ディザスタリカバリの実装

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します。クラスタに障害が発生すると、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する方法については、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 （16 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ーにあり、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ー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 （7 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 （16 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） システムのスタンバイサイトを現在表示していることを示すメッセージが表示されます。アクティブサイトからすべてのディザスタリカバリタスクを開始する必要があります。

- 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す。
  - 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ーリングでモニターできます。
  - 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 （34 ページ）を参照してください。

重要

- 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。
- フェールオーバー後、Cisco DNA Center インベントリサービスはデバイスの完全な同期をトリガーします。これには、管理対象のデバイスの数に応じて、数分から数時間かかる場合があります。Cisco DNA Center の通常スケジュールされたデバイス同期が実行されている場合と同様に、フェールオーバーによってトリガーされたデバイス同期が完了するまで、新しくアクティブ化されたクラスタでデバイスをプロビジョニングすることはできません。

- 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停止 （37 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ー始動型の操作。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。

データレプリケーションの概要

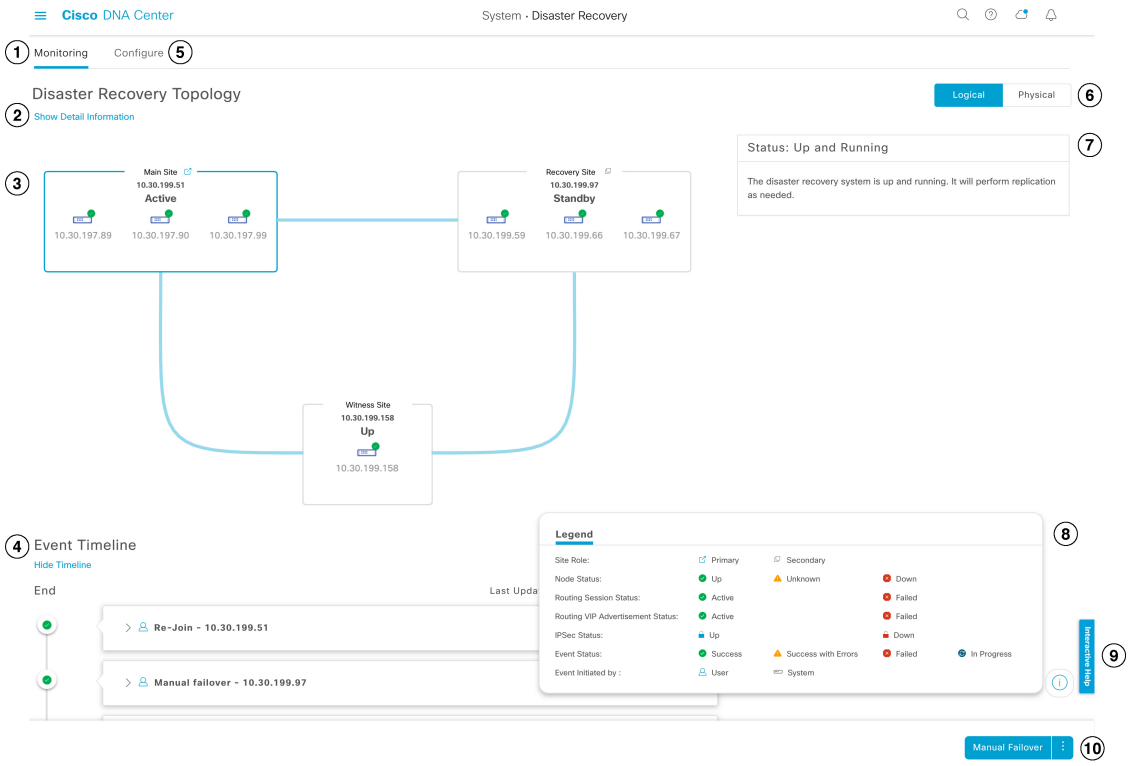
データ レプリケーション プロセスは、ディザスタリカバリシステムのメインサイトとリカバリサイトの間でデータを同期します。その期間は、レプリケートする必要があるデータの量、ネットワークの有効な帯域幅、およびメインサイトとリカバリサイト間に存在する待機時間など、いくつかの要因によって異なります。Cisco DNA Center の展開でディザスタリカバリがアクティブになっている場合、データレプリケーションは、現在アクティブなサイト（ネットワークを管理している）での操作やアプリケーションの使用に影響を与えません。

次のシナリオのどれが該当するかに応じて、データの完全レプリケーションまたは増分レプリケーションが実行されます。

- **初期アクティブ化後**：ディザスタリカバリシステムの初期構成とアクティブ化の後で、リカバリサイトにデータがありません。このシナリオでは、メインサイトとリカバリサイトの間でデータの完全なレプリケーションが行われます。
- **フェールオーバー後**：現在アクティブなサイトで障害が発生すると、ディザスタリカバリシステムがフェールオーバーをトリガーします。このシナリオでは、障害が発生したサイトがシステムに再参加した後に、メインサイトとリカバリサイト間でデータの完全なレプリケーションが発生します。
- **通常の操作時**：これは、通常、システムに適用されるシナリオです。日常の運用中に、現在のアクティブサイトで発生した変更は、現在のスタンバイサイトと継続的に同期されます。

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。



引き出し線	説明
1	[Monitoring] タブ：次の操作を実行する場合にクリックします。 • 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	[Show Detail Information] リンク：クリックして、[Disaster Recovery System] スライドインペインを開きます。詳細については、ディザスタリカバリシステムのステータスの表示 （6 ページ） を参照してください。

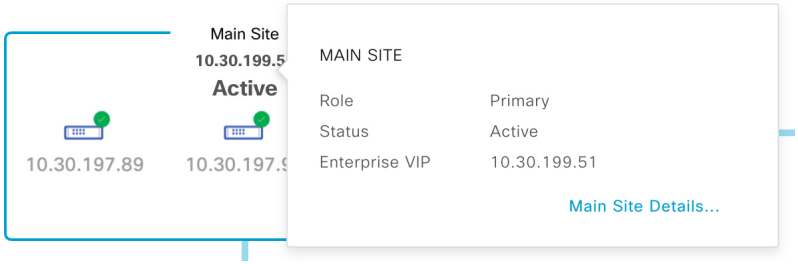
引き出し線	説明
3	[Topology]：サイトとそのメンバーの現在のステータスを示すシステムの論理トポロジまたは物理トポロジが表示されます。 • 論理トポロジと物理トポロジの両方で、青色のボックスは、現在システムのアクティブサイトとして機能しているサイトを示します。 • 論理トポロジでは、青色の線は 2 つのサイトを接続する IPSec トンネルが動作していることを示し、赤色の線はトンネルが現在ダウンしていることを示します。 • サイトの状態については、システムおよびサイトの状態 （28 ページ）を参照してください。
4	[Event Timeline]：システムのディザスタリカバリタスクについて、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ーリング （26 ページ）を参照してください。
5	[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 （16 ページ）を参照してください。
6	[Logical] タブと [Physical] タブ：適切なタブをクリックして、システムの論理トポロジと物理トポロジを切り替えます。
7	[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 （28 ページ）を参照してください。
8	[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。
9	[Interactive Help] ボタン：クリックすると、スライドインペインが開き、Cisco DNA Center の特定のタスクを完了するための画面上のガイダンスを示すウォークスルーへのリンクが表示されます。
10	[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。

ディザスタリカバリシステムのステータスの表示

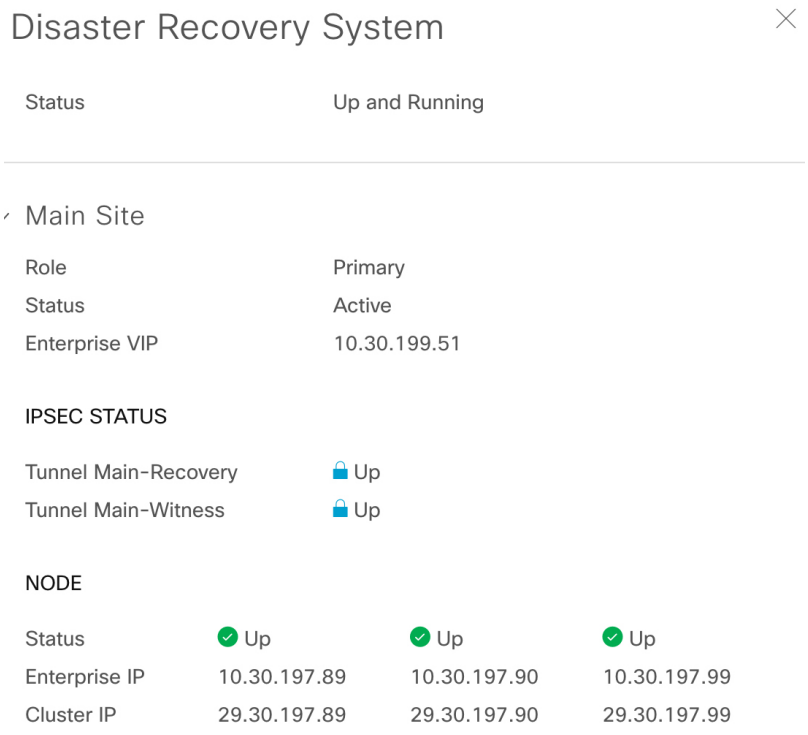
トポロジでは、ディザスタリカバリシステムの現在のステータスが視覚的に表示されます。[Disaster Recovery System] スライドインペインでは、この情報を表形式で確認できます。このペインを開くには、次のいずれかを実行します。

- [Show Detail Information] リンクをクリックします。次に、スライドインペインでステータスを確認するサイトを展開します。

- トポロジで、サイトのエンタープライズ仮想 IP アドレスまたは特定のノードのアイコンにカーソルを合わせます。開いたポップアップウィンドウで、ウィンドウの右下隅にあるリンクをクリックします。



スライドインペインが開き、関連サイトの情報が表示されます。



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 Cisco DNA Center 2.3.3 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、「アップグレードされた Cisco DNA Center アプライアンスでの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。

一般的な前提条件

- Cisco DNA Center は、次の 2 つのディザスタリカバリ設定をサポートしています。
  - **1+1+1 セットアップ**：1 つ目の Cisco DNA Center アプライアンスはメインサイトとして機能し、2 つ目のアプライアンスはリカバリサイトとして機能し、3 つ目のシステム（仮想マシン上に常駐）は監視サイトとして機能します。次のアプライアンスとバージョンがこのセットアップをサポートしています。
    - DN1-HW-APL/DN2-HW-APL（44 コアアプライアンス）：Cisco DNA Center 2.2.2.x 以降
    - DN2-HW-APL-L（56 コアアプライアンス）：Cisco DNA Center 2.2.1.x 以降
    - DN2-HW-APL-XL（112 コアアプライアンス）：Cisco DNA Center 2.2.1.x 以降
  - **3+3+1 セットアップ**：1 つ目の 3 ノード Cisco DNA Center クラスタはメインサイトとして機能し、2 つ目の 3 ノードクラスタはリカバリサイトとして機能し、3 つ目のシステム（仮想マシン上に常駐）は監視サイトとして機能します。次のアプライアンスとバージョンがこのセットアップをサポートしています。
    - DN1-HW-APL/DN2-HW-APL（44 コアアプライアンス）：Cisco DNA Center 2.2.2.x 以降
    - DN2-HW-APL-L（56 コアアプライアンス）：Cisco DNA Center 2.1.2.x 以降
    - DN2-HW-APL-XL（112 コアアプライアンス）：Cisco DNA Center 2.1.2.x以降
- 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 Advanced Install Configuration 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ー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ー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 1 GB リンクで、RTT 遅延が 350 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
- 1 つの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。

メインサイトとリカバリ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）がこの証明書に含まれていることを確認してください。また、証明書の [keyUsage] パラメータに [nonRepudiation] と [DigitalSignature] が指定されていることを確認します。サードパーティ証明書を生成する方法については、『*Cisco DNA CenterSecurity Best Practices Guide*』の「Generate a Certificate Request Using Open SSL」を参照してください。

- 『Cisco DNA CenterSecurity Best Practices Guide』の「Disaster Recovery Ports」トピックに記載されているすべてのポートを開いておきます。

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が同じ数のノードで構成されている必要があります。Cisco DNA Center では、この要件を満たさないディザスタリカバリシステムを登録してアクティブにすることはできません。
- 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 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 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 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。

サポートされる Cisco DNA Center アプライアンス	シスコ製品番号
第 1 世代および第 2 世代の 44 コアアプライアンス	• DN1-HW-APL • DN1-HW-APL-U • DN2-HW-APL • DN2-HW-APL-U
第 2 世代 56 コアアプライアンス	• DN2-HW-APL-L • DN2-HW-APL-L-U

サポートされる Cisco DNA Center アプライアンス	シスコ製品番号
第 2 世代 112 コアアプライアンス	• DN2-HW-APL-XL • DN2-HW-APL-XL-U

また、メインサイトとリカバリサイトが同じバージョンの Cisco DNA Center を実行していることを確認してください。

- 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。

重要 これは、3 ノードセットアップにのみ適用されます。

- メインサイトとリカバリサイトの連邦情報処理標準（FIPS）モード設定が同じであることを確認します。FIPS モードが一方のサイトで有効になっていて、もう一方のサイトで無効になっている場合、検証エラーが原因でディザスタリカバリシステムの登録が失敗します。FIPS モードの詳細については、[IP addressing mode used for the services] 画面の説明を参照してください（『Cisco DNA Center Second-Generation Appliance Installation Guide』の「Configure the Primary Node Using the Maglev Wizard」トピックにあります）。
- 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、ネイバールータのローカルおよびリモート AS 番号です。
- `10.30.197.57` はネイバールータの 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、ネイバールータのローカル AS 番号です。
- 64555 は、ネイバールータのリモート AS 番号です。
- 10.30.197.57 はネイバールータの 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 DENY_ALL out
!
ip prefix-list DENY_ALL seq 5 deny 0.0.0.0/0 le 32
!
route-map DENY_ALL 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。
- パブリッククラウドでの監視サイトの展開はサポートされていません。
- 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 サーバーを設定しておきます。この NTP サーバーをメインサイトとリカバリサイトで使用される NTP サーバーと同期する必要があります。

アップグレードされた Cisco DNA Center アプライアンスでのディザスタリカバリの設定

システムを最新の Cisco DNA Center 2.3.3. にアップグレードした後でディザスタリカバリを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、アプライアンスにインストールされた最初の Cisco DNA Center バージョンは 2.1.x より前のバージョンです。そこで、2.1.x から 2.3.3 へのアップグレードを行います。アップグレード後にディザスタリカバリが正しく機能するように、次の手順を実行します。

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 2.3.3 にアップグレードします（『Cisco DNA CenterUpgrade 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ーにあることを確認します。

ステップ 3 アプライアンスに Cisco DNA Center 2.3.3 の ISO イメージをインストールします（『Cisco DNA CenterSecond-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、これを 2.3.3 にアップグレードします。次の手順を実行します。

ステップ 1 監視サイトのインストール （13 ページ）。

ステップ 2 ディザスタリカバリの設定 （16 ページ）。

ディザスタリカバリ証明書の追加

Cisco DNA Center は、X.509 証明書と秘密キーの Cisco DNA Center へのインポートとストレージをサポートします。ディザスタリカバリ証明書は、クラスタ内通信に使用されます。

内部 CA から発行された有効な X.509 証明書を取得する必要があります。証明書は所有する秘密キーに対応している必要があります。

（注）

- Cisco DNA Center で使用するのと同じ証明書をディザスタリカバリシステムで使用する場合は、この手順をスキップできます。証明書を設定する場合は、[Use system certificate for Disaster Recovery as well] チェックボックスをオンにします（Cisco DNA Center サーバー証明書の更新を参照）。
- ディザスタリカバリ証明書の要件の詳細については、『Security Best Practices Guide』を参照してください。

ステップ 1 メニューアイコン（☰）をクリックして、**[System]** > **[Settings]** > **[Trust & Privacy]** > **[Certificates]** > **[Disaster Recovery]** の順に選択します。

ステップ 2 [Add Certificate] 領域で、Cisco DNA Center にインポートする証明書のファイル形式タイプを選択します。

- [PEM]：プライバシー エンハンスト メール ファイル形式
- [PKCS]：公開キー暗号化標準ファイル形式

ステップ 3 [PEM] を選択した場合、次のタスクを実行します。

a) 強調表示されている領域に PEM ファイルをドラッグアンドドロップして、証明書をインポートします。

（注） PEM ファイルには、有効な PEM 形式の拡張子（.pem）が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

b) [Private Key] 領域で、強調表示されている領域に秘密キーをドラッグアンドドロップしてインポートします。

（注） 秘密キーには、有効な秘密キー形式の拡張子（.key）が必須です。秘密キーの最大ファイルサイズは 10 MB です。

アップロードに成功すると、秘密キーが検証されます。

c) 適切なオプションボタンをクリックして、秘密キーを暗号化するかどうかを指定します。

d) 秘密キーを暗号化する場合、[Password] フィールドに秘密キーのパスワードを入力します。

ステップ 4 [PKCS] を選択した場合、次のタスクを実行します。

a) 強調表示されている領域に PKCS ファイルをドラッグアンドドロップして、証明書をインポートします。

（注） PKCS ファイルには、有効な PKCS 形式の拡張子（.pfx または .p12）が必須です。証明書の最大ファイルサイズは 10 MB です。

アップロードに成功すると、システム証明書が検証されます。

b) [Password] フィールドに、証明書のパスワードを入力します（PKCS の要件）。

c) 適切なオプションボタンをクリックして、秘密キーを暗号化するかどうかを指定します。

d) 秘密キーを暗号化する場合、[Password] フィールドに秘密キーのパスワードを入力します。

ステップ 5 **[Save]** をクリックします。

Cisco DNA Center サーバーの SSL 証明書が置き換えられると、自動的にログアウトされるため、再度ログインする必要があります。

監視サイトのインストール

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) 管理者ユーザー（*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 サーバーの IP アドレス

d) NTP サーバー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。

（注） 後で、監視サイトの VM で **maglev** ユーザー用に設定された**パスワード**を変更する必要がある場合は、標準の Linux passwd ユーティリティを使用します。これを行う前にディザスタリカバリシステムを一時停止する必要はありません。また、パスワードを変更しても、ディザスタリカバリ操作に機能上の影響はありません。

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。

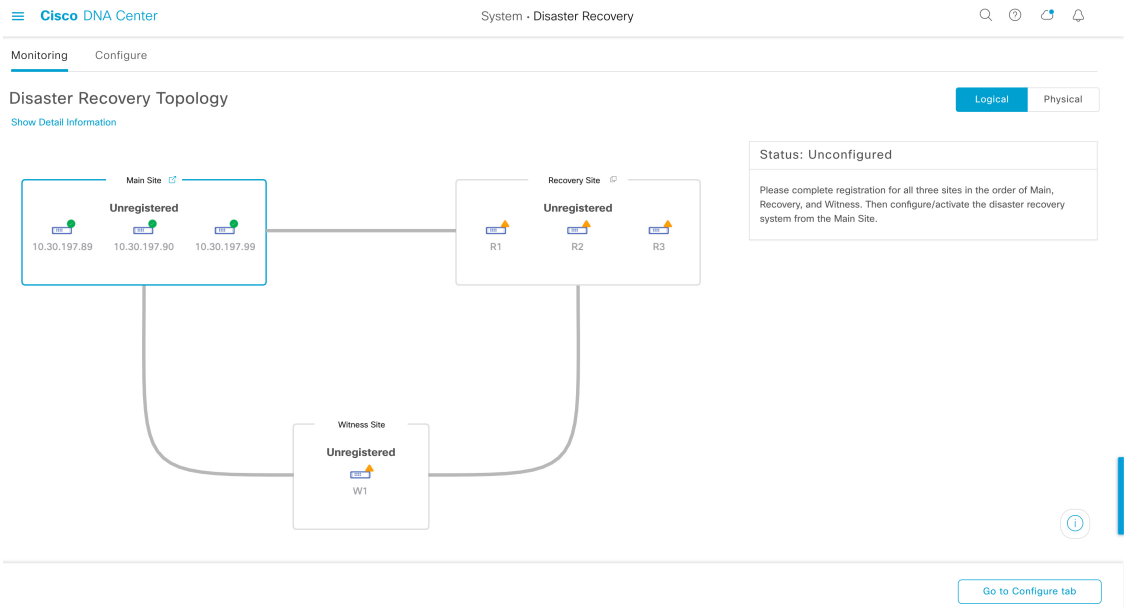
- ボーダー ゲートウェイ プロトコル（BGP）ルート アドバタイジングを使用する仮想 IP アドレスを指定できます。
- 仮想 IP アドレスを設定しないように選択することもできます。このオプションを選択した場合は、デバイスの可制御性を有効にして、フェールオーバー発生後にサイトの仮想IP アドレスを再設定できるようにする必要があります。詳細については、デバイスの可制御性を参照してください。

始める前に

アシュアランスデータ（Elasticsearch）と展開のバックアップスケジュールは、フェールオーバー後にレプリケートされません。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が存在するクラスタの場合は、システムを構成する前に次の手順を実行します。

- サイトごとに個別の NFS デバイスを構成します。
- 同じバックアップスケジュールを設定します。

ステップ 1 メニューアイコン（☰）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。

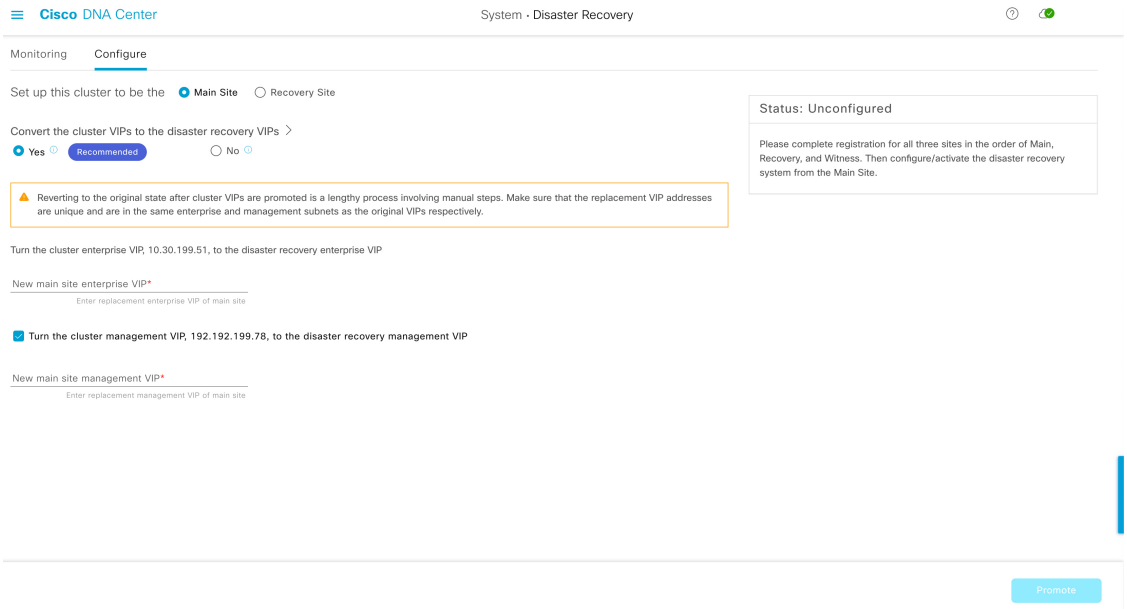


デフォルトでは、[Monitoring] タブが選択されています。

ステップ 2 メインサイトを登録します。

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) [Convert the cluster VIPs to the disaster recovery VIPs] 領域で、次のいずれかのオプションボタンをクリックします。

- クラスタをメインサイトとして設定し、このクラスタに接続されているデバイスに仮想 IP アドレスの変更を自動的に伝達するには、[Yes] をクリックします。これは、クラスタに現在設定さ

れている仮想 IP アドレスを昇格させ、それらをディザスタリカバリシステムのグローバル仮想 IP アドレスとして割り当てることによって実現します。多数のデバイスが接続されているクラスタでディザスタリカバリを有効にする場合は、このオプションを選択することをお勧めします。このオプションを選択しない場合、新しいディザスタリカバリ仮想 IP アドレスと通信するようにこれらのデバイスを再設定する必要があります。このオプションを選択する場合は、次の手順を実行します。

1. [New main site enterprise VIP] フィールドに、サイトのエンタープライズ ネットワークの新しい仮想 IP アドレスを入力します。これにより、昇格するアドレスが置き換えられます。このアドレスがまだ使用されていない一意のアドレスであり、以前の仮想 IP アドレスと同じサブネットにあることを確認します。
2. （オプション）[Turn the cluster management VIP, <IP-address>, to the disaster recovery management VIP] チェックボックスをオンにします。
3. （オプション）[New main site management VIP] フィールドに、サイトの管理ネットワークの新しい仮想IPアドレスを入力します。これにより、昇格するアドレスが置き換えられます。このアドレスがまだ使用されていない一意のアドレスであり、以前の仮想 IP アドレスと同じサブネットにあることを確認します。

- 仮想 IP アドレスの変更を接続デバイスに伝達せず、クラスタをメインサイトとして設定するには、[No] をクリックします。まだどのデバイスにも接続されていない、または少数のデバイスにのみ接続されている新しいクラスタには、このオプションをお勧めします。このオプションを選択する場合は、ステップ 2f に進みます。

c) [Action] 領域で、[Promote] をクリックします。

[Disaster Recovery VIP Promotion] ダイアログが開きます。

d) [Continue] をクリックします。

Cisco DNA Center は、入力した仮想 IP アドレスを検証します。

e) [Details] 領域に検証ステータスが表示されます。

- 入力したアドレスのいずれかが無効である場合（アドレスが置換するアドレスと同じサブネットに存在しない可能性があります）、必要な修正を行い、ステップ 2c を繰り返します。
- 入力したアドレスが正常に検証されると、ディザスタリカバリシステム用に設定されるすべての仮想 IP アドレスが [Details] 領域に表示されます。次のステップに進みます。

f) 次の情報を [Site VIP/IPs] 領域に入力します。

- [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。Cisco DNA Center では、このフィールドはシステムの情報に基づいて入力されます。
- [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。

（注） 手順 2f および 2j の間の任意の時点で、[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。その後、メインサイトを登録する前に、手順 2f を繰り返して正しい設定を入力する必要があります。

g) [Route advertisement] 領域で、次のいずれかのオプションボタンをクリックします。

- [Border Gateway Protocol (BGP)]：このオプションは、ほとんどのディザスタリカバリシステムで推奨されており、デフォルトで選択されています。BGP ルートアドバタイズメントにより、システムの現在アクティブなサイトに確実にアクセスすることができます。これはフェールオーバーの発生後に重要になります。
- [Disaster recovery VIPs without route advertisement]：ルートが BGP を使用してアドバタイズされないシステムの仮想 IP アドレスを設定する場合は、このオプションを選択します。このオプションは、メインサイトとリカバリサイトの両方が、システムのグローバル仮想 IP アドレスが存在するサブネットにアクセスできるデータセンターに適しています。
- [No disaster recovery VIPs]：このオプションを選択すると、サイトに設定された仮想 IP アドレスが、そのサイトに属するデバイスで自動的に設定されます。フェールオーバーが発生するたびに、これらの仮想 IP アドレスがデバイスで再設定されます。手順 2k に進みます。

h) 前の手順で最初の 2 つのオプションボタンのいずれかをクリックした場合は、[Enterprise VIP for Disaster Recovery] フィールドに値を入力します。

このフローティング仮想 IP アドレスを設定しておくと、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)] オプションボタンをクリックし、管理仮想 IP アドレスを設定しない場合は、手順 2j に進みます。
- [Disaster recovery VIPs without route advertisement] をクリックし、管理仮想 IP アドレスを設定しない場合は、手順 2k に進みます。

i) （任意） [Management VIP for Disaster Recovery] フィールドに値を入力します。

このフローティング仮想 IP アドレスを設定しておくと、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。

j) [Border Gateway Protocol (BGP)] オプションボタンをクリックした場合は、ルートアドバタイズメントを有効にするために必要な情報を入力します。

- [Border Gateway Protocol Type] 領域で、BGP ピアが相互に外部（[Exterior BGP (eBGP)]）セッションを確立するか、内部（[Interior BGP (iBGP)]）セッションを確立するかを指定します。
- [Main Site Router Settings for Enterprise Network] 領域および [Recovery Site Router Settings for Enterprise Network] 領域に、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設定されているエンタープライズ仮想 IP アドレスのアドバタイズのために Cisco DNA Center が使用するリモートルータの IP アドレスを入力します。また、ルータのリモートおよびローカル AS 番号も入力します。

  次の点に注意してください。

  - 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。サイトごとに最大 2 台のルータを設定できます。
  - AS 番号を入力する場合は、1 ー 4,294,967,295 の範囲内の 32 ビットの符号なし数であることを確認します。
  - [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。
  - 前の手順で管理仮想 IP アドレスを設定した場合は、[Main Site Router Settings for Management Network] 領域および [Recovery Site Router Settings for Management Network] 領域も表示されます。Cisco DNA Center でこの仮想 IP アドレスのアドバタイズに使用されるリモートルータに関する適切な情報を入力します。

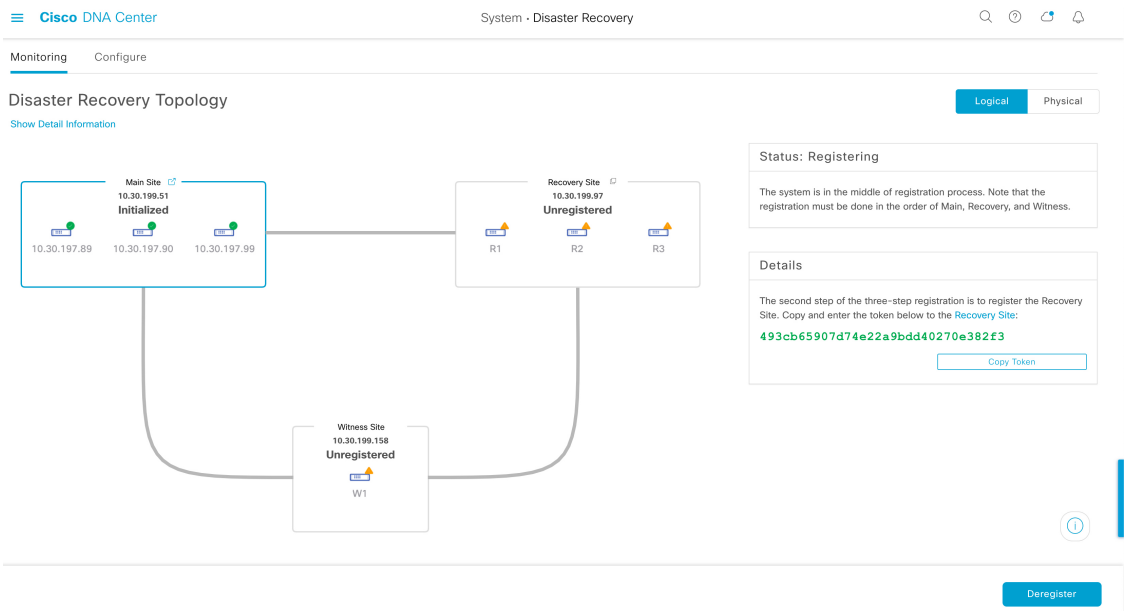
k) [Action] 領域で、[Register] をクリックします。

[Disaster Recovery Registration] ダイアログが開きます。

l) [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 [Details] 領域で、[Copy Token] をクリックします。



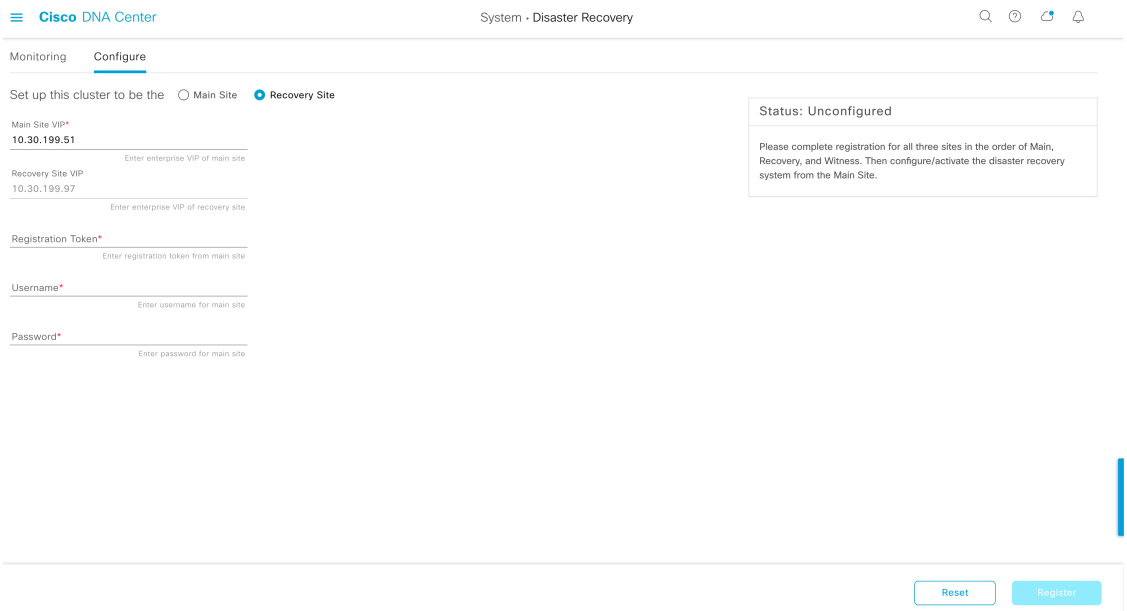
ステップ 4 リカバリサイトを登録します。

（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) [Details] 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、適切なユーザー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。



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。Cisco DNA Center では、このフィールドはシステムの情報に基づいて入力されます。
- 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ーに対して設定されたユーザー名とパスワード。

d) [Action] 領域で、[Register] をクリックします。

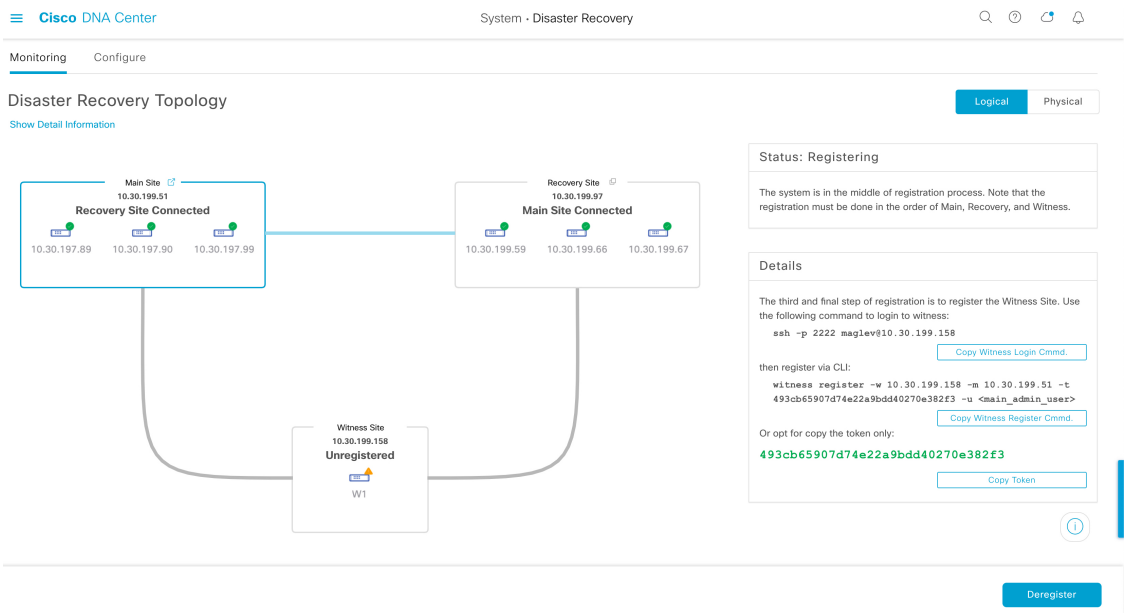
[Disaster Recovery Registration] ダイアログが開きます。

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。

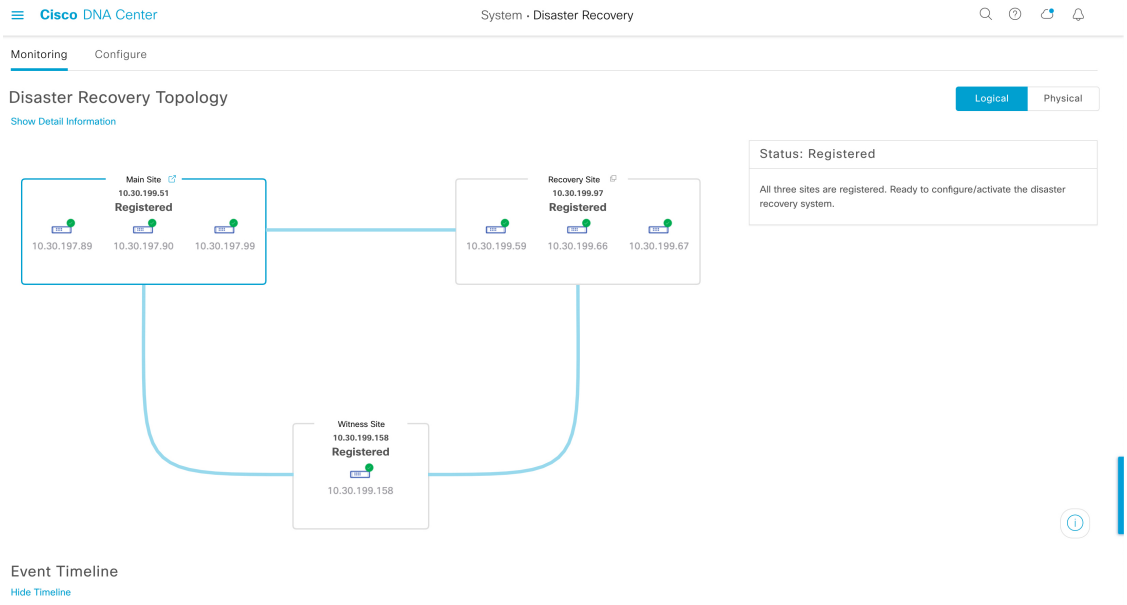
a) メインサイトのブラウザタブに戻ります。



b) [Details] 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ー（maglev）のパスワードを入力します。
e) [Details] 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ーのユーザー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ーのパスワードを入力します。

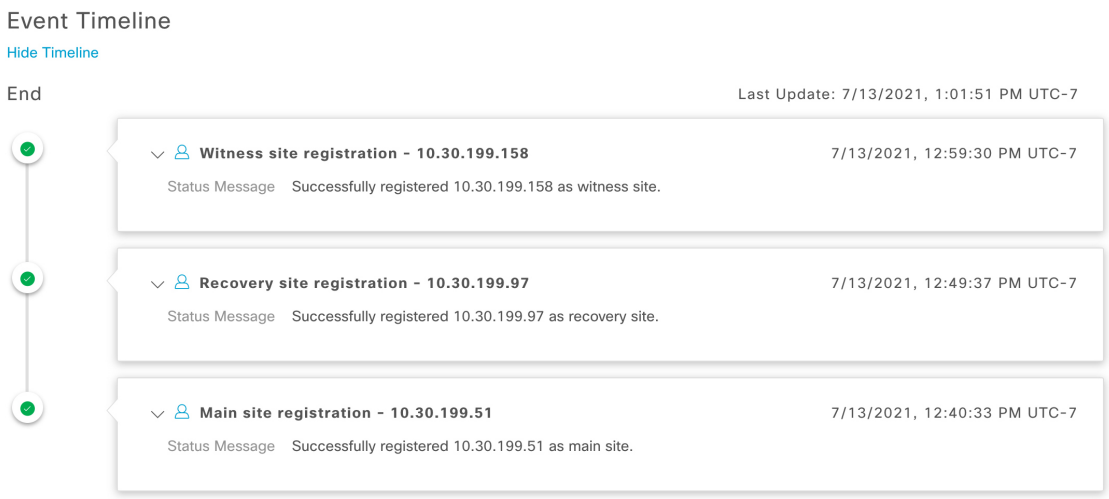
ステップ 6 メインサイト、リカバリサイト、および監視サイトが正常に登録されていることを確認します。

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。

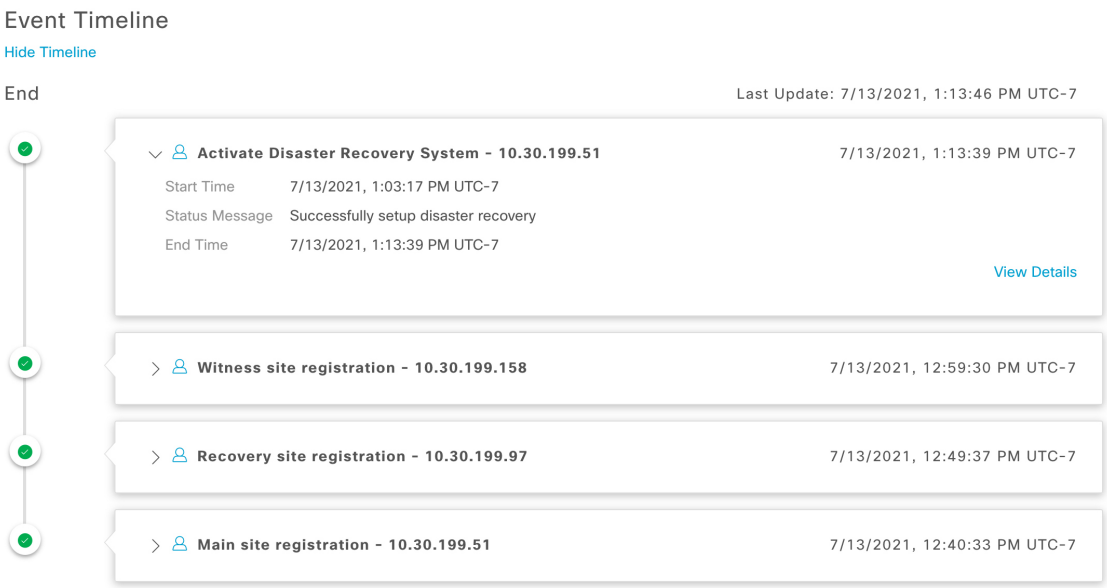
ステップ 8 ディザスタリカバリシステムの設定とメインサイトのデータのリカバリサイトへの複製を開始するには、[Continue] をクリックします。

（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。進捗状況をモニターするには、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。

2. イベントのタイムラインを表示し、[Activate Disaster Recovery System] 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ー（maglev）のパスワードを入力します。

（注） 次の手順に進む前に、監視サイトの IP アドレスをメモしておきます。監視サイトをアップグレードした後、同じアドレスを設定する必要があります。設定しない場合、監視サイトは期待どおりには機能しません。

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 監視サイトのインストール （13 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ー（maglev）のパスワードを入力します。

ステップ 6 **witness reconnect -w *witness-site's-IP-address* -m *system's-virtual-IP-address* -u *admin-username*** コマンドを実行します。

次の点に注意してください。

- メインサイトの現在のディザスタリカバリ ステータスに関係なく、監視サイトを再接続するときは、メインサイトのエンタープライズ VIP を使用します。
- このコマンドの実行後に監視サイトが動作していることを確認するには、次の手順を実行します。
  1. ディザスタリカバリトポロジから、[Show Detail Information] リンクをクリックして、[Disaster Recovery System] スライドインペインを開きます。
  2. [Witness Site] セクションで、監視サイトと設定済みの IPSec リンクのステータスが `[Up]` であることを確認します。
- このコマンドで使用可能なすべてのオプションを表示するには、**witness reconnect --help** 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] 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 （37 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 （16 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ーリング

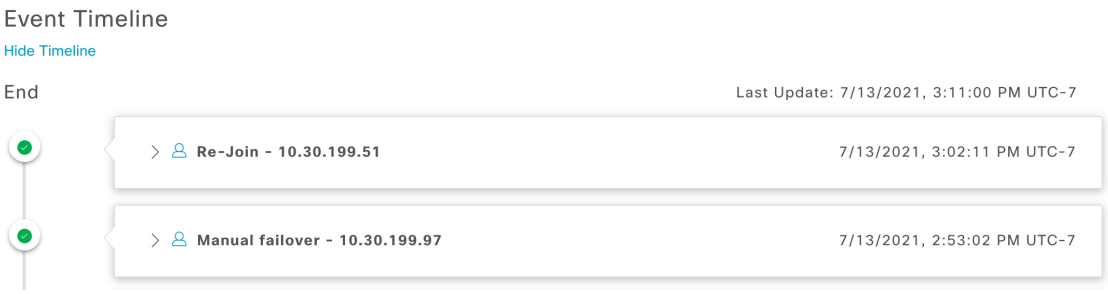
イベントのタイムラインから、現在実行されているディザスタリカバリタスクの進捗状況を追跡し、それらのタスクが完了したときに確認できます。タイムラインを表示するには、次の手順を実行します。

1. メニューアイコン（☰）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。

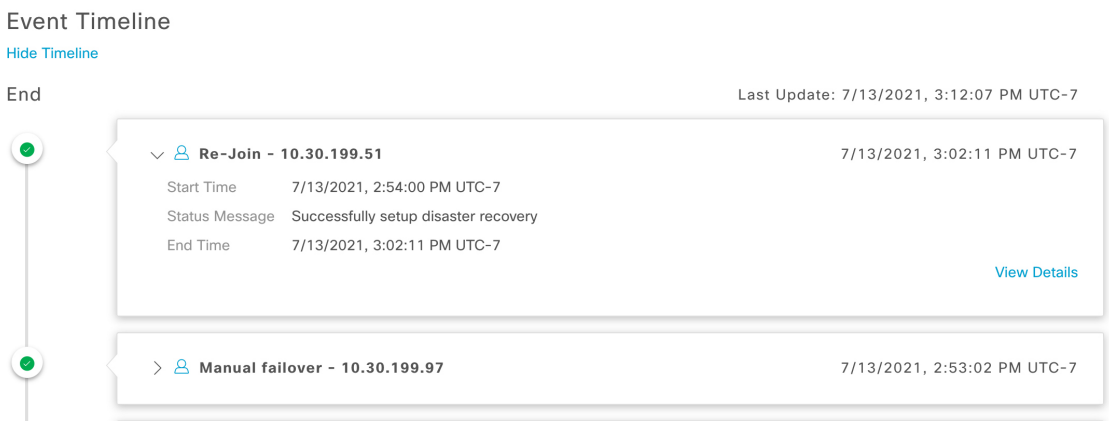
2. ページの下部までスクロールします。

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（⌨）またはユーザー（👤）のどちらによって開始されたかが示されます。

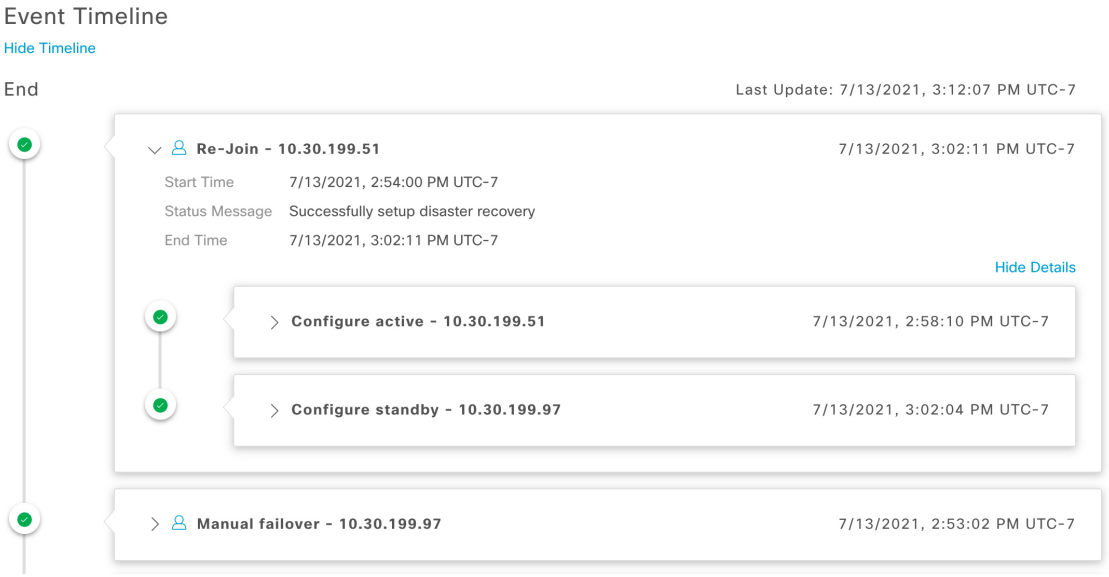


たとえば、システムの一時停止後の復元についてモニターするとします。この場合、復元プロセスの各タスクが開始されたときと完了したときに、Cisco DNA Center でイベントのタイムラ

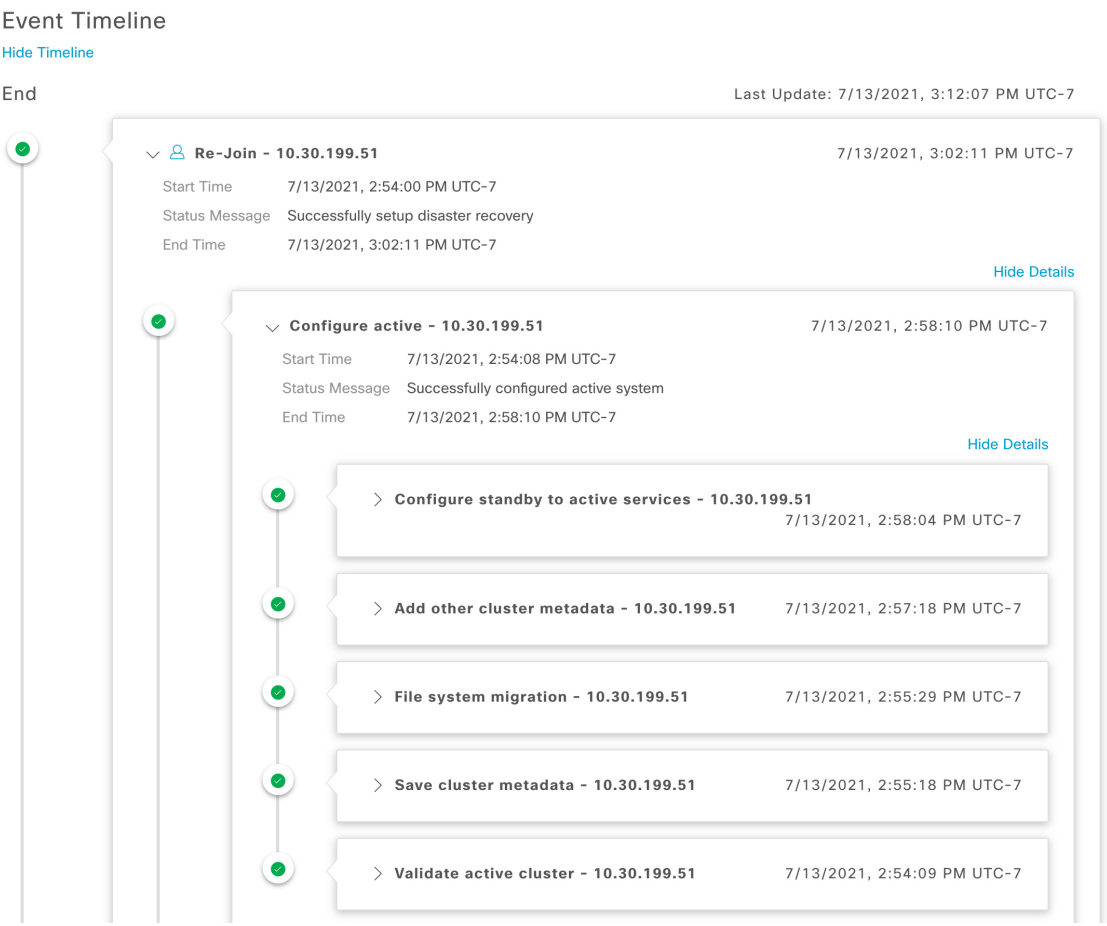
インが更新されます。特定のタスクにおける処理の概要を表示するには、[>] をクリックします。



タスクに対して [View Details] 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。



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。



イベントタイムラインのモニタリング中に発生する可能性のある問題とその解決方法については、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 （45 ページ）を参照してください。

システムおよびサイトの状態

ディザスタリカバリ GUI の [Status] 領域には、システムの現在の状態が表示されます。次の表で、トポロジに表示されるシステムの個々のサイトの状態を説明します。

表 *1:* アクティブサイトの状態

状態	説明
Unregistered	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。
Initializing	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために、他のサイトが必要とするデータを送信する準備をしています。
Initialized	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトに送信するデータを正常に準備しました。

状態	説明
Failed to Initialize	登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトが必要とするデータを送信する準備をしているときに、サイトでエラーが発生しました。
Connecting Recovery	メインサイトは、リカバリサイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Connecting Witness	メインサイトは、監視サイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Recovery Site Connected	メインサイトは、リカバリサイトとのセキュア通信を正常に確立しました。
Failed to Connect Recovery	リカバリサイトとの安全なチャネルを確立しているときに、メインサイトでエラーが発生しました。
Failed to Connect Witness	監視サイトとの安全なチャネルを確立しているときに、メインサイトでエラーが発生しました。
Registered	アクティブサイトは、他の 2 つのサイトとのセキュア通信を正常に確立しました。
Deregistering	システムから現在のディザスタリカバリ構成を削除します。
Deregister Failed	システムから現在のディザスタリカバリ構成を削除しているときにエラーが発生しました。
Validating	ディザスタリカバリ構成を開始する前に、システムの状態を検証しています。
Validated	ディザスタリカバリ構成を開始する前に、システムの状態を正常に検証しました。
Validation Failed	ディザスタリカバリ構成を開始する前にシステムの状態を検証中にエラーが発生しました。
Configuring Active	このサイトをアクティブサイトとして確立するためのワークフローを実行しています。
Failed to Configure	このサイトでディザスタリカバリを有効にするワークフローの実行中にエラーが発生しました。
Syncing Config Data	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しています。
Config Data Synced	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを正常に同期しました。
Active Sync Failed	保留中のアクティブサイトが、ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しているときにエラーが発生しました。

状態	説明
Waiting Standby Configuration	このサイトをアクティブサイトとして確立するためのワークフローが正常に完了しました。スタンバイサイトのワークフローが完了するのを待っています。
Active	サイトは、アクティブサイトとしてネットワークを正常に管理しています。
Failed to Configure	サイトは、ディザスタリカバリクラスタのアクティブサイトとして自身を有効にするワークフローの一部を実行できませんでした。
Isolating	サイトは、他の 2 つのサイトとの接続が失われたため、または（手動フェールオーバーの一部として）スタンバイ準備ができているため、自身を隔離するワークフローを実行しています。
Isolated	サイトは、他の 2 つのサイトとの接続が失われたため、または（手動フェールオーバーの一部として）スタンバイ準備ができているため、自身を隔離するワークフローを正常に実行しました。
Failed to Isolate	サイトは、他の 2 つのサイトとの接続が失われたため、または（手動フェールオーバーの一部として）スタンバイ準備ができているため、自身を隔離するワークフローを実行中にエラーが発生しました。
Configuring Active	（システムトリガーまたは手動フェールオーバーの一部として）以前のスタンバイサイトをアクティブサイトとして構成しています。
Failed during Failover	（フェールオーバーまたは 2 つのシステムの障害からのリカバリの一部として）このサイトをアクティブサイトとして確立するワークフローの実行中にエラーが発生しました。
Pausing Active	（管理操作または計画的な停止に備えるために）アクティブサイトでディザスタリカバリ操作を無効にするワークフローを実行しています。
Active Paused	アクティブサイトでディザスタリカバリ操作を無効にしました。
Failed to Pause Active	アクティブサイトでディザスタリカバリ操作を無効にしているときにエラーが発生しました。
Active Stand Alone	他の 2 つのサイトとの接続を失った以前のアクティブサイトを、すべてのディザスタリカバリ構成を削除することにより、独立したシステムとして確立するワークフローを実行しています。
Down	アクティブサイトは、他の 2 つのサイトとの接続を失いました。

表 *2:* スタンバイサイトの状態

状態	説明
Unregistered	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。

状態	説明
Initializing	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために、他のサイトが必要とするデータを送信する準備をしています。
Initialized	サイトは、登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトに送信するデータを正常に準備しました。
Failed to Initialize	登録プロセス中にディザスタリカバリクラスタをセットアップするために他のサイトが必要とするデータを送信する準備をしているときに、サイトでエラーが発生しました。
Connecting Main	リカバリサイトは、メインサイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Connecting Witness	リカバリサイトは、監視サイトに接続して、メインサイトとのセキュア通信をセットアップするために必要な初期化されたデータを取得しています。
Main Site Connected	リカバリサイトは、メインサイトとのセキュア通信を正常に確立しました。
Failed to Connect Main	メインサイトとの安全なチャネルを確立しているときに、リカバリサイトでエラーが発生しました。
Failed to Connect Witness	監視サイトとの安全なチャネルを確立しているときに、リカバリサイトでエラーが発生しました。
Registered	スタンバイサイトは、他の 2 つのサイトとのセキュア通信を正常に確立しました。
Deregistering	システムから現在のディザスタリカバリ構成を削除します。
Deregister Failed	システムから現在のディザスタリカバリ構成を削除しているときにエラーが発生しました。
Validating	ディザスタリカバリ構成を開始する前に、システムの状態を検証しています。
Validated	ディザスタリカバリ構成を開始する前に、システムの状態を正常に検証しました。
Validation Failed	ディザスタリカバリ構成を開始する前にシステムの状態を検証中にエラーが発生しました。
Configuring Standby	このサイトをスタンバイサイトとして確立するためのワークフローを実行しています。
Failed to Configure	このサイトでディザスタリカバリを有効にするワークフローの実行中にエラーが発生しました。
Syncing Config Data	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しています。

状態	説明
Config Data Synced	ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを正常に同期しました。
Standby Sync Failed	保留中のスタンバイサイトが、ディザスタリカバリシステムをセットアップするために他のサイトから必要なデータを同期しているときにエラーが発生しました。
Waiting Active Configuration	このサイトをスタンバイサイトとして確立するためのワークフローが正常に完了しました。アクティブサイトのワークフローが完了するのを待っています。
Standby	サイトは、ディザスタリカバリクラスタのスタンバイサイトとして正常に構成されています。
Failed to Configure	サイトは、ディザスタリカバリクラスタのスタンバイサイトとして自身を有効にするワークフローの一部を実行できませんでした。
Isolating	他の 2 つのサイトとの接続が失われたため、サイトは自身を隔離するワークフローを実行しています。
Isolated	他の 2 つのサイトとの接続が失われたため、サイトは自身を隔離するワークフローを正常に実行しました。
Failed to Isolate	他の 2 つのサイトとの接続が失われたため、サイトが自身を隔離するワークフローを実行中にエラーが発生しました。
Configuring Standby	（手動フェールオーバーの一部として）以前のアクティブサイトをスタンバイ準備サイトとして構成しています。
Standby Ready	以前のアクティブシステムは、（フェールオーバーの結果として）スタンバイシステムとして構成する準備ができています。
Pausing Standby	（管理操作または計画的な停止に備えるために）スタンバイサイトでディザスタリカバリ操作を無効にするワークフローを実行しています。
Standby Paused	スタンバイサイトでディザスタリカバリ操作を無効にしました。
Failed to Pause Standby	スタンバイサイトでディザスタリカバリ操作を無効にしているときにエラーが発生しました。
Standby Stand Alone	他の 2 つのサイトとの接続を失った以前のスタンバイサイトを、すべてのディザスタリカバリ構成を削除することにより、独立したシステムとして確立するワークフローを実行しています。
Down	サイトは、他の 2 つのサイトとの接続を失いました。

表 3: 監視サイトの状態

状態	説明
Unregistered	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	サイトは、他の 2 つのサイトとの接続を失いました。

ディザスタリカバリシステムのアップグレード

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、これを 2.3.3 にアップグレードします。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。アップグレードを完了するには、次の手順を実行します。

ステップ 1 システムの一時停止 （37 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バージョン 2.3.3 にアップグレードします。『Cisco DNA Center Upgrade Guide』の「Upgrade to Cisco DNA Center 2.3.3.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 （25 ページ）。

ステップ 4 システムへの再参加 （39 ページ）。

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ー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 メニューアイコン（☰）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。

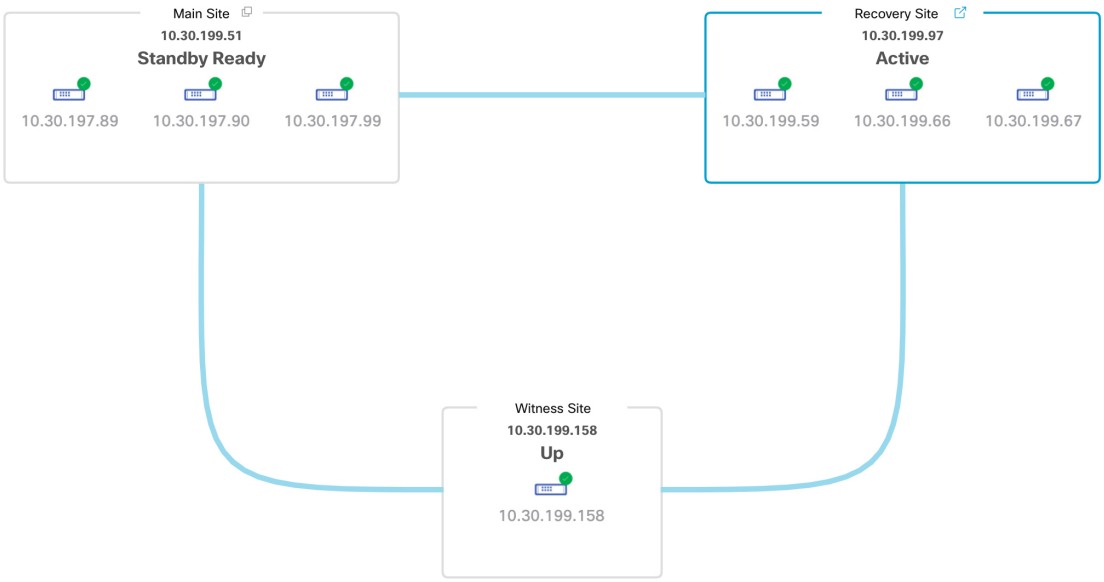
デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。次の例では、ユーザーは現在のアクティブサイトにログインしています。

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。



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ー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。

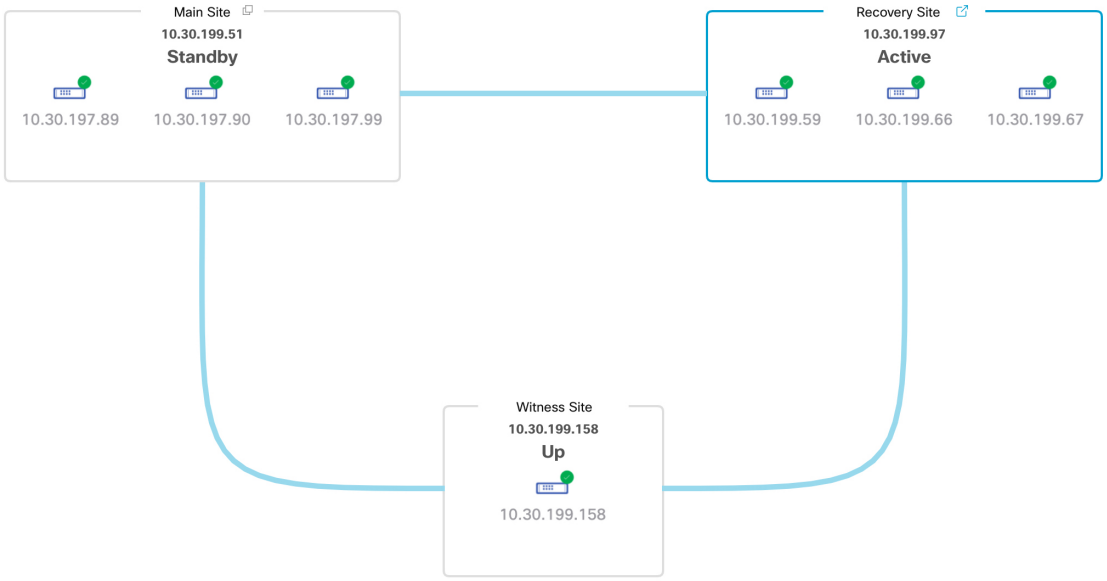
ステップ 4 メインサイトとリカバリサイトを再接続し、ディザスタリカバリシステムを再設定します。

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。

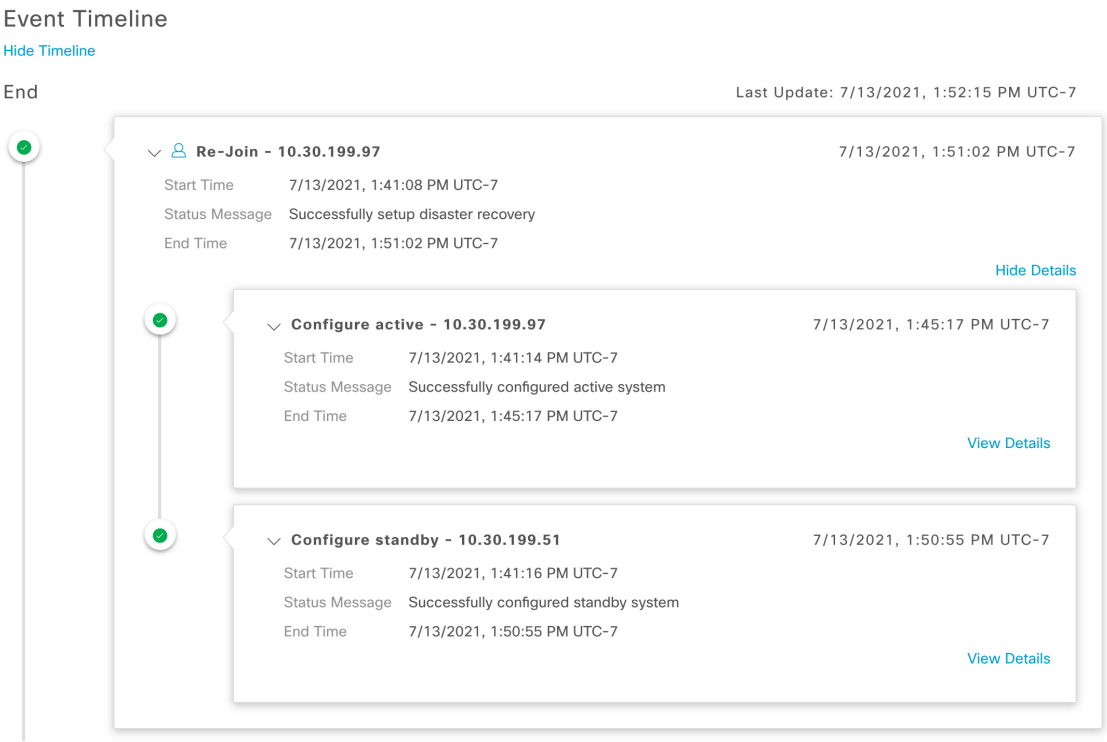
ステップ 5 [Continue] をクリックして次に進み、データの複製を再開します。

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。



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。



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、ディザスタリカバリシステムを一時停止して、次のいずれかを実行します。

- クラスタのアップグレードや追加パッケージのインストールなどの管理タスクを完了する
- システムまたはディザスタリカバリ証明書を置き換える
- メイン、リカバリ、または監視サイトクラスタでメンテナンスを実行する
- 計画的なネットワーク停止または停電に備える

システムの一時停止

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 メニューアイコン（☰）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。

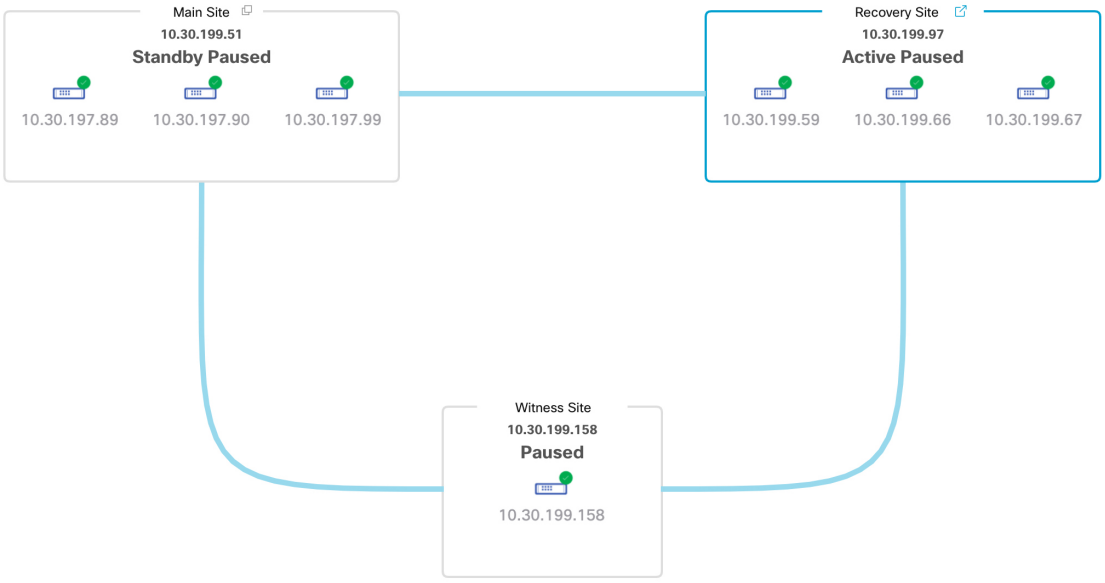
デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。

ステップ 2 [Action] 領域で、[Pause] 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。

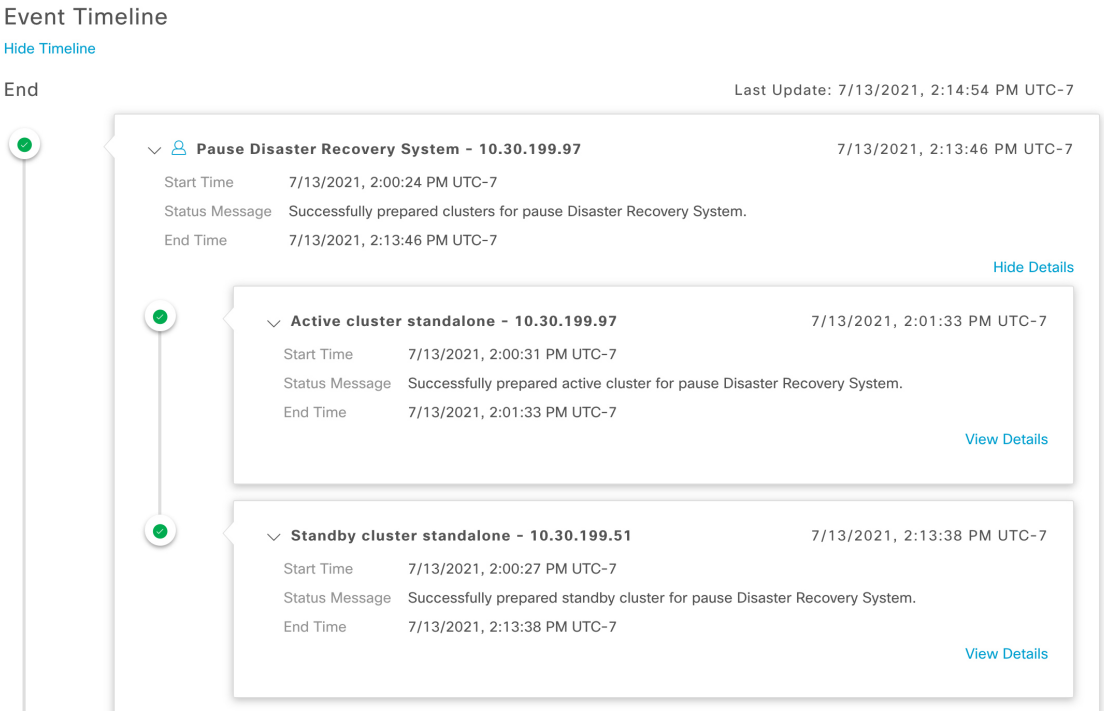
ページの右下隅に、システムを一時停止するプロセスが開始されたことを示すメッセージが表示されます。システムを一時停止するために、Cisco DNA Center でデータとサービスの複製が無効化されます。また、リカバリサイト側の停止していたサービスが再開されます。このプロセスの実行中は、トポロジにおいて、メインサイトとリカバリサイトのステータスが [Pausing] に設定されます。

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。



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] タブの右上に表示されたステータスが [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 Disaster Recovery System] タスクが正常に完了したことを確認します。



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 メニューアイコン（☰）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。

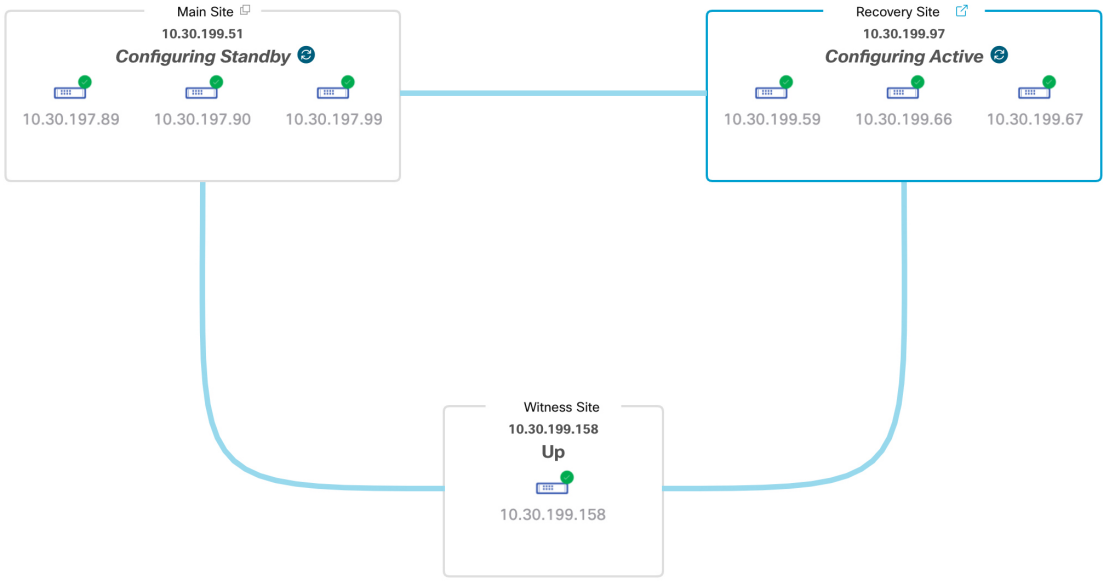
デフォルトでは、[Monitoring] タブが選択され、ディザスタリカバリシステムのトポロジが表示されます。

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

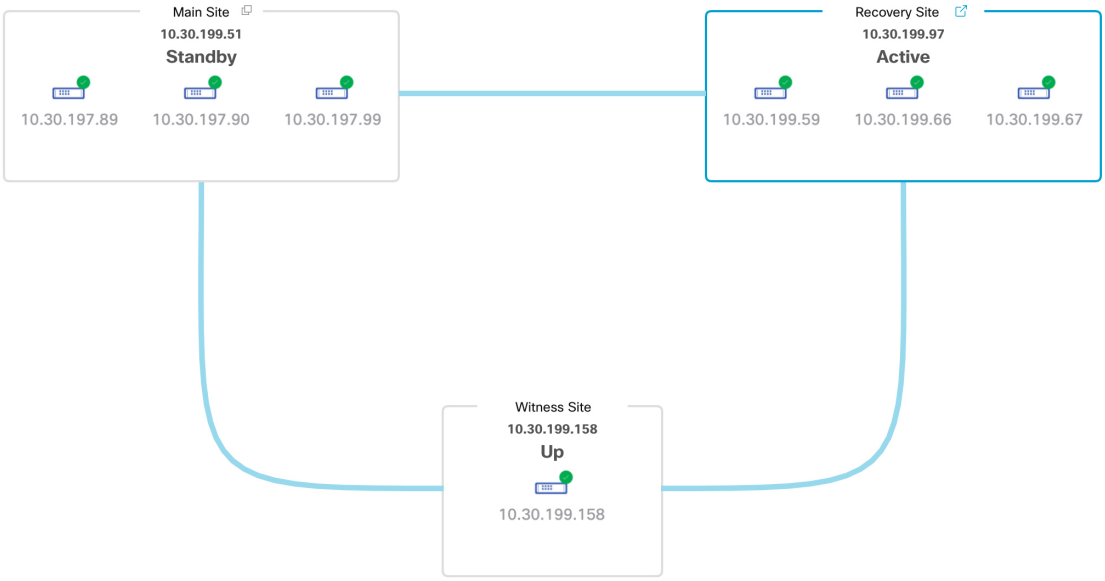
スタンバイサイトのすべてのデータが消去されることを示すダイアログが表示されます。

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。



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。



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。

ディザスタリカバリシステムの考慮事項

このセクションでは、ディザスタリカバリシステムを管理する際の注意事項について説明します。

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 （37 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 （39 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。

- フェールオーバーが発生すると、展開のバックアップと復元の設定およびスケジュールは、新しいアクティブサイトに複製されません。再度構成する必要があります。
- 展開に適用する場合は、Cisco DNA Center への着信 TLS 接続の TLS バージョンをアップグレードすることをお勧めします。『Cisco DNA CenterSecurity Best Practices Guide』の「Change the Minimum TLS Version and Enable RC4-SHA (Not Secure)」トピックを参照してください。

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。

ノードまたはクラスタの交換に関する考慮事項

ディザスタリカバリシステムの構成を壊さずに、次のいずれかを実行することはできません。

- 1+1+1 セットアップでノードの 1 つを置き換える。
- 3+3+1 セットアップで 1 つのサイトのすべてのノードを置き換える。

この必要がある場合は、システムの登録解除 （26ページ）で説明されている手順を完了して、システムを再起動してください。

再構成に関する考慮事項

リカバリサイトにあるアプライアンスに存在するデータは、次のシナリオで削除されます。

- ディザスタリカバリシステムを初めてセットアップし、システムをアクティブ化するとき。
- リカバリサイトが現在アクティブなサイトである場合に、システムを一時停止し、登録を解除してから、リカバリサイトとして再登録するとき。

既存のディザスタリカバリシステムを再構成するときは、どのサイトが現在アクティブなサイトであるかを確認し、それをシステムのメインサイトとして登録してください。または、リカバリサイトのデータ（現在アクティブな場合）のバックアップを作成し、システムの再構成の前にこのデータをシステムのメインサイトに復元することもできます。

HA に関する考慮事項

ディザスタリカバリシステムの構成を壊さずに、メインサイトとリカバリサイトを単一ノードクラスタから HA クラスタに変換することはできません。必要な場合は、次の手順を実行します。

1. システムの登録解除 （26 ページ）。
2. 両方のサイトを HA クラスタに変換します。

3. 再登録し、ディザスタリカバリを再アクティブ化します（ディザスタリカバリの設定（16ページ）を参照）。

サイト障害に関する考慮事項

デフォルトでは、ディザスタリカバリシステムは7分間待機してから、サイトに障害が発生したことを認識し、次のいずれかのアクションを実行します。

- アクティブサイトがダウンすると、フェールオーバープロセスが開始されます。
- スタンバイサイトまたは監視サイトのいずれかがダウンすると、システムはそのサイトをダウンとしてマークし、[Action] 領域からタスクを開始する機能を無効にします。

7分が経過する前にタスクを開始しようとすると、完了できない理由を示すメッセージが[Details]領域に表示されます。

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 Event Notifications」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（37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。メニューアイコン（☰）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（39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)`

システムのヘルスステータス	イベント	通知
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
OK	メインサイトの登録が正常に完了しました。	Successfully Registered Main Site
OK	リカバリサイトの登録が正常に完了しました。	Successfully Registered Recovery Site
OK	監視サイトの登録が正常に完了しました。	Successfully Registered Witness Site
OK	ディザスタリカバリシステムが正常に一時停止しました。	DR Pause Success
OK	スタンバイサイトが動作しています。	Standby Site Up
OK	監視サイトが動作しています。	Witness Site Up
OK	ディザスタリカバリシステムが正常に登録解除されました。	Unregister Success
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

システムのヘルスステータス	イベント	通知
NotOk	ディザスタリカバリシステムの登録解除に失敗しました。	`Unregistration Failed`
NotOk	メインサイトの登録に失敗しました。	`Main Registration Failed`
NotOk	リカバリサイトの登録に失敗しました。	`Recovery Registration Failed`
NotOk	監視サイトの登録に失敗しました。	`Witness Registration Failed`

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。

（注） ディザスタリカバリ操作が失敗またはタイムアウトした場合は、[Retry] をクリックして操作を再度実行します。問題が解消されず、その解決策が次の表に記載されていない場合は、Cisco TAC にお問い合わせください。

表 *4*: ディザスタリカバリシステムの問題

エラーコード	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 (`*`package names`*`) 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	`() site is trying to () with invalid IP address. Expected is (); actual is ().`	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 (`*`recovery or witness site`*`).`	メインサイトが稼働していることを確認します。

エラーコード	メッセージ	ソリューション
SODR10072	`All the nodes are not up for (main or recovery site).`	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。
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。 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. メニューアイコン（≡）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 サーバー証明書の更新」を参照してください。
SODR10113	`Save cluster metadata failed.`	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。
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 （54 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 （54 ページ）」を参照してください。
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。Cisco TAC に連絡して、サポートを受けてください。
SODR10124	`Cannot ping VIP: (main, recovery, or witness site's VIP or IP address).`	次の手順を実行します。 • 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。

エラーコード	メッセージ	ソリューション
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。 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。
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 Certificates]** 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	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。
—	`External postgres services does not exists to check service endpoints.`	次の手順を実行します。 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。 • **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。
—	`Success with errors.`	フェールオーバーの開始後またはディザスタリカバリシステムの一時停止後にこのメッセージが表示される場合は、1 つ以上のサービスで軽微なエラーが発生したにもかかわらず操作が正常に完了したことを示しています。先に進み、[Rejoin] をクリックすることで、システムを再起動できます。これらのエラーは、その操作によって解決されます。

エラーコード	メッセージ	ソリューション
—	`Failed.`	このメッセージは、1 つ以上のサービスで重大なエラーが発生したためにディザスタリカバリ操作が失敗したことを示しています。この障害をトラブルシューティングするために、イベントタイムラインを表示し、関連するエラーにドリルダウンすることをお勧めします。このメッセージが表示されたら、[Retry]をクリックして操作を再実行します。
—	`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。
—	`The GUI indicates that the standby site is still down after it has come back online.`	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。 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。 **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.** メニューアイコン（≡）をクリックして、**[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	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。 • **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。 • **kubectl get svc --all-namespaces | grep postgres** • **magctl service unexpose postgres** *<port-number>*

2 サイト障害シナリオ

2 サイト障害は、ディザスタリカバリシステムにある 3 つのサイトのうち少なくとも 2 つが同時にダウンした場合、またはサイトがパーティション化された場合に発生します。Cisco DNA Center がさまざまな障害シナリオにどのように対応するか、および実行する必要があるユーザーアクションについては、次の表を参照してください。

障害シナリオ	システムおよびユーザーの応答
シナリオ1：システムの2つのサイトがダウンします。	**1.** システムは、まだオンラインのサイトを分離します。 **重要** この操作が失敗した場合でも、このサイトをスタンドアロンサイトとして運用する場合は、手順 3 で説明されている最初のタスクを完了します。 **2.** このサイトにログインします。 **3.** サイトをスタンドアロンサイトとして動作させる場合は、[Standalone] をクリックし、表示されるダイアログボックスで [Continue] をクリックします。 サイトをスタンドアロンサイトとして動作させたくない場合は、まず、ダウンした 2 つのサイトを復旧します。次のいずれかを実行します。 • 監視サイトがオフラインのままである場合は、シナリオ 3 のシステムとユーザーの応答を参照してください。 • スタンバイサイトがオフラインのままの場合は、シナリオ 4 のシステムとユーザーの対応を参照してください。 • アクティブサイトがオフラインのままである場合は、シナリオ 5 のシステムとユーザーの応答を参照してください。 サイトがスタンドアロンモードになると、システムはそのサイトの仮想 IP アドレスを自動的に構成します。また、ネットワークの再プロビジョニングを防ぐために、仮想 IP アドレスルートをアドバタイズします。

障害シナリオ	システムおよびユーザーの応答
シナリオ2：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ダウンし、ほぼ同時にオンラインに戻ります。	1. システムは、アクティブサイトとスタンバイサイトを分離します。 2. システムはアクティブサイトを復元し、スタンバイサイトは [Standby Ready] 状態に入ります。 3. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムラインのモニターリング」を参照してください。 4. ディザスタリカバリの設定 （16 ページ）。
シナリオ3：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ダウンします。アクティブサイトとスタンバイサイトはオンラインに戻りますが、監視サイトはオフラインのままです。	1. システムは、アクティブサイトとスタンバイサイトを分離します。 2. システムはアクティブサイトを復元し、スタンバイサイトは [Standby Ready] 状態に入ります。 3. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムラインのモニターリング」を参照してください。 4. 次のいずれかを実行します。 • 監視サイトがオンラインに戻った後、ディザスタリカバリの設定 （16 ページ）に従います。 • システムの一時停止 （37 ページ）。

障害シナリオ	システムおよびユーザーの応答
シナリオ4：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ダウンします。アクティブサイトと監視サイトはオンラインに戻りますが、スタンバイサイトはオフラインのままです。	**1.** システムはアクティブサイトを分離してから復元します。 **2.** システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムラインのモニターリング」を参照してください。 **3.** 以前のアクティブサイトがオンラインに戻り、[Standby Ready] 状態になった後、ディザスタリカバリの設定 （16 ページ）に従います。 スタンバイサイトのノードを交換する必要があると判断した場合は、代わりに次の手順を実行します。 **1.** 監視サイトにログインして **witness reset** コマンドを実行します。 **2.** アクティブサイトにログインし、[Standalone] をクリックしてから、[Continue] をクリックします。 **3.** スタンバイサイトのノードを交換します。 **4.** 監視サイトが以前に使用されていたものよりも新しい仮想マシンを使用する場合は、監視サイトのインストール （13 ページ）で説明されている手順を実行します。それ以外の場合は、次のステップに進みます。 **5.** ディザスタリカバリの設定 （16 ページ）。

障害シナリオ	システムおよびユーザーの応答
シナリオ5：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ダウンします。スタンバイサイトと監視サイトはオンラインに戻り、アクティブサイトはオフラインのままです。	1. システムはスタンバイサイトを分離し、新しいアクティブサイトとして確立します。 2. システムが 2 つのシステム障害から回復したことが通知されます。 確認については、「イベントタイムラインのモニターリング」を参照してください。 3. 以前のアクティブサイトがオンラインに戻り、[Standby Ready] 状態になった後、ディザスタリカバリの設定 （16 ページ）に従います。 スタンバイサイトのノードを交換する必要があると判断した場合は、代わりに次の手順を実行します。 1. 監視サイトにログインして **witness reset** コマンドを実行します。 2. アクティブサイトにログインし、[Standalone] をクリックしてから、[Continue] をクリックします。 3. スタンバイサイトのノードを交換します。 4. 監視サイトが以前に使用されていたものよりも新しい仮想マシンを使用する場合は、監視サイトのインストール （13 ページ）で説明されている手順を実行します。それ以外の場合は、次のステップに進みます。 5. ディザスタリカバリの設定 （16 ページ）。

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 Disaster Recovery System]** > **[View Details]** > **[Configure active]** > **[View Details]** 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ールータが稼働しているかどうかを確認する。
2. ネイバールータと 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、ネイバー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) 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 | lql**

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。

d) 次のコマンドを実行して、Cisco DNA Center とそのネイバールータ間の 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、ネイバールータの 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ールータから、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 であるとします。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。

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。