



BlueXP DRaaSを使用した災害復旧

NetApp public and hybrid cloud solutions

NetApp
February 04, 2026

目次

BlueXP DRaaSを使用した災害復旧	1
概要	1
NFS データストア向けBlueXP DRaaS を使用した DR	1
開始	2
BlueXP disaster recovery構成	4
ソースサイトアレイと宛先サイトアレイ間のストレージレプリケーションの構成	5
VMware Disaster Recoveryの設定方法	6
BlueXP disaster recoveryは何を実現できるのでしょうか?	7
テストフェイルオーバー	15
クリーンアップフェイルオーバーテスト操作	17
計画的な移行とフェイルオーバー	18
フェイルバック	20
監視とダッシュボード	21
VMFS データストア向けBlueXP DRaaS を使用した DR	22
開始	23
BlueXP disaster recovery構成	25
ソースサイトと宛先サイト間のストレージレプリケーションの構成	27
VMware Disaster Recoveryの設定方法	27
BlueXP disaster recoveryは何を実現できるのでしょうか?	29
フェイルオーバーまたはテストフェイルオーバー操作中に何が起こりますか?	37

BlueXP DRaaSを使用した災害復旧

概要

災害復旧は、すべての VMware 管理者にとって最も重要な事項です。VMware は、サーバー全体を仮想マシンを構成する一連のファイルにカプセル化するため、管理者はクローン、スナップショット、レプリカなどのブロック ストレージ ベースの技術を利用してこれらの VM を保護します。ONTAP アレイには、ボリューム データ、および指定されたデータストア LUN 上に存在する仮想マシンをあるサイトから別のサイトに転送するための組み込みレプリケーション機能が備わっています。BlueXP DRaaS は vSphere と統合し、災害発生時にシームレスなフェイルオーバーとフェイルバックを実現するためにワークフロー全体を自動化します。ストレージ レプリケーションとインテリジェントな自動化を組み合わせることで、管理者は災害復旧計画を構成、自動化、テストだけでなく、災害発生時にそれらを簡単に実行できる手段も管理できるようになります。

VMware vSphere 環境での DR フェイルオーバーで最も時間のかかる部分は、DR サイトでの VM のインベントリ、登録、再構成、および電源投入に必要な手順の実行です。理想的なソリューションは、RPO (分単位で測定) と RTO (分から時間単位で測定) の両方が低いものです。DR ソリューションで見落とされがちな要素の 1 つは、DR ソリューションを定期的に効率的にテストする機能です。

DR ソリューションを設計するには、次の要素を考慮してください。

- 目標復旧時間 (RTO)。RTO とは、企業が災害からどれだけ早く回復できるか、より具体的には、ビジネス サービスを再び利用できるようにするために回復プロセスを実行するのにどれだけの時間がかかるかということです。
- 回復ポイント目標 (RPO)。RPO は、災害が発生した時間に対して、回復されたデータが利用可能になってからどのくらい経っているかを示します。
- スケーラビリティと適応性。この要素には、需要の増加に応じてストレージ リソースを段階的に拡張する機能が含まれます。

利用可能なソリューションに関する詳細な技術情報については、以下を参照してください。

- ["NFS データストア向けBlueXP DRaaS を使用した DR"](#)
- ["VMFS データストア向けBlueXP DRaaS を使用した DR"](#)

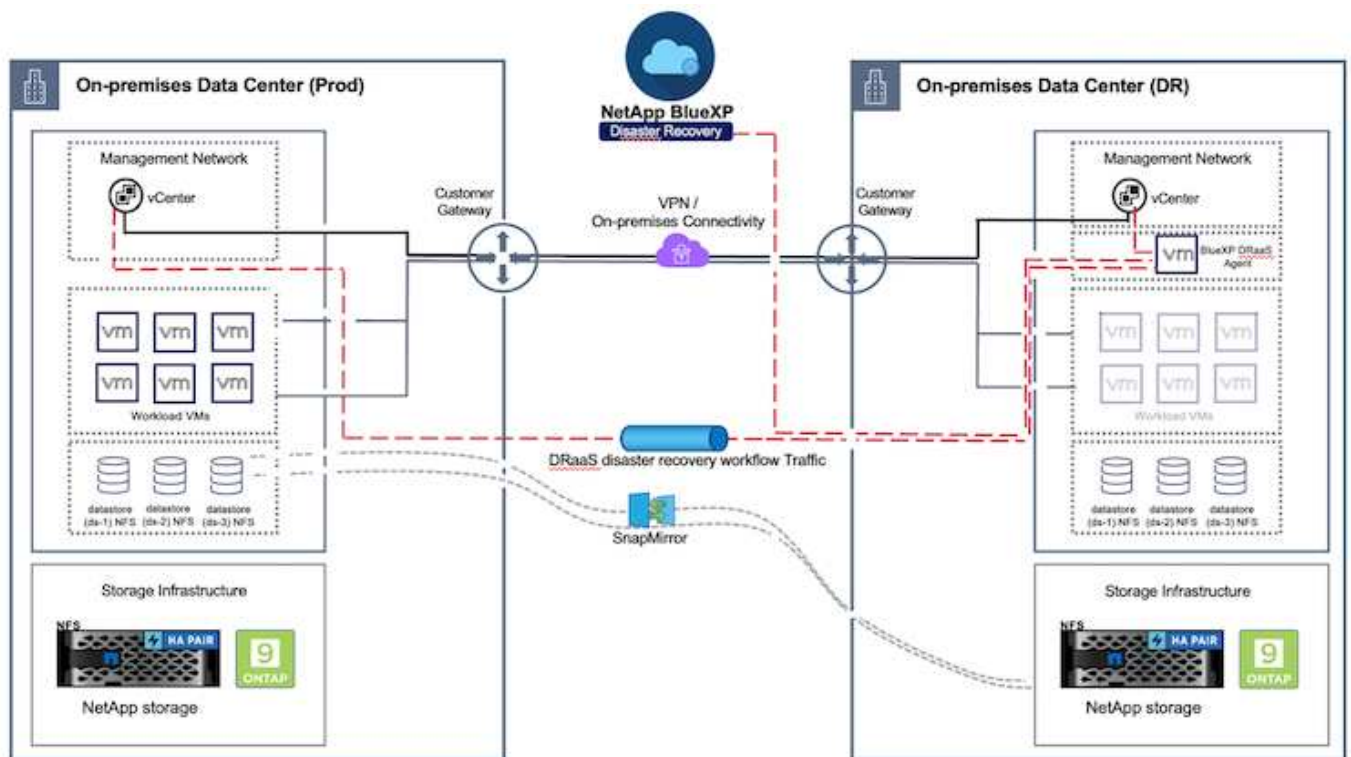
NFS データストア向けBlueXP DRaaS を使用した DR

運用サイトから災害復旧サイトへのブロックレベルのレプリケーションを通じて災害復旧を実装することは、サイトの停止やランサムウェア攻撃などのデータ破損イベントからワークロードを保護するための、回復力がありコスト効率に優れた方法です。NetApp SnapMirrorレプリケーションを使用すると、NFS データストアを備えたオンプレミスのONTAPシステムで実行されている VMware ワークロードを、VMware も導入されている指定されたリカバリ データセンターにある別のONTAPストレージ システムに複製できます。

このドキュメントのセクションでは、オンプレミスの VMware VM の災害復旧を別の指定サイトに設定するための BlueXP DRaaS の構成について説明します。このセットアップの一部として、BlueXP アカウント、BlueXP コネクタ、VMware vCenter から ONTAP ストレージへの通信を可能にするために必要な ONTAP アレイが BlueXP ワークスペース内に追加されます。さらに、このドキュメントでは、サイト間のレプリケーションを構成する方法と、リカバリ プランを設定およびテストする方法についても詳しく説明します。最後のセクションでは、サイト全体のフェールオーバーを実行する手順と、プライマリ サイトが回復されオンラインで購入されたときにフェールバックする方法について説明します。

NetApp BlueXP コンソールに統合された BlueXP disaster recovery サービスを利用することで、企業はオンプレミスの VMware vCenter と ONTAP ストレージを簡単に検出できます。組織は、リソース グループを作成し、災害復旧計画を作成し、それをリソース グループに関連付け、フェールオーバーとフェールバックをテストまたは実行できます。SnapMirror は、ストレージ レベルのブロック レプリケーションを提供して、2 つのサイトを増分変更で最新の状態に保ち、最大 5 分のリカバリ ポイント目標 (RPO) を実現します。さらに、本番環境に影響を与えたり、追加のストレージ コストが発生したりすることなく、災害復旧手順をシミュレートできます。

BlueXP disaster recovery は、ONTAP の FlexClone テクノロジーを活用して、ディザスタ リカバリ サイトで最後に複製されたスナップショットから NFS データストアのスペース効率の高いコピーを作成します。災害復旧テストを完了すると、実際の複製された本番リソースに影響を与えることなく、テスト環境を簡単に削除できます。実際のフェールオーバーが発生した場合、BlueXP disaster recovery サービスは、数回クリックするだけで、指定された災害復旧サイトで保護された仮想マシンを自動的に起動するために必要なすべての手順を調整します。このサービスは、必要に応じて、プライマリ サイトとの SnapMirror 関係を逆転させ、フェールバック操作のためにセカンダリ サイトからプライマリ サイトへの変更を複製します。これらすべての機能は、他のよく知られた代替手段に比べて、ほんのわずかなコストで提供されます。

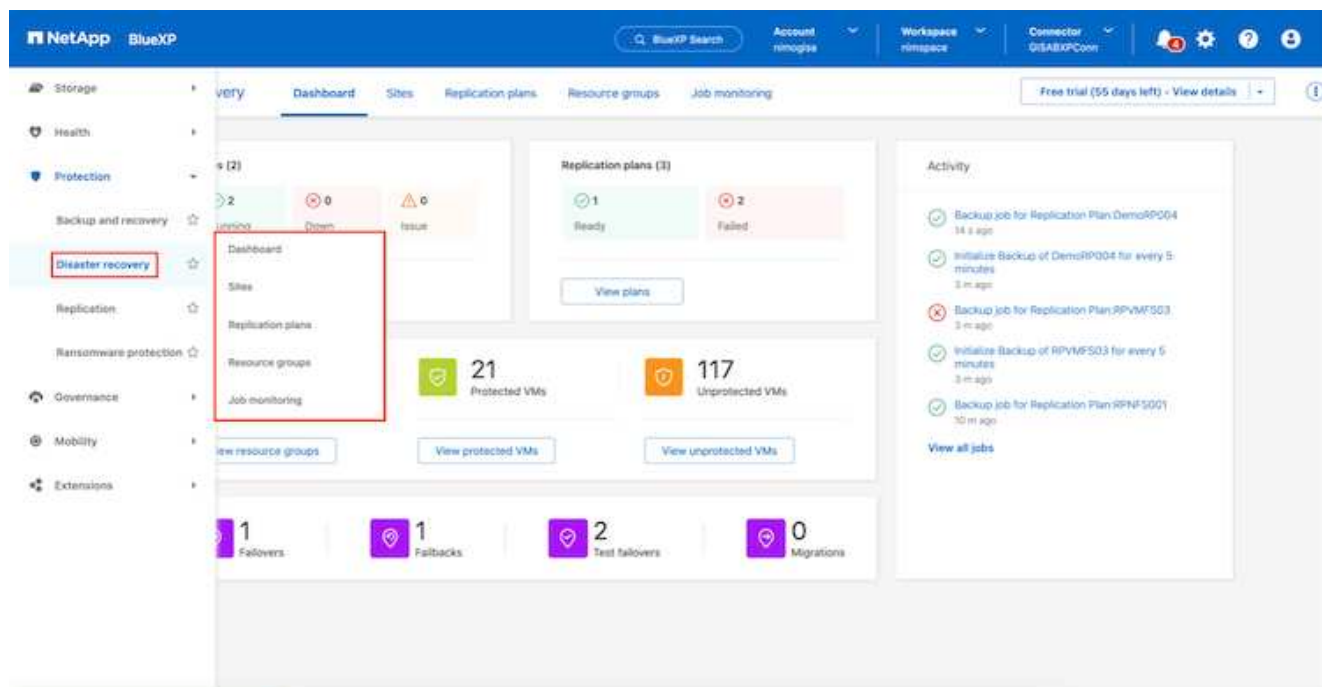


開始

BlueXP disaster recoveryを開始するには、BlueXP コンソールを使用してサービスにアクセスします。

1. BlueXPにログインします。

2. BlueXP 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. BlueXP disaster recoveryダッシュボードが表示されます。



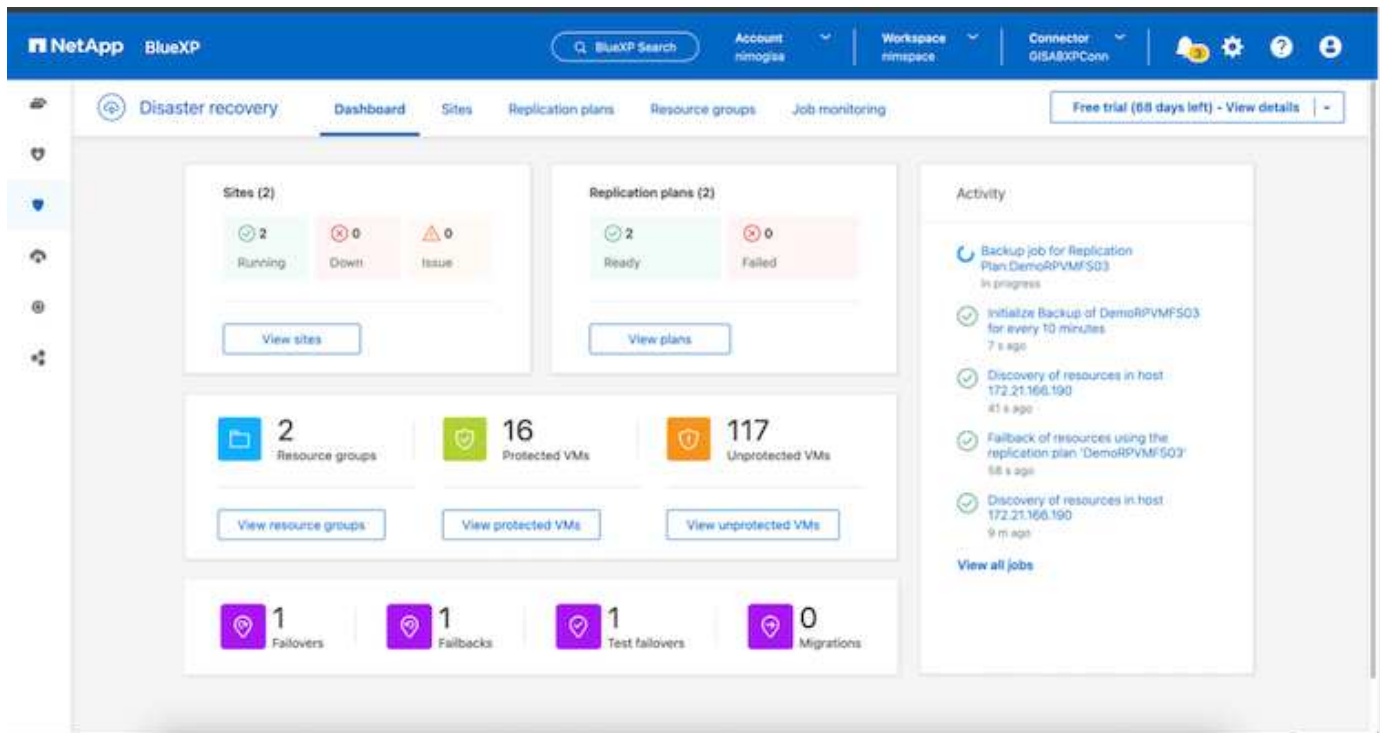
災害復旧計画を構成する前に、次の前提条件が満たされていることを確認してください。

- BlueXPコネクタはNetApp BlueXPに設定されます。
- BlueXPコネクタ インスタンスは、ソースおよびターゲットの vCenter およびストレージ システムに接続できます。
- ストレージ NFS データストアを提供するNetApp Data ONTAPクラスター。
- VMware 用の NFS データストアをホストするオンプレミスのNetAppストレージ システムがBlueXPに追加されました。
- DNS 名を使用する場合は、DNS 解決を実施する必要があります。それ以外の場合は、vCenter の IP アドレスを使用します。
- 指定された NFS ベースのデータストア ボリュームに対してSnapMirrorレプリケーションが構成されます。
- 環境にサポートされているバージョンの vCenter Server および ESXi サーバーがインストールされていることを確認します。

ソースサイトと宛先サイト間の接続が確立されたら、構成手順に進みます。これには数回のクリックと約 3 ～ 5 分かかります。



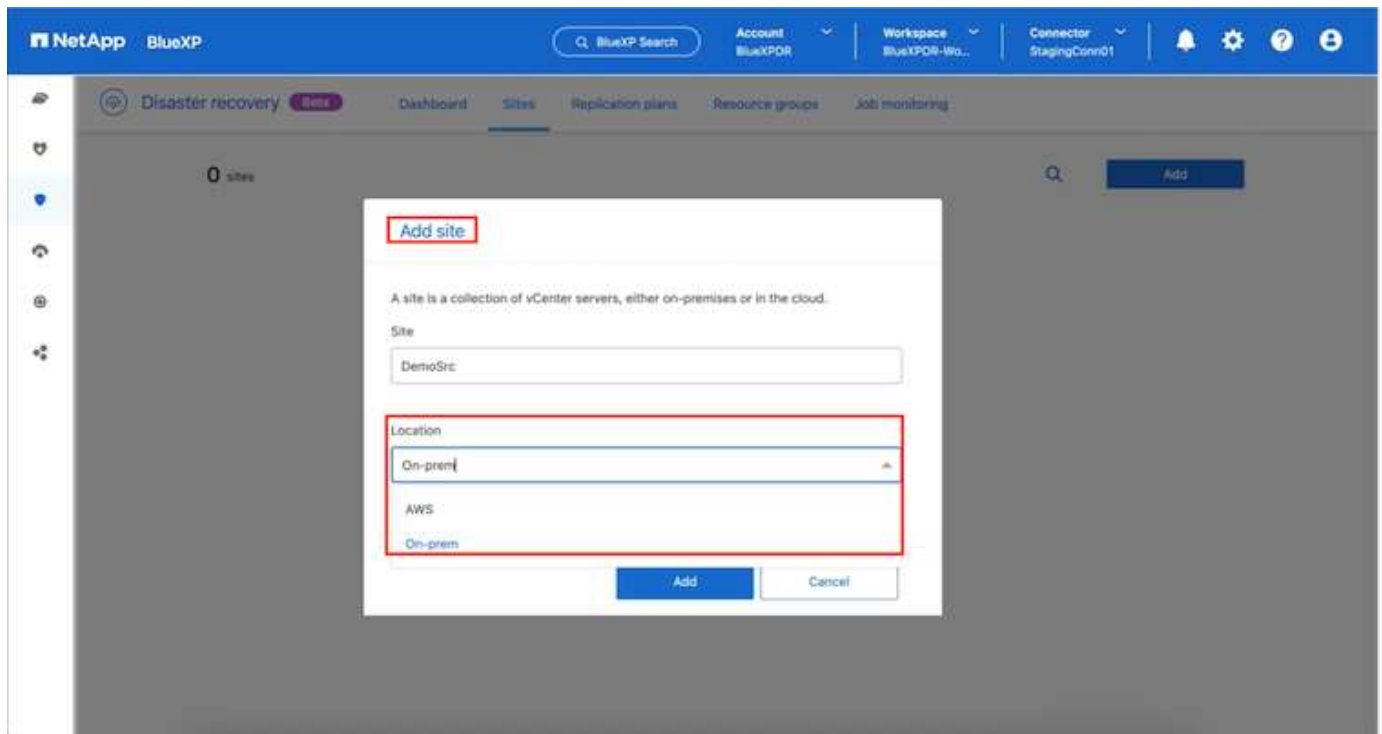
NetApp、BlueXPコネクタがネットワークを介してソース リソースおよび宛先リソースと通信できるように、宛先サイトまたは 3 番目のサイトにBlueXPコネクタを展開することを推奨しています。



BlueXP disaster recovery構成

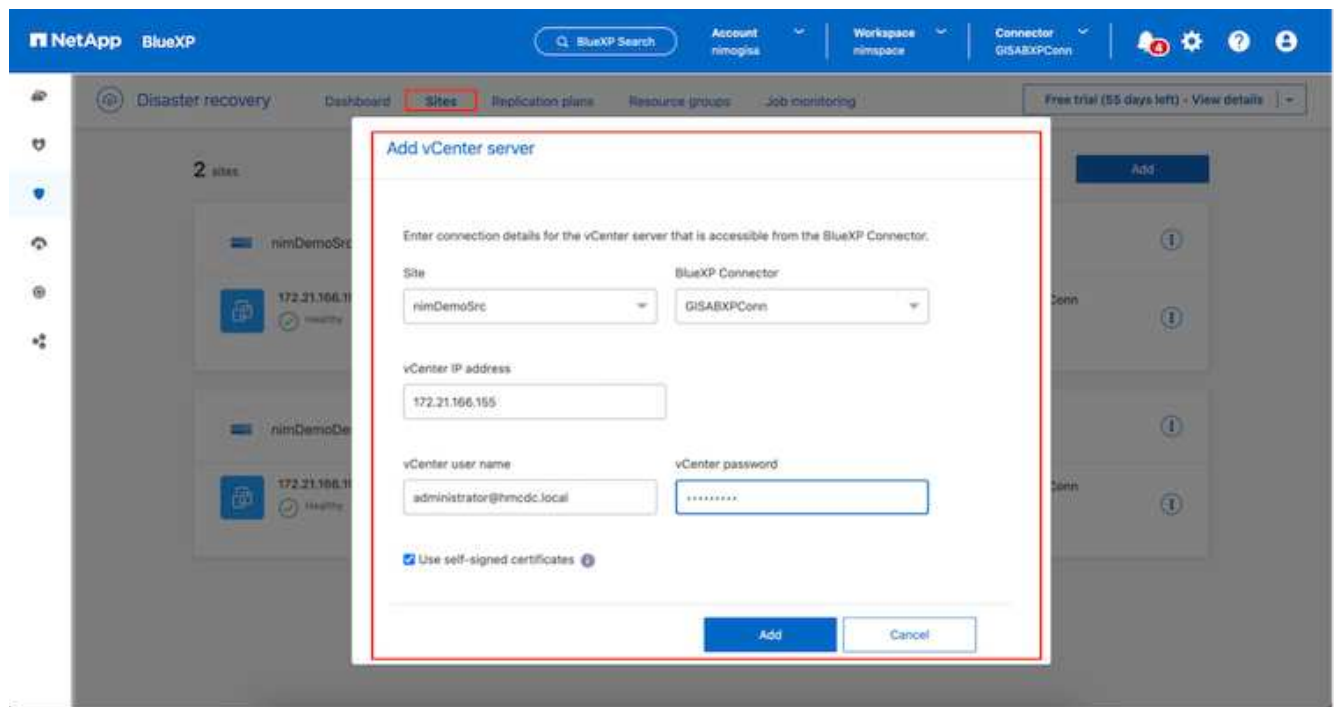
災害復旧の準備の最初のステップは、オンプレミスの vCenter とストレージ リソースを検出し、BlueXP disaster recoveryに追加することです。

BlueXPコンソールを開き、左側のナビゲーションから 保護 > 災害復旧 を選択します。vCenter サーバーの検出 を選択するか、トップメニューを使用して サイト > 追加 > vCenter の追加 を選択します。

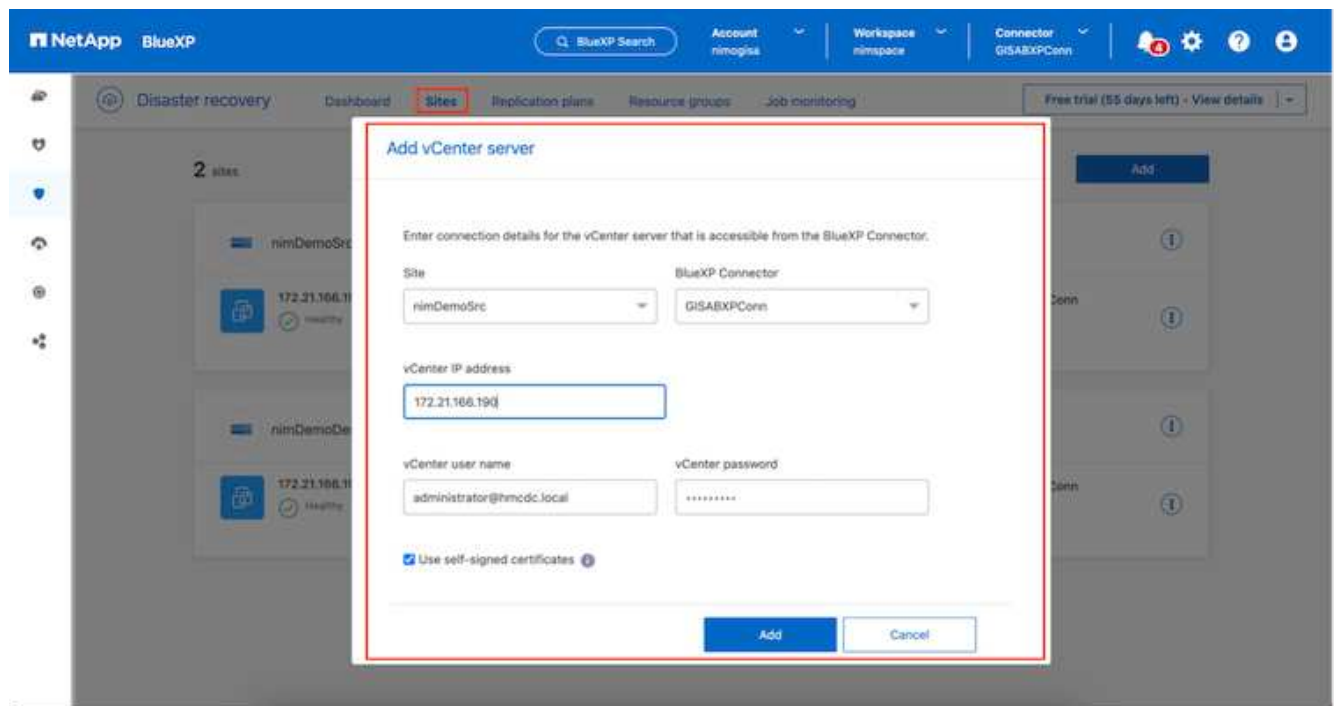


次のプラットフォームを追加します。

- ソース。オンプレミスの vCenter。



- 行き先。VMC SDDC vCenter。



vCenter が追加されると、自動検出がトリガーされます。

ソースサイトアレイと宛先サイトアレイ間のストレージレプリケーションの構成

SnapMirror は、NetApp環境でのデータ複製を提供します。NetApp Snapshot テクノロジーに基づいて構築されたSnapMirrorレプリケーションは、前回の更新以降に変更または追加されたブロックのみを複製するた

め、非常に効率的です。 SnapMirror は、 NetApp OnCommand System Manager または ONTAP CLI を使用して簡単に設定できます。 BlueXP DRaaS は、クラスターと SVM ピアリングが事前に構成されている場合、 SnapMirror 関係も作成します。

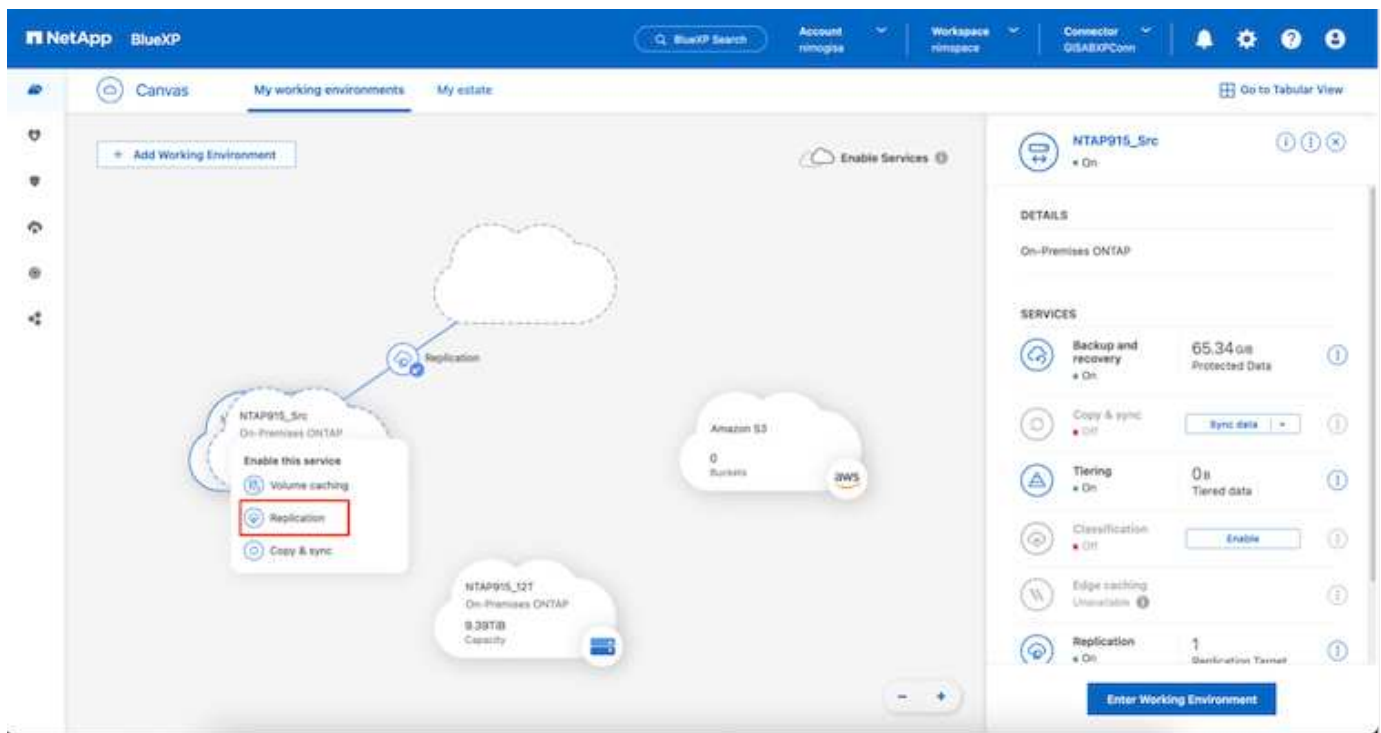
プライマリ ストレージが完全に失われていない場合、 SnapMirror はプライマリ サイトと DR サイトを再同期する効率的な手段を提供します。 SnapMirror は2 つのサイトを再同期し、 SnapMirror 関係を単純に反転するだけで、変更されたデータまたは新しいデータのみを DR サイトからプライマリ サイトに転送できます。つまり、 BlueXP DRaaS のレプリケーション プランは、フェイルオーバー後にボリューム全体を再コピーすることなく、どちらの方向にも再同期できます。関係が逆方向に再同期される場合、スナップショット コピーの最後の正常な同期以降に書き込まれた新しいデータのみが宛先に送り返されます。



CLI または System Manager を介してボリュームに SnapMirror 関係がすでに構成されている場合、 BlueXP DRaaS はその関係を取得し、残りのワークフロー操作を続行します。

VMware Disaster Recovery の設定方法

SnapMirror レプリケーションを作成するプロセスは、どのアプリケーションでも同じです。このプロセスは手動でも自動でも実行できます。最も簡単な方法は、 BlueXP を利用して、環境内のソース ONTAP システムを宛先にドラッグ アンド ドロップするだけで SnapMirror レプリケーションを構成し、残りのプロセスをガイドするウィザードを起動することです。



BlueXP DRaaS では、次の 2 つの条件が満たされている場合、同じことを自動化することもできます。

- ソース クラスターと宛先クラスターにはピア関係があります。
- ソース SVM と宛先 SVM にはピア関係があります。



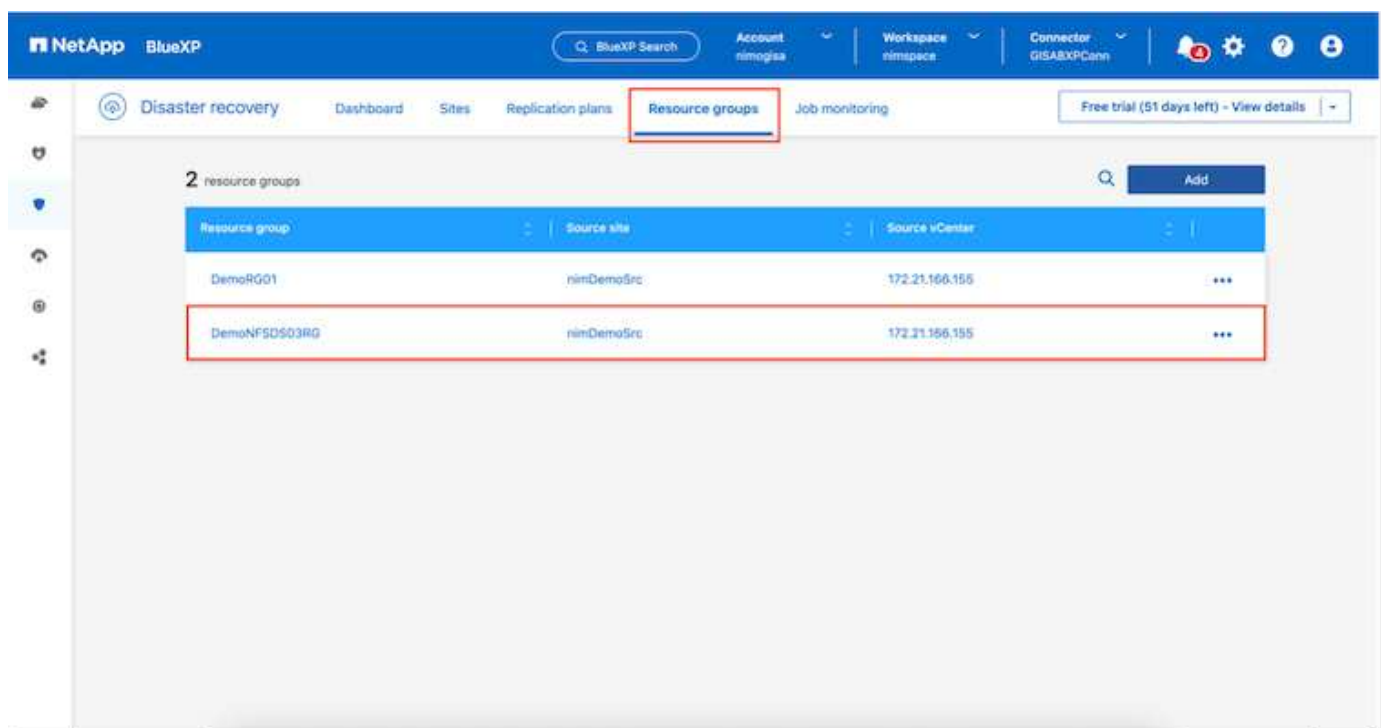
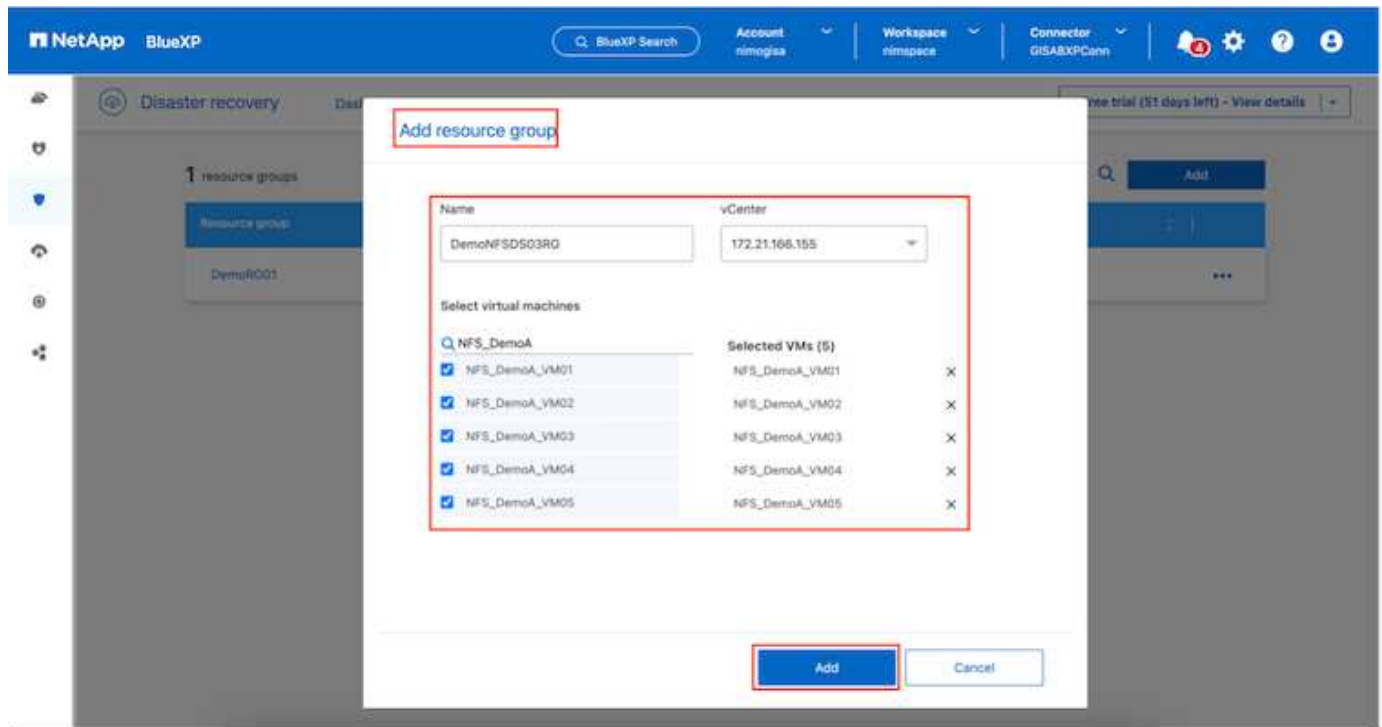
CLI 経由でボリュームにSnapMirror関係がすでに設定されている場合、BlueXP DRaaS はその関係を取得し、残りのワークフロー操作を続行します。

BlueXP disaster recoveryは何を実現できるのでしょうか？

ソース サイトと宛先サイトが追加されると、BlueXP disaster recoveryは自動的に詳細な検出を実行し、VM と関連メタデータを表示します。BlueXP disaster recoveryでは、VM で使用されるネットワークとポート グループも自動的に検出し、それらを入力します。

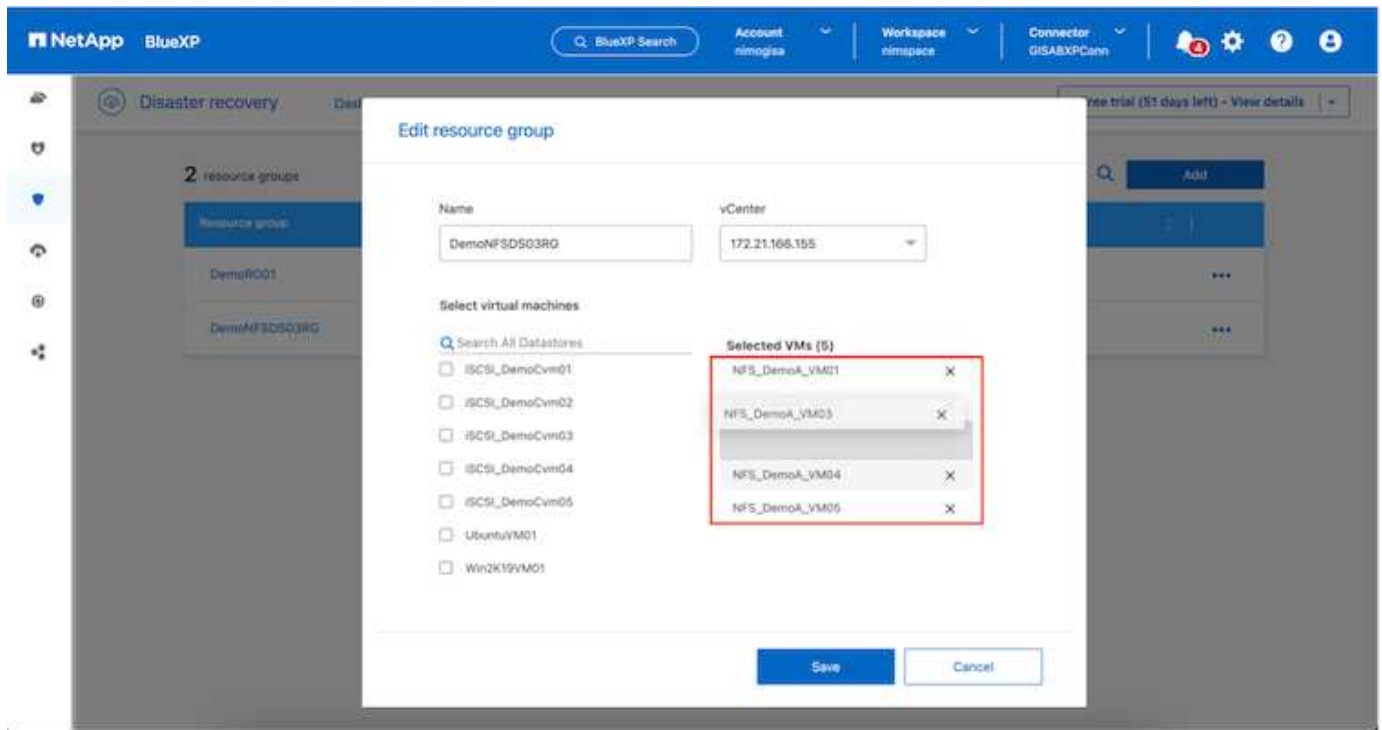
Site	IP	Health	VMs	Datastores	Resource group	Connector
nimDemoSrc	172.21.166.155	Healthy	72	13	1	GISABXPCnn
nimDemoDest	172.21.166.190	Healthy	61	3	0	GISABXPCnn

サイトを追加した後、VM をリソース グループにグループ化できます。BlueXP disaster recoveryリソースグループを使用すると、依存する VM のセットを、復旧時に実行できるブート順序とブート遅延を含む論理グループにグループ化できます。リソース グループの作成を開始するには、[リソース グループ] に移動し、[新しいリソース グループの作成] をクリックします。

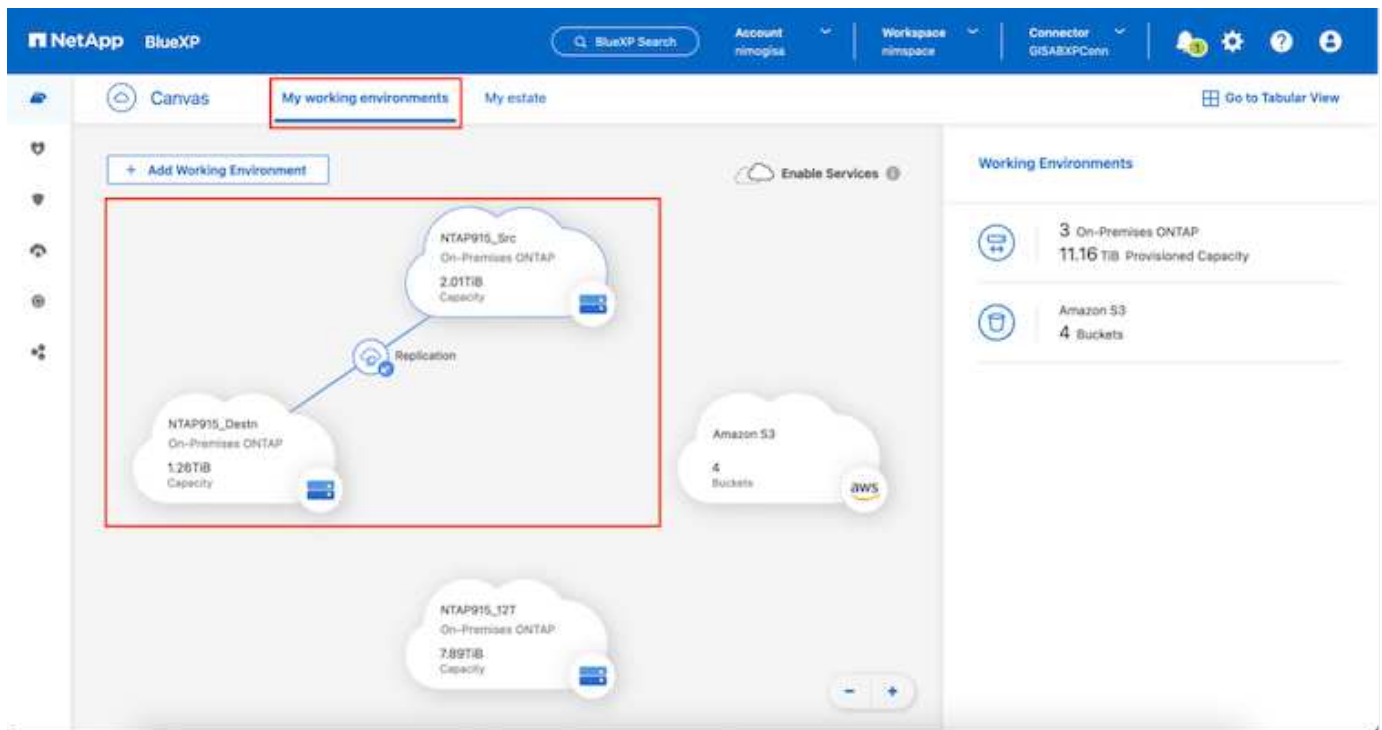


レプリケーション プランの作成時にリソース グループを作成することもできます。

VM のブート順序は、リソース グループの作成中に、簡単なドラッグ アンド ドロップ メカニズムを使用して定義または変更できます。



リソースグループを作成したら、次のステップは、災害発生時に仮想マシンとアプリケーションを復旧するための実行ブループリントまたは計画を作成することです。前提条件で述べたように、SnapMirrorレプリケーションは事前に構成することも、レプリケーションプランの作成時に指定されたRPOと保持数を使用してDRaaSで構成することもできます。



Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Replication
	NTAP915_Src	NTAP915_Destn				2023 Sep
✓	Demo_TPS_DS01 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Destn	13 seconds	idle	snapirored	Aug 5, 2024, 6:15 386.63 MiB
✓	Src_250_Vol01 NTAP915_Src	Src_250_Vol01_Copy NTAP915_Destn	4 seconds	idle	snapirored	Aug 16, 2024, 12:11 79.23 MiB
✓	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_CP NTAP915_Destn	12 seconds	idle	snapirored	Aug 16, 2024, 12:11 24.64 MiB
✓	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_CP NTAP915_Destn	3 seconds	idle	snapirored	Aug 16, 2024, 12:11 47.38 MiB
✓	Src_JSCSI_DS04 NTAP915_Src	Src_JSCSI_DS04_copy NTAP915_Destn	4 seconds	idle	snapirored	Aug 16, 2024, 12:11 108.87 MiB
✓	nimpra NTAP915_Src	nimpra_dest NTAP915_Destn	2 seconds	idle	snapirored	Aug 16, 2024, 12:11 3.48 KiB

ドロップダウンからソースと宛先の vCenter プラットフォームを選択してレプリケーション プランを構成し、プランに含めるリソース グループ、アプリケーションの復元方法と電源オン方法のグループ化、およびクラスタとネットワークのマッピングを選択します。リカバリ プランを定義するには、[レプリケーション プラン] タブに移動し、[プランの追加] をクリックします。

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

Replication plan name: DemoNFSDS03RP

Select a source vCenter where your data exists, to replicate to the selected target vCenter.

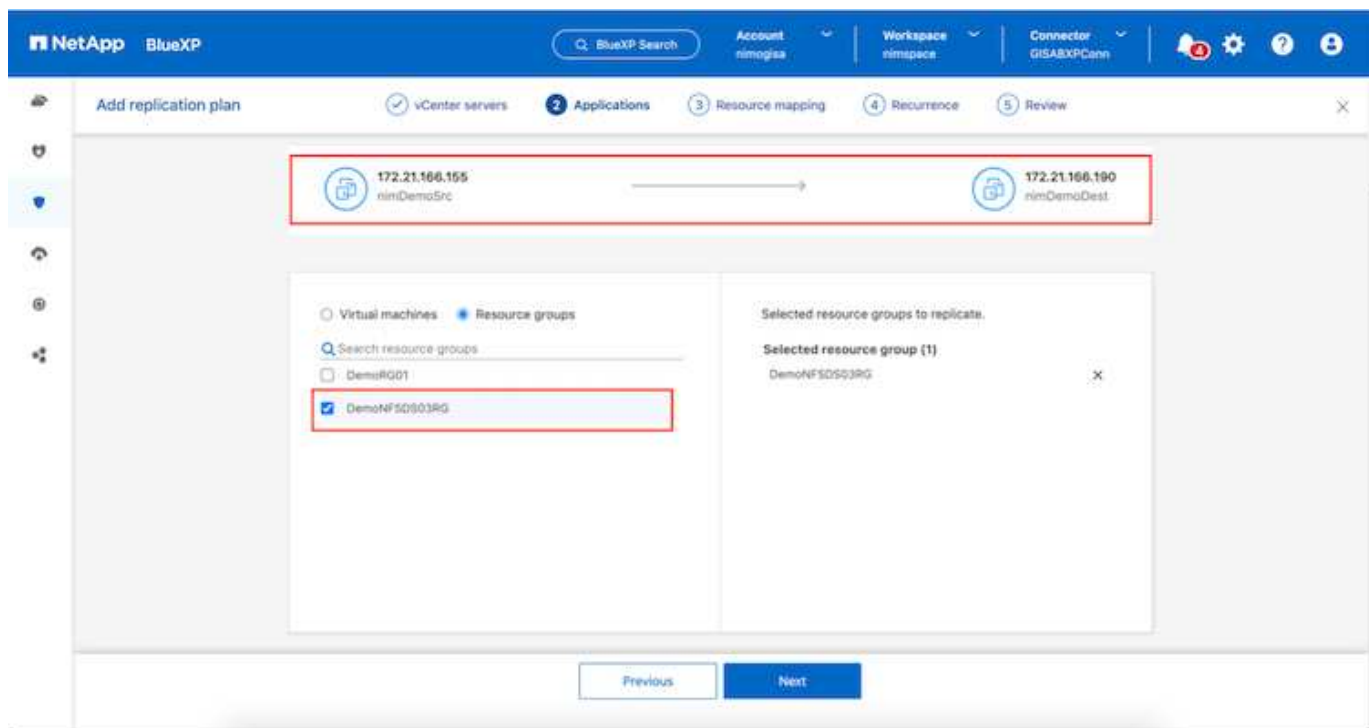
Source vCenter: 172.21.166.155

Target vCenter: 172.21.166.190

Buttons: Cancel, Next

次のステップは、既存のリソース グループを選択することです。リソース グループが作成されていない場合、ウィザードは、回復目標に基づいて必要な仮想マシンをグループ化します (基本的には機能リソース グループを作成します)。これは、アプリケーション仮想マシンを復元する操作シーケンスを定義するのに役立

ちます。

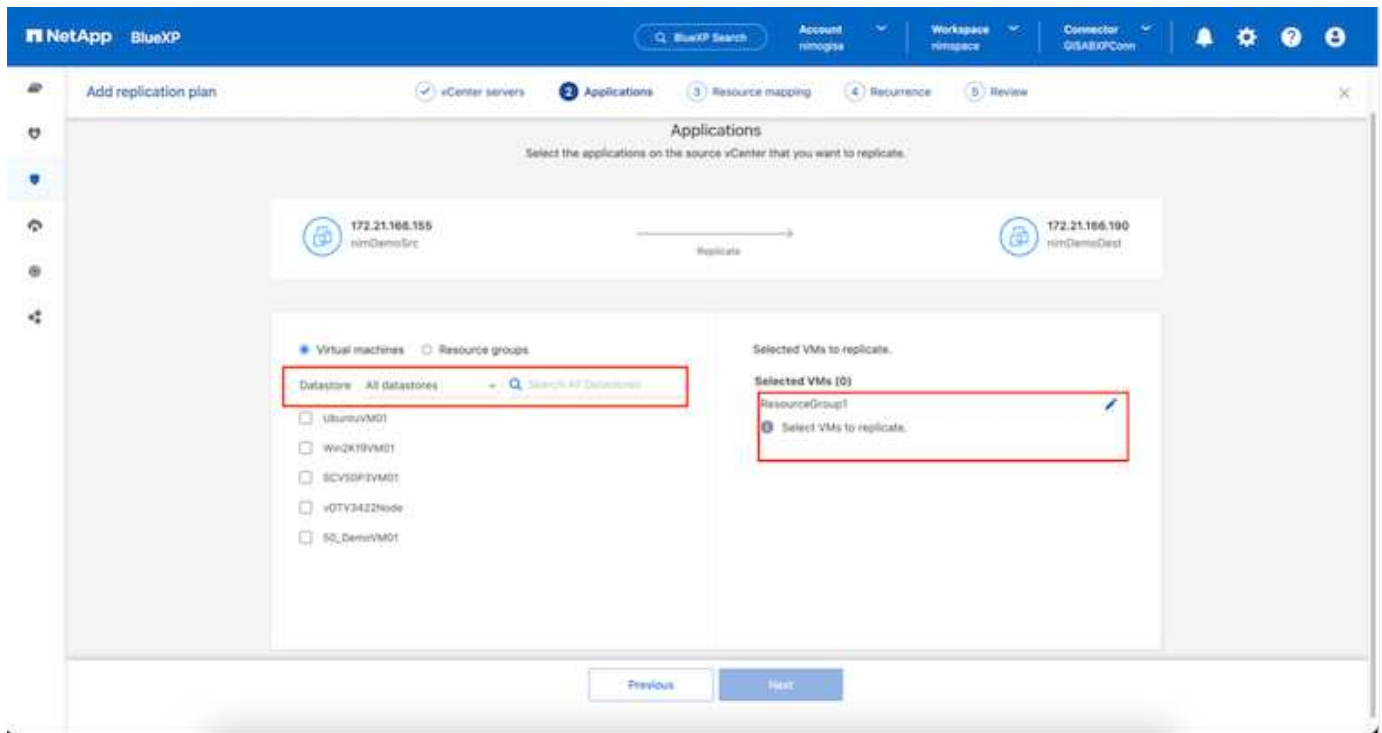


リソースグループでは、ドラッグアンドドロップ機能を使用してブート順序を設定できます。これを使用すると、リカバリプロセス中に VM の電源がオンになる順序を簡単に変更できます。

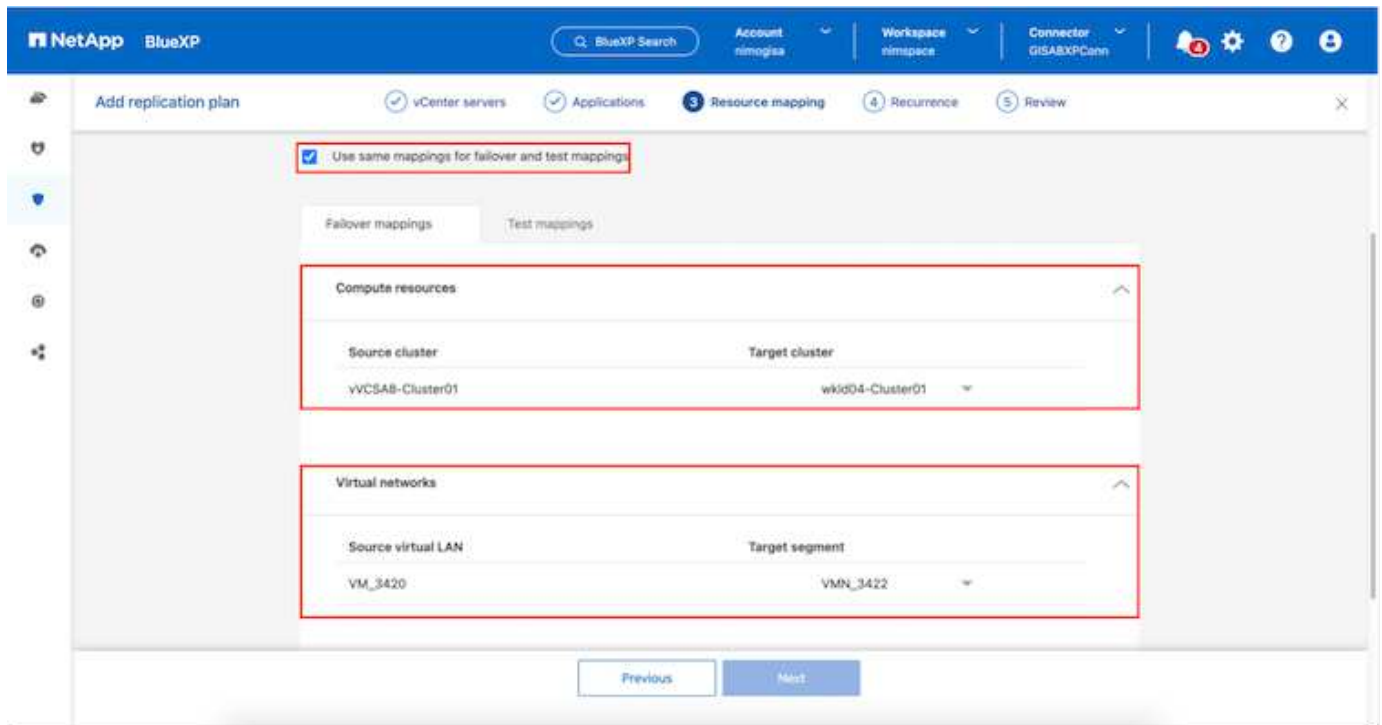


リソースグループ内の各仮想マシンは、順序に基づいて順番に起動されます。2つのリソースグループが並行して開始されます。

以下のスクリーンショットは、リソースグループが事前に作成されていない場合に、組織の要件に基づいて仮想マシンまたは特定のデータストアをフィルターするオプションを示しています。



リソース グループを選択したら、フェールオーバー マッピングを作成します。このステップでは、ソース環境のリソースを宛先にマップする方法を指定します。これには、コンピューティング リソース、仮想ネットワークが含まれます。IP カスタマイズ、事前スクリプトと事後スクリプト、ブート遅延、アプリケーションの一貫性など。詳細については、"[レプリケーションプランを作成する](#)"。



デフォルトでは、テスト操作とフェイルオーバー操作の両方に同じマッピング パラメータが使用されます。テスト環境に異なるマッピングを設定するには、以下に示すようにチェックボックスをオフにした後、テスト マッピング オプションを選択します。

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPCann

Add replication plan vCenter servers Applications **3 Resource mapping** 4 Recurrence 5 Review

Virtual machines

IP address type: Static Target IP: Same as source

☐ Use the same credentials for Same as source

☐ Use the same script for all VMs Different from source

Source VM	CPU	RAM	Boot delay (mins between 0 and 10)	Create application consistent replicas
DemoNFS03R0				
NFS_DemoA_VM01	2	4 GB	0	<input type="checkbox"/>
NFS_DemoA_VM02	2	4 GB	0	<input type="checkbox"/>

Previous Next

リソース マッピングが完了したら、[次へ] をクリックします。

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPCann

Add replication plan vCenter servers Applications **3 Resource mapping** 4 Recurrence 5 Review

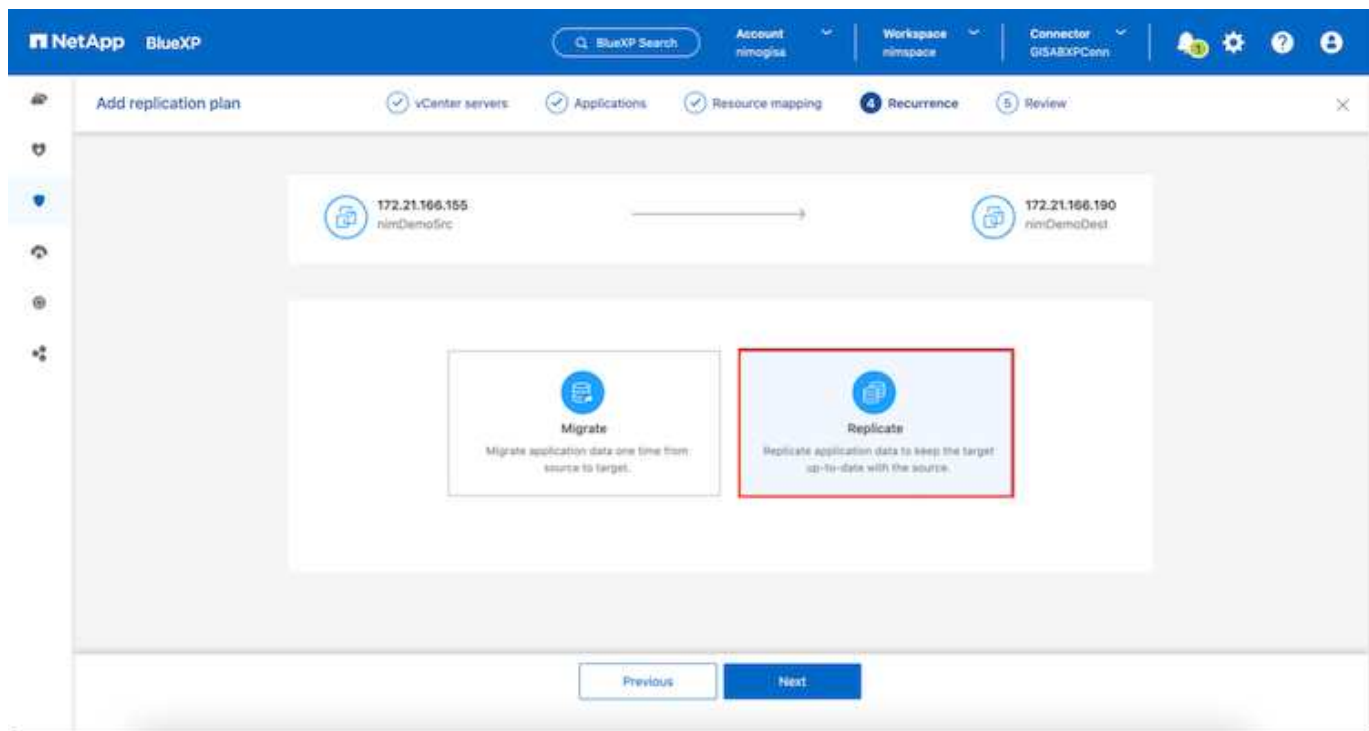
172.21.166.165 nimDemoSrc → 172.21.166.190 nimDemoDest

☒ Use same mappings for failover and test mappings

Fallover mappings	Test mappings
Compute resources	Mapped
Virtual networks	Mapped
Virtual machines	Mapped

Previous Next

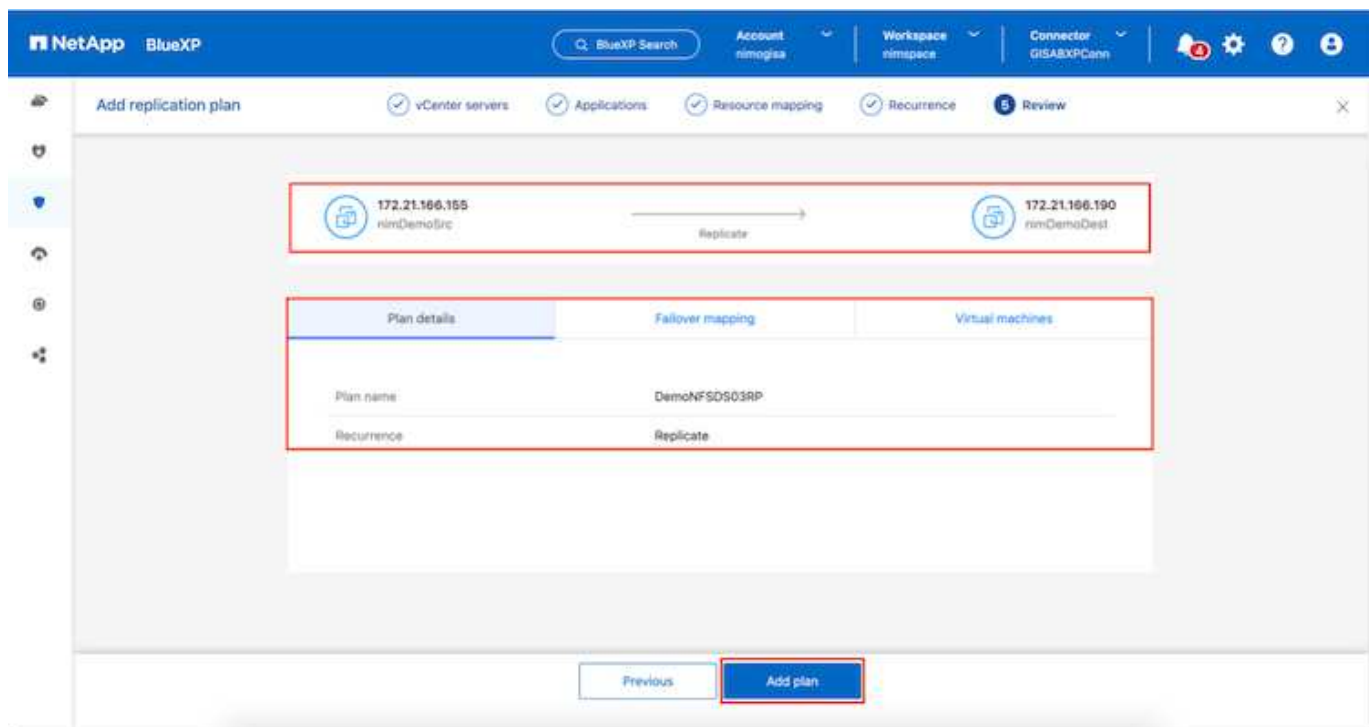
繰り返しタイプを選択します。簡単に言えば、「移行」（フェイルオーバーを使用した 1 回限りの移行）または定期的な連続レプリケーション オプションを選択します。このチュートリアルでは、「複製」オプションが選択されています。

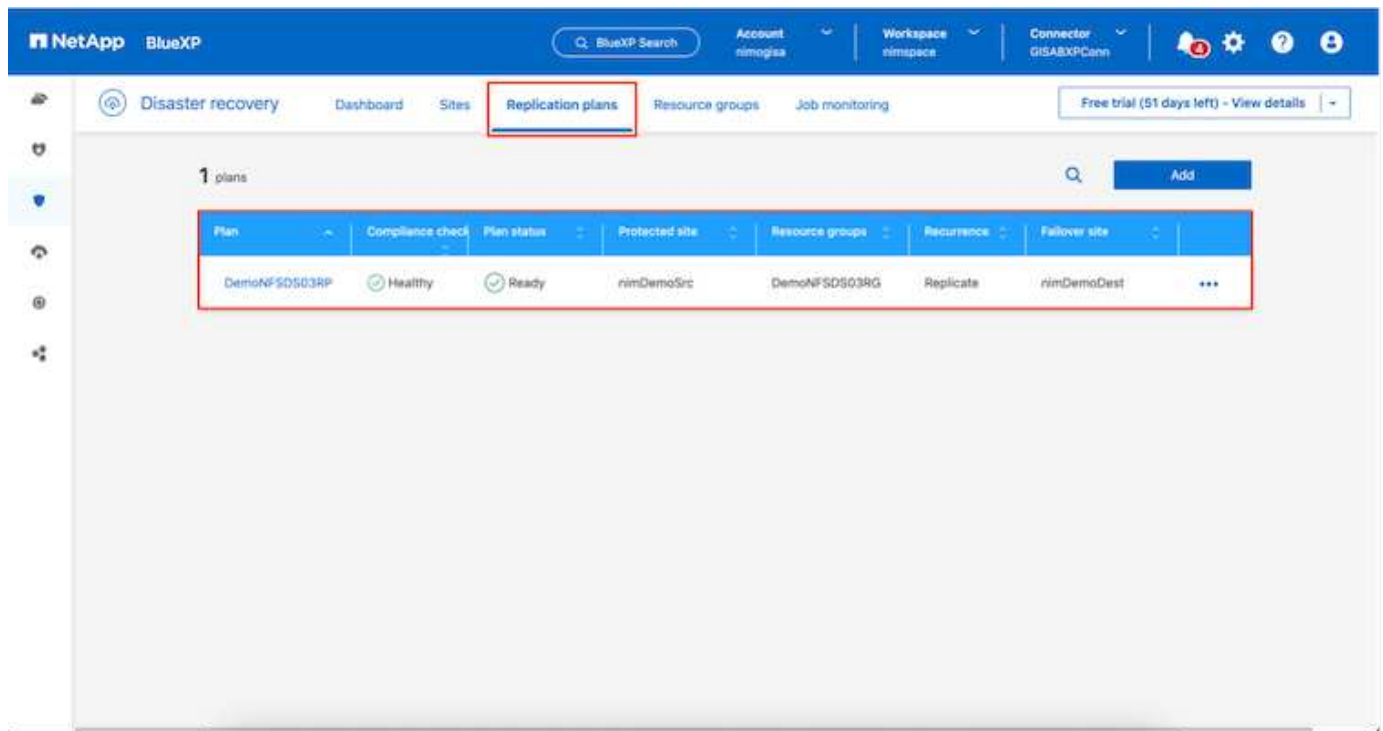


完了したら、作成されたマッピングを確認し、「プランの追加」をクリックします。



異なるボリュームおよび SVM からの VM をレプリケーション プランに含めることができます。VM の配置 (同じボリューム上、同じ SVM 内の別のボリューム上、異なる SVM 上の別のボリューム上など) に応じて、BlueXP disaster recoveryでは整合性グループ スナップショットが作成されます。



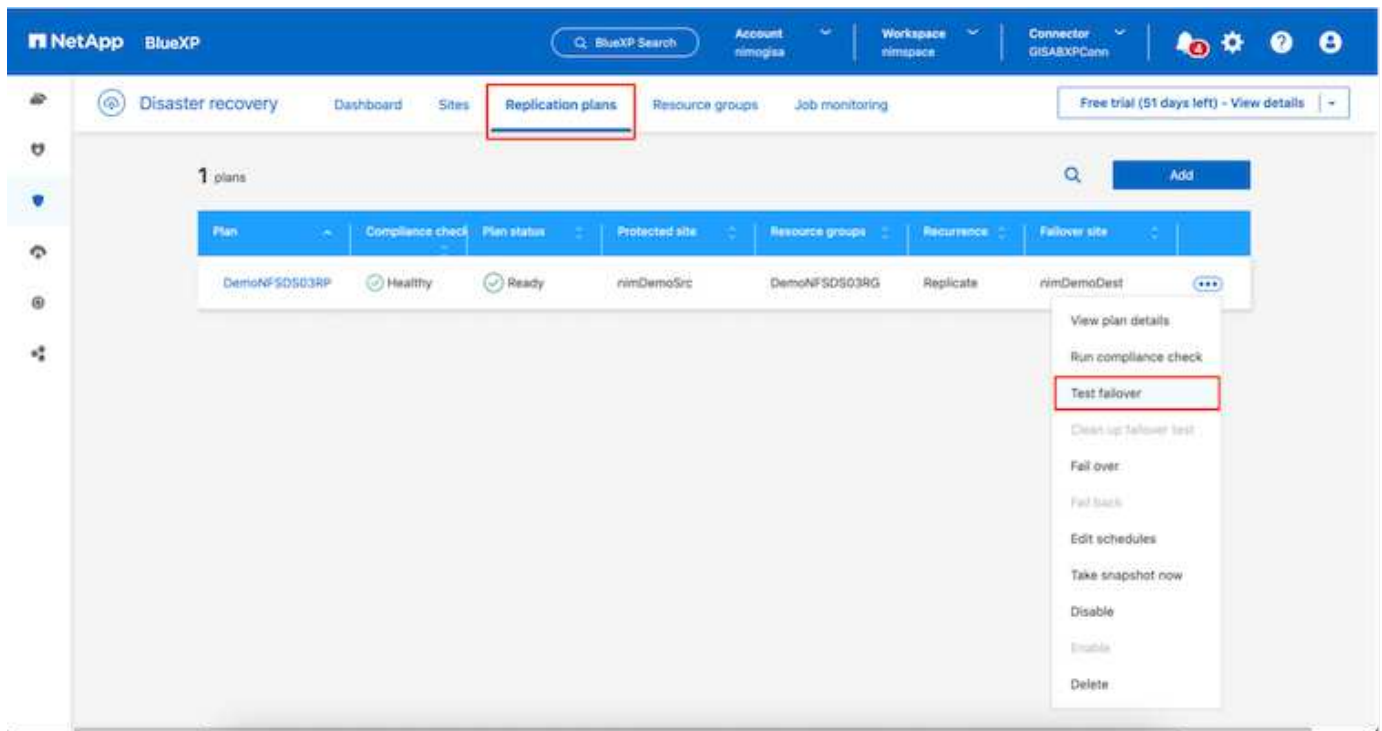


BlueXP DRaaS は次のワークフローで構成されています。

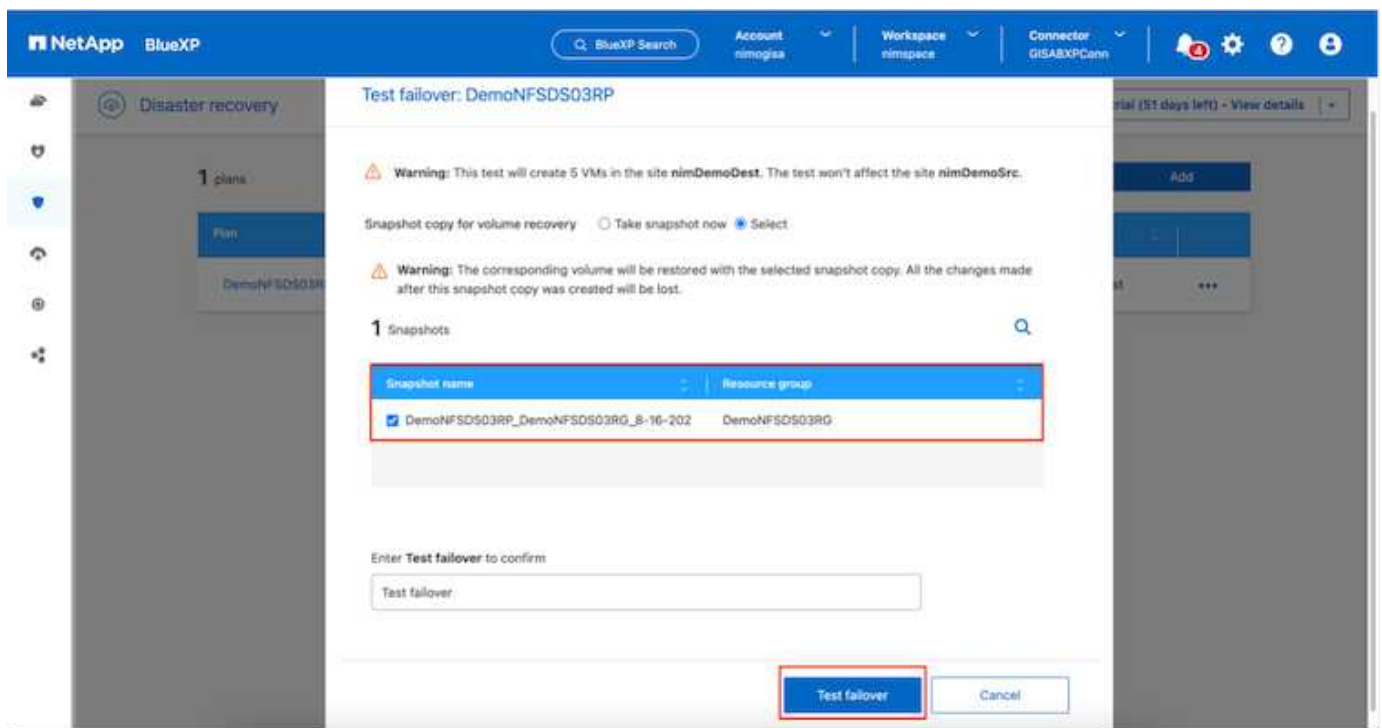
- テストフェイルオーバー（定期的な自動シミュレーションを含む）
- クリーンアップフェイルオーバーテスト
- フェイルオーバー
- フェイルバック

テストフェイルオーバー

BlueXP DRaaS のテスト フェイルオーバーは、VMware 管理者が実稼働環境を中断することなくリカバリ プランを完全に検証できるようにする運用手順です。



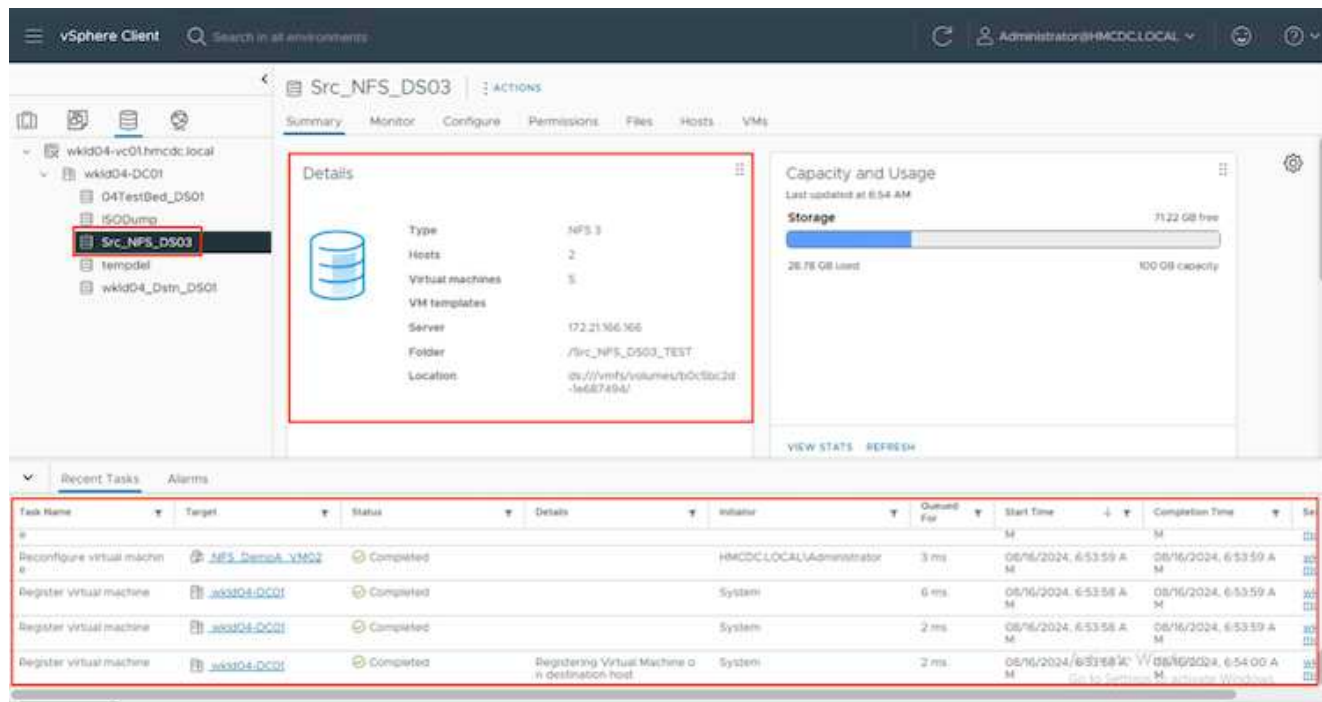
BlueXP DRaaS には、テスト フェイルオーバー操作のオプション機能としてスナップショットを選択する機能が組み込まれています。この機能により、VMware 管理者は、環境で最近行われた変更が宛先サイトに複製され、テスト中に存在していることを確認できます。このような変更には、VMゲストオペレーティングシステムへのパッチが含まれます。



VMware 管理者がテスト フェイルオーバー操作を実行すると、BlueXP DRaaS は次のタスクを自動化します。

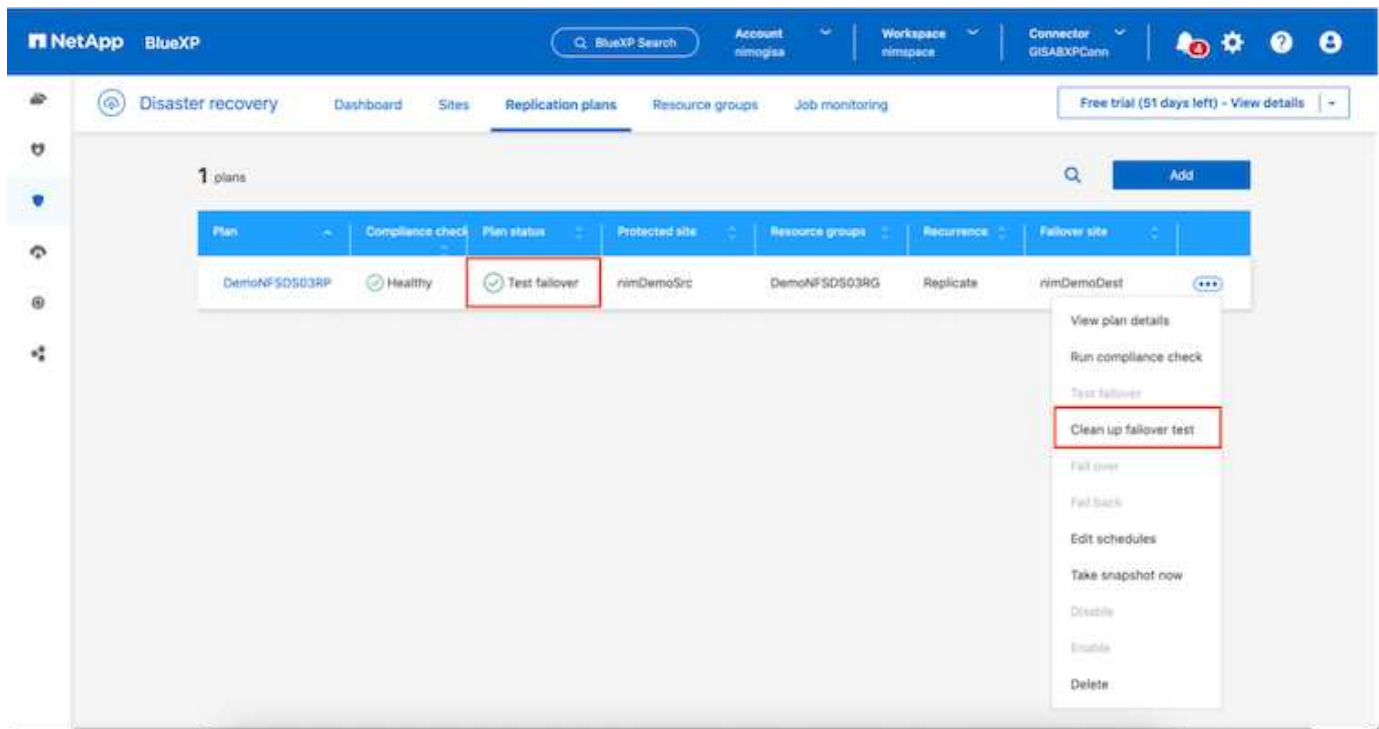
- SnapMirror関係をトリガーして、本番サイトで行われた最近の変更を宛先サイトのストレージに反映します。

- DR ストレージ アレイ上のFlexVolボリュームのNetApp FlexCloneボリュームを作成します。
- FlexCloneボリューム内の NFS データストアを DR サイトの ESXi ホストに接続します。
- マッピング中に指定されたテスト ネットワークに VM ネットワーク アダプターを接続します。
- DR サイトのネットワークの定義に従って、VM ゲスト オペレーティング システムのネットワーク設定を再構成します。
- レプリケーション プランに保存されているカスタム コマンドを実行します。
- レプリケーション プランで定義された順序で VM の電源をオンにします。



クリーンアップフェイルオーバーテスト操作

クリーンアップ フェイルオーバー テスト操作は、レプリケーション プラン テストが完了し、VMware 管理者がクリーンアップ プロンプトに応答した後に実行されます。



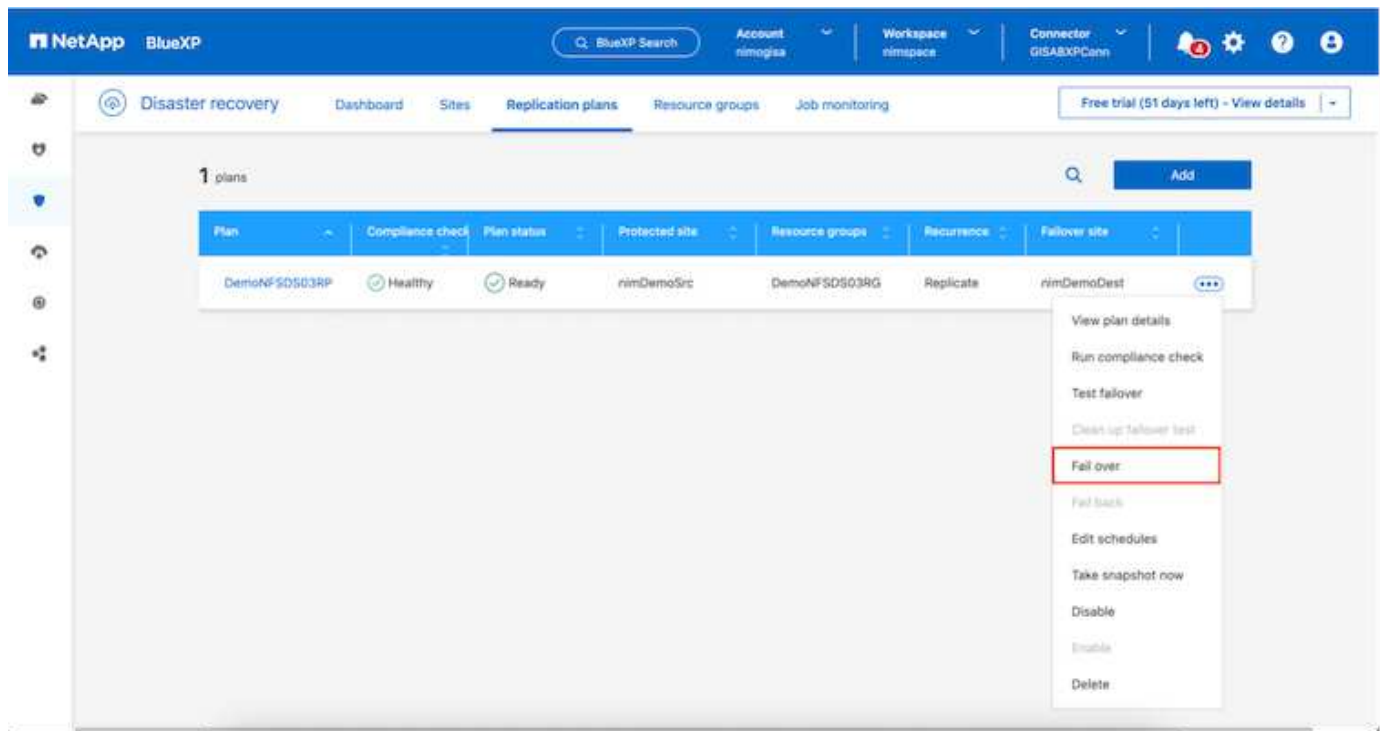
このアクションにより、仮想マシン (VM) とレプリケーション プランのステータスが準備完了状態にリセットされます。

VMware 管理者がリカバリ操作を実行すると、BlueXP DRaaS は次のプロセスを完了します。

1. テストに使用されたFlexCloneコピー内の回復された各 VM の電源をオフにします。
2. テスト中に回復された VM を表示するために使用されたFlexCloneボリュームを削除します。

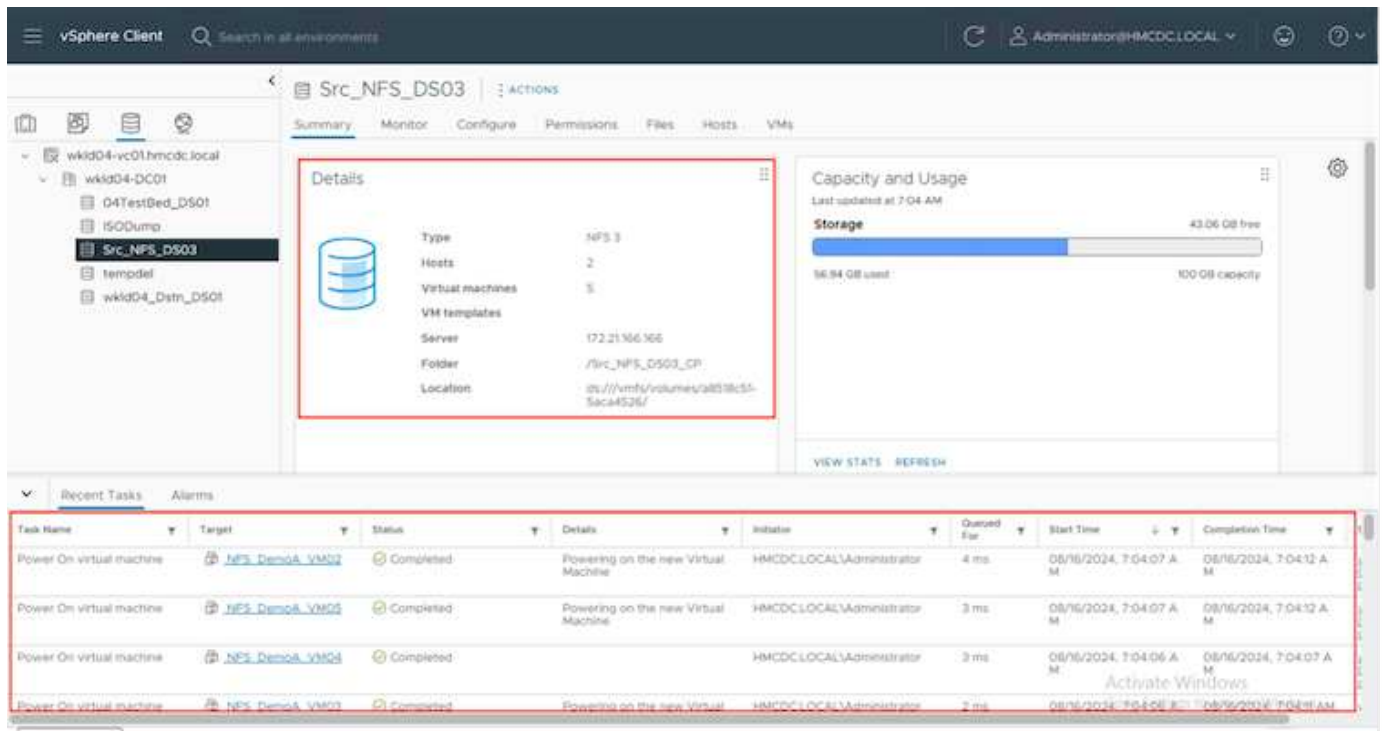
計画的な移行とフェイルオーバー

BlueXP DRaaS には、実際のフェイルオーバーを実行するための 2 つの方法 (計画された移行とフェイルオーバー) があります。最初の方法である計画移行では、VM のシャットダウンとストレージ レプリケーションの同期をプロセスに組み込んで、VM を回復するか、効率的に移行先サイトに移動させます。計画された移行にはソース サイトへのアクセスが必要です。2 番目の方法であるフェイルオーバーは、計画済み/計画外のフェイルオーバーであり、完了できた最後のストレージ レプリケーション間隔から宛先サイトで VM が回復されます。ソリューションに設計された RPO に応じて、DR シナリオではある程度のデータ損失が予想されます。



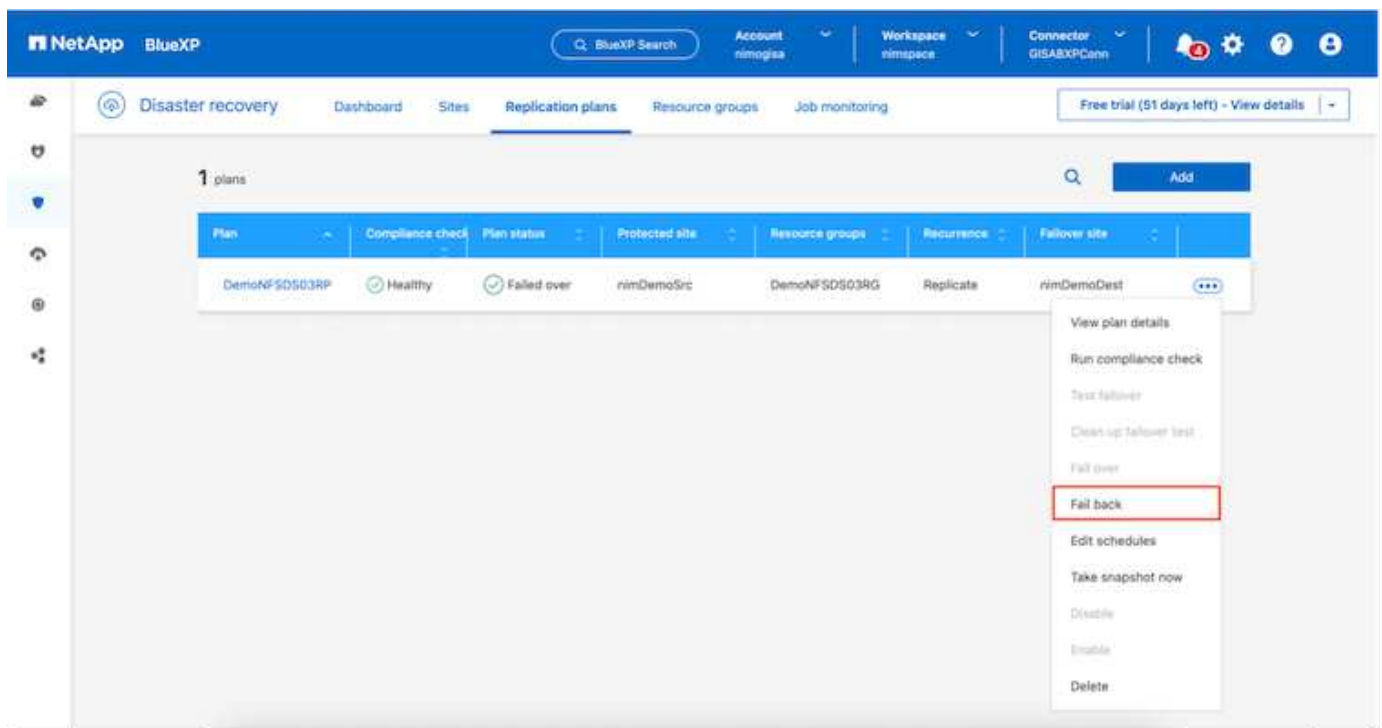
VMware 管理者がフェイルオーバー操作を実行すると、BlueXP DRaaS は次のタスクを自動化します。

- NetApp SnapMirror関係を解除してフェイルオーバーします。
- 複製された NFS データストアを DR サイトの ESXi ホストに接続します。
- VM ネットワーク アダプターを適切な宛先サイト ネットワークに接続します。
- 宛先サイトのネットワークの定義に従って、VM ゲスト オペレーティング システムのネットワーク設定を再構成します。
- レプリケーション プランに保存されているカスタム コマンド (存在する場合) を実行します。
- レプリケーション プランで定義された順序で VM の電源をオンにします。



フェイルバック

フェイルバックは、回復後にソース サイトと宛先サイトの元の構成を復元するオプションの手順です。



VMware 管理者は、サービスを元のソース サイトに復元する準備ができれば、フェイルバック手順を構成して実行できます。

注意: BlueXP DRaaS 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。

- 仮想マシンの電源をオフにして登録を解除すると、宛先サイトのボリュームがマウント解除されます。
- 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。
- ソースにボリュームをマウントし、ソース仮想マシンをパワーオンして登録します。

BlueXP DRaaSへのアクセスと設定の詳細については、"[BlueXP Disaster Recovery for VMware について学ぶ](#)"。

監視とダッシュボード

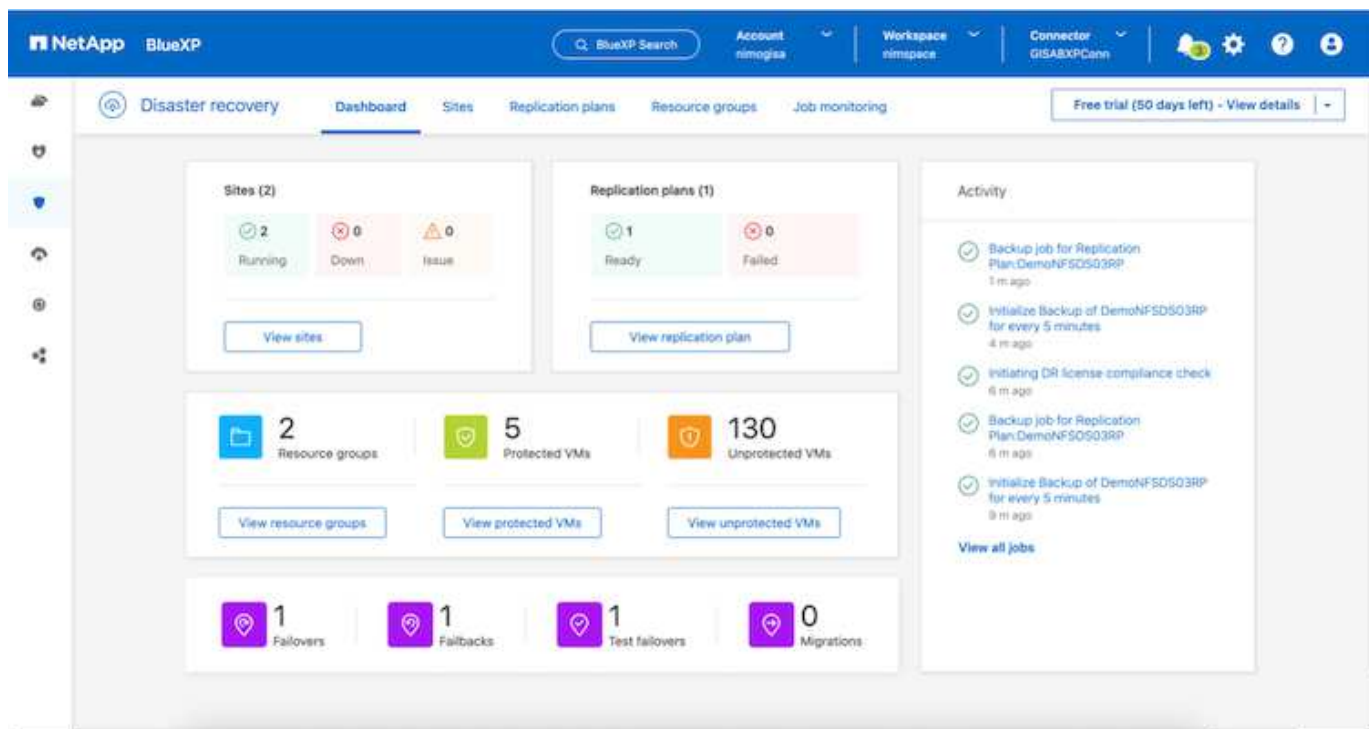
BlueXPまたはONTAP CLI から、適切なデータストア ボリュームのレプリケーションのヘルス ステータスを監視し、ジョブ監視を介してフェイルオーバーまたはテスト フェイルオーバーのステータスを追跡できます。

ID	Status	Workload	Name	Start time	End time	
d923e507-b2c2-401	In pro...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:5...	-	Cancel job?
3549cc9c-aa4e-45e	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:5...	08/16/2024, 04:5...	
5cb01bcc-9ea6-4af1	Succe...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:5...	
a2f225d9-b7be-4c2f	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
2f8b44d4-4be2-46e	Succe...	Compliance	Compliance check for Replication Plan: D...	08/16/2024, 04:4...	08/16/2024, 04:4...	
398bc6a3-ata8-45d	Succe...	Compliance	Initialize Compliance of DemoNFSD503R...	08/16/2024, 04:4...	08/16/2024, 04:4...	
97fdbed8-6f77-459f	Succe...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:4...	
bffc018e-ca3a-409d	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
cde759a8-ebef-498e	Succe...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:3...	08/16/2024, 04:4...	
a414daba-9830-4c5	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:3...	08/16/2024, 04:3...	



ジョブが現在進行中またはキューに入っており、それを停止したい場合は、キャンセルするオプションがあります。

BlueXP disaster recoveryダッシュボードを使用すると、災害復旧サイトとレプリケーション プランの状態を確実に評価できます。これにより、管理者は正常なサイトやプラン、切断されたサイトやプラン、または機能低下したサイトやプランを迅速に特定できます。



これにより、調整およびカスタマイズされた災害復旧計画を処理するための強力なソリューションが提供されます。フェイルオーバーは、計画されたフェイルオーバーとして実行することも、災害が発生して DR サイトをアクティブ化する決定が下されたときにボタンをクリックするだけでフェイルオーバーを実行することもできます。

このプロセスについて詳しく知りたい場合は、詳細なウォークスルービデオをご覧ください。 ["ソリューションシミュレータ"](#)。

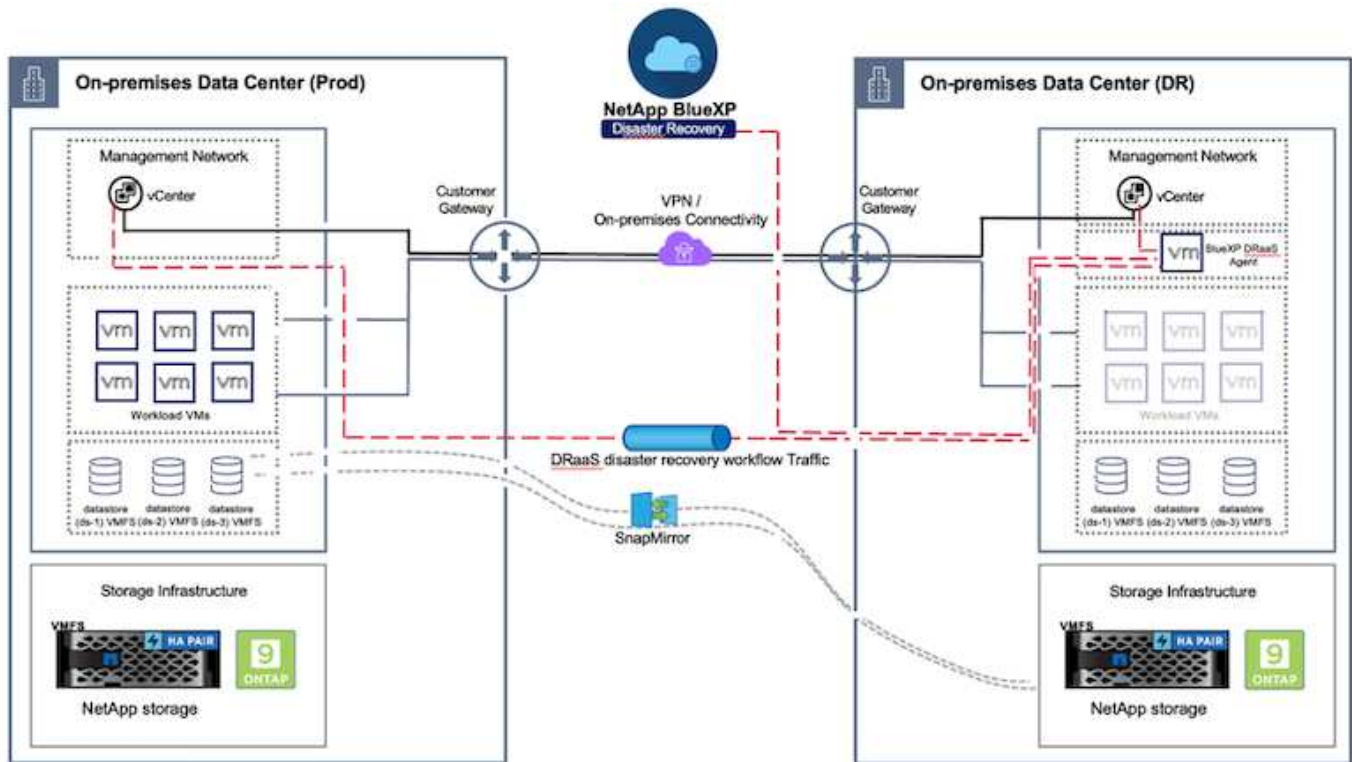
VMFS データストア向けBlueXP DRaaS を使用した DR

運用サイトから災害復旧サイトへのブロックレベルのレプリケーションを使用した災害復旧は、サイトの停止やランサムウェア攻撃などの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 SnapMirrorレプリケーションを使用すると、VMFSデータストアを使用してオンプレミスのONTAPシステムで実行されているVMwareワークロードを、VMwareが存在する指定されたリカバリデータセンター内の別のONTAPストレージシステムに複製できます。

このドキュメントのセクションでは、オンプレミスの VMware VM の災害復旧を別の指定サイトに設定するためのBlueXP DRaaS の構成について説明します。このセットアップの一部として、BlueXPアカウント、BlueXPコネクタ、VMware vCenter からONTAPストレージへの通信を可能にするために必要なONTAPアレイがBlueXPワークスペース内に追加されます。さらに、このドキュメントでは、サイト間のレプリケーションを構成する方法と、リカバリ プランを設定およびテストする方法についても詳しく説明します。最後のセクションでは、サイト全体のフェールオーバーを実行する手順と、プライマリ サイトが回復されオンラインで購入されたときにフェールバックする方法について説明します。

NetApp BlueXPコンソールに統合されているBlueXP disaster recoveryサービスを使用すると、顧客はオンプレミスの VMware vCenter とONTAPストレージを検出し、リソース グループを作成し、ディザスタ リカバリプランを作成してリソース グループに関連付け、フェイルオーバーとフェールバックをテストまたは実行できます。 SnapMirror は、ストレージ レベルのブロック レプリケーションを提供し、2 つのサイトを増分変更で最新の状態に保ち、RPO を最大 5 分に抑えます。また、本番環境や複製されたデータストアに影響を与え

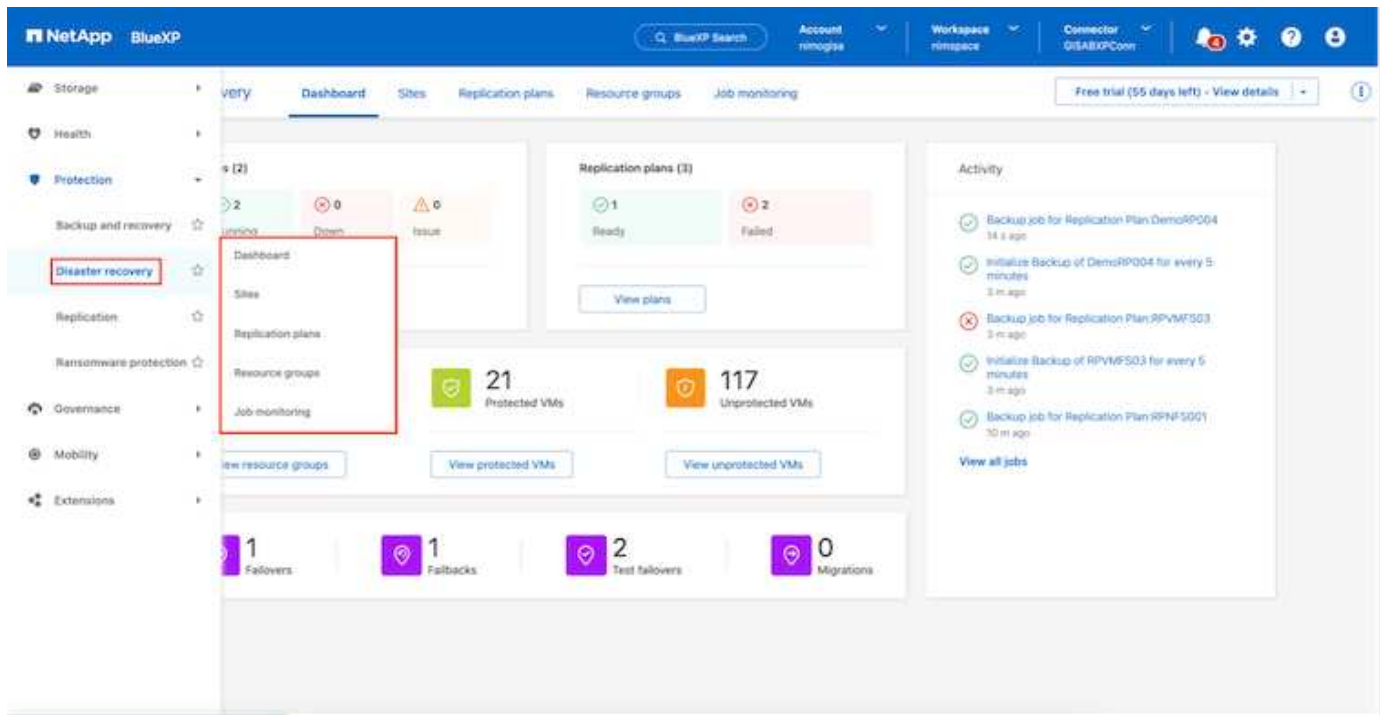
たり、追加のストレージコストを発生させたりすることなく、定期的な訓練として DR 手順をシミュレートすることもできます。BlueXP disaster recoveryは、ONTAP のFlexCloneテクノロジーを活用して、DR サイトで最後に複製されたスナップショットから VMFS データストアのスペース効率の高いコピーを作成します。DR テストが完了すると、顧客はテスト環境を削除するだけで済み、実際の複製された本番リソースには影響しません。実際のフェイルオーバー (計画的または計画外) が必要な場合、数回クリックするだけで、BlueXP disaster recoveryサービスが、指定された災害復旧サイトで保護された仮想マシンを自動的に起動するために必要なすべての手順を調整します。このサービスは、必要に応じて、プライマリ サイトへの SnapMirror関係を逆転させ、フェイルバック操作のためにセカンダリ サイトからプライマリ サイトへの変更を複製します。これらすべては、他のよく知られている代替手段に比べて、ほんのわずかなコストで実現できます。



開始

BlueXP disaster recoveryを開始するには、BlueXPコンソールを使用してサービスにアクセスします。

1. BlueXPにログインします。
2. BlueXP 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. BlueXP disaster recoveryダッシュボードが表示されます。



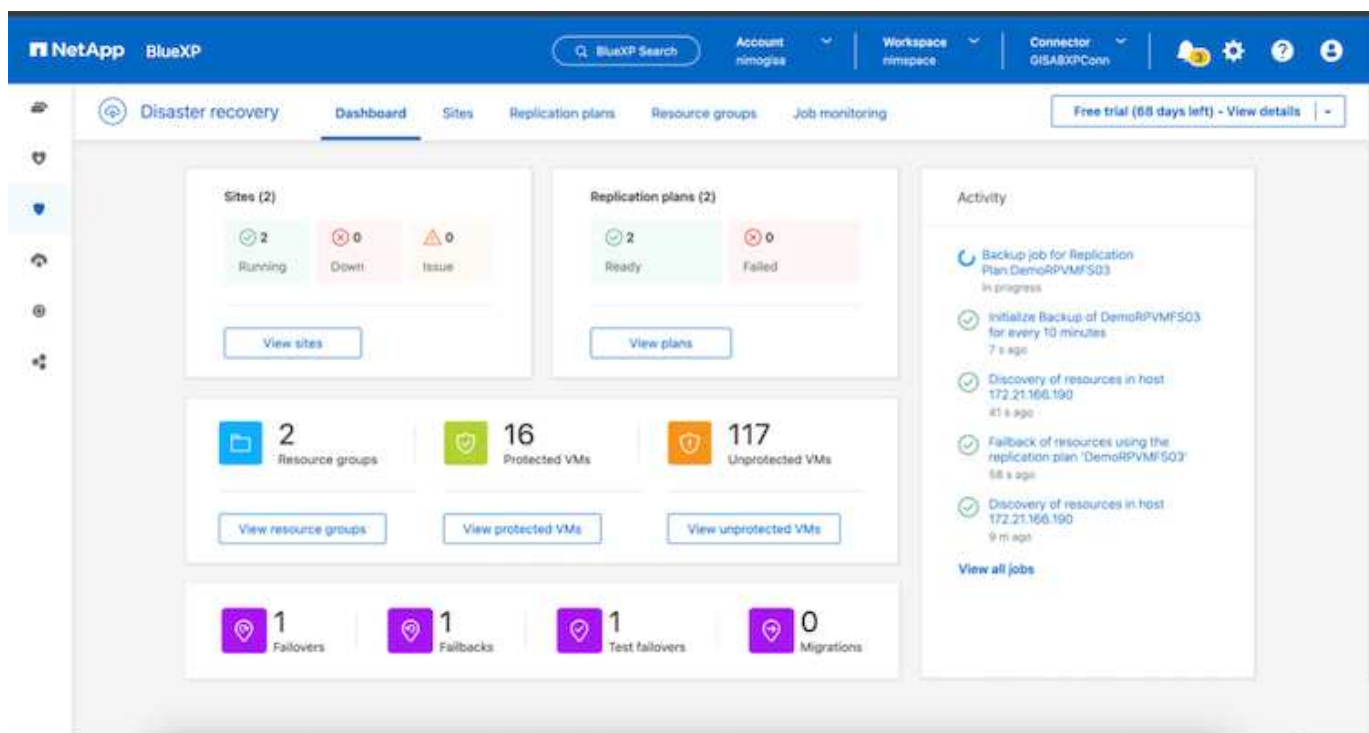
災害復旧計画を構成する前に、次の前提条件が満たされていることを確認してください。

- BlueXPコネクタはNetApp BlueXPに設定されます。コネクタはAWS VPC にデプロイする必要があります。
- BlueXPコネクタ インスタンスは、ソースおよびターゲットの vCenter およびストレージ システムに接続できます。
- VMware 用の VMFS データストアをホストするオンプレミスのNetAppストレージ システムがBlueXPに追加されます。
- DNS 名を使用する場合は、DNS 解決を実施する必要があります。それ以外の場合は、vCenter の IP アドレスを使用します。
- 指定された VMFS ベースのデータストア ボリュームに対してSnapMirrorレプリケーションが構成されます。

ソース サイトと宛先サイト間の接続が確立されたら、構成手順に進みます。これには約 3 ～ 5 分かかります。



NetApp、実際の障害や自然災害の発生時にBlueXPコネクタがネットワークを介してソース リソースおよび宛先リソースと通信できるように、災害復旧サイトまたは第 3 のサイトにBlueXP コネクタを導入することを推奨しています。



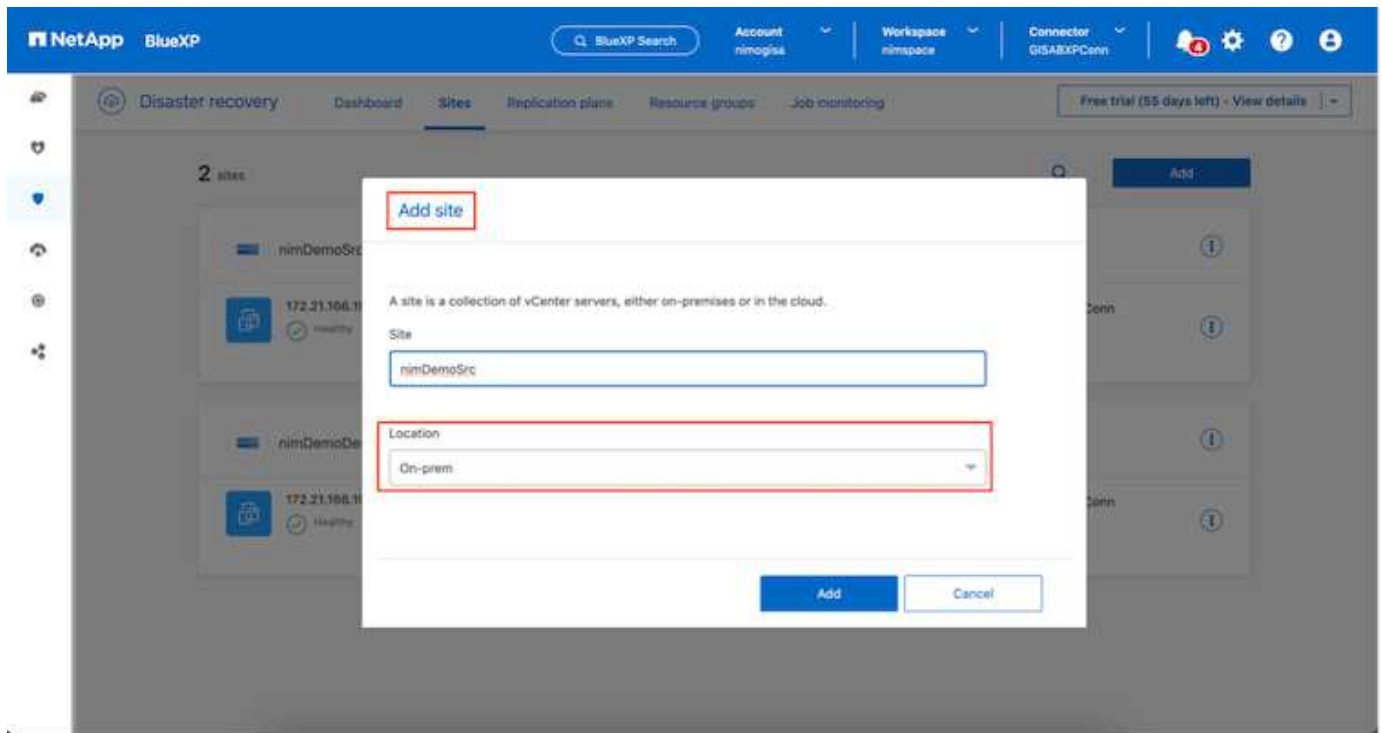
このドキュメントの執筆時点では、オンプレミスからオンプレミスへの VMFS データストアのサポートはテクノロジー プレビュー段階です。この機能は、FC および iSCSI プロトコル ベースの VMFS データストアの両方でサポートされます。

BlueXP disaster recovery構成

災害復旧の準備の最初のステップは、オンプレミスの vCenter とストレージ リソースを検出し、BlueXP disaster recoveryに追加することです。

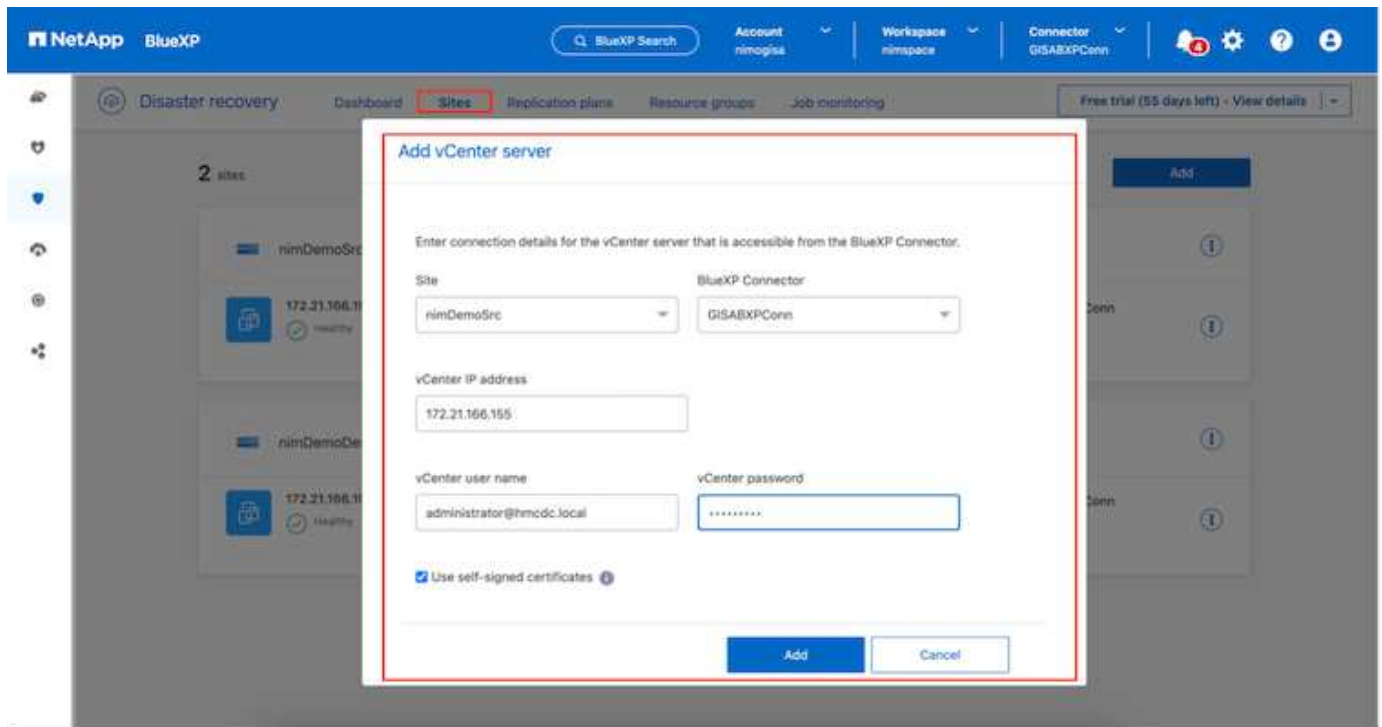


ONTAPストレージ システムがキャンバス内の作業環境に追加されていることを確認します。BlueXPコンソールを開き、左側のナビゲーションから 保護 > 災害復旧 を選択します。**vCenter** サーバーの検出 を選択するか、トップ メニューを使用して サイト > 追加 > **vCenter** の追加 を選択します。

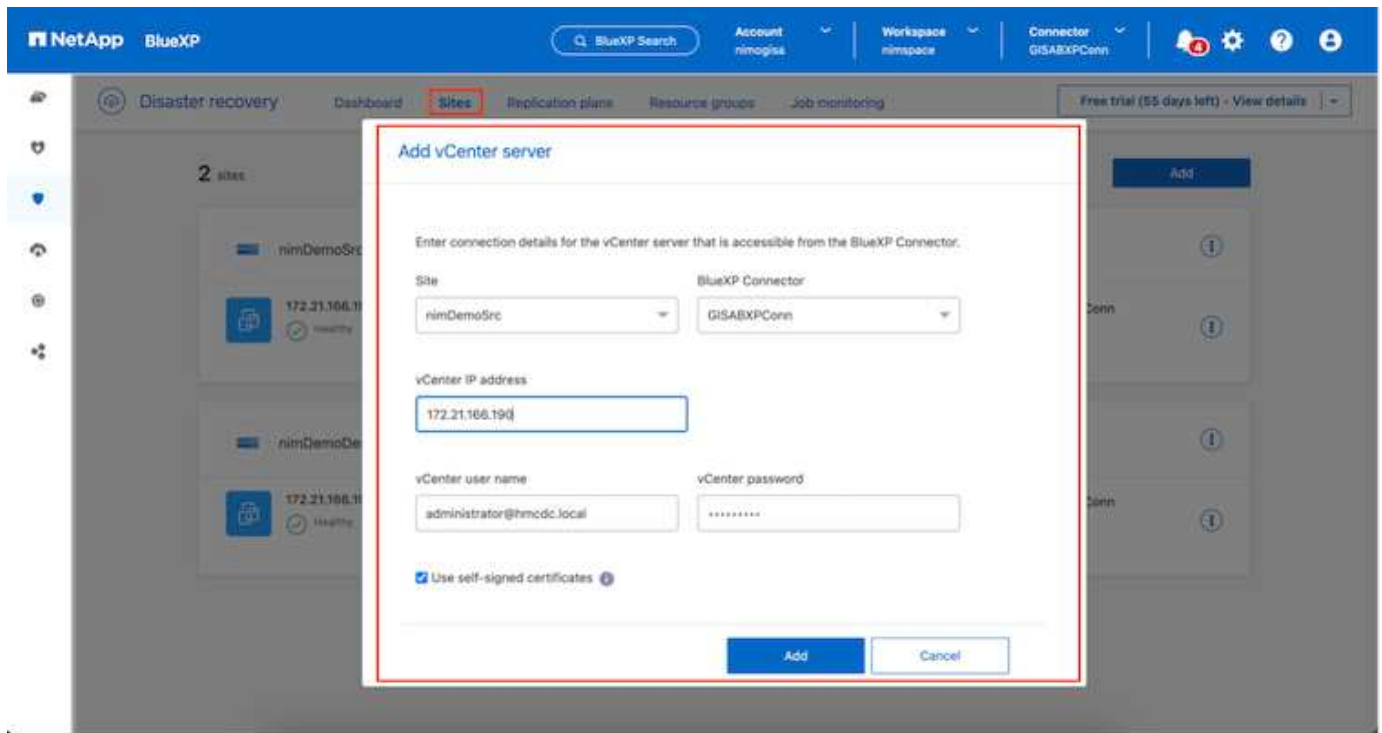


次のプラットフォームを追加します。

- ソース。オンプレミスの vCenter。



- 行き先。VMC SDDC vCenter。



vCenter が追加されると、自動検出がトリガーされます。

ソースサイトと宛先サイト間のストレージレプリケーションの構成

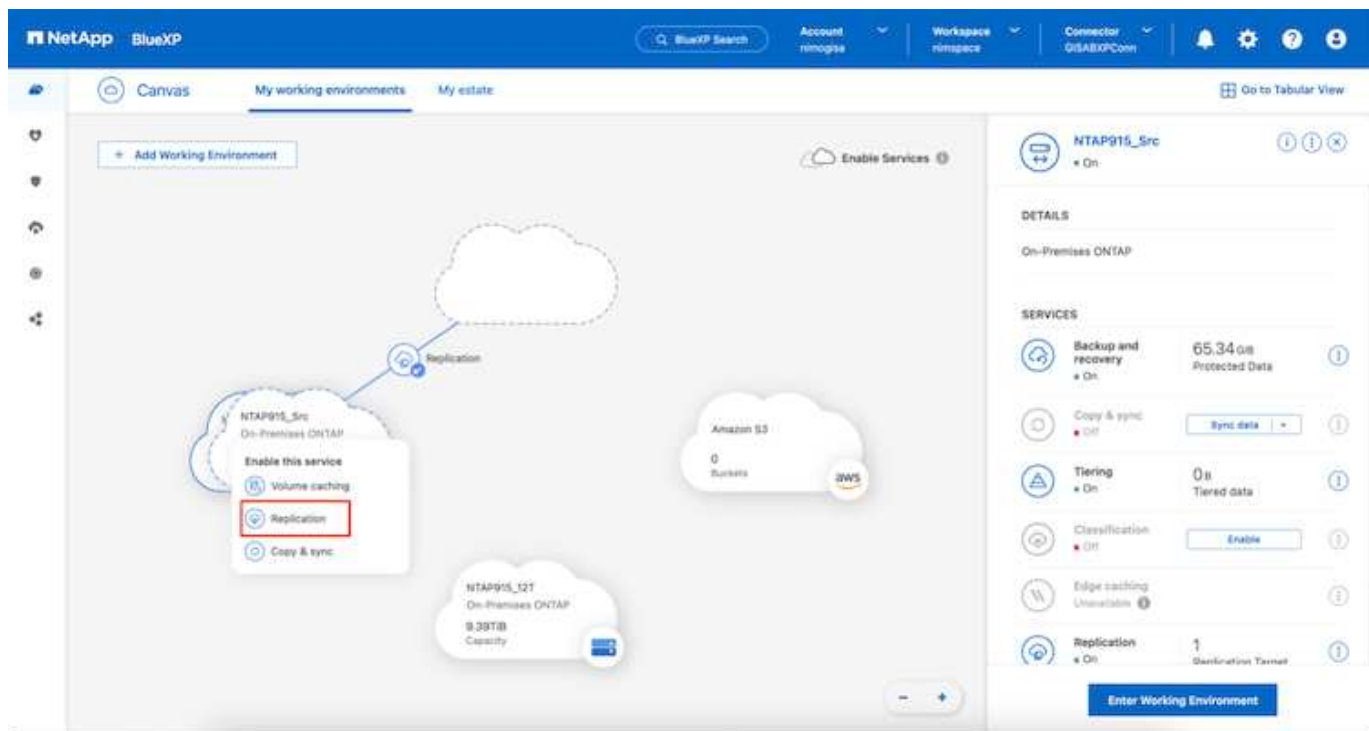
SnapMirror は ONTAP スナップショットを利用して、ある場所から別の場所へのデータの転送を管理します。最初に、ソース ボリュームのスナップショットに基づく完全なコピーが宛先にコピーされ、ベースライン同期が実行されます。ソースでデータの変更が発生すると、新しいスナップショットが作成され、ベースライン スナップショットと比較されます。変更されたと判明したブロックは宛先に複製され、新しいスナップショットが現在のベースライン、つまり最新の共通スナップショットになります。これにより、プロセスを繰り返し、増分更新を宛先に送信できるようになります。

SnapMirror 関係が確立されると、宛先ボリュームはオンライン読み取り専用状態になり、引き続きアクセス可能になります。SnapMirror は、ファイルやその他の論理レベルではなく、ストレージの物理ブロックで動作します。つまり、複製先ボリュームは、スナップショット、ボリューム設定などを含め、複製元ボリュームと同一のレプリカになります。データ圧縮やデータ重複排除などの ONTAP スペース効率機能が複製元ボリュームで使用されている場合、複製されたボリュームではこれらの最適化が保持されます。

SnapMirror 関係を解除すると、宛先ボリュームが書き込み可能になり、通常は SnapMirror を使用して DR 環境にデータを同期しているときにフェイルオーバーを実行するために使用されます。SnapMirror は非常に洗練されており、フェイルオーバー サイトで変更されたデータをプライマリ システムに効率的に再同期し、プライマリ システムが後でオンラインに戻ったときに、元の SnapMirror 関係を再確立することができます。

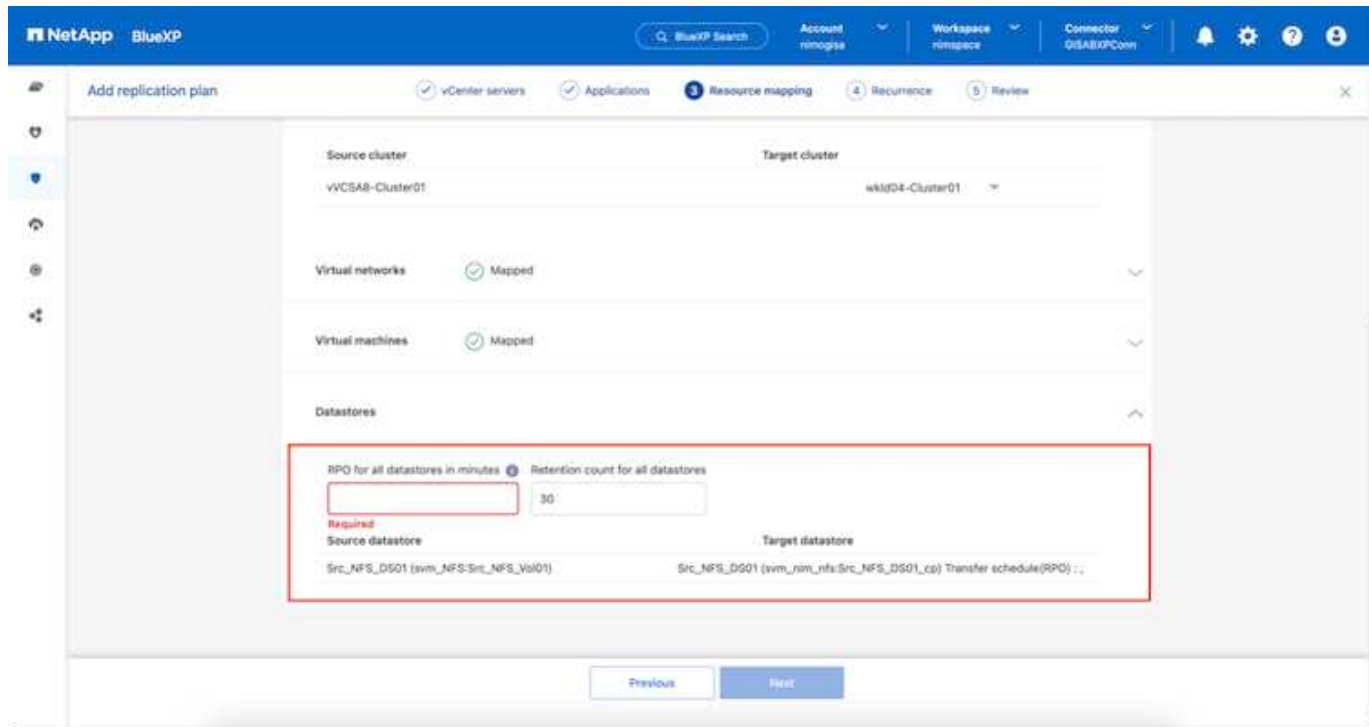
VMware Disaster Recovery の設定方法

SnapMirror レプリケーションを作成するプロセスは、どのアプリケーションでも同じです。このプロセスは手動でも自動でも実行できます。最も簡単な方法は、BlueXP を利用して、環境内のソース ONTAP システムを宛先にドラッグ アンド ドロップするだけで SnapMirror レプリケーションを構成し、残りのプロセスをガイドするウィザードを起動することです。



BlueXP DRaaS では、次の 2 つの条件が満たされている場合、同じことを自動化することもできます。

- ソース クラスターと宛先クラスターにはピア関係があります。
- ソース SVM と宛先 SVM にはピア関係があります。



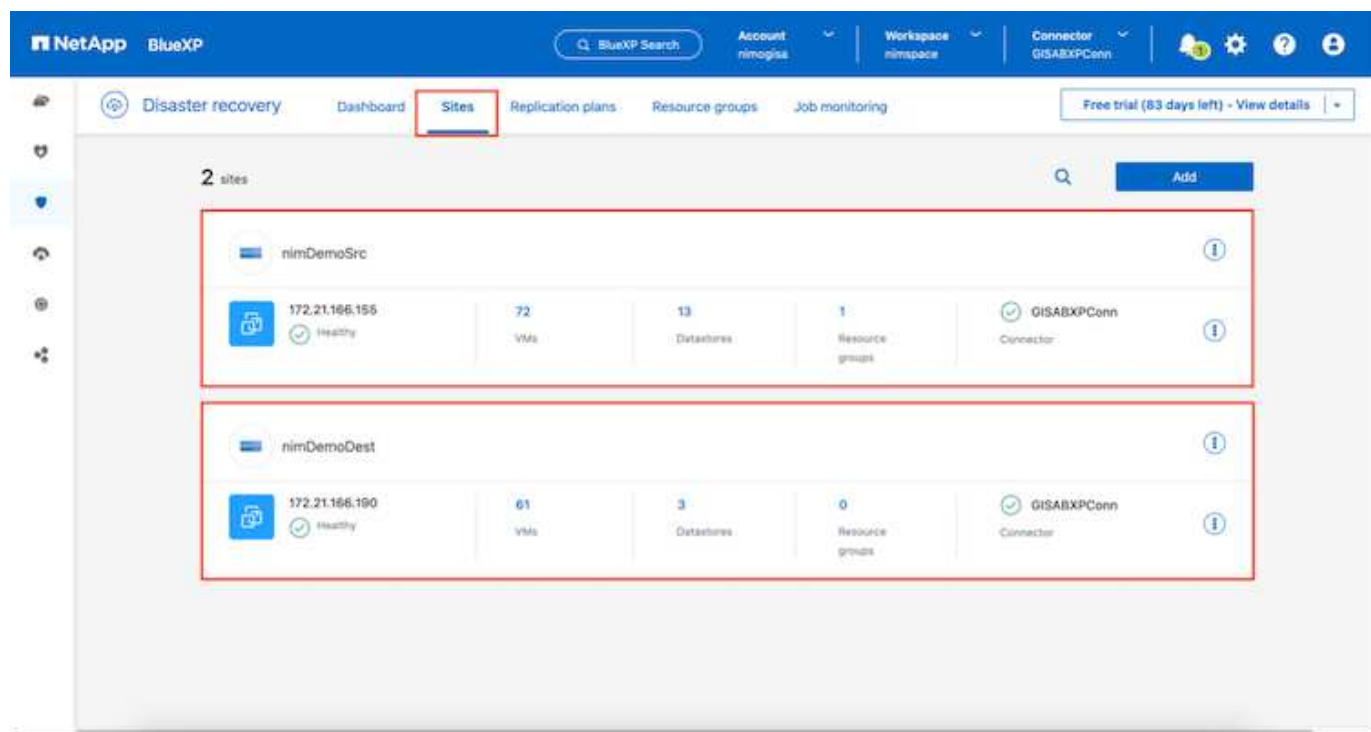
CLI 経由でボリュームに SnapMirror 関係がすでに設定されている場合、BlueXP DRaaS はその関係を取得し、残りのワークフロー操作を続行します。



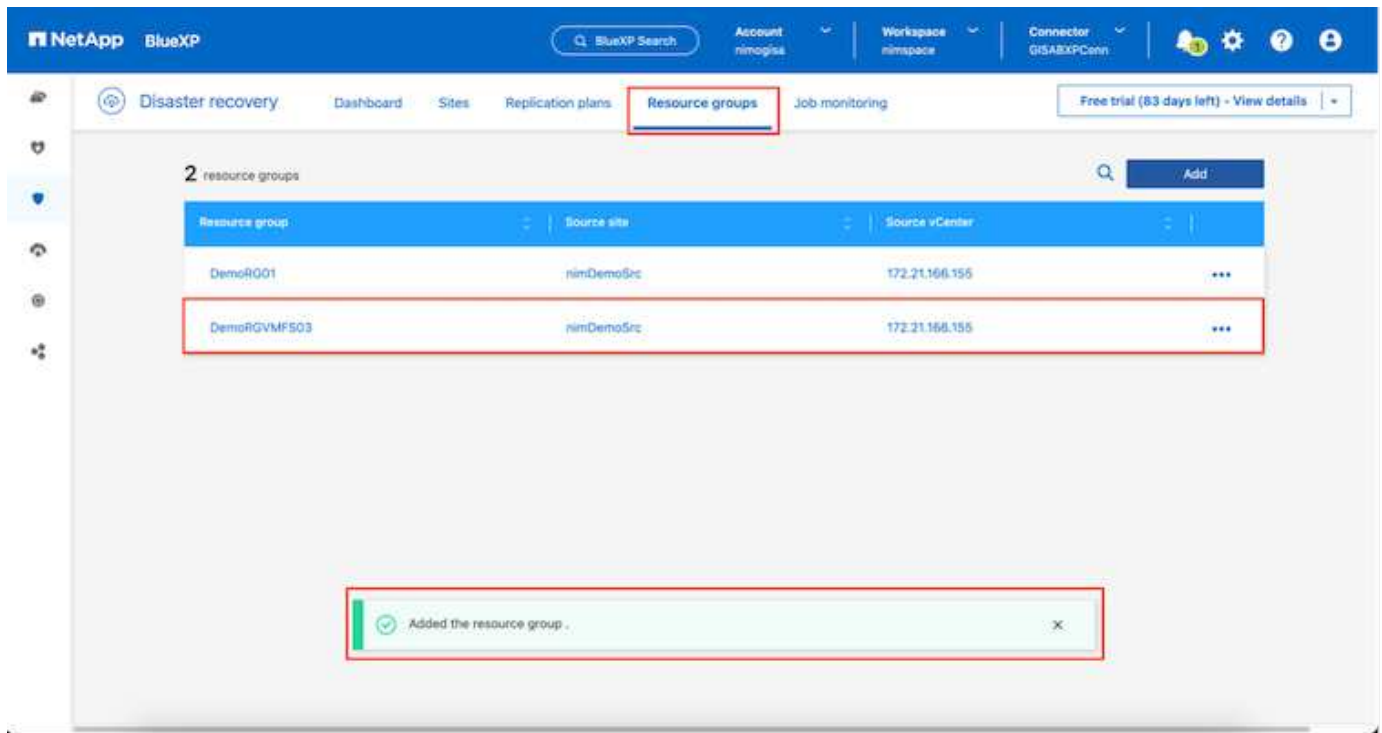
上記の方法以外にも、SnapMirrorレプリケーションはONTAP CLI または System Manager 経由で作成することもできます。SnapMirrorを使用してデータを同期するために使用されるアプローチに関係なく、BlueXP DRaaS は、シームレスで効率的な災害復旧操作のワークフローを調整します。

BlueXP disaster recoveryは何を実現できるのでしょうか？

ソース サイトと宛先サイトが追加されると、BlueXP disaster recoveryは自動的に詳細な検出を実行し、VM と関連メタデータを表示します。BlueXP disaster recoveryでは、VM で使用されるネットワークとポートグループも自動的に検出し、それらを入力します。

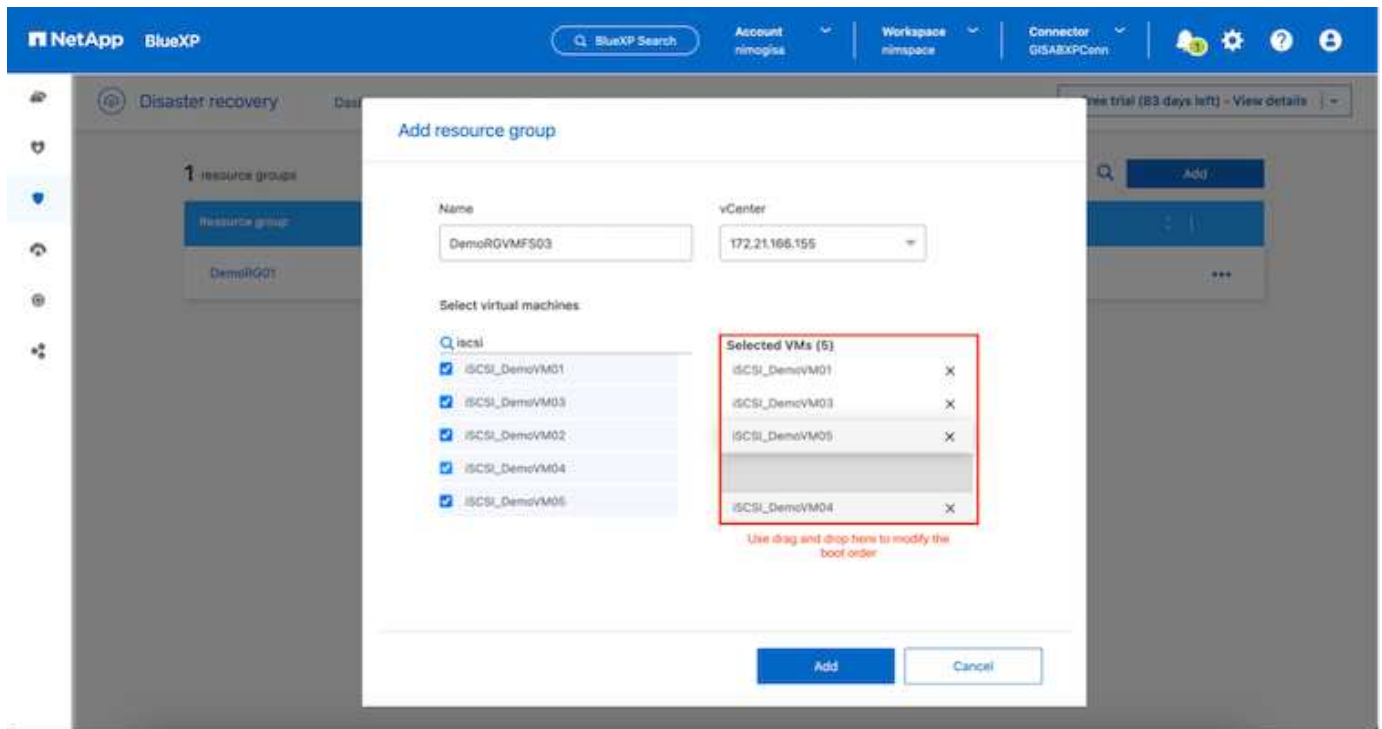


サイトを追加した後、VM をリソース グループにグループ化できます。BlueXP disaster recoveryリソース グループを使用すると、依存する VM のセットを、復旧時に実行できるブート順序とブート遅延を含む論理グループにグループ化できます。リソース グループの作成を開始するには、[リソース グループ] に移動し、[新しいリソース グループの作成] をクリックします。

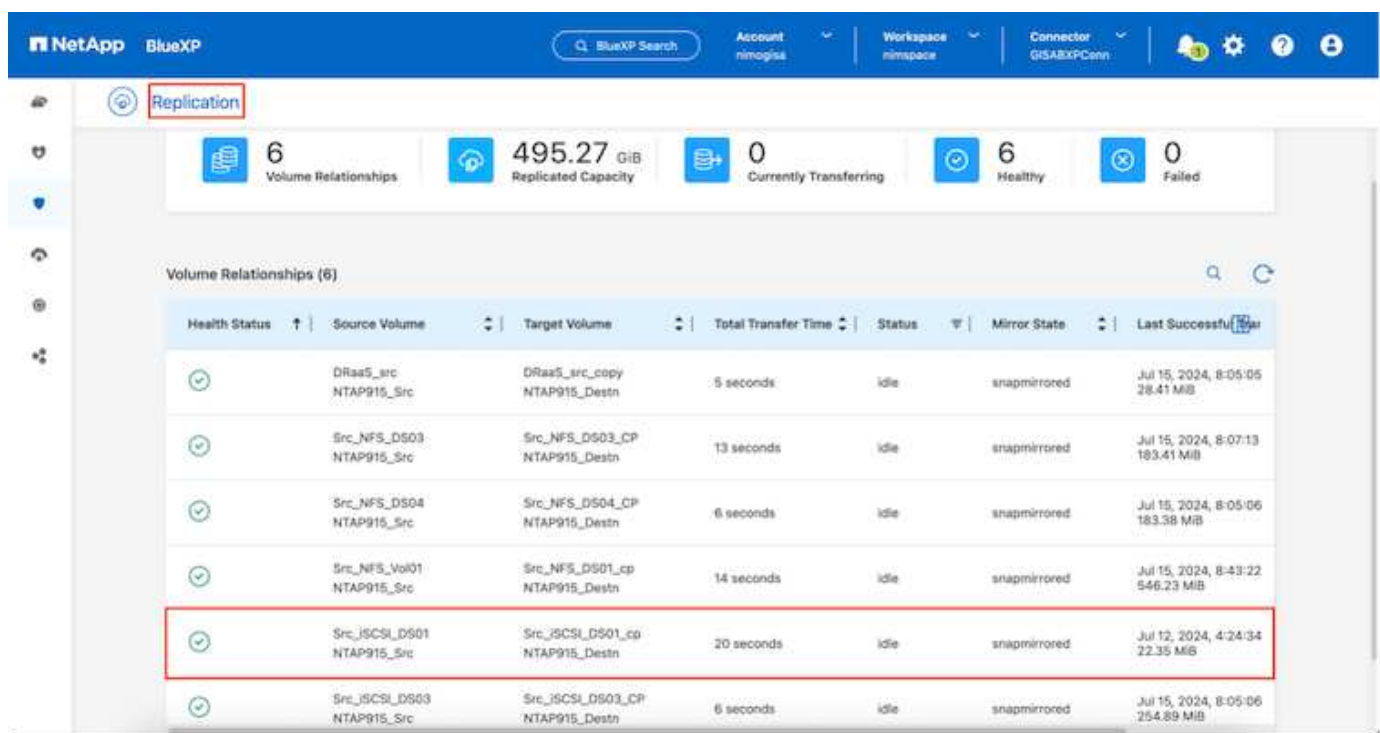
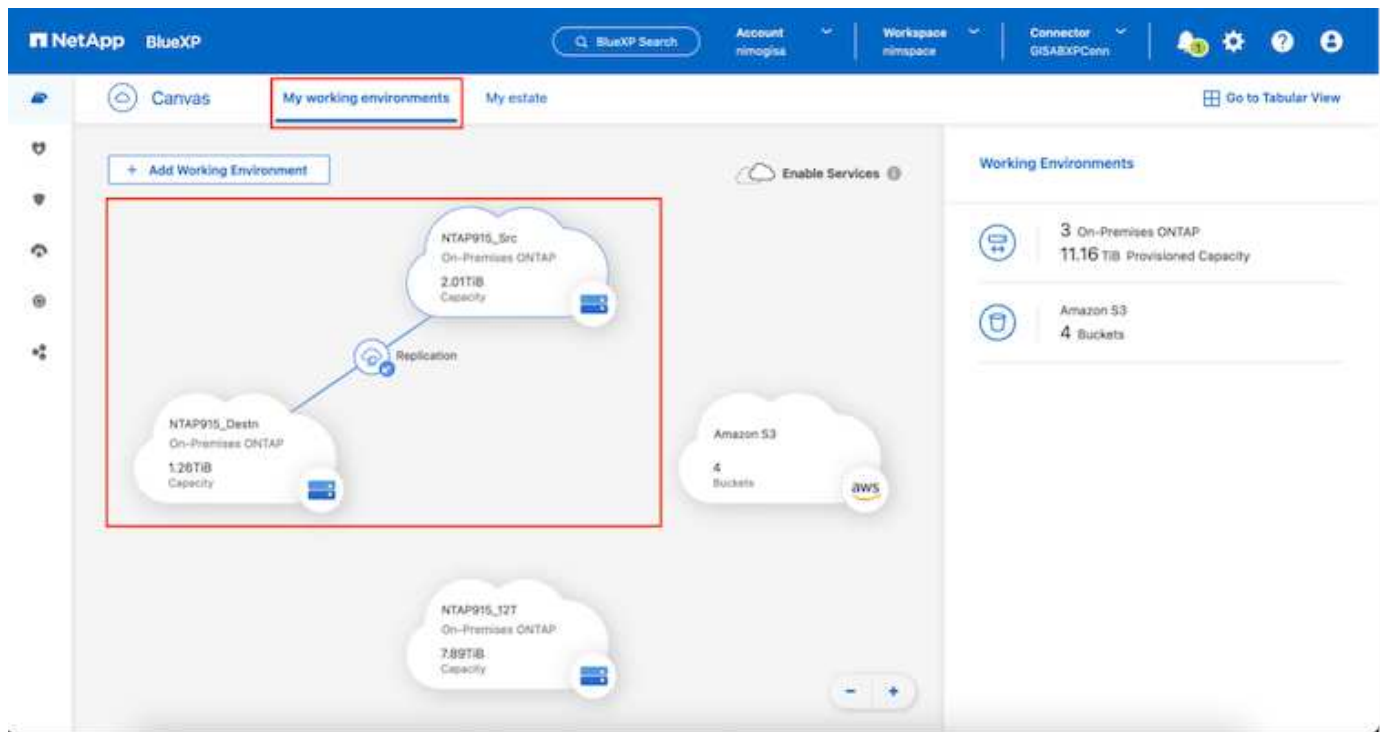


レプリケーションプランの作成時にリソースグループを作成することもできます。

VM のブート順序は、リソースグループの作成中に、簡単なドラッグアンドドロップメカニズムを使用して定義または変更できます。

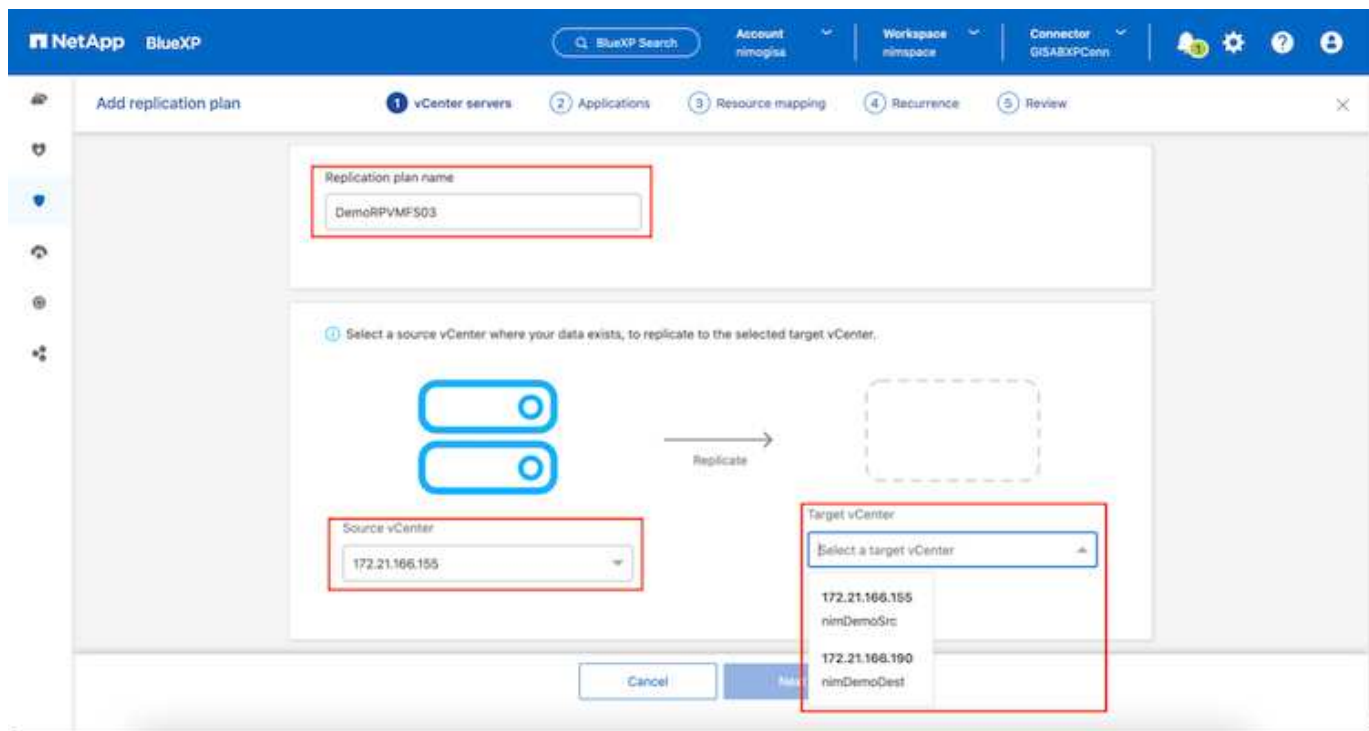


リソースグループを作成したら、次のステップは、災害発生時に仮想マシンとアプリケーションを復旧するための実行ブループリントまたは計画を作成することです。前提条件で述べたように、SnapMirrorレプリケーションは事前に構成することも、レプリケーションプランの作成時に指定されたRPOと保持数を使用してDRaaSで構成することもできます。

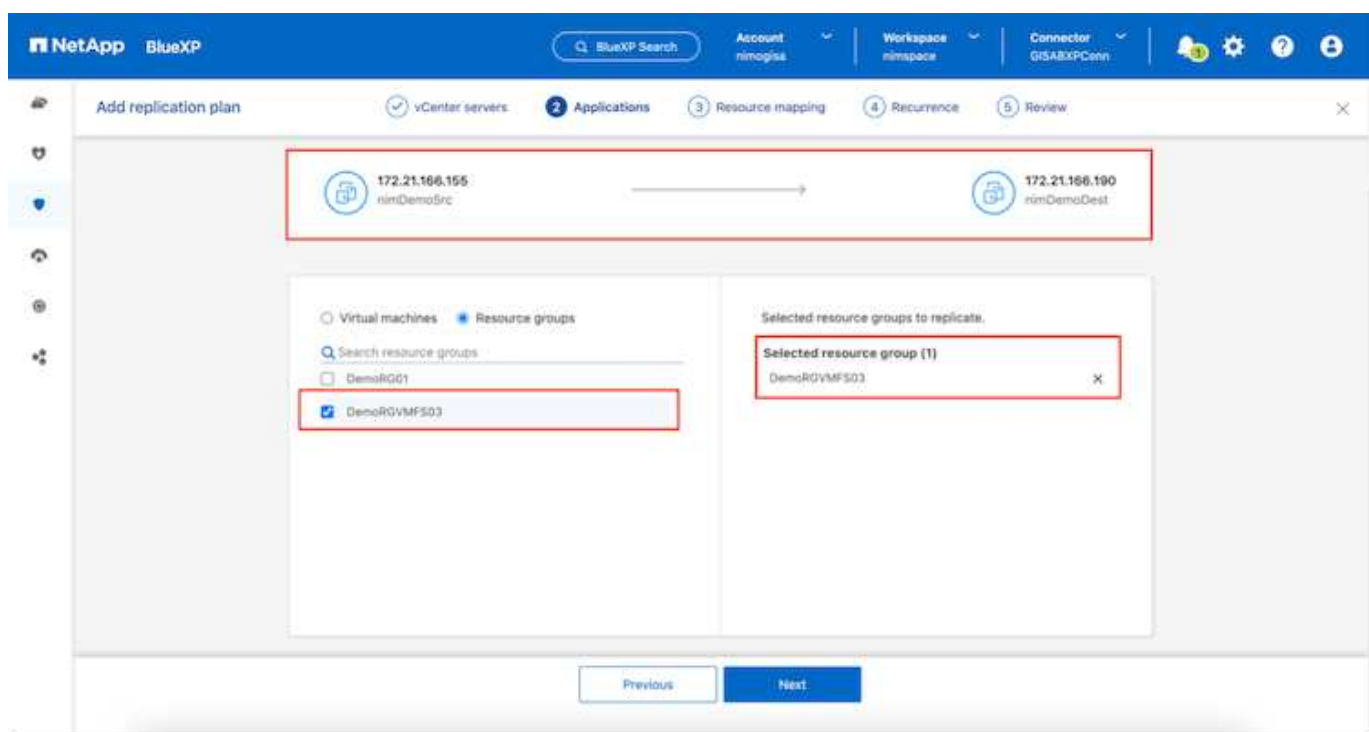


ドロップダウンからソースと宛先の vCenter プラットフォームを選択してレプリケーション プランを構成し、プランに含めるリソース グループ、アプリケーションの復元方法と電源オン方法のグループ化、およびクラスタとネットワークのマッピングを選択します。リカバリ プランを定義するには、[レプリケーション プラン] タブに移動し、[プランの追加] をクリックします。

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



次のステップは、既存のリソースグループを選択することです。リソースグループが作成されていない場合、ウィザードは、回復目標に基づいて必要な仮想マシンをグループ化します (基本的には機能リソースグループを作成します)。これは、アプリケーション仮想マシンを復元する操作シーケンスを定義するのにも役立ちます。

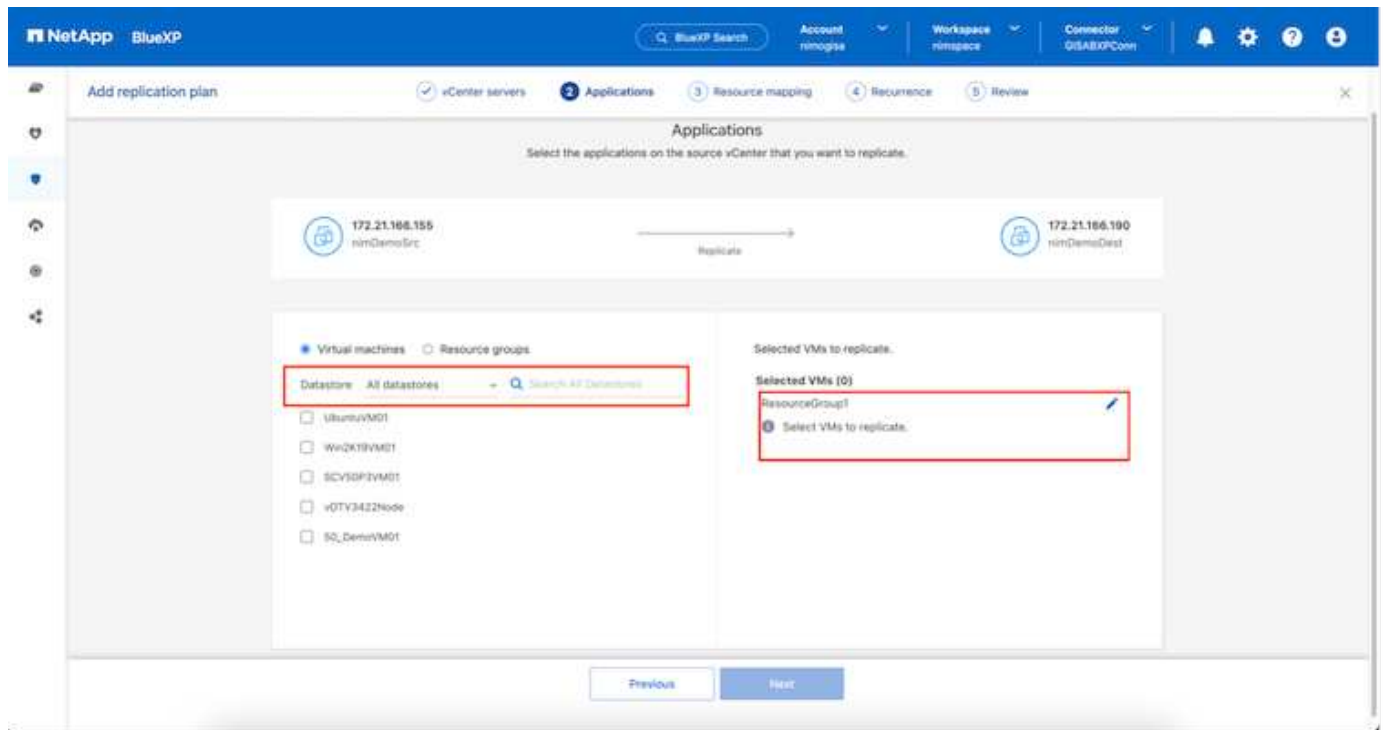


リソースグループでは、ドラッグアンドドロップ機能を使用してブート順序を設定できます。これを使用すると、リカバリプロセス中に VM の電源がオンになる順序を簡単に変更できます。



リソース グループ内の各仮想マシンは、順序に基づいて順番に起動されます。2つのリソースグループが並行して開始されます。

以下のスクリーンショットは、リソース グループが事前に作成されていない場合に、組織の要件に基づいて仮想マシンまたは特定のデータストアをフィルターするオプションを示しています。



リソース グループを選択したら、フェールオーバー マッピングを作成します。このステップでは、ソース環境のリソースを宛先にどのようにマップするかを指定します。これには、コンピューティング リソース、仮想ネットワークが含まれます。IP カスタマイズ、事前スクリプトと事後スクリプト、ブート遅延、アプリケーションの一貫性など。詳細については、"[レプリケーションプランを作成する](#)"。

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

Source VM	CPUs	RAM	Boot delay (mins between 0 and 10)	Create application consistent replicas	Scripts
DemoR001					
S0_DemoVM	2	4 GiB	0	<input type="checkbox"/>	None
S0_DemoVM01	2	4 GiB	0	<input type="checkbox"/>	None
S0_DemoVM02	2	4 GiB	0	<input type="checkbox"/>	None

Previous Next



デフォルトでは、テスト操作とフェイルオーバー操作の両方に同じマッピング パラメータが使用されます。テスト環境に異なるマッピングを適用するには、以下に示すようにチェックボックスをオフにした後、テスト マッピング オプションを選択します。

Resource mapping

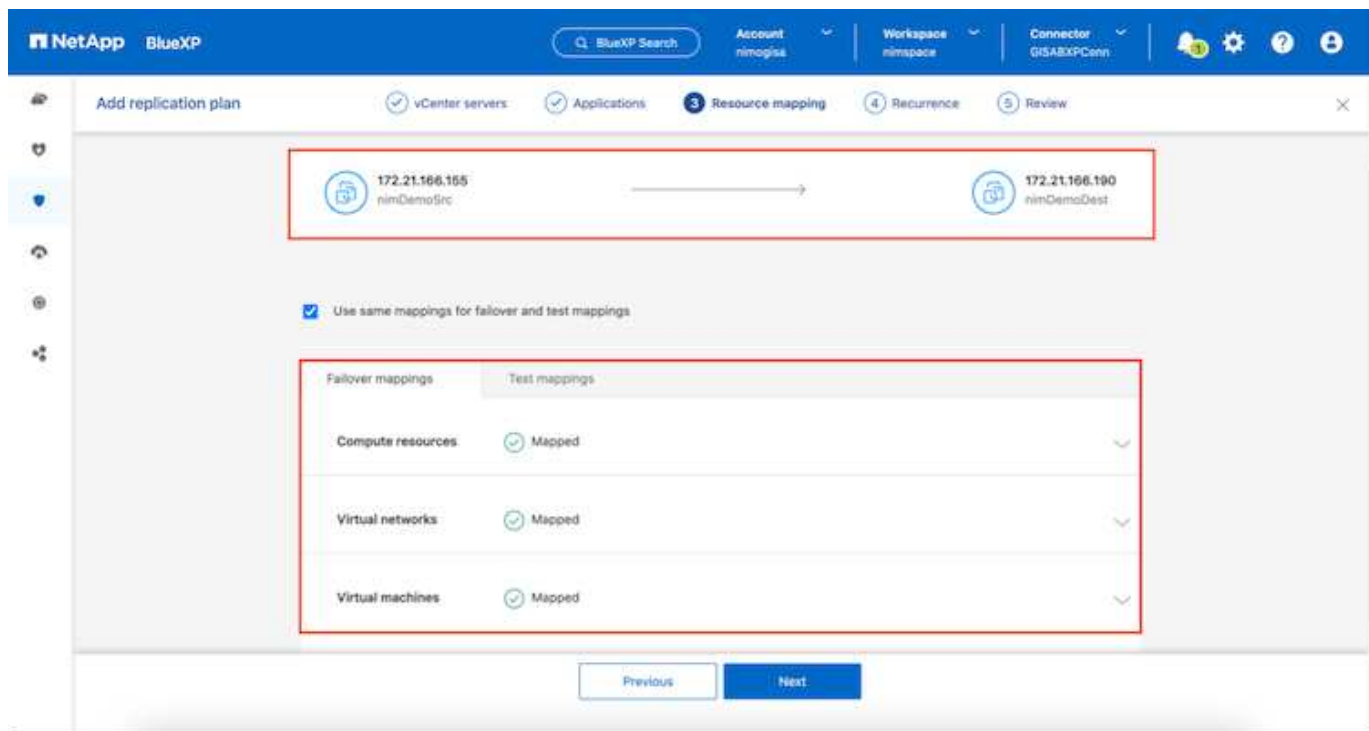
Specify how resources map from the source to the target.

172.21.166.155 → 172.21.166.190

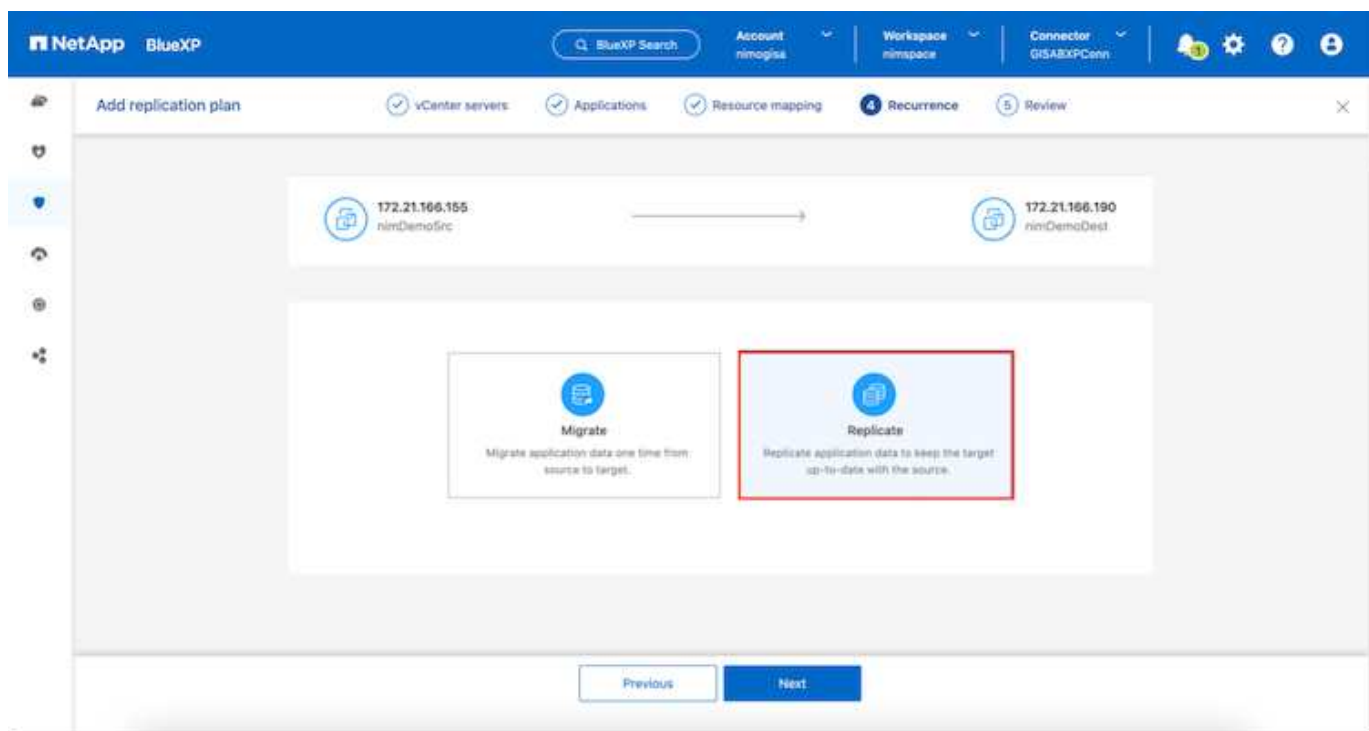
☒ Use same mappings for failover and test mappings

Failover mappings Test mappings

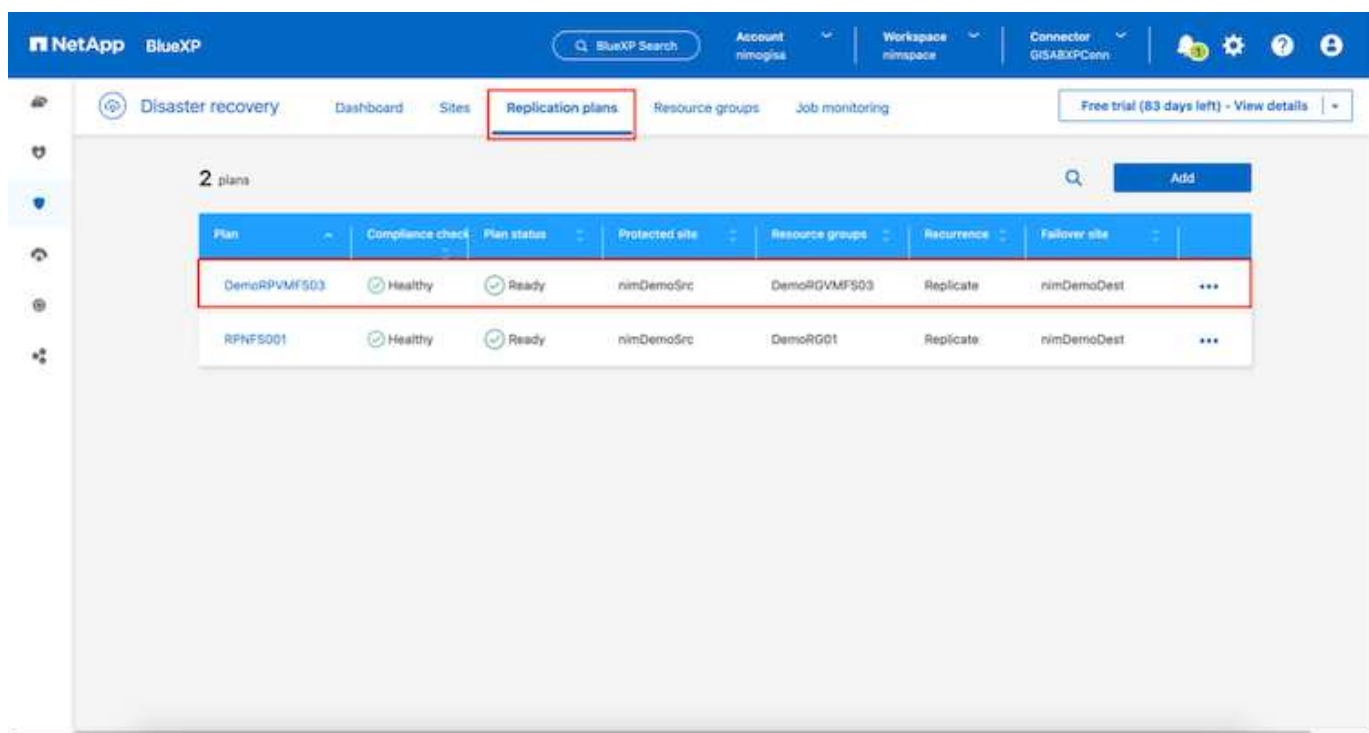
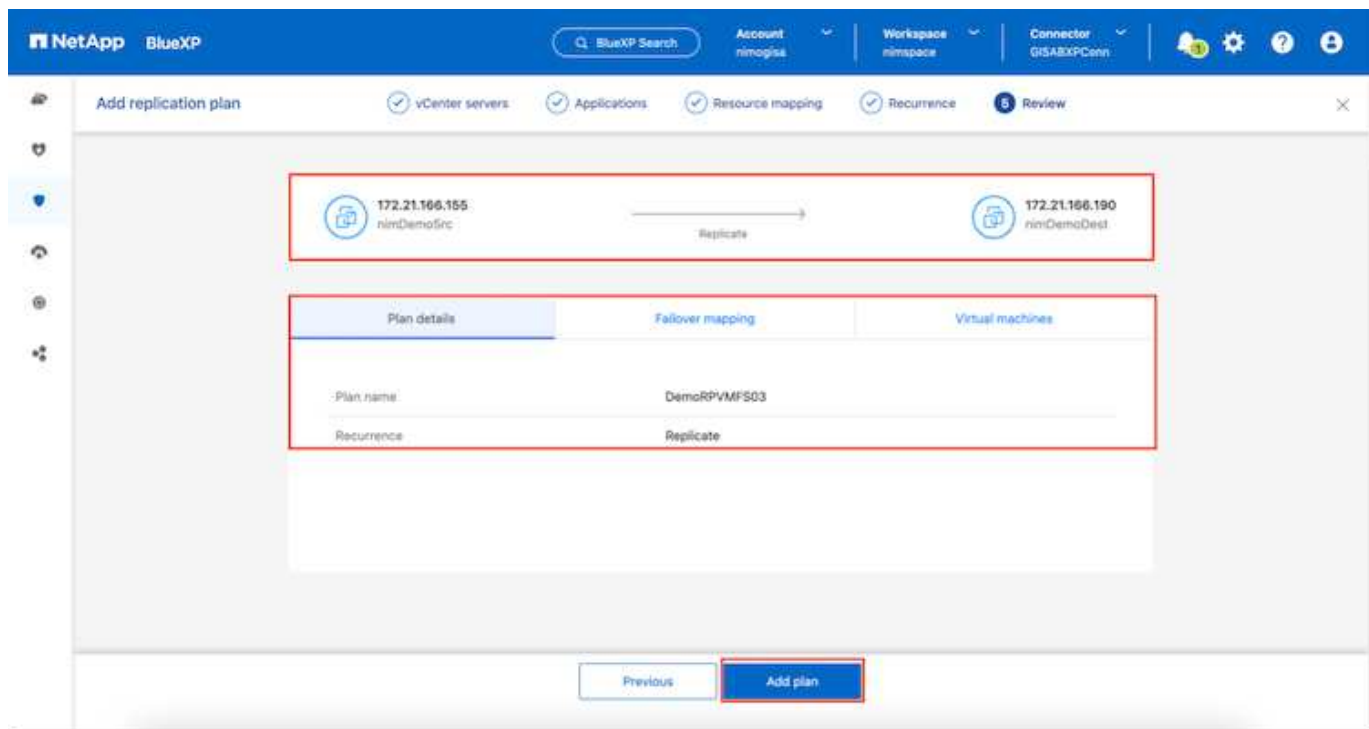
リソース マッピングが完了したら、[次へ] をクリックします。



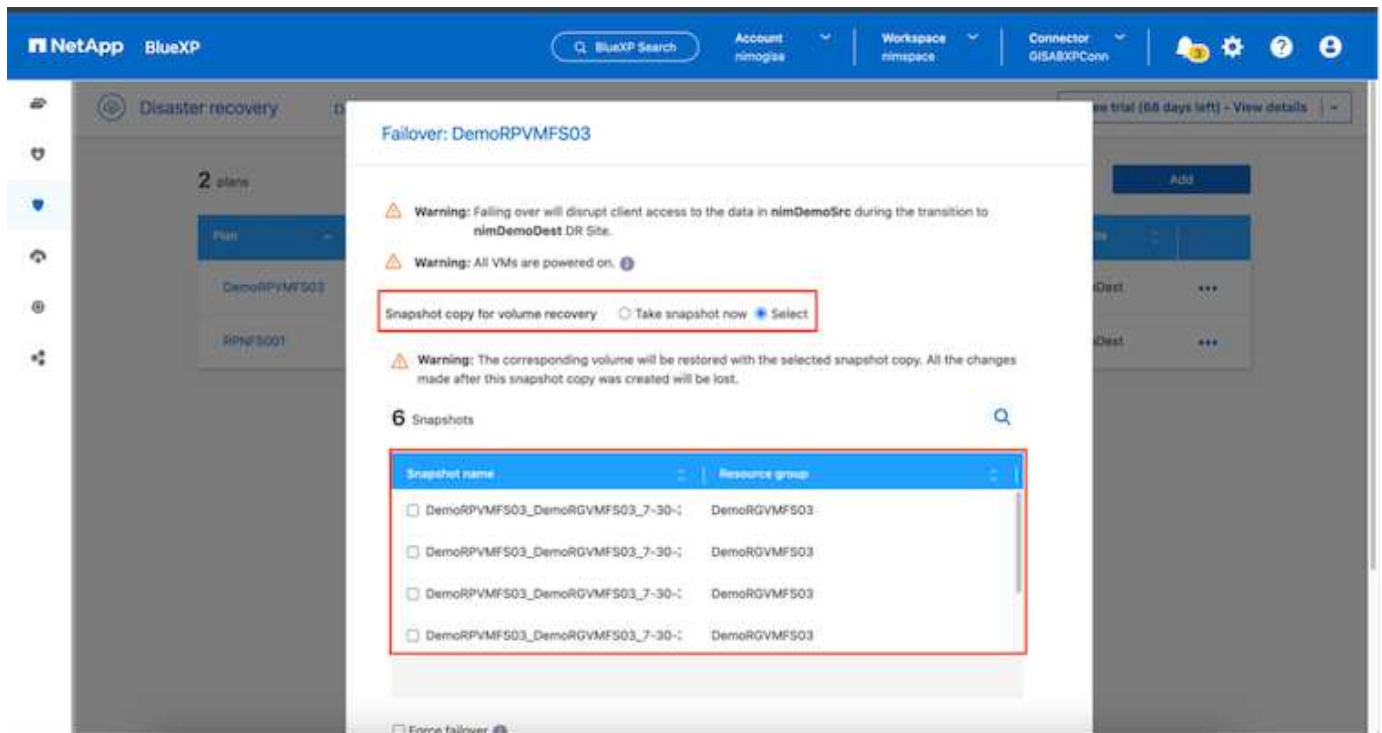
繰り返しタイプを選択します。簡単に言えば、「移行」（フェイルオーバーを使用した1回限りの移行）または定期的な連続レプリケーション オプションを選択します。このチュートリアルでは、「複製」オプションが選択されています。



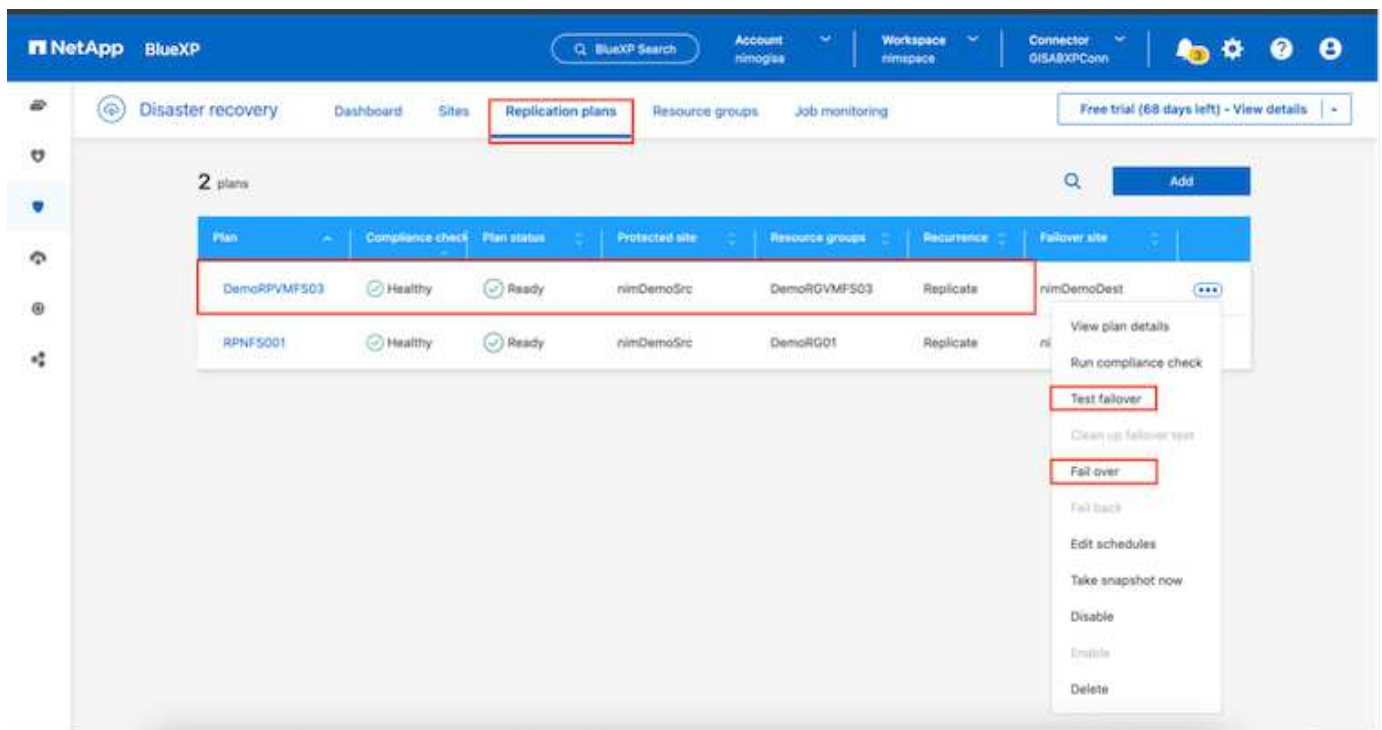
完了したら、作成されたマッピングを確認し、「プランの追加」をクリックします。



レプリケーションプランが作成されると、フェールオーバーオプション、テストフェールオーバーオプション、または移行オプションを選択して、要件に応じてフェールオーバーを実行できます。BlueXP disaster recoveryでは、レプリケーションプロセスが30分ごとに計画に従って実行されることが保証されます。フェールオーバーおよびテストフェールオーバーのオプションでは、最新のSnapMirror Snapshotコピーを使用することも、ポイントインタイム Snapshot コピーから特定の Snapshot コピーを選択することもできます (SnapMirrorの保持ポリシーに従って)。ランサムウェアなどの破損イベントが発生し、最新のレプリカがすでに侵害されたり暗号化されたりしている場合、ポイントインタイムオプションは非常に役立ちます。BlueXP disaster recoveryでは、利用可能なすべての復旧ポイントが表示されます。



レプリケーション プランで指定された構成でフェイルオーバーまたはテスト フェイルオーバーをトリガーするには、[フェイルオーバー] または [フェイルオーバーのテスト] をクリックします。



フェイルオーバーまたはテストフェイルオーバー操作中に何が起こりますか？

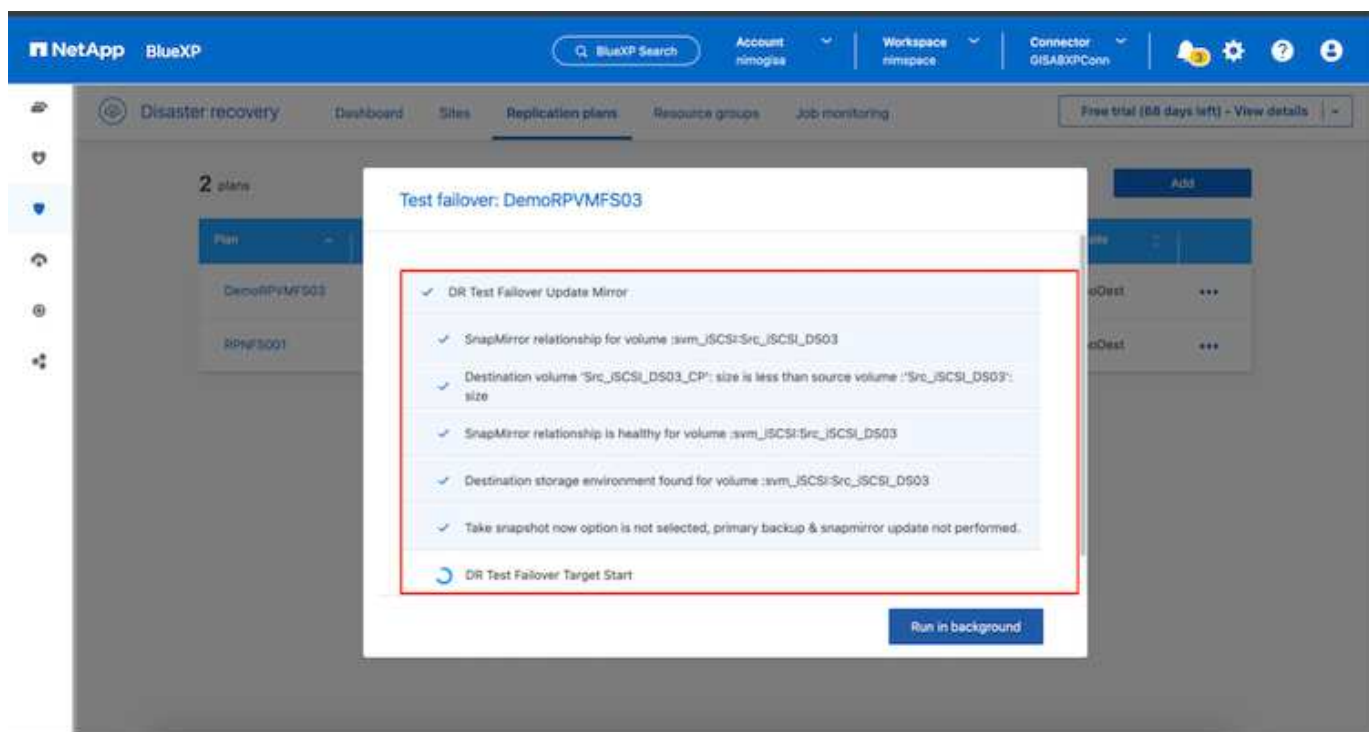
テスト フェイルオーバー操作中に、BlueXP disaster recoveryは、最新の Snapshot コピーまたは宛先ボリュームの選択されたスナップショットを使用して、宛先ONTAPストレージ システムにFlexCloneボリュームを作成します。



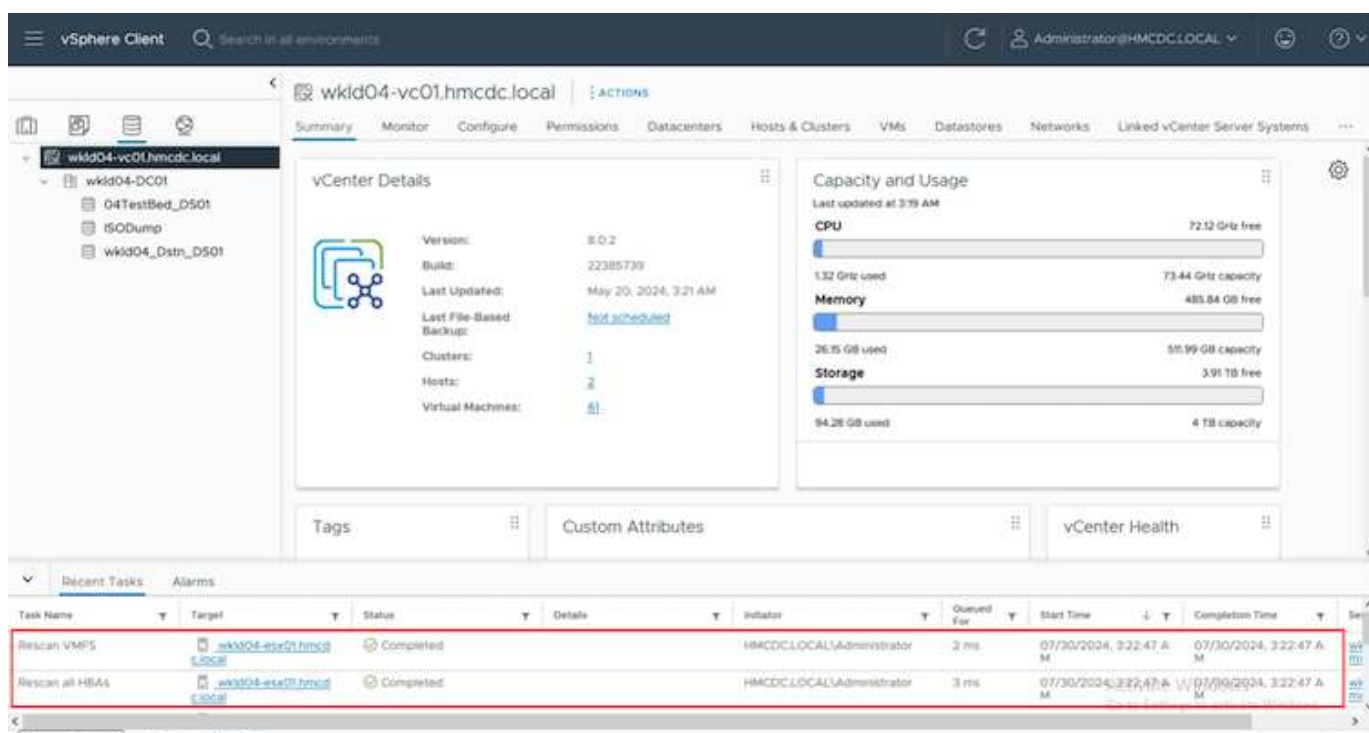
テスト フェイルオーバー操作では、宛先のONTAPストレージ システムにクローン ボリュームが作成されます。

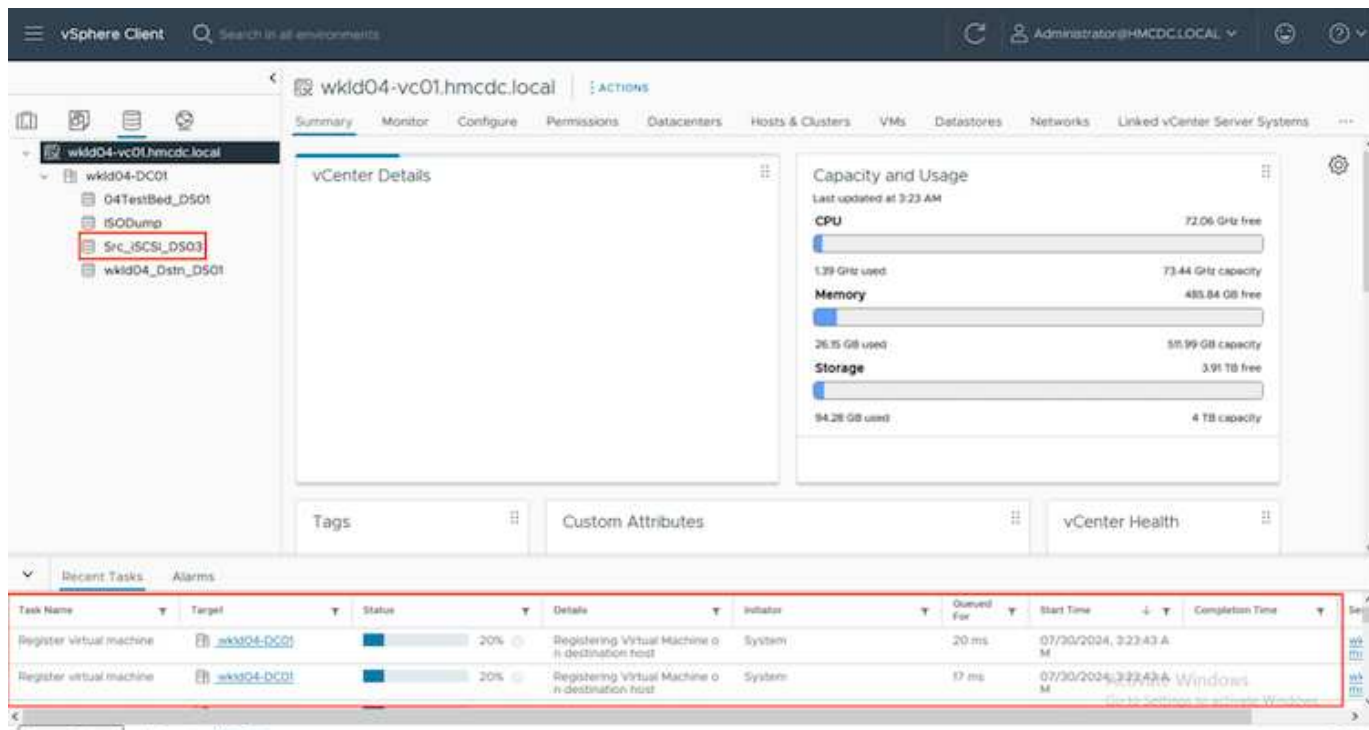


テスト リカバリ操作を実行しても、 SnapMirrorレプリケーションには影響しません。



プロセス中、 BlueXP disaster recoveryは元のターゲット ボリュームをマップしません。代わりに、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ボリュームをサポートする一時データストアが ESXi ホストにマップされます。

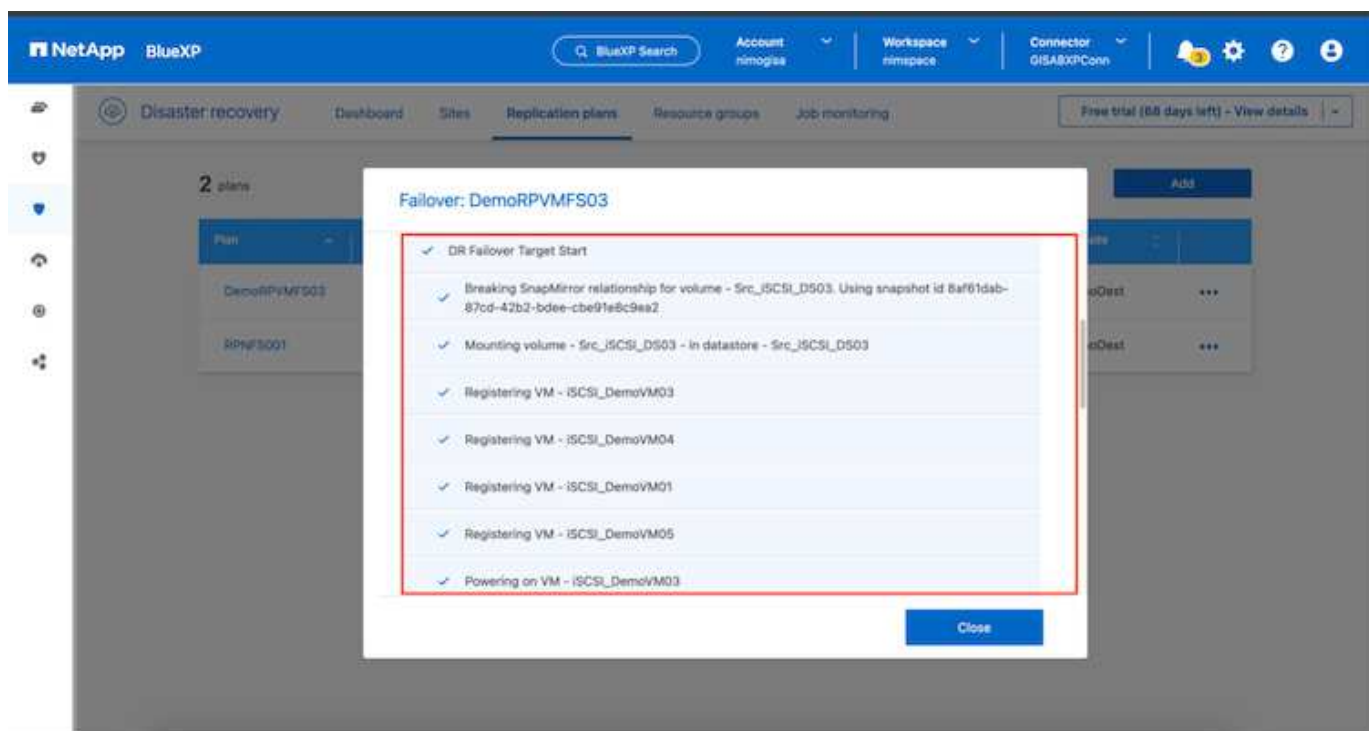




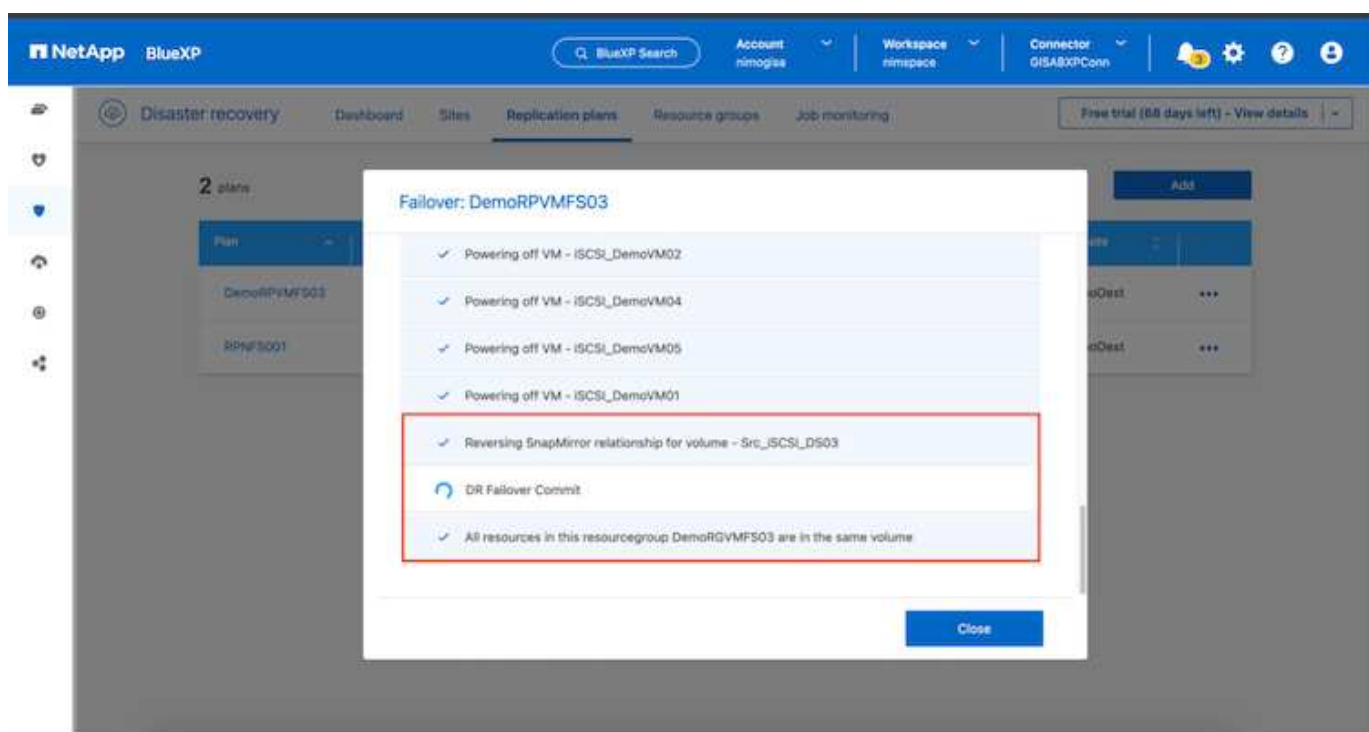
テスト フェイルオーバー操作が完了すると、「クリーンアップ フェイルオーバー テスト」を使用してクリーンアップ操作をトリガーできます。この操作中、BlueXP disaster recoveryは、操作で使用されたFlexCloneボリュームを破棄します。

実際の災害が発生した場合、BlueXP disaster recoveryは次の手順を実行します。

1. サイト間のSnapMirror関係を解除します。
2. 再署名後に VMFS データストア ボリュームをマウントし、すぐに使用できるようにします。
3. VMを登録する
4. VMの電源をオンにする

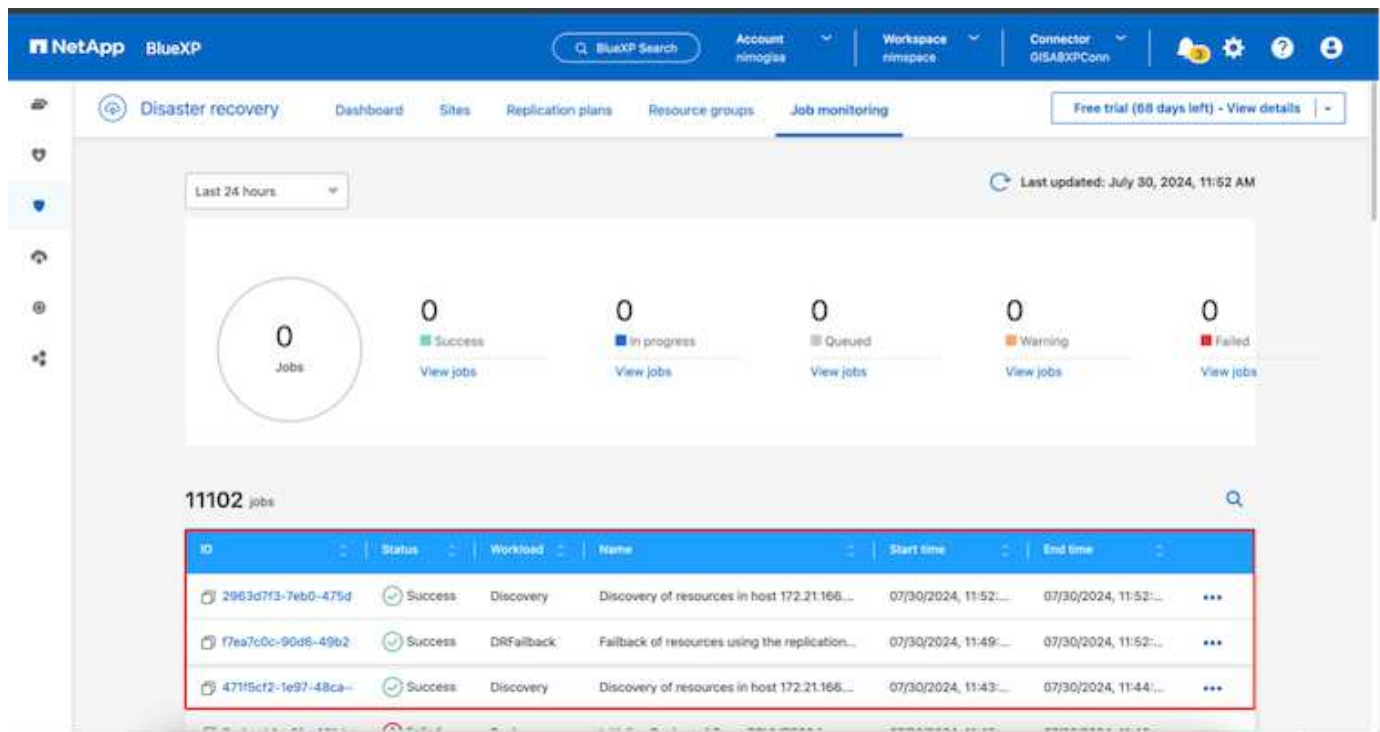


プライマリ サイトが起動すると、BlueXP disaster recoveryによってSnapMirrorの逆再同期が有効になり、フェイルバックが有効になります。これもボタンをクリックするだけで実行できます。



移行オプションを選択した場合は、計画されたフェイルオーバー イベントと見なされます。この場合、ソース サイトの仮想マシンをシャットダウンする追加の手順がトリガーされます。残りの手順はフェイルオーバー イベントと同じままです。

BlueXPまたはONTAP CLI から、適切なデータストア ボリュームのレプリケーションのヘルス ステータスを監視し、ジョブ監視を介してフェイルオーバーまたはテスト フェイルオーバーのステータスを追跡できます。



これにより、調整およびカスタマイズされた災害復旧計画を処理するための強力なソリューションが提供されます。フェイルオーバーは、計画されたフェイルオーバーとして実行することも、災害が発生して DR サイトをアクティブ化する決定が下されたときにボタンをクリックするだけでフェイルオーバーを実行することもできます。

このプロセスについて詳しく知りたい場合は、詳細なウォークスルービデオをご覧ください。 ["ソリューションシミュレータ"](#)。

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。