



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 クラスター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 \(3 ページ\)](#)
- [アーキテクチャの概要 \(3 ページ\)](#)
- [前提条件 \(4 ページ\)](#)
- [ベストプラクティスと推奨事項 \(5 ページ\)](#)
- [ディザスタリカバリの有効化 \(6 ページ\)](#)
- [ディザスタリカバリの登録 \(6 ページ\)](#)
- [ディザスタリカバリ登録の確認 \(7 ページ\)](#)
- [ディザスタリカバリの削除 \(8 ページ\)](#)
- [管理者トリガーフェールオーバーの実行 \(8 ページ\)](#)
- [ディザスタリカバリ操作 \(9 ページ\)](#)
- [Cisco SD-WAN Manager または Cisco Catalyst SD-WAN Validator 管理者パスワードの変更 \(10 ページ\)](#)
- [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 \(10 ページ\)](#)
- [ディザスタリカバリアラートの設定 \(12 ページ\)](#)

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。

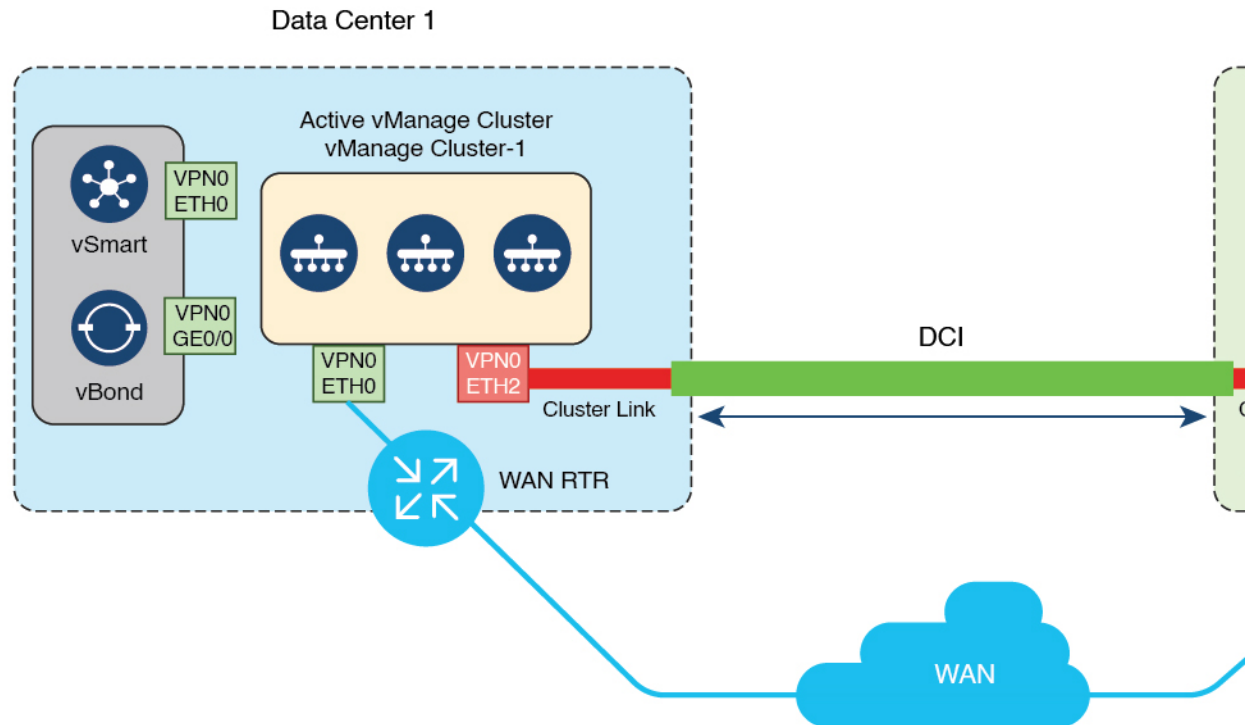
ディザスタリカバリは、管理者トリガー型のフェールオーバープロセスを提供します。ディザスタリカバリを登録すると、データは、プライマリとセカンダリの Cisco SD-WAN Manager クラスタ間で自動的に複製されます。必要に応じて、セカンダリクラスタへのフェールオーバーを手動で実行します。

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（VPN0）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り得てください。
- 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 - 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 (VPN0) 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리를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리를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してい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리를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一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 (Administration)]** > **[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 (Administration)]** > **[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。