーラブルグループを作成することで、ACI から TrustSec ドメインへのパケットをサポートします。これらのスケーラブルグループは、[Learned From] フィールドに ACI という値を持つ [Scalable Groups] ウィンドウに表示されます。ACI から学習したスケーラブルグループを編集または削除することはできませんが、ポリシーで使用することはできます。

IEPG が ACI で更新されると、対応するスケーラブルグループ設定が Cisco ISE で更新されます。Cisco ISE でスケーラブルグループが作成されると、新しい EEPG が ACI に作成されます。

スケーラブルグループの詳細を表示するには、[Scalable Group Name] のリンクをクリックします。スケーラブルグループの詳細を更新するには、[View Scalable Group] ウィンドウで [Edit] をクリックします。[Deploy] をクリックすると、Cisco DNA Center は Cisco ISE に、ネットワークデバイスへの変更に関する通知を送信するように要求します。[Deploy] 列の展開ステータスを確認できます。



(注) 名前が「ANY」またはタグ値が 0xFFFF/65535 のスケーラブルグループを作成することはできません。スケーラブルグループ ANY/65535 は、Cisco DNA Center デフォルトポリシーに使用される予約済みの内部スケーラブルグループです。

Cisco DNA Center でスケーラブルグループを Cisco ISE と同期する場合、次のようになります。

- スケーラブルグループが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- スケーラブルグループが Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- Cisco DNA Center と Cisco ISE の両方でスケーラブルグループ名が同じだが、説明と ACI データが異なっている場合は、Cisco DNA Center が Cisco ISE で指定されたデータを使用して更新されます。
- Cisco DNA Center と Cisco ISE でスケーラブルグループ名が同じだが、タグ値が異なる場合は、Cisco ISE で指定されたタグ値を持つ新しいスケーラブルグループが Cisco DNA Center に作成されます。Cisco DNA Center に既存のスケーラブルグループの名前は、サフィックス _DNAC で更新されます。
- タグ値が同じだが、スケーラブルグループ名が異なる場合は、Cisco DNA Center のスケーラブルグループ名が Cisco ISE で指定された名前更新されます。

アクセス契約の作成

アクセス契約は、送信元と宛先のスケーラブルグループ間の通過を許可されるネットワークトラフィックのタイプを制御する一連のルールです。Access contracts define the actions (permit or deny) performed when the traffic matches a network application, protocol, and port.



(注) Cisco ISE のセキュリティ グループ アクセス コントロール リスト (SGACL) は、Cisco DNA Center のアクセス契約と呼ばれます。

始める前に

次のタスクを実行するには、スーパー管理者またはネットワーク管理者である必要があります。

ステップ 1 [Policy] > [Group-Based Access Control] > [Access Contracts] の順に選択します。

ステップ 2 [Create Access Contract] をクリックします。

ステップ 3 [Create Access Contract] スライドインペインで、契約の名前と説明を入力します。

ステップ 4 トラフィックフィルタルールを作成します。

- [Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。
- From the **Application** drop-down list, choose the application for which you want to apply that action. ポートとプロトコルは、選択したアプリケーションに基づいて自動的に選択されます。
トランスポートプロトコル、送信元ポート、および宛先ポートを指定する場合は、[Application] ドロップダウンリストから [Advanced] オプションを選択します。

複数のルールを作成できます。1つの契約に複数のルールを作成するには、[Plus] 記号をクリックし、[Action] 列と [Application] 列の設定を選択します。ルールは、契約に記載されている順序でチェックされます。ルールの左端にあるハンドルアイコンを使用してドラッグして、ルールの順序を変更します。

[Logging] トグルを使用して、任意のトラフィックフィルタルール（デフォルトアクションを含む）のロギングを有効化または無効化できます。ロギングはデフォルトではディセーブルになっています。ロギングが有効になっている場合、トラフィックフィルタルールにヒットすると、ネットワークデバイスは syslog メッセージを送信します。これは、ポリシーのトラブルシューティングと初期化テストに役立つ場合があります。ただし、ネットワークデバイスのリソースとパフォーマンスに影響を与える可能性があるため、このオプションは慎重に使用することを推奨します。

ステップ 5 [Default Action] ドロップダウンリストで、[Deny] または [Permit] を選択します。

必要に応じて、デフォルトアクションのロギングを有効にできます。

ステップ 6 [Save] をクリックします。

[Access Contracts] リストウィンドウで、契約の表示、作成、複製、更新、および削除ができます。

また、[Access Contracts] ウィンドウでサンプル契約を表示することもできます。それらのサンプル契約は使用または削除できます。ただし、デフォルトの契約 (Permit IP、Deny IP、Permit_IP_Log、Deny_IP_Log) は削除できません。

[Filter] オプションを使用して、探している契約を検索できます。

Cisco ISE との同期が完了していない場合は、契約の横にオレンジ色の三角形のアイコンが表示されます。

[Access Contracts] ウィンドウの [Contract Name] リンクをクリックして、契約の詳細を表示します。契約の詳細を編集するには、[View Contract] ウィンドウで [Edit] をクリックします。

[Rules Count] 列で、各契約で使用されているルールを確認できます。

スケーラブルグループ、契約、またはポリシーを更新する場合は、ネットワークデバイスに変更を展開する必要があります。ポリシーを更新し、更新したポリシーを展開しない場合、ポリシーの変更に関する通知はネットワークデバイスに送信されず、ネットワークで現在アクティブになっているポリシーは、Cisco DNA Center に表示されるポリシー情報と一致しない可能性があります。この状況を解決するには、ネットワークデバイスに、更新したポリシーを展開する必要があります。展開ステータスが [Deployed] 列に表示されます。

契約を使用するポリシーを表示するには、契約の [Policies] 列のリンクをクリックします。

ポリシーで使用されている場合、契約を削除することはできません。契約を削除する前に、そのポリシーから契約を削除する必要があります。

既存の契約を複製し、必要な詳細を編集して新しい契約を作成することができます。契約を複製すると、既存の契約内のすべての情報がコピーされ、コピーされた契約には、末尾に文字列「Copy」が付加された既存の契約名が含まれます。

Cisco DNA Center のアクセス契約を Cisco ISE と同期している間：

- 契約が Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- コントラクトがに存在Cisco ISEし、にCisco DNA Center存在しない場合は、にCisco DNA Center作成されます。
- Cisco DNA CenterとCisco ISEの契約名が同じであるが、説明とトラフィックルールの内容が異なっている場合、Cisco DNA CenterはCisco ISEで指定されたデータを使用して更新されます。
- 契約名とルールが同じですが、説明が異なっている場合Cisco DNA Centerは、でCisco ISE指定された説明を使用して更新されます。
- Cisco ISEの Text SGACL コマンドラインは、非解析コンテンツとして移行されます。これらの契約は編集できますが、Cisco DNA Centerでは解析または構文チェックは実行されません。Cisco DNA Center で加えた変更は、同様に Cisco ISE にも反映されます。
- Cisco ISE でポリシーに複数の SGACL がある場合、それらの契約は Cisco DNA Center のデフォルトポリシーとして移行されます。

グループベースのアクセスコントロールポリシーの作成

スケーラブルグループおよびアクセス契約は、アクセスコントロールポリシーの基本的な構成要素です。アクセスコントロールポリシーを作成する際には、以前に作成したスケーラブルグループと契約を使用したり、ポリシーの作成時に新しいスケーラブルグループと契約を作

成したりできます。特定の送信元グループからアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成できます。一方、特定のネットワークリソースへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先グループと複数の送信元グループを含むアクセスコントロールポリシーを作成できます。たとえば、「請負業者」送信元スケーラブルグループに関連付けられたユーザがアクセスできるネットワークリソースを指定する場合は、1つの送信元グループと複数の宛先グループを含むアクセスコントロールポリシーを作成できます。「Finance Servers」宛先スケーラブルグループへのアクセスが許可されている送信元グループを指定する場合は、1つの宛先と複数の送信元グループを使用してアクセスコントロールポリシーを作成できます。

グループベースのアクセスコントロールポリシーの作成

ステップ1 [Policy List] または [Matrix]ビューで、[Create Policies] をクリックします。

ステップ2 [Source To Destination(s)] をクリックして、単一の送信元と複数の宛先グループを含むアクセスコントロールポリシーを作成します。

- a) 選択する送信元スケーラブルグループの横にあるオプションボタンをクリックします。必要なスケーラブルグループが存在しない場合は、[Create Scalable Group] をクリックして、新しいスケーラブルグループを作成します。詳細については、「[スケーラブルグループの作成 \(6 ページ\)](#)」を参照してください。
- b) [Next] をクリックします。
- c) 選択した送信元スケーラブルグループにマッピングする宛先スケーラブルグループを選択します。

必要に応じて、スケーラブルグループの詳細を表示したり、スケーラブルグループを編集したりできます。

送信元と宛先の間にはポリシーがすでに存在する場合、スケーラブルグループの近くにはオレンジ色の三角形のアイコンが表示されます。

- d) [次へ (Next)] をクリックします。
- e) 選択する契約の横にあるオプションボタンをクリックします。必要な契約が存在しない場合は、[Create Contract] をクリックして新しい契約を作成します。詳細については、「[アクセス契約の作成 \(7 ページ\)](#)」を参照してください。

必要に応じて、契約の詳細を表示および編集できます。

(注) 1つのポリシーに対して1つの契約のみを選択できます。

- f) [次へ (Next)] をクリックします。

[Summary] ウィンドウには、選択したスケーラブルグループと契約に基づいて作成されたポリシーが一覧表示されます。

- g) [Save] をクリックします。

ステップ3 [Destination to Source(s)] をクリックして、1つの宛先と複数の送信元グループを含むアクセスコントロールポリシーを作成します。

- a) 選択する宛先スケーラブルグループの横にあるオプションボタンをクリックします。必要なスケーラブルグループが存在しない場合は、[Create Scalable Group] をクリックします。

- b) **[次へ (Next)]** をクリックします。
- c) 選択した宛先スケーラブルグループにマッピングする送信元スケーラブルグループを選択します。
- 必要に応じて、スケーラブルグループの詳細を表示したり、スケーラブルグループを編集したりできます。
- 送信元と宛先の間にはポリシーがすでに存在する場合、スケーラブルグループの近くにはオレンジ色の三角形のアイコンが表示されます。
- d) **[次へ (Next)]** をクリックします。
- e) 選択する契約の横にあるオプションボタンをクリックします。必要な契約が存在しない場合は、**[Create Contract]** をクリックします。
- 必要に応じて、契約の詳細を表示および編集できます。
- (注) 1つのポリシーに対して1つの契約のみを選択できます。
- f) **[次へ (Next)]** をクリックします。
- [Summary]** ウィンドウには、選択したスケーラブルグループと契約に基づいて作成されたポリシーが一覧表示されます。
- g) **[Save]** をクリックします。
- (注) **[Scalable Group]** リストエリアの右上隅にある **[Toggle]** ボタンを使用して、**[List]** ビューと **[Drag and Drop]** ビューを切り替えることができます。**[Drag and Drop]** ビューを使用すると、アクセスコントロールポリシーの作成時に、スケーラブルグループを **[Source]** フィールドと **[Destination]** フィールドにドラッグアンドドロップすることができます。ただし、**[Drag and Drop]** ビューには、最初の 50 のスケーラブルグループのみが表示されます。スケーラブルグループの数が少ない場合（最大 50）は、**[Drag and Drop]** ビューを使用できます。スケーラブルグループが 50 を超える場合は、**[List]** ビューを使用してすべてのグループを表示します。

Cisco DNA Center でポリシーを Cisco ISE と同期する場合、次のようになります。

- ポリシーが Cisco DNA Center に存在し、Cisco ISE に存在しない場合は、Cisco ISE に作成されます。
- 契約が Cisco ISE に存在し、Cisco DNA Center に存在しない場合は、Cisco DNA Center に作成されます。
- Cisco ISE でポリシー契約が異なる場合、Cisco DNA Center は Cisco ISE で指定された契約で更新されます。
- ポリシーモード情報（有効、無効、またはモニタ）も Cisco ISE からインポートされます。

Cisco ISE には、単一のポリシーに対して複数の SGACL を許可するオプションがあります（このオプションは Cisco ISE ではデフォルトで有効になっていません）。Cisco DNA Center では、単一のポリシーに対して複数のアクセス契約を使用することはサポートされていません。ポリシーの同期中に、Cisco ISE のポリシーに複数の SGACL がある場合、Cisco DNA Center 管理者には、そのポリシーを変更して契約を選択しないようにするオプションがあります（デフォルト

トポリシーを使用する場合)。管理者は、ポリシーの同期が完了した後に、そのポリシーに対して新規または既存のアクセス契約を選択できます。

IP ベースのアクセスコントロールポリシー

IP ベースのアクセスコントロールポリシーは、アクセスコントロールリスト (ACL) と同じ方法でシスコデバイスに出入りするトラフィックを制御します。ACL と同様に、IP ベースのアクセスコントロールポリシーにはプロトコルタイプ、送信元 IP アドレス、宛先 IP アドレス、宛先ポート番号などのさまざまな条件に基づいてトラフィックフローに適用される許可条件および拒否条件のリストが含まれています。

IP ベースのアクセスコントロールポリシーを使用して、セキュリティ、モニタリング、ルート選択、ネットワークアドレス変換などのさまざまな目的のためにトラフィックをフィルタ処理できます。

IP ベースのアクセスコントロールポリシーには、次の2つの主要コンポーネントがあります。

- [IP Network Groups] : IP ネットワークグループは、同じアクセス制御要件を共有する IP サブネットで構成されています。これらのグループは Cisco DNA Center でのみ定義できます。IP ネットワークグループに含めることができる IP サブネットは1つだけです。
- [Access Contract] : アクセスコントラクトは、IP ベースのアクセスコントロールポリシーとグループベースのアクセスコントロールポリシーの両方で使用される共通の構成要素です。これはアクセス制御ポリシーを構成するルールを定義します。これらのルールでは、トラフィックが特定のポートまたはプロトコルに一致したときに実行されるアクション（許可または拒否）や他のルールが一致しないときに実行される暗黙のアクション（許可または拒否）を指定します。

IP ベースのアクセスコントロールポリシー設定のワークフロー

始める前に

- [Policy] > [IP Based Access Control] > [IP Network Groups] ウィンドウから IP ネットワークグループを作成するには、Cisco ISE と Cisco DNA Center が統合されていることを確認します。 >>ただし、新しいIP ベースのアクセスコントロールポリシーを作成中に、[Policy] > [IP Based Access Control] > [IP Network Groups] ウィンドウでグループを追加する場合は、Cisco ISE は必須ではありません。 >>



(注) Cisco ISE なしでも、[Policy] > [IP Based Access Control] ウィンドウで IP ネットワークグループを編集できます。 >ただし、[IP Based Access Control] ウィンドウからの IP ネットワークグループの作成には、Cisco ISE が必要です。

- 次のグローバルネットワーク設定が定義されていることを確認し、デバイスをプロビジョニングします。
 - ネットワークサーバ (AAA、DHCP、DNS サーバなど) : [グローバル ネットワーク サーバの設定](#) を参照してください。
 - デバイスログイン情報 (CLI、SNMP、HTTP、HTTPS など) : [グローバル デバイス クレデンシャルについて](#) を参照してください。
 - IP アドレスプール : [IP アドレス プールを設定する](#) を参照してください。
 - ワイヤレス設定 (SSID、ワイヤレスインターフェイス、ワイヤレス無線周波数プロファイルなど) : [グローバル ワイヤレス設定の構成](#) を参照してください。
 - プロビジョニングデバイス : [プロビジョニング](#) を参照してください。

ステップ 1 IP ネットワーク グループを作成します。

詳細については、「[IP ネットワーク グループの作成 \(14 ページ\)](#)」を参照してください。

ステップ 2 IP ベースのアクセス制御契約を作成します。

IP ベースのアクセス制御契約は、送信元と宛先の間の一連のルールを定義します。これらのルールは、ネットワーク デバイスが、指定されたプロトコルまたはポートに一致するトラフィックに基づいて実行するアクション (許可または拒否) を指定します。詳細については、「[IP ベースのアクセスコントロール契約の作成 \(15 ページ\)](#)」を参照してください。

ステップ 3 IP ベースのアクセス コントロール ポリシーの作成アクセス コントロール ポリシーは、送信元と宛先の IP ネットワーク グループ間のトラフィックを制御するアクセス制御契約を定義します。

詳細については、[IP ベースのアクセス コントロール ポリシーの作成 \(16 ページ\)](#) を参照してください。

グローバル ネットワーク サーバの設定

ネットワーク全体のデフォルトになるグローバル ネットワーク サーバを定義することができます。



(注) サイト固有の設定を定義することで、サイトのグローバル ネットワーク設定を上書きできます。

ステップ 1 Cisco DNA Center のホームページで、**[Design] > [Network Settings] > [Network]** の順に選択します。

ステップ 2 **[DHCP サーバ (DHCP Server)]** フィールドに、DHCP サーバの IP アドレスを入力します。

- (注) プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。
IP アドレス プールを作成するには、少なくとも 1 つの DHCP サーバを定義する必要があります。

ステップ 3 [DNS サーバ (DNS Server)] フィールドに、DNS サーバのドメイン名を入力します。

- (注) プラスアイコンをクリックすると、IPv4 アドレスと IPv6 アドレスの両方を入力できます。
IP アドレス プールを作成するために、少なくとも 1 つの DNS サーバを定義する必要があります。

ステップ 4 (任意) Syslog、SNMP トラップ、NetFlow コレクタサーバ情報を入力してください。[サーバの追加 (Add Servers)] をクリックして NTP サーバを追加します。

Cisco DNA Center を Syslog サーバとして設定し、ネットワークデバイスがこのサーバに Syslog メッセージを送信するよう設定するには、[Cisco DNA Center を syslog サーバとする (Cisco DNA Center as syslog server)] チェックボックスをオンにします。

ファブリック コンプライアンス チェックをトリガするには、Cisco DNA Center の IP アドレスを使用して SNMP サーバを設定します。詳細については、「[ファブリックへのデバイスの追加 \(Add a Device to a Fabric\)](#)」を参照してください。

ステップ 5 [Save] をクリックします。

IP ネットワーク グループの作成

ステップ 1 Cisco DNA Center ホームページで、[ポリシー (Policy)] >> [IP ベースのアクセスコントロール (IP Based Access Control)] >> [IP ネットワーク グループ (IP Network Groups)] の順に選択します。

ステップ 2 [グループの追加 (Add Group)] をクリックします。

ステップ 3 [名前 (Name)] フィールドに、IP ネットワーク グループの名前を入力します。

ステップ 4 [説明 (Description)] フィールドに、IP ネットワーク グループを説明する単語またはフレーズを入力します。

ステップ 5 [IP アドレスまたは IP/CIDR (IP Address or IP/CIDR)] フィールドに、IP ネットワーク グループを構成する IP アドレスを入力します。

ステップ 6 [Save] をクリックします。

IP ネットワーク グループの編集または削除

ステップ 1 Cisco DNA Center ホームページで、[ポリシー (Policy)] >> [IP ベースのアクセスコントロール (IP Based Access Control)] >> [IP ネットワーク グループ (IP Network Groups)] の順に選択します。

ステップ 2 [IP ネットワーク グループ (IP Network Groups)] テーブルで、編集または削除するグループの横にあるチェックボックスをオンにします。

ステップ3 次のいずれか1つのタスクを実行します。

- グループを変更するには、[編集 (Edit)] をクリックします。フィールドの定義については、[IP ネットワーク グループの作成 \(14 ページ\)](#) を参照してください。
- グループを削除するには、[削除 (Delete)] をクリックし、次に [はい (Yes)] をクリックして確定します。

IP ベースのアクセス コントロール契約の作成

ステップ1 Cisco DNA Center のホームページで、[Policy] > [IP Based Access Control] > [Access Contract] の順に選択します。

ステップ2 [コントラクトの追加 (Add Contract)] をクリックします。

ステップ3 ダイアログボックスに、契約の名前と説明を入力します。

ステップ4 [暗黙的アクション (Implicit Action)] ドロップダウンリストから、[拒否 (Deny)] または [許可 (Permit)] を選択します。

ステップ5 テーブルの [アクション (Action)] ドロップダウンリストから、[拒否 (Deny)] または [許可 (Permit)] を選択します。

ステップ6 [ポート/プロトコル (Port/Protocol)] ドロップダウンリストから、ポートまたはプロトコルを選択します。

- a) Cisco DNA Center に必要なポートまたはプロトコルがない場合は、[ポート/プロトコルの追加 (Add Port/Protocol)] をクリックして、自分で作成します。
- b) [名前 (Name)] フィールドで、ポートまたはプロトコルの名前を入力します。
- c) [プロトコル (Protocol)] ドロップダウンリストで、[UDP]、[TDP]、または [TCP/UDP] を、プロトコルとして選択します。
- d) [ポート範囲 (Port Range)] フィールドにポート範囲を入力します。
- e) Cisco DNA Center で定義したとおりにポートまたはプロトコルを設定し、競合をレポートしないようにするには、[競合を無視する (Ignore Conflict)] チェックボックスをオンにします。

ステップ7 (任意) 契約にさらにルールを含めるには、[追加 (Add)] をクリックして、手順5 および6 を繰り返します。

ステップ8 [Save] をクリックします。

Edit or Delete an IP-Based Access Control Contract

ポリシーで使用されている契約を編集すると、[IP ベースのアクセス コントロール ポリシー (IP Based Access Control Policies)] ウィンドウのポリシーの状態が [変更 (MODIFIED)] に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [IP ベースのアクセスコントロール (IP Based Access Control)] > [契約へのアクセス (Access Contract)] の順に選択します。

ステップ 2 編集または削除する契約の横にあるチェックボックスをオンにして、次のいずれかのタスクを実行します。

- 契約を変更するには、[編集 (Edit)] をクリックして変更を行い、[保存 (Save)] をクリックします。フィールドの定義については、[IP ベースのアクセスコントロール契約の作成 \(15 ページ\)](#) を参照してください。

(注) ポリシーで使用されている契約を変更した場合は、[ポリシー (Policy)] > [IP ベースのアクセスコントロール (IP-Based Access Control)] > [IP ベースのアクセスコントロールポリシー (IP-Based Access Control Policies)] の順に選択し、ポリシー名の横にあるチェックボックスをオンにして、[展開 (Deploy)] をクリックすることによって、変更したポリシーを展開する必要があります。

- 契約を削除するには、[削除 (Delete)] をクリックします。

IP ベースのアクセスコントロールポリシーの作成

IP ネットワーク グループ間のトラフィックを制限する、IP ベースのアクセスコントロールポリシーを作成します。

- 1 つのポリシーに異なる設定で複数のルールを追加することができます。
- IP グループと契約の分類子の特定の組み合わせでルールが作成され、デバイスにプッシュされます。この数は、Cisco WLC が ACL でのルールを最大 64 に制限しているため、64 個のルールを超えることはできません。
- **展開された** ポリシー内で使用されるカスタム契約または IP グループが変更された場合、そのポリシーは古いものであり、デバイスにプッシュする新しい設定のために再展開される必要があることを示す [変更済み (Modified)] というステータスでフラグが付けられます。

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [IP ベースのアクセスコントロール (IP Based Access Control)] > [IP ベースのアクセスコントロールポリシー (IP Based Access Control Policy)] の順に選択します。

ステップ 2 [ポリシーの追加 (Add Policy)] をクリックします。

ステップ 3 次のフィールドに入力します。

| フィールド | 説明 |
|---------------|-------------------|
| [Policy Name] | ポリシーの名前。 |
| 説明 | ポリシーを表す単語またはフレーズ。 |

| フィールド | 説明 |
|-----------------------|---|
| SSID | <p>SSID の設計中に作成された FlexConnect SSID および 非 FlexConnect SSID をリストします。選択した SSID が FlexConnect モードで設定されている場合、アクセスポリシーも FlexConnect モードで設定されます。そうでない場合は、通常の方法で設定されます。</p> <p>(注) SSID が 1 つのポリシーの一部である場合は、その SSID は別のポリシーで使用できません。</p> <p>ポリシーの展開には有効なサイト SSID の組み合わせが必要です。選択した SSID がデバイスの下でプロビジョニングされていない場合、ポリシーを展開することはできません。</p> |
| サイトの範囲 | <p>サイトのポリシーが適用される範囲。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービスセット識別子 (SSID) のワイヤレスポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレス デバイスにポリシーが適用されます。詳細については、サイトの範囲 (20 ページ) を参照してください。</p> |
| [Source] | <p>契約の影響を受けるトラフィックの送信元。[送信元の検索 (SearchSource)] ドロップダウンリストから、IP ネットワーク グループを選択します。使用したい IP ネットワークがない場合は、[+グループの追加 (+Group)] をクリックして作成します。</p> |
| コントラクト | <p>ACL 内で送信元と宛先間のネットワーク連携を管理するルール。[契約の追加 (Add Contract)] をクリックして、ポリシーの契約を定義します。ダイアログボックスで、使用する契約の横にあるラジオ ボタンをクリックします。または、契約の [許可 (permit)] (すべてのトラフィックを許可) または [拒否 (deny)] (すべてのトラフィックを拒否) を選択することもできます。</p> |
| Destination | <p>契約の影響を受けるトラフィックの宛先。[宛先 (Destination)] ドロップダウンリストをクリックして、IP ネットワーク グループを選択します。使用したい IP ネットワークがない場合は、[+IP ネットワーク グループの作成 (+Create IP Network Group)] をクリックして作成します。</p> |
| 方向 (Direction) | <p>送信元と宛先間のトラフィックフローの関係を設定します。送信元から宛先へのトラフィックフローの契約を有効にするには、[一方向 (One-Way)] を選択します。両方向 (送信元から宛先へ、および宛先から送信元へ) でのトラフィックフローの契約を有効にするには、[双方向 (Bi-directional)] を選択します。</p> |

ステップ 4 (任意) IP ネットワーク グループを作成するには、[IP ネットワーク グループの作成 (Create IP Network Group)] をクリックします。

ステップ 5 (任意) 別のルールを追加するには、プラス記号をクリックします。

(注) ルールを削除するには、[x] をクリックします。

ステップ 6 (任意) ルールの順序を変更するには、変更したい順序でルールをドラッグアンドドロップします。

ステップ 1 [展開 (Deploy)] をクリックします。

「IP ベースのアクセス コントロール ポリシーが作成され、正常に展開されました」という成功メッセージが表示されます。選択した SSID によっては、FlexConnect ポリシーまたは標準ポリシーが異なるマッピング情報レベルで作成され、展開されます。ポリシーの [ステータス (Status)] は、[展開済み (DEPLOYED)] として表示されます。[ポリシー名 (Policy Name)] の横にあるワイヤレス アイコンは、展開されたアクセス ポリシーがワイヤレス ポリシーであることを示しています。

IP ベースのアクセスコントロールポリシーの編集または削除

必要な場合は、IP ベースのアクセス コントロール ポリシーを変更または削除できます。



(注) ポリシーを編集すると、[IPベースのアクセスコントロールポリシー (IP-Based Access Control Policies)] ウィンドウのポリシーの状態が [変更 (MODIFIED)] に変わります。変更されたポリシーは、ネットワークに導入されたポリシーと一致しないため、古いと見なされます。この問題を解決するには、ネットワークにポリシーを再展開する必要があります。

ステップ 1 Cisco DNA Center のホームページで、[Policy] > [IP Based Access Control] > [IP Based Access Control Policies] > の順に選択します。

ステップ 2 編集または削除するポリシーの横にあるチェック ボックスをオンにして、次のいずれかのタスクを実行します。

- 変更するには、[編集 (Edit)] をクリックします。完了したら、[Save] をクリックします。フィールドの定義については、[IP ベースのアクセス コントロール ポリシーの作成 \(16 ページ\)](#) を参照してください。
- ポリシーを削除するには、[削除 (Delete)] をクリックします。

ステップ 3 ポリシーを変更した場合は、ポリシー名の横にあるチェック ボックスをオンにして [展開 (Deploy)] をクリックすることによって、変更したポリシーを展開します。

IP ベースのアクセスコントロールポリシーの展開

ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再度展開する必要があります。

ステップ 1 Cisco DNA Center のホームページで、[Policy] > [IP Based Access Control] > [IP Based Access Control Policies] > の順に選択します。

ステップ 2 展開するポリシーを探します。

ステップ3 ポリシーの横にあるチェックボックスをオンにします。

ステップ4 [展開 (Deploy)] をクリックします。

ポリシーを今すぐ展開するか、または後でスケジュールするかどうかを求められます。

ステップ5 次のいずれかを実行します。

- ポリシーをすぐに展開するには、[今すぐ実行 (Run Now)] ラジオ ボタンをクリックし、[適用 (Apply)] をクリックします。
- 将来の日付と時刻でポリシー展開をスケジュールするには、[後でスケジュール (Schedule Later)] ラジオ ボタンをクリックし、展開する日時を定義します。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーションポリシー

Quality of Service (QoS) とは、選択したネットワーク トラフィックに、優先的なサービスやニーズに合ったサービスを提供するネットワーク機能を意味します。QoSを設定することで、ビジネスの目標（音声品質が会社の標準規格を満たしていることの保証、ビデオの高いQuality of Experience (QoE) の確保など）を引き続き順守しながら、ネットワーク リソースを最も効率的に使用する方法でネットワーク トラフィックを処理することができます。

QoS は、Cisco DNA Center のアプリケーションポリシーを使用してネットワークに設定できます。アプリケーションポリシーは、次の基本的なパラメータで構成されています。

- [アプリケーションセット (Application Sets)] : 同様のネットワーク トラフィックを必要とする一連のアプリケーション。各アプリケーションセットには、トラフィックの優先順位を定義するビジネスとの関連性グループ（ビジネス関連、デフォルト、またはビジネスと無関係）が割り当てられます。QoS パラメータは、Cisco Validated Design (CVD) に基づいて3つのグループごとに定義されます。一部のパラメータは、それぞれの目的に合わせてより詳細に調整できます。詳細については、「[アプリケーションおよびアプリケーションセット](#)」を参照してください。
- [サイトの範囲 (Site Scope)] : アプリケーションポリシーが適用されているサイト。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービスセット識別子 (SSID) のワイヤレスポリシーを設定すると、範囲内で SSID が定義されているすべてのワイヤレスデバイスにポリシーが適用されます。詳細については、[サイトの範囲 \(20 ページ\)](#) を参照してください。

Cisco DNA Center はこれらのパラメータをすべて受け取り、適切なデバイスの CLI コマンドに変換します。Cisco DNA Center はポリシーの展開時に、サイトの範囲で定義されているデバイスに各コマンドを設定します。



- (注) Cisco DNA Center はデバイスで使用可能な QoS 機能セットに基づいて、各デバイスに QoS ポリシーを設定します。デバイスの QoS 実装の詳細については、対応するデバイスの製品マニュアルを参照してください。

アプリケーションポリシーでの CVD ベースの設定

アプリケーションポリシーのデフォルトの QoS 信頼およびキューイング設定は、Enterprise Medianet の QoS デザイン向けの Cisco Validated Design (CVD) に基づいています。CVD は、一般的な使用例や現行のシステム設計上の優先事項に基づき、システム設計の基盤を提示しています。CVD には、お客様のニーズに応じるための幅広いテクノロジー、機能、アプリケーションが組み込まれています。それぞれのソリューションには、エンジニアによる包括的なテストと文書化が実施されており、迅速で、信頼性が高く、予測可能な導入が確保されています。

QoS に関連する最新の検証済み設計は、Cisco Press の書籍『*End-to-End QoS Network Design: Quality of Service for Rich-Media & Cloud Networks, 2nd Edition*』

(<http://www.ciscopress.com/store/end-to-end-qos-network-design-quality-of-service-for-9781587143694>) で公開されています。追加情報については、次のシスコのドキュメントを参照してください。

- [シスコ検証済みデザイン](#)
- [Enterprise Medianet Quality of Service Design 4.0](#)
- [Medianet Campus QoS Design 4.0](#)
- [Medianet WAN Aggregation QoS Design 4.0](#)

サイトの範囲

サイト範囲は、アプリケーションポリシーが適用されるサイトを定義します。ポリシーを定義するときに、ポリシーが有線デバイス用かワイヤレスデバイス用かを設定します。また、サイト範囲も設定します。有線ポリシーを設定すると、ポリシーは、サイト範囲内のすべての有線デバイスに適用されます。同様に、選択したサービスセット識別子 (SSID) のワイヤレスポリシーを設定すると、サイト範囲内で SSID が定義されている、サイト範囲内のすべてのワイヤレス デバイスにポリシーが適用されます。

これにより、有線ネットワーク セグメントとワイヤレス ネットワークセグメントの動作の相違を補うために、必要に応じてトレードオフを実施できます。たとえば、ワイヤレス ネットワークでは通常、有線ネットワークと比較した場合に低帯域幅、低速、パケット損失増加の特徴があります。個々のワイヤレスセグメントは、ローカルの RF 干渉、輻輳、ネットワーク デバイスの機能の違いなどの要因によってさらに変動が見られます。個々のワイヤレスセグメントにセグメントごとのポリシーを適用できるすることで、優先順位の高いトラフィックが受ける、ワイヤレスネットワークの劣化による影響が小さくなるように、トラフィック処理ルールを調整できます。

ビジネス関連のグループ

ビジネス関連グループは、ビジネスや事業への関連性に応じて、指定されたアプリケーションセットを分類します。

ビジネス関連グループ（ビジネス関連、デフォルト、ビジネスと無関係）は、基本的に3種類のトラフィック（高優先順位、ニュートラル、低優先順位）にマッピングされます。

- **ビジネス関連 (Business Relevant)** : (高優先トラフィック) このグループのアプリケーションは組織の目的に直接関与し、音声、ビデオ、ストリーミング、コラボレーション型マルチメディア アプリケーション、データベース アプリケーション、エンタープライズリソースアプリケーション、電子メール、ファイル転送、コンテンツ配布など、さまざまな種類があります。ビジネス関連として指定されているアプリケーションは、Internet Engineering Task Force (IETF) RFC 4594 の規定に従い、業界推奨のベストプラクティスに従って処理されます。
- **デフォルト (Default)** : (平均的優先度のトラフィック) このグループは、ビジネスに関連している場合もあればしていない場合もあるアプリケーションを対象としています。たとえば一般的な HTTP または HTTPS トラフィックは、組織の目的に寄与する場合もしない場合もあります。たとえば、レガシーアプリケーションや新しく導入されたアプリケーションなどでも、一部のアプリケーションの目的については分析していない場合があります。したがって、これらのアプリケーションのトラフィックフローは、IETF RFC 2747 および 4594 で説明されているように、デフォルトの転送サービスで処理する必要があります。
- **ビジネスと無関係 (Business Irrelevant)** : (低優先トラフィック) このグループは、組織の目的達成に寄与しないと識別されたアプリケーションを対象としています。主にコンシューマ向けかエンターテイメント向け、あるいは本質的にその両方に該当するアプリケーションです。この種類のトラフィックは、IETF RFC 3662 および 4594 で説明されている「スカベンジャ」サービスとして処理することをお勧めします。

アプリケーションはアプリケーションセットに分類されて、ビジネス関連グループにソートされます。アプリケーションセットはポリシーに現状のまま含めることができます。または、ビジネス目標やネットワーク構成のニーズを満たすように変更することができます。

たとえば、YouTube はコンシューマ メディア アプリケーションセットのメンバーです。一般的に、ほとんどのお客様がこのアプリケーションをこのように分類しているため、(デフォルトでは) YouTube はビジネスと無関係です。ただし、この分類がすべての企業に当てはまるわけではありません。たとえば、いくつかのビジネスでは YouTube をトレーニング目的で使用することがあります。このような場合、管理者は、デフォルトでビジネス関連であるストリーミング ビデオ アプリケーションセットに YouTube アプリケーションを移動できます。

コンシューマとプロデューサ

あるアプリケーションから別のアプリケーションにトラフィックが送られた (特定の a から b へのトラフィック フローが作成された) ときにトラフィックが特定の 방법으로処理されるよう

に、アプリケーション間の関係を設定することができます。このような関係のアプリケーションをプロデューサとコンシューマと呼び、次のように定義しています。

- **プロデューサ**：アプリケーショントラフィックの送信元。たとえば、クライアント/サーバアーキテクチャでは、トラフィックフローは主にサーバからクライアントの方向であるため、アプリケーションサーバがプロデューサと見なされます。ピアツーピアアプリケーションの場合は、リモートピアがプロデューサと見なされます。
- **コンシューマ**：アプリケーショントラフィックの受信者。コンシューマに該当するのは、クライアント/サーバアーキテクチャの場合はクライアントエンドポイント、ピアツーピアアプリケーションの場合はローカルデバイスなどです。コンシューマはエンドポイントデバイスであることがありますが、場合によっては、そのようなデバイスの特定のユーザであることもあります（通常、IPアドレスまたは特定のサブネットによって識別される）。また、あるアプリケーションが別のアプリケーショントラフィックフローのコンシューマになる場合もあります。

このような関係を設定することにより、このシナリオに一致するトラフィックに特定のサービスレベルを設定することが可能になります。

マーキング、キューイング、ドロップングの処理

Cisco DNA Center は、IETF RFC 4594 およびアプリケーションに割り当てられたビジネス関連のカテゴリでの処理のマーキング、キューイング、およびドロップングをベースとしています。Cisco DNA Center は、デフォルトカテゴリのすべてのアプリケーションをデフォルトの転送アプリケーションクラスに割り当て、無関係なビジネスカテゴリのすべてのアプリケーションをスカベンジャアプリケーションクラスに割り当てます。関連するビジネスカテゴリのアプリケーションについては、Cisco DNA Center はアプリケーションのタイプに基づいてトラフィッククラスをアプリケーションに割り当てます。次の表に、アプリケーションクラスとそれぞれの処理を示します。

表 1: マーキング、キューイング、ドロップの処理

| ビジネス関連性 | アプリケーションクラス | ホップ毎の挙動 | キューイングとドロップ | アプリケーションの説明 |
|---------|--|---------------------------|---|--|
| 該当する | VoIP ¹ | Expedited Forwarding (EF) | プライオリティキューイング (PQ) | VoIP テレフォニー (ベアラのみ) トラフィック。たとえば、Cisco IP 電話。 |
| | ブロードキャストビデオ | クラス セレクタ (CS) 5 | PQ | ブロードキャスト TV、ライブイベント、ビデオ監視フロー、同様の非弾性ストリーミングメディアフロー (Cisco IP Video Surveillance や Cisco Enterprise TV など)。(非弾性フローとは、非常にドロップされやすく、再送信またはフロー制御機能のいずれか、または両方がないフローを意味します。) |
| | リアルタイムインタラクティブ | CS4 | PQ | 非弾性の高解像度インタラクティブ ビデオアプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント (Cisco TelePresence など)。 |
| | マルチメディア会議 | 相対的優先転送 (AF) 41 | 帯域幅 (BW) キューと Differentiated Services Code Point (DSCP) Weighted Random Early Detect (WRED) | デスクトップソフトウェアのマルチメディアコラボレーションアプリケーションおよびそれらのアプリケーションのオーディオおよびビデオコンポーネント (Cisco Jabber や Cisco WebEx など)。 |
| | マルチメディアストリーミング | AF31 | BW キューと DSCP WRED | ビデオオンデマンド (VoD) ストリーミングビデオフローおよび仮想デスクトップアプリケーション。たとえば、Cisco Digital Media System。 |
| | ネットワーク制御 | CS6 | BW キューのみ ² | EIGRP、OSPF、BGP、HSRP、IKE などのエンタープライズネットワークの信頼性の高い運用のために必要とされるネットワークコントロールプレーントラフィック。 |
| | シグナリング | CS3 | BW キューと DSCP | IP 音声およびビデオ テレフォニー インフラストラクチャのコントロールプレーントラフィック。 |
| | Operations, Administration, and Management (OAM) | CS2 | BW キューと DSCP ³ | SSH、SNMP、syslog などのネットワーク運用、管理、管理トラフィック |
| | AF21 | | | |

| ビジネス関連性 | アプリケーションクラス | ホップ毎の挙動 | キューイングとドロッピング | アプリケーションの説明 |
|---------|---------------------|---------|----------------------------|---|
| | トランザクションデータ（低遅延データ） | | BW キューと DSCP WRED | エンタープライズ リソース プランニング（ERP）、顧客関係管理（CRM）、およびその他のデータベースアプリケーションなどのインタラクティブ（フォアグラウンド）データアプリケーション。 |
| | バルクデータ（高スループットデータ） | AF11 | BW キューと DSCP WRED | 電子メール、File Transfer Protocol (FTP)、バックアップアプリケーションなどの非インタラクティブ（バックグラウンド）データアプリケーション。 |
| デフォルト | デフォルトの転送（ベストエフォート） | DF | デフォルトキューと RED | デフォルトのアプリケーション、およびデフォルトのビジネス関連グループに割り当てられるアプリケーション。プライオリティ、保証された帯域幅、または差分サービスクラスに割り当てられるのはごく少数のアプリケーションであるため、大部分のアプリケーションは引き続きデフォルトでベストエフォート型サービスになります。 |
| 非関連 | スカベンジャー | CS1 | 最小 BW キュー（ディファレンシャル）と DSCP | 非ビジネス関連のトラフィックフロー、およびビジネス関連でないグループに割り当てられているアプリケーション（エンターテイメント向けのデータやメディアアプリケーションなど）。たとえば、YouTube、Netflix、iTunes、Xbox Live。 |

¹ VoIP シグナリングトラフィックは、コールシグナリングクラスに割り当てられます。

² ネットワーク制御トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。

³ OAM トラフィックはドロップされるべきではないため、このクラスでは WRED が有効になりません。

サービスプロバイダーのプロファイル

サービスプロバイダー（SP）プロファイルは、特定の WAN プロバイダーのサービスクラスを定義します。4 クラス、5 クラス、6 クラス、8 クラスのモデルを定義できます。

アプリケーションポリシーがデバイスに展開されると、各 SP プロファイルには、各 SP クラスを DSCP 値と帯域幅割当てのパーセンテージにマップする特定のサービスレベル契約（SLA）が割り当てられます。

アプリケーションポリシーを設定するときに SP プロファイルの DSCP 値と帯域幅割当てのパーセンテージをカスタマイズできます。

SP プロファイルを作成したら、そのプロファイルを WAN インターフェイスで設定する必要があります。

表 2:4 クラスでの SP プロファイルのデフォルト SLA 属性

| クラス名 | DSCP | プライオリティ クラス | SLA | |
|-----------|------|----------------|---------|----------------------------|
| | | | 帯域幅 (%) | Remaining Bandwidth (%) |
| 音声 | EF | はい | 10 | — |
| クラス 1 データ | AF31 | — | — | 44 |
| クラス 2 データ | AF21 | — | — | 25 |
| デフォルト | 0 | — | — | 31 |

表 3:5 クラスでの SP プロファイルのデフォルト SLA 属性

| クラス名 | DSCP | プライオリティ クラス | SLA | |
|-----------|-----------|----------------|---------|----------------------------|
| | | | 帯域幅 (%) | Remaining Bandwidth (%) |
| 音声 | EF | はい | 10 | — |
| クラス 1 データ | AF31 | — | — | 44 |
| クラス 2 データ | AF21 | — | — | 25 |
| クラス 3 データ | AF11 | — | — | 1 |
| デフォルト | ベスト エフォート | — | — | 30 |

表 4:6 クラスでの SP プロファイルのデフォルト SLA 属性

| クラス名 | DSCP | プライオリティ クラス | SLA | |
|-----------|------|----------------|---------|----------------------------|
| | | | 帯域幅 (%) | Remaining Bandwidth (%) |
| クラス 1 データ | AF31 | — | — | 10 |
| クラス 3 データ | AF11 | — | — | 1 |
| ビデオ | AF41 | — | — | 34 |
| 音声 | EF | はい | 10 | — |
| デフォルト | 0 | — | — | 30 |

| クラス名 | DSCP | プライオリティ クラス | SLA | |
|-----------|------|----------------|---------|----------------------------|
| | | | 帯域幅 (%) | Remaining Bandwidth (%) |
| クラス 2 データ | AF21 | — | — | 25 |

表 5:8 クラスでの SP プロファイルのデフォルト SLA 属性

| クラス名 | DSCP | プライオリティ クラス | SLA | |
|---------------------|------|----------------|---------|----------------------------|
| | | | 帯域幅 (%) | Remaining Bandwidth (%) |
| ネットワーク-コ ントロール管理 | CS6 | — | — | 5 |
| ストリーミング ビデオ | AF31 | — | — | 10 |
| コール シグナリ ング | CS3 | — | — | 4 |
| スカベンジャー | CS1 | — | — | 1 |
| インタラクティブ ビデオ | AF41 | — | — | 30 |
| 音声 | EF | はい | 10 | — |
| デフォルト | 0 | — | — | 25 |
| 重要なデータ | AF21 | — | — | 25 |

キューイング プロファイル

キューイング プロファイルでは、インターフェイス速度とトラフィック クラスに基づいたインターフェイスの帯域幅割り当てを定義することができます。



(注) キューイング プロファイルは、サービス プロバイダー プロファイルに接続されている WAN 側インターフェイスには適用されません。

次のインターフェイス速度がサポートされます。

- 100 Gbps
- 10/40 Gbps
- 1 Gbps

- 100 Mbps
- 10 Mbps
- 1 Mbps

インターフェイスの速度が 2 つのインターフェイス速度の間である場合、Cisco DNA Center は、より低いインターフェイス速度でインターフェイスを取り扱います。



(注) Cisco DNA Center は、正しいポリシーを適用するためにインターフェイスの動作速度の検出を試みます。ただし、スイッチポートが管理上ダウンしている場合、Cisco DNA Center は速度を検出できません。この場合、Cisco DNA Center は、インターフェイスのサポートされた速度を使用します。

キューイング ポリシーは、アプリケーション ポリシーの一部として定義します。アプリケーションポリシーを展開すると、サイト範囲内の選択されたサイトのデバイスが、割り当てられた LAN キューイング ポリシーで設定されます。LAN キューイング ポリシーが割り当てられていない場合、アプリケーションポリシーはデフォルトの CVD キューイング ポリシーを使用します。

すでに展開されているアプリケーション ポリシーのキューイング ポリシーを変更すると、ポリシーは失効し、変更をデバイスに適用するにはポリシーを展開しなおす必要があります。

キューイング ポリシーに関する次の追加の注意事項および制約事項に注意してください。

- LAN キューイング プロファイルは、ポリシーで使用されている場合には削除できません。
- ポリシーに関連付けられているキューイング プロファイルを更新すると、ポリシーは期限切れとしてマーキングされます。最新の変更をプロビジョニングするには、ポリシーを展開しなおす必要があります。
- トラフィック クラス キューイング をカスタマイズしても、シスコのサービスプロバイダー スイッチおよびルータのインターフェイスは影響を受けません。これらのインターフェイスの設定は、引き続き Cisco DNA Center を使用することなく実施します。

表 6: デフォルト CVD LAN キューイング ポリシー

| トラフィック クラス | デフォルトの帯域幅 (合計= 100%) ⁴ |
|-----------------|-----------------------------------|
| 音声 | 10 % |
| ブロードキャスト ビデオ | 10 % |
| リアルタイム インタラクティブ | 13 % |
| マルチメディア会議 | 10 % |
| マルチメディア ストリーミング | 10 % |
| ネットワーク制御 | 3 % |

| トラフィック クラス | デフォルトの帯域幅 (合計= 100%) ⁴ |
|--------------|-----------------------------------|
| シグナリング | 2 % |
| OAM | 2 % |
| トランザクション データ | 10 % |
| バルク データ | 4 % |
| スカベンジャー | 1 % |
| ベスト エフォート | 25 % |

⁴ 音声、ブロードキャストビデオ、およびリアルタイムインタラクティブトラフィッククラスの合計帯域幅を 33% 以下にすることを推奨します。

リソースが制限されているデバイスの処理順

ネットワーク デバイスの中には、ネットワーク アクセス コントロール リスト (ACL) および ACE を格納するためのメモリ (TCAM と呼ばれる) が制限されているものがあります。このため、アプリケーション用の ACL と ACE がこれらのデバイス上に設定されている場合は、利用可能な TCAM 領域が使用されます。When the TCAM space is depleted, QoS settings for additional applications cannot be configured on that device.

そのようなデバイスで最も重要なアプリケーションの QoS ポリシーが確実に設定されるように、Cisco DNA Center は次の順序で TCAM スペースを割り当てます。

1. [Rank] : カスタムアプリケーションおよびお気に入りのアプリケーションに割り当てられた番号 (ただし既存のデフォルト NBAR アプリケーションは除く)。ランクの番号が小さくなるほど、優先順位が高くなります。たとえば、ランク 1 のアプリケーションはランク 2 のアプリケーションよりも優先順位が高くなります。ランクがない場合は、優先順位が最も低くなります。



- (注)
- カスタム アプリケーションには、デフォルトでランク 1 が割り当てられています。
 - NBAR アプリケーションをお気に入りとしてマークすると、ランクは 1000 に設定されます。
2. [Traffic Class] : 優先順位は次の順序に基づいています。シグナリング、バルクデータ、ネットワーク制御、Operations Administration Management (Ops Admin Mgmt)、トランザクションデータ、スカベンジャー、マルチメディアストリーミング、マルチメディア会議、リアルタイムインタラクティブ、ブロードキャストビデオ、VoIP テレフォニー。
 3. [Popularity] : CVD の基準に基づいて割り当てられた番号 (1 ~ 10)。ポピュラリティの番号は変更できません。ポピュラリティが 10 のアプリケーションは、ポピュラリティが 9 のアプリケーションよりも優先順位が高くなります。



- (注)
- カスタムアプリケーションには、ポピュラリティ 0 が割り当てられます。
 - デフォルト NBAR アプリケーションには、CVD の基準に基づいてポピュラリティ番号 (1 ~ 10) が割り当てられます。アプリケーションをお気に入りとしてマークしても、ポピュラリティ番号は変わりません (ランクのみ変更されます)。
-
4. [Alphabetization] : 2 つ以上のアプリケーションのランクとポピュラリティ番号が同一の場合、それらのアプリケーションはアプリケーション名のアルファベット順にソートされ、ソート順に従い優先順位が割り当てられます。

たとえば、次のアプリケーションを指定したポリシーを定義する場合を想定しましょう。

- カスタム アプリケーション `custom_realtime`。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- カスタム アプリケーション `custom_salesforce`。デフォルトでランク 1 とポピュラリティ 10 が割り当てられています。
- `corba-iiop` という名前のトランザクション データ トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および (CVD に基づいて) ポピュラリティ 9 が付与されています。
- `gss-http` という名前の Ops Admin Mgmt トラフィック クラスのアプリケーション。お気に入りとして指定されており、ランク 10,000、および (CVD に基づいて) ポピュラリティ 10 が付与されています。
- 他のすべてのデフォルト NBAR アプリケーションにはランクはありませんが、トラフィック クラスと (CVD に基づいて) デフォルト ポピュラリティに従って処理されます。

優先順位付けのルールに従って、アプリケーションはデバイスにおいて次の順序で設定されます。

| アプリケーションの設定順 | 理由 |
|---|--|
| 1. カスタム アプリケーション <code>custom_realtime</code> | カスタム アプリケーションには最も高い優先順位が付与されます。 <code>custom_salesforce</code> アプリケーションと <code>custom_realtime</code> アプリケーションのランクおよびポピュラリティが同じであるとする、これらのアプリケーションはアルファベット順にソートされ、 <code>custom_realtime</code> が <code>custom_salesforce</code> より前になります。 |
| 2. カスタム アプリケーション <code>custom_salesforce</code> | |

| アプリケーションの設定順 | 理由 |
|---------------------------------|--|
| 3. お気に入りのアプリケーション gss-http | これら両方のアプリケーションはお気に入りとして指定されているため、同じアプリケーション ランクになります。そのため、Cisco DNA Center は各アプリケーションをトラフィック クラスに基づいて評価します。gss-http は、Ops Admin Mgmt トラフィック クラスであるため、先に処理され、その後にトランザクションデータ トラフィック クラスの corba-iiop アプリケーションが処理されます。トラフィック クラスによって処理順が決まっているため、ポピュラリティは考慮されません。 |
| 4. お気に入りのアプリケーション corba-iiop | |
| 5. 他のすべてのデフォルト NBAR アプリケーション | 他のすべてのアプリケーションは、トラフィック クラスとポピュラリティに従って次に優先され、ポピュラリティが同じアプリケーションは、アプリケーション名のアルファベット順にソートされます。 |

ポリシーのドラフト

ポリシーを作成するときに、ポリシーを展開せずにドラフトとして保存できます。ドラフトとして保存すると、後でポリシーを開いて変更できます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。



(注) ポリシーを保存または展開した後に、名前を変更することはできません。

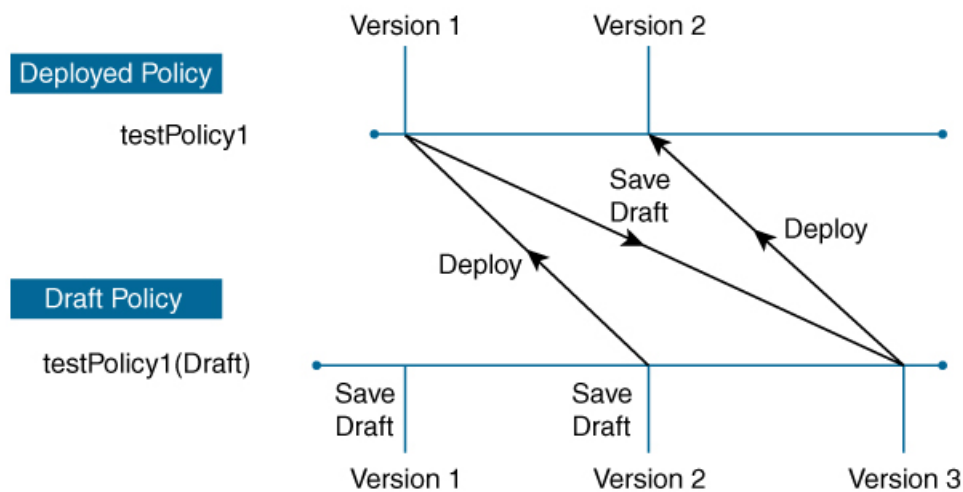
ドラフト ポリシーと展開したポリシーは相互に関連付けられますが、次のように独自にバージョン管理されます。

ポリシーをドラフトとして保存すると、Cisco DNA Center はポリシー名に (Draft) を追加してバージョン番号を 1 つ上げます。ポリシーを展開すると、Cisco DNA Center が展開したポリシーのバージョン番号を 1 つ上げます。

たとえば、次の図に示すように、testPolicy1 という名前のポリシーを作成してドラフトとして保存します。ポリシーは testPolicy1 (Draft)、バージョン番号 1 として保存されます。ドラフトを変更して、再度保存します。ポリシーの名前は同じ testPolicy1 (Draft) のままですが、バージョン番号は 2 に上がります。

ポリシーが気に入ったのでネットワークに展開します。ポリシーは testPolicy1 という名前で展開され、バージョン番号は 1 です。展開したポリシーを変更して、ドラフトとして保存します。ドラフト ポリシー testPolicy1 (Draft) は、バージョン番号 3 に上がります。最終的にそのバージョンを展開するとき、testPolicy1 はバージョン 2 になります。

図 1: 展開したポリシーとドラフトポリシーのバージョン管理



355556

ドラフトポリシーまたは展開したポリシーのいずれかを変更および保存するときは、ドラフトポリシーのバージョン番号が上がります。同様に、ドラフトポリシーまたは変更した展開済みポリシーのいずれかを展開するときは、展開したポリシーのバージョンが上がります。

展開したポリシーと同様に、ドラフトポリシーの履歴を表示し、以前のバージョンにロールバックすることができます。

ポリシーバージョンの履歴表示と以前のバージョンへのロールバックについては、[ポリシーのバージョン管理 \(32 ページ\)](#) を参照してください。

ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用される CLI を生成できます。

プレビュー操作では、ポリシーの CLI コマンドが生成され、デバイスの実行コンフィギュレーションの CLI コマンドと比較され、デバイスでポリシーを設定するのに必要な残りの CLI だけが返されます。

プレビュー出力の確認後、範囲内の全デバイスにポリシーを展開するか、ポリシーの変更を続行することができます。

Policy Precheck

アプリケーションポリシーを作成するとき、ポリシーを展開する前に、サイト範囲のデバイスでサポートされるかどうかを確認できます。事前チェック機能では、デバイスタイプ、モデル、ラインカード、およびソフトウェアイメージが作成したアプリケーションポリシーをサポートするかどうかをチェックします。これらのコンポーネントのいずれかがサポートされず Cisco DNA Center されていない場合、はデバイスの障害を報告します。Cisco DNA Center また、障害を修正する方法についても説明します。これらの対応で障害が修正されない場合、サイト範囲からデバイスを削除できます。

アプリケーションポリシーをそのまま展開すると、事前チェックプロセス中に障害が報告されたデバイスでポリシー展開が失敗します。失敗を回避するには、サイト範囲からデバイスを削除するか、デバイスコンポーネントをアプリケーションポリシーがサポートするレベルに更新します。サポート対象デバイスのリストについては、[Cisco DNA Center のサポート対象デバイスドキュメント](#)を参照してください。

ポリシーのスケジューリング

ポリシーを作成または変更した後に、そのポリシーを、ポリシーに関連付けられたデバイスに展開または再展開できます。このポリシーの展開/再展開は、すぐに行うことも、特定の日時（たとえば、週末のオフピーク時）に行うこともできます。ポリシー導入のスケジューリングは有線またはワイヤレスのデバイスに対して実施できます。

展開するポリシーのスケジュールを設定すると、そのポリシーとサイト範囲がロックされます。ポリシーの表示は可能ですが、編集することはできません。ポリシーを展開する予定が変更された場合は、その展開をキャンセルできます。



- (注) スケジュールイベントが発生すると、ポリシーは、さまざまなポリシーコンポーネント（アプリケーション、アプリケーションセット、およびキューイングプロファイルなど）に対して検証されます。この検証に失敗すると、ポリシーの変更は行われません。

ポリシーのバージョン管理

このポリシーのバージョン管理により、次のタスクが可能になります。

- 以前のバージョンと現在（最新）のバージョンを比較して相違点を確認する。
- ポリシーの以前のバージョンを表示し、サイト範囲内のデバイスに再適用するバージョンを選択する。

あるバージョンのポリシーを編集しても、そのポリシーの別のバージョンやポリシーのコンポーネント（そのポリシーによって管理されるアプリケーションセットなど）は影響を受けません。たとえば、ポリシーからアプリケーションセットを削除しても、そのアプリケーションセットは Cisco DNA Center、そのポリシーの別のバージョン、または他のポリシーからは削除されません。ポリシーとアプリケーションセットは互いに独立して存在するため、存在しなくなったアプリケーションセットを含むバージョンのポリシーを保持できます。存在しなくなったアプリケーションセットを参照するポリシーを展開しようとしたり、それらのポリシーを古いバージョンにロールバックしようとしたりすると、エラーが発生します。



- (注) ポリシーのバージョン管理では、アプリケーション（ランク、ポート、プロトコルなど）、アプリケーションセットメンバー、LAN キューイングプロファイル、およびサイトの変更は取得されません。

オリジナルポリシーの復元

初めてデバイスにポリシーを展開する際、Cisco DNA Center は、デバイスの元の Cisco Modular QoS CLI ポリシー設定をデタッチしますが、それらはデバイス上に残ります。Cisco DNA Center は、デバイスの元の NBAR 設定を Cisco DNA Center に保存します。このアクションにより、必要に応じてオリジナルのモジュラー式 QoS CLI ポリシーと NBAR 設定を後でデバイスに復元することが可能になります。



(注) このようにモジュラー式 QoS CLI ポリシーはデバイスから削除されませんが、ユーザがこれらのポリシーを削除すると、元のポリシー復元する Cisco DNA Center の機能を使用してそれらを復元することができなくなります。

元のポリシー設定をデバイスに復元する際、Cisco DNA Center は、展開されている既存のポリシー設定を削除し、デバイス上にあった元の設定に戻します。

アプリケーションポリシーを展開する前に存在していたモジュラー式 QoS CLI ポリシー設定はすべて、インターフェイスに再アタッチされます。ただし、マルチレイヤスイッチング (MLS) 設定などのキューイングポリシーは復元されません。代わりに、デバイスは、Cisco DNA Center によって最後に適用された MLS 設定を維持します。

元のポリシー設定をデバイスに復元すると、Cisco DNA Center に保存されているポリシーが削除されます。

この機能には、次のような追加のガイドラインと制限事項があるので、注意してください。

- 初めてポリシーをデバイスに展開する試みが失敗すると、Cisco DNA Center は、元のポリシー設定をデバイスに復元することを自動的に試みます。
- そのポリシーがデバイスに適用された後にデバイスがアプリケーションポリシーから削除された場合、そのポリシーはデバイス上に残ります。Cisco DNA Center は、ポリシーを自動的に削除したり、デバイスの QoS 設定を元の (事前 Cisco DNA Center) 設定に復元したりしません。

陳腐化したアプリケーションポリシー

ポリシーで参照されているものの設定を変更すると、アプリケーションポリシーが陳腐化する可能性があります。アプリケーションポリシーが陳腐化した場合、変更を有効化するためにアプリケーションポリシーを再展開する必要があります。

アプリケーションポリシーは、次の理由で陳腐化する可能性があります。

- アプリケーション設定で参照されているアプリケーションの変更。
- SP プロファイルの割り当て、WAN サブ回線のレート、WAN または LAN マーキングなどのインターフェイスの変更。
- キューイングプロファイルの変更。

- ポリシーの親サイト下への新規サイトの追加。
- ポリシーによって参照されるサイトへのデバイスの追加。
- ポリシーが同じサイト間でのデバイスの移動。
- インターフェイス除外/包含の変更。
- デバイスコントローラベースのアプリケーション認識 (CBAR) ステータスの変更

アプリケーションポリシーのガイドラインと制限事項

- Cisco DNA Center は、ワイヤレスコントローラ (WLC) 上で同じ SSID 名を使用して複数のワイヤレス LAN (WLAN) を学習することはできません。WLC には、名前は同じで WLAN プロファイル名が異なる複数のエントリを含めることもできますが、Cisco DNA Center はどの時点においても、一意の名前を持つ WLAN に対するエントリを 1 つだけ持ちます。

WLC ごとに重複する SSID 名を意図的に持つことも、Cisco DNA Center を使用して重複する SSID 名を持つ WLC を誤って追加してしまうこともあります。いずれの場合も、WLC ごとに重複する SSID 名を持つことは一部の機能にとって問題になります。

- [Learn Config] : Cisco DNA Center は WLC ごとにランダムに選択された 1 つの SSID 名のみ学習し、残りの重複する SSID 名はすべて破棄します。([設定の学習 (Learn Config)] は、通常はブラウフィールドシナリオで使用されます)。
- [Application Policy] : Cisco DNA Center は、アプリケーションポリシーの展開時に、重複するいずれかの SSID 名にのみポリシーをランダムに適用して、他には適用しません。さらに、ポリシーの復元、CLI プレビュー、EasyQoS ファーストトレイン、および PSK オーバーライド機能が失敗するか、予期しない結果が生じることになります。
- [Multiscale Network] : MULTISCALE ネットワークでは、複数のデバイスの複数の重複する SSID 名が原因で問題が発生することもあります。たとえば、1 台のデバイスには非ファブリック SSID として WLAN が設定されていて、2 台目のデバイスには同じ WLAN がファブリック SSID として設定されている場合、[設定の学習 (Learn Config)] を実行すると、1 つの SSID 名のみ学習されます。その他のデバイスの他の SSID 名は破棄されます。この動作により、特に、2 台目のデバイスがファブリック SSID 名のみサポートしていて、Cisco DNA Center が非ファブリック SSID 名を持つデバイスに対して操作を実行しようとする場合に競合が生じることがあります。
- [IPACL Policy] : Cisco DNA Center は、IPACL ポリシーの展開時に、重複する SSID のいずれか 1 つにのみランダムにポリシーを適用します。また、Flex Connect が関係するシナリオも影響を受けます。
- Cisco DNA Center では、デバイス設定に対するアウト オブ バンド (OOB) の変更は推奨されません。OOB に変更を加えると、Cisco DNA Center のポリシーとデバイスに設定されているポリシーは一貫性のない状態になります。2 つのポリシーは、Cisco DNA Center のポリシーをデバイスに再度展開するまで一貫性のない状態のままになります。

- QoS trust 機能は変更できません。

アプリケーションポリシーの管理

ここでは、アプリケーションポリシーの管理の方法に関する情報について説明します。

前提条件

アプリケーションポリシーを設定する場合は、次の要件を満たしていることを確認してください。

- Cisco DNA Center は、ほとんどの Cisco LAN、WAN、WLAN デバイスをサポートします。お使いのネットワーク内でデバイスとソフトウェアバージョンがサポートされているかどうかを確認するには、[Cisco DNA Center のサポート対象デバイス](#) を参照してください。
- ISR-G2、ASR 1000、ワイヤレス LAN コントローラなど、シスコのネットワーク デバイスに AVC (Application Visibility and Control) 機能のライセンスがインストールされていることを確認します。詳細については、「[NBAR2 \(Next Generation NBAR\) Protocol Pack FAQ](#)」を参照してください。
- AVC サポートは、スイッチで自動 QoS が設定されていない場合にのみ、IOS-XE バージョン 16.9 を実行しているスイッチで使用できます。AVC サポートを利用するには、自動 QoS 設定のスイッチを IOS-XE バージョン 16.11 以降にアップグレードする必要があります。
- ポリシーが必要な WAN インターフェイスを Cisco DNA Center で特定するには、インターフェイス タイプ (WAN) および (必要に応じて) 副回線レートとサービス プロバイダーのサービス クラス モデルを指定する必要があります。詳細については、[サービス プロバイダー プロファイルの WAN インターフェイスへの割り当て \(50 ページ\)](#) を参照してください。
- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、[デバイスのロールの変更 \(インベントリ\)](#) を参照してください。


アプリケーションポリシーの作成

ここでは、アプリケーションポリシーの作成方法について説明します。

始める前に

- ビジネス目標を定義します。たとえば、ネットワーク応答時間を最小化させたり、非ビジネスアプリケーションを特定して優先度を下げたりすることで、ユーザの生産性を向上させるようなものです。これらの目標に基づいて、どのビジネスとの関連性カテゴリがアプリケーションに分類されるかを決定します。
- インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスクバリ機能を使用して検出します。

- ディスカバリプロセス中にデバイスに割り当てられたデバイスロールが、ネットワークに適切であることを確認します。必要に応じて、不適切なデバイスロールを変更します。詳細については、[デバイスのロールの変更（インベントリ）](#)を参照してください。
- サイトへのデバイスの追加詳細については、「[デバイスをサイトに追加する](#)」を参照してください。
- Cisco DNA Center で定義されていないアプリケーションがある場合、それらを追加し、QoS 属性を定義することができます。詳細については、「[カスタムアプリケーション](#)」を参照してください。
- SP 向けのトラフィック用に対してこのポリシーを SP プロファイルで設定する場合は、SP プロファイルが設定されていることを確認してください。アプリケーションポリシーの作成後に SP プロファイルに戻り、SLA 属性をカスタマイズして SP プロファイルを WAN インターフェイスに割り当てます。詳細については、「[サービス プロバイダー プロファイルの設定](#)」を参照してください。
- デバイス上にあるアプリケーションより先に一部のアプリケーションを設定する場合は、それらのアプリケーションをお気に入りとしてマークします。詳細については、「[アプリケーションをお気に入りにする](#)」を参照してください。


-
- ステップ 1** Cisco DNA Center のホームページで、**[Policy] > [Application] > [Application Policies]** の順に選択します。
- ステップ 2** [ポリシーの追加 (Add Policy)] をクリックします。
- ステップ 3** [アプリケーション ポリシー名 (Application Policy Name)] フィールドに、ポリシーの名前を入力します。
- ステップ 4** [有線 (Wired)] または [ワイヤレス (Wireless)] ラジオ ボタンのいずれかを選択します。
- ステップ 5** ワイヤレスネットワークの場合は、[SSID] ドロップダウンリストからプロビジョニングされた SSID を選択します。
- ステップ 6** [サイトの範囲 (Site Scope)] をクリックし、展開するポリシーの横にあるチェック ボックスをオンにします。
- (注) 有線デバイスのポリシーでは、別のポリシーに割り当て済みのサイトは選択することができません。ワイヤレス デバイスのポリシーでは、同じ SSID で別のポリシーに割り当て済みのサイトを選択することができません。
- ステップ 7** 有線デバイスのポリシーでは、デバイスまたは特定のインターフェイスがポリシーで設定されないようにすることができます。
- a) [サイトの範囲 (Site Scope)] ペインで、興味のあるサイトの横にある  をクリックします。
選択した範囲内のデバイスのリストが表示されます。
 - b) 除外するデバイスを見つけ、関連する [ポリシーの除外 (Policy Exclusions)] 列にあるトグル ボタンをクリックします。
 - c) 特定のインターフェイスを除外するには、[Exclude Interfaces] をクリックします。

- d) [Applicable Interfaces] のリストから、除外するインターフェイスの横にあるトグルボタンをクリックします。

デフォルトでは、[Applicable Interfaces] のみが表示されます。すべてのインターフェイスを表示するには、[Show] ドロップダウンリストから [All] を選択します。

- e) [< サイト名のデバイスへ戻る] をクリックします。
f) [< サイト範囲へ戻る (< Back to Site Scope)] をクリックします。

ステップ 8 WAN デバイスでは、特定のインターフェイスを設定できます。

- a) [サイトの範囲 (Site Scope)] ペインで、興味のあるサイトの横にある  をクリックします。
b) サイト内のデバイスのリストで、興味のあるデバイスの横にある [SP プロファイルの設定 (SP Profile Settings)] 列の [設定 (Configure)] をクリックします。

(注) このオプションは、ルータの場合にのみ使用可能です。

- c) [WAN インターフェイス (WAN Interface)] 列で、[インターフェイスの選択 (Select Interface)] ドロップダウン リストからインターフェイスを選択します。
d) [ロール (Role)] 列で[ロールの選択 (Select Role)] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。

• **物理インターフェイス** : **WAN** を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。

• **トンネル インターフェイス** : [DMVPN ブランチ (DMVPN Branch)] または のいずれかを選択します。[DMVPN ハブ (DMVPN Hub)] を選択した場合、関連するブランチに帯域幅を定義することもできます。

(注) これらのポリシー設定を展開する前に、デバイスにトンネルインターフェイスが作成されていることを確認します。

- e) [サービスプロバイダープロファイル (Service Provider Profile)] 列で、[プロファイルの選択 (Select Profile)] ドロップダウン リストから SP プロファイルを選択します。
f) (任意) 必要に応じて、[サブ回線のレート (Mbps) (Sub-Line Rate (Mbps))] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。
g) (任意) 追加の WAN インターフェイスを設定するには、[+] をクリックし、手順 c ~ f を繰り返します。
h) [Save] をクリックします。
i) [< サイト範囲へ戻る (< Back to Site Scope)] をクリックします。

ステップ 9 [サイトの範囲 (Site Scope)] ペインで、[OK] をクリックします。

ステップ 10 (任意) Cisco Validated Design (CVD) キューイング プロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

- a) [キューイング プロファイル (Queuing Profiles)] をクリックします。
b) 左ペインのリストから、キューイング プロファイルを選択します。
c) [Select] をクリックします。

ステップ 11 (任意) このポリシーが SP 向けトラフィックである場合は、SP プロファイルの SLA 属性をカスタマイズします。


- a) [SP プロファイル (SP Profile)] をクリックします。
- b) SP プロファイルを選択します。
- c) SLA 属性をカスタマイズします ([DSCP]、[SP 帯域幅 (%) (SP Bandwidth %)]、および [キューイング帯域幅 (%) (Queuing Bandwidth %)])。

ステップ 12 (任意) ネットワークで使用されるアプリケーションセットのビジネスとの関連性を設定します。

Cisco DNA Center には、ビジネス関連性グループに事前設定されたアプリケーションセットが付属しています。あるビジネス関連性グループから別のグループにアプリケーションセットをドラッグアンドドロップして、この設定を維持したり、変更したりすることができます。

お気に入りとしてマークされたアプリケーションは、アプリケーションセットの上部に表示されます。お気に入りを変更するには、[Applications registry] に移動します。詳細については、[アプリケーションをお気に入りにする](#)を参照してください。

ステップ 13 (任意) コンシューマを作成してアプリケーションに割り当てるか、アプリケーションを双方向としてマークすることにより、アプリケーションをカスタマイズします。

- a) アプリケーショングループを展開します。
- b) 興味のあるアプリケーションの横にある歯車のアイコン  をクリックします。
- c) [トラフィックの方向 (Traffic Direction)] エリアで、[単方向 (Unidirectional)] または [双方向 (Bi-directional)] ラジオ ボタンを選択します。
- d) 既存のコンシューマを選択するには、[コンシューマ (Consumer)] ドロップダウンリストから設定するコンシューマを選択します。新しいコンシューマを作成するには、[+ コンシューマの追加 (+ Add Consumer)] をクリックして、[コンシューマ名 (Consumer Name)]、[IP/サブネット (IP/Subnet)]、[プロトコル (Protocol)]、および [ポート/範囲 (Port/Range)] を定義します。
- e) [OK] をクリックします。

ステップ 14 ホストトラッキングを設定します。[ホストトラッキング (Host Tracking)] トグル ボタンをクリックして、ホストトラッキングのオンとオフを切り替えます。

アプリケーションポリシーを展開する際に、Cisco DNA Center では、コラボレーションエンドポイント (テレプレゼンス ユニットやシスコ電話など) が接続されているスイッチに、ACLのエントリを自動的に適用します。

ACE は、コラボレーションエンドポイントによって生成された音声およびビデオトラフィックと一致し、音声およびビデオトラフィックが正しくマークされるようにします。

ホストトラッキングが開始されると、Cisco DNA Center はサイトの範囲内でコラボレーションエンドポイントの接続をトラッキングし、コラボレーションエンドポイントがネットワークに接続されるか、1つのインターフェイスから別のインターフェイスに移動したときに、ACL エントリを自動的に再設定します。

ホストトラッキングが終了すると、Cisco DNA Center は、コラボレーションエンドポイントが新しいインターフェイスに移動または接続したときに、デバイスにポリシーを自動的に展開しません。代わりに、コラボレーションエンドポイントで正しく設定されるように、ACLのポリシーを再展開する必要があります。

ステップ 15 (任意) デバイスに送信される CLI コマンドをプレビューします。詳細については、「[アプリケーションポリシーのプレビュー \(45 ページ\)](#)」を参照してください。

ステップ 16 (任意) ポリシーを展開するデバイスを事前にチェックします。詳細については、「[アプリケーションポリシーの事前チェック \(46 ページ\)](#)」を参照してください。

ステップ 17 次のいずれか 1 つのタスクを実行します。

- [ドラフトの保存 (Save Draft)] をクリックして、ポリシーをドラフトとして保存します。詳細については、「[ポリシーのドラフト \(30 ページ\)](#)」を参照してください。
- [展開 (Deploy)] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

ポリシーをすぐに展開するには、[今すぐ実行 (Now)] ラジオボタンをクリックし、[適用 (Apply)] をクリックします。

将来の日付と時刻でポリシー展開をスケジュールするには、[後で実行 (Later)] ラジオ ボタンをクリックし、展開する日時を定義します。詳細については、[ポリシーのスケジュールリング \(32 ページ\)](#) を参照してください。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーションポリシー情報の表示

作成および展開したアプリケーション ポリシーに関するさまざまな情報を表示できます。

始める前に

少なくとも 1 つの展開されたアプリケーション ポリシーがなければなりません。

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。

ステップ 2 ポリシーを名前ですべて替えたり、名前、ステータス、キューイングプロファイルによってフィルタ処理したりします。

ステップ 3 ポリシーのリストと、それぞれに関する次の情報が表示されます。

- [ポリシー名 (Policy Name)] : ポリシーの名前。
- バージョン (Version) : ポリシーのバージョン。ポリシーが展開されるか、または、ドラフトとして保存されるたびに、バージョンが 1 ずつ増分されます。たとえば、ポリシーを作成して展開すると、ポリシーはバージョン 1 になります。ポリシーを変更して、再度展開すると、ポリシーのバージョンはバージョン 2 に増分されます。詳細については、[ポリシーのドラフト \(30 ページ\)](#) および [ポリシーのバージョン管理 \(32 ページ\)](#) を参照してください。

- **ポリシーのステータス (Policy Status)** : ポリシーの状態。Cisco Catalyst 3850、Catalyst 4500、および Catalyst 9K デバイスに適用されたポリシーがポートチャネルの更新 (作成/変更/削除) によって影響を受ける場合は、アラートがポリシーステータスに表示されます。
- **導入ステータス (Deployment Status)** : 最新の導入の状態 (デバイスごと)。次の概要を示します。
 - 正常にプロビジョニングされたデバイス
 - プロビジョニングに失敗したデバイス
 - 導入が中止されたために、プロビジョニングされなかったデバイス

最新の導入の状態をクリックすると、[ポリシーの展開 (Policy Deployment)] ウィンドウが表示され、ポリシーが展開されたデバイスのフィルタ処理可能なリストが示されます。デバイスごとに、次の情報が表示されます。

- デバイスの詳細 (名前、サイト、タイプ、ロール、および IP アドレス)
- 成功した導入のステータス。ステータスの横にある歯車アイコンをクリックすると、デバイスに展開された有効なマーキングポリシーの詳細が表示されます。TCAM リソースまたは古い NBAR プロトコルパックに限定されているデバイスの場合は、ポリシーに含まれるアプリケーションのサブセットのみをプロビジョニングでき、それらがビューで表示されます。
- 障害ステータスには、障害の理由が示されます。
- **スコープ (Scope)** : ポリシーに割り当てられているサイト (デバイスではなく) の数。ワイヤレスデバイスのポリシーの場合は、ポリシーの適用先の SSID の名前が含まれます。
- **LAN キューイングプロファイル (LAN Queuing Profile)** : ポリシーに割り当てられている LAN キューイングプロファイルの名前。

アプリケーションポリシーの編集

アプリケーションポリシーを編集できます。

始める前に

少なくとも 1 つのポリシーを作成しておく必要があります。

- ステップ 1** Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
- ステップ 2** 編集するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ 3** 対応するポリシーの横にあるラジオ ボタンをクリックします。
- ステップ 4** [Actions] ドロップダウン リストから、[Edit] を選択します。
- ステップ 5** 必要に応じて、アプリケーションポリシーを変更します。

ステップ6 アプリケーションのビジネスとの関連性を変更するには、ビジネス関連、ビジネスと無関係、およびデフォルトグループの間でアプリケーションセットを移動します。

アプリケーションポリシーの設定については、[アプリケーションポリシーの作成 \(35 ページ\)](#) を参照してください。

ステップ7 キューイングプロファイルを更新するには、[Queuing Profiles] をクリックし、左ペインのリストからキューイングプロファイルを選択します。

ステップ8 [Select] をクリックします。

ステップ9 次のいずれか1つのタスクを実行します。

- [ドラフトの保存 (Save Draft)] をクリックして、ポリシーをドラフトとして保存します。詳細については、「[ポリシーのドラフト \(30 ページ\)](#)」を参照してください。
- [展開 (Deploy)] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

ポリシーをすぐに導入するには、[今すぐ実行 (Run Now)] ラジオボタンをクリックし、[適用 (Apply)] をクリックします。

将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール (Schedule Later)] ラジオボタンをクリックし、導入する日時を定義します。詳細については、[ポリシーのスケジュールリング \(32 ページ\)](#) を参照してください。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーションポリシーのドラフトの保存

ポリシーを作成、編集、または複製する際、ドラフトとして保存し、後で変更を続けることができます。また、展開したポリシーを変更して、ドラフトとして保存することもできます。

ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。

ステップ2 ポリシーを[アプリケーションポリシーの作成](#)、[アプリケーションポリシーの編集](#)、または[アプリケーションポリシーの複製](#)します。

ステップ3 [ドラフトの保存 (Save Draft)] をクリックします。

詳細については、[ポリシーのドラフト \(30 ページ\)](#) を参照してください。

アプリケーションポリシーの展開

新しいアプリケーションの追加や、アプリケーションをお気に入りとしてマークするなど、ポリシーの設定に影響する変更を加えた場合は、これらの変更を実装するポリシーを再展開する必要があります。



(注) Cisco Catalyst 3850、Catalyst 3650、および IOS バージョン 16.x 以降がインストールされた Catalyst 9K デバイスでは、ポリシーを展開する前に、自動 QoS 設定が自動的に削除されます。

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。

ステップ 2 導入するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。

ステップ 3 導入するポリシーの横のラジオ ボタンをクリックします。

ステップ 4 [アクション (Actions)] ドロップダウンリストから、[導入 (Deploy)] を選択します。

a) ポリシーを再展開すると、ポリシーの範囲から削除されたデバイスに対して適切なアクションを実行するように求められます。次のいずれかの適切なアクションを選択します。

- Delete policy from the devices (Recommended)
- ポリシーの範囲からデバイスを削除する
- ポリシーの範囲からデバイスを削除し、デバイスをブラウンフィールド設定に復元する

b) [Apply] をクリックします。

ステップ 5 ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。次のいずれかを実行します。

- ポリシーをすぐに導入するには、[今すぐ実行 (Run Now)] ラジオ ボタンをクリックし、[適用 (Apply)] をクリックします。
- 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール (Schedule Later)] ラジオ ボタンをクリックし、導入する日時を定義します。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

ポリシー導入のキャンセル

[導入 (Deploy)] をクリックすると、Cisco DNA Center は、サイト範囲内のデバイスに関するポリシーの設定を開始します。間違いがあることに気付いた場合は、ポリシーの導入をキャンセルできます。

ポリシー設定プロセスはバッチ処理として実行され、一度に40台のデバイスが設定されます。したがって、デバイスが40台以下の場合にポリシーの導入をキャンセルしても、デバイスの最初のバッチへの導入がすでに行われているため、デバイスが設定されている可能性があります。ただし、何百台ものデバイスがある場合は、必要に応じてポリシー導入のキャンセルを活用できます。

[中止 (Abort)] をクリックすると、Cisco DNA Centerによって設定がまだ開始されていないデバイスの設定プロセスがキャンセルされ、デバイスのステータスが [ポリシーの中止 (Policy Aborted)] に変更されます。Cisco DNA Center では、完了している、または完了する予定の処理での導入はキャンセルされません。これらのデバイスでは、更新されたポリシー設定が維持され、ポリシー設定の状態 (設定中、成功、または失敗) が反映されます。

手順

ポリシー導入中に [中止 (Abort)] をクリックしてポリシー設定プロセスをキャンセルします。

アプリケーションポリシーの削除

不要になったアプリケーションポリシーを削除できます。

ポリシーを削除すると、クラスマップ、ポリシーマップ、およびポリシーマップとワイヤレスポリシープロファイルの関連付けが削除されます。

- ステップ 1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
- ステップ 2 削除するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ 3 削除するポリシーの横にあるラジオ ボタンを選択します。
- ステップ 4 [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。
- ステップ 5 [Undeploy Policy] ウィンドウで、[Delete policy from devices] ラジオボタンをクリックし、[Apply] をクリックします。
- ステップ 6 削除を確定する場合は、[OK] をクリックします。それ以外の場合は、[キャンセル (Cancel)] をクリックします。
- ステップ 7 削除を確認するメッセージが表示されたら、[OK] を再度クリックします。

[Application Policies] ページで、ポリシーの削除ステータスを表示できます。ステータスに [deletion failed] と表示された場合は、次の手順を実行します。

- a) [Application Policies] ページの [Deployment Status] の下にある失敗状態リンクをクリックします。
- b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを削除します。

アプリケーションポリシーの複製

既存のアプリケーションポリシーに、新しいポリシーに必要な設定のほとんどが含まれている場合は、既存のポリシーの複製し、変更してから異なる範囲に展開することで時間を節約できます。

始める前に

少なくとも1つのポリシーを作成しておく必要があります。

-
- ステップ1** Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
- ステップ2** 複製するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ3** 複製するポリシーの横にあるラジオ ボタンを選択します。
- ステップ4** [アクション (Actions)] ドロップダウンリストから、[複製 (Clone)] を選択します。
- ステップ5** 必要に応じてアプリケーションポリシーを設定します。アプリケーションポリシーの設定については、[アプリケーションポリシーの作成 \(35 ページ\)](#) を参照してください。
- ステップ6** 次のいずれか1つのタスクを実行します。

- [ドラフトの保存 (Save Draft)] をクリックして、ポリシーをドラフトとして保存します。詳細については、「[ポリシーのドラフト \(30 ページ\)](#)」を参照してください。
- [展開 (Deploy)] をクリックしてポリシーを展開します。ポリシーを今すぐ展開するか、または後でスケジュールできます。

ポリシーをすぐに導入するには、[今すぐ実行 (Run Now)] ラジオボタンをクリックし、[適用 (Apply)] をクリックします。

将来の日付と時刻でポリシー展開をスケジュールするには、[後でスケジュール (Schedule Later)] ラジオボタンをクリックし、展開する日時を定義します。詳細については、[ポリシーのスケジュールリング \(32 ページ\)](#) を参照してください。

(注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

アプリケーションポリシーの復元

ポリシーを作成または変更してから、最初からやり直すことを決定した場合、Cisco DNA Center を使ってこれを設定する前に、デバイスにあった元の QoS 設定を復元することができます。

-
- ステップ1** Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
- ステップ2** リセットするポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ3** ポリシーの横にあるラジオ ボタンをクリックします。
- ステップ4** [Actions] ドロップダウンリストから、[Undeploy Policy] を選択します。
- ステップ5** In the **Undeploy Policy** window, click the **Restore devices to original configurations** radio button and click **Apply**.
- ステップ6** [OK] をクリックして変更を確認するか、[Cancel] をクリックして中止します。

You can view the restoration status of the policies in the **Application Policies** page. ステータスに [restoration failed] と表示された場合は、次の手順を実行します。

- a) Click the failed state link under **Deployment Status** in the **Application Policies** page.
- b) [Undeployment Status] ウィンドウで、[Retry] をクリックしてポリシーを復元します。

デフォルトの CVD アプリケーション ポリシーをリセット

CVD 設定は、アプリケーションのデフォルト設定です。ポリシーの作成または変更を行った後で最初からやり直す必要が生じた場合は、アプリケーションを CVD 設定にリセットすることができます。CVD 設定の詳細については、[アプリケーション ポリシー \(19 ページ\)](#) を参照してください。

- ステップ 1** Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。
- ステップ 2** リセットするポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ 3** ポリシーの横にあるラジオ ボタンをクリックします。
- ステップ 4** [Actions] ドロップダウン リストから、[Edit] を選択します。
- ステップ 5** [シスコ検証済みデザインのリセット (Reset to Cisco Validated Design)] をクリックします。
- ステップ 6** [OK] をクリックして変更を確認するか、[Cancel] をクリックして中止します。
- ステップ 7** 次のいずれか 1 つのタスクを実行します。
 - ポリシーのドラフトを保存するには、[ドラフトの保存 (Save Draft)] をクリックします。
 - ポリシーを展開するには、[展開 (Deploy)] をクリックします。

アプリケーション ポリシーのプレビュー

ポリシーを展開する前に、デバイスに適用する CLI を生成して設定をプレビューできます。

- ステップ 1** Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。
- ステップ 2** [アプリケーションポリシーの作成 \(35 ページ\)](#) または [アプリケーションポリシーの編集 \(40 ページ\)](#) の説明に従って、ポリシーを作成または編集します。
- ステップ 3** ポリシーを展開する前に、[プレビュー (Preview)] をクリックします。
範囲内のデバイスのリストが表示されます。
- ステップ 4** 対象のデバイスの横にある [生成 (Generate)] をクリックします。
Cisco DNA Center により、ポリシーの CLI が生成されます。

ステップ5 [表示 (View)] をクリックして CLI を表示するか、CLI をクリップボードにコピーします。

アプリケーションポリシーの事前チェック

アプリケーションポリシーを展開する前に、サイト範囲内のデバイスがサポート対象であるかどうかをチェックできます。事前チェックプロセスには、デバイスのモデル、ラインカード、およびソフトウェアイメージの検証が含まれます。

ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。

ステップ2 [アプリケーションポリシーの作成 \(35 ページ\)](#) または [アプリケーションポリシーの編集 \(40 ページ\)](#) の説明に従って、ポリシーを作成または編集します。

ステップ3 [事前チェック (Pre-check)] をクリックします。

Cisco DNA Center は、デバイスをチェックして、問題があれば [事前チェック結果 (Pre-Check Result)] 列に内容を報告します。[Errors] タブには、このポリシーをサポートしていないデバイスが表示されます。[Warnings] タブには、デバイスにこのポリシーを展開することを選択した場合に、サポートされていない制限や機能が表示されます。[Warnings] タブに一覧表示されているデバイスのポリシーを展開することもできます。問題を解決するには、[Cisco DNA Center のサポート対象デバイス](#)に記載されている仕様にデバイスを準拠させます。

アプリケーションポリシー履歴の表示

アプリケーションポリシーのバージョン履歴を表示できます。バージョン履歴には、ポリシーのシリーズ番号 (反復) と、バージョンが保存された日付と時刻が含まれています。

ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。

ステップ2 表示したいポリシーの横にあるラジオ ボタンをクリックします。

ステップ3 [アクション (Actions)] ドロップダウンリストから、[履歴 (History)] を選択します。

ステップ4 [ポリシー履歴 (Policy History)] ダイアログボックスでは、次のことを実行できます。

- 現在のバージョンとバージョンを比較するには、関心のあるバージョンの横にある [差異 (Difference)] をクリックします。
- ポリシーの前のバージョンにロールバックするには、ロールバック先となるバージョンの横にある [ロールバック (Rollback)] をクリックします。

ポリシーの以前のバージョンにロールバック

ポリシー設定を変更し、その後その設定が不適切だと判明した場合、またはネットワークで目的の効果が得られなかった場合、最大で5バージョン前のポリシーに戻すことができます。

始める前に

以前のポリシーバージョンにロールバックするには、少なくとも2つのポリシーバージョンを作成しておく必要があります。

-
- ステップ 1** Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーションポリシー (Application Policies)] の順に選択します。
- ステップ 2** 表示したいポリシーの横にあるラジオ ボタンをクリックします。
- ステップ 3** [アクション (Actions)] ドロップダウンリストから、[履歴の表示 (Show History)] を選択します。
- 選択したポリシーの以前のバージョンは降順に表示され、最も新しいバージョン (最も大きい番号) が一覧の最上部に表示され、最も古いバージョン (最も小さい番号) が最下部に表示されます。
- ステップ 4** (任意) 選択したバージョンと最新バージョンの間の差異を表示するには、[View] 列で [Difference] をクリックします。
- ステップ 5** ロールバックする先のポリシーバージョンを決定した場合、そのポリシーバージョンに対して [Rollback] をクリックします。
- (注) 選択したサイトの範囲がポリシーバージョン間で変更された場合、ロールバックは選択されている現在 (最新) のサイトでは行われません。ポリシーのコンテンツのみがロールバックされます。
- ステップ 6** [OK] をクリックして、ロールバック手順を確定します。
- ロールバック先のバージョンが最新バージョンになります。
-

キューイング プロファイルの管理

次のセクションでは、キューイングプロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

キューイング プロファイルの作成

Cisco DNA Center では、デフォルトの CVD キューイング プロファイル (CVD_QUEUING_PROFILE) を提供します。このキューイングプロファイルがニーズを満たしていない場合は、カスタム キューイング プロファイルを作成することができます。

-
- ステップ 1** Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [キューイング プロファイル (Queuing Profile)] の順に選択します。
- ステップ 2** [プロファイルを追加 (Add Profile)] をクリックします。

ステップ 3 [Profile Name] フィールドに、プロファイルの名前を入力します。

ステップ 4 スライダを使用して各トラフィック クラスに帯域幅を設定します。プラス記号 (+) またはマイナス (-) 記号をクリックするか、フィールドに特定の数値を入力します。

数値は、選択したアプリケーションクラスに確保されるインターフェイス帯域幅の合計に対しての割合を示します。帯域幅の合計は 100 なので、1つのアプリケーションクラスに帯域幅を追加すると、別のアプリケーションクラスから帯域幅が差し引かれます。

開いた錠のアイコンは、そのアプリケーションクラスの帯域幅を編集できることを示します。閉じた錠のアイコンは、編集できないことを示します。

間違えた場合は、[シスコ検証済みデザインのリセット (Reset to Cisco Validated Design)] をクリックして CVD 設定に戻ることができます。

中央のグラフは、各アプリケーションクラスを設定している帯域幅の量の視覚化に役立ちます。

ステップ 5 (高度なユーザ向け) Cisco DNA Center が各トラフィック クラスで使用する DSCP コードポイントをカスタマイズするには、[表示 (Show)] ドロップダウンリストで、[DSCP値 (DSCP Values)] を選択し、フィールドに特定の数値を入力して、各アプリケーションクラスの値を設定します。

SP のクラウド内で必要な DSCP コードポイントをカスタマイズするには、SP のプロファイルを設定します。

ステップ 6 [Save] をクリックします。

キューイング プロファイルの編集または削除

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [キューイング プロファイル (Queuing Profile)] の順に選択します。

ステップ 2 [キューイング プロファイル (Queuing Profile)] ペインで、編集または削除するキューイング プロファイルの横にあるラジオ ボタンをクリックします。

ステップ 3 次のいずれか 1 つのタスクを実行します。

- プロファイルを編集するには、プロファイル名を除くフィールドの値を変更し、[保存 (Save)] をクリックします。フィールドの詳細については、[キューイング プロファイルの作成 \(47 ページ\)](#) を参照してください。
- プロファイルを削除するには、[削除 (Delete)] をクリックします。

(注) アプリケーションポリシーによって参照されている場合は、キューイングプロファイルを削除できません。

WAN インターフェイスのアプリケーション ポリシーの管理

次のセクションでは、WAN インターフェイスのアプリケーション プロファイルを管理するために実行できるさまざまなタスクについて詳しく説明します。

サービス プロバイダー プロファイルの SLA 属性をカスタマイズ

自身のクラスモデルによって SP プロファイルに割り当てられたデフォルトの SLA 属性を使用しない場合は、要件に合わせて SP プロファイルの SLA 属性をカスタマイズすることができます。SP プロファイルの SLA 属性の詳細については、[サービスプロバイダーのプロファイル \(24 ページ\)](#) を参照してください。

始める前に

インベントリにデバイスがあることを確認します。デバイスがない場合は、ディスカバリ機能を使用して検出します。

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。

ステップ 2 変更するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。

ステップ 3 ポリシーの横にあるラジオ ボタンを選択します。

ステップ 4 [Actions] ドロップダウン リストから、[Edit] を選択します。

ステップ 5 [SP プロファイル (SP Profiles)] をクリックし、SP プロファイルを選択します。

ステップ 6 次のフィールドの情報を変更することができます。

- [DSCP] : Differentiated Services Code Point (DSCP) 値。有効値は 0 ~ 63 です。
 - Expedited Forwarding (EF)
 - [Class Selector (CS)] : CS1、CS2、CS3、CS4、CS5、CS6
 - [Assured Forwarding] : AF11、AF21、AF41
 - [Default Forwarding (DF)]

これらの DSCP 値の詳細については、[マーキング、キューイング、ドロップの処理 \(22 ページ\)](#) を参照してください。

- [SP 帯域幅の割合 (SP Bandwidth %)] : 特定のサービス クラスに割り当てられた帯域幅の割合。
- [キューイング帯域幅の割合 (Queuing Bandwidth %)] : 各トラフィック クラスに割り当てられた帯域幅の割合。次のうちいずれかの変更を行うことができます。
 - キューイング帯域幅をカスタマイズするには、鍵アイコンをクリックして、帯域幅の設定をアンロックし、帯域幅の割合を調整します。
 - SP 帯域幅から自動的にキューイング帯域幅を計算するには、鍵アイコンをクリックしてキューイング帯域幅の設定をロックし、次に [OK] をクリックして確認します。デフォルトでは、Cisco

DNA Center は、SP クラスのすべてのトラフィック クラスのキューイング帯域幅の合計がそのクラスの SP 帯域幅の割合と一致するように、キューイング帯域幅の割合を自動的に配信します。


ステップ7 [OK] をクリックします。

サービス プロバイダー プロファイルの WAN インターフェイスへの割り当て

アプリケーション ポリシーがすでに作成済みで、SP プロファイルを WAN インターフェイスに割り当てる場合は、ポリシーを編集してこの設定を実行し、必要に応じてインターフェイスに Subline Rate の設定を含めます。

始める前に

ポリシーを作成していない場合は、ポリシーを作成し、同時に SP プロファイルを WAN インターフェイスに割り当てることができます。詳細については、「[アプリケーションポリシーの作成 \(35 ページ\)](#)」を参照してください。

- ステップ1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [アプリケーション (Application)] > [アプリケーション ポリシー (Application Policies)] の順に選択します。
- ステップ2 編集するポリシーを見つけるには、[フィルタ (Filter)] フィールドを使用します。
- ステップ3 ポリシーの横にあるラジオ ボタンをクリックします。
- ステップ4 [Actions] ドロップダウン リストから、[Edit] を選択します。
- ステップ5 [サイトの範囲 (Site Scope)] ペインで、対象のサイトの横にある歯車アイコン  をクリックします。
- ステップ6 対象のデバイスの [SPプロファイル設定 (SP Profile Settings)] 列にある [設定 (Configure)] をクリックします。
- ステップ7 [WAN インターフェイス (WAN Interface)] 列で、[インターフェイスの選択 (Select Interface)] ドロップダウン リストからインターフェイスを選択します。
- ステップ8 [ロール (Role)] 列で [ロールの選択 (Select Role)] ドロップダウン リストから設定するインターフェイスのタイプに従ってロールを選択します。
- **物理インターフェイス** : WAN を選択します。このロールは、物理インターフェイスに対してのみ有効なロールです。
 - **トンネル インターフェイス** : [DMVPN ブランチ (DMVPN Branch)] または のいずれかを選択します。[DMVPN ハブ (DMVPN Hub)] を選択した場合、関連するブランチに帯域幅を定義することもできます。
- (注) これらのポリシー設定を展開する前に、デバイスにトンネル インターフェイスが作成されていることを確認します。
- ステップ9 [サービス プロバイダー プロファイル (Service Provider Profile)] 列で、[プロファイルの選択 (Select Profile)] ドロップダウン フィールドをクリックし、SP プロファイルを選択します。

- ステップ 10 必要に応じて、[サブ回線のレート (Mbps) (Sub-Line Rate (Mbps))] 列で、インターフェイスに必要なアップストリーム帯域幅を入力します。
- ステップ 11 追加の WAN インターフェイスを設定するには [+] をクリックし、ステップ 7 ~ 10 を繰り返します。
- ステップ 12 [Save] をクリックします。
- ステップ 13 [< サイト範囲へ戻る (< Back to Site Scope)] をクリックします。
- ステップ 14 [OK] をクリックします。
- ステップ 15 [展開 (Deploy)] をクリックします。

ポリシーを今すぐ導入するか、または後でスケジュールするかどうかを求められます。

- ステップ 16 次のいずれかを実行します。
- ポリシーをすぐに導入するには、[今すぐ実行 (Run Now)] ラジオ ボタンをクリックし、[適用 (Apply)] をクリックします。
 - 将来の日付と時刻でポリシー導入をスケジュールするには、[後でスケジュール (Schedule Later)] ラジオ ボタンをクリックし、導入する日時を定義します。
- (注) アプリケーションポリシーの展開のスケジュール設定では、サイトのタイムゾーンの設定はサポートされていません。

トラフィック コピー ポリシー

Cisco DNA Center を使用して、2つのエンティティ間の IP トラフィック フローがモニタリングまたはトラブルシューティングのために指定された宛先にコピーされるように Encapsulated Remote Switched Port Analyzer (ERSPAN) を設定できます。

Cisco DNA Center を使用して ERSPAN を設定するには、コピーするトラフィック フローの送信元と宛先を定義するトラフィック コピー ポリシーを作成します。トラフィックのコピーを送信するデバイスおよびインターフェイスを指定するトラフィック コピー契約も定義できます。



- (注) トラフィック コピー ポリシーにはスケーラブル グループまたは IP ネットワーク グループのいずれかを含めることができるため、このガイド全体を通して、グループという用語を使用する場合は他に指定がなければスケーラブル グループおよび IP ネットワーク グループの両方を指します。

送信元、宛先、およびトラフィックのコピー先

Cisco DNA Center トラフィックのモニタリングプロセスを簡素化します。物理ネットワーク トポロジを知っている必要はありません。必要なのは、トラフィック フローの送信元および宛先

とコピーされたトラフィックの宛先となるトラフィック コピーの宛先を定義することだけです。

- [送信元 (Source)] : モニタするトラフィックが通過する 1 つまたは複数のネットワーク デバイス インターフェイス。このインターフェイスは、エンドポイント デバイス、これらのデバイスの特定ユーザ、またはアプリケーションに接続することがあります。送信元 グループを構成できるのは、イーサネット、ファストイーサネット、ギガビットイーサネット、10 ギガビットイーサネット、またはポート チャネル インターフェイスのみです。
- [宛先 (Destination)] : モニタするトラフィックが流れる IP サブネットです。IP サブネットはサーバ、リモートピア、またはアプリケーションに接続することがあります。
- [トラフィックコピーの宛先 (Traffic Copy Destination)] : ERSPAN データを受信、処理、および分析するデバイス上にあるレイヤ 2 またはレイヤ 3 の LAN インターフェイス。このデバイスは、通常、分析用にトラフィックのコピーを受信するパケットキャプチャツールまたはネットワーク分析ツールになります。



(注) 宛先では、スイッチプロンプト デバイスなどのネットワークアナライザやその他のリモートモニタリング (RMON) プロンプトを使用してトラフィック分析を実行することを推奨します。

使用可能なインターフェイスタイプは、イーサネット、ファストイーサネット、ギガビットイーサネット、または 10 ギガビットイーサネットのみです。宛先として設定されると、そのインターフェイスはコピーされたトラフィックのみを受信するために使用されません。このインターフェイスは今後その他のタイプのトラフィックを受信できなくなり、トラフィック コピー機能が必要とする以外のトラフィックを転送できません。トランク インターフェイスを宛先として設定できます。この設定により、インターフェイスはカプセル化されたトラフィックを送信できるようになります。



(注) 1 つのトラフィック コピー契約で使用できるトラフィック コピーの宛先は 1 つのみです。

トラフィック コピー ポリシーの注意事項と制限事項

トラフィック コピー ポリシー機能には次の制約事項があります。

- 最大 8 つのトラフィック コピー ポリシー、16 のコピー契約、および 16 のコピーの宛先を作成できます。
- 同じインターフェイスを複数のトラフィック コピーの宛先に使用することはできません。
- Cisco DNA Center は、トラフィック コピー ポリシーが変更され、ネットワークに展開されているポリシーとの整合性が失われていることを示すステータスメッセージを表示します。

せん。ただし、トラフィック コピー ポリシーが展開された後に変更されたことが分かった場合は、そのポリシーを展開しなおすことができます。

- 管理インターフェイスを送信元グループまたはトラフィック コピーの宛先として設定することはできません。

トラフィック コピー ポリシー設定のワークフロー

始める前に

- モニタ対象にする、トラフィック コピー ポリシーで使用されている送信元スケラブルグループが、スイッチとそれらのインターフェイスに静的にマッピングされている必要があります。
- トラフィック コピー ポリシー宛先グループは、IP ネットワーク グループとして設定されている必要があります。詳細については、「[IP ネットワーク グループの作成 \(14 ページ\)](#)」を参照してください。

ステップ 1

 トラフィック コピーの宛先を作成します。

これは、さらに分析するためにトラフィック フローがコピーされる、デバイス上のインターフェイスです。詳細については、[トラフィック コピーの宛先の作成 \(53 ページ\)](#) を参照してください。

ステップ 2

 トラフィック コピーの契約を作成します。

契約はコピーの宛先を定義します。詳細については、[トラフィック コピー契約の作成 \(54 ページ\)](#) を参照してください。

ステップ 3

 トラフィック コピー ポリシーを作成します。

ポリシーは、トラフィック フローの送信元と宛先、およびコピーされたトラフィックが送信される宛先を指定するトラフィック コピーの契約を定義します。詳細については、[トラフィック コピーポリシーの作成 \(55 ページ\)](#) を参照してください。

トラフィック コピーの宛先の作成

ステップ 1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピーの宛先 (Traffic Copy Destination)] の順に選択します。

ステップ 2 トラフィック コピーの宛先の名前と説明を入力します。

ステップ 3 デバイスと 1 つまたは複数のポートを選択します。

ステップ 4 [Save] をクリックします。

トラフィック コピーの宛先の編集または削除

- ステップ1 Cisco DNA Center のホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピーの宛先 (Traffic Copy Destination)] の順に選択します。
- ステップ2 編集または削除する宛先の横にあるチェックボックスをオンにします。
- ステップ3 次のいずれかを実行します。
 - 変更を行うには、[編集 (Edit)] をクリックして必要な変更を行い、[保存 (Save)] をクリックします。
 - 宛先を削除するには、[削除 (Delete)] をクリックします。

トラフィック コピー契約の作成

- ステップ1 Cisco DNA Center ホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピー契約 (Traffic Copy Contracts)] の順に選択します。
- ステップ2 [Add] をクリックします。
- ステップ3 ダイアログボックスに、契約の名前と説明を入力します。
- ステップ4 [コピー先 (Copy Destination)] ドロップダウン リストから、コピー先を選択します。

(注) コピー先は、1つのトラフィック コピー契約に対し1つだけ指定できます。

選択可能なコピー先がない場合は、1つ作成できます。詳細については、[トラフィック コピーの宛先の作成 \(53 ページ\)](#) を参照してください。
- ステップ5 [Save] をクリックします。

トラフィック コピー契約の編集または削除

- ステップ1 Cisco DNA Center ホームページで、[ポリシー (Policy)] > [トラフィック コピー (Traffic Copy)] > [トラフィック コピー契約 (Traffic Copy Contracts)] の順に選択します。
- ステップ2 編集または削除する契約の横にあるチェックボックスをオンにします。
- ステップ3 次のいずれかを実行します。
 - 変更を行うには、[編集 (Edit)] をクリックして必要な変更を行い、[保存 (Save)] をクリックします。
 - 契約を削除するには、[削除 (Delete)] をクリックします。

トラフィック コピー ポリシーの作成

- ステップ1 Cisco DNA Center のホームページで、[Policy] > [Traffic Copy] > [Traffic Copy Policies] の順に選択します。
- ステップ2 [ポリシーの追加 (Add Policy)] をクリックします。
- ステップ3 [ポリシー名 (Policy Name)] フィールドに名前を入力します。
- ステップ4 [説明 (Description)] フィールドにポリシーを表す単語またはフレーズを入力します。
- ステップ5 [契約 (Contract)] フィールドで、[契約の追加 (Add Contract)] をクリックします。
- ステップ6 使用する契約の隣にあるラジオ ボタンをクリックし、次に [保存 (Save)] をクリックします。
- ステップ7 [使用可能なグループ (Available Groups)] エリアから、[送信元 (Source)] エリアにグループをドラッグアンドドロップします。
- ステップ8 [使用可能なグループ (Available Groups)] エリアから、[宛先 (Destination)] エリアにグループをドラッグアンドドロップします。
- ステップ9 [Save] をクリックします。

トラフィックコピーポリシーの編集または削除

- ステップ1 Cisco DNA Center のホームページで、[Policy] > [Traffic Copy] > [Traffic Copy Policies] の順に選択します。
- ステップ2 編集または削除したいポリシーの横のチェック ボックスをオンにします。
- ステップ3 次のいずれかを実行します。
 - 変更を行うには、[編集 (Edit)] をクリックして必要な変更を行い、[保存 (Save)] をクリックします。
 - ポリシーを削除するには、[削除 (Delete)] をクリックします。

仮想ネットワーク

仮想ネットワークは、独立したルーティングおよびスイッチング環境です。仮想ネットワークを使用して、物理ネットワークを複数の論理ネットワークにセグメント化できます。

仮想ネットワークに入れることができるのは、割り当てられたユーザグループのみです。仮想ネットワーク内で、ユーザとデバイスは、アクセスポリシーによって明示的にブロックされていなければ相互に通信できます。異なる仮想ネットワークにまたがるユーザは、相互に通信できません。ただし、例外ポリシーを作成して、一部のユーザに異なる仮想ネットワークをまたぐ通信を許可することができます。

一般的な使用例はビルディング管理です。照明、冷暖房空調 (HVAC) システム、セキュリティ システムなどのビルディング システムからユーザ コミュニティをセグメント化する必要

があります。このケースでは、ユーザコミュニティとビルディングシステムを2つ以上の仮想ネットワークにセグメント化して、ビルディングシステムの不正アクセスをブロックします。

仮想ネットワークは、複数のサイトロケーションやネットワークドメイン（ワイヤレス、キャンパス、およびWAN）にまたがる場合があります。

デフォルトでは、Cisco DNA Centerには単一の仮想ネットワークがあり、すべてのユーザおよびエンドポイントがこの仮想ネットワークに属しています。Cisco DNA CenterがCisco Identity Services Engine (ISE)と統合されると、デフォルトの仮想ネットワークにCisco ISEのユーザグループおよびエンドポイントが移入されます。

Cisco DNA Centerでは、仮想ネットワークの概念はワイヤレス、キャンパス、およびWANネットワークで共通です。仮想ネットワークが作成されたら、ワイヤレス、有線、またはWAN導入が組み合わされているサイトと関連付けることができます。たとえば、ワイヤレスデバイスと有線デバイスが含まれるキャンパスファブリックがサイトで展開されている場合、仮想ネットワークの作成プロセスによってキャンパスファブリックでサービスセット識別子 (SSID)とVirtual Routing and Forwarding (VRF)の作成がトリガーされます。また、サイトにWANファブリックも展開されている場合、VRFがキャンパスからWANに同様に拡張します。

サイトの設計および初期設定時に、ワイヤレスデバイス、有線スイッチ、およびWANルータをサイトに追加できます。Cisco DNA Centerは、仮想ネットワークと関連付けられたポリシーがサイトに対して作成されたことを検出し、それらを異なるデバイスに適用します。

仮想ネットワークに関する注意事項と制限事項

仮想ネットワークには次の注意事項と制約事項があります。

- VRFはすべてのドメインで共通です。VRFの最大数は、ドメイン内のVRFが最も少ないデバイスに基づきます。


ゲストアクセス用の複数の仮想ネットワーク

ゲストアクセス用に複数の仮想ネットワークを作成できます。この機能を使用すると、企業のトラフィックが存在しない場所で、ゲストトラフィック用に異なる仮想ネットワークを使用できます。ワイヤレスゲストSSIDを異なる仮想ネットワークのIPプールに制限なしでマッピングできるようになりました。

仮想ネットワークの作成

仮想ネットワークを作成し、物理ネットワークを複数の論理ネットワークにセグメント化することができます。

ステップ 1 Cisco DNA Centerのホームページで、[ポリシー (Policy)] > [仮想ネットワーク (Virtual Network)] > [概要 (Overview)]の順に選択します。

ステップ2  をクリックして、新しい仮想ネットワークを作成します。

ステップ3 [仮想ネットワーク名 (Virtual Network Name)] フィールドに、仮想ネットワークの名前を入力します。

ステップ4 仮想ネットワークをゲストネットワークとして設定するには、[ゲスト仮想ネットワーク (Guest Virtual Network)] チェックボックスをオンにします。

ゲストに制限されたアクセスを許可する、特別なルールが設定されているデバイス。

ステップ5 [使用可能なスケーラブル グループ (Available Scalable Groups)] エリアから、[仮想ネットワーク内のグループ (Groups in the Virtual Network)] エリアにドラッグアンドドロップします。

ステップ6 [Save] をクリックします。

ステップ7 複数のゲスト仮想ネットワークを作成するには、ステップ2～6を繰り返します。

仮想ネットワークの編集または削除

あるカスタム仮想ネットワークから別のカスタム仮想ネットワークにスケーラブルなグループを移動すると、スケーラブルなグループのマッピングが変更されます。この変更によって、グループ内のユーザまたはデバイスに影響が及ぶ可能性があることに注意してください。

ステップ1 Cisco DNA Center のホームページで、[Policy] > [Virtual Network] > [Overview] の順に選択します。

ステップ2 次のいずれか1つのタスクを実行します。

- 仮想ネットワークを編集するには、左側のナビゲーションウィンドウから仮想ネットワークの名前をクリックし、次の表に示す任意のフィールドの情報を変更します（仮想ネットワーク名を除きます）。

表 7: 仮想ネットワーク フィールド

| フィールド | 説明 |
|--|---|
| ネットワーク名 | 仮想ネットワークの名前。（変更できません。） |
| ゲスト仮想ネットワーク (Guest Virtual Network) | ゲストに制限されたアクセスを許可する、特別なルールが設定されているデバイス。ゲスト ネットワークとして仮想ネットワークを設定するには、このチェックボックスをオンにします。ゲスト仮想ネットワークを1つだけ作成することができます。 |
| Available Groups | 仮想ネットワークに含めることができるスケーラブルなグループ。[使用可能なグループ (Available Groups)] エリアから、[仮想ネットワーク内のグループ (Groups in the Virtual Network)] エリアにドラッグアンドドロップします。 |
| 仮想ネットワーク内のグループ (Groups in the Virtual Network) | 仮想ネットワーク内にあるスケーラブルなグループ。[使用可能なグループ (Available Groups)] エリアから、[仮想ネットワーク内のグループ (Groups in the Virtual Network)] エリアにドラッグアンドドロップします。 |

- 仮想ネットワークを削除するには、 をクリックし、削除を確定します。
-