クイックスタートガイド – Catalyst SD-WAN簡素化された設定とポリシー

内容

はじめに

このドキュメントは、Catalyst SD-WANでの設定とポリシーの簡素化のためのクイックスタートガイドです。

要約

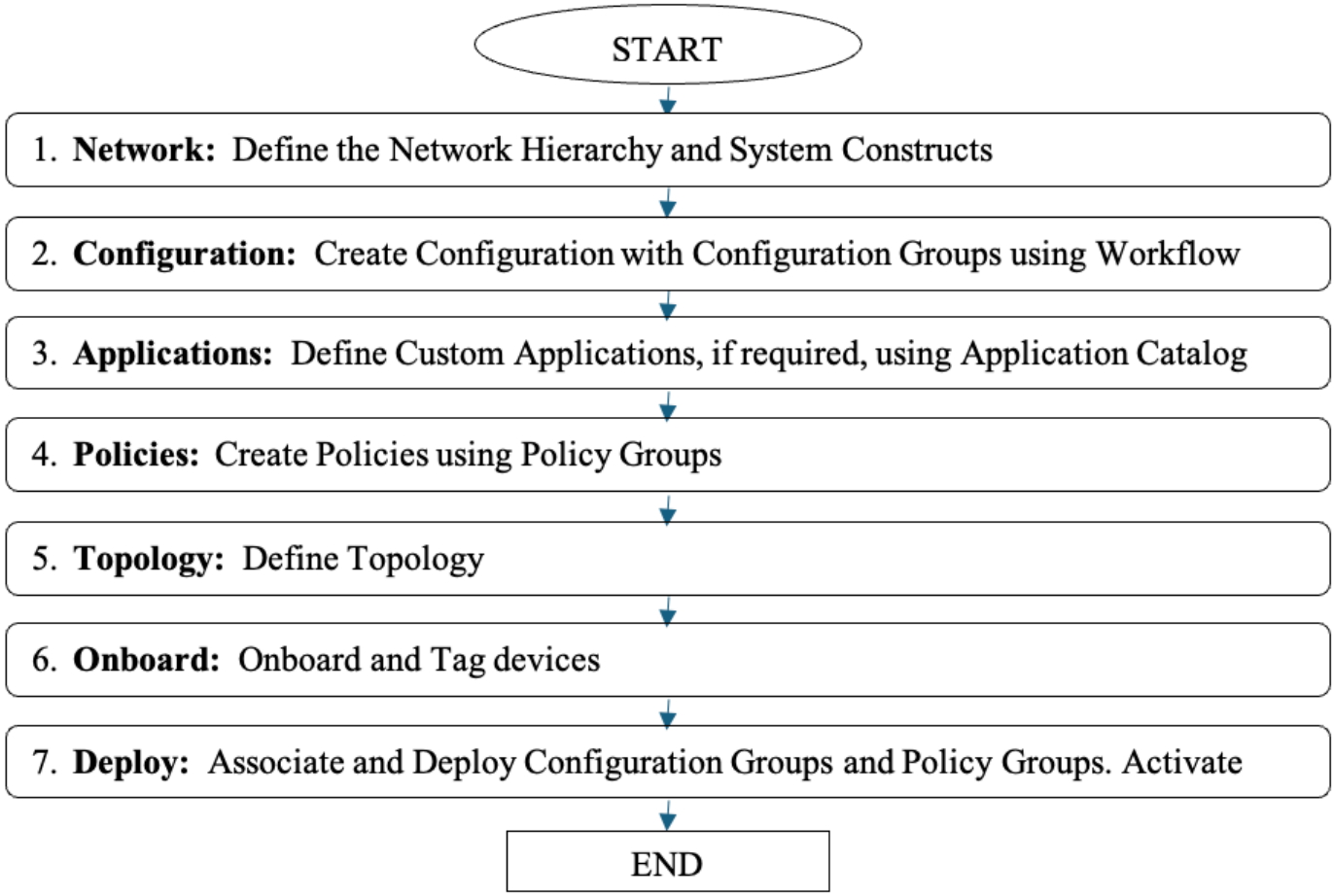
Cisco Catalyst SD-WANソフトウェアリリース20.12/17.12を使用する場合、デバイスと機能のテンプレートに基づく従来の設定から、設定グループとポリシーグループに基づく新しい設定方法への移行を開始することが推奨されます。このドキュメントでは、新しい設定方法に関する重要な詳細について説明します。

このドキュメントの主な目的は、20.12ゴールデンリリースで、設定、ポリシー、オンボーディングの新しい構成を使用することから始めるためのガイドとして役立つことです。 このドキュメントでは、個々の機能については説明しません。

新規導入

新しい設定方法を正しく利用するには、次の手順を実行する必要があります。

1. ネットワーク：ネットワーク階層とシステム構造の定義
2. 構成：ワークフローを使用した構成グループを含む構成の作成
3. アプリケーション：アプリケーションカタログを使用して、必要に応じてカスタムアプリケーションを定義します。
4. ポリシー：ポリシーグループを使用したポリシーの作成
5. トポロジ：トポロジを定義する
6. オンボード：オンボードデバイスとタグデバイス
7. 展開：構成グループとポリシーグループを関連付けて展開します。トポロジをアクティブにします。



新規導入のフローチャート

既存の導入

1. 「既存の導入」セクションで説明されている手順を実行します
2. 変換ツールを使用して、既存の設定/ポリシーを新しい設定/ポリシーに変換します。

ユーザエクスペリエンスの強化と運用の簡素化

Cisco Catalyst SD-WANは、ユーザエクスペリエンスの向上と運用の簡素化を実現します。

- 共通UI：新しいUXフレームワークがCatalyst SD-WAN Managerおよび他のシスコ製品に導入されました。これは、User eXperienceの一貫性を保ち、製品間で共通のルックアンドフィールを提供するものです。
- 設定：直感的なインテントベースのワークフローとシスコ推奨のスマートデフォルトの使用により、設定とポリシーの作成および導入が簡素化されます。
- モニタリング：新しいウィジェットとカスタマイズ可能で強化されたダッシュボードにより、ネットワークおよびアプリケーションのパフォーマンスと健全性に関する豊富な情報を提供します。
- トラブルシューティング：動的なサイトおよびネットワークトポロジビュー、コンテキストベースのトラブルシューティングツールへのアクセス、ネットワークおよびアプリケーションパフォーマンスに関するレポートを定期的に提供します。

利点

使いやすい	直感的なガイド付きワークフロー
構成の無秩序な増加	無秩序な増加の抑制（モデルに依存しない、再利用、構造）
構成の作成	スマートなデフォルト設定で迅速かつ簡単に
設定の変更	今すぐ変更、後で選択的に展開
可視性	新しいダッシュボード、アプリケーション/サイトのパフォーマンスモニタリング
トラブルシューティングガイダンス	サイトトポロジ、トラブルシューティングツールのガイダンス

ネットワーク階層とシステム構成の定義

ネットワーク階層

ネットワークの「階層」、つまりサイト、リージョン、エリアの概念を提供します。これはネットワークに基づいて作成できます。

以下に例を挙げます。

Global (15 of 15 nodes)

AMER

BR1_SanJose

BR2_NewYork

BR6_Dallas

APJC

BR3_Mumbai

BR4_Singapore

これらのオプションを使用可能にするには、必要に応じてProtocolをBOTHからIPv4またはIPv6に変更します。

組み込みセキュリティ

オンボックスのNGFW、IPS、マルウェア、およびコンテンツフィルタリングのセキュリティポリシーを定義

セキュアインターネットゲートウェイ/セキュアサービスエッジ

Cisco Secure Accessなどのクラウドベースのコンテンツおよびセキュリティエンティティへのトンネルを確立するために必要な設定を定義します。

注：

従来の設定方法では、これは機能テンプレートとして使用できました。

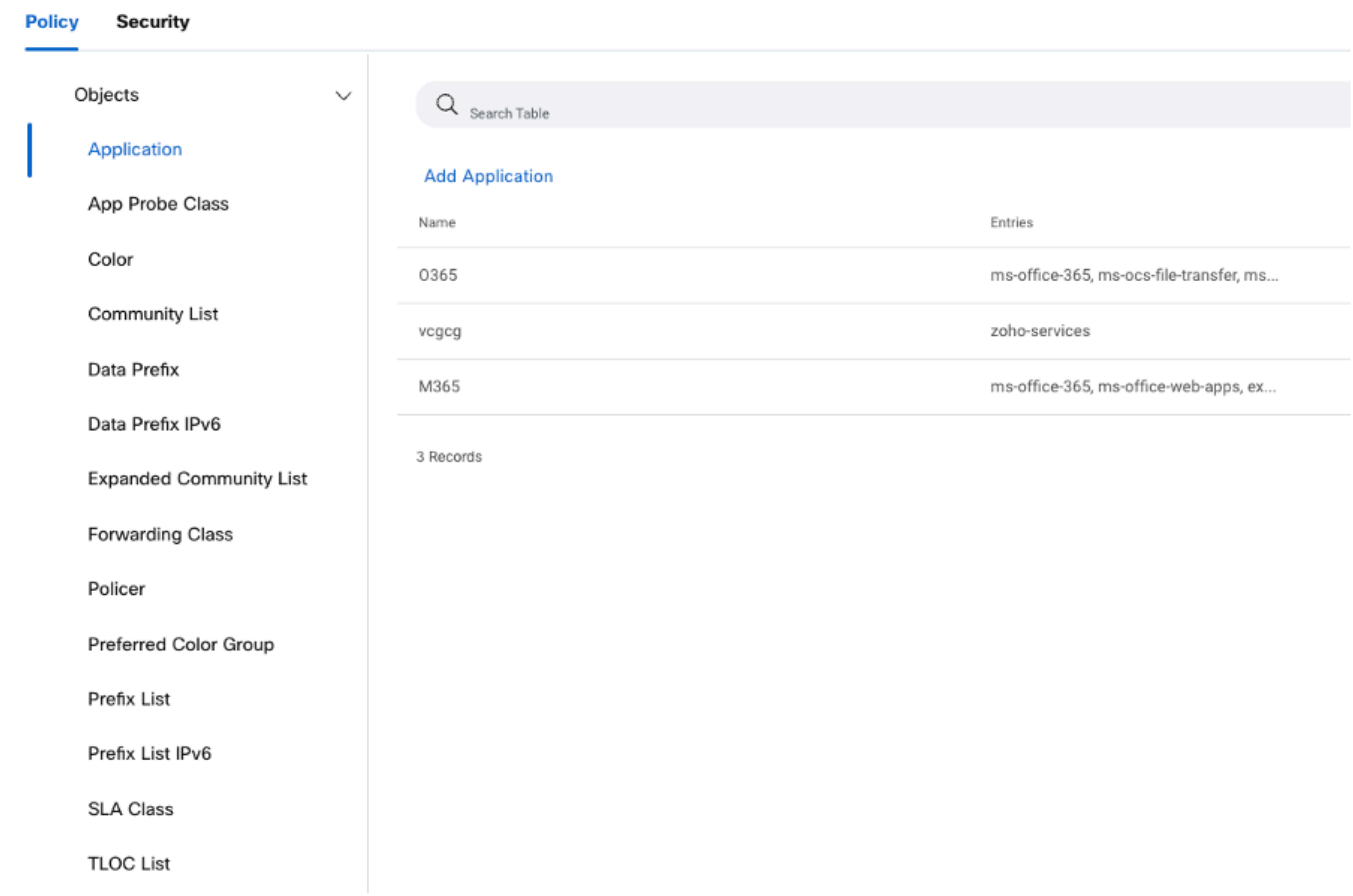
DNSセキュリティ

コンテンツフィルタリングにクラウドベースのDNSセキュリティサービスの使用を許可する設定を定義します。

関心のあるグループ

ポリシーで使用するオブジェクトリストを定義します。例：アプリケーションリスト、VPNリスト、サイトリスト、プレフィックスリストなど。

また、セキュリティポリシーについては、高度な検査プロファイル、SSL復号化ポリシーなどのプロファイルを定義します。



ポリシーグループ：対象のグループ

関連付けと導入

設定グループと同様に、デバイスをポリシーグループに関連付けて展開します。

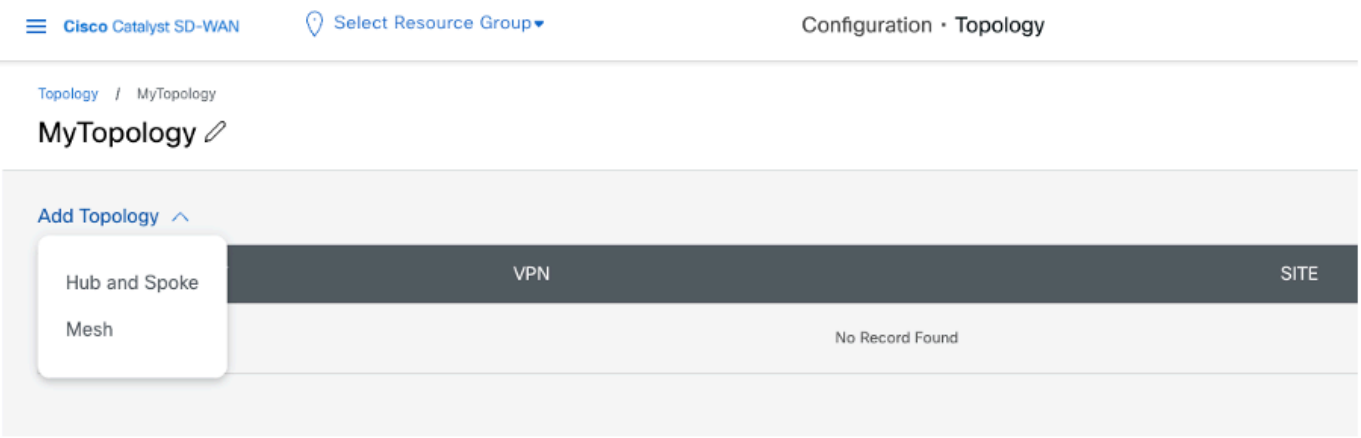
ローカライズされたポリシー

ACL、ルートポリシー、デバイスアクセスポリシーなどのローカライズされたポリシーは、設定グループで定義されます。

トポロジ

ネットワークトポロジを定義します。

フルメッシュまたはハブアンドスポークから開始し、必要に応じてカスタマイズします。



トポロジメニュー

トポロジとVPN

トポロジを作成し、VPNを指定する際には、これらの設計変更に留意してください。

新しい設計では、1:1マッピングではなく、VPN名からVPN IDへのダイナミックマッピングが可能です。

複数のVPN IDへのVPN名のマッピング

図:
2つの異なる設定グループに、Corporateという名前のVPNがあるとします。

一方にはVPN ID 10があり、もう一方にはVPN ID 20があります。

トポロジワークフローVPNリストには、社内 VPNの1つのインスタンスだけが表示されます。

Corporate VPNを選択すると、SD-WAN Managerはトポロジに基づいてVPN IDを判別します。
2つのサイトに2つのデバイスがあるとします。
1. サイト100のDevice1、VPN 10としてCorporateを使用
2. サイト200のDevice2、VPN 20としてCorporateを使用

サイト100とサイト200の両方がトポロジの一部である場合、SD-WAN Managerは両方のVPN ID（10と20）を持つVPNリストを作成します。
サイト100のみがトポロジに含まれている場合、SD-WAN ManagerはVPN ID 10のみを持つVPNリストを作成します。
サイト200のみがトポロジに含まれている場合、SD-WAN ManagerはVPN ID 20のみを持つVPNリストを作成します。

同じVPN IDにマッピングする複数のVPN名

同じVPN名を持つ複数のトポロジポリシーを設定し、異なるサイトの異なるVPN IDにマッピングできます。

SD-WAN Managerは、どのトポロジがどのサイトに関連付けられているかに基づいて、実際のマッピングを決定します。

図:

2人のユーザが2つの異なる設定グループを作成できます。

一方はVPN ID 100をFinance VPNとして指定し、もう一方はEngineering VPNとして指定します。

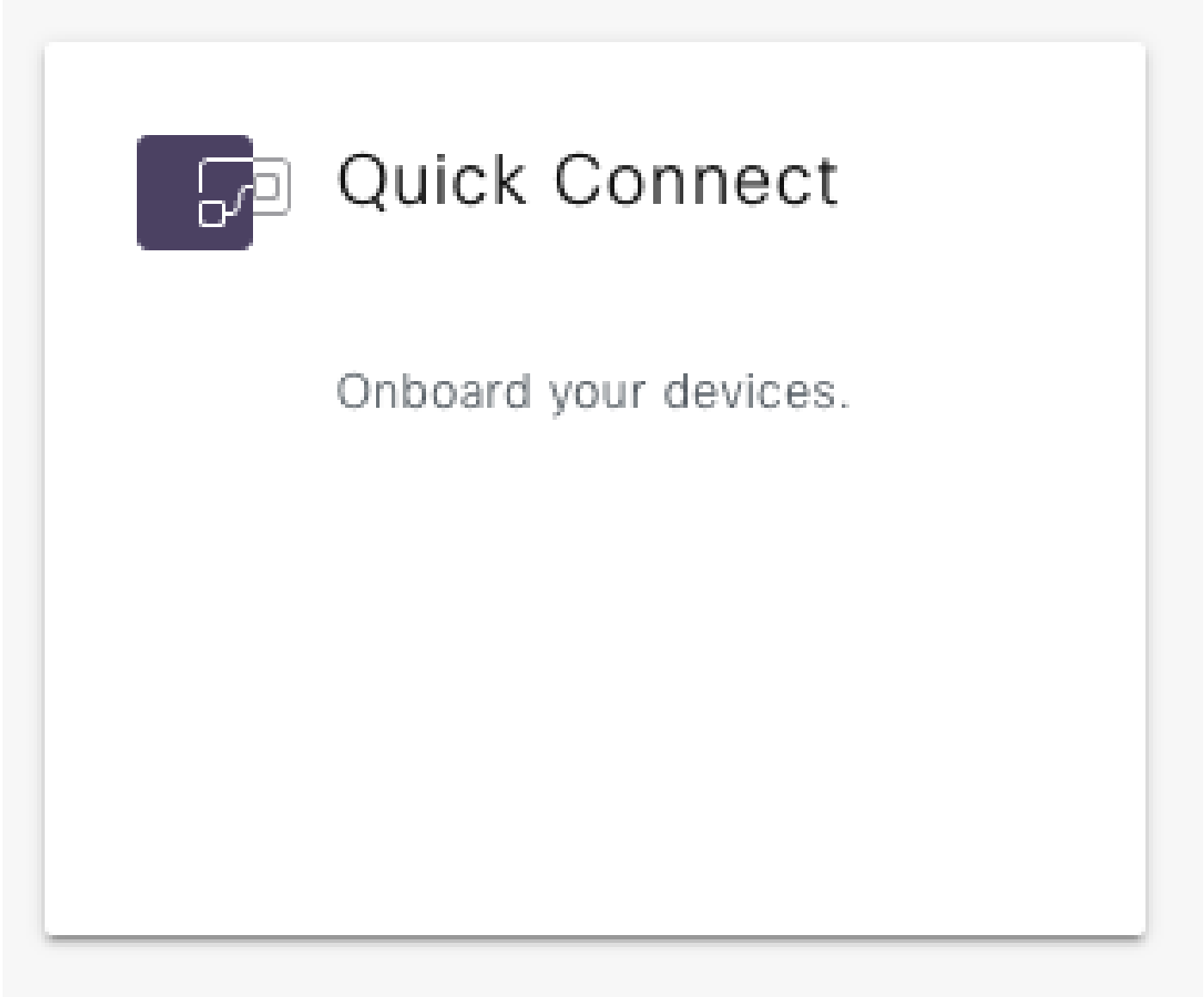
その後、それぞれのVPN名を使用してトポロジを作成できます。

オンボーディング

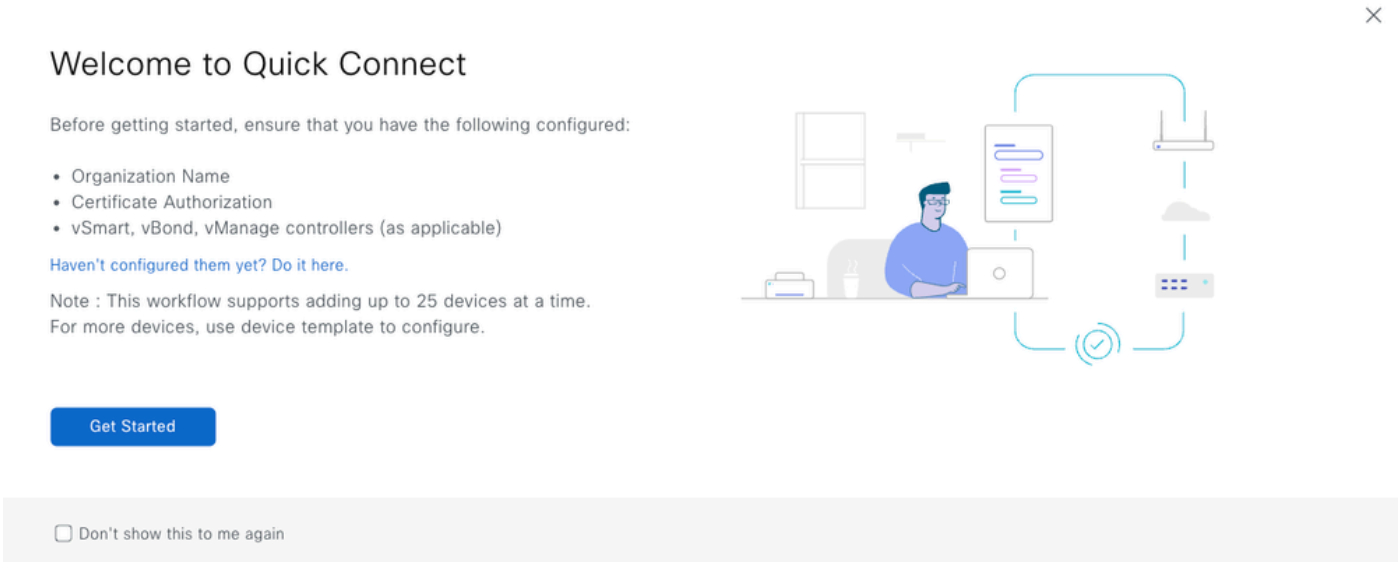
物理ルータのオンボーディングには、Quick Connect Workflowを使用します。

このワークフローを使用して、オンボーディングするデバイスのホスト名、システムIP、およびサイト名/IDを事前に定義します。これらは自動的に生成されますが、必要に応じて変更できます。デバイスにタグを付けて、そのデバイスを設定グループに自動関連付けするために使用することもできます。

PnP ZTPオンボーディングプロセス中に、デバイスはSD-WAN Managerへのコントロールプレーントンネル接続を確立します。SD-WAN Managerが事前に定義されたファブリック構成をデバイスにプッシュし、デバイスがSD-WANファブリックに参加します。



クイック接続ワークフロー



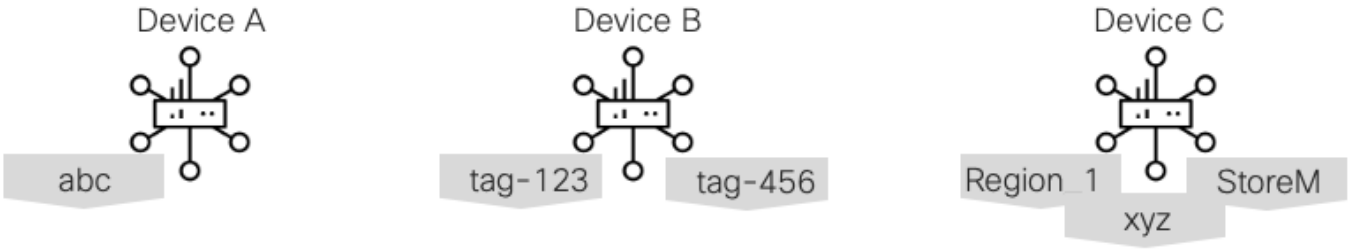
クイック接続ワークフローの説明

タグ付け

デバイスは、ユーザ定義のタグに関連付けることができます。

タグは、デバイスのグループ化、説明、検索、管理に使用できます。

タグを使用すると、デバイスをグループ化して他の機能で使用できます。



タグ付けの例

例：デバイスへの設定グループの関連付け

設定グループのルールを設定すると、特定のタグを持つデバイスをその設定グループに自動的に関連付けることができます。

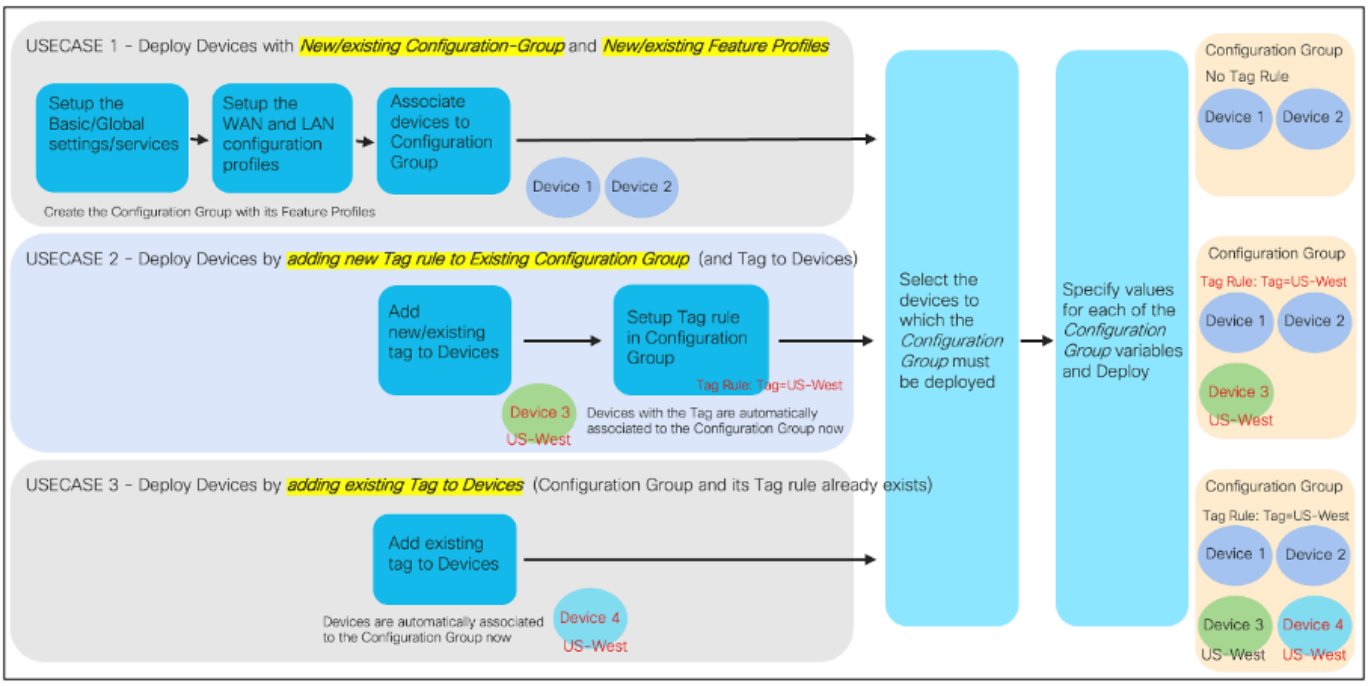
タグの追加

Configuration->Devicesでは、デバイスに対してタグの作成、追加、削除を行うことができます。

設定グループ内のタグ規則

Configuration Group -> Associated Devicesページで、タグルールを追加/編集できます。

図



タグ付けの図

既存の導入

SD-WANネットワークでは、従来の構成とポリシーを使用するデバイスは、簡素化された構成とポリシーを使用するデバイスと共存できます。

このセクションでは、簡素化された設定とポリシーを利用する場合の推奨事項について説明します。また、推奨事項についても説明します。

最初のステップでは、デバイスをデバイステンプレートから設定グループに移行する必要があります。　これが完了すると、ポリシーグループやトポロジを展開できます。

構成グループ

デバイステンプレートと設定グループは、エッジデバイス設定を提供します。　だから、共存は簡単に起こります。　デバイステンプレートから設定グループに移行する手順は次のとおりです。

手順 1	デバイステンプレートからデバイス値のコピーを抽出します。　これを行うには、設定>テンプレートで、デバイスグループの右側の省略記号(...)をクリックし、「CSVのエクスポート」を選択します。
手順 2	構成グループを作成します（手動または変換ツールを使用）。
手順 3	デバイステンプレートをデバイスから切り離します。　この時点で、デバイスは接続ポイントで設定を維持しますが、デバイステンプレート（また

	はコンポーネントフィーチャテンプレート）に対する今後の変更は受け取りません。
手順 4	デバイスを新しい設定グループに関連付けます。
手順 5	設定グループに関連付けられたデバイスを導入します。　このプロセスを簡単に行うには、エクスポートされたCSVファイルを開き、CSVカラムヘッダーを変更して、設定グループの新しい変数に一致させます。
手順 6	デバイス変数の入力画面が表示されたら、デバイス設定をプレビューできます。　これにより、設定グループのどの部分が以前のインスタンスと一致しないか、またはデバイステンプレートからどの変数が変更されたかについてプレビューできます。

変数に対して一貫した命名方式を維持すると、デバイス固有の設定が簡素化されます。 すべてのデバイスの値が1つのCSVファイル内にある場合は、カラムヘッダーの名前を変更する必要があるのは1回だけです。

注：デバイステンプレートまたは設定グループ用のCSVファイルを操作してカラムヘッダーを統合し、アルファベット順に並べ替えるPythonスクリプトが存在します。　スクリプトは次の場所にあります。

https://github.com/BradEdgeworth/CSVMerger

ポリシーグループ

設定グループを介して設定されたデバイスは、一元化されたポリシーを使用するか、ポリシーグループに移行できますが、同じアプリケーションに対して同時に両方を同時に移行することはできません。 基本的に、目標はエッジデバイスに対して同じ基本ポリシーを維持することです。ポリシーグループは、元のAARポリシーとデータポリシーを1つのアプリケーションプライオリティおよびSLA PGコンポーネントに統合します。 基本的に、ポリシーの設定の構築方法を変更するだけです（ただし、SD-WAN Managerには送信されません）。

データポリシーまたはAARポリシーは、両方とも同じ設定を設定するため、アプリケーションプライオリティおよびSLAコンポーネントを持つサイトを含むサイトリストを参照できないことに注意してください。

制御ポリシーのみを使用する一元化ポリシーは、アプリケーションの優先順位とSLAを持つポリシーグループを使用するサイトを参照できます。これは、一元化ポリシーのさまざまなコンポーネントを設定するためです。

一元化ポリシーからポリシーグループにデバイスを移行するには、次の手順を実行します。

手順 1	必要なポリシーグループコンポーネント（アプリケーションプライオリティとSLA、組み込みセキュリティ、セキュアインターネットゲートウェイ/セキュアサービスエッジ、DNSセキュリティ）を作成します。
手順 2	ポリシーグループを作成し、必要なコンポーネントを関連付けます。
手順 3	AARまたはデータポリシーで参照されているSiteListからサイトIDの関連付けを解除します。 この時点で、SD-WAN Managerは更新された設定をコントローラに送信し、コントローラはエッジデバイスからアクティブなデータポリシー命令をすべて削除します。 これにより、この時点では意図しないトラフィックフローが発生する可能性があることに注意してください。
手順 4	デバイスをポリシーグループに関連付け、ポリシーグループを保存します。
手順 5	選択したデバイスにポリシーグループを展開します。 この時点で、SD-WAN Managerはエッジデバイス（QoS/SIG用）とコントローラに更新された設定を送信します。これにより、コントローラは更新されたデータポリシーをエッジデバイスに送信できます。

注：ポリシーグループは集中型ポリシーと共存できますが、エッジデバイスを設定グループに変換する間、（AARおよびデータポリシーに対して）集中型ポリシーのままにしておくことをお勧めします。 次に、この時点で、アプリケーションプライオリティおよびSLAコンポーネント内の機能を使用するために、一元化ポリシーからポリシーグループへの移行を開始します。

これは単純な作業で、運用スタッフ間の混乱を減らすために行います。

注：
ポリシーグループエンジンは、異なる形式で情報を保存します。したがって、一元化ポリシーで使用されるプレフィックスリストは、ポリシーグループ内で再作成する必要があります。これは、サイトリストなどの他の場合にも発生する可能性があります。

トポロジ

設定グループを介して設定されたデバイスは、中央集中型ポリシーを使用するか、トポロジに移行できます。基本的に、目標はSD-WANコントローラと同じ制御ポリシーを維持することです。トポロジは、制御ポリシーの最新のイテレーションです。

コントロールポリシーポリシーは、関連付けられたトポロジを持つサイトを持つサイトリストを参照することはできないことに注意してください。どちらも同じ設定を設定するためです。

データポリシーまたはAARポリシーのみを使用する一元化ポリシーと、さまざまなコンポーネントを設定するトポロジポリシーを設定できます。

一元化ポリシーからポリシーグループにデバイスを移行する手順：

手順 1	必要なトポロジコンポーネントの作成
手順 2	中央集中型ポリシーの古いトポロジリストからサイドの関連付けを解除します。
手順 3	AARまたはデータポリシーで参照されているサイトリストからサイトIDの関連付けを解除します。 この時点で、SD-WAN Managerは更新された設定をコントローラに送信し、コントローラは移行されるサイトのアクティブなトポロジ設定をすべて削除します。 これにより、この時点で意図しないトラフィックフローが発生する可能性があることに注意してください。
手順 4	トポロジをアクティブにします。この時点で、SD-WAN Managerは更新された設定をコントローラに送信し、エッジデバイスに送信されるすべてのルートを変更します。

注：トポロジは中央集中型ポリシーと共存できますが、エッジデバイスを設定グループに変換する間、（トポロジおよびルート操作のための）中央集中型ポリシーのままにしておくことをお勧めします。 次に、その時点で、トポロジの変更とルーティング操作を行う機能のために、中央集中型ポリシーからトポロジへの移行を開始します。

これは単純な作業で、運用スタッフ間の混乱を減らすために行います。

変換ツール

対象範囲

変換ツールは、テンプレートを設定グループに1対1で変換します。このツールは、SD-WAN Managerインスタンスからテンプレートを収集し、それらを構成グループ（機能プロファイルと機能パーセルを含む）に変換し、新しく変換した構成をSD-WAN Managerにアップロードします。

* ポリシーからポリシーグループへの変換は、2024年10月に変換ツールで利用可能になる予定です。

アクセスの詳細

ツールのベータ版が利用可能です。詳細については、sdwan-ux-conversion-tool@cisco.comまでお問い合わせください。

使用方法

前提条件

このツールを使用する前に、SD-WAN Managerで20.12.xが実行されていることを確認してください。そうでない場合は、先に進む前に20.12にアップグレードします。

変換ツールのワークフロー

手順 1	シスコから提供されたクレデンシャルを使用してツールにサインインします。(注：これらはCCOクレデンシャルではありません。詳細については、sdwan-ux-conversion-tool@cisco.comまでお問い合わせください)。
手順 2	ホームページから「変換ツール」ワークフローを選択します。 ・ このワークフローを以前に実行したことがあり、変換後の構成を含むJSONファイルがある場合は、[ファイルからアップロード]ワークフローを選択する必要があります。
手順 3	Login: SD-WANマネージャのIPまたはURLとユーザクレデンシャルを入力します。 ・ ユーザーは読み取り/書き込みアクセス権を持っている必要があります。 ・ ポートおよびサブドメインのフィールドはオプションです。
ステップ 4：	インポート: SD-WAN Managerからすべてのレガシー構成（デバイステンプレート、機能テンプレート、ポリシー、および関連する構成）を取得するには、[収集]ボタンをクリックします。 ・ 収集したら、すべての設定を含むJSONファイルをダウンロードする必要があります。このファイルは、SD-WAN Managerから再度収集するので

	はなく、この手順で後から使用する必要があります。
ステップ5：	次を選択します： 新しい同等のテンプレートおよびポリシーに変換するテンプレートおよびポリシーを選択します。[マイグレーション]をクリックして、選択した構成を変換します。
手順 6：	Transform: このページには、新しく変換されたすべての構成が表示されます。準備ができたら、「アップロード」をクリックして、これらの設定をSD-WAN Managerにプッシュします。 ・ まだSD-WAN Managerにプッシュする準備ができていない場合は、変換された構成をJSONファイルとしてダウンロードし、後で「ファイルからアップロード」ワークフローを使用できます。
手順 7：	要約： この時点で、設定はSD-WAN Managerにプッシュされて作成されます。設定をプッシュすると、経過表示バーが表示されます。アップロードが完了すると、アップロードされた設定の概要が表示されます。 ・ 「構成グループ」、「機能プロファイル」、「ポリシーグループ」の各クイックリンクを使用して、SD-WAN Managerの新しい構成を表示できます。 ・ エラーまたはミスが発生した場合は、このステップでロールバックも使用できます。ロールバックを実行すると、このワークフロー/セッション中にSD-WAN Managerにプッシュされたすべての構成が削除されます。

変換後

これで、新しい構成を使用する準備ができました。「既存の導入」セクションの手順を実行して、デバイスを新しく変換した設定グループに移行します。

考慮事項

- このツールで提供される変換は、ガイダンスとして機能することを目的としています。実稼働環境に導入する前に、分析とテストを行ってください。
- このツールでは、設定グループのデバイスに依存しない機能は考慮されません。ユーザは、変換または分析する設定グループを選択する前にテンプレートを分析し、デバイスに依存しない機能を活用できるようにデバイスを関連付けることができます。
- 旧形式の構成の変数名とグローバル値は、新しく変換された構成にコピーされます。

- このツールでは、設定はデバイスにプッシュされません。変換を実行した後、ユーザはデバイスをテンプレートから切り離し、新しい設定グループに関連付ける必要があります。

20.12考慮事項

No.	アイテムの説明
1	17.12より前のバージョンを実行するエッジに設定グループを展開する場合は、CLIアドオンプロファイルを使用してDNS設定をプッシュする必要があります。
2	トポロジを作成するには、NHMで定義されたエリアを選択するのではなく、サイトを選択する必要があります。
3	構成グループの作成ワークフローでは、VPN512およびこのVPNのインターフェイスはWANプロファイルに作成されません。これが必要な場合は、設定グループを編集して手動で作成できます。
4	機能プロファイルをコピー/複製する機能。ポリシーはサポートされていません。　Pythonスクリプトのセットは、このタスクを実行でき、次の場所にあります。 https://github.com/dbrown92700/configGroups/
5	ポリシー設定（ローカライズされたポリシー）に関連する機能パーセルを作成する前に、ポリシーオブジェクトプロファイルを設定グループに関連付ける必要があります。例：ACL
6	インターフェイス変数のCSVのインポートは、セミコロンを文字列に挿入して失敗します
7	AppQoE最適化（TCP OptおよびDRE）と損失修正（FECおよびPkt Dup）の設定では、引き続き従来のテンプレート/ポリシーを使用します。設定/ポリシーグループでもCLIプロファイルを使用して設定可能（UIパーセル内の20.14）
8	SaaS向けクラウドオンランプは、従来のテンプレート/ポリシーを引き続き使用します。

9	TrustSec/SGTはCLIプロファイルでのみサポート
10	CLIプロファイルのみでサポートされるUC音声/DSPファーム/SRST（UIパーセルで20.13以降）

関連情報

- Cisco SD-WANおよびクラウドネットワーキングYouTubeチャネル：https://www.youtube.com/@CiscoSDWANandCloudNetworking
- UX2.0 – 運用の簡素化：1.単一ルータサイトの設定：https://www.youtube.com/watch?v=98z-d3knd
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。