



TR-4955: FSx ONTAPと VMC を使用した災害復旧 (AWS VMware Cloud)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

目次

TR-4955: FSx ONTAPと VMC を使用した災害復旧 (AWS VMware Cloud)	1
概要	1
開始	1
VMware Cloud on AWS の導入と構成	2
FSx ONTAP のプロビジョニングと構成	2
SnapMirrorをFSx ONTAPに導入して設定する	2
DROのインストール	3
前提条件	3
OSの要件	3
パッケージをインストールする	3
DRO構成	4
リソースのグループ化	6
レプリケーションプラン	7
ランサムウェアからの回復	15
利点	15

TR-4955: FSx ONTAPと VMC を使用した災害復旧 (AWS VMware Cloud)

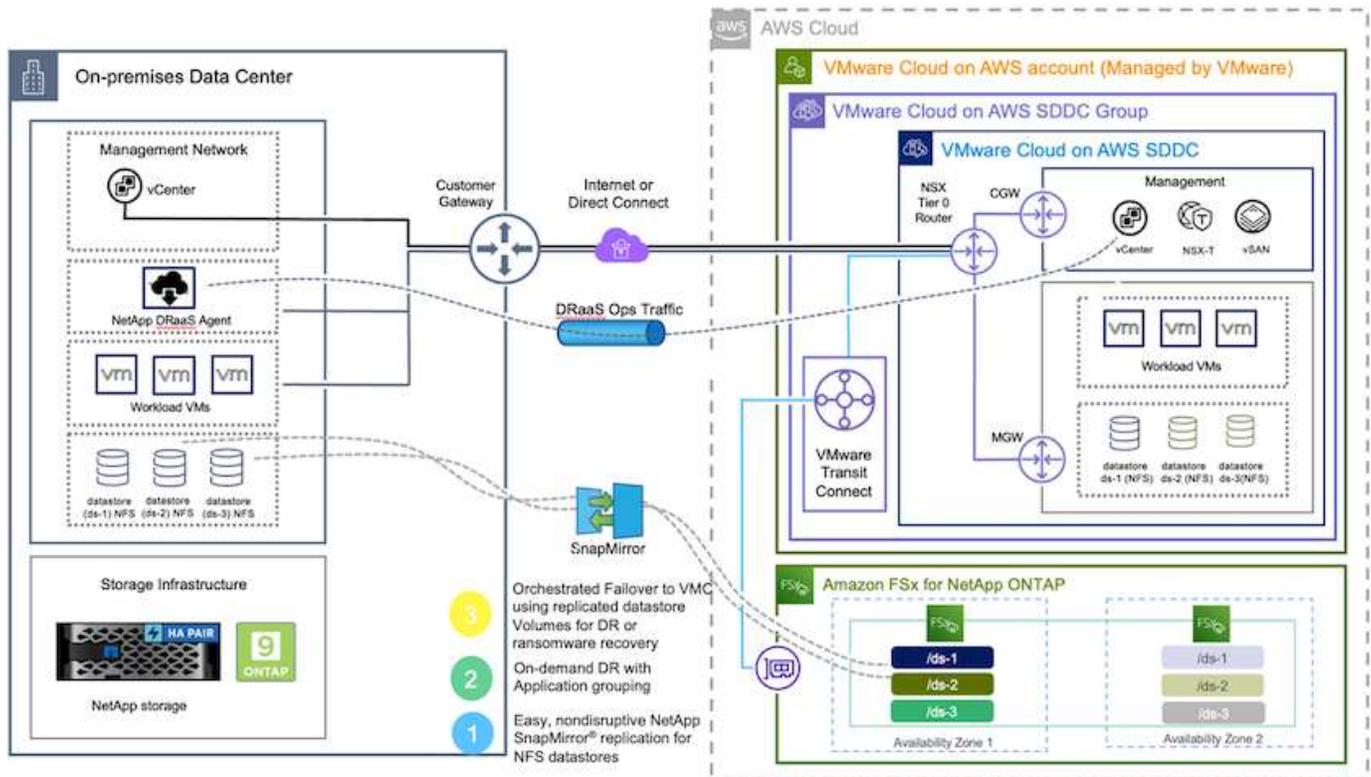
ディザスタ リカバリ オーケストレーター (DRO、UI 付きのスクリプト ソリューション) を使用すると、オンプレミスから FSx ONTAPに複製されたワークロードをシームレスにリカバリできます。DROは、 SnapMirrorレベルからVMCへのVM登録、そしてNSX-T上のネットワークマッピングまで、リカバリを自動化します。この機能はすべてのVMC環境に含まれています。

ニヤズ・モハメド、 NetApp

概要

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 (ランサムウェアなど) 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テクノロジーを使用すると、オンプレミスの VMware ワークロードを AWS で実行されている FSx ONTAPに複製できます。

ディザスタ リカバリ オーケストレーター (DRO、UI 付きのスクリプト ソリューション) を使用すると、オンプレミスから FSx ONTAPに複製されたワークロードをシームレスにリカバリできます。DROは、 SnapMirrorレベルからVMCへのVM登録、そしてNSX-T上のネットワークマッピングまで、リカバリを自動化します。この機能はすべてのVMC環境に含まれています。



開始

VMware Cloud on AWS の導入と構成

"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 VMC 環境を構成するには、次の手順に従ってください。"リンク"。パイロットライト クラスタは DR 目的にも使用できます。



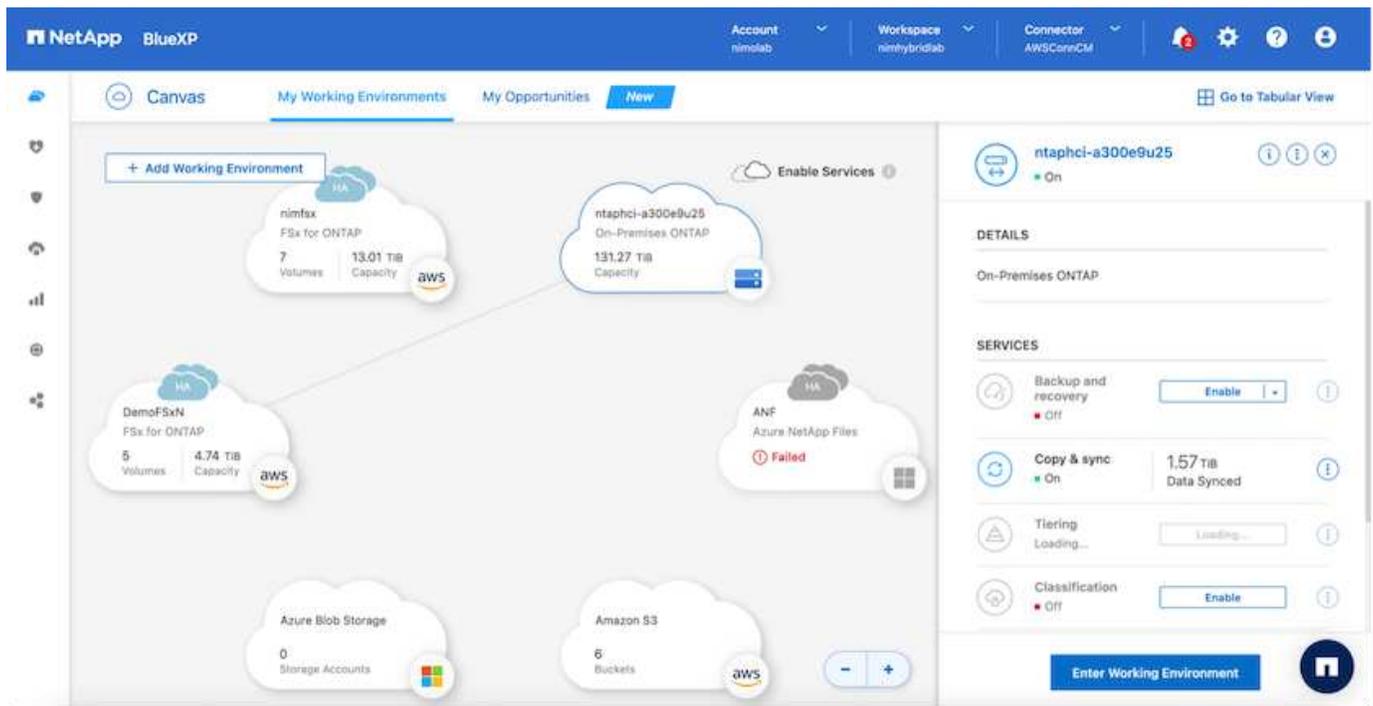
最初のリリースでは、DRO は既存のパイロットライト クラスタをサポートします。オンデマンド SDDC 作成は、今後のリリースで利用可能になります。

FSx ONTAP のプロビジョニングと構成

Amazon FSx ONTAP は、人気の 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。この手順に従ってください"リンク"FSx ONTAP をプロビジョニングおよび構成します。

SnapMirror を FSx ONTAP に導入して設定する

次のステップでは、NetApp BlueXP を使用して、AWS インスタンス上でプロビジョニングされた FSx ONTAP を検出し、適切な頻度と NetApp Snapshot コピー保持期間で、必要なデータストア ボリュームをオンプレミス環境から FSx ONTAP に複製します。



BlueXP を設定するには、このリンクの手順に従ってください。このリンクに従って、NetApp ONTAP CLI を使用してレプリケーションをスケジュールすることもできます。



SnapMirror 関係は前提条件であり、事前に作成する必要があります。

DROのインストール

DROを開始するには、指定された EC2 インスタンスまたは仮想マシンで Ubuntu オペレーティング システムを使用して、前提条件を満たしていることを確認します。次にパッケージをインストールします。

前提条件

- ソースおよびターゲットの vCenter およびストレージ システムへの接続が存在することを確認します。
- DNS 名を使用している場合は、DNS 解決を実施する必要があります。それ以外の場合は、vCenter およびストレージ システムに IP アドレスを使用する必要があります。
- ルート権限を持つユーザーを作成します。EC2 インスタンスで `sudo` を使用することもできます。

OSの要件

- Ubuntu 20.04 (LTS)、最低 2GB および 4 つの vCPU
- 指定されたエージェント VM に次のパッケージをインストールする必要があります。
 - Docker
 - Docker-compose
 - Jq

権限を変更する `docker.sock`: `sudo chmod 666 /var/run/docker.sock`。



その `deploy.sh` スクリプトは必要な前提条件をすべて実行します。

パッケージをインストールする

1. 指定された仮想マシンにインストール パッケージをダウンロードします。

```
git clone https://github.com/NetApp/DRO-AWS.git
```



エージェントはオンプレミスまたは AWS VPC 内にインストールできます。

2. パッケージを解凍し、デプロイメント スクリプトを実行して、ホスト IP (例: 10.10.10.10) を入力します。

```
tar xvf DRO-prereq.tar
```

3. ディレクトリに移動し、次のようにデプロイ スクリプトを実行します。

```
sudo sh deploy.sh
```

4. 次の方法で UI にアクセスします。

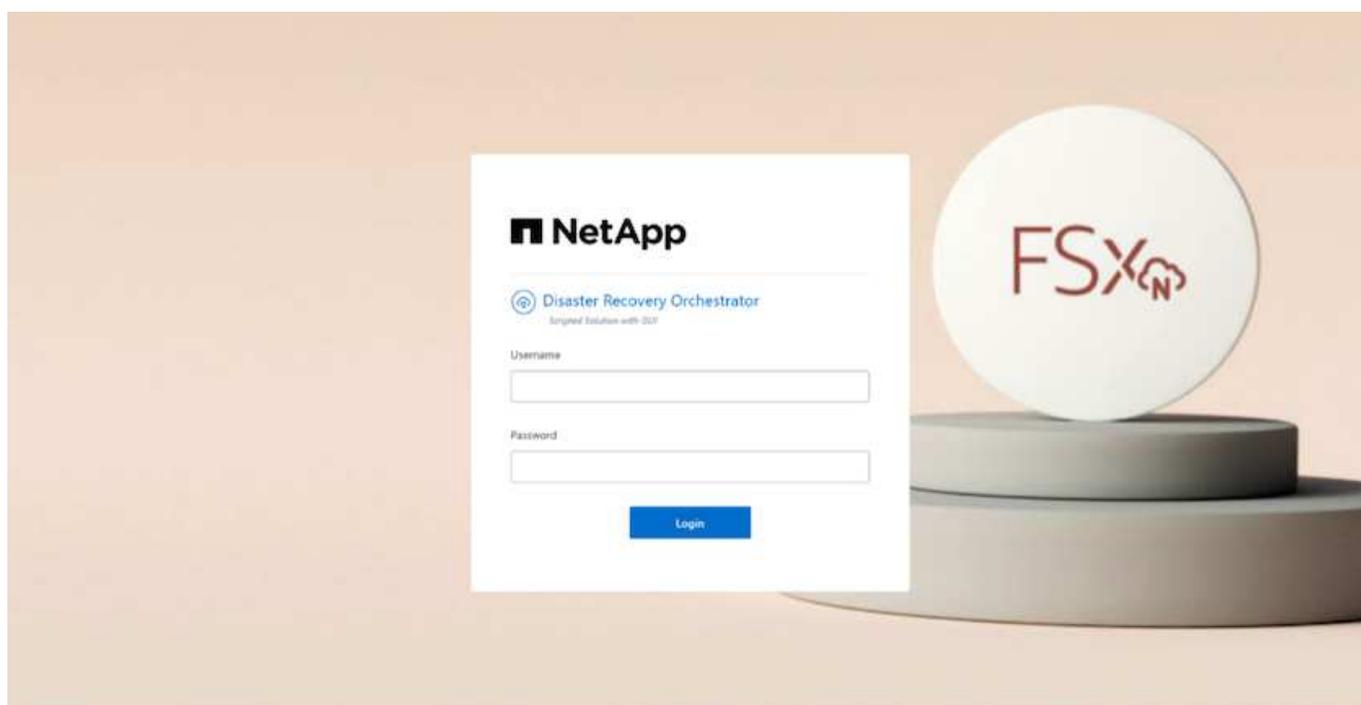
```
https://<host-ip-address>
```

次のデフォルトの資格情報を使用します。

```
Username: admin  
Password: admin
```



パスワードは「パスワードの変更」オプションを使用して変更できます。



DRO構成

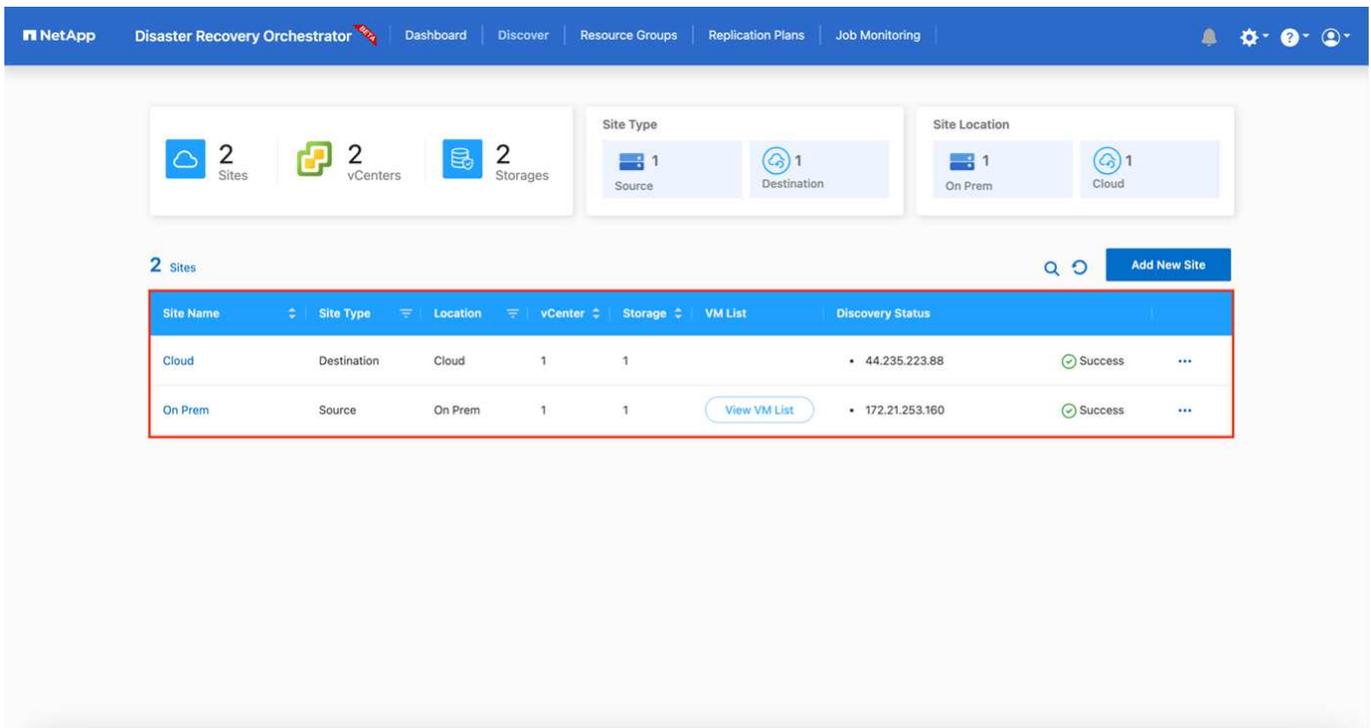
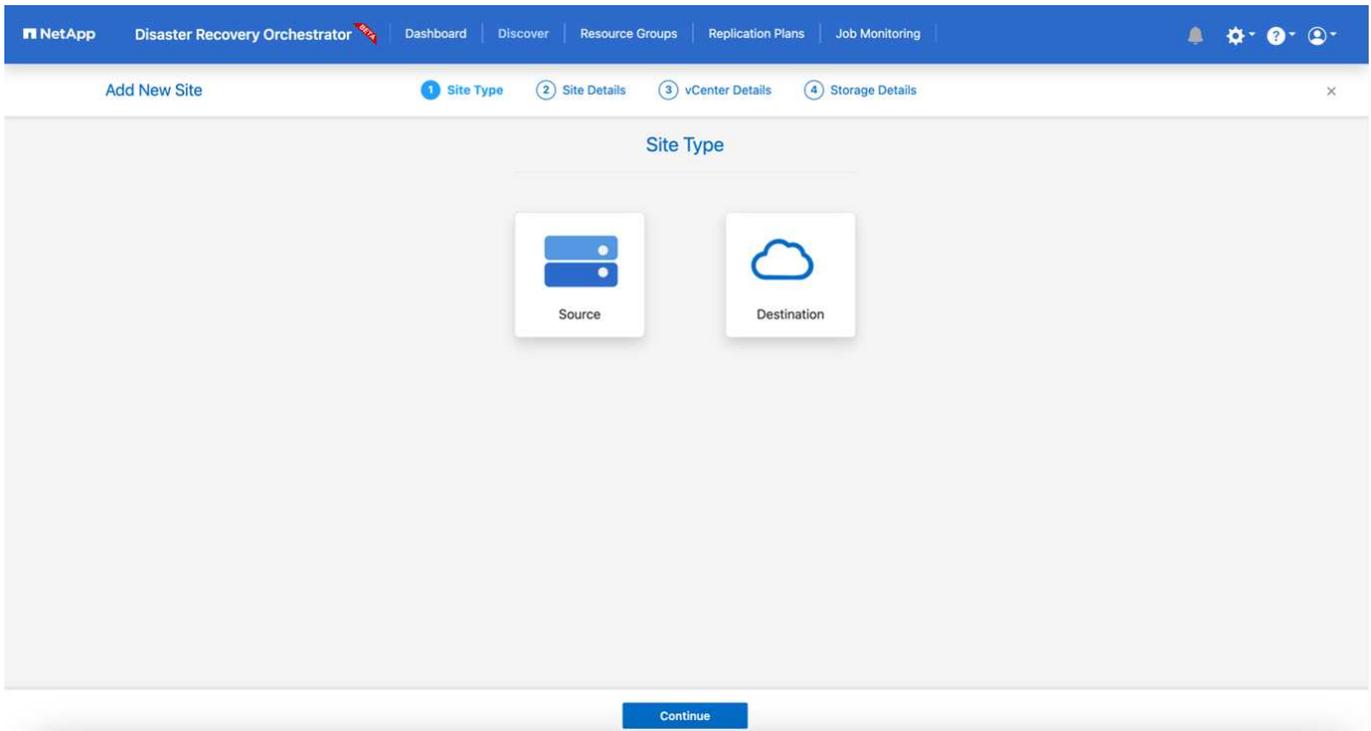
FSx ONTAPと VMC が適切に構成されたら、FSx ONTAP上の読み取り専用SnapMirrorコピーを使用してオンプレミスのワークロードを VMC に自動的にリカバリするように DRO の構成を開始できます。

NetApp、DRO エージェントがオンプレミスのコンポーネントだけでなく、FSx ONTAPや VMC リソースともネットワークを介して通信できるように、DRO エージェントを AWS に導入し、さらに FSx ONTAPが導入されているのと同じ VPC (ピア接続も可能) にも導入することを推奨しています。

最初のステップは、オンプレミスとクラウドのリソース (vCenter とストレージの両方) を検出して DRO に追加することです。サポートされているブラウザで DRO を開き、デフォルトのユーザー名とパスワード (admin/admin) を使用して、サイトを追加します。検出オプションを使用してサイトを追加することもできます。次のプラットフォームを追加します。

- オンプレミス
 - オンプレミスの vCenter

- ONTAPストレージシステム
- クラウド
 - VMC vCenter
 - FSx ONTAP



追加されると、DRO は自動検出を実行し、ソース ストレージから FSx ONTAPに対応するSnapMirrorレプリカを持つ VM を表示します。DRO は、VM で使用されるネットワークとポートグループを自動的に検出し、それらを入力します。

NetApp Disaster Recovery Orchestrator Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Back VM List Site: On Prem | vCenter: 172.21.253.160

10 Datastores | 219 Virtual Machines | VM Protection: 3 Protected, 216 Unprotected

38 VMs Create Resource Group

VM Name	VM Status	VM State (1)	DataStore	CPU	Memory (MB)
a300-vcsa02	Not Protected	Powered On	A300_NFS_DS04	16	65536
PFSense	Not Protected	Powered On	A300_NFS_DS04	4	8192
PFsense260	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimDC02	Not Protected	Powered On	A300_NFS_DS04	4	8192
jRBhoja-1B7	Not Protected	Powered On	A300_NFS_DS04	4	16384
jNimo-1B7	Not Protected	Powered On	A300_NFS_DS04	4	16384
NimMSdesktop	Not Protected	Powered On	A300_NFS_DS04	8	12288

次のステップは、必要な VM を機能グループにグループ化し、リソースグループとして機能するようにすることです。

リソースのグループ化

プラットフォームを追加したら、回復する VM をリソースグループにグループ化できます。DRO リソースグループを使用すると、依存する VM のセットを、ブート順序、ブート遅延、および回復時に実行できるオプションのアプリケーション検証を含む論理グループにグループ化できます。

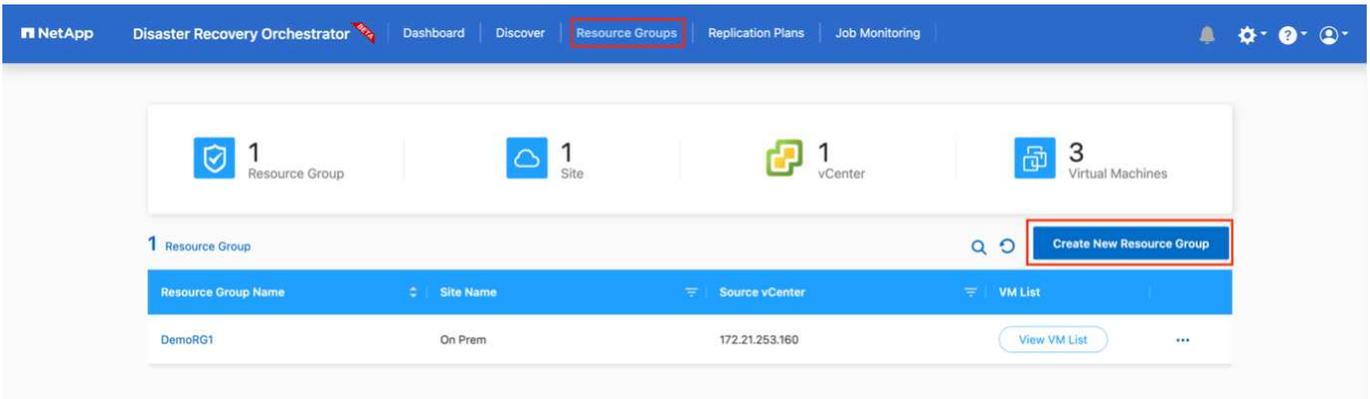
リソースグループの作成を開始するには、次の手順を実行します。

1. リソースグループにアクセスし、新しいリソースグループの作成をクリックします。
2. 新しいリソースグループの下で、ドロップダウンからソースサイトを選択し、作成をクリックします。
3. リソースグループの詳細を入力し、[続行]をクリックします。
4. 検索オプションを使用して適切な VM を選択します。
5. 選択した VM のブート順序とブート遅延 (秒) を選択します。各 VM を選択し、その優先順位を設定することで、電源オンシーケンスの順序を設定します。すべての VM のデフォルト値は 3 です。

オプションは次のとおりです。

1 – 最初にパワーオンする仮想マシン 3 – デフォルト 5 – 最後にパワーオンする仮想マシン

6. *リソースグループの作成*をクリックします。

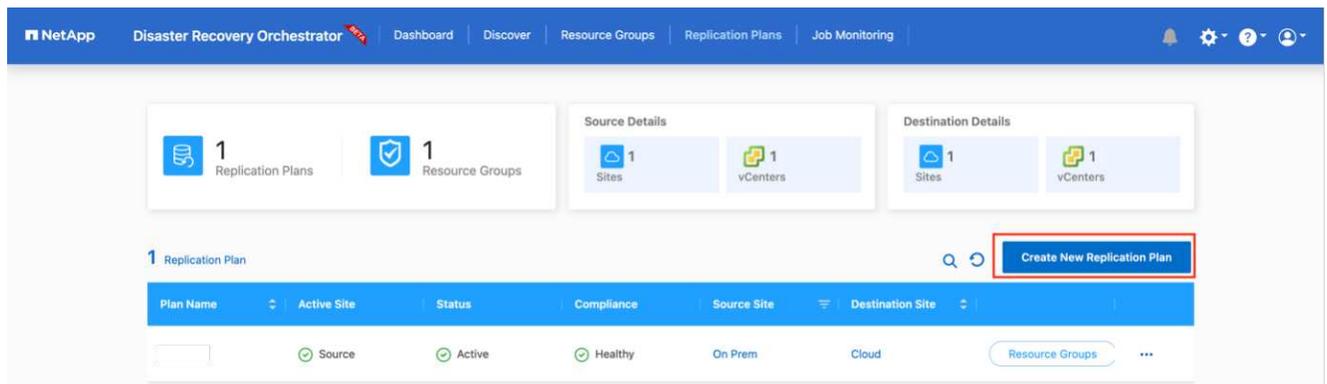


レプリケーションプラン

災害が発生した場合にアプリケーションを回復するための計画が必要です。ドロップダウンからソースとターゲットの vCenter プラットフォームを選択し、このプランに含めるリソースグループと、アプリケーションを復元してパワーオンする方法のグループ化 (たとえば、ドメインコントローラ、次に Tier 1、次に Tier 2 など) を選択します。このような計画は、青写真と呼ばれることもあります。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、[新しいレプリケーションプラン] をクリックします。

レプリケーションプランの作成を開始するには、次の手順を実行します。

1. *レプリケーションプラン*にアクセスし、*新しいレプリケーションプランの作成*をクリックします。



2. 新しいレプリケーションプランで、プランの名前を指定し、ソースサイト、関連付けられた vCenter、宛先サイト、および関連付けられた vCenter を選択して、リカバリマッピングを追加します。

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | **Replication Plans** | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

Replication Plan Details

Plan Name

Recovery Mapping

Source Site Destination Site

Source vCenter Destination vCenter

Pre-requisite - You must configure SnapMirror relationships between the source site and target site to create successful replication plan

[Continue](#)

3. リカバリ マッピングが完了したら、クラスター マッピングを選択します。

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | **Replication Plans** | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

Replication Plan Details

Plan Name

Recovery Mapping

Source Site Destination Site

Source vCenter Destination vCenter

Cluster Mapping

Source Site Resource Destination Site Resource [Add](#)

Source Resource	Destination Resource	
A300-Cluster01	Cluster-1	Delete

[Continue](#)

4. *リソース グループの詳細*を選択し、*続行*をクリックします。
5. リソース グループの実行順序を設定します。このオプションを使用すると、複数のリソース グループが存在する場合に操作のシーケンスを選択できます。
6. 完了したら、適切なセグメントへのネットワーク マッピングを選択します。セグメントはすでに VMC 内でプロビジョニングされているはずなので、適切なセグメントを選択して VM をマップします。
7. 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。



SnapMirrorはボリューム レベルで行われます。したがって、すべての VM がレプリケーション先にレプリケートされます。データストアの一部であるすべての VM を選択してください。選択されていない場合は、レプリケーション プランの一部である VM のみが処理されます。

NetApp Disaster Recovery Orchestrator Dashboard Discover Resource Groups Replication Plans Job Monitoring

Create New Replication Plan

Replication Plan and Site Details Select Resource Groups **3 Set Execution Order** 4 Set VM Details

Replication Plan Details

Select Execution Order

Resource Group Name	Execution Order
DemoRG1	3

Network Mapping

No more Source/Destination network resources available for mapping

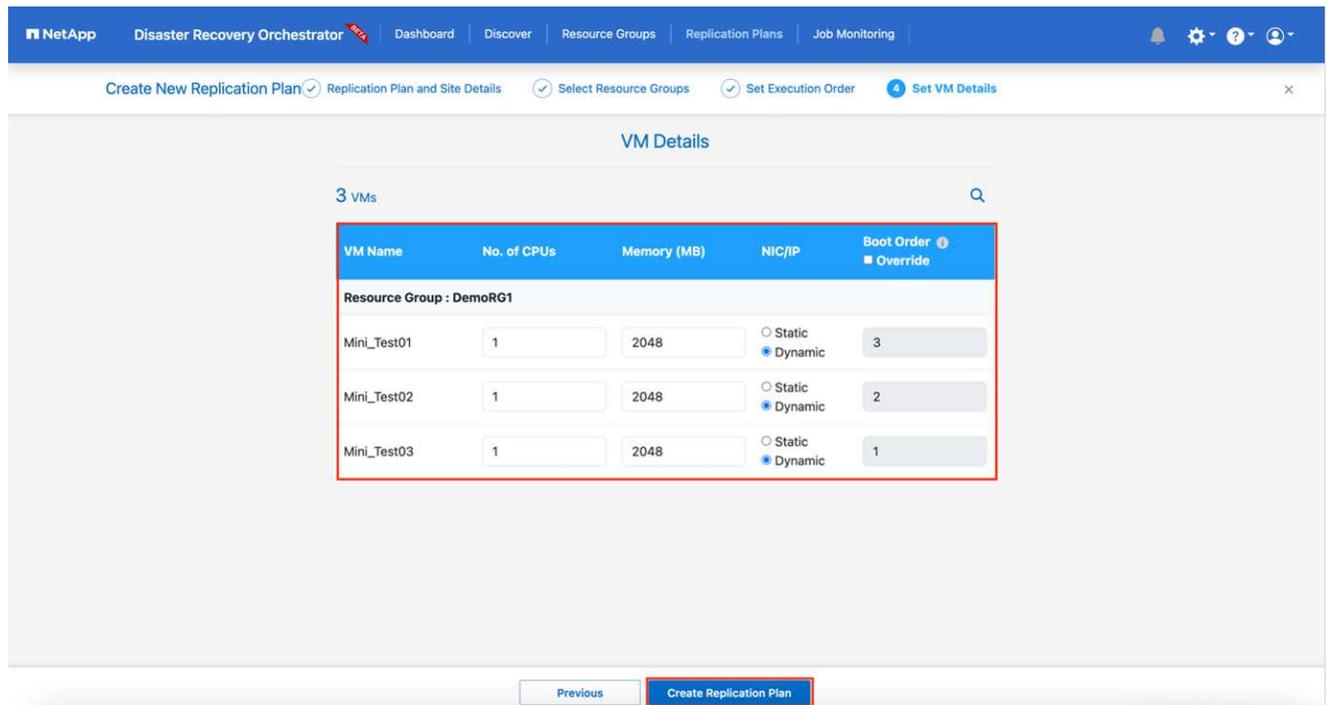
Source Resource	Destination Resource	
VLAN 3375	sddc-cgw-network-1	Delete

DataStore Mapping

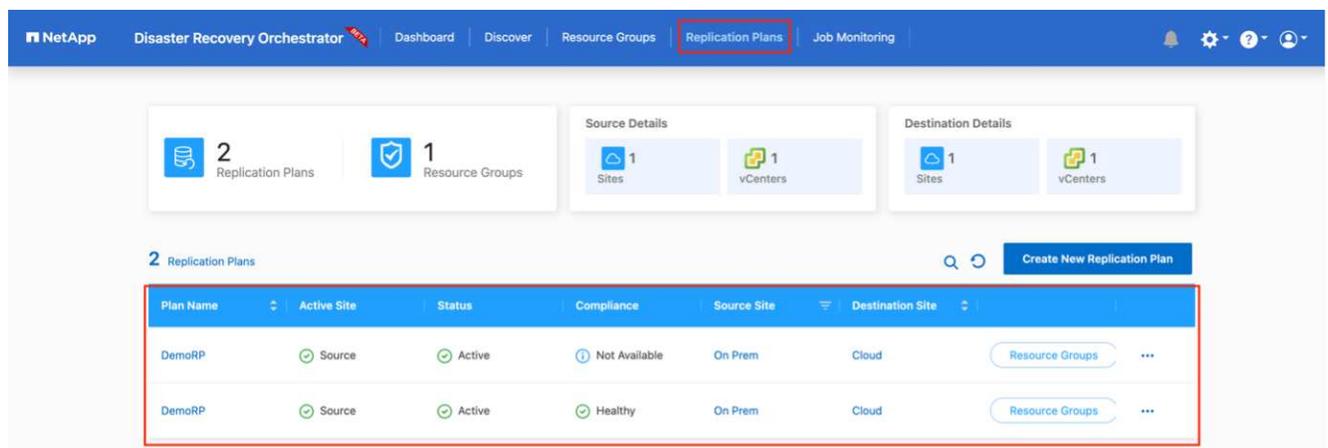
Source DataStore	Destination Volume
DRO_Mini	DRO_Mini_copy

Previous Continue

8. VM の詳細では、オプションで VM の CPU および RAM パラメータのサイズを変更できます。これは、大規模な環境を小規模なターゲット クラスターに回復する場合や、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 DR テストを実施する場合に非常に役立ちます。また、リソース グループ全体で選択したすべての VM のブート順序とブート遅延 (秒) を変更することもできます。リソース グループのブート順序の選択時に選択したものから変更が必要な場合、ブート順序を変更するための追加オプションがあります。デフォルトでは、リソース グループの選択時に選択されたブート順序が使用されますが、この段階で変更を実行することもできます。



9. *レプリケーションプランの作成*をクリックします。



レプリケーションプランが作成された後、要件に応じて、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実行できます。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中は、最新のSnapMirrorスナップショットコピーが使用されるか、または特定のスナップショットコピーをポイントインタイムスナップショットコピーから選択できます (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に直面していて、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は、ポイントインタイムオプションが非常に役立ちます。DROは利用可能なすべての時点を表示します。レプリケーションプランで指定された構成でフェールオーバーまたはテストフェールオーバーをトリガーするには、[フェールオーバー]または[フェールオーバーのテスト]をクリックします。

NetApp Disaster Recovery Orchestrator **NEW** Dashboard Discover Resource Groups Replication Plans Job Monitoring

2 Replication Plans 1 Resource Groups

Source Details: 1 Sites, 1 vCenters

Destination Details: 1 Sites, 1 vCenters

2 Replication Plans Create New Replication Plan

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource

- Plan Details
- Edit Plan
- Failover**
- Test Failover
- Migrate
- Run Compliance
- Delete Plan

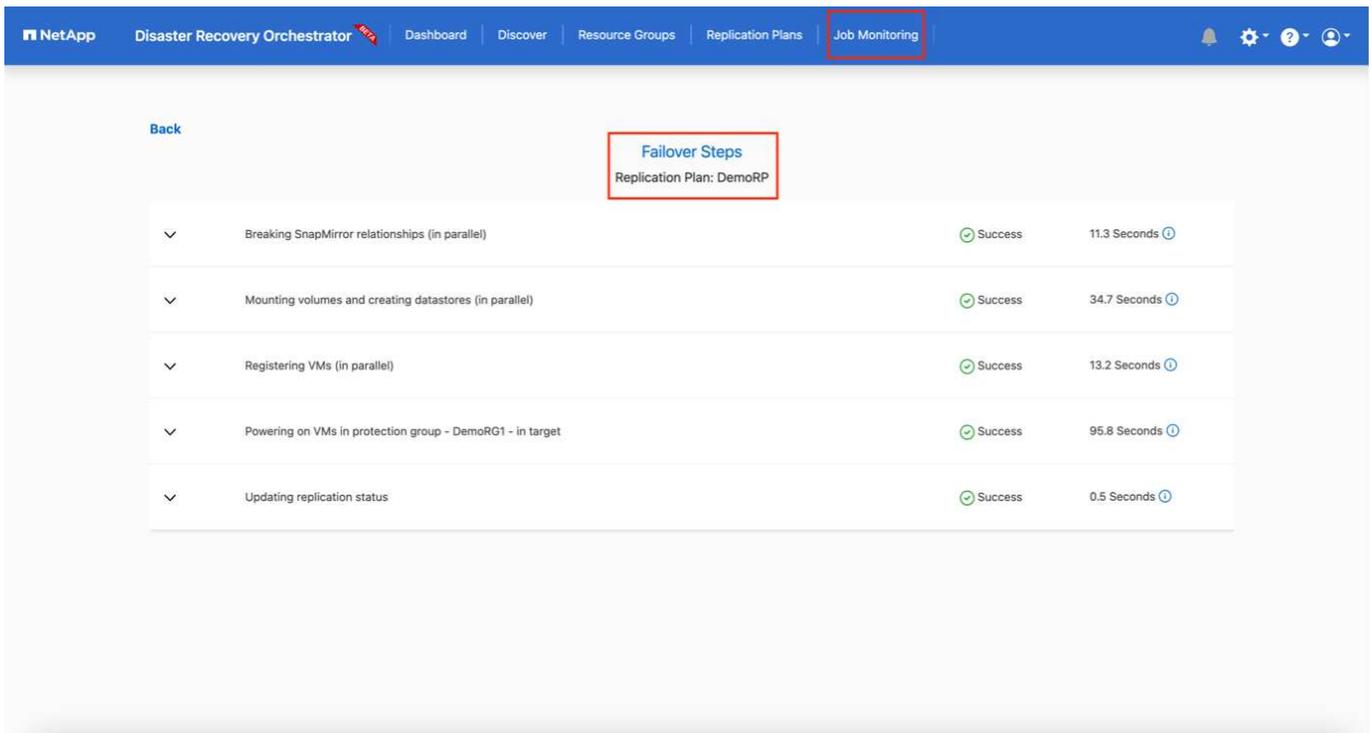
Failover Details

Volume Snapshot Details

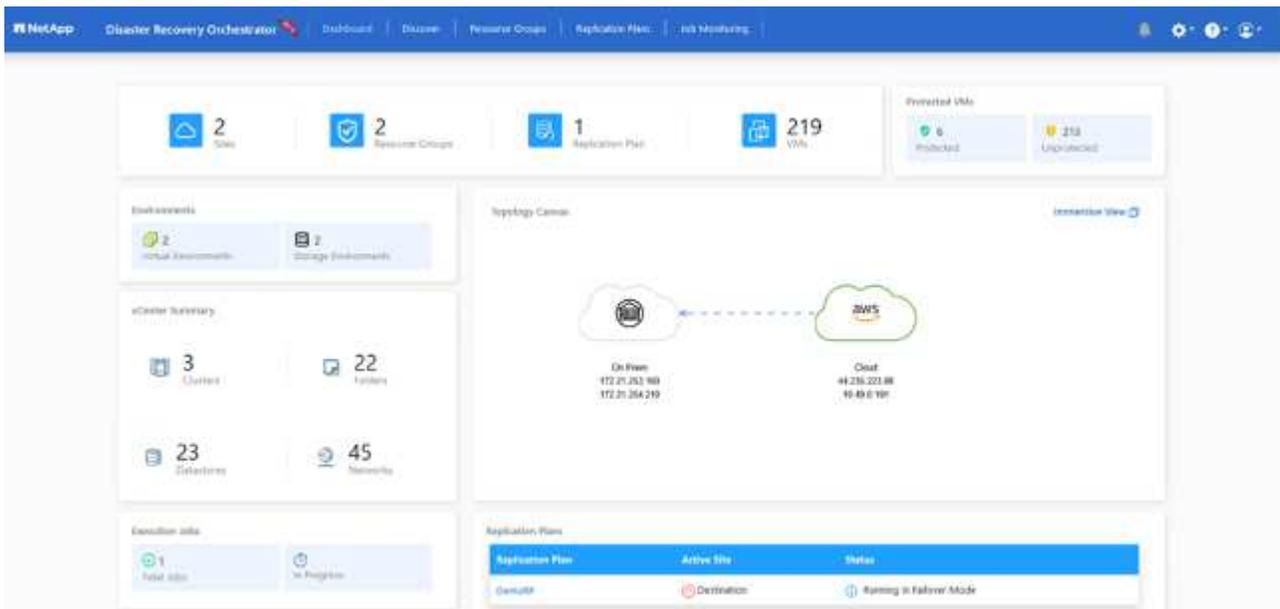
- Use latest snapshot ⓘ
- Select specific snapshot ⓘ

Start Failover

レプリケーション プランはタスク メニューで監視できます。



フェイルオーバーがトリガーされると、回復された項目が VMC vCenter (VM、ネットワーク、データストア) に表示されます。デフォルトでは、VM はワークロード フォルダーに回復されます。



フェイルバックはレプリケーション プラン レベルでトリガーできます。テストフェイルオーバーの場合、ティアダウン オプションを使用して変更をロールバックし、FlexClone関係を削除できます。フェイルオーバーに関連するフェイルバックは2段階のプロセスです。レプリケーション プランを選択し、逆データ同期を選択します。

NetApp Disaster Recovery Orchestrator **BETA** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

2 Replication Plans | 1 Resource Groups

Source Details: 1 Sites, 1 vCenters | Destination Details: 1 Sites, 1 vCenters

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Destination	Running In Failover h	Healthy	On Prem	Cloud	Resource Groups
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups

Plan Details: Reverse Data Sync, Failback

NetApp Disaster Recovery Orchestrator **BETA** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Back

Reverse Data Sync Steps

Replication Plan: DemoRP

Powering off VMs in protection group - DemoRG1 - in source	In progress	
Reversing SnapMirror relationships (in parallel)	Initialized	

完了したら、フェイルバックをトリガーして元の運用サイトに戻ることができます。

NetApp Disaster Recovery Orchestrator **BETA** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

2 Replication Plans | 1 Resource Groups

Source Details: 1 Sites, 1 vCenters | Destination Details: 1 Sites, 1 vCenters

2 Replication Plans

Plan Name	Active Site	Status	Compliance	Source Site	Destination Site	
DemoRP	Destination	Active	Healthy	On Prem	Cloud	Resource Groups
DemoRP	Source	Active	Healthy	On Prem	Cloud	Resource Groups

Plan Details: Failback

NetApp Disaster Recovery Orchestrator **BETA** | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

NetApp Disaster Recovery Orchestrator Dashboard

Failback Steps

Replication Plan: DemoRP

Powering off VMs in protection group - DemoRG1 - in target	In progress
Unregistering VMs in target (in parallel)	Initialized
Unmounting volumes in target (in parallel)	Initialized
Breaking reverse SnapMirror relationships (in parallel)	Initialized
Updating VM networks (in parallel)	Initialized
Powering on VMs in protection group - DemoRG1 - in source	Initialized
Deleting reverse SnapMirror relationships (in parallel)	Initialized
Resuming SnapMirror relationships to target (in parallel)	Initialized

NetApp BlueXPから、適切なボリューム（読み取り/書き込みボリュームとしてVMCにマップされたもの）のレプリケーションの正常性が失われていることがわかります。テストフェイルオーバー中、DROは宛先ボリュームまたはレプリカボリュームをマップしません。代わりに、必要なSnapMirror（またはSnapshot）インスタンスのFlexCloneコピーを作成し、FlexCloneインスタンスを公開します。これにより、FSx ONTAPの追加の物理容量が消費されることはありません。このプロセスにより、ボリュームが変更されず、DRテストまたはトリアージワークフロー中でもレプリカジョブが継続できるようになります。さらに、このプロセスにより、エラーが発生した場合や破損したデータが回復された場合に、レプリカが破壊されるリスクなしに回復をクリーンアップできるようになります。

NetApp Disaster Recovery Orchestrator Dashboard

2 Sites

1 Resource Group

2 Replication Plans

219 VMs

3 Protected

216 Unprotected

2 Virtual Environments

2 Storage Environments

3 Clusters

22 Folders

23 Datastores

45 Networks

Topology Canvas

Immersive View

3 Total Jobs

1 In Progress

Replication Plans

Replication Plan	Active Site	Status
DemoRP	Source	Active

ランサムウェアからの回復

ランサムウェアからの回復は困難な作業になる可能性があります。具体的には、IT 組織にとって、安全な復帰ポイントがどこにあるかを正確に特定することは困難であり、また、それが特定された後、たとえば休眠中のマルウェアや脆弱なアプリケーションによる再発する攻撃から回復したワークロードを保護することも困難です。

DRO は、利用可能な任意の時点からシステムを回復できるようにすることで、これらの懸念に対処します。また、アプリケーションが南北トラフィックにさらされていない場所でも機能し、相互に通信できるように、ワークロードを機能しながらも分離されたネットワークにリカバリすることもできます。これにより、セキュリティ チームは安全な場所でフォレンジックを実施し、隠れたマルウェアや潜伏中のマルウェアがないことを確認できます。

利点

- 効率的で回復力のある SnapMirror レプリケーションの使用。
- スナップショット コピーの保持により、利用可能な任意の時点にリカバリできます。
- ストレージ、コンピューティング、ネットワーク、アプリケーションの検証手順から数百から数千の VM を回復するために必要なすべての手順を完全に自動化します。
- 複製されたボリュームを変更しない方法を使用した、ONTAP FlexClone テクノロジーによるワークロードのリカバリ。
 - ボリュームまたはスナップショット コピーのデータ破損のリスクを回避します。
 - DR テスト ワークフロー中のレプリケーションの中断を回避します。
 - DevTest、セキュリティ テスト、パッチまたはアップグレード テスト、修復テストなど、DR 以外のワークフローにクラウド コンピューティング リソースで DR データを使用する可能性。
- CPU と RAM の最適化により、より小規模なコンピューティング クラスターへのリカバリが可能になり、クラウド コストが削減されます。

著作権に関する情報

Copyright © 2025 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。