Amazon EVS でNetApp Disaster Recoveryを使用する

NetApp Disaster Recovery

NetApp
February 04, 2026

目次

Amazon EVS でNetApp Disaster Recoveryを使用する

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

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

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

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

Amazon EVS にはストレージリソースが付属していますが、ネイティブストレージを使用すると、ストレージ負荷の高いワークロードを持つ組織ではその有効性が低下する可能性があります。このような場合、Amazon EVS とAmazon FSx for NetApp ONTAPストレージ (Amazon FSxN) を組み合わせると、より柔軟なストレージソリューションを提供できます。さらに、オンプレミスのNetApp ONTAPストレージソリューションを使用して VMware インフラストラクチャをホストしている場合、FSx for ONTAPを備えた Amazon EVS を使用すると、オンプレミスとクラウドでホストされるインフラストラクチャ間でクラス最高のデータ相互運用性と保護機能が得られます。

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

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

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

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

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

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

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

1. Amazon EVS は、単一のアベイラビリティーゾーン (AZ) 構成でアカウントにデプロイされ、仮想プライベートクラウド (VPC) 内にもデプロイされます。
2. FSx for ONTAPファイルシステムは、Amazon EVS デプロイメントと同じ AZ にデプロイされます。ファイルシステムは、Elastic Network Interface (ENI)、VPC ピア接続、または AmazonTransit Gateway を介して Amazon EVS に直接接続します。
3. NetApp Consoleエージェントが VPC にインストールされます。 NetApp Consoleエージェントは、ローカルの物理データセンターと Amazon AWS がホストするリソースの両方で VMware インフラストラクチャの DR を管理するNetApp Disaster Recoveryエージェントを含む、複数のデータ管理サービス (エージェントと呼ばれる) をホストします。
4. NetApp Disaster Recoveryエージェントは、 NetApp Consoleクラウド ホスト サービスと安全に通信してタスクを受信し、それらのタスクを適切なオンプレミスおよび AWS ホストの vCenter およびONTAPストレージ インスタンスに配布します。
5. NetApp Consoleのクラウド ホスト UI コンソールを使用してレプリケーション プランを作成し、保護する必要がある VM、それらの VM を保護する頻度、オンプレミス サイトからのフェイルオーバーが発生した場合にそれらの VM を再起動するために実行する必要がある手順を指定します。
6. レプリケーション プランは、保護された VM をホストしている vCenter データストアと、それらのデータストアをホストしているONTAPボリュームを決定します。 FSx for ONTAPクラスターにボリュームがまだ存在しない場合は、 NetApp Disaster Recoveryによって自動的に作成されます。
7. 識別されたソースONTAPボリュームごとに、各宛先 FSx for ONTAPがホストするONTAPボリュームへのSnapMirror関係が作成され、レプリケーション プランでユーザーが指定した RPO に基づいてレプリケーション スケジュールが作成されます。
8. プライマリ サイトに障害が発生した場合、管理者はNetApp Console内で手動のフェイルオーバー プロセスを開始し、復元ポイントとして使用するバックアップを選択します。
9. NetApp Disaster Recoveryエージェントは、FSx for ONTAPでホストされるデータ保護ボリュームをアクティブ化します。
10. エージェントは、アクティブ化された各 FSx for ONTAPボリュームを Amazon EVS vCenter に登録し、保護された各 VM を Amazon EVS vCenter に登録し、レプリケーション プランに含まれる定義済みルールに従って各 VM を起動します。

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

NetApp Console エージェントを使用すると、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。

   [システムを追加]

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。

   [システムイメージを追加する]

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

   [システムイメージを追加する]

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

   [システムイメージを追加する]

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。

   [システムイメージを追加する]

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。

   [システムイメージを追加する]

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

   [システムイメージを追加する]

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。

[システムイメージを追加する]

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

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

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

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

ライセンス タイプ

ライセンスには主に 2 つの種類があります。

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

災害復旧能力のニーズを予測する

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

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

手順

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

例えば：

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

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

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

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

以下を作成する必要があります。

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

オンプレミスサイトを作成する

本番環境の vCenter サイトを作成します。

手順

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

   [サイトオプション]

3. [サイト] オプションから [追加] を選択します。

   [サイトオプションの追加オプション]

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。

   [サイト作成ダイアログボックス]

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。

   [サイトオプション]

2. [サイト] オプションから [追加] を選択します。

   [サイトページのオプションの追加]

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。

   [ダイアログボックスの追加]

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。

   [vCenterオプションの追加]

2. [vCenter サーバーの追加] ダイアログ ボックスで、次の情報を選択または入力します。
   a. AWS VPC 内でホストされるNetApp Consoleエージェント。
   b. 追加する vCenter の IP アドレスまたは FQDN。
   c. 異なる場合は、ポート値を vCenter クラスタ マネージャが使用する TCP ポートに変更します。

d. 以前に作成したアカウントの vCenter ユーザー名。NetApp NetApp Disaster Recoveryが vCenter を管理するために使用します。

e. 指定されたユーザー名の vCenter パスワード。

f. 会社が外部の証明機関 (CA) または vCenter エンドポイント証明書ストアを使用して vCenter にアクセスする場合は、[自己署名証明書を使用する] チェックボックスをオフにします。それ以外の場合は、ボックスをオンのままにしておきます。

3. *追加*を選択します。

[vCenter の追加ダイアログボックス]

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。

[レプリケーションプランオプション]

2. レプリケーション プラン ページで、[追加] を選択します。

[レプリケーションプラン画面]

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。

[レプリケーションプランを作成し、vCentersを選択します]

続ける"レプリケーションプラン作成ウィザード ステップ 2"。

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

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

保護する VM を選択する方法はいくつかあります。

- 個々の **VM** を選択: 仮想マシン ボタンをクリックすると、保護する個々の VM を選択できます。各 VM を選択すると、サービスによって画面の右側にあるデフォルトのリソース グループに追加されます。
- 以前に作成したリソース グループを選択: NetApp Disaster Recoveryメニューの [リソース グループ] オプションを使用して、事前にカスタム リソース グループを作成できます。他の 2 つの方法を使用して、レプリケーション プラン プロセスの一部としてリソース グループを作成できるため、これは必須ではありません。詳細については、 "レプリケーションプランを作成する" 。
- **vCenter** データストア全体を選択: このレプリケーション プランで保護する VM が多数ある場合は、個々の VM を選択するのが効率的ではない可能性があります。 NetApp Disaster Recoveryボリュームベースのsnapmirrorレプリケーションを使用して VM を保護するため、データストアに存在するすべての VM がボリュームの一部として複製されます。ほとんどの場合、 NetApp Disaster Recovery を使用して、データストアにあるすべての VM を保護し、再起動する必要があります。このオプションを使用して、選択したデータストアでホストされているすべての VM を保護された VM のリストに追加するようにサービスに指示します。

このガイド付きの手順では、vCenter データストア全体を選択します。

このページにアクセスする手順

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

[レプリケーションプラン、アプリケーションページ]

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（[25.25]) 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（[25.25]) 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。

   [レプリケーションプランの作成、リソースマッピングページ]

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。

   [レプリケーションプランの作成、リソースの計算]

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。

[レプリケーションプラン、ネットワークリソースの作成]

フェイルオーバー中の**VM**再構成のオプションを定義する

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

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

ネットワークの再構成

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

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

サブネットを構成すると、サブネット マッピングでは、ソース VM 構成と宛先 VM 構成の両方に IP アドレスの同じユニット コンポーネントが使用されますが、提供された CIDR 情報に基づいて IP アドレスのサブネット コンポーネントが置き換えられます。この機能を使用するには、送信元と宛先の仮想ネットワークの両方が同じIPアドレスクラス（ `/xx` CIDR のコンポーネント)。これにより、保護されたすべての VM をホストするのに十分な IP アドレスが宛先サイトで使用可能になります。

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

ネットワーク設定の再構成を変更する

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

[レプリケーションプラン、ネットワークリソースの作成]

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。

   [レプリケーションプラン、VMリソースの作成]

起動順序

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

起動順序設定を変更する

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

   [レプリケーションプラン、ブート順序の作成]

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。

[レプリケーションプランの作成、カスタムゲストOS操作]

マップデータストア

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

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

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

データストア（ボリューム）マッピングを構成するには

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

   [レプリケーションプラン、データストアマッピングの作成]

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[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[レプリケーションプランページ]

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

レプリケーション プラン ページでは、次の情報を確認できます。

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

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

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

フェイルオーバー

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

フェイルオーバーは手動で開始されるプロセスです。

フェイルオーバー操作にアクセスする手順

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

フェイルオーバーを実行する手順

1. レプリケーションプランページで、レプリケーションプランのアクションオプションを選択します。[アクションメニューの水平ドット] 。
2. *フェイルオーバー*を選択します。

   [フェイルオーバーメニューオプション]

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。

   [フェイルオーバーダイアログボックス]

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[アクションメニューの水平ドット]。
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。

   [テストフェイルオーバーメニューオプション]

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。

   [テストフェイルオーバーダイアログボックス]

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[NetApp Disaster Recoveryサービスのアクション メニュー アイコン]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。

   [コンプライアンスチェックの実行メニューオプション]

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

リソースを更新する

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

更新が必要となるケースは 2 つあります。

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

[リソースメニューオプションの更新] | *evs-rp-menu-refresh-resources.png*

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[NetApp Disaster Recoveryサービスのアクション メニュー アイコン]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。

   [移行メニューオプション] | *evs-rp-menu-migrate.png*

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[NetApp Disaster Recoveryサービスのアクション メニュー アイコン]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。

   [今すぐスナップショットを撮るメニューオプション] | *evs-rp-menu-take-snapshot-now.png*

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。

   [無効化/有効化メニューオプション] | *evs-rp-menu-disable-enable.png*

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[NetApp Disaster Recoveryサービスのアクション メニュー アイコン]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。

   [古いスナップショットをクリーンアップするメニューオプション] | *evs-rp-menu-cleanup-old-*

snapshots.png

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[NetApp Disaster Recoveryサービスのアクション メニュー アイコン]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。

   [スナップショットの調整メニューオプション] | *evs-rp-menu-reconcile-snapshots.png*

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[NetApp Disaster Recoveryサービスのアクション メニュー アイコン]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。

   [削除メニューオプション] | *evs-rp-menu-delete.png*

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[NetApp Disaster Recoveryサービスのアクション メニュー アイコン]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。

   [スケジュール編集メニューオプション] | *evs-rp-menu-edit-schedules.png*

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。

[コンプライアンスチェックスケジュール] | *evs-rp-edit-compliance-check-schedule.png*

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[NetApp Disaster Recoveryサービスのアクション メニュー アイコン]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。

    [スケジュールテストフェイルオーバーの編集] | *evs-rp-edit-schedule-test-failover.png*