



ディザスタリカバリの実装

- [概要 \(1 ページ\)](#)
- [前提条件 \(5 ページ\)](#)
- [監視サイトの設定 \(9 ページ\)](#)
- [ディザスタリカバリの設定 \(11 ページ\)](#)
- [フェールオーバー：概要 \(22 ページ\)](#)
- [ディザスタリカバリシステムの一時的停止 \(26 ページ\)](#)
- [システムへの再参加 \(28 ページ\)](#)
- [バックアップおよび復元の検討事項 \(31 ページ\)](#)
- [ディザスタリカバリイベントの通知 \(31 ページ\)](#)
- [ディザスタリカバリシステムのトラブルシューティング \(32 ページ\)](#)

概要

ディザスタリカバリは、ネットワークのダウンタイムに対する保護策として追加の冗長性レイヤを提供する Cisco DNA Center の高可用性 (HA) に基づいて構築されます。HA では、クラスタノードに障害が発生したときに、運用を接続されたクラスタノードに切り替えることで対処します。ディザスタリカバリでは、クラスタに障害が発生したときに、ネットワーク管理作業を接続されたクラスタ (転送先サイト) に移すことで対処します。

Cisco DNA Center のディザスタリカバリの実装は、メインサイト、リカバリサイト、および監視サイトの 3 つのコンポーネントで構成されます。メインサイトとリカバリサイトは、常にアクティブまたはスタンバイのいずれかの役割を担います。アクティブサイトでネットワークが管理され、アクティブサイトで更新されたデータおよびマネージドサービスの最新のコピーがスタンバイサイトで維持されます。アクティブサイトがダウンすると、Cisco DNA Center で自動的にフェールオーバーが開始され、スタンバイサイトを新しいアクティブサイトにするための必要なタスクが実行されます。

実稼働環境でディザスタリカバリを設定して使用方法については、この章のトピックを参照してください。

主な用語

次に、Cisco DNA Center のディザスタリカバリの実装について理解する上で重要な用語を示します。

- **メインサイト**：ディザスタリカバリシステムを設定するときに設定する1つ目のサイト。デフォルトでは、ネットワークを管理するアクティブサイトとして動作します。システムでサイトを設定する方法については、[ディザスタリカバリの設定 \(11 ページ\)](#) を参照してください。
- **リカバリサイト**：ディザスタリカバリシステムを設定するときに設定する2つ目のサイト。デフォルトでは、システムのスタンバイサイトとして機能します。
- **監視サイト**：ディザスタリカバリシステムを設定するときに設定する3つ目のサイト。このサイトは、仮想マシンまたは別のサーバにあり、データやマネージドサービスの複製には関与しません。このサイトには、現在アクティブなサイトにディザスタリカバリタスクを実行するために必要なクォーラムを割り当てる役割があります。これにより、サイトで障害が発生した場合のスプリットブレイン状況を回避できます。この状況は、2メンバのシステムでサイトが相互に通信できない場合に発生する可能性があります。その場合、両方のサイトがそれぞれアクティブになろうとし、アクティブサイトが2つになります。Cisco DNA Center では、アクティブサイトが常に1つだけになるように、監視サイトを使用してアクティブサイトとスタンバイサイトを調停します。監視サイトの要件については、[前提条件 \(5 ページ\)](#) を参照してください。
- **登録**：ディザスタリカバリシステムにサイトを追加するには、最初にメインサイトのVIPなどの情報を提供してシステムに登録する必要があります。リカバリサイトまたは監視サイトを登録する際は、メインサイトの登録時に生成されるトークンも提供する必要があります。詳細については、[ディザスタリカバリの設定 \(11 ページ\)](#) を参照してください。
- **アクティブ設定**：サイトをアクティブサイトとして確立するプロセス。該当するマネージドサービスのポートの公開などのタスクが含まれます。
- **アクティブサイト**：現在ネットワークを管理しているサイト。このサイトのデータはCisco DNA Center によってスタンバイサイトに継続的に複製されます。
- **スタンバイ設定**：サイトをスタンバイサイトとして確立するプロセス。アクティブサイトのデータの複製の設定やスタンバイサイトのネットワークを管理するサービスの無効化などのタスクが含まれます。
- **スタンバイ準備完了**：分離されたサイトがスタンバイサイトになるための前提条件を満たすと、Cisco DNA Center によってこの状態に移行されます。このサイトをシステムのスタンバイサイトとして確立するには、[Action] 領域で [Rejoin] をクリックします。
- **スタンバイサイト**：アクティブサイトのデータおよびマネージドサービスの最新のコピーを保持するサイト。アクティブサイトがダウンすると、フェールオーバーが開始され、スタンバイサイトにアクティブサイトの役割が引き継がれます。



(注) フェールオーバー後はアシュアランスが再起動され、新しいアクティブサイトで新規のデータセットが処理されます。アシュアランスデータの履歴は前のアクティブサイトから移行されません。

- フェールオーバー：Cisco DNA Center では2種類のフェールオーバーがサポートされません。
 - システムトリガー：アクティブサイトがダウンしたことがわかった時点で、スタンバイサイトを新しいアクティブサイトとして確立するための必要なタスクがCisco DNA Centerで自動的に実行されます。これらのタスクは、[イベントタイムラインのモニタリング](#)でモニタできます。
 - 手動：手動でフェールオーバーを開始して現在のスタンバイサイトを新しいアクティブサイトとして指定できます。詳細については、[手動フェールオーバーの開始 \(22 ページ\)](#)を参照してください。
- 分離：フェールオーバーの際に前のアクティブサイトがディザスタリカバリシステムから切り離されます。Cisco DNA Center のサービスが一時停止され、仮想 IP アドレス (VIP) のアドバタイズが停止します。その状態で、スタンバイサイトを新しいアクティブサイトとして確立するための必要なタスクがCisco DNA Center で実行されます。
- 一時停止：システムを構成するサイトを切り離してデータとサービスの複製を停止するために、一時的にディザスタリカバリシステムを停止します。詳細については、[ディザスタリカバリシステムの一時的停止 \(26 ページ\)](#)を参照してください。
- 再参加：フェールオーバーの発生後にスタンバイ準備完了または一時停止状態のサイトをディザスタリカバリシステムに新しいスタンバイサイトとして追加するには、**[Disaster Recovery]** > **[Monitoring]** タブの **[Action]** 領域で **[Rejoin]** ボタンをクリックします。また、現在一時停止しているディザスタリカバリシステムを再起動する場合もこのボタンをクリックします。
- DR のアクティブ化：システムのアクティブサイトとスタンバイサイトを作成するユーザ始動型の操作。この操作では、クラスタ内通信を設定し、サイトがディザスタリカバリの前提条件を満たしていることを確認し、2つのサイト間でデータを複製します。
- 登録解除：ディザスタリカバリシステム用に設定した3つのサイトを削除するには、**[Action]** 領域で **[Deregister]** ボタンをクリックします。前に入力したサイト設定を変更するには、この操作を実行する必要があります。
- 再試行：前に失敗したアクションを再度実行するには、**[Action]** 領域で **[Retry]** ボタンをクリックします。

ディザスタリカバリの GUI のナビゲーション

次の表に、Cisco DNA Center のディザスタリカバリの GUI を構成するコンポーネントとその機能を示します。

The screenshot shows the Cisco DNA Center interface for Disaster Recovery. It includes a navigation menu with 'Monitoring' (1) and 'Configure' (4) tabs. The 'Logical Topology' (2) view displays a network diagram with three sites: Main Site (Active), Witness Site (Up), and Recovery Site (Standby). A status box (5) indicates 'Status: Up and Running'. An event timeline (3) is visible at the bottom. A legend (6) defines various status icons. Manual Failover and Pause buttons (7) are at the bottom right.

引き出し線	説明
1	<p>[Monitoring] タブ：次の操作を実行する場合にクリックします。</p> <ul style="list-style-type: none"> システムを構成するサイトのトポロジを表示します。 システムの現在のステータスを確認します。 ディザスタリカバリタスクを実行します。 現在までに完了しているタスクのリストを表示します。
2	<p>[Logical Topology]：サイトとそのメンバの現在のステータスを示すシステムのトポロジが表示されます。サイトの状態については、システムおよびサイトの状態（18 ページ）を参照してください。</p>
3	<p>[Event Timeline]：システムのディザスタリカバリタスクについて、現在進行中のタスクと完了したタスクがすべて表示されます。詳細については、イベントタイムラインのモニタリング（16 ページ）を参照してください。</p>
4	<p>[Configure] タブ：ディザスタリカバリシステムのサイト間の接続を確立するために必要な設定を入力する場合にクリックします。詳細については、ディザスタリカバリの設定（11 ページ）を参照してください。</p>
5	<p>[Status] 領域：システムの現在のステータスを示します。システムの状態については、システムおよびサイトの状態（18 ページ）を参照してください。</p>

引き出し線	説明
6	[Legend] : トポロジのアイコンの意味を示します。凡例を表示するには、[Disaster Recovery] ページの右下隅にある  をクリックします。
7	[Action] 領域 : 現在開始できるディザスタリカバリタスクが表示されます。選択できるタスクは、サイトの設定が完了しているかどうかやシステムのステータスによって異なります。

前提条件

実稼働環境でディザスタリカバリを有効にする前に、次の前提条件を満たしていることを確認してください。



重要

最新の Cisco DNA Center 2.1.2.x リリースにアップグレードする場合は、アップグレード後にディザスタリカバリが適切に機能するように、いくつかの手順を実行する必要があります。詳細については、「[アップグレード後のディザスタリカバリの設定 \(8 ページ\)](#)」を参照してください。

一般的な前提条件

- ディザスタリカバリに、合計7台のノードで構成された3つのシステムを割り当てておきます。1つ目はメインサイトとして機能する3台のノードクラスタ、2つ目はリカバリサイトとして機能する3台のノードクラスタ、3つ目は監視サイトとして機能するシステム（仮想マシン上に常駐）となります。
- Cisco DNA Center アプライアンスでエンタープライズポートのインターフェイスにVIPを設定しておきます。ディザスタリカバリではサイト内通信にエンタープライズネットワークを使用するため、この設定が必要になります。『[Cisco DNA Center Second-Generation Appliance Installation Guide](#)』で、次のトピックを参照してください。
 - エンタープライズポートの詳細については、「[Interface Cable Connections](#)」のトピックを参照してください。
 - エンタープライズポートの設定の詳細については、「[Configure the Primary Node Using the Maglev Wizard](#)」または「[Configure the Primary Node Using the Browser-Based Wizard](#)」のトピックを参照してください。
- ディザスタリカバリタスクを実行できるように、ネットワーク管理者ユーザを割り当てておきます。この機能には、この特権レベルのユーザしかアクセスできません。
- 次の両サイトを接続するリンクが1GBリンクで、RTT遅延が200ミリ秒以下であることを確認しておきます。
 - メインサイトとリカバリサイト

- メインサイトと監視サイト
- リカバリサイトと監視サイト
- サードパーティ証明書を生成し、メインサイトとリカバリサイトの両方にインストールしておきます。これがインストールされていないと、サイトの登録は失敗します。



(注) Cisco DNA Center は、登録プロセス中にこの証明書を監視サイトに自動的にコピーします。

それらのサイトで使用するすべての IP アドレスと完全修飾ドメイン名 (FQDN) が証明書に含まれていることを確認してください。サードパーティ証明書を生成する方法については、『Cisco DNA Center Security Best Practices Guide』の「[Generate a Certificate Request Using Open SSL](#)」を参照してください。

メインサイトとリカバリサイトの前提条件

- メインサイトとリカバリサイトの両方について、同じ数のコアを持つ 3 つの Cisco DNA Center アプライアンスで構成する必要があります。つまり、1 つのサイトを 3 つの 56 コア第 2 世代アプライアンスで構成し、もう一方のサイトを 3 つの 112 コアアプライアンスで構成することはできません。次の表に、ディザスタリカバリをサポートするアプライアンスとそれぞれのシスコ製品番号を示します。

第 2 世代の Cisco DNA Center アプライアンス。Cisco UCS C220 M5 小型フォームファクタ (SFF) シャーシまたは Cisco UCS C480 M5 シャーシのいずれかをベースとします。	56 コアアプライアンス：シスコ製品番号 DN2-HW-APL-L
	56 コアプロモーションアプライアンス：シスコ製品番号 DN2-HW-APL-L-U
	112 コアアプライアンス：シスコ製品番号 DN2-HW-APL-XL
	112 コアプロモーションアプライアンス：DN2-HW-APL-XL-U

- メインサイトとリカバリサイトの両方で、高可用性 (HA) を設定して有効にしておきます。これが設定されていないと、これらのサイトの登録は失敗します。詳細については、最新の『Cisco DNA Center High Availability Guide』を参照してください。
- ボーダー ゲートウェイ プロトコル (BGP) を使用してシステムの仮想 IP アドレスルートをアドバタイズする場合は、メインサイトとリカバリサイトの各ネイバールータでシステムのエンタープライズ仮想 IP アドレスを設定する必要があります。入力する必要がある設定は、次の例のようになります。

内部 BGP (iBGP) の設定例

```
router bgp 64555
  bgp router-id 10.30.197.57
  neighbor 172.25.119.175 remote-as 64555
```

```
neighbor 172.25.119.175 update-source 10.30.197.57
neighbor 172.25.119.175 next-hop-self
```

引数の説明

- 64555 は、ネイバルータのローカルおよびリモート AS 番号です。
- 10.30.197.57 はネイバルータの IP アドレスです。
- 172.25.119.175 は、システムのエンタープライズ仮想 IP アドレスです。

外部 BGP (eBGP) の設定例

```
router bgp 62121
  bgp router-id 10.30.197.57
  neighbor 172.25.119.175 remote-as 64555
  neighbor 172.25.119.175 update-source 10.30.197.57
  neighbor 172.25.119.175 next-hop-self
  neighbor 172.25.119.175 ebgp-multihop 255
```

引数の説明

- 62121 は、ネイバルータのローカル AS 番号です。
 - 64555 は、ネイバルータのリモート AS 番号です。
 - 10.30.197.57 はネイバルータの IP アドレスです。
 - 172.25.119.175 は、システムのエンタープライズ仮想 IP アドレスです。
- BGP ルートアドバタイズメントを有効にする場合（前の項目を参照）、パフォーマンスを向上させるために Cisco DNA Center へのルートをフィルタリングすることを推奨します。フィルタリングを行うには、次の設定を入力します。

```
neighbor system's-Enterprise-virtual-IP-address route-map DENYALL out
!
ip prefix-list deny-all seq 5 deny 0.0.0.0/0 le 32
!
route-map DENYALL permit 10
match ip address prefix-list deny-all
```

監視サイトの前提条件

- 監視サイトをホストする仮想マシンが、最低でも 2.1 GHz コアと 2 つの仮想 CPU、4 GB の RAM、および 10 GB のハードドライブ領域を搭載した VMware ESXi ハイパーバイザバージョン 6.0 以降を実行していることを確認しておきます。
- 監視サイトをメインサイトおよびリカバリサイトとは別の場所に用意し、それらの両方のサイトから到達可能であることを確認しておきます。
- 監視サイトからアクセス可能な NTP サーバを設定しておきます。この NTP サーバをメインサイトとリカバリサイトで使用される NTP サーバと同期する必要があります。

アップグレード後のディザスタリカバリの設定

システムを最新の Cisco DNA Center 2.1.2.x バージョンにアップグレードした後でディザスタリカバ리를正常に設定するには、状況に応じて次の手順を実行します。

シナリオ 1

このシナリオでは、アプライアンスに最初にインストールされた Cisco DNA Center のバージョンは 1.3.x でしたが、最新の 2.1.2.x バージョンにアップグレードする必要があります。ディザスタリカバリは Cisco DNA Center 1.3.x からアップグレードされたアプライアンスでは正しく機能しないため、次の手順を実行してこの問題を回避する必要があります。

ステップ 1 アプライアンスで、現在の Cisco DNA Center のバージョンから最新の 2.1.2.x バージョンにアップグレードします（『[Cisco DNA Center Upgrade Guide](#)』を参照）。

ステップ 2 データをバックアップします（[今すぐデータをバックアップ](#)を参照）。

次の手順でアプライアンスと仮想マシンのデータが完全に消去されるため、バックアップファイルがリモートサーバにあることを確認します。

ステップ 3 アプライアンスに最新の Cisco DNA Center 2.1.2.x の ISO イメージをインストールします（『[Cisco DNA Center Second-Generation Appliance Installation Guide](#)』の「Reimage the Appliance」を参照）。

ステップ 4 バックアップファイルからデータを復元します（[バックアップからデータを復元](#)を参照）。

ステップ 5 ディザスタリカバリシステムの設定に進みます。

シナリオ 2

このシナリオでは、アプライアンスに最初にインストールされた Cisco DNA Center のバージョンは 2.1.x 以前でしたが、最新の 2.1.2.x バージョンにアップグレードする必要があります。また、これらのアプライアンスではディザスタリカバリが有効であり、動作可能です。次の手順を実行します。

ステップ 1 システムの一時停止（[26 ページ](#)）。

ステップ 2 メインサイトとリカバリサイトのアプライアンスを最新の 2.1.2.x バージョンにアップグレードします。『[Cisco DNA Center Upgrade Guide](#)』の「Upgrade to Cisco DNA Center 2.1.2.x」の章を参照してください。

ステップ 3 現在の監視サイトの置換（[15 ページ](#)）。

ステップ 4 システムへの再参加（[28 ページ](#)）。

シナリオ 3

このシナリオでは、アプライアンスに最初にインストールされた Cisco DNA Center のバージョンは 2.1.x 以前でしたが、最新の 2.1.2.x バージョンにアップグレードする必要があります。シ

ナリオ 2 とは異なり、これらのアプライアンスではディザスタリカバリが設定されていません。次の手順を実行します。

ステップ 1 監視サイトの設定 (9 ページ)。

ステップ 2 ディザスタリカバリの設定 (11 ページ)。

監視サイトの設定

ディザスタリカバリシステムの監視サイトとして機能する仮想マシンを設定するには、次の手順を実行します。

ステップ 1 監視サイトで実行している Cisco DNA Center のバージョンに固有の OVF パッケージをダウンロードします。

a) <https://software.cisco.com/download/home/286316341/type> を開きます。

(注) この URL にアクセスするには、Cisco.com のアカウントが必要です。アカウントの作成方法については、次のページを参照してください。 <https://www.cisco.com/c/en/us/about/help/registration-benefits-help.html>

b) [Select a Software Type] 領域で、Cisco DNA Center のソフトウェアリンクをクリックします。

[Software Download] ページが更新され、Cisco DNA Center の最新リリースで使用可能なソフトウェアのリストが表示されます。

c) 次のいずれかを実行します。

- 必要な OVF パッケージ (*.ova) がすでに表示されている場合は、その [Download] アイコンをクリックします。
- [Search] フィールドに関連するバージョン番号を入力し、ナビゲーションペインでそのリンクをクリックして、該当するバージョンの OVF パッケージに対応する [Download] アイコンをクリックします。

ステップ 2 このパッケージを、VMware vSphere 6.0 または 6.5 を実行しているローカルマシンにコピーします。

ステップ 3 vSphere クライアントで、[File] > [Deploy OVF Template] を選択します。

ステップ 4 [Deploy OVF Template] ウィザードを完了します。

a) ウィザードの [Source] 画面で、次の手順を実行します。

1. [参照 (Browse)] をクリックします。
2. 監視サイトの OVF パッケージ (.ova) まで移動します。
3. [Open] をクリックします。

4. [Deploy from a file or URL] フィールドで、パッケージのパスが表示されていることを確認し、[Next >] をクリックします。

ウィザードの [OVF Template Details] 画面が開きます。

- b) **Next >** をクリックします。
- c) ウィザードの [Name and Location] 画面で、次の手順を実行します。
 - [Name] フィールドに、パッケージに対して設定する名前を入力します。
 - [Inventory Location] フィールドで、パッケージを配置するフォルダを選択します。
 - **Next >** をクリックします。

ウィザードの [Host/Cluster] 画面が開きます。

- d) 展開したテンプレートを実行するホストまたはクラスタをクリックし、[Next >] をクリックします。
ウィザードの [Storage] 画面が開きます。
- e) 仮想マシンファイルを配置するストレージドライブをクリックし、[Next >] をクリックします。
ウィザードの [Disk Format] 画面が開きます。
- f) [Thick Provision] オプションボタンをクリックし、[Next >] をクリックします。
- g) ウィザードの [Network Mapping] 画面で、次の手順を実行してから [Next >] をクリックします。
 1. [Destination Networks] 列にリストされている IP アドレスをクリックします。
 2. 表示されたドロップダウンリストで、展開したテンプレートで使用するネットワークを選択します。

ウィザードの [Ready to Complete] 画面が開き、入力したすべての設定が表示されます。

- h) [Power on after deployment] チェックボックスをオンにし、[Finish] をクリックします。
- i) [Deployment Completed Successfully] ダイアログボックスが表示されたら、[Close] をクリックします。

ステップ 5 監視サイトのネットワーク設定を入力します。

- a) 次のいずれかを実行して、作成した仮想マシンのコンソールを開きます。
 - vSphere クライアントのリストから仮想マシンを右クリックし、[Open Console] を選択します。
 - vSphere クライアントのメニューで [Open Console] アイコンをクリックします。

[Witness User Configuration] ウィンドウが表示されます。

- b) 管理者ユーザ (*maglev*) のパスワードを入力して確認用にもう一度入力し、N を押して次に進みます。
- c) 次の設定を入力し、N を押して次に進みます。
 - IP アドレス
 - 仮想マシンの IP アドレスに関連付けられているネットマスク
 - デフォルトゲートウェイの IP アドレス

- (オプション) 優先 DNS サーバの IP アドレス
- d) NTP サーバのアドレスまたはホスト名を 1 つ以上入力し (複数の場合はカンマで区切る)、S を押し て設定を送信します。監視サイトの設定が開始されます。
1 つ以上の NTP アドレスまたはホスト名が必要です。
- e) 監視サイトに設定した IP アドレスに SSH ポート 2222 を使用してログインし、設定が完了したことを 確認します。

ディザスタリカバリの設定

ディザスタリカバリシステムを使用するように設定するには、次の手順で説明するタスクを実行します。



(注) システムを設定する場合、いくつかのオプションがあります。

- ボーダー ゲートウェイ プロトコル (BGP) ルートアドバタイジングを使用する仮想 IP アドレスを指定できます。
- 仮想 IP アドレスを設定しないように選択することもできます。このオプションを選択した場合は、デバイスの可制御性を有効にして、フェールオーバー発生後にサイトの仮想 IP アドレスを再設定できるようにする必要があります。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。

デフォルトでは、[Monitoring] タブが選択されています。

ステップ 2 メインサイトを登録します。

(注) 手順 2d の前の任意の時点で、[Reset] をクリックして、入力したすべての設定をクリアできます。メインサイトを登録する前に、手順 2 を繰り返して正しい設定を入力する必要があります。

a) [Configure] タブをクリックします。

[Main Site] オプションボタンはすでに選択されている必要があります。

b) [Setting up this cluster] 領域に次の情報を入力します。

- [Main Site VIP] : アクティブサイトのクラスタノードとエンタープライズネットワークの間のトラフィックを管理する仮想 IP アドレス。メインサイトのエンタープライズ仮想 IP アドレスをドロップダウンリストから選択します。

- [Recovery Site VIP] : リカバリサイトのクラスタノードとエンタープライズ ネットワークの間のトラフィックを管理するエンタープライズ仮想 IP アドレス。
- [Witness Site IP] : 監視サイトの仮想マシンとエンタープライズ ネットワークの間のトラフィックを管理する IP アドレス。

重要 入力したアドレスが現在到達可能であることを確認します。到達できない場合、システムのサイトの登録は失敗します。

c) [Additional Protocols] 領域に次の情報を入力します。

- [Routing Protocol] : BGP を使用してシステムの仮想 IP アドレスルートをアドバタイズするかどうかを指定します。
- [Border Gateway Protocol Type] : [Border Gateway Protocol (BGP)] オプションボタンをクリックした場合、BGP ピアが相互に外部 (外部 BGP (eBGP)) セッションを確立するか、内部 (内部 BGP (iBGP)) セッションを確立するかを指定します。
- [Enterprise VIP for Disaster Recovery] : このフローティング仮想 IP アドレスを設定しておく、ネットワークのアクティブサイトとして現在動作しているサイトに自動的に切り替えて運用されます。このアドレスは、ディザスタリカバリシステムとエンタープライズネットワークの間のトラフィックを管理します。

(注) [Border Gateway Protocol (BGP)] オプションを選択した場合は、このフィールドに値を入力する必要があります。

- [Main Site Router Settings] : [Border Gateway Protocol (BGP)] オプションを選択した場合は、メインサイトのリモートルータの IP アドレスと、そのローカルおよびリモートの自律システム (AS) 番号を入力します。追加のリモートルータを設定する場合は、[Add] (+) アイコンをクリックします。

(注) [iBGP] オプションを選択すると、Cisco DNA Center はローカル AS 番号をリモート AS 番号として入力した値に自動的に設定します。

- [Recovery Site Router Settings] : [Border Gateway Protocol (BGP)] オプションを選択した場合は、リカバリサイトのリモートルータの IP アドレスと、そのローカルおよびリモートの AS 番号を入力します。追加のリモートルータを設定する場合は、[Add] (+) アイコンをクリックします。

(注) [iBGP] オプションを選択すると、Cisco DNA Center はローカル AS 番号をリモート AS 番号として入力した値に自動的に設定します。

- (オプション) [Management VIP for Disaster Recovery] : これはフローティング仮想 IP アドレスであり、設定しておけばネットワークのアクティブサイトとして現在動作しているサイトに自動的に切り替えて運用されます。このアドレスは、ディザスタリカバリシステムと管理ネットワークの間のトラフィックを管理します。

(注) 管理仮想 IP アドレスを設定し、[Border Gateway Protocol (BGP)] オプションを選択した場合は、適切なリモートルータ情報を入力する必要があります (エンタープライズ仮想 IP アドレスの場合と同様)。

- d) [Action] 領域で、[Register] をクリックします。
[Disaster Recovery Registration] ダイアログが開きます。
- e) [Continue] をクリックします。
リカバリサイトおよび監視サイトをメインサイトに登録するために必要なトークンが生成されます。

ステップ3 [Supplement] 領域で、[Copy Token] をクリックします。

ステップ4 リカバリサイトを登録します。

(注) 手順4dの前の任意の時点で、[Reset] をクリックして、入力したすべての設定をクリアできます。
リカバリサイトを登録する前に、手順4を繰り返して正しい設定を入力する必要があります。

- a) [Supplement] 領域で [Recovery Site] リンクを右クリックします。新しいブラウザタブでページが開きます。
- b) 必要に応じて、適切なユーザ名とパスワードを入力してリカバリサイトにログインします。
[Disaster Recovery] ページに、[Recovery Site] オプションボタンがすでに選択された状態で [Configure] タブが開きます。
- (注) 手順2cで設定したエンタープライズVIPにブラウザから到達できない場合は、エンタープライズVIPをリカバリサイトの管理VIPに置き換えてURLを更新し、そのURLを開きます。

- c) 次の情報を入力します。
- [Main Site VIP] : アクティブサイトのクラスタノードとエンタープライズネットワークの間のトラフィックを管理する仮想IPアドレス。
 - [Recovery Site VIP] : リカバリサイトのクラスタノードとエンタープライズネットワークの間のトラフィックを管理する仮想IPアドレス。リカバリサイトのエンタープライズ仮想IPアドレスをドロップダウンリストから選択します。
 - 手順2で生成した登録トークン。
 - アクティブサイトのネットワーク管理者ユーザに対して設定されたユーザ名とパスワード。
- d) [Action] 領域で、[Register] をクリックします。
[Disaster Recovery Registration] ダイアログが開きます。
- e) [Continue] をクリックします。
メインサイトとリカバリサイトの接続が確立されると、トポロジでステータスが更新されます。

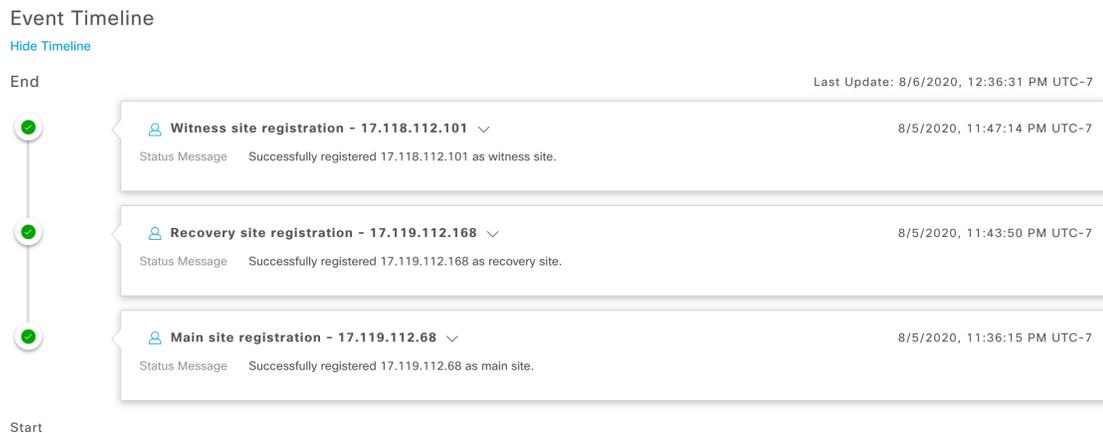
ステップ5 監視サイトを登録します。

- a) メインサイトのブラウザタブに戻ります。
- b) [Supplement] 領域で、[Copy Witness Login Cmmd] をクリックします。
- c) 監視サイトへのSSHコンソールを開き、コピーしたコマンドを貼り付けてログインします。
- d) 要求された場合は、デフォルトのユーザ (maglev) のパスワードを入力します。
- e) [Supplement] 領域に戻り、[Copy Witness Register Cmmd] をクリックします。

- f) SSH コンソールで、コピーしたコマンドを貼り付けます。
- g) <main_admin_user> をネットワーク管理者ユーザのユーザ名に置換してコマンドを実行します。
- h) 要求された場合は、ネットワーク管理者ユーザのパスワードを入力します。

ステップ 6 メインサイト、リカバリサイト、および監視サイトが正常に登録されていることを確認します。

- a) メインサイトのブラウザタブに戻り、[Monitoring] をクリックしてディザスタリカバリの [Monitoring] タブを表示します。
- b) [Logical Topology] 領域で、3 つのサイトが表示され、ステータスが [Registered] であることを確認します。
- c) [Event Timeline] 領域で、各サイトの登録がイベントとしてリストされ、各タスクが正常に完了したことを確認します。



ステップ 7 [Actions] 領域で [Activate] をクリックします。

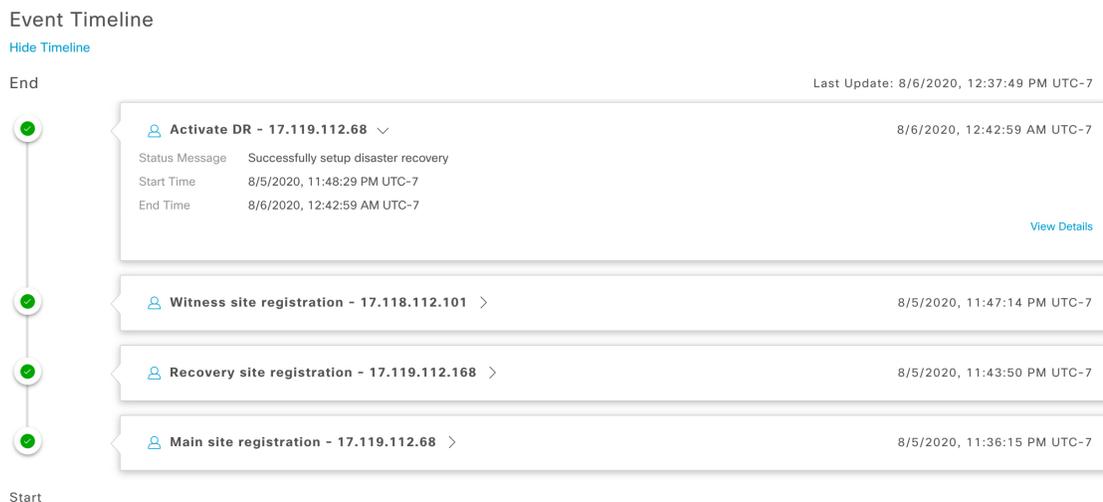
リカバリサイトに現在存在するすべてのデータが消去されることを示すダイアログが表示されます。

ステップ 8 ディザスタリカバリシステムの設定とメインサイトのデータのリカバリサイトへの複製を開始するには、[Continue] をクリックします。

(注) アクティブ化プロセスは、完了までに時間がかかる場合があります。進捗状況をモニタするには、イベントのタイムラインを表示します。

ステップ 9 Cisco DNA Center で必要なタスクが完了したら、システムが動作していることを確認します。

1. トポロジを表示し、それぞれのサイトのステータスが次のように表示されていることを確認します。
 - メインサイト : [Active]
 - リカバリサイト : [Standby]
 - 監視サイト : [Up]
2. イベントのタイムラインを表示し、[Activate DR] タスクが正常に完了したことを確認します。



3. メインサイトから ping を実行して、サイトに到達できることを確認します。

現在の監視サイトの置換

現在の監視サイトをアップグレードまたは置換する必要がある場合は、次の手順を実行します。

ステップ 1 現在の監視サイトにログインします。

- a) 監視サイトの SSH コンソールを開き、`ssh -p 2222 maglev@witness-site's-IP-address` コマンドを実行します。
- b) デフォルトのユーザ (maglev) のパスワードを入力します。

ステップ 2 `witness reset` コマンドを実行します。

ステップ 3 現在の監視サイトの仮想マシンを削除します。

ステップ 4 [監視サイトの設定 \(9 ページ\)](#) の説明に従って、新しい監視サイトの仮想マシンをインストールします。

ステップ 5 新しい監視サイトにログインします。

- a) 監視サイトの SSH コンソールを開き、`ssh -p 2222 maglev@witness-site's-IP-address` コマンドを実行します。
- b) デフォルトのユーザ (maglev) のパスワードを入力します。

ステップ 6 `witness reconnect` コマンドを実行します。

システムの登録解除

ディザスタリカバリシステムがアクティブ化された後、特定のサイトについて入力した設定の更新が必要になることがあります。この状況が発生した場合は、次の手順を実行します。この手順を実行すると、システム内のすべてのサイトについての現在の設定がクリアされることに注意してください。

ステップ 1 [Action] 領域で、[Pause DR] をクリックしてシステムの運用を一時停止します。

詳細については、「[システムの一時停止（26 ページ）](#)」を参照してください。

ステップ 2 [Action] 領域で、[Deregister] をクリックします。

Cisco DNA Center で以前にシステムのサイトについて設定した内容がすべて削除されます。

ステップ 3 適切な設定を入力してサイトを再登録し、システムを再度アクティブ化するには、[ディザスタリカバリの設定（11 ページ）](#) で説明されているタスクを実行します。

イベントタイムラインのモニタリング

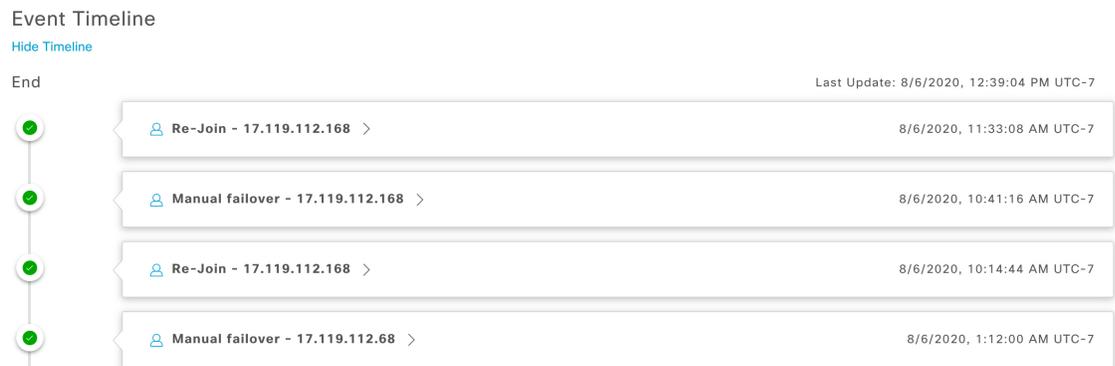
イベントのタイムラインから、現在実行されているディザスタリカバリタスクの進捗状況を追跡し、それらのタスクが完了したときに確認できます。タイムラインを表示するには、次の手順を実行します。

1. Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。

デフォルトでは、[Monitoring] タブが選択されています。

2. ページの下部までスクロールします。

システムに対する進行中のタスクと完了したタスクが、最新のタスク（完了時のタイムスタンプに基づく）から順番に降順で表示されます。Cisco DNA Center では、それぞれのタスクについて、システム (☑) またはユーザ (👤) のどちらによって開始されたかが示されます。



たとえば、システムの一部停止後の復元についてモニタするとします。この場合、復元プロセスの各タスクが開始されたときと完了したときに、Cisco DNA Center でイベントのタイムラインが更新されます。特定のタスクにおける処理の概要を表示するには、[>]をクリックします。

Event Timeline

[Hide Timeline](#)

End

Last Update: 8/6/2020, 12:42:01 PM UTC-7

The screenshot shows an event timeline with two tasks. The first task, 'Re-Join - 17.119.112.168', is expanded to show its details: 'Status Message: Successfully setup disaster recovery', 'Start Time: 8/6/2020, 10:44:57 AM UTC-7', and 'End Time: 8/6/2020, 11:33:08 AM UTC-7'. A 'View Details' link is visible at the bottom right of this task. The second task, 'Manual failover - 17.119.112.168', is collapsed and shows a right-pointing chevron (>).

タスクに対して [ViewDetails] リンクが表示されている場合は、そのリンクをクリックすると、完了した関連するサブタスクのリストが表示されます。

Event Timeline

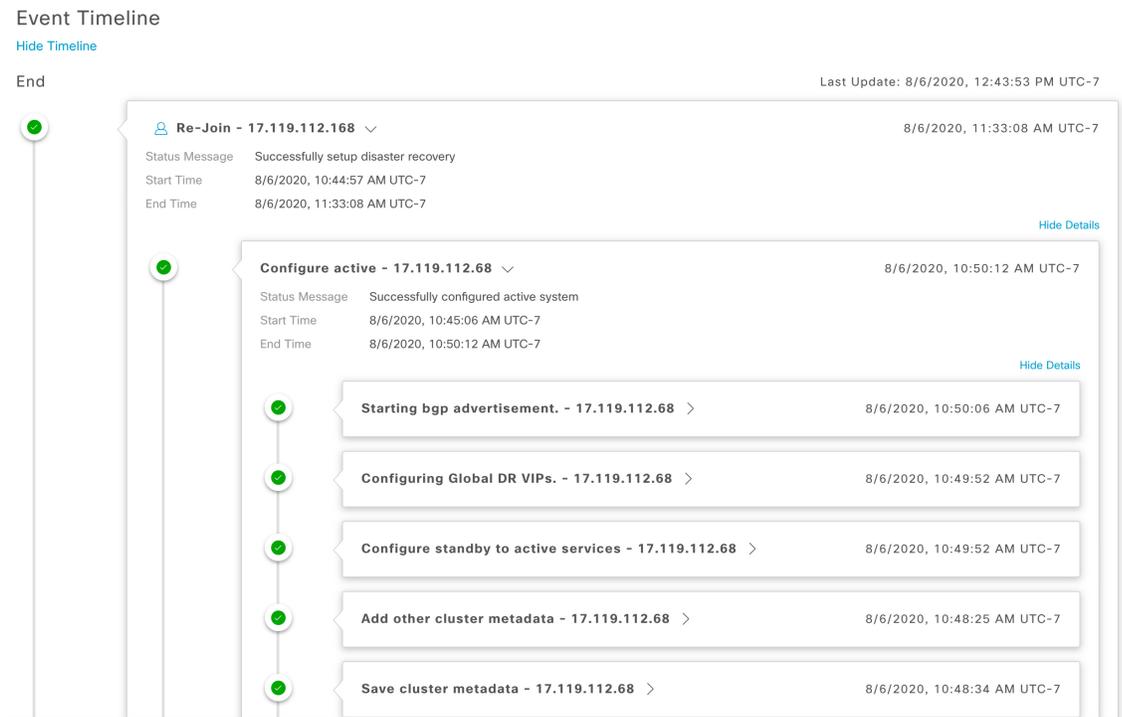
[Hide Timeline](#)

End

Last Update: 8/6/2020, 12:42:39 PM UTC-7

This screenshot shows the same event timeline as above, but with the 'Re-Join' task expanded further. It now displays two sub-tasks: 'Configure active - 17.119.112.68' and 'Configure standby - 17.119.112.168', each with its own start and end times. A 'Hide Details' link is visible at the bottom right of the 'Re-Join' task. The 'Manual failover' task remains collapsed.

タスクと同様に、[>] をクリックして特定のサブタスクの概要情報を表示できます。



システムおよびサイトの状態

次の表に、[Status] 領域に表示されるシステムの状態とトポロジに表示されるサイトの状態について、それぞれの状態の意味を示します。

表 1: ディザスタリカバリシステムの状態

状態	説明
未構成	新規に導入されたシステムです。ディザスタリカバリはまだ設定されていません。
Registered	アクティブサイト、スタンバイサイト、および監視サイトが登録され、登録に関するすべての検証チェックが正常に完了しました。3つのサイトの間で相互に通信できます。
の設定	この状態は、次のいずれかの状況を示しています。 <ul style="list-style-type: none"> [Action] 領域で [Activate DR] をクリックしました。アクティブサイトとスタンバイサイトの両方で複数のワークフローが開始されます。これらのワークフローのいずれかが失敗した場合、このサイトは [Registered] 状態に戻ります。 システムのアクティブサイトとスタンバイサイトを設定するために事前に実行するタスクが正常に完了しました。

状態	説明
Up	この状態は、次のいずれかの状況を示しています。 <ul style="list-style-type: none"> ディザスタリカバリが設定済みで、システムトリガーのフェールオーバーを開始できます。 ディザスタリカバリが設定されています。ただし、監視サイトが設定されていないか停止しているため、システムトリガーのフェールオーバーを開始できません。 スタンバイシステムが使用できず、データの複製が行われていません。 システムトリガーまたは手動のフェールオーバーが正常に完了しました。
Up (with no Failover)	システムは、次のいずれかの場合にこの状態になります。 <ul style="list-style-type: none"> アクティブサイトおよびスタンバイサイトと監視サイトの接続が失われている。 アクティブサイトおよび監視サイトとスタンバイサイトの接続が失われている。
Down	アクティブサイトが停止したことが検出され、ディザスタリカバリシステムでフェールオーバーが開始されましたが、フェールオーバーに失敗しました。システムがこの状態の場合は、問題を解決してから手動フェールオーバーを開始します。
Failover in progress	アクティブサイトが停止したことが検出され、ディザスタリカバリシステムでフェールオーバーがトリガーされました。
Deregistering	登録解除が進行中です。このプロセスが完了すると、すべての登録情報と関連するネットワーク設定がリセットされます。
Deregistered	メインサイト、リカバリサイト、および監視サイトがディザスタリカバリシステムから登録解除されています。
Pausing Disaster Recovery System	メンテナンスなどのアクティビティのために、ディザスタリカバリシステムを一時停止しています。
Disaster Recovery System Paused	ディザスタリカバリシステムが一時停止されました。現在はメインサイトとリカバリサイトが2つのスタンドアロンクラスタとして機能しています。サイト間のデータの複製は行われていません。システムを再起動してデータの複製を再開するには、[Rejoin] をクリックします。
Pausing Disaster Recovery Failed	ディザスタリカバリシステムの一時停止中にエラーが発生しました。
User intervention required	メインサイトとリカバリサイトの両方がオフラインになり、再起動されました。ただし、ディザスタリカバリシステムは切断された状態のままになっています。システムを一時停止してから再起動し、問題が解決したかどうかを確認します。

表 2: Active Site States

状態	説明
未構成	新規に導入されたサイトです。ディザスタリカバリの情報はまだありません。
Registered	このサイトがアクティブサイトとして指定されました。検証チェックと登録も正常に完了しています。
Configuring Active	サイトをアクティブサイトとして設定するためのワークフローを実行中です。
アクティブ	サイトをアクティブサイトまたはスタンバイサイトのいずれかとして設定するためのワークフローが正常に完了しました。
Failed to Configure	サイトをアクティブサイトとして設定するためのワークフローを完了できません。
アクティブ	このサイトがアクティブサイトとして正常に設定されました。
Isolating	このサイトをディザスタリカバリシステムから分離する処理を実行中です。これは、手動フェールオーバーを開始した後、それまでアクティブサイトとして機能していたサイトがオンラインに戻るとトリガーされます。
隔離 (Isolated)	このサイトがディザスタリカバリシステムから正常に分離されました。
Isolate Failed	このサイトをディザスタリカバリシステムから分離できません。
Down	自動ヘルスマニタで監視システムが停止していることが確認されたか、設定されている時間しきい値の間にシステムから正常性の更新情報が提供されませんでした。
Pausing Active	メンテナンスなどのアクティビティのために、アクティブサイトを一時停止しています。
Active Paused	アクティブサイトが一時停止されました。現在はアクティブサイトとスタンバイサイトが2つのスタンドアロンクラスタとして機能し、サイト間のデータの複製は行われていません。システムを再起動してデータの複製を再開するには、[Rejoin]をクリックします。
Pausing Active Failed	アクティブサイトの一時停止中にエラーが発生しました。

表 3: スタンバイサイトの状態

状態	説明
未構成	新規に導入されたサイトです。ディザスタリカバリの情報はまだありません。
Registered	このサイトがスタンバイサイトとして指定され、検証チェックが正常に完了しました。
Configuring Standby	サイトをスタンバイサイトとして設定するためのワークフローを実行中です。

状態	説明
Standby	サイトをスタンバイサイトとして設定するためのワークフローが正常に完了しました。
Failed to Configure	サイトをスタンバイサイトとして設定するためのワークフローを完了できません。
パッシブ	このサイトがスタンバイサイトとして正常に設定されました。
Activating passive	システムトリガーまたは手動のフェールオーバーが進行中であることを示します。これにより、スタンバイサイトが新しいアクティブサイトに変換されます。
Failover success	システムトリガーまたは手動のフェールオーバーが正常に完了し、ディザスタリカバリシステムを運用可能な状態です。
Failover failed	システムトリガーまたは手動のフェールオーバーが正常に完了しませんでした。
Standby ready	前にアクティブサイトとして機能していたサイトを新しいスタンバイサイトとして設定する準備ができました。
Down	自動ヘルスマニタで監視システムが停止していることが確認されたか、設定されている時間しきい値の間にシステムから正常性の更新情報が提供されませんでした。
Pausing Standby	メンテナンスなどのアクティビティのために、スタンバイサイトを一時停止しています。
Standby Paused	スタンバイサイトが一時停止されました。現在はアクティブサイトとスタンバイサイトが2つのスタンドアロンクラスタとして機能し、サイト間のデータの複製は行われていません。システムを再起動してデータの複製を再開するには、[Rejoin] をクリックします。
Pausing Standby Failed	スタンバイサイトの一時停止中にエラーが発生しました。

表 4: 監視サイトの状態

状態	説明
未構成	新規に導入されたサイトです。ディザスタリカバリの情報はまだありません。
Registered	このサイトが監視サイトとして指定され、検証チェックが正常に完了しました。
Up	監視サイトの設定が正常に完了しました。
Down	自動ヘルスマニタで監視サイトが停止していることが確認されたか、設定されている時間しきい値の間に監視サイトから正常性の更新情報が提供されませんでした。
Up and Replicating	ディザスタリカバリシステムは稼働中です。複製が進行中です。
Up (Manual failover)	監視サイトから提供されるクォーラムなしでディザスタリカバリシステムが稼働しています。現在、システムトリガーのフェールオーバーは開始できません。

状態	説明
Failover in progress	フェールオーバーが進行中です。フェールオーバーが完了したら、新しいスタンバイサイトに問題がある場合は解決してから [Rejoin] をクリックします。
Failover in progress (User initiated)	手動で開始されたフェールオーバーが進行中です。現在は監視サイトに到達できません。
Up (No failover)	ディザスタリカバリシステムの設定とアクティブ化が完了しました。ただし、監視サイトに到達できないため、現在はフェールオーバーを開始できません。
Down (User intervention required)	フェールオーバーが正常に完了しませんでした。監視システムに到達できません。システムを一時停止してから再起動し、問題が解決したかどうかを確認します。

フェールオーバー：概要

フェールオーバーが実行されると、ディザスタリカバリシステムのスタンバイサイトがそれまでのアクティブサイトの役割を引き継ぎ、新しいアクティブサイトになります。Cisco DNA Center では、次の2種類のフェールオーバーをサポートしています。

- システムトリガー：ハードウェアの不具合やネットワークの停止などの問題によってシステムのアクティブサイトがオフラインになると実行されます。Cisco DNA Center では、アクティブサイトが残りのエンタープライズネットワーク（およびスタンバイサイトと監視サイト）と7分間通信できなかったことを認識すると、スタンバイサイトがその役割を引き受けるために必要なタスクを完了するため、中断することなくネットワーク動作を継続できます。
- 手動：ネットワーク管理者であるユーザがシステムのアクティブサイトとスタンバイサイトの現在の役割を入れ替えるように Cisco DNA Center に指示することで実行されます。通常は、サイトのアプライアンスにインストールされている Cisco DNA Center ソフトウェアの更新前やサイトの定期メンテナンスの実行前に行います。

いずれかの種類のフェールオーバーの実行後、前のアクティブサイトがオンラインに戻ると、ディザスタリカバリシステムは自動的に [Standby Ready] 状態に移行します。このサイトを新しいスタンバイサイトとして確立するには、[Monitoring] タブの [Action] 領域で [Rejoin] をクリックします。

手動フェールオーバーの開始

手動でフェールオーバーを開始する場合は、Cisco DNA Center でディザスタリカバリシステムのメインサイトとリカバリサイトに現在割り当てられているロールを入れ替えます。これは、現在のアクティブサイトで問題が発生していることが判明し、スタンバイサイトを新しいアクティブサイトとしてプロアクティブに指定する場合に便利です。手動フェールオーバーを開始するには、次の手順を実行します。

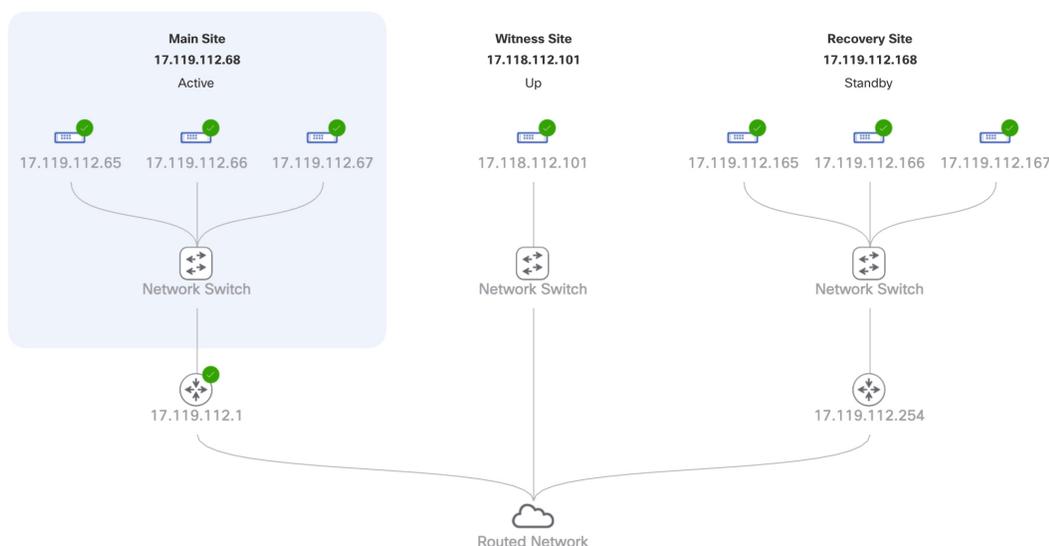


(注) 手動フェールオーバーは、監視サイトから開始することはできません。これは、現在アクティブなサイトからのみ実行できます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。

デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。次の例では、ユーザは現在のアクティブサイトにログインしています。

Logical Topology



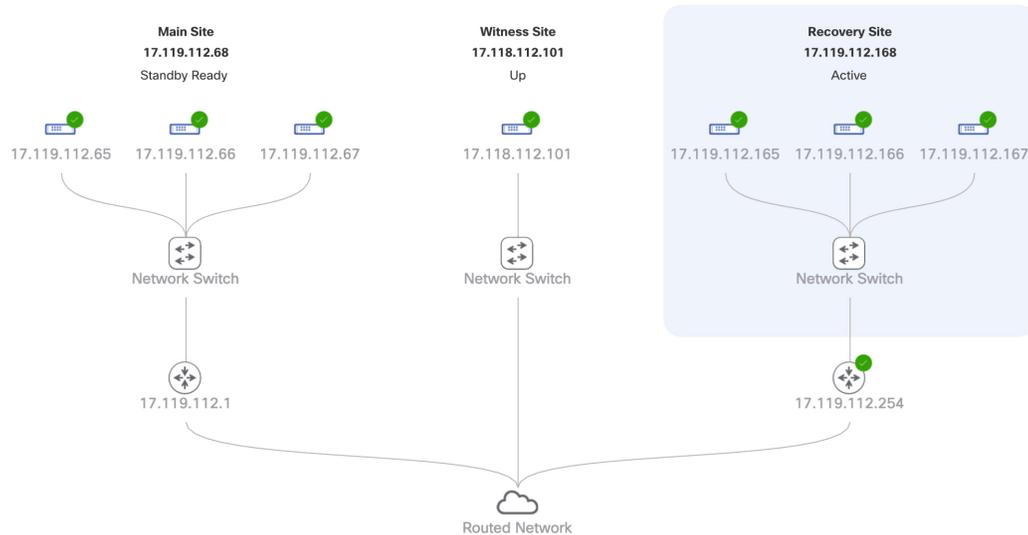
ステップ 2 [Action] 領域で、[Manual Failover] をクリックします。

スタンバイサイトのロールを [Active] に切り替えることを示す [Disaster Recovery Manual Failover] ダイアログが表示されます。

ステップ 3 [Continue] をクリックして進みます。

ページの右下隅に、フェールオーバープロセスが開始されたことを示すメッセージが表示されます。これまでアクティブサイトとして機能していたサイトは、システムから切り離されて [Standby Ready] 状態になります。

Logical Topology



この時点で、メインサイトとリカバリサイトの接続が解除され、データの複製は行われなくなります。前のアクティブサイトに問題がある場合は、この間にそれらの問題を解決します。

前のアクティブサイトをディザスタリカバリシステムに再度追加するまで、次のフェールオーバー（システムによるフェールオーバーとユーザによるフェールオーバーの両方）を開始することはできません。

ステップ 4 メインサイトとリカバリサイトを再接続し、ディザスタリカバリシステムを再設定します。

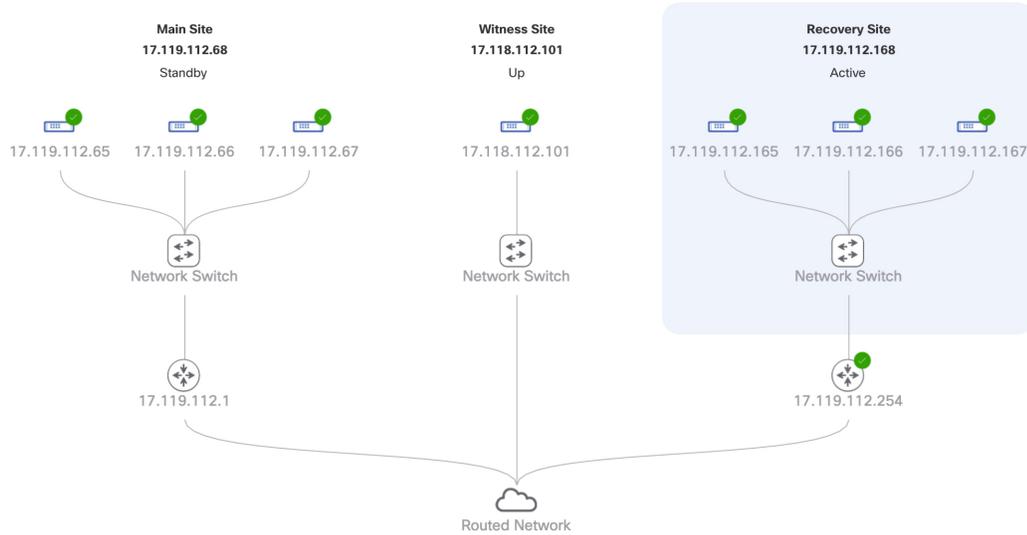
1. リカバリサイトにログインします。
2. [Action] 領域で、[Rejoin] をクリックします。

スタンバイサイトのデータが消去されることを示すダイアログが表示されます。

ステップ 5 [Continue] をクリックして次に進み、データの複製を再開します。

Cisco DNA Center で関連するワークフローが完了すれば、手動フェールオーバーは完了です。現在アクティブサイトとして機能していたメインサイトがスタンバイサイトになります。

Logical Topology



ステップ 6 ディザスタリカバリシステムが稼働状態に戻ったことを確認します。

1. [Monitoring] タブの右上に表示されたステータスが [Up and Running] になっていることを確認します。
2. イベントのタイムラインで、[Rejoin] タスクが正常に完了したことを確認します。

Event Timeline

[Hide Timeline](#)

End

Last Update: 8/6/2020, 3:28:55 PM UTC-7

Event Timeline showing the sequence of operations:

- Re-Join - 17.119.112.168** (8/6/2020, 3:27:11 PM UTC-7)
 - Status Message: Successfully setup disaster recovery
 - Start Time: 8/6/2020, 1:14:04 PM UTC-7
 - End Time: 8/6/2020, 3:27:11 PM UTC-7
- Configure active - 17.119.112.168** (8/6/2020, 1:21:34 PM UTC-7)
 - Status Message: Successfully configured active system
 - Start Time: 8/6/2020, 1:14:09 PM UTC-7
 - End Time: 8/6/2020, 1:21:34 PM UTC-7
- Configure standby - 17.119.112.68** (8/6/2020, 3:27:10 PM UTC-7)
 - Status Message: Successfully configured standby system
 - Start Time: 8/6/2020, 1:14:05 PM UTC-7
 - End Time: 8/6/2020, 3:27:10 PM UTC-7

ディザスタリカバリシステムの一時停止

メインサイトとリカバリサイトを一時停止することで、ディザスタリカバリシステムが実質的に停止します。サイト間の接続が解除され、各サイトがスタンドアロンクラスタとして機能するようになります。長期間にわたってシステムを停止する場合は、システムを一時停止して、アクティブサイトからスタンバイサイトへのデータの複製を一時的に無効にする必要があります。また、追加パッケージのインストールなどの管理タスクを実行する必要がある場合も、システムを一時停止します。ディザスタリカバリシステムを一時停止することで、Cisco DNA Center を計画的なネットワークの中断から保護したり、システムの設定を削除することなくディザスタリカバリを無効にしたりできます。

システムの一時的停止

システムコンポーネントのメンテナンスを実施する前などにディザスタリカバリシステムを一時的に停止するには、次の手順を実行します。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。

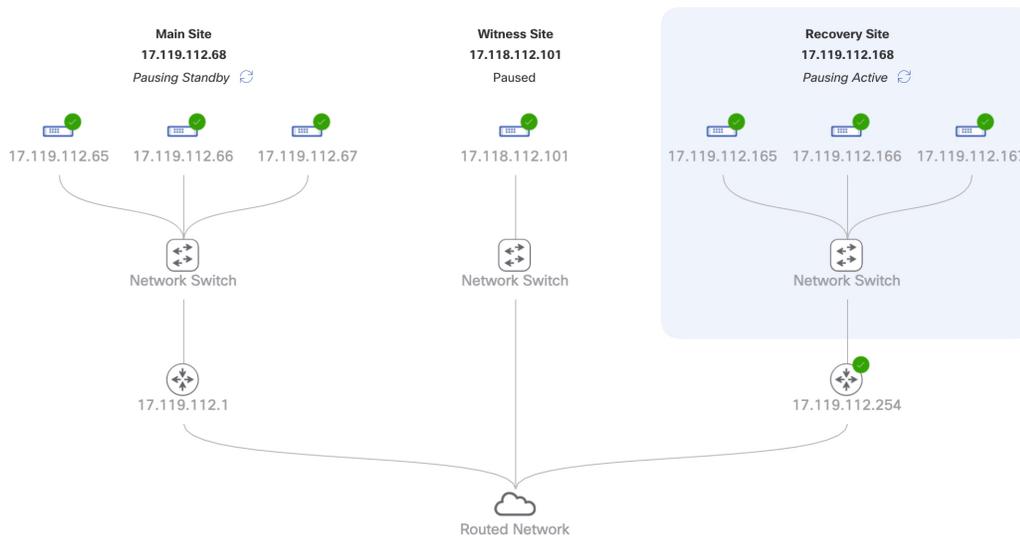
デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。

ステップ 2 [Action] 領域で、[Pause DR] をクリックします。

ステップ 3 表示されたダイアログで、[Continue] をクリックして次に進みます。

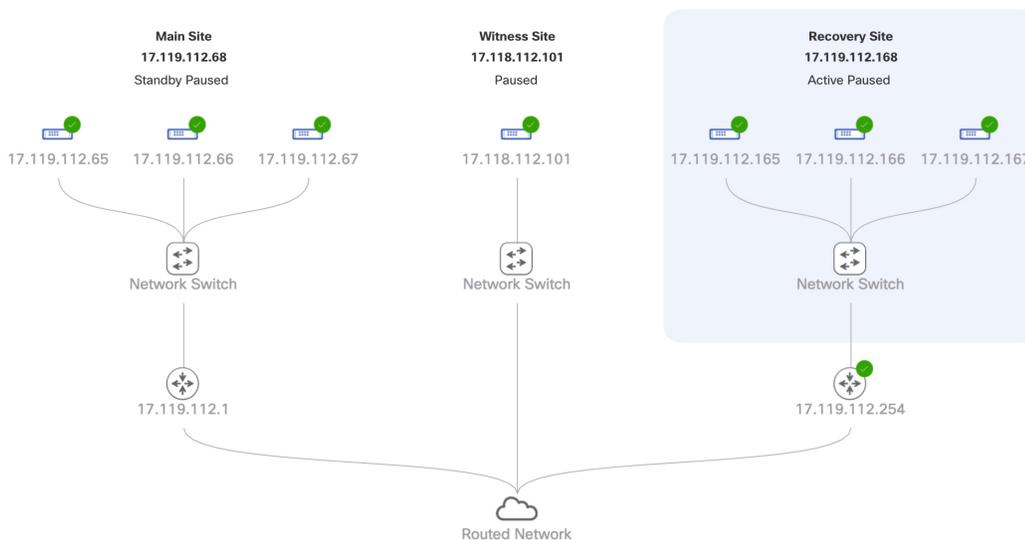
ページの右下隅に、システムを一時停止するプロセスが開始されたことを示すメッセージが表示されます。システムを一時停止するために、Cisco DNA Center でデータとサービスの複製が無効化されます。また、リカバリサイト側の停止していたサービスが再開されます。このプロセスの実行中は、トポロジにおいて、メインサイトとリカバリサイトのステータスが [Pausing] に設定されます。

Logical Topology



Cisco DNA Center で必要なタスクが完了すると、トポロジに表示されたメインサイト、リカバリサイト、および監視サイトのステータスが更新されて [Paused] に設定されます。

Logical Topology



ステップ 4 ディザスタリカバリシステムが一時停止していることを確認します。

1. [Monitoring] タブの右上隅に表示されたステータスが [Disaster Recovery System Paused] になっていることを確認します。
2. イベントのタイムラインで、[Pause DR] タスクが正常に完了したことを確認します。

Event Timeline

[Hide Timeline](#)

End Last Update: 8/6/2020, 3:42:47 PM UTC-7

Pause DR - 17.119.112.168 8/6/2020, 3:41:04 PM UTC-7

Status Message: Successfully prepared clusters for pause DR.

Start Time: 8/6/2020, 3:30:15 PM UTC-7

End Time: 8/6/2020, 3:41:04 PM UTC-7

[Hide Details](#)

Active cluster standalone - 17.119.112.168 8/6/2020, 3:33:14 PM UTC-7

Status Message: Successfully prepared active cluster for pause DR.

Start Time: 8/6/2020, 3:30:17 PM UTC-7

End Time: 8/6/2020, 3:33:14 PM UTC-7

[View Details](#)

Standby cluster standalone - 17.119.112.68 8/6/2020, 3:40:59 PM UTC-7

Status Message: Successfully prepared standby cluster for pause DR.

Start Time: 8/6/2020, 3:30:21 PM UTC-7

End Time: 8/6/2020, 3:40:59 PM UTC-7

[View Details](#)

監視サイトのリリース 2.1.2.x へのアップグレード

Cisco DNA Center 2.1.2.x より前のバージョンを実行しているアプライアンスでディザスタリカバリを設定した場合は、次の手順を実行して最新の Cisco DNA Center 2.1.2.x バージョンにアップグレードした後、監視サイトが正しく動作することを確認する必要があります。

- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして **[System] > [Disaster Recovery]** の順に選択して [Disaster Recovery] ページを開きます。
- ステップ 2 [Action] 領域で、[Pause DR] をクリックします。
- ステップ 3 メインサイトとリカバリサイトのアプライアンスを最新の Cisco DNA Center 2.1.2.x バージョンにアップグレードします。『[Cisco DNA Center Upgrade Guide](#)』の「Upgrade to Cisco DNA Center 2.1.2.x」章にある最初のトピックを参照してください。
- ステップ 4 監視サイトの OVF パッケージをインストールします（[現在の監視サイトの置換 \(15 ページ\)](#) を参照）。
- ステップ 5 Cisco DNA Center の GUI で [Disaster Recovery] ページに戻り、[Action] 領域の [Rejoin] をクリックします。

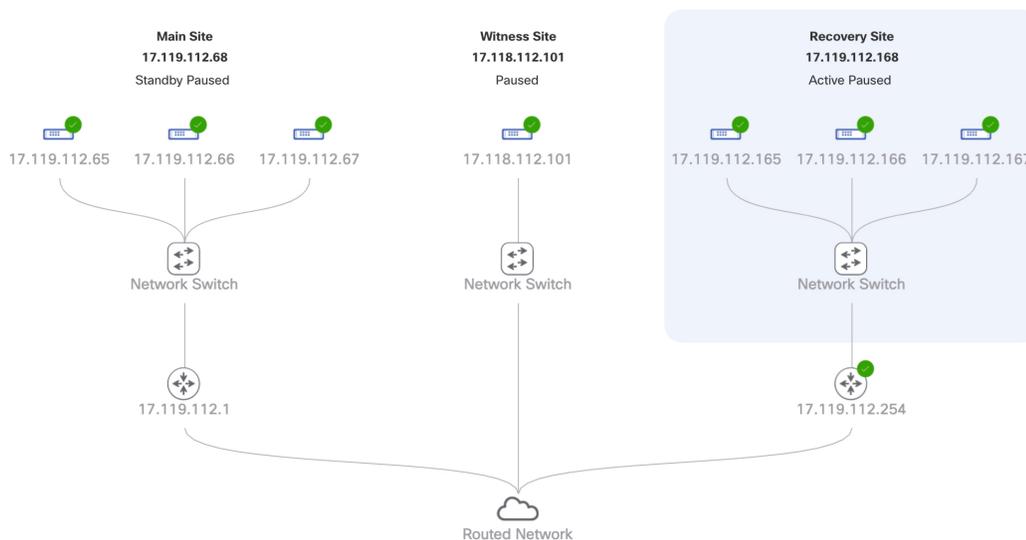
システムへの再参加

現在一時停止しているディザスタリカバリシステムを再起動するには、次の手順を実行します。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Disaster Recovery] の順に選択して [Disaster Recovery] ページを開きます。

デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。

Logical Topology



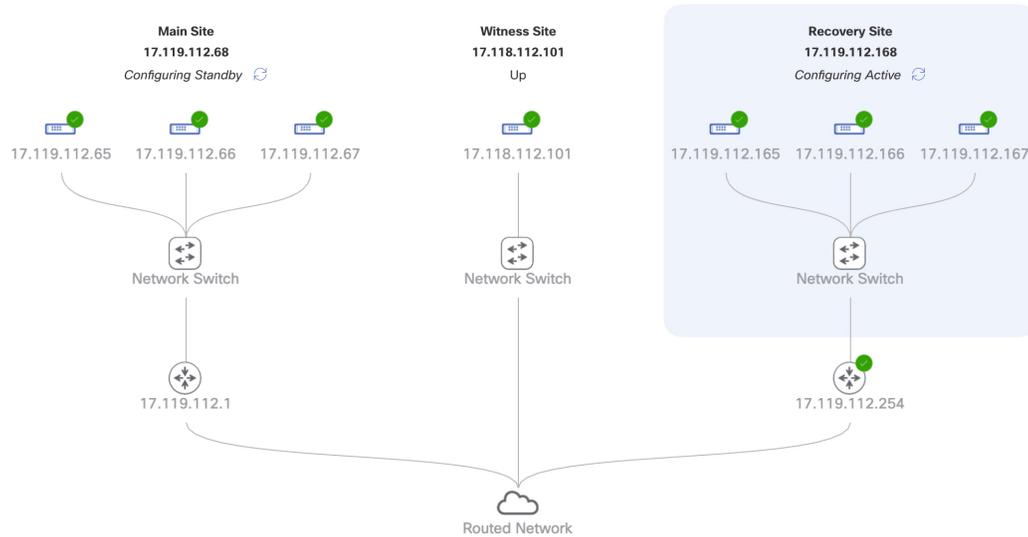
ステップ 2 [Action] 領域で、[Rejoin] をクリックします。

スタンバイサイトのすべてのデータが消去されることを示すダイアログが表示されます。

ステップ 3 [Continue] をクリックして進みます。

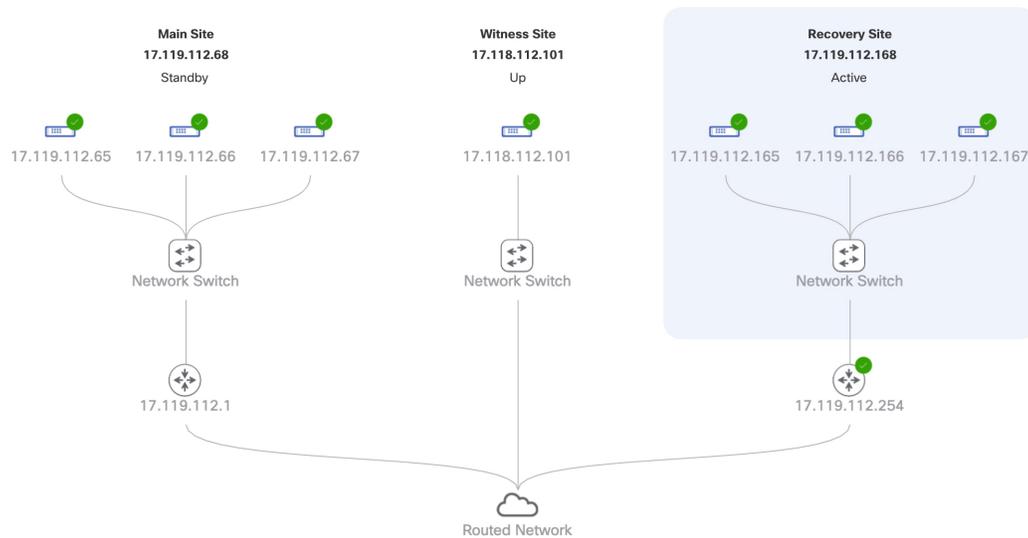
ページの右下隅に、メインサイト、リカバリサイト、および監視サイトを再接続するプロセスが開始されたことを示すメッセージが表示されます。このプロセスの実行中は、トポロジにおいて、メインサイトとリカバリサイトのステータスが [Configuring] に設定されます。

Logical Topology



Cisco DNA Center で必要なタスクが完了すると、トポロジに表示されたメインサイト、リカバリサイト、および監視サイトのステータスが更新されます。

Logical Topology



ステップ 4 [Monitoring] タブの右上隅に表示されたステータスが [Up and Running] になっていることを確認して、ディザスタリカバリシステムが稼働状態に戻ったことを確認します。

バックアップおよび復元の検討事項

ディザスタリカバリシステムをバックアップおよび復元する際は、次の点に注意してください。

- バックアップは、システムのアクティブサイトからのみスケジュールできます。
- バックアップファイルの復元は、ディザスタリカバリが有効になっている状態では実行できません。まずシステムを一時停止する必要があります。詳細については、「[システムの一時停止 \(26 ページ\)](#)」を参照してください。
- バックアップファイルの復元は、システムを一時停止する前にアクティブだったサイトでのみ実行してください。バックアップファイルを復元した後、システムのサイトに再参加する必要があります。これにより、ディザスタリカバリが再開され、アクティブサイトのデータのスタンバイサイトへの複製が開始されます。詳細については、「[システムへの再参加 \(28 ページ\)](#)」を参照してください。
- バックアップファイルの復元は、システム内の他のノードと同じバージョンの Cisco DNA Center がインストールされているクラスタノードでのみ実行できます。

ディザスタリカバリシステムのバックアップと復元の詳細については、[バックアップと復元](#)を参照してください。

ディザスタリカバリイベントの通知

ディザスタリカバリイベントが発生するたびに通知を送信するように Cisco DNA Center を設定できます。これらの通知を設定およびサブスクライブする方法については、『[Cisco DNA Center Platform User Guide](#)』の「Work with Events」を参照してください。この手順を完了したら、**[Platform] > [Developer Toolkit] > [Events]** テーブルで **[SYSTEM-DISASTER-RECOVERY]** イベントを選択し、サブスクライブしていることを確認します。

サブスクライブ後、Cisco DNA Center は、システムの証明書の有効期限が切れたために IPsec セッションがダウンしていることを示す通知を送信します。この証明書を更新するには、次の手順を実行します。

1. [システムの一時停止 \(26 ページ\)](#)。
2. メインサイトとリカバリサイトの両方で、現在のシステム証明書を置き換えます。Cisco DNA Center GUI で **[Menu]** アイコン (☰) をクリックして **[System] > [Settings] > [Trust & Privacy] > [System Certificate]** の順に選択します。
3. [システムへの再参加 \(28 ページ\)](#)。

サポートされるイベント

次の表に、ディザスタリカバリイベントを示します。Cisco DNA Center では、イベントが発生すると通知を生成します。

システムのヘルスステータス	イベント	通知
OK	ディザスタリカバリシステムが動作中です。	Activate DR (Disaster Recovery Setup Successful)
OK	メインサイトまたはリカバリサイトへのフェールオーバーが正常に完了しました。	Failover Successful
Degraded	メインサイトまたはリカバリサイトへのフェールオーバーが失敗しました。	Failover Failed
Degraded	スタンバイサイトが現在ダウンしているため、自動フェールオーバーは使用できません。	Standby Cluster Down
Degraded	監視サイトが現在ダウンしているため、自動フェールオーバーは使用できません。	Witness Cluster Down
Degraded	ディザスタリカバリシステムを一時停止できません。	Pause Failure
Degraded	BGP ルートアドバタイズメントが失敗しました。	BGP Failure
Degraded	システムのサイト間を接続する IPsec トンネルが動作中です。	IPsec Up
Degraded	システムのサイト間を接続する IPsec トンネルが現在ダウンしています。	IPsec Down
NotOk	ディザスタリカバリシステムの設定に失敗しました。	Activate DR Failure
NotOk	現在 [Standby Ready] 状態にあるサイトは、ディザスタリカバリシステムに再参加できません。	Activate DR Failure

ディザスタリカバリシステムのトラブルシューティング

次の表に、ディザスタリカバリシステムで発生する可能性がある問題とその対処方法を示します。

表 5:ディザスタリカバリシステムの問題

エラーコード (Error Code)	メッセージ	ソリューション
SODR10007	Token does not match.	リカバリサイトの登録時に提供されたトークンが、メインサイトの登録時に生成されたトークンと一致しません。メインサイトの [Disaster Recovery] > [Configuration] タブで、 [Copy Token] をクリックして正しいトークンをコピーします。
SODR10048	Packages (<i>package names</i>) are mandatory and not installed on the main site.	システムを登録する前に、リストされているパッケージをインストールします。
SODR10056	クレデンシャルが無効である。	リカバリサイトおよび監視サイトの登録時に、メインサイトの正しいクレデンシャルを入力したことを確認します。
SODR10062	(<i>)</i> site is trying to (<i>)</i> with invalid IP address. Expected is (<i>)</i> ; actual is (<i>)</i> .	リカバリサイトおよび監視サイトの登録時に提供されたメインサイトのIPアドレスが、メインサイトの登録時に提供されたIPアドレスと異なります。
SODR10067	Unable to connect to (<i>recovery or witness site</i>).	メインサイトが稼働していることを確認します。
SODR10072	All the nodes are not up for (<i>main or recovery site</i>).	サイトの3台のノードすべてが稼働しているかどうかを確認します。

エラーコード (Error Code)	メッセージ	ソリューション
SODR10076	High availability should be enabled on (main or recovery) site cluster.	次の手順を実行して、高可用性 (HA) を有効にします。 <ol style="list-style-type: none"> 1. HA を有効にする必要があるサイトにログインします。 2. Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして [System] > [Settings] > [System Configuration] > [High Availability] の順に選択します。 3. [Activate High Availability] をクリックします。
SODR10100	(Main or recovery) site has no third party certificate.	Cisco DNA Center で現在使用しているデフォルトの証明書をサードパーティ証明書に置き換えます。詳細については、「 Cisco DNA Center サーバ証明書の更新 」を参照してください。
SODR10118	Appliance mismatch between main () and recovery ().	メインサイトとリカバリサイトで異なるアプライアンスが使用されています。ディザスタリカバリを正常に登録するには、両方のサイトで同じ 56 または 112 コアアプライアンスを使用する必要があります。
SODR10121	Failed to advertise BGP. Reason: ().	詳細については、「 BGP ルートアドバタイズメントに関する問題のトラブルシューティング (40 ページ) 」を参照してください。
SODR10122	Failed to stop BGP advertisement. Reason: ().	詳細については、「 BGP ルートアドバタイズメントに関する問題のトラブルシューティング (40 ページ) 」を参照してください。

エラーコード (Error Code)	メッセージ	ソリューション
SODR10123	Failed to establish secure connection between main () and () ().	この問題に対する解決策はありません。サポートについては、Cisco TAC にお問い合わせください。
SODR10124	Cannot ping VIP: (main, recovery, or witness site's VIP or IP address).	次の手順を実行します。 <ul style="list-style-type: none"> 指定したアドレスが正しいことを確認します。 アドレスが他のアドレスから到達可能であるかどうかを確認します。
SODR10129	Unable to reach main site. ()	メインサイトに設定されたエンタープライズ仮想IPアドレスが、リカバリサイトと監視サイトから到達可能であるかどうかを確認します。
SODR10132	Unable to check IP addresses are on the same interface. 操作をやり直します。 ()	試行した操作をやり直します。
SODR10133	The disaster recovery enterprise VIP () and the IP addresses () are not configured or reachable via the same interface. Check the gateway or static routes configuration.	ディザスタリカバリシステムのサイト間の通信は、エンタープライズネットワークに依存します。メインサイトとリカバリサイトのエンタープライズ仮想IPアドレス、および監視サイトのIPアドレスは、エンタープライズインターフェイスを介して到達できるようにする必要があります。 <p>このエラーは、1つまたは複数のサイトに設定されたIPアドレス/仮想IPアドレスが、通信にエンタープライズインターフェイス以外のインターフェイスを使用していることを示します。</p>

エラーコード (Error Code)	メッセージ	ソリューション
SODR10134	The disaster recovery management VIP (VIP address) and the IPs (IP addresses) are configured/reachable via same interface. It should be configured/reachable via management interface. Check the gateway or static routes' configuration.	ディザスタリカバリシステムの管理仮想IPアドレスは、管理インターフェイスで設定する必要があります。このエラーは、管理クラスタの仮想IPアドレスが設定されていないインターフェイスで仮想IPアドレスが現在設定されていることを示します。 管理インターフェイスで設定されている管理仮想IPアドレスに /32 静的ルートを追加します。
SODR10136	Certificates required to establish IPsec session not found.	[System Certificate] ページ ([System] > [Settings] > [Trust & Privacy] > [System Certificate] の順に選択) からサードパーティ証明書を再度アップロードして、登録を再試行します。問題が解決しない場合は、Cisco TAC にお問い合わせください。
SODR10138	Self-signed certificate is not allowed. Upload a third-party certificate and retry.	—
SODR10139	Disaster recovery requires first non-wildcard DNS name to be same in main and recovery. {} in {} site certificate is not same as {} in {} site certificate.	メインサイトとリカバリサイトにインストールされているサードパーティ証明書に、ディザスタリカバリシステム用に指定された別のDNS名があります。お使いのシステムのDNS名を指定するサードパーティ証明書を生成し、この証明書を両方のサイトにアップロードします。 (注) DNS名にワイルドカードが使用されていないことを確認します。

エラーコード (Error Code)	メッセージ	ソリューション
SODR10140	Disaster recovery requires at least one non-wildcard DNS name. No DNS name found in certificate.	メインサイトとリカバリサイトにインストールされているサードパーティ証明書で、ディザスタリカバリシステムのDNS名が指定されていません。Cisco DNA Centerでは、この名前を使用して、システムのサイト間を接続するIPsecトンネルを設定します。お使いのシステムのDNS名を指定するサードパーティ証明書を生成し、この証明書を両方のサイトにアップロードします。 (注) DNS名にワイルドカードが使用されていないことを確認します。
—	—	ネットワークのパーティショニングまたは別の条件により、システムで使用する3つのサイトすべてが接続されていない場合は、Cisco DNA Centerでサイトのステータスを [Isolated] に設定します。適切なリカバリ手順の実行については、Cisco TACにお問い合わせください。

エラーコード (Error Code)	メッセージ	ソリューション
—	External postgres services does not exists to check service endpoints.	<p>次の手順を実行します。</p> <ol style="list-style-type: none"> 1. エラーが発生したサイトにログインします。 2. 次のコマンドを実行します。 <ul style="list-style-type: none"> • Kubectl get sep -A • kubectl get svc -A grep external 3. 結果の出力で、external-postgres を検索します。 4. 存在する場合は、kubectl delete sep external-postgres -n fusion コマンドを実行します。 5. 以前に失敗した操作を再試行します。
—	Cannot ping VIP: (VIP address).	システムに設定されているエンタープライズVIPアドレスが到達可能であることを確認します。
—	VIP drop-down list is empty.	システムのVIPアドレスとクラスタ内リンクが正しく設定されていることを確認します。
—	Cannot perform (disaster recovery operation) due to ongoing workflow: BACKUP. Please try again at a later time.	スケジュールされたバックアップの実行中にディザスタリカバリ操作がトリガーされました。バックアップの完了後に操作を再試行してください。

エラーコード (Error Code)	メッセージ	ソリューション
—	The GUI indicates that the standby site is still down after it has come back online.	<p>スタンバイサイトがダウンしたときに、そのサイトを Cisco DNA Center の最初の試行でディザスタリカバリシステムから分離できなかった場合、2 回目の試行が自動的に開始されないことがあります。この場合、そのサイトが稼働状態に戻っても、GUI ではダウンしているものとして表示されます。スタンバイサイトがメンテナンスモードのままであるため、システムを再起動することもできません。</p> <p>スタンバイサイトを復元するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. SSH クライアントで、スタンバイサイトにログインします。 2. maglev maintenance disable コマンドを実行して、サイトをメンテナンスモードから復旧させます。 3. Cisco DNA Center にログインします。 4. GUI で [Menu] アイコン (☰) をクリックし、[System] > [Disaster Recovery] の順に選択します。 デフォルトでは、[Monitoring] タブが選択されています。 5. ディザスタリカバリシステムを再起動するために、[Action] 領域で [Rejoin] をクリックします。

エラーコード (Error Code)	メッセージ	ソリューション
—	Multiple services exists for MongoDB to check node-port label.	デバッグ用に、MongoDB ノードポートがサービスとして公開されます。このポートを特定して非表示にするには、次のコマンドを実行します。 <ul style="list-style-type: none"> • kubectl get svc --all-namespaces grep mongodb • magctl service unexpose mongodb <port-number>
—	Multiple services exist for Postgres to check node-port label.	デバッグ用に、Postgres ノードポートがサービスとして公開されます。このポートを特定して非表示にするには、次のコマンドを実行します。 <ul style="list-style-type: none"> • kubectl get svc --all-namespaces grep postgres • magctl service unexpose postgres <port-number>

BGP ルートアドバタイズメントに関する問題のトラブルシューティング

BGP ルート アドバタイズメント エラーを受信した場合は、次の手順を実行して原因をトラブルシューティングします。

ステップ 1 Cisco DNA Center クラスタから、BGP セッションのステータスを検証します。

- a) イベントタイムラインで、[Starting BGP advertisement] タスクが正常に完了したかどうかを確認します ([Activate DR] > [View Details] > [Configure active] の順に選択)。

タスクが失敗した場合は、次を実行してから手順 1b に進みます。

1. エラーメッセージに示されているネイバルータが稼働しているかどうかを確認する。
2. ネイバルータと Cisco DNA Center の接続があるかどうかを確認する。接続がない場合は、接続を復元してから新しいディザスタリカバリシステムをアクティブにするか、一時停止された既存のシステムを再起動します。

- b) Cisco DNA Center GUI で、ディザスタリカバリシステムの論理トポロジを表示し、ネイバルータが現在アクティブかどうかを確認します。

ダウンしている場合は、ルータの観点から、Cisco DNA Center クラスタが BGP ネイバーとして設定されているかどうかを確認します。設定されていない場合は、クラスタをネイバーとして設定し、新しいディザスタリカバリシステムをアクティブにするか、一時停止された既存のシステムを再起動して再試行します。

- c) 次のコマンドを実行して、Cisco DNA Center とそのネイバルータ間の BGP セッションのステータスを確認します。

```
etcdctl get /maglev/config/network_advertisement/bgp/address1_address2 | jq
```

引数の説明

- *address1* は Cisco DNA Center クラスタの仮想 IP アドレスです。
- *address2* は、ネイバルータの IP アドレスです。

[Established] が [state] フィールドにリストされている場合は、セッションがアクティブであり、正しく機能していることを示します。

- d) bgpd および bgpmanager のログファイルを表示するには、次のコマンドを実行します。

- `sudo vim /var/log/quagga/bgpd.log`
- `magctl service logs -rf bgpmanager | lq`

ログファイルを表示するときは、エラーメッセージがないか確認します。メッセージがない場合は、BGP セッションが正しく機能していることを示します。

- e) 次のコマンドを実行して、Cisco DNA Center とそのネイバルータ間の BGP セッションのステータスを確認します：`echo admin-password | sudo VTYSH_PAGER=more -S -i vtysh -c 'show ip bgp summary'`

コマンド出力で、ネイバルータの IP アドレスを検索します。同じ行の末尾に、ルータの接続状態が [0] とリストされていることを確認します。この場合、BGP セッションがアクティブであり、適切に機能していることを示します。

ステップ 2 エラーメッセージに示されているネイバルータから、BGP セッションのステータスを検証します。

- a) `show ip bgp summary` コマンドを実行します。
- b) コマンド出力で、Cisco DNA Center クラスタの仮想 IP アドレスを検索します。同じ行の末尾に、クラスタの接続状態が [0] とリストされていることを確認します。この場合、BGP セッションがアクティブであり、適切に機能していることを示します。
- c) `show ip route` コマンドを実行します。
- d) コマンドの出力を表示し、ディザスタリカバリシステムのエンタープライズ仮想 IP アドレスがアドバタイズされているかどうかを確認します。

たとえば、システムのエンタープライズ仮想 IP アドレスが 10.30.50.101 であるとし、これが出力に表示される最初の IP アドレスである場合は、アドバタイズされていることを確認します。

