Cisco Catalyst SD-WAN ハイ アベイラビリティ コンフィギュレーション ガイド、Cisco IOS XE Catalyst SD-WAN リリース 17.x

初版：2020 年 5 月 16 日

最終更新：2023 年 8 月 22 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 1 章 最初にお読みください 1

第 2 章 Cisco IOS XE（SD-WAN）の新機能 3

第 3 章 ハイ アベイラビリティ 5

Cisco Catalyst SD-WAN Validator の冗長性 10

Cisco Catalyst SD-WAN Manager サーバーの冗長性 12

Cisco Catalyst SD-WAN コントローラ の冗長性 15

Cisco IOS XE Catalyst SD-WAN デバイス の冗長性 17

Cisco Catalyst SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス 間のアフィニティの設定 18

Cisco Catalyst SD-WAN Controller でのコントローラグループ ID の設定 18

Cisco IOS XE Catalyst SD-WAN デバイス でのアフィニティの設定 19

Cisco Catalyst SD-WAN Controller グループの設定 19

制御接続の最大数の設定 20

単一データセンターにおける Cisco Catalyst SD-WAN Controller のアフィニティの設定 21

2 つのデータセンターにおける Cisco Catalyst SD-WAN Controller のアフィニティの設定 25

単一デバイスでの冗長性制御接続の設定 27

コントロールプレーンおよびデータプレーンの高可用性パラメータの設定 28

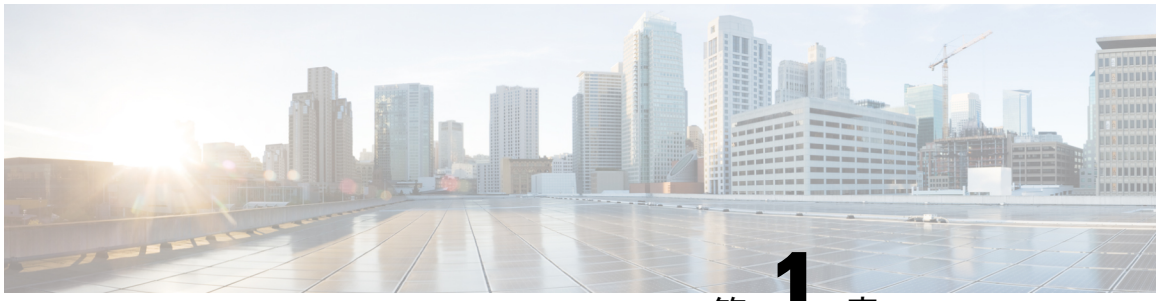
ハイ アベイラビリティの設定 29

アフィニティ設定のベストプラクティス 30

第 4 章 ディザスタリカバリ 33

ディザスタリカバリに関する情報 35

アーキテクチャの概要 35
前提条件 36
ベストプラクティスと推奨事項 37
ディザスタリカバリの有効化 38
ディザスタリカバリの登録 38
ディザスタリカバリ登録の確認 39
ディザスタリカバリの削除 40
管理者トリガーフェールオーバーの実行 40
ディザスタリカバリ操作 41
Cisco SD-WAN Manager または Cisco Catalyst SD-WAN Validator 管理者パスワードの変更 42
ディザスタ リカバリ コンポーネント用ディザスタ リカバリ ユーザー パスワードの変更 42
ディザスタリカバリアラートの設定 44



第 1 章

最初にお読みください

（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。

参考資料

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations [英語]
- Cisco Catalyst SD-WAN Device Compatibility [英語]

ユーザーマニュアル

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17 [英語]

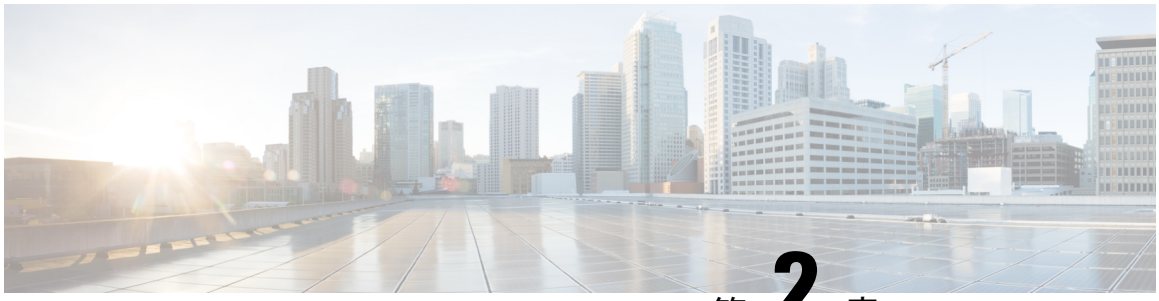
通信、サービス、およびその他の情報

- Cisco Profile Manager で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンストサービス、リモートサービスについては、シスコサービスにアクセスしてください。
- 安全かつ検証されたエンタープライズクラスのアプリ、製品、ソリューション、サービスをお求めの場合は、CiscoDevnet にアクセスしてください。

- Cisco Press 出版社による一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。
- リリースで未解決および解決済みのバグをご覧になる場合は、Cisco Bug Search Toolにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



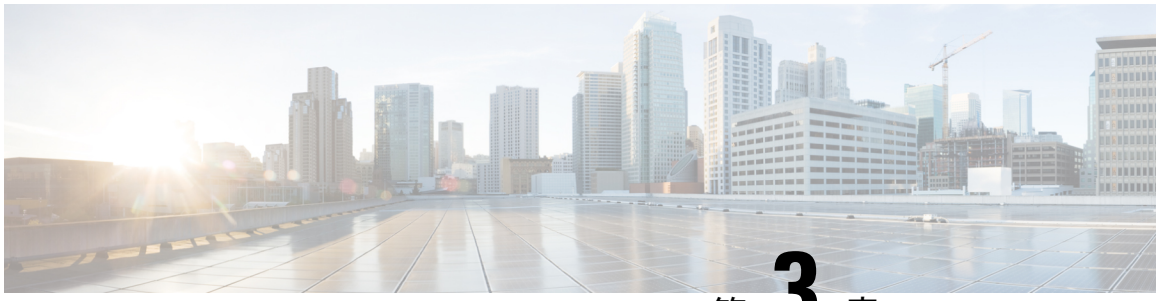
第 2 章

Cisco IOS XE（SD-WAN）の新機能

（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。

（注） シスコでは、リリースごとに Cisco Catalyst SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次の表に、コンフィギュレーション ガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されている新機能と変更された機能を示します。Cisco Catalyst SD-WAN ソリューションに関係する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x [英語]



第 3 章

ハイ アベイラビリティ

（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。

高可用性とは、すべてのネットワークサービスが障害に対して十分な復元力を備えていることを意味します。このようなソリューションは、機能、設計、およびベストプラクティスを使用してダウンタイムの潜在的な原因に対処することで、ネットワークリソースへの継続的なアクセスを提供することを目的としています。Cisco Catalyst SD-WAN 高可用性ソリューションのコアは、次の 3 つの要素を組み合わせて実現されます。

- 機能的ハードウェアデバイスの冗長性。基本戦略は、冗長ハードウェアデバイスをインストールしプロビジョニングすることと、ハードウェアで冗長コンポーネントをインストールしプロビジョニングすることからなります。これらのデバイスは、Datagram Transport Layer Security（DTLS）接続のセキュアなコントロール プレーン メッシュによって接続されます。これにより、デバイスに障害が発生したり、使用できなくなったりした場合に迅速なフェールオーバーが可能になります。Cisco Catalyst SD-WAN コントロールプレーンの主な機能は、 Cisco IOS XE Catalyst SD-WANデバイスとこのソフトウェア自体によって自動的に確立および維持されることです。
- 堅牢なネットワーク設計。
- ソフトウェアメカニズムにより、障害からの迅速な回復が確実に実行されます。復元力のあるコントロールプレーンを提供するために、Cisco Catalyst SD-WAN オーバーレイ管理プロトコル（OMP）では、ネットワーク内のすべての Cisco IOS XE Catalyst SD-WAN デバイスのステータスを定期的にモニターし、デバイスがネットワークに出入りする際に、ト

ポロジの変更に合わせて自動的に調整します。データプレーンの復元力を実現するために、Cisco Catalyst SD-WAN ソフトウェアは、ルータ間のセキュアな IPsec トンネル上で動作する標準的なプロトコルメカニズムである Bidirectional Forwarding Detection（BFD）を導入します。

障害からのリカバリは、障害を検出してから修復または回復するまでにかかる時間の関数です。Cisco Catalyst SD-WAN ソリューションは、ネットワークの障害を検出する時間を制御する機能を提供します。ほとんどの場合、障害の修復はごく短時間で完了します。

高可用性のハードウェアサポート

ネットワーク設定における標準的なベストプラクティスは、すべてのレベルで冗長ハードウェアをインストールすることです。これには、二重化された並列ルータやその他のシステム、冗長ファン、電源、およびこれらのデバイスに搭載される他のハードウェアコンポーネント、およびバックアップネットワーク接続が含まれます。Cisco Catalyst SD-WAN ソリューションでの高可用性の提供も例外ではありません。ハードウェア障害が発生した場合の復元力を備えたネットワーク設計には、冗長 Cisco SD-WAN Validator、Cisco SD-WAN コントローラ、ルータ、および使用可能な冗長ハードウェアコンポーネントを含める必要があります。

Cisco Catalyst SD-WAN オーバーレイネットワークのハードウェアコンポーネントが陥った全面的な障害からの回復は、他のネットワークと基本的に同じ方法で実行されます。バックアップコンポーネントは事前設定されており、必要なすべての機能を単独で実行できます。

堅牢なネットワーク設計

ハードウェアコンポーネントの単純な重複に加えて、障害に直面した場合に備えた堅牢なネットワークを設計するためのベストプラクティスに従うことで、Cisco Catalyst SD-WAN ネットワークの高可用性を強化できます。このようなネットワーク設計では、冗長コンポーネントが可能な限りネットワーク全体に分散されます。設計プラクティスには、冗長な Cisco SD-WAN Validator および Cisco SD-WAN コントローラ を地理的に分散させて配置し、それらを異なるトランスポートネットワークに接続することが含まれます。同様に、ローカルサイトのルータは、異なるトランスポートネットワークに接続でき、異なる NAT および DMZ を介してこれらのネットワークに到達できます。

高可用性のソフトウェアサポート

障害発生時の高可用性と復元力に関する Cisco Catalyst SD-WAN ソフトウェアサポートは、標準の DTLS プロトコルと独自の Cisco Catalyst SD-WAN オーバーレイ管理プロトコル（OMP）を使用するコントロールプレーンと、業界標準プロトコル BFD、BGP、OSPF、VRRP を使用するデータプレーンの両方で提供されます。

高可用性のコントロール プレーン ソフトウェア サポート

Cisco Catalyst SD-WAN コントロールプレーンは、冗長コンポーネントと連携して動作し、コンポーネントの 1 つに障害が発生した場合にオーバーレイネットワークの復元力が確実に維持されるようにします。コントロールプレーンは、シスコデバイス間の DTLS 接続を使用して構築され、Cisco Catalyst SD-WAN OMP プロトコルによってモニターされます。OMP プロトコルは、Cisco SD-WAN コントローラ とルータのペア間、および Cisco SD-WAN コントローラ の

ペア間でピアリングセッション（BGP ピアリングセッションと同様）を確立します。これらのピアリングセッションにより、OMP はシスコデバイスのステータスをモニターし、デバイス間で情報を共有できるため、ネットワーク内の各デバイスがオーバーレイネットワークの一貫したビューを取得できます。OMP ピアリングセッションでのコントロールプレーン情報の交換は、Cisco Catalyst SD-WAN 高可用性ソリューションの重要な要素です。

- Cisco SD-WAN コントローラ は、Cisco SD-WAN Validator またはルータがネットワークに参加したとき、またはネットワークから離れたときに、迅速かつ自動的に状況を確認します。その後、ルータに送信するルート情報に必要な変更を迅速に加えることができます。
- Cisco SD-WAN Validator は、デバイスがネットワークに参加したときと Cisco SD-WAN コントローラ コントローラがネットワークから離れたときに、迅速かつ自動的に状況を確認します。その後、ネットワークに参加しているルータに送信する Cisco SD-WAN コントローラ IP アドレスのリストに必要な変更をすばやく加えることができます。
- Cisco SD-WAN Validator は、ドメインに複数の Cisco SD-WAN コントローラ コントローラがある場合に状況を確認し、ネットワークに参加するルータに複数の Cisco SD-WAN コントローラ アドレスを提供できます。
- Cisco SD-WAN コントローラ は、他の Cisco SD-WAN コントローラ の存在を把握し、すべてがルートテーブルを自動的に同期します。1 つの Cisco SD-WAN コントローラ で障害が発生すると、残りのシステムがコントロールプレーンの管理をそのまま自動的に引き継ぐため、ネットワーク内のすべてのルータが、残りの Cisco SD-WAN コントローラ から最新の一貫したルーティングおよび TLOC の更新を受信し続けます。

次に、ネットワークの高可用性をサポートするために、各 Cisco Catalyst SD-WAN ハードウェアデバイスによって提供される冗長性について説明します。

コントロールプレーンでの障害からの回復

ハードウェアコンポーネントの冗長性と Cisco Catalyst SD-WAN コントロールプレーンのアーキテクチャの組み合わせにより、可用性の高いネットワークが実現します。このネットワークは、冗長コントロール プレーン コンポーネントの 1 つで障害が発生しても中断することなく正常に動作し続けます。Cisco SD-WAN コントローラ、Cisco SD-WAN Validator、またはオーバーレイネットワークに含まれる Cisco Catalyst SD-WAN ルータの全面的な障害からの回復は、ネットワーク上の通常のルータまたはサーバーで発生した障害からの回復と基本的に同じ方法で行われます。事前設定されたバックアップコンポーネントは、必要なすべての機能を単独で実行できます。

Cisco Catalyst SD-WAN ソリューションでは、ネットワークデバイスに障害が発生したときに、冗長デバイスが存在する場合、ネットワーク動作は中断することなく継続します。これは、すべてのシスコデバイス、Cisco SD-WAN Validator、Cisco SD-WAN コントローラ、およびルータに当てはまります。この動作を導入するためのユーザー設定は必要ありません。自動的に実行されます。シスコデバイス間で実行される OMP ピアリングセッションにより、すべてのデバイスにネットワークトポロジの最新かつ正確なビューが表示されることが保証されます。

これから障害回復についてデバイスごとに説明します。

高可用性のデータ プレーン ソフトウェア サポート

データプレーンの復元力を高めるため、Cisco Catalyst SD-WAN ソフトウェアには標準的な BFD プロトコルが導入されています。BFD プロトコルは、ルータ間のセキュアな IPsec 接続で自動的に動作します。これらの IPsec 接続は、データプレーンとデータトラフィックに使用され、コントロールプレーンで使用される DTLS トンネルから独立しています。BFDは、ルータ間の接続障害を検出するために使用されます。データトンネルで発生したデータの損失や遅延を測定して、接続の両端にあるデバイスのステータスを判断します。

BFD は、Cisco IOS XE Catalyst SD-WAN デバイス および Cisco vEdge デバイス 間のすべての接続でデフォルトで有効になっています。BFD は Hello パケットを定期的に（デフォルトでは 1 秒ごとに）送信して、セッションがまだ動作しているかどうかを判断します。特定の数の Hello パケットが受信されない場合、BFD はリンクに障害が発生したと見なし、BFD セッションを停止します（デフォルトのデッドタイムは3秒です）。BFDセッションがダウンすると、その IPSec トンネル上のネクストホップを指すルートは転送テーブル（FIB）から削除されますが、ルートテーブル（RIB）には引き続き存在します。

Cisco Catalyst SD-WAN ソフトウェアで、Hello パケットとデッドタイム間隔を調整できます。BFD リンクの両端でタイマーが異なる場合、BFD は低い方の値を使用するようにネゴシエートします。

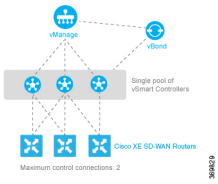
アフィニティを使用したネットワーク拡張の管理

Cisco Catalyst SD-WAN オーバーレイネットワークでは、すべての Cisco IOS XE Catalyst SD-WAN デバイス および Cisco vEdge デバイス がすべての Cisco SD-WAN コントローラ への制御接続を確立し、ルータがネットワーク全体でデータトラフィックを常時適切にルーティングできるようにします。ネットワークの規模が拡大して、ルータが数千のサイトに存在し、複数のデータセンターにある Cisco SD-WAN コントローラ がルータ間の制御フローとデータトラフィックを管理するようになると、ルータが接続できる Cisco SD-WAN コントローラ の数を制限することで、ネットワーク運用を改善できます。データセンターが広い地域に分散している場合も、ルータに、同じ地理的地域に配置された Cisco SD-WAN コントローラ のみと制御接続を確立させることで、ネットワーク運用をより適切に管理できます。

Cisco SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス の間にアフィニティを確立すると、 Cisco IOS XE Catalyst SD-WAN デバイス が制御接続を確立（および TLOC を形成）できる Cisco SD-WAN コントローラ の数を制限することで、オーバーレイネットワークの拡張を制御できます。単一のデータセンターに冗長ルータがある場合、アフィニティを使用すると、複数の Cisco SD-WAN コントローラ に vEdge 制御接続を分散できます。同様に、オーバーレイネットワークに複数のデータセンターがある場合、アフィニティを使用すると、全データセンターにvEdge制御接続を分散できます。アフィニティを使用すると、プライマリ制御接続とバックアップ制御接続を定義して、単一の Cisco SD-WAN コントローラ または単一のデータセンターへの接続に失敗した場合にオーバーレイネットワークの動作を維持することもできます。

アフィニティのシンプルな使用例の 1 つは、冗長な Cisco SD-WAN コントローラ が単一のデータセンターに配置されている場合です。これらの Cisco SD-WAN コントローラ は、オーバーレイネットワーク内のすべての Cisco IOS XE Catalyst SD-WAN デバイス にサービスを提供します。次の図は、前述の状況を図示したものです。データセンターに 3 つの Cisco SD-WAN コン

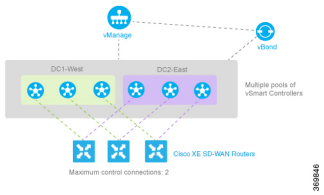
トローラが存在するシナリオを示しており、わかりやすくするために、ネットワークに含まれる多数の Cisco IOS XE Catalyst SD-WAN デバイス のうち 3 つだけを示しています。



アフィニティを有効にしない場合、各 Cisco IOS XE Catalyst SD-WAN デバイス は、データセンターに含まれる 3 つの Cisco SD-WAN コントローラ それぞれへの制御接続、つまり TLOC を確立します。結果として、合計 9 つの TLOC が確立されます。各ルータは各コントローラと OMP 更新についてやり取りします。これだけ多くの TLOC があると、Cisco SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス の両方のリソースに負担がかかる可能性があり、 Cisco IOS XE Catalyst SD-WAN デバイス の数が多いネットワークでは負担が大きくなります。

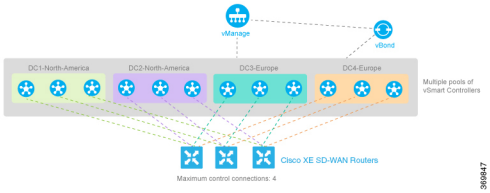
アフィニティを有効にすると、各 Cisco IOS XE Catalyst SD-WAN デバイス は Cisco SD-WAN コントローラ のサブセットのみとの TLOC 接続を確立できます。上の図では、各ルータが 3 つの Cisco SD-WAN コントローラ のうち 2 つに接続されているため、TLOC の総数が 9 から 6 に減少しています。両方の TLOC 接続をアクティブにできるため、合計 6 つの制御接続が可能になります。また、一方の TLOC 接続をプライマリ（優先）にし、もう一方をバックアップにして、プライマリが使用できない場合にのみ代替手段として使用することもできます。これにより、アクティブな TLOC の数を 3 つに減らすことができます。

アフィニティは、複数の Cisco SD-WAN コントローラ が 2 つ以上のデータセンターに配置されているシナリオで、データセンター間の冗長性も有効にします。その後、 Cisco IOS XE Catalyst SD-WAN デバイス といずれかのデータセンター間のリンクがダウンした場合、第 2 のデータセンターの Cisco SD-WAN コントローラ を使用してオーバーレイネットワークのサービスを継続できます。次の図はこのシナリオを図示したもので、2 つのデータセンターのそれぞれに属する 3 つの Cisco SD-WAN コントローラ を示しています。3 つの Cisco IOS XE Catalyst SD-WAN デバイス はそれぞれ、West データセンターの 1 つのコントローラと East データセンターの 1 つのコントローラへの TLOC 接続を確立します。



上の図のシナリオは、世界の同じ地域（同じ都市、県、国など）に冗長データセンターがある場合と考えることができます。大陸全体や複数の大陸間など、より大きな地域にまたがるオーバーレイネットワークの場合は、アフィニティを使用して、ローカルの Cisco SD-WAN コントローラ のみに接続するように Cisco IOS XE Catalyst SD-WAN デバイス を制限するか、 Cisco IOS XE Catalyst SD-WAN デバイス が同じ地理的地域にあるデータセンターと優先的に制御接続を確立するようにすることで、ネットワークスケールを制限できます。地理的アフィニティを使用すると、 Cisco IOS XE Catalyst SD-WAN デバイス は、よりローカルなデータセンターに

ある Cisco SD-WAN コントローラ と唯一の TLOC 接続またはプライマリ TLOC 接続を確立しますが、近い場所にあるデータセンターが使用できなくなった場合に備えた冗長性を実現するため、もっと離れた地域にバックアップを配置できます。次の図はこのシナリオを示しています。このシナリオでは、ヨーロッパにある Cisco IOS XE Catalyst SD-WAN デバイス に、ヨーロッパの 2 つのデータセンターへのプライマリ TLOC 接続と、北米のデータセンターへの代替接続があります。同様に、北米にある Cisco IOS XE Catalyst SD-WAN デバイス の場合、プライマリ接続は北米の 2 つのデータセンターに接続され、バックアップ接続はヨーロッパの 2 つのデータセンターに接続されます。



複数の Cisco SD-WAN コントローラ を含むオーバーレイネットワークの場合と同様に、すべての Cisco SD-WAN コントローラ のポリシー設定すべては同じである必要があります。

高可用性を設定する前に、設定トランザクションを開始するには、次のようなコマンドを使用できます。

```
ntp server 198.51.241.229 source GigabitEthernet1 version 4
```


- Cisco Catalyst SD-WAN Validator の冗長性 （10 ページ）
- Cisco Catalyst SD-WAN Manager サーバーの冗長性 （12 ページ）
- Cisco Catalyst SD-WAN コントローラ の冗長性 （15 ページ）
- Cisco IOS XE Catalyst SD-WAN デバイス の冗長性 （17 ページ）
- Cisco Catalyst SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス 間のアフィニティの設定 （18 ページ）

Cisco Catalyst SD-WAN Validator の冗長性

Cisco SD-WAN Validator は、Cisco Catalyst SD-WAN オーバーレイネットワークで次の 2 つの主要な機能を実行します。

- Cisco Catalyst SD-WAN ネットワークへの参加を試みるすべての Cisco SD-WAN コントローラ およびルータを認証し検証します。
- Cisco SD-WAN コントローラ とルータ間のコントロールプレーン接続を調整し、Cisco Catalyst SD-WAN ネットワーク内で Cisco SD-WAN コントローラ とルータが相互に接続できるようにします。

Cisco SD-WAN Validator は、ネットワークサーバーで VM として実行されます。

複数の Cisco SD-WAN Validator を設定すると、ルータや Cisco SD-WAN コントローラ などのシスコデバイスがネットワークに参加しようとするたびに、Cisco SD-WAN Validator のうちの 1 つが常に使用可能になります。

冗長 Cisco Catalyst SD-WAN Validator の設定

ルータは、その設定から Cisco SD-WAN Validator として機能していることを学習します。Cisco Catalyst SD-WAN オーバーレイネットワーク内の Cisco SD-WAN Validator（または Validator）の IP アドレスを定義する **system vbond** コンフィギュレーション コマンドに、**local** オプションを含めます。このコマンドには、Cisco SD-WAN Validator のローカルパブリック IP アドレスも含めます（Cisco IOS XE Catalyst SD-WAN デバイス および Cisco SD-WAN コントローラ では、Cisco SD-WAN Validator の IP アドレスを DNS 名として指定できますが、Cisco SD-WAN Validator 自体では IP アドレスとして指定する必要があります）。

Cisco SD-WAN コントローラ および Cisco IOS XE Catalyst SD-WAN デバイス では、ネットワークに Cisco SD-WAN Validator が 1 つしかない場合、Cisco SD-WAN Validator システムの場所を IP アドレスまたは DNS サーバーの名前（vbond.cisco.com など）として設定できます。（この場合も **system vbond** コマンドで設定します）。ネットワークに複数の Cisco SD-WAN Validator があり、それらすべてが到達可能である必要がある場合は、DNS サーバーの名前を使用します。DNS サーバーは、名前を単一の IP アドレスに解決し、そのアドレスを Cisco SD-WAN Validator が Cisco IOS XE Catalyst SD-WAN デバイス に返します。DNS 名が複数の IP アドレスに解決される場合、Cisco SD-WAN Validator はそれらをすべて Cisco IOS XE Catalyst SD-WAN デバイス に返し、ルータは接続が成功するまで各アドレスを順番に試行します。

Cisco Catalyst SD-WAN ネットワークに Cisco SD-WAN Validator が 1 つしかない場合でも、ベストプラクティスとして、**system vbond** コンフィギュレーション コマンドで IP アドレスではなく DNS 名を指定することを推奨します。これにより、スケーラブルな設定が実現するためです。その後、ネットワークに Cisco SD-WAN Validator を追加する場合、ネットワーク内のルータまたは Cisco SD-WAN コントローラ の設定を変更する必要はありません。

Cisco Catalyst SD-WAN Validator の障害からの復旧

複数の Cisco SD-WAN Validator があるネットワークでは、そのうちの 1 つに障害が発生しても、他の Cisco SD-WAN Validator は動作を継続し、シスコデバイスによるネットワークへの参加要求をすべて処理できます。コントロールプレーンの観点から、Cisco SD-WAN Validator はネットワーク内の各 Cisco SD-WAN コントローラ への定常的な DTLS 接続を維持します。（ただし、Cisco SD-WAN Validator 同士の間に接続がないことに注意してください）。Cisco SD-WAN コントローラ とルータは相互に検出し合ってネットワークに参加できるため、1 つの Cisco SD-WAN Validator がドメイン内に存在する限り、Cisco Catalyst SD-WAN ネットワークは中断することなく動作し続けることができます。

Cisco SD-WAN Validator はオーバーレイネットワークのデータプレーンに参加しないため、いずれかの Cisco SD-WAN Validator の障害がデータトラフィックに影響を与えることはありません。Cisco SD-WAN Validator は、ルータが最初にネットワークに参加するときにのみルータと通信します。参加するルータは、Cisco SD-WAN Validator との一時的な DTLS 接続を確立して、Cisco SD-WAN コントローラ の IP アドレスを学習します。 Cisco IOS XE Catalyst SD-WAN デバイス の設定に DNS 名として Cisco SD-WAN Validator のアドレスが一覧表示されている場合、ルータは、DTLS 接続を確立できるようになるまで、リスト内の Cisco SD-WAN Validator を 1 つずつ試行します。このメカニズムにより、Cisco SD-WAN Validator のグループのいずれかに障害が発生した後でも、ルータは常にネットワークに参加できます。

Cisco Catalyst SD-WAN Manager サーバーの冗長性

Cisco SD-WAN Manager サーバーは、オーバーレイネットワーク内のシスコデバイスの設定と管理を可能にする集中型ネットワーク管理システムを構成します。また、ネットワークとネットワークデバイスのステータスに関するリアルタイムダッシュボードも提供します。Cisco SD-WAN Manager サーバーは、ネットワーク内のすべての Cisco IOS XE Catalyst SD-WAN デバイス との定常的な通信チャネルを維持します。これらのチャネルを使用して、Cisco SD-WAN Manager サーバーは、すべての有効なデバイスのシリアル番号を一覧表示したファイルをプッシュし、各デバイスの設定をプッシュし、ソフトウェア アップグレード プロセスの一環として新しいソフトウェアイメージをプッシュします。各ネットワークデバイスから、Cisco SD-WAN Manager サーバーは、Cisco SD-WAN Manager の **[モニター（Monitor）]** > **[概要（Overview）]** ページに表示されるさまざまなステータス情報を受信します。

（注） Cisco vManage リリース 20.6.1 以前のリリースでは、ステータス情報は **[ダッシュボード（Dashboard）]** > **[メインダッシュボード（ Main Dashboard）]** ページで確認できます。

可用性の高い Cisco Catalyst SD-WAN ネットワークには、各ドメインに 3 つ以上の Cisco SD-WAN Manager サーバーが含まれています。このシナリオは Cisco SD-WAN Manager サーバーのクラスタと呼ばれ、クラスタ内の各 Cisco SD-WAN Manager サーバーは Cisco SD-WAN Manager インスタンスと呼ばれます。クラスタ内の各 Cisco SD-WAN Manager インスタンスは約 2000 のデバイスを管理できるため、3 つの Cisco SD-WAN Manager インスタンスのクラスタでは最大 6000 のデバイスを管理できます。Cisco SD-WAN Manager インスタンスは、管理するデバイスを自動的にロードバランシングします。インスタンスが 3 つある場合、Cisco SD-WAN Manager クラスタ内のいずれかのデバイスに障害が発生しても、クラスタは動作を維持します。

関連情報については、『Troubleshooting TechNotes』[英語] を参照してください。

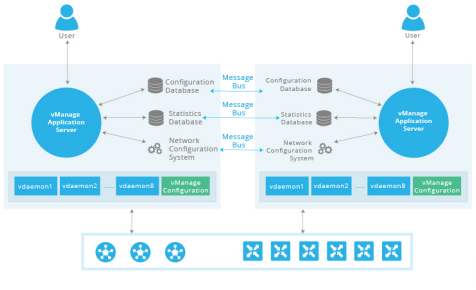
Cisco SD-WAN Manager クラスタは、次のアーキテクチャ コンポーネントで構成されています。

- アプリケーションサーバー：ユーザーセッション用の Web サーバーを提供します。ユーザーセッションを通じて、ログインユーザは、ネットワークイベントとステータスの高レベルのダッシュボードサマリーを表示し、ドリルダウンしてこれらのイベントの詳細を表示できます。ユーザーは、ネットワークシリアル番号ファイル、証明書、ソフトウェアアップグレード、デバイスのリブート、および Cisco SD-WAN Manager クラスタ自体の設定を Cisco SD-WAN Manager アプリケーションサーバーから管理することもできます。
- 設定データベース：すべての Cisco IOS XE Catalyst SD-WAN デバイス のインベントリと状態、および設定を保存します。
- ネットワーク設定システム：すべての設定情報、ポリシー、テンプレート、証明書などを保存します。
- 統計データベース：オーバーレイネットワーク内のすべてのシスコデバイスから収集された統計情報を保存します。

- メッセージバス：異なる Cisco SD-WAN Manager インスタンス間の通信バス。このバスは、クラスタ内の Cisco SD-WAN Manager インスタンス間でデータを共有し、動作を調整するために使用されます。

統計データベースおよび設定データベースサービスは、奇数の Cisco SD-WAN Manager インスタンス（3 つ以上）で実行する必要があります。これらのデータベースを書き込み可能にするには、実行中の Cisco SD-WAN Manager インスタンスのクォーラムが存在し、同期されている必要があります。クォーラムは単純多数です。たとえば、これらのデータベースを実行する 3 つの Cisco SD-WAN Manager インスタンスのクラスタがある場合、2 つのインスタンスが実行され、同期されている必要があります。最初は、すべての Cisco SD-WAN Manager インスタンスが同じサービスを実行します。とはいえ、一部のインスタンスで一部のサービスが実行されないように選択できます。[クラスタ管理（Cluster Management）] ウィンドウから、各 Cisco SD-WAN Manager インスタンスで実行できるサービスを選択できます。4 番目の Cisco SD-WAN Manager インスタンスを追加して、より多くの Cisco IOS XE Catalyst SD-WAN デバイス をロードバランシングできます。その場合、これらのサービスは奇数のインスタンスで実行する必要があるため、Cisco SD-WAN Manager インスタンスの 1 つで統計データベースと設定データベースを無効にします。必要に応じて、単一のインスタンスで設定データベースを実行して、デバイス間で共有される情報の量を減らし、負荷を軽減できます。

次の図は、クラスタ内の Cisco SD-WAN Manager インスタンス間の連携を示していますが、少なくとも 3 つのデバイスが必要です。次の図は、Cisco SD-WAN Manager インスタンス間で同期される Cisco SD-WAN Manager サービスを示しています。またこの図では、各 Cisco SD-WAN Manager インスタンスが仮想マシン（VM）に存在することが示されています。VM には 1 ～ 8 のコアがあり、各コアで Cisco Catalyst SD-WAN ソフトウェアプロセス（vdaemon）が実行されます。さらに、VM は Cisco SD-WAN Manager サーバー自体の実際の設定を保存します。



Cisco SD-WAN Manager クラスタは、次の方法でアクティブ-アクティブ アーキテクチャを導入します。

- クラスタ内の各 Cisco SD-WAN Manager インスタンスは、独立した処理ノードです。
- すべての Cisco SD-WAN Manager インスタンスが同時にアクティブになります。
- アプリケーションサーバーに対するすべてのユーザーセッションは、外部ロードバランサを使用してロードバランスされます。
- Cisco SD-WAN Manager アプリケーションサーバーとルータ間のすべての制御セッションがロードバランスされます。1 つの Cisco SD-WAN Manager インスタンスで最大約 2000 の Cisco IOS XE Catalyst SD-WAN デバイス を管理できます。ただし、すべてのコントローラ

セッション（Cisco SD-WAN Manager インスタンスと Cisco Catalyst SD-WAN コントローラ間のセッション、Cisco SD-WAN Manager インスタンスと Cisco Catalyst SD-WAN Validator 間のセッション）は、フルメッシュトポロジで調整されます。

- 設定データベースと統計データベースは、すべての Cisco SD-WAN Manager インスタンスで複製することが可能です。これらのデータベースは、すべての Cisco SD-WAN Manager インスタンスからアクセスして使用できます。
- クラスタ内のいずれかの Cisco SD-WAN Manager インスタンスに障害が発生した場合や、使用できなくなった場合でも、Cisco SD-WAN Manager サーバーによって提供されるネットワーク管理サービスは、ネットワーク全体で引き続きフルに使用できます。

クラスタ内の Cisco SD-WAN Manager インスタンス間のメッセージバスにより、すべてのインスタンスがアウトオブバンドネットワークを使用して通信できます。Cisco SD-WAN Manager VM 上の 3 番目の vNIC を利用するこの設計では、管理トラフィックに WAN 帯域幅を使用する必要がありません。

Cisco SD-WAN Manager Web アプリケーションサーバーから Cisco SD-WAN Manager クラスタを設定します。設定プロセス中に、次のサービスを実行できる各 Cisco SD-WAN Manager インスタンスを設定できます。

- アプリケーションサーバー：各 Cisco SD-WAN Manager サーバーはアプリケーション サーバー インスタンスを実行します。
- 設定データベース：Cisco SD-WAN Manager クラスタ内では、設定データベースの反復処理を 3 回まで実行できます。
- ロードバランサ：Cisco SD-WAN Manager クラスタには、クラスタ内の Cisco SD-WAN Manager インスタンス間でユーザーログインセッションを分散するためのロードバランサが必要です。前述のように、1 つの Cisco SD-WAN Manager インスタンスで最大約 2000 台の WAN エッジデバイスを管理できます。
- メッセージングサーバー：メッセージバスを実行するように各 Cisco SD-WAN Manager インスタンスを設定して、クラスタ内のすべてのインスタンスが相互に通信できるようにすることを推奨します。
- 統計データベース：Cisco SD-WAN Manager クラスタ内では、統計データベースの反復処理を 3 回まで実行できます。
- 調整サーバー：メッセージングサーバーによって内部的に使用されます。

Cisco SD-WAN Manager クラスタの設計上の考慮事項は次のとおりです。

- Cisco SD-WAN Manager クラスタは、少なくとも 3 つの Cisco SD-WAN Manager インスタンスで構成する必要があります。
- アプリケーションサーバーとメッセージバスをすべての Cisco SD-WAN Manager インスタンスで実行する必要があります。
- 1 つのクラスタ内で、設定データベースのインスタンスを 3 つまで、統計データベースのインスタンスを 3 つまで実行できます。ただし、個々の Cisco SD-WAN Manager インスタ

ンスでは、これら2種類のデータベースの両方を実行することも、いずれか一方を実行することも、いずれも実行しないことも選択できます。

- 最大限の可用性を実現するために、3つのCisco SD-WAN Managerインスタンスで設定データベースと統計データベースを実行することを推奨します。

クラスタの Cisco SD-WAN Manager インスタンスの展開と管理の詳細については、『*Cisco Getting Started Guide*』[英語] の「Cluster Management」の章を参照してください。

Cisco Catalyst SD-WAN Manager のバックアップ

シスコは、致命的な障害または破損からのリカバリのために、デバイスの定期的なスナップショットを取得することで Cisco SD-WAN Manager を管理します。これらのスナップショットの頻度と保持期間は、オーバーレイごとに設定されます。通常、スナップショットは毎日取得され、最大 10 日間保持されます。デバイスのアップグレードなど、特定の計画的なメンテナンスアクティビティでは、計画的アクティビティの前に別のスナップショットを取得できます。それ以外の場合は、お客様の責任において、Cisco SD-WAN Manager 設定データベースと Cisco SD-WAN Manager 仮想マシンのスナップショットを定期的にバックアップし、シスコが遵守している頻度と保持期間の例に従う必要があります。

Cisco Catalyst SD-WAN Manager データベースのバックアップ

Cisco SD-WAN Managerクラスタは高可用性と一定レベルの耐障害性を提供しますが、設定データベースの定期的なバックアップを取得し、オフサイトで安全に保存する必要があります。Cisco SD-WAN Manager には、設定データベースのバックアップの収集をスケジュールに従って自動化し、別のサーバーにコピーするメカニズムがありません。バックアップからリカバリが必要になるまでの時間が長いほど、データが失われるリスクが高くなります。設定データベースのバックアップを頻繁に実行してください。設定データベースのバックアップファイルを作成するには、次のコマンドを使用します。

```
request nms configuration-db backup path <path>
```

Cisco Catalyst SD-WAN コントローラ の冗長性

Cisco Catalyst SD-WAN コントローラ の冗長性

Cisco SD-WAN コントローラ は、コントロールプレーンの中心的なオーケストレータです。ネットワーク内のすべてのシスコデバイスとの定常的な通信チャネルがあります。Cisco SD-WAN コントローラ と Cisco SD-WAN Validator の間、および Cisco SD-WAN コントローラ のペア間の DTLS 接続を介して、デバイスは定期的にネットワークのビューを交換し、ルートテーブルの同期が維持されるようにします。Cisco SD-WAN コントローラ は、DTLS 接続を介して、正確でタイムリーなルート情報を Cisco IOS XE Catalyst SD-WAN デバイス に渡します。

可用性の高い Cisco Catalyst SD-WAN ネットワークには、各ドメインに 2 つ以上の Cisco SD-WAN コントローラ が含まれています。Cisco Catalyst SD-WAN ドメインには、最大 20 の Cisco SD-WAN コントローラ を含めることができ、デフォルトでは、それぞれのルータがそのうちの 2 つに接続します。ドメイン内の Cisco SD-WAN コントローラ の数が、ドメインのルータ

が接続を許可されているコントローラの最大数よりも多い場合、Cisco Catalyst SD-WAN ソフトウェアは、使用可能な Cisco SD-WAN コントローラ の間の接続をロードバランシングします。

すべての Cisco SD-WAN コントローラ の設定は機能的に類似している必要がありますが、制御ポリシーは同一である必要があります。これは、すべての Cisco IOS XE Catalyst SD-WAN デバイスがネットワークの一貫したビューをいつでも確実に受信できるようにするために必要です。制御ポリシーが完全に同一でない場合、複数の Cisco SD-WAN コントローラ によって異なる情報が Cisco IOS XE Catalyst SD-WAN デバイス に提供される場合があり、その結果、ネットワーク接続の問題が発生する可能性があります。

（注） 繰り返しますが、Cisco Catalyst SD-WAN オーバーレイネットワークは、すべての Cisco SD-WAN コントローラ の制御ポリシーが同一である場合にのみ正常に機能します。ポリシーのわずかな違いでも、ネットワークの機能に問題が発生します。

相互の同期を維持するために、Cisco SD-WAN コントローラ 同士が相互に DTLS 制御接続のフルメッシュと OMP セッションのフルメッシュを確立します。OMP セッションでは、Cisco SD-WAN コントローラ がルート、TLOC、ポリシー、サービス、および暗号キーをアドバタイズします。Cisco SD-WAN コントローラ が同期を維持できるのは、この情報交換によります。

Cisco SD-WAN コントローラ はネットワーク上の任意の場所に配置できます。可用性を確保するため、Cisco SD-WAN コントローラ を地理的に分散させることを強く推奨します。

各 Cisco SD-WAN コントローラ は、各 Cisco SD-WAN Validator への定常的な DTLS 接続を確立します。これらの接続により、Cisco SD-WAN Validator は、どの Cisco SD-WAN コントローラ が存在し動作しているかを追跡できます。そのため、Cisco SD-WAN コントローラ のいずれかに障害が発生した場合、Cisco SD-WAN Validator が、使用できない Cisco SD-WAN コントローラ のアドレスをネットワークに参加しようとしているルータに提供することはありません。

繰り返しますが、Cisco Catalyst SD-WAN オーバーレイネットワークは、すべての Cisco SD-WAN コントローラ の制御ポリシーが同一である場合にのみ正常に機能します。ポリシーのわずかな違いでも、ネットワークの機能に問題が発生します。

Cisco Catalyst SD-WAN Controller の障害からの復旧

Cisco SD-WAN コントローラ は、ネットワークのプライマリコントローラです。この制御を維持するため、すべての Cisco SD-WAN Validator と Cisco IOS XE Catalyst SD-WAN デバイス および Cisco vEdge デバイス への定常的な DTLS 接続を維持します。これらの接続により、Cisco SD-WAN コントローラ はネットワークトポロジの変更を常に認識できます。ネットワークに複数の Cisco SD-WAN コントローラ がある場合：

- 複数の Cisco SD-WAN コントローラ 間に OMP セッションのフルメッシュがあります。
- 各 Cisco SD-WAN Validator には、各 Cisco SD-WAN コントローラ に対する定常的な DTLS 接続があります。

- Cisco SD-WAN コントローラ には、Cisco IOS XE Catalyst SD-WAN デバイス および Cisco vEdge デバイス への定常的な DTLS 接続があります。具体的には、各ルータに Cisco SD-WAN コントローラ のいずれかへの DTLS 接続があります。

Cisco SD-WAN コントローラ の 1 つに障害が発生した場合、他の Cisco SD-WAN コントローラがネットワーク制御の処理をシームレスに引き継ぎます。残りの Cisco SD-WAN コントローラはネットワークに参加して Cisco IOS XE Catalyst SD-WAN デバイス および Cisco vEdge デバイス と連携することができ、ルータへのルート更新の送信を続行できます。Cisco SD-WAN コントローラ が存在し、ドメイン内で動作している限り、Cisco Catalyst SD-WAN ネットワークは中断することなく動作を継続できます。

タイマーを 6 時間に設定して、Cisco IOS XE Catalyst SD-WAN デバイス での OMP のグレースフルリスタートを設定するには、次を参照してください。

```
ISR4331(config)# sdwan omp graceful-restart timers graceful-restart-timer 21600
ISR4331(config-timers)# commit
Commit complete.
ISR4331(config-timers)# end
```

```
ISR4331#show sdwan running-config | section sdwan
tunnel mode sdwan
sdwan
interface GigabitEthernet0/0/1
  tunnel-interface
   encapsulation ipsec
   max-control-connections 1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
  exit
exit
omp
  no shutdown
  graceful-restart
  timers
   graceful-restart-timer 21600
  exit
  address-family ipv4
   advertise connected
   advertise static
  !
!
```

Cisco IOS XE Catalyst SD-WAN デバイス の冗長性

Cisco IOS XE Catalyst SD-WAN デバイス は、通常、Cisco Catalyst SD-WAN ネットワーク内でブランチサイトの Cisco Catalyst SD-WAN ルータとして使用する方法と、ブランチルータが接続するハブサイトを作成する方法の 2 つの方法で使用されます。

1 つのブランチサイトに、冗長性のため 2 つの Cisco IOS XE Catalyst SD-WAN デバイス を設定できます。各ルータは以下を維持します。

- DTLS 接続を介した、ドメイン内の各 Cisco SD-WAN コントローラ とのセキュアなコントロールプレーン接続。
- サイトの他のルータとのセキュアなデータプレーン接続。

両方のルータが Cisco SD-WAN コントローラ から同じルーティング情報を受信するため、それぞれが異なるトランスポートプロバイダーに接続されていても、1 つのルータに障害が発生した場合に、それぞれのルータでトラフィックのルーティングを続行できます。

Cisco IOS XE Catalyst SD-WAN デバイス および Cisco vEdge デバイス をハブサイトで使用する場合は、2 つの Cisco IOS XE Catalyst SD-WAN デバイス を設置することで冗長性を実現できます。ブランチルータは、各ハブルータに別個の DTLS 接続を使用して接続する必要があります。

単一のルータでトンネルインターフェイスまで設定することで、Cisco IOS XE Catalyst SD-WAN デバイスの冗長性を実現することもできます。各トンネルインターフェイスは、同じまたは異なるファイアウォール、サービスプロバイダー、およびネットワーククラウドを通過することが可能で、DTLS トンネルを使用して、ドメイン内の Cisco SD-WAN コントローラ とのセキュアなコントロールプレーン接続を維持します。

Cisco IOS XE Catalyst SD-WAN デバイス の障害からの復旧

Cisco IOS XE Catalyst SD-WAN デバイス および Cisco vEdge デバイス のルートテーブルは、Cisco SD-WAN コントローラ から受信した OMP ルートによって入力されます。冗長ルータを備えたサイトまたはブランチの場合、両方のルータのルートテーブルが同期されたままになるため、いずれかのルータに障害が発生しても、もう一方のルータが引き続きデータトラフィックを宛先にルーティングできます。

Cisco Catalyst SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス 間のアフィニティの設定

ネットワークの規模を管理する方法の 1 つは、Cisco SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス 間のアフィニティを設定することです。この設定を行うには、各 Cisco SD-WAN コントローラ をコントローラグループに配置し、Cisco IOS XE Catalyst SD-WAN デバイスが制御接続を確立できるグループを設定します。このコントローラグループが、Cisco SD-WAN コントローラ と Cisco IOS XE Catalyst SD-WAN デバイス 間のアフィニティを確立します。

Cisco Catalyst SD-WAN Controller でのコントローラグループ ID の設定

アフィニティに参加するには、各 Cisco SD-WAN コントローラ にコントローラグループ ID を割り当てる必要があります。

```
vSmart(config)#system controller-group-id number
```

ID 番号は 0 ～ 100 の範囲で指定できます。

複数の Cisco SD-WAN コントローラ が異なるデータセンターにある場合は、各 Cisco SD-WAN コントローラ に異なるコントローラグループ ID を割り当てることを推奨します。これにより、データセンターが到達不能になった場合に備えて、データセンター間の冗長性を実現できます。

同じデータセンターに属する Cisco SD-WAN コントローラ の場合、同じコントローラグループ ID または異なる ID を指定できます。

- 複数の Cisco SD-WAN コントローラ が同じコントローラグループ ID を持つ場合、 Cisco IOS XE Catalyst SD-WAN デバイス はそれらのいずれかへの制御接続を確立します。Cisco SD-WAN コントローラ が到達不能になった場合、ルータがデータセンター内の別のコントローラとの制御接続を確立するだけで対処できます。これがどのように機能するかの例を示します。ソフトウェアのアップグレード中に 1 つの Cisco SD-WAN コントローラ が使用できなくなった場合、 Cisco IOS XE Catalyst SD-WAN デバイス はすぐに別の Cisco SD-WAN コントローラ を使用して新しい TLOC を確立します。ルータのネットワーク動作は中断されません。このネットワーク設計は、データセンターの Cisco SD-WAN コントローラ の間における冗長性を実現します。

- Cisco SD-WAN コントローラ のコントローラグループ ID が異なる場合、 Cisco IOS XE Catalyst SD-WAN デバイス は一方のコントローラを優先して使用し、もう一方をバックアップとして使用できます。これがどのように機能するかの例を示します。Cisco SD-WAN コントローラ ソフトウェアをアップグレードする場合、一度に 1 つのコントローラグループをアップグレードできます。アップグレードで問題が発生した場合、 Cisco IOS XE Catalyst SD-WAN デバイス は 第 2 のバックアップ コントローラ グループに含まれる Cisco SD-WAN コントローラ との TLOC を確立します。ルータのネットワーク動作は中断されません。最初のグループの Cisco SD-WAN コントローラ が再び使用可能になると、 Cisco IOS XE Catalyst SD-WAN デバイス は TLOC をそのコントローラに戻します。このネットワーク設計は、データセンター内の Cisco SD-WAN コントローラ 間の冗長性を実現すると同時に、付加的な障害分離も可能にします。

Cisco IOS XE Catalyst SD-WAN デバイス でのアフィニティの設定

Cisco IOS XE Catalyst SD-WAN デバイス をアフィニティに参加させるには、ルータが制御接続の確立を許可する Cisco SD-WAN コントローラ を設定するとともに、 Cisco IOS XE Catalyst SD-WAN デバイス 自体およびルータ上の個々のトンネルが確立することを許可される制御接続（または TLOC）の最大数を設定します。

Cisco Catalyst SD-WAN Controller グループの設定

ルータが制御接続を確立できるように Cisco SD-WAN コントローラ を設定するには、次の 2 段階のプロセスを実行します。

- システムレベルで、オーバーレイネットワークに存在する全コントローラグループ ID の単一のリストを設定します。
- VPN 0（sdwan）のトンネルインターフェイスごとに、トンネルインターフェイスがどのコントローラグループ ID と制御接続を確立できるかを制限できます。制限するには、除外リストを設定します。

システムレベルで、Cisco SD-WAN コントローラ グループの ID を設定します。

```
ISR4331(config)#system controller-group-list numbers
```

Cisco IOS XE Catalyst SD-WAN デバイス 上のトンネル接続のいずれかが制御接続を確立する Cisco SD-WAN コントローラ グループ ID のリストを作成します。このリストには、オーバーレイネットワーク内の全 Cisco SD-WAN コントローラ グループの ID を含めることを推奨します。

VPN 0（sdwan）の特定のトンネルインターフェイスについて、全 Cisco SD-WAN コントローラ グループのサブセットのみへの制御接続を確立する場合は、除外するグループ ID を設定します。

```
ISR4331(config-interface-GigabitEthernets0/0/1)#tunnel-interface
exclude-controller-group-list numbers
```

```
ISR4331(config-sdwan)# interface GigabitEthernets0/0/1 tunnel-interface
exclude-controller-group-list numbers
```

このコマンドにより、特定のトンネルインターフェイスが制御接続を確立しない Cisco SD-WAN コントローラ グループの ID が表示されます。このリスト内のコントローラグループは、**system controller-group-list** コマンドで設定されたコントローラグループのサブセットである必要があります。

Cisco IOS XE Catalyst SD-WAN デバイス で設定されているコントローラグループを表示するには、**show sdwan control connections** コマンドを使用します。

制御接続の最大数の設定

Cisco IOS XE Catalyst SD-WAN デバイス の制御接続の最大数を設定するには、次の 2 段階のプロセスを実行します。

- システムレベルで、 Cisco IOS XE Catalyst SD-WAN デバイス が Cisco SD-WAN コントローラ に対して確立できる制御接続の最大数を設定します。
- VPN 0（sdwan）のトンネルインターフェイスごとに、トンネルが Cisco SD-WAN コントローラ に対して確立できる制御接続の最大数を設定します。

デフォルトでは、 Cisco IOS XE Catalyst SD-WAN デバイス は Cisco SD-WAN コントローラ への制御接続に関する 2 つの OMP セッションを確立できます。 OMP セッションの最大数を変更するには、次の手順を実行します。

```
ISR4331(config)#system max-omp-sessions number
```

OMP セッションの数は 0 ～ 100 の範囲で指定できます。

Cisco IOS XE Catalyst SD-WAN デバイス は、次の手順で OMP セッションを確立します。

- 各 DTLS および各 TLS コントロール プレーン トンネルが個別の OMP セッションを作成します。
- Cisco SD-WAN コントローラ との OMP セッションを確立するのは、VPN 0（sdwan）の個々のトンネルインターフェイスではなく、全体としての Cisco IOS XE Catalyst SD-WAN デバイス です。ルータ上の異なるトンネルインターフェイスに同じ Cisco SD-WAN コントローラ グループとのアフィニティが設定されている場合、 Cisco IOS XE Catalyst SD-WAN デバイス はそのグループに属する Cisco SD-WAN コントローラ のいずれかに対して単一の OMP セッションを作成し、複数のトンネルインターフェイスがこの単一の OMP セッションを使用します。

デフォルトでは、VPN 0（sdwan）の各トンネルインターフェイスは 2 つの制御接続を確立できます。これを変更するには、次の手順を実行します。

```
ISR4331(config)#sdwan interface interface-name tunnel-interface max-control-connections
 number
```

制御接続の数は 0 ～ 100 の範囲で指定できます。デフォルト値は、**system max-omp-sessions** コマンドで設定された OMP セッションの最大数です。

Cisco IOS XE Catalyst SD-WAN デバイス に複数の WAN トランスポート接続があり、VPN 0（sdwan）に複数のトンネルインターフェイスがある場合、すべてのトンネルが確立できる制御接続の最大数の合計を、ルータ自体で許可されている最大数を上回る値にすることはできません。

インターフェイスに設定されている制御接続の最大数を表示するには、**show sdwan control local-properties** コマンドを使用します。

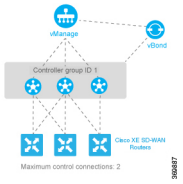
各トンネルインターフェイスの実際の制御接続数を表示するには、**show sdwan control affinity config** コマンドを使用します。

各トンネルインターフェイスが制御接続を確立した Cisco SD-WAN コントローラ のリストを表示するには、**show sdwan control affinity status** コマンドを使用します。

単一データセンターにおける Cisco Catalyst SD-WAN Controller のアフィニティの設定

複数の Cisco SD-WAN コントローラ を備えた単一データセンターを含むオーバーレイネットワークで、 Cisco IOS XE Catalyst SD-WAN デバイス がいずれかの Cisco SD-WAN コントローラに対して単一の制御接続を確立する場合、この状況はデフォルトの動作であるため、アフィニティを設定する必要はありません。

ただし、コントローラの 1 つが使用できなくなった場合の冗長性を提供するために、Cisco IOS XE Catalyst SD-WAN デバイス と複数の Cisco SD-WAN コントローラ との制御接続を確立する場合は、アフィニティを設定します。通常、Cisco SD-WAN コントローラ は同じコントローラグループに配置します。



すべての Cisco SD-WAN コントローラ が同じコントローラグループ ID 1 を使用しているとします。次のように、3 つのコントローラすべてにこの識別子を設定します。

```
vSmart(config)# system controller-group-id 1
```

設定を確認するには、**show running-config** コマンドを使用します。

```
vSmart# show running-config system
system
 description         "vSmart in data center 1"
 host-name           vSmart
 gps-location latitude 37.368140
 gps-location longitude -121.913658
 system-ip           172.16.255.19
 site-id             100
 controller-group-id 1
 organization-name   "Cisco"
 clock timezone America/Los_Angeles
```

3 つの Cisco IOS XE Catalyst SD-WAN デバイス は、3 つの Cisco SD-WAN コントローラ のうち 2 つへの 2 系統の制御接続を確立する必要があります。この操作は、コントローラの 1 つが使用可能になった場合の冗長性を確保するために行われます。すべての Cisco SD-WAN コントローラ が同じコントローラグループに属しているため、 Cisco IOS XE Catalyst SD-WAN デバイスが接続する 2 つのコントローラを指定したり、その指定に影響を与えたりすることはできません。3 つのルータすべての設定は実質的に同一です。ここでは、ルータ Cisco IOS XE Catalyst SD-WAN デバイス-1 の設定を取り上げます。

まず、使用可能な Cisco SD-WAN コントローラ グループを設定します。このシナリオには、グループが 1 つだけ含まれています。

```
ISR4331-1(config)# system controller-group-list 1
```

デフォルトでは、 Cisco IOS XE Catalyst SD-WAN デバイス は 2 つの制御接続を確立できます。各 Cisco IOS XE Catalyst SD-WAN デバイス と各トンネルインターフェイスを 2 つの Cisco SD-WAN コントローラ に接続する必要があるため、この時点での設定は必要ありません。ただし、これらのパラメータを明示的に設定する場合は、システムレベルで OMP セッションの最大数を設定し、トンネルごとの制御接続の最大数を設定します。

```
ISR4331-1(config)# system max-omp-sessions 2
ISR4331-1(config)# sdwan interface GigabitEthernets0/0/1 tunnel-interface
ISR4331-1(config-tunnel-interface)# max-control-connections 2
```

Cisco IOS XE Catalyst SD-WAN デバイス-1 からの関連する設定スニペットを次に示します。

```
ISR4331-1# show sdwan running-config | section system
system
 host-name              ISR4331-1
gps-location latitude 43.0
gps-location longitude -75.0
system-ip             172.16.255.11
site-id               100
max-omp-sessions      2
```

```
controller-group-list 1
admin-tech-on-failure
organization-name     Cisco
 ...
ISR4331-1# show running-config | section sdwan
...
 interface GigabitEthernets0/0/1
  tunnel-interface
   encapsulation ipsec
   max-control-connections 1
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   no allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
  exit
exit
…
```

Cisco SD-WAN コントローラ との制御接続を表示するには、 **show sdwan control connections** コマンドを使用します。最後の列の [コントローラグループID（Controller Group ID）] には、ルータが属する Cisco SD-WAN コントローラ グループが表示されます。

```
ISR4331-1# show sdwan control connections

                                                                                       PEER
PEER                                    CONTROLLER
PEER    PEER PEER            SITE       DOMAIN PEER                                    PRIV  PEER
PUB                                     GROUP
TYPE    PROT SYSTEM IP       ID         ID     PRIVATE IP                              PORT  PUBLIC IP                                PORT
LOCAL COLOR     PROXY STATE UPTIME      ID
--------------------------------------------------------------------------------------------------------------------------------------------
------------------------------------------
vsmart  dtls 10.255.2.120     1          1      10.2.1.120                               12346 10.2.1.120                                 12346
default              up     0:00:06:17  1
vmanage dtls 10.255.2.100  1    1          0      10.2.1.100                               12346 10.2.1.100
12346 default              up     0:00:06:13  0
```

ルータで許可される制御接続の最大数を表示するには、 **show sdwan control local-properties** コマンドを使用します。出力の最後の行に、コントローラの最大数が表示されます。次に、このコマンドの出力を簡略化して示します。

```
ISR4331-1# show sdwan control local-properties

personality                  vedge
organization-name            Cisco
certificate-status           Installed
root-ca-chain-status         Installed

certificate-validity         Valid
certificate-not-valid-before Sep 27 03:14:18 2016 GMT
certificate-not-valid-after  Sep 27 03:14:18 2026 GMT
...

                         PUBLIC          PUBLIC PRIVATE         PRIVATE                                 PRIVATE                                MAX
 RESTRICT/           LAST          SPI
TIME    NAT  VM
INTERFACE                IPv4            PORT   IPv4            IPv6                                    PORT    VS/VM COLOR            STATE CNTRL
 CONTROL/     LR/LB  CONNECTION
REMAINING   TYPE CON
STUN                                                 PRF
----------------------------------------------------------------------------------------------------------------------------------------------------
-------------------
GigabitEthernet0/0/1     2.2.1.17        12406  2.2.1.17        ::                                      12406    2/1  default          up     2
   no/yes/no    No/No  17:15:53:07
0:08:02:33  N    5
```

2 つのコマンドで、アフィニティ設定によって確立された制御接続に関する情報が表示されます。設定されているコントローラグループとインターフェイスの接続先をインターフェイスごとに確認するには、 **show sdwan control affinity config** コマンドを使用します。

```
ISR4331-1# show sdwan control affinity config
EFFECTIVE CONTROLLER LIST FORMAT - G(C),...     - Where G is the Controller Group ID
                                                  C is the Required vSmart Count

CURRENT CONTROLLER LIST FORMAT   - G(c)s,...    - Where G is the Controller Group ID
                                                  c is the current vSmart count
                                                  s Status Y when matches, N when
 does not match


                EFFECTIVE
                REQUIRED
                                                                  LAST-RESORT
INDEX INTERFACE VS COUNT  EFFECTIVE CONTROLLER LIST                          CURRENT
 CONTROLLER LIST                                EQUILIBRIUM  INTERFACE
-------------------------------------------------------------------------------------
0     GigabitEthernet0/0/11         1(1)
     1(1)Y                                                  Yes          No
```

上記のコマンド出力は、インターフェイス GigabitEthernet 0/0/11 でアフィニティが設定されていることを示しています。

- [有効な必須項目とカウント（Effective Required and Count）] 列は、インターフェイスが 2 つの制御接続を作成するように設定されており、実際に 2 つの制御接続が確立されていることを示しています。**max-control-connections** コマンドを使用して、トンネルインターフェイスの制御接続の数を設定します。
- [有効なコントローラリスト（Effective Controller List）] 列には、インターフェイスのアフィニティが Cisco Catalyst SD-WAN コントローラ 識別子 1 を使用するように設定されており、ルータが 2 つの OMP セッションをサポートしていることが示されます。アフィニティコントローラ識別子は、**controller-group-list** コマンドを使用して（**system** レベルで）設定します。トンネルインターフェイスの場合は **exclude-controller-group-list** コマンドを使用します。
- [現在のコントローラリスト（Current Controller List）] 列には、インターフェイスの実際のアフィニティ設定が一覧表示されます。この出力は、インターフェイスにグループ 1 の Cisco Catalyst SD-WAN コントローラ との制御接続が 2 つあることを示しています。チェックマークは、現在のコントローラリストと有効なコントローラリストが互いに一致していることを示します。たとえば、トンネルが Cisco SD-WAN コントローラ への TLOC 接続を 1 つのみ確立した場合、この列には「1(1)X」と表示されます。
- [均衡（Equilibium）] 列は、現在のコントローラリストが、そのトンネルインターフェイスのアフィニティ設定から予期されるものと一致することを示します。

トンネルインターフェイスが制御接続を確立した Cisco Catalyst SD-WAN コントローラ を正確に判別するには、**show control affinity status** コマンドを使用します。

```
ISR4331-1# show sdwan control affinity status
ASSIGNED CONNECTED CONTROLLERS   - System IP( G),..  - System IP of the assigned vSmart
                                                      G is the group ID to which
 the vSmart belongs to
```

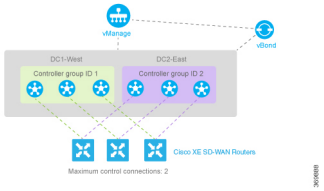
```
UNASSIGNED CONNECTED CONTROLLERS - System IP( G),..  - System IP of the unassigned vSmart

                                                                    G is the group ID to which
 the vSmart belongs to

INDEX            INTERFACE           ASSIGNED   CONNECTED CONTROLLERS
                                UNASSIGNED CONNECTED CONTROLLERS
-------------------------------------------------------------------------------------------------
0          GigabitEthernet 0/0/1     10.255.2.120(  1)
```

上記のコマンド出力は、インターフェイス **GigabitEthernet 0/0/1** に、グループ 1 に属する Cisco SD-WAN コントローラ（10.255.2.120）への制御接続があることを示しています。インターフェイスがコントローラグループリストにない Cisco SD-WAN コントローラ に接続されていた場合は、[未割り当ての接続済みコントローラ（Unassigned Connected Controllers）] 列に表示されます。

データセンターに複数の Cisco SD-WAN コントローラ が存在する場合、それらを異なるコントローラグループに属するように設定できます。たとえば、2 つの異なるコントローラグループに属するように設定した場合、各 Cisco IOS XE Catalyst SD-WAN デバイス が 2 つの制御接続（各グループに 1 つずつ）を確立できます。この設定の設計は、Cisco SD-WAN コントローラへの冗長制御接続を提供する、前のセクションで説明した設計と似ていますが、データセンター内の 2 つの Cisco Catalyst SD-WAN コントローラ グループ間の障害分離が可能になる点でわずかに異なります。このシナリオの設定は、Cisco Catalyst SD-WAN コントローラ が 2 つのデータセンターである場合の設定とほぼ同じです。唯一の違いは、2 つの Cisco Catalyst SD-WAN コントローラ グループが同じデータセンターに配置されていることです。次のセクションの設定例を参照してください。

2 つのデータセンターにおける Cisco Catalyst SD-WAN Controller のアフィニティの設定

複数の Cisco SD-WAN コントローラ が 2 つ以上のデータセンターに分散しているネットワーク設計では、アフィニティを使用してデータセンター間の冗長性を有効にすることができます。その後、 Cisco IOS XE Catalyst SD-WAN デバイス といずれかのデータセンター間のリンクがダウンした場合、第 2 のデータセンターの Cisco SD-WAN コントローラ を使用してオーバーレイネットワークのサービスを継続できます。次の図はこのシナリオを図示したもので、2 つのデータセンターのそれぞれに属する 3 つの Cisco SD-WAN コントローラ を示しています。3 つの Cisco IOS XE Catalyst SD-WAN デバイス はそれぞれ、West データセンターの 1 つのコントローラと East データセンターの 1 つのコントローラへの TLOC 接続を確立します。



コントローラグループ ID 1 を使用して、DC1-West の 3 つの Cisco SD-WAN コントローラ を設定します。

```
vSmart-DC1(config)# system controller-group-id 1
```

DC2-East の 3 つの Cisco SD-WAN コントローラ は、コントローラグループ 2 に属しています。

```
vSmart-DC2(config)# system controller-group-id 2
```

すべての Cisco IOS XE Catalyst SD-WAN デバイス に最大 2 つの OMP セッションを設定し、各トンネルインターフェイスに最大2つの制御接続を設定し、いずれのコントローラグループも除外しないようにします。したがって、ルータで実行する必要がある設定は、コントローラグループリストを設定することだけです。West の Cisco IOS XE Catalyst SD-WAN デバイス が DC2-East よりも DC1-West の Cisco Catalyst SD-WAN コントローラ を優先するようにします。

```
ISR4331-West(config)#  system controller-group-list 1 2
```

同様に、East の Cisco IOS XE Catalyst SD-WAN デバイス が DC2-East を優先するようにします。

```
ISR4331-East(config)# system controller-group-list 2 1
```

ソフトウェアはコントローラグループリストを順番に評価するため、この設定では、Cisco IOS XE Catalyst SD-WAN デバイス-West は Cisco SD-WAN コントローラ グループ 1（West データセンター）を優先し、Cisco IOS XE Catalyst SD-WAN デバイス-East は Cisco SD-WAN コントローラ グループ 2 を優先します。

他の方法でコントローラグループの設定を微調整できます。

- ルータで許可される OMP セッションの最大数を 2 に設定します（**system max-omp-sessions 1**）。これがどのように機能するかを示すため、Cisco IOS XE Catalyst SD-WAN デバイス-West に注目します。このルータにはトンネルインターフェイスが 1 つだけあり、そのインターフェイスは Cisco SD-WAN コントローラ リスト 1 への制御接続を 1 つ作成します。このグループに属するすべての Cisco SD-WAN コントローラ が使用できなくなった場合、または DC1-West データセンターとルータ間の接続がダウンした場合、トンネルインターフェイスは Cisco SD-WAN コントローラ リスト 2 への 1 つの制御接続を確立します。このグループが **system controller-group-list** コマンドのリストに含まれているためです。両方のコントローラグループに属するすべての Cisco SD-WAN コントローラ、またはそれらへの接続が使用できなくなり、これらのすべての Cisco SD-WAN コントローラ が到達不能であることが Cisco SD-WAN Validator に示されている場合、トンネルインターフェイスは、他のコントローラが存在する場合、オーバーレイネットワークに含まれる他の任意の Cisco SD-WAN コントローラ への制御接続を確立します。

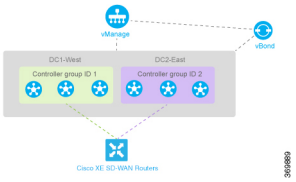
- トンネルインターフェイスが確立できる制御接続の最大数を 1 に設定します（**vpn 0 sdwan interface tunnel-interface max-control-connections 1**）。ソフトウェアはコントローラグループリストを順番に評価するため、Cisco IOS XE Catalyst SD-WAN デバイス-West の場合、この設定により、トンネルインターフェイスは Cisco SD-WAN コントローラ グループ 1 への制御接続の確立を強制されます。この場合も、このコントローラグループまたはデータセンターが到達不能になると、トンネルはコントローラグループ 2 との制御接続を確立します。このグループが **system controller-group-list** コマンドで設定されているためです。また、コントローラグループ 1 と 2 のいずれも使用できないときに、ネットワークにもう 1 つの Cisco SD-WAN コントローラ が存在する場合、トンネルインターフェイスはそのコントローラとの制御接続を確立します。

- 特定のトンネルの非優先 Cisco SD-WAN コントローラ グループを除外します。たとえば、Cisco IOS XE Catalyst SD-WAN デバイス-West にコントローラグループ 1 を優先させるに

は、**vpn 0 sdwan interface tunnel-interface exclude-controller-group-list 2** を設定します。上記の設定と同様に、このコントローラグループまたはデータセンターが到達不能になると、トンネルはコントローラグループ2との制御接続を確立します。このグループが**system controller-group-list** コマンドで設定されているためです。また、コントローラグループ 1 と 2 のいずれも使用できないときに、ネットワークにもう 1 つの Cisco SD-WAN コントローラが存在する場合、トンネルインターフェイスはそのコントローラとの制御接続を確立します。

単一デバイスでの冗長性制御接続の設定

ルータに 2 つのトンネル接続があり、ネットワークに 2 つ（またはそれ以上）のデータセンターがある場合は、2 つのデータセンターで Cisco IOS XE Catalyst SD-WAN デバイス から Cisco SD-WAN コントローラ への冗長制御接続を設定できます。最小数の OMP セッション（この場合は2）を使用して設定することを推奨します。これを実行するには、一方のトンネルインターフェイスを 1 つのデータセンターのみに接続し、もう一方を 2 番目のデータセンターのみに接続するように設定します。この設定により、最小数の OMP セッションで Cisco SD-WAN コントローラ の冗長性が実現します。



Cisco IOS XE Catalyst SD-WAN デバイス ルータで、コントローラグループリストを定義し、OMP セッションの最大数を 2 に設定します。

```
ISR4331(config)# system controller-group-list 1 2
ISR4331(config)#  system max-omp-sessions 2
```

いずれかのトンネルについて、デフォルトのアフィニティ設定（つまり何も設定しない状態）を使用して、このトンネルにグループ 1 の Cisco Catalyst SD-WAN コントローラ を優先させることができます。このトンネルが必ず Cisco Catalyst SD-WAN コントローラ グループ 1 を優先するように明示的に設定することもできます。

```
ISR4331(config-tunnel-interface-1)# max-control-connections 1
```

ソフトウェアはコントローラグループリストをグループ 1 から順に評価するため、**exclude-controller-group-list 2** を設定する必要はありません。ただし、Cisco SD-WAN コントローラ グループ 2 を明示的に除外することもできます。

次に、2 番目のトンネルがグループ 2 の Cisco SD-WAN コントローラ を優先するように設定します。他のトンネルと同様に、制御接続の最大数を 1 に制限します。さらに、このトンネルのコントローラグループ 1 を除外する必要があります。

```
ISR4331(config-tunnel-interface-2)# max-control-connections 1
ISR4331(config-tunnel-interface-2)# exclude-controller-group-list 1
```

コントロールプレーンおよびデータプレーンの高可用性パラメータの設定

このトピックでは、コントロールプレーンとデータプレーンの設定可能な高可用性パラメータについて説明します。

コントロールプレーンの高可用性

可用性の高いCisco Catalyst SD-WANネットワークには、各ドメインに2つ以上のCisco SD-WANコントローラ が含まれています。Cisco Catalyst SD-WAN ドメインには、最大 20 の Cisco SD-WANコントローラを含めることができ、デフォルトでは、それぞれのCisco IOS XE Catalyst SD-WANデバイス がそのうちの 2 つに接続します。この値は、トンネルごとに変更します。

```
ISR4331(config)# sdwan interface interface-name tunnel-interface
max-control-connections number
```

ドメイン内の Cisco SD-WAN コントローラ の数が、ドメインの Cisco IOS XE Catalyst SD-WANデバイスが接続を許可されているコントローラの最大数よりも多い場合、Cisco Catalyst SD-WANソフトウェアは、使用可能な Cisco SD-WAN コントローラ の間の接続をロードバランシングします。

（注） Cisco SD-WAN コントローラ 間のロードバランシングの効率を最大化するには、ドメイン内のCisco IOS XE Catalyst SD-WANデバイス にシステム IP アドレスを割り当てるときに連番を使用します。たとえば、172.1.1.1、172.1.1.2、172.1.1.3 などの連番を付与します。あるいは172.1.1.1、172.1.2.1、172.1.3.1 なども使用できます。

データプレーンの高可用性

Cisco Catalyst SD-WAN 高可用性ソリューションの一部としてリンク障害を検出する BFD は、シスコのすべてのデバイスでデフォルトで有効になっています。BFD は、 Cisco IOS XE Catalyst SD-WANデバイス 間のすべてのIPsecデータトンネルで自動的に実行されます。Cisco SD-WANコントローラ がネットワーク内のシスコのデバイスすべてと確立するコントロールプレーン（DTLS または TLS）トンネルでは実行されません。

BFD がリンクの障害を宣言する前に、BFD Hello パケット間隔および欠落した Hello パケットの数（BFD 間隔乗数）を変更できます。

BFD Hello パケット間隔の変更

BFD は、2 つの Cisco IOS XE Catalyst SD-WAN デバイス 間の IPsec データトンネル障害を検出するために、定期的にHelloパケットを送信します。デフォルトでは、BFD はこれらのパケットを 1000 ミリ秒ごとに（つまり、1 秒に 1 回）送信します。1 つ以上のトラフィックフローでこの間隔を変更するには、**hello-interval** コマンドを使用します。

```
ISR4331(config)#bfd color color hello-interval milliseconds
```

この間隔には、100 ～ 300000 ミリ秒（5 分）の範囲の値を指定できます。

色で識別される各トンネル接続の間隔を設定します。色は、**3g**、**biz-internet**、**blue**、**bronze**、**custom1**、**custom2**、**custom3**、**default**、**gold**、**green**、**lte**、**metro-ethernet**、**mpls**、**private1**、**private2**、**public-internet**、**red**、**silver** のいずれかになります。

BFD パケット間隔乗数の変更

BFD は、リンクで一定数の Hello パケットを受信しなかった場合、そのリンクに障害が発生したと宣言します。このパケット数は、Hello パケット間隔時間の乗数です。デフォルトでは、この乗数はハードウェアルータの場合は7、クラウドソフトウェアルータの場合は20です。これは、BFD が 7 秒間 Hello パケットを受信しなかった場合、リンクに障害が発生したと見なし、冗長性プランを導入することを意味します。

BFD パケット間隔乗数を変更するには、**multiplier** コマンドを使用します。

```
ISR4331(config)#bfd color color multiplier integer
```

乗数の範囲：1 ～ 60（整数）

色で表される各トンネル接続の乗数を設定します。

PMTU ディスカバリの制御

トランスポート接続ごとに（つまり、TLOC または色ごとに）、Cisco Catalyst SD-WAN BFD ソフトウェアはパス MTU（PMTU）ディスカバリを実行します。この動作により、接続でのパケット フラグメンテーションを最小限に抑えるか排除するために、MTU サイズが自動的にネゴシエートされます。BFD PMTU ディスカバリはデフォルトで有効になっています。BFD PMTUディスカバリを無効にせずに使用することを推奨します。明示的に有効にするには、次の手順を実行します。

```
ISR4331(config)#bfd color color pmtu-discovery
```

PMTU ディスカバリが有効になっている場合、トンネル接続のパス MTU は定期的に（約 1 分に1回）チェックされ、動的に更新されます。PMTUディスカバリが有効になっている場合、PMTU ディスカバリには 16 バイトが必要になる可能性があるため、有効なトンネル MTU は 1452バイトと低くなります。カプセル化の観点からすると、GRE のデフォルト IP MTU は1468 バイトであり、IPsec の場合はオーバーヘッドが大きいため 1442 バイトになります。PMTU ディスカバリを無効にすると、 Cisco IOS XE Catalyst SD-WAN デバイス 間で送信される BFD パケットのオーバーヘッドが追加されますが、通常のデータトラフィックのオーバーヘッドは追加されません。

PMTU ディスカバリが無効な場合、予想されるトンネル MTU は 1472 バイトです（1500 バイトのトンネル MTU から GRE ヘッダーの 4 バイト、外部 IP ヘッダーの 20 バイト、MPLS ヘッダーの 4 バイトを引いた値）。ただし、ソフトウェアが誤って 4 バイトをヘッダーに追加する場合があるため、有効なトンネル MTU は 1468 バイトになる場合があります。

ハイ アベイラビリティの設定

高可用性を設定およびモニタリングするための CLI コマンド。

高可用性設定コマンド

Cisco IOS XE Catalyst SD-WAN デバイス で高可用性を設定するには、次のコマンドを使用します。

```
bfd
  app-route
    multiplier number
    poll-interval milliseconds
  color color
    hello-interval milliseconds
    multiplier number
    pmtu-discovery
```

高可用性モニタリングコマンド

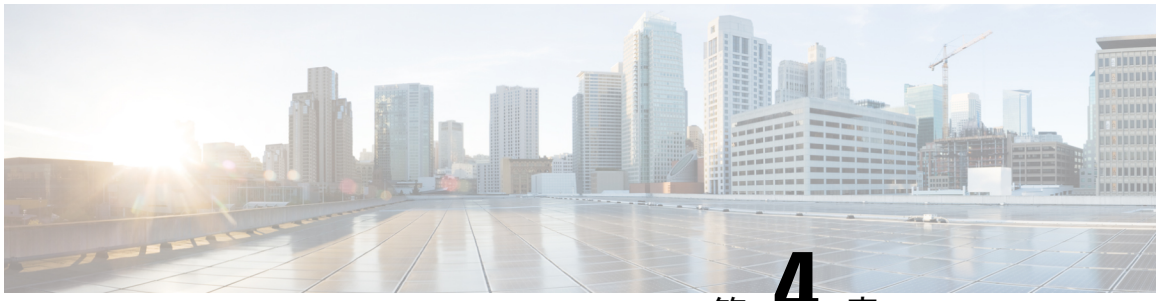
show sdwan bfd sessions：ローカル Cisco IOS XE Catalyst SD-WAN デバイス で実行されている BFD セッションに関する情報を表示します。

アフィニティ設定のベストプラクティス

- Cisco IOS XE Catalyst SD-WAN デバイス の **system controller-group-list** コマンドで、オーバーレイネットワークで使用可能なすべてのコントローラグループが一覧表示されます。この操作により、オーバーレイネットワーク内のすべての Cisco SD-WAN コントローラ をアフィニティ設定に使用できるようになり、優先グループへの接続が失われた場合に備えた冗長性が向上します。ルータの OMP セッションの最大数、トンネルの制御接続の最大数、トンネルが使用しないコントローラグループに基づいて、制御接続の数と優先順位を操作します。**system controller-group-list** コマンドですべてのコントローラグループを一覧表示することで冗長性が向上するのは、コントローラグループリスト内の Cisco SD-WAN コントローラ への到達時に Cisco IOS XE Catalyst SD-WAN デバイス サイトで接続の問題が発生している場合です。こうした状況の例を示します。3 つのコントローラグループ（1、2、3）を含むネットワークで、 Cisco IOS XE Catalyst SD-WAN デバイス のコントローラグループリストにグループ 1 と 2 のみが記載されているとします。これらが優先グループであるためです。ルータがグループ 1 と 2 の Cisco SD-WAN コントローラ が稼働していることを Cisco SD-WAN Validator から学習したものの、ルータに両方のサイトへの接続の問題がある場合、ルータはオーバーレイネットワークへの接続を失います。ただし、コントローラグループリストに3つのコントローラグループすべてが記載されている場合、グループ 3 が優先グループではなくても、ルータがグループ 1 またはグループ 2 の Cisco SD-WAN コントローラ に接続できない場合、ルータはフォールバックしてグループ 3 のコントローラに接続できます。アフィニティと Cisco SD-WAN コントローラ に接続する順序の設定は、優先順位にすぎません。この優先順位は可能な限り尊重されます。それでも、オーバーレイネットワークで高可用性を適用するための包括的なルールでは、動作している Cisco SD-WAN コントローラ が使用されます。ネットワークは、動作している Cisco SD-WAN コントローラ がない場合にのみ機能を停止します。そのため、特定の時点でネットワーク内で動作している唯一のコントローラが最も優先順位の低い Cisco SD-WAN コントローラ である場合、これが使用されることがあります。 Cisco IOS XE Catalyst SD-WAN デバイス は、起動時にオーバーレイネットワーク内のすべての Cisco SD-WAN コントローラ について学習し、Cisco SD-WAN Validator は、Cisco SD-WAN コントローラ が稼働しているルータと継続的に通信します。そのため、 Cisco IOS XE Catalyst SD-WAN デバイス

が、設定されたコントローラグループ内で優先される Cisco SD-WAN コントローラ のいずれにも到達できず、別の Cisco SD-WAN コントローラ が稼働している場合、ルータは稼働中のコントローラに接続します。別の言い方をすれば、複数の Cisco SD-WAN コントローラ が含まれるネットワークでは、最後の手段として、 Cisco IOS XE Catalyst SD-WAN デバイスは、コントローラがルータのコントローラグループリストで設定されているかどうかに関係なく、いずれかのコントローラに接続し、オーバーレイネットワークの動作を維持します。

- **exclude-controller-group-list** コマンドに一覧表示されるコントローラグループは、**system controller-group-list** コマンドで、ルータ全体に対して設定されたコントローラグループのサブセットである必要があります。
- データセンターに同じコントローラグループ ID を使用する複数の Cisco SD-WAN コントローラがあり、オーバーレイネットワークに2つ以上のデータセンターがある場合は、各コントローラグループに含まれる Cisco SD-WAN コントローラ の数を同数にすることを推奨します。たとえば、データセンター 1 に 3 つの Cisco SD-WAN コントローラ があり、すべてが同じグループ ID（たとえば 1）を持つ場合、データセンター 2 にも同じグループ ID（たとえば 2）を持つ 3 つの Cisco SD-WAN コントローラ が必要です。さらに、その他のセンターにも 3 つの Cisco SD-WAN コントローラ が必要です。
- 1 つのデータセンターが、同じコントローラグループ内にある複数の Cisco SD-WAN コントローラ を含む場合、すべての Cisco SD-WAN コントローラ のハードウェア機能（特にメモリと CPU）は同一である必要があります。さらに言えば、オーバーレイネットワーク内のすべての Cisco SD-WAN コントローラ は、1 つのデータセンター内にあるか多数のデータセンター内にあるかにかかわらず、同じハードウェア機能を備えている必要があります。各 Cisco SD-WAN コントローラ は、ネットワークに含まれるいずれの Cisco IOS XE Catalyst SD-WAN デバイス からの制御接続も処理できる同等のキャパシティと機能を備えている必要があります。
- ルータに 2 つのトンネル接続があり、ネットワークに 2 つ（またはそれ以上）のデータセンターがある場合は、トンネルインターフェイスの一方を 1 つのデータセンターに接続し、もう一方を他方のデータセンターに接続するように設定することを推奨します。この設定により、最小数の OMP セッションで Cisco SD-WAN コントローラ の冗長性が実現します。
- ネットワーク設計で可能な限り、アフィニティ設定を活用して障害分離ドメインを作成する必要があります。



第 4 章

ディザスタリカバリ

（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
Cisco SD-WAN Manager のディザスタリカバリ	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b Cisco Catalyst SD-WAN Manager リリース 20.12.1 Cisco vManage リリース 19.2.1	この機能は、予期しない状況が原因で発生する可能性のあるハードウェアまたはソフトウェアの障害に対処するために、Cisco SD-WAN Manager をアクティブモードまたはスタンバイモードに設定するのに役立ちます。
6 ノード Cisco SD-WAN Manager クラスタのディザスタリカバリ	Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能は、6 ノード Cisco SD-WAN Manager クラスタのディザスタリカバリをサポートします。

機能名	リリース情報	説明
単一ノード Cisco SD-WAN Manager クラスタのディザスタリカバリ	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能は、単一のプライマリノードを使用した Cisco SD-WAN Manager 展開のディザスタリカバリをサポートします。
ディザスタ リカバリ ユーザー パスワードの変更	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能を使用すると、Cisco SD-WAN Manager の [ディザスタ リカバリ（Disaster Recovery）] ウィンドウから、ディザスタ リカバリ コンポーネントのディザスタ リカバリ ユーザー パスワードを変更できます。
ディザスタリカバリアラート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1 以下の点にも注意してください。 Cisco IOS XE リリース 17.6.4 以降の 17.6.x リリース Cisco SD-WAN Manager リリース 20.6.4 以降の 20.6.x リリース	ディザスタ リカバリ ワークフローの障害または発生したイベントに関して、アラームと syslog メッセージを生成するように Cisco SD-WAN Manager アラートを設定できます。

- ディザスタリカバリに関する情報 （35 ページ）
- アーキテクチャの概要 （35 ページ）
- 前提条件 （36 ページ）
- ベストプラクティスと推奨事項 （37 ページ）
- ディザスタリカバリの有効化 （38 ページ）
- ディザスタリカバリの登録 （38 ページ）
- ディザスタリカバリ登録の確認 （39 ページ）
- ディザスタリカバリの削除 （40 ページ）
- 管理者トリガーフェールオーバーの実行 （40 ページ）
- ディザスタリカバリ操作 （41 ページ）
- Cisco SD-WAN Manager または Cisco Catalyst SD-WAN Validator 管理者パスワードの変更 （42 ページ）
- ディザスタ リカバリ コンポーネント用ディザスタ リカバリ ユーザー パスワードの変更 （42 ページ）
- ディザスタリカバリアラートの設定 （44 ページ）

ディザスタリカバリに関する情報

Cisco Catalyst SD-WAN ソリューションを構成する 3 つのコントローラ（Cisco SD-WAN Manager、Cisco Catalyst SD-WAN コントローラ、Cisco Catalyst SD-WAN Validator）のうち、Cisco SD-WAN Managerは、ステートフルであり、アクティブ-アクティブモードで展開できない唯一のコントローラです。ディザスタ リカバリ ソリューションの目標は、Cisco SD-WAN Manager をプライマリ/セカンダリモードで 2 つのデータセンターに展開することです。

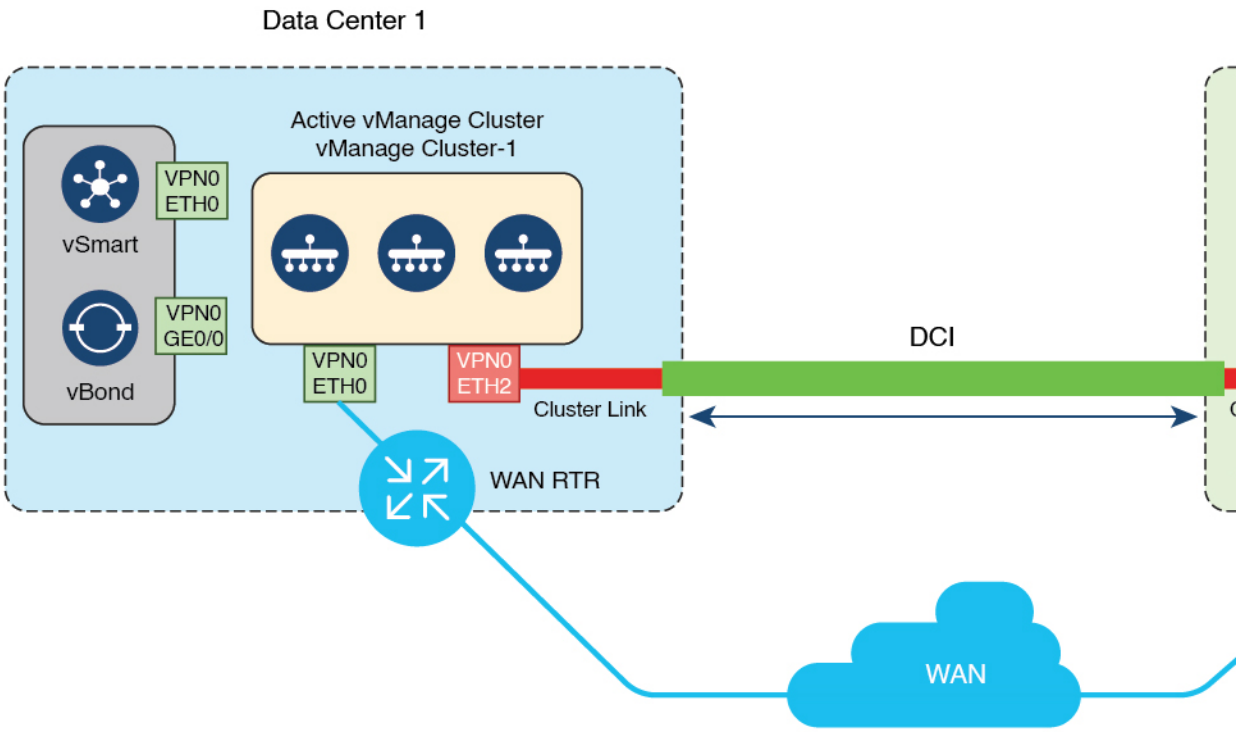
ディザスタリカバリは、管理者トリガー型のフェールオーバープロセスを提供します。ディザスタリカバリを登録すると、データは、プライマリとセカンダリの Cisco SD-WAN Manager クラスタ間で自動的に複製されます。必要に応じて、セカンダリクラスタへのフェールオーバーを手動で実行します。

ディザスタリカバリは次のように検証されます。

- Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a および Cisco SD-WAN リリース 20.4.1 より前のリリースの場合、ディザスタリカバリは 3 ノードクラスタで検証されます。
- Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a および Cisco SD-WAN リリース 20.4.1 では、ディザスタリカバリは 6 ノードクラスタで検証されます。
- Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a および Cisco SD-WAN リリース 20.5.1 では、ディザスタリカバリは単一のプライマリノードによる展開で検証されます。

アーキテクチャの概要

次の図は、ディザスタ リカバリ ソリューションのアーキテクチャの概要を示しています。



前提条件

ディザスタリカバリを登録する前に、次の要件を満たしていることを確認してください。

- リリースで検証された特定の数のノードを含む 2 つの Cisco SD-WAN Manager クラスタがあることを確認します。（各リリースの検証済みノード数については、この章で前述しています）。
- プライマリクラスタとセカンダリクラスタが、トランスポート VPN（VPN 0）上の HTTPS によって到達可能であることを確認します。
- セカンダリクラスタの Cisco Catalyst SD-WAN コントローラ と Cisco Catalyst SD-WAN Validator がプライマリクラスタに接続されていることを確認します。
- プライマリクラスタとセカンダリクラスタの Cisco SD-WAN Manager ノードが同じ Cisco SD-WAN Manager バージョンを実行していることを確認します。
- ディザスタリカバリに使用される各 Cisco SD-WAN Manager ノードの VPN 0 で、アウトオブバンドまたはクラスタインターフェイスを設定します。このインターフェイスは、Cisco SD-WAN Manager がクラスタ内のピアとの通信に使用するのと同じインターフェイスです。
- すべての Cisco SD-WAN Manager ノードが、アウトオブバンドインターフェイスを介して相互に到達できることを確認します。

- クラスタ内のすべての Cisco SD-WAN Manager ノードで、すべてのサービス（アプリケーションサーバー、設定データベース、メッセージングサーバー、調整サーバー、および統計データベース）が有効になっていることを確認します。
- クラスタ内のすべての Cisco SD-WAN Manager ノードが同じ LAN セグメントに存在することを確認します。
- Cisco SD-WAN Manager クラスタがデータセンター間で相互に通信できるようにするには、データセンターのファイアウォールで TCP ポート 8443 および 830 を有効にします。
- Cisco Catalyst SD-WAN Validator を含むすべてのコントローラを、プライマリデータセンターとセカンダリデータセンターの両方に分散させます。分散されたコントローラが、これらのデータセンターに分散された Cisco SD-WAN Manager ノードから到達可能であることを確認します。コントローラはプライマリ Cisco SD-WAN Manager クラスタにのみ接続します。
- 単一の物理サーバーの停止がデータセンター内の Cisco SD-WAN Manager クラスタに影響しないように、各 Cisco SD-WAN Manager VM を別個の物理サーバーに分散させます。
- アクティブ（プライマリ）およびスタンバイ（セカンダリ）Cisco SD-WAN Manager クラスタで他の操作が実行中でないことを確認します。たとえば、アップグレード中のサーバーや、デバイスへのテンプレートの添付プロセスを実行しているテンプレートがないことを確認します。
- Cisco SD-WAN Manager HTTP/HTTPS プロキシサーバーが有効になっている場合は無効にします。「HTTP/HTTPS Proxy Server for Cisco vManage Communication with External Servers」[英語] を参照してください。プロキシサーバーを無効にしない場合、Cisco SD-WAN Manager は、Cisco SD-WAN Manager アウトオブバンドクラスタ IP アドレスが直接到達可能であっても、プロキシ IP アドレスを介してディザスタリカバリ通信を確立しようとします。ディザスタリカバリの登録が完了した後、Cisco SD-WAN Manager HTTP/HTTPS プロキシサーバーを再度有効にすることができます。
- ディザスタリカバリ登録プロセスを開始する前に、プライマリ Cisco SD-WAN Manager ノードの **[ツール（Tools）]** > **[ネットワークの再検出（Rediscover Network）]** ウィンドウに移動し、Cisco Catalyst SD-WAN Validator を再検出します。

ベストプラクティスと推奨事項

- ディザスタリカバリ登録には netadmin ユーザー権限を使用してください。登録プロセスを開始する前に、工場出荷時のデフォルトパスワード admin を変更することを推奨します。
- Cisco SD-WAN Validator がディザスタリカバリ認証に使用する IP アドレスを設定する場合は、プライマリおよびセカンダリ Cisco SD-WAN Manager クラスタの両方から到達可能な Cisco SD-WAN Validator の VPN 0 インターフェイス IP アドレスを指定します。トンネルインターフェイスが設定されている場合、トンネルインターフェイスで NETCONF を許可する必要があります。

- ユーザーログイン情報を変更する際、Cisco Catalyst SD-WAN デバイスの CLI ではなく、Cisco SD-WAN Manager GUI を使用することを推奨します。
- Cisco SD-WAN Manager が機能テンプレートを使用して設定されている場合は、プライマリクラスタとセカンダリクラスタの両方に別個の機能テンプレートを作成してください。プライマリクラスタでこれらのテンプレートを作成します。テンプレートがセカンダリクラスタに複製されたら、デバイスをセカンダリクラスタのテンプレートにアタッチできます。
- オンプレミス展開の場合は、アクティブな Cisco SD-WAN Manager インスタンスから設定データベースのバックアップを定期的に取得してください。
- 設定データベースを復元し、コントローラをオンボードする際、組み込みの管理ユーザー権限のみを使用してください。

ディザスタリカバリの有効化

デバイスが共有されていない（Cisco SD-WAN コントローラ、または Cisco SD-WAN Validator または Cisco SD-WAN Manager デバイスが共有されていない）2 つの別個のクラスタを起動する必要があります。

次のアクションを実行します。

- セカンダリ Cisco SD-WAN Manager クラスタを起動します。
- プライマリクラスタ、セカンダリクラスタ、および Cisco SD-WAN Validator の間の到達可能性を確認します。

ディザスタリカバリの登録

ディザスタリカバリは、プライマリ Cisco SD-WAN Manager クラスタに登録する必要があります。クラスタ内の到達可能な Cisco SD-WAN Manager ノードのアウトオブバンド IP アドレスをディザスタリカバリ登録に使用できます。

登録が完了するまでに最大 30 分かかることがあります。登録が開始されると、「No Data Available（利用可能なデータがありません）」というメッセージがディザスタ登録タスクビューに短時間表示されることがあります。登録プロセスの間、「In-progress（進行中）」というメッセージが表示されます。

「Error occurred retrieving status for action disaster_recovery_registration（アクション disaster_recovery_registration のステータス取得中にエラーが発生しました）」というメッセージが表示されたら、最後のアクティブな Cisco SD-WAN Manager ノードの再起動後、ブラウザで [リロード（Reload）] ボタンをクリックします。

今後 Cisco SD-WAN Manager ソフトウェアをアップグレードする必要がある場合は、ディザスタリカバリを一時停止し、アップグレードを実行してから、ディザスタリカバリを再開しま

す。Cisco SD-WAN Manager をアップグレードする場合は、「Cisco SD-WAN vManage Cluster Creation and Troubleshooting」[英語] で説明されているベストプラクティスに従ってください。

1. netadmin ユーザーとして Cisco SD-WAN Manager にログインします。
2. Cisco SD-WAN Manager メニューから、[管理（Administration）] > [ディザスタリカバリ（Disaster Recovery）] の順に選択します。
3. [ディザスタリカバリの管理（Manage Disaster Recovery）] をクリックします。
4. プライマリクラスタとセカンダリクラスタを設定するには、Cisco SD-WAN Manager のディザスタリカバリ画面で、それぞれのクラスタに含まれる任意の Cisco SD-WAN Manager ノードの IP アドレスを選択します。

   クラスタがロードバランサの背後にある場合は、ロードバランサの IP アドレスを指定します。
5. プライマリクラスタからセカンダリクラスタにデータを複製する場合は、[開始時刻（Start Time）]、[レプリケーション間隔（Replication Interval）]、および [遅延しきい値（Delay Threshold）] を指定します。

   [遅延しきい値（Delay Threshold）] のデフォルト値は 30 分です。

   [レプリケーション間隔（Replication Interval）] のデフォルト値 15 分です。
6. Cisco SD-WAN Manager メニューから、[管理（Administration）] > [ディザスタリカバリ（Disaster Recovery）] を選択し、クラスタ 2（セカンダリ）について [プライマリにする（Make Primary）] をクリックします。

   すべてのデバイスからすべての変更がプッシュされるまで、10 ー 15 分かかることがあります。
7. また、ディザスタリカバリの一時停止、レプリケーションの一時停止、またはディザスタリカバリ登録の削除を決定することもできます。

   ディザスタリカバリが登録され、データが複製された後に、次の情報を表示できます。

   - データが最後に複製された日時、複製にかかった時間、複製されたデータのサイズ。
   - プライマリクラスタがセカンダリクラスタに切り替えられた日時とスイッチオーバーの理由。
   - レプリケーション スケジュールと遅延しきい値。

ディザスタリカバリ登録の確認

ディザスタリカバリを登録した後、次の手順を実行します。

- プライマリクラスタからセカンダリクラスタへの複製が、設定された間隔で発生することを確認します。

- [管理（Administration）]>[ディザスタリカバリ（Disaster Recovery）]を選択して、ステータスチェックを実行します。

ディザスタリカバリの登録に失敗した場合は、次の点を確認します。

- セカンダリクラスタのすべてのクラスタメンバーから Cisco SD-WAN Validator への到達可能性。
- トランスポートインターフェイス（VPN 0）でのセカンダリクラスタとプライマリクラスタ間の到達可能性。
- ユーザー名とパスワードが正しいことを確認します。

ディザスタリカバリの削除

ディザスタリカバリを削除する場合は、プライマリクラスタで削除操作を開始することを推奨します。削除する前に、保留状態のデータ レプリケーション セッションがないこと、およびセカンダリクラスタがデータのインポート中ではないことを確認します。

プライマリ Cisco SD-WAN Manager クラスタがダウンしている場合は、セカンダリ Cisco SD-WAN Manager クラスタで削除操作を実行できます。

ディザスタリカバリの削除操作中にオフラインだった Cisco SD-WAN Manager クラスタがオンラインになった場合は、そのクラスタで次の POST 要求を実行して、ディザスタリカバリの削除操作を完了します。

POST /dataservice/disasterrecovery/deleteLocalDC

ディザスタリカバリを削除した後、プライマリクラスタとセカンダリクラスタが正しく動作していることを確認します。確認するには、**[管理（Administration）]>[クラスタ管理（Cluster Management）]** ウィンドウに移動し、すべての Cisco SD-WAN Manager ノードがクラスタに存在することを確認します。ノードが存在しない場合は、アプリケーションサーバーを再起動します。また、**[管理（Administration）]>[ディザスタリカバリ（Disaster Recovery）]** ウィンドウに移動し、表示されるノードがないことを確認します。

データセンターのディザスタリカバリを再登録する前に、データセンターをディザスタリカバリから削除する必要があります。

管理者トリガーフェールオーバーの実行

管理者トリガーフェールオーバーを実行するには、次の手順に従います。

（注） スタンバイクラスタは、アクティブになると他のクラスタから ZTP 設定を継承しなくなります。フェールオーバーが完了したら、「Start the Enterprise ZTP Server」の説明に従って、新しいアクティブクラスタの ZTP を有効にします。

1. プライマリクラスタ内の Cisco SD-WAN Manager デバイスからテンプレートをデタッチします。
2. スイッチオーバー中にデバイスが切り替わらないように、プライマリ Cisco SD-WAN Manager クラスタのトンネルインターフェイスをシャットダウンします。
3. セカンダリクラスタ上の Cisco SD-WAN Manager システムから、**[管理（Administration）]**、> **[ディザスタリカバリ（Disaster Recovery）]** の順に選択します。
4. データの複製が完了するのを待ってから、[プライマリにする（Make Primary）] をクリックします。

   デバイスとコントローラはセカンダリクラスタに収束し、セカンダリクラスタがプライマリクラスタの役割を担います。このプロセスが完了すると、元のプライマリクラスタはセカンダリクラスタのロールを引き継ぎます。その後、新しいプライマリクラスタから新しいセカンダリクラスタにデータが複製されます。

元のプライマリクラスタに戻すには、前述の手順を繰り返します。

ディザスタリカバリ操作

このセクションでは、さまざまな状況でディザスタリカバリを実行する方法について説明します。

プライマリ Cisco SD-WAN Manager クラスタの損失

プライマリ Cisco SD-WAN Manager クラスタがダウンした場合は、次の手順に従ってディザスタリカバリを実行します。

1. セカンダリクラスタ上の Cisco SD-WAN Manager システムから、**[管理（Administration）]**、> **[ディザスタリカバリ（Disaster Recovery）]** の順に選択します。
2. [プライマリにする（Make Primary）] をクリックします。

   デバイスとコントローラはセカンダリクラスタに収束し、セカンダリクラスタがプライマリクラスタの役割を担います。

   元のプライマリクラスタが回復してオンラインに戻ると、セカンダリクラスタのロールが引き継がれ、プライマリクラスタからのデータの受信が開始されます。

プライマリデータセンターの損失

プライマリ データセンター クラスタがダウンした場合は、次の手順に従ってディザスタリカバリを実行します。

1. セカンダリクラスタ上の Cisco SD-WAN Manager システムから、**[管理（Administration）]**、> **[ディザスタリカバリ（Disaster Recovery）]** の順に選択します。
2. [プライマリにする（Make Primary）] をクリックします。

スイッチオーバープロセスが開始されます。このプロセスでは、セカンダリデータセンターの Cisco SD-WAN Validator のみが新しい有効な Cisco SD-WAN Manager リストで更新されます。オンラインのデバイスとコントローラはセカンダリクラスタに収束し、セカンダリクラスタがプライマリクラスタの役割を担います。

元のプライマリデータセンターが回復し、コントローラを含むすべての VM がオンラインに戻ると、コントローラは新しい有効な Cisco SD-WAN Manager に更新され、新しいプライマリ Cisco SD-WAN Manager クラスタに収束します。元のプライマリクラスタはセカンダリクラスタの役割を担い、プライマリクラスタからのデータの受信が開始されます。

プライマリ Cisco SD-WAN Manager クラスタの部分的な損失

プライマリ Cisco SD-WAN Manager クラスタの部分的な損失が発生した場合は、セカンダリクラスタに切り替えるのではなく、プライマリクラスタの回復を試みることを推奨します。

N 個のノードを持つクラスタは、（N/2）+1 個のノードが動作している場合に動作していると見なされます。

N 個のノードを持つクラスタは、（N/2）+1 個以上のノードが失われた場合に読み取り専用になります。

データセンター間のエンタープライズネットワークの損失

データセンター間でリンク障害が発生したものの、プライマリデータセンターの WAN が動作している場合、データレプリケーションは失敗します。この状況では、データレプリケーションを再開できるようにリンクの回復を試みます。

スプリットブレインシナリオを回避するため、スイッチオーバー操作を実行しないでください。

Cisco SD-WAN Manager または Cisco Catalyst SD-WAN Validator 管理者パスワードの変更

Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a 以前のリリースでは、ディザスタリカバリの登録時に入力したユーザーパスワードを変更するために Cisco SD-WAN Manager を使用する場合は、まず Cisco SD-WAN Manager クラスタからディザスタリカバリの登録を解除し、パスワードを変更してから、クラスタのディザスタリカバリを再登録します。

ディザスタ リカバリ コンポーネント用ディザスタ リカバリ ユーザー パスワードの変更

ディザスタリカバリの登録時に、次のディザスタ リカバリ コンポーネントで使用する Cisco SD-WAN Manager または Cisco SD-WAN Validator ユーザーのユーザー名とパスワードを指定します。該当する各コンポーネントに同じユーザーの名前とパスワードを指定することも、さまざまなコンポーネントに異なるユーザーの名前とパスワードを指定することもできます。コン

ポーネントに指定するユーザー名とパスワードによって、コンポーネントのディザスタリカバリ操作にアクセスできるディザスタリカバリユーザーが識別されます。

- アクティブ（プライマリ）クラスタおよびスタンバイ（セカンダリ）クラスタ内の Cisco SD-WAN Manager サーバー。これらのコンポーネントでは、Cisco SD-WAN Manager ユーザーのパスワードが使用されます。
- 各 Cisco SD-WAN Validator。このコンポーネントでは、Cisco SD-WAN Validator ユーザーのパスワードが使用されます。

ディザスタリカバリユーザーの Cisco SD-WAN Manager または Cisco SD-WAN Validator パスワードを変更する場合は、このユーザーのディザスタ リカバリ コンポーネントのパスワードを新しいパスワードに変更する必要があります。

ディザスタリカバリユーザーのパスワードを変更するには、次の手順を実行します。

1. Cisco SD-WAN Manager メニューから、**[管理（Administration）]** > **[ディザスタリカバリ（Disaster Recovery）]** の順に選択します。
2. [ディザスタリカバリの一時停止（Pause Disaster Recovery）] をクリックしてから、表示される [ディザスタリカバリの一時停止（Pause Disaster Recovery）] ダイアログボックスで [OK] をクリックします。

   プライマリデータセンターとセカンダリデータセンター間のデータレプリケーションが停止し、このオプションが [ディザスタリカバリの再開（Resume Disaster Recovery）] に変わります。
3. [パスワードの管理（Manage Password）] をクリックします。
4. [パスワードの管理（Manage Password）] ウィンドウで、次のアクションを実行します。
   1. [アクティブクラスタ（Active Cluster）]をクリックし、表示される [パスワード（Password）] フィールドに、ディザスタリカバリユーザーの新しいアクティブ クラスタ パスワードを入力します。
   2. [スタンバイクラスタ（Standby Cluster）]をクリックし、表示される [パスワード（Password）] フィールドに、[アクティブクラスタ（Active Cluster）] フィールドに入力したものと同じディザスタリカバリユーザーのパスワードを入力します。
   3. [vBond] をクリックし、表示される各 [パスワード（Password）] フィールドに、ディザスタリカバリユーザーの新しい Cisco Catalyst SD-WAN Validator パスワードを入力します。各 Cisco SD-WAN Validator に 1 つの [パスワード（Password）] フィールドがあります。
   4. [Update] をクリックします。

      パスワードが更新され、[パスワードの管理（Manage Password）] ウィンドウが閉じます。
5. [ディザスタリカバリの再開（Resume Disaster Recovery）] をクリックしてから、表示される [ディザスタリカバリの再開（Resume Disaster Recovery）] ダイアログボックスで [OK] をクリックします。

データレプリケーションはプライマリサーバーとセカンダリサーバーの間で行われます。

ディザスタリカバリアラートの設定

サポートされている最小リリース：Cisco vManage リリース 20.9.1 Cisco vManage リリース 20.6.4 以降の 20.6.x リリース

ディザスタリカバリ ワークフローの障害または発生したイベントに関して、アラームと syslog メッセージを生成するように Cisco SD-WAN Manager アラートを設定できます。その後は、syslog 通知、イベント通知、およびウェブフックを介して、ディザスタリカバリのワークフローとイベントをモニターできます。

ディザスタリカバリアラートを設定するには、次の手順に従います。

1. プライマリクラスタ内の任意の Cisco SD-WAN Manager サーバーで、**[管理（Administation）] > [ディザスタリカバリ（Disaster Recovery）]** を選択し、[ディザスタリカバリの一時停止（Pause Disaster Recovery）] をクリックして、ディザスタリカバリを一時停止します。
2. プライマリクラスタ内の任意の Cisco SD-WAN Manager サーバーおよびセカンダリクラスタ内の任意の Cisco SD-WAN Manager サーバーで、**[管理（Administation）] > [設定（Settings）]** ウィンドウの [アラーム通知（Alarm Notifications）] を有効にします。

   『*Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*』[英語] の「Alarms」で「Enable Email Notifications」を参照してください。
3. ディザスタリカバリアラーム通知ルールを定義するには、プライマリクラスタ内の任意の Cisco SD-WAN Manager サーバーおよびセカンダリクラスタ内の任意の Cisco SD-WAN Manager サーバーで次のアクションを実行します。
   1. Cisco SD-WAN Manager のメニューから、**[モニター（Monitor）] > [ログ（Logs）]** の順に選択します。
   2. [アラーム（Alarms）] をクリックします。
   3. [Alarm Notifications] をクリックします。
   4. [Add Alarm Notification] をクリックします。
   5. [重大度（Severity）] ドロップダウンリストから、アラームが生成されるイベントの重大度を選択します。
   6. [アラーム名（Alarm Name）] ドロップダウンリストから、[ディザスタリカバリ（Disaster Recovery）] を選択します。
   7. 必要に応じてルールの他のオプションを設定します。

      詳細な手順については、『*Cisco Catalyst SD-WAN Monitor and Maintain Configuration Guide*』[英語] の「Alarms」で「Send Alarm Notifications」を参照してください。

8. [デバイスの選択（Select Devices）] エリアで、[カスタム（Custom）] をクリックします。
9. [使用可能なデバイス（Available Devices）] リストで対応するデバイスをクリックしてから、矢印をクリックしてデバイスを [選択したデバイス（Selected Devices）] リストに移動させることで、ディザスタリカバリアラームが生成される Cisco SD-WAN Manager サーバーを選択します。
10. [Add]をクリックします。

4. プライマリクラスタ内の任意の Cisco SD-WAN Manager サーバーで、**[管理（Administration）] > [ディザスタリカバリ（Administration Disaster Recovery）]** を選択し、[ディザスタリカバリの再開（Resume Disaster Recovery）] をクリックして、ディザスタリカバリを再開します。

ディザスタリカバリアラートを設定した後、必要に応じて、プライマリクラスタおよびセカンダリクラスタ内の各 Cisco SD-WAN Manager サーバーから、ローカルデバイスおよびリモートデバイスへの syslog メッセージのロギングを設定します。手順については、『Cisco Catalyst SD-WAN*Systems and Interfaces Configuration Guide*』[英語] の「Configure System Logging Using CLI」で、「Log Syslog Messages to a Local Device」および「Log Syslog Messages to a Remote Device」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。