自己管理コンポーネントを備えたハイブリッドクラウド

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

目次

自己管理コンポーネントを備えたハイブリッドクラウド

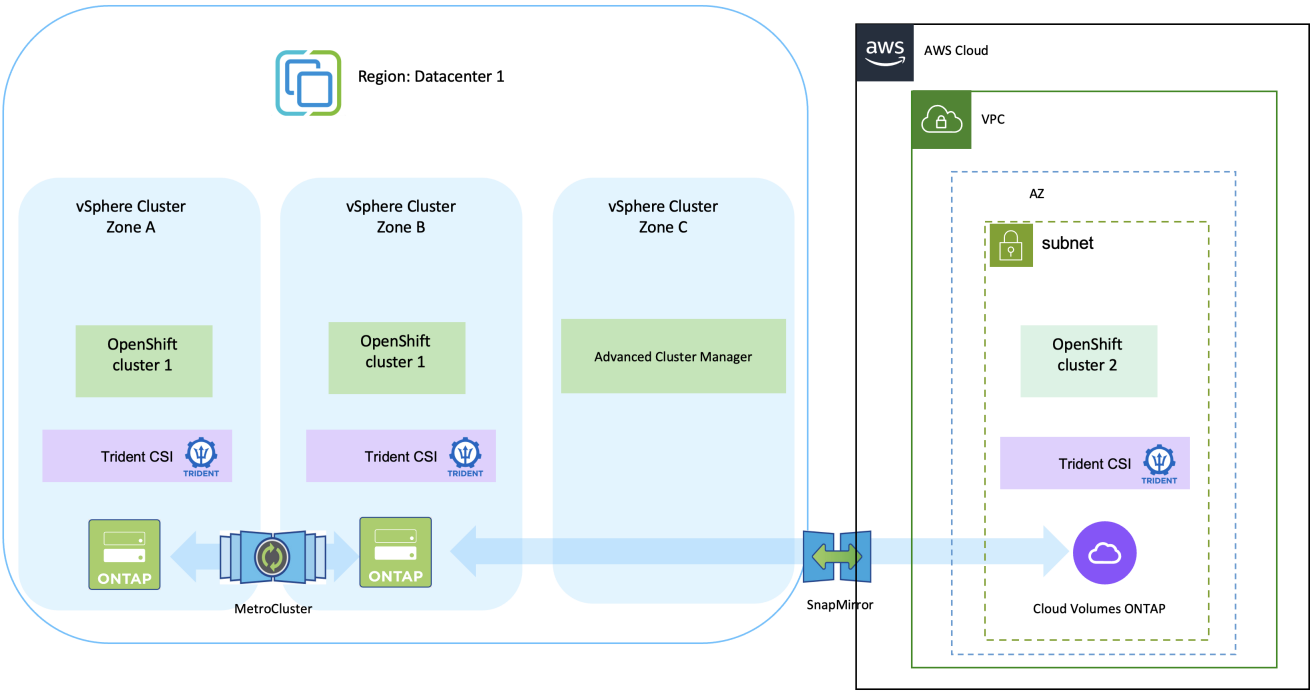
ハイブリッドクラウドにおける **Red Hat OpenShift Container** プラットフォームのワークロードに対応した**NetApp**ソリューション

顧客は、モダナイゼーションの取り組みの中で、一部の選択したワークロードまたはすべてのワークロードをデータセンターからクラウドに移行する準備が整っている場合があります。さまざまな理由から、クラウドでセルフ管理型 OpenShift コンテナとセルフ管理型NetAppストレージを使用することを選択する場合があります。データセンターからコンテナ ワークロードを移行するための本番環境を正常に構築するには、クラウドで Red Hat OpenShift コンテナ プラットフォーム (OCP) を計画して導入する必要があります。 OCP クラスターは、データセンター内の VMware またはベアメタル、およびクラウド環境内の AWS、Azure、または Google Cloud に展開できます。

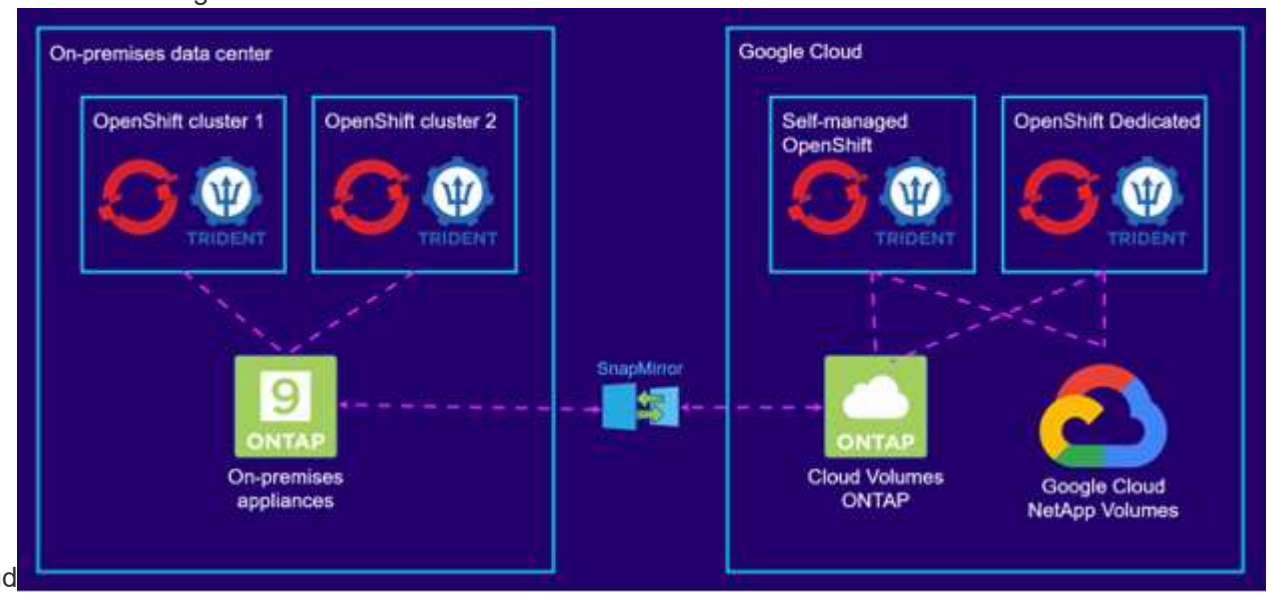
NetApp Cloud Volumes ONTAPストレージは、AWS、Azure、Google Cloud でのコンテナ導入にデータ保護、信頼性、柔軟性を提供します。 Trident は、顧客のステートフル アプリケーション用に永続的なCloud Volumes ONTAPストレージを使用する動的ストレージ プロビジョナーとして機能します。 Trident Protect は、データ保護、移行、ビジネス継続性などのステートフル アプリケーションのデータ管理要件に使用できます。

Trident Protectを使用したハイブリッド クラウドにおける **OpenShift Container** ワークロードのデータ保護および移行ソリューション

オンプレミスと
AWS

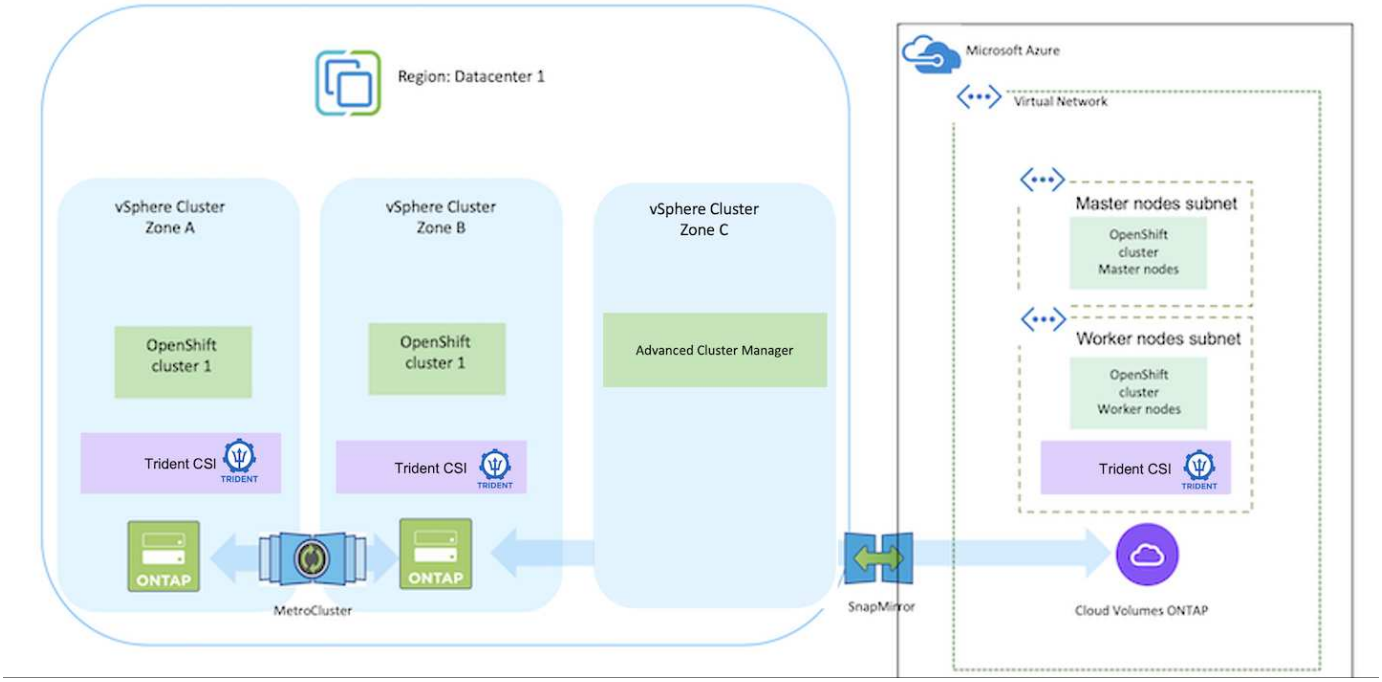


オンプレミスとGoogle



Cloud

オンプレミスとAzureクラウド

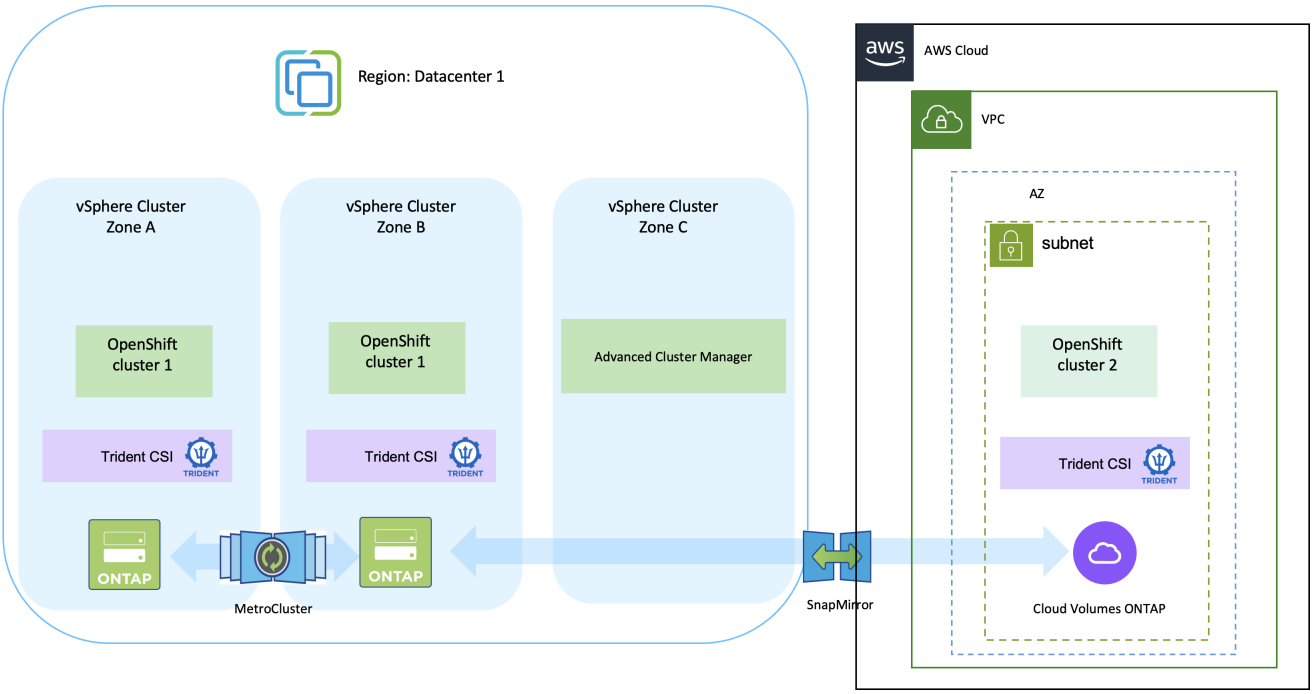


AWS 上で Red Hat OpenShift Container プラットフォームをデプロイおよび構成する

このセクションでは、AWS で OpenShift クラスターをセットアップおよび管理し、そこにステートフルアプリケーションをデプロイする方法の高レベルのワークフローについて説明します。これは、永続ボリュームを提供するためにTridentを活用したNetApp Cloud Volumes ONTAPストレージの使用方法を示しています。 Trident Protect を使用してステートフル アプリケーションのデータ保護および移行アクティビティを実行する方法について詳しく説明します。

> AWS に Red Hat OpenShift Container プラットフォーム クラスターをデプロイする方法はいくつかあります。このセットアップの概要説明には、使用された特定の方法に関するドキュメント リンクが提供されます。その他の方法については、以下の関連リンクを参照してください。"リソースセクション" 。

以下は、AWS にデプロイされ、VPN を使用してデータセンターに接続されたクラスターを示す図です。



セットアッププロセスは次の手順に分けられます。

高度なクラスター管理から **AWS** に **OCP** クラスターをインストールします。

- オンプレミス ネットワークに接続するために、サイト間 VPN 接続 (pfsense を使用) を持つ VPC を作成します。
- オンプレミス ネットワークにはインターネット接続があります。
- 3 つの異なる AZ に 3 つのプライベート サブネットを作成します。
- VPC 用の Route 53 プライベートホストゾーンと DNS リゾルバーを作成します。

高度なクラスター管理 (ACM) ウィザードから AWS 上に OpenShift クラスターを作成します。説明書を参照してください"ここをクリックしてください。"。

OpenShift Hybrid Cloud コンソールから AWS にクラスターを作成することもできます。参照する"ここをクリックしてください。"手順についてはこちらをご覧ください。

ACM を使用してクラスターを作成する場合、フォーム ビューに詳細を入力した後に yaml ファイルを編集してインストールをカスタマイズできます。クラスターが作成された後、トラブルシューティングや追加の手動構成のために、クラスターのノードに SSH ログインできます。インストール時に指定した SSH キーとユーザー名 core を使用してログインします。

BlueXPを使用して **AWS** に**Cloud Volumes ONTAP** をデプロイします。

- オンプレミスの VMware 環境にコネクタをインストールします。説明書を参照してください"ここをクリックしてください。"。
- コネクタを使用して AWS に CVO インスタンスをデプロイします。説明書を参照してください"ここをクリックしてください。"。

コネクタはクラウド環境にもインストールできます。参照する"ここをクリックしてください。"追加情報については。

OCP クラスターに**Trident**をインストールする

- Helm を使用してTrident Operator をデプロイします。説明書を参照してください"ここをクリックしてください。"
- バックエンドとストレージ クラスを作成します。説明書を参照してください"ここをクリックしてください。"。

マルチゾーンアーキテクチャに**Trident**の**CSI**トポロジ機能を使用する

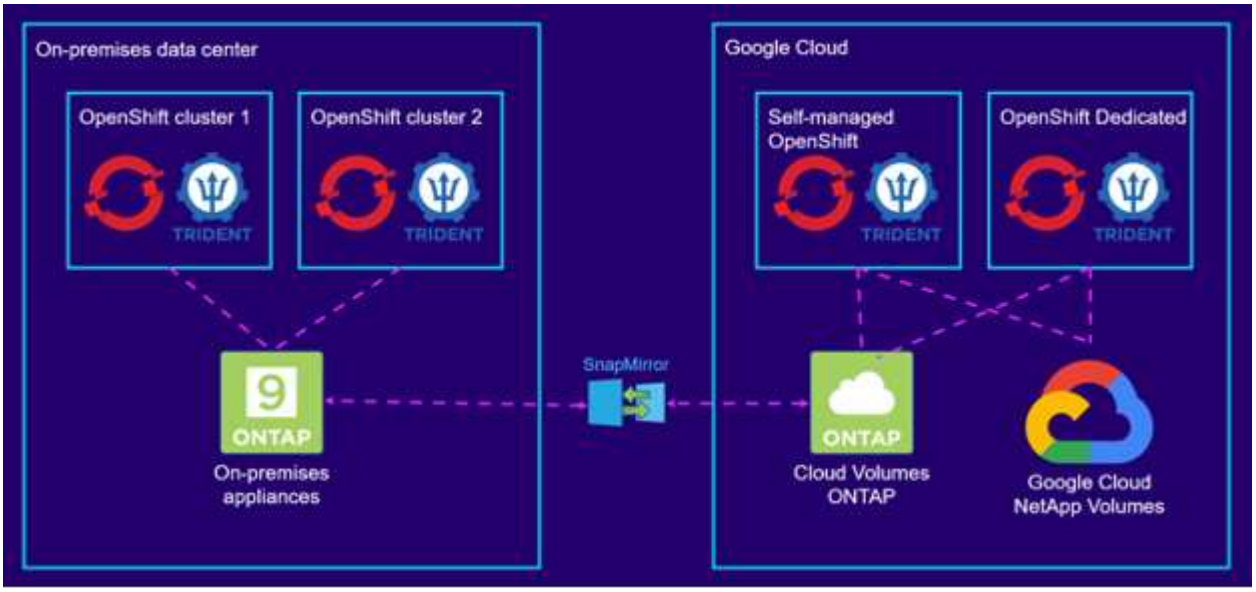
現在、クラウド プロバイダーは、Kubernetes/OpenShift クラスター管理者がゾーン ベースのクラスターのノードを生成できるようにしています。ノードは、リージョン内の異なるアベイラビリティーゾーン、または複数のリージョンに配置できます。マルチゾーン アーキテクチャでのワークロードのボリュームのプロビジョニングを容易にするために、 Trident はCSI トポロジを使用します。 CSI トポロジ機能を使用すると、リージョンとアベイラビリティーゾーンに基づいて、ボリュームへのアクセスをノードのサブセットに制限できます。参照する"ここをクリックしてください。"詳細については、こちらをご覧ください。

Kubernetes は 2 つのボリューム バインディング モードをサポートしています。 - ***VolumeBindingMode*** が ***Immediate*** (デフォルト) に設定されている場合、 Trident はトポロジを認識せずにボリュームを作成します。永続ボリュームは、要求元のポッドのスケジュール要件に依存せずに作成されます。 - ***VolumeBindingMode*** が ***WaitForFirstConsumer*** に設定されている場合、PVC を使用するポッドがスケジュールされて作成されるまで、PVC の永続ボリュームの作成とバインドは遅延されます。このようにして、トポロジ要件によって適用されるスケジュール制約を満たすボリュームが作成されます。 Tridentストレージ バックエンドは、可用性ゾーンに基づいてボリュームを選択的にプロビジョニングするように設計できます (トポロジ対応バックエンド)。このようなバックエンドを利用する StorageClasses の場合、ボリュームは、サポートされているリージョン/ゾーンでスケジュールされているアプリケーションによって要求された場合にのみ作成されます。 （トポロジー対応ストレージクラス）参照"ここをクリックしてください。"詳細については、こちらをご覧ください。

Google Cloud に Red Hat OpenShift Container Platform をデプロイして構成する

このセクションでは、GCP で OpenShift クラスターをセットアップおよび管理し、そこにステートフル アプリケーションをデプロイする方法のワークフローの概要について説明します。これは、永続ボリュームを提供するためにTridentを利用してGoogle Cloud NetApp VolumesとNetApp Cloud Volumes ONTAPストレージを使用する方法を示しています。

以下は、GCP にデプロイされ、VPN を使用してデータセンターに接続されたクラスターを示す図です。



GCP に Red Hat OpenShift Container Platform クラスターをデプロイする方法はいくつかあります。このセットアップの概要説明には、使用された特定の方法に関するドキュメント リンクが提供されます。その他の方法については、以下の関連リンクを参照してください。"リソース セクション" 。

セットアッププロセスは次の手順に分けられます。

CLI から **GCP** に **OCP** クラスタをインストールする

- 記載されているすべての前提条件を満たしていることを確認してください"ここをクリックしてください。"。
- オンプレミスと GCP 間の VPN 接続用に、pfsense VM が作成および構成されました。手順については、"ここをクリックしてください。" 。
  - pfsense のリモート ゲートウェイ アドレスは、Google Cloud Platform で VPN ゲートウェイを作成した後にのみ構成できます。
  - フェーズ 2 のリモート ネットワーク IP アドレスは、OpenShift クラスター インストール プログラムが実行され、クラスターのインフラストラクチャ コンポーネントが作成された後にのみ構成できます。
  - Google Cloud の VPN は、インストール プログラムによってクラスタのインフラストラクチャ コンポーネントが作成された後にのみ構成できます。
- 次に、GCP に OpenShift クラスターをインストールします。
  - インストールプログラムとプルシークレットを取得し、ドキュメントに記載されている手順に従ってクラスターをデプロイします。 "ここをクリックしてください。" 。
  - インストールにより、Google Cloud Platform に VPC ネットワークが作成されます。また、Cloud DNS にプライベート ゾーンを作成し、A レコードを追加します。
    - VPC ネットワークの CIDR ブロック アドレスを使用して pfsense を設定し、VPN 接続を確立します。ファイアウォールが正しく設定されていることを確認します。
    - Google Cloud DNS の A レコードの IP アドレスを使用して、オンプレミス環境の DNS に A レコードを追加します。

- クラスターのインストールが完了し、クラスターのコンソールにログインするための kubeconfig ファイルとユーザー名とパスワードが提供されます。

Google Cloud NetApp Volumesをデプロイする

- Google Cloud NetApp Volumesは、概要に従ってプロジェクトに追加できます。"ここをクリックしてください。" 。

BlueXPを使用して **GCP** に**Cloud Volumes ONTAP**を導入する

- Google Cloud にコネクタをインストールします。説明書を参照してください "ここをクリックしてください。"。
- コネクタを使用して Google Cloud に CVO インスタンスをデプロイします。こちらの手順を参照してください。 https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

GCP の **OCP** クラスタに**Trident**をインストールする

- Tridentを展開する方法は数多くある。 "ここをクリックしてください。" 。
- このプロジェクトでは、以下の手順に従ってTrident Operatorを手動で展開することでTridentをインストールしました。 "ここをクリックしてください。" 。
- バックエンドとストレージ クラスを作成します。説明書を参照してください"ここをクリックしてください。"。

マルチゾーンアーキテクチャに**Trident**の**CSI**トポロジ機能を使用する

現在、クラウド プロバイダーは、Kubernetes/OpenShift クラスター管理者がゾーン ベースのクラスターのノードを生成できるようにしています。ノードは、リージョン内の異なるアベイラビリティーゾーン、または複数のリージョンに配置できます。マルチゾーン アーキテクチャでのワークロードのボリュームのプロビジョニングを容易にするために、 Trident はCSI トポロジを使用します。 CSI トポロジ機能を使用すると、リージョンとアベイラビリティーゾーンに基づいて、ボリュームへのアクセスをノードのサブセットに制限できます。参照する"ここをクリックしてください。"詳細については、こちらをご覧ください。

> Kubernetes は 2 つのボリューム バインディング モードをサポートしています。 - ***VolumeBindingMode*** が ***Immediate*** (デフォルト) に設定されている場合、 Trident はトポロジを認識せずにボリュームを作成します。永続ボリュームは、要求元のポッドのスケジュール要件に依存せずに作成されます。 - ***VolumeBindingMode*** が ***WaitForFirstConsumer*** に設定されている場合、PVC を使用するポッドがスケジュールされて作成されるまで、PVC の永続ボリュームの作成とバインドは遅延されます。このようにして、トポロジ要件によって適用されるスケジュール制約を満たすボリュームが作成されます。 Tridentストレージ バックエンドは、可用性ゾーンに基づいてボリュームを選択的にプロビジョニングするように設計できます (トポロジ対応バックエンド)。このようなバックエンドを利用する StorageClasses の場合、ボリュームは、サポートされているリージョン/ゾーンでスケジュールされているアプリケーションによって要求された場合にのみ作成されます。 （トポロジー対応ストレージクラス）参照"ここをクリックしてください。"詳細については、こちらをご覧ください。

デモビデオ

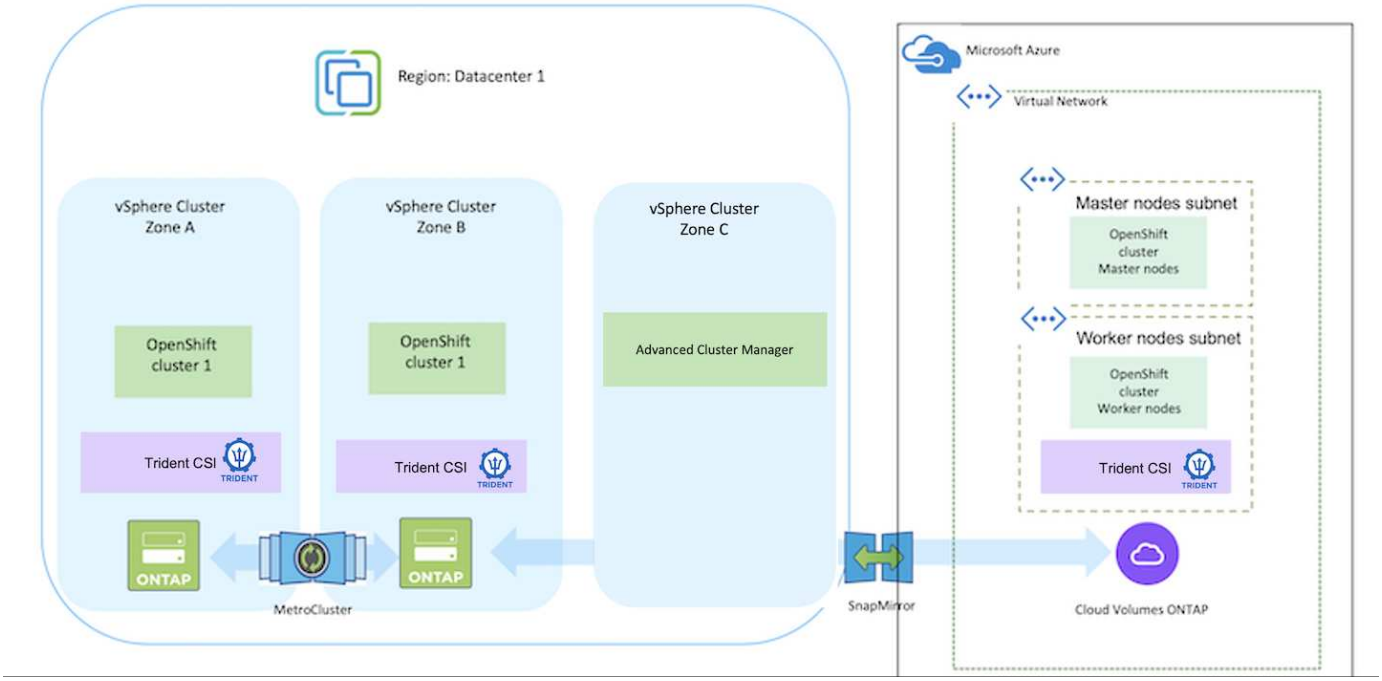
Google Cloud Platform への OpenShift Cluster のインストール

OpenShift クラスターをTrident Protect にインポートする

Azure に Red Hat OpenShift Container プラットフォームをデプロイして構成する

このセクションでは、Azure で OpenShift クラスターをセットアップおよび管理し、そこにステートフル アプリケーションをデプロイする方法の大まかなワークフローについて説明します。これは、永続ボリュームを提供するためにTridentを活用したNetApp Cloud Volumes ONTAPストレージの使用方法を示しています。 Trident Protect を使用してステートフル アプリケーションのデータ保護および移行アクティビティを実行する方法について詳しく説明します。

以下は、Azure にデプロイされ、VPN を使用してデータ センターに接続されたクラスターを示す図です。



Azure に Red Hat OpenShift Container Platform クラスターをデプロイする方法はいくつかあります。このセットアップの概要説明には、使用された特定の方法に関するドキュメント リンクが提供されます。その他の方法については、以下の関連リンクを参照してください。"リソースセクション" 。

セットアッププロセスは次の手順に分けられます。

CLI から **Azure** に **OCP** クラスターをインストールします。

- 記載されているすべての前提条件を満たしていることを確認してください"ここをクリックしてください。"。
- VPN、サブネット、ネットワーク セキュリティ グループ、およびプライベート DNS ゾーンを作成します。 VPN ゲートウェイとサイト間 VPN 接続を作成します。
- オンプレミスと Azure 間の VPN 接続用に、pfsense VM が作成および構成されました。手順については、"ここをクリックしてください。" 。
- インストールプログラムとプルシークレットを取得し、ドキュメントに記載されている手順に従ってクラスターをデプロイします。"ここをクリックしてください。" 。
- クラスターのインストールが完了し、クラスターのコンソールにログインするための kubeconfig ファイルとユーザー名とパスワードが提供されます。

サンプルの install-config.yaml ファイルを以下に示します。

```
apiVersion: v1
baseDomain: sddc.netapp.com
compute:
- architecture: amd64
  hyperthreading: Enabled
  name: worker
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 512
        diskType: "StandardSSD_LRS"
      type: Standard_D2s_v3
      ultraSSDCapability: Disabled
      #zones:
      #- "1"
      #- "2"
      #- "3"
  replicas: 3
controlPlane:
  architecture: amd64
  hyperthreading: Enabled
  name: master
  platform:
    azure:
      encryptionAtHost: false
      osDisk:
        diskSizeGB: 1024
        diskType: Premium_LRS
      type: Standard_D8s_v3
```

```
      ultraSSDCapability: Disabled
  replicas: 3
metadata:
  creationTimestamp: null
  name: azure-cluster
networking:
  clusterNetwork:
  - cidr: 10.128.0.0/14
    hostPrefix: 23
  machineNetwork:
  - cidr: 10.0.0.0/16
  networkType: OVNKubernetes
  serviceNetwork:
  - 172.30.0.0/16
platform:
  azure:
    baseDomainResourceGroupName: ocp-base-domain-rg
    cloudName: AzurePublicCloud
    computeSubnet: ocp-subnet2
    controlPlaneSubnet: ocp-subnet1
    defaultMachinePlatform:
      osDisk:
        diskSizeGB: 1024
        diskType: "StandardSSD_LRS"
      ultraSSDCapability: Disabled
    networkResourceGroupName: ocp-nc-us-rg
    #outboundType: UserDefinedRouting
    region: northcentralus
    resourceGroupName: ocp-cluster-ncusrg
    virtualNetwork: ocp_vnet_ncus
publish: Internal
pullSecret:
```

BlueXPを使用して **Azure** に**Cloud Volumes ONTAP** をデプロイします。

- Azure にコネクタをインストールします。説明書を参照してください "ここをクリックしてください。"。
- コネクタを使用して Azure に CVO インスタンスをデプロイします。手順についてはリンクhttps://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [こちら]を参照してください。

マルチゾーンアーキテクチャに**Trident**の**CSI**トポロジ機能を使用する

現在、クラウド プロバイダーは、Kubernetes/OpenShift クラスター管理者がゾーン ベースのクラスターのノードを生成できるようにしています。ノードは、リージョン内の異なるアベイラビリティーゾーン、または複数のリージョンに配置できます。マルチゾーン アーキテクチャでのワークロードのボリュームのプロビジョ

ニングを容易にするために、 Trident はCSI トポロジを使用します。 CSI トポロジ機能を使用すると、リージョンとアベイラビリティーゾーンに基づいて、ボリュームへのアクセスをノードのサブセットに制限できます。参照する"ここをクリックしてください。"詳細については、こちらをご覧ください。

> Kubernetes は 2 つのボリューム バインディング モードをサポートしています。 - ***VolumeBindingMode*** が ***Immediate*** (デフォルト) に設定されている場合、 Trident はトポロジを認識せずにボリュームを作成します。永続ボリュームは、要求元のポッドのスケジュール要件に依存せずに作成されます。 - ***VolumeBindingMode*** が ***WaitForFirstConsumer*** に設定されている場合、PVC を使用するポッドがスケジュールされて作成されるまで、PVC の永続ボリュームの作成とバインドは遅延されます。このようにして、トポロジ要件によって適用されるスケジュール制約を満たすボリュームが作成されます。 Tridentストレージ バックエンドは、可用性ゾーンに基づいてボリュームを選択的にプロビジョニングするように設計できます (トポロジ対応バックエンド)。このようなバックエンドを利用する StorageClasses の場合、ボリュームは、サポートされているリージョン/ゾーンでスケジュールされているアプリケーションによって要求された場合にのみ作成されます。 （トポロジー対応ストレージクラス）参照"ここをクリックしてください。"詳細については、こちらをご覧ください。

Trident Protectを使用したデータ保護

このページでは、VMware vSphere 上またはTrident Protect (ACC) を使用してクラウドで実行される Red Hat OpenShift Container ベースのアプリケーションのデータ保護オプションを示します。

ユーザーが Red Hat OpenShift を使用してアプリケーションを最新化する際には、誤った削除やその他の人為的エラーからアプリケーションを保護するためのデータ保護戦略を策定する必要があります。多くの場合、規制やコンプライアンス上の目的でデータを災害から保護するための保護戦略も必要になります。

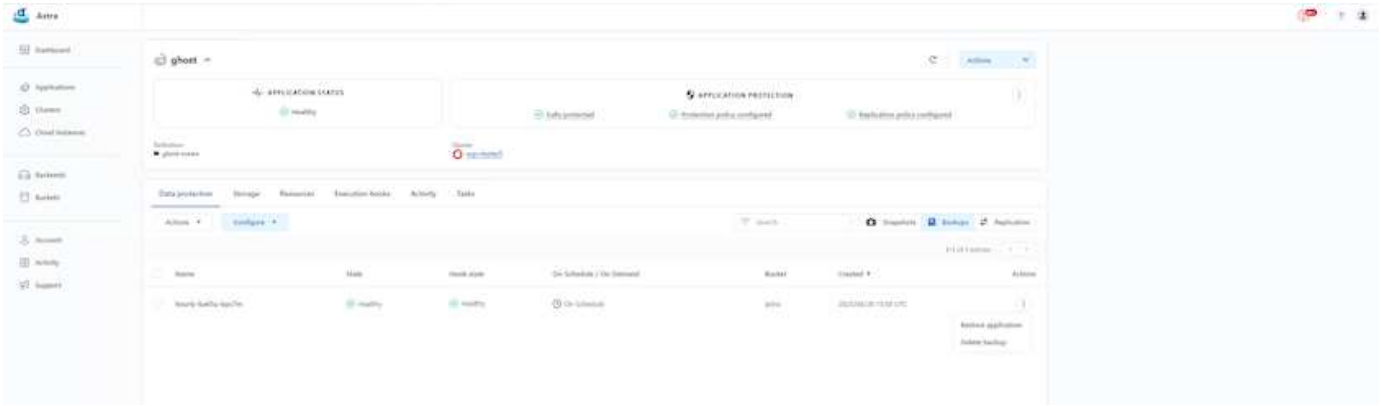
データ保護の要件は、ある時点のコピーに戻すことから、人間の介入なしに別の障害ドメインに自動的にフェイルオーバーすることまで多岐にわたります。多くのお客様が、マルチテナンシー、マルチプロトコル、高パフォーマンスと高容量の提供、複数サイトのレプリケーションとキャッシュ、セキュリティと柔軟性などの豊富な機能を備えているため、Kubernetes アプリケーション用の優先ストレージ プラットフォームとしてONTAPを選択しています。

顧客はデータ センターの拡張としてクラウド環境をセットアップすることで、クラウドの利点を活用できるだけでなく、将来的にワークロードを移行する準備も整う場合があります。このような顧客にとって、OpenShift アプリケーションとデータをクラウド環境にバックアップすることは避けられない選択になります。その後、アプリケーションと関連データをクラウド内の OpenShift クラスターまたはデータセンターに復元できます。

ACC によるバックアップと復元

アプリケーション所有者は、ACC によって検出されたアプリケーションを確認し、更新できます。 Trident Protect は、CSI を使用してスナップショット コピーを取得し、ポイント イン タイム スナップショット コピーを使用してバックアップを実行できます。バックアップ先はクラウド環境内のオブジェクト ストアにすることができます。スケジュールされたバックアップと保持するバックアップ バージョンの数に対して保護ポリシーを構成できます。最小 RPO は 1 時間です。

ACC を使用してバックアップからアプリケーションを復元する



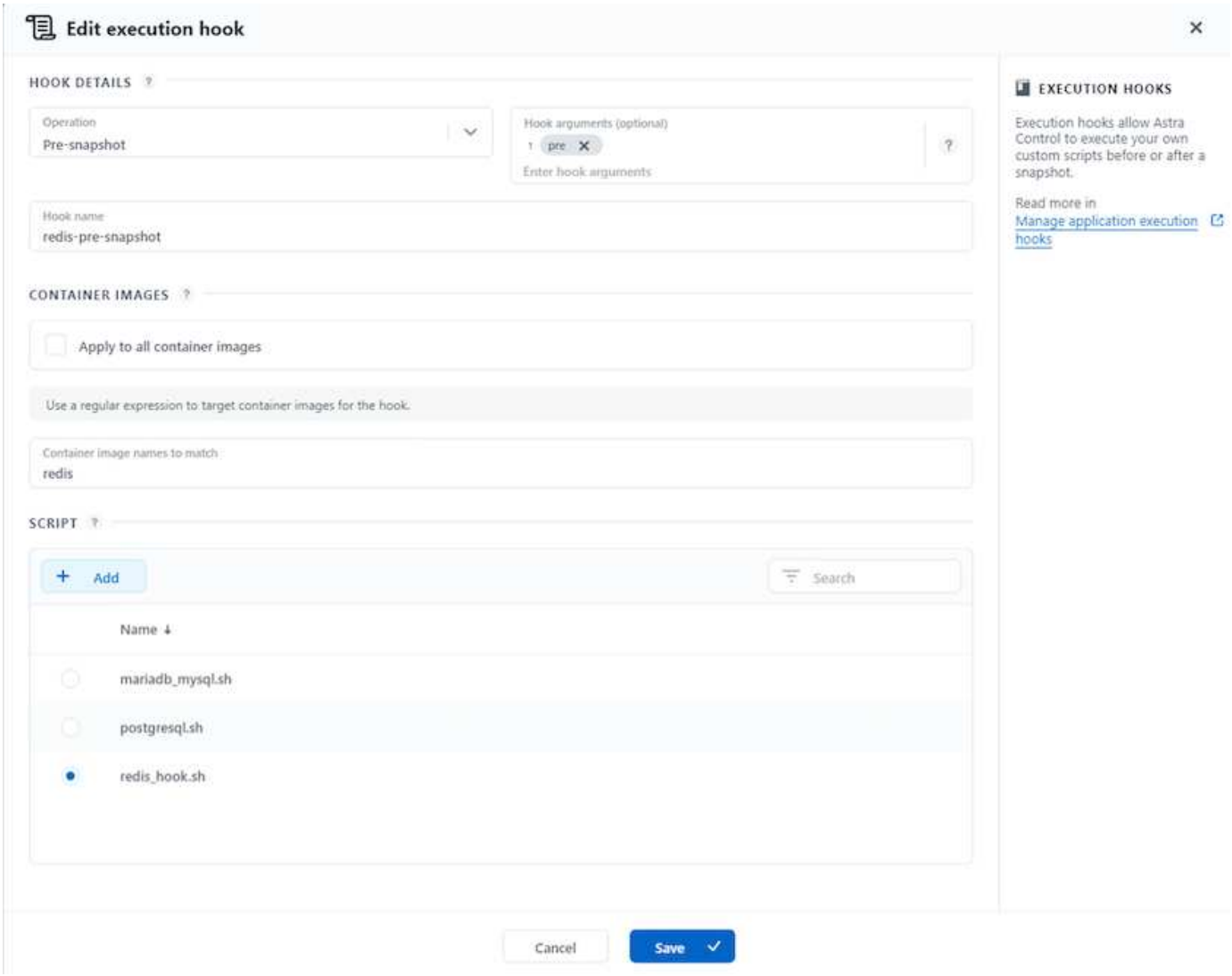
アプリケーション固有の実行フック

ストレージ アレイ レベルのデータ保護機能が利用可能であっても、バックアップと復元のアプリケーションの一貫性を保つために追加の手順が必要になることがよくあります。アプリ固有の追加手順は次のようになります: - スナップショット コピーが作成される前または後。 - バックアップが作成される前または後。 - スナップショット コピーまたはバックアップから復元した後。

Trident Protect は、実行フックと呼ばれるカスタム スクリプトとしてコーディングされたアプリ固有のステップを実行できます。

NetAppの"オープンソースプロジェクトVerda"一般的なクラウドネイティブ アプリケーションの実行フックを提供することで、アプリケーションの保護を簡単かつ堅牢にし、簡単にオーケストレーションできるようにします。リポジトリにないアプリケーションに関する十分な情報をお持ちの場合は、ぜひそのプロジェクトに貢献してください。

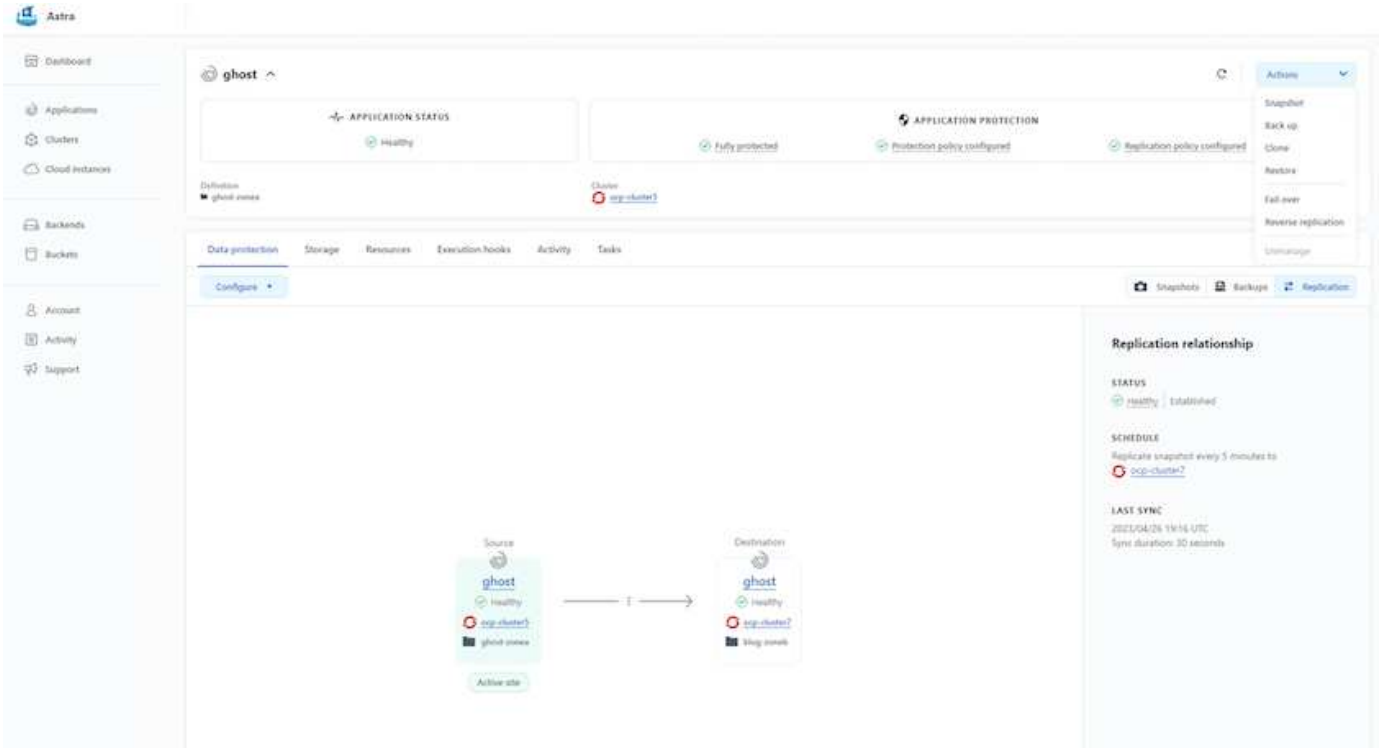
Redis アプリケーションの事前スナップショット用のサンプル実行フック。



ACCによるレプリケーション

地域保護や RPO および RTO が低いソリューションの場合、アプリケーションを別のサイト (できれば別のリージョン) で実行されている別の Kubernetes インスタンスに複製できます。 Trident Protect は、最短 5 分の RPO でONTAP非同期SnapMirrorを活用します。参照する"ここをクリックしてください。"SnapMirror のセットアップ手順については、こちらをご覧ください。

ACC 搭載SnapMirror



san-economy および nas-economy ストレージ ドライバーはレプリケーション機能をサポートしていません。参照する"ここをクリックしてください。"詳細については、こちらをご覧ください。

デモビデオ:

"Trident Protectによる災害復旧のデモビデオ"

Trident Protectによるデータ保護

Trident Protectデータ保護機能の詳細については、"ここをクリックしてください。"

ACC による災害復旧 (レプリケーションを使用したフェイルオーバーとフェイルバック)

アプリケーションのフェイルオーバーとフェイルバックにAstra Control を使用する

Trident Protectを使用したデータ移行

このページでは、 Trident Protect (ACC) を使用した Red Hat OpenShift クラスター上のコンテナー ワークロードのデータ移行オプションについて説明します。具体的には、顧客はTrident Protectを使用して、選択したワークロードの一部またはすべてをオンプレミスのデータセンターからクラウドに移動する、テスト目的でアプリをクラウドに複製するか、データセンターからクラウドに移動するといったことが可能です。

データ マイグレーション

アプリケーションをある環境から別の環境に移行するには、ACC の次のいずれかの機能を使用できます。

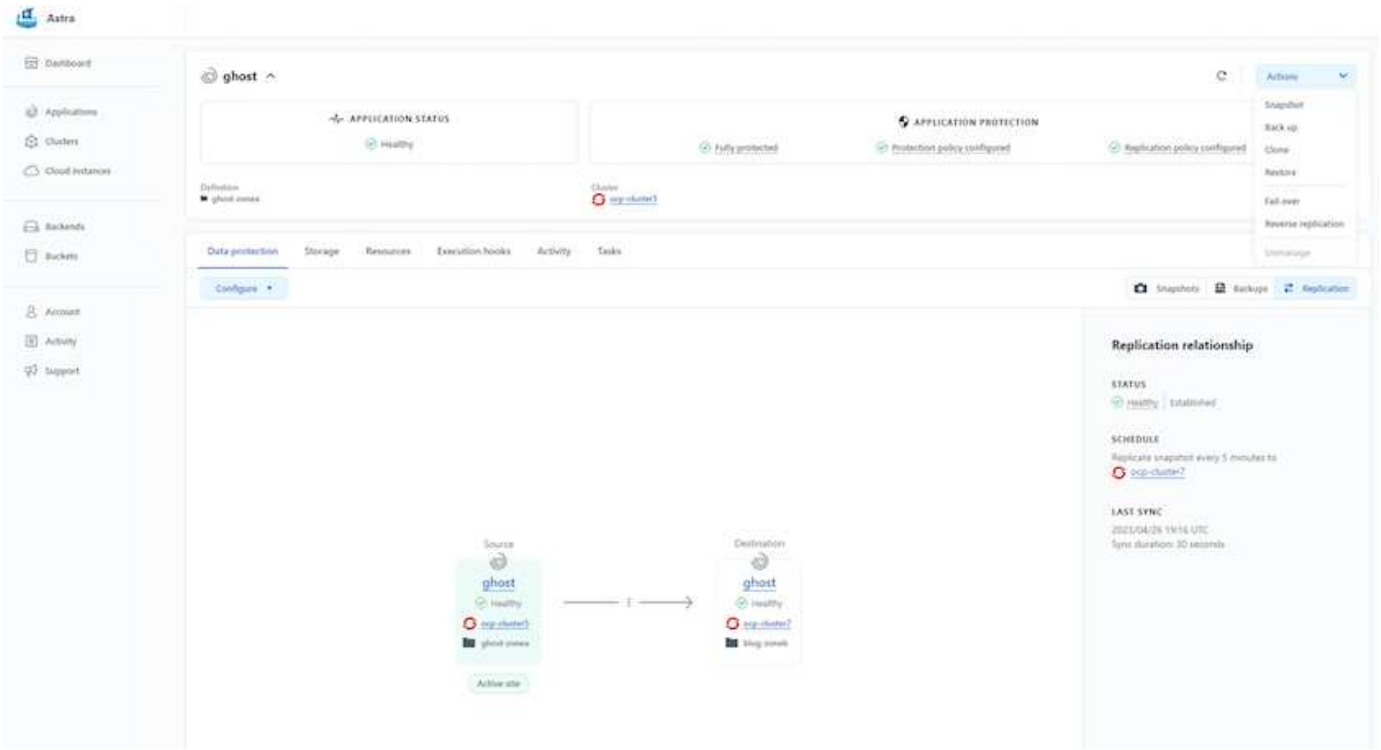
- レプリケーション
- バックアップと復元
- クローン

参照link:os-sm-data-protection.html<strong class=""データ保護セクション"">レプリケーションとバックアップと復元 オプションについて。

参照するlink:https://docs.netapp.com/us-en/astra-control-center/use/clone-apps.html<strong class=""ここをクリックしてください。"">クローン作成 に関する追加の詳細については、こちらをご覧ください。

Astraレプリケーション機能は、 Trident Container Storage Interface (CSI) でのみサポートされます。ただし、レプリケーションは nas-economy および san-economy ドライバーではサポートされていません。

ACC を使用したデータ複製の実行



著作権に関する情報

商標に関する情報