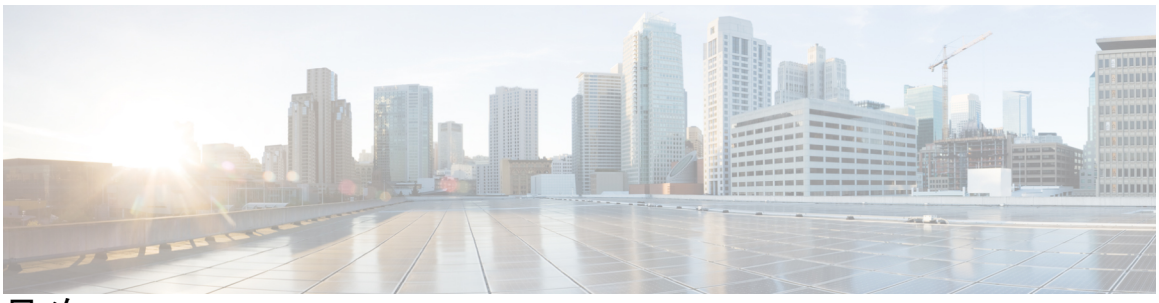
Cisco SD-WAN CloudOps

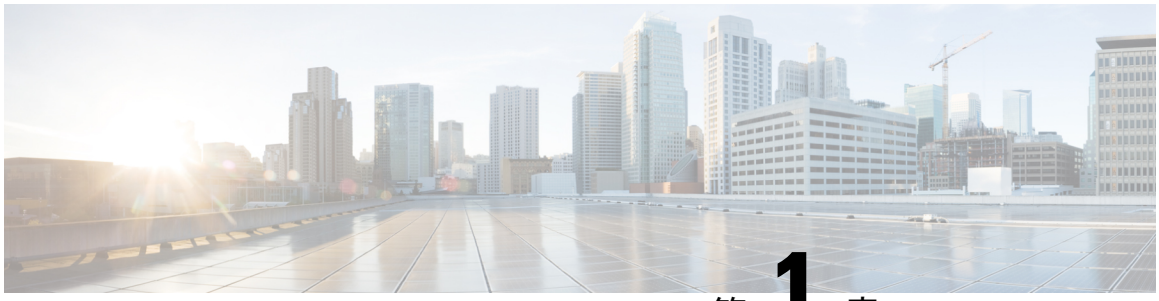
初版：2019 年 4 月 30 日

最終更新：2022 年 4 月 25 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/



目 次



第 1 章

Cisco CloudOps の概要

シスコは、Cisco vManage、Cisco vBond オーケストレーション、および Cisco vSmart コントローラ などの Cisco SD-WAN コントローラ向けにクラウドホスト型サブスクリプションを提供しており、それらのコントローラを単独で実行するコストを削減しながら、簡単かつ迅速に Cisco SD-WAN を展開します。クラウド導入モデルには、インスタンスのモニタリングサービスと高度な分析も含まれます。

このマニュアルについて

本書では、シスコが管理するクラウドホスト型 Cisco SD-WAN コントローラと、その機能およびサービスについて説明します。また、クラウドインフラストラクチャのホスティングプロセス、責任、および推奨事項についても詳しく説明します。

対象読者

本書の対象読者は、Cisco SD-WAN 向けのクラウドベース サブスクリプション オプションを購入または展開する、ネットワーク設計エンジニアとネットワークオペレータです。

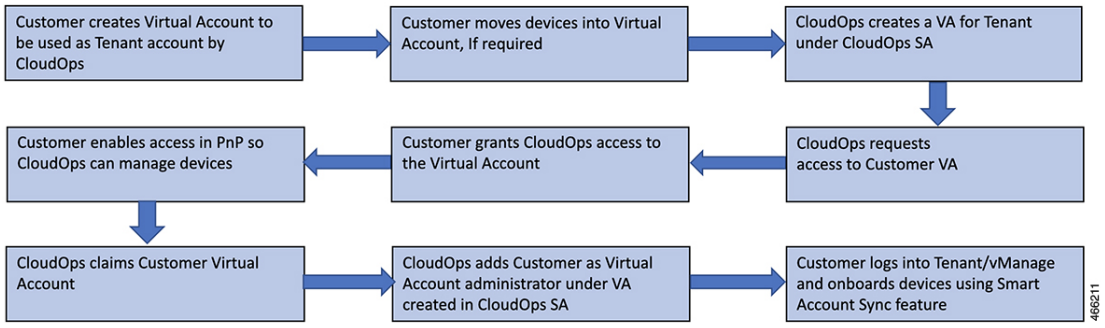
Cisco SD-WAN 内オーバーレイネットワークのタイプ

- **専用オーバーレイ**：このタイプのオーバーレイでは、Cisco vManage、Cisco vBond オーケストレーション、Cisco vSmart コントローラ などの Cisco SD-WAN コントローラのホスティングは、お客様専用です。
- **共有オーバーレイ**：このタイプのオーバーレイでは、Cisco vManage、Cisco vBond オーケストレーション、Cisco vSmart コントローラ、などの Cisco SD-WAN コントローラのホスティングは、複数のお客様間で共有されます。

このオーバーレイには次の主な機能が含まれます。

- データプレーン、コントローラプレーン、および管理プレーンのトラフィックは、お客様ごとに分離されます。
- Cisco SD-WAN コントローラ リリース 20.6.3 以降、すべてのオーバーレイは同じ長期リリースで維持されます。共有オーバーレイは、常に最新の長期スター付きリリースで実行されます。
- お客様は、仮想アカウント（VA）の外部管理を許可します。Cisco CloudOps は、仮想アカウント管理を受け入れて、Cisco Digital Network Architecture（DNA）サブスクリプションをお客様の仮想アカウントに保持します。このマッピングに基づいてオーバーレイを作成します。

図 *1*：お客様の仮想アカウントの管理



- Cisco Software-Defined AVC（SD-AVC）および Web 証明書が利用可能で、Cisco CloudOps によって管理されます。
- このタイプのオーバーレイに関する唯一の制限は、TrustSec、合法的傍受、および Radius/TACACS が現在サポートされていないことです。

- **専用マルチテナント（MT）オーバーレイ**：このタイプのオーバーレイでは、Cisco vManage、Cisco vBond オーケストレーション、Cisco vSmart コントローラ などの Cisco SD-WAN コントローラのホスティングは、お客様専用です。マネージドサービス プロバイダーは、エンドカスタマー向けの共有オーバーレイをホストします。

（注） 専用のマルチテナントオーバーレイは、AWS クラウドでのみホストできます。

カバレッジの概要

タスク	シングルテナント	共有	マルチテナント（MT）	注
オーバーレイのプロビジョニング				
Cisco SD-WAN セルフサービスポータル	カスタマー	Cisco CloudOps	Cisco CloudOps	CloudOps は、シングルテナントまたは専用、共有のオーバーレイ、およびクラスタをプロビジョニングします。 Cisco CloudOps は、お客様へのコントローラアクセス、カスタム DNS、スナップショットの頻度または保持をプロビジョニングします。
Cisco SD-WAN コントローラ インフラストラクチャのモニタリングとトラブルシューティング				
CPU とデータディスクの使用率	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
ネットワーク インターフェイスへの接続の損失	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
インスタンスへの到達の失敗	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Cisco SD-WAN サービスのモニタリング				
コントローラ SSL 証明書の有効期限の通知	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Cisco vManage Web サーバーの可用性	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	

タスク	シングルテナント	共有	マルチテナント（MT）	注
コントローラへの接続制御の損失	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Cisco SD-WAN コントローラのキャパシティ管理	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps は、オーバーレイ上のデバイスの数をモニタリングして、デバイス数に基づいてクラスタへの拡張のアップグレードを行います。
ディザスタ リカバリ	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
ボリュームベースのスナップショットを定期的に取得	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
設定ベースのバックアップを定期的に実行	Cisco CloudOps	—	—	
オンデマンド スナップショット	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
ボリュームまたは設定に基づくオーバーレイの復元	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
Cisco vAnalytics へのアクセスのプロビジョニング	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
オンプレミスからクラウドへの移行	Cisco CloudOps	—	—	
カスタムサブネットと TACACS	Cisco CloudOps	—	—	カスタムサブネットは、Day-0 プロビジョニング中にのみ使用できます。現在、TACACS はマルチテナント オーバーレイには使用できません。

タスク	シングルテナント	共有	マルチテナント（MT）	注
コントローラ証明書の承認（Symantec/Digicert）	Cisco CloudOps	Cisco CloudOps	Cisco CloudOps	
コントローラ証明書の更新（期限切れ前）	カスタマー	Cisco CloudOps	カスタマー	
ソフトウェアのアップグレード				
コントローラソフトウェアのアップグレード	カスタマー	Cisco CloudOps	カスタマー	
エッジデバイス/ノードソフトウェアのアップグレード	カスタマー	カスタマー	カスタマー	
Cisco CloudOps 通知に応答し、サービス時間帯の承認、インスタンスの再起動、Cisco CloudOps による変更の見直しまたは確認を実行	カスタマー	カスタマー	カスタマー	
software.cisco.com でスマートアカウント（SA）またはバーチャルアカウント（VA）を作成し、Cisco SD-WAN に登録済みのデバイスを SA または VA に接続	カスタマー	カスタマー	カスタマー	
PNP Connect での VA の外部管理を許可	—	カスタマー	—	
SA/VA の外部管理を受け入れ、テナント VA をお客様の SA/VA にマッピング	—	Cisco CloudOps	—	
Cisco vManage を使用してデバイス設定テンプレートとポリシーを定義	カスタマー	カスタマー	カスタマー	
Cisco vManage にログインする必要があるその他のアクティビティを実行。たとえば、テンプレートやポリシーの設定、エッジデバイスの管理	カスタマー	カスタマー	カスタマー	

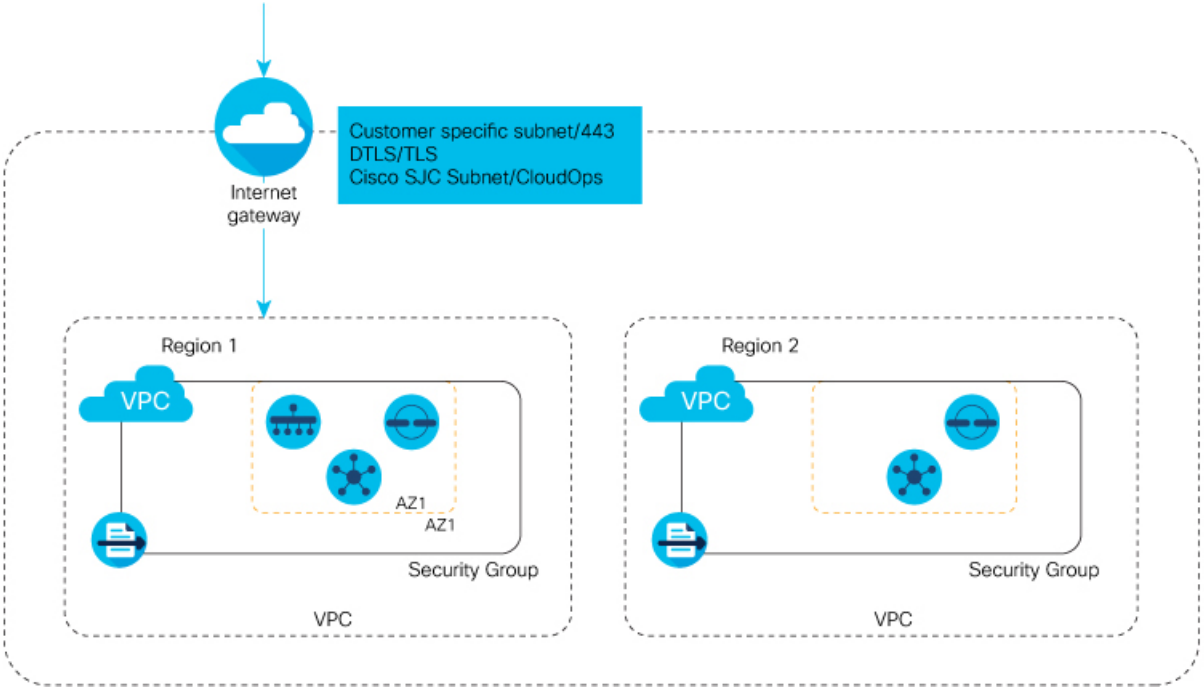
タスク	シングルテナント	共有	マルチテナント（MT）	注
Web サーバー証明書	カスタマー	Cisco CloudOps	カスタマー （注） カスタムドメインオプションを使用したマルチテナントオーバーレイには適用されません。	

ソリューション設計

このソリューションについて

Cisco SD-WAN コントローラのクラウドベースのサブスクリプションを選択すると、シスコは Cisco SD-WAN コントローラ（具体的には Cisco vManage、Cisco vBond オーケストレーション、および Cisco vSmart コントローラ）を、パブリッククラウドに展開します。その後、シスコは管理者アクセスを提供します。デフォルトでは、1 つの Cisco vManage、Cisco vBond オーケストレーション、および Cisco vSmart コントローラ がプライマリ クラウド リージョンに展開され、もう 1 つの Cisco vBond オーケストレーション および Cisco vSmart コントローラ はセカンダリまたはバックアップリージョンに展開されます。

図 *2:* ソリューションのアーキテクチャ



サポートされるクラウドとクラウドリージョン

Cisco SD-WAN コントローラの展開でサポートされるクラウドおよびクラウドリージョンは次のとおりです。

Amazon Web Services	Microsoft Azure
アジア太平洋：ジャカルタ	インドネシア	北米・中米・南米	ブラジル南部：サンパウロ州
アジア太平洋：ムンバイ	インド	北米・中米・南米	米国東部：バージニア州
アジア太平洋：ソウル	韓国	北米・中米・南米	米国西部：カリフォルニア州
アジア太平洋：シンガポール	シンガポール	北米・中米・南米	米国西部 2：ワシントン
アジア太平洋：シドニー	オーストラリア	アジア太平洋	オーストラリア中部：キャンベラ
アジア太平洋：東京	日本	アジア太平洋|オーストラリア東部：シドニー	ニューサウスウェールズ
カナダ中部：モントリオール	カナダ	アジア太平洋|オーストラリア南東部：メルボルン	ビクトリア

Amazon Web Services	Microsoft Azure
EU：フランクフルト	ドイツ	アジア太平洋	東日本：東京
EU：アイルランド	ダブリン	アジア太平洋	東南アジア：シンガポール
EU：ロンドン	英国	アジア太平洋	西インド：ムンバイ
EU：ストックホルム	スウェーデン	ヨーロッパ	フランス中部：パリ
南米：サンパウロ	ブラジル	ヨーロッパ	北ヨーロッパ：アイルランド
米国東部：バージニア州北部	米国	ヨーロッパ	英国南部：ロンドン
米国西部：カリフォルニア州北部	米国	ヨーロッパ	西ヨーロッパ：オランダ
米国西部：オレゴン州	米国	UAE 北部：ドバイ

マルチテナントサポートつきのクラウドとクラウドリージョン

Cisco SD-WAN コントローラの展開でマルチテナント機能をサポートするクラウドおよびクラウドリージョンは次のとおりです。

Amazon Web Services	Microsoft Azure
北米・中米・南米	米国東部：バージニア州	北米・中米・南米	米国東部：バージニア州
	UAE 北部：ドバイ

お客様側の責任

- 期限内にコントローラ証明書を更新します。
- ソフトウェアをアップグレードします。
  - 次に関する TAC ケースをオープンできます。
    - ソフトウェアのアップグレードで問題が発生した場合。
    - Cisco vManage のボリュームまたは設定のバックアップを取る必要がある場合。
    - ロールバックが必要な場合。
  - Cisco vBond オーケストレーション と Cisco vSmart コントローラ はステートレスサービスです。したがって、それらのバックアップを取る必要はありません。Cisco vManage は設定を自動的にプッシュします。
  - Cisco SD-WAN サポートチームは、クラスタやマルチテナントテナントオーバーレイなどの複雑な展開のソフトウェアアップグレードをカバーできる場合があります。た

だし、このサポートは、単一テナントの単一ノードオーバーレイでは利用できません。

- エッジデバイスのソフトウェアバージョンのアップグレードは、お客様側で行う必要があります。コントローラのバージョンに基づくエッジデバイスの互換性のあるバージョンについては、Cisco SD-WAN コントローラの互換性マトリックスを参照してください。

- Cisco CloudOps から送信された通知に対応して、サービス時間帯の承認、インスタンスの再起動、Cisco CloudOps による変更の見直しまたは確認を行います。
- Cisco CloudOps から通知を受信したら、TAC ケースをオープンしてサービス時間帯を設定します。一部の操作は、お客様の同意がある場合にのみ実行できます。例として、コントロール プレーン フラップを引き起こすインスタンスのアップグレードを実行する場合などがあります。
- `software.cisco.com` でスマートアカウント（SA）またはバーチャルアカウント（VA）を作成して、Cisco SD-WAN に登録済みのデバイスを SA または VA に接続します。
- Cisco vManage を使用してデバイス設定テンプレートとポリシーを定義します。
- Cisco vManage にログインする必要があるその他のアクティビティを実行。

お客様が本項に記載されている責任を果たさない場合、SD-WAN クラウド SLA（保証されたサービス稼働時間を含む）は無効になります。

Cisco CloudOps 側の責任

オーバーレイのプロビジョニング

- Cisco SD-WAN オーバーレイのクラウドホスト型コントローラをプロビジョニングし、有効期限が 1 週間の一意の管理者パスワードを設定し、Cisco vManage をお客様に引き渡します。
- お客様が SO でデフォルトのテンプレートとポリシー プッシュ オプションを選択した場合は、デフォルトのテンプレートとポリシーを使用して Cisco vManage を設定します。
- 必要に応じて、シングルテナントおよびマルチテナントクラスタを作成および管理します。
- マルチテナント オーバーレイでテナントを作成および管理します（直接取引の企業・官公庁のお客様）。

モニタとトラブルシューティング

Cisco CloudOps は、クラウドホスト型オーバーレイの状態をモニタリングし、問題がある場合はトラブルシューティングを行います。

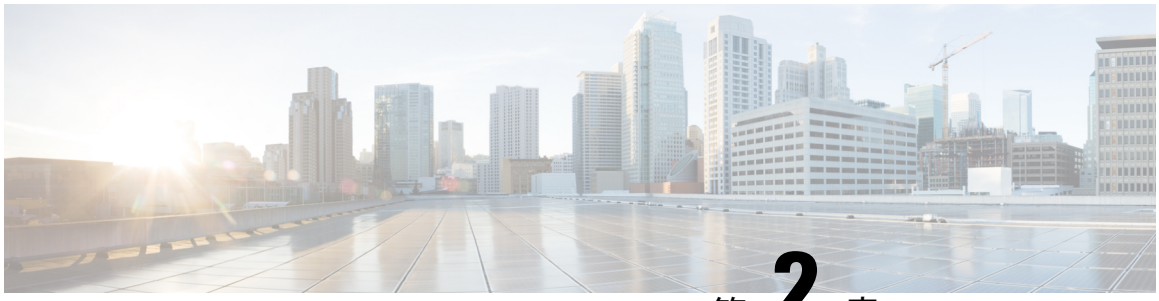
- Cisco CloudOps は、Cisco SD-WAN コントローラの状態をチェックしてアラートを生成する、リアルタイムのモニタリングシステムによってサポートされています。このチェックには、Cisco vManage、アプリケーションまたは Web サーバー、その他のマイクロサービス、設定または統計データベースの状態が含まれます。
- ユーザーが制御できないクラウドインフラストラクチャの問題に対して、プロアクティブなアクションを実行します。または、潜在的な問題についてお客様に通知し、詳細な調査のために Cisco TAC サポートケースをオープンするようにお客様に要求します。
- インスタンスのアップまたはダウン状態、CPU、ネットワーク非アクティブステータスに関するクラウドプロバイダー環境からの通知に基づいてアラートを管理します。
- サービスのダウンタイムを必要としない場合は、アラートをプロアクティブに解決します。サービスがフラップしたときにお客様に通知します。
- 90、60、および 30 日目の通知をお客様に送信して Cisco vManage で期限切れになる証明書を更新し、必要に応じて承認も行います（Symantec 証明書）。Cisco SD-WAN コントローラの証明書の有効期限は 1 年間です。

クラウド インフラストラクチャ サポート

- スナップショットボリュームまたは設定を含むディザスタ リカバリ ワークフローを実行します。ボリュームまたは設定に基づいて Cisco vManage クラスターを復元します。
- お客様の構内ネットワークをクラウドホスト型オーバーレイネットワークに拡張するため、カスタムサブネットをプロビジョニングします。
- オンプレミスからクラウドへの移行を管理します。

Capacity Management

- CPU、ディスク、メモリ使用率などのコントローラ インスタンス キャパシティ パラメータとともに、オーバーレイごとのデバイスの増加をモニタリングします。事前に設定されたガイドラインに従って、必要に応じてサービスインスタンスのキャパシティを増やします。



第 2 章

注文、検証、およびアカウント管理

Cisco プラグアンドプレイのロール

Cisco プラグアンドプレイは、Cisco SD-WAN Salesforce（SFDC）のレガシープロセスに代わるものです。

Cisco SD-WAN プラグアンドプレイについては、次のマニュアルを参照してください。

- Cisco プラグアンドプレイ サポート ガイド
- FAQ

Cisco SD-WAN クラウドホスト型コントローラのプロビジョニング

Cisco CloudOps システムでは、次の条件が満たされた後に、SO の Cisco SD-WAN クラウドホスト型コントローラを作成できます。

1. SO にクラウド サブスクリプション ライセンスが付与されている。
2. SO に含まれる Cisco SD-WAN の品目が [Shipped] としてマークされている。
3. SO がアクティブなスマートアカウント（SA）とそのスマートアカウント内のバーチャルアカウント（VA）に割り当てられている。

注文

ライセンスタイプと発注情報

ライセンスと契約には、次の 3 種類があります。

- **アラカルト**：お客様は、各 Cisco SD-WAN コントローラの型番（SKU）を個別に購入します。
- **エンタープライズ アグリーメント（EA）**： お客様は、Cisco SD-WAN コントローラ の SKU を含む EA バンドルを購入します。ただし、現時点では利用できません。EA 契約と併せて、コントローラのアラカルトライセンスを、クラウドコントローラのプロビジョニングに使用する必要があります。
- **マネージドサービス ライセンス契約（MSLA）**：お客様は、Cisco SD-WAN コントローラ SKU を含む MSLA 契約を購入します。ただし、現時点では利用できません。

アラカルト発注

Cisco SD-WAN コントローラのアラカルト方式ライセンスの購入を希望するお客様は、『Cisco SD-WAN Controllers Ordering Guide』を参照してください。

EA の注文

エンタープライズ アグリーメント（EA）のお客様向けの Cisco SD-WAN クラウドホスト型コントローラをプロビジョニングするには、次の手順を実行します。

1. EA ワークスペース（EAWS）にリクエストを送信します。
2. アラカルト型番を使用して、Cisco SD-WAN コントローラの型番 （SKU）を個別に注文します。注文の詳細については、『Cisco SD-WAN Controllers Ordering Guide』を参照してください。
3. Cisco CloudOps チームが注文の詳細を検証し、オーバーレイをプロビジョニングするか、オーバーレイのプロビジョニングを行う Cisco SD-WAN セルフサービスポータル にお客様を誘導します。

検証

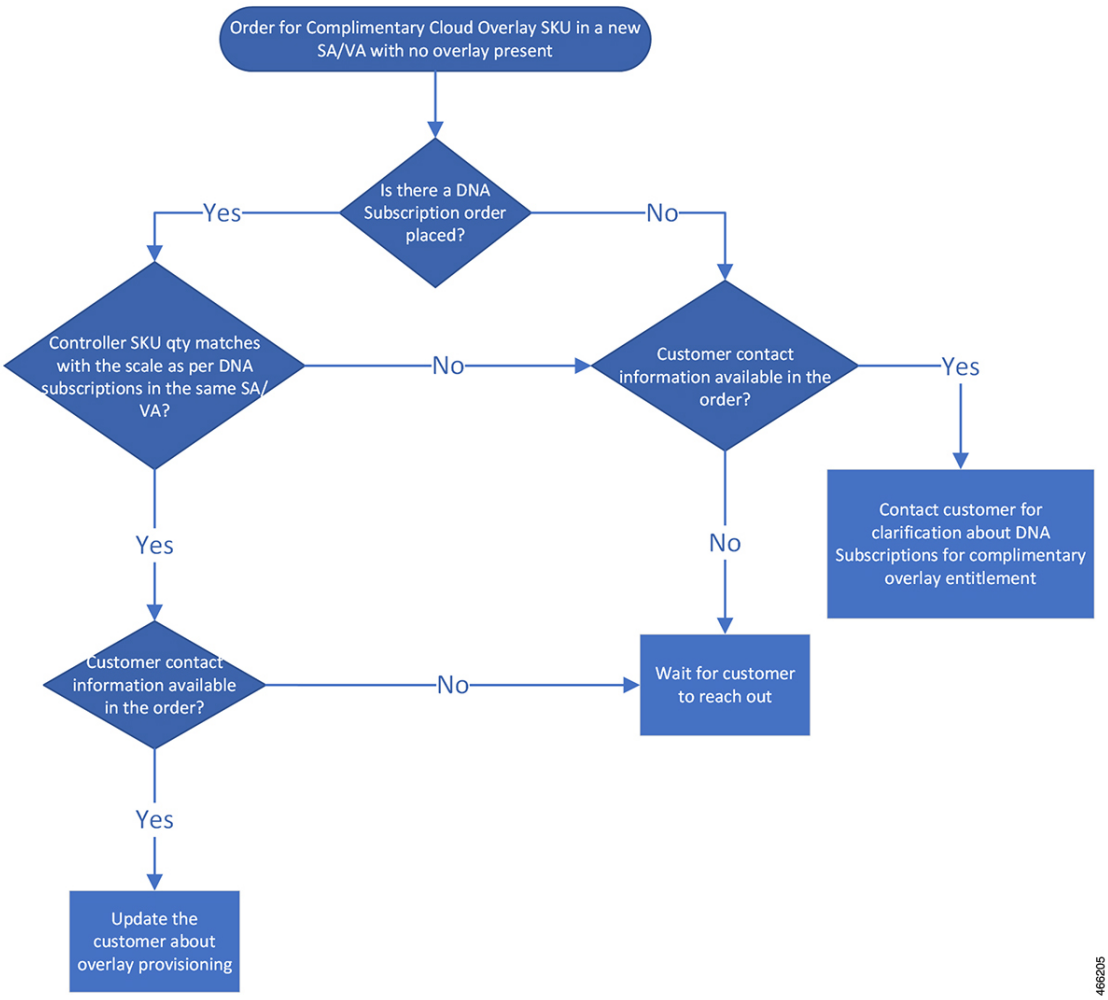
無償 Cisco SD-WAN コントローラ SKU

Cisco CloudOps は、次の項目をチェックすることにより、コントローラの型番（SKU）に基づいて無償コントローラのプロビジョニングを検証します。

- 対応するネットワーク規模をサポートする Cisco Digital Network Architecture（Cisco DNA）サブスクリプションの数（必須の Cisco SD-WAN サブスクリプション）
- 対応するネットワーク規模 （デバイス数）に対するコントローラ SKU の正しい選択。

両方の項目が確認され、それらに互換性がある場合、Cisco CloudOps はお客様に連絡して、コントローラのプロビジョニングに必要な、より詳細な情報を収集します。このために、Cisco CloudOps チームは、新しい注文に提供された連絡先情報を使用します。お客様から必要な情報を受け取ると、Cisco CloudOps はクラウドコントローラのプロビジョニングに進みます。

図 *3 :* 無償 *Cisco SD-WAN* クラウドコントローラ *SKU* のワークフロー



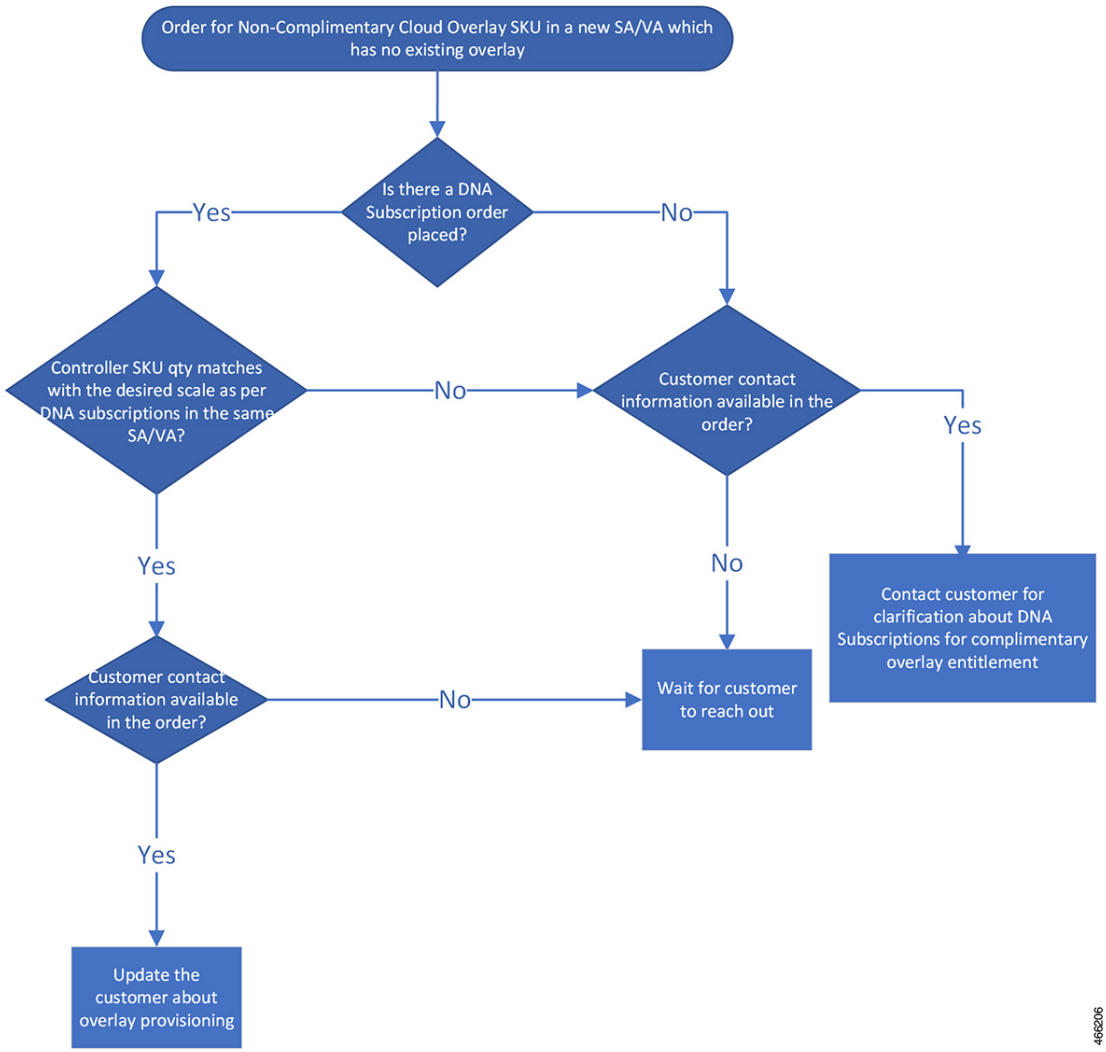
有償 Cisco SD-WAN コントローラ SKU

Cisco CloudOps は、次の項目をチェックすることにより、コントローラの型番（SKU）に基づいて有償コントローラのプロビジョニングを検証します。

- 対応するネットワーク規模 （デバイス数）に対するコントローラ SKU の正しい選択。

選択したコントローラの SKU が、対応するネットワークの規模と互換性がある場合、Cisco CloudOps はお客様に連絡して、コントローラのプロビジョニングに必要な、より詳細な情報を収集します。このために、Cisco CloudOps チームは、新しい注文に提供された連絡先情報を使用します。お客様から必要な情報を受け取ると、Cisco CloudOps はクラウドコントローラのプロビジョニングに進みます。

図 *4 :* 無償 *Cisco SD-WAN* コントローラ *SKU* のワークフロー

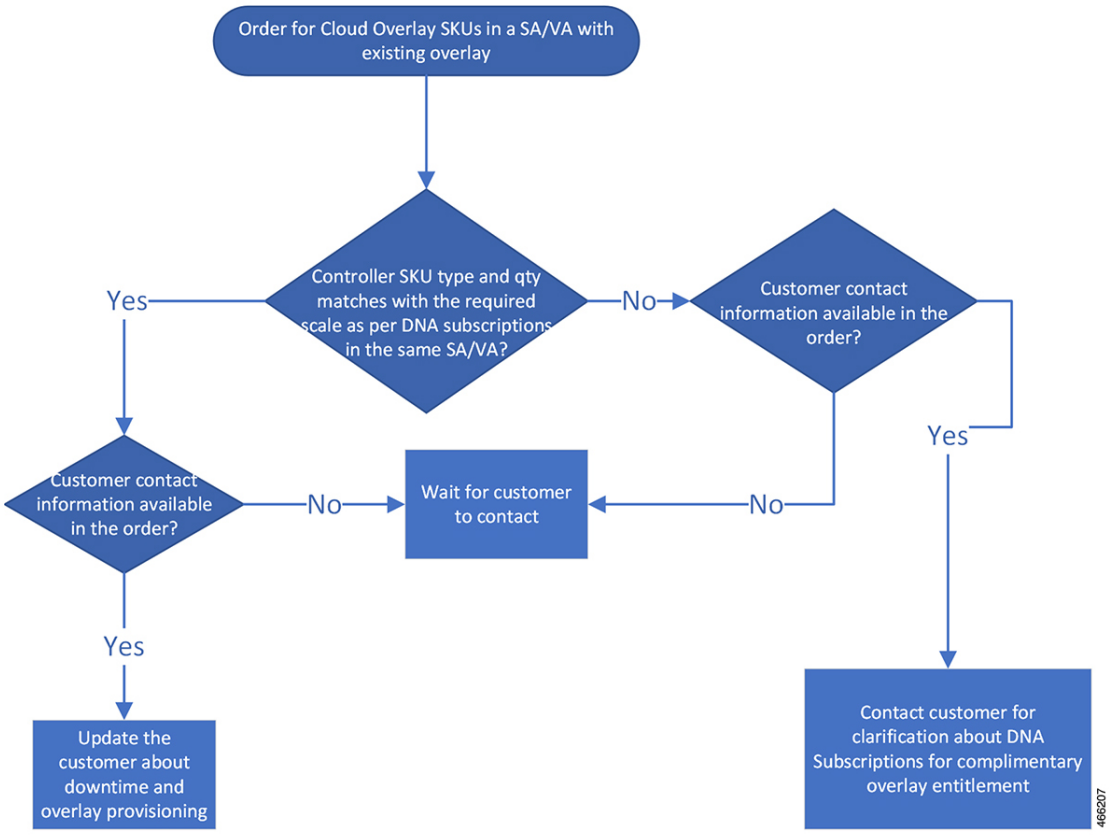


既存のオーバーレイ内の新しいコントローラ

Cisco CloudOps は、次の項目をチェックすることにより、コントローラの型番（SKU）に基づいたコンピューティングリソースの追加を（水平または垂直の拡張）検証します。

- 対応するネットワーク規模 （デバイス数）に対するコントローラ SKU の正しい選択。
- 対応するネットワーク規模をサポートする Cisco Digital Network Architecture（Cisco DNA）サブスクリプションの数（無償 SKU の必須 Cisco SD-WAN サブスクリプション）
- メンテナンス時間帯（ダウンタイムが必要なため）

図 *5:* 既存のオーバーレイ内の新しいコントローラのワークフロー



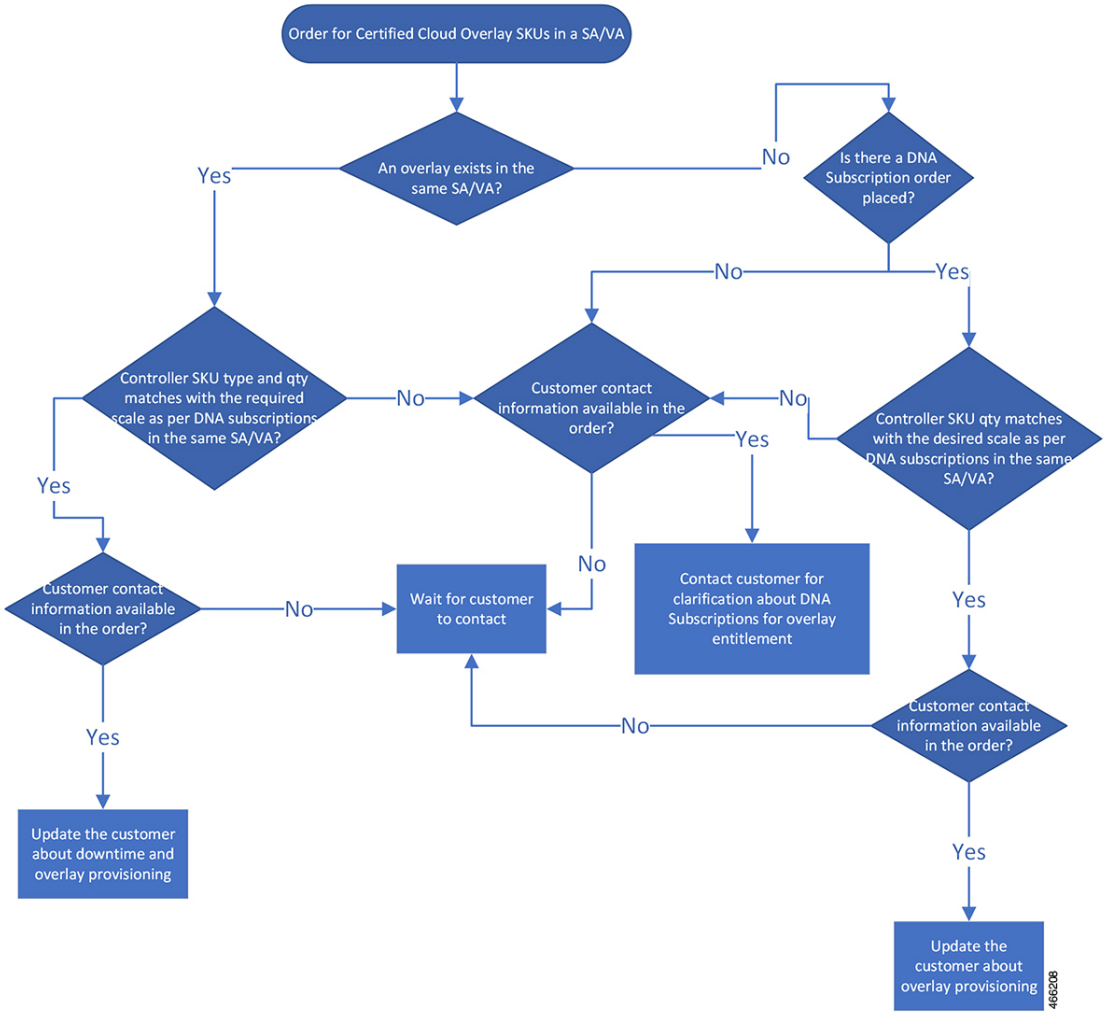
認定環境内のコントローラ

Cisco CloudOps は、次の項目をチェックすることにより、コントローラの型番（SKU）に基づいて認定コントローラーのプロビジョニングを検証します。

- 対応するネットワーク規模（デバイス数）に対する認定コントローラ SKU の正しい選択。
- CloudOps は、コントローラ SKU または既存のコントローラに基づいて注文をクロスチェックします。非認定オーバーレイから認定オーバーレイに移行するには、オーバーレイの再プロビジョニングが必要です。再プロビジョニングとは、既存のコントローラが削除され、新しいコントローラが同じ組織名でスピンアップされることを意味します。
- メンテナンス時間帯（ダウンタイムが必要なため）

選択した認定コントローラ SKU が、選択したコントローラ型番または既存のコントローラとネットワークの規模の両方と互換性がある場合、Cisco CloudOps はお客様に連絡して、コントローラのプロビジョニングに必要な、より詳細な情報を収集します。このために、Cisco CloudOps チームは、新しい注文に提供された連絡先情報を使用します。お客様から必要な情報を受け取ると、Cisco CloudOps はクラウドコントローラのプロビジョニングに進みます。

図 *6* : 認定環境内コントローラのワークフロー



アカウント管理

別のアカウントへのオーバーレイの転送

あるスマートアカウント（SA）またはバーチャルアカウント（VA）から別の SA または VA にオーバーレイを移動するには、次の手順を実行します。

- 送信元 SA/VA および宛先 SA/VA の詳細を TAC に提供します。
- オーバーレイの所有者/SE は、移行のために TAC csone をオープンする必要があります。
- 移行について予定されるダウンタイムはありません。

PNP の [Transfer Selected] ボタンを使用してデバイスシリアルを新しい SA/VA に移動するか、Cisco TAC サポートケースをオープンしてサポートを受けられます。

オーバーレイの機能および次の詳細は、移行によって変更されません。

1. 組織名
2. Cisco vBond オーケストレーション、Cisco vManage、または Cisco vSmart コントローラ DNS 名
3. すべてのコントローラに割り当てられているすべての現在のパブリック IP
4. 証明書を含む Cisco vManage 設定全体
5. IP アドレスの現在の許可リスト

移行後、Cisco vManage で設定された SA クレデンシャルを更新する必要があります。

オンプレミスからクラウドへの移行プロセスの詳細

既存のオンプレミス Cisco SD-WAN オーバーレイを、シスコがプロビジョニングしたクラウドホスト型コントローラに移行する必要がある場合の、プロセスの概要は次のとおりです。

全体的なプロセス

- Cisco SD-WAN クラウドサブスクリプションを入手します。
- Cisco CloudOps チームで Cisco TAC サポートケースをオープンして、オンプレミスからクラウドへの移行を要求します。
- 以下に関する詳細を提供する必要があります。
  - オンプレミス オーバーレイ コントローラ プロファイルが作成される既存のスマートアカウント（SA）およびバーチャルアカウント（VA）。
  - クラウドサブスクリプションを購入した SO の番号。
  - オンプレミスで設定されているオーバーレイの現在の組織名。
  - 必要なクラウドタイプの選択。
  - プロビジョニングの必要なプライマリリージョンとセカンダリリージョンの選択。
  - Cisco CloudOps チームからのアラート通知およびその他の連絡を受信するための連絡先となる、単一の電子メールアドレス（チームの電子メールアドレスが望ましい）。
  - プロビジョニングする Cisco vManage と Cisco vBond オーケストレーション の FQDN のホスト名のオプションの選択。
  - TACACS/AAA/Syslog などのユースケースに必要なカスタムプライベート IP サブネットのオプションの選択（プロビジョニングの 2 つのリージョンに、それぞれ /24 IP プレフィックスを指定）。

- 展開されたエッジの数に関する現在のオンプレミス オーバーレイ ファブリックのサイズ。
- 現在のオンプレミスオーバーレイで実行している Cisco vManage、Cisco vBond オーケストレーション、および Cisco vSmart コントローラ インスタンスのソフトウェアバージョン。
- 現在のオンプレミス オーバーレイ コントローラ証明書ソース（Cisco/Symantec/Enterprise）ルート CA。
- 現在のオンプレミスオーバーレイ Cisco vManage からのコンフィギュレーション データベースのバックアップコピー。

（注） Cisco vManage コンフィギュレーション データベースのパスワードをデフォルトにリセットしてからバックアップを取得するか、設定したパスワードでバックアップを取得して、そのパスワードを Cisco TAC ケースで共有することができます。

- 現在のオンプレミスオーバーレイ Cisco vManage からの実行コンフィギュレーションのコピー 。
- クラウドホスト型コントローラに使用されるシステム IP アドレスの範囲（現在のオンプレミス Cisco SD-WAN ファブリック内の未使用の範囲である必要があります）。

- Cisco CloudOps チームは、クラウドホスト型コントローラセットをプロビジョニングし、コントローラ証明書をインストールして、詳細を共有します。
- Cisco CloudOps チームは、オンプレミス Cisco vManage から提供されたコンフィギュレーションデータベースのバックアップと実行コンフィギュレーションを新しいクラウドホスト型 Cisco vManage インスタンスに適用します。
- 必要に応じて、クラウドホスト型コントローラの新しい IP を使用して、エンタープライズ ファイアウォールを更新する必要がある場合があります。
- パイロット変更時間帯を設定して実行し、1 つ以上のテストエッジノードをクラウドホスト型コントローラに移行してから、オンプレミス Cisco vManage にロールバックします。
- エッジノードで新しい Cisco vBond オーケストレーション FQDN を構成することで移行がトリガーされます。
- 必要な措置を講じて、最終の変更時間帯に備えます。
- すべてのエッジノードをオンプレミスからクラウドホスト型コントローラセットに移行するための、最終変更時間帯を設定して実行します。
- テンプレートが作成され、オンプレミスの Cisco vManage 、Cisco vBond オーケストレーション、および Cisco vSmart コントローラに適用されている場合は、これらのテンプレー

トを確認して修正してから、移行後にクラウドホスト型コントローラに適用する必要があります。インターフェイス設定に関しては、特別な注意が必要です。

前提条件

- ケースを開く前に、既存のすべてのコントローラとエッジノードをシスコが推奨する最新のリリースバージョンのいずれかにアップグレードし、データプレーンが安定していることを確認する必要があります。
- すべてのエッジノードをテンプレートにアタッチするか、移行のためにエッジノードを手動で再構成することに同意する必要があります。
- NTP と DNS が機能するすべてのエッジノードが必要です。
- オンプレミスコントローラでエンタープライズ証明書を使用している場合は、ルート CA をシスコに提供する必要があります。
- エッジノードがリカバリのために手動設定を必要とする場合は、コンソールまたは代替の方法でエッジノードにアウトオブバンドアクセスする必要があります。

検討事項と影響

- Cisco SD-WAN クラウドサブスクリプションを調達し、オンプレミス オーバーレイ コントローラ プロファイルが作成される既存のスマートアカウント（SA）および仮想アカウント（VA）に追加するには、シスコアカウントチームまたはシスコサポートと連携する必要があります。
- Cisco CloudOps チームは、プライマリリージョンでのみ Cisco vManage をプロビジョニングします。

  プライマリリージョンとセカンダリリージョンの両方にプロビジョニングされた Cisco vBond オーケストレーション と Cisco vSmart コントローラ インスタンスがあります。
- Cisco CloudOps チームは、既存のオンプレミスオーバーレイと同じ SA/VA に新しいコントローラプロファイルを作成します。

  これにより、クラウドホスト型コントローラセットに、既存のオンプレミスオーバーレイと同じ組織名を付けることができ、コンフィギュレーションデータベースをオンプレミス Cisco vManage からクラウドホスト型 Cisco vManage に転送できるようになります。

  ソースインスタンスと宛先の Cisco vManage インスタンスに異なる組織名が設定されていると、コンフィギュレーションデータベースの復元方法を使用できません。クラウドホスト型 Cisco vManage インスタンスの組織名は、プロビジョニング後に変更することはできません。
- 新しい Cisco vManage はコンフィギュレーション データベースの復元方法を使用して構成されているため、オンプレミス Cisco vManage の統計データベースは移行されません。
- オンプレミスのオーバーレイでCisco vAnalytics が使用されている場合は、引き続き機能します。

新しいクラウド Cisco vManage が新しいデータ収集を開始してCisco vAnalytics サーバーに送信するため、移行が行われると、一部のデータが失われる可能性があります。

- Cisco vBond オーケストレーション FQDN が変更されると、移行のためにエッジノードの構成を更新する必要があります。

  これは、すべてのエッジノードに適用された Cisco vManage の CLI テンプレートを使用して実行できます。オンプレミス Cisco vManage に CLI テンプレートが存在しない場合は、移行の開始前に作成して適用する必要があります。CLI テンプレートを使用しない場合は、コンソールまたは ssh を介してすべてのエッジノードを個別に手動で再構成する必要があります。

- エッジノードの移行中に問題が発生した場合、エッジノードへのアウトオブバンド管理アクセスを確保して、手動による変更で新しい Cisco vBond オーケストレーション に切り替える必要があります。

- 移行時に、各エッジノードが新しい Cisco vBond オーケストレーション DNS を指して新しいクラウドホスト型コントローラに再接続する際に、各エッジノードのコントロールとデータプレーンがフラップします。

- 移行の前に、すべてのエッジノードで NTP と DNS が機能するように構成する必要があります。

- ロールバックプランには、 Cisco vBond オーケストレーション 設定をエッジノードでオンプレミス Cisco vBond オーケストレーション に戻す操作が含まれます。

- 移行が完了したら、ホストしたコントローラプロファイルを Cisco PNP SA/VA から削除できます。

クラウドホスト型コントローラの削除ポリシー

シスコは、次の条件に基づいて、お客様のクラウドホスト型コントローラオーバーレイを削除できます。

証明書の有効期限

- **識別ステージ**：お客様のコントローラの証明書の期限が切れて 15 日以上過ぎており、証明書が更新されていない場合、シスコはクラウドホスト型コントローラをシャットダウン状態に移行できます。期限切れのコントローラ証明書は、クラウドホスト型コントローラオーバーレイおよび接続されたデバイスが使用されていないことを意味します。

- **最終終了**：オーバーレイが少なくとも3ヵ月間シャットダウン状態であり、コントローラを復旧するための連絡がない場合、シスコはコントローラを削除します。その結果、お客様のデータは回復できなくなります。

- **再プロビジョニング**：オーバーレイが削除された場合、再プロビジョニングする必要があります。アクティブな Cisco Digital Network Architecture（Cisco DNA）ライセンスがある場合は、新しいクラウドホスト型コントローラオーバーレイをリクエストできます。

放棄されたオーバーレイ

- **識別ステージ**：クラウドホスト型コントローラが 6 か月以上プロビジョニングされており、かつ：

  1. アクティブなエッジデバイスがない場合
  2. または、そのクラウドホスト型コントローラのポリシーに記載されている以外の理由で、オーバーレイが 30 日以上シャットダウン状態になっている場合

  シスコは、そのクラウドホスト型コントローラが放棄されたとみなすことができます。アクティブなエッジデバイスがないこと、またはオーバーレイがシャットダウンされていることは、 Cisco SD-WAN オーバーレイおよびクラウドホスト型コントローラデバイスが使用されていないことを示していることに注意してください。

- **通知ステージ**：シスコは、ターゲットのシャットダウン日程とともに、オーバーレイの放棄状態を知らせる通知をお客様に送信します。
- **シャットダウンステージ**：通知後もお客様のオーバーレイが引き続き使用されない場合、シスコは指定日にオーバーレイをシャットダウンします。
- **最終終了**：オーバーレイのシャットダウン後 30 日以内に Cisco SD-WAN クラウドホスト型コントローラを復旧するための連絡がない場合、シスコはコントローラを削除します。その結果、お客様のデータは回復できなくなります。
- **再プロビジョニング**：オーバーレイが削除された場合、再プロビジョニングする必要があります。アクティブな Cisco Digital Network Architecture（Cisco DNA）ライセンスがある場合は、新しいクラウドホスト型コントローラオーバーレイをリクエストできます。

DNA サブスクリプション期限切れ

このポリシーは、シスコがクラウド コントローラ サブスクリプションを個別に利用可能にする前に、ライセンス付与されたデバイスの Cisco Digital Network Architecture（Cisco DNA）サブスクリプションに適用されます。これは、事前コントローラ サブスクリプション オファリングとも呼ばれます。

- **識別ステージ**：クラウドホスト型コントローラに接続されているデバイスのすべての Cisco DNA サブスクリプションが期限切れになっている場合、シスコは対応するクラウドホスト型コントローラをサブスクリプションの期限切れと見なすことができます。
- **通知ステージ**：シスコは、ターゲットのシャットダウン日程とともに、オーバーレイの放棄状態を知らせる通知をお客様に送信します。通知をタイムリーに受け取るために、連絡先情報を最新の状態に保つようにしてください。
- **シャットダウンステージ**：通知後も引き続きお客様のオーバーレイが期限切れの DNA サブスクリプションで実行している場合、シスコは指定日にオーバーレイをシャットダウンします。

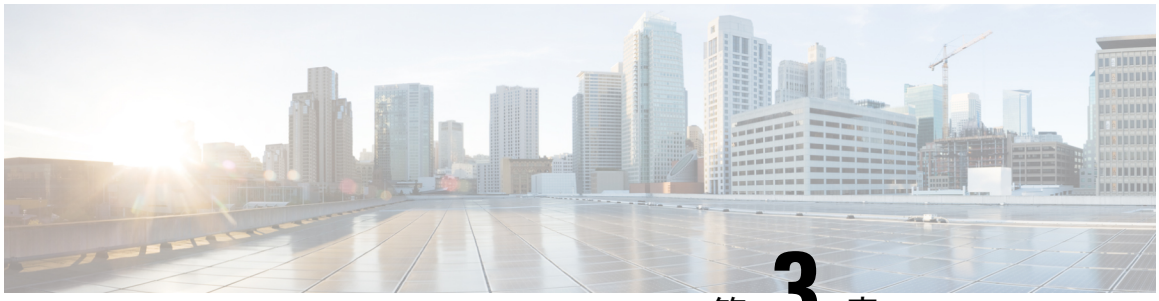
- **最終終了**：オーバーレイのシャットダウン後 30 日以内にお客様の Cisco SD-WAN クラウドホスト型コントローラを復旧するための連絡がない場合、シスコはコントローラを削除します。その結果、お客様のデータは回復できなくなります。
- **再プロビジョニング**：オーバーレイが削除された場合、再プロビジョニングする必要があります。必要な型番（SKU）を購入することで、クラウドホスト型の新しいコントローラオーバーレイを購入できます。

コントローラ サブスクリプション期限切れ

コントローラのサブスクリプションは、デバイスの Cisco Digital Network Architecture（Cisco DNA）サブスクリプションとは別にライセンス付与されます。

- **識別ステージ**：クラウドホスト型コントローラのサブスクリプションが期限切れになっている場合で、お客様がそのサブスクリプションを更新していない場合、シスコは対応するクラウドホスト型コントローラをサブスクリプションの期限切れと見なすことができます。
- **通知ステージ**：シスコは、ターゲットのシャットダウン日程とともに、オーバーレイの放棄状態を知らせる通知をお客様に送信します。通知をタイムリーに受け取るために、連絡先情報を最新の状態に保つようにしてください。
- **シャットダウンステージ**：通知後も引き続きコントローラのサブスクリプションが更新されない場合、シスコは指定日にオーバーレイをシャットダウンします。
- **最終終了**：オーバーレイのシャットダウン後 30 日以内にお客様の Cisco SD-WAN クラウドホスト型コントローラを復旧するための連絡がない場合、シスコはコントローラを削除します。その結果、お客様のデータは回復できなくなります。
- **再プロビジョニング**：オーバーレイが削除された場合、再プロビジョニングする必要があります。必要な型番（SKU）を購入することで、クラウドホスト型の新しいコントローラオーバーレイを購入できます。

（注） シスコのクラウドホスト型コントローラの DNA サブスクリプションを更新しない場合、デバイスの Cisco DNA サブスクリプションの一部である Cisco SD-WAN 機能の動作に影響を与える可能性があります。これは、これらの機能が Cisco SD-WAN コントローラに依存しているためです。



第 3 章

証明書の管理

Web サーバー証明書

シスコは Cisco vManage の Web 証明書を発行しません。証明書署名要求（CSR）を生成し、ドメインネームシステム（DNS）名の認証局（CA）の署名を得ることをお勧めします。その後、IP の DNS サーバーに A エントリを追加するか、`.viptela.net / .sdwan.cisco.com` vManage DNS 名に CNAME を追加します。

（注） シスコが発行するコントローラ証明書は、コントローラが内部で使用するためのものです。これらの証明書を使用して Web サーバー証明書を発行することはできません。

詳細については、『Cisco SD-WAN Getting Started Guide』の「Web Server Certificates」の項を参照してください。

コントローラの Cisco SD-WAN SSL 証明書の更新

署名付き証明書は、オーバーレイネットワーク内のデバイスの認証に使用されます。認証されたデバイスは、相互にセキュアなセッションを確立できます。

Cisco vManage を使用して、証明書署名要求（CSR）を生成し、署名付き証明書をインストールできます。証明書ルート CA には、次の 3 つのオプションがあります。

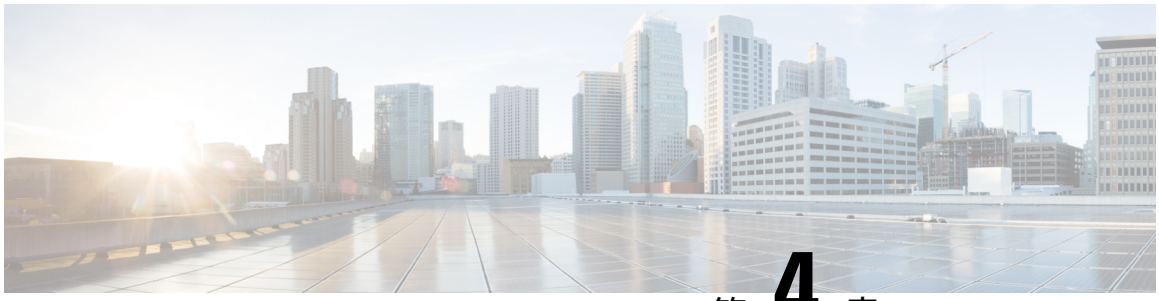
1. Cisco Root CA バンドル（ソフトウェアバージョン 19.2.3 以降を搭載のコントローラ、ソフトウェアバージョン 19.2.3 以降を搭載の Cisco SD-WAN デバイス、ソフトウェアバージョン 16.12.3+ または 16.10.4+ または 17.x+ 以降を搭載の Cisco IOS XE SD-WAN に提供済み）
2. Symantec/Digicert Root CA（すべてのコントローラ、Cisco SD-WAN デバイス、および Cisco IOS XE SD-WAN デバイスに提供済み）

3. お客様自身の Enterprise Root CA

（注） 証明書生成方式を 1 回だけ選択します。選択した方法は、オーバーレイネットワークにデバイスを追加するたびに自動的に適用されます。

コントローラ証明書を更新するには、展開タイプと証明書タイプに基づく適切なプロセスに従う必要があります。

- コントローラの認定許可設定は、すべてのコントローラデバイスの認証生成プロセスを設定します。詳細については、「Cisco SD-WAN Controller Certificates」[英語] を参照してください。
- 証明書の更新にはコントロールプレーンのフラップ全体が含まれるため、シスコのプロビジョニング済みのクラウドホスト型コントローラの場合でも、上記の手順に従う必要があります。
- Cisco CloudOps チームは、お客様の証明書を自動的に更新しません。
- [Cisco vManage Settings] ページには、[Symantec Automated] または [Cisco Automated] のオプションがあります。このオプションの「自動」とは、CSR の自動送信と証明書の自動取得を指します。このオプションには、手動オプションと比較すると、プロセスの特定のステップの自動化が含まれます。ただし、各コントローラの CSR の生成をトリガーするステップは手動のままで、更新プロセスはお客様自身で開始します。
- Cisco vManage ダッシュボードには、証明書の有効期限が近づいているという警告が 6 ヵ月前に表示されます。
- 有効期限は、**[Cisco vManage]** > **[Configuration]** > **[Certificates]** > **[Controllers]** で、いつでも確認できます。
- Cisco CloudOps チームは、有効期限の 30 日、15 日、5 日前に、システム内オーバーレイの登録済み電子メールアドレスの連絡先に電子メール通知を送信します。
- お客様は、現在の登録済み電子メールアドレスのリクエストや変更のために、いつでもケースをオープンできます。すべての Cisco CloudOps 通知について、所有者の電子メールアドレスを常に最新の状態に保つことをお勧めします。アラート通知用のお客様の連絡先電子メールアドレスを更新することを強くお勧めします。できれば、個人のユーザーではなく、チームのメールアドレスを使用してください。
- また、コントローラ証明書の有効期限に注意し、失効日の少なくとも 1 ヵ月前に更新を計画することをお勧めします。



第 4 章

プロビジョニング

クラウドホスト型コントローラへのアクセスの取得

シスコ マネージド クラウドホスト型コントローラは、デフォルトで管理アクセス用にクローズされています。シスコでは、セキュリティ上の理由から、クラウドホスト型 SD-WAN コントローラ向けの 0.0.0.0/0 へのアクセスを許可していません。お客様のエンタープライズ VPN 内にアクセス用の特定のパブリック IP プレフィックスがあると考えられるため、そのパブリック IP プレフィックスのみがアクセス用にオープンされます。特定の送信元 IP プレフィックスについては、https と ssh のみを許可リストに含めるようにリクエストして、アクセスを制限できます。シスコは、すべての宛先ポートおよびプロトコルへのアクセスを許可するように、お客様が指定したすべての送信元 IP プレフィックスをデフォルトでマークします。

クラウドホスト型コントローラのインターフェイスにはプライベート IP があります。各プライベート IP には、クラウド上のパブリック IP への 1 対 1 NAT があります。これらの IP は、インターフェイスが静的 IP または DHCP のどちらで設定されているかどうかにかかわらず、変更されません。インスタンスが復旧または交換された場合にのみ IP が変更されます。

許可リストは、パブリック IP アドレスを持つすべてのコントローラのすべてのネットワークインターフェイスに適用されます。クラウドホスト型コントローラセットに適用される許可リストを更新または表示するには、Cisco TAC でケースをオープンします。

クラウド セキュリティ グループの許可リストを追加、削除、または変更するには、次のいずれかのオプションを使用します。

- https://ssp.sdwan.cisco.com でシスコ セルフサービス ポータルにログインし、アクセスリストを管理します。オーバーレイ コントローラ プロファイルを基本とするスマートアカウントの Cisco PNP スマートアカウント管理者である必要があります。
- Cisco TAC サポートケースをオープンして、次の情報を入力します。
  - オーバーレイ/VA 名

- Cisco vManage IP/FQDN
- 許可リストで追加、削除、または変更する必要があるプレフィックス/ルール（vManage GUI アクセス）
- IP アドレス
- すべてのトラフィックまたは選択したトラフィック（https、SSH など）で IP アドレスを許可するかどうかの指定

Cisco SD-WAN セルフサービスポータルについて、シスコではスマートアカウント管理者に Cisco SD-WAN セルフサービスポータルにアクセスする権限を付与しています。スマートアカウント管理者は、コントローラの IP アドレスの表示やコントローラの IP アクセスリストの変更など、顧客のホスト型コントローラインフラストラクチャに関連する運用タスクを表示および実行できます。このアクセスを特定のユーザに付与しない場合は、Cisco Software Central の [Manage Smart Account] セクションに移動し、それらのユーザをスマートアカウント管理者から削除するか、IDP（ID プロバイダー）オンボーディング機能を使用して、Cisco SD-WAN セルフサービスポータルへのアクセスを IDP の信頼できるユーザに基づいて付与してください。

クラウドホスト型コントローラ IP のプロビジョニング

Cisco vManage完全修飾ドメイン名（FQDN）は VPN 512 パブリック IP にマップされ、管理アクセスに使用されます。ただし、エッジノードは、VPN 0 上にあり、異なるパブリック IP アドレスを持つ Cisco vManage のトランスポート インターフェイスでトンネルを形成します。シスコは、クラウドホスティングのために Cisco vManage と Cisco vBond オーケストレーションに FQDN を割り当てています。

Cisco vBond オーケストレーション では HTTP アクセスは使用できず、Cisco vManage のみが Web サーバーと Web/https へのアクセスを使用できます。

各コントローラインスタンスには、パブリック IP 1:1 に NAT 処理されるプライベート IP インターフェイスがあります。一般に、インスタンス インターフェイスのパブリック IP およびプライベート IP アドレスは変更されません。Cisco vBond オーケストレーション/Cisco vSmart コントローラ/Cisco vManage のプライベート/パブリック IP は、インスタンスを置き換えるか、新しいリージョンに移動する必要がある場合にのみ変更されます。

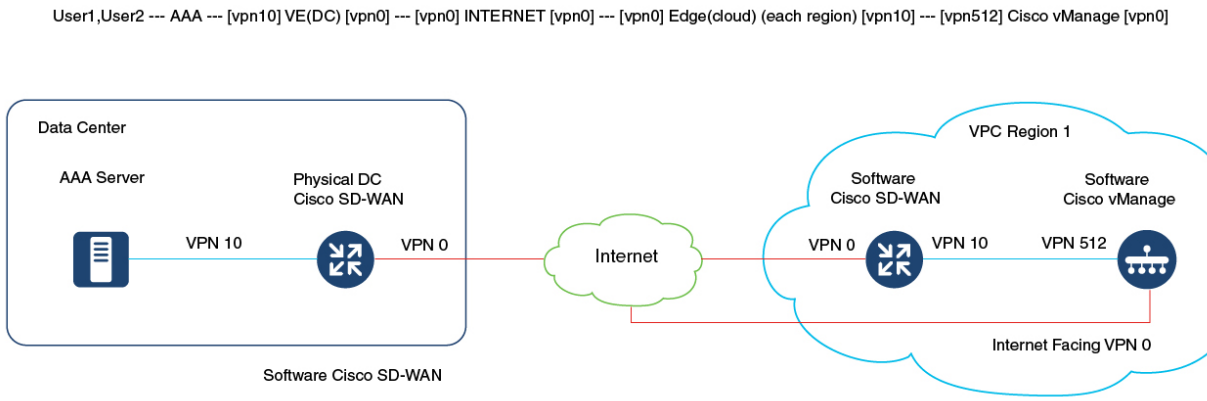
すべてのエッジはDTLS/TLS ポートを介してコントローラと通信するため、これらのDTLS/TLS ポートの任意の IP、またはクラウドコントローラの現在のパブリック IP に対してファイアウォールを開くことができます。DTLS/TLS ポートの詳細については、「複数の vCPU を実行する Cisco SD-WAN デバイスで使用されるポート」セクションの表 3 を参照してください。

クラウドホスト型コントローラのカスタムIPプレフィックス

一部のユースケースでは、管理アクセスと制御のため、クラウド コントローラ インターフェイスでカスタム ネットワーク プレフィックスに基づく IP が必要になる場合があります。次に例を示します。

- AAA または TACACS ベースの認証を使用した Cisco SD-WAN トンネル経由の Cisco vManage、Cisco vBond オーケストレーション、または Cisco vSmart コントローラ のデバイスの管理 VPN 512 にアクセスする。
- VPN 512 を介して Cisco vManage から Cisco SD-WAN トンネル経由で syslog サーバーに syslog を送信する。

図 *7 : AAA TACAS*



デフォルトでは、シスコ マネージド クラウドホスト型コントローラは、VPN 512 サブネットを含む 10.0.0.0/16 ベースのサブネットで展開されます。クラウド Cisco SD-WAN を追加し、VPN 512 サブネットをファブリック内の到達可能なサブネットとして使用すると、既存のサブネットと競合する可能性があります。

このような場合は、コントローラの展開の 2 つのリージョンごとに /24 プレフィックスを共有する必要があります。これらの IP プレフィックスはコントローラの作成に使用され、サブネットは Cisco SD-WAN ファブリック内で使用できるように設定されます。

オーバーレイ プロビジョニング後の AAA/TACAC を目的としたクラウド vEdge へのリクエスト

TAC-CSOne で CloudOps のケースをオープンして、次の詳細を確認および実行します。

1. AAA または TACAC の有効化をリクエストするには、既存のファブリック内で使用されていない IP プレフィックスを指定する必要があり、そのプレフィックスを使用してコントローラを作成できます（元のコントローラはシャットダウンされてスナップショットが作成され、複製されます）。

コントローラが設定されている各リージョンは、1 つの /24 ファブリックに関する一意のカスタムサブネットを持ちます。各オーバーレイには 2 つのリージョンがあるため、2 つのサブネットが必要となります。

2. Cisco vBond オーケストレーション、Cisco vSmart コントローラ、および Cisco vManage デバイスへの管理者クレデンシャルがあります。
3. CloudOps エンジニアによる事前承認と事前チェックの完了後、8 時間のメンテナンス期間をスケジュールできます。
4. プロセスを開始する前に、Cisco vBond オーケストレーション の DNS を有効にし、すべてのコントローラを設定します。
5. Cisco SD-WAN または Cisco vSmart コントローラ デバイスで、GR がデフォルトで 12 時間以上に設定されていることを確認します。
6. 2 つの使用可能なクラウド Cisco SD-WAN UUID を PNP 経由で予約し、Cisco vManage に接続します。
7. プロビジョニングされたコントローラ用にはシングルテナントかつシングルノードの Cisco vManage オーバーレイ、およびシングルテナントかつクラスタノードの Cisco vManage オーバーレイでのみサポートされ、プロビジョニング予定のコントローラセットに対してはすべて新規となります。この機能は、Cisco Multi-tenant vManage クラスタオーバーレイではサポートされません。
8. Cisco vBond オーケストレーション、Cisco vSmart コントローラ、およびもしあればシスコ提供のクラウド Cisco SD-WAN デバイスに、Cisco vManage のテンプレートを接続することをお勧めします。

シスコプロビジョニング後のクラウド vEdge の構成

1. Cisco CloudOps がクラウドホスト型コントローラの横にあるクラウド vEdge のプロビジョニングを完了すると、CloudOps は各クラウド vEdge の顧客へのパブリックおよびプライベート IP 割り当てを共有します。フォーマットは（VPN 512, VPN 0, VPN X）です。

   Cisco CloudOps は、新しくプロビジョニングされたクラウド vEdge のログイン情報を共有します。
2. クラウド vEdge の VPN 512 および VPN X インターフェイスは、そのリージョンのコントローラの VPN 512 と同じサブネットにあります。

   Cisco CloudOps によってプロビジョニングされるクラウド vEdge は、特に AAA/TACACS を目的とし、常に上記のネットワーク レイアウト フォーマットで作成されます。

   クラウド vEdge への到達可能性に問題がある場合は、一般に、クラウド vEdge のインターフェイス IP またはルート構成に問題があります。
3. また、パブリック IP とプライベート IP は 1:1 NAT されており、クラウド vEdge インターフェイスに割り当てられています。vEdge インターフェイス自体は dhcp で設定できますが、常に同じ IP をクラウドから取得します。

VPN X インターフェイスの場合は、Cisco CloudOps で共有されているものとまったく同じ静的 IP を設定する必要があります。

サブネット内のランダム IP は使用できません。

4. クラウド vEdge は、オーバーレイごとに同じ固有の環境でプロビジョニングされるため、コントローラと同じインバウンド許可アクセスリストの対象となります。

   パブリック IP と提供されたログイン情報で、SSH 経由で vEdge にログインする必要があります。

5. 次に、必要な構成を使用して新しいクラウド vEdge を設定する必要があります。たとえば、サイト ID、システム IP、組織名、vBond DNS または IP などです。

6. エンタープライズルート CA を使用している場合は、クラウド vEdge にも同様にアップロードしてインストールする必要があります。

7. viptelatac/ciscotacro/ciscotacrw ユーザーが有効になっているローカルで auth-fallback を使用して Cisco vManage 上の AAA/TACACS をローカルに設定できます。これにより、シスコサポートは必要に応じてログインし、問題のトラブルシュートを行うことができます。

8. プロビジョニングされたクラウド vEdge ごとに 1 つずつ、Cisco vManage のデバイスリストから未使用のクラウド vEdge UUID を取得する必要があります。

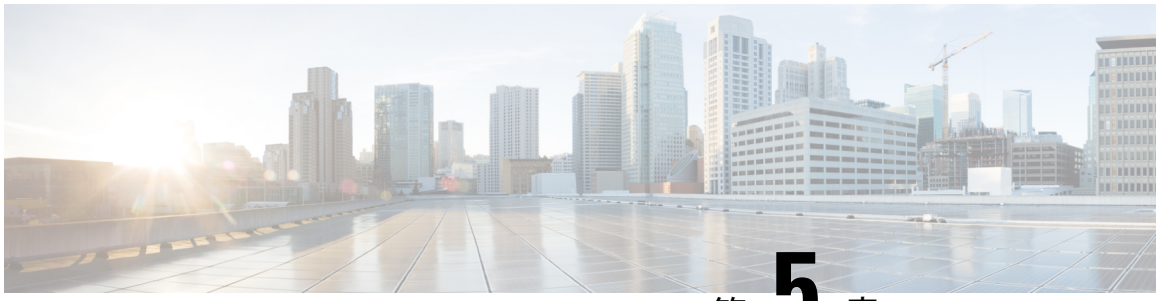
   使用している Cisco vManage の WAN エッジデバイスリストで使用可能なクラウド vEdge UUID がない場合は、Cisco PNP ポータルにログインし、オーバーレイに関連付けられているスマートアカウントとバーチャルアカウントにログインし、ソフトウェアデバイス（VEDGE-CLOUD- DNA）を追加してから、Cisco vManage 上でスマートアカウントを同期する必要があります。

9. 次に、クラウド vEdge で UUID をアクティブにして、Cisco vManage によって認証され、Cisco SD-WAN ファブリックに参加できるようにする必要があります。

10. クラウド vEdge の VPN X 静的 IP を指すように、（管理用のコントローラにアクセスするための顧客管理チームからの）顧客のエンタープライズサブネット用の特定の静的ルートを使用して、コントローラ（Cisco vManage、Cisco vBond オーケストレーション、Cisco vSmart コントローラ）の vpn 512 を設定する必要があります。

11. Azure でシスコがホストするオーバーレイの場合は、Cisco TAC ケースを開き、特定のエンタープライズサブネットプレフィックスを指定してください。ここから、コントローラの vpn 512 への接続が必須となります。

    Azure サブネットのデフォルトゲートウェイは、vEdge サービスの VPN IP をエンタープライズサブネットのゲートウェイとして構成した場合でも、事実上のゲートウェイです。したがって、コントローラの vpn 512 での構成に加えて、Azure 側で追加の構成が必要になります。シスコは、必要なエンタープライズサブネットごとに Azure ルート テーブル（RT）エントリを適用し、クラウド vEdge インターフェイスで IP 転送を有効にします。



第 5 章

モニタリング

Cisco SD-WAN クラウドホスト型コントローラのモニタリング

クラウドホスト型コントローラのモニタリングは、次の項目を対象としています。

- 以下についてのインフラストラクチャのモニタリング
  - CPU とデータディスクの使用率
  - ネットワーク インターフェイスへの接続の損失
  - インスタンスへの到達の失敗
- 以下についてのサービスのモニタリング
  - コントローラの SSL 証明書の有効期限
  - Cisco vManage Web サーバーの可用性
  - コントローラへの接続制御の損失

Cisco vManage 20.3.x より前のバージョンを使用したオーバーレイのヘルスモニタリング

クラウドモニタリングは、Cisco SD-WAN クラウド ホスティング サービスの一部として実行され、Cisco SD-WAN コントローラの可用性を確保します。デフォルトでは、Cisco vManage は `operator` 権限を持つ `viptelatac` というユーザーで設定されます。シスコは、このユーザーを使用して Cisco vManage にログインし、Cisco SD-WAN のヘルス状態を収集およびモニタリングします。

Cisco vManage の監査ログには、viptelatac ユーザーを使用したモニタリングシステムからの定期的なログインが表示されます。モニタリングサービスは、RestAPI を使用して Cisco vManage からヘルス情報を収集します。

シスコのクラウド モニタリング システムを無効にする場合は、Cisco SD-WAN クラウド インフラ チームで Cisco TAC ケースをオープンして、クラウドモニタリングを無効にするようにリクエストできます。モニタリングを無効にしたら、設定済みの viptelatac ユーザーを Cisco vManage から削除することも可能です。

また、Cisco Cloud Infra チームは、viptelatac ユーザーを使用して Cisco vManage にログインし、追加のヘルスチェックを実行し、内部で生成されたアラートに対応して問題をトリアージし、お客様がオープンした TAC ケースを支援します。

バージョン 20.3.x 以降を実行する Cisco vManage を使用したオーバーレイのヘルスモニタリング

Cisco SD-WAN リリース 20.3.1 以降では、プッシュベースのモデルが使用されます。

このモデルでは、モニタリングアーキテクチャは Cisco vManage を使用してシステムで認証を行い、ヘルスデータを送信します。 viptelatac ユーザーで Cisco vManage にログインすることで、Cisco vManage は、システムをモニタリングする代わりにデータをプッシュします。これを機能させるには、Cisco vManage の設定ページで明示的に同意し、ワンタイムパスワード（OTP）を設定する必要があります。Cisco vManage を 20.3.1 以降にアップグレードすると、viptelatac ユーザーは不要になります。

Cisco vManage にログインし、次の手順を実行できます。

1. **[Settings]** > **[Cloud Services]** > **[Enable]** の順に移動します。
2. OTP 値を入力します。Cisco TAC サポートケースをオープンすることで、Cisco CloudOps チームにトークンをリクエストできます。
3. [Cloud Gateway] URL は空白のままにしておきます。
4. [vMonitoring] をオンにしてモニタリングを有効にします。
5. オーバーレイのヘルスステータスに関するデータを Cisco vManage から収集する権限を承認します。

バージョン 20.3.x 以降では、シスコ クラウド インフラストラクチャ チームは ciscotacro および ciscotacrw ユーザーを使用して Cisco vManage に ログインし、追加のヘルス チェックを実行して、内部で生成されたアラートに対応して問題をトリアージし、お客様がオープンした TAC ケースを支援します。同じユーザーを使用して、インフラストラクチャの自動アップグレード、およびオーバーレイについてお客様の連絡先に事前通知された変更に基づいた特定のソフトウェア アップデートを実行します。

ciscotacro ユーザーには読み取り専用の *operator* グループ権限があり、一方 ciscotacrw には読み取り/書き込みの *netadmin* グループ権限があります。特定の拡張デバッグ、クラウド イン

フラストラクチャのアップグレードおよび管理のために、シスコ クラウド インフラストラクチャ チームは ciscotacrw ユーザーを使用する必要があります。

特定のシスコ サポートチームだけがこれらのユーザーを介してログインできます。これらのユーザーはトークンチャレンジおよびトークン応答ベースのパスワードメカニズムに基づいています。つまり、この 2 つのユーザーは静的パスワードには基づいていません。

いずれかの SD-WAN ファブリックコントローラでこのアクセスを無効にする必要がある場合は、いつでも設定からユーザーを削除できます。ただし、これにより、シスコが問題をトリアージする能力が制限されます。

CloudOps によるアラート通知

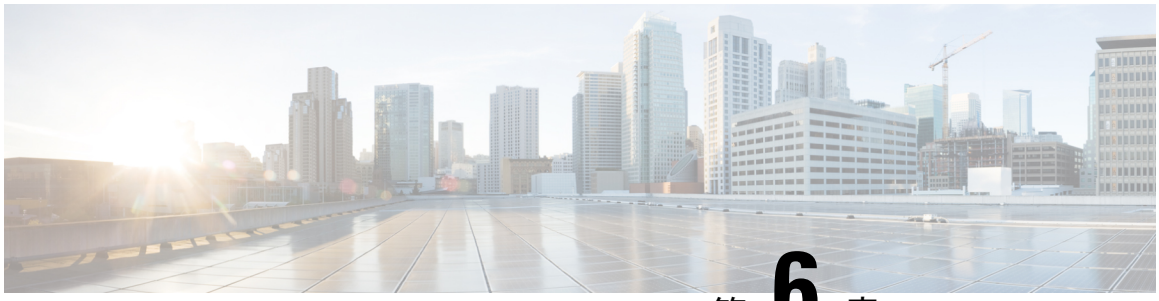
CloudOps チームは、クラウドホスト型インスタンスのインフラストラクチャを管理し、モニタリングとバックエンドインフラストラクチャのメンテナンスを支援します。ただし、CloudOps チームは、インスタンスの実行中のソフトウェアバージョンや設定を変更したり、管理したりすることはありません。

CloudOps チームは、発生した問題に基づいてアラート通知をお客様に送信する場合があります。アラート通知は、ソフトウェアの問題や誤設定、または CloudOps チームが認識していない一部の機能を示しています。チームが認識していない独自のテスト、変更、または設定の更新などが、お客様によって実行されている場合があります。

そのため、CloudOps チームはホストされたコントローラインスタンスで直接アクションを実行せず、お客様には通知するだけです。その後、必要に応じて支援と評価を行うため、Cisco TAC サポートケースをオープンするようお客様にリクエストします。お客様が TAC のケースをオープンすると、Cisco TAC と CloudOps チームは、必要に応じてお客様と協力して問題を解決できます。

アラート通知を受信するためのオーバーレイ連絡先の更新

- シスコがプロビジョニングしたすべてのクラウドホスト型オーバーレイには、CloudOps アラート通知を受信するために、所有者として登録された 1 つの顧客連絡先電子メールアドレスがあります。
- デフォルトでは、シスコ SO のエンドカスタマーの詳細に記載されている連絡先の電子メール アドレスが、所有者の連絡先として使用されています。
- お客様は、Cisco TAC ケースを開いて、いつでも連絡先を確認または更新することができます。
- Cisco SD-WANセルフサービスポータル（https://ssp.sdwan.cisco.com）が利用できるようになったため、顧客は所有者の連絡先メールアドレスを直接更新できます。
- 所有者の連絡先としてサポートされるメールアドレスの連絡先は 1 つだけであるため、グループメーリングリストのメールアドレスを提供することを推奨します。



第 6 章

クラウド インフラストラクチャ

シスコのクラウドホスト型コントローラのスナップショット

シスコは、スナップショットの頻度に基づいて、シスコが管理するクラウドホスト型 Cisco vManage コントローラの定期的なスナップショットを作成します。スナップショットの頻度はデフォルトで毎日 1 回（通常は展開された地域の午前 0 時）に設定され、最後の 10 個のスナップショットが保持されます。スナップショットの頻度は、1 日に 1 回から 4 日に 1 回まで設定できます。お客様は Cisco CloudOpsチームとともに Cisco TAC サポートケースをオープンし、現在のスナップショット設定を確認したり、Cisco SD-WAN セルフサービスポータル（SSP）で変更したりできます。保持できるのは、最大で最後の 10 個の定期スナップショットのみです。Cisco vSmart コントローラ と Cisco vBond オーケストレーション はステートレスであるため、スナップショットは取得されません。これらの設定は、ディザスタリカバリ目的で Cisco vManage のテンプレートを使用して行うことが推奨されます。

スナップショットは Cisco Cloud アカウント内に保存されるため、スナップショットをダウンロードすることはできません。ただし、Cisco vManage から config-db バックアップファイルをダウンロードし、request nms configuration-db backup path コマンドを使用して、テンプレートを含む設定を保存できます。

（注） Cisco vBond オーケストレーション および Cisco vSmart コントローラ はステートレスであるため、スナップショットはキャプチャされません。Cisco vManage テンプレートを使用して Cisco vBond オーケストレーション および Cisco vSmart コントローラ の設定を保存します。

オンデマンド スナップショットのリクエスト

Cisco vManage 用に計画されている主要な変更時間帯については、Cisco vManage のオンデマンドスナップショットをリクエストできます。オンデマンドスナップショットは、Cisco CloudOps チームとともに Cisco TAC サポートケースをオープンしてリクエストできます。オンデマンドスナップショットを取得して完了するには、変更時間帯の 8 時間前までに設定変更を凍結して割り当てる必要があります。オンデマンドのスナップショットは 1 つまで保存できます。このオンデマンドスナップショットは、スナップショットの作成日から 3 か月間保存されます。また、新しいオンデマンドスナップショットが作成されるたびに、前のスナップショットがあれば、それが自動的に削除され、新しいスナップショットに置き換えられます。

vAnalytics

Cisco vAnalytics を参照してください。

ペンテスト

AWS でオーバーレイコントローラを使用しているお客様は、以下を使用して、承認なしで Cisco SD-WAN ソリューションの独自のペンテストを実施できます。

- https://aws.amazon.com/security/penetration-testing/

Azure でオーバーレイコントローラを使用しているお客様は、以下を使用して、承認なしで Cisco SD-WAN ソリューションの独自のペンテストを実施できます。

- https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement

クラウドホスト型コントローラの必須メンテナンス

Cisco CloudOps チームは、AWS でホストされている場合にのみ、シスコが管理する特定のクラウドホスト型コントローラのリブートが必須であることを通知する電子メール通知をお客様に送信します。クラウドプロバイダーのメンテナンス時間帯の前に、インスタンスのメンテナンスが必要になり、インスタンスをリブートする場合があります。サービスの中断を回避するために、メンテナンスが必要な現在のハードウェアノードから新しい正常なハードウェアノードに移動できます。

Cisco CloudOps チームは、お客様の登録済み電子メールアドレスに通知を送信します。この電子メールアドレスは、Cisco CloudOps システム内のオーバーレイ用に登録された単一の電子メールアドレスです。この登録済み電子メールアドレスは、**最初に元の** SO の [End Customer Email Address] フィールドを使用して設定され、Cisco SD-WAN セルフサービスポータル（https://ssp.sdwan.cisco.com）にログインしていつでも更新できます。この登録済み電子メールアドレスは、Cisco vManage の設定ページから取得されたものではありません。

リクエストされた日時がクラウドプロバイダーのメンテナンス時間帯より前であれば、変更時間帯を更新するように再スケジュールできます。事前通知の量は保証されず、クラウドプロバイダー側のハードウェアノードの問題のシビラティ（重大度）によって異なります。

Cisco SD-WAN ディザスタ リカバリ ガイドライン

- Cisco SD-WANディザスタリカバリは、Cisco vManageディスクボリュームのスナップショットまたはコンフィギュレーション データベースのバックアップに基づいています。
- コンフィギュレーション データベースのバックアップとボリュームのスナップショットは、毎日（通常は Cisco vManage インスタンスが位置するタイムゾーンの午前零時頃）に取得され、クラウドに安全に保存されます。
- Cisco SD-WAN リリース 20.3.x 以降では、必要に応じてコンフィギュレーション データベースのバックアップ機能を無効にし、独自のバックアップを作成して、必要なときに CloudOps で使用してサービスを回復させることができます。
- Cisco vManage ディスクボリュームのスナップショットは毎晩、場合によっては顧客の要求に応じてオンデマンドで、または主要な変更時間帯の開始時に取得されます。Cisco vManage には 2 つ以上のディスクがあり、各ボリュームのスナップショットが完全に同時に取得され、Cisco vManage インスタンスの全体的なバックアップが形成されます。Cisco vManage が実行されているリージョンでスナップショットが完了すると、指定されたバックアップリージョン（通常は別の地理的リージョン）にコピーされます。

  たとえば、Cisco vManage が US-East で実行されていて、バックアップリージョンが US-West として指定されている可能性があります。バックアップリージョンは基本的に同じリージョンであり、2 番目の Cisco vBond オーケストレーション と Cisco vSmart コントローラがすでに実行されています。
- Cisco vBond オーケストレーション と Cisco vSmart コントローラ はステートレスサービスであり、CLI で管理された構成を持っているか、Cisco vManage が構成を提供しているため、バックアップされません。
- バックアップリージョンにはスタンバイサービスもアクティブ Cisco vManage サービスもありません。3 ノードまたは 6 ノードのクラスタは、同じ可用性ゾーンおよびリージョン内で実行される Cisco vManage の高可用性を提供します。
- Cisco vBond オーケストレーション および Cisco vSmart コントローラ サービスはプライマリリージョンとバックアップリージョンにデプロイされます。Cisco vBond オーケストレーション と Cisco vSmart コントローラ はどちらもアクティブモードで動作します。デバイスとポリシーの情報は、Cisco vManage から両方のインスタンスにプッシュされます。1 つのリージョンに障害が発生した場合、Cisco vSmart コントローラ と Cisco vBond オーケストレーション はバックアップリージョンで引き続き正常に機能します。
- Cisco SD-WAN は、すべてのコントローラに障害が発生した場合でも、データプレーンが機能し続けるように設計されています。GR（グレースフルリスタート）タイマー構成により、データプレーンの高可用性が可能になります。GR タイマーは、Cisco vSmart コントローラ によってアドバタイズされたルートをデフォルトで 12 時間保持するように設定

されています。障害が発生した場合にコントローラがバックアップできるようにすると同時に、変更されたネットワーク構成から新しいルートを学習できるように、Cisco SD-WANのお客様はGRタイマー値を慎重に選択することを推奨します。

- コンフィギュレーションデータベースベースのリカバリ方法を使用すると、テンプレートとポリシーのみを復元できます。ボリュームベースのリカバリは、収集された統計データを含めるためにも使用されます。

ボリューム スナップショット ベースのリカバリプロセス

- Cisco vManage インスタンスをバックアップで置き換える必要があると判断したら、ディザスタ リカバリ（DR）プロセスを開始できます。
- 同じリージョンでの DR の場合、シスコは既存の Cisco vManage インスタンスの場所と同じリージョンと同じデータセンターを選択します。

  また、要件と可用性に基づいて、使用するスナップショットセットの時刻/日付も指定します。
- DR がトリガーされると、システムは最初に既存の Cisco vManage インスタンスをシャットダウンします。
- 次に、システムはボリュームスナップショットを使用して、同じディスクセット、同じインスタンスサイズ仕様、同じプライベートサブネット、同じセキュリティアクセスリスト、元のCisco vManageと同じ分離環境を持つ新しいクラウドインスタンスを作成します。インスタンスが起動すると、システムはパブリックIPを古いシャットダウンCisco vManageインスタンスから新しい Cisco vManage インスタンスにスワップします。
- 全体として、新しい実行中の Cisco vManage インスタンスは同じパブリック IP を持ちますが、新しいプライベートIPはスナップショットが作成された時点と同じソフトウェアバージョン、同じ構成、同じデータを持ちます。
- Cisco vManage には、ファブリックに参加するために必要な情報があります。以前と同じ FQDN/URL を使用して Cisco vManage インスタンスにログインできます。
- バックアップリージョンへの DR については、Cisco vManage のプライマリリージョンに障害が発生して使用できないというまれなケースが考えられますが、バックアップ クラウド リージョンが選択されていることを除いて、まったく同じプロセスが使用されます。
- バックアップリージョンへの DR との違いは、新しい Cisco vManage インスタンスがバックアップリージョンで実行されると、古いリージョンから新しいリージョンへのパブリック IP のスワップがないことです。クラウドリージョンには、リージョンごとに特定のパブリックIPプールがあり、リージョン間でインスタンスに割り当てることはできません。

  そのため、バックアップリージョンの新しい DR Cisco vManage インスタンスには、新しいパブリック IP があります。システムは、Cisco vManage の新しいパブリック IP で FQDN/DNS を更新します。

  この場合、エンタープライズエンドファイアウォールをCisco vManageの新しいパブリック IP で更新する必要があります。

Cisco CloudInfra System によるコンフィギュレーション データベースのバックアップ

- Cisco vManage リリース 20.3.1 以前は、コンフィギュレーション データベースは次の場合にのみバックアップされました。
  - モニタリングは、Cisco CloudInfra システムで有効になっている。「viptelatac」ユーザーがなんらかの理由により Cisco vManage 上で使用できない場合、モニタリングは無効になり、お客様には修正要求が通知される。
  - 「viptelatac」ユーザーは、Cisco vManage で使用可能である。
  - コンフィギュレーション データベースのサイズは 4GB 未満。
- Cisco vManage リリース 20.3.1 以降、コンフィギュレーション データベースは次の場合にのみバックアップされます。
  - モニタリングは、Cisco CloudInfra システムで有効になっている。

（注） Cisco vManage では、クラウドサービスが何らかの理由で無効になっている場合、モニタリングは Cisco CloudInfra システムで無効になり、お客様には修正要求が通知されます。

  - Cisco vManage メニューから **[Adminstration]** > **[Settings]**を選択し、同じセクションに追加された OTP と共にクラウドサービスと vMonitoring を有効にします。
  - Cisco vManage CLI では、**`nms configuration-db daily-backup`** サービスが有効になっています。
  - コンフィギュレーション データベースのサイズは 4GB 未満。

コンフィギュレーション データベースのリカバリプロセス

- ボリュームスナップショットが何らかの理由で DR に使用できない場合、シスコはコンフィギュレーションデータベースのリカバリプロセスを使用します。新しい Cisco vManage インスタンスを作成し、コンフィギュレーションデータベースのバックアップを使用して元の構成ファイルを復元します。このリカバリ方法では、元の Cisco vManage インスタンスの統計データベースは復元されません。テンプレートとポリシーの構成が復元されます。この場合の新しい Cisco vManage インスタンスには、新しいパブリック IP と新しいプライベート IP の両方があります。
- Cisco vManage の FQDN/DNS を更新して、新しいインスタンスの新しいパブリック IP を使用します。
- この場合、エンタープライズエンドファイアウォールを Cisco vManage の新しいパブリック IP で更新する必要があります。

- コンフィギュレーション データベースのバックアップを使用したディザスタリカバリメソッドを使用するプロセスは、同じリージョンのリカバリとバックアップリージョンのリカバリの両方で同じです。
- プロセスの詳細については、トラブルシューティングのテクニカルノートを参照してください。

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。