Cisco IOS XE Catalyst SD-WAN デバイス と ACI の統合

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます：**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、および **Cisco vSmart** から **Cisco Catalyst SD-WAN Controller** への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

表 *1* : 機能の履歴

機能名	リリース情報	説明
ACI との統合	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	Cisco IOS XE Catalyst SD-WAN と ACI の統合機能で、事前定義された SLA クラウドベッドがサポートされるようになりました。また、データプレフィックスリストから動的に生成されたマッピングをサポートし、ACI によって提供される SLA クラスへの VPN リストが含まれています。

ACI リリース 4.1(1) では、WAN SLA ポリシーのサポートが追加されています。この機能を使用すると、テナント管理者は事前構成されたポリシーを適用して、WAN 経由のテナントトラフィックのパケット損失、ジッター、および遅延のレベルを指定できます。WAN SLA ポリシーをテナントトラフィックに適用すると、Cisco APIC は事前設定されたポリシーを Cisco Catalyst SD-WAN コントローラ に送信します。Cisco IOS XE Catalyst SD-WAN 機能を提供する外部デバイスマネージャとして ACI で設定されている Cisco Catalyst SD-WAN コントローラは、SLA ポリシーで指定された損失、ジッター、および遅延パラメータを満たす最適な WAN リンクを選択します。

WAN SLA ポリシーは、契約を通じてテナントトラフィックに適用されます。

この機能が役立つ例として、MPLS、インターネット、4G などの複数の転送技術を使用して、ブランチがデータセンターにWAN を介して接続するという展開を考えてみます。このような展開では、ブランチとデータセンターの間に複数のパスが存在する可能性があります。この機能は、アプリケーショングループと SLA に基づき、このような状況下でも最適化パスを選択できるようにします。

Cisco ACI との統合に関するガイドライン

統合を設定するために Cisco SD-WAN Manager で実行する一般的な手順は次のとおりです。

1. Cisco ACI 登録の確認 （3 ページ） の手順の説明に従って、Cisco ACI が目的のコントローラを Cisco Catalyst SD-WAN コントローラ のパートナーとして登録したことを確認します。
2. 「ACI サイトのマッピング」セクションの説明に従って、デバイスを Cisco Catalyst SD-WAN コントローラ に接続します。

Cisco ACI と Cisco SD-WAN Manager を統合する場合は、次のガイドラインが適用されます。

- この統合は、新しい Cisco IOS XE Catalyst SD-WAN 展開でのみサポートされます。
- Cisco APIC がポリシーを送信するデバイスに、アプリケーション認識型ルーティングポリシーが設定されていないことを確認します。
- Cisco APIC がポリシーを送信する各デバイスにテンプレートが添付されていることを確認します。
- 統合を開始する前に、CLI ポリシービルダーを使用して一元管理型ポリシーを作成し、Cisco SD-WAN Manager ポリシービルダーを使用してアクティブにします。
- WAN SLA ポリシーを適用する前に、Cisco Catalyst SD-WAN コントローラ と Cisco APIC 間の接続を確立します。手順については、「Cisco ACI と Cisco IOS XE Catalyst SD-WAN 統合」を参照してください。
- デバイスを接続する前に、この統合用に Cisco ACI を設定します。

Cisco ACI 登録の確認

Cisco SD-WAN Manager との統合用に Cisco ACI を設定した後、Cisco SD-WAN Manager の次の手順を実行して、Cisco ACI が目的のコントローラを Cisco SD-WAN Manager パートナーとして登録したことを確認します。

1. Cisco SD-WAN Manager で、**[管理（Administration）]** > **[統合管理（Integration Management）]** を選択します 。

   [統合管理（Integration Management）] ページが表示されます。

2. [統合管理（Integration Management）] ページで、Cisco APIC がポリシーを送信するコントローラの [説明（Description）] に ACI パートナー登録が表示されていることを確認します。

SLA クラス

Cisco SD-WAN Manager は、ACI 統合で使用する事前設定された SLA クラスを提供します。これらの SLA クラスは自動的に使用可能になり、変更または削除できません。

これらの SLA を表示するには、次の手順に従います。

1. Cisco SD-WAN Manager で、**[設定（Configuration）]** > **[ポリシー（Policies）]** の順に選択します。
2. [カスタムオプション（Custom Options）] ドロップダウンリストから、[リスト（Lists）] を選択します。
3. 左側のタイプ一覧から [SLA クラス（SLA Class）] を選択します。

次の SLA クラスを使用できます。

- [ビジネス通常（Business Normal）]：通常の事業運営向けに設計されたもの
- [音声（Voice）]：音声操作用に設計されたもの
- [ビジネス重要（Business Critical）]：低パケット損失と低遅延を必要とする重要な事業運営向けに設計されたもの
- [ビジネス高（Business High）]：非常に重要なビジネス運営向けに設計されたもの

データプレフィックス

Cisco ACI は、統合に必要なデータプレフィックスリストを作成し、必要に応じてこれらのリストを動的に更新します。Cisco SD-WAN Manager でデータプレフィックスを設定する必要はありません。

これらのデータプレフィックスを表示するには、次の手順に従います。

1. Cisco SD-WAN Manager で、[設定（Configuration）] > [ポリシー（Policies）] を選択します。
2. [カスタムオプション（Custom Options）] ドロップダウンリストから、[リスト（Lists）] を選択します。
3. 左側のタイプリストから [データプレフィックス（Data Prefix）] を選択します。

Cisco ACI はこれらのデータプレフィックスを自動的に提供するため、このリストの情報は異なる場合があります。最新の情報を表示するため、随時ページを更新してください。

VPNs

ACI は、統合に必要な VPN を作成し、Cisco SD-WAN Manager に送信します。これらの VPN は Cisco SD-WAN Manager で自動的に使用可能になります。Cisco SD-WAN Manager で VPN を設定する必要はありません。

これらの VPN を表示するには、次の手順に従います。

1. Cisco SD-WAN Manager で、**[設定（Configuration）]** > **[ポリシー（Policies）]** の順に選択します。
2. [カスタムオプション（Custom Options）] ドロップダウンリストから、[リスト（Lists）] を選択します。
3. 左側のタイプ一覧から **[VPN]** を選択します。

SLA へのデータプレフィックスと VPN のマッピング

ACI はデータプレフィックスリストと VPN リストから SLA クラスへのマッピングを確立した後、そのマッピングを Cisco SD-WAN Manager に送信します。これらのマッピングは、Cisco SD-WAN Manager のアプリケーション ルート ポリシーを設定するページで確認できます。

App-Route-Policy の作成

ACI によってデータプレフィックスと VPN が SLA クラスリストにマッピングされると、app-rout-policy を作成して Cisco ACI 統合のシーケンスルールを定義できます。

App-route-policyを作成するには、次の手順を実行します。

1. Cisco SD-WAN Manager で、**[設定（Configuration）]** > **[ポリシー（Policies）]** の順に選択します。
2. 一元管理型ポリシーを含む行の右側にある [その他のアクション（More Actions）] アイコンをクリックして、[編集（Edit）] をクリックします。

3. [トラフィックルール（Traffic Rules）] を選択します。
4. **[ポリシーの追加（Add Policy）]** > **[新規作成（Create New）]** の順に選択します。
5. [ACIシーケンスルール（ACI Sequence Rules）] をクリックします。
6. [VPN] ドロップダウンから、VPN ID を選択します。Cisco SD-WAN Manager で、この VPN にマッピングされているデータプレフィックスと SLA クラスのリストが表示されます。（これらのマッピングを送信したのは ACI です）。
7. ポリシーに含めるデータプレフィックスと SLA クラスの左側にあるチェックボックスをオンにし、[インポート（Import）] をクリックします。
8. [名前（Name）] フィールドにはポリシーの名前を、[説明（Description）] フィールドにはポリシーの説明を入力し、[アプリケーション認識型ルーティングポリシーの保存（Save Application Aware Routing Policy）] をクリックします。Cisco SD-WAN Manager によってポリシーが作成されます。
9. サイトリストと VPN リストをポリシーに適用するには、[ポリシーアプリケーション（Policy Application）] を選択して、[アプリケーション認識型ルーティング（Application-Aware Routing）] を選択し、[新規サイトリストと VPN リスト（New Site Lists and VPN List）] をクリックします。
10. ポリシーに適用するサイトリストと VPN リストを選択します。
11. 必要に応じて、ポリシーにシーケンスルールを追加します。
12. [ポリシーの変更の保存（Save Policy Changes）] をクリックします。

ACI サイトのマッピング

ACI サイトのマッピングは、Cisco APIC からのポリシーが適用されるコントローラデバイスを指定します。

開始する前に、Cisco ACI との統合に関するガイドラインセクションのガイドラインを確認してください。

デバイスをコントローラにアタッチするには、次の手順に従います。

1. Cisco SD-WAN Manager で、**[管理（Administration）]** > **[統合管理（Integration Management）]** を選択します。
2. 該当するサイトの行の右側にある [その他のアクション（More Actions）]アイコンをクリックし、[デバイスのアタッチ（Attach Devices）] を選択します。
3. 左側の [Available Devices] 列で、グループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[Select All] をクリックします。
4. 右向きの矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。

（注） [選択されたデバイス（Selected Devices）] 列からデバイスを削除するには、その列でグループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[すべて選択（Select All）] をクリックしてから左向きの矢印をクリックします。

5. [Attach] をクリックします。

ACI サイトのマッピング解除

ACI サイトのマッピングを解除すると、マッピングが解除されたデバイスに Cisco APIC ポリシーが適用されなくなります。

コントローラからデバイスを切り離すには、次の手順に従います。

1. Cisco SD-WAN Manager で、**[管理（Administration）] > [統合管理（Integration Management）]** を選択します。

   [統合管理（Integration Management）] ページが表示されます。

2. 該当するサイトの行の右側にある [その他のアクション（More Actions）] アイコンをクリックし、[デバイスの切断（Detach Devices）] を選択します。

3. 左側の [Available Devices] 列で、グループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[Select All] をクリックします。

4. 右向きの矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。

（注） [選択されたデバイス（Selected Devices）] 列からデバイスを削除するには、その列でグループを選択して 1 つ以上のデバイスを検索するか、リストからデバイスを選択するか、[すべて選択（Select All）] をクリックしてから左向きの矢印をクリックします。

5. [Detach] をクリックします。

コントローラの削除

ACI のパートナーとしてのコントローラを削除する場合は、Cisco SD-WAN Manager で削除するのではなく、ACI を使用してその登録を削除することを推奨します。Cisco SD-WAN Manager から ACI パートナーを削除すると、ACI がパートナー用に作成したデータプレフィックスと VPN が自動的に削除されます。

開始する前に、ポリシー定義、および ACI が作成したデータプレフィックスリストと VPN リストから登録を削除し、これらのリストがどのポリシーからも参照されていないことを確認します。

1. Cisco SD-WAN Manager で、**[管理（Administration）]** > **[統合管理（Integration Management）]** を選択します。
2. コントローラにアタッチされているすべてのデバイスを切り離します。

   手順については、「コントローラからのデバイスの切り離し」のセクションを参照してください。
3. 該当するサイトの行の右側にある [さらに多くのアクション（More Actions）] アイコンをクリックし、[コントローラの削除（Delete Controller）] を選択します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。