NetApp Disaster Recoveryドキュメント

NetApp Disaster Recovery

NetApp
October 14, 2025

目次

NetApp Disaster Recoveryドキュメント

リリース ノート

NetApp Disaster Recoveryの新機能

NetApp Disaster Recoveryの新機能について説明します。

2025年10月6日

BlueXP disaster recoveryはNetApp Disaster Recoveryになりました

BlueXP disaster recoveryはNetApp Disaster Recoveryに名前が変更されました。

BlueXPはNetApp Consoleになりました

NetApp Consoleは、強化され再構築されたBlueXP基盤上に構築され、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのNetAppストレージとNetApp Data Servicesの集中管理を提供し、リアルタイムの分析情報、より高速なワークフロー、および高度なセキュリティとコンプライアンスを備えた簡素化された管理を実現します。

変更内容の詳細については、"NetApp Consoleのリリースノート" 。

その他のアップデート

- Amazon FSx for NetApp ONTAPを使用した Amazon Elastic VMware Service (EVS) のサポートはパブリックプレビュー段階です。このリリースにより、一般公開されました。詳細については、"Amazon Elastic VMware Service とAmazon FSx for NetApp ONTAPを使用したNetApp Disaster Recoveryの紹介" 。
- オンプレミス展開での検出時間の短縮を含む、ストレージ検出の改善
- ロールベースのアクセス制御（RBAC）や強化されたユーザー権限を含む、アイデンティティおよびアクセス管理（IAM）のサポート
- Azure VMware ソリューションとCloud Volumes ONTAPのプライベート プレビュー サポート。このサポートにより、 Cloud Volumes ONTAPストレージを使用して、オンプレミスから Azure VMware ソリューションへのディザスター リカバリー保護を構成できるようになりました。

2025年8月4日

バージョン4.2.5P2

NetApp Disaster Recoveryのアップデート

このリリースには次の更新が含まれています。

- 複数のストレージ仮想マシンから提示される同じ LUN を処理できるように VMFS サポートが改善されました。
- すでにアンマウントまたは削除されているデータストアを処理するために、テストのティアダウン クリーンアップが改善されました。
- サブネット マッピングが改善され、入力されたゲートウェイが指定されたネットワーク内に含まれているかどうかが検証されるようになりました。

- VM 名に「.com」が含まれている場合にレプリケーション プランが失敗する可能性がある問題を修正しました。
- レプリケーション プラン作成の一環としてボリュームを作成するときに、宛先ボリュームがソース ボリュームと同じになることを妨げる制限を削除しました。
- Azure Marketplace のNetApp Intelligent Services への従量課金制 (PAYGO) サブスクリプションのサポートが追加され、無料試用版ダイアログに Azure Marketplace へのリンクが追加されました。

  詳細については、 "NetApp Disaster Recoveryライセンス"そして "NetApp Disaster Recoveryのライセンスを設定する"。

2025年7月14日

バージョン4.2.5

NetApp Disaster Recoveryにおけるユーザーロール

NetApp Disaster Recoveryでは、各ユーザーの特定の機能やアクションへのアクセスを制御するためにロールを採用するようになりました。

このサービスは、NetApp Disaster Recoveryに固有の次のロールを使用します。

- ディザスタ リカバリ管理者: NetApp Disaster Recoveryであらゆるアクションを実行します。
- 災害復旧フェイルオーバー管理者: NetApp Disaster Recoveryでフェイルオーバーと移行アクションを実行します。
- 災害復旧アプリケーション管理者: レプリケーション プランを作成および変更し、テスト フェイルオーバーを開始します。
- ディザスタ リカバリ ビューアー: NetApp Disaster Recoveryの情報を表示できますが、アクションを実行することはできません。

NetApp Disaster Recoveryサービスをクリックして初めて構成する場合は、**SnapCenterAdmin** 権限または **Organization Admin** ロールが必要です。

詳細については、 "NetApp Disaster Recoveryにおけるユーザーの役割と権限" 。

"すべてのサービスのアクセスロールについて学ぶ" 。

NetApp Disaster Recoveryのその他のアップデート

- 強化されたネットワーク検出
- スケーラビリティの改善:
  - すべての詳細ではなく必要なメタデータをフィルタリングする
  - VM リソースをより速く取得および更新するための検出の改善
  - データ取得とデータ更新のためのメモリ最適化とパフォーマンス最適化
  - vCenter SDK クライアントの作成とプール管理の改善
- 次回のスケジュールされた検出または手動検出時の古いデータの管理:

- vCenter で VM が削除されると、 NetApp Disaster Recoveryによってその VM がレプリケーション プランから自動的に削除されるようになりました。
- vCenter でデータストアまたはネットワークが削除されると、 NetApp Disaster Recoveryによってレプリケーション プランとリソース グループからそれが削除されるようになりました。
- vCenter でクラスタ、ホスト、またはデータセンターが削除されると、 NetApp Disaster Recoveryによってレプリケーション プランとリソース グループからそれが削除されるようになりました。

- ブラウザのシークレット モードで Swagger ドキュメントにアクセスできるようになりました。NetApp Disaster Recovery内の [設定] オプション > [API ドキュメント] からアクセスするか、ブラウザのシークレット モードで次の URL から直接アクセスできます。 "Swaggerドキュメント" 。
- 状況によっては、フェイルバック操作後に、操作の完了後に iGroup が残されることがあります。このアップデートでは、古くなった iGroup が削除されます。
- レプリケーション プランで NFS FQDN が使用されていた場合、 NetApp Disaster Recovery はそれを IP アドレスに解決するようになりました。この更新は、災害復旧サイトで FQDN を解決できない場合に役立ちます。
- UIの配置の改善
- 検出が成功した後に vCenter のサイズ設定の詳細をキャプチャするためのログの改善

2025年6月30日

バージョン4.2.4P2

発見の改善

このアップデートにより検出プロセスが改善され、検出に必要な時間が短縮されます。

2025年6月23日

バージョン4.2.4P1

サブネットマッピングの改善

このアップデートでは、新しい検索機能によりサブネット マッピングの追加と編集ダイアログが強化されています。検索語を入力することで特定のサブネットをすばやく見つけることができるようになり、サブネット マッピングの管理が容易になりました。

2025年6月9日

バージョン4.2.4

Windows ローカル管理者パスワードソリューション **(LAPS)** のサポート

Windows ローカル管理者パスワード ソリューション (Windows LAPS) は、Active Directory 上のローカル管理者アカウントのパスワードを自動的に管理およびバックアップする Windows 機能です。

ドメイン コントローラーの詳細を指定して、サブネット マッピング オプションを選択し、LAPS オプションを確認できるようになりました。このオプションを使用すると、仮想マシンごとにパスワードを入力する必要がなくなります。

詳細については、 "レプリケーションプランを作成する" 。

2025年5月13日

バージョン4.2.3

サブネットマッピング

このリリースでは、サブネット マッピングを使用してフェイルオーバー時の IP アドレスを新しい方法で管理できるようになり、vCenter ごとにサブネットを追加できるようになりました。これを実行すると、各仮想ネットワークの IPv4 CIDR、デフォルト ゲートウェイ、および DNS が定義されます。

フェイルオーバー時に、 NetApp Disaster Recovery は、マッピングされた仮想ネットワークに提供された CIDR を調べて各 vNIC の適切な IP アドレスを決定し、それを使用して新しい IP アドレスを導出します。

例えば：

- ネットワークA = 10.1.1.0/24
- ネットワークB = 192.168.1.0/24

VM1 には、NetworkA に接続された vNIC (10.1.1.50) があります。レプリケーション プラン設定では、NetworkA は NetworkB にマップされます。

フェイルオーバー時に、 NetApp Disaster Recovery は元の IP アドレス (10.1.1) のネットワーク部分を置き換え、元の IP アドレス (10.1.1.50) のホスト アドレス (.50) を保持します。 VM1 の場合、 NetApp Disaster Recovery はNetworkB の CIDR 設定を確認し、NetworkB のネットワーク部分 192.168.1 を使用し、ホスト部分 (.50) を保持して VM1 の新しい IP アドレスを作成します。新しい IP は 192.168.1.50 になります。

要約すると、ホスト アドレスは同じままですが、ネットワーク アドレスはサイトのサブネット マッピングで構成されているものに置き換えられます。これにより、特に数百のネットワークと数千の VM を管理する場合に、フェイルオーバー時の IP アドレスの再割り当てをより簡単に管理できるようになります。

サイトにサブネットマッピングを含める方法の詳細については、以下を参照してください。 "vCenter Server サイトを追加する" 。

スキップ保護

レプリケーション プランのフェイルオーバー後にサービスが自動的に逆保護関係を作成しないように、保護をスキップできるようになりました。これは、NetApp Disaster Recovery内でサイトをオンラインに戻す前に、復元されたサイトで追加の操作を実行する場合に役立ちます。

フェールオーバーを開始すると、元のソース サイトがオンラインの場合、デフォルトでは、サービスによってレプリケーション プラン内の各ボリュームに対して逆方向の保護関係が自動的に作成されます。これは、サービスがターゲット サイトからソース サイトへのSnapMirror関係を作成することを意味します。また、フェイルバックを開始すると、このサービスはSnapMirror関係を自動的に元に戻します。

フェイルオーバーを開始するときに、*保護をスキップ*オプションを選択できるようになりました。これにより、サービスはSnapMirror関係を自動的に逆転させなくなります。代わりに、レプリケーション プランの両側に書き込み可能なボリュームを残します。

元のソース サイトがオンラインに戻った後、レプリケーション プランの [アクション] メニューから [リソースの保護] を選択して、逆方向の保護を確立できます。これにより、プラン内の各ボリュームに対して逆方向

のレプリケーション関係を作成しようとします。保護が復元されるまで、このジョブを繰り返し実行できます。保護が復元されると、通常の方法でフェイルバックを開始できます。

スキップ保護の詳細については、 "アプリケーションをリモートサイトにフェイルオーバーする" 。

SnapMirrorはレプリケーションプランで更新をスケジュールします

NetApp Disaster Recovery、ネイティブのONTAP SnapMirrorポリシー スケジューラやONTAPとのサードパーティ統合などの外部スナップショット管理ソリューションの使用がサポートされるようになりました。レプリケーション プラン内のすべてのデータストア (ボリューム) に、別の場所で管理されているSnapMirror関係がすでに存在する場合は、それらのスナップショットをNetApp Disaster Recoveryのリカバリ ポイントとして使用できます。

設定するには、レプリケーション プラン > リソース マッピング セクションで、データストア マッピングを設定するときに プラットフォーム管理のバックアップと保持スケジュールを使用する チェックボックスをオンにします。

このオプションを選択すると、 NetApp Disaster Recovery はバックアップ スケジュールを構成しません。ただし、テスト、フェイルオーバー、フェイルバック操作のためにスナップショットが作成される可能性があるため、保持スケジュールを構成する必要があります。

これが構成されると、サービスは定期的にスケジュールされたスナップショットを取得せず、代わりに外部エンティティに依存してスナップショットを取得および更新します。

レプリケーションプランで外部スナップショットソリューションを使用する方法の詳細については、 "レプリケーションプランを作成する" 。

2025年4月16日

バージョン4.2.2

VMのスケジュールされた検出

NetApp Disaster Recovery は24 時間ごとに検出を実行します。このリリースでは、ニーズに合わせて検出スケジュールをカスタマイズし、必要なときにパフォーマンスへの影響を軽減できるようになりました。たとえば、多数の VM がある場合は、検出スケジュールを 48 時間ごとに実行するように設定できます。 VM の数が少ない場合は、検出スケジュールを 12 時間ごとに実行するように設定できます。

検出をスケジュールしたくない場合は、スケジュールされた検出オプションを無効にして、いつでも手動で検出を更新できます。

詳細については、 "vCenter Server サイトを追加する" 。

リソース グループ データストアのサポート

以前は、VM ごとにのみリソース グループを作成できました。このリリースでは、データストアごとにリソース グループを作成できるようになりました。レプリケーション プランを作成し、そのプランのリソース グループを作成すると、データストア内のすべての VM が一覧表示されます。これは、多数の VM があり、それらをデータストアごとにグループ化したい場合に便利です。

次の方法で、データストアを含むリソース グループを作成できます。

- データストアを使用してリソース グループを追加する場合は、データストアの一覧を表示できます。 1 つ以上のデータストアを選択してリソース グループを作成できます。
- レプリケーション プランを作成し、プラン内にリソース グループを作成すると、データストア内の VM を確認できます。

詳細については、 "レプリケーションプランを作成する" 。

無料トライアルまたはライセンスの有効期限の通知

このリリースでは、ライセンスを取得する時間を確保するために、無料トライアルが 60 日後に期限切れになることを通知します。このリリースでは、ライセンスの有効期限が切れる日に通知も提供されます。

サービス更新の通知

このリリースでは、サービスがアップグレードされ、メンテナンス モードになっていることを示すバナーが上部に表示されます。バナーは、サービスのアップグレード中に表示され、アップグレードが完了すると消えます。アップグレードの進行中も UI での作業は続行できますが、新しいジョブを送信することはできません。更新が完了し、サービスが本番モードに戻った後に、スケジュールされたジョブが実行されます。

2025年3月10日

バージョン4.2.1

インテリジェントなプロキシサポート

NetApp Consoleエージェントはインテリジェント プロキシをサポートします。インテリジェント プロキシは、オンプレミス システムをNetApp Disaster Recoveryに接続するための軽量かつ安全で効率的な方法です。VPN や直接のインターネット アクセスを必要とせずに、システムとNetApp Disaster Recovery間の安全な接続を提供します。この最適化されたプロキシ実装は、ローカル ネットワーク内の API トラフィックをオフロードします。

プロキシが設定されている場合、 NetApp Disaster Recovery はVMware またはONTAPと直接通信を試み、直接通信が失敗した場合は設定されたプロキシを使用します。

NetApp Disaster Recoveryプロキシの実装では、コンソール エージェントと、HTTPS プロトコルを使用した vCenter Server およびONTAPアレイ間のポート 443 通信が必要です。コンソール エージェント内のNetApp Disaster Recoveryエージェントは、アクションを実行するときに VMware vSphere、VC、またはONTAPと直接通信します。

NetApp Disaster Recoveryのインテリジェントプロキシの詳細については、以下を参照してください。 "NetApp Disaster Recovery用のインフラストラクチャをセットアップする" 。

NetApp Consoleでの一般的なプロキシ設定の詳細については、以下を参照してください。 "プロキシサーバーを使用するようにコンソールエージェントを構成する" 。

無料トライアルはいつでも終了できます

無料トライアルはいつでも停止できます。また、有効期限が切れるまで待つこともできます。

見る "無料トライアルを終了する"。

2025年2月19日

バージョン4.2

VMFSストレージ上の**VM**およびデータストアに対する**ASA r2**のサポート

NetApp Disaster Recoveryのこのリリースでは、VM および VMFS ストレージ上のデータストアに対してASA r2 のサポートが提供されます。 ASA r2 システムでは、 ONTAPソフトウェアは基本的な SAN 機能をサポートしますが、SAN 環境でサポートされていない機能は削除されます。

このリリースでは、 ASA r2 の次の機能がサポートされています。

- プライマリ ストレージの整合性グループのプロビジョニング (フラットな整合性グループのみ、つまり階層構造のない 1 つのレベルのみ)
- SnapMirror自動化を含むバックアップ（コンシステンシグループ）操作

NetApp Disaster RecoveryにおけるASA r2 のサポートには、 ONTAP 9.16.1 が使用されます。

データストアはONTAPボリュームまたはASA r2 ストレージ ユニットにマウントできますが、 NetApp Disaster Recoveryのリソース グループにはONTAPのデータストアとASA r2 のデータストアの両方を含めることはできません。リソース グループでは、 ONTAPのデータストアまたはASA r2 のデータストアのいずれかを選択できます。

2024年10月30日

レポート

ランドスケープの分析に役立つレポートを生成してダウンロードできるようになりました。事前に設計されたレポートでは、フェイルオーバーとフェイルバックの概要、すべてのサイトのレプリケーションの詳細、過去 7 日間のジョブの詳細が表示されます。

参照 "災害復旧レポートを作成する"。

30日間無料トライアル

NetApp Disaster Recoveryの 30 日間無料トライアルに今すぐサインアップできます。以前は、無料トライアルは 90 日間でした。

参照 "ライセンスの設定"。

レプリケーションプランの無効化と有効化

以前のリリースには、日次および週次スケジュールをサポートするために必要だったフェールオーバー テスト スケジュール構造の更新が含まれていました。この更新では、新しい毎日および毎週のフェールオーバー テスト スケジュールを使用できるように、既存のすべてのレプリケーション プランを無効にしてから再度有効にする必要がありました。これは 1 回限りの要件です。

方法は次のとおりです。

1. メニューから*レプリケーション プラン*を選択します。
2. プランを選択し、[アクション] アイコンを選択してドロップダウン メニューを表示します。

3. *無効*を選択します。
4. 数分後、「有効」を選択します。

フォルダマッピング

レプリケーション プランを作成し、コンピューティング リソースをマップするときに、データセンター、クラスター、ホストに指定したフォルダーに VM が回復されるようにフォルダーをマップできるようになりました。

詳細については、 "レプリケーションプランを作成する" 。

フェイルオーバー、フェイルバック、テストフェイルオーバーに利用可能な **VM** の詳細

障害が発生し、フェイルオーバーを開始したり、フェイルバックを実行したり、フェイルオーバーをテストしたりするときに、VM の詳細を表示して、再起動しなかった VM を特定できるようになりました。

参照 "アプリケーションをリモートサイトにフェイルオーバーする"。

順序付けられたブートシーケンスによる **VM** ブート遅延

レプリケーション プランを作成するときに、プラン内の各 VM のブート遅延を設定できるようになりました。これにより、VM の起動シーケンスを設定して、後続の優先度の VM が起動される前に、優先度 1 の VM がすべて実行されていることを確認できます。

詳細については、 "レプリケーションプランを作成する" 。

VM オペレーティング システム情報

レプリケーション プランを作成すると、プラン内の各 VM のオペレーティング システムを確認できるようになりました。これは、VM をリソース グループにグループ化する方法を決定するのに役立ちます。

詳細については、 "レプリケーションプランを作成する" 。

VM名のエイリアシング

レプリケーション プランを作成するときに、災害復旧サイトの VM 名にプレフィックスとサフィックスを追加できるようになりました。これにより、プラン内の VM に、より説明的な名前を使用できるようになります。

詳細については、 "レプリケーションプランを作成する" 。

古いスナップショットをクリーンアップする

指定した保持数を超えて不要になったスナップショットは削除できます。スナップショットの保持数を減らすと、時間の経過とともにスナップショットが蓄積される可能性があります。これで、スナップショットを削除してスペースを解放できます。これは、オンデマンドでいつでも、またはレプリケーション プランを削除するときに実行できます。

詳細については、 "サイト、リソース グループ、レプリケーション プラン、データストア、仮想マシンの情報の管理" 。

スナップショットを調整する

ソースとターゲット間で同期されていないスナップショットを調整できるようになりました。これは、NetApp Disaster Recoveryの外部のターゲットでスナップショットが削除された場合に発生する可能性があります。サービスは、ソース上のスナップショットを 24 時間ごとに自動的に削除します。ただし、これをオンデマンドで実行できます。この機能により、すべてのサイト間でスナップショットの一貫性を確保できます。

詳細については、 "レプリケーションプランの管理" 。

2024年9月20日

オンプレミスからオンプレミスへの **VMware VMFS** データストアのサポート

このリリースには、オンプレミス ストレージに保護された iSCSI および FC 用の VMware vSphere 仮想マシン ファイル システム (VMFS) データストアにマウントされた VM のサポートが含まれています。以前は、このサービスは、iSCSI および FC 用の VMFS データストアをサポートする テクノロジー プレビュー を提供していました。

iSCSI プロトコルと FC プロトコルの両方に関する追加の考慮事項を次に示します。

- FC サポートは、レプリケーション用ではなく、クライアント フロントエンド プロトコル用です。
- NetApp Disaster Recovery、 ONTAPボリュームごとに 1 つの LUN のみをサポートします。ボリュームには複数の LUN を含めることはできません。
- どのレプリケーション プランでも、宛先ONTAPボリュームは、保護された VM をホストするソースONTAPボリュームと同じプロトコルを使用する必要があります。たとえば、ソースが FC プロトコルを使用する場合、宛先も FC を使用する必要があります。

2024年8月2日

FC 向けオンプレミスからオンプレミスへの **VMware VMFS** データストアのサポート

このリリースには、オンプレミス ストレージに保護された FC 用の VMware vSphere 仮想マシン ファイル システム (VMFS) データストアにマウントされた VM のサポートの テクノロジ プレビュー が含まれています。以前は、このサービスは iSCSI 用の VMFS データストアをサポートするテクノロジ プレビューを提供していました。

NetApp は、プレビューされたワークロード容量に対して料金を請求しません。

ジョブのキャンセル

このリリースでは、ジョブ モニター UI でジョブをキャンセルできるようになりました。

参照 "ジョブの監視"。

2024年7月17日

フェイルオーバーテストスケジュール

このリリースには、日次および週次スケジュールをサポートするために必要だったフェールオーバー テスト

スケジュール構造の更新が含まれています。この更新では、新しい毎日および毎週のフェールオーバー テスト スケジュールを使用できるように、既存のすべてのレプリケーション プランを無効にしてから再度有効にする必要があります。これは 1 回限りの要件です。

方法は次のとおりです。

1. メニューから*レプリケーション プラン*を選択します。
2. プランを選択し、[アクション] アイコンを選択してドロップダウン メニューを表示します。
3. *無効*を選択します。
4. 数分後、「有効」を選択します。

レプリケーションプランの更新

このリリースには、レプリケーション プラン データの更新が含まれており、「スナップショットが見つかりません」という問題が解決されています。これには、すべてのレプリケーション プランの保持数を 1 に変更し、オンデマンド スナップショットを開始する必要があります。このプロセスにより、新しいバックアップが作成され、古いバックアップはすべて削除されます。

方法は次のとおりです。

1. メニューから*レプリケーション プラン*を選択します。
2. レプリケーション プランを選択し、[フェールオーバー マッピング] タブをクリックして、[編集] 鉛筆アイコンをクリックします。
3. *データストア*矢印をクリックして展開します。
4. レプリケーション プランの保持カウントの値をメモします。これらの手順が完了したら、この元の値を復元する必要があります。
5. カウントを 1 に減らします。
6. オンデマンド スナップショットを開始します。これを行うには、[レプリケーション プラン] ページでプランを選択し、[アクション] アイコンをクリックして、[今すぐスナップショットを作成] を選択します。
7. スナップショット ジョブが正常に完了したら、レプリケーション プランのカウントを、最初の手順でメモした元の値に戻します。
8. 既存のすべてのレプリケーション プランに対してこれらの手順を繰り返します。

2024年7月5日

このNetApp Disaster Recoveryリリースには、次の更新が含まれています。

AFF Aシリーズのサポート

このリリースでは、 NetApp AFF A シリーズ ハードウェア プラットフォームがサポートされています。

オンプレミスからオンプレミスへの **VMware VMFS** データストアのサポート

このリリースには、オンプレミス ストレージに保護された VMware vSphere 仮想マシン ファイル システム (VMFS) データストアにマウントされた VM のサポートの テクノロジ プレビュー が含まれています。このリリースでは、オンプレミスの VMware ワークロードから VMFS データストアを備えたオンプレミスの VMware 環境への災害復旧がテクノロジー プレビューでサポートされます。

NetApp は、プレビューされたワークロード容量に対して料金を請求しません。

レプリケーションプランの更新

アプリケーション ページでデータストア別に VM をフィルタリングし、リソース マッピング ページでターゲットの詳細を選択することにより、レプリケーション プランをより簡単に追加できます。参照 "レプリケーションプランを作成する"。

レプリケーションプランを編集する

このリリースでは、フェイルオーバー マッピング ページが強化され、よりわかりやすくなりました。

参照 "プランを管理する"。

VMを編集する

このリリースでは、プラン内の VM を編集するプロセスに、いくつかの小さな UI の改善が加えられました。

参照 "VMを管理する"。

フェイルオーバー更新

フェイルオーバーを開始する前に、VM のステータスと、VM の電源がオンかオフかを確認できるようになりました。フェイルオーバー プロセスでは、今すぐスナップショットを作成したり、スナップショットを選択したりできるようになりました。

参照 "アプリケーションをリモートサイトにフェイルオーバーする"。

フェイルオーバーテストスケジュール

フェールオーバー テストを編集し、フェールオーバー テストの日次、週次、月次スケジュールを設定できるようになりました。

参照 "プランを管理する"。

前提条件情報の更新

NetApp Disaster Recovery の前提条件情報が更新されました。

参照 "NetApp Disaster Recoveryの前提条件"。

2024年5月15日

このNetApp Disaster Recoveryリリースには、次の更新が含まれています。

VMware ワークロードをオンプレミスからオンプレミスに複製する

これは一般提供機能としてリリースされました。以前は、機能が制限されたテクノロジ プレビューでした。

ライセンスの更新

NetApp Disaster Recoveryでは、90 日間の無料トライアルにサインアップしたり、Amazon Marketplace で従量課金制 (PAYGO) サブスクリプションを購入したり、NetApp の営業担当者またはNetAppサポート サイト (NSS) から取得したNetAppライセンス ファイル (NLF) である Bring Your NetApp License (BYOL) を使用したりすることができます。

NetApp Disaster Recoveryのライセンス設定の詳細については、以下を参照してください。"ライセンスの設定" 。

"NetApp Disaster Recoveryの詳細" 。

2024年3月5日

これはNetApp Disaster Recoveryの一般提供リリースであり、次の更新が含まれています。

ライセンスの更新

NetApp Disaster Recoveryでは、90 日間の無料トライアルにサインアップするか、 NetApp の営業担当者から取得したNetAppライセンス ファイル (NLF) である Bring Your Own License (BYOL) を使用することができます。ライセンス シリアル番号を使用して、 NetApp Consoleサブスクリプションで BYOL をアクティブ化できます。 NetApp Disaster Recovery料金は、データストアのプロビジョニングされた容量に基づいて決まります。

NetApp Disaster Recoveryのライセンス設定の詳細については、以下を参照してください。 "ライセンスの設定" 。

すべてのNetApp Consoleデータサービスのライセンス管理の詳細については、 "すべてのNetApp Consoleデータサービスのライセンスを管理する" 。

スケジュールを編集する

このリリースでは、コンプライアンス テストとフェイルオーバー テストのスケジュールを設定して、必要に応じて正しく動作することを確認できるようになりました。

詳細については、 "レプリケーションプランを作成する" 。

2024年2月1日

このNetApp Disaster Recoveryプレビュー リリースには、次の更新が含まれています。

ネットワークの強化

このリリースでは、VM の CPU と RAM の値のサイズを変更できるようになりました。また、VM のネットワーク DHCP または静的 IP アドレスを選択することもできます。

- DHCP: このオプションを選択した場合は、VM の資格情報を提供します。
- 静的 IP: ソース VM と同じ情報または異なる情報を選択できます。ソースと同じものを選択した場合は、資格情報を入力する必要はありません。一方、ソースとは異なる情報を使用する場合は、資格情報、IP アドレス、サブネット マスク、DNS、ゲートウェイ情報を提供できます。

詳細については、 "レプリケーションプランを作成する" 。

カスタムスクリプト

フェイルオーバー後のプロセスとして含めることができるようになりました。カスタム スクリプトを使用すると、フェイルオーバー プロセス後にNetApp Disaster Recoveryでスクリプトを実行できます。たとえば、カスタム スクリプトを使用して、フェイルオーバーが完了した後にすべてのデータベース トランザクションを再開できます。

詳細については、 "リモートサイトへのフェイルオーバー" 。

SnapMirror関係

レプリケーション プランを開発しながらSnapMirror関係を作成できるようになりました。以前は、 NetApp Disaster Recoveryの外部で関係を作成する必要がありました。

詳細については、 "レプリケーションプランを作成する" 。

一貫性グループ

レプリケーション プランを作成するときに、異なるボリュームおよび異なる SVM からの VM を含めることができます。 NetApp Disaster Recovery は、すべてのボリュームを含めて整合性グループのスナップショットを作成し、すべてのセカンダリ ロケーションを更新します。

詳細については、 "レプリケーションプランを作成する" 。

VM電源オン遅延オプション

レプリケーション プランを作成するときに、リソース グループに VM を追加できます。リソース グループを使用すると、各 VM に遅延を設定して、遅延されたシーケンスで VM の電源をオンにすることができます。

詳細については、 "レプリケーションプランを作成する" 。

アプリケーション整合性のあるスナップショットコピー

アプリケーション整合性のあるスナップショット コピーを作成するように指定できます。サービスはアプリケーションを静止させ、スナップショットを取得してアプリケーションの一貫した状態を取得します。

詳細については、 "レプリケーションプランを作成する" 。

2024年1月11日

NetApp Disaster Recoveryのこのプレビュー リリースには、次の更新が含まれています。

ダッシュボードをより速く

このリリースでは、ダッシュボードから他のページの情報にさらに迅速にアクセスできるようになりました。

"NetApp Disaster Recoveryについて学ぶ" 。

2023年10月20日

NetApp Disaster Recoveryのこのプレビュー リリースには、次の更新が含まれています。

オンプレミスの **NFS** ベースの **VMware** ワークロードを保護する

NetApp Disaster Recovery を使用すると、パブリック クラウドに加えて、オンプレミスの NFS ベースの VMware 環境を別のオンプレミスの NFS ベースの VMware 環境への災害から保護できるようになります。NetApp Disaster Recovery は、災害復旧計画の完了を調整します。

> このプレビュー オファリングでは、 NetApp は一般提供開始前にオファリングの詳細、内容、およびタイムラインを変更する権利を留保します。

"NetApp Disaster Recoveryの詳細" 。

2023年9月27日

NetApp Disaster Recoveryのこのプレビュー リリースには、次の更新が含まれています。

ダッシュボードの更新

ダッシュボードのオプションをクリックできるようになり、情報をすばやく簡単に確認できるようになりました。また、ダッシュボードにはフェイルオーバーと移行のステータスが表示されるようになりました。

参照 "ダッシュボードで災害復旧計画の健全性を確認する"。

レプリケーションプランの更新

- **RPO**: レプリケーション プランのデータストア セクションで、復旧ポイント目標 (RPO) と保持数を入力できるようになりました。これは、設定された時間よりも古くない、存在する必要があるデータの量を示します。たとえば、これを 5 分に設定すると、災害が発生した場合にシステムが最大 5 分間のデータを失っても、ビジネスクリティカルなニーズには影響しません。

  参照 "レプリケーションプランを作成する"。

- ネットワークの機能強化: レプリケーション プランの仮想マシン セクションでソースとターゲットの場所の間でネットワークをマッピングするときに、 NetApp Disaster RecoveryDHCP または静的 IP の 2 つのオプションが提供されるようになりました。以前は、DHCP のみがサポートされていました。静的 IP の場合は、サブネット、ゲートウェイ、および DNS サーバーを構成します。さらに、仮想マシンの資格情報を入力できるようになりました。

  参照 "レプリケーションプランを作成する"。

- スケジュールの編集: レプリケーション プランのスケジュールを更新できるようになりました。

  参照 "リソースを管理する"。

- * SnapMirror の自動化*: このリリースでレプリケーション プランを作成するときに、次のいずれかの構成でソース ボリュームとターゲット ボリューム間のSnapMirror関係を定義できます。
  - 1〜1
  - ファンアウトアーキテクチャにおける1対多
  - 一貫性グループとしての多対1
  - 多対多

参照 "レプリケーションプランを作成する"。

2023年8月1日

NetApp Disaster Recoveryプレビュー

NetApp Disaster Recoveryプレビューは、災害復旧ワークフローを自動化するクラウドベースの災害復旧サービスです。最初に、 NetApp Disaster Recoveryプレビューを使用すると、 Amazon FSx for ONTAPを使用して、 NetAppストレージを実行しているオンプレミスの NFS ベースの VMware ワークロードを AWS 上の VMware Cloud (VMC) に保護できます。

> このプレビュー オファリングでは、 NetApp は一般提供開始前にオファリングの詳細、内容、およびタイムラインを変更する権利を留保します。

"NetApp Disaster Recoveryの詳細" 。

このリリースには次の更新が含まれています。

ブート順序のリソース グループの更新

災害復旧またはレプリケーション プランを作成するときに、機能リソース グループに仮想マシンを追加できます。リソース グループを使用すると、依存関係にある仮想マシンのセットを、要件を満たす論理グループにまとめることができます。たとえば、グループには回復時に実行できるブート順序を含めることができます。このリリースでは、各リソース グループに 1 つ以上の仮想マシンを含めることができます。仮想マシンは、プランに含めた順序に基づいて電源がオンになります。参照 "複製するアプリケーションを選択し、リソース グループを割り当てます"。

レプリケーション検証

災害復旧またはレプリケーション プランを作成し、ウィザードで繰り返しを指定して、災害復旧サイトへのレプリケーションを開始すると、 NetApp Disaster Recovery は30 分ごとに、レプリケーションがプランに従って実際に実行されているかどうかを確認します。ジョブ モニター ページで進行状況を監視できます。。 "アプリケーションを別のサイトに複製する" 。

レプリケーション計画は、リカバリポイント目標（**RPO**）の転送スケジュールを示します。

災害復旧またはレプリケーション プランを作成するときに、VM を選択します。このリリースでは、データストアまたは VM に関連付けられている各ボリュームに関連付けられているSnapMirror を表示できるようになりました。SnapMirrorスケジュールに関連付けられている RPO 転送スケジュールも表示できます。RPO は、災害後の復旧にバックアップ スケジュールが十分かどうかを判断するのに役立ちます。参照 "レプリケーションプランを作成する"。

ジョブモニターの更新

ジョブ モニター ページに更新オプションが追加され、操作の最新ステータスを取得できるようになりました。。 "災害復旧ジョブを監視する" 。

2023年5月18日

これはNetApp Disaster Recoveryの最初のリリースです。

クラウドベースの災害復旧サービス

NetApp Disaster Recovery は、災害復旧ワークフローを自動化するクラウドベースの災害復旧サービスです。最初に、 NetApp Disaster Recoveryプレビューを使用すると、 Amazon FSx for ONTAPを使用して、 NetApp ストレージを実行しているオンプレミスの NFS ベースの VMware ワークロードを AWS 上の VMware Cloud (VMC) に保護できます。

"NetApp Disaster Recoveryの詳細" 。

NetApp Disaster Recoveryの限界

既知の制限事項では、このリリースのサービスでサポートされていない、または正しく相互運用されないプラットフォーム、デバイス、または機能が特定されます。

フェイルバックが完了するまで待ってから検出を実行してください

フェイルオーバーが完了したら、ソース vCenter で検出を手動で開始しないでください。フェイルバックが完了するまで待ってから、ソース vCenter で検出を開始します。

NetApp ConsoleがAmazon FSx for NetApp ONTAPを検出しない可能性があります

場合によっては、 NetApp ConsoleでAmazon FSx for NetApp ONTAPクラスターが検出されないことがあります。 FSx 資格情報が正しくなかったことが原因である可能性があります。

回避策: NetApp ConsoleにAmazon FSx for NetApp ONTAPクラスターを追加し、定期的にクラスターを更新して変更を表示します。

NetApp Disaster RecoveryからONTAP FSx クラスターを削除する必要がある場合は、次の手順を実行します。

1. NetApp Consoleエージェントでは、クラウドプロバイダーの接続オプションを使用して、コンソールエージェントが実行されるLinux VMに接続し、 `docker restart occm`指示。

参照 "既存のコンソールエージェントを管理する"。

1. NetApp Consoleシステム ページで、 Amazon FSx for ONTAPシステムを再度追加し、FSx 認証情報を入力します。

   参照 "Amazon FSx for NetApp ONTAPファイルシステムを作成する"。

2. NetApp Disaster Recoveryから*Sites*を選択し、vCenter行で*Actions*オプションを選択します。  をクリックし、[アクション] メニューから [更新] を選択して、 NetApp Disaster Recoveryの FSx 検出を更新します。

   これにより、データストア、その仮想マシン、およびその宛先関係が再検出されます。

始めましょう

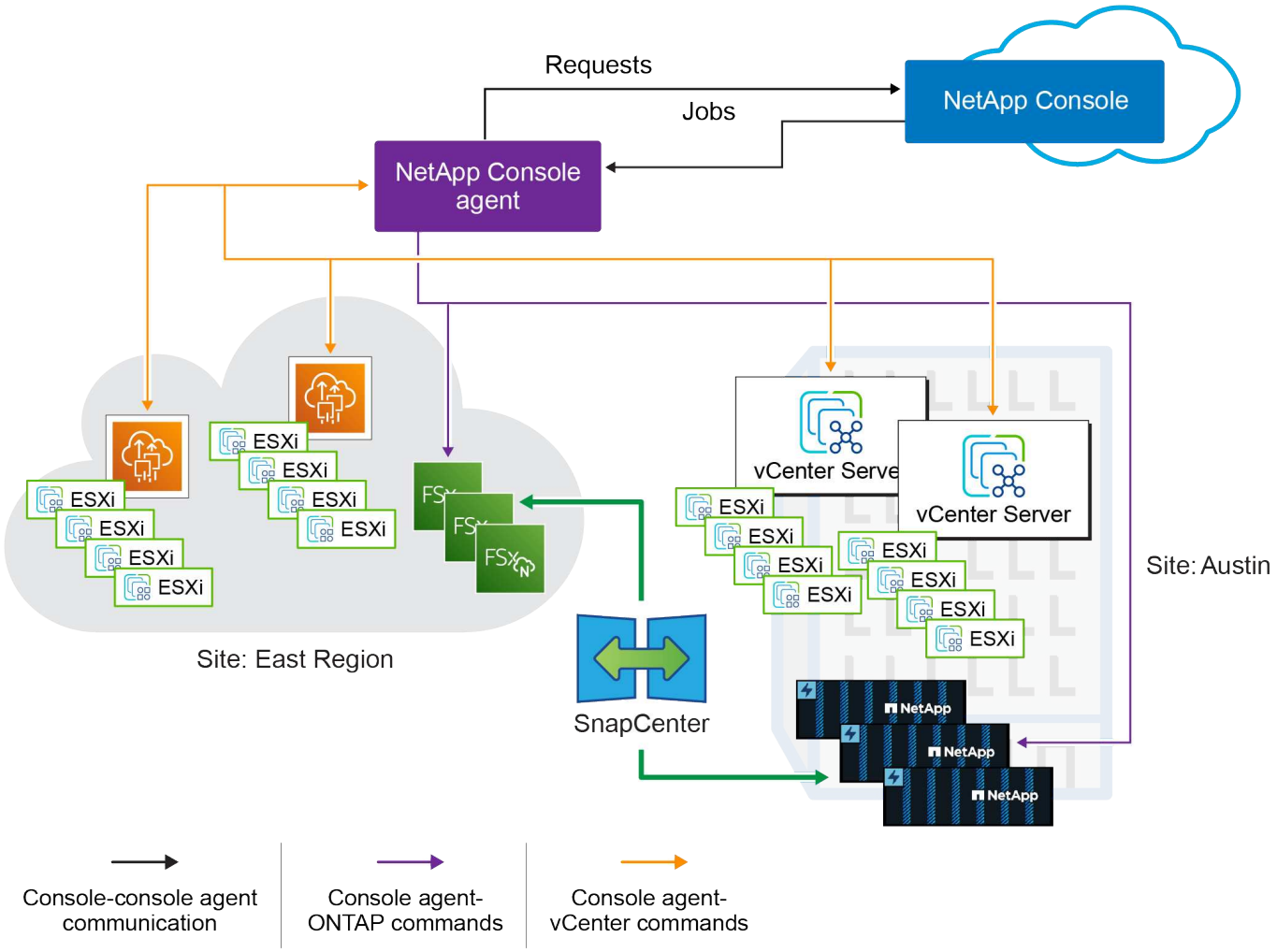
NetApp Disaster Recoveryについて学ぶ

クラウドへの災害復旧は、サイトの停止やデータ破損イベントからワークロードを保護する、回復力がありコスト効率に優れた方法です。 NetApp Disaster Recovery for VMware を使用すると、 ONTAPストレージを実行しているオンプレミスの VMware VM またはデータストアのワークロードを、 NetAppクラウド ストレージを使用してパブリック クラウド内の VMware ソフトウェア定義データセンターにレプリケートしたり、ONTAPストレージをディザスタ リカバリ サイトとして使用している別のオンプレミスの VMware 環境にレプリケートしたりできます。ディザスタ リカバリを使用して、VM ワークロードをあるサイトから別のサイトに移行することもできます。

NetApp Disaster Recovery は、災害復旧ワークフローを自動化するクラウドベースの災害復旧サービスです。NetApp Disaster Recoveryを使用すると、オンプレミスの NFS ベースのワークロードと、iSCSI および FC で実行されるNetAppストレージの VMware vSphere 仮想マシン ファイル システム (VMFS) データストアを次のいずれかに保護できます。

- VMware Cloud (VMC) on AWS とAmazon FSx for NetApp ONTAP
- Amazon Elastic VMware Service (EVS) とAmazon FSx for NetApp ONTAP の詳細については、"Amazon Elastic VMware Service とAmazon FSx for NetApp ONTAPを使用したNetApp Disaster Recoveryの紹介" 。
- Azure VMware Solution (AVS) とNetApp Cloud Volumes ONTAP (iSCSI) (プライベート プレビュー)
- ONTAPストレージを備えた別のオンプレミス NFS または VMFS ベース (iSCSI/FC) VMware 環境

NetApp Disaster Recovery は、統合されたネイティブ VMware オーケストレーションを備えたONTAP SnapMirrorテクノロジーを使用して、 ONTAPのすべてのストレージ効率の利点を維持しながら、VMware VM とそれに関連付けられたディスク上の OS イメージを保護します。災害復旧では、これらのテクノロジを災害復旧サイトへのレプリケーション トランスポートとして使用します。これにより、プライマリ サイトとセカンダリ サイトで業界最高のストレージ効率 (圧縮と重複排除) が実現されます。



NetApp Console

NetApp Disaster Recovery には、NetApp Consoleからアクセスできます。

NetApp Consoleは、オンプレミスとクラウド環境全体にわたるエンタープライズ グレードのNetAppストレージとデータ サービスの集中管理を提供します。NetAppデータ サービスにアクセスして使用するには、コンソールが必要です。管理インターフェースとして、1 つのインターフェースから多数のストレージ リソースを管理できます。コンソール管理者は、企業内のすべてのシステムのストレージとサービスへのアクセスを制御できます。

NetApp Consoleの使用を開始するためにライセンスやサブスクリプションは必要ありません。ストレージ システムまたはNetAppデータ サービスへの接続を確保するためにクラウドにコンソール エージェントを展開する必要がある場合にのみ料金が発生します。ただし、コンソールからアクセスできる一部のNetAppデータ サービスは、ライセンスまたはサブスクリプションベースです。

詳細はこちら "NetApp Console"。

NetApp Disaster Recovery for VMware を使用するメリット

NetApp Disaster Recoveryには次のような利点があります。

- 複数のポイントインタイムリカバリ操作によるアプリケーションの vCenter 検出およびリカバリのユーザ

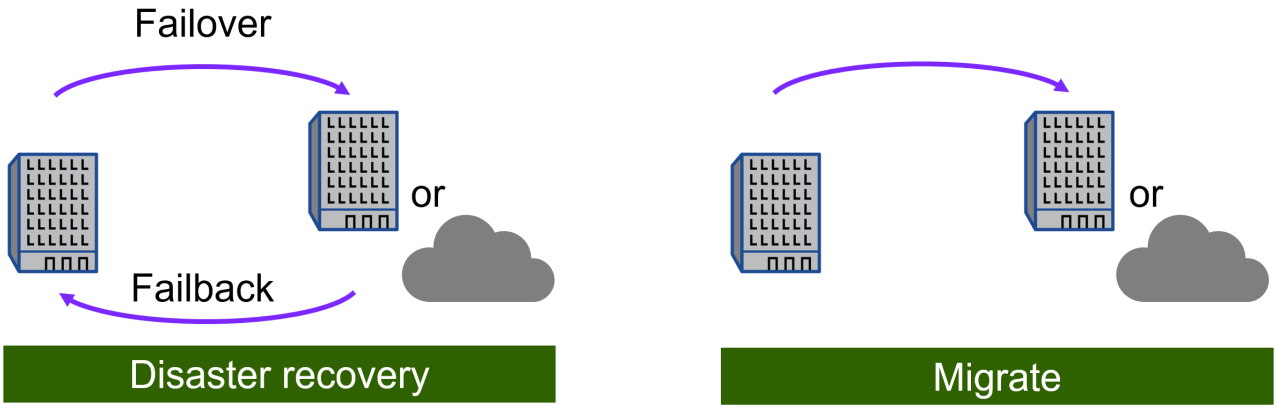
ー エクスペリエンスが簡素化されます。

- 運用コストが削減され、最小限のリソースで災害復旧計画を作成および調整できるため、総所有コストが削減されます。
- 運用を中断しない仮想フェイルオーバー テストによる継続的な災害復旧の準備。実稼働ワークロードに影響を与えることなく、DR フェイルオーバー プランを定期的にテストできます。
- IT 環境の動的な変化と災害復旧計画でそれに対応する能力により、価値実現までの時間が短縮されます。
- 導入および保守が必要な仮想サーバーアプライアンス (VSA) を必要とせずに、 ONTAPと VMware の両方のバックエンドオーケストレーションを通じて、ストレージレイヤーと仮想レイヤーの両方を同時に管理できます。
- VMware の DR ソリューションは大量のリソースを必要とする場合があります。多くの DR ソリューションは、VSA を使用して VMware 仮想レイヤーで VM を複製しますが、これによりコンピューティング リソースがさらに消費され、 ONTAPの貴重なストレージ効率が失われる可能性があります。ディザスタ リカバリではONTAP SnapMirrorテクノロジーが使用されるため、 ONTAPのネイティブ データ圧縮と重複排除の効率性をすべて備えた永久増分レプリケーション モデルを使用して、実稼働データストアから DR サイトにデータを複製できます。

NetApp Disaster Recovery for VMwareでできること

NetApp Disaster Recoveryでは、いくつかのNetAppテクノロジーをフル活用して、次の目標を達成できます。

- SnapMirrorレプリケーションを使用して、オンプレミスの運用サイトにある VMware アプリケーションをクラウドまたはオンプレミスの災害復旧リモート サイトにレプリケートします。
- VMware ワークロードを元のサイトから別のサイトに移行します。
- フェイルオーバー テストを実行します。これを行うと、サービスによって一時的な仮想マシンが作成されます。ディザスタ リカバリでは、選択したスナップショットから新しいFlexCloneボリュームが作成され、 FlexCloneボリュームによってバックアップされる一時データストアが ESXi ホストにマップされます。このプロセスでは、オンプレミスのONTAPストレージまたは AWS の FSx for NetApp ONTAPストレージの追加の物理容量は消費されません。元のソース ボリュームは変更されず、災害復旧中でもレプリカジョブを続行できます。
- 災害が発生した場合は、プライマリサイトをオンデマンドで災害復旧サイトにフェイルオーバーします。災害復旧サイトには、 Amazon FSx for NetApp ONTAPを使用した VMware Cloud on AWS またはONTAPを使用したオンプレミスの VMware 環境を使用できます。
- 災害が解決したら、要求に応じて災害復旧サイトからプライマリ サイトにフェールバックします。
- 効率的な管理のために、VM またはデータストアを論理リソース グループにグループ化します。



vSphere サーバーの構成は、vSphere Server のNetApp Disaster Recoveryの外部で行われます。

料金

NetApp は、NetApp Disaster Recoveryの試用版の使用に対して料金を請求しません。

NetApp Disaster Recovery は、 NetAppライセンスまたは Amazon Web Services を介した年間サブスクリプションベースのプランで使用できます。

一部のリリースにはテクノロジープレビューが含まれています。 NetApp は、プレビューされたワークロード容量に対して料金を請求しません。見る"NetApp Disaster Recoveryの新機能"最新のテクノロジープレビューに関する情報をご覧ください。

ライセンス

次のライセンス タイプを使用できます。

- 30 日間の無料トライアルにサインアップしてください。
- Amazon Web Services (AWS) Marketplace または Microsoft Azure Marketplace で従量課金制 (PAYGO) サブスクリプションを購入します。このライセンスを使用すると、長期契約なしで固定の保護容量ライセンスを購入できます。
- BYOL (Bring Your Own License) は、 NetApp の営業担当者から取得したNetAppライセンス ファイル (NLF) です。ライセンス シリアル番号を使用して、 NetApp Consoleで BYOL をアクティブ化できます。

すべてのNetAppデータ サービスのライセンスは、 NetApp Consoleのサブスクリプションを通じて管理されます。 BYOL を設定すると、コンソールでサービスのアクティブなライセンスを確認できます。

このサービスは、保護されたONTAPボリュームでホストされるデータの量に基づいてライセンスされます。このサービスは、保護された VM を vCenter データストアにマッピングすることで、ライセンスの対象となるボリュームを決定します。各データストアは、 ONTAPボリュームまたは LUN 上でホストされます。そのボリュームまたは LUN についてONTAPによって報告された使用容量は、ライセンスの決定に使用されます。

保護されたボリュームは多数の VM をホストできます。一部はNetApp Disaster Recoveryリソース グループ

の一部ではない可能性があります。いずれにしても、そのボリュームまたは LUN 上のすべての VM によって消費されるストレージは、ライセンスの最大容量に対して使用されます。

> NetApp Disaster Recovery料金は、レプリケーション プランを持つ VM が少なくとも 1 つある場合、ソース サイトのデータストアの使用済み容量に基づいて計算されます。フェイルオーバーされたデータストアの容量は、容量許容量に含まれません。 BYOL の場合、データが許可された容量を超えると、追加の容量ライセンスを取得するか、 NetApp Consoleでライセンスをアップグレードするまで、サービスでの操作が制限されます。

NetApp Disaster Recoveryのライセンス設定の詳細については、以下を参照してください。"NetApp Disaster Recoveryライセンスを設定する" 。

30日間無料トライアル

30 日間の無料トライアルを使用して、 NetApp Disaster Recovery を試すことができます。

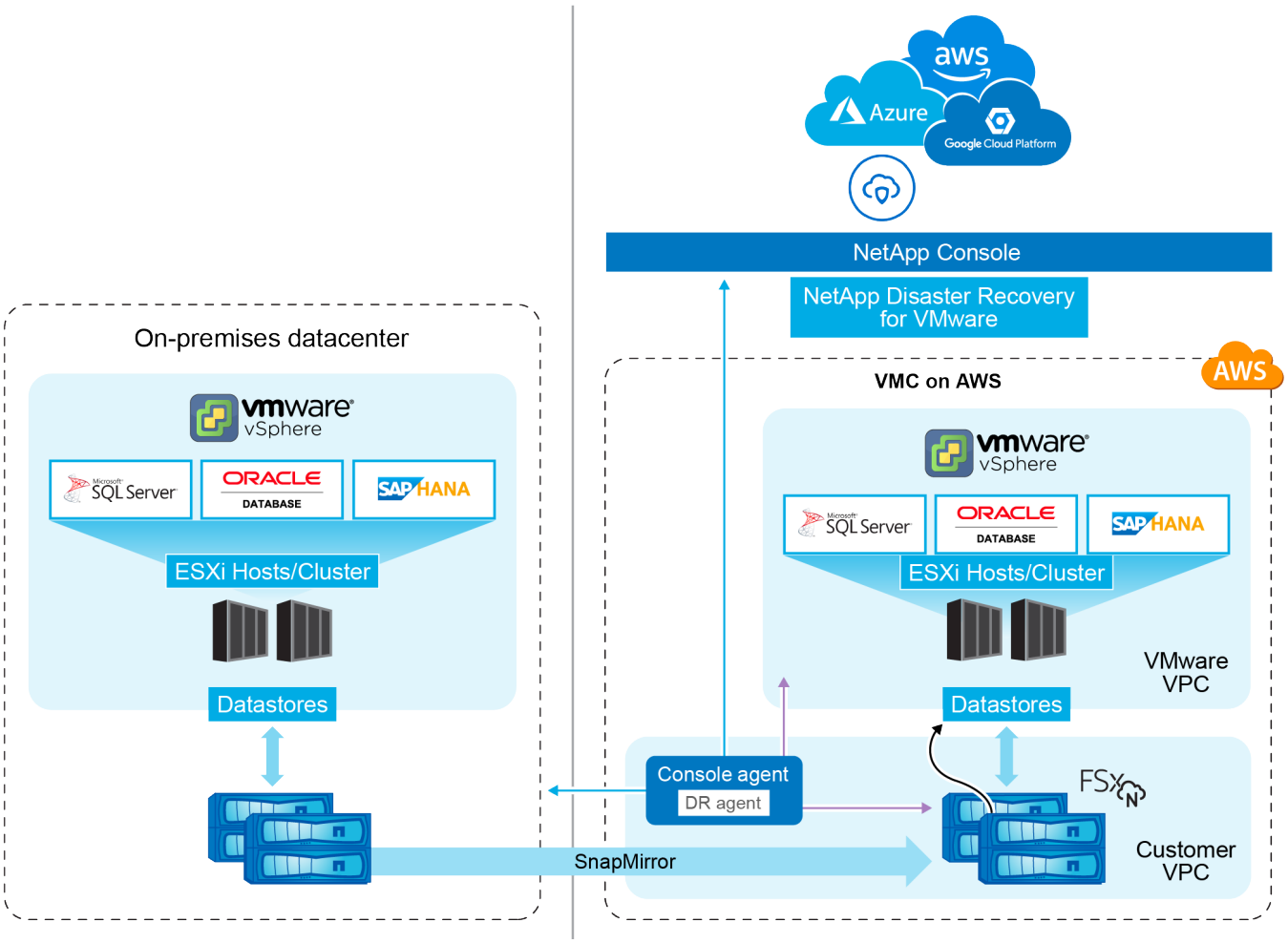
30 日間の試用期間後に継続するには、クラウド プロバイダーから従量課金制 (PAYGO) サブスクリプションを取得するか、 NetAppから BYOL ライセンスを購入する必要があります。

ライセンスはいつでも購入でき、30 日間の試用期間が終了するまで料金は発生しません。

NetApp Disaster Recoveryの仕組み

NetApp Disaster Recoveryは、 NetApp Consoleのソフトウェア アズ ア サービス (SaaS) 環境内でホストされるサービスです。ディザスタリカバリでは、オンプレミスサイトからAmazon FSx for ONTAPまたは別のオンプレミスサイトに複製されたワークロードを回復できます。このサービスは、 SnapMirrorレベルからのリカバリ、VMware Cloud on AWSへの仮想マシン登録、そしてVMwareネットワーク仮想化およびセキュリティプラットフォームであるNSX-Tへのネットワークマッピングまでを自動化します。この機能は、すべての仮想マシンクラウド環境に含まれています。

NetApp Disaster Recovery は、非常に効率的なレプリケーションを提供し、 ONTAP の永久増分スナップショットの効率を維持するONTAP SnapMirrorテクノロジーを使用します。 SnapMirrorレプリケーションにより、アプリケーション整合性のあるスナップショット コピーが常に同期され、フェイルオーバー後すぐにデータが使用できるようになります。



災害が発生した場合、このサービスは、 SnapMirror関係を解除し、宛先サイトをアクティブにすることで、他のオンプレミスの VMware 環境または VMC 内の仮想マシンを復旧するのに役立ちます。

- このサービスを使用すると、仮想マシンを元のソースの場所にフェールバックすることもできます。
- 元の仮想マシンを中断することなく、災害復旧フェールオーバー プロセスをテストできます。テストでは、ボリュームのFlexCloneを作成して、仮想マシンを分離されたネットワークに復旧します。
- フェールオーバーまたはテスト フェールオーバー プロセスでは、仮想マシンを復元するための最新 (デフォルト) または選択したスナップショットを選択できます。

災害復旧の構成要素

ディザスタ リカバリでは、次のコンポーネントを使用して VMware ワークロードのディザスタ リカバリを提供します。

- * NetApp Console*: 災害復旧計画を管理するためのユーザー インターフェイス。 NetApp Consoleを使用すると、オンプレミス環境とクラウド環境全体でレプリケーション プラン、リソース グループ、フェイルオーバー操作を作成および管理できます。
- コンソール エージェント: クラウドでホストされるネットワークまたはオンプレミスの VMware 環境で実行される軽量のソフトウェア コンポーネント。 NetApp Consoleと通信し、オンプレミス環境とディザスタ リカバリ サイト間のデータのレプリケーションを管理します。コンソール エージェントは、VMware 環境内の仮想マシンにインストールされます。

- * ONTAPストレージ クラスター*: ONTAPストレージ クラスターは、VMware ワークロードをホストするプライマリ ストレージ システムです。 ONTAPストレージ クラスターは、災害復旧計画の基盤となるストレージ インフラストラクチャを提供します。ディザスタリカバリでは、 ONTAPストレージ API を使用して、オンプレミスアレイなどのONTAPストレージクラスターや、 Amazon FSx for NetApp ONTAPなどのクラウドベースのソリューションを管理します。
- **vCenter** サーバー: VMware vCenter は、VMware 環境の管理サーバーです。 ESXi ホストとそれに関連付けられたデータストアを管理します。コンソール エージェントは VMware vCenter と通信して、オンプレミス環境と災害復旧サイト間のデータのレプリケーションを管理します。これには、 ONTAP LUN とボリュームをデータストアとして登録すること、VM を再構成すること、VM を起動および停止することが含まれます。

災害復旧保護ワークフロー

レプリケーション プランがリソース グループに割り当てられると、Disaster Recovery はリソース グループとプラン内のすべてのコンポーネントの検出チェックを実行し、プランをアクティブ化できるかどうかを確認します。

このチェックが成功した場合、Disaster Recovery は次の初期化手順を実行します。

1. ターゲット リソース グループ内の各 VM について、ホスティング VMware データストアを識別します。
2. 見つかった VMware データストアごとに、ホスティングしているONTAP FlexVol volumeまたは LUN を識別します。
3. 見つかった各ONTAPボリュームと LUN について、ソース ボリュームと宛先サイトの宛先ボリュームの間に既存のSnapMirror関係があるかどうかを判断します。
    a. 既存のSnapMirror関係が存在しない場合は、新しい宛先ボリュームを作成し、保護されていない各ソース ボリューム間に新しいSnapMirror関係を作成します。
    b. 既存のSnapMirror関係がある場合は、その関係を使用してすべてのレプリケーション操作を実行します。

ディザスタリカバリによってすべての関係が作成および初期化された後、スケジュールされたバックアップごとに、サービスは次のデータ保護手順を実行します。

1. 「アプリケーション整合性」のフラグが付けられた各 VM について、VMtools を使用して、サポートされているアプリケーションをバックアップ状態にします。
2. 保護された VMware データストアをホストするすべてのONTAPボリュームの新しいスナップショットを作成します。
3. SnapMirror更新操作を実行して、これらのスナップショットを宛先ONTAPクラスタに複製します。
4. 保持されたスナップショットの数がレプリケーション プランで定義された最大スナップショット保持期間を超えているかどうかを確認し、ソース ボリュームと宛先ボリュームの両方から不要なスナップショットを削除します。

サポートされている保護対象とデータストアの種類

サポートされるデータストアの種類 NetApp Disaster Recovery は、次のデータストアの種類をサポートします。

- ONTAPクラスタ上に存在するONTAP FlexVolボリューム上でホストされる NFS データストア。
- iSCSI または FC プロトコルを使用した VMware vSphere 仮想マシン ファイル システム (VMFS) データ

ストア

サポートされている保護対象

- VMware Cloud (VMC) on AWS とAmazon FSx for NetApp ONTAP
- ONTAPストレージまたはオンプレミス FC/iSCSI VMSF を備えた別のオンプレミス NFS ベースの VMware 環境
- Amazon Elastic VMware サービス
- Azure VMware Solution (AVS) とNetApp Cloud Volumes ONTAP (iSCSI) (プライベート プレビュー)

NetApp Disaster Recoveryに役立つ用語

災害復旧に関連するいくつかの用語を理解しておくと役立つかもしれません。

- データストア: ファイル システムを使用して VMDK ファイルを保持する VMware vCenter データ コンテナー。一般的なデータストアの種類は、NFS、VMFS、vSAN、vVol です。ディザスタ リカバリでは、NFS および VMFS データストアがサポートされます。各 VMware データストアは、単一のONTAPボリュームまたは LUN でホストされます。ディザスタ リカバリは、 ONTAPクラスタに存在するFlexVolボリュームでホストされる NFS および VMFS データストアをサポートします。
- レプリケーション プラン: バックアップの実行頻度とフェイルオーバー イベントの処理方法に関する一連のルール。プランは 1 つ以上のリソース グループに割り当てられます。
- 目標復旧ポイント **(RPO)**: 災害発生時に許容できるデータ損失の最大量。 RPO は、レプリケーション プランのデータ レプリケーションの頻度またはレプリケーション スケジュールで定義されます。
- 目標復旧時間 **(RTO)**: 災害からの復旧に許容される最大時間。 RTO はレプリケーション プランで定義され、DR サイトにフェールオーバーしてすべての VM を再起動するのにかかる時間です。
- リソース グループ: 複数の VM を 1 つのユニットとして管理できる論理コンテナー。 VM は一度に 1 つのリソース グループにのみ存在できます。保護するアプリケーションまたはワークロードごとにリソース グループを作成できます。
- サイト: 通常、1 つ以上の vCenter クラスターとONTAPストレージをホストする物理データセンターまたはクラウドの場所に関連付けられた論理コンテナ。

NetApp Disaster Recoveryの前提条件

NetApp Disaster Recoveryを使用する前に、環境がONTAPストレージ、VMware vCenterクラスタ、およびNetApp Consoleの要件を満たしていることを確認する必要があります。

ソフトウェアバージョン

コンポーネント	最小バージョン
ONTAPソフトウェア	ONTAP 9.10.0以降
VMware オンプレミス vCenter	7.0u3以降

コンポーネント	最小バージョン
AWS 向け VMware クラウド	最新バージョン
Amazon FSx for NetApp ONTAP	最新バージョン

ONTAPストレージの前提条件

これらの前提条件は、 ONTAPまたは Amazon FSX for NetApp ONTAPインスタンスに適用されます。

- ソース クラスターと宛先クラスターにはピア関係が必要です。
- ディザスタ リカバリ ボリュームをホストする SVM は、宛先クラスタ上に存在している必要があります。
- ソース SVM と宛先 SVM にはピア関係が必要です。
- Amazon FSx for NetApp ONTAPを使用してデプロイする場合は、次の前提条件が適用されます。
  - VMware DR データストアをホストするAmazon FSx for NetApp ONTAPインスタンスが VPC 内に存在している必要があります。 Amazon FSx for ONTAPのドキュメントを参照してください。 "始め方" 。

VMware vCenter クラスタの前提条件

これらの前提条件は、オンプレミスの vCenter クラスタと VMware Cloud for AWS ソフトウェア定義データセンター (SDDC) の両方に適用されます。

- レビュー"vCenter 権限"NetApp Disaster Recoveryに必要です。
- NetApp Disaster Recoveryで管理するすべての VMware クラスターは、保護する VM をホストするためにONTAPボリュームを使用します。
- NetApp Disaster Recoveryによって管理されるすべての VMware データストアでは、次のいずれかのプロトコルを使用する必要があります。
  - NFS
  - iSCSI または FC プロトコルを使用した VMFS
- VMware vSphere バージョン 7.0 Update 3 (7.0v3) 以降
- VMware Cloud SDDC を使用している場合は、次の前提条件が適用されます。
  - VMware Cloud コンソールでは、管理者および NSX Cloud 管理者のサービス ロールを使用します。組織ロールには組織の所有者も使用します。参照 "VMware Cloud Foundations と AWS FSx for NetApp ONTAP の使用に関するドキュメント"。
  - VMware Cloud SDDC をAmazon FSx for NetApp ONTAPインスタンスにリンクします。参照 "VMware Cloud on AWS とAmazon FSx for NetApp ONTAP の統合の展開情報"。

NetApp Consoleの前提条件

NetApp Consoleを使い始める

まだお済みでない場合は、 "NetApp Consoleにサインアップして組織を作成する" 。

ONTAPとVMwareの資格情報を収集する

- NetApp Disaster Recoveryを管理するために使用されるNetApp Consoleプロジェクト内のシステムに、Amazon FSx for ONTAPと AWS 認証情報を追加する必要があります。
- NetApp Disaster Recovery には vCenter の資格情報が必要です。 NetApp Disaster Recoveryでサイトを追加するときに、vCenter の資格情報を入力します。

  必要なvCenter権限のリストについては、"NetApp Disaster Recoveryに必要な vCenter 権限" 。サイトを追加する方法については、"サイトを追加する" 。

NetApp Consoleエージェントを作成する

コンソール エージェントは、コンソールがONTAPストレージおよび VMware vCenter クラスターと通信できるようにするソフトウェア コンポーネントです。災害復旧が適切に機能するために必要です。エージェントはプライベート ネットワーク（オンプレミス データセンターまたはクラウド VPC 内）に常駐し、 ONTAPストレージ インスタンスやその他のサーバーおよびアプリケーション コンポーネントと通信します。災害復旧の場合、これは管理対象の vCenter クラスターへのアクセスです。

NetApp Consoleにコンソール エージェントを設定する必要があります。エージェントを使用すると、災害復旧サービスに適切な機能が含まれるようになります。

- NetApp Disaster Recovery は、標準モード エージェントの展開でのみ機能します。見る "NetApp Console の標準モードでの使用開始"。
- ソース vCenter とターゲット vCenter の両方で同じコンソール エージェントが使用されていることを確認します。
- 必要なコンソール エージェントの種類:
  - オンプレミスからオンプレミスへの災害復旧: 災害復旧サイトにコンソールのオンプレミス エージェントをインストールします。この方法を使用すると、プライマリ サイトに障害が発生しても、サービスが DR サイトで仮想リソースを再起動できなくなります。参照 "オンプレミスでコンソールエージェントをインストールしてセットアップする"。
  - オンプレミスから **AWS**: AWS VPC に AWS 用コンソールエージェントをインストールします。参照 "AWS のコンソールエージェントのインストールオプション"。

    オンプレミスからオンプレミスへの接続には、オンプレミスのコンソール エージェントを使用します。オンプレミスから AWS の場合、ソースのオンプレミス vCenter と宛先のオンプレミス vCenter にアクセスできる AWS コンソールエージェントを使用します。

  - インストールされたコンソール エージェントは、 NetApp Disaster Recoveryが管理するすべての VMware クラスターにアクセスできる必要があります。
- NetApp Disaster Recoveryによって管理されるすべてのONTAPアレイは、 NetApp Disaster Recoveryの管理に使用されるNetApp Consoleプロジェクト内のすべてのシステムに追加する必要があります。

  見る "オンプレミスのONTAPクラスタの検出"。

- NetApp Disaster Recoveryのインテリジェントプロキシの設定については、以下を参照してください。"NetApp Disaster Recovery用のインフラストラクチャをセットアップする" 。

ワークロードの前提条件

アプリケーション整合性プロセスが確実に成功するには、次の前提条件を適用します。

- 保護する VM 上で VMware ツール (または Open VM ツール) が実行されていることを確認します。
- Microsoft SQL Server または Oracle Database、あるいはその両方を実行している Windows VM の場合、データベースで VSS ライターが有効になっている必要があります。
- Linux オペレーティング システムで実行されている Oracle データベースでは、Oracle データベース SYSDBA ロールに対してオペレーティング システム ユーザー認証が有効になっている必要があります。

NetApp Disaster Recoveryのクイックスタート

NetApp Disaster Recoveryを開始するために必要な手順の概要を以下に示します。各ステップ内のリンクをクリックすると、詳細情報を提供するページに移動します。

1 前提条件を確認する

"システムがこれらの要件を満たしていることを確認してください"。

2 **NetApp Disaster Recovery**のセットアップ

- "サービスのインフラストラクチャを構築する"。
- "ライセンスの設定"。

3 次は何**?**

サービスを設定したら、次に行うことは次のとおりです。

- "vCenter サイトをNetApp Disaster Recoveryに追加する"。
- "最初のリソースグループを作成する"。
- "最初のレプリケーションプランを作成する"。
- "アプリケーションを別のサイトに複製する"。
- "アプリケーションをリモートサイトにフェイルオーバーする"。
- "アプリケーションを元のソースサイトにフェイルバックする"。
- "サイト、リソース グループ、レプリケーション プランを管理する"。
- "災害復旧オペレーションの監視"。

NetApp Disaster Recovery用のインフラストラクチャをセットアップする

NetApp Disaster Recoveryを使用するには、Amazon Web Services (AWS) とNetApp Consoleの両方でいくつかの手順を実行してセットアップする必要があります。

レビュー"前提条件"システムの準備ができていることを確認します。

NetApp Disaster Recovery は、次のインフラストラクチャで使用できます。

- オンプレミスの VMware とONTAPデータセンターを、VMware Cloud on AWS とAmazon FSx for NetApp ONTAPに基づく AWS DR インフラストラクチャに複製するハイブリッド クラウド DR。
- オンプレミスの VMware とONTAP vCenter を別のオンプレミスの VMware とONTAP vCenter に複製するプライベート クラウド DR。

VMware Cloud とAmazon FSx for NetApp ONTAPハイブリッド クラウド

この方法は、NFS プロトコルを使用してONTAP FlexVolボリュームでホストされるデータストアを使用するオンプレミスの本番環境の vCenter インフラストラクチャで構成されます。 DR サイトは、NFS プロトコルを使用する 1 つ以上の FSx for ONTAPインスタンスによって提供されるFlexVolボリューム上でホストされるデータストアを使用する 1 つ以上の VMware Cloud SDDC インスタンスで構成されます。

本番サイトと DR サイトは、AWS 互換の安全な接続によって接続されます。一般的な接続タイプは、安全な VPN (プライベートまたは AWS 提供)、AWS Direct Connect、またはその他の承認された相互接続方法です。

AWS クラウド インフラストラクチャに関連する災害復旧の場合は、AWS のコンソール エージェントを使用する必要があります。エージェントは、FSx for ONTAPインスタンスと同じ VPC にインストールする必要があります。追加の FSx for ONTAPインスタンスが他の VPC に導入されている場合、エージェントをホストしている VPC は他の VPC にアクセスできる必要があります。

AWS アベイラビリティゾーン

AWS は、特定のリージョン内の 1 つ以上のアベイラビリティーゾーン (AZ) でのソリューションのデプロイをサポートしています。ディザスタリカバリでは、VMware Cloud for AWS と AWS FSx for NetApp ONTAP2 つの AWS ホストサービスが使用されます。

- **VMware Cloud for AWS**: シングル AZ またはデュアル AZ ストレッチ クラスタ SDDC 環境での展開をサポートします。ディザスタリカバリは、Amazon VMware Cloud for AWS の単一 AZ SDDC デプロイメントのみをサポートします。
- **AWS FSx for NetApp ONTAP**: これをデュアル AZ 構成で導入すると、各ボリュームは単一の FSx システムによって所有されます。各ボリュームは単一の FSx システムによって所有されます。ボリュームのデータは 2 番目の FSx システムにミラーリングされます。 FSx for ONTAPシステムは、シングル AZ またはデュアル AZ のいずれかのデプロイメントで導入できます。ディザスタ リカバリでは、FSx for ONTAP のデプロイメントにおいて、単一 AZ とマルチ AZ の両方の FSx がサポートされます。

ベスト プラクティス: AWS DR サイト構成の場合、 NetApp、VMware Cloud と AWS FSx for ONTAPインスタンスの両方に単一の AZ デプロイメントを使用することを推奨しています。 DR用にAWSを利用している為、複数AZを導入するメリットはありません。マルチ AZ ではコストと複雑さが増す可能性があります。

オンプレミスから**AWS**へ

AWS は、プライベートデータセンターを AWS クラウドに接続するための次の方法を提供します。各ソリューションには利点とコストに関する考慮事項があります。

- **AWS Direct Connect**: これは、プライベートデータセンターと同じ地理的領域にあり、AWS パートナーによって提供される AWS クラウド相互接続です。このソリューションは、パブリックインターネット接続を必要とせずに、ローカルデータセンターと AWS クラウド間の安全なプライベート接続を提供しま

す。これは AWS が提供する最も直接的で効率的な接続方法です。

- **AWS** インターネットゲートウェイ: AWS クラウドリソースと外部コンピューティングリソース間のパブリック接続を提供します。このタイプの接続は通常、セキュリティが要求されない HTTP/HTTPS サービスなど、外部の顧客にサービスを提供するために使用されます。サービス品質の制御、セキュリティ、接続の保証はありません。このため、この接続方法は、実稼働データセンターをクラウドに接続する場合には推奨されません。
- **AWS** サイト間 **VPN**: この仮想プライベートネットワーク接続は、パブリックインターネットサービスプロバイダーとともに安全なアクセス接続を提供するために使用できます。 VPN は、AWS クラウドとの間でやり取りされるすべてのデータを暗号化および復号化します。 VPN はソフトウェアベースまたはハードウェアベースのいずれかになります。エンタープライズ アプリケーションの場合、パブリック インターネット サービス プロバイダー (ISP) は、DR レプリケーションに十分な帯域幅と待機時間が提供されるように、サービス品質の保証を提供する必要があります。

ベストプラクティス: AWS DR サイト構成の場合、 NetAppAWS Direct Connect の使用を推奨しています。このソリューションは、エンタープライズ アプリケーションに最高のパフォーマンスとセキュリティを提供します。利用できない場合は、VPN と併用した高性能パブリック ISP 接続を使用する必要があります。適切なネットワーク パフォーマンスを確保するために、ISP が商用 QoS サービス レベルを提供していることを確認します。

VPC 間の相互接続

AWS では、次のタイプの VPC 間相互接続を提供しています。各ソリューションには利点とコストに関する考慮事項があります。

- **VPC** ピアリング: これは 2 つの VPC 間のプライベート接続です。これは AWS が提供する最も直接的で効率的な接続方法です。 VPC ピアリングを使用すると、同じまたは異なる AWS リージョン内の VPC を接続できます。
- **AWS** インターネットゲートウェイ: これは通常、AWS VPC リソースと AWS 以外のリソースおよびエンドポイント間の接続を提供するために使用されます。すべてのトラフィックは「ヘアピン」パスをたどります。このパスでは、別の VPC 宛ての VPC トラフィックがインターネットゲートウェイを介して AWS インフラストラクチャから出て、同じゲートウェイまたは別のゲートウェイを介して AWS インフラストラクチャに戻ります。これは、エンタープライズ VMware ソリューションに適した VPC 接続タイプではありません。
- **AWS Transit Gateway**: これは集中型のルーターベースの接続タイプであり、各 VPC が単一の中央ゲートウェイに接続できるようにします。このゲートウェイは、すべての VPC 間トラフィックの中央ハブとして機能します。これを VPN ソリューションに接続して、オンプレミスのデータセンター リソースが AWS VPC でホストされているリソースにアクセスできるようにすることもできます。このタイプの接続を実装するには、通常、追加のコストが必要です。

ベスト プラクティス: VMware Cloud と単一の FSx for ONTAP VPC を含む DR ソリューションの場合、NetAppVPC ピア接続を使用することをお勧めします。複数の FSx for ONTAP VPC を導入する場合は、AWS Transit Gateway を使用して複数の VPC ピア接続の管理オーバーヘッドを削減することをお勧めします。

AWS を使用したオンプレミスからクラウドへの保護の準備

AWS を使用してオンプレミスからクラウドへの保護用にNetApp Disaster Recovery を設定するには、以下を設定する必要があります。

- NetApp ONTAP用の AWS FSx をセットアップする
- VMware Cloud on AWS SDDC をセットアップする

NetApp ONTAP用の AWS FSx をセットアップする

- Amazon FSx for NetApp ONTAPファイルシステムを作成します。
  - FSx for ONTAPをプロビジョニングおよび構成します。 Amazon FSx for NetApp ONTAP は、 NetApp ONTAPファイルシステム上に構築された、信頼性が高く、スケーラブルで、高性能かつ機能豊富なファイルストレージを提供する、フルマネージドサービスです。
  - 以下の手順に従ってください "テクニカルレポート 4938: VMware Cloud on AWS でAmazon FSx ONTAP をNFS データストアとしてマウントする"そして "Amazon FSx for NetApp ONTAP のクイックスタート"FSx for ONTAPをプロビジョニングおよび構成します。
- Amazon FSx for ONTAPをシステムに追加し、 FSx for ONTAPの AWS 認証情報を追加します。
- AWS FSx for ONTAPインスタンスで宛先ONTAP SVM を作成または検証します。
- NetApp Consoleで、ソースのオンプレミスONTAPクラスターと FSx for ONTAPインスタンス間のレプリケーションを構成します。

参照 "FSx for ONTAPシステムのセットアップ方法"詳細な手順については、こちらをご覧ください。

VMware Cloud on AWS SDDC をセットアップする

"VMware Cloud on AWS"AWS エコシステム内の VMware ベースのワークロードにクラウドネイティブのエクスペリエンスを提供します。各 VMware ソフトウェア定義データセンター (SDDC) は Amazon Virtual Private Cloud (VPC) で実行され、完全な VMware スタック (vCenter Server を含む)、NSX-T ソフトウェア定義ネットワーク、vSAN ソフトウェア定義ストレージ、およびワークロードにコンピューティング リソースとストレージ リソースを提供する 1 つ以上の ESXi ホストを提供します。

AWS上でVMware Cloud環境を構成するには、以下の手順に従ってください。 "AWS 上で仮想化環境を展開および構成する"パイロットライト クラスターは、災害復旧の目的にも使用できます。

プライベート クラウド

NetApp Disaster Recoveryを使用すると、VM データストアを同じプライベート データセンター内またはリモートのプライベート データセンターまたは併置されたデータセンター内の別の vCenter クラスタに複製することで、1 つ以上の vCenter クラスタでホストされている VMware VM を保護できます。

オンプレミスからオンプレミスへの状況では、物理サイトの 1 つにコンソール エージェントをインストールします。

災害復旧は、イーサネットと TCP/IP を使用したサイト間レプリケーションをサポートします。すべての変更を復旧ポイント目標 (RPO) の時間枠内に DR サイトに複製できるように、運用サイトの VM 上のデータ変更率をサポートするために十分な帯域幅が利用可能であることを確認します。

オンプレミスからオンプレミスへの保護の準備

オンプレミス間の保護のためにNetApp Disaster Recovery を設定する前に、次の要件が満たされていることを確認してください。

- ONTAPストレージ
  - ONTAP認証情報があることを確認します。
  - 災害復旧サイトを作成または検証します。
  - 宛先のONTAP SVM を作成または検証します。

- ソースとデスティネーションのONTAP SVM がピアリングされていることを確認します。

- vCenter クラスタ
  - 保護する VM が NFS データストア (ONTAP NFS ボリュームを使用) または VMFS データストア (NetApp iSCSI LUN を使用) でホストされていることを確認します。
  - レビュー"vCenter 権限"NetApp Disaster Recoveryに必要です。
  - 災害復旧ユーザー アカウント (デフォルトの vCenter 管理者アカウントではない) を作成し、そのアカウントに vCenter 権限を割り当てます。

インテリジェントなプロキシサポート

NetApp Consoleエージェントはインテリジェント プロキシをサポートします。インテリジェント プロキシは、オンプレミス環境をNetApp Consoleに接続するための軽量かつ安全で効率的な方法です。 VPN や直接のインターネット アクセスを必要とせずに、システムとコンソール サービス間の安全な接続を提供します。この最適化されたプロキシ実装は、ローカル ネットワーク内の API トラフィックをオフロードします。

プロキシが設定されている場合、 NetApp Disaster Recovery はVMware またはONTAPと直接通信を試み、直接通信が失敗した場合は設定されたプロキシを使用します。

NetApp Disaster Recoveryプロキシの実装では、コンソール エージェントと、HTTPS プロトコルを使用した vCenter Server およびONTAPアレイ間のポート 443 通信が必要です。コンソール エージェント内のNetApp Disaster Recoveryエージェントは、アクションを実行するときに VMware vSphere、VC、またはONTAPと直接通信します。

NetApp Consoleでの一般的なプロキシ設定の詳細については、以下を参照してください。 "プロキシサーバーを使用するようにコンソールエージェントを構成する" 。

NetApp Disaster Recoveryにアクセス

NetApp Consoleを使用して、 NetApp Disaster Recoveryサービスにログインします。

ログインするには、 NetAppサポート サイトの認証情報を使用するか、電子メールとパスワードを使用してNetAppクラウド ログインにサインアップすることができます。 "ログインについて詳しくはこちら" 。

特定のタスクには特定のユーザー ロールが必要です。"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

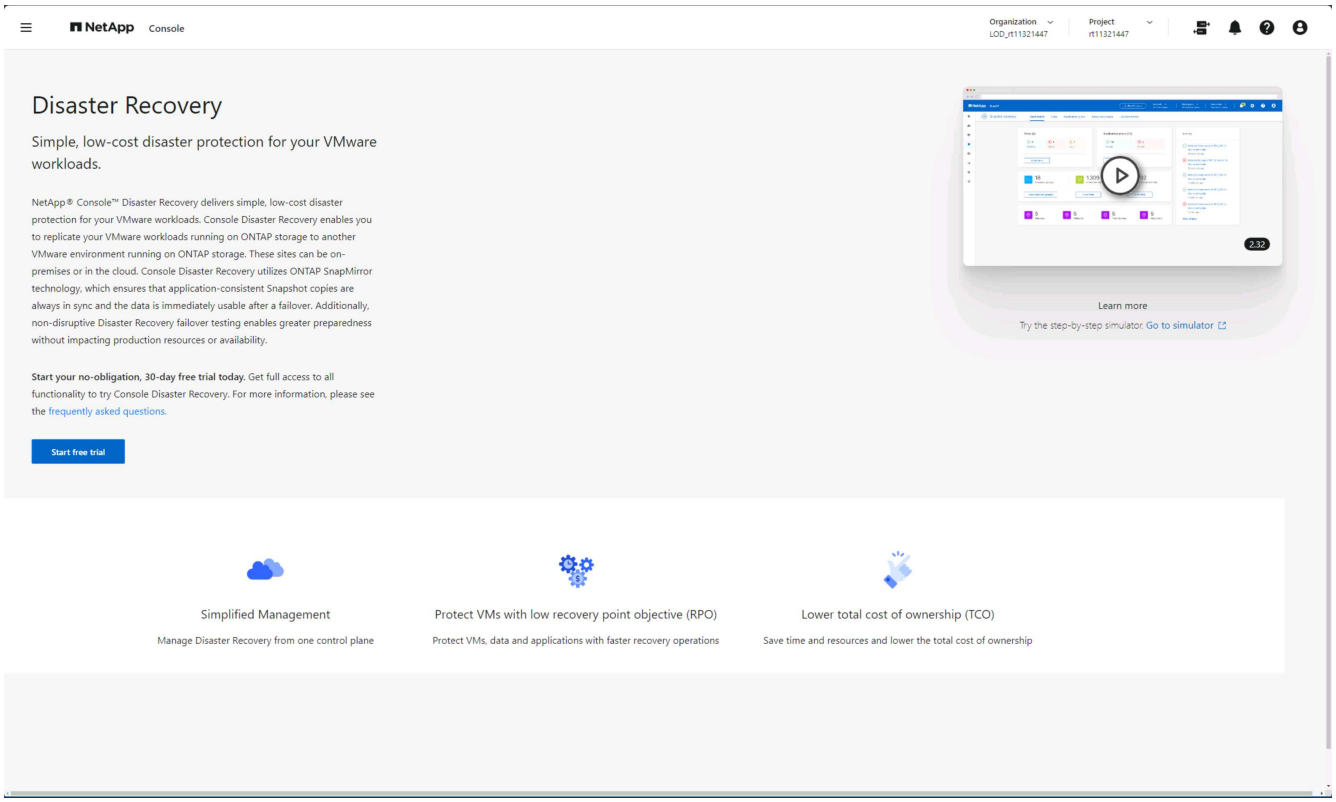
手順

1. ウェブブラウザを開いて、 "NetApp Console" 。

   NetApp Consoleのログイン ページが表示されます。

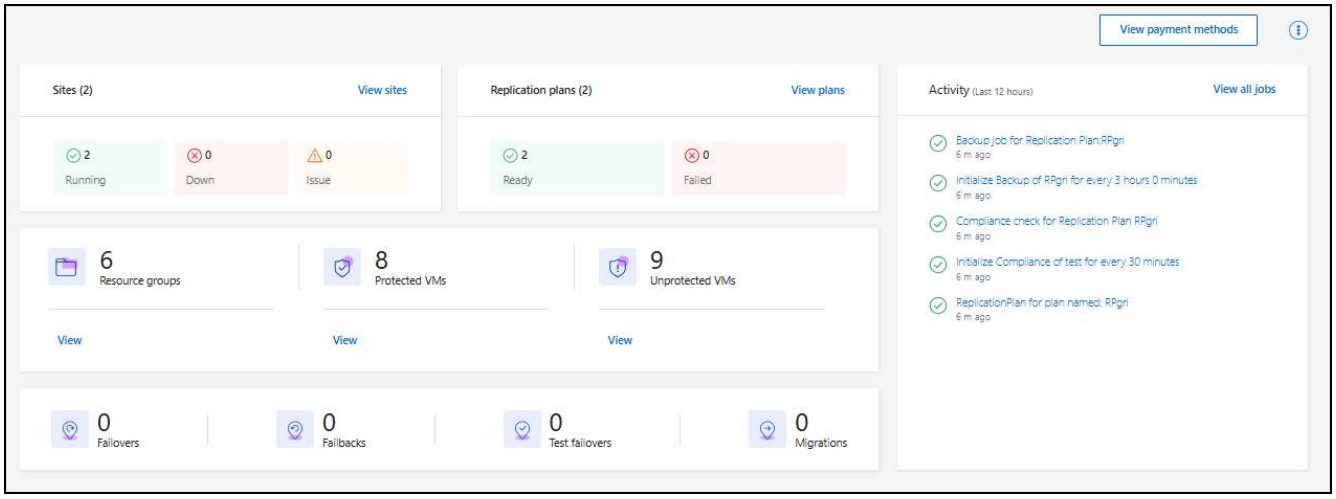
2. NetApp Consoleにログインします。
3. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。

   このサービスに初めてログインする場合は、ランディング ページが表示され、無料トライアルにサインアップできます。



それ以外の場合は、 NetApp Disaster Recoveryボードが表示されます。

- NetApp Consoleエージェントをまだ追加していない場合は、追加する必要があります。エージェントを追加するには、 "コンソールエージェントについて学ぶ" 。
- 既存のエージェントを持つNetApp Consoleユーザーの場合は、「ディザスタ リカバリ」を選択すると、サインアップに関するメッセージが表示されます。
- すでにサービスを使用している場合は、「災害復旧」を選択するとダッシュボードが表示されます。



NetApp Disaster Recoveryのライセンスを設定する

NetApp Disaster Recoveryでは、無料トライアル、従量課金制サブスクリプション、独自のライセンスの使用など、さまざまなライセンス プランを使用できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、またはディザスタ リカバリ アプリケーション管理者のロール。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスのアクセスロールについて学ぶ"^] 。

ライセンス オプション 次のライセンス オプションを使用できます。

- 30 日間の無料トライアルにサインアップしてください。
- Amazon Web Services (AWS) Marketplace または Microsoft Azure Marketplace の従量課金制 (PAYGO) サブスクリプションを購入します。
- BYOL (Bring Your Own License) は、 NetApp の営業担当者から取得したNetAppライセンス ファイル (NLF) です。ライセンス シリアル番号を使用して、 NetApp Consoleで BYOL をアクティブ化できます。

> NetApp Disaster Recovery料金は、レプリケーション プランを持つ VM が少なくとも 1 つある場合、ソース サイトのデータストアの使用済み容量に基づいて計算されます。フェイルオーバーされたデータストアの容量は、容量許容量に含まれません。 BYOL の場合、データが許可された容量を超えると、追加の容量ライセンスを取得するか、 NetApp Consoleでライセンスをアップグレードするまで、サービスでの操作が制限されます。

"サブスクリプションについて詳しくはこちら" 。

無料トライアルが終了した後、またはライセンスの有効期限が切れた後でも、サービス内で次の操作を実行できます。

- ワークロードやレプリケーション プランなどのリソースを表示します。
- ワークロードやレプリケーション プランなどのリソースを削除します。
- 試用期間中またはライセンスに基づいて作成されたすべてのスケジュールされた操作を実行します。

30日間の無料トライアルでお試しください

30 日間の無料トライアルを使用して、 NetApp Disaster Recoveryを試すことができます。

> トライアル期間中は容量制限は適用されません。

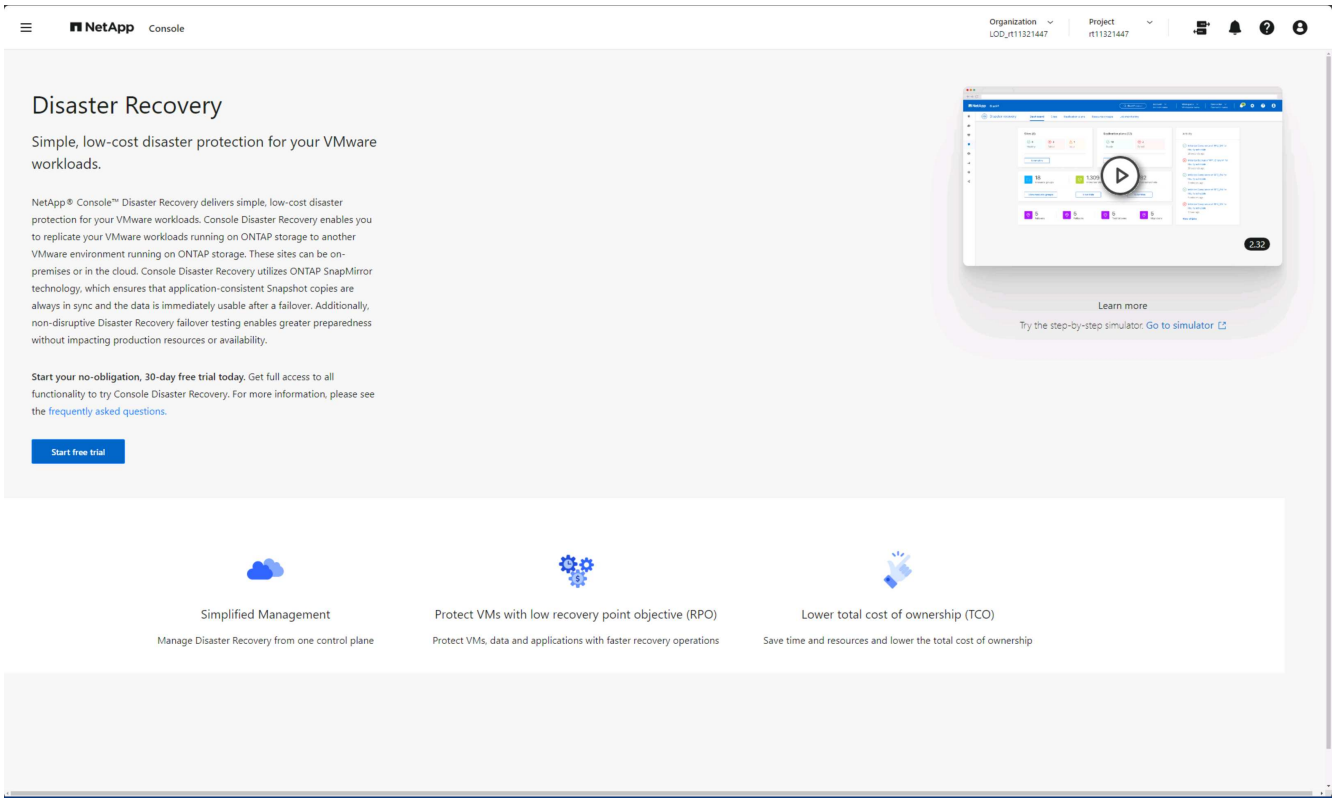
試用期間後に継続するには、BYOL ライセンスまたは PAYGO AWS サブスクリプションを購入する必要があります。ライセンスはいつでも取得でき、試用期間が終了するまで料金は発生しません。

試用期間中は、すべての機能をご利用になれます。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。

   このサービスに初めてログインする場合は、ランディング ページが表示されます。



3. 他のサービス用のコンソール エージェントをまだ追加していない場合は、追加します。

   コンソールエージェントを追加するには、 "コンソールエージェントについて学ぶ" 。

4. エージェントを設定すると、 NetApp Disaster Recoveryランディング ページで、エージェントを追加するボタンが無料トライアルを開始するためのボタンに変わります。 *無料トライアルを開始*を選択します。
5. まず、vCenter を追加します。

   詳細については、 "vCenterサイトを追加する" 。

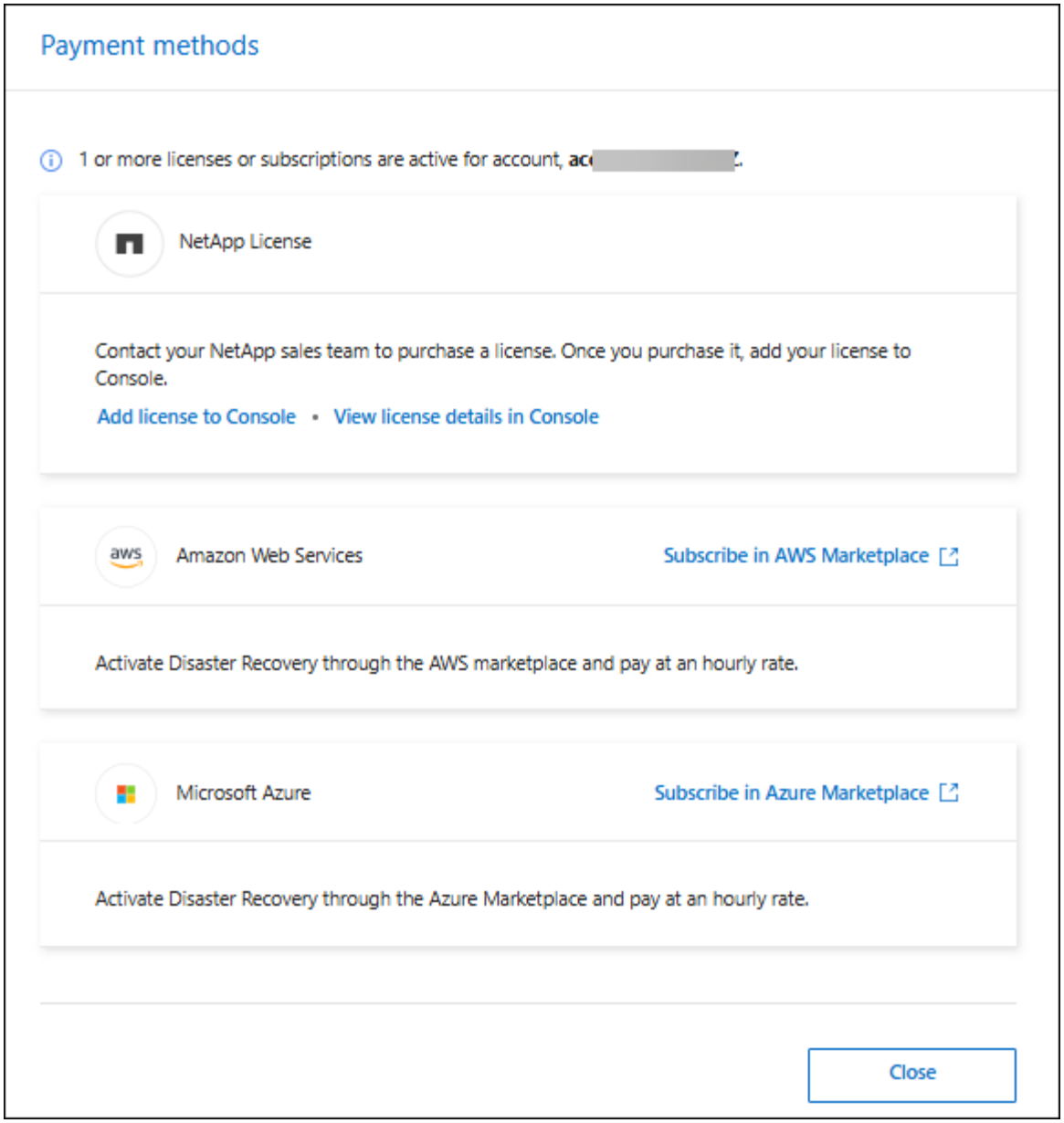
トライアル終了後は、マーケットプレイスのいずれかから登録してください。

無料トライアルが終了したら、 NetAppからライセンスを購入するか、AWS Marketplace または Microsoft Azure Marketplace を通じてサブスクライブすることができます。この手順では、マーケットプレイスのいずれかで直接サブスクライブする方法の概要を説明します。

手順

1. NetApp Disaster Recoveryで、無料トライアルの有効期限が切れるというメッセージが表示されます。メッセージで、[サブスクライブまたはライセンスを購入] を選択します。

   または、 から [支払い方法の表示] を選択します。



2. **AWS Marketplace** でサブスクライブ または **Azure Marketplace** でサブスクライブ を選択します。
3. AWS Marketplace または Microsoft Azure Marketplace を使用して * NetApp Disaster Recovery* をサブスクライブします。
4. NetApp Disaster Recoveryに戻ると、サブスクライブしたことを示すメッセージが表示されます。

   サブスクリプションの詳細は、NetApp Consoleのサブスクリプション ページで確認できます。"NetApp Consoleを使用したサブスクリプションの管理の詳細" 。

トライアル終了後は、 **NetApp**を通じて**BYOL**ライセンスを購入してください。

試用期間が終了したら、 NetApp の営業担当者を通じてライセンスを購入できます。

独自のライセンスを持ち込む場合 (BYOL)、セットアップにはライセンスの購入、 NetAppライセンス ファイル (NLF) の取得、 NetApp Consoleへのライセンスの追加が含まれます。

- NetApp Consoleにライセンスを追加します ** NetApp の営業担当者からNetApp Disaster Recoveryライセンスを購入したら、コンソールでライセンスを管理できます。

"NetApp Consoleでライセンスを追加する方法について学習します" 。

ライセンスの有効期限が切れたら更新してください

ライセンスの有効期限が近づいている場合、またはライセンス容量が制限に達した場合は、 NetApp Disaster Recovery UI で通知されます。 NetApp Disaster Recoveryライセンスは期限が切れる前に更新できるので、スキャンしたデータへのアクセスが中断されることはありません。

このメッセージはNetApp Consoleと "通知"。

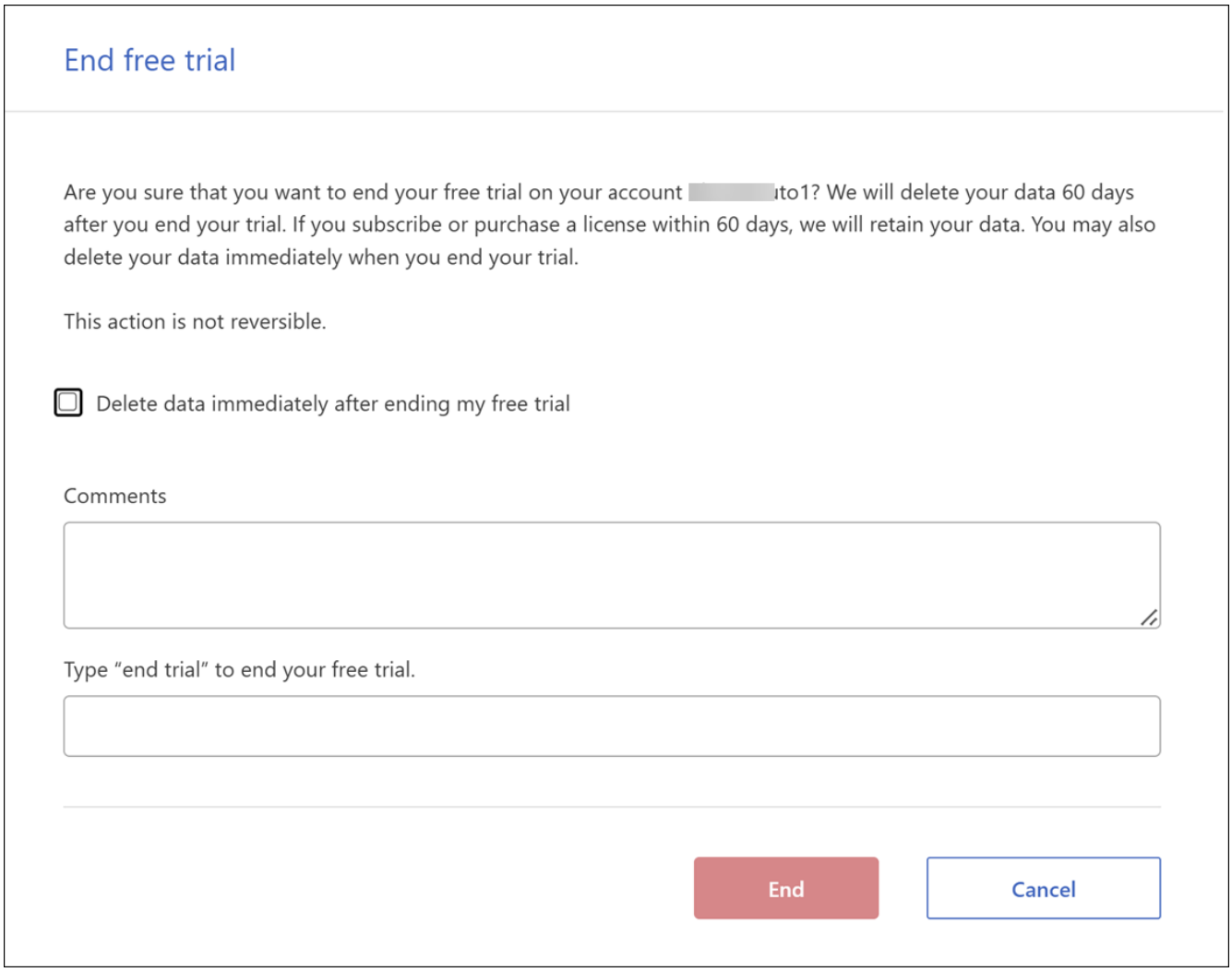
"NetApp Consoleでライセンスを更新する方法について学習します" 。

無料トライアルを終了する

無料トライアルはいつでも停止できます。また、有効期限が切れるまで待つこともできます。

手順

1. NetApp Disaster Recoveryで、*無料トライアル - 詳細を表示*を選択します。
2. ドロップダウンの詳細で、[無料トライアルを終了]を選択します。



3. すべてのデータを削除したい場合は、「無料トライアル終了後すぐにデータを削除する」にチェックを入れてください。

   これにより、すべてのスケジュール、レプリケーション プラン、リソース グループ、vCenter、およびサイトが削除されます。監査データ、操作ログ、ジョブ履歴は、製品の寿命が終了するまで保持されます。

   無料トライアルを終了し、データの削除を要求せず、ライセンスまたはサブスクリプションを購入しなかった場合、 NetApp Disaster Recovery は無料トライアルの終了から 60 日後にすべてのデータを削除します。

4. テキストボックスに「トライアル終了」と入力します。
5. *終了*を選択します。

NetApp Disaster Recoveryを使用する

NetApp Disaster Recoveryの概要

NetApp Disaster Recovery を使用すると、次の目標を達成できます。

- "災害復旧計画の健全性を確認する" 。
- "vCenterサイトを追加する" 。
- "VM をまとめて整理するためのリソース グループを作成する"
- "災害復旧計画を作成する" 。
- "VMwareアプリを複製する"SnapMirrorレプリケーションを使用して、プライマリ サイトのデータをクラウド内の災害復旧リモート サイトに移行します。
- "VMwareアプリの移行"プライマリサイトから別のサイトへ。
- "フェイルオーバーをテストする"元の仮想マシンを中断することなく。
- 災害が発生した場合、"プライマリサイトをフェイルオーバーする" FSx for NetApp ONTAPを使用してVMware Cloud on AWS に移行します。
- 災害が解決した後、"フェイルバック"災害復旧サイトからプライマリ サイトへ。
- "災害復旧オペレーションの監視"ジョブ監視ページで。

ダッシュボードでNetApp Disaster Recoveryプランの健全性を確認する

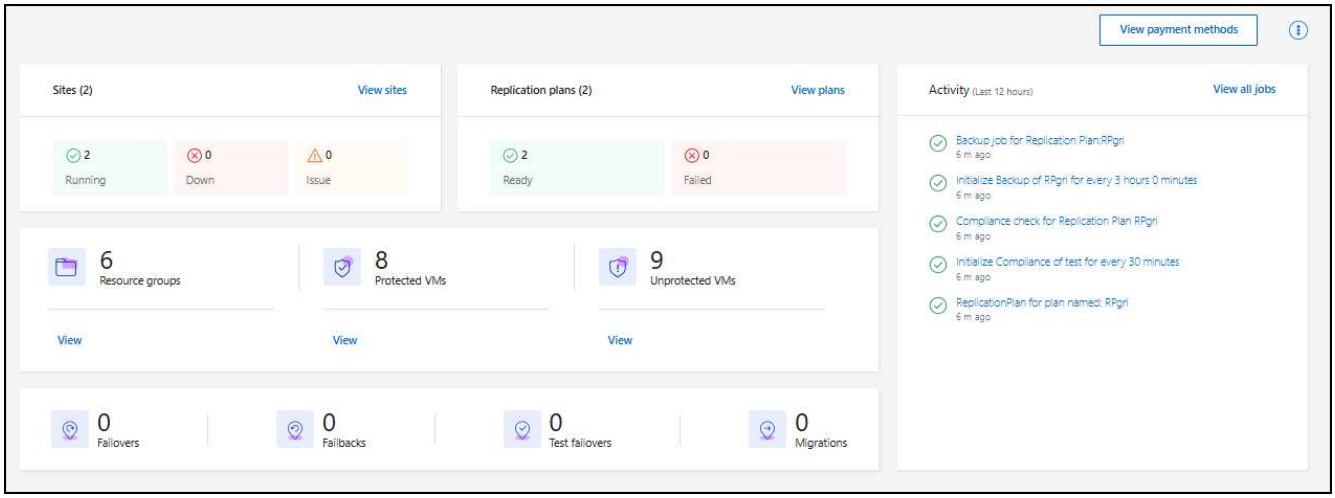
NetApp Disaster Recoveryダッシュボードを使用すると、ディザスタ リカバリ サイトとレプリケーション プランの健全性を確認できます。どのサイトとプランが正常か、切断されているか、または劣化しているかをすぐに確認できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ アプリケーション管理者、またはディザスタ リカバリ ビューア ロール。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。
3. NetApp Disaster Recoveryメニューから、ダッシュボード を選択します。



4. ダッシュボードで次の情報を確認します。
   - サイト: サイトの健全性を表示します。サイトのステータスは次のいずれかになります。
     - 実行中: vCenter は接続されており、正常に動作しており、実行中です。
     - ダウン: vCenter にアクセスできないか、接続の問題が発生しています。
     - 問題: vCenter にアクセスできないか、接続の問題が発生しています。

       サイトの詳細を表示するには、ステータスの場合は「すべて表示」を選択するか、すべてを表示するには「サイトを表示」を選択します。
   - レプリケーション プラン: プランの健全性を表示します。プランのステータスは次のいずれかになります。
     - 準備ができて
     - 失敗した

       レプリケーション プランの詳細を確認するには、ステータスの [すべて表示] を選択するか、[レプリケーション プランを表示] を選択してすべてを表示します。
   - リソース グループ: リソース グループの正常性を表示します。リソース グループのステータスは次のいずれかになります。
   - 保護された **VM**: VM はリソース グループの一部です。
   - 保護されていない **VM**: VM はリソース グループの一部ではありません。

     詳細を確認するには、それぞれの下にある 表示 リンクを選択してください。
   - フェイルオーバー、テストフェイルオーバー、および移行の数。たとえば、2 つのプランを作成し、移行先に移行した場合、移行数は「2」と表示されます。
5. アクティビティ ペインですべての操作を確認します。ジョブ モニターですべての操作を表示するには、[すべてのジョブを表示] を選択します。

NetApp Disaster Recoveryのサイトに vCenter を追加する

災害復旧プランを作成する前に、 NetApp Consoleでサイトにプライマリ vCenter Server

を追加し、ターゲットの vCenter 災害復旧サイトを追加する必要があります。

ソース vCenter とターゲット vCenter の両方で同じNetApp Consoleエージェントが使用されていることを確認します。

vCenter が追加されると、 NetApp Disaster Recovery は、vCenter クラスタ、ESXi ホスト、データストア、ストレージ フットプリント、仮想マシンの詳細、 SnapMirrorレプリカ、仮想マシン ネットワークなどの vCenter 環境の詳細な検出を実行します。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、またはディザスタ リカバリ管理者。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

このタスクについて

以前のリリースで vCenter を追加し、検出スケジュールをカスタマイズする場合は、vCenter Server サイトを編集してスケジュールを設定する必要があります。

NetApp Disaster Recovery は24 時間ごとに検出を実行します。サイトを設定した後で、vCenter を編集して、ニーズに合った検出スケジュールをカスタマイズできます。たとえば、多数の VM がある場合は、検出スケジュールを 23 時間 59 分ごとに実行するように設定できます。 VM の数が少ない場合は、検出スケジュールを 12 時間ごとに実行するように設定できます。最小間隔は 30 分、最大間隔は 24 時間です。

環境に関する最新情報を取得するには、まず手動でいくつかの検出を実行する必要があります。その後、自動的に実行されるようにスケジュールを設定できます。

以前のバージョンの vCenter があり、検出の実行タイミングを変更する場合は、vCenter Server サイトを編集してスケジュールを設定します。

新しく追加または削除された VM は、次回のスケジュールされた検出時または即時の手動検出時に認識されます。

レプリケーション プランが次のいずれかの状態にある場合にのみ、VM を保護できます。

- 準備完了
- フェイルバックがコミットされました
- テストフェイルオーバーがコミットされました

サイト内の **vCenter** クラスター 各サイトには 1 つ以上の vCenter が含まれます。これらの vCenter は、1 つ以上のONTAPストレージ クラスターを使用して NFS または VMFS データストアをホストします。

vCenter クラスタは 1 つのサイトにのみ存在できます。 vCenter クラスタをサイトに追加するには、次の情報が必要です。

- vCenter管理IPアドレスまたはFQDN
- 操作を実行するために必要な権限を持つ vCenter アカウントの資格情報。見る"必要なvCenter権限"詳細についてはこちらをご覧ください。

- クラウドホスト型VMwareサイトの場合、必要なクラウドアクセスキー
- vCenter にアクセスするためのセキュリティ証明書。

> このサービスは、自己署名セキュリティ証明書または中央証明機関 (CA) からの証明書をサポートします。

手順

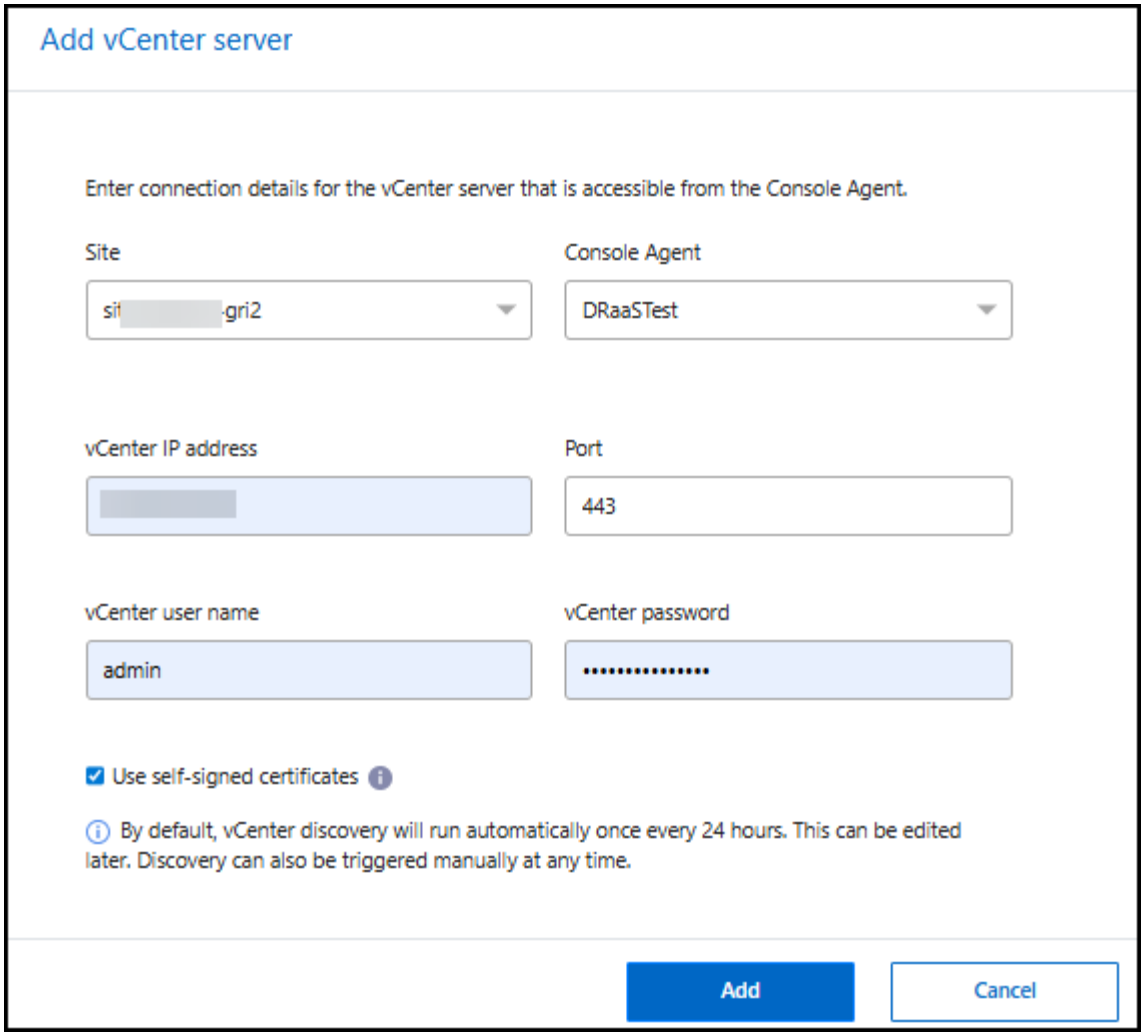
1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。

   NetApp Disaster Recoveryボード ページが表示されます。サービスを初めて開始するときは、vCenter 情報を追加する必要があります。その後、ダッシュボードにサイトとレプリケーション プランに関するデータが表示されます。

   > 追加するサイトの種類に応じて、さまざまなフィールドが表示されます。

3. すでにいくつかの vCenter サイトが存在し、さらに追加する場合は、メニューから [サイト] を選択し、[追加] を選択します。
4. [サイト] ページでサイトを選択し、[vCenter の追加] を選択します。
5. ソース: **vCenter** サーバーの検出 を選択して、ソース vCenter サイトに関する情報を入力します。

   > すでにいくつかの vCenter サイトが存在し、さらに追加する場合は、上部のメニューから [サイト] を選択し、[追加] を選択します。



- サイトを選択し、 NetApp Consoleエージェントを選択して、vCenter の資格情報を入力します。
- (オンプレミス サイトにのみ適用) ソース vCenter の自己署名証明書を受け入れるには、チェックボックスをオンにします。

> 自己署名証明書は他の証明書ほど安全ではありません。 vCenter が証明機関 (CA) 証明書で構成されていない場合は、このボックスをオンにする必要があります。そうしないと、vCenter への接続が機能しません。

6. *追加*を選択します。

   次に、ターゲット vCenter を追加します。

7. ターゲット vCenter のサイトを再度追加します。
8. 再度、「vCenter の追加」を選択し、ターゲットの vCenter 情報を追加します。
9. ターゲット：

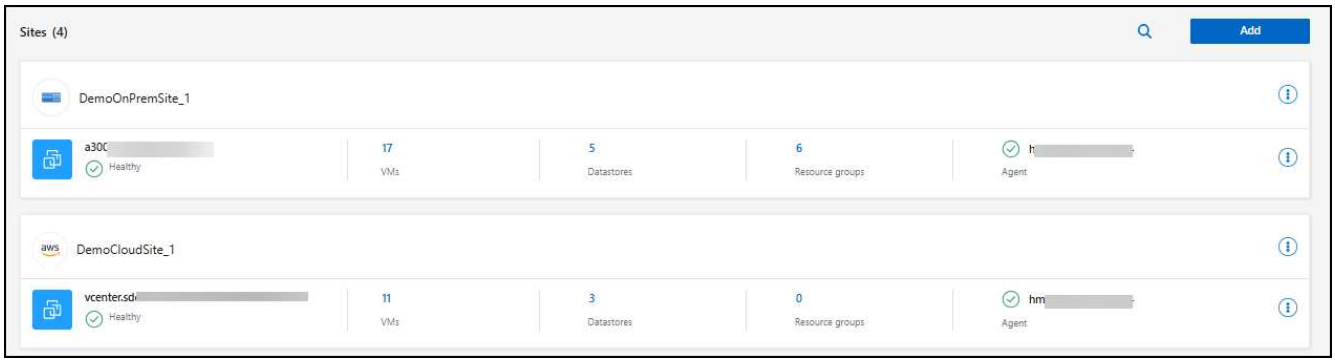
   a. 対象サイトと場所を選択します。ターゲットがクラウドの場合は*AWS*を選択します。

      - (クラウド サイトにのみ適用) **API** トークン: 組織のサービス アクセスを承認するための API トークンを入力します。特定の組織およびサービス ロールを指定して API トークンを作成します。

- (クラウド サイトにのみ適用) 長い組織 **ID**: 組織の一意の ID を入力します。この ID は、NetApp Consoleのアカウント セクションでユーザー名をクリックすると識別できます。

b. *追加*を選択します。

ソース vCenter とターゲット vCenter がサイトのリストに表示されます。



10. 操作の進行状況を確認するには、メニューから「ジョブ監視」を選択します。

vCenter サイトのサブネット マッピングを追加する

サブネット マッピングを使用してフェイルオーバー操作時の IP アドレスを管理できます。これにより、vCenter ごとにサブネットを追加できます。これを実行すると、各仮想ネットワークの IPv4 CIDR、デフォルト ゲートウェイ、および DNS が定義されます。

フェイルオーバー時に、 NetApp Disaster Recovery はマッピングされたネットワークの CIDR を使用して各 vNIC に新しい IP アドレスを割り当てます。

例えば：

- ネットワークA = 10.1.1.0/24
- ネットワークB = 192.168.1.0/24

VM1 には、NetworkA に接続された vNIC (10.1.1.50) があります。レプリケーション プラン設定では、NetworkA は NetworkB にマップされます。

フェイルオーバー時に、 NetApp Disaster Recovery は元の IP アドレス (10.1.1) のネットワーク部分を置き換え、元の IP アドレス (10.1.1.50) のホスト アドレス (.50) を保持します。 VM1 の場合、 NetApp Disaster Recovery はNetworkB の CIDR 設定を確認し、NetworkB のネットワーク部分 192.168.1 を使用し、ホスト部分 (.50) を保持して VM1 の新しい IP アドレスを作成します。新しい IP は 192.168.1.50 になります。

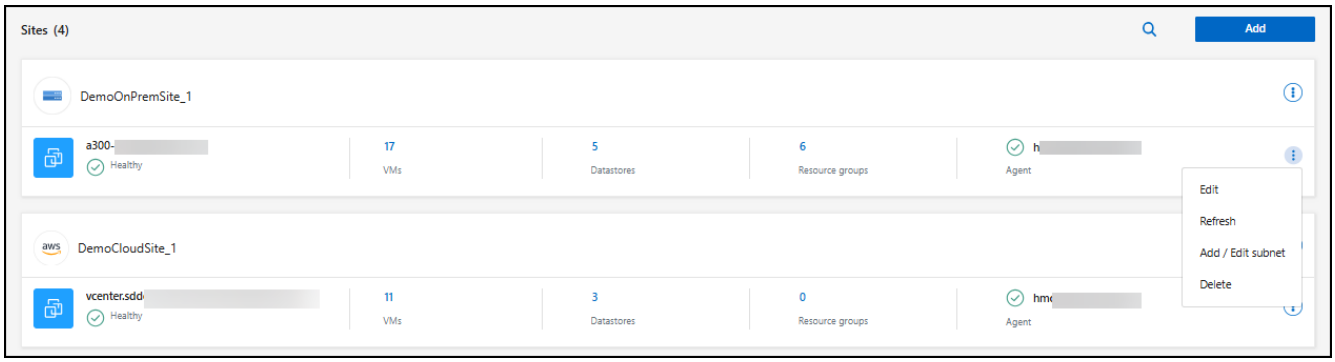
要約すると、ホスト アドレスは同じままですが、ネットワーク アドレスはサイトのサブネット マッピングで構成されているものに置き換えられます。これにより、特に数百のネットワークと数千の VM を管理する場合に、フェイルオーバー時の IP アドレスの再割り当てをより簡単に管理できるようになります。

サブネット マッピングの使用は、オプションの 2 段階のプロセスです。

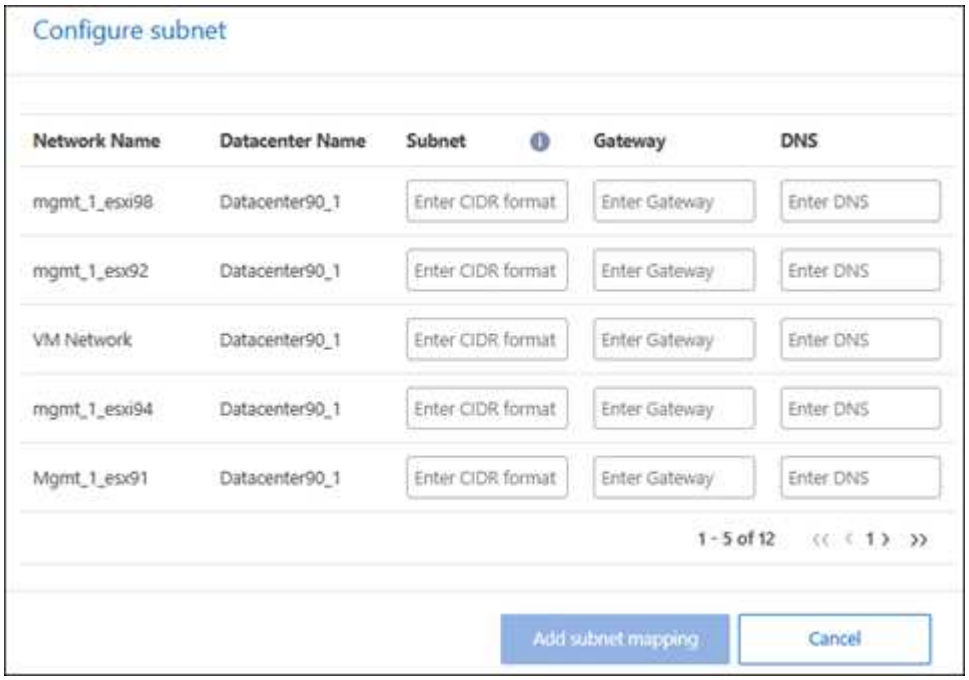
- まず、各 vCenter サイトのサブネット マッピングを追加します。
- 次に、レプリケーション プランの [仮想マシン] タブと [ターゲット IP] フィールドでサブネット マッピングを使用することを指定します。

手順

1. NetApp Disaster Recoveryメニューから、サイト を選択します。
2. 行動から 右側のアイコンをクリックし、*サブネットの追加*を選択します。



サブネットの構成ページが表示されます。



3. 「サブネットの構成」ページで、次の情報を入力します。
   a. サブネット: /32 までのサブネットの IPv4 CIDR を入力します。

> CIDR 表記は、IP アドレスとそのネットワーク マスクを指定する方法です。 /24 はネットマスクを表します。この番号は IP アドレスと、「/」の後の数字で構成され、IP アドレスの何ビットがネットワークを表すかを示します。たとえば、192.168.0.50/24 の場合、IP アドレスは 192.168.0.50 で、ネットワーク アドレスのビットの合計数は 24 です。 192.168.0.50 255.255.255.0 は 192.168.0.0/24 になります。

   b. ゲートウェイ: サブネットのデフォルトゲートウェイを入力します。
   c. DNS: サブネットの DNS を入力します。
4. *サブネット マッピングの追加*を選択します。

レプリケーションプランのサブネットマッピングを選択する

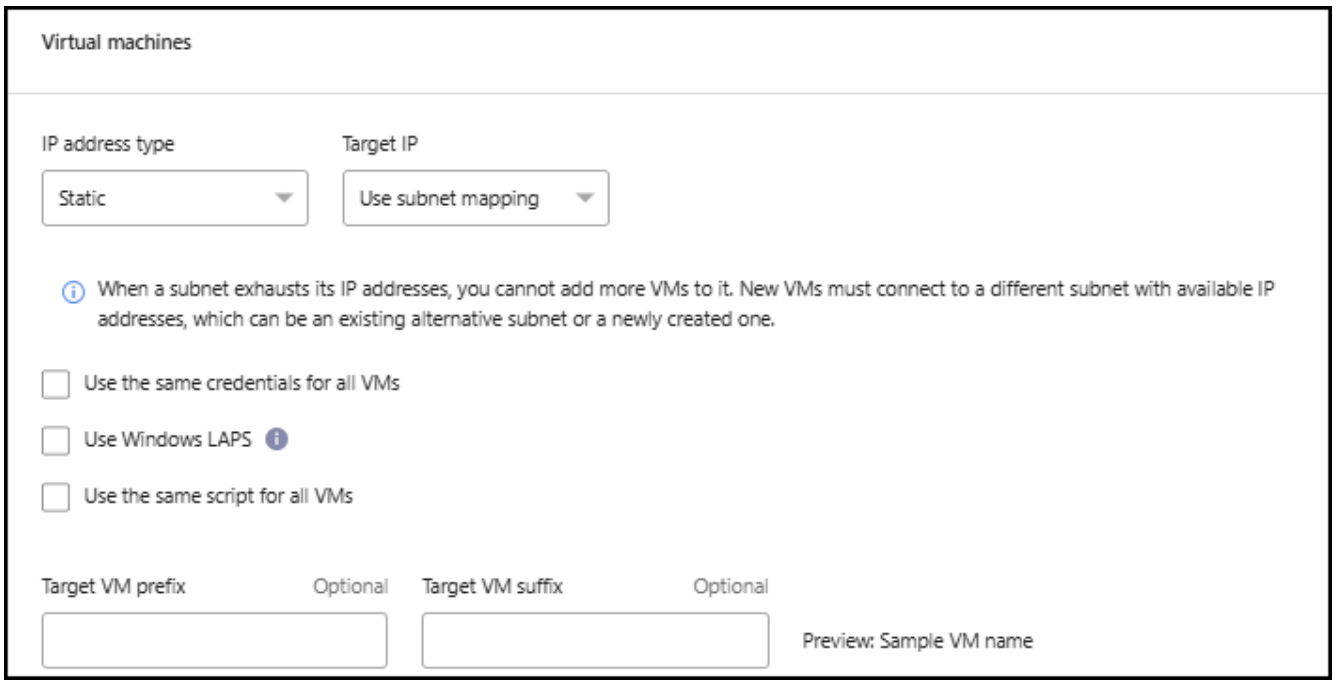
レプリケーション プランを作成するときに、レプリケーション プランのサブネット マッピングを選択できます。

サブネット マッピングの使用は、オプションの 2 段階のプロセスです。

- まず、各 vCenter サイトのサブネット マッピングを追加します。
- 次に、レプリケーション プランで、サブネット マッピングを使用することを指定します。

手順

1. NetApp Disaster Recoveryメニューから、レプリケーション プラン を選択します。
2. レプリケーション プランを追加するには、[追加] を選択します。
3. vCenter サーバーを追加し、リソース グループまたはアプリケーションを選択し、マッピングを完了して、通常の方法でフィールドを入力します。
4. レプリケーション プラン > リソース マッピング ページで、仮想マシン セクションを選択します。



5. ターゲット **IP** フィールドで、ドロップダウン リストから サブネット マッピングを使用する を選択します。

> VM が 2 つある場合 (たとえば、1 つは Linux で、もう 1 つは Windows)、資格情報は Windows に対してのみ必要です。

6. レプリケーション プランの作成を続行します。

vCenter Server サイトを編集し、検出スケジュールをカスタマイズします

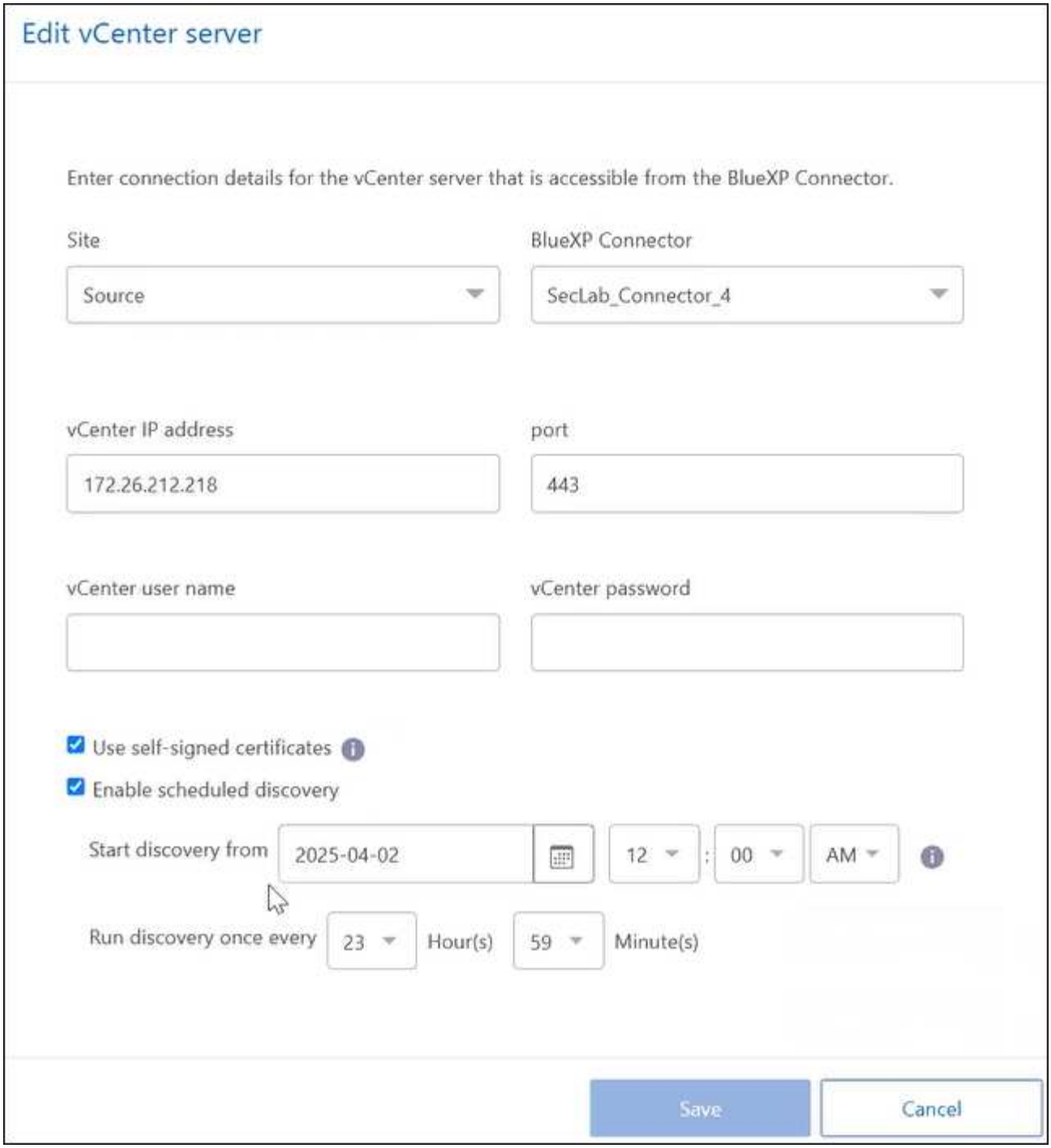
vCenter Server サイトを編集して検出スケジュールをカスタマイズできます。たとえば、多数の VM がある場合は、検出スケジュールを 23 時間 59 分ごとに実行するように設定できます。 VM の数が少ない場合は、検出スケジュールを 12 時間ごとに実行するように設定できます。

以前のバージョンの vCenter があり、検出の実行タイミングを変更する場合は、vCenter Server サイトを編集してスケジュールを設定します。

検出をスケジュールしたくない場合は、スケジュールされた検出オプションを無効にして、いつでも手動で検出を更新できます。

手順

1. NetApp Disaster Recoveryメニューから、サイト を選択します。
2. 編集したいサイトを選択します。
3. アクションを選択  右側のアイコンをクリックし、[編集] を選択します。
4. 「vCenter サーバーの編集」ページで、必要に応じてフィールドを編集します。
5. 検出スケジュールをカスタマイズするには、[スケジュールされた検出を有効にする] ボックスをオンにして、必要な日付と時刻間隔を選択します。



6. *保存*を選択します。

検出を手動で更新する

検出はいつでも手動で更新できます。これは、VM を追加または削除し、 NetApp Disaster Recoveryの情報を更新する場合に便利です。

手順

1. NetApp Disaster Recoveryメニューから、サイト を選択します。
2. 更新するサイトを選択します。

3. アクションを選択  右側のアイコンをクリックし、[更新] を選択します。

NetApp Disaster Recoveryで VM を整理するためのリソース グループを作成する

vCenter サイトを追加した後、VM またはデータストアを単一のユニットとして保護するためのリソース グループを作成できます。リソース グループを使用すると、依存する一連の VM を、要件を満たす論理グループに編成できます。たとえば、1 つのアプリケーションに関連付けられた VM をグループ化したり、同様の層を持つアプリケーションをグループ化したりすることができます。別の例として、グループには回復時に実行できる遅延ブート オーダーが含まれる場合があります。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、またはディザスタ リカバリ アプリケーション管理者のロール。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

このタスクについて

VM 自体またはデータストア内の VM をグループ化できます。

次の方法を使用してリソース グループを作成できます。

- リソースグループオプションから
- 災害復旧またはレプリケーション プランを作成している間。ソース vCenter クラスターによってホストされている VM が多数ある場合は、レプリケーション プランの作成時にリソース グループを作成する方が簡単な場合があります。レプリケーションプランの作成中にリソースグループを作成する手順については、"レプリケーションプランを作成する" 。

各リソース グループには、1 つ以上の VM またはデータストアを含めることができます。 VM は、レプリケーション プランに含めた順序に基づいて電源がオンになります。 VM またはデータストアをリソース グループ リスト内で上下にドラッグすることで、順序を変更できます。

リソースグループについて

リソース グループを使用すると、VM またはデータストアを 1 つのユニットとして結合できます。

たとえば、POS アプリケーションでは、データベース、ビジネス ロジック、ストアフロント用に複数の VM が使用される場合があります。これらすべての VM を 1 つのリソース グループで管理できます。 VM の起動順序、ネットワーク接続、およびアプリケーションに必要なすべての VM の回復に関するレプリケーション プラン ルールを適用するリソース グループを設定します。

どのように機能しますか**?**

NetApp Disaster Recovery は、リソース グループ内の VM をホストしている基盤となるONTAPボリュームと LUN を複製することで VM を保護します。これを行うには、システムはリソース グループ内の VM をホストしている各データ ストアの名前を vCenter に照会します。次に、 NetApp Disaster Recovery は、そのデータストアをホストしているソースONTAPボリュームまたは LUN を識別します。すべての保護は、 SnapMirror

レプリケーションを使用してONTAPボリューム レベルで実行されます。

リソース グループ内の VM が異なるデータ ストアでホストされている場合、 NetApp Disaster Recovery は次のいずれかの方法を使用して、 ONTAPボリュームまたは LUN のデータ整合性のあるスナップショットを作成します。

FlexVolボリュームの相対的な位置	スナップショットレプリカプロセス
複数のデータストア - 同じ **SVM** 内のFlexVolボリューム	• ONTAP整合性グループが作成されました • 整合性グループのスナップショットを取得 • ボリュームスコープのSnapMirrorレプリケーションが実行される
複数のデータストア - 複数の **SVM** 内のFlexVolボリューム	• ONTAP API: `cg_start` 。スナップショットを取得できるようにすべてのボリュームを静止し、すべてのリソース グループ ボリュームのボリューム スコープのスナップショットを開始します。 • ONTAP API: `cg_end` 。スナップショットが取得された後、すべてのボリューム上の I/O を再開し、ボリューム スコープのSnapMirrorレプリケーションを有効にします。

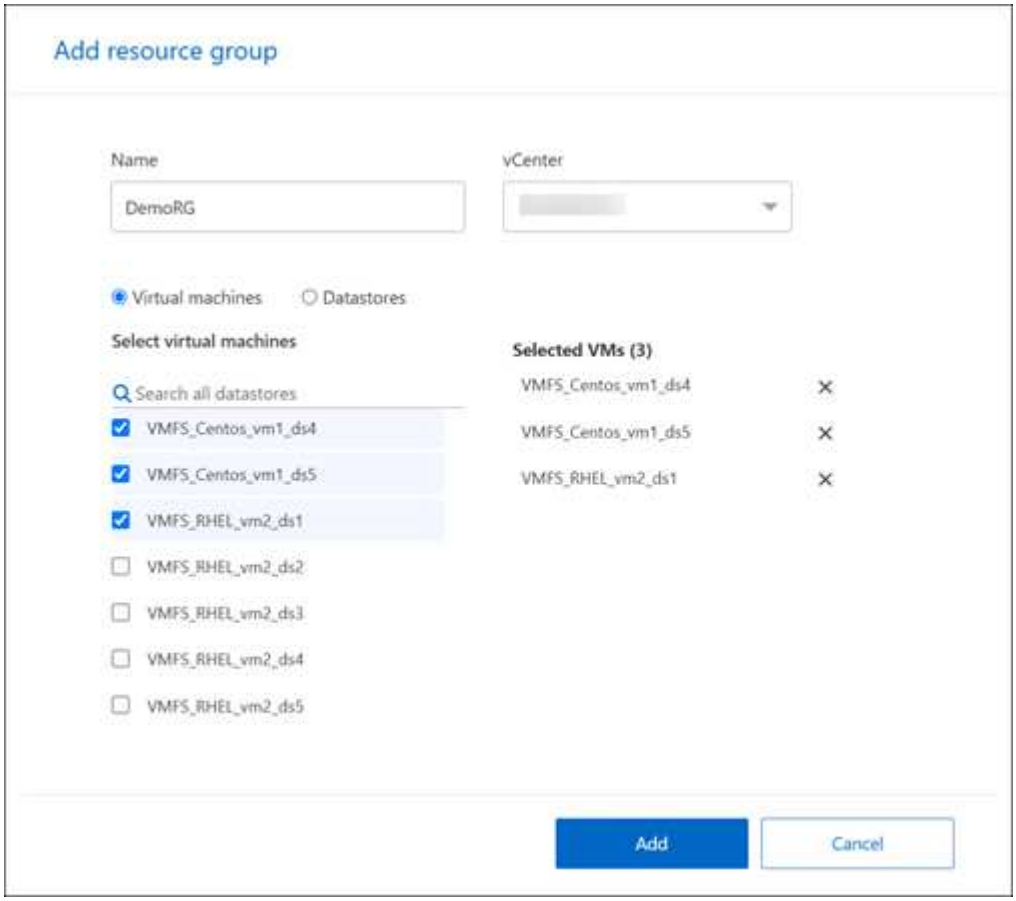
リソース グループを作成するときは、次の点を考慮してください。

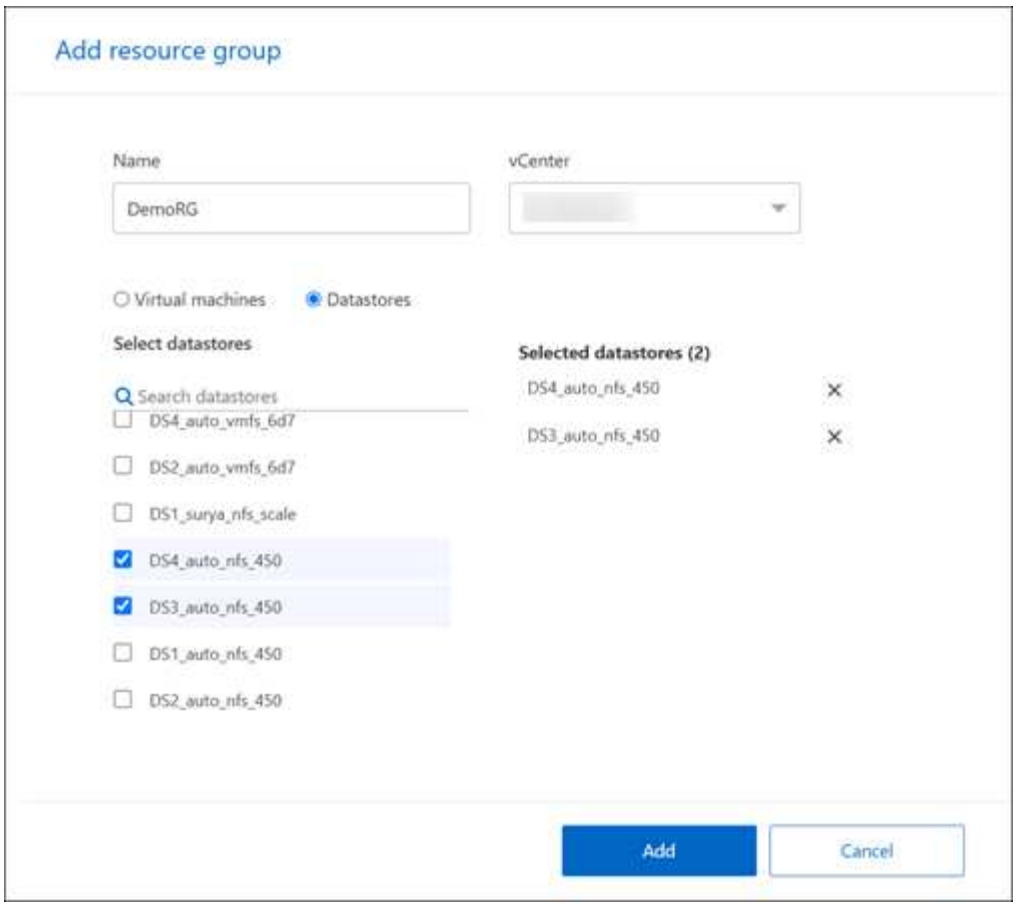
- データストアをリソース グループに追加する前に、まず VM の手動検出またはスケジュールされた検出を開始します。これにより、VM が検出され、リソース グループにリストされるようになります。手動検出を開始しないと、VM がリソース グループにリストされない可能性があります。
- データストアに少なくとも 1 つの VM があることを確認します。データストアに VM がない場合、Disaster Recovery はデータストアを検出しません。
- 単一のデータストアは、複数のレプリケーション プランによって保護されている VM をホストしないでください。
- 保護された VM と保護されていない VM を同じデータストアにホストしないでください。保護された VM と保護されていない VM が同じデータストアでホストされている場合、次の問題が発生する可能性があります。
  - NetApp Disaster Recovery はSnapMirrorを使用し、システムがONTAPボリューム全体を複製するため、そのボリュームの使用容量がライセンスの考慮に使用されます。この場合、保護された VM と保護されていない VM の両方によって消費されるボリューム スペースがこの計算に含まれます。
  - リソース グループとそれに関連付けられたデータストアを災害復旧サイトにフェイルオーバーする必要がある場合、保護されていない VM (リソース グループの一部ではないが、 ONTAPボリュームでホストされている VM) はフェイルオーバー プロセスによってソース サイトに存在しなくなり、その結果、ソース サイトで保護されていない VM に障害が発生します。また、 NetApp Disaster Recovery、フェールオーバー vCenter サイトで保護されていない VM を起動しません。
- VM を保護するには、VM をリソース グループに含める必要があります。

ベスト プラクティス: NetApp Disaster Recoveryを展開する前に VM を整理して、「データストアの無秩序な増加」を最小限に抑えます。保護が必要な VM をデータストアのサブセットに配置し、保護する必要のない VM をデータストアの別のサブセットに配置します。特定のデータストア上の VM が異なるレプリケーション プランによって保護されていないことを確認します。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。
3. NetApp Disaster Recoveryメニューから、リソース グループ を選択します。
4. *追加*を選択します。
5. リソース グループの名前を入力します。
6. VM が配置されているソース vCenter クラスタを選択します。
7. 検索方法に応じて、仮想マシン または データストア のいずれかを選択します。
8. リソース グループの追加 タブを選択します。システムは、選択した vCenter クラスタ内のすべてのデータストアまたは VM を一覧表示します。 データストア を選択した場合、システムは選択した vCenter クラスタ内のすべてのデータストアを一覧表示します。 仮想マシン を選択した場合、システムは選択した vCenter クラスター内のすべての仮想マシンを一覧表示します。
9. [リソース グループの追加] ページの左側で、保護する VM を選択します。





10. 必要に応じて、各 VM をリスト内で上下にドラッグして、右側の VM の順序を変更します。 VM は、追加した順序に基づいて電源がオンになります。
11. *追加*を選択します。

NetApp Disaster Recoveryでレプリケーションプランを作成する

vCenter サイトを追加したら、災害復旧またはレプリケーション プランを作成する準備が整います。レプリケーション プランは、VMware インフラストラクチャのデータ保護を管理します。ソースと宛先の vCenter を選択し、リソース グループを選択して、アプリケーションを復元してパワーオンする方法をグループ化します。たとえば、1 つのアプリケーションに関連付けられた仮想マシン (VM) をグループ化したり、同様の層を持つアプリケーションをグループ化したりすることができます。このような計画は、_青写真_と呼ばれることもあります。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ フェールオーバー管理者、またはディザスタ リカバリ アプリケーション管理者のロール。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

このタスクについて

レプリケーション プランを作成し、コンプライアンスとテストのスケジュールを編集することもできます。運用ワークロードに影響を与えずに VM のテスト フェイルオーバーを実行します。

複数のデータストア上の複数の VM を保護できます。 NetApp Disaster Recovery は、保護された VM データストアをホストするすべてのONTAPボリュームに対してONTAP整合性グループを作成します。

レプリケーション プランが次のいずれかの状態にある場合にのみ、VM を保護できます。

- 準備完了
- フェイルバックがコミットされました
- テストフェイルオーバーがコミットされました

レプリケーションプランのスナップショット

ディザスタ リカバリでは、ソース クラスターと宛先クラスターで同じ数のスナップショットが維持されます。デフォルトでは、サービスは 24 時間ごとにスナップショット調整プロセスを実行し、ソース クラスターと宛先クラスターのスナップショットの数が同じであることを確認します。

次の状況では、ソース クラスターと宛先クラスター間でスナップショットの数が異なる可能性があります。

- 状況によっては、ディザスタ リカバリ以外のONTAP操作によってボリュームからスナップショットが追加または削除されることがあります。
  - ソース サイトに不足しているスナップショットがある場合、関係のデフォルトのSnapMirrorポリシーに応じて、宛先サイト上の対応するスナップショットが削除される可能性があります。
  - 宛先サイトで不足しているスナップショットがある場合、関係のデフォルトのSnapMirrorポリシーに応じて、サービスによって、次にスケジュールされたスナップショット調整プロセス中にソース サイトの対応するスナップショットが削除されることがあります。
- レプリケーション プランのスナップショット保持数を削減すると、新たに削減された保持数を満たすために、ソース サイトと宛先サイトの両方で最も古いスナップショットがサービスによって削除される可能性があります。

このような場合、ディザスタ リカバリでは、次の整合性チェック時にソース クラスターと宛先クラスターから古いスナップショットが削除されます。または、管理者は*アクション*を選択して即時スナップショットのクリーンアップを実行することもできます。 ••• レプリケーション プランのアイコンをクリックし、[スナップショットのクリーンアップ] を選択します。

サービスは 24 時間ごとにスナップショットの対称性チェックを実行します。

始める前に

SnapMirror関係を作成する前に、Disaster Recovery の外部でクラスタと SVM ピアリングを設定します。

ベスト プラクティス: NetApp Disaster Recoveryを展開する前に VM を整理して、「データストアの無秩序な増加」を最小限に抑えます。保護が必要な VM をデータストアのサブセットに配置し、保護する必要のない VM をデータストアの別のサブセットに配置します。データストアベースの保護を使用して、特定のデータストア上の VM が確実に保護されるようにします。

計画を作成する

ウィザードに従って次の手順を実行します。

- vCenter サーバーを選択します。
- 複製する VM またはデータストアを選択し、リソース グループを割り当てます。
- ソース環境のリソースが宛先にどのようにマップされるかをマップします。
- プランの実行頻度を設定し、ゲストホスト スクリプトを実行し、ブート順序を設定し、回復ポイントの目標を選択します。
- 計画を見直します。

計画を作成するときは、次のガイドラインに従う必要があります。

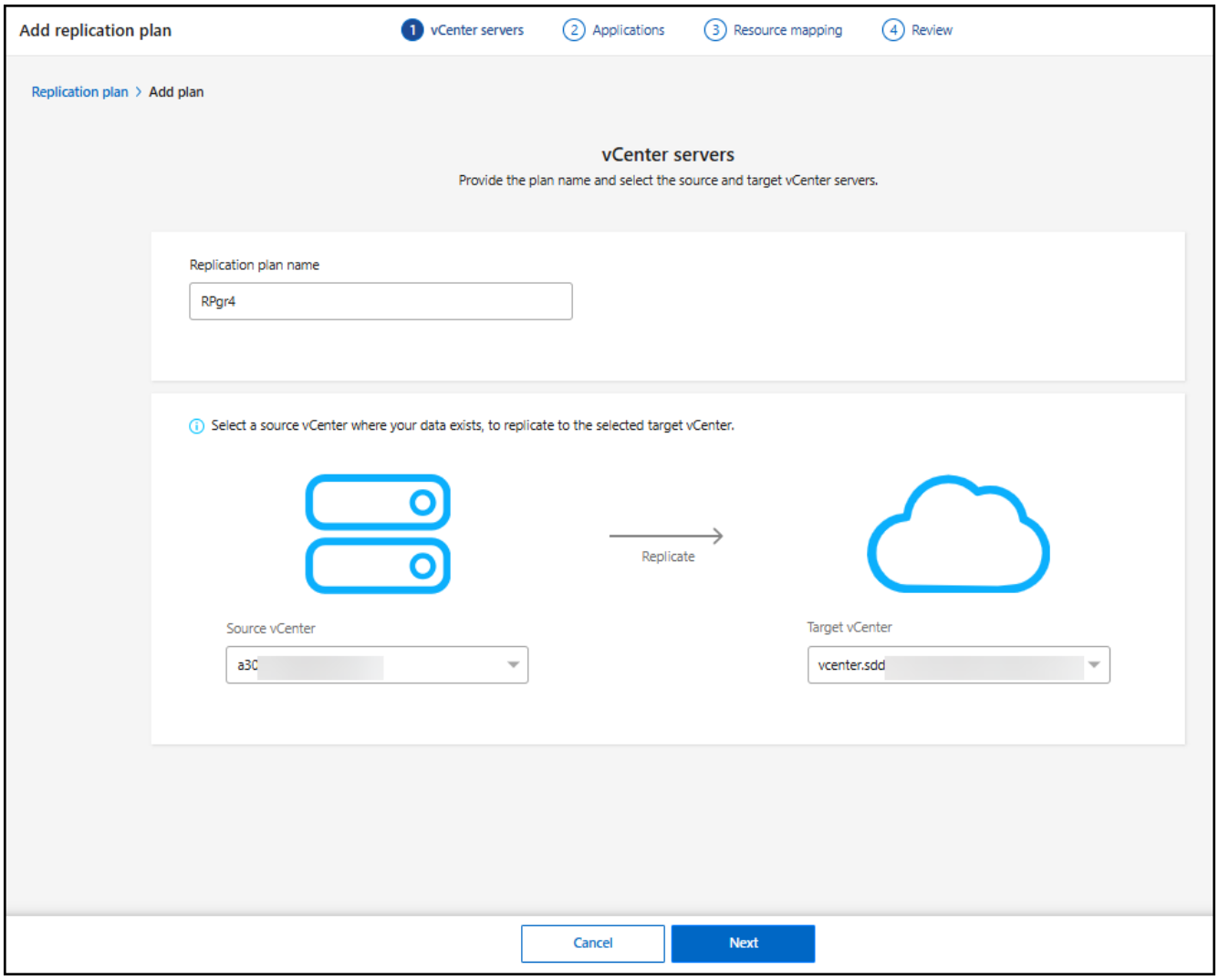
- プラン内のすべての VM に同じ資格情報を使用します。
- プラン内のすべての VM に同じスクリプトを使用します。
- プラン内のすべての VM に同じサブネット、DNS、ゲートウェイを使用します。

vCenterサーバーを選択

まず、ソース vCenter を選択し、次に宛先 vCenter を選択します。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。
3. NetApp Disaster Recoveryメニューから、レプリケーション プラン を選択し、追加 を選択します。または、サービスを使い始めたばかりの場合は、ダッシュボードから [レプリケーション プランの追加] を選択します。



4. レプリケーション プランの名前を作成します。
5. ソース vCenter およびターゲット vCenter リストからソース vCenter とターゲット vCenter を選択します。
6. *次へ*を選択します。

複製するアプリケーションを選択し、リソース グループを割り当てます

次のステップは、必要な VM またはデータストアを機能リソース グループにグループ化することです。リソース グループを使用すると、共通のスナップショットを使用して一連の VM またはデータストアを保護できます。

レプリケーション プランでアプリケーションを選択すると、プラン内の各 VM またはデータストアのオペレーティング システムが表示されます。これは、VM またはデータストアをリソース グループにグループ化する方法を決定するのに役立ちます。

各リソース グループには、1 つ以上の VM またはデータストアを含めることができます。

リソース グループを作成するときは、次の点を考慮してください。

- データストアをリソース グループに追加する前に、まず VM の手動検出またはスケジュールされた検出を

開始します。これにより、VM が検出され、リソース グループにリストされるようになります。手動検出をトリガーしないと、VM がリソース グループにリストされない可能性があります。

- データストアに少なくとも 1 つの VM があることを確認します。データストアに VM がない場合、データストアは検出されません。
- 単一のデータストアは、複数のレプリケーション プランによって保護されている VM をホストしないでください。
- 保護された VM と保護されていない VM を同じデータストアにホストしないでください。保護された VM と保護されていない VM が同じデータストアでホストされている場合、次の問題が発生する可能性があります。
  - NetApp Disaster Recovery はSnapMirrorを使用し、システムがONTAPボリューム全体を複製するため、そのボリュームの使用容量がライセンスの考慮に使用されます。この場合、保護された VM と保護されていない VM の両方によって消費されるボリューム スペースがこの計算に含まれます。
  - リソース グループとそれに関連付けられたデータストアを災害復旧サイトにフェイルオーバーする必要がある場合、保護されていない VM (リソース グループの一部ではないが、 ONTAPボリュームでホストされている VM) はフェイルオーバー プロセスによってソース サイトに存在しなくなり、その結果、ソース サイトで保護されていない VM に障害が発生します。また、 NetApp Disaster Recovery、フェールオーバー vCenter サイトで保護されていない VM を起動しません。
- VM を保護するには、VM をリソース グループに含める必要があります。

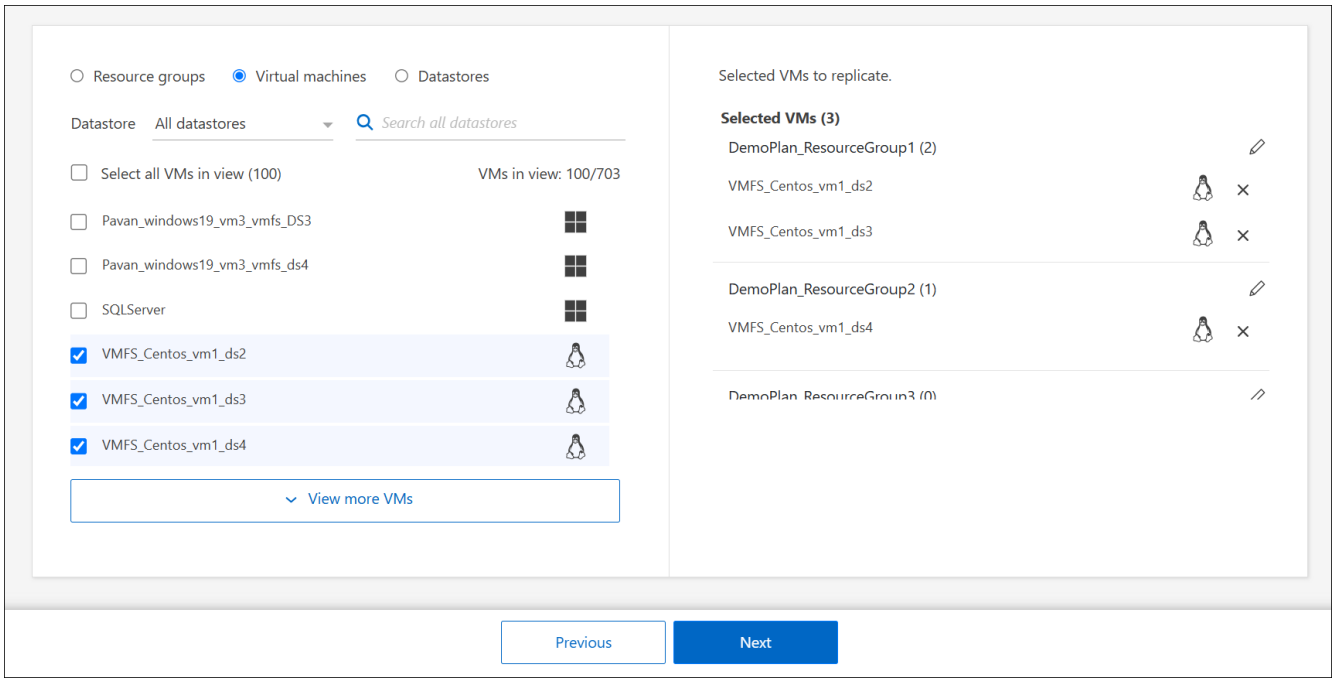
ベスト プラクティス: フェイルオーバー テスト用に別の専用マッピング セットを作成し、同じ IP アドレスを使用して VM が実稼働ネットワークに接続されるのを防ぎます。

手順

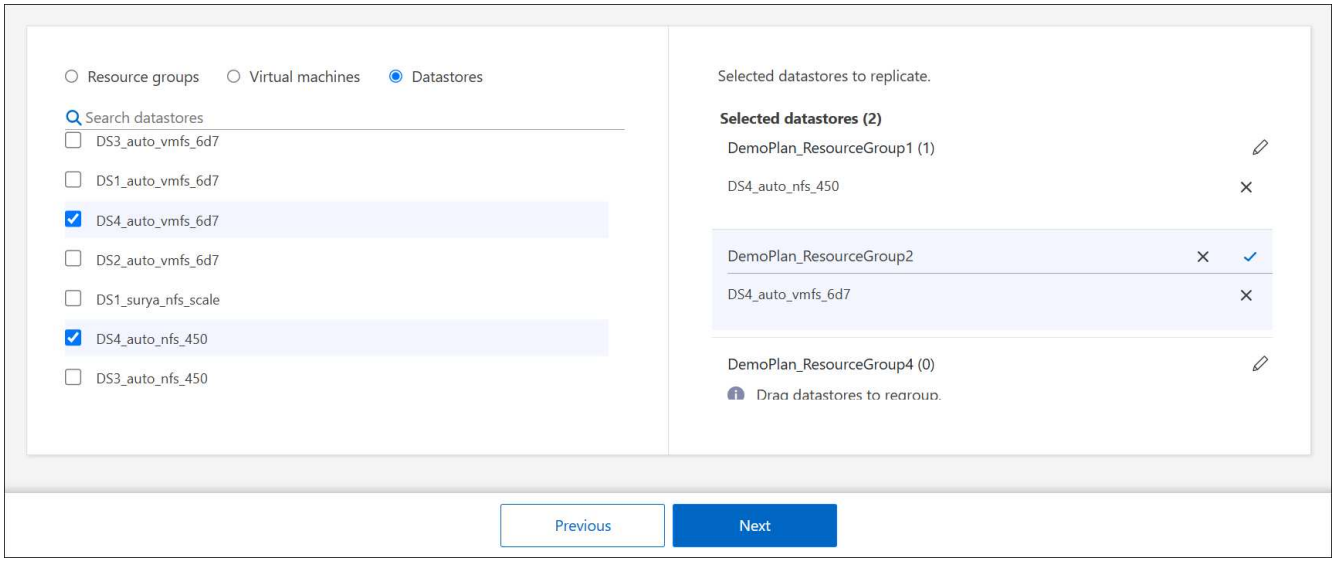
1. *仮想マシン*または*データストア*を選択します。
2. 必要に応じて、特定の VM またはデータストアを名前で検索します。
3. 「アプリケーション」ページの左側で、保護する VM またはデータストアを選択し、選択したグループに割り当てます。

   ソース vCenter はオンプレミスの vCenter 上に存在している必要があります。ターゲット vCenter は、同じサイトまたはリモート サイト内の 2 番目のオンプレミス vCenter、または VMware Cloud on AWS などのクラウドベースのソフトウェア定義データ センター (SDDC) にすることができます。両方の vCenter はすでにBlueXP disaster recovery作業環境に追加されているはずです。

   選択したリソースは自動的にグループ 1 に追加され、新しいグループ 2 が開始されます。最後のグループにリソースを追加するたびに、別のグループが追加されます。



または、データストアの場合:



4. 必要に応じて、次のいずれかを実行します。
   - グループの名前を変更するには、グループの*編集*をクリックします。 アイコン。
   - グループからリソースを削除するには、リソースの横にある **X** を選択します。
   - リソースを別のグループに移動するには、新しいグループにドラッグ アンド ドロップします。

   データストアを別のリソース グループに移動するには、不要なデータストアの選択を解除し、レプリケーション プランを送信します。次に、他のレプリケーション プランを作成または編集し、データストアを再度選択します。

5. *次へ*を選択します。

ソースリソースをターゲットにマッピングする

リソース マッピング ステップでは、ソース環境のリソースをターゲットにどのようにマッピングするかを指定します。レプリケーション プランを作成するときに、プラン内の各 VM のブート遅延と順序を設定できます。これにより、VM の起動順序を設定できます。

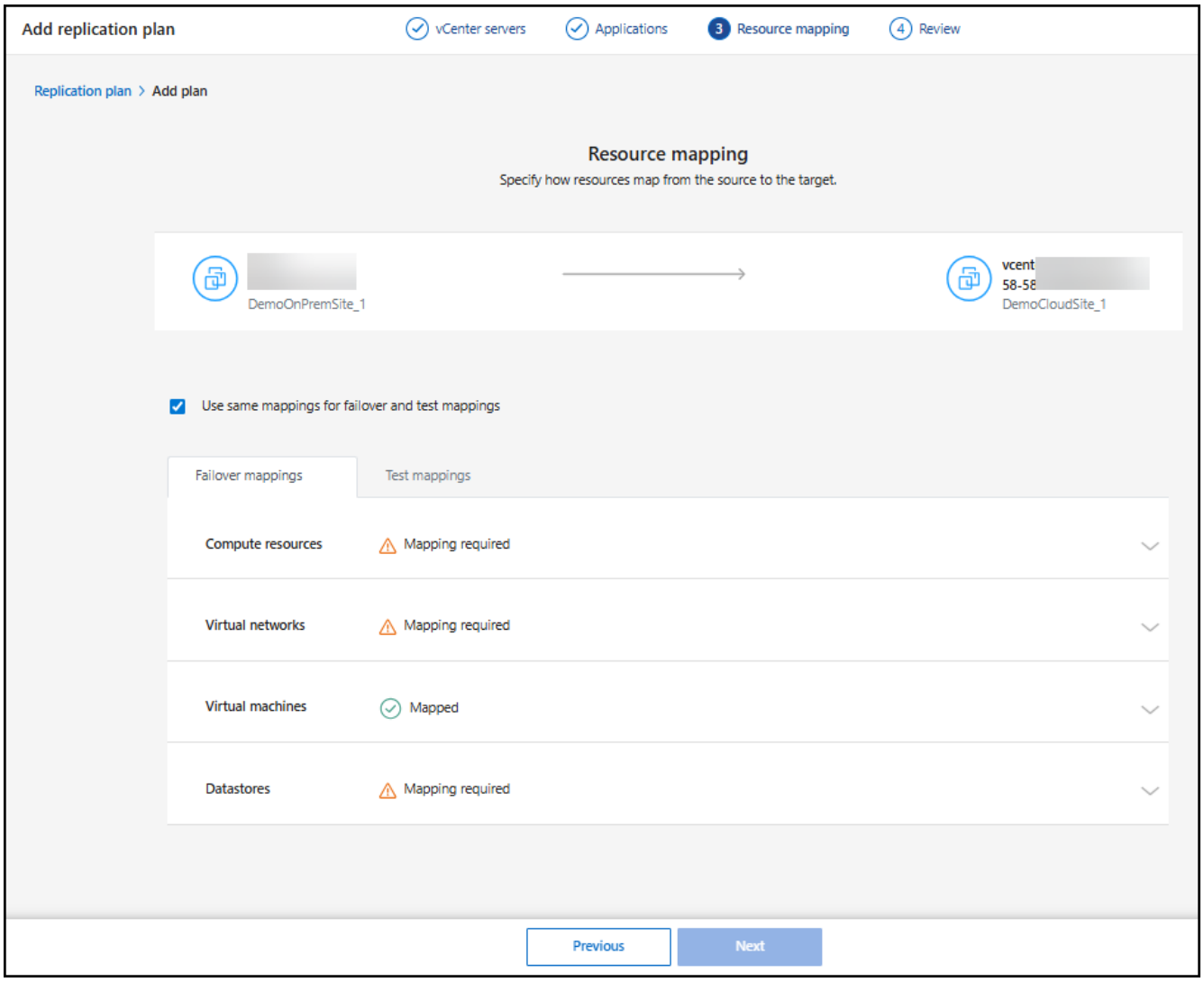
DR 計画の一環としてテスト フェールオーバーを実行する予定の場合は、フェールオーバー テスト中に起動された VM が運用 VM に干渉しないように、一連のテスト フェールオーバー マッピングを提供する必要があります。これを実現するには、テスト VM に異なる IP アドレスを提供するか、テスト VM の仮想 NIC を、運用環境から分離されているが同じ IP 構成を持つ別のネットワーク (バブル または テスト ネットワーク と呼ばれる) にマッピングします。

開始する前に

このサービスでSnapMirror関係を作成する場合は、クラスタとその SVM ピアリングがNetApp Disaster Recoveryの外部ですでに設定されている必要があります。

手順

1. リソース マッピング ページで、フェールオーバーとテスト操作の両方に同じマッピングを使用するには、チェックボックスをオンにします。



2. フェールオーバー マッピング タブで、各リソースの右側にある下矢印を選択し、各セクションのリソー

スをマッピングします。

- コンピューティングリソース
- 仮想ネットワーク
- 仮想マシン
- データストア

マップリソース > コンピューティングリソースセクション

コンピューティング リソース セクションでは、フェイルオーバー後に VM が復元される場所を定義します。ソース vCenter データセンターとクラスタをターゲット データセンターとクラスタにマップします。

オプションで、特定の vCenter ESXi ホストで VM を再起動できます。 VMWare DRS が有効になっている場合は、DR で構成されたポリシーを満たすために必要に応じて、VM を代替ホストに自動的に移動できます。

オプションで、このレプリケーション プラン内のすべての VM を vCenter の一意のフォルダーに配置できます。これにより、vCenter 内でフェールオーバーされた VM をすばやく整理する簡単な方法が提供されます。

コンピューティング リソース の横にある下矢印を選択します。

- ソースデータセンターとターゲットデータセンター
- ターゲットクラスター
- ターゲット ホスト (オプション): クラスターを選択した後、この情報を設定できます。

vCenter にクラスタ内の複数のホストを管理するように構成された Distributed Resource Scheduler (DRS) がある場合は、ホストを選択する必要はありません。ホストを選択すると、NetApp Disaster Recovery はすべての VM を選択したホストに配置します。 * ターゲット **VM** フォルダー (オプション): 選択した VM を保存するための新しいルート フォルダーを作成します。

マップリソース > 仮想ネットワークセクション

VM は仮想ネットワークに接続された仮想 NIC を使用します。フェイルオーバー プロセスでは、サービスはこれらの仮想 NIC を、宛先の VMware 環境で定義された仮想ネットワークに接続します。リソース グループ内の VM によって使用されるソース仮想ネットワークごとに、サービスでは宛先仮想ネットワークの割り当てが必要です。

複数のソース仮想ネットワークを同じターゲット仮想ネットワークに割り当てることができます。ただし、これにより IP ネットワーク構成の競合が発生する可能性があります。複数のソース ネットワークを単一のターゲット ネットワークにマップして、すべてのソース ネットワークの構成が同じになるようにすることができます。

フェールオーバー マッピング タブで、仮想ネットワーク の横にある下矢印を選択します。ソース仮想 LAN とターゲット仮想 LAN を選択します。

適切な仮想 LAN へのネットワーク マッピングを選択します。仮想 LAN はすでにプロビジョニングされているはずなので、適切な仮想 LAN を選択して VM をマップします。

マップリソース > 仮想マシンセクション

次のいずれかのオプションを設定することで、レプリケーション プランによって保護されるリソース グループ内の各 VM を、宛先の vCenter 仮想環境に適合するように構成できます。

- 仮想CPUの数
- 仮想DRAMの量
- IPアドレスの設定
- フェイルオーバープロセスの一部としてゲストOSシェルスクリプトを実行する機能
- 固有のプレフィックスとサフィックスを使用してフェイルオーバーされたVM名を変更する機能
- VMフェイルオーバー時の再起動順序を設定する機能

フェールオーバー マッピング タブで、仮想マシン の横にある下矢印を選択します。

VM のデフォルトがマップされます。デフォルトのマッピングでは、VM が実稼働環境で使用するのと同じ設定 (同じ IP アドレス、サブネット マスク、ゲートウェイ) が使用されます。

デフォルト設定を変更する場合は、[ターゲット IP] フィールドを [ソースと異なる] に変更する必要があります。

設定を「ソースと異なる」に変更する場合は、VM ゲスト OS の資格情報を提供する必要があります。

このセクションには、選択内容に応じて異なるフィールドが表示される場合があります。

フェールオーバーされた各 VM に割り当てられる仮想 CPU の数を増減できます。ただし、各 VM には少なくとも 1 つの仮想 CPU が必要です。各 VM に割り当てられる仮想 CPU と仮想 DRAM の数を変更できます。デフォルトの仮想 CPU および仮想 DRAM 設定を変更する最も一般的な理由は、ターゲット vCenter クラスタ ノードに、ソース vCenter クラスタと同じ数の使用可能なリソースがない場合です。

ネットワーク設定 ディザスタ リカバリでは、VM ネットワークの広範な構成オプションがサポートされています。ターゲット サイトに、ソース サイトの運用仮想ネットワークとは異なる TCP/IP 設定を使用する仮想ネットワークがある場合は、これらを変更する必要がある場合があります。

最も基本的な (そしてデフォルトの) レベルでは、設定は、ソース サイトで使用されているものと同じ TCP/IP ネットワーク設定を、宛先サイトの各 VM に対して単純に使用します。これには、ソース仮想ネットワークと宛先仮想ネットワークで同じ TCP/IP 設定を構成する必要があります。

このサービスは、VM の静的または動的ホスト構成プロトコル (DHCP) IP 構成のネットワーク設定をサポートします。 DHCP は、ホスト ネットワーク ポートの TCP/IP 設定を動的に構成する標準ベースの方法を提供します。 DHCP は、少なくとも TCP/IP アドレスを提供する必要があり、デフォルト ゲートウェイ アドレス (外部インターネット接続へのルーティング用)、サブネット マスク、および DNS サーバー アドレスも提供できます。 DHCP は、従業員のデスクトップ、ラップトップ、携帯電話の接続などのエンドユーザー コンピューティング デバイスによく使用されますが、サーバーなどのあらゆるネットワーク コンピューティング デバイスにも使用できます。

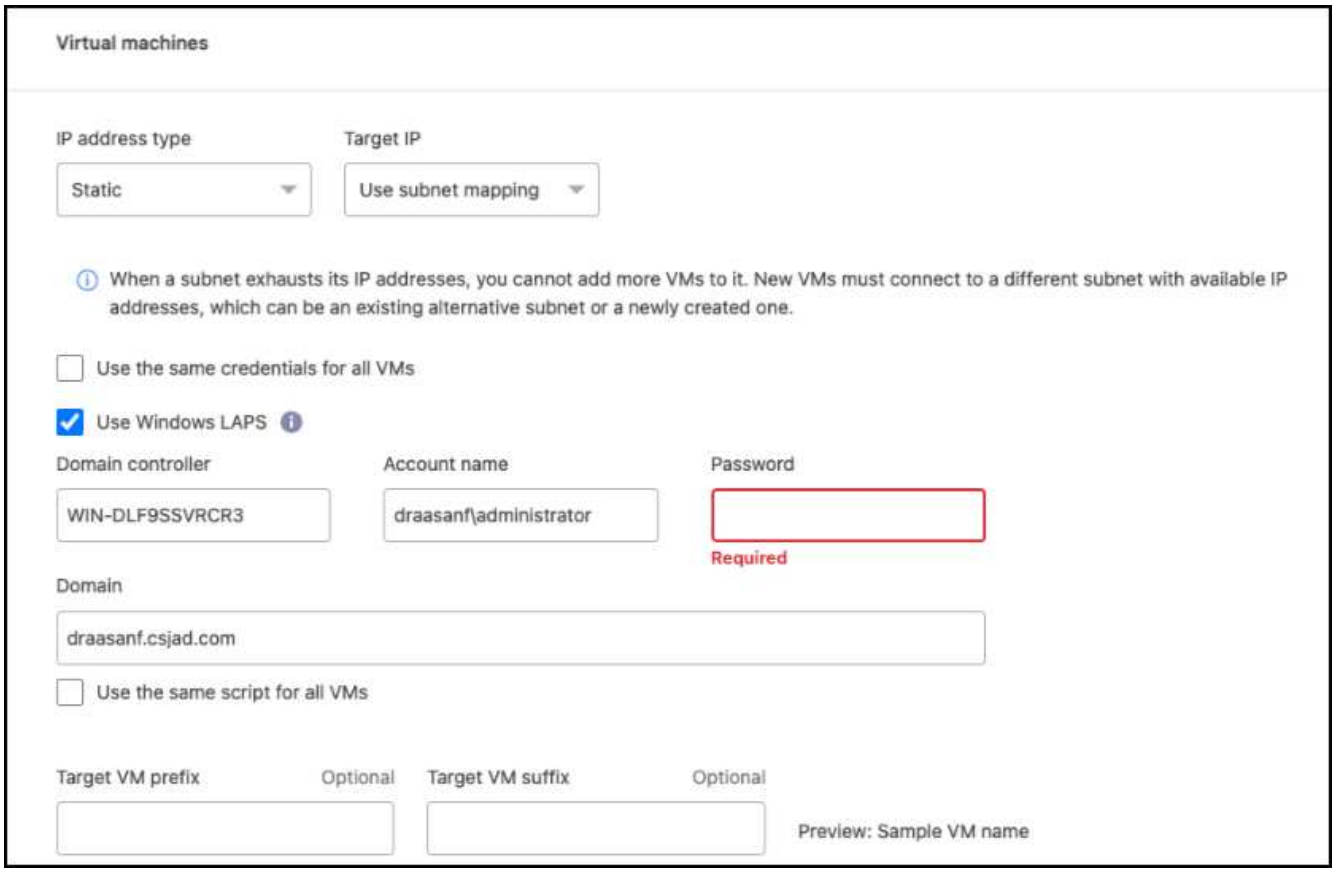
- 同じサブネット マスク、**DNS**、およびゲートウェイ設定を使用する オプション: これらの設定は通常、同じ仮想ネットワークに接続されているすべての VM で同じであるため、これらを一度構成して、レプリケーション プランによって保護されているリソース グループ内のすべての VM に対してディザスター リカバリーでその設定を使用する方が簡単な場合があります。一部の VM が異なる設定を使用する場合は、こ

のチェックボックスをオフにして、各 VM に対してそれらの設定を提供する必要があります。

- **IP** アドレスの種類: ターゲットの仮想ネットワークの要件に合わせて VM の構成を再構成します。NetApp Disaster Recovery には、DHCP または静的 IP の 2 つのオプションがあります。静的 IP の場合は、サブネット マスク、ゲートウェイ、および DNS サーバーを構成します。さらに、VM の資格情報を入力します。

  - **DHCP**: VM が DHCP サーバーからネットワーク構成情報を取得するようにする場合は、この設定を選択します。このオプションを選択した場合は、VM の資格情報のみを指定します。
  - 静的 **IP**: IP 構成情報を手動で指定する場合は、この設定を選択します。次のいずれかを選択できます: ソースと同じ、ソースと異なる、またはサブネット マッピング。ソースと同じものを選択した場合は、資格情報を入力する必要はありません。一方、ソースとは異なる情報を使用する場合は、資格情報、VM の IP アドレス、サブネット マスク、DNS、ゲートウェイ情報を提供できます。 VM ゲスト OS の資格情報は、グローバル レベルまたは各 VM レベルのいずれかに提供する必要があります。

    これは、大規模な環境を小規模なターゲット クラスターにリカバリする場合や、1 対 1 の物理 VMware インフラストラクチャをプロビジョニングせずに災害復旧テストを実施する場合に非常に役立ちます。



- スクリプト: .sh、.bat、または .ps1 形式のカスタム ゲスト OS ホスト スクリプトをポスト プロセスとして含めることができます。カスタム スクリプトを使用すると、 BlueXP disaster recoveryは、フェイルオーバー、フェイルバック、および移行プロセスの後にスクリプトを実行できます。たとえば、カスタム スクリプトを使用して、フェイルオーバーが完了した後にすべてのデータベース トランザクションを再開できます。このサービスは、Microsoft Windows またはコマンドライン パラメータがサポートされている任意の Linux バリアントを実行している VM 内でスクリプトを実行できます。スクリプトを個々の VM に割り当てることも、レプリケーション プラン内のすべての VM に割り当てることもできます。

  VM ゲスト OS でスクリプトの実行を有効にするには、次の条件を満たす必要があります。

- VM に VMware Tools がインストールされている必要があります。
- スクリプトを実行するには、適切なゲスト OS 権限を持つ適切なユーザー資格情報を提供する必要があります。
- 必要に応じて、スクリプトのタイムアウト値（秒単位）を含めます。

Microsoft Windows を実行している **VM**: Windows バッチ (.bat) または PowerShell (ps1) スクリプトのいずれかを実行できます。 Windows スクリプトではコマンドライン引数を使用できます。各引数をフォーマットする `arg_name$value`フォーマット、ここで `arg_name`は引数の名前であり、`$value`は引数の値であり、セミコロンで区切られます。 `argument$value`ペア。

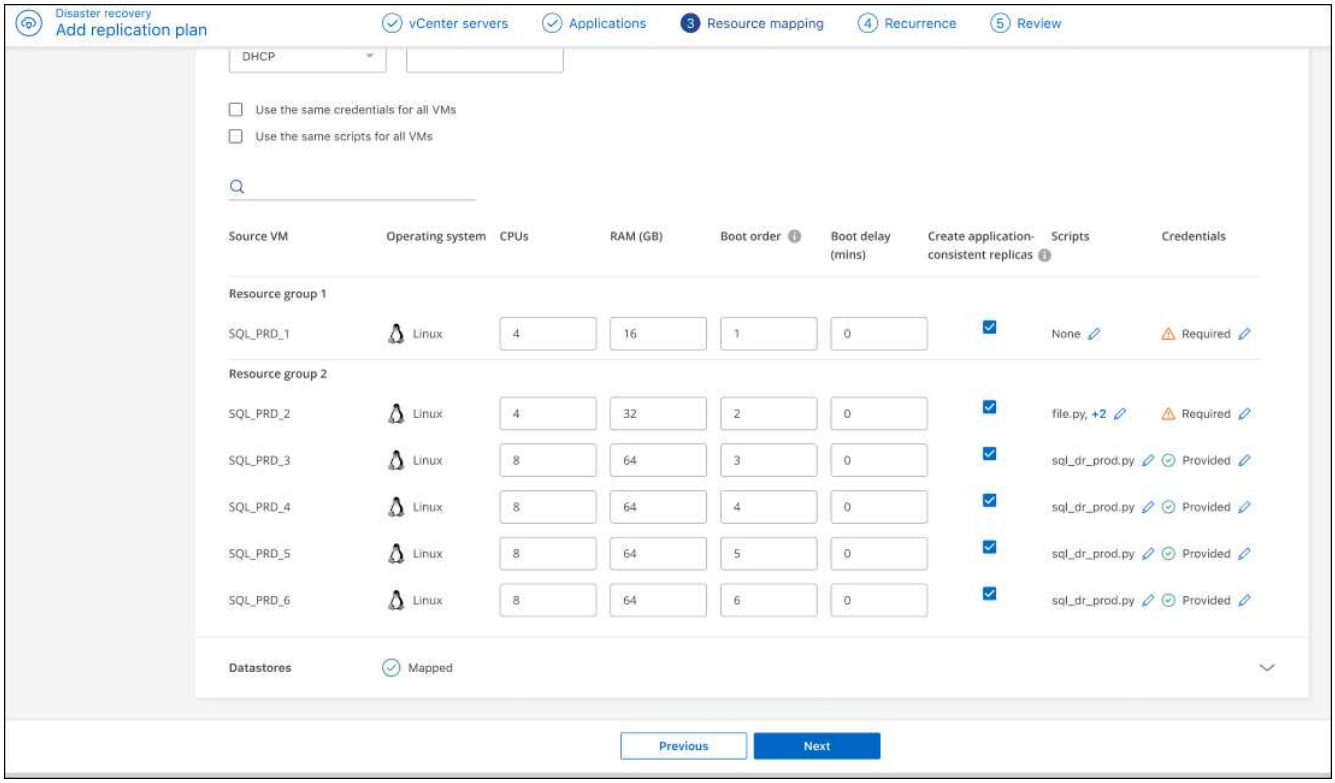
Linux を実行する **VM**: VM で使用される Linux バージョンでサポートされている任意のシェル スクリプト (.sh) を実行できます。 Linux スクリプトではコマンドライン引数を使用できます。セミコロンで区切られた値のリストで引数を指定します。名前付き引数はサポートされていません。各引数を `Arg[x]`引数リストとポインタを使用して各値を参照します。 `Arg[x]`配列、例えば、 `value1;value2;value3` 。

- ターゲット **VM** のプレフィックスとサフィックス: 仮想マシンの詳細で、フェールオーバーされた各 VM 名にプレフィックスとサフィックスをオプションで追加できます。これは、フェールオーバーされた VM と、同じ vCenter クラスター上で実行されている本番環境の VM を区別するのに役立ちます。たとえば、VM 名にプレフィックス「DR-」とサフィックス「-failover」を追加できます。災害発生時に別のサイトで一時的に VM をホストするために、2 番目の本番 vCenter を追加する人もいます。プレフィックスまたはサフィックスを追加すると、フェールオーバーされた VM をすばやく識別できるようになります。カスタム スクリプトでプレフィックスまたはサフィックスを使用することもできます。

  コンピューティング リソース セクションでターゲット VM フォルダーを設定する別の方法を使用することもできます。

- ソース **VM** の **CPU** と **RAM**: 仮想マシンの詳細で、必要に応じて VM の CPU と RAM のパラメータのサイズを変更できます。

> DRAM はギガバイト (GiB) またはメガバイト (MiB) で構成できます。各 VM に少なくとも 1 MiB の RAM が必要ですが、実際の量は VM ゲスト OS と実行中のアプリケーションが効率的に動作できるようにする必要があります。



- ブート順序: フェールオーバー後に、リソース グループ全体で選択したすべての仮想マシンのブート順序を変更できます。デフォルトでは、すべての VM が同時に並行して起動しますが、この段階で変更を加えることができます。これは、後続の優先度の VM が起動される前に、優先度 1 の VM がすべて実行されていることを確認するのに役立ちます。

  BlueXP disaster recoveryは、同じブート順序番号を持つすべての VM を並行してブートします。

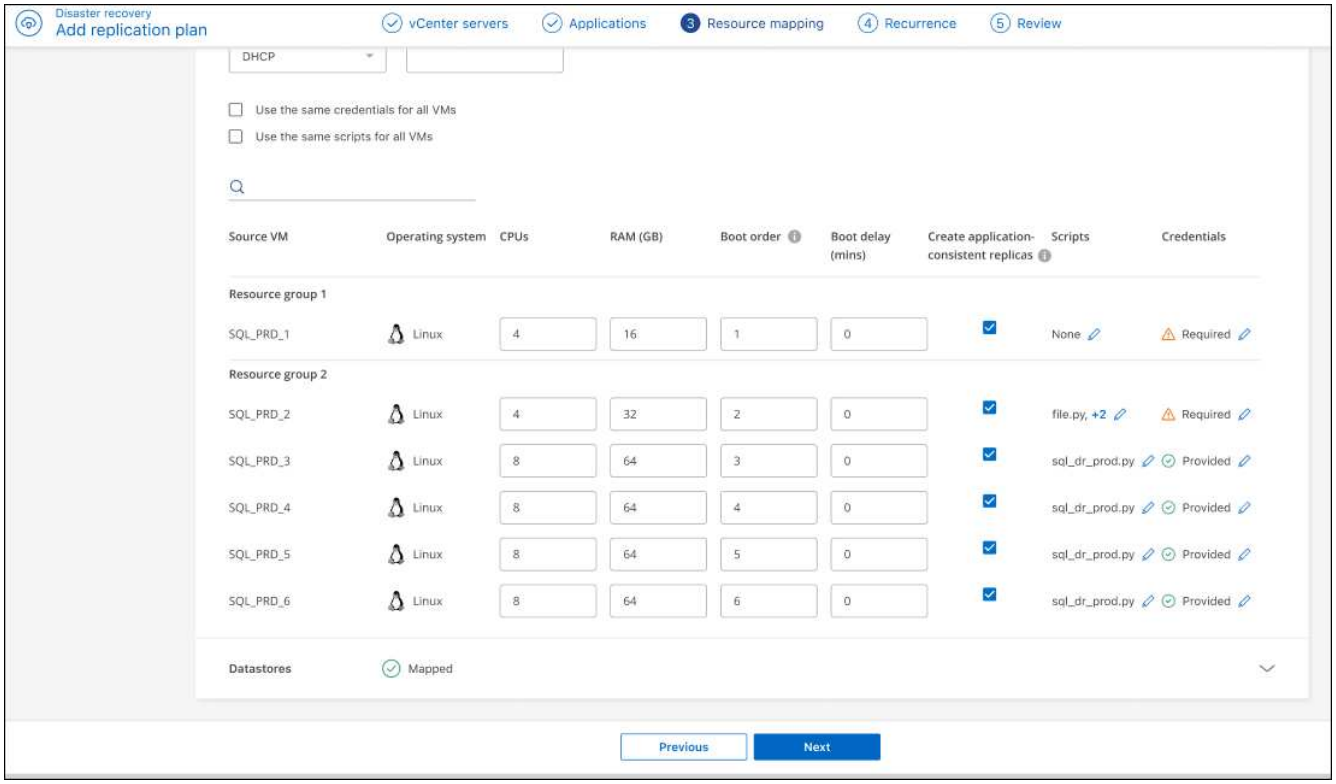
  - シーケンシャル ブート: 各 VM に一意の番号を割り当てて、割り当てられた順序 (例: 1、2、3、4、5) で VM を起動します。
  - 同時起動: 同時に起動するには、すべての VM に同じ番号を割り当てます (例: 1、1、1、1、2、2、3、4、4)。
- ブート遅延: ブートアクションの遅延を分単位で調整し、VM が電源オンプロセスを開始する前に待機する時間を示します。 0～10 分までの値を入力します。

起動順序をデフォルトにリセットするには、[**VM** 設定をデフォルトにリセット] を選択し、デフォルトに戻す設定を選択します。

- アプリケーション整合性のあるレプリカを作成する: アプリケーション整合性のあるスナップショット コピーを作成するかどうかを示します。サービスはアプリケーションを静止させ、スナップショットを取得してアプリケーションの一貫した状態を取得します。この機能は、Windows および Linux 上で実行されている Oracle と、Windows 上で実行されている SQL Server でサポートされています。次に詳細をご覧ください。
- **Windows LAPS** を使用する: Windows ローカル管理者パスワード ソリューション (Windows LAPS) を使用している場合は、このボックスをオンにします。このオプションは、「静的 IP」オプションを選択した場合にのみ使用できます。このボックスをチェックすると、仮想マシンごとにパスワードを入力する必要がなくなります。代わりに、ドメイン コントローラーの詳細を提供します。

  Windows LAPS を使用しない場合、VM は Windows VM であり、VM 行の資格情報オプションが有効にな

ります。 VM の資格情報を提供できます。



アプリケーション整合性のあるレプリカを作成する

多くの VM は、Oracle や Microsoft SQL Server などのデータベース サーバーをホストします。これらのデータベース サーバーでは、スナップショットが取得されたときにデータベースが一貫した状態であることを保証するために、アプリケーション整合性のあるスナップショットが必要です。

アプリケーション整合性スナップショットにより、スナップショットが取得されたときにデータベースが整合性のある状態であることが保証されます。これは、フェイルオーバーまたはフェイルバック操作後にデータベースを一貫した状態に復元できることを保証するため重要です。

データベース サーバーによって管理されるデータは、データベース サーバーをホストしている VM と同じデータストアでホストされる場合もあれば、別のデータストアでホストされる場合もあります。次の表は、ディザスタ リカバリにおけるアプリケーション整合性スナップショットでサポートされている構成を示しています。

データの場所	サポート	注記
VMと同じvCenterデータストア内	はい	データベース サーバーとデータベースは両方とも同じデータストアに存在するため、フェイルオーバー時にはサーバーとデータの両方が同期されます。

データの場所	サポート	注記
VMとは異なるvCenterデータストア内	いいえ	ディザスタ リカバリでは、データベース サーバーのデータが異なる vCenter データストアにあるかどうかを識別できません。このサービスではデータを複製することはできませんが、データベース サーバー VM を複製することはできます。 データベース データは複製できませんが、このサービスにより、VM バックアップ時にデータベースが停止していることを確認するために必要なすべての手順がデータベース サーバーで実行されるようになります。
外部データソース内	いいえ	データがゲストマウントされた LUN または NFS 共有に存在する場合、Disaster Recovery はデータを複製できませんが、データベース サーバー VM を複製できます。 データベース データは複製できませんが、このサービスにより、VM バックアップ時にデータベースが停止していることを確認するために必要なすべての手順がデータベース サーバーで実行されるようになります。

スケジュールされたバックアップ中に、Disaster Recovery はデータベース サーバーを静止させ、データベース サーバーをホストしている VM のスナップショットを取得します。これにより、スナップショットが取得されたときにデータベースが一貫した状態になることが保証されます。

- Windows VM の場合、サービスは Microsoft ボリューム シャドウ コピー サービス (VSS) を使用していずれかのデータベース サーバーと調整します。
- Linux VM の場合、サービスは一連のスクリプトを使用して Oracle サーバーをバックアップ モードにします。

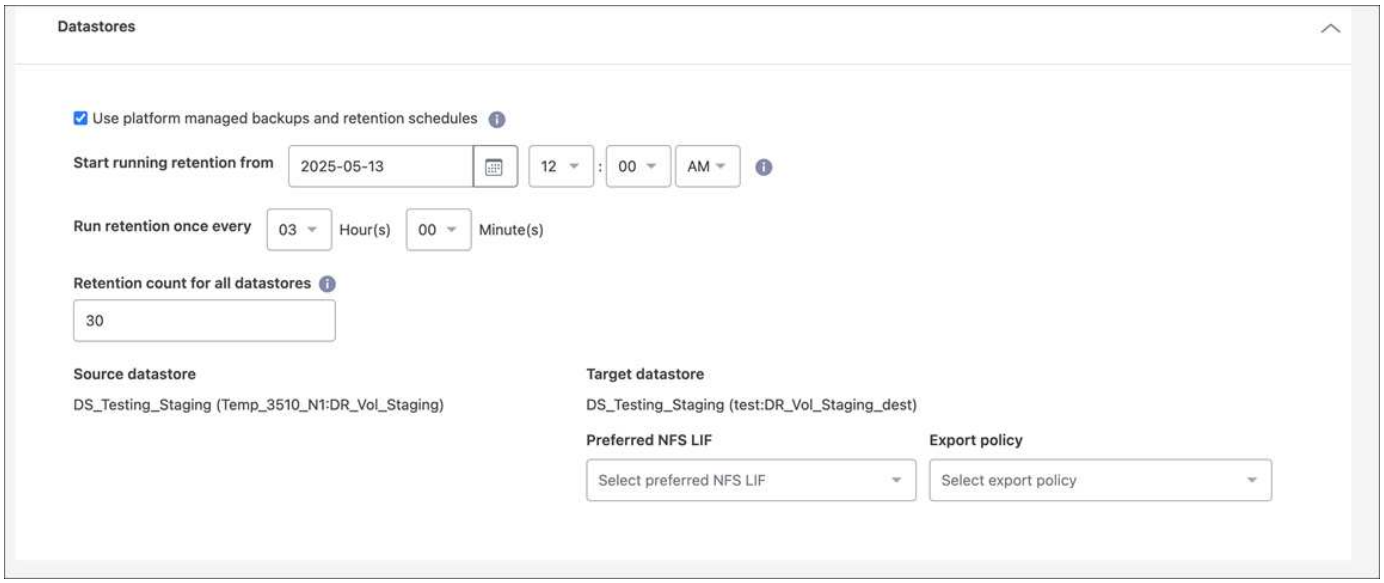
VM とそのホスティング データストアのアプリケーション整合性レプリカを有効にするには、各 VM の [アプリケーション整合性レプリカを作成する] の横にあるチェックボックスをオンにし、適切な権限を持つゲスト ログイン資格情報を提供します。

マップリソース > データストアセクション

VMware データストアは、 ONTAP FlexVolボリューム、または VMware VMFS を使用するONTAP iSCSI または FC LUN 上でホストされます。データストア セクションを使用して、ディスク上のデータを宛先に複製するためのターゲットONTAPクラスタ、ストレージ仮想マシン (SVM)、およびボリュームまたは LUN を定義します。

*データストア*の横にある下矢印を選択します。VM の選択に基づいて、データストア マッピングが自動的に選択されます。

このセクションは、選択内容に応じて有効または無効になります。



- プラットフォーム管理のバックアップと保持スケジュールを使用する: 外部のスナップショット管理ソリューションを使用している場合は、このチェックボックスをオンにします。 NetApp Disaster Recoveryは、ネイティブのONTAP SnapMirrorポリシー スケジューラやサードパーティ統合などの外部スナップショット管理ソリューションの使用をサポートしています。レプリケーション プラン内のすべてのデータストア (ボリューム) に、別の場所で管理されているSnapMirror関係がすでに存在する場合は、それらのスナップショットをNetApp Disaster Recoveryのリカバリ ポイントとして使用できます。

  このオプションを選択すると、 NetApp Disaster Recovery はバックアップ スケジュールを構成しません。ただし、テスト、フェイルオーバー、フェイルバック操作のためにスナップショットが作成される可能性があるため、保持スケジュールを構成する必要があります。

  これが構成されると、サービスは定期的にスケジュールされたスナップショットを取得せず、代わりに外部エンティティに依存してスナップショットを取得および更新します。

- 開始時刻: バックアップと保持の実行を開始する日時を入力します。
- 実行間隔: 時間間隔を時間と分で入力します。たとえば、1 時間を入力すると、サービスは 1 時間ごとにスナップショットを作成します。
- 保持数: 保持するスナップショットの数を入力します。

  保持されるスナップショットの数と各スナップショット間のデータ変更率によって、ソースと宛先の両方で消費されるストレージ容量が決まります。保持するスナップショットの数が増えるほど、消費されるストレージ容量も増えます。

- ソースおよびターゲット データストア: 複数の (ファンアウト) SnapMirror関係が存在する場合は、使用する宛先を選択できます。ボリュームにSnapMirror関係がすでに確立されている場合は、対応するソース データストアとターゲット データストアが表示されます。ボリュームにSnapMirror関係がない場合は、ターゲット クラスタを選択し、ターゲット SVM を選択して、ボリューム名を指定することで、今すぐ SnapMirror 関係を作成できます。サービスはボリュームとSnapMirror の関係を作成します。

  このサービスでSnapMirror関係を作成する場合は、クラスタとその SVM ピアリングがNetApp Disaster Recoveryの外部ですでに設定されている必要があります。

  - VM が同じボリュームと同じ SVM からのものである場合、サービスは標準のONTAPスナップショットを実行し、セカンダリ デスティネーションを更新します。

- VM が異なるボリュームと同じ SVM からのものである場合、サービスはすべてのボリュームを含めて整合性グループのスナップショットを作成し、セカンダリ デスティネーションを更新します。
- VM が異なるボリュームおよび異なる SVM からのものである場合、サービスは同じまたは異なるクラスター内のすべてのボリュームを含めて、整合性グループ開始フェーズおよびコミット フェーズのスナップショットを実行し、セカンダリ デスティネーションを更新します。
- フェイルオーバー中は、任意のスナップショットを選択できます。最新のスナップショットを選択した場合、サービスはオンデマンド バックアップを作成し、宛先を更新し、そのスナップショットをフェールオーバーに使用します。

- 優先 **NFS LIF** と エクスポート ポリシー: 通常、サービスによって優先 NFS LIF とエクスポート ポリシーが選択されます。特定の NFS LIF またはエクスポート ポリシーを使用する場合は、各フィールドの横にある下矢印を選択し、適切なオプションを選択します。

  オプションで、フェイルオーバー イベント後にボリュームの特定のデータ インターフェイス (LIF) を使用することもできます。これは、ターゲット SVM に複数の LIF がある場合に、データ トラフィックのバランスをとるのに役立ちます。

  NAS データ アクセス セキュリティをさらに制御するために、このサービスでは、異なるデータストア ボリュームに固有の NAS エクスポート ポリシーを割り当てることができます。エクスポート ポリシーは、データストア ボリュームにアクセスする NFS クライアントのアクセス制御ルールを定義します。エクスポート ポリシーを指定しない場合、サービスは SVM のデフォルトのエクスポート ポリシーを使用します。

ベスト プラクティス: 保護された VM をホストするソースとターゲットの vCenter ESXi ホストのみにボリューム アクセスを制限する専用のエクスポート ポリシーを作成することを強くお勧めします。これにより、外部エンティティが NFS エクスポートにアクセスできないようになります。

テストフェイルオーバーマッピングを追加する

手順

1. テスト環境に異なるマッピングを設定するには、ボックスのチェックを外して、[テスト マッピング] タブを選択します。
2. 前と同じように各タブを確認しますが、今回はテスト環境です。

   テスト マッピング タブでは、仮想マシンとデータストアのマッピングが無効になっています。

   後で計画全体をテストできます。現在、テスト環境のマッピングを設定しています。

レプリケーション計画を確認する

最後に、少し時間を取ってレプリケーション プランを確認します。

後でレプリケーション プランを無効にしたり削除したりできます。

手順

1. 各タブ（プランの詳細、フェールオーバー マッピング、VM）の情報を確認します。
2. *プランを追加*を選択します。

   プランがプランのリストに追加されます。

コンプライアンスをテストし、フェイルオーバー テストが機能することを確認するためにスケジュールを編集します

コンプライアンス テストとフェールオーバー テストをテストするスケジュールを設定して、必要に応じて正しく機能することを確認できるようにすることをお勧めします。

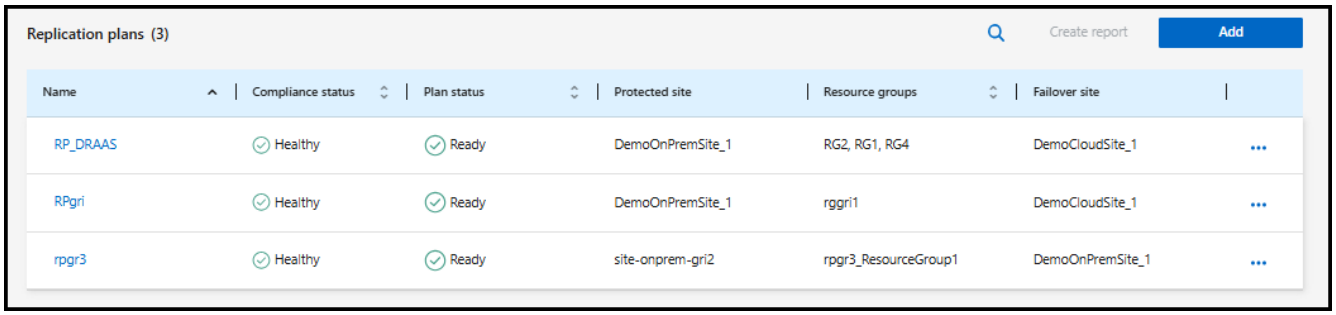
- コンプライアンス時間の影響: レプリケーション プランが作成されると、サービスはデフォルトでコンプライアンス スケジュールを作成します。デフォルトのコンプライアンス時間は 30 分です。この時間を変更するには、レプリケーション プランのスケジュールを編集します。
- フェールオーバーの影響をテスト: フェールオーバー プロセスをオンデマンドまたはスケジュールに従ってテストできます。これにより、レプリケーション プランで指定された宛先への仮想マシンのフェールオーバーをテストできます。

  テスト フェイルオーバーでは、 FlexCloneボリュームが作成され、データストアがマウントされ、そのデータストア上のワークロードが移動されます。テスト フェイルオーバー操作は、実稼働ワークロード、テスト サイトで使用されるSnapMirror関係、および正常に動作し続ける必要がある保護されたワークロードには影響しません。

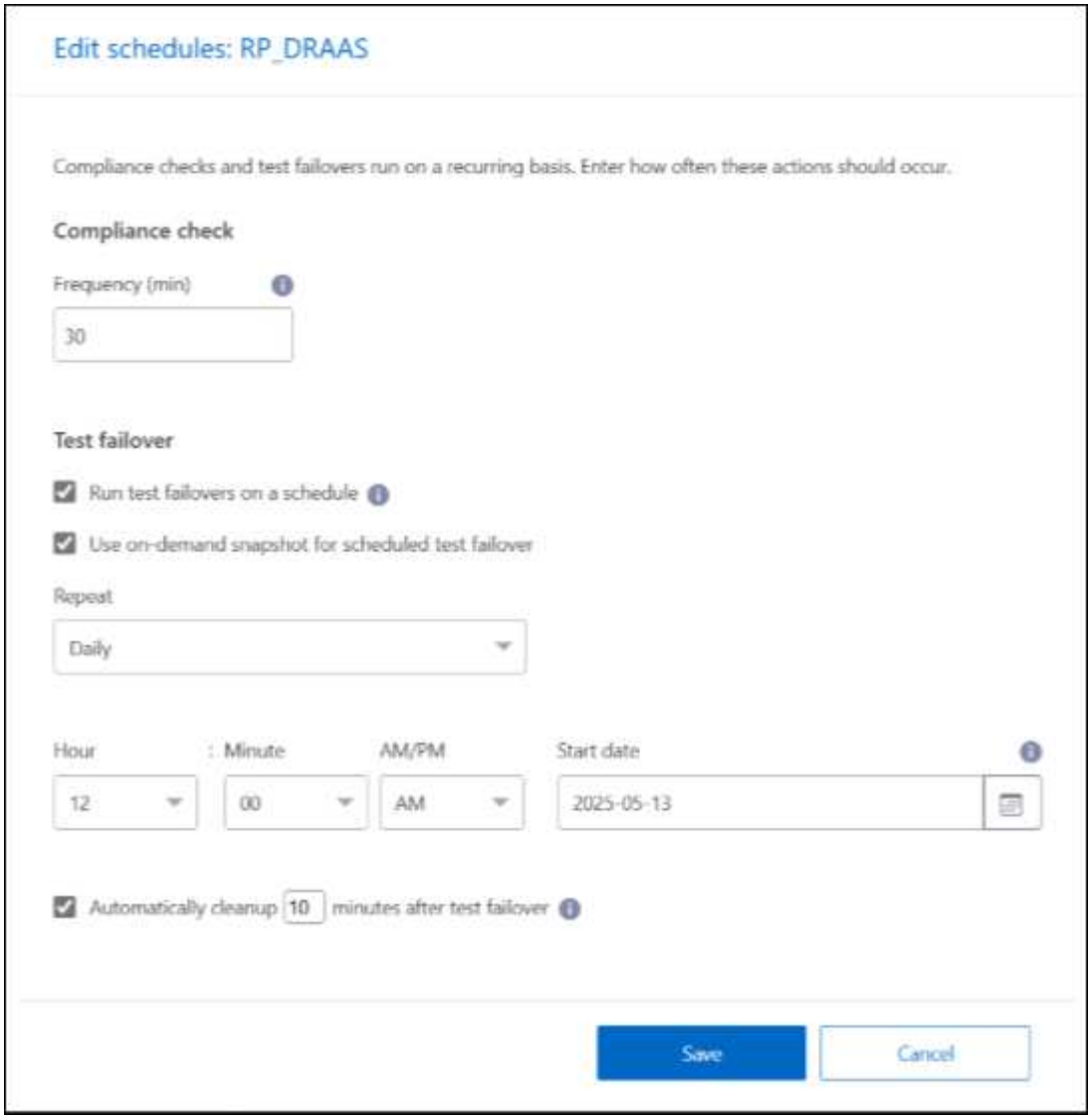
スケジュールに基づいてフェイルオーバー テストが実行され、ワークロードがレプリケーション プランで指定された宛先に移動されていることが確認されます。

手順

1. NetApp Disaster Recoveryメニューから、レプリケーション プラン を選択します。



2. *アクション*を選択します ••• アイコンをクリックし、[スケジュールの編集] を選択します。
3. NetApp Disaster Recovery でテストのコンプライアンスをチェックする頻度を分単位で入力します。
4. フェールオーバー テストが正常に動作していることを確認するには、[フェールオーバーを毎月実行する] をオンにします。
   a. これらのテストを実行する月日と時刻を選択します。
   b. テストを開始する日付を yyyy-mm-dd 形式で入力します。



5. スケジュールされたテスト フェイルオーバーにオンデマンド スナップショットを使用する: 自動テスト フェイルオーバーを開始する前に新しいスナップショットを取得するには、このボックスをオンにします。
6. フェールオーバー テストが終了した後にテスト環境をクリーンアップするには、[テスト フェールオーバー後に自動的にクリーンアップする] をオンにし、クリーンアップを開始する前に待機する分数を入力します。

> このプロセスでは、テスト場所から一時 VM を登録解除し、作成されたFlexCloneボリュームを削除し、一時データストアをマウント解除します。

7. *保存*を選択します。

NetApp Disaster Recoveryでアプリケーションを別のサイトに複製する

NetApp Disaster Recoveryを使用すると、 SnapMirrorレプリケーションを使用して、ソース サイトの VMware アプリケーションをクラウド内の災害復旧リモート サイトに複

製できます。

> 災害復旧計画を作成し、ウィザードで繰り返しを識別し、災害復旧サイトへのレプリケーションを開始すると、 NetApp Disaster Recovery は30 分ごとに、レプリケーションが計画に従って実際に実行されているかどうかを確認します。ジョブ モニター ページで進行状況を監視できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、またはディザスタ リカバリ フェールオーバー管理者のロール。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

開始する前に

レプリケーションを開始する前に、レプリケーション プランを作成し、アプリをレプリケートすることを選択する必要があります。次に、[アクション] メニューに [複製] オプションが表示されます。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。
3. メニューから*レプリケーション プラン*を選択します。
4. レプリケーション プランを選択します。
5. 右側で*アクション*オプションを選択します ••• *複製*を選択します。

NetApp Disaster Recoveryを使用してアプリケーションを別のサイトに移行する

NetApp Disaster Recoveryを使用すると、ソース サイトの VMware アプリケーションを別のサイトに移行できます。

> レプリケーション プランを作成し、ウィザードで繰り返しを指定して移行を開始すると、NetApp Disaster Recovery は30 分ごとに移行がプランに従って実際に行われているかどうかを確認します。ジョブ モニター ページで進行状況を監視できます。

開始する前に

移行を開始する前に、レプリケーション プランを作成し、アプリの移行を選択する必要があります。次に、[アクション] メニューに [移行] オプションが表示されます。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。
3. メニューから*レプリケーション プラン*を選択します。
4. レプリケーション プランを選択します。

5. 右側で*アクション*オプションを選択します ••• *移行*を選択します。

NetApp Disaster Recoveryでアプリケーションをリモート サイトにフェイルオーバーする

災害が発生した場合は、プライマリのオンプレミス VMware サイトを別のオンプレミスの VMware サイトまたは VMware Cloud on AWS にフェイルオーバーします。フェールオーバー プロセスをテストして、必要なときに成功することを確認できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、またはディザスタ リカバリ フェールオーバー管理者のロール。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

このタスクについて

フェイルオーバー中、ディザスタ リカバリでは最新のSnapMirrorスナップショット コピーが使用されます。または、ポイントインタイム スナップショットから特定のスナップショットを選択することもできます (SnapMirrorの保持ポリシーに従って)。

ランサムウェア攻撃時など、最新のレプリカが侵害された場合は、ポイントインタイム オプションを使用します。 BlueXP disaster recoveryでは、利用可能なすべての時点が表示されます。

このプロセスは、運用サイトが正常かどうか、および重要なインフラストラクチャの障害以外の理由で災害復旧サイトへのフェイルオーバーを実行しているかどうかによって異なります。

- ソース vCenter またはONTAPクラスタにアクセスできない重大な本番サイトの障害: NetApp Disaster Recovery を使用すると、復元する利用可能なスナップショットを自由に選択できます。
- 運用環境は正常です: 「今すぐスナップショットを作成する」か、以前に作成したスナップショットを選択できます。

この手順では、レプリケーション関係を解除し、vCenter ソース VM をオフラインにして、ボリュームをディザスタ リカバリ vCenter のデータストアとして登録し、プランのフェールオーバー ルールを使用して保護された VM を再起動し、ターゲット サイトで読み取り/書き込みを有効にします。

フェイルオーバープロセスをテストする

フェイルオーバーを開始する前に、プロセスをテストできます。テストでは仮想マシンはオフラインになりません。

フェイルオーバー テスト中に、 BlueXP disaster recoveryによって一時的に仮想マシンが作成されます。 BlueXP disaster recoveryは、 FlexCloneボリュームをバックアップする一時データストアを ESXi ホストにマップします。

このプロセスでは、オンプレミスのONTAPストレージまたは AWS の FSx for NetApp ONTAPストレージの追加の物理容量は消費されません。元のソース ボリュームは変更されず、災害復旧中でもレプリカ ジョブを続行できます。

テストが終了したら、テストのクリーンアップ オプションを使用して仮想マシンをリセットする必要があります。これは推奨されますが、必須ではありません。

テスト フェイルオーバー操作は、実稼働ワークロード、テスト サイトで使用されるSnapMirror関係、および正常に動作し続ける必要がある保護されたワークロードには影響しません。

テスト フェイルオーバーの場合、Disaster Recovery は次の操作を実行します。

- 宛先クラスタとSnapMirror関係の事前チェックを実行します。
- ターゲット サイトのONTAPクラスタ上の保護された各ONTAPボリュームに対して、選択したスナップショットから新しいFlexCloneボリュームを作成します。
- データストアが VMFS である場合は、iGroup を作成して各 LUN にマップします。
- ターゲット仮想マシンを vCenter 内に新しいデータストアとして登録します。
- リソース グループ ページでキャプチャされたブート順序に基づいて、ターゲット仮想マシンの電源をオンにします。
- 「アプリケーション整合性」と示されている VM 内のサポートされているデータベース アプリケーションを静止解除します。
- ソース vCenter およびONTAPクラスタがまだアクティブな場合は、逆方向のSnapMirror関係を作成し、フェイルオーバー状態中に行われた変更を元のソース サイトに複製します。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。
3. NetApp Disaster Recoveryメニューから、レプリケーション プラン を選択します。
4. レプリケーション プランを選択します。
5. 右側で*アクション*オプションを選択します •••*フェイルオーバーのテスト*を選択します。
6. テスト フェイルオーバー ページで、「テスト フェイルオーバー」と入力し、テスト フェイルオーバーを選択します。
7. テストが完了したら、テスト環境をクリーンアップします。

フェイルオーバーテスト後にテスト環境をクリーンアップする

フェイルオーバー テストが終了したら、テスト環境をクリーンアップする必要があります。このプロセスでは、テスト場所、FlexClone、および一時データストアから一時 VM が削除されます。

手順

1. NetApp Disaster Recoveryメニューから、レプリケーション プラン を選択します。
2. レプリケーション プランを選択します。
3. 右側で*アクション*オプションを選択します •••*フェールオーバー テストのクリーンアップ*を選択します。
4. [テスト フェールオーバー] ページで、「フェールオーバーのクリーンアップ」と入力し、[フェールオーバー テストのクリーンアップ] を選択します。

ソースサイトを災害復旧サイトにフェイルオーバーする

災害が発生した場合、FSx for NetApp ONTAPを使用して、プライマリオンプレミス VMware サイトを別のオンプレミス VMware サイトまたは VMware Cloud on AWS にオンデマンドでフェイルオーバーします。

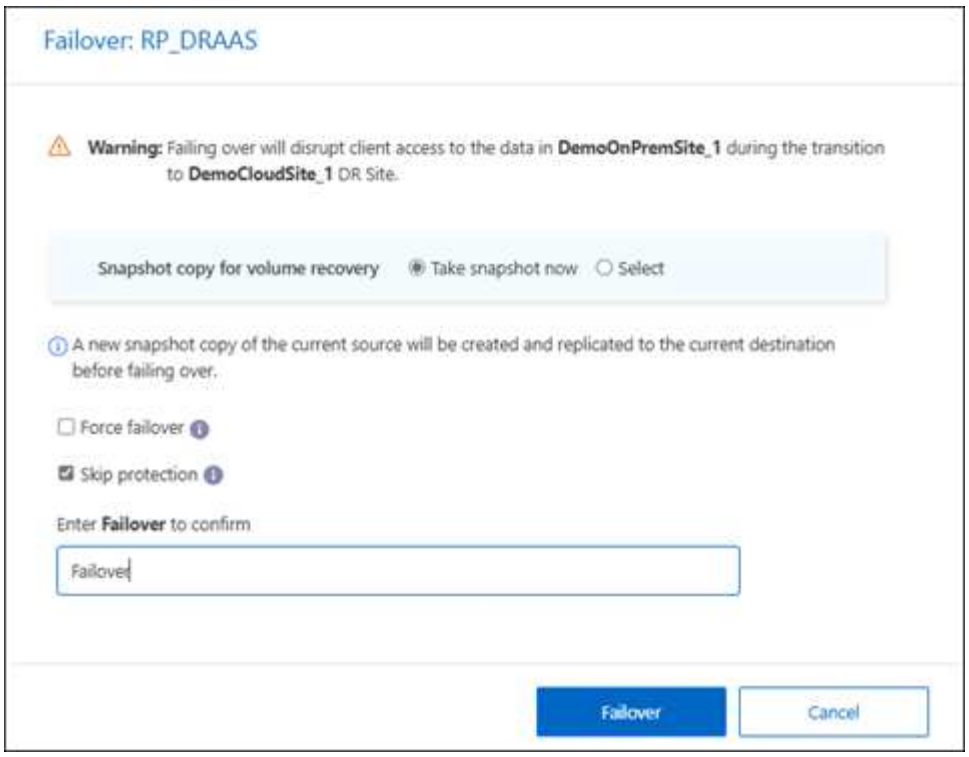
フェイルオーバー プロセスには次の操作が含まれます。

- ディザスタ リカバリでは、宛先クラスタとSnapMirror関係の事前チェックを実行します。
- 最新のスナップショットを選択した場合は、最新の変更を複製するためにSnapMirror更新が実行されます。
- ソース仮想マシンの電源がオフになっています。
- SnapMirror関係が解除され、ターゲット ボリュームが読み取り/書き込み可能になります。
- スナップショットの選択に基づいて、アクティブなファイル システムが指定されたスナップショット (最新または選択されたもの) に復元されます。
- レプリケーション プランでキャプチャされた情報に基づいて、データストアが作成され、VMware または VMC クラスターまたはホストにマウントされます。データストアが VMFS である場合は、iGroup を作成して各 LUN にマップします。
- ターゲット仮想マシンは、vCenter 内に新しいデータストアとして登録されます。
- ターゲット仮想マシンは、リソース グループ ページでキャプチャされたブート順序に基づいて電源がオンになります。
- ソース vCenter がまだアクティブな場合は、フェールオーバーされているすべてのソース側 VM の電源をオフにします。
- 「アプリケーション整合性」と示されている VM 内のサポートされているデータベース アプリケーションを静止解除します。
- ソース vCenter およびONTAPクラスタがまだアクティブな場合は、逆方向のSnapMirror関係を作成し、フェイルオーバー状態中に行われた変更を元のソース サイトに複製します。 SnapMirror関係はターゲット仮想マシンからソース仮想マシンに逆転されます。

フェイルオーバーが開始すると、災害復旧サイトの vCenter で復旧した VM (仮想マシン、ネットワーク、データストア) を確認できます。デフォルトでは、仮想マシンはワークロード フォルダーに回復されます。

手順

1. NetApp Disaster Recoveryメニューから、レプリケーション プラン を選択します。
2. レプリケーション プランを選択します。
3. 右側で*アクション*オプションを選択します ••• *フェイルオーバー*を選択します。



4. フェールオーバー ページで、今すぐスナップショットを開始するか、回復するデータストアのスナップショットを選択します。デフォルトは最新です。

   フェイルオーバーが発生する前に、現在のソースのスナップショットが作成され、現在の宛先に複製されます。

5. 通常はフェイルオーバーの発生を妨げるエラーが検出された場合でもフェイルオーバーを発生させる場合は、必要に応じて「強制フェイルオーバー」を選択します。
6. オプションで、レプリケーション プランのフェイルオーバー後にサービスによってリバースSnapMirror保護関係が自動的に作成されないようにするには、[保護をスキップ] を選択します。これは、NetApp Disaster Recovery内でサイトをオンラインに戻す前に、復元されたサイトで追加の操作を実行する場合に役立ちます。

   レプリケーション プランの [アクション] メニューから [リソースの保護] を選択すると、逆保護を確立できます。これにより、プラン内の各ボリュームに対して逆方向のレプリケーション関係を作成しようとします。保護が復元されるまで、このジョブを繰り返し実行できます。保護が復元されると、通常の方法でフェイルバックを開始できます。

7. ボックスに「failover」と入力します。
8. *フェイルオーバー*を選択します。
9. 進行状況を確認するには、メニューで*ジョブ監視*を選択します。

NetApp Disaster Recoveryでアプリケーションを元のソースにフェイルバック

災害が解決したら、災害復旧サイトからソース サイトにフェールバックして通常の運用に戻ります。復元するスナップショットを選択できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、またはディザスタ リカバリ フェールオーバー管理者のロール。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

このタスクについて

このワークフローでは、 NetApp Disaster Recovery は、レプリケーションの方向を反転する前に、すべての変更を元のソース仮想マシンにレプリケート (再同期) します。このプロセスは、ターゲットへのフェールオーバーが完了した関係から開始され、次の手順が含まれます。

- 回復したサイトでコンプライアンス チェックを実行します。
- 回復されたサイトにあると特定された各 vCenter クラスタの vCenter 情報を更新します。
- ターゲット サイトで、仮想マシンの電源をオフにして登録を解除し、ボリュームをマウント解除します。
- 元のソースのSnapMirror関係を解除して、読み取り/書き込み可能にします。
- レプリケーションを元に戻すには、 SnapMirror関係を再同期します。
- ソース仮想マシンの電源をオンにして登録し、ソースにボリュームをマウントします。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。
3. NetApp Disaster Recoveryメニューから、レプリケーション プラン を選択します。
4. レプリケーション プランを選択します。
5. 右側で*アクション*オプションを選択します •••*フェイルバック*を選択します。
6. レプリケーション プラン名を入力して確認し、フェイルバックを開始します。
7. 復元するデータストアのスナップショットを選択します。デフォルトは最新です。
8. 進行状況を確認するには、メニューで*ジョブ監視*を選択します。

NetApp Disaster Recoveryを使用して、サイト、リソース グループ、レプリケーション プラン、データストア、仮想マシンの情報を管理します。

NetApp Disaster Recoveryリソースのすべてをざっと確認したり、それぞれの詳細を確認したりできます。

- サイト
- リソース グループ
- レプリケーションプラン
- データストア

- 仮想マシン

タスクには異なるNetApp Consoleロールが必要です。詳細については、各タスクの 必要な**NetApp Console**ロール セクションを参照してください。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

vCenter サイトの管理

vCenter サイト名とサイト タイプ (オンプレミスまたは AWS) を編集できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、またはディザスタ リカバリ管理者のロール。

手順

1. メニューから*サイト*を選択します。
2. アクション*オプションを選択します  **vCenter** 名の右側にある **[*編集]** を選択します。
3. vCenter サイトの名前と場所を編集します。

リソース グループの管理

レプリケーション プランの作成の一環としてリソース グループを追加することもできますが、グループを個別に追加し、後でそのグループをプラン内で使用する方が便利な場合があります。リソース グループは、VM またはデータストアごとに作成します。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、またはディザスタ リカバリ アプリケーション管理者のロール。

次の方法で、データストアごとにリソース グループを作成できます。

- データストアを使用してリソース グループを追加する場合は、データストアの一覧を表示できます。 1 つ以上のデータストアを選択してリソース グループを作成できます。
- レプリケーション プランを作成し、プラン内にリソース グループを作成すると、データストア内の VM を確認できます。

リソース グループでは次のタスクを実行できます。

- リソース グループ名を変更します。
- リソース グループに VM を追加します。
- リソース グループから VM を削除します。
- リソース グループを削除します。

リソースグループの作成の詳細については、"VMをまとめて整理するためのリソースグループを作成する" 。

手順

1. メニューから*リソース グループ*を選択します。
2. リソース グループを追加するには、[グループの追加] を選択します。
3. リソースグループでアクションを実行するには、[アクション] オプションを選択します。 ••• 右側にあるリソース グループの編集 や リソース グループの削除 などのオプションのいずれかを選択します。

レプリケーションプランの管理

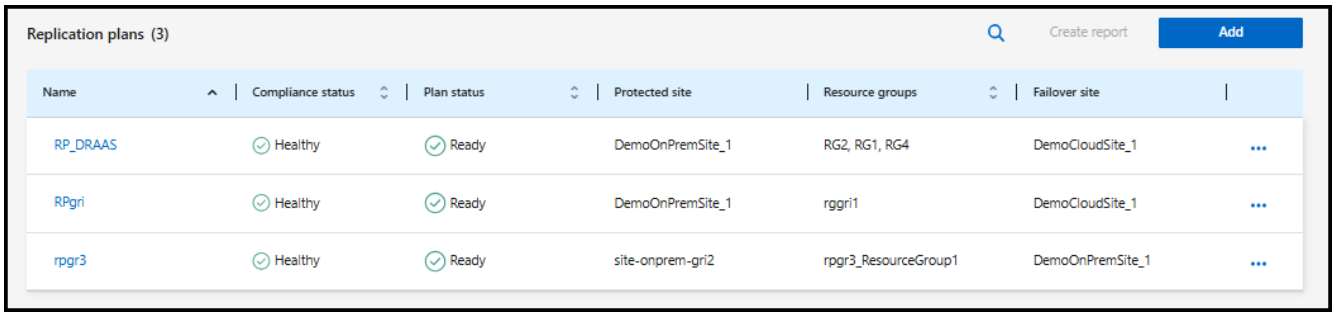
レプリケーション プランを無効化、有効化、および削除できます。スケジュールは変更できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ フェールオーバー管理者、またはディザスタ リカバリ アプリケーション管理者のロール。

- レプリケーション プランを一時的に一時停止する場合は、無効にして後で有効にすることができます。
- プランが不要になった場合は削除できます。

手順

1. メニューから*レプリケーション プラン*を選択します。



2. プランの詳細を表示するには、「アクション」オプションを選択します ••• *プランの詳細を表示*を選択します。
3. 次のいずれかを実行します。
   - プランの詳細を編集する（繰り返しを変更する）には、[プランの詳細] タブを選択し、右側の [編集] アイコンを選択します。
   - リソース マッピングを編集するには、[フェールオーバー マッピング] タブを選択し、[編集] アイコンを選択します。
   - 仮想マシンを追加または編集するには、[仮想マシン] タブを選択し、[**VM** の追加] オプションまたは [編集] アイコンを選択します。
4. 左側のパンくずリストから「レプリケーション プラン」を選択して、プランのリストに戻ります。
5. プランでアクションを実行するには、レプリケーションプランのリストから*アクション*オプションを選択します。 ••• プランの右側にある をクリックし、スケジュールの編集、フェイルオーバーのテスト、フェイルオーバー、フェイルバック、移行、今すぐスナップショットを作成、古いスナップショットのクリーンアップ、無効化、有効化、削除 などのオプションのいずれかを選択します。
6. テストフェイルオーバースケジュールを設定または変更したり、コンプライアンス頻度チェックを設定するには、[アクション] オプションを選択します。 ••• プランの右側にある [スケジュールの編集] を選択します。

a. [スケジュールの編集] ページで、フェールオーバー コンプライアンス チェックを実行する頻度を分単位で入力します。

b. *スケジュールに従ってテストフェイルオーバーを実行する*をチェックします。

c. 「繰り返し」オプションで、毎日、毎週、または毎月のスケジュールを選択します。

d. *保存*を選択します。

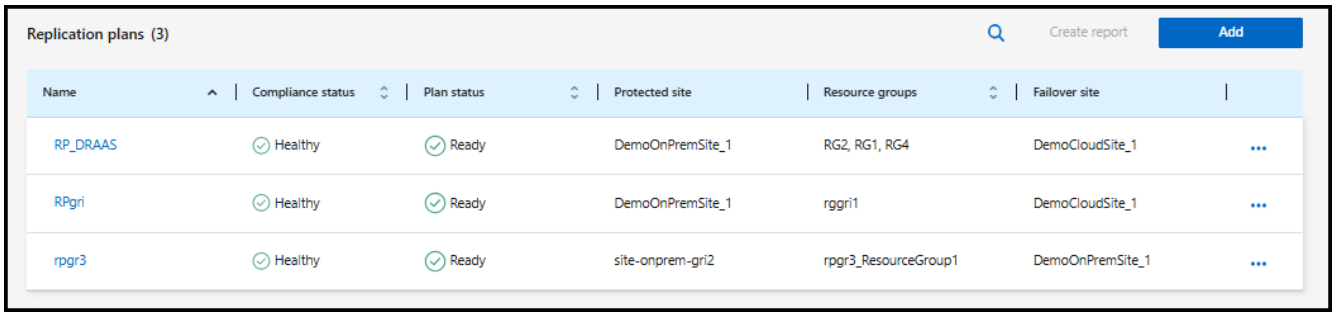
オンデマンドでスナップショットを調整する

ソースとターゲット間で同期されていないスナップショットを調整できます。これは、NetApp Disaster Recoveryの外部のターゲットでスナップショットが削除された場合に発生する可能性があります。サービスは、ソース上のスナップショットを 24 時間ごとに自動的に削除します。ただし、これをオンデマンドで実行できます。この機能により、すべてのサイト間でスナップショットの一貫性を確保できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ フェールオーバー管理者、またはディザスタ リカバリ アプリケーション管理者のロール。

手順

1. メニューから*レプリケーション プラン*を選択します。



2. レプリケーションプランのリストから*アクション*オプションを選択します ••• プランの右側にある [スナップショットの調整] を選択します。

3. 調整情報を確認します。

4. *調整*を選択します。

レプリケーションプランを削除する

不要になったレプリケーション プランは削除できます。レプリケーション プランを削除すると、そのプランによって作成されたプライマリ スナップショットとセカンダリ スナップショットも削除できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ フェールオーバー管理者、またはディザスタ リカバリ アプリケーション管理者のロール。

手順

1. メニューから*レプリケーション プラン*を選択します。

2. アクション*オプションを選択します ••• プランの右側にある [*削除] を選択します。

3. プライマリ スナップショット、セカンダリ スナップショット、またはプランによって作成されたメタデータのみを削除するかどうかを選択します。

4. 削除を確認するには「delete」と入力します。
5. *削除*を選択します。

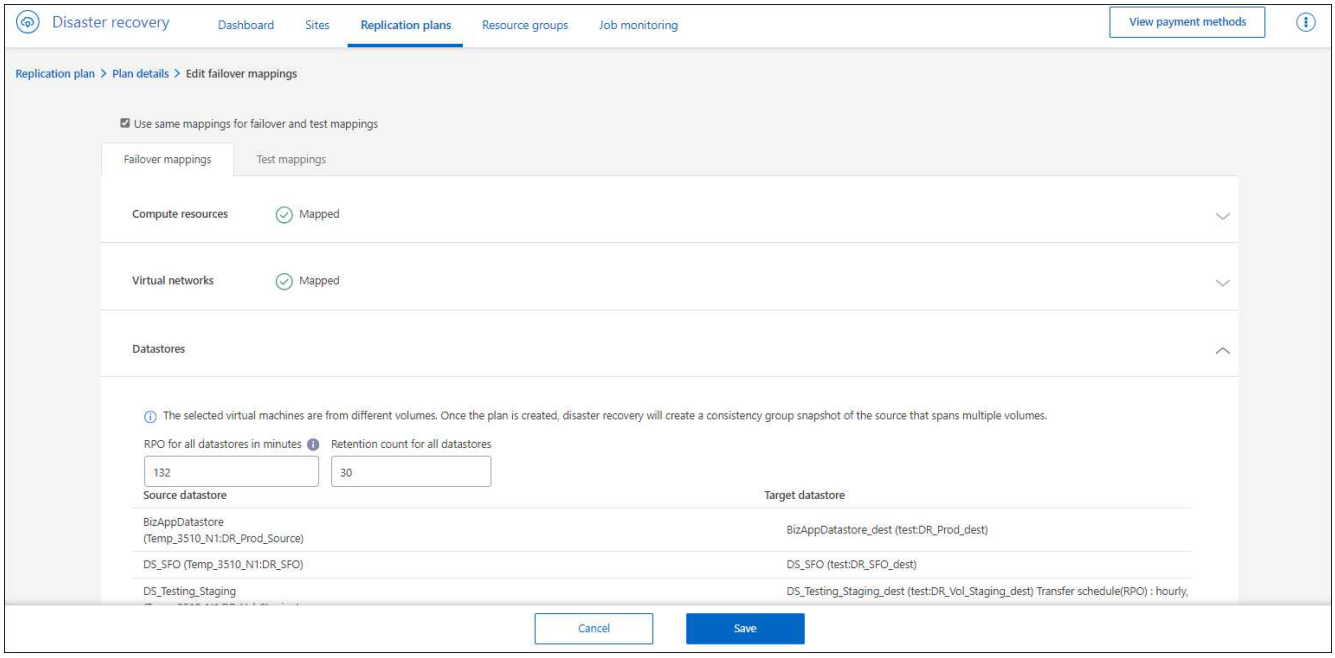
フェイルオーバースケジュールの保持数を変更する

保持されるデータストアの数を変更できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ フェールオーバー管理者、またはディザスタ リカバリ アプリケーション管理者のロール。

手順

1. メニューから*レプリケーション プラン*を選択します。
2. レプリケーション プランを選択し、[フェールオーバー マッピング] タブを選択して、[編集] 鉛筆アイコンを選択します。
3. *データストア*矢印を選択して展開します。



4. レプリケーション プラン内の保持カウントの値を変更します。
5. レプリケーション プランを選択した状態で、[アクション] メニューを選択し、[古いスナップショットのクリーンアップ] を選択して、新しい保持カウントに合わせてターゲット上の古いスナップショットを削除します。

データストア情報を表示する

ソースとターゲットに存在するデータストアの数に関する情報を表示できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ フェールオーバー管理者、ディザスタ リカバリ アプリケーション管理者、またはディザスタ リカバリ ビューア ロール。

手順

1. メニューから*ダッシュボード*を選択します。
2. サイト行で vCenter を選択します。
3. *データストア*を選択します。
4. データストアの情報を表示します。

仮想マシンの情報を表示する

ソースとターゲットに存在する仮想マシンの数、CPU、メモリ、使用可能な容量に関する情報を表示できます。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ フェールオーバー管理者、ディザスタ リカバリ アプリケーション管理者、またはディザスタ リカバリ ビューア ロール。

手順

1. メニューから*ダッシュボード*を選択します。
2. サイト行で vCenter を選択します。
3. *仮想マシン*を選択します。
4. 仮想マシンの情報を表示します。

NetApp Disaster Recoveryジョブの監視

すべてのNetApp Disaster Recoveryジョブを監視し、その進行状況を確認できます。

ジョブの表示

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ アプリケーション管理者、またはディザスタ リカバリ ビューア ロール。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。
3. メニューから*ジョブ監視*を選択します。
4. 操作に関連するすべてのジョブを調べ、タイムスタンプとステータスを確認します。
5. 特定のジョブの詳細を表示するには、その行を選択します。
6. 情報を更新するには、[更新] を選択します。

ジョブをキャンセルする

ジョブが進行中またはキュー状態にあり、続行したくない場合は、キャンセルできます。ジョブが同じ状態の

まま停止し、キュー内の次の操作を解放したい場合は、ジョブをキャンセルする必要があります。タイムアウトする前にジョブをキャンセルする必要がある場合があります。

必要な**NetApp Console**ロール 組織管理者、フォルダまたはプロジェクト管理者、ディザスタ リカバリ管理者、ディザスタ リカバリ フェールオーバー管理者、またはディザスタ リカバリ アプリケーション管理者のロール。

"NetApp Disaster Recoveryにおけるユーザーの役割と権限について学習します" 。https://docs.netapp.com/us-en/bluexp-setup-admin/reference-iam-predefined-roles.html["すべてのサービスに対するNetApp Consoleのアクセスロールについて学習します"^] 。

手順

1. NetApp Consoleの左側のナビゲーション バーから、保護 > 災害復旧 を選択します。
2. メニューから*ジョブ監視*を選択します。
3. ジョブ モニター ページで、キャンセルするジョブの ID をメモします。

   ジョブは「進行中」または「キューに登録済み」の状態である必要があります。
4. [アクション] 列で、[ジョブのキャンセル] を選択します。

NetApp Disaster Recoveryレポートを作成する

NetApp Disaster Recoveryレポートを確認すると、ディザスタ リカバリへの備えを分析するのに役立ちます。事前に設計されたレポートには、過去 7 日間のアカウント内のすべてのサイトのテスト フェイルオーバーの概要、レプリケーション プランの詳細、ジョブの詳細が含まれます。

レポートは PDF、HTML、または JSON 形式でダウンロードできます。

ダウンロードリンクは6時間有効です。

手順

1. ログイン "NetApp Console"。
2. NetApp Consoleの左側のナビゲーションから、保護 > 災害復旧 を選択します。
3. NetApp Consoleの左側のナビゲーション バーから、レプリケーション プラン を選択します。
4. *レポートの作成*を選択します。
5. ファイル形式の種類と過去 7 日間の期間を選択します。
6. *作成*を選択します。

   レポートが表示されるまで数分かかる場合があります。
7. レポートをダウンロードするには、[レポートのダウンロード] を選択し、管理者のダウンロード フォルダーで選択します。

参照

NetApp Disaster Recoveryに必要な vCenter 権限

NetApp Disaster Recovery がデータストアの登録と登録解除、VM の起動と停止、仮想マシン (VM) の再構成などのサービスを実行できるようにするには、vCenter アカウントに最低限の vCenter 権限が必要です。次の表には、NetApp Disaster Recovery がvCenterクラスタとインターフェースするために必要なすべての権限がリストされています。

タイプ	権限名	説明
データストア	データストア.データストアを構成する	データストアを構成するために使用します。
	データストア.データストアを削除	データストアを削除するために使用します。
仮想マシン	仮想マシン.構成.設定の変更	一般的な VM 設定を変更するために使用します。
	仮想マシン.構成.デバイス設定の変更	既存のデバイスのプロパティを変更するために使用します。
	仮想マシン.構成.パスからの再読み込み	VM の ID を保持しながら VM 構成パッチを変更するために使用します。 VMware vCenter Site Recovery Manager などのソリューションは、この操作を使用して、フェイルオーバーおよびフェイルバック中に VM の識別を維持します。
	仮想マシン.構成.名前の変更	VM の名前を変更したり、VM に関連付けられたノードを変更したりするために使用します。
	仮想マシン.構成.ゲスト情報をリセット	VM のゲスト オペレーティング システム情報を編集するために使用します。
	仮想マシン.構成.メモリの変更	VM に割り当てられるメモリの量を変更するために使用します。
	仮想マシン.構成.CPU数の変更	仮想 CPU の数を変更するために使用します。
仮想マシンゲスト	仮想マシン.ゲスト操作.ゲスト操作の変更	VM へのファイルの転送など、VM 内のゲスト オペレーティング システムの変更を伴う VM ゲスト操作を有効にします。

タイプ	権限名	説明
仮想マシンの相互作用	仮想マシン.インタラクション.電源オフ	電源がオンになっている VM の電源をオフにするために使用します。この操作により、ゲスト オペレーティング システムの電源がオフになります。
	仮想マシン.インタラクション.電源オン	電源がオフになっている VM の電源をオンにし、一時停止されている VM を再開するために使用します。
	仮想マシン.相互作用.VMware Tools のインストール	VMware Tools CD インストーラをゲスト オペレーティング システムの CD-ROM としてマウントおよびアンマウントするために使用します。
仮想マシンインベントリ	仮想マシン.インベントリ.新規作成	VM を作成し、その実行のためのリソースを割り当てるために使用します。
	仮想マシン.インベントリ.登録	既存の VM を vCenter Server またはホスト インベントリに追加するために使用します。
	仮想マシン.インベントリ.登録解除	vCenter Server またはホスト インベントリから VM を登録解除するために使用します。
仮想マシンの状態	仮想マシン。スナップショット管理。スナップショットの作成	VM の現在の状態からスナップショットを作成するために使用します。
	仮想マシン.スナップショット管理.スナップショットの削除	スナップショット履歴からスナップショットを削除するために使用します。
	仮想マシン。スナップショット管理。スナップショットへの復元	VM を特定のスナップショットの状態に設定する場合に使用します。

NetApp Disaster Recovery の機能へのロールベースのアクセス

NetApp Disaster Recovery、ロールを使用して、各ユーザーの特定の機能やアクションへのアクセスを制御します。

このサービスは、NetApp Disaster Recoveryに固有の次のロールを使用します。

- ディザスタ リカバリ管理者: NetApp Disaster Recoveryであらゆるアクションを実行します。
- 災害復旧フェイルオーバー管理者: NetApp Disaster Recoveryでフェイルオーバーと移行アクションを実行します。

- 災害復旧アプリケーション管理者: レプリケーション プランを作成および変更し、テスト フェイルオーバーを開始します。
- ディザスタ リカバリ ビューアー: NetApp Disaster Recoveryの情報を表示できますが、アクションを実行することはできません。

これらのロールはNetApp Disaster Recoveryに固有のものであり、 NetApp Consoleで使用されるプラットフォーム ロールとは異なります。 NetApp Consoleプラットフォームのすべてのロールの詳細については、"NetApp Consoleのセットアップと管理に関するドキュメント" 。

次の表は、各NetApp Disaster Recoveryロールが実行できるアクションを示しています。

特徴とアクション	災害復旧管理者	災害復旧フェイルオーバー管理者	災害復旧アプリケーション管理者	災害復旧ビューア
ダッシュボードとすべてのタブを表示	はい	はい	はい	はい
無料トライアルを始める	はい	いいえ	いいえ	いいえ
ワークロードの検出を開始する	はい	いいえ	いいえ	いいえ
ライセンス情報を表示	はい	はい	はい	はい
ライセンスを有効化	はい	いいえ	はい	いいえ
サイトオプションで:				
サイトを表示	はい	はい	はい	はい
サイトの追加、変更、削除	はい	いいえ	いいえ	いいえ
レプリケーション プラン オプションについて:				
レプリケーションプランの表示	はい	はい	はい	はい
レプリケーションプランの詳細を表示する	はい	はい	はい	はい
レプリケーションプランを作成または変更する	はい	はい	はい	いいえ
レポートを作成する	はい	いいえ	いいえ	いいえ
スナップショットを表示	はい	はい	はい	はい
フェイルオーバーテストを実行する	はい	はい	はい	いいえ
フェイルオーバーを実行する	はい	はい	いいえ	いいえ

特徴とアクション	災害復旧管理者	災害復旧フェイルオーバー管理者	災害復旧アプリケーション管理者	災害復旧ビューア
フェイルバックを実行する	はい	はい	いいえ	いいえ
移行を実行する	はい	はい	いいえ	いいえ
リソース グループ オプションについて:				
リソース グループを表示する	はい	はい	はい	はい
リソース グループの作成、変更、または削除	はい	いいえ	はい	いいえ
オンザジョブ監視オプション:				
ジョブの表示	はい	いいえ	はい	はい
ジョブをキャンセルする	はい	はい	はい	いいえ

Amazon EVS でNetApp Disaster Recoveryを使用する

Amazon Elastic VMware Service とAmazon FSx for NetApp ONTAPを使用したNetApp Disaster Recoveryの紹介

顧客は、実稼働コンピューティング ワークロード用の VMware vSphere ベースの仮想化インフラストラクチャにますます依存するようになっています。これらの仮想マシン (VM) がビジネスにとってより重要になるにつれ、顧客はこれらの VM を物理コンピューティング リソースと同じ種類の災害から保護する必要があります。現在提供されている災害復旧 (DR) ソリューションは複雑で高価であり、多くのリソースを必要とします。仮想化インフラストラクチャに使用される最大のストレージ プロバイダーであるNetAppは、 ONTAPストレージでホストされるあらゆる種類のデータを保護するのと同じ方法で、自社の顧客の VM を確実に保護することに強い関心を持っています。この目標を達成するために、 NetApp はNetApp Disaster Recoveryサービスを作成しました。

あらゆる DR ソリューションの主な課題の 1 つは、DR レプリケーションおよびリカバリ インフラストラクチャを提供するためだけに、追加のコンピューティング、ネットワーク、およびストレージ リソースを購入、構成、維持するための増分コストを管理することです。重要なオンプレミスの仮想リソースを保護するための一般的なオプションの 1 つは、クラウドでホストされる仮想リソースを DR レプリケーションおよびリカバリ インフラストラクチャとして使用することです。 Amazon は、 NetApp ONTAPがホストする VM インフラストラクチャと互換性のあるコスト効率の高いリソースを提供できるソリューションの一例です。

Amazon は、仮想プライベートクラウド (VPC) 内で VMware Cloud Foundation を有効にする Amazon Elastic VMware Service (Amazon EVS) を導入しました。 Amazon EVS は、使い慣れた VMware ソフトウェアおよびツールとともに AWS の回復力とパフォーマンスを提供し、Amazon EVS vCenter をオンプレミスの仮想化インフラストラクチャの拡張機能として統合できるようにします。

Amazon EVS にはストレージリソースが付属していますが、ネイティブストレージを使用すると、ストレージ負荷の高いワークロードを持つ組織ではその有効性が低下する可能性があります。このような場

合、Amazon EVS とAmazon FSx for NetApp ONTAPストレージ (Amazon FSxN) を組み合わせると、より柔軟なストレージソリューションを提供できます。さらに、オンプレミスのNetApp ONTAPストレージソリューションを使用して VMware インフラストラクチャをホストしている場合、FSx for ONTAPを備えた Amazon EVS を使用すると、オンプレミスとクラウドでホストされるインフラストラクチャ間でクラス最高のデータ相互運用性と保護機能が得られます。

Amazon FSx for NetApp ONTAPの詳細については、以下を参照してください。 "Amazon FSx for NetApp ONTAPを使い始める" 。

Amazon EVS と Amazon FSs for NetApp ONTAPを使用したNetApp Disaster Recoveryのソリューション概要

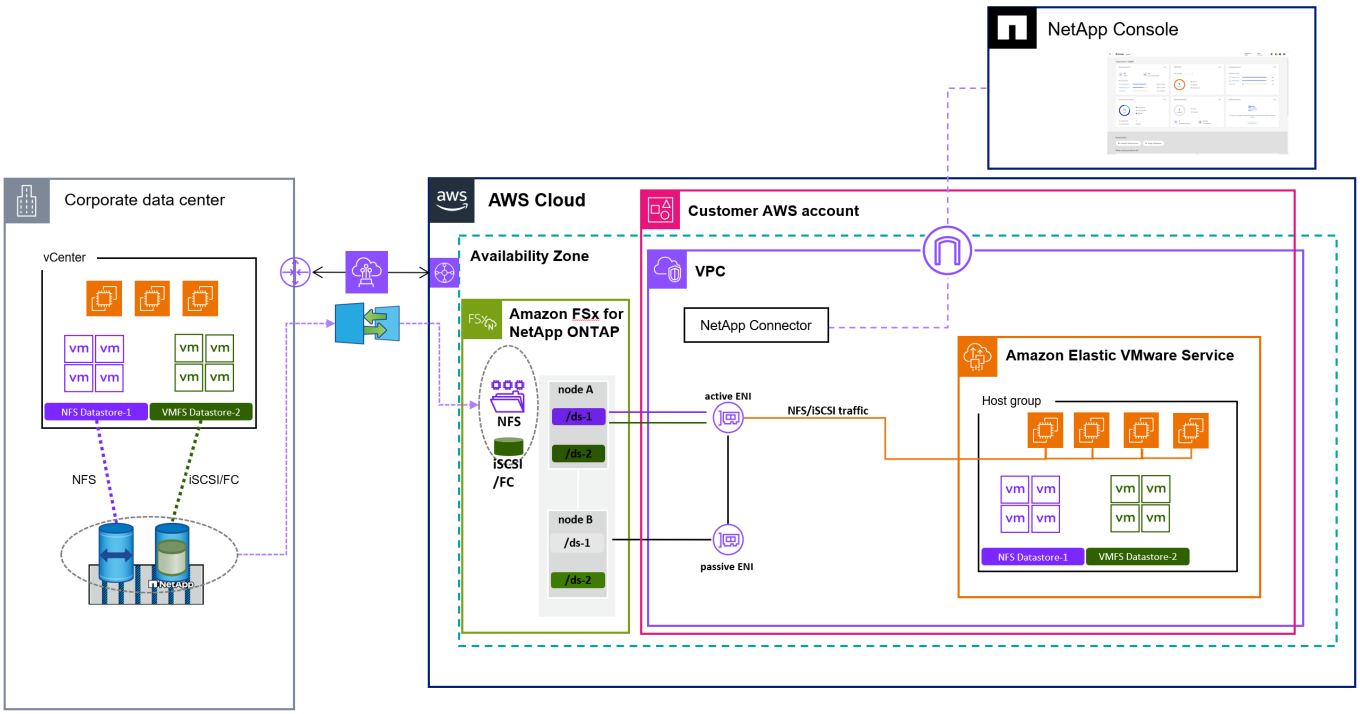
NetApp Disaster Recoveryは、 NetApp Consoleのコア アーキテクチャに依存する、NetAppNetApp Consoleのソフトウェア アズ ア サービス環境内でホストされる付加価値サービスです。コンソール内の VMware 保護の DR サービスは、いくつかの主要コンポーネントで構成されています。

NetApp Disaster Recoveryソリューションの完全な概要については、以下を参照してください。"NetApp Disaster Recoveryについて学ぶ" 。

オンプレミスの VMware がホストする仮想マシンを Amazon AWS に保護する場合は、 Amazon FSx for NetApp ONTAPストレージがホストするデータストアを使用して Amazon EVS にバックアップするサービスを使用します。

次の図は、Amazon EVS を使用して VM を保護するサービスがどのように機能するかを示しています。

Amazon EVS と FSx for ONTAPを使用したNetApp Disaster Recoveryの概要



1. Amazon EVS は、単一のアベイラビリティーゾーン (AZ) 構成でアカウントにデプロイされ、仮想プライベートクラウド (VPC) 内にもデプロイされます。

2. FSx for ONTAPファイルシステムは、Amazon EVS デプロイメントと同じ AZ にデプロイされます。ファイルシステムは、Elastic Network Interface (ENI)、VPC ピア接続、または AmazonTransit Gateway を介して Amazon EVS に直接接続します。
3. NetApp Consoleエージェントが VPC にインストールされます。 NetApp Consoleエージェントは、ローカルの物理データセンターと Amazon AWS がホストするリソースの両方で VMware インフラストラクチャの DR を管理するNetApp Disaster Recoveryエージェントを含む、複数のデータ管理サービス (エージェントと呼ばれる) をホストします。
4. NetApp Disaster Recoveryエージェントは、 NetApp Consoleクラウド ホスト サービスと安全に通信してタスクを受信し、それらのタスクを適切なオンプレミスおよび AWS ホストの vCenter およびONTAPストレージ インスタンスに配布します。
5. NetApp Consoleのクラウド ホスト UI コンソールを使用してレプリケーション プランを作成し、保護する必要がある VM、それらの VM を保護する頻度、オンプレミス サイトからのフェイルオーバーが発生した場合にそれらの VM を再起動するために実行する必要がある手順を指定します。
6. レプリケーション プランは、保護された VM をホストしている vCenter データストアと、それらのデータストアをホストしているONTAPボリュームを決定します。 FSx for ONTAPクラスターにボリュームがまだ存在しない場合は、 NetApp Disaster Recoveryによって自動的に作成されます。
7. 識別されたソースONTAPボリュームごとに、各宛先 FSx for ONTAPがホストするONTAPボリュームへのSnapMirror関係が作成され、レプリケーション プランでユーザーが指定した RPO に基づいてレプリケーション スケジュールが作成されます。
8. プライマリ サイトに障害が発生した場合、管理者はNetApp Console内で手動のフェイルオーバー プロセスを開始し、復元ポイントとして使用するバックアップを選択します。
9. NetApp Disaster Recoveryエージェントは、FSx for ONTAPでホストされるデータ保護ボリュームをアクティブ化します。
10. エージェントは、アクティブ化された各 FSx for ONTAPボリュームを Amazon EVS vCenter に登録し、保護された各 VM を Amazon EVS vCenter に登録し、レプリケーション プランに含まれる定義済みルールに従って各 VM を起動します。

NetApp Disaster Recovery用のNetApp Consoleエージェントをインストールする

NetApp Consoleエージェントは、クラウドまたはオンプレミス ネットワークで実行されるNetAppソフトウェアです。 NetApp Consoleがデータ インフラストラクチャを管理するために実行する必要があるアクションを実行します。コンソール エージェントは、実行する必要があるアクションがあるかどうか、NetApp Disaster Recoveryソフトウェアをサービス レイヤーとして継続的にポーリングします。

NetApp Disaster Recoveryの場合、実行されるアクションは、それぞれのサービスごとにネイティブ API を使用して VMware vCenter クラスターとONTAPストレージ インスタンスをオーケストレーションし、オンプレミスの場所で実行されている本番環境の VM を保護します。コンソール エージェントはネットワーク上の任意の場所にインストールできますが、 NetApp Disaster Recoveryの場合は、コンソール エージェントを DR サイトにインストールすることをお勧めします。これにより、プライマリ サイトに障害が発生した場合でも、 NetAppクラウドベースのコンソール UI はコンソール エージェントとの接続を維持し、その DR サイト内でリカバリ プロセスを調整できるようになります。

サービスを使用するには、コンソール エージェントを標準モードでインストールします。コンソールエージェントのインストールの種類の詳細については、次のサイトをご覧ください。 "NetApp Consoleの導入モードについて学ぶ | NetAppドキュメント" 。

コンソール エージェントはサービスを使用する上で重要ですが、コンソール エージェントをインストールす

る手順は、ニーズとネットワーク構成によって異なります。インストールに関する具体的な手順を説明することは、この情報の範囲外です。

Amazon AWS を使用してコンソールエージェントをインストールする最も簡単な方法は、AWS Marketplace を使用することです。 AWS Marketplaceを使用したコンソールエージェントのインストールの詳細については、以下を参照してください。 "AWS Marketplace からコンソールエージェントを作成する | NetAppドキュメント" 。

Amazon EVS 用のNetApp Disaster Recoveryを構成する

Amazon EVS 向けNetApp Disaster Recoveryの構成の概要

NetApp Consoleエージェントをインストールした後、災害復旧プロセスに参加するすべてのONTAPストレージと VMware vCenter リソースをNetApp Disaster Recoveryと統合する必要があります。

- "NetApp Disaster Recoveryを使用した Amazon EVS の前提条件"
- "NetApp Disaster RecoveryにONTAPストレージアレイを追加する"
- "Amazon EVS でNetApp Disaster Recoveryを有効にする"
- "NetApp Disaster Recoveryに vCenter サイトを追加する"
- "NetApp Disaster Recoveryに vCenter クラスタを追加する"

NetApp Disaster Recoveryを使用した Amazon EVS の前提条件

NetApp Disaster Recoveryを使用して Amazon EVS の設定を続行する前に、いくつかの前提条件が満たされていることを確認する必要があります。

具体的には、次の操作を実行します。

- NetApp Disaster Recovery が必要な操作を実行するために必要な特定の VMware 権限を持つ vCenter ユーザー アカウントを作成します。

  デフォルトの「administrator@vsphere.com」管理者アカウントの使用はお勧めしません。代わりに、DR プロセスに参加するすべての vCenter クラスタにNetApp Disaster Recovery 専用のユーザー アカウントを作成する必要があります。必要な特定の権限のリストについては、"NetApp Disaster Recoveryに必要な vCenter 権限" 。

- NetApp Disaster Recoveryによって保護される VM をホストするすべての vCenter データストアが、NetApp ONTAPストレージ リソース上に配置されていることを確認します。

  このサービスは、 NetApp ONTAPでAmazon FSxを使用する場合、iSCSI 上の NFS および VMFS (FC はサポートされません) をサポートします。このサービスは FC をサポートしていますが、 Amazon FSx for NetApp ONTAP はFC をサポートしていません。

- Amazon EVS vCenter がAmazon FSx for NetApp ONTAPストレージクラスターに接続されていることを確認します。
- 保護されているすべての VM に VMware ツールがインストールされていることを確認します。

- Amazon が承認した接続方法を使用して、オンプレミス ネットワークが AWS VPC ネットワークに接続されていることを確認します。 AWS Direct Connect、AWS Private Link、または AWS サイト間 VPN を使用することをお勧めします。

NetApp Disaster Recoveryを使用して **Amazon EVS** の**NetApp Console**システムにオンプレミス アレイを追加する

NetApp Disaster Recoveryを使用する前に、オンプレミスおよびクラウドホストのストレージ インスタンスをNetApp Consoleシステムに追加する必要があります。

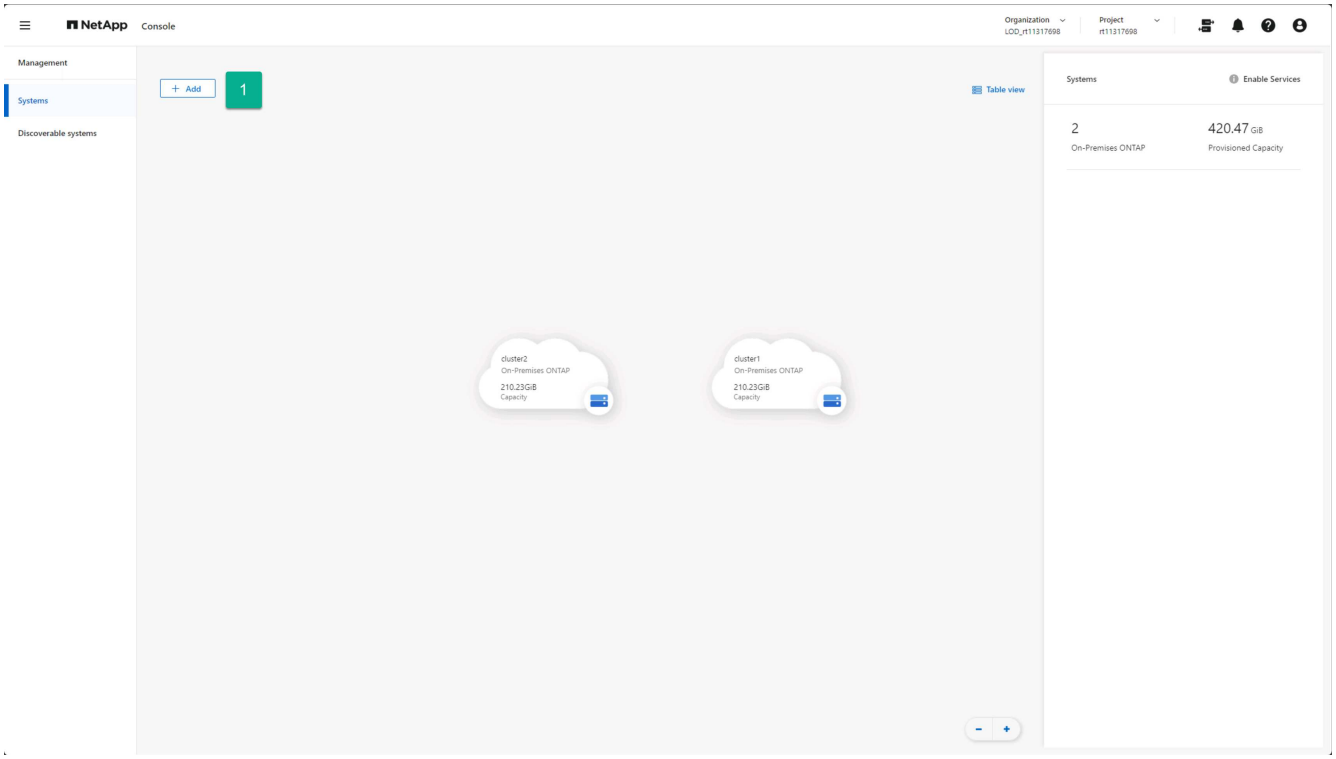
次の操作を行う必要があります。

- オンプレミスのアレイをNetApp Consoleシステムに追加します。
- Amazon FSx for NetApp ONTAP (FSx for ONTAP) インスタンスをNetApp Consoleシステムに追加します。

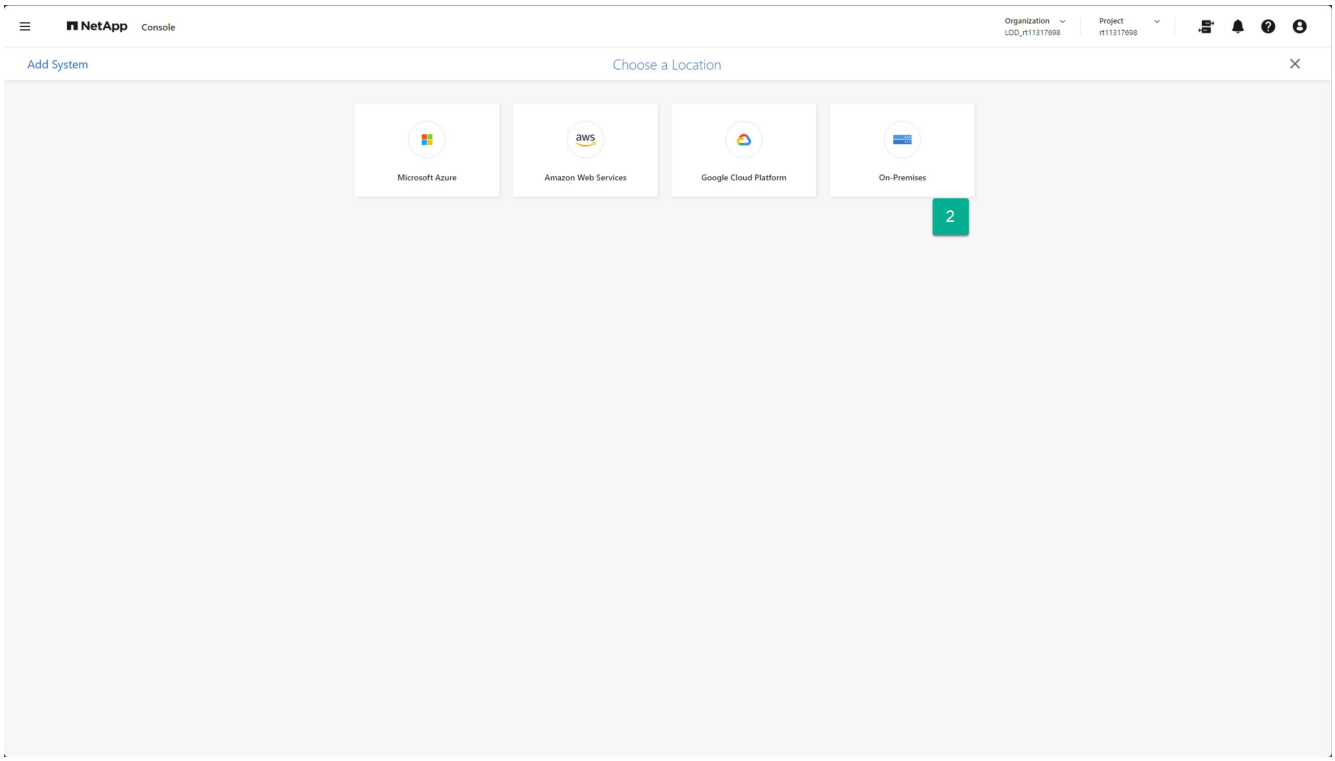
NetApp Consoleシステムにオンプレミスのストレージアレイを追加する

オンプレミスのONTAPストレージ リソースをNetApp Consoleシステムに追加します。

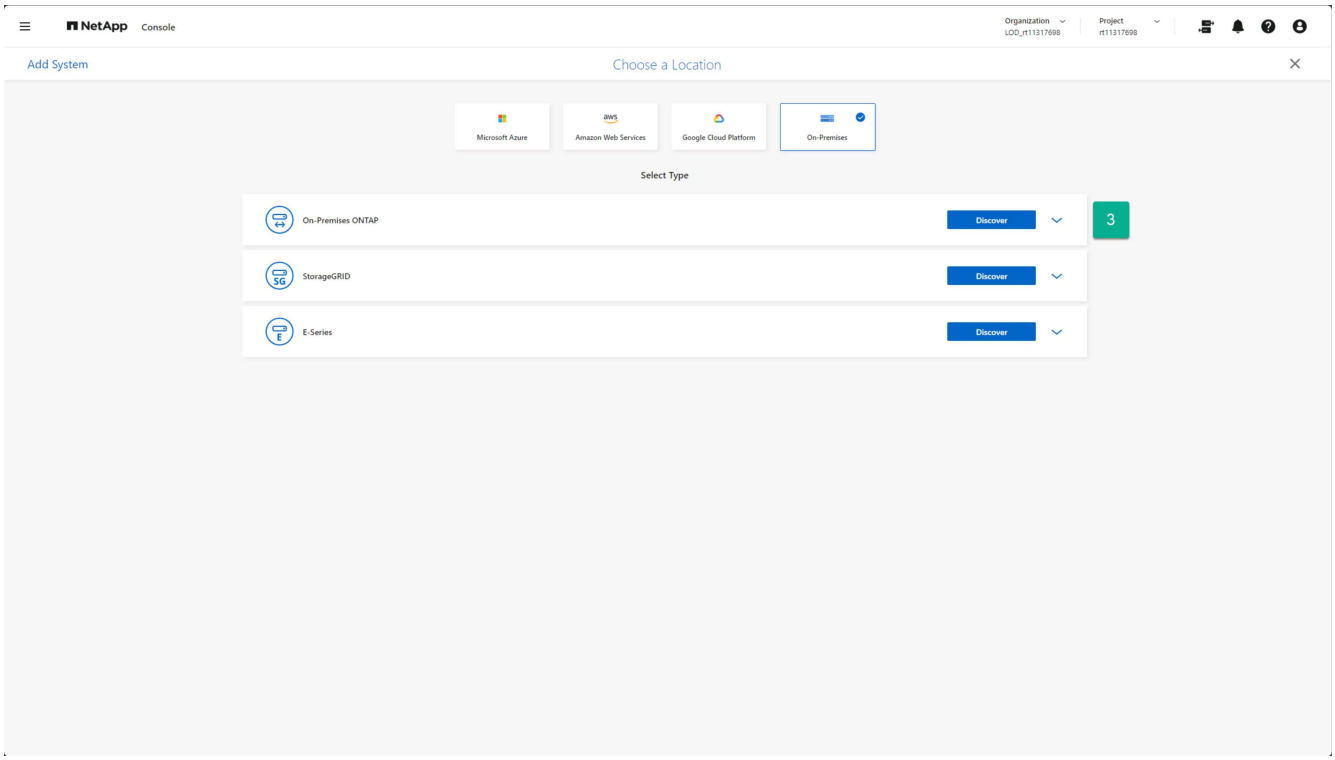
1. NetApp Consoleシステム ページから、[システムの追加] を選択します。



2. 「システムの追加」ページで、「オンプレミス」カードを選択します。

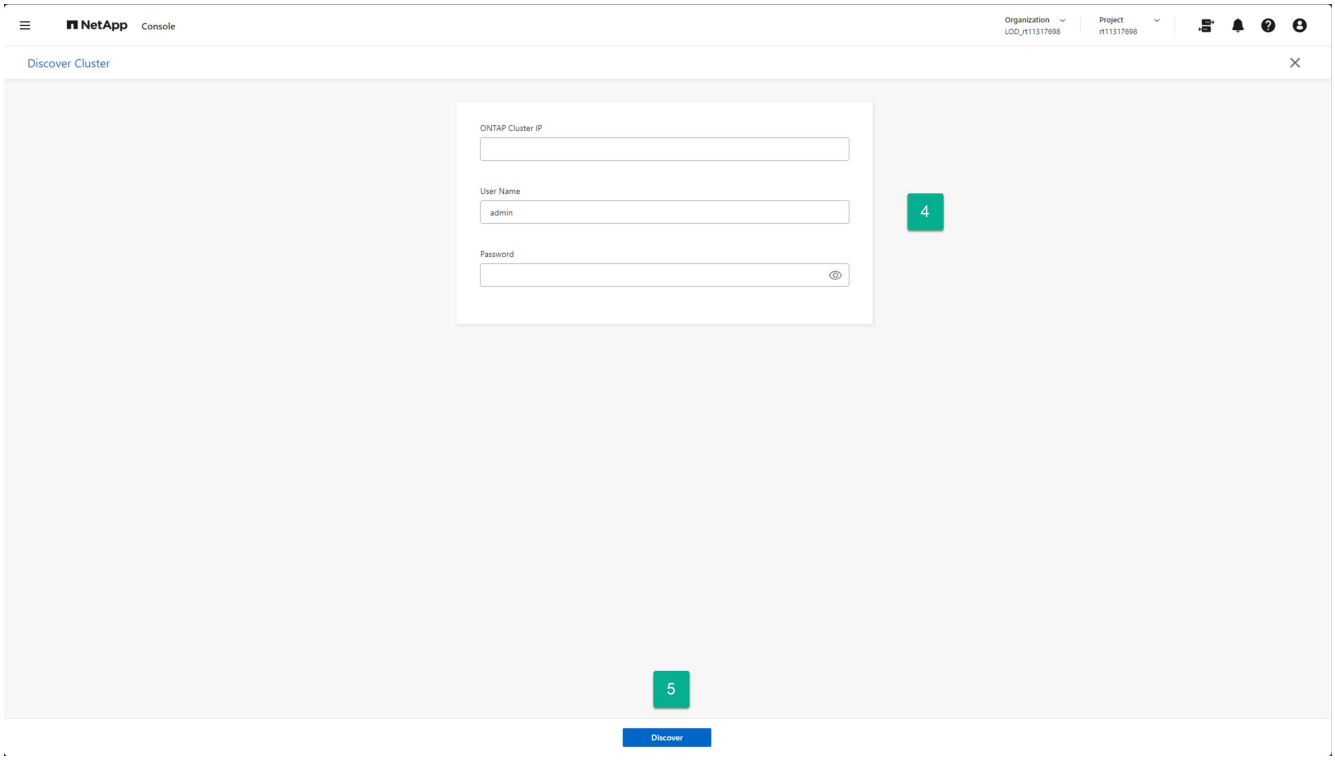


3. On-Premises ONTAPカードで **Discover** を選択します。



4. 「クラスターの検出」ページで、次の情報を入力します。
   a. ONTAPアレイクラスタ管理ポートのIPアドレス
   b. 管理者のユーザー名
   c. 管理者パスワード

5. ページの下部にある*Discover*を選択します。

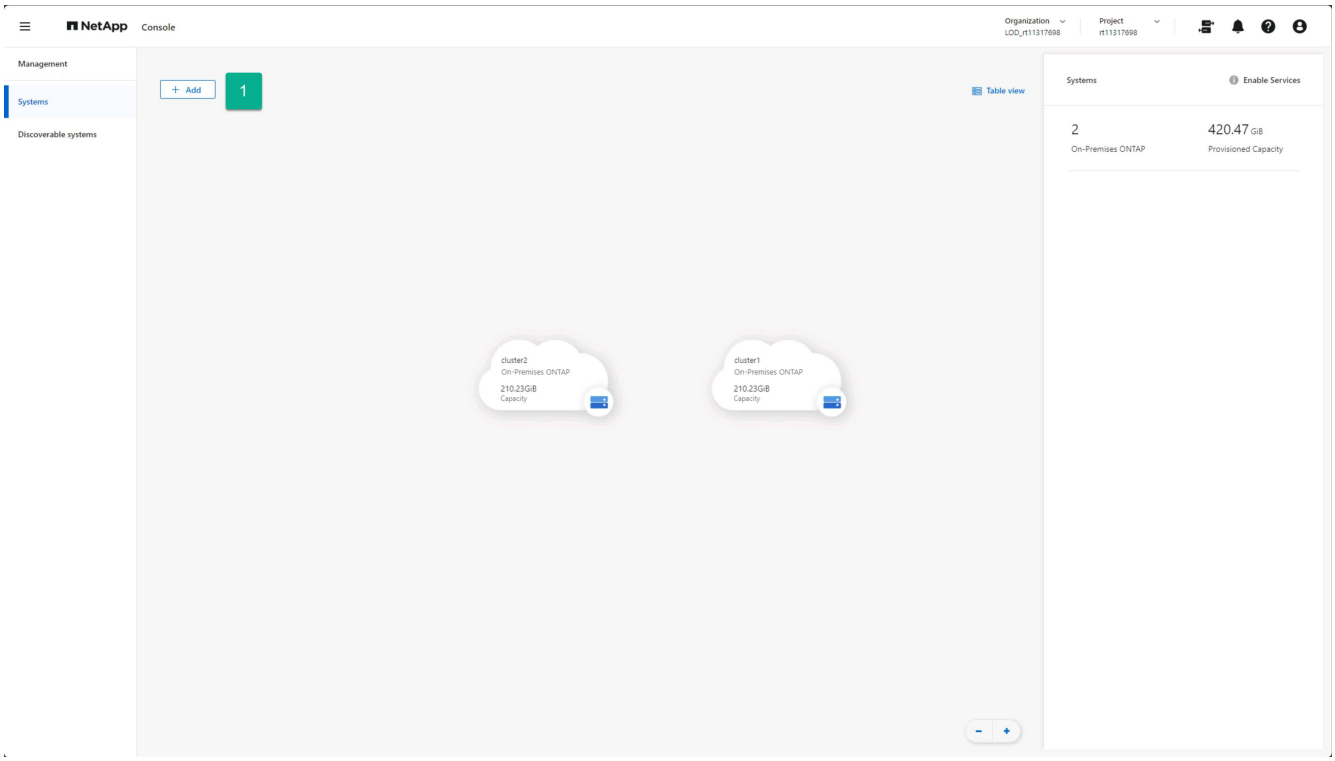


6. vCenter データストアをホストする各ONTAPアレイに対して手順 1 ～ 5 を繰り返します。

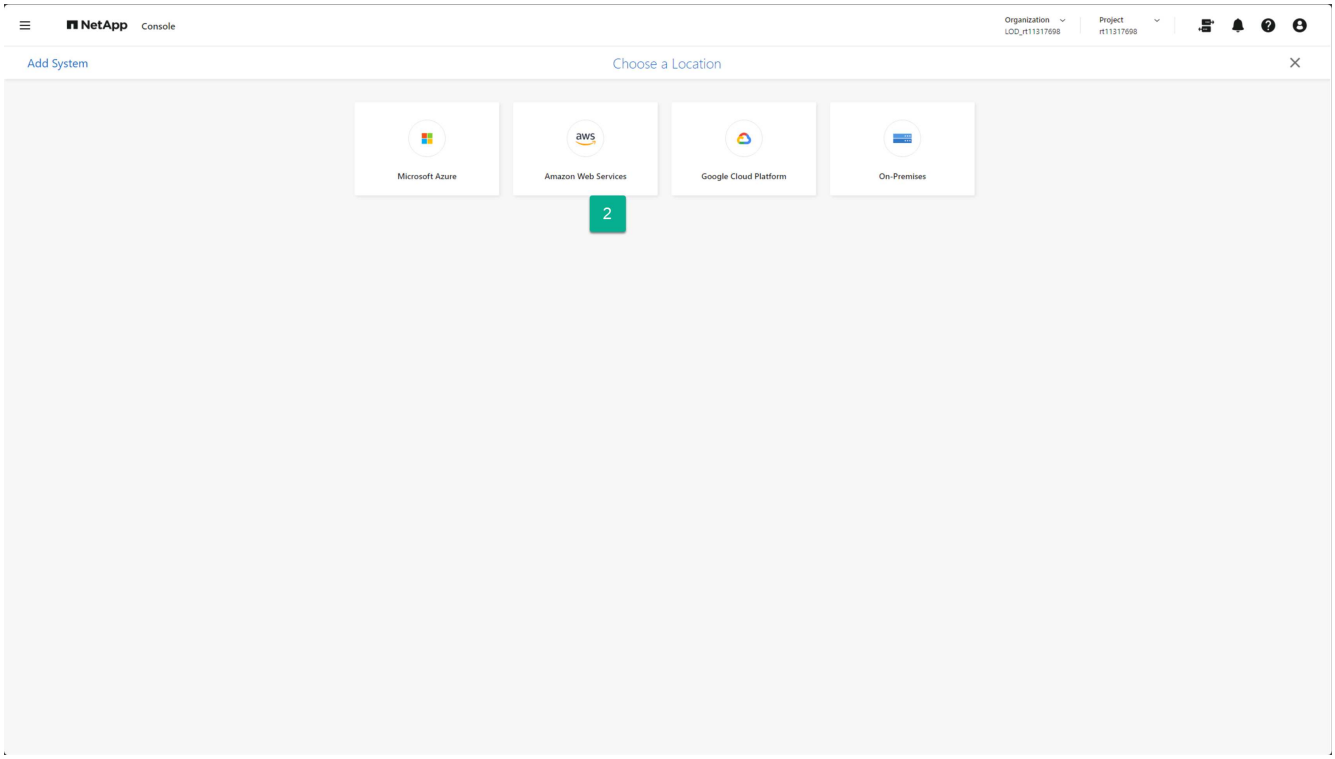
Amazon FSx for NetApp ONTAPストレージインスタンスを**NetApp Console**システムに追加する

次に、 Amazon FSx for NetApp ONTAPストレージリソースをNetApp Consoleシステムに追加します。

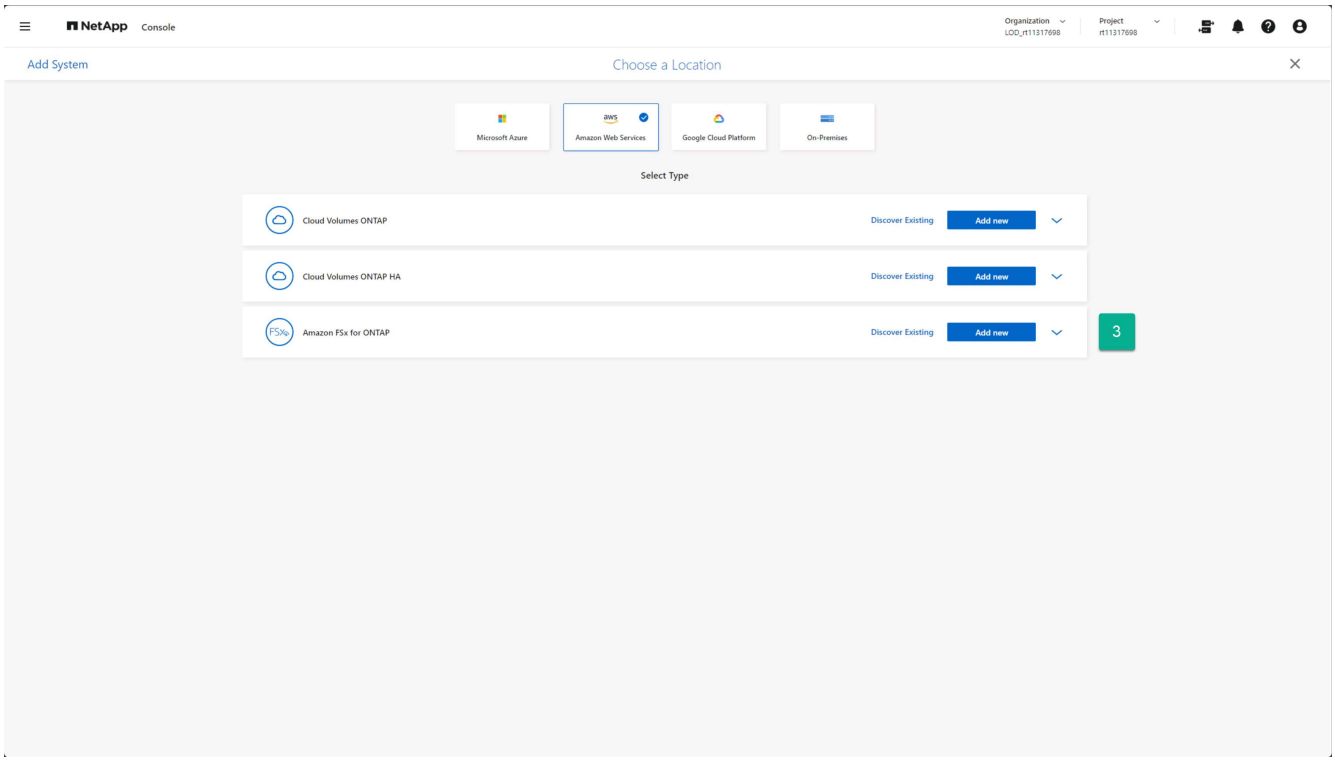
1. NetApp Consoleシステム ページから、[システムの追加] を選択します。



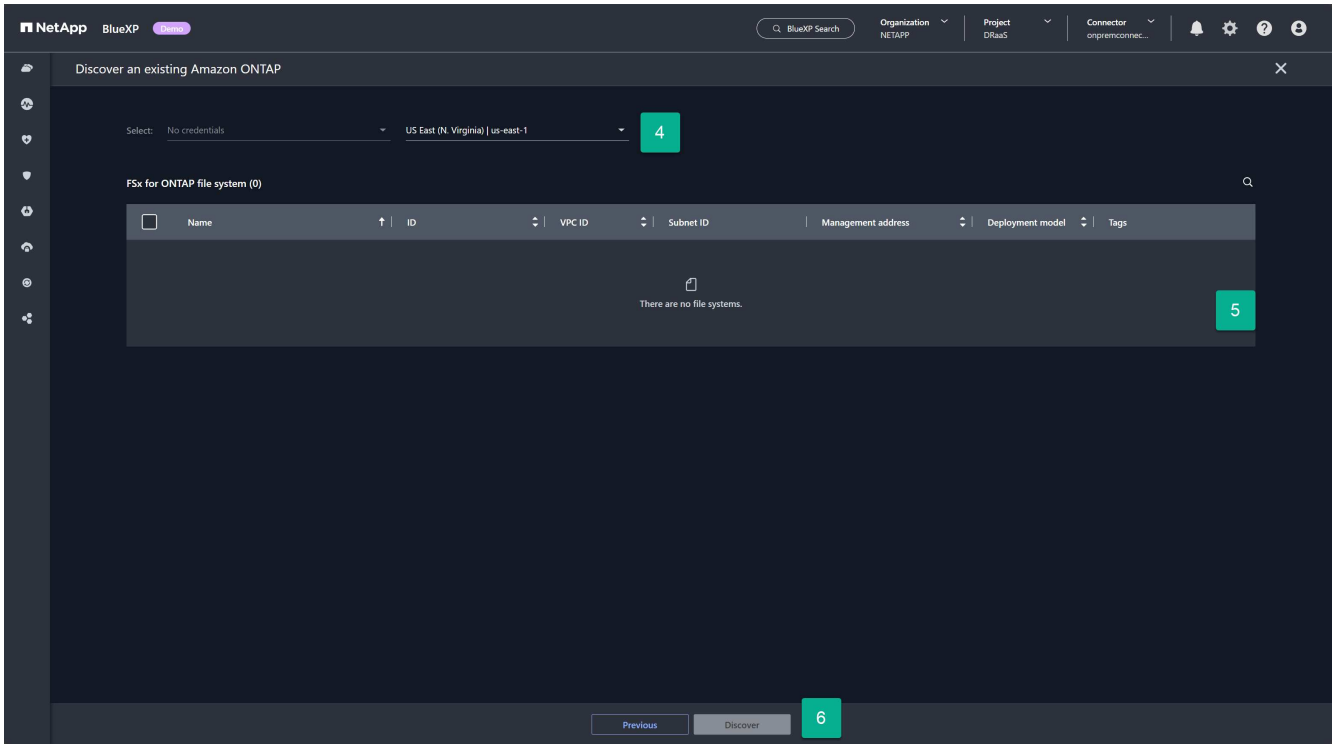
2. 「システムの追加」ページから、**Amazon Web Services** カードを選択します。



3. Amazon FSx for ONTAPカードの **Discover Existing** リンクを選択します。



4. FSx for ONTAPインスタンスをホストしている認証情報と AWS リージョンを選択します。
5. 追加する FSx for ONTAPファイル システムを 1 つ以上選択します。
6. ページの下部にある*Discover*を選択します。



7. vCenter データストアをホストする各 FSx for ONTAPインスタンスに対して手順 1 ～ 6 を繰り返します。

Amazon EVS のNetApp Consoleアカウントに NetApp Disaster Recoveryサービスを追加します

NetApp Disaster Recovery はライセンス製品であり、使用する前に購入する必要があります。ライセンスにはいくつかの種類があり、ライセンスを購入する方法もいくつかあります。ライセンスにより、特定の期間にわたって特定の量のデータを保護する権利が付与されます。

NetApp Disaster Recoveryライセンスの詳細については、以下を参照してください。"NetApp Disaster Recoveryのライセンスを設定する" 。

ライセンス タイプ

ライセンスには主に 2 つの種類があります。

- NetAppは"30日間試用ライセンス"ONTAPおよび VMware リソースを使用してNetApp Disaster Recoveryを評価するために使用できます。このライセンスでは、保護された容量を無制限に 30 日間使用できます。
- 30 日間の試用期間を超えて DR 保護が必要な場合は、製品ライセンスを購入してください。このライセンスは、NetApp のクラウド パートナーのマーケットプレイスを通じて購入できますが、このガイドでは、Amazon AWS Marketplace を使用してNetApp Disaster Recoveryのマーケットプレイス ライセンスを購入することをお勧めします。 Amazonマーケットプレイスでライセンスを購入する方法の詳細については、"AWS Marketplace からサブスクライブする" 。

災害復旧能力のニーズを予測する

ライセンスを購入する前に、保護する必要があるONTAPストレージ容量を把握しておく必要があります。NetApp ONTAPストレージを使用する利点の 1 つは、 NetApp がデータを保存する際の効率性が高いことです。 ONTAPボリュームに保存されるすべてのデータ (VMware データストアをホストする VM など) は、非常に効率的な方法で保存されます。 ONTAP は、物理ストレージにデータを書き込むときに、圧縮、重複排除、圧縮という 3 種類のストレージ効率をデフォルトに設定します。最終的な結果は、保存されるデータの種類に応じて、1.5:1 から 4:1 のストレージ効率になります。実際、 NetAppは "ストレージ効率保証"特定のワークロード向け。

NetApp Disaster Recovery は、すべてのONTAPストレージ効率が適用された後にライセンスの目的で容量を計算するため、これは有益です。たとえば、サービスを使用して保護する 100 台の仮想マシンをホストするために、vCenter 内に 100 テラバイト (TiB) の NFS データストアをプロビジョニングしたとします。さらに、データがONTAPボリュームに書き込まれるときに、自動的に適用されるストレージ効率化技術により、これらの VM が消費するストレージ効率は 33TiB のみ (3:1 のストレージ効率) になると仮定します。 NetApp Disaster Recovery のライセンスは、100TiB ではなく 33TiB のみ必要です。これは、他の DR ソリューションと比較した場合、DR ソリューションの総所有コストにとって非常に大きなメリットとなります。

手順

1. 保護対象の VMware データストアをホストしている各ボリュームで消費されているデータ量を確認するには、各ボリュームに対してONTAP CLI コマンドを実行して、ディスク上の容量消費量を確認します。
   `volume show-space -volume < volume name > -vserver < SVM name >` 。

   例えば：

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature                                  Used      Used%
------------------------------      --------     ------
User Data                             163.4MB         3%
Filesystem Metadata                     172KB         0%
Inodes                                 2.93MB         0%
Snapshot Reserve                      292.9MB         5%
Total Metadata                          185KB         0%
Total Used                            459.4MB         8%
Total Physical Used                   166.4MB         3%
```

2. 各ボリュームの*Total Physical Used*の値をメモします。これは、 NetApp Disaster Recovery が保護する必要があるデータの量であり、ライセンスが必要な容量を決定するために使用する値です。

NetApp Disaster Recovery for Amazon EVS にサイトを追加する

VM インフラストラクチャを保護する前に、保護対象の VM をホストしている VMware vCenter クラスターと、それらの vCenter が配置されている場所を特定する必要があります。最初のステップは、ソース データ センターと宛先データ センターを表すサイトを作成することです。サイトは障害ドメインまたは回復ドメインです。

以下を作成する必要があります。

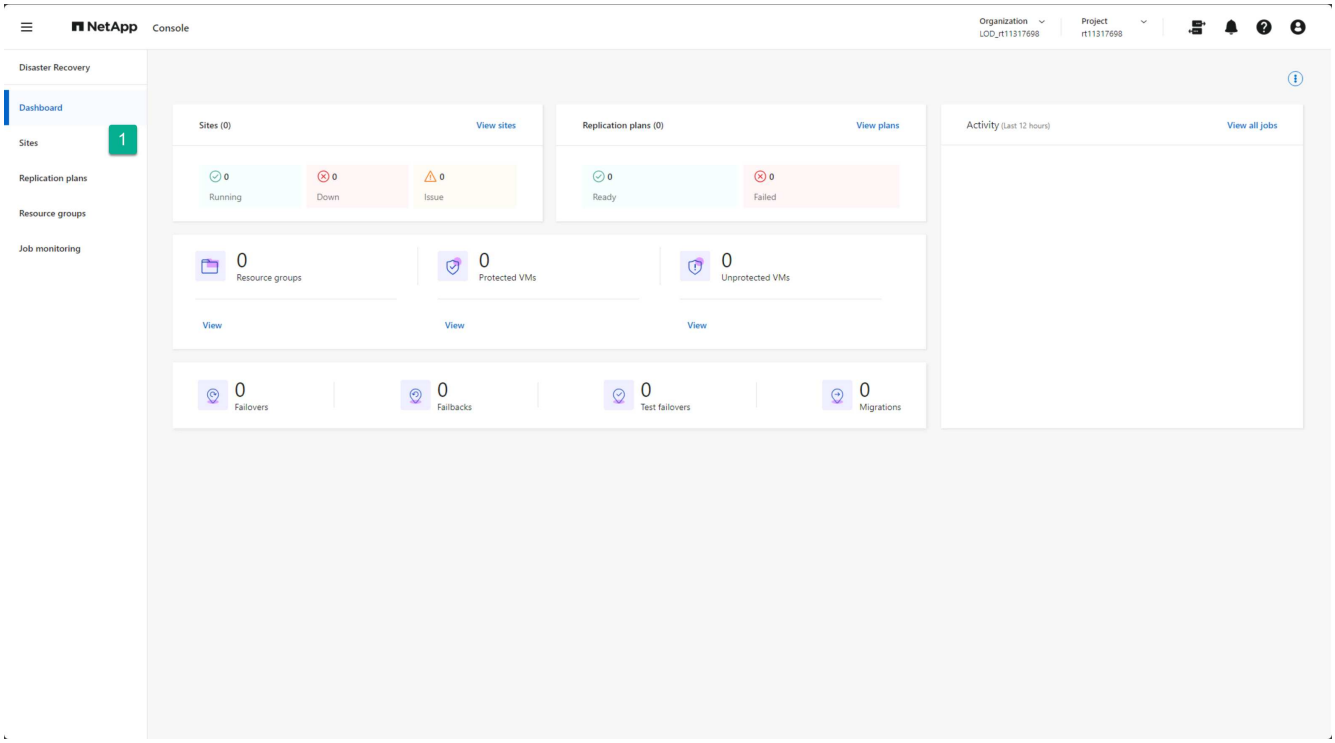
- 実稼働 vCenter クラスタが存在する各実稼働データセンターを表すサイト
- Amazon EVS/ Amazon FSx for NetApp ONTAPクラウドデータセンターのサイト

オンプレミスサイトを作成する

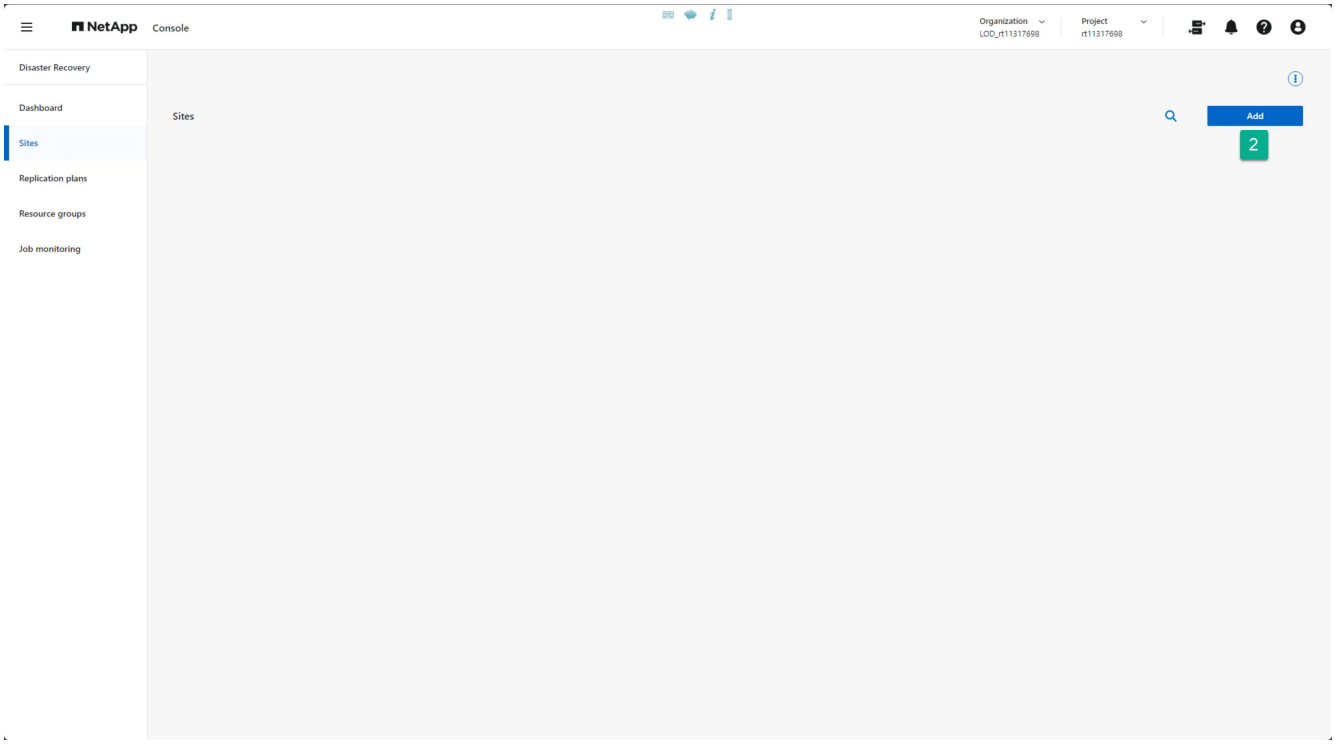
本番環境の vCenter サイトを作成します。

手順

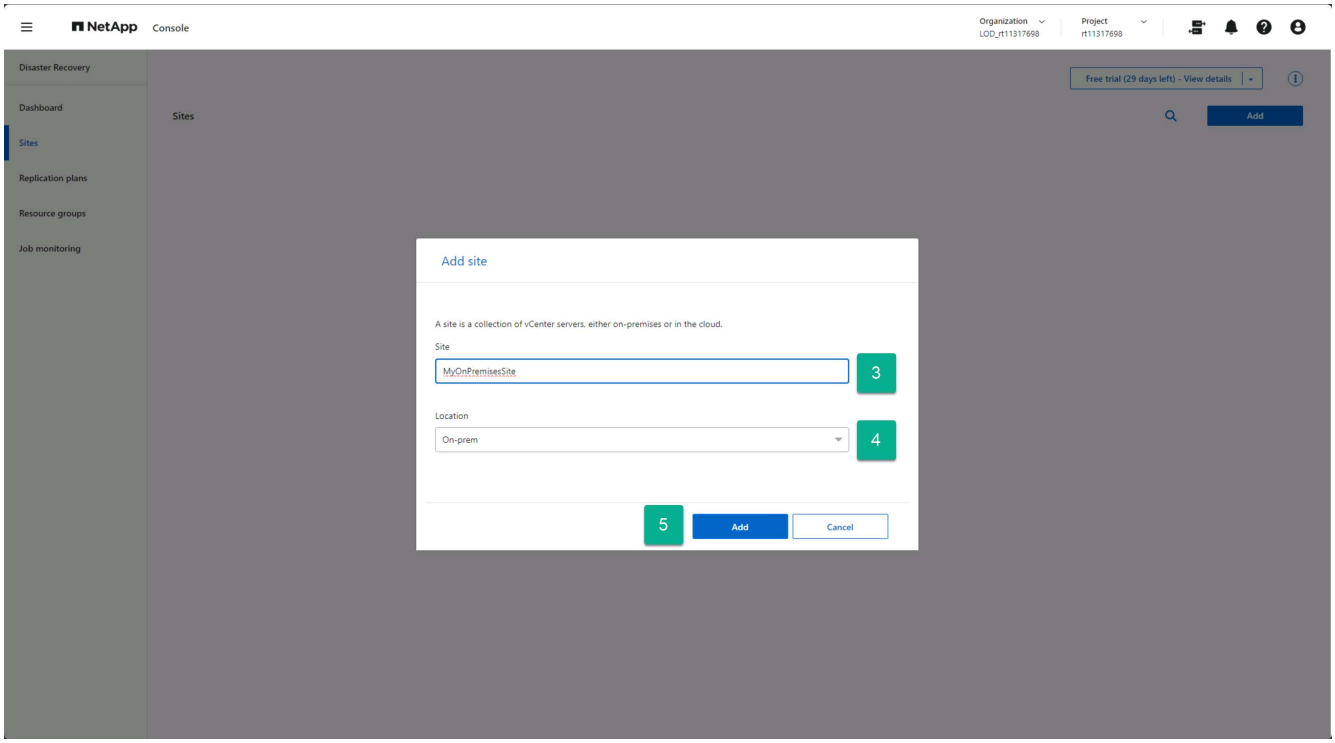
1. NetApp Consoleの左側のナビゲーション バーから、保護 > ディザスタ リカバリ を選択します。
2. NetApp Disaster Recoveryの任意のページから、サイト オプションを選択します。



3. [サイト] オプションから [追加] を選択します。



4. [サイトの追加] ダイアログ ボックスで、サイト名を入力します。
5. 場所として「オンプレミス」を選択します。
6. *追加*を選択します。

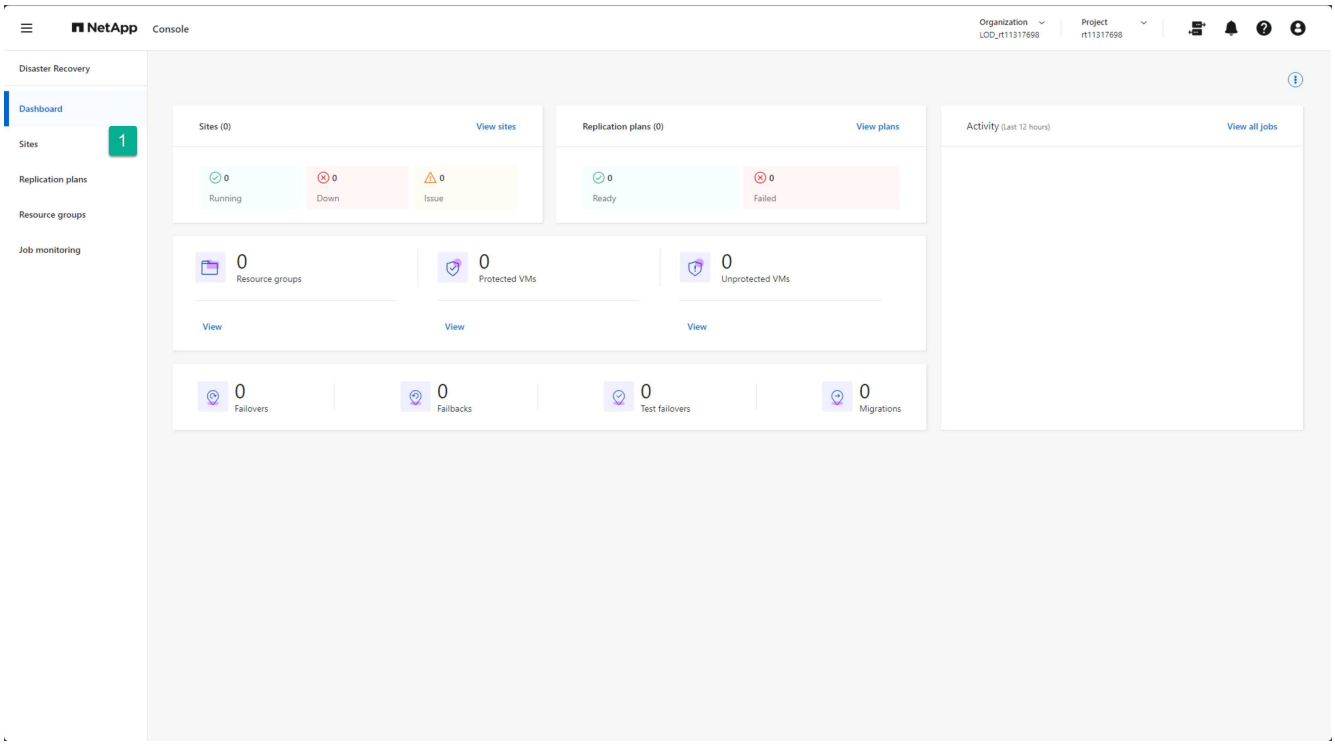


他に本番環境の vCenter サイトがある場合は、同じ手順で追加できます。

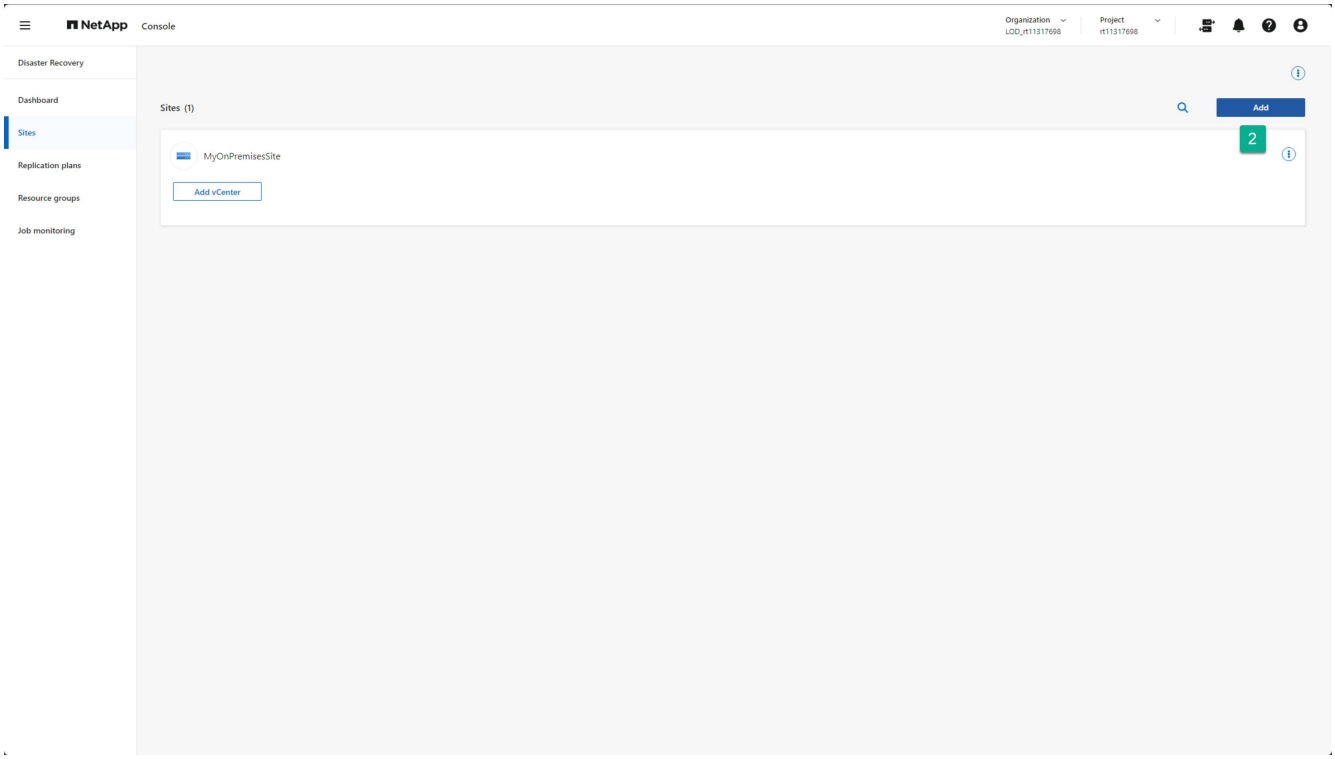
Amazonクラウドサイトを作成する

Amazon FSx for NetApp ONTAPストレージを使用して Amazon EVS の DR サイトを作成します。

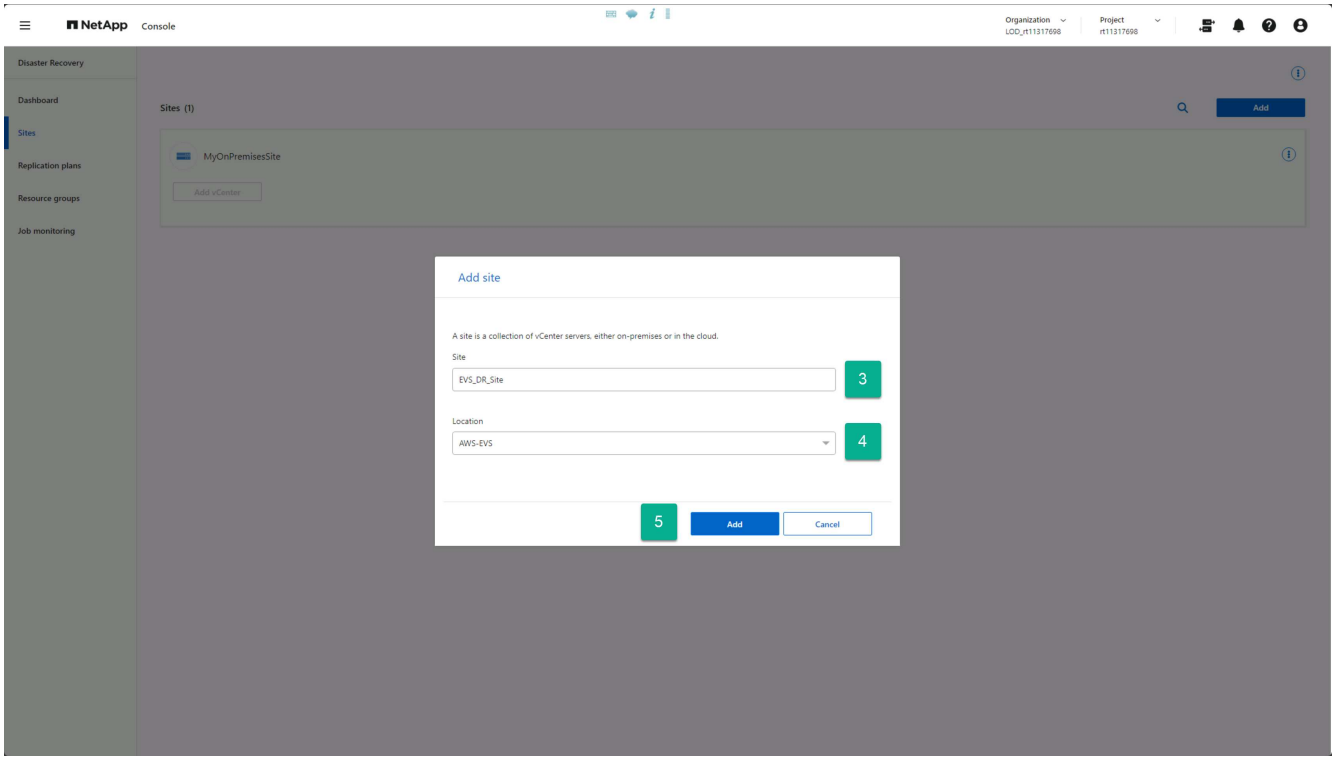
1. NetApp Disaster Recoveryの任意のページから、サイト オプションを選択します。



2. [サイト] オプションから [追加] を選択します。



3. [サイトの追加] ダイアログ ボックスで、サイト名を入力します。
4. 場所として「AWS-EVS」を選択します。
5. *追加*を選択します。



結果

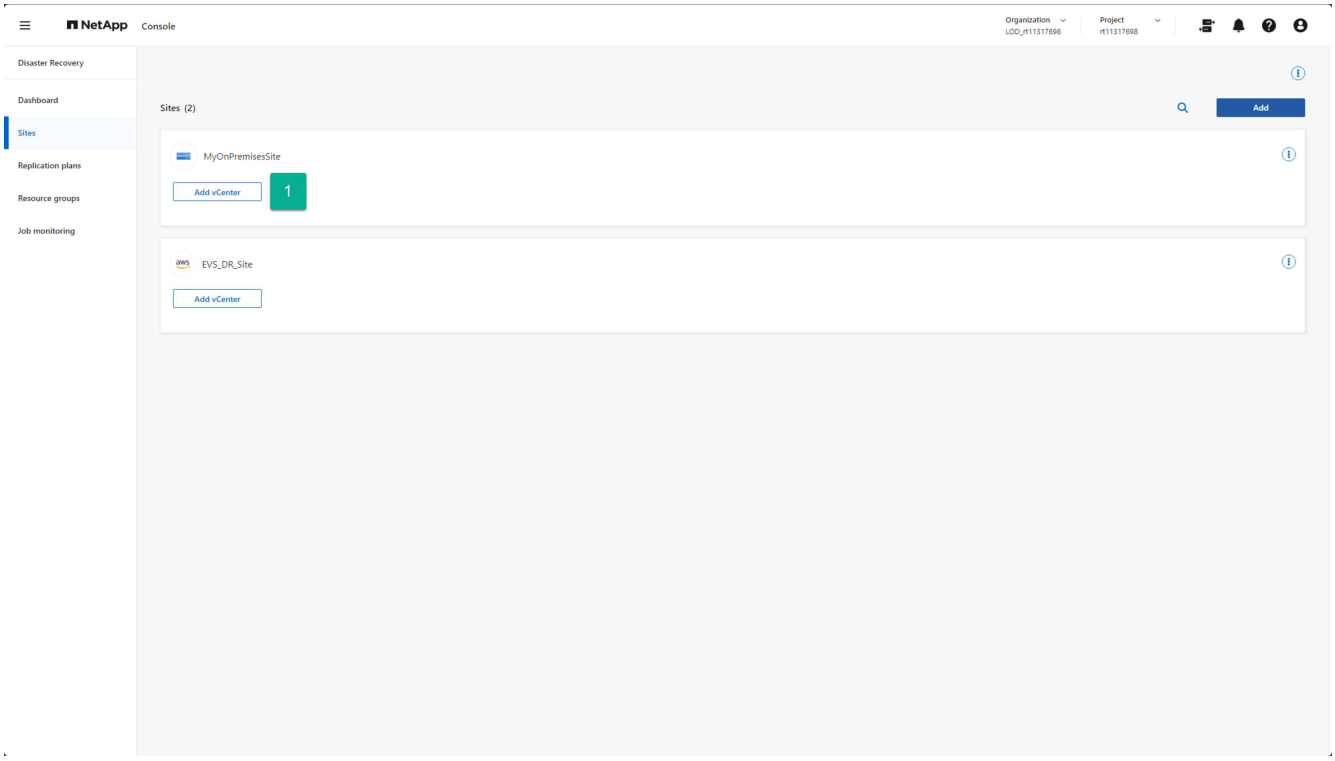
これで、本番 (ソース) サイトと DR (宛先) サイトが作成されました。

NetApp Disaster Recoveryにオンプレミスおよび Amazon EVS vCenter クラスターを追加する

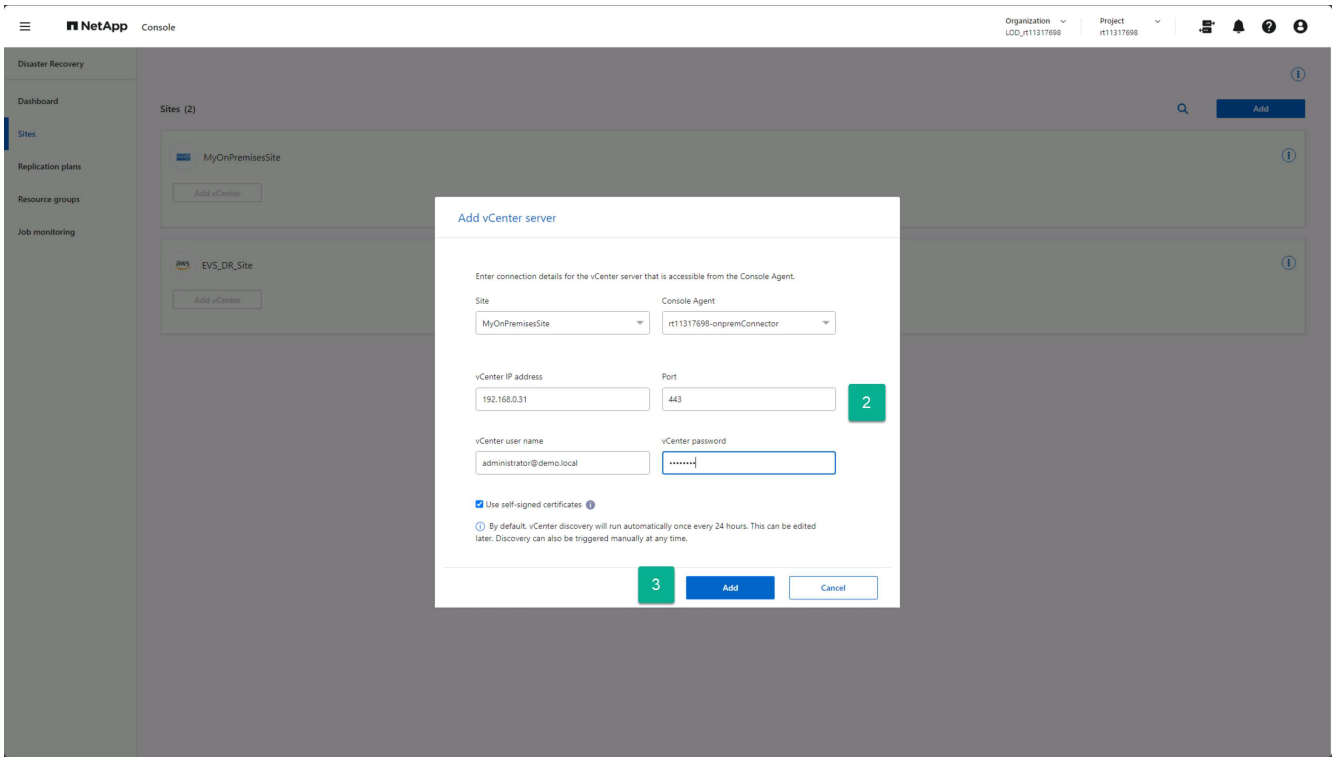
サイトが作成されたら、 NetApp Disaster Recoveryの各サイトに vCenter クラスターを追加します。各サイトを作成するときに、各サイトの種類を指定しました。これにより、 NetApp Disaster Recovery は、各サイト タイプでホストされている vCenter に必要なアクセス タイプを把握できるようになります。 Amazon EVS の利点の 1 つは、Amazon EVS vCenter とオンプレミスの vCenter の間に実質的な違いがないことです。どちらも同じ接続および認証情報が必要です。

各サイトに**vCenter**を追加する手順

1. サイト オプションから、必要なサイトの **vCenter** の追加 を選択します。



2. [vCenter サーバーの追加] ダイアログ ボックスで、次の情報を選択または入力します。
   a. AWS VPC 内でホストされるNetApp Consoleエージェント。
   b. 追加する vCenter の IP アドレスまたは FQDN。
   c. 異なる場合は、ポート値を vCenter クラスタ マネージャが使用する TCP ポートに変更します。
   d. 以前に作成したアカウントの vCenter ユーザー名。NetApp NetApp Disaster Recoveryが vCenter を管理するために使用します。
   e. 指定されたユーザー名の vCenter パスワード。
   f. 会社が外部の証明機関 (CA) または vCenter エンドポイント証明書ストアを使用して vCenter にアクセスする場合は、[自己署名証明書を使用する] チェックボックスをオフにします。それ以外の場合は、ボックスをオンのままにしておきます。
3. *追加*を選択します。



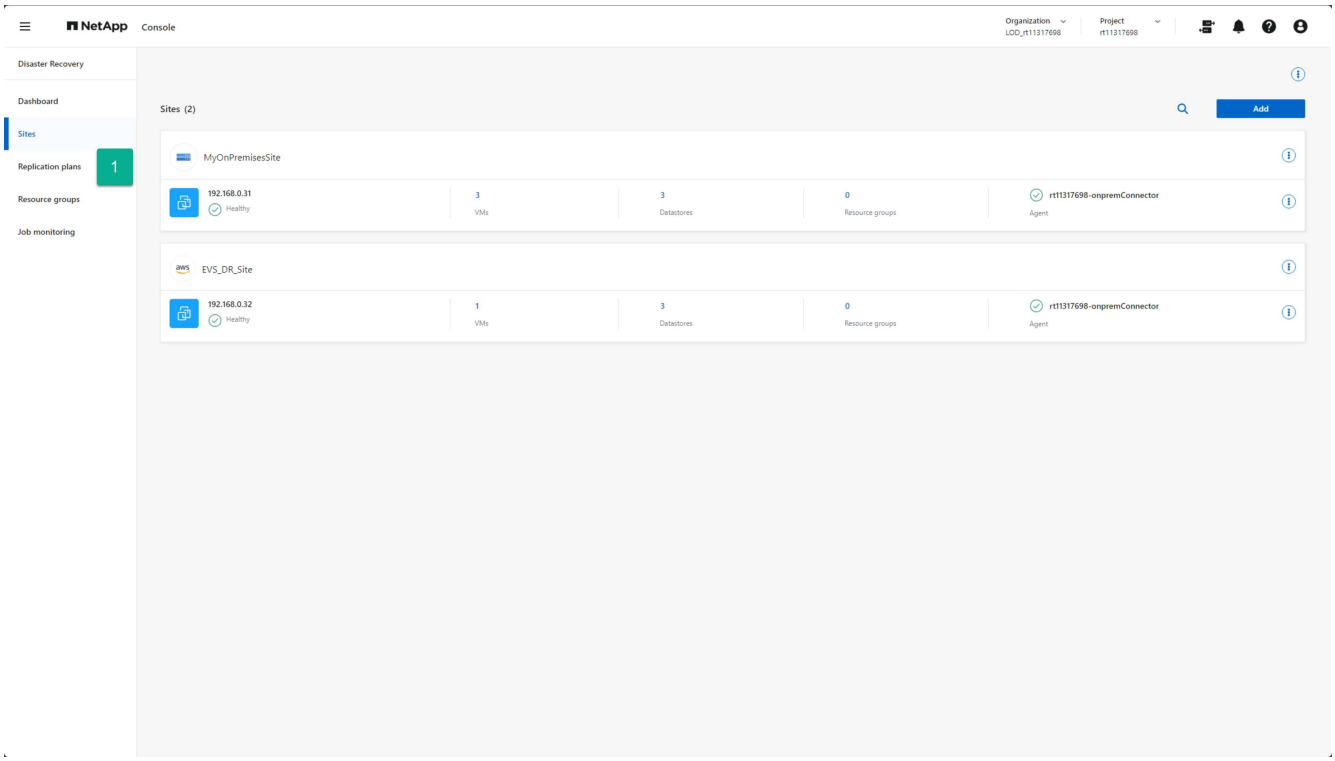
Amazon EVS のレプリケーション プランを作成する

NetApp Disaster Recoveryでレプリケーション プランを作成する方法の概要

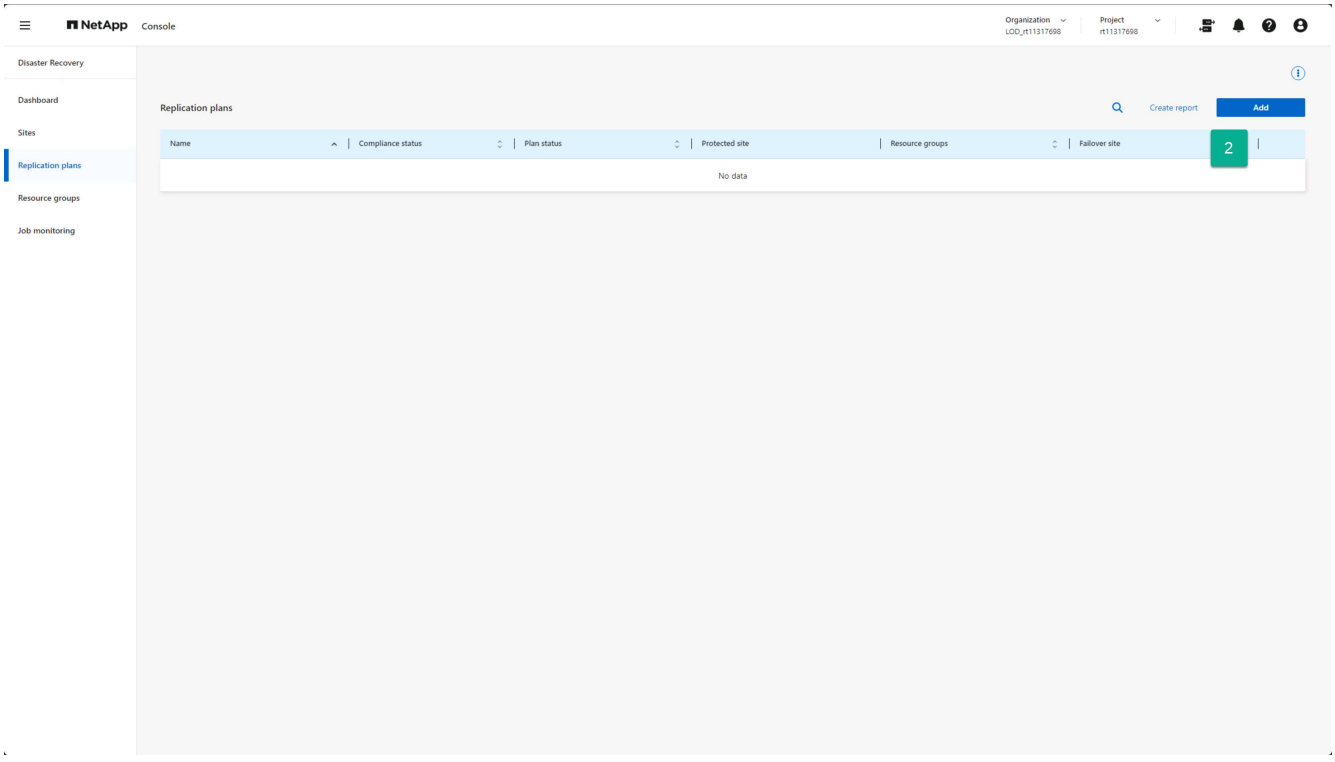
オンプレミスサイトで保護する vCenter があり、DR の宛先として使用できるAmazon FSx for NetApp ONTAPを使用するように設定された Amazon EVS サイトがある場合は、オンプレミスサイト内の vCenter クラスターでホストされている VM のセットを保護するためのレプリケーションプラン (RP) を作成できます。

レプリケーション プランの作成プロセスを開始するには:

1. 任意のNetApp Disaster Recovery画面から、レプリケーション プラン オプションを選択します。



2. レプリケーション プラン ページで、[追加] を選択します。



これにより、レプリケーション プランの作成ウィザードが開きます。

続ける"レプリケーションプラン作成ウィザード ステップ 1"。

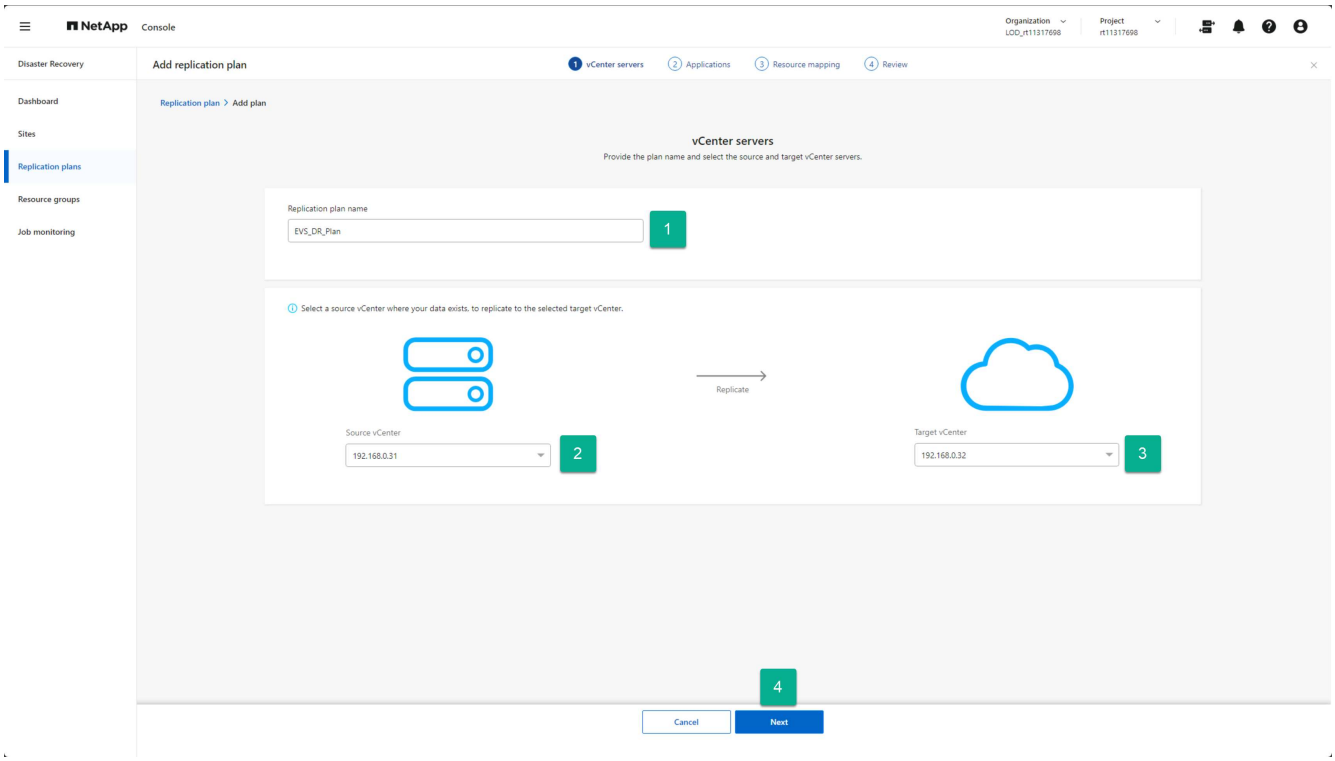
レプリケーションプランの作成: ステップ **1 - NetApp Disaster Recovery**で **vCenter** を選択する

まず、 NetApp Disaster Recoveryを使用して、レプリケーション プラン名を指定し、レプリケーションのソース vCenter とターゲット vCenter を選択します。

1. レプリケーション プランの一意の名前を入力します。

   レプリケーション プラン名には、英数字とアンダースコア (_) のみを使用できます。

2. ソース vCenter クラスタを選択します。
3. 宛先の vCenter クラスタを選択します。
4. *次へ*を選択します。



続ける"レプリケーションプラン作成ウィザード ステップ 2"。

レプリケーションプランの作成: ステップ **2 - NetApp Disaster Recovery**で **VM** リソースを選択する

NetApp Disaster Recoveryを使用して保護する仮想マシンを選択します。

保護する VM を選択する方法はいくつかあります。

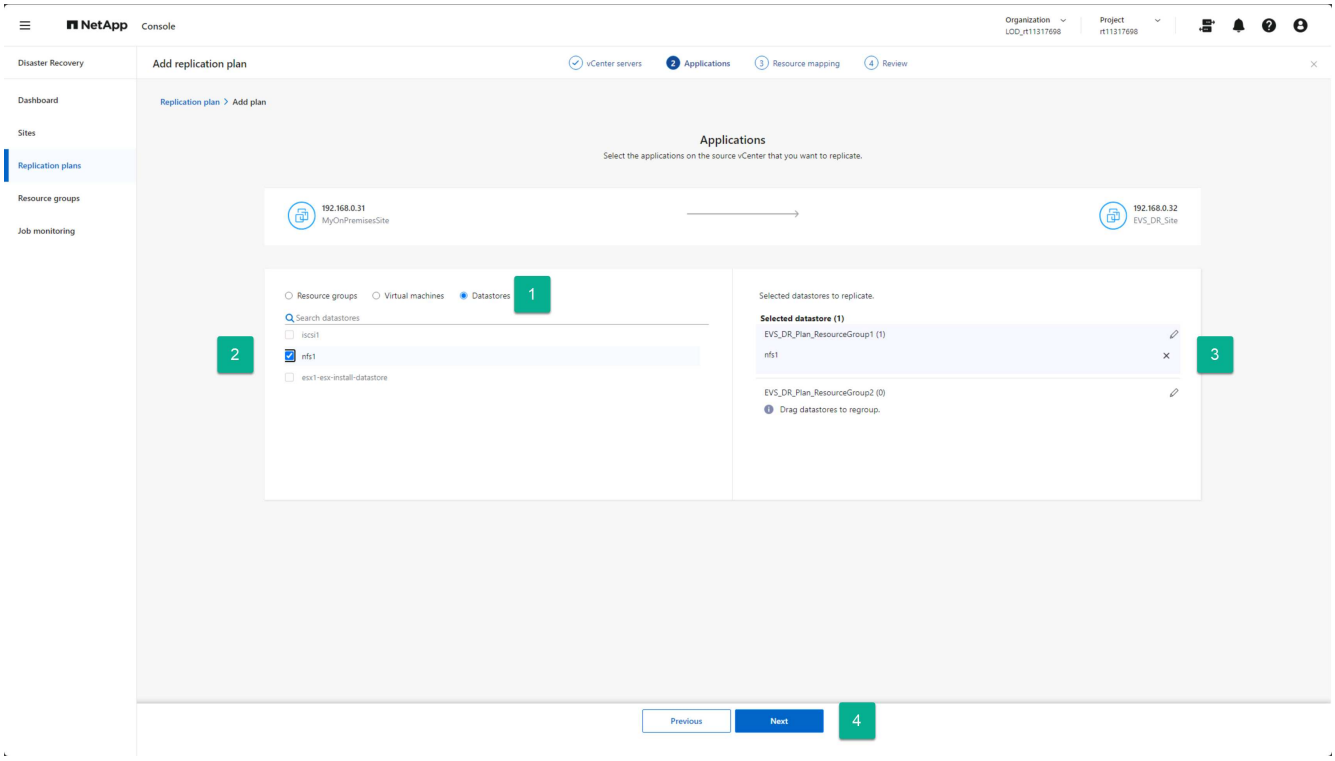
- 個々の **VM** を選択: 仮想マシン ボタンをクリックすると、保護する個々の VM を選択できます。各 VM を選択すると、サービスによって画面の右側にあるデフォルトのリソース グループに追加されます。
- 以前に作成したリソース グループを選択: NetApp Disaster Recoveryメニューの [リソース グループ] オプションを使用して、事前にカスタム リソース グループを作成できます。他の 2 つの方法を使用して、レプリケーション プラン プロセスの一部としてリソース グループを作成できるため、これは必須ではありません。詳細については、 "レプリケーションプランを作成する" 。

- **vCenter** データストア全体を選択: このレプリケーション プランで保護する VM が多数ある場合は、個々の VM を選択するのが効率的ではない可能性があります。 NetApp Disaster Recoveryボリュームベースのsnapmirrorレプリケーションを使用して VM を保護するため、データストアに存在するすべての VM がボリュームの一部として複製されます。ほとんどの場合、 NetApp Disaster Recovery を使用して、データストアにあるすべての VM を保護し、再起動する必要があります。このオプションを使用して、選択したデータストアでホストされているすべての VM を保護された VM のリストに追加するようにサービスに指示します。

このガイド付きの手順では、vCenter データストア全体を選択します。

このページにアクセスする手順

1. レプリケーション プラン ページから、アプリケーション セクションに進みます。
2. 開いた*アプリケーション*ページの情報を確認します。



データストアを選択する手順:

1. *データストア*を選択します。
2. 保護する各データストアの横にあるチェックボックスをオンにします。
3. (オプション) リソース グループ名の横にある鉛筆アイコンを選択して、リソース グループの名前を適切な名前に変更します。
4. *次へ*を選択します。

続ける"レプリケーションプラン作成ウィザード ステップ 3"。

レプリケーション プランの作成: ステップ **3 - NetApp Disaster Recovery**でリソースをマップする

NetApp Disaster Recoveryを使用して保護する VM のリストを作成したら、フェイルオーバー中に使用するフェイルオーバー マッピングと VM 構成情報を指定します。

主に次の 4 種類の情報をマッピングする必要があります。

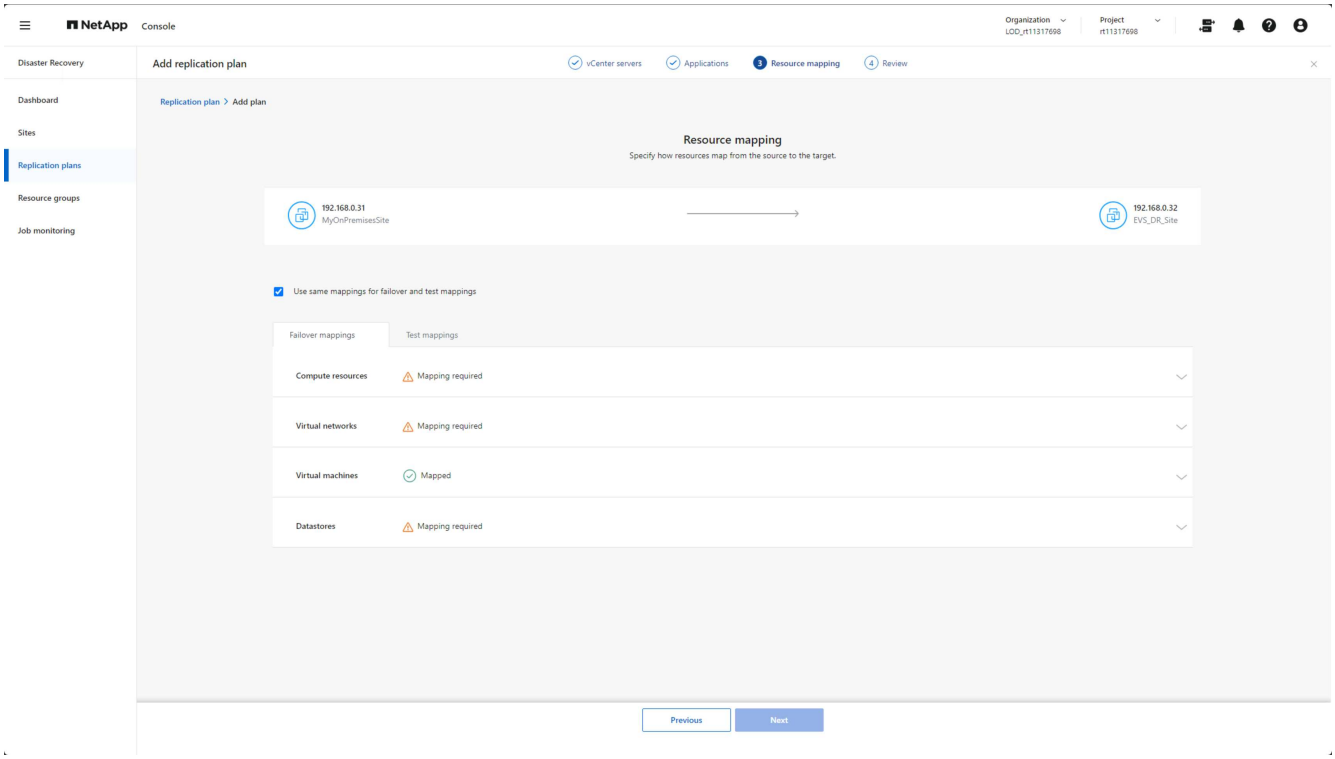
- コンピューティングリソース
- 仮想ネットワーク
- VM再設定
- データストアのマッピング

各 VM には最初の 3 種類の情報が必要です。保護する VM をホストする各データストアには、データストアマッピングが必要です。

- 注意アイコン（) では、マッピング情報を提供する必要があります。
- チェックアイコン（) はマッピングされているか、デフォルトのマッピングがあります。これらを確認して、現在の構成が要件を満たしていることを確認してください。

このページにアクセスする手順

1. レプリケーション プラン ページから、リソース マッピング セクションに進みます。
2. 開いた*リソース マッピング* ページの情報を確認します。



3. 必要なマッピングの各カテゴリを開くには、セクションの横にある下矢印 (**v**) を選択します。

コンピューティングリソースのマッピング

サイトは複数の仮想データセンターと複数の vCenter クラスターをホストする可能性があるため、フェイルオーバーが発生した場合に VM を回復する vCenter クラスターを特定する必要があります。

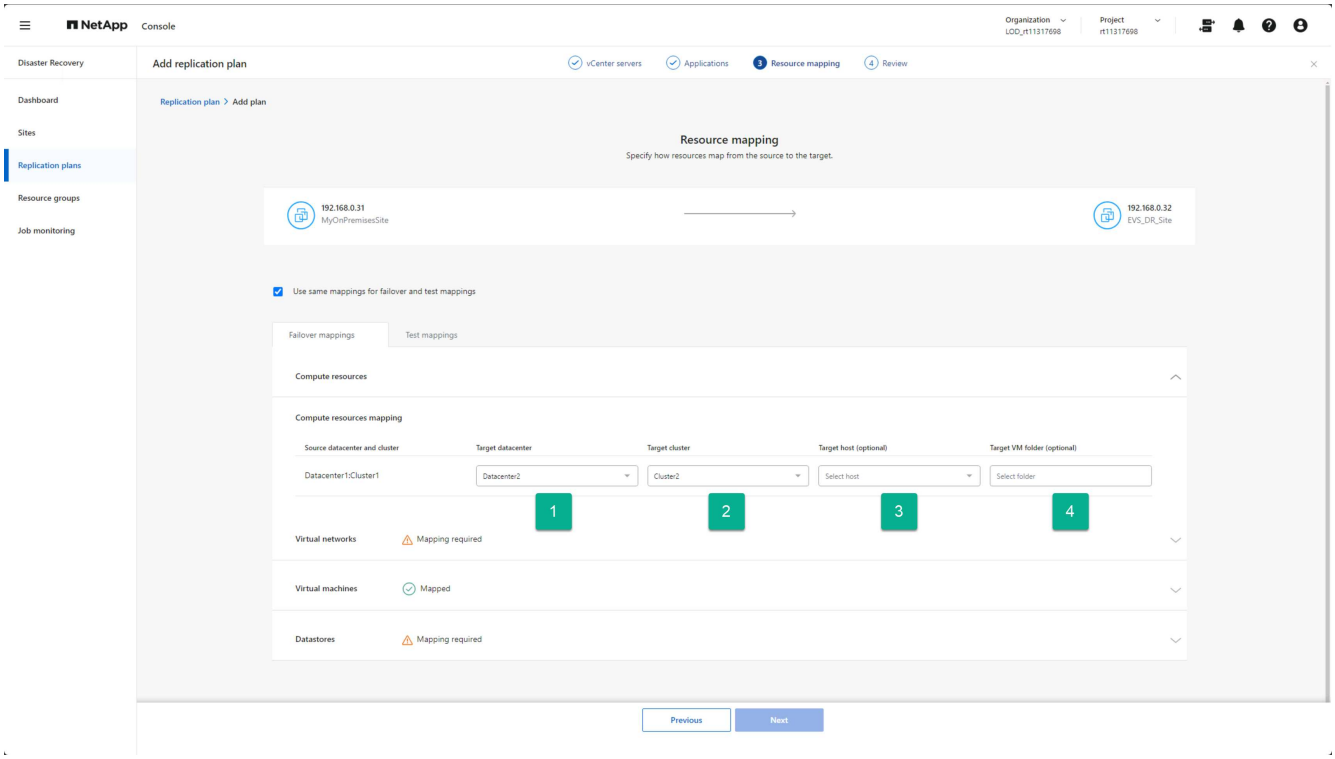
コンピューティングリソースをマッピングする手順

1. DR サイトにあるデータセンターのリストから仮想データセンターを選択します。
2. 選択した仮想データセンター内のクラスターのリストから、データストアと VM をホストするクラスターを選択します。
3. (オプション) ターゲット クラスター内のターゲット ホストを選択します。

   NetApp Disaster Recovery はvCenter でクラスタに追加された最初のホストを選択するため、この手順は必要ありません。その時点で、VM はその ESXi ホスト上で引き続き実行されるか、VMware DRS は構成された DRS ルールに基づいて必要に応じて VM を別の ESXi ホストに移動します。

4. (オプション) VM 登録を配置する最上位の vCenter フォルダの名前を指定します。

   これは組織のニーズを満たすものであり、必須ではありません。

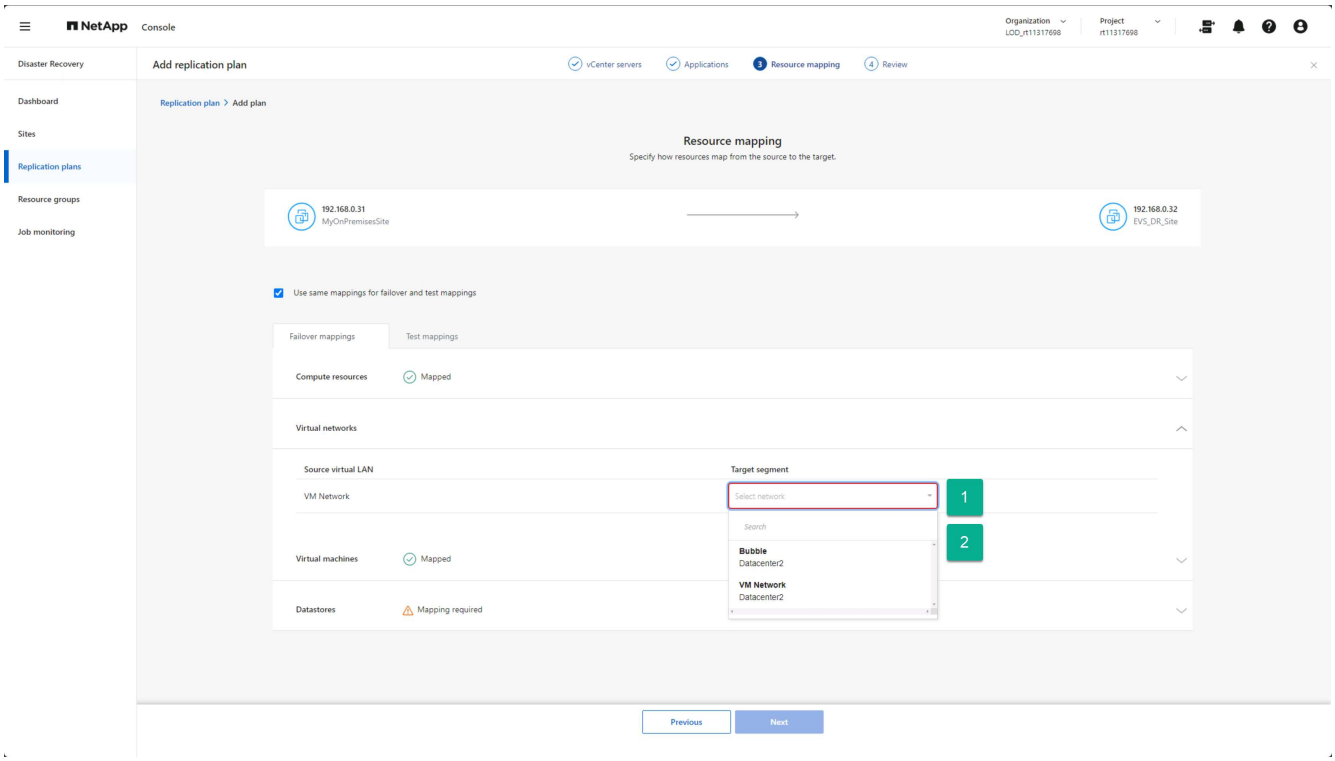


仮想ネットワークリソースをマップする

各 VM には、vCenter ネットワーク インフラストラクチャ内の仮想ネットワークに接続された 1 つ以上の仮想 NIC を設定できます。 DR サイトでの再起動時に各 VM が目的のネットワークに正しく接続されるようにするには、これらの VM を接続する DR サイトの仮想ネットワークを特定します。これを行うには、オンプレミス サイトの各仮想ネットワークを DR サイト上の関連ネットワークにマッピングします。

各ソース仮想ネットワークをマッピングする宛先仮想ネットワークを選択します

1. ドロップダウン リストからターゲット セグメントを選択します。
2. リストされているソース仮想ネットワークごとに前の手順を繰り返します。



フェイルオーバー中の**VM**再構成のオプションを定義する

各 VM は、DR vCenter サイトで正しく動作するために変更が必要になる場合があります。仮想マシンセクションでは、必要な変更を加えることができます。

デフォルトでは、 NetApp Disaster Recovery は、ソースのオンプレミス サイトで使用されているのと同じ設定を各 VM に使用します。これは、VM が同じ IP アドレス、仮想 CPU、および仮想 DRAM 構成を使用することを前提としています。

ネットワークの再構成

サポートされる IP アドレスの種類は、静的と DHCP です。静的 IP アドレスの場合、次のターゲット IP 設定があります。

- ソースと同じ: 名前が示すように、サービスはソース サイトの VM で使用されていたのと同じ IP アドレスを宛先 VM でも使用します。これには、前の手順でマップされた仮想ネットワークを同じサブネット設定で構成する必要があります。
- ソースと異なる: サービスは、前のセクションでマップした宛先仮想ネットワークで使用される適切なサブネットに対して構成する必要がある各 VM の IP アドレス フィールドのセットを提供します。各 VM に対して、IP アドレス、サブネット マスク、DNS、およびデフォルト ゲートウェイの値を指定する必要があります。必要に応じて、すべての VM に同じサブネット マスク、DNS、ゲートウェイ設定を使用して、すべての VM が同じサブネットに接続される場合のプロセスを簡素化します。
- サブネット マッピング: このオプションは、宛先仮想ネットワークの CIDR 構成に基づいて各 VM の IP アドレスを再構成します。この機能を使用するには、[サイト] ページの vCenter 情報で変更されたとおりに、各 vCenter の仮想ネットワークにサービス内で定義された CIDR 設定があることを確認します。

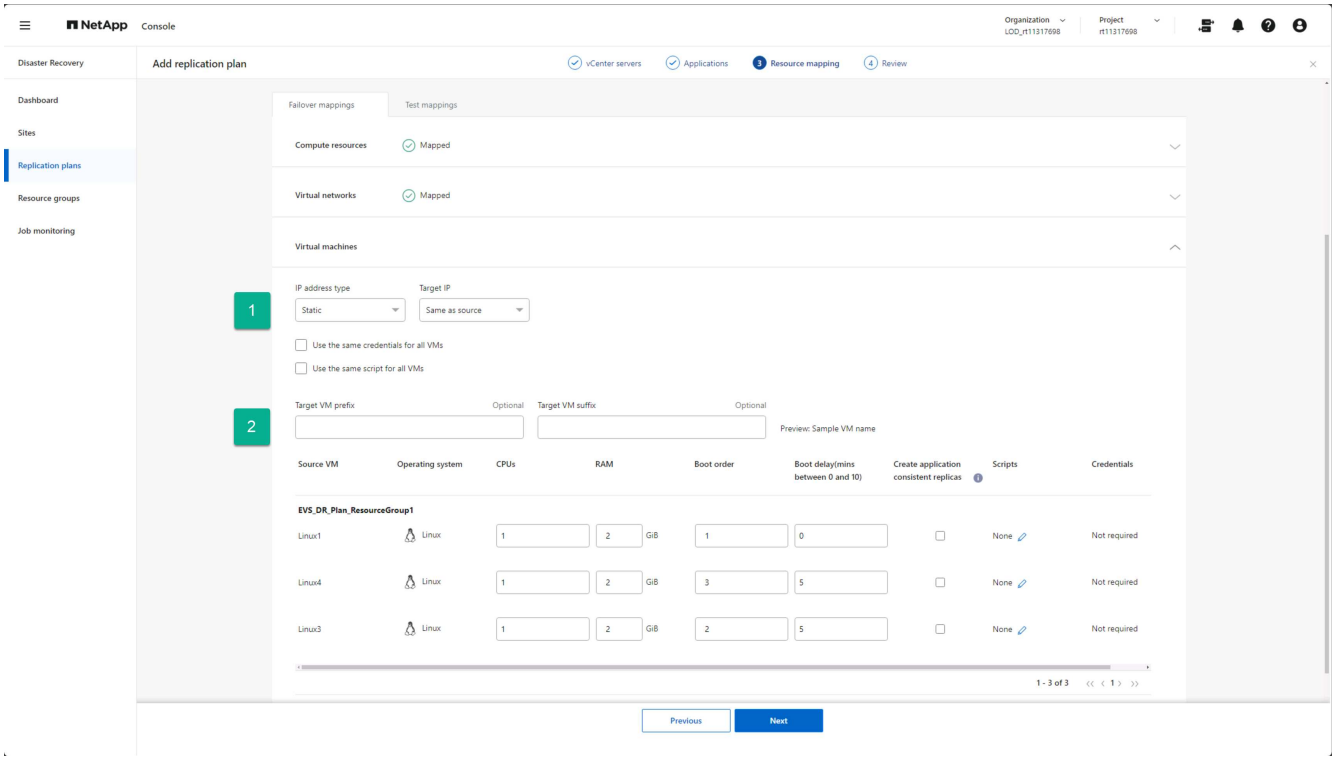
サブネットを構成すると、サブネット マッピングでは、ソース VM 構成と宛先 VM 構成の両方に IP アドレスの同じユニット コンポーネントが使用されますが、提供された CIDR 情報に基づいて IP アドレスのサブネット コンポーネントが置き換えられます。この機能を使用するには、送信元と宛先の仮想ネットワークの両方

が同じIPアドレスクラス（ /xx CIDR のコンポーネント)。これにより、保護されたすべての VM をホストするのに十分な IP アドレスが宛先サイトで使用可能になります。

この EVS セットアップでは、送信元と宛先の IP 構成が同じであり、追加の再構成は必要ないと想定しています。

ネットワーク設定の再構成を変更する

1. フェールオーバーされた VM に使用する IP アドレスの種類を選択します。
2. (オプション) オプションのプレフィックスとサフィックスの値を指定して、再起動された VM の VM 名変更スキームを指定します。

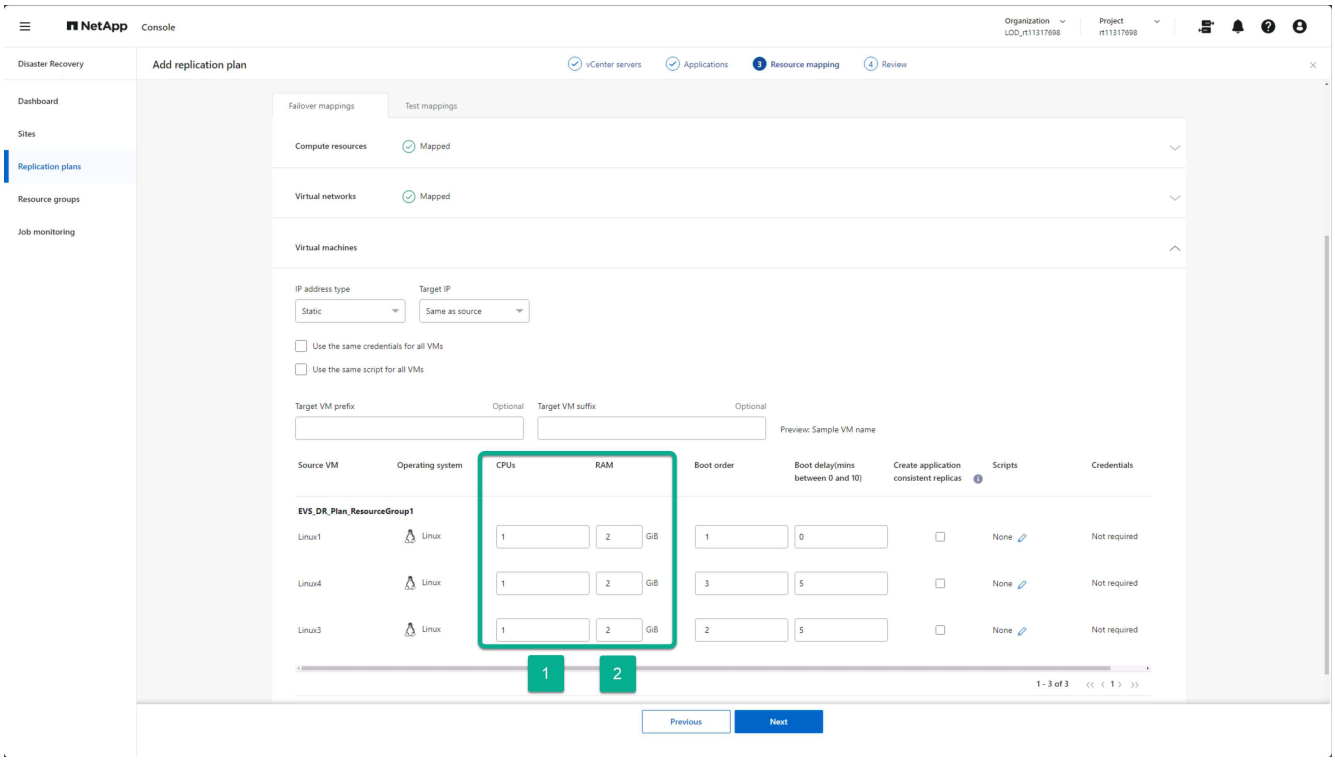


VMコンピューティングリソースの再構成

VM コンピューティング リソースを再構成するには、いくつかのオプションがあります。 NetApp Disaster Recovery は、仮想 CPU の数、仮想 DRAM の量、および VM 名の変更をサポートしています。

VM構成の変更を指定する

1. (オプション) 各 VM が使用する仮想 CPU の数を変更します。 DR vCenter クラスタ ホストにソース vCenter クラスタと同じ数の CPU コアがない場合、これが必要になることがあります。
2. (オプション) 各 VM が使用する仮想 DRAM の量を変更します。 DR vCenter クラスタ ホストにソース vCenter クラスタ ホストほどの物理 DRAM がない場合に、これが必要になることがあります。

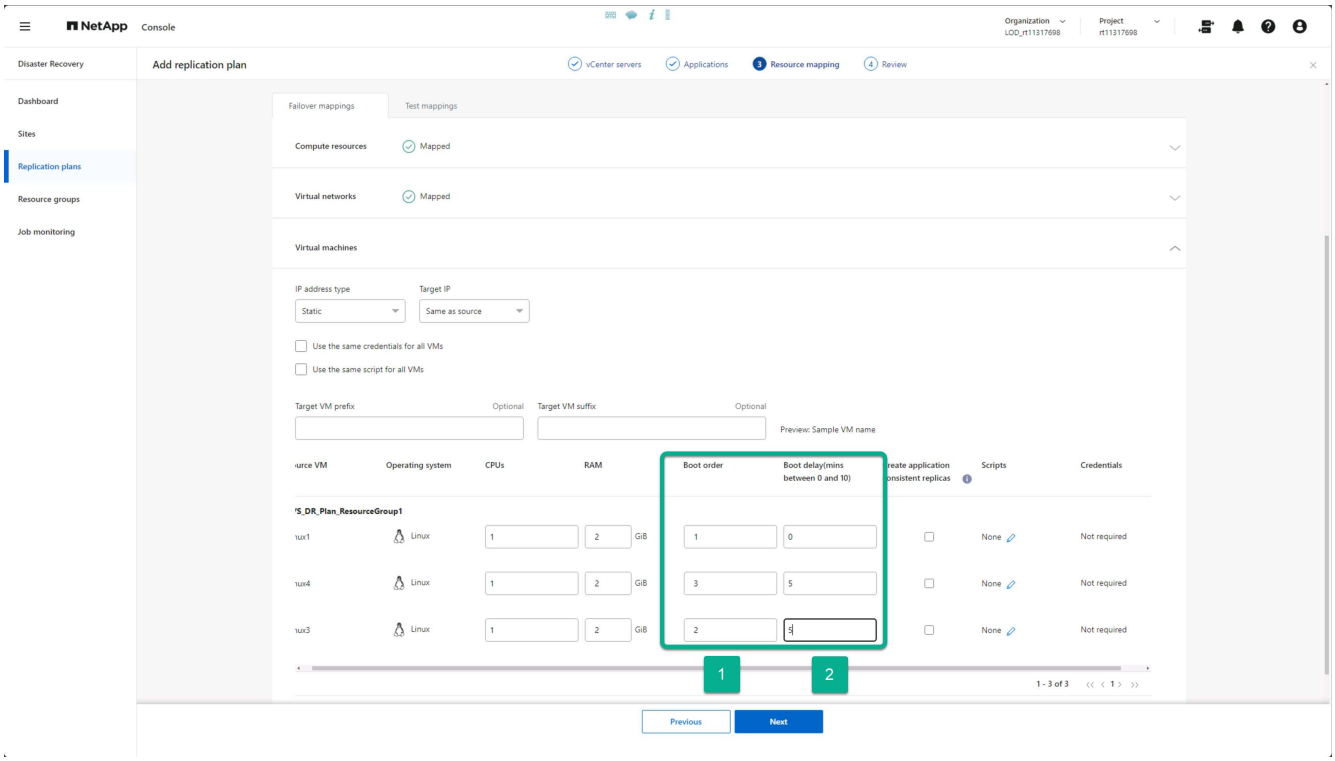


起動順序

NetApp Disaster Recovery は、ブート順序フィールドに基づいて VM の順序付けられた再起動をサポートします。ブート順序フィールドは、各リソース グループ内の VM の起動方法を示します。ブート順序フィールドに同じ値を持つ VM は並行して起動します。

起動順序設定を変更する

1. (オプション) VM を再起動する順序を変更します。このフィールドには任意の数値を指定できます。NetApp Disaster Recovery は、同じ数値を持つ VM を並列に再起動しようとします。
2. (オプション) 各 VM の再起動の間に使用する遅延を指定します。この VM の再起動が完了した後、次に高いブート順序番号を持つ VM の前に時間が挿入されます。この数値は分単位です。



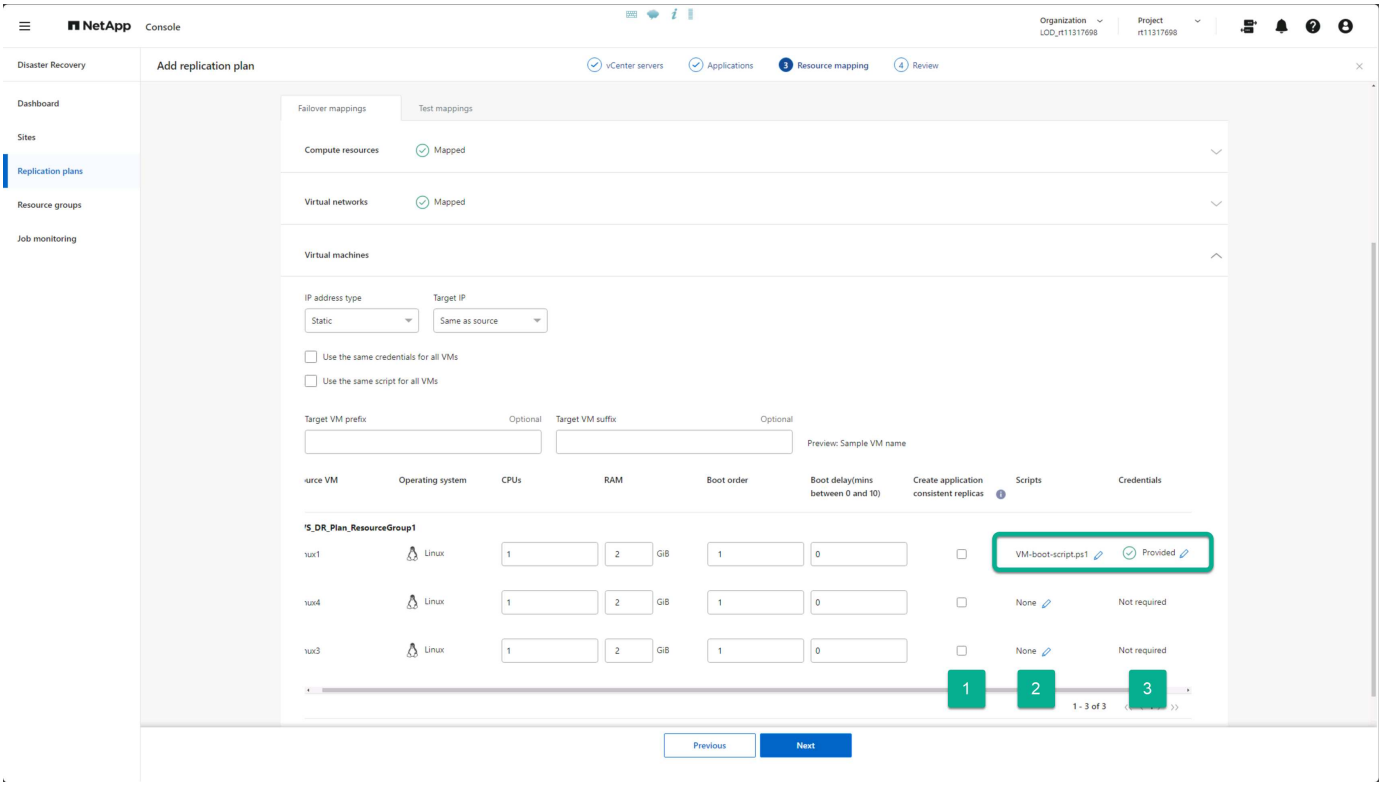
カスタムゲスト**OS**操作

NetApp Disaster Recovery は、各 VM に対していくつかのゲスト OS 操作の実行をサポートしています。

- NetApp Disaster Recovery は、 Oracle データベースおよび Microsoft SQL Server データベースを実行している VM のアプリケーション整合性のあるバックアップを取得できます。
- NetApp Disaster Recovery、各 VM のゲスト OS に適したカスタム定義のスクリプトを実行できます。このようなスクリプトを実行するには、スクリプトにリストされている操作を実行するための十分な権限を持ち、ゲスト OS が受け入れ可能なユーザー資格情報が必要です。

各**VM**のカスタムゲスト**OS**操作を変更する

1. (オプション) VM が Oracle または SQL Server データベースをホストしている場合は、[アプリケーション整合性レプリカを作成する] チェックボックスをオンにします。
2. (オプション) 起動プロセスの一部としてゲスト OS 内でカスタムアクションを実行するには、任意の VM のスクリプトをアップロードします。すべての VM で 1 つのスクリプトを実行するには、強調表示されたチェックボックスを使用してフィールドに入力します。
3. 特定の構成変更には、操作を実行するための適切な権限を持つユーザー資格情報が必要です。次の場合に資格情報を提供します。
    - スクリプトはゲスト OS によって VM 内で実行されます。
    - アプリケーション整合性スナップショットを実行する必要があります。



マップデータストア

レプリケーション プランを作成する最後の手順は、 ONTAP がデータストアを保護する方法を特定することです。これらの設定では、レプリケーション プランのリカバリ ポイント目標 (RPO)、維持するバックアップの数、各 vCenter データストアのホスティングONTAPボリュームをレプリケートする場所を定義します。

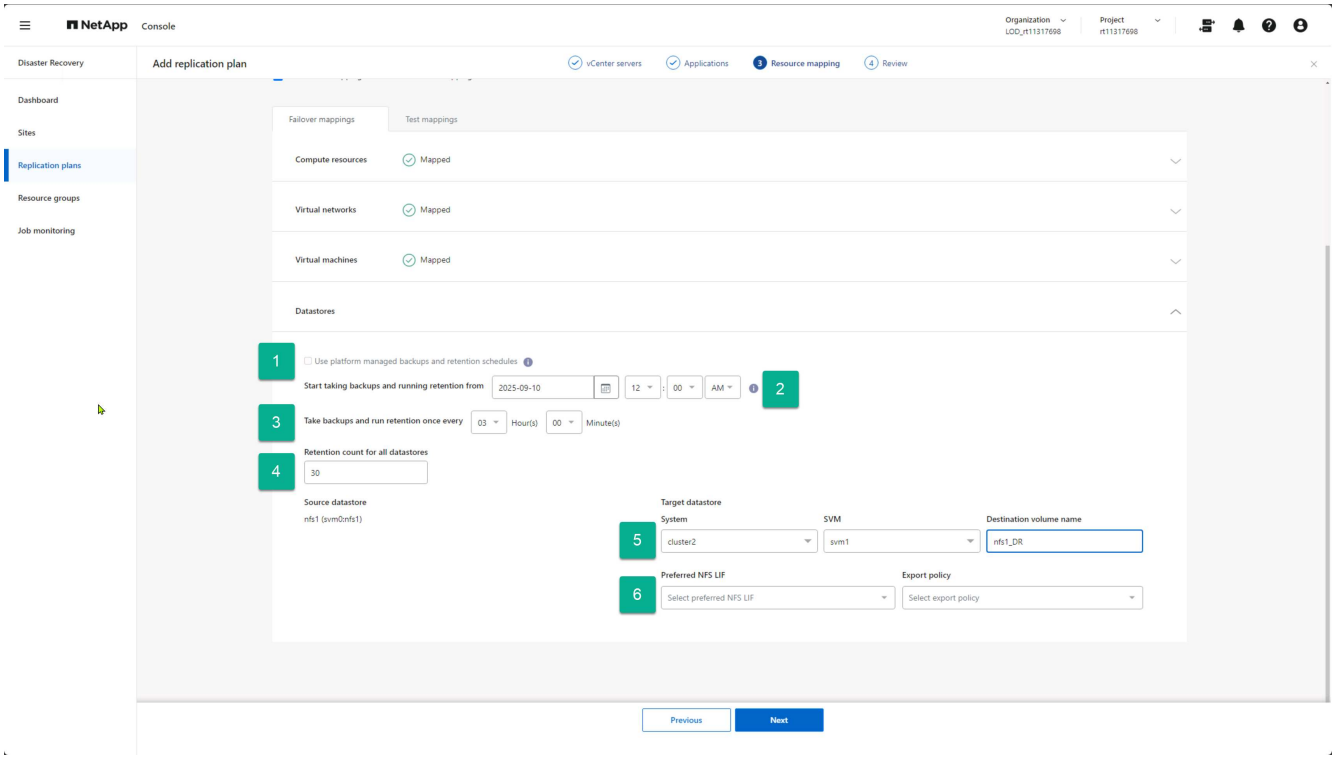
デフォルトでは、 NetApp Disaster Recovery は独自のスナップショット レプリケーション スケジュールを管理しますが、オプションで、データストアの保護に既存のSnapMirrorレプリケーション ポリシー スケジュールを使用するように指定できます。

さらに、オプションで、使用するデータ LIF (論理インターフェイス) とエクスポート ポリシーをカスタマイズすることもできます。これらの設定を指定しない場合、 NetApp Disaster Recovery は適切なプロトコル (NFS、iSCSI、または FC) に関連付けられているすべてのデータ LIF を使用し、NFS ボリュームのデフォルトのエクスポート ポリシーを使用します。

データストア（ボリューム）マッピングを構成するには

1. (オプション) 既存のONTAP SnapMirrorレプリケーション スケジュールを使用するか、 NetApp Disaster Recoveryで VM の保護を管理するか (デフォルト) を決定します。
2. サービスがバックアップを開始するタイミングの開始点を指定します。
3. サービスがバックアップを取得し、それを DR 宛先のAmazon FSx for NetApp ONTAPクラスターに複製する頻度を指定します。
4. 保持する履歴バックアップの数を指定します。このサービスは、ソース ストレージ クラスターと宛先ストレージ クラスターで同じ数のバックアップを維持します。
5. (オプション) 各ボリュームのデフォルトの論理インターフェイス (データ LIF) を選択します。何も選択しない場合は、ボリューム アクセス プロトコルをサポートする宛先 SVM 内のすべてのデータ LIF が設定されます。
6. (オプション) NFS ボリュームのエクスポート ポリシーを選択します。選択されていない場合は、デフォ

ルトのエクスポートポリシーが使用されます。



続ける"レプリケーションプラン作成ウィザード ステップ 4"。

レプリケーションプランの作成: ステップ**4 - NetApp Disaster Recovery**の設定を確認する

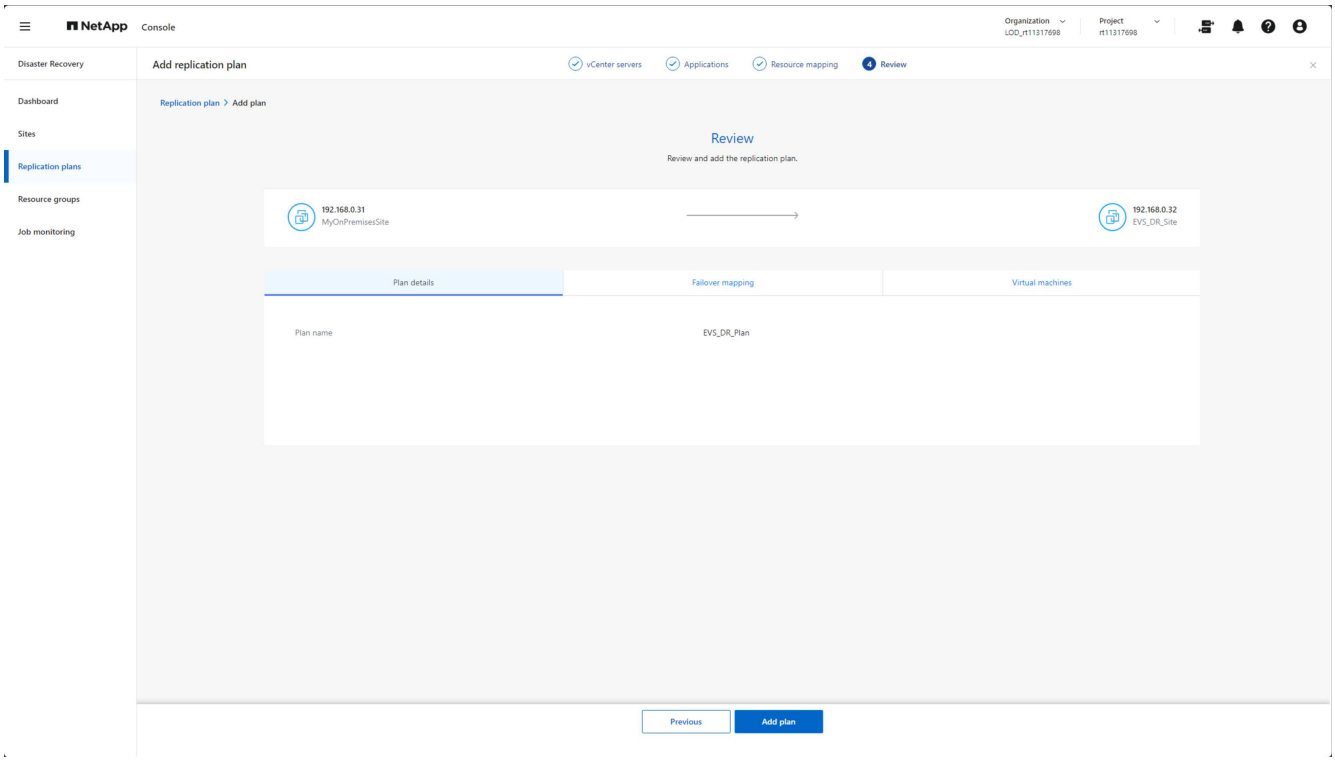
NetApp Disaster Recoveryでレプリケーション プラン情報を追加した後、入力した情報が正しいことを確認します。

手順

1. レプリケーション プランをアクティブ化する前に、[保存] を選択して設定を確認します。

   各タブを選択して設定を確認したり、鉛筆アイコンを選択して任意のタブで変更を加えたりすることができます。

   レプリケーションプラン設定の確認



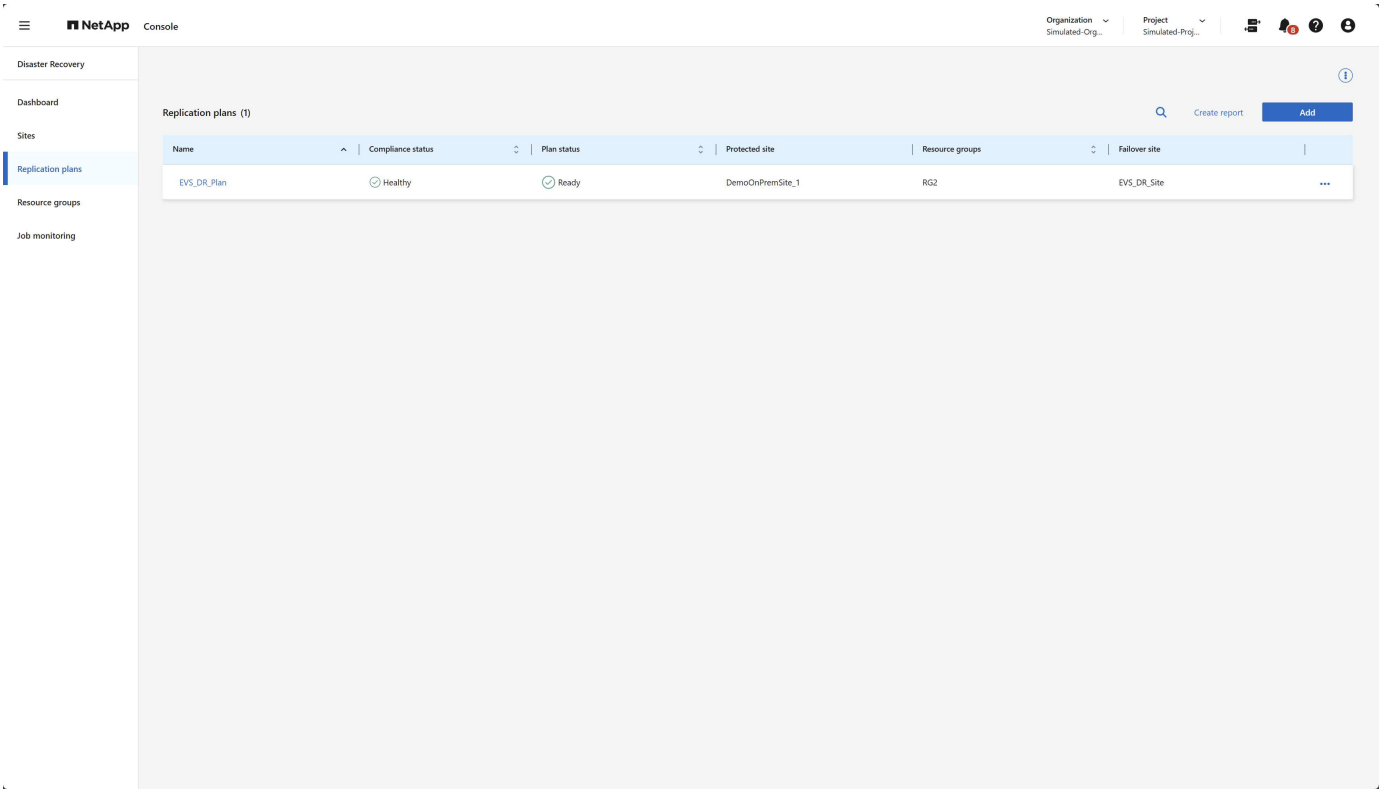
2. すべての設定が正しいことを確認したら、画面下部の*プランの追加*を選択します。

続ける"レプリケーションプランを確認する"。

NetApp Disaster Recoveryですべてが正常に動作していることを確認する

NetApp Disaster Recoveryでレプリケーション プランを追加したら、[レプリケーション プラン] ページに戻り、レプリケーション プランとそのステータスを確認できます。レプリケーション プランが 正常 な状態であることを確認する必要があります。そうでない場合は、続行する前にレプリケーション プランのステータスを確認し、問題を修正する必要があります。

図: レプリケーション プラン ペー
ジ



NetApp Disaster Recovery は、一連のテストを実行して、すべてのコンポーネント (ONTAPクラスタ、vCenter クラスタ、および VM) がアクセス可能であり、VM を保護するためのサービスが適切な状態にあることを確認します。これはコンプライアンス チェックと呼ばれ、定期的に実行されます。

レプリケーション プラン ページでは、次の情報を確認できます。

- 最後のコンプライアンスチェックのステータス
- レプリケーションプランのレプリケーション状態
- 保護された（ソース）サイトの名前
- レプリケーションプランによって保護されているリソースグループのリスト
- フェイルオーバー（宛先）サイトの名前

NetApp Disaster Recoveryを使用してレプリケーション プラン操作を実行する

NetApp Disaster Recovery をAmazon EVS およびAmazon FSx for NetApp ONTAPと併用して、フェイルオーバー、フェイルオーバーのテスト、リソースの更新、移行、今すぐスナップショットを作成する、レプリケーション プランの無効化/有効化、古いスナップショットのクリーンアップ、スナップショットの調整、レプリケーション プランの削除、スケジュールの編集などの操作を実行します。

フェイルオーバー

実行する必要がある主な操作は、決して起こらないことを願う操作、つまり、オンプレミスの運用サイトで壊滅的な障害が発生した場合に DR (宛先) データセンターにフェールオーバーすることです。

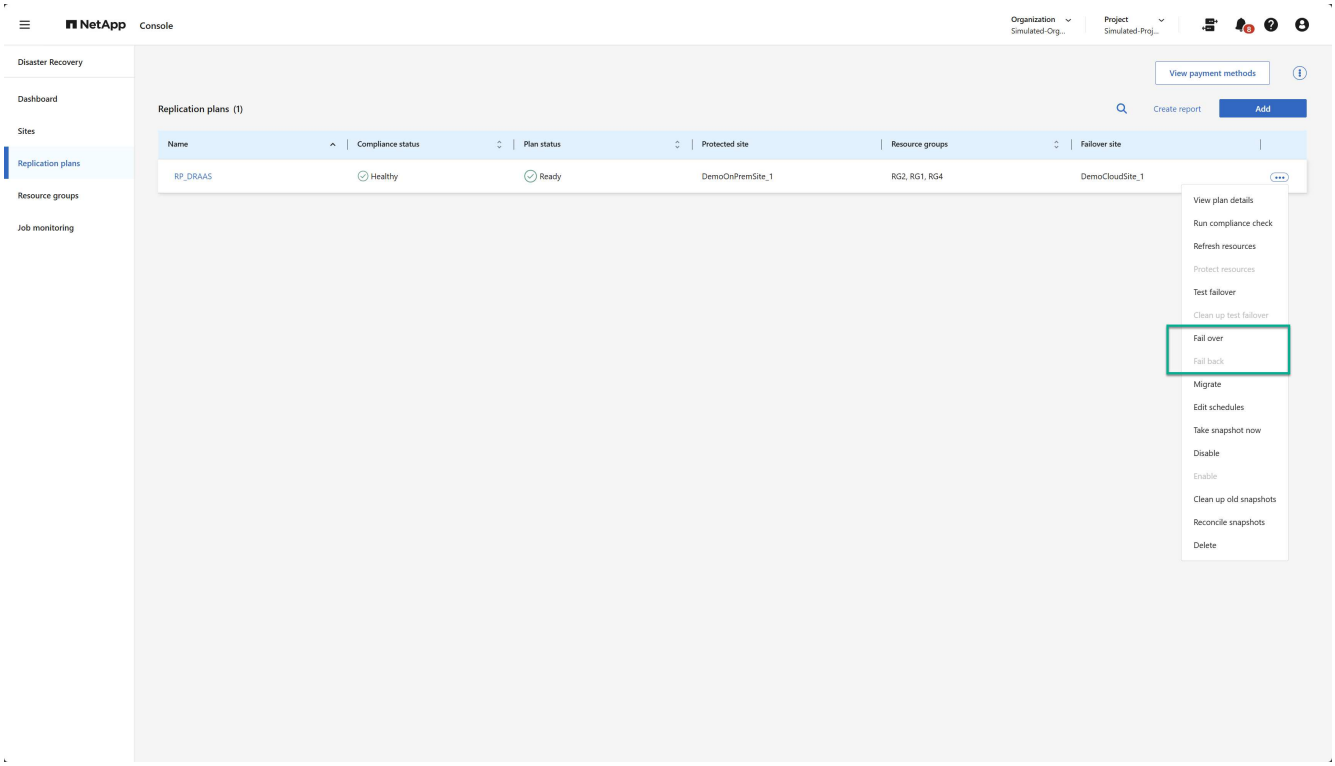
フェイルオーバーは手動で開始されるプロセスです。

フェイルオーバー操作にアクセスする手順

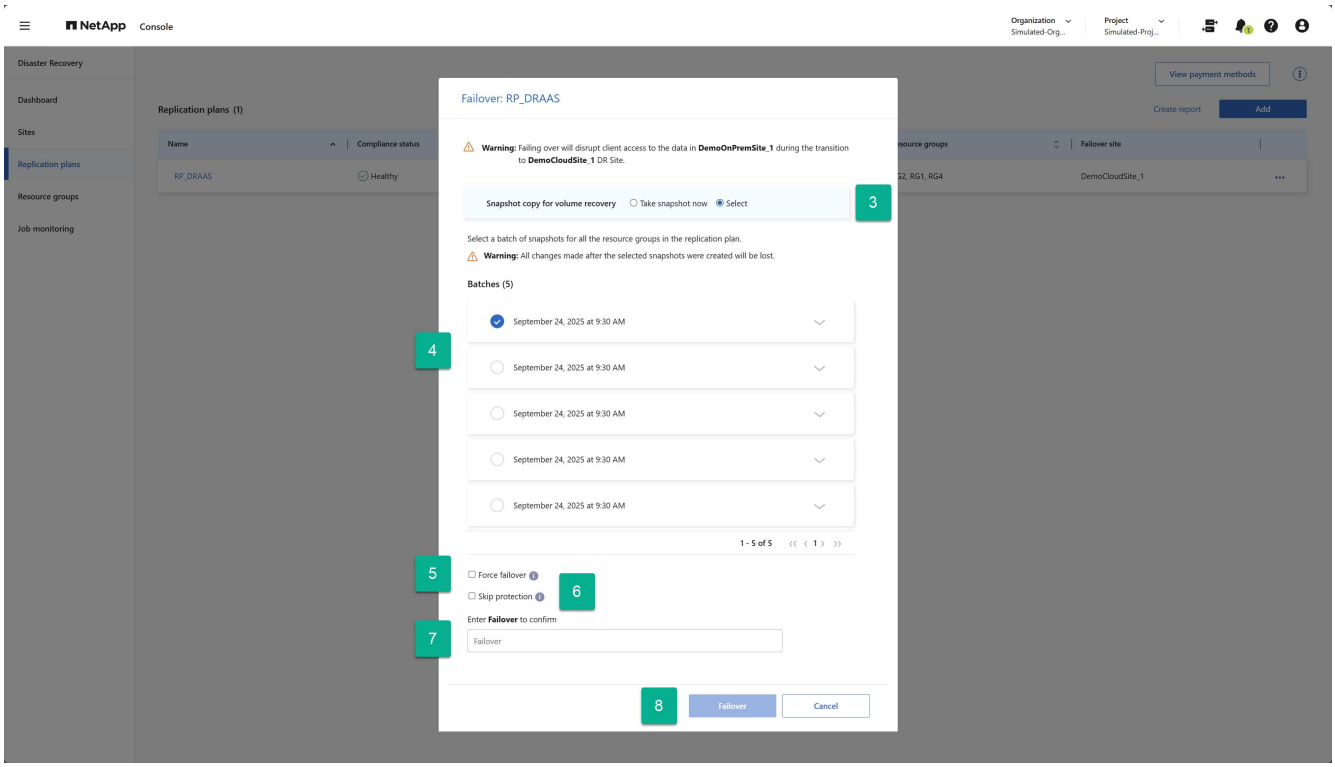
1. NetApp Consoleの左側のナビゲーション バーから、保護 > ディザスタ リカバリ を選択します。
2. NetApp Disaster Recoveryメニューから、レプリケーション プラン を選択します。

フェイルオーバーを実行する手順

1. レプリケーションプランページで、レプリケーションプランのアクションオプションを選択します。 ••• 。
2. *フェイルオーバー*を選択します。



3. 実稼働 (保護) サイトにアクセスできない場合は、以前に作成したスナップショットをリカバリ イメージとして選択します。これを行うには、[選択] を選択します。
4. リカバリに使用するバックアップを選択します。
5. (オプション) レプリケーション プランの状態に関係なく、 NetApp Disaster Recovery でフェイルオーバー プロセスを強制するかどうかを選択します。これは最後の手段としてのみ行う必要があります。
6. (オプション) 本番サイトが復旧された後に、 NetApp Disaster Recovery でリバース保護関係を自動的に作成するかどうかを選択します。
7. 続行することを確認するには、「Failover」という単語を入力します。
8. *フェイルオーバー*を選択します。



テストフェイルオーバー

テスト フェイルオーバーは、2 つの違いを除いてフェイルオーバーと似ています。

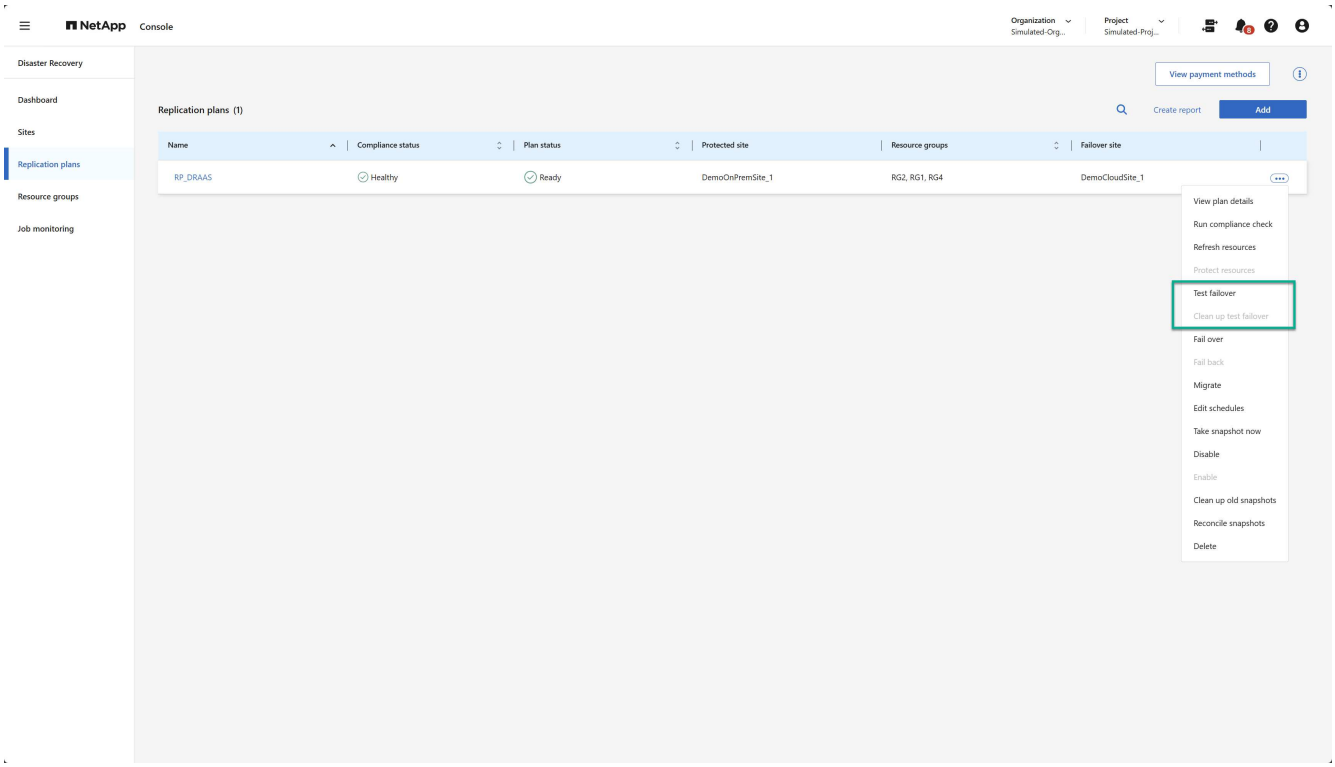
- 実稼働サイトは引き続きアクティブであり、すべての VM は引き続き期待どおりに動作しています。
- 実稼働 VM のNetApp Disaster Recovery保護は継続されます。

これは、宛先サイトでネイティブのONTAP FlexCloneボリュームを使用することで実現されます。テストフェイルオーバーの詳細については、以下を参照してください。"リモートサイトへのアプリケーションのフェイルオーバー | NetAppドキュメント" 。

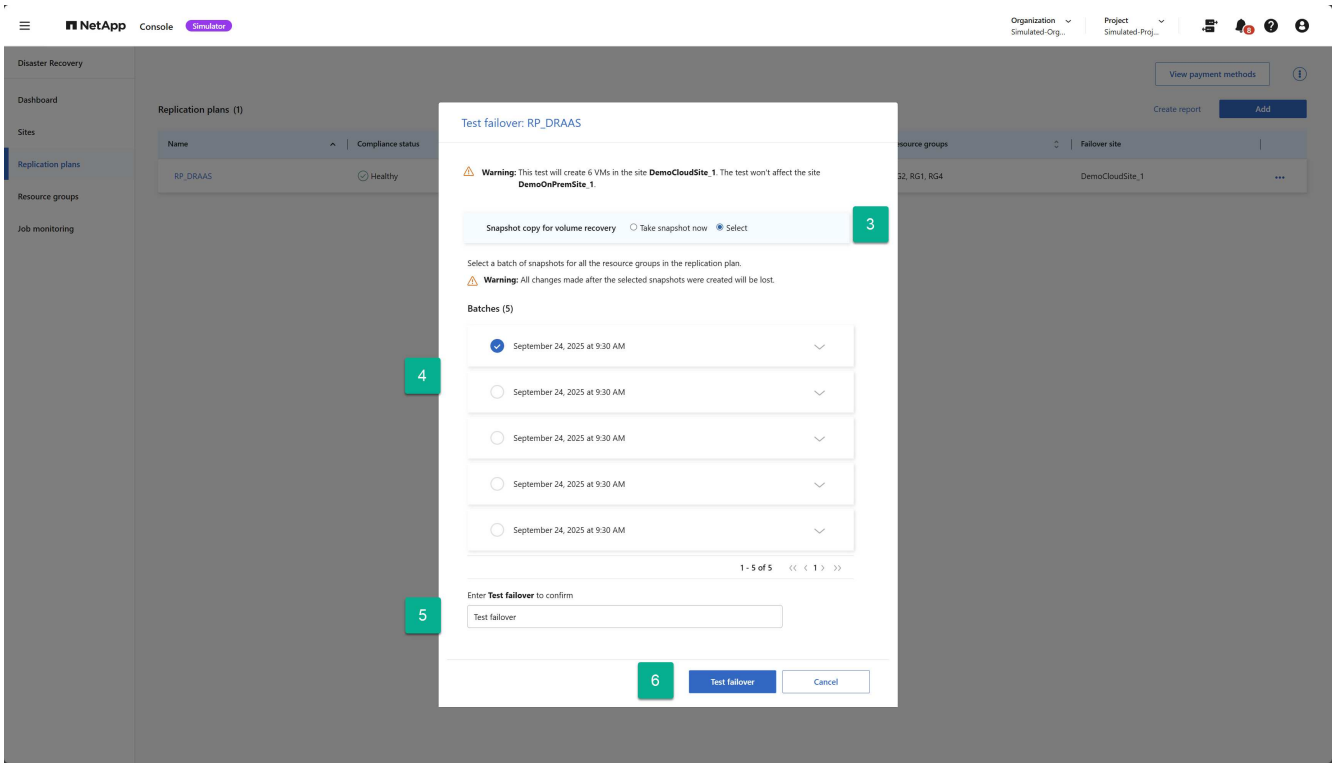
テスト フェイルオーバーを実行する手順は、レプリケーション プランのコンテキスト メニューの [テスト フェイルオーバー] 操作を使用することを除いて、実際のフェイルオーバーを実行する手順と同じです。

手順

1. レプリケーションプランのアクションオプションを選択します ••• 。
2. メニューから*フェイルオーバーのテスト*を選択します。



3. 本番環境の最新の状態を取得するか（今すぐスナップショットを取得する）、以前に作成したレプリケーション プランのバックアップを使用するか（選択）を決定します。
4. 以前に作成したバックアップを選択した場合は、復元に使用するバックアップを選択します。
5. 続行するかどうかを確認するには、「Test failwold」という単語を入力します。
6. *フェイルオーバーのテスト*を選択します。

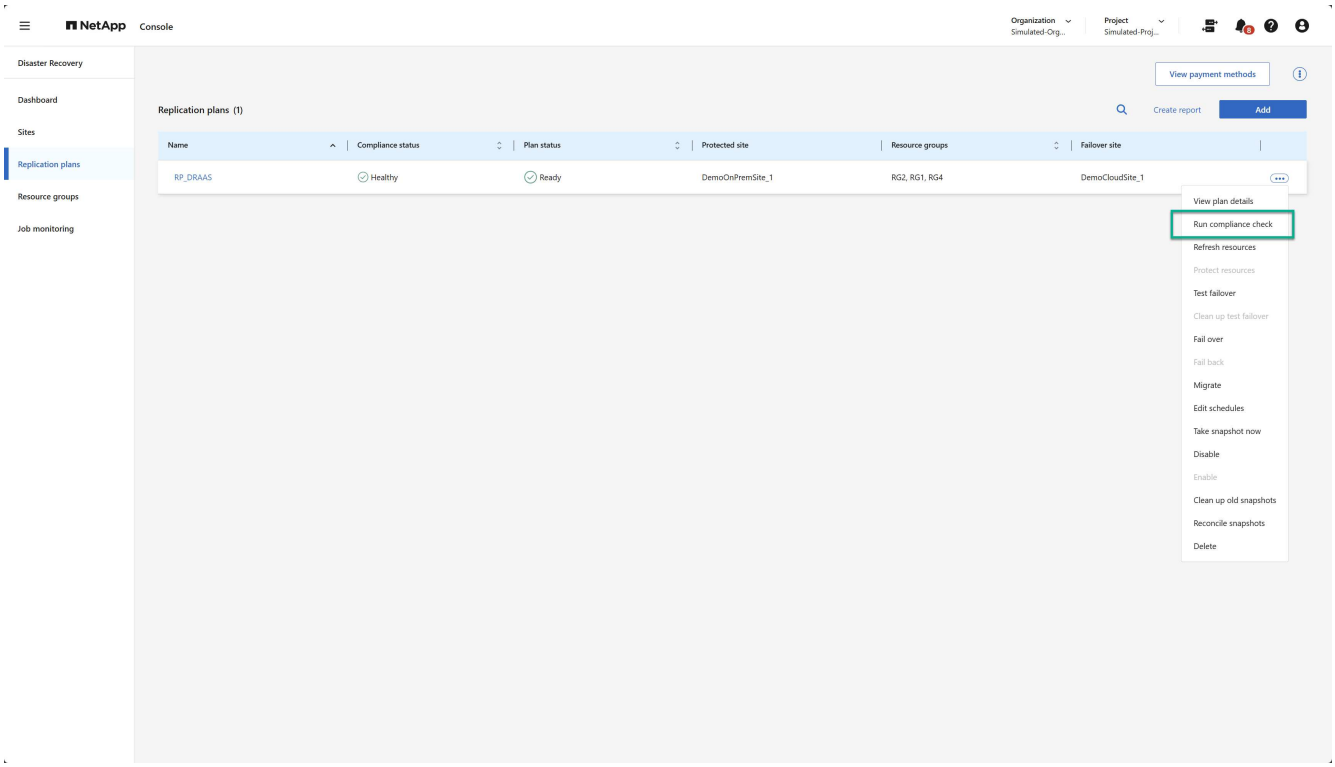


コンプライアンスチェックを実行する

コンプライアンス チェックは、デフォルトでは 3 時間ごとに実行されます。いつでも、コンプライアンス チェックを手動で実行する必要がある場合があります。

手順

1. *アクション*オプションを選択します ••• レプリケーション プランの横にあります。
2. レプリケーション プランの [アクション] メニューから [コンプライアンス チェックを実行] オプションを選択します。



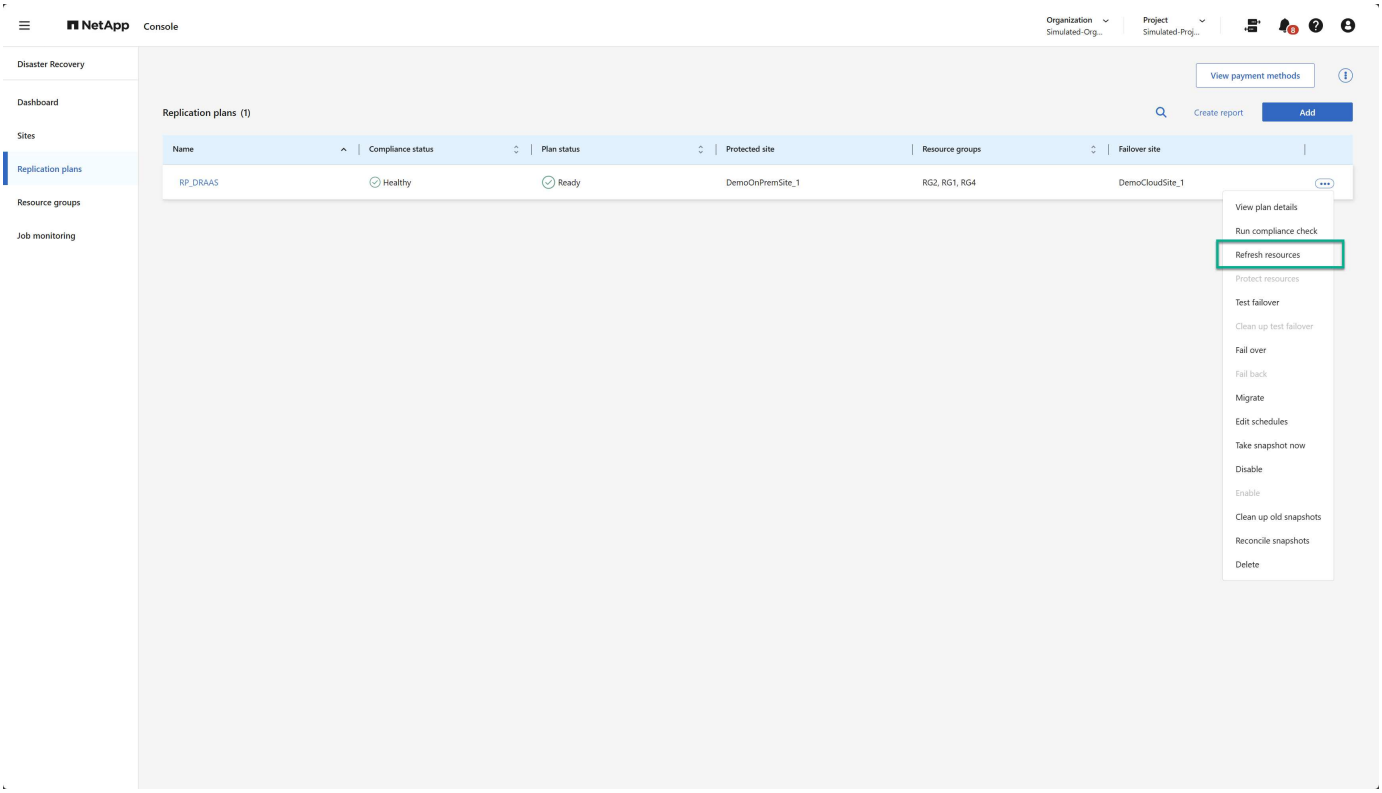
3. NetApp Disaster Recovery がコンプライアンス チェックを自動的に実行する頻度を変更するには、レプリケーション プランの [アクション] メニューから [スケジュールの編集] オプションを選択します。

リソースを更新する

VM の追加や削除、データストアの追加や削除、データストア間での VM の移動など、仮想インフラストラクチャに変更を加えるたびに、 NetApp Disaster Recoveryサービスで影響を受ける vCenter クラスターの更新を実行する必要があります。デフォルトでは、このサービスは 24 時間に 1 回これを自動的に実行しますが、手動で更新すると、最新の仮想インフラストラクチャ情報が利用可能になり、DR 保護に考慮されるようになります。

更新が必要となるケースは 2 つあります。

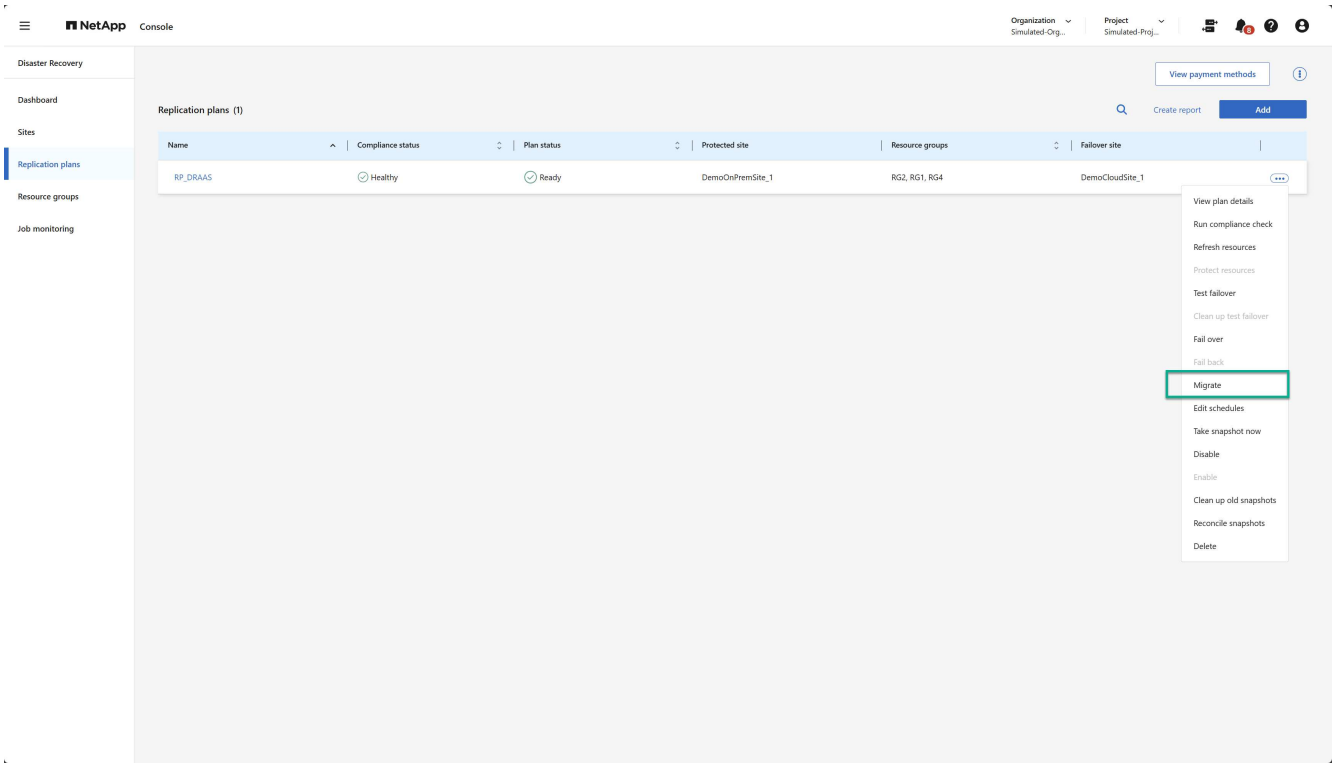
- vCenter の更新: vCenter クラスターに VM が追加、削除、または移動されるたびに、vCenter の更新を実行します。
- レプリケーション プランの更新: 同じソース vCenter クラスタ内のデータストア間で VM が移動されるたびに、レプリケーション プランの更新を実行します。



移行

NetApp Disaster Recovery は主に災害復旧のユースケースに使用されますが、VM セットをソース サイトから宛先サイトに 1 回だけ移動することもできます。これは、クラウド プロジェクトへの協調的な移行のため、または悪天候、政治的紛争、その他の潜在的な一時的な大惨事などの災害回避のために使用できます。

1. *アクション*オプションを選択します ••• レプリケーション プランの横にあります。
2. レプリケーション プラン内の VM を宛先の Amazon EVS クラスターに移動するには、レプリケーション プランの [アクション] メニューから [移行] を選択します。

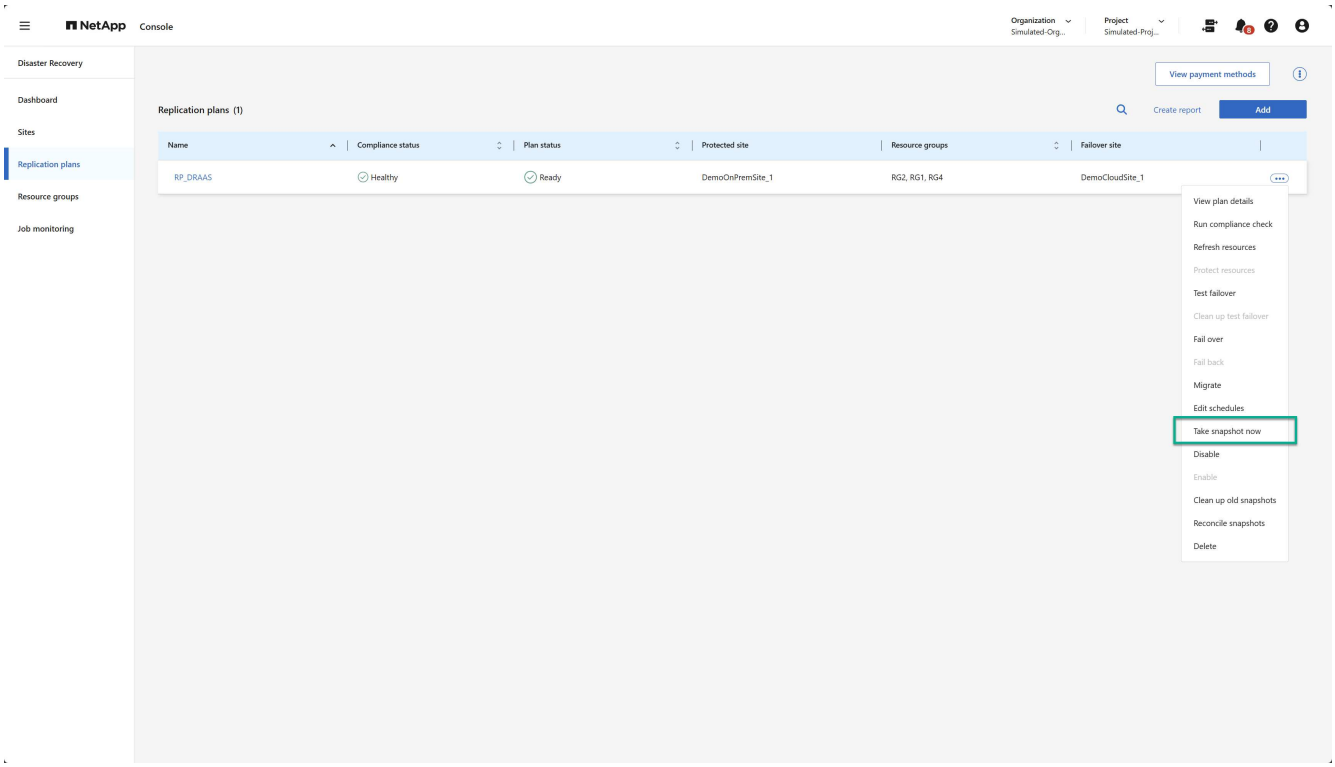


3. 移行ダイアログ ボックスに情報を入力します。

今すぐスナップショットを撮る

いつでも、レプリケーション プランの即時スナップショットを取得できます。このスナップショットは、レプリケーション プランのスナップショット保持数によって設定されるNetApp Disaster Recoveryの考慮事項に含まれます。

1. *アクション*オプションを選択します ••• レプリケーション プランの横にあります。
2. レプリケーション プランのリソースのスナップショットをすぐに取得するには、レプリケーション プランの [アクション] メニューで [今すぐスナップショットを取得] を選択します。

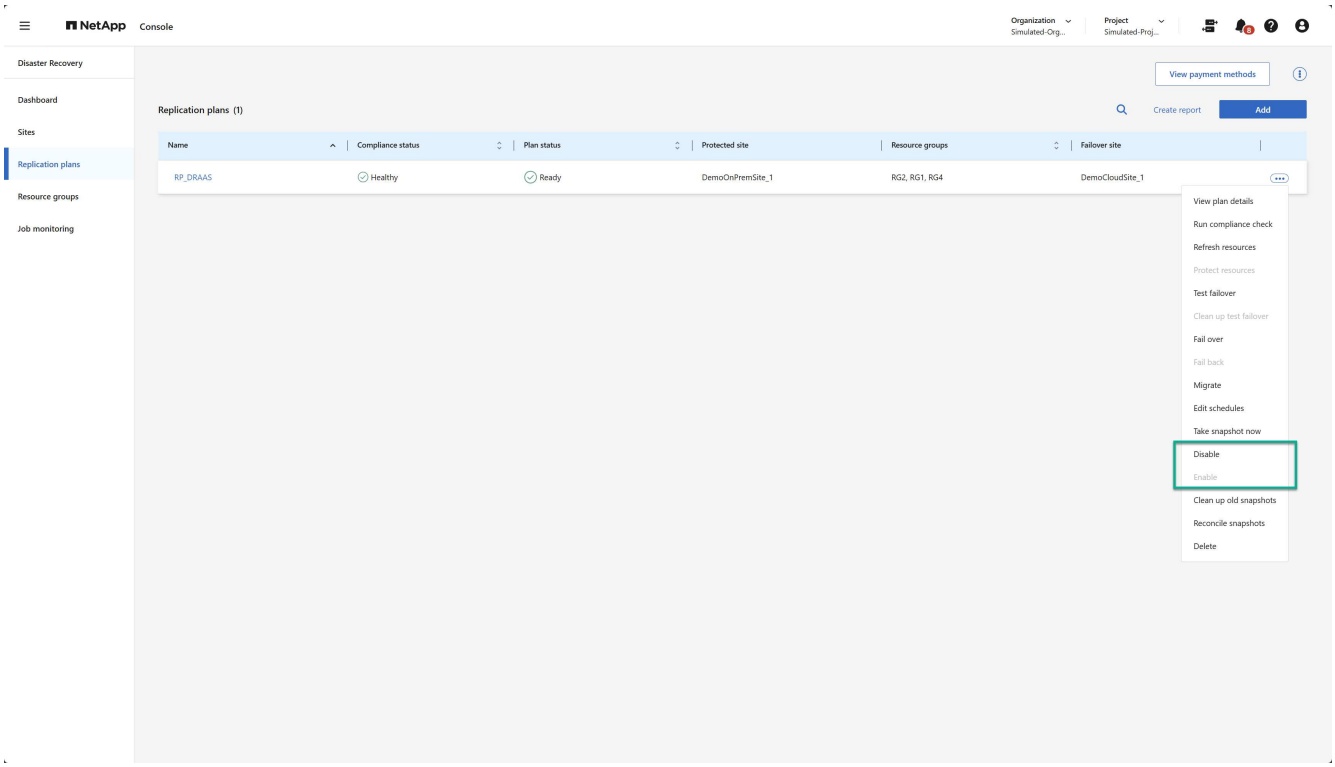


レプリケーションプランを無効または有効にする

レプリケーション プロセスに影響を及ぼす可能性のある操作やメンテナンスを実行するために、レプリケーション プランを一時的に停止する必要がある場合があります。このサービスは、レプリケーションを停止および開始する方法を提供します。

1. レプリケーションを一時的に停止するには、レプリケーション プランの [アクション] メニューで [無効] を選択します。
2. レプリケーションを再開するには、レプリケーション プランの [アクション] メニューで [有効] を選択します。

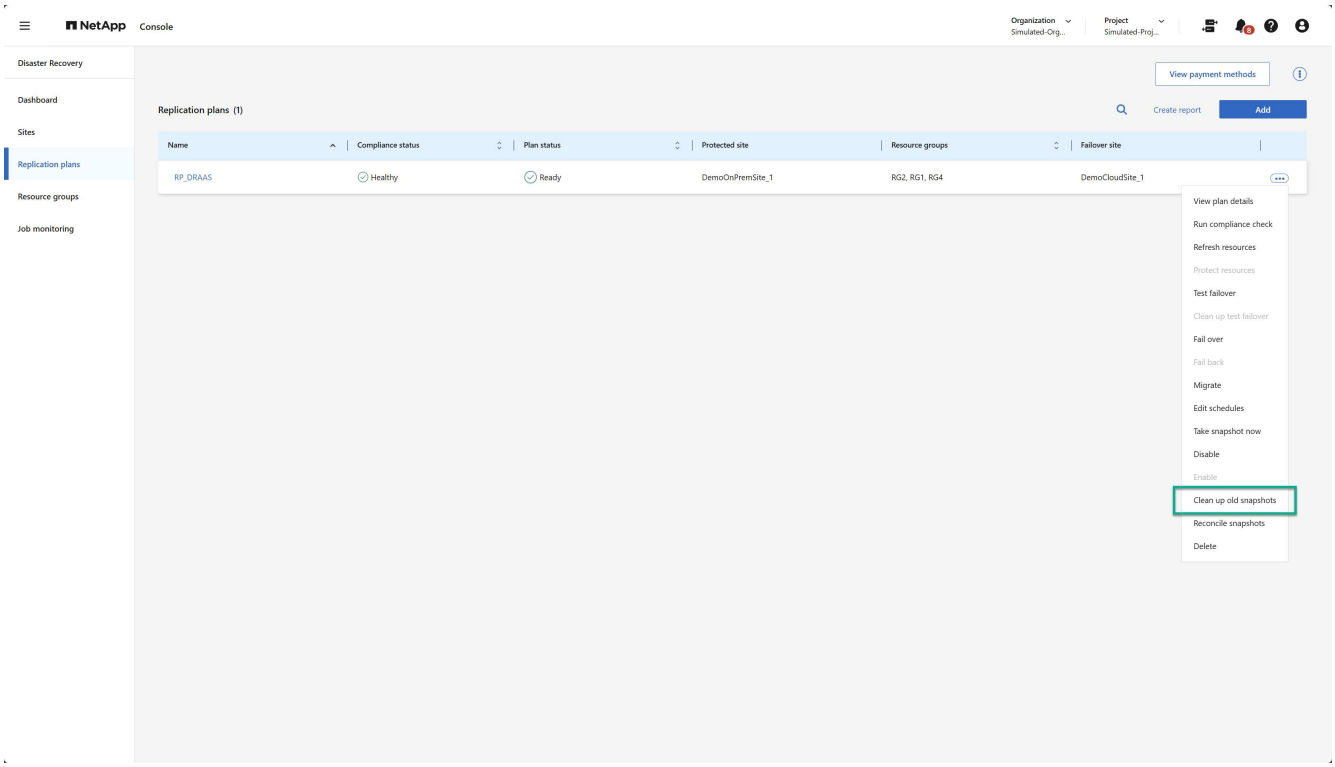
   レプリケーション プランがアクティブな場合、[有効にする] コマンドはグレー表示されます。レプリケーション プランが無効になっている場合、[無効] コマンドはグレー表示されます。



古いスナップショットをクリーンアップする

ソース サイトと宛先サイトに保持されている古いスナップショットをクリーンアップする必要がある場合があります。これは、レプリケーション プランのスナップショット保持数が変更された場合に発生する可能性があります。

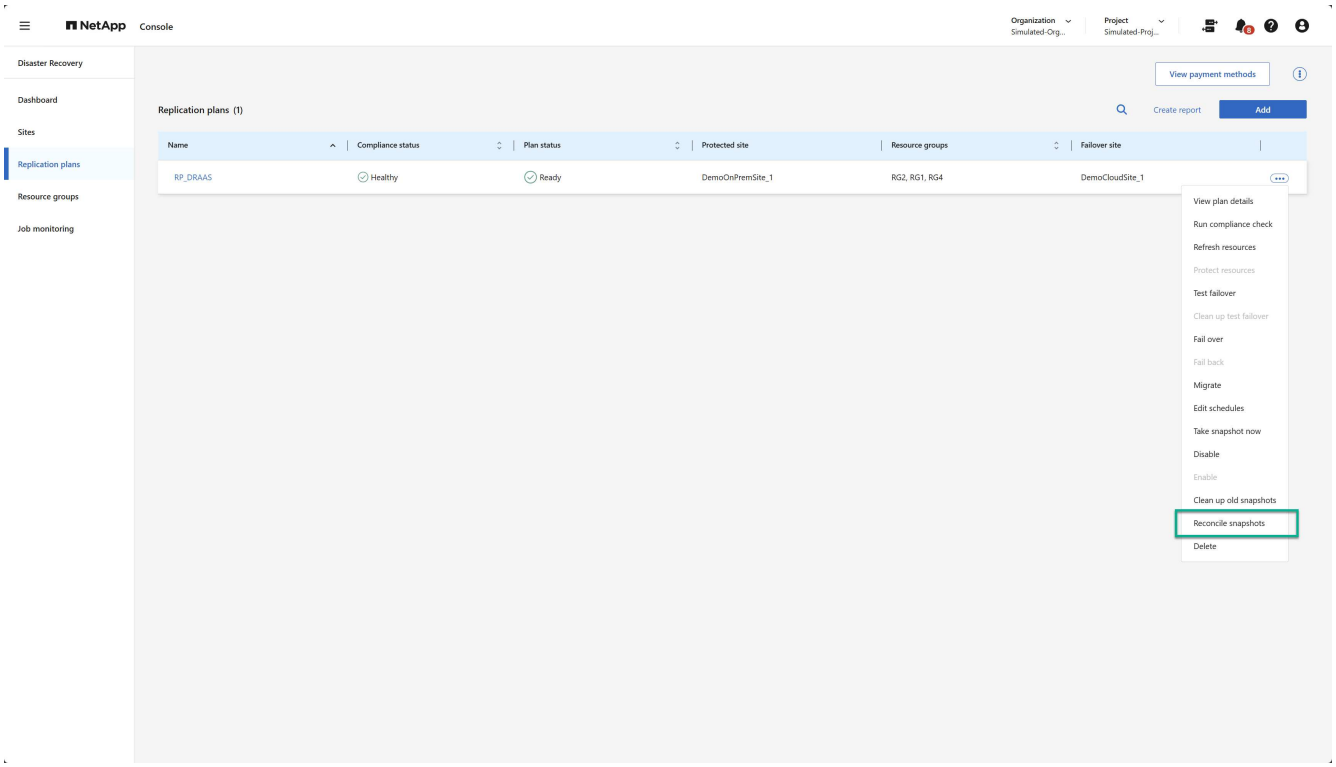
1. *アクション*オプションを選択します ••• レプリケーション プランの横にあります。
2. これらの古いスナップショットを手動で削除するには、レプリケーション プランの [アクション] メニューから [古いスナップショットをクリーンアップ] を選択します。



スナップショットを調整する

このサービスはONTAPボリューム スナップショットを調整するため、 ONTAPストレージ管理者は、サービスの認識なしに、 ONTAP System Manager、 ONTAP CLI、またはONTAP REST API を使用してスナップショットを直接削除できます。サービスは、宛先クラスター上に存在しないソース上のスナップショットを 24 時間ごとに自動的に削除します。ただし、これをオンデマンドで実行できます。この機能により、すべてのサイト間でスナップショットの一貫性を確保できます。

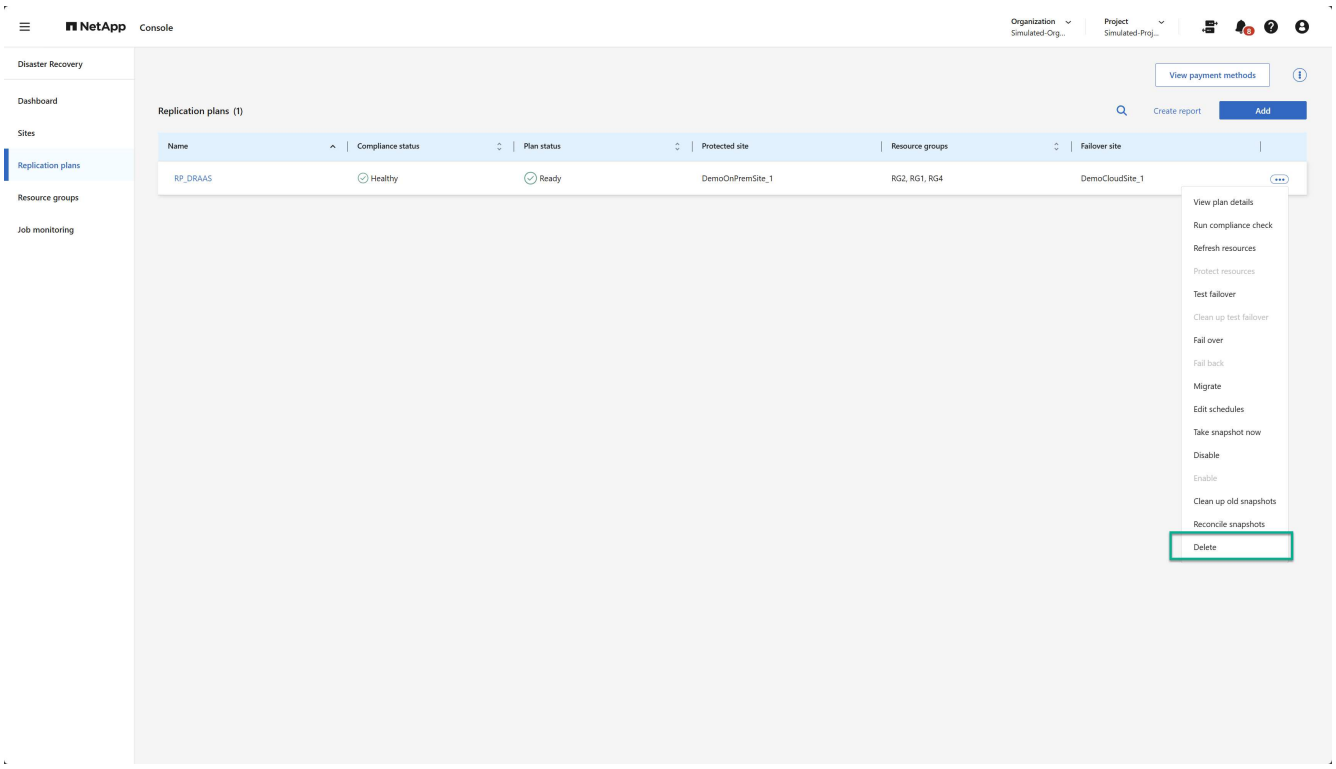
1. *アクション*オプションを選択します ••• レプリケーション プランの横にあります。
2. 宛先クラスターに存在しないスナップショットをソース クラスターから削除するには、レプリケーション プランの [アクション] メニューから [スナップショットの調整] を選択します。



レプリケーションプランを削除する

レプリケーション プランが不要になった場合は、削除できます。

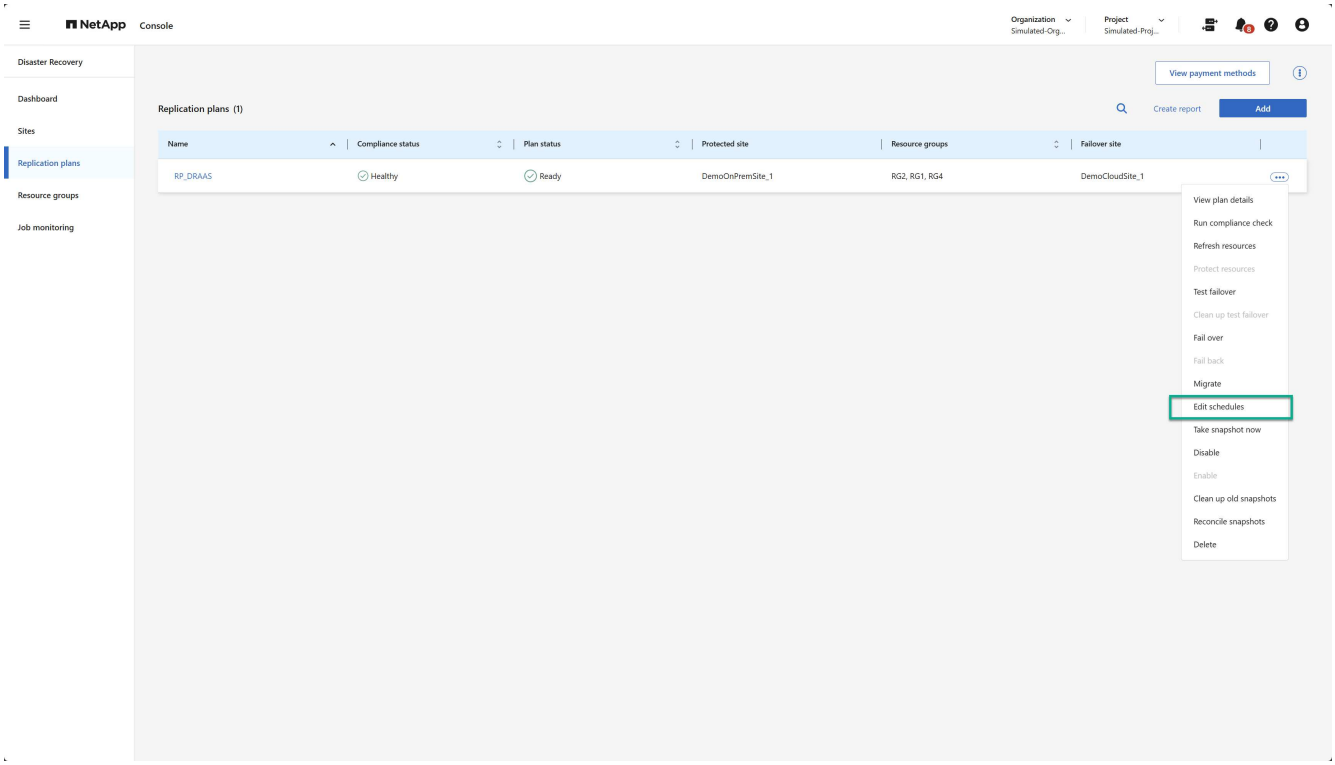
1. *アクション*オプションを選択します ••• レプリケーション プランの横にあります。
2. レプリケーション プランを削除するには、レプリケーション プランのコンテキスト メニューから [削除] を選択します。



スケジュールを編集する

テストフェイルオーバーとコンプライアンス チェックの 2 つの操作が定期的に自動的に実行されます。

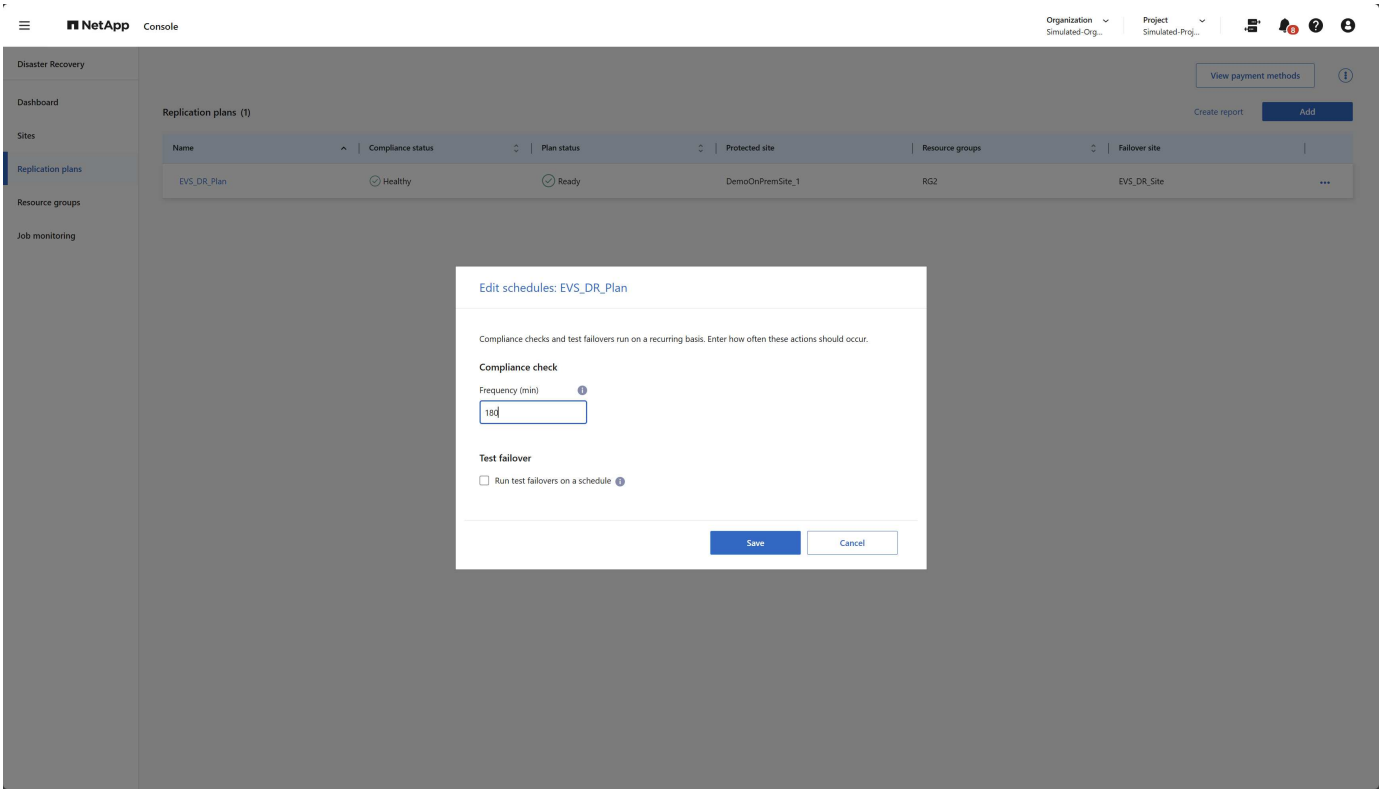
1. *アクション*オプションを選択します ••• レプリケーション プランの横にあります。
2. これら 2 つの操作のいずれかのスケジュールを変更するには、レプリケーション プランの [スケジュールの編集] を選択します。



コンプライアンスチェック間隔を変更する

デフォルトでは、コンプライアンス チェックは 3 時間ごとに実行されます。これを 30 分から 24 時間までの任意の間隔に変更できます。

この間隔を変更するには、[スケジュールの編集] ダイアログ ボックスの [頻度] フィールドを変更します。

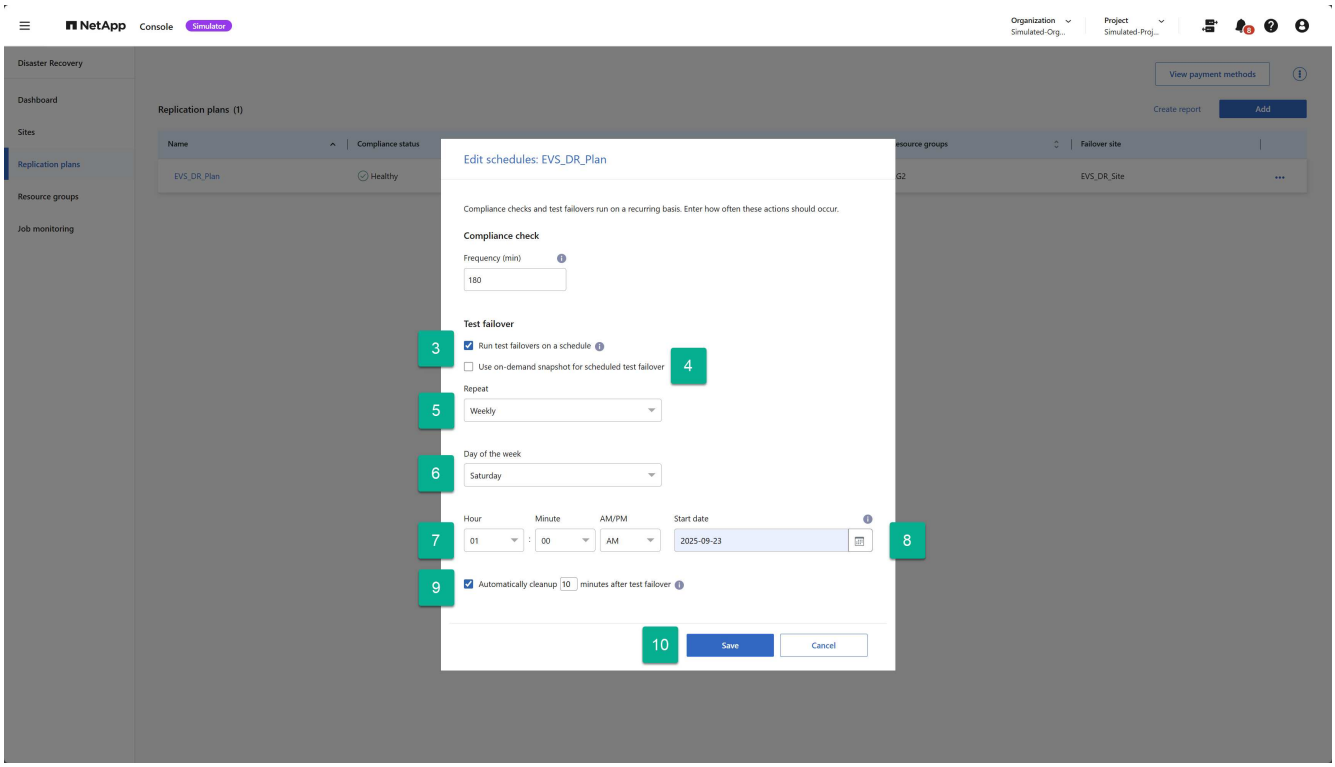


自動テストフェイルオーバーをスケジュールする

テストフェイルオーバーは、デフォルトでは手動で実行されます。自動テストフェイルオーバーをスケジュールすることで、レプリケーション プランが期待どおりに実行されることを確認できます。テストフェイルオーバープロセスの詳細については、以下を参照してください。"フェイルオーバープロセスをテストする" 。

テストフェイルオーバーをスケジュールする手順

1. *アクション*オプションを選択します ••• レプリケーション プランの横にあります。
2. *フェイルオーバーの実行*を選択します。
3. *スケジュールに従ってテストフェイルオーバーを実行する*チェックボックスをオンにします。
4. (オプション) スケジュールされたテストフェイルオーバーにオンデマンドスナップショットを使用する をオンにします。
5. 「繰り返し」ドロップダウンで間隔の種類を選択します。
6. テストフェイルオーバーを実行するタイミングを選択する
   a. 毎週: 曜日を選択
   b. 月次: 月の日付を選択
7. テストフェイルオーバーを実行する時刻を選択します
8. 開始日を選択してください。
9. サービスでテスト環境を自動的にクリーンアップするかどうか、またクリーンアップ プロセスを開始する前にテスト環境をどのくらいの時間実行するかを決定します。
10. *保存*を選択します。


NetApp Console
Simulator
Organization
Simulated-Org...
Project
Simulated-Proj...
Disaster Recovery
Dashboard
Sites
Replication plans
Resource groups
Job monitoring
View payment methods
Replication plans (1)
Create report
Add
Name
Compliance status
Failover site
EVS_DR_Plan
Healthy
EVS_DR_Site
Edit schedules: EVS_DR_Plan
Compliance checks and test failovers run on a recurring basis. Enter how often these actions should occur.
Compliance check
Frequency (min)
180
Test failover
3
Run test failovers on a schedule
Use on-demand snapshot for scheduled test failover
4
Repeat
5
Weekly
Day of the week
6
Saturday
Hour
Minute
AM/PM
Start date
7
01
00
AM
2025-09-23
8
9
Automatically cleanup 10 minutes after test failover
10
Save
Cancel

NetApp Disaster Recoveryに関するよくある質問

質問に対する簡単な回答を探している場合は、この FAQ が役立ちます。

- NetApp Disaster RecoveryURL とは何ですか?* URL については、ブラウザで次のように入力します。"https://console.netapp.com/" NetAppコンソールにアクセスします。
- NetApp Disaster Recovery を使用するにはライセンスが必要ですか?*完全なアクセスには、 NetApp Disaster Recoveryライセンスが必要です。ただし、無料トライアルで試してみることはできます。

NetApp Disaster Recoveryのライセンス設定の詳細については、以下を参照してください。"NetApp Disaster Recoveryライセンスを設定する" 。

- NetApp Disaster Recoveryにどのようにアクセスしますか?* NetApp Disaster Recovery有効化は必要ありません。災害復旧オプションは、NetApp Consoleの左側のナビゲーションに自動的に表示されます。

知識とサポート

サポートに登録する

BlueXPおよびそのストレージ ソリューションとサービスに固有のテクニカル サポートを受けるには、サポート登録が必要です。Cloud Volumes ONTAPシステムの主要なワークフローを有効にするには、サポート登録も必要です。

サポートに登録しても、クラウド プロバイダー ファイル サービスに対するNetAppサポートは有効になりません。クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品のBlueXPドキュメントの「ヘルプの取得」を参照してください。

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

サポート登録の概要

サポート資格を有効にするには、次の 2 つの登録形式があります。

- BlueXPアカウントのシリアル番号を登録します (BlueXPのサポート リソース ページにある 20 桁の 960xxxxxxxxx シリアル番号)。

  これは、BlueXP内のすべてのサービスに対する単一のサポート サブスクリプション ID として機能します。各BlueXPアカウント レベルのサポート サブスクリプションを登録する必要があります。

- クラウド プロバイダーのマーケットプレイスで、サブスクリプションに関連付けられたCloud Volumes ONTAPシリアル番号を登録します (これらは 20 桁の 909201xxxxxxxx シリアル番号です)。

  これらのシリアル番号は一般に *PAYGO* シリアル番号 と呼ばれ、 Cloud Volumes ONTAP の展開時にBlueXPによって生成されます。

両方のタイプのシリアル番号を登録すると、サポート チケットの開設やケースの自動生成などの機能が有効になります。登録は、以下の説明に従ってNetAppサポート サイト (NSS) アカウントをBlueXPに追加することで完了します。

NetAppサポートのために**BlueXP**を登録する

サポートに登録し、サポート資格を有効にするには、 BlueXP組織 (またはアカウント) 内の 1 人のユーザーがNetAppサポート サイト アカウントをBlueXPログインに関連付ける必要があります。NetAppサポートに登録する方法は、 NetAppサポート サイト (NSS) アカウントをすでにお持ちかどうかによって異なります。

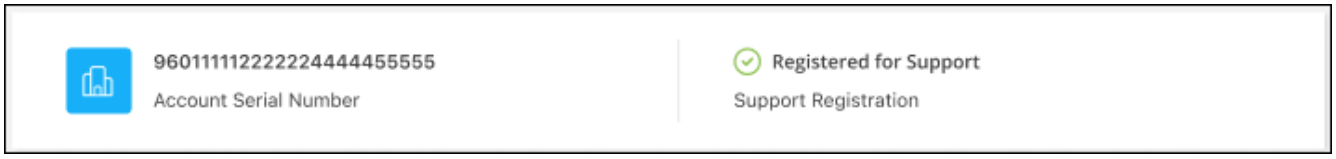
NSSアカウントをお持ちの既存顧客

NSS アカウントをお持ちのNetApp のお客様の場合は、 BlueXPを通じてサポートに登録するだけです。

手順

1. BlueXPコンソールの右上にある設定アイコンを選択し、*資格情報*を選択します。
2. *ユーザー資格情報*を選択します。
3. **NSS** 資格情報の追加 を選択し、 NetAppサポート サイト (NSS) の認証プロンプトに従います。
4. 登録プロセスが成功したことを確認するには、[ヘルプ] アイコンを選択し、[サポート] を選択します。

   リソース ページには、 BlueXP組織がサポートに登録されていることが表示されます。



   他のBlueXPユーザーは、 NetAppサポート サイト アカウントをBlueXPログインに関連付けていない場合、同じサポート登録ステータスを表示しないことに注意してください。ただし、これはBlueXP組織がサポートに登録されていないことを意味するものではありません。組織内の 1 人のユーザーがこれらの手順を実行すれば、組織は登録されます。

既存の顧客だが**NSS**アカウントがない

既存のNetApp顧客であり、既存のライセンスとシリアル番号を持っているものの、NSS アカウントを持っていない場合は、NSS アカウントを作成し、それをBlueXPログインに関連付ける必要があります。

手順

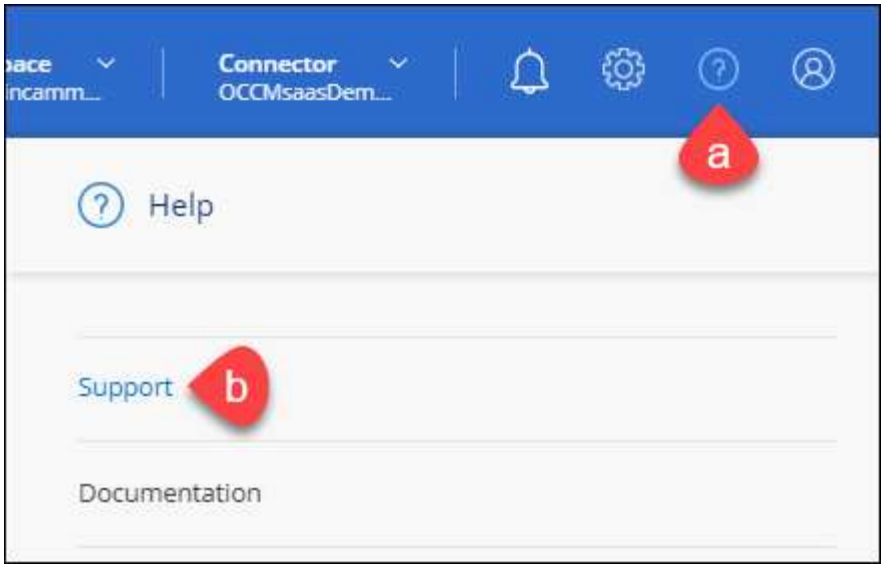
1. NetAppサポートサイトのアカウントを作成するには、 "NetAppサポートサイト ユーザー登録フォーム"
   a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
   b. 上記で使用したBlueXPアカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより、アカウント処理が高速化されます。
2. 以下の手順を完了して、新しいNSSアカウントをBlueXPログインに関連付けます。NSSアカウントをお持ちの既存顧客 。

NetAppの新着情報

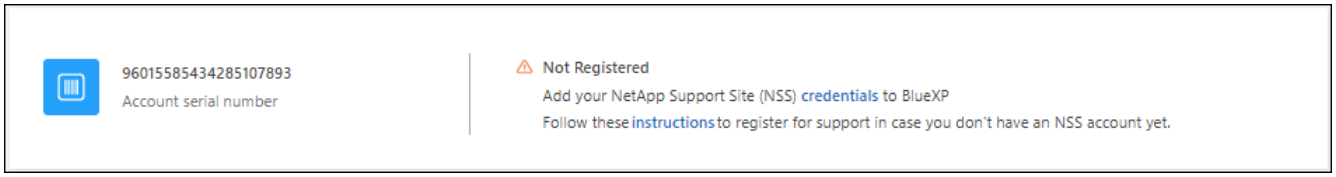
NetAppを初めて使用し、NSS アカウントをお持ちでない場合は、以下の手順に従ってください。

手順

1. BlueXPコンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。



2. サポート登録ページからアカウント ID シリアル番号を見つけます。



3. 移動先 "NetAppのサポート登録サイト"私は登録済みの**NetApp**顧客ではありません を選択します。
4. 必須フィールド（赤いアスタリスクが付いているフィールド）に入力します。
5. 製品ライン フィールドで、**Cloud Manager** を選択し、該当する請求プロバイダーを選択します。
6. 上記の手順 2 からアカウントのシリアル番号をコピーし、セキュリティ チェックを完了して、NetApp のグローバル データ プライバシー ポリシーを読んだことを確認します。

   この安全な取引を完了するために、指定されたメールボックスに電子メールが直ちに送信されます。検証メールが数分以内に届かない場合は、必ずスパム フォルダーを確認してください。

7. メール内からアクションを確認します。

   確認すると、リクエストがNetAppに送信され、 NetAppサポート サイトのアカウントを作成することが推奨されます。

8. NetAppサポートサイトのアカウントを作成するには、 "NetAppサポートサイト ユーザー登録フォーム"
   a. 適切なユーザー レベル (通常は * NetApp顧客/エンド ユーザー*) を選択してください。
   b. 上記で使用したアカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより処理速度が向上します。

終了後の操作

このプロセス中に、 NetAppから連絡が来るはずです。これは、新規ユーザー向けの 1 回限りのオンボーディング演習です。

NetAppサポートサイトのアカウントを取得したら、以下の手順を実行してアカウントをBlueXPログインに関連付けます。NSSアカウントをお持ちの既存顧客 。

Cloud Volumes ONTAPサポートに NSS 認証情報を関連付ける

Cloud Volumes ONTAPの次の主要なワークフローを有効にするには、 NetAppサポート サイトの認証情報をBlueXP組織に関連付ける必要があります。

- 従量課金制のCloud Volumes ONTAPシステムをサポート対象として登録する

  システムのサポートを有効にし、 NetAppテクニカル サポート リソースにアクセスするには、NSS アカウントを提供する必要があります。

- BYOL（個人ライセンス使用）時にCloud Volumes ONTAP を導入する

  BlueXP がライセンス キーをアップロードし、購入した期間のサブスクリプションを有効にするには、NSS アカウントを提供する必要があります。これには、期間更新の自動更新が含まれます。

- Cloud Volumes ONTAPソフトウェアを最新リリースにアップグレードする

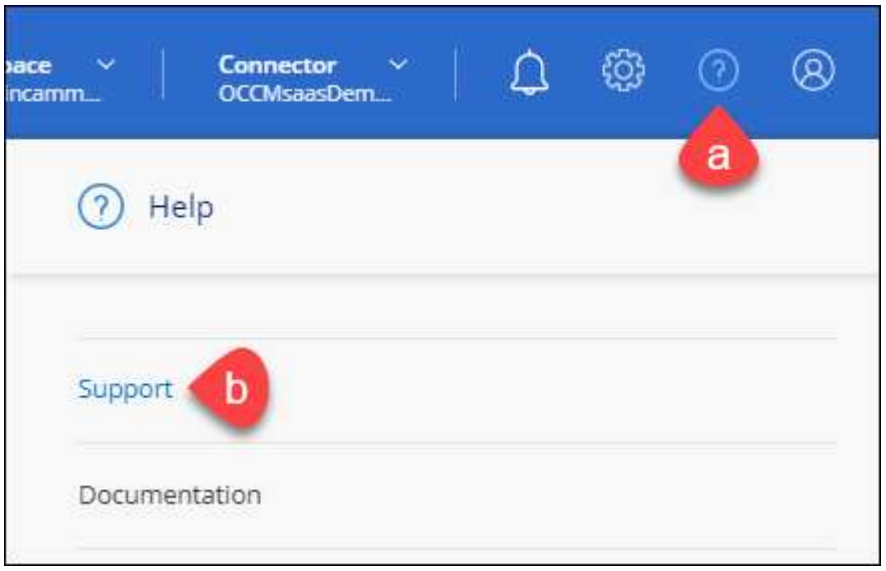
NSS 資格情報をBlueXP組織に関連付けることは、 BlueXPユーザー ログインに関連付けられている NSS アカウントとは異なります。

これらの NSS 資格情報は、特定のBlueXP組織 ID に関連付けられています。BlueXP組織に属するユーザーは、サポート **> NSS** 管理 からこれらの資格情報にアクセスできます。

- 顧客レベルのアカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できます。
- パートナー アカウントまたは再販業者アカウントをお持ちの場合は、1 つ以上の NSS アカウントを追加できますが、顧客レベルのアカウントと一緒に追加することはできません。

手順

1. BlueXPコンソールの右上にあるヘルプ アイコンを選択し、サポート を選択します。



2. *NSS管理 > NSSアカウントの追加*を選択します。
3. プロンプトが表示されたら、[続行] を選択して、Microsoft ログイン ページにリダイレクトします。

   NetApp は、サポートとライセンスに固有の認証サービスの ID プロバイダーとして Microsoft Entra ID を使用します。

4. ログイン ページで、 NetAppサポート サイトに登録した電子メール アドレスとパスワードを入力して、認証プロセスを実行します。

   これらのアクションにより、 BlueXP はライセンスのダウンロード、ソフトウェア アップグレードの検証、将来のサポート登録などに NSS アカウントを使用できるようになります。

   次の点に注意してください。

   - NSS アカウントは顧客レベルのアカウントである必要があります (ゲスト アカウントや一時アカウントではありません)。顧客レベルの NSS アカウントを複数持つことができます。
   - パートナー レベルのアカウントの場合、NSS アカウントは 1 つだけ存在できます。顧客レベルの NSS アカウントを追加しようとしたときに、パートナー レベルのアカウントが存在する場合は、次のエラー メッセージが表示されます。

     「異なるタイプの NSS ユーザーがすでに存在するため、このアカウントでは NSS 顧客タイプは許可されません。」

   既存の顧客レベルの NSS アカウントがあり、パートナー レベルのアカウントを追加しようとする場合も同様です。

   - ログインが成功すると、 NetApp はNSS ユーザー名を保存します。

     これは、メールにマッピングされるシステム生成の ID です。*NSS管理*ページでは、 ••• メニュー。

   - ログイン認証トークンを更新する必要がある場合は、 ••• メニュー。

     このオプションを使用すると、再度ログインするよう求められます。これらのアカウントのトークンは 90 日後に期限切れになることに注意してください。これを知らせる通知が投稿されます。

ヘルプを受ける

NetAppは、 BlueXPとそのクラウドサービスに対して、様々なサポートを提供しています。ナレッジベース（KB）記事やコミュニティフォーラムなど、充実した無料のセルフサポートオプションを24時間365日ご利用いただけます。サポート登録には、Webチケットによるリモートテクニカルサポートも含まれます。

クラウドプロバイダーのファイルサービスのサポートを受ける

クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品のBlueXPドキュメントの「ヘルプの取得」を参照してください。

- "Amazon FSx for ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

BlueXPとそのストレージ ソリューションおよびサービスに固有のテクニカル サポートを受けるには、以下に説明するサポート オプションを使用してください。

セルフサポートオプションを使用する

以下のオプションは、24 時間 365 日無料でご利用いただけます。

- ドキュメント

  現在表示しているBlueXPドキュメント。

- "ナレッジベース"

  BlueXPナレッジベースを検索して、問題のトラブルシューティングに役立つ記事を見つけます。

- "コミュニティ"

  BlueXPコミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりしてください。

NetAppサポートでケースを作成する

上記のセルフ サポート オプションに加えて、サポートを有効にした後は、 NetAppサポート スペシャリストと協力して問題を解決することもできます。

始める前に

- *ケースの作成*機能を使用するには、まずNetAppサポート サイトの資格情報をBlueXPログインに関連付ける必要があります。 "BlueXPログインに関連付けられた資格情報を管理する方法を学びます" 。
- シリアル番号を持つONTAPシステムのケースを開く場合は、NSS アカウントがそのシステムのシリアル番号に関連付けられている必要があります。

手順

1. BlueXPで、*ヘルプ > サポート*を選択します。
2. *リソース*ページで、テクニカル サポートの下にある利用可能なオプションのいずれかを選択します。

   a. 電話で誰かと話したい場合は、「電話する」を選択してください。電話をかけることができる電話番号をリストした netapp.com のページに移動します。

   b. NetAppサポート スペシャリストとのチケットを開くには、[ケースを作成] を選択します。

      - サービス: 問題が関連付けられているサービスを選択します。たとえば、サービス内のワークフローまたは機能に関するテクニカル サポートの問題に固有の場合はBlueXP。
      - 作業環境: ストレージに該当する場合は、* Cloud Volumes ONTAP* または * On-Prem* を選択し、関連する作業環境を選択します。

        作業環境のリストは、サービスのトップバナーで選択したBlueXP組織 (またはアカウント)、プロジェクト (またはワークスペース)、およびコネクタの範囲内にあります。

      - ケースの優先度: ケースの優先度 (低、中、高、重大) を選択します。

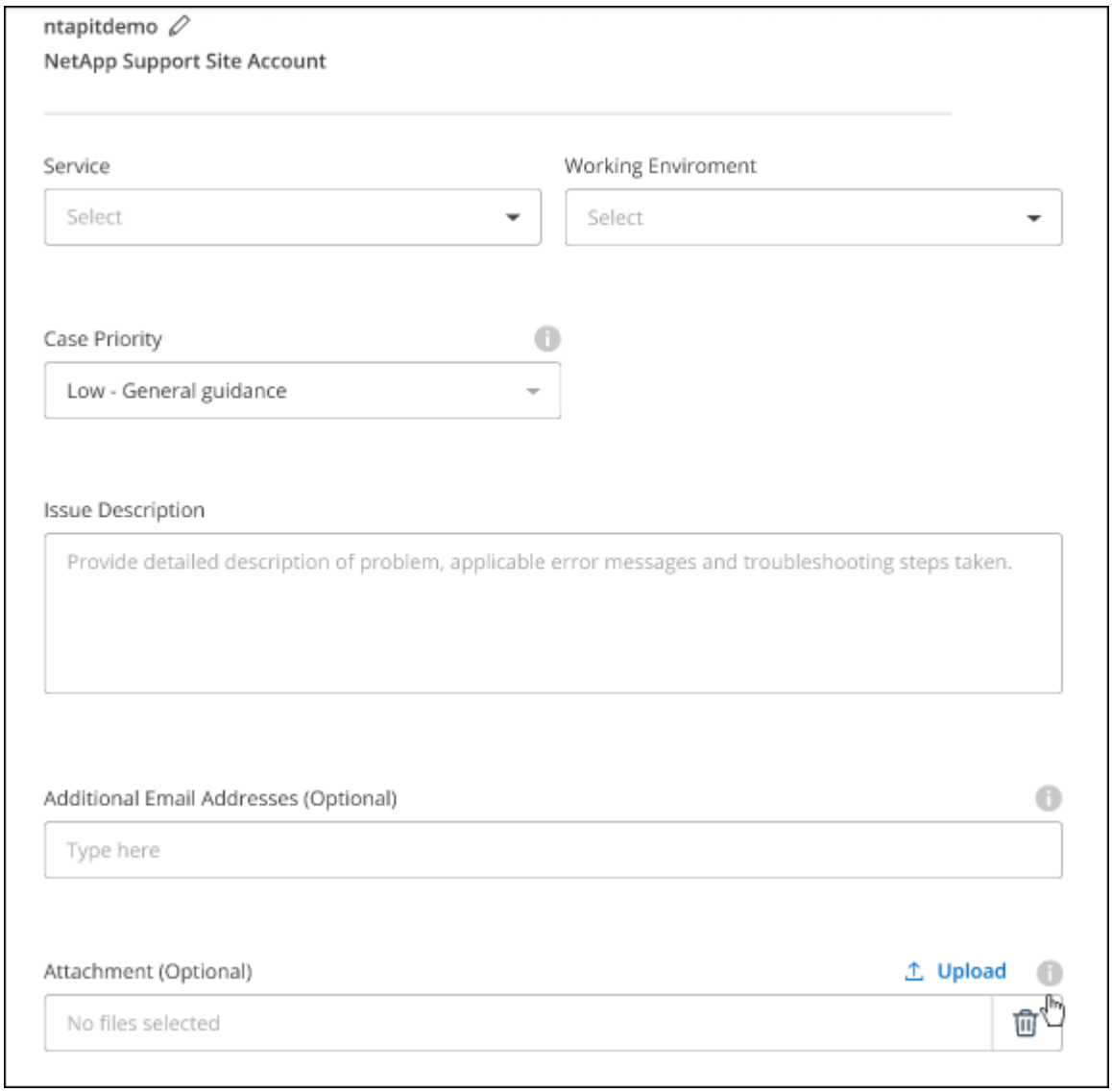
        これらの優先順位の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスを置きます。

      - 問題の説明: 該当するエラー メッセージや実行したトラブルシューティング手順など、問題の詳細

な説明を入力します。

- 追加のメールアドレス:この問題を他の人に知らせたい場合は、追加のメールアドレスを入力してください。
- 添付ファイル (オプション): 一度に 1 つずつ、最大 5 つの添付ファイルをアップロードします。

  添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。



終了後の操作

サポート ケース番号を示すポップアップが表示されます。NetAppサポート スペシャリストがお客様のケースを確認し、すぐにご連絡いたします。

サポート ケースの履歴については、設定 > タイムライン を選択し、「サポート ケースの作成」というアクションを探します。右端のボタンを使用すると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラー メッセージが表示される場合があります。

「選択したサービスに対してケースを作成する権限がありません」

このエラーは、NSS アカウントとそれに関連付けられているレコード会社が、 BlueXPアカウントのシリアル番号のレコード会社と同じではないことを意味している可能性があります (つまり、960xxxx) または作業環境のシリアル番号。次のいずれかのオプションを使用してサポートを求めることができます。

- 製品内チャットを使用する
- 非技術的なケースを提出する https://mysupport.netapp.com/site/help

サポートケースを管理する（プレビュー）

アクティブおよび解決済みのサポート ケースをBlueXPから直接表示および管理できます。NSS アカウントおよび会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして利用できます。今後のリリースでは、このエクスペリエンスを改良し、機能強化を追加する予定です。製品内チャットを使用してフィードバックをお送りください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の 2 つのビューがあります。
  - 左側のビューには、指定したユーザー NSS アカウントによって過去 3 か月間に開かれたケースの合計が表示されます。
  - 右側のビューには、ユーザーの NSS アカウントに基づいて、会社レベルで過去 3 か月間に開かれたケースの合計が表示されます。

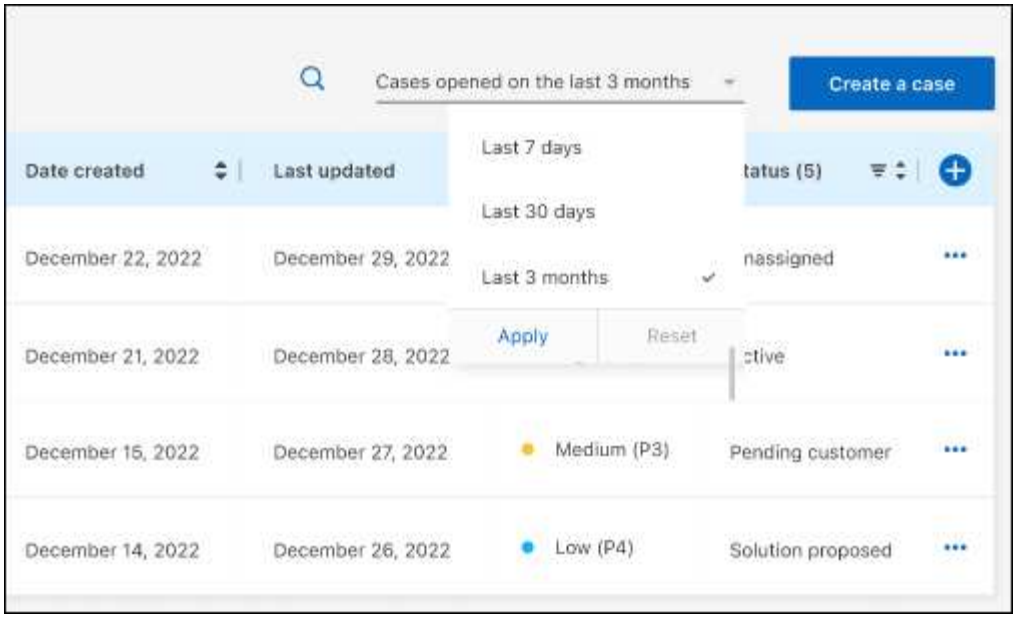
  表の結果には、選択したビューに関連するケースが反映されます。
- 関心のある列を追加または削除したり、優先度やステータスなどの列の内容をフィルタリングしたりできます。その他の列は並べ替え機能のみを提供します。

  詳細については、以下の手順をご覧ください。
- ケースごとに、ケースメモを更新したり、まだ「クローズ」または「クローズ保留中」ステータスになっていないケースをクローズしたりする機能を提供します。

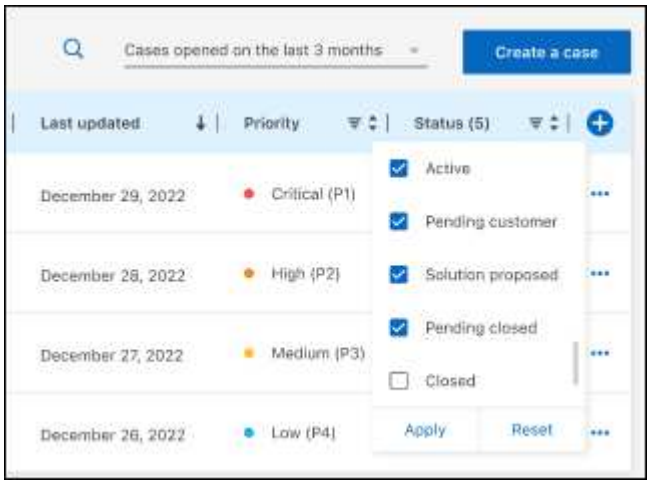
手順

1. BlueXPで、*ヘルプ > サポート*を選択します。
2. *ケース管理*を選択し、プロンプトが表示されたら、NSS アカウントをBlueXPに追加します。

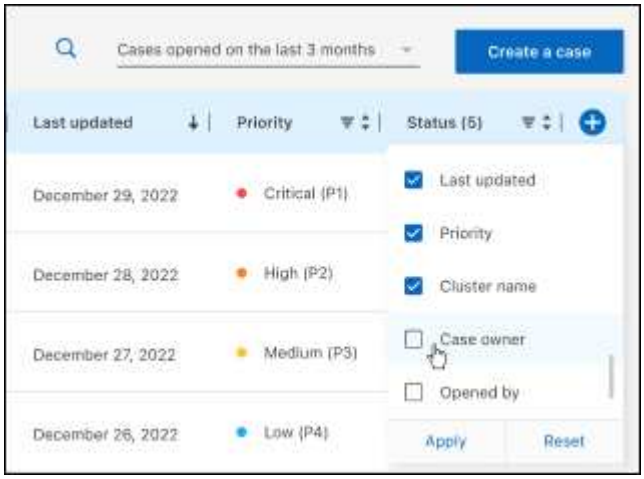
   ケース管理 ページには、 BlueXPユーザー アカウントに関連付けられている NSS アカウントに関連するオープン ケースが表示されます。これは、**NSS** 管理 ページの上部に表示される NSS アカウントと同じです。
3. 必要に応じて、テーブルに表示される情報を変更します。
   - *組織のケース*の下で*表示*を選択すると、会社に関連付けられているすべてのケースが表示されます。
   - 正確な日付範囲を選択するか、別の期間を選択して日付範囲を変更します。



◦ 列の内容をフィルタリングします。



◦ 表に表示される列を変更するには、次に、表示する列を選択します。

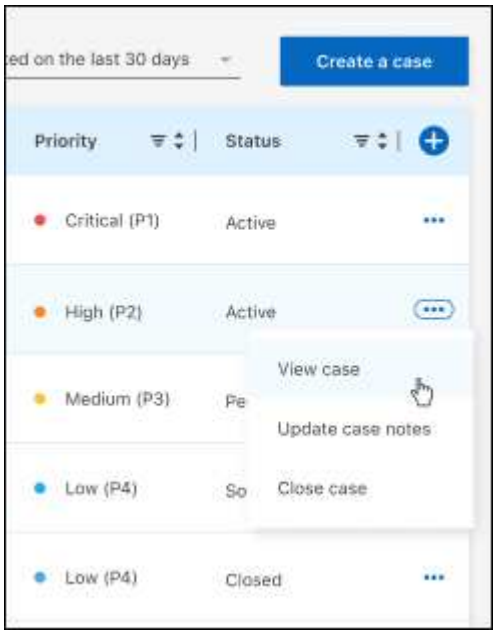


4. 既存のケースを管理するには、利用可能なオプションのいずれかを選択します。

- ケースを表示: 特定のケースに関する詳細をすべて表示します。
- ケースノートを更新: 問題に関する追加の詳細を入力するか、*ファイルのアップロード*を選択して最大 5 つのファイルを添付します。

  添付ファイルはファイルごとに 25 MB までに制限されます。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、csv です。

- ケースを閉じる: ケースを閉じる理由の詳細を入力し、[ケースを閉じる] を選択します。



法律上の表示

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。

"https://www.netapp.com/company/legal/trademarks/"

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

プライバシー ポリシー

"https://www.netapp.com/company/legal/privacy-policy/"

オープンソース

通知ファイルには、 NetAppソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が提供されます。

"NetApp Disaster Recoveryに関するお知らせ"

著作権に関する情報

商標に関する情報