



参照 NetApp Disaster Recovery

NetApp
February 04, 2026

This PDF was generated from <https://docs.netapp.com/ja-jp/data-services-disaster-recovery/reference/vcenter-privileges.html> on February 04, 2026. Always check docs.netapp.com for the latest.

目次

参照	1
NetApp Disaster Recovery に必要な vCenter 権限	1
NetApp Disaster Recoveryを使用する場合のスイッチコンソールエージェント	4
開始する前に	4
手順	4
詳細情報	5
Amazon EVS でNetApp Disaster Recoveryを使用する	5
Amazon Elastic VMware Service とAmazon FSx for NetApp ONTAPを使用したNetApp Disaster Recoveryの紹介	5
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	6
NetApp Disaster Recovery用のNetApp Consoleエージェントをインストールする	8
Amazon EVS 用のNetApp Disaster Recoveryを構成する	8
Amazon EVS のレプリケーション プランを作成する	21
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	34

参照

NetApp Disaster Recovery に必要な vCenter 権限

NetApp Disaster Recoveryがサービスを実行するには、vCenterアカウントに最小限のvCenter権限セットが必要です。これらの権限には、データストアの登録と登録解除、仮想マシン（VM）の起動と停止、VMの再構成が含まれます。

次の表は、Disaster RecoveryがvCenterクラスとインターフェースするために必要なすべての権限を示しています。

タイプ	権限名（vSphere クライアント）	権限名（API）	説明
データストア	Datastore.Config	データストアを設定する	データストアの設定を許可します。
	Datastore.Delete	Remove datastore	データストアの削除を許可します。
	Datastore.Rename	Rename datastore	データストアの名前の変更を許可します。
フォルダ	フォルダー作成	フォルダを作成	新しいフォルダーの作成を許可します。
	フォルダーの削除	フォルダを削除	フォルダーの削除を許可します。オブジェクトとその親の両方に対する権限が必要です。
	フォルダー名の変更	フォルダ名を変更する	フォルダー名の変更を許可します。
ネットワーク	Network.Assign	Assign network	VM にネットワークを割り当てることを許可します。
	Network.Config	設定	ネットワークの構成を許可します。

タイプ	権限名 (vSphere クライアント)	権限名 (API)	説明
仮想マシンの構成	VirtualMachine.Config.AdvancedConfig	高度な設定	VM の構成ファイル内の高度なパラメータを追加または変更することを許可します。
	VirtualMachine.Config.Settings	設定の変更	一般的な VM 設定の変更を許可します。
	VirtualMachine.Config.CPUCount	Change CPU count	仮想 CPU の数の変更を許可します。
	VirtualMachine.Config.Memory	メモリを変更する	VM に割り当てられるメモリの量を変更できます。
	VirtualMachine.Config.Resource	Change resource	リソース プール内の VM ノードのリソース構成の変更を許可します。
	VirtualMachine.Config.Rename	名前を変更	VM の名前を変更したり、メモを変更したりすることを許可します。
	VirtualMachine.Config.EditDevice	Modify device settings	既存のデバイスのプロパティを変更できます。
	VirtualMachine.Config.ReloadFromPath	Reload from path	ID を保持しながら VM 構成パスを変更することを許可します。
	VirtualMachine.Config.ResetGuestInfo	ゲスト情報をリセットする	VM のゲスト オペレーティング システム情報の編集を許可します。
仮想マシンゲスト	VirtualMachine.GuestOperations.ModifyAliases	ゲスト操作エイリアスの変更	VM のエイリアスの変更を許可します。
	VirtualMachine.GuestOperations.QueryAliases	ゲスト操作エイリアス クエリ	VM のエイリアスのクエリを許可します。
	VirtualMachine.GuestOperations.Modify	Guest operation modifications	VM へのファイルの転送を含む変更操作を許可します。
	VirtualMachine.GuestOperations.Execute	ゲスト操作プログラムの実行	VM 内でアプリケーションを実行することを許可します。
	VirtualMachine.GuestOperations.Query	ゲスト操作クエリ	ゲスト OS へのクエリを許可します。操作にはファイルのリスト表示が含まれます。

タイプ	権限名 (vSphere クライアント)	権限名 (API)	説明
仮想マシンの操作	VirtualMachine.Interact.AnswerQuestion	Answer question	VM の状態遷移中またはランタイム エラー中の問題を解決できます。
	VirtualMachine.Interact.PowerOff	Power off	電源がオンになっている VM の電源をオフにすることを許可します。
	VirtualMachine.Interact.PowerOn	Power on	VM の電源オンまたは再開を許可します。
	VirtualMachineの操作.ToolsInstall	VMware Toolsのインストール	VMware Tools インストーラのマウント / アンマウントを許可します。
	VirtualMachine.Inventory.CreateFromExisting	Create from existing	テンプレートから VM のクローニングまたは導入を許可します。
	VirtualMachine.Inventory.Create	Create new	VM の作成とリソースの割り当てを許可します。
	VirtualMachine.Inventory.Register	登録	既存の VM をインベントリに追加することを許可します。
	VirtualMachine.Inventory.Delete	削除	VM とそのファイルの削除を許可します。オブジェクトとその親の両方に対する権限が必要です。
	VirtualMachine.Inventory.Unregister	登録解除	VM の登録解除を許可します。この権限には、オブジェクトとその親の両方に対する権限が必要です。
仮想マシンのプロビジョニング	VirtualMachineのプロビジョニング：クローン	Clone virtual machine	VM の複製とリソースの割り当てを許可します。
	VirtualMachineのプロビジョニング：カスタマイズ	ゲストをカスタマイズ	VM のゲスト オペレーティング システムをカスタマイズできます。
	VirtualMachineのプロビジョニング：ModifyCustSpecs	カスタマイズ仕様の変更	カスタマイズ仕様の作成、変更、または削除を許可します。
	VirtualMachineのプロビジョニング：ReadCustSpecs	Read customization specifications	VM のカスタマイズ仕様の読み取りを許可します。
仮想マシンサービスの構成	VirtualMachine.Namespace.Query	クエリ サービス構成	VM サービスのリストの取得を許可します。
	VirtualMachine.Namespace.ReadContent	サービス構成の読み取り	既存の VM サービス構成の取得を許可します。

タイプ	権限名 (vSphere クライアント)	権限名 (API)	説明
仮想マシンのスナップショット	VirtualMachine.State.CreateSnapshot	Snapshot 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ことを許可します。
	VirtualMachine.State.RemoveSnapshot	Remove snapshot	スナップショットの削除を許可します。
	VirtualMachineの状態 . RenameSnapshot	スナップショットの名前を変更する	スナップショットの名前を変更したり、その説明を更新したりできます。
	VirtualMachine.State.RevertToSnapshot	Revert to snapshot	VM を特定のスナップショットの状態に戻すことを許可します。

NetApp Disaster Recoveryを使用する場合のスイッチコンソールエージェント

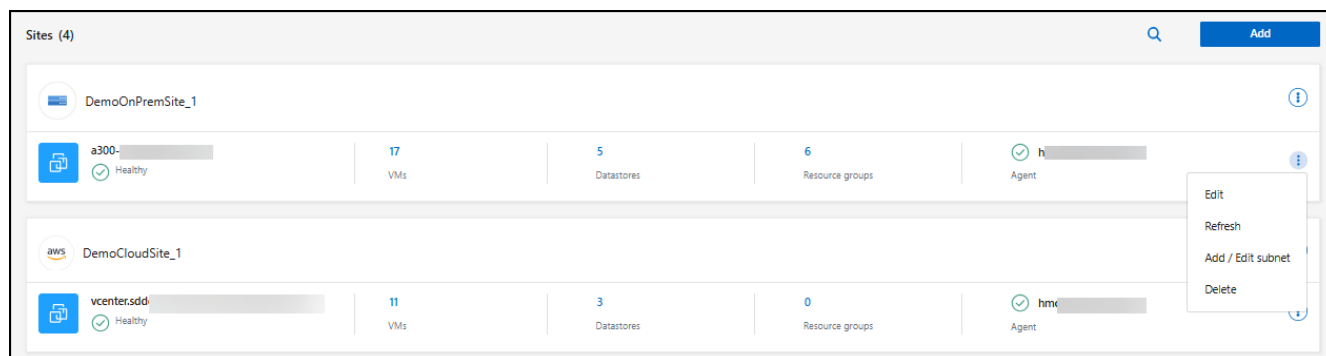
NetApp Consoleは、単一の作業環境で複数のコンソール エージェントの使用をサポートしています。複数のコンソール エージェントを使用すると、別のコンソール エージェントでメンテナンスを実行しているときや、コンソール エージェントに障害が発生したときに、リソースへのアクセスを維持するのに役立ちます。各コンソール エージェントには一意の識別子があるため、コンソール エージェントを不適切に切り替えると、作業環境におけるリソースの可用性が損なわれる可能性があります。

開始する前に

- あなたには作業環境に少なくとも 2 つのコンソール エージェントを追加しました。
- 両方のコンソール エージェントに同じONTAPクラスターが含まれている必要があります。

手順

1. 災害復旧で、[サイト] を選択します。
2. ソース vCenter とターゲット vCenter の両方のコンソール エージェントを変更する必要があります。変更する vCenter を特定します。vCenter のアクション メニューを選択し、[編集] を選択します。



3. ドロップダウン メニューから使用するコンソール エージェントを選択し、vCenter のユーザー名とパスワードを再入力します。保存を選択します。

Enter connection details for the vCenter server that is accessible from the Console Agent.

Site	Console Agent
<input type="text" value="DemoOnPremSite_1"/>	<input type="text" value="hmcdrasconnector4"/>
vCenter IP address	<div>ShivaOnPremConnDemo hmcdrasconnector4 DRaaSTest</div>
<input type="text" value="a300-vcsa06.ehcdc.com"/>	
vCenter user name	vCenter password
<input type="text"/>	<input type="text"/>
<input checked="" type="checkbox"/> Use self-signed certificates ⓘ	
<input type="checkbox"/> Enable scheduled discovery	
<div>Save Cancel</div>	

4. 変更する追加の vCenter ごとに手順 2 と 3 を繰り返します。
5. 変更した vCenter で、vCenter を更新して新しいコンソール エージェントを検出します。変更したすべての vCenter に対してこの手順を繰り返します。
6. 災害復旧で、レプリケーション プラン に移動します。
7. ワークフローを再開するために使用するレプリケーション プランを識別します。アクションメニューを選択し、次にリソースを更新します。ジョブ監視 でジョブのステータスを監視できます。

詳細情報

- ["コンソールエージェントについて学ぶ"](#)

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きます。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

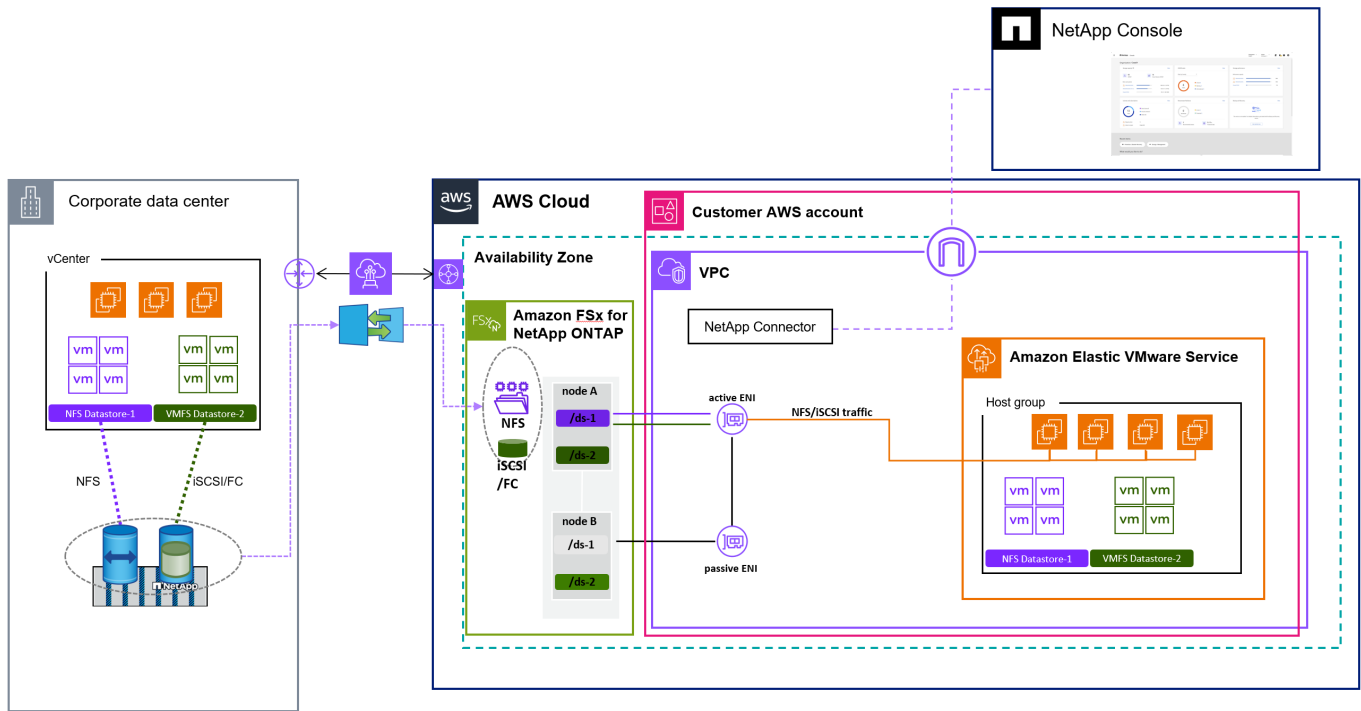
NetApp Disaster Recoveryは、NetApp Consoleのコア アーキテクチャに依存する、NetAppNetApp Consoleのソフトウェア アズ ア サービス環境内でホストされる付加価値サービスです。コンソール内の VMware 保護の DR サービスは、いくつかの主要コンポーネントで構成されています。

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 Amazon Transit 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 エージェントを使用すると、NetApp Console の導入をインフラストラクチャに接続して、AWS、Azure、Google Cloud、またはオンプレミス環境全体でソリューションを安全にオーケストレーションできます。Console エージェントは、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。Console エージェントは、NetApp Disaster Recovery の SaaS レイヤーを常にポーリングして、実行する必要があるアクションを確認します。

NetApp Disaster Recoveryでは、実行されるアクションは、各サービスのネイティブ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VMを保護します。Console agent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の災害復旧サイトにConsole agentをインストールすることをお勧めします。DRサイトにインストールすることで、プライマリサイトに障害が発生した場合でも、NetApp Console UIはConsole agentへの接続を維持し、そのDRサイト内でリカバリプロセスをオーケストレーションできます。

インストール

- Disaster Recoveryを使用するには、Consoleエージェントを標準モードでインストールします。Console エージェントのインストールの種類の詳細については、"[NetApp Console の導入モードについて](#)"を参照してください。

コンソールエージェントの具体的なインストール手順は、導入タイプによって異なります。詳細については、"[コンソールエージェントについて学ぶ](#)"を参照してください。



Amazon AWS を使用して Console 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 Console エージェントのインストールの詳細については、"[AWS MarketplaceからConsoleエージェントを作成する](#)"を参照してください。

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 クラスターを追加する](#)"

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

Amazon EVSをNetApp Disaster Recoveryで構成するための要件を確認し、満たしていることを確認してください。

前提条件

- ["Disaster Recovery の一般的な前提条件"](#)を確認します。
- 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」管理者アカウントは使用しないことを推奨します。代わりに、ディザスタリカバリプロセスに参加するすべてのvCenterクラスター上で、NetApp Disaster Recovery専用のユーザーアカウントを作成してください。必要な特定の権限の一覧については、["NetApp Disaster Recoveryに必要な vCenter 権限"](#)をご参照ください。

- Disaster Recoveryで保護される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てください。

Disaster Recoveryは、Amazon FSx for NetApp ONTAP使用時に、iSCSI上のNFSとVMFS（FCではない）をサポートします。Disaster RecoveryはFCをサポートしていますが、Amazon FSx for NetApp ONTAPは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てください。
- 保護されているすべての VM に VMware Tools がインストールされていることを確認します。
- オンプレミスネットワークが、Amazon が承認した接続方法を使用して AWS VPC ネットワークに接続されていることを確認してください。AWS Direct Connect、AWS Private Link、または AWS Site-to-Site VPN を使用することをお勧めします。
- Disaster Recovery を使用した EVS の接続およびポート要件を確認し、準拠していることを確認します。

ソース	デスティネーション	ポート	詳細
Amazon FSxN	オンプレミス ONTAP	TCP 11104、11105 、ICMP	SnapMirror
オンプレミス ONTAP	Amazon FSxN	TCP 11104、11105 、ICMP	SnapMirror
NetApp Console エージェント	オンプレミス ONTAP	TCP 443、ICMPのみ	API呼び出し
NetApp Console エージェント	Amazon FSxN	TCP 441、ICMPのみ	API呼び出し
NetApp Console エージェント	vCenter（オンプレミス、EVS）、ESXiホスト（オンプレミス、EVS）	443	API呼び出し、スクリプト実行

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。

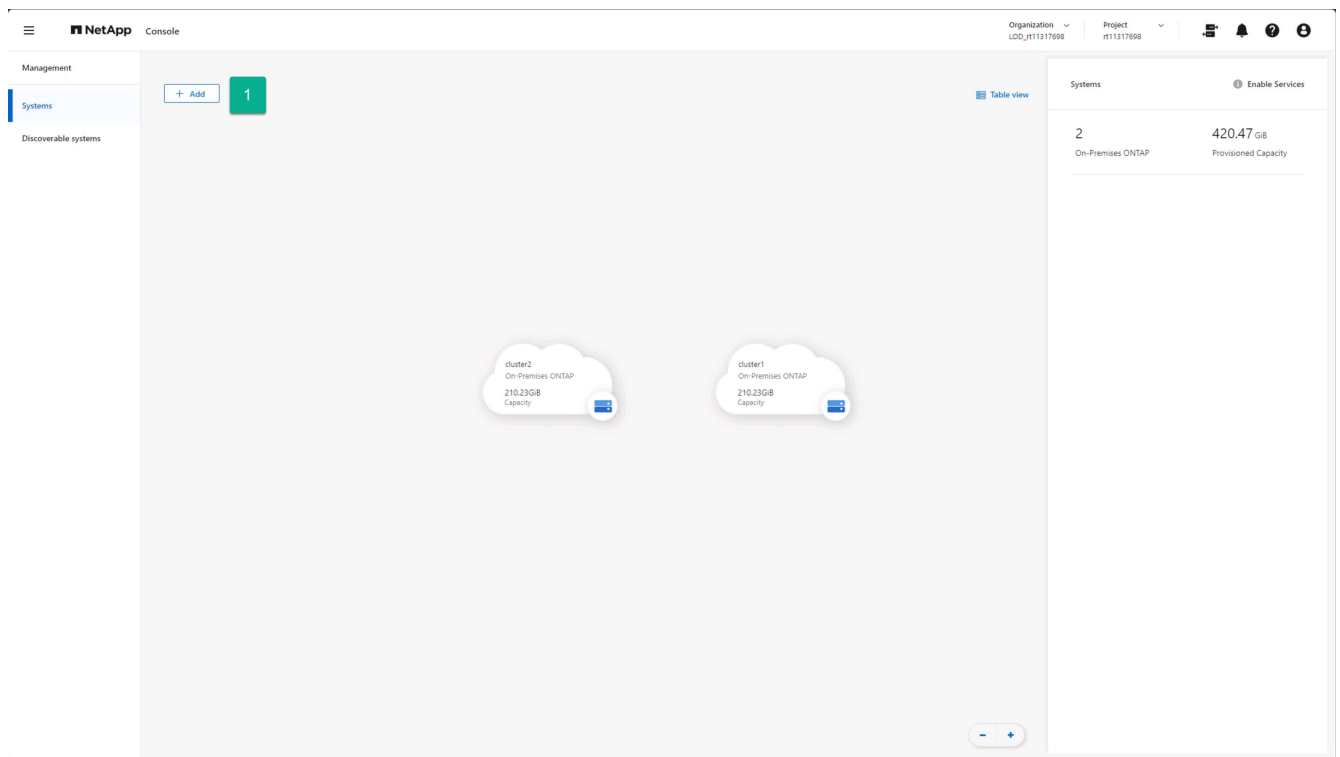
次の操作を行う必要があります。

- 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。

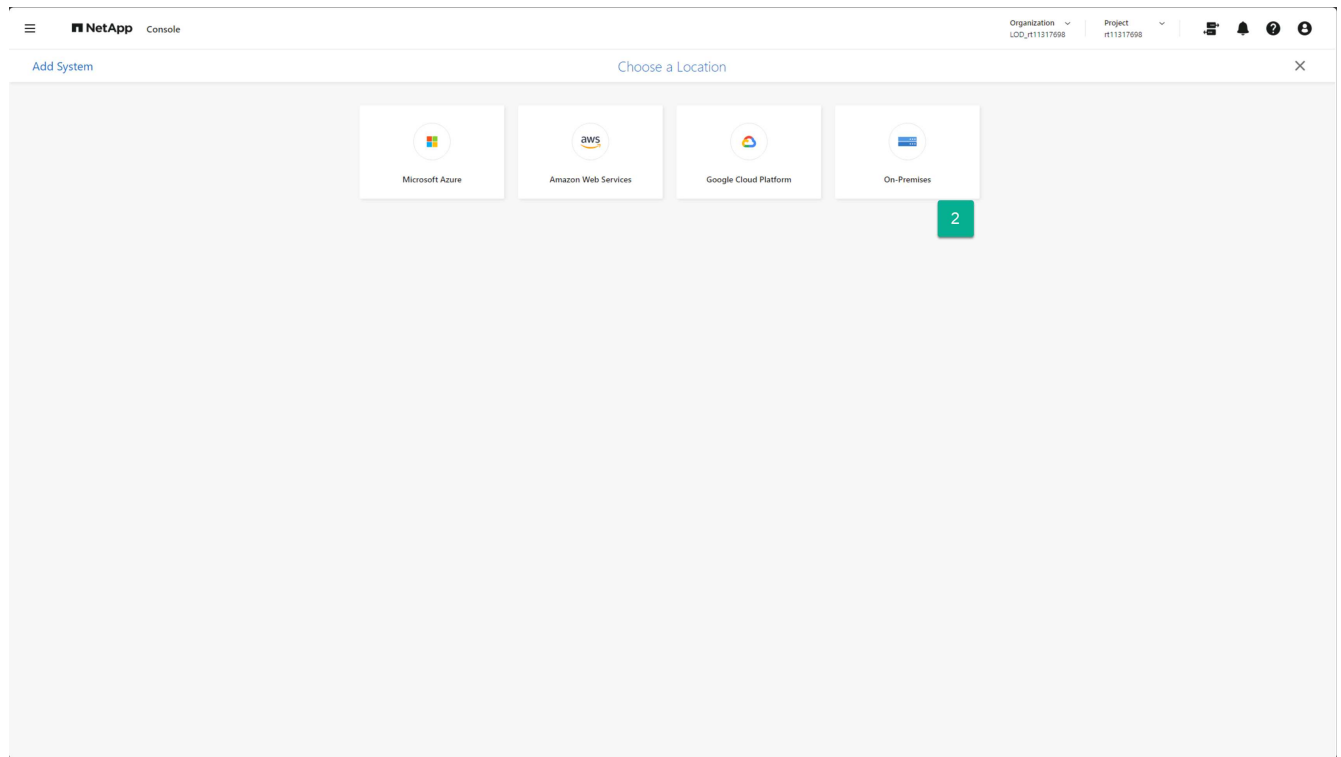
NetApp Consoleシステムにオンプレミスのストレージアレイを追加する

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。

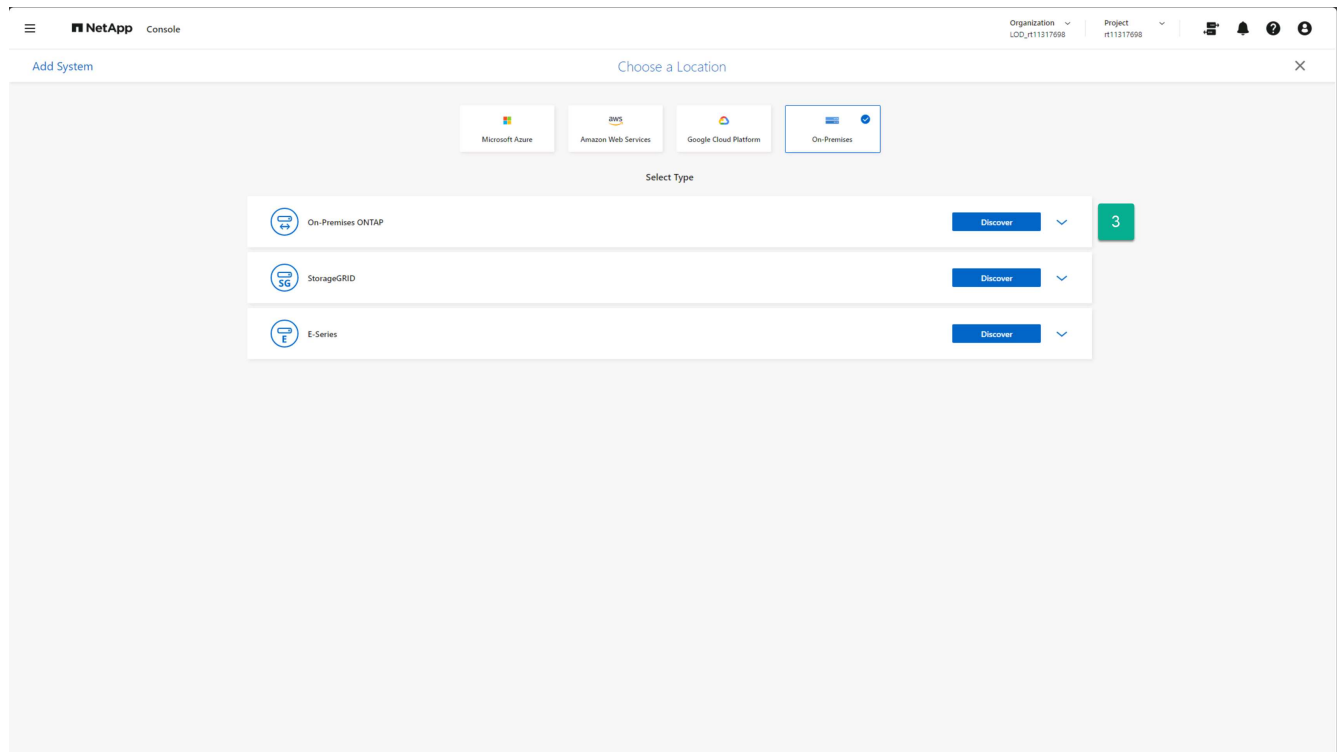
1. NetApp Consoleシステム ページから、[システムの追加] を選択します。



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. 「クラスタの検出」 ページで、次の情報を入力します。

- ONTAPアレイクラスタ管理ポートのIPアドレス
- 管理者のユーザー名
- 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。

NetApp Console

Organization: LCO_r11317698 | Project: r11317698

Discover Cluster

ONTAP Cluster IP

User Name: admin

Password

4

5

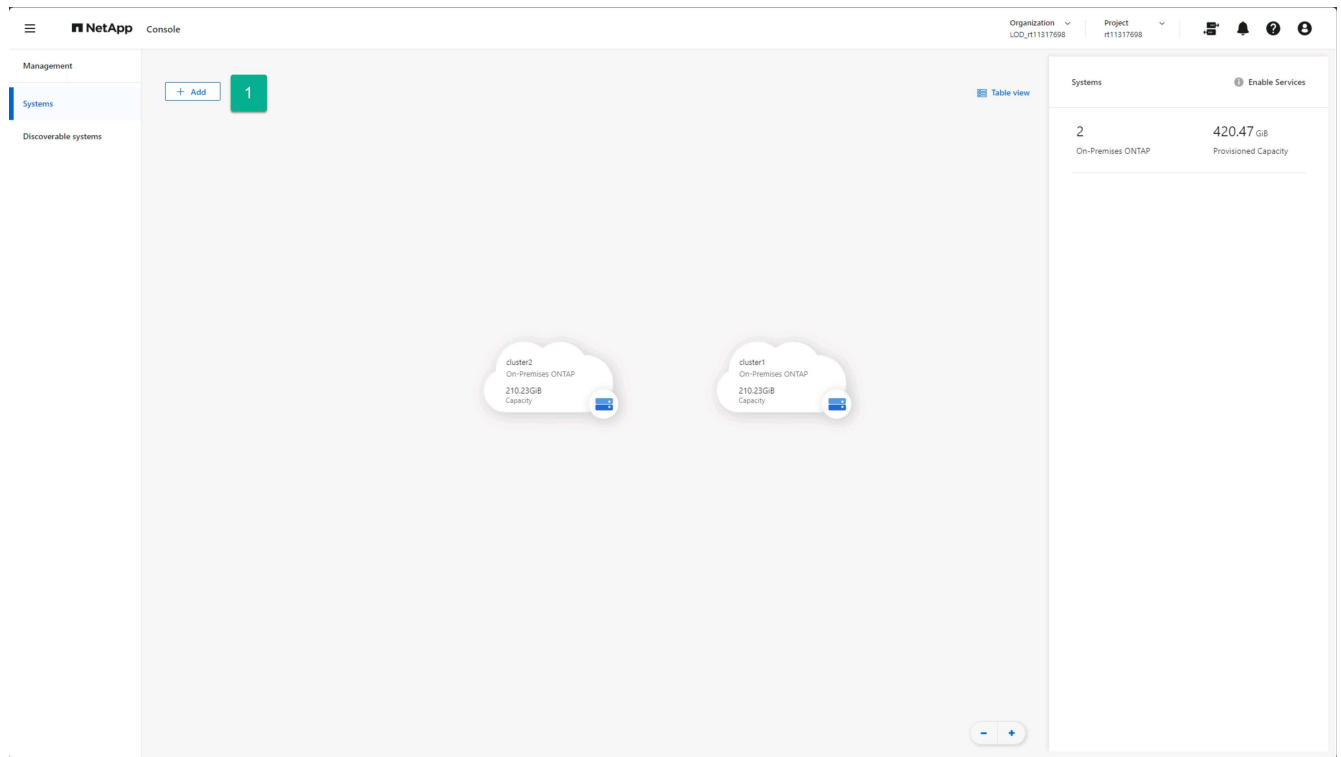
Discover

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。

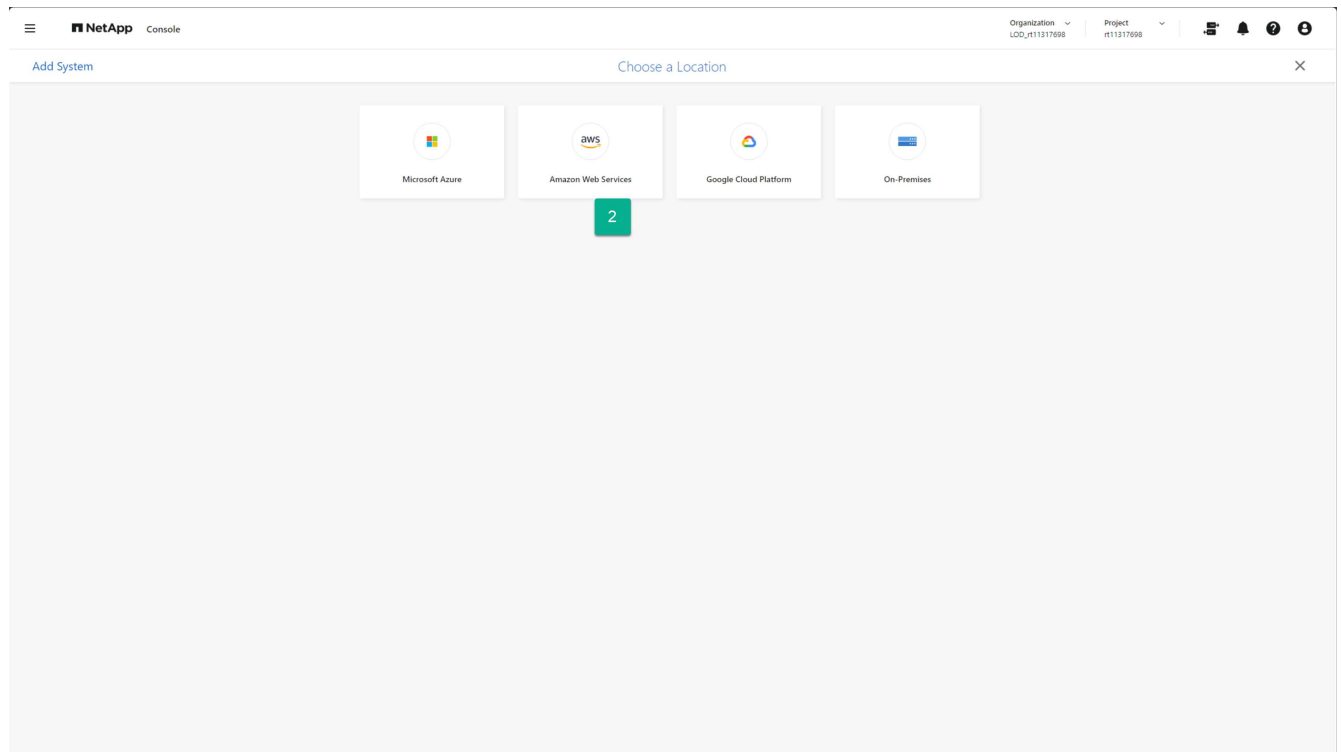
Amazon FSx for NetApp ONTAPストレージインスタンスを**NetApp Console**システムに追加する

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。

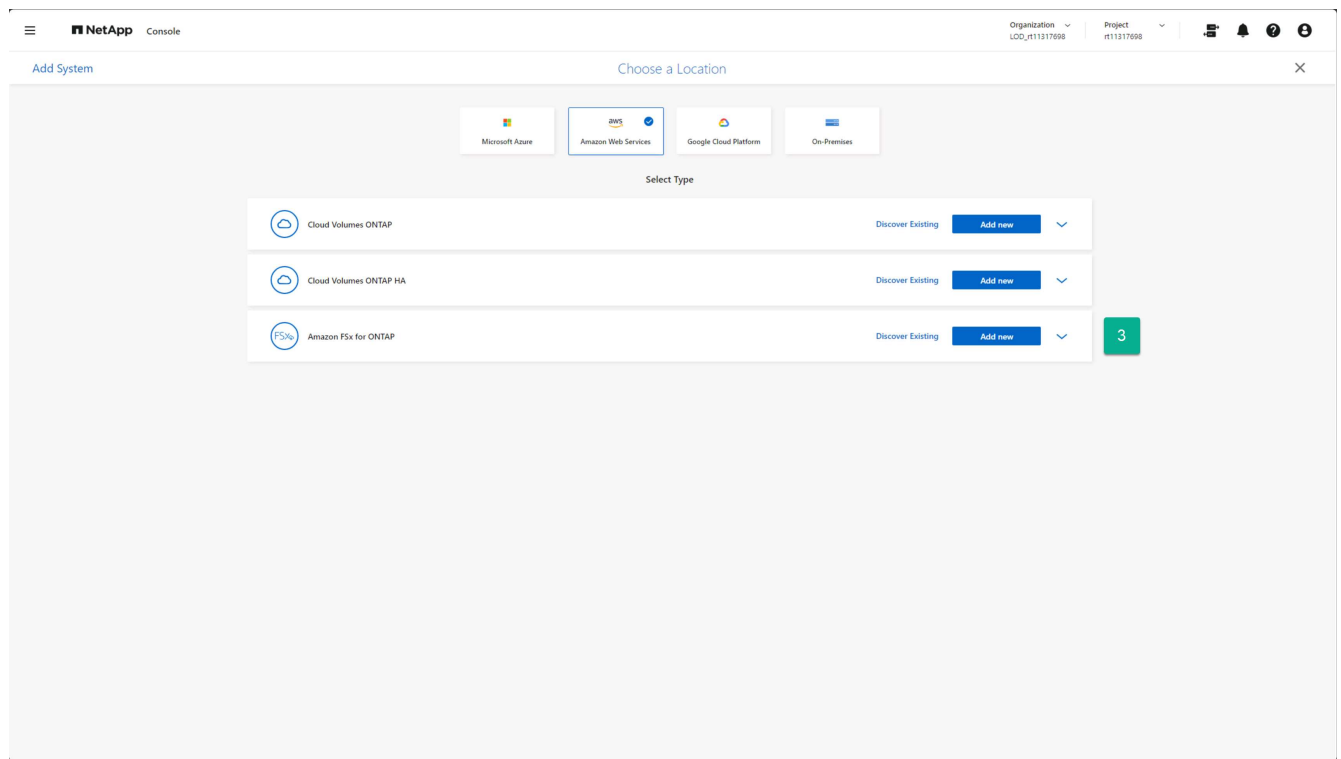
1. NetApp Consoleシステム ページから、[システムの追加] を選択します。



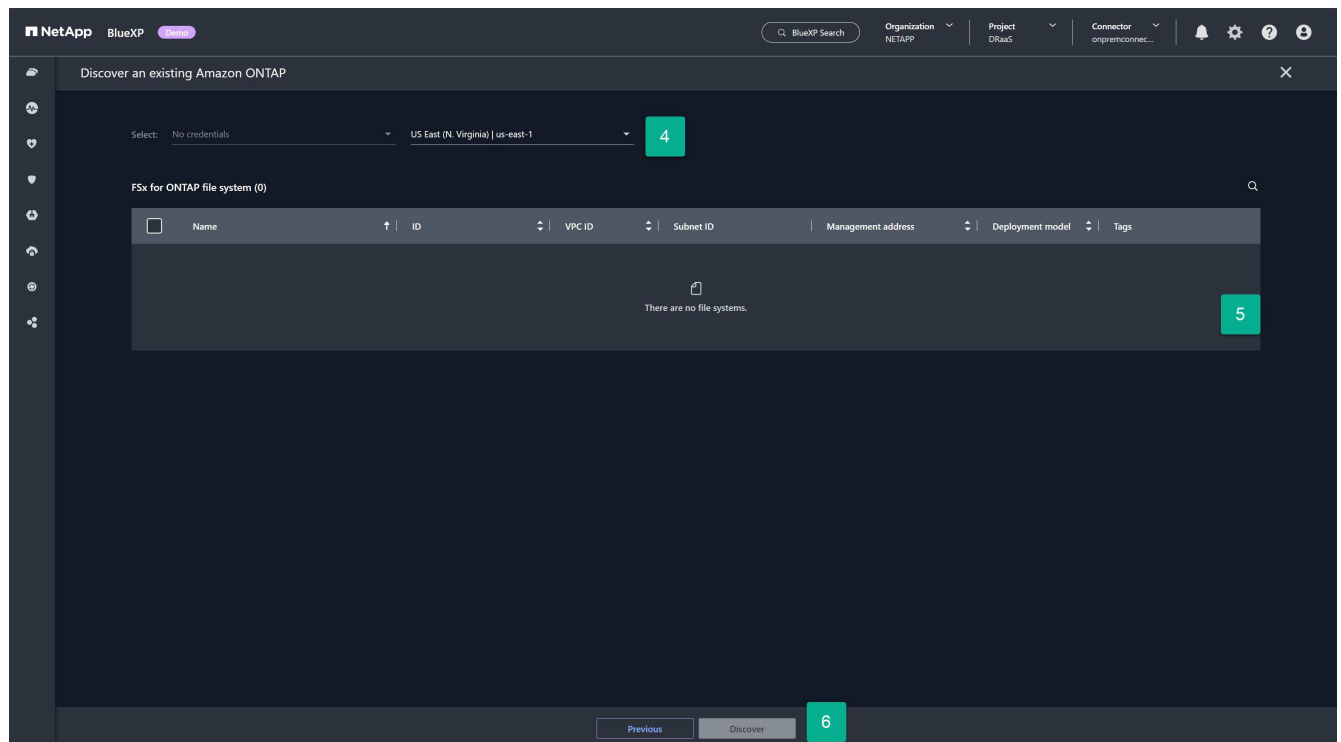
2. 「システムの追加」 ページから、**Amazon Web Services** カードを選択します。



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。

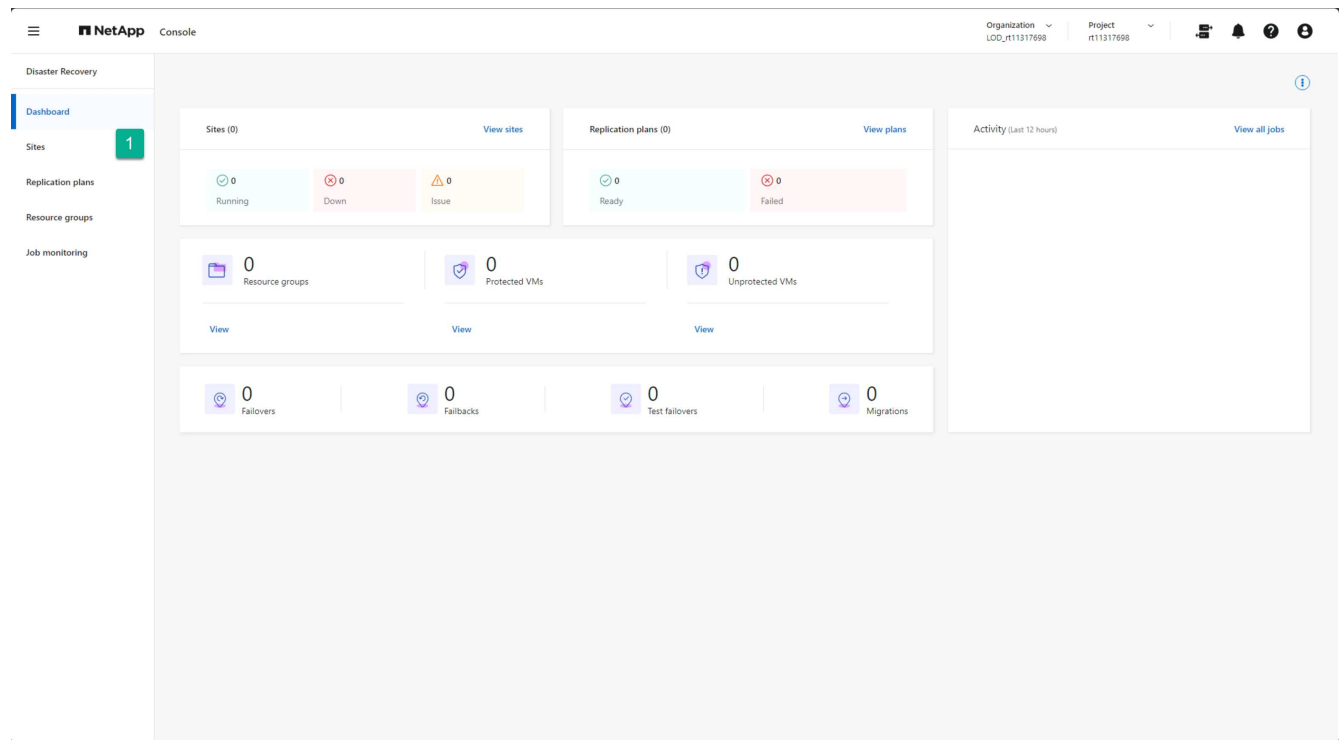
- 実稼働 vCenter クラスターが存在する各実稼働データセンターを表すサイト
- Amazon EVS/ Amazon FSx for NetApp ONTAPクラウドデータセンターのサイト

オンプレミスサイトを作成する

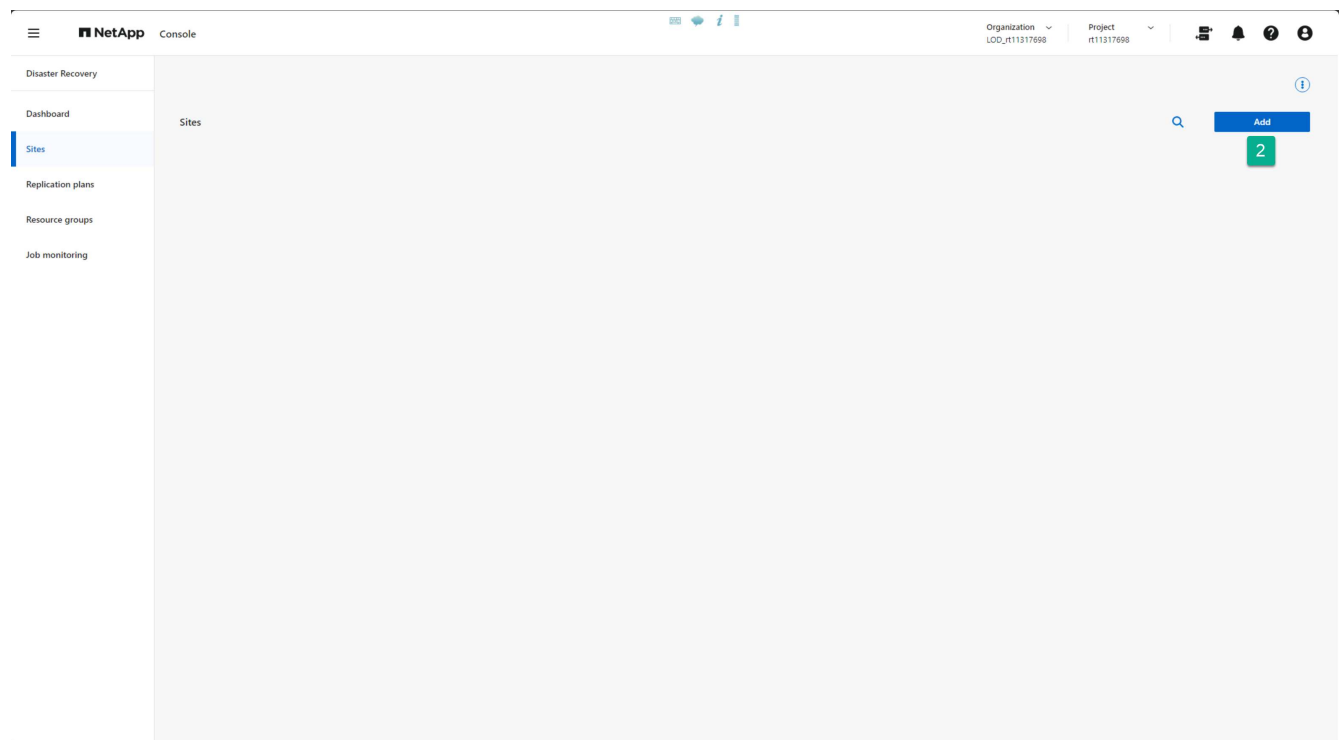
本番環境の vCenter サイトを作成します。

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。



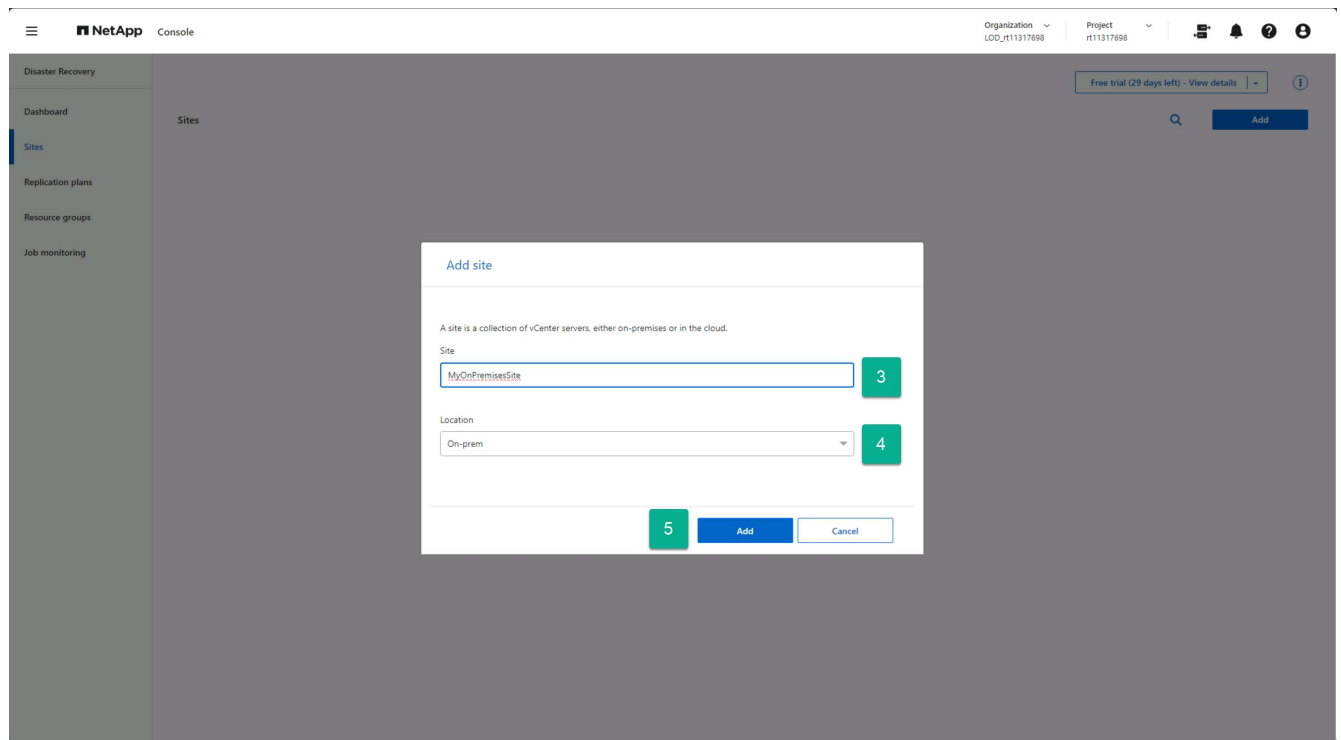
3. [サイト] オプションから [追加] を選択します。



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。

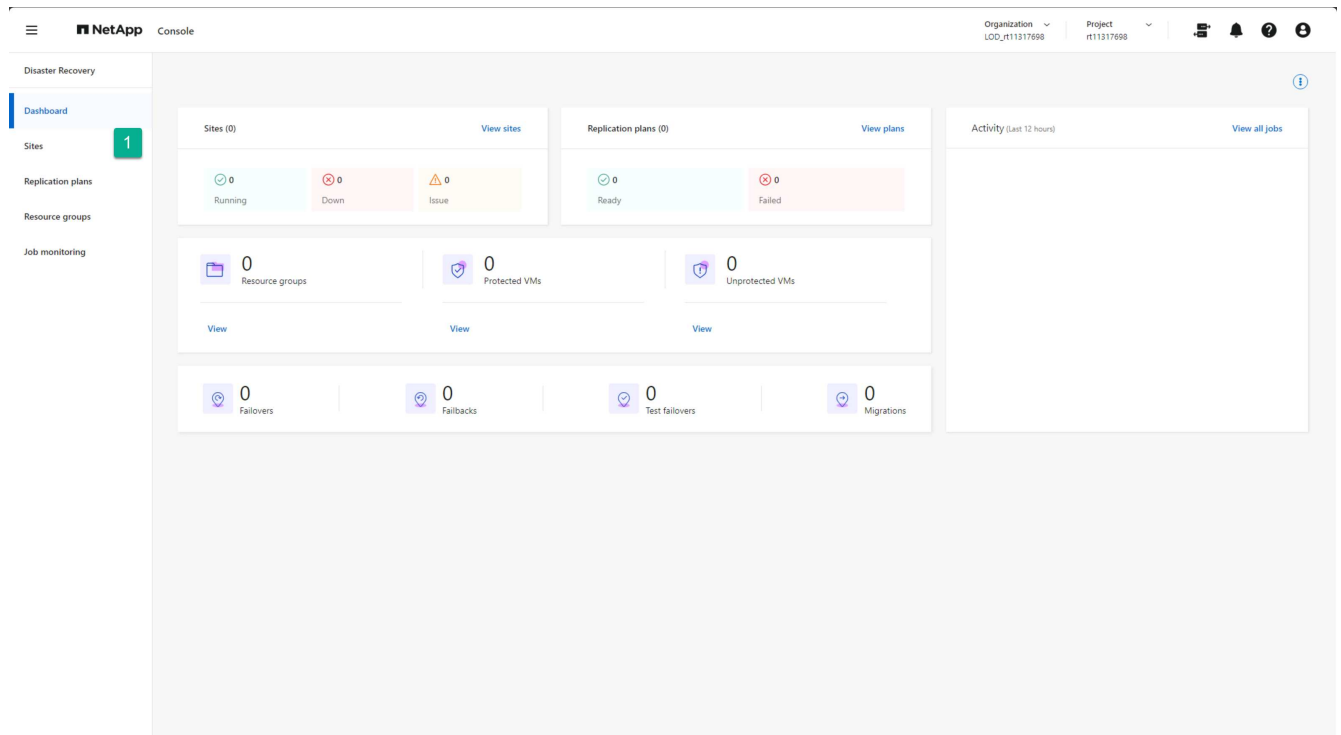


他に本番環境の vCenter サイトがある場合は、同じ手順で追加できます。

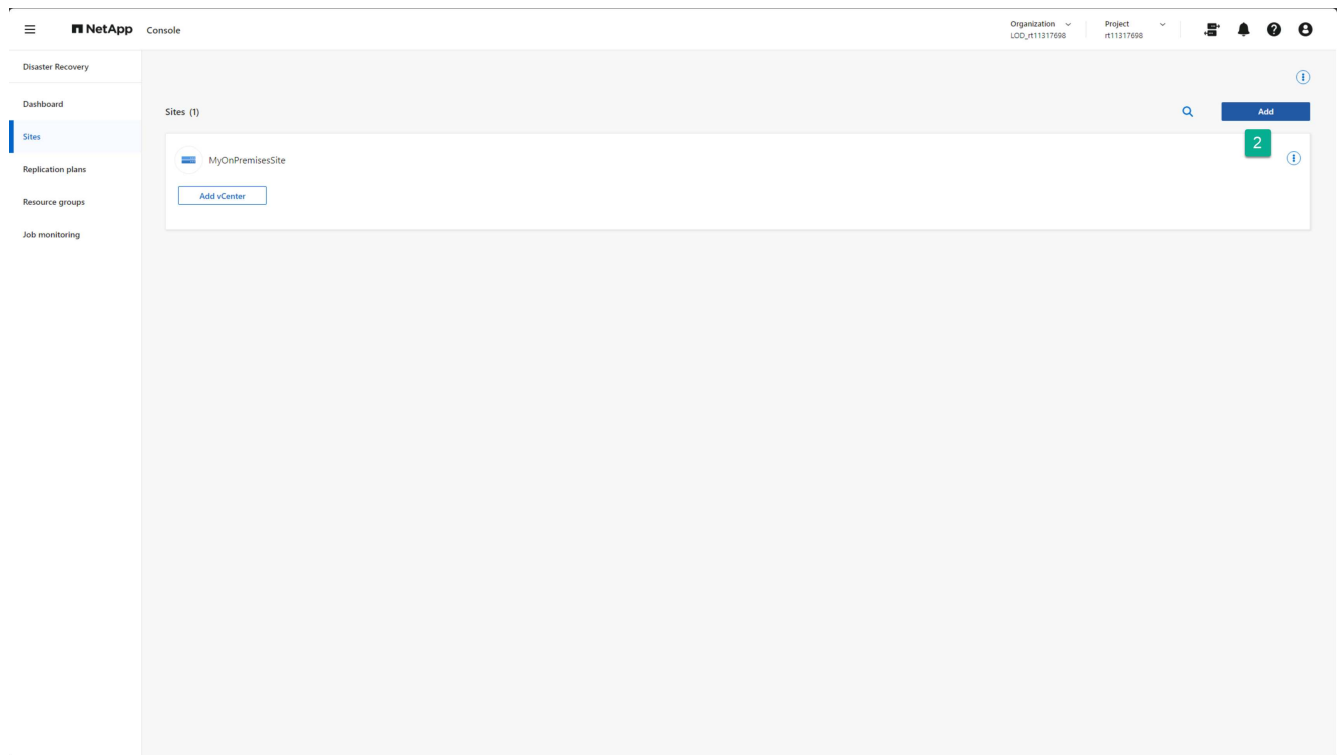
Amazonクラウドサイトを作成する

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。

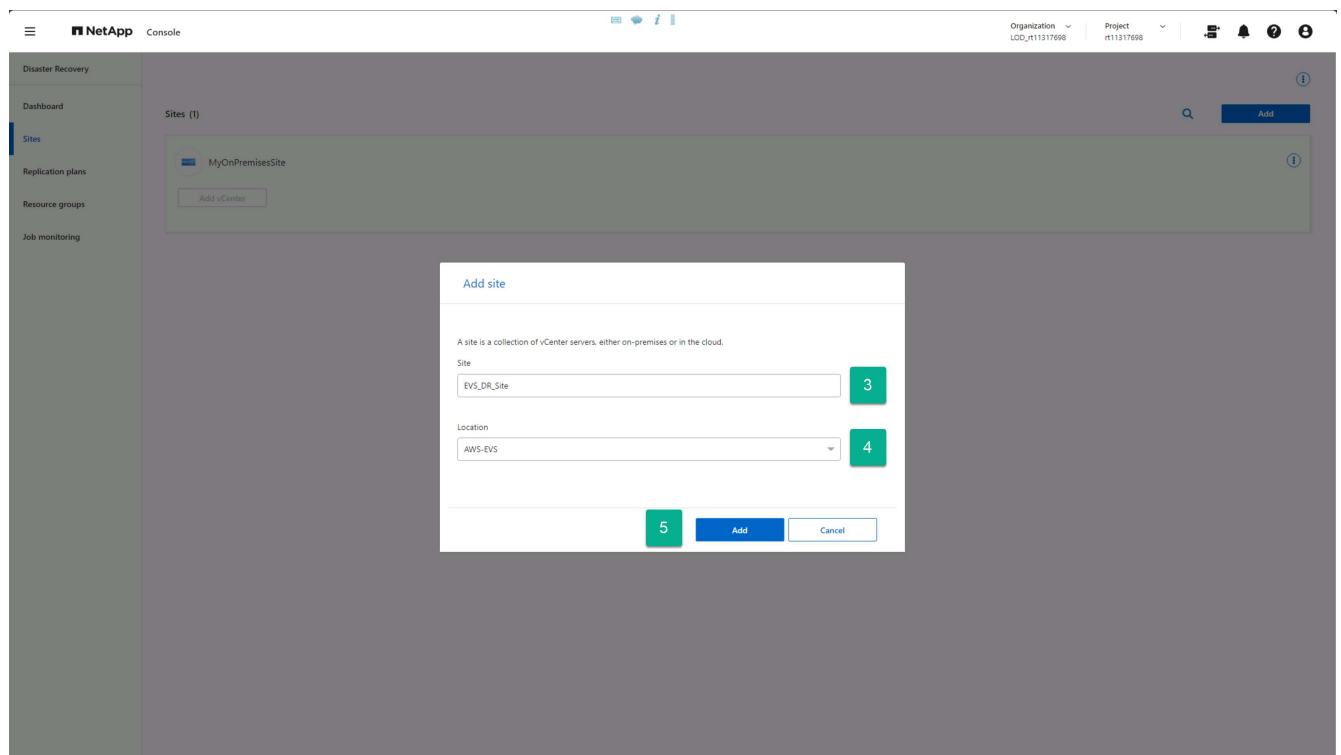
1. NetApp Disaster Recoveryの任意のページから、サイト オプションを選択します。



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

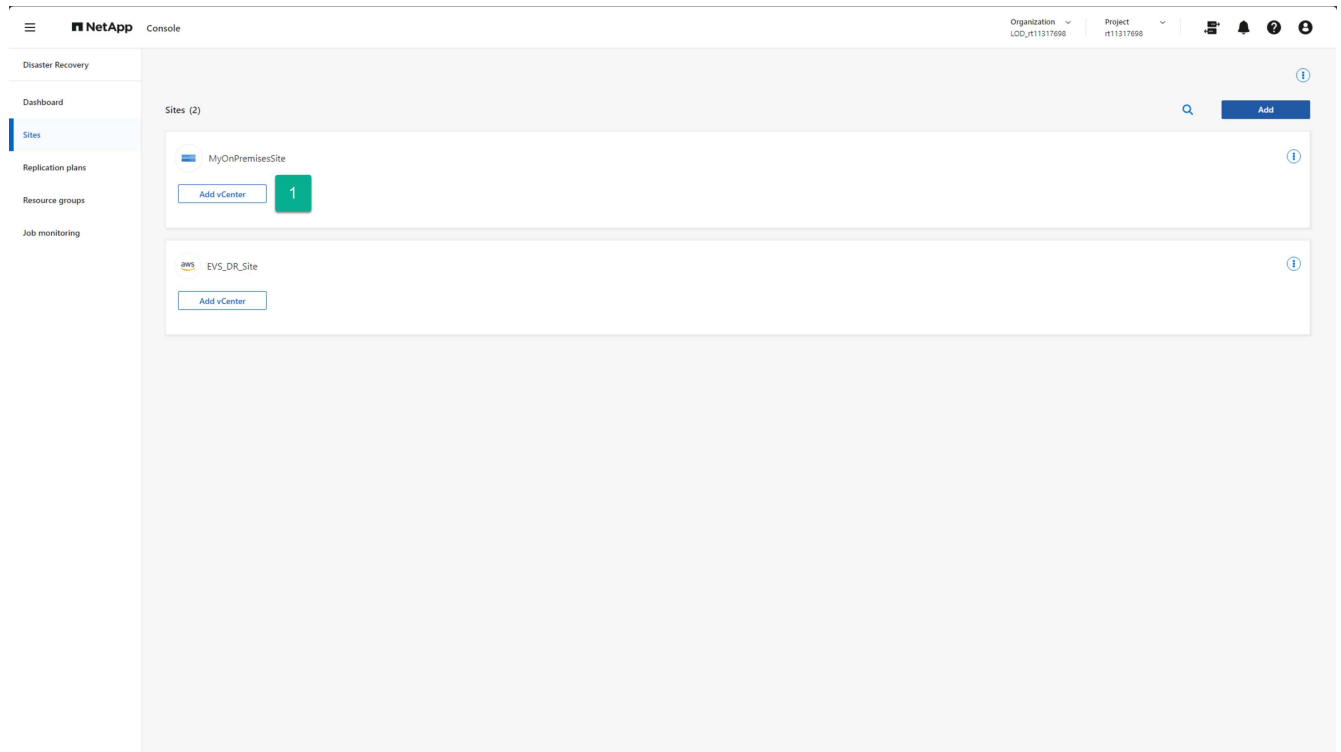
これで、本番 (ソース) サイトと DR (宛先) サイトが作成されました。

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

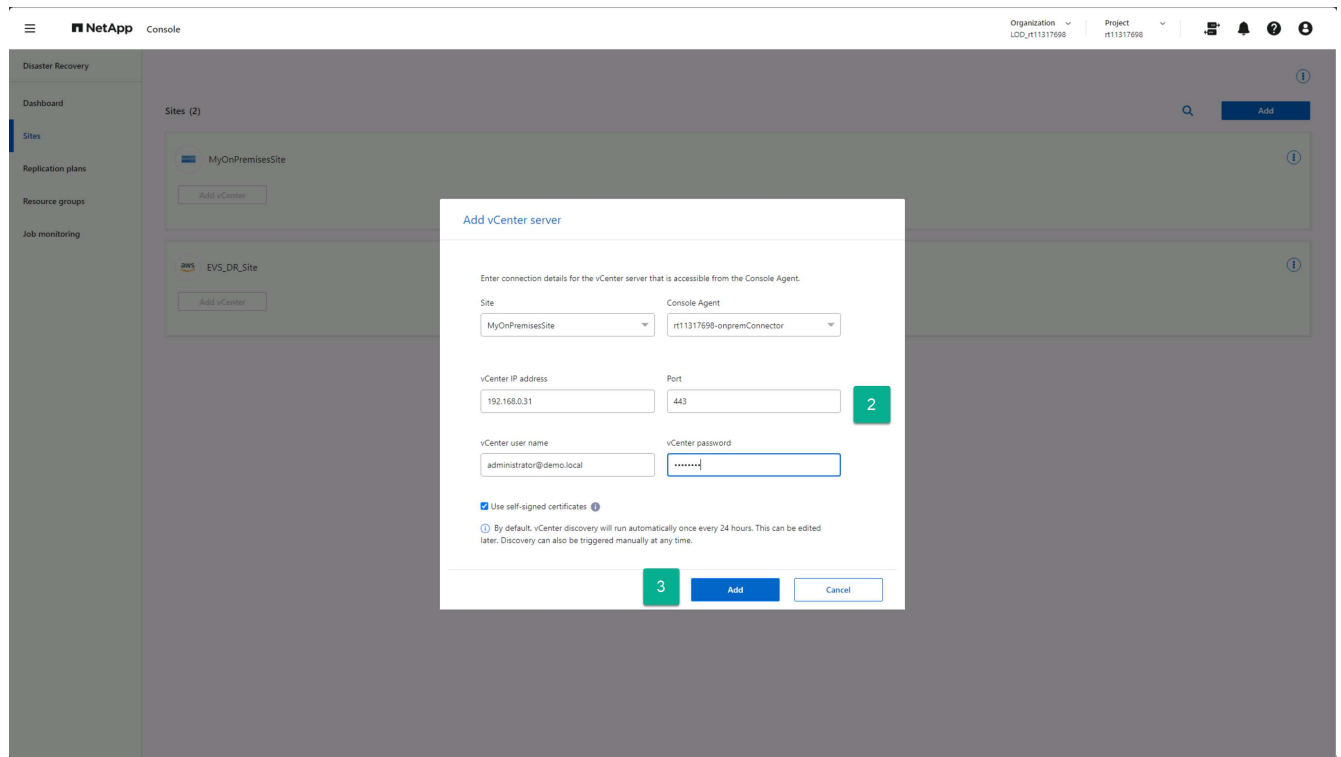
サイトが作成されたら、NetApp Disaster Recoveryの各サイトに vCenter クラスターを追加します。各サイトを作成するときに、各サイトの種類を指定しました。これにより、NetApp Disaster Recovery は、各サイト タイプでホストされている vCenter に必要なアクセス タイプを把握できるようになります。Amazon EVS の利点の 1 つは、Amazon EVS vCenter とオンプレミスの vCenter の間に実質的な違いがないことです。どちらも同じ接続および認証情報が必要です。

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 クラスター 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。



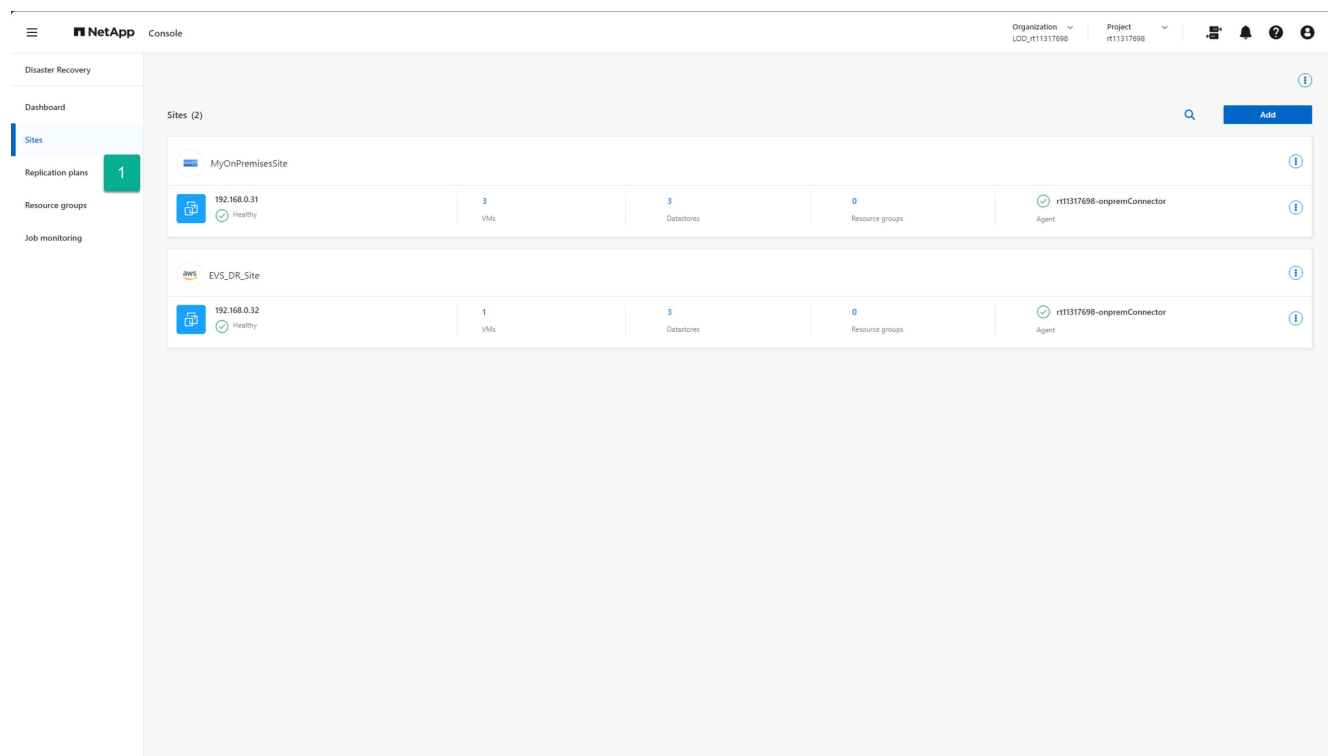
Amazon EVS のレプリケーション プランを作成する

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

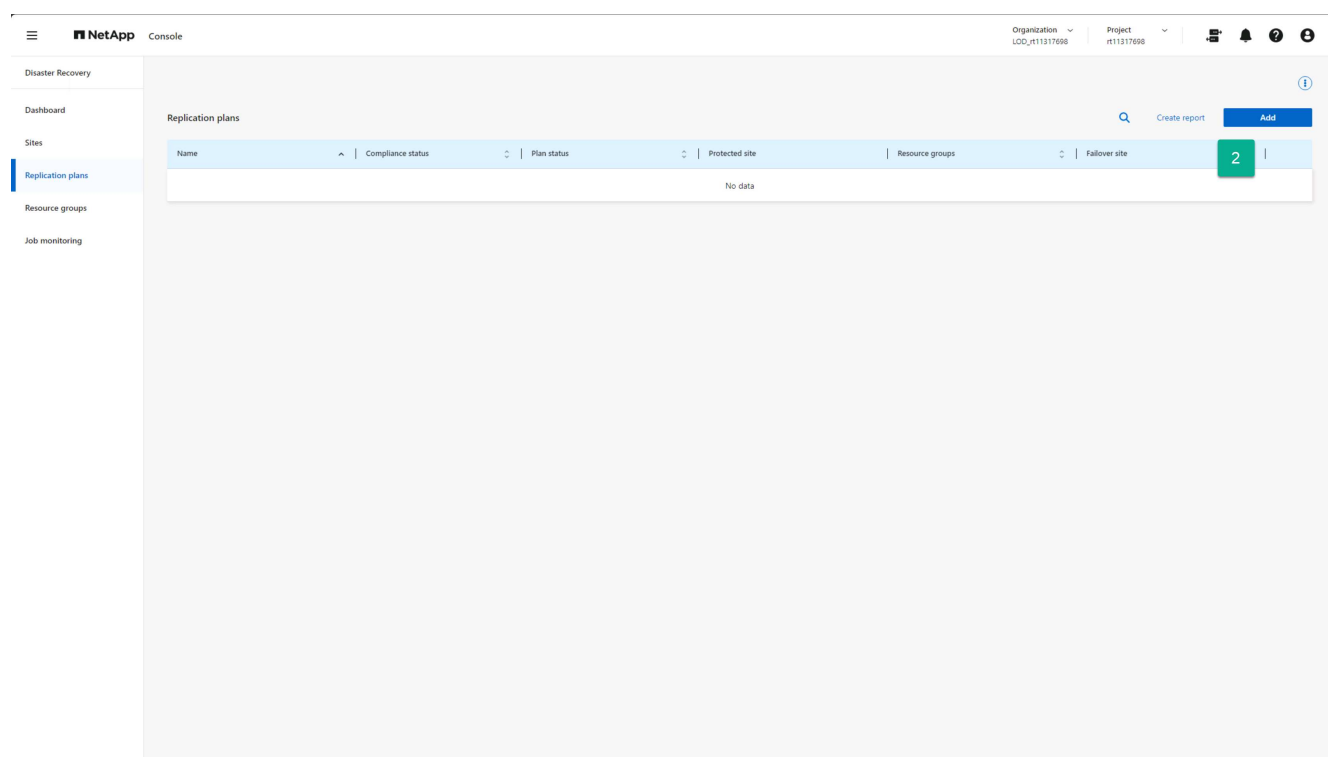
オンプレミスサイトで保護する vCenter があり、DR の宛先として使用できるAmazon FSx for NetApp ONTAPを使用するように設定された Amazon EVS サイトがある場合は、オンプレミスサイト内の vCenter クラスターでホストされている VM のセットを保護するためのレプリケーションプラン (RP) を作成できます。

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。

The screenshot shows the NetApp Disaster Recovery console interface. The sidebar on the left has 'Replication plans' selected. The main area displays the 'Add replication plan' wizard with four steps: 1. 'Replication plan name' (EVS_DR_Plan), 2. 'Source vCenter' (192.168.0.31), 3. 'Target vCenter' (192.168.0.32), and 4. 'Next' button. A diagram shows data replication from a server icon to a cloud icon.

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。

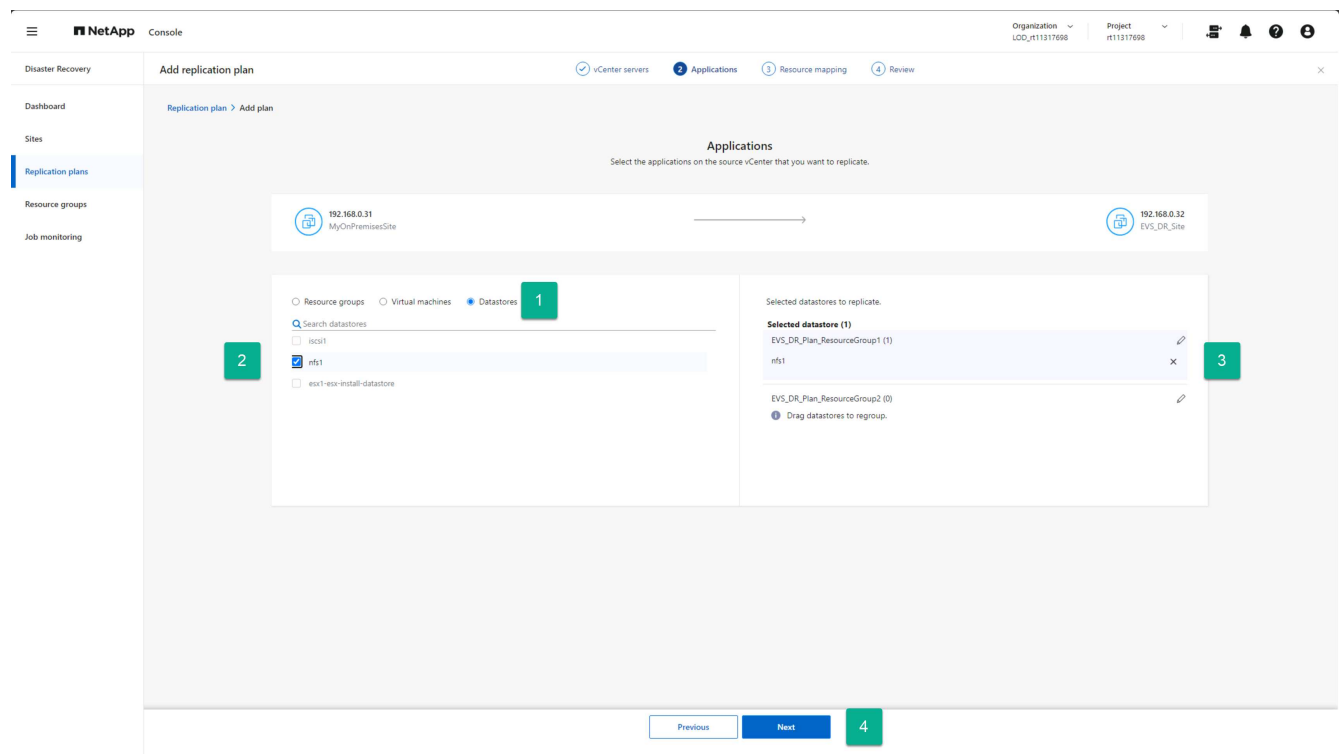
- 個々の **VM** を選択: 仮想マシン ボタンをクリックすると、保護する個々の VM を選択できます。各 VM を選択すると、サービスによって画面の右側にあるデフォルトのリソース グループに追加されます。
- 以前に作成したリソース グループを選択: NetApp Disaster Recoveryメニューの[リソース グループ] オプションを使用して、事前にカスタム リソース グループを作成できます。他の 2 つの方法を使用して、レプリケーション プラン プロセスの一部としてリソース グループを作成できるため、これは必須ではありません。詳細については、["レプリケーションプランを作成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

- **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。

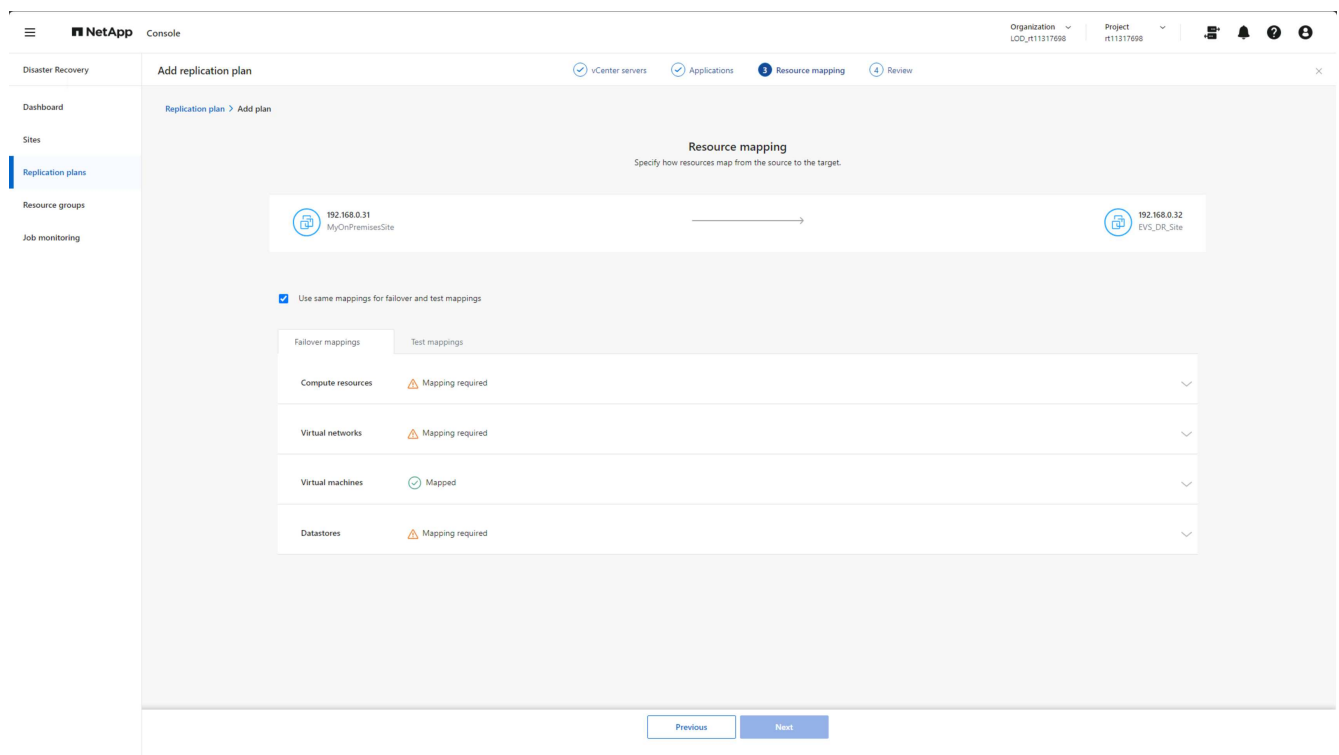
- コンピューティングリソース
- 仮想ネットワーク
- VM再設定
- データストアのマッピング

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。

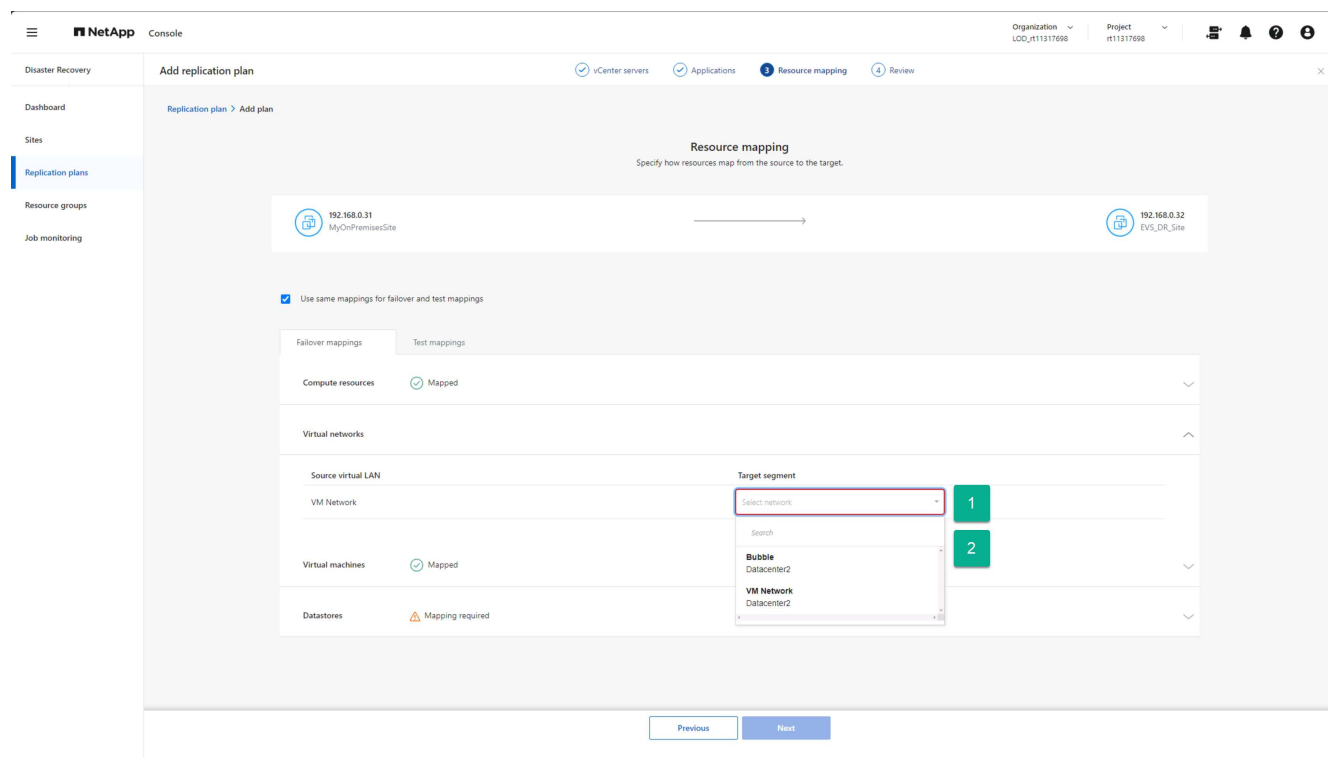
The screenshot displays the NetApp Disaster Recovery console's 'Resource mapping' step. The interface features a sidebar on the left with 'Replication plans' selected. The top navigation bar includes 'vCenter servers', 'Applications', 'Resource mapping', and 'Review'. The main content area is titled 'Resource mapping' and shows a mapping from 'MyOnPremisesSite' to 'EVS_DR_Site'. Below this, there are checkboxes for 'Use same mappings for failover and test mappings' and tabs for 'Failover mappings' and 'Test mappings'. The 'Compute resources mapping' section is expanded, showing a table with columns: 'Source datacenter and cluster', 'Target datacenter', 'Target cluster', 'Target host (optional)', and 'Target VM folder (optional)'. The table contains one row with 'Datacenter1:Cluster1' as the source, and 'Datacenter2', 'Cluster2', and 'Select host' as targets. Below the table, there are sections for 'Virtual networks' (Mapping required), 'Virtual machines' (Mapped), and 'Datastores' (Mapping required). At the bottom, there are 'Previous' and 'Next' buttons.

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す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 情報で変更された通りに、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。

NetApp Console

Organization: LCO_r11317698 Project: r11317698

Disaster Recovery Add replication plan

✓ vCenter servers ✓ Applications 1 Resource mapping 4 Review

Falover mappings Test mappings

Compute resources Mapped

Virtual networks Mapped

Virtual machines

IP address type: Static Target IP: Same as source

☐ Use the same credentials for all VMs

☐ Use the same script for all VMs

Target VM prefix: Optional Target VM suffix: Optional Preview: Sample VM name

Source VM	Operating system	CPUs	RAM	Boot order	Boot delay (mins between 0 and 10)	Create application consistent replicas	Scripts	Credentials
EVS_DR_Plan_ResourceGroup1								
Linux1	Linux	1	2 GiB	1	0	<input type="checkbox"/>	None	Not required
Linux4	Linux	1	2 GiB	3	5	<input type="checkbox"/>	None	Not required
Linux3	Linux	1	2 GiB	2	5	<input type="checkbox"/>	None	Not required

1 - 3 of 3 << < 1 > >>

Previous Next

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。

NetApp Console

Organization: LCO_r11317698 Project: r11317698

Disaster Recovery Add replication plan

✓ vCenter servers ✓ Applications 1 Resource mapping 4 Review

Falover mappings Test mappings

Compute resources Mapped

Virtual networks Mapped

Virtual machines

IP address type: Static Target IP: Same as source

☐ Use the same credentials for all VMs

☐ Use the same script for all VMs

Target VM prefix: Optional Target VM suffix: Optional Preview: Sample VM name

Source VM	Operating system	CPUs	RAM	Boot order	Boot delay(mins between 0 and 10)	Create application consistent replicas	Scripts	Credentials
Linux1	Linux	1	2 GiB	1	0	<input type="checkbox"/>	None	Not required
Linux4	Linux	1	2 GiB	3	5	<input type="checkbox"/>	None	Not required
Linux3	Linux	1	2 GiB	2	5	<input type="checkbox"/>	None	Not required

1 2

1 - 3 of 3 << < 1 > >>

Previous Next

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

- (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。
- (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。

NetApp Console

Organization: LCO_r11317698 Project: r11317698

Disaster Recovery Add replication plan

✓ vCenter servers ✓ Applications 1 Resource mapping 4 Review

Fallover mappings Test mappings

Compute resources Mapped

Virtual networks Mapped

Virtual machines

IP address type: Static Target IP: Same as source

☐ Use the same credentials for all VMs

☐ Use the same script for all VMs

Target VM prefix: Optional Target VM suffix: Optional Preview: Sample VM name

Source VM	Operating system	CPU's	RAM	Boot order	Boot delay (mins between 0 and 10)	Create application consistent replicas	Scripts	Credentials
15_DR_Plan_ResourceGroup1								
vx1	Linux	1	2 GIB	1	0	<input type="checkbox"/>	None	Not required
vx4	Linux	1	2 GIB	3	5	<input type="checkbox"/>	None	Not required
vx3	Linux	1	2 GIB	2	4	<input type="checkbox"/>	None	Not required

1 2

1 - 3 of 3 << < > >>

Previous Next

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。

NetApp Console

Disaster Recovery | Add replication plan

1 vCenter servers | 2 Applications | 3 Resource mapping | 4 Review

Failover mappings | Test mappings

Compute resources: Mapped

Virtual networks: Mapped

Virtual machines

IP address type: Static | Target IP: Same as source

☐ Use the same credentials for all VMs

☐ Use the same script for all VMs

Target VM prefix: | Optional | Target VM suffix: | Optional | Preview: Sample VM name

source VM	Operating system	CPU	RAM	Boot order	Boot delay (mins between 0 and 10)	Create application consistent replicas	Scripts	Credentials
15_DR_Plan_ResourceGroup1								
vux1	Linux	1	2 GiB	1	0	<input type="checkbox"/>	VM-boot-script.ps1 ✎ Provided ✎	
vux4	Linux	1	2 GiB	1	0	<input type="checkbox"/>	None ✎	Not required
vux3	Linux	1	2 GiB	1	0	<input type="checkbox"/>	None ✎	Not required

1 2 3 1 - 3 of 3

Previous Next

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

- (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。
- 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。
- 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。
- 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。
- (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。
- (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

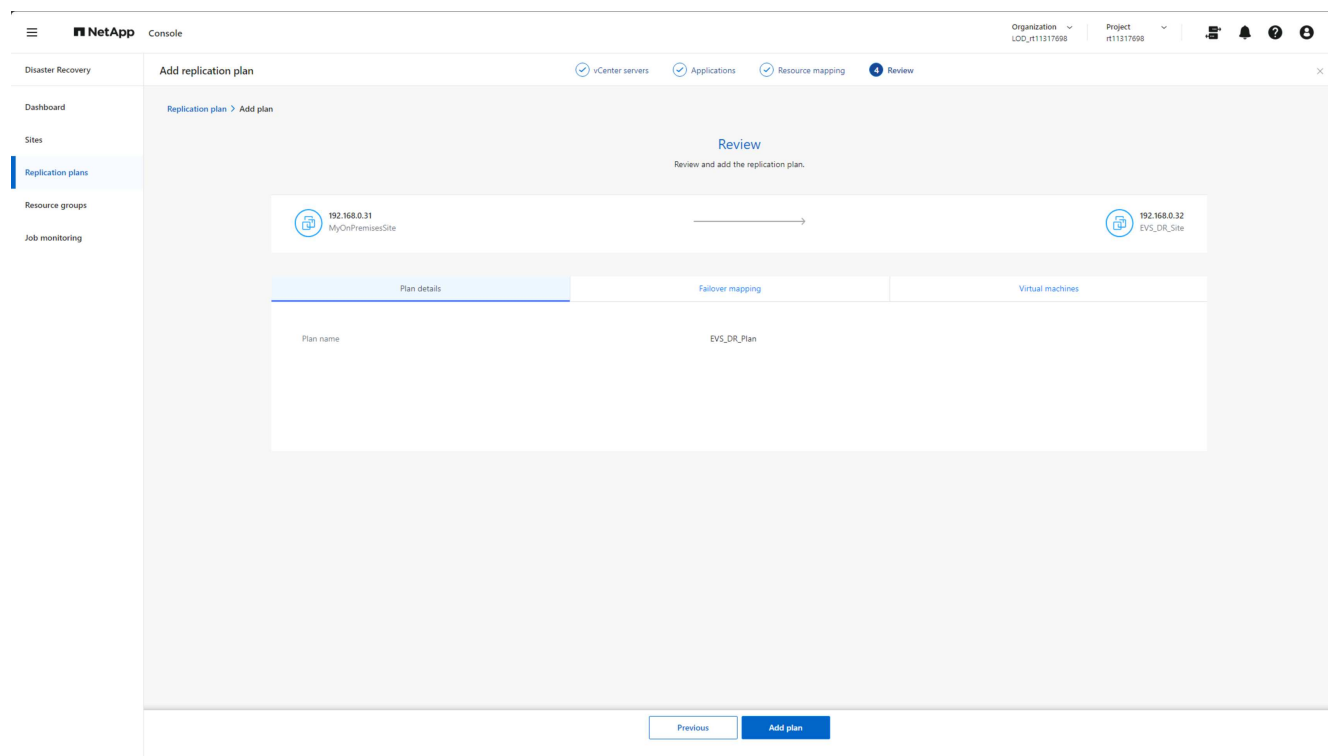
NetApp Disaster Recoveryでレプリケーション プラン情報を追加した後、入力した情報が正しいことを確認します。

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



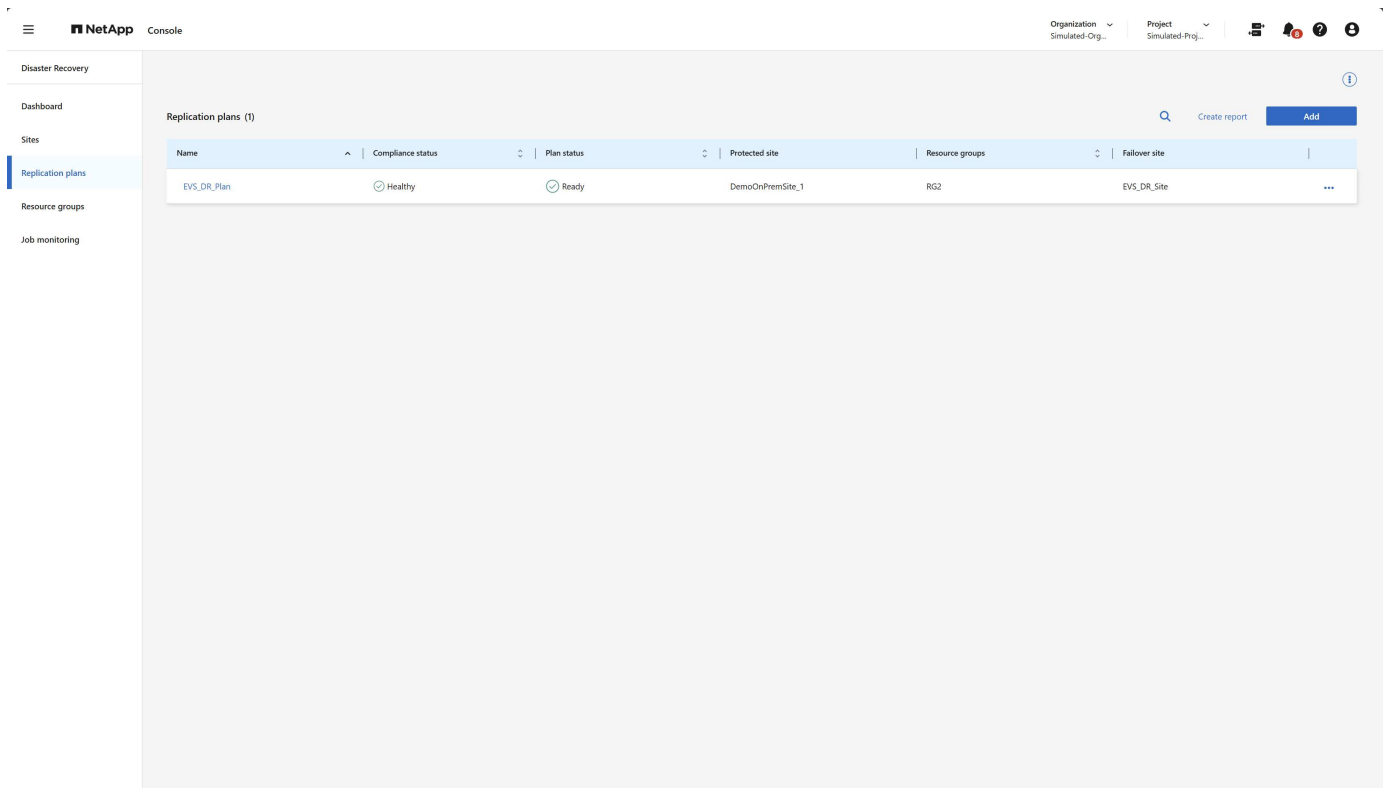
2. すべての設定が正しいことを確認したら、画面下部の*プランの追加*を選択します。

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、定期的に行われます。

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イルオーバーすることです。

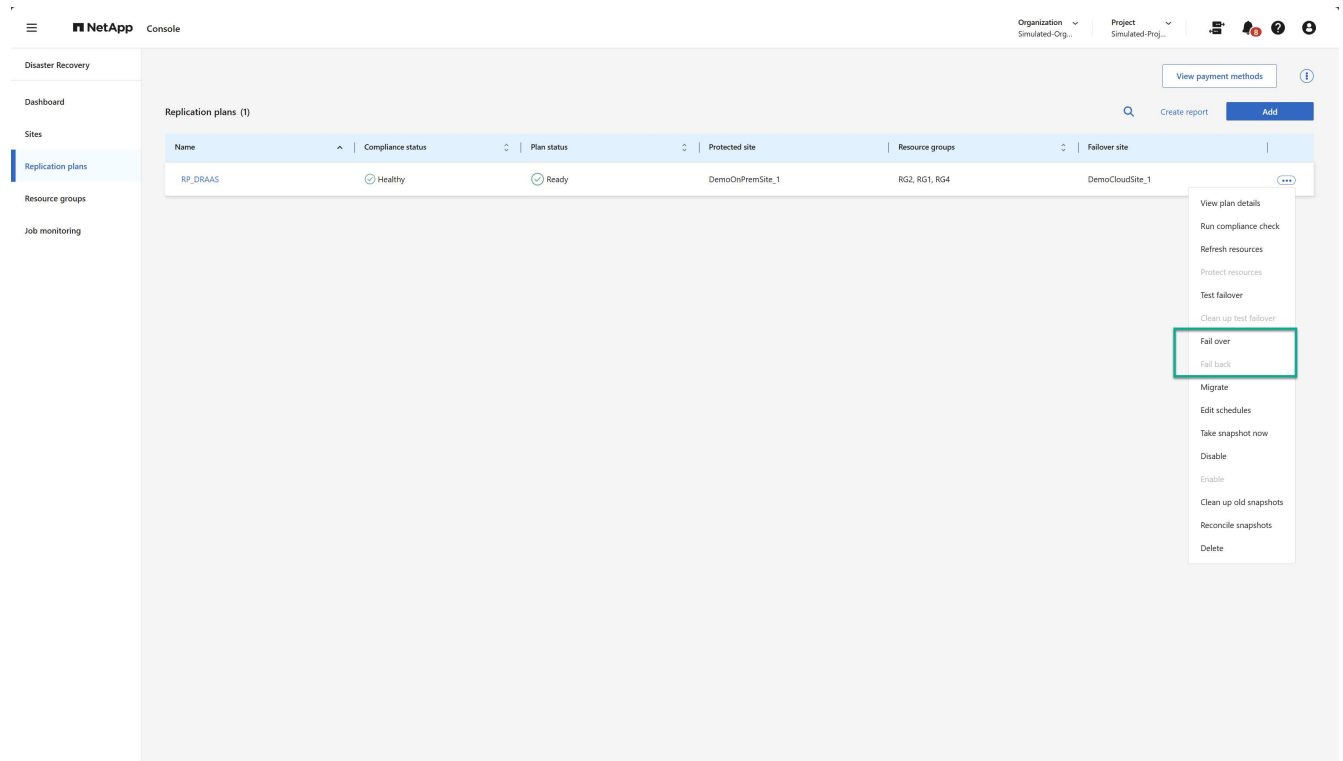
フェイルオーバーは手動で開始されるプロセスです。

フェイルオーバー操作にアクセスする手順

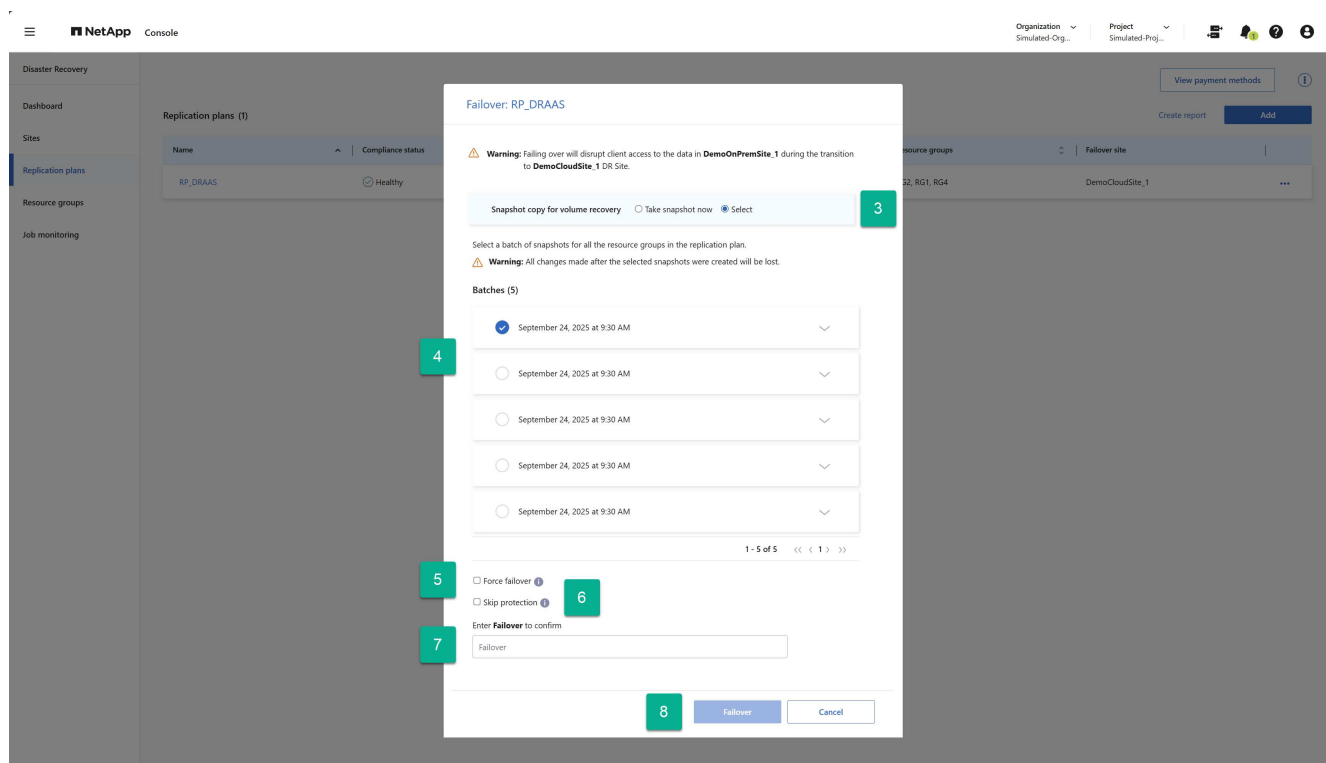
1. NetApp Consoleの左側のナビゲーション バーから、保護 > ディザスタ リカバリ を選択します。
2. NetApp Disaster Recoveryメニューから、レプリケーション プラン を選択します。

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。

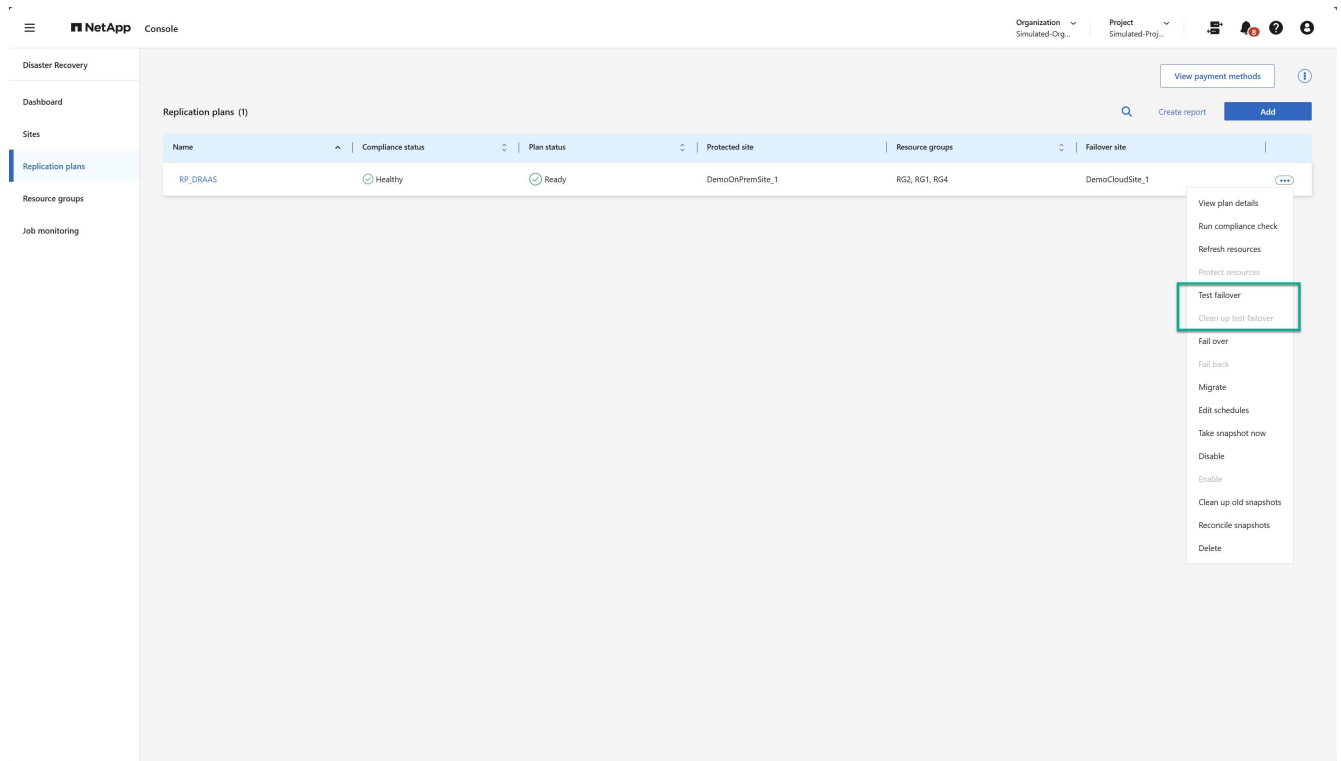
- 実稼働サイトは引き続きアクティブであり、すべての VM は引き続き期待どおりに動作しています。
- 実稼働 VM のNetApp Disaster Recovery保護は継続されます。

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](#)"。

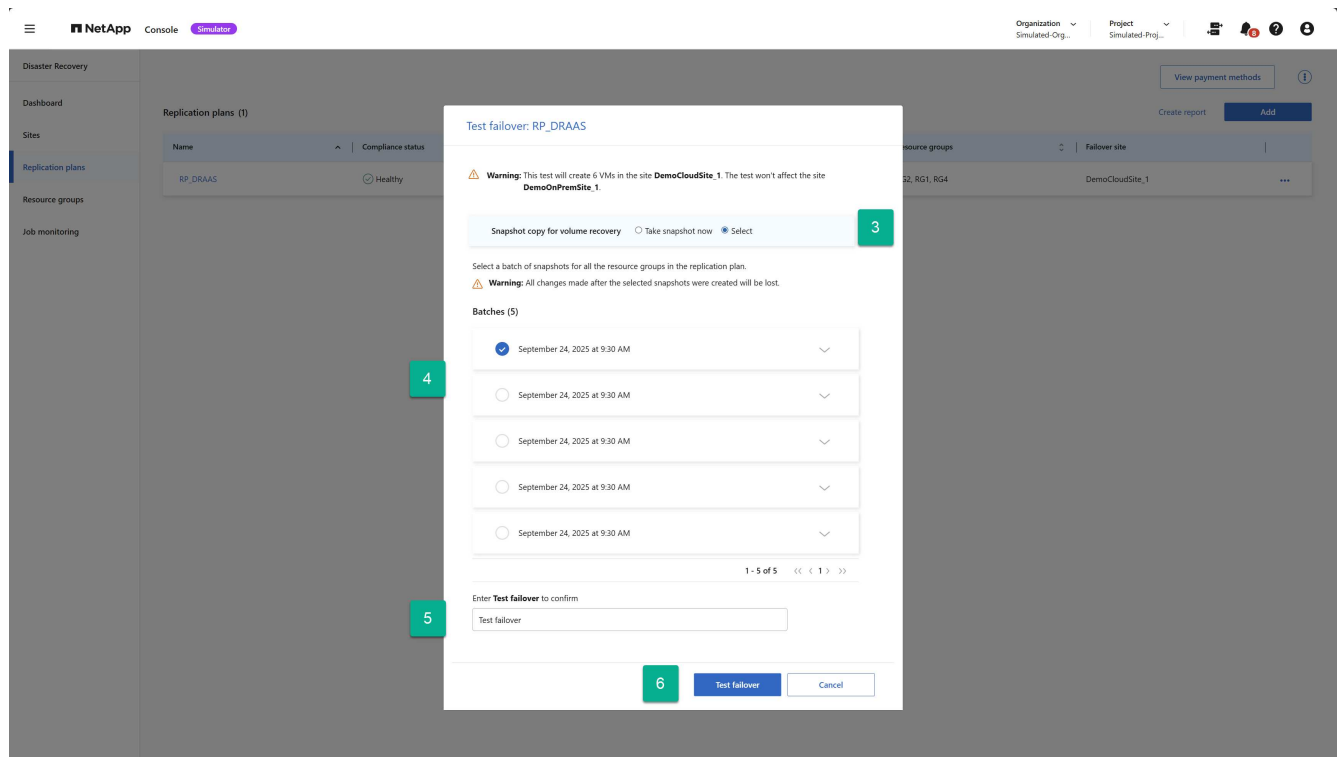
テスト フェイルオーバーを実行する手順は、レプリケーション プランのコンテキスト メニューの[テスト フェイルオーバー] 操作を使用することを除いて、実際のフェイルオーバーを実行する手順と同じです。

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。

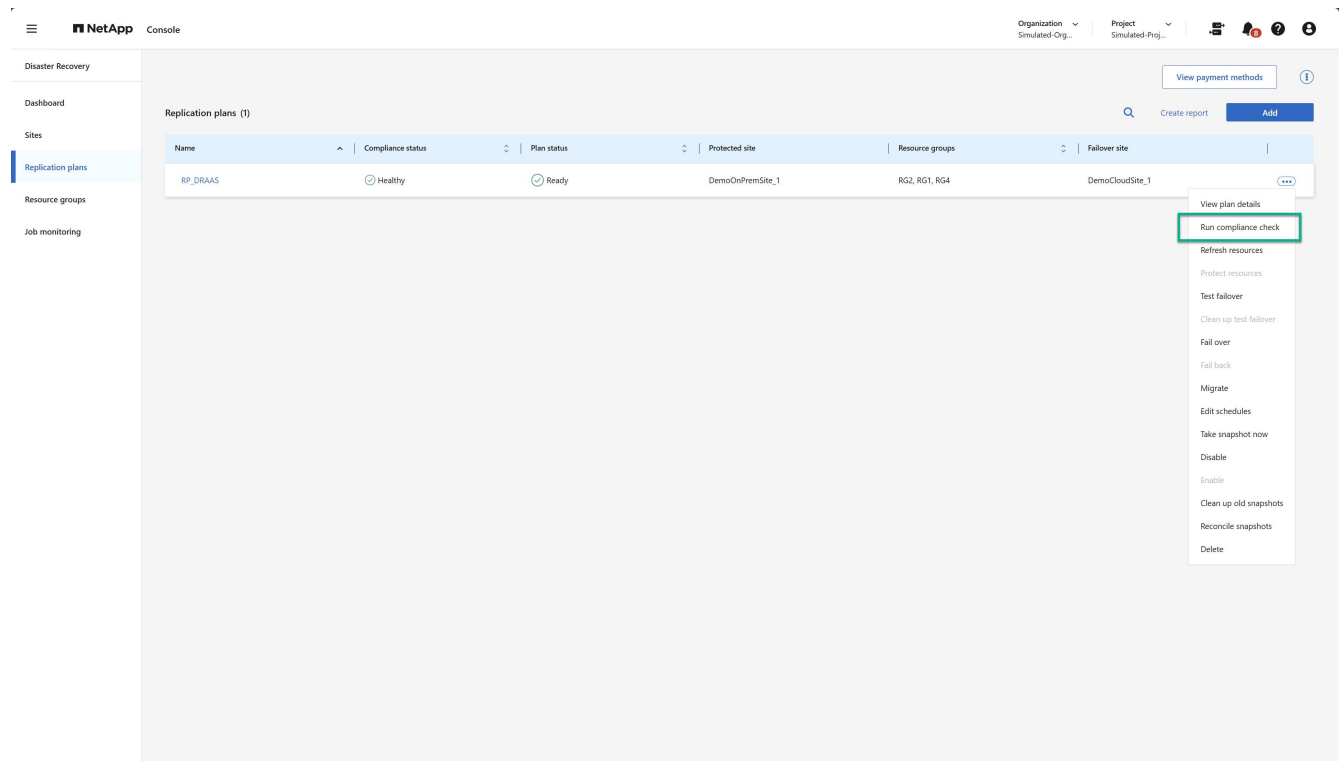


コンプライアンスチェックを実行する

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。



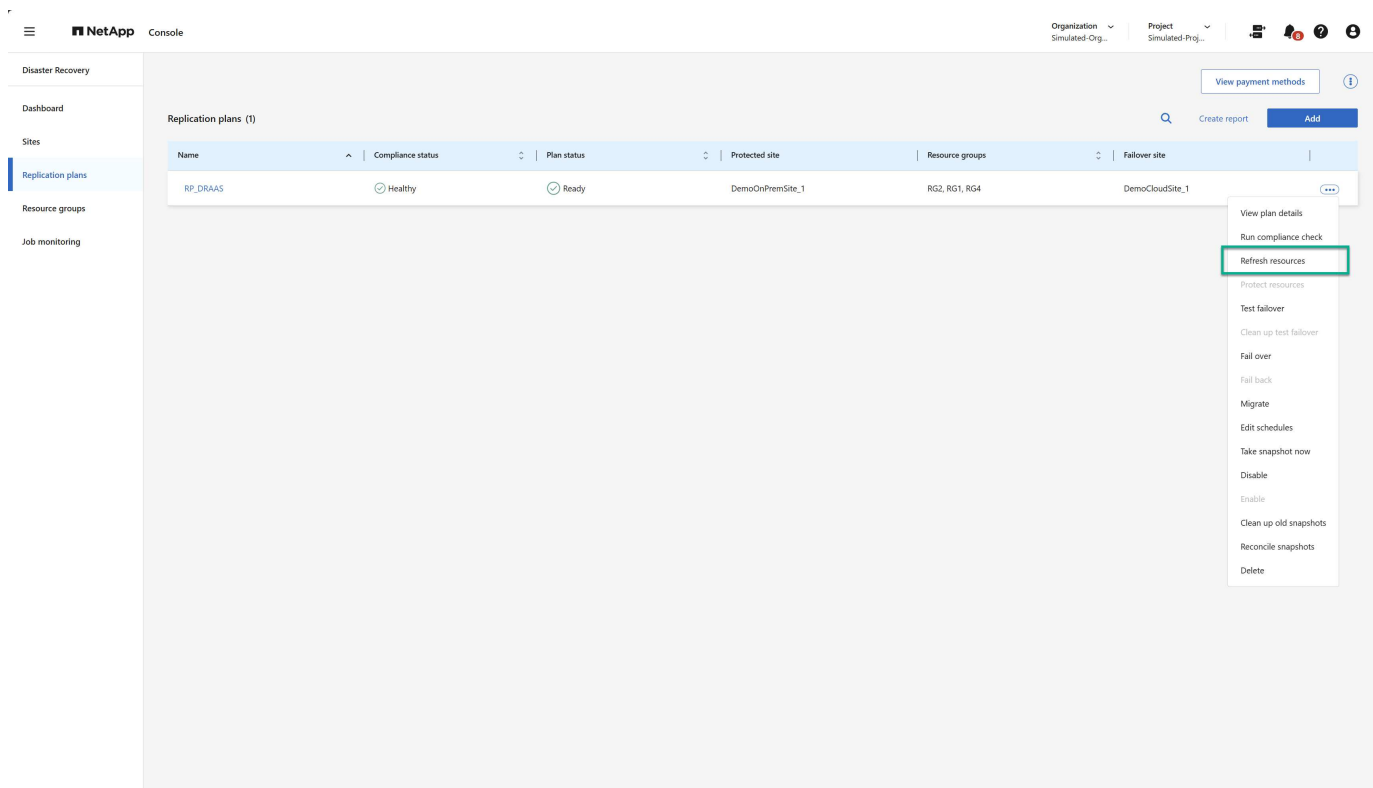
3. NetApp Disaster Recovery がコンプライアンス チェックを自動的に実行する頻度を変更するには、レプリケーション プランの [アクション] メニューから [スケジュールの編集] オプションを選択します。

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。

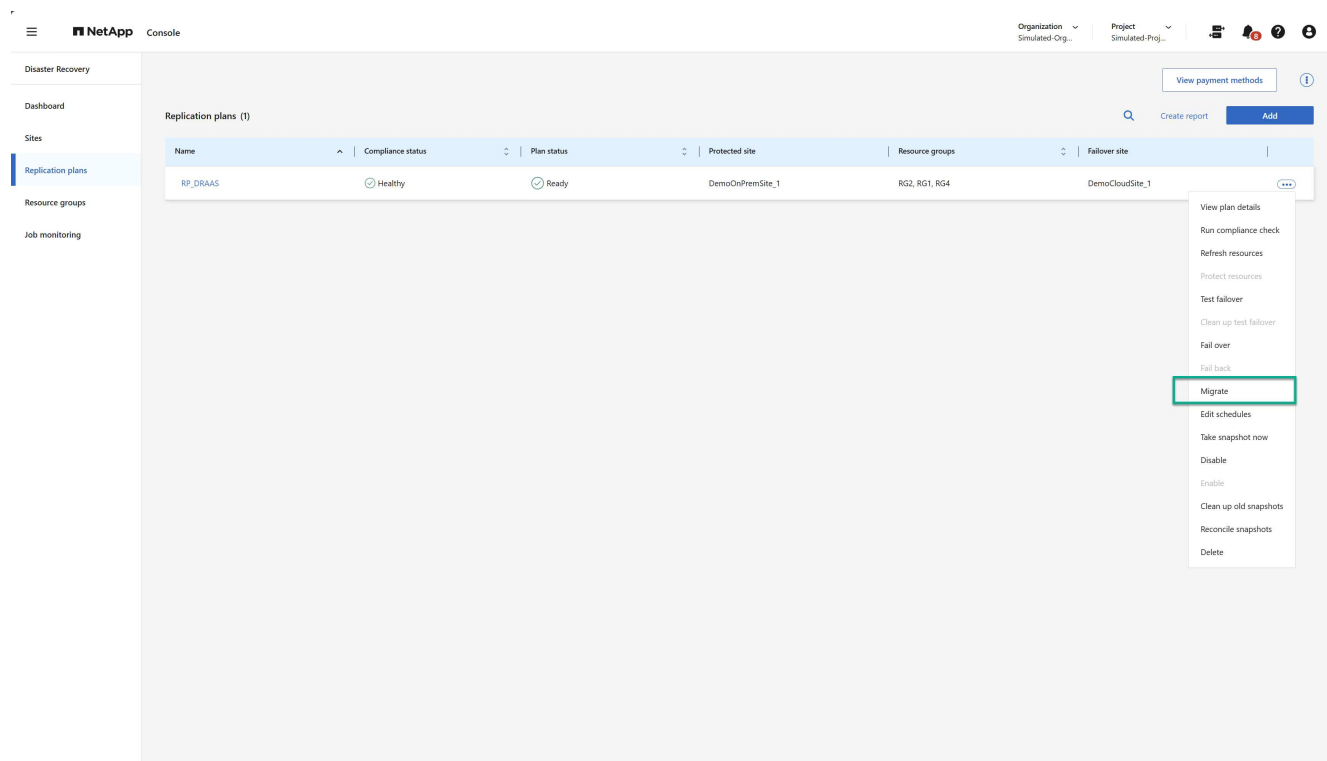
- vCenter の更新: vCenter クラスターに VM が追加、削除、または移動されるたびに、vCenter の更新を実行します。
- レプリケーション プランの更新: 同じソース vCenter クラスター内のデータストア間で VM が移動されるたびに、レプリケーション プランの更新を実行します。



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。

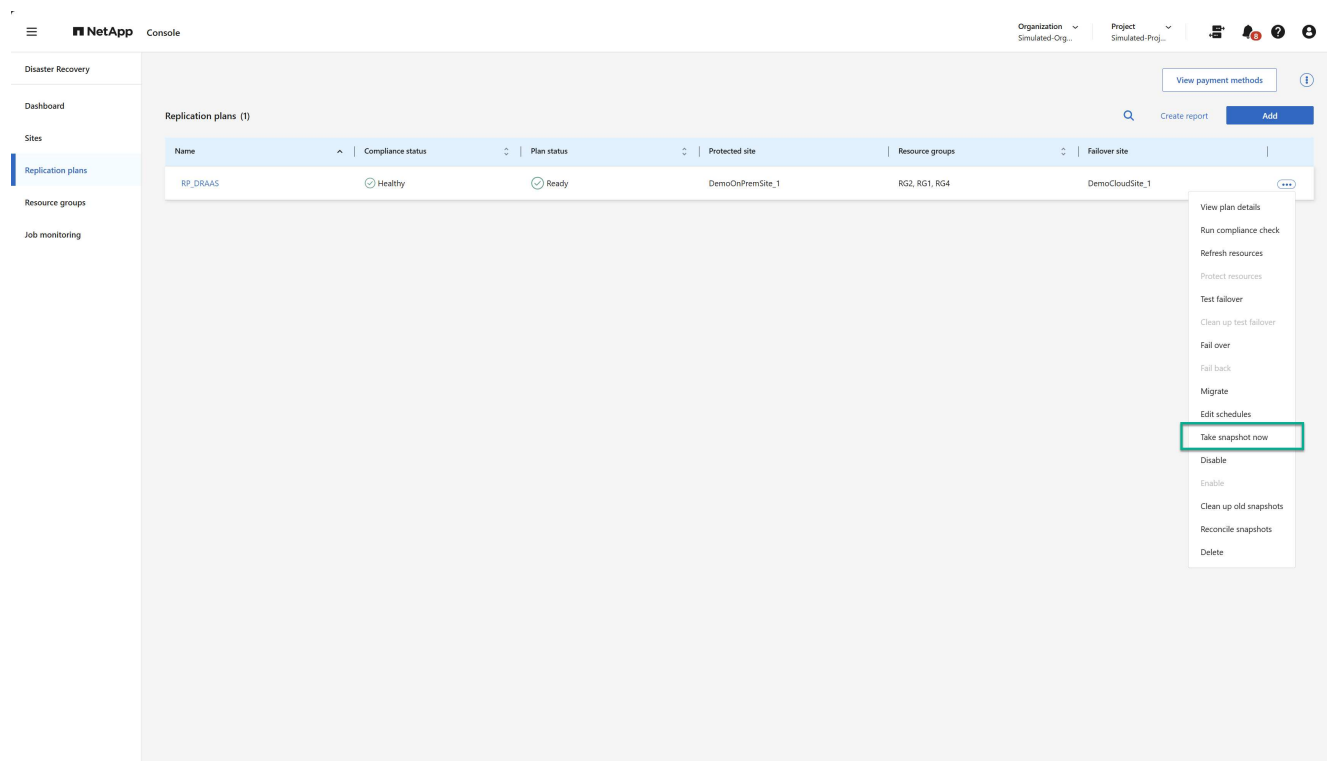


3. 移行ダイアログ ボックスに情報を入力します。

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。

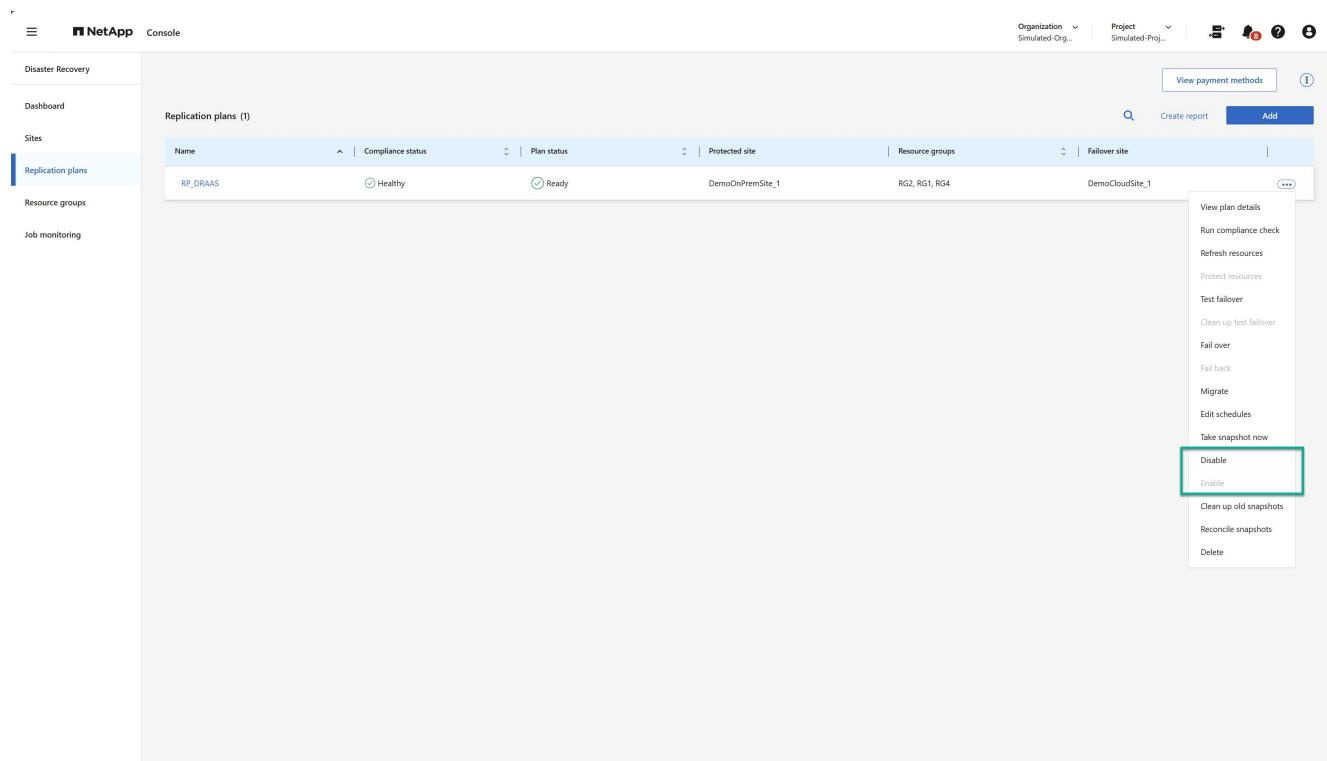


レプリケーションプランを無効または有効にする

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。

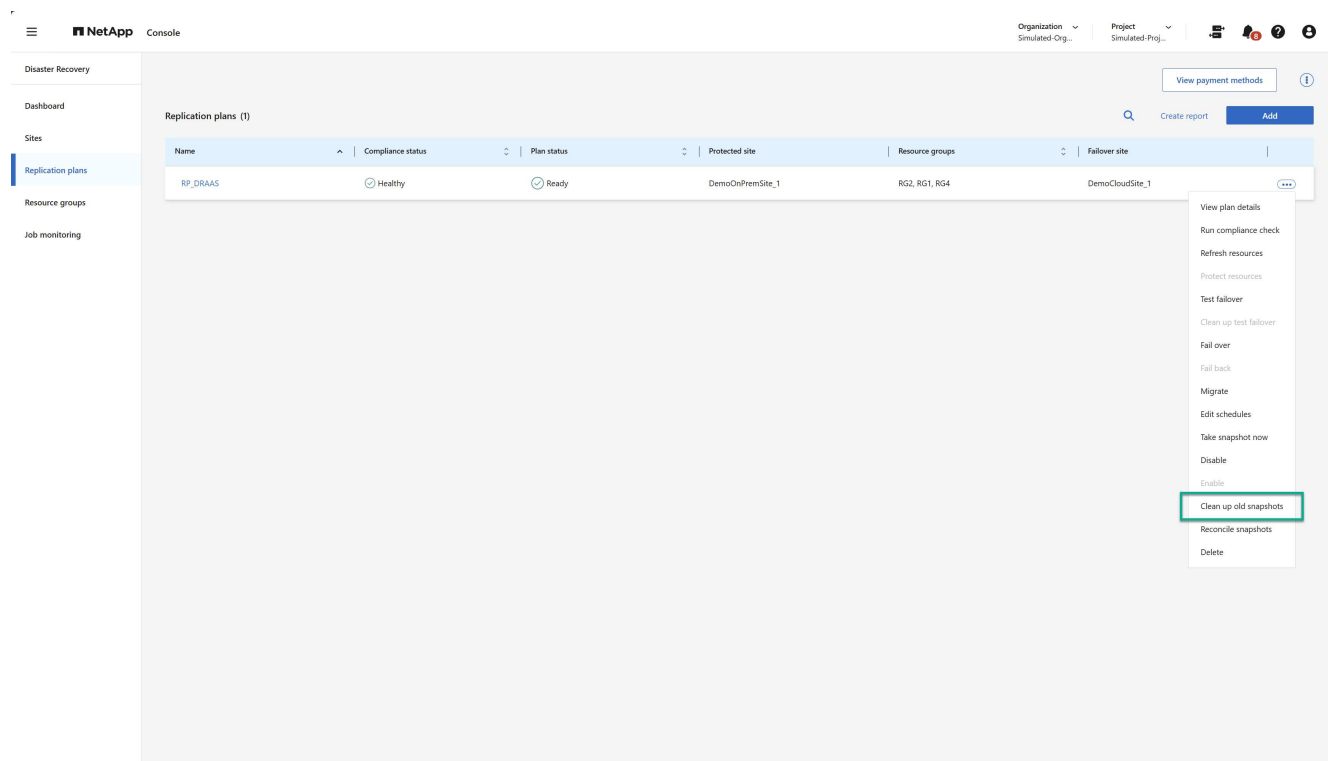
レプリケーション プランがアクティブな場合、[有効にする] コマンドはグレー表示されます。レプリケーション プランが無効になっている場合、[無効] コマンドはグレー表示されます。



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。

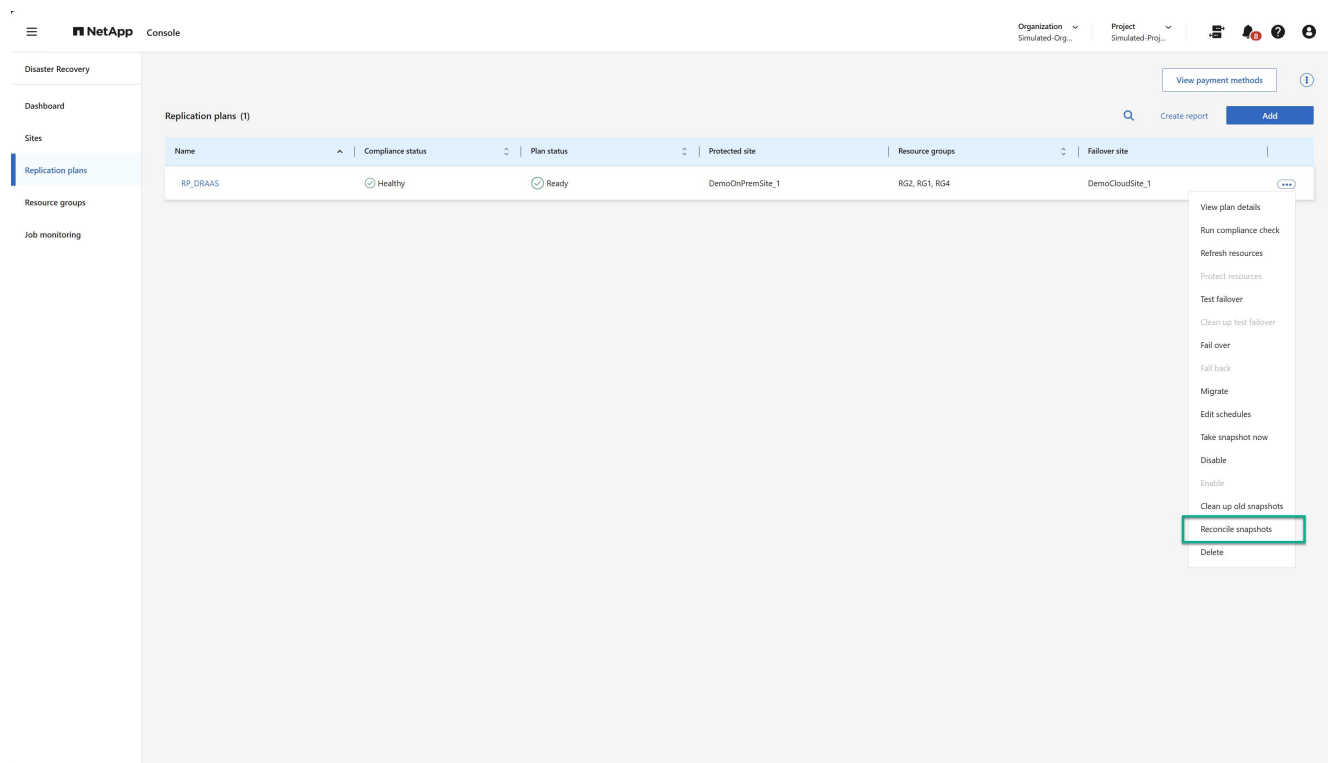
1. *アクション*オプションを選択します ●●●レプリケーション プランの横にあります。
2. これらの古いスナップショットを手動で削除するには、レプリケーション プランの [アクション] メニューから [古いスナップショットをクリーンアップ] を選択します。



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。

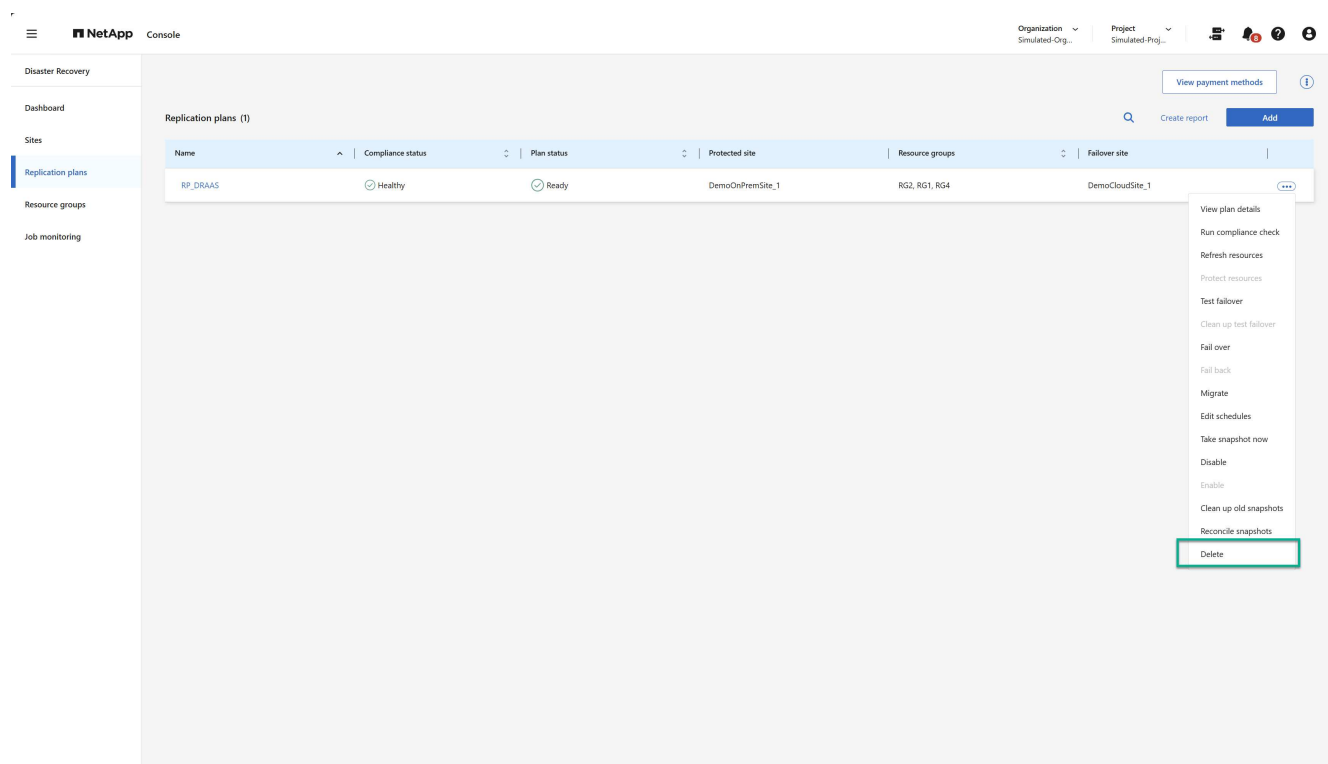
1. *アクション*オプションを選択します ●●●レプリケーション プランの横にあります。
2. 宛先クラスターに存在しないスナップショットをソース クラスターから削除するには、レプリケーションプランの [アクション] メニューから [スナップショットの調整] を選択します。



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。

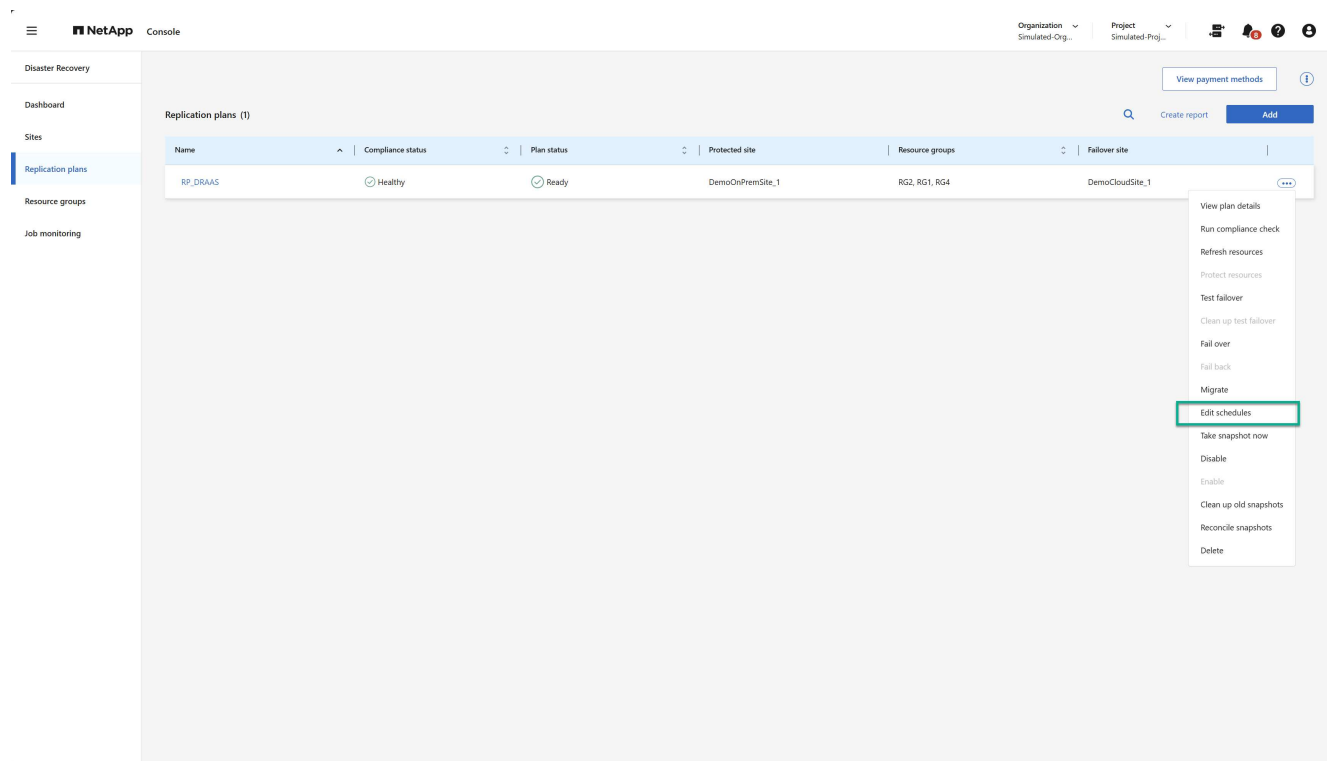
1. *アクション*オプションを選択します ●●●レプリケーション プランの横にあります。
2. レプリケーション プランを削除するには、レプリケーション プランのコンテキスト メニューから [削除] を選択します。



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。

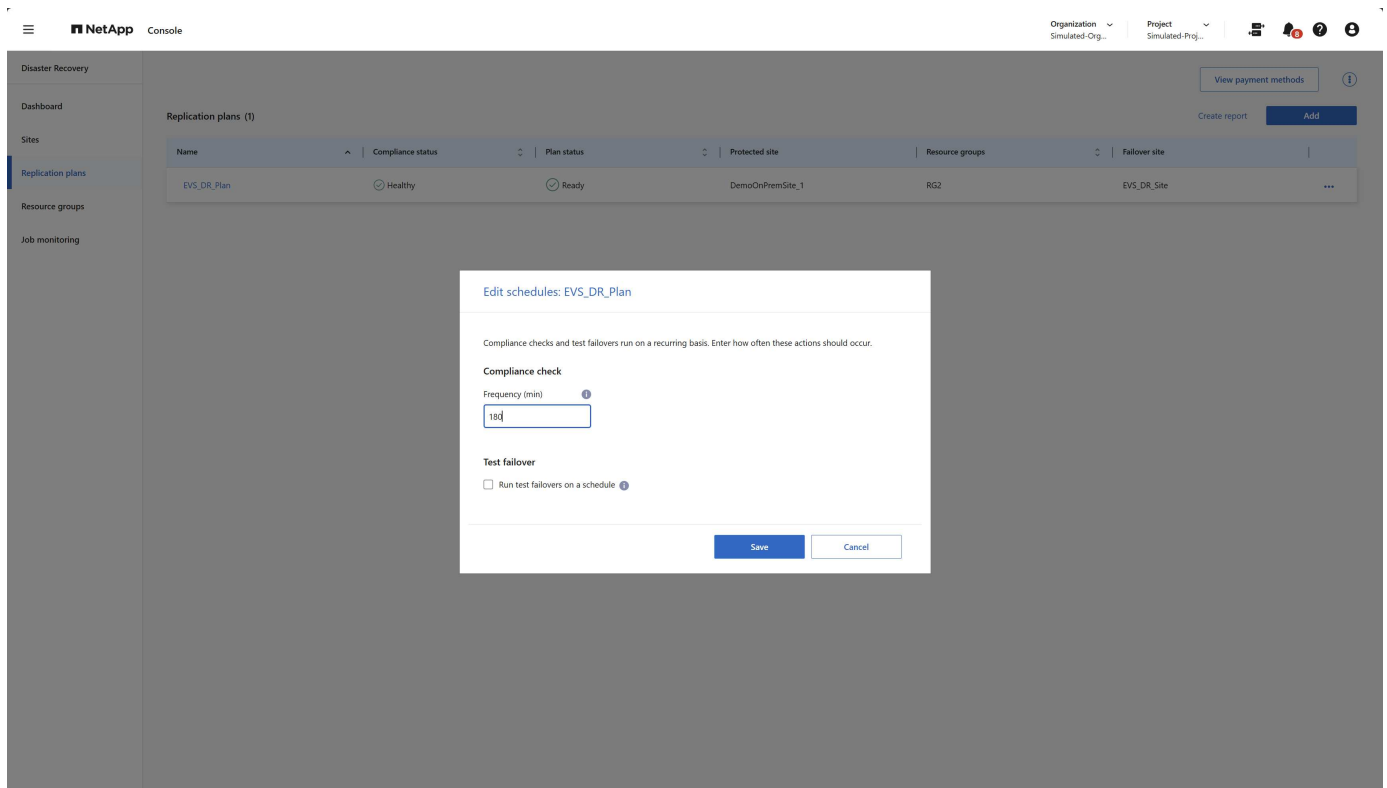
1. *アクション*オプションを選択します ●●●レプリケーション プランの横にあります。
2. これら 2 つの操作のいずれかのスケジュールを変更するには、レプリケーション プランの [スケジュールの編集] を選択します。



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-Orig...

Project
Simulated-Proj...

Disaster Recovery

Dashboard

Sites

Replication plans

Resource groups

Job monitoring

Replication plans (1)

Name	Compliance status
EVS_DR_Plan	Healthy

View payment methods

Create report

Add

Resource groups

Fallover site

62	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

4

5

Use on-demand snapshot for scheduled test failover

Repeat

Weekly

6

Day of the week

Saturday

7

Hour

01

Minute

00

AM/PM

AM

Start date

2025-09-23

8

9

Automatically cleanup

10

minutes after test failover

10

Save

Cancel

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用权を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用权については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、<http://www.netapp.com/TM>に記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。