自己管理型コンポーネントを使用したハイブリッドクラウド（オンプレミス/ **AWS / GCP / Azure**）

NetApp Solutions

NetApp
April 10, 2024

目次

Red Hat OpenShift Containerワークロード向けのネットアップハイブリッドマルチクラウドソリューション

概要

ネットアップでは、従来型エンタープライズアプリケーションを最新化し、Kubernetesを中心に構築されたコンテナとオーケストレーションプラットフォームを使用して新しいアプリケーションを構築するお客様が大幅に増えています。Red Hat OpenShift Container Platformは、多くのお客様に採用されている例の1つです。

企業内でコンテナを採用するお客様がますます増えています。ネットアップは、ステートフルアプリケーションの永続的ストレージのニーズに加え、データ保護、データセキュリティ、データ移行などの従来のデータ管理のニーズにも応えることができます。しかし、これらのニーズは、さまざまな戦略、ツール、方法を使用して満たしています。

- NetApp ONTAP **ベースのストレージオプションを次に示します。コンテナとKubernetes環境にセキュリティ、データ保護、信頼性、柔軟性を提供します。
  - オンプレミスの自己管理型ストレージ：
- ネットアップファブリック接続ストレージ（FAS ）、ネットアップオールフラッシュFAS アレイ（AFF ）、ネットアップオールSANアレイ（ASA ）、ONTAP Select
  - オンプレミスのプロバイダ管理ストレージ：
- NetApp Keystone が提供するストレージサービス（STaaS）
  - クラウド内の自己管理型ストレージ：
- NetApp Cloud Volumes ONTAP（CVO）は、ハイパースケーラに自己管理型ストレージを提供します
  - クラウド上のプロバイダが管理するストレージ：
- Cloud Volumes Service for Google Cloud（CVS）、Azure NetApp Files （ANF）、Amazon FSx for NetApp ONTAP は、ハイパースケーラにフルマネージドストレージを提供します

ONTAP feature highlights

Storage Administration

- Multi-tenancy
- FlexVol & FlexGroup
- LUN
- Quotas
- ONTAP CLI & API
- System Manager & BlueXP

Performance & Scalability

- FlexCache
- FlexClone
- nconnect, session trunking, multipathing
- Scale-out clusters

Availability & Resilience

- Multi-AZ HA deployment (MetroCluster)
- SnapShot & SnapRestore
- SnapMirror
- SnapMirror Business Continuity
- SnapMirror Cloud

Access Protocols

- NFS –v3, v4, v4.1, v4.2
- SMB – v2, v3
- iSCSI
- Multi-protocol access

Storage Efficiency

- Deduplication & Compression
- Compaction
- Thin provisioning
- Data Tiering (Fabric Pool)

Security & Compliance

- Fpolicy & Vscan
- Active Directory integration
- LDAP & Kerberos
- Certificate based authentication

- NetApp BlueXP **を使用すると、すべてのストレージ資産とデータ資産を単一のコントロールプレーン/インターフェイスから管理できます。

BlueXPを使用して、クラウドストレージ（Cloud Volumes ONTAP やAzure NetApp Files など）の作成と管理、データの移動、保護、分析、オンプレミスやエッジの多くのストレージデバイスの管理を行うことができます。

- NetApp Astra Trident **はCSI準拠のストレージオーケストレーションツールです。上記のさまざまなネットアップストレージオプションを利用して、永続的ストレージをすばやく簡単に利用できます。ネットアップが保守、サポートしているオープンソースのソフトウェアです。

Astra Trident CSI feature highlights

CSI specific

- CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies
- CSI topology
- Volume expansion

Security

- Dynamic-export policy management
- iSCSI initiator-groups dynamic management
- iSCSI bidirectional CHAP

Control

- Storage and performance consumption
- Monitoring
- Volume Import
- Cross Namespace Volume Access

Installation methods

- Binary
- Helm chart
- Operator
- GitOps

Choose your access mode

- RWO (ReadWriteOnce, i.e 1⇔1)
- RWX (*ReadWriteMany*, i.e 1⇔n)
- ROX (*ReadOnlyMany*)
- RWOP (ReadWriteOnce POD)

Choose your protocol

- NFS
- SMB
- iSCSI

ビジネスクリティカルなコンテナワークロードに必要なのは、永続的ボリュームだけではありません。同社のデータ管理要件では、アプリケーションのKubernetesオブジェクトの保護と移行も必要です。

> アプリケーションデータには、ユーザデータに加えてKubernetesオブジェクトが含まれます。例を次に示します。 -ポッド仕様、PVC、デプロイ、サービスなどのKubernetesオブジェクト- 設定マップやシークレットなどのカスタム設定オブジェクト- Snapshotコピー、バックアップ、クローンなどの永続的データ- CRSやCRDなどのカスタムリソース

- NetApp Astra Control **は、フルマネージドと自己管理型の両方のソフトウェアとして提供され、堅牢なアプリケーションデータ管理のためのオーケストレーションを提供します。を参照してください "Astra のドキュメント" を参照してください。

このリファレンスドキュメントでは、NetApp Astra Control Centerを使用して、Red Hat OpenShiftコンテナプラットフォームに導入されたコンテナベースアプリケーションの移行と保護について検証します。また、解決策 では、コンテナプラットフォームを管理するためのRed Hat Advanced Cluster Management（ACM）の導入と使用に関する詳細についても説明しています。また、Astra Trident CSIプロビジョニングツールを使用して、ネットアップストレージとRed Hat OpenShiftコンテナプラットフォームを統合する方法についても詳しく説明します。Astra Control Centerはハブクラスタに導入され、コンテナアプリケーションとその永続的ストレージライフサイクルの管理に使用されます。最後に、Amazon FSx for NetApp ONTAP （FSxN）を永続的ストレージとして使用し、AWS（ROSA）のマネージドRed Hat OpenShiftクラスタ上のコンテナワークロードのレプリケーション、フェイルオーバー、フェイルバックのための解決策 を提供します。

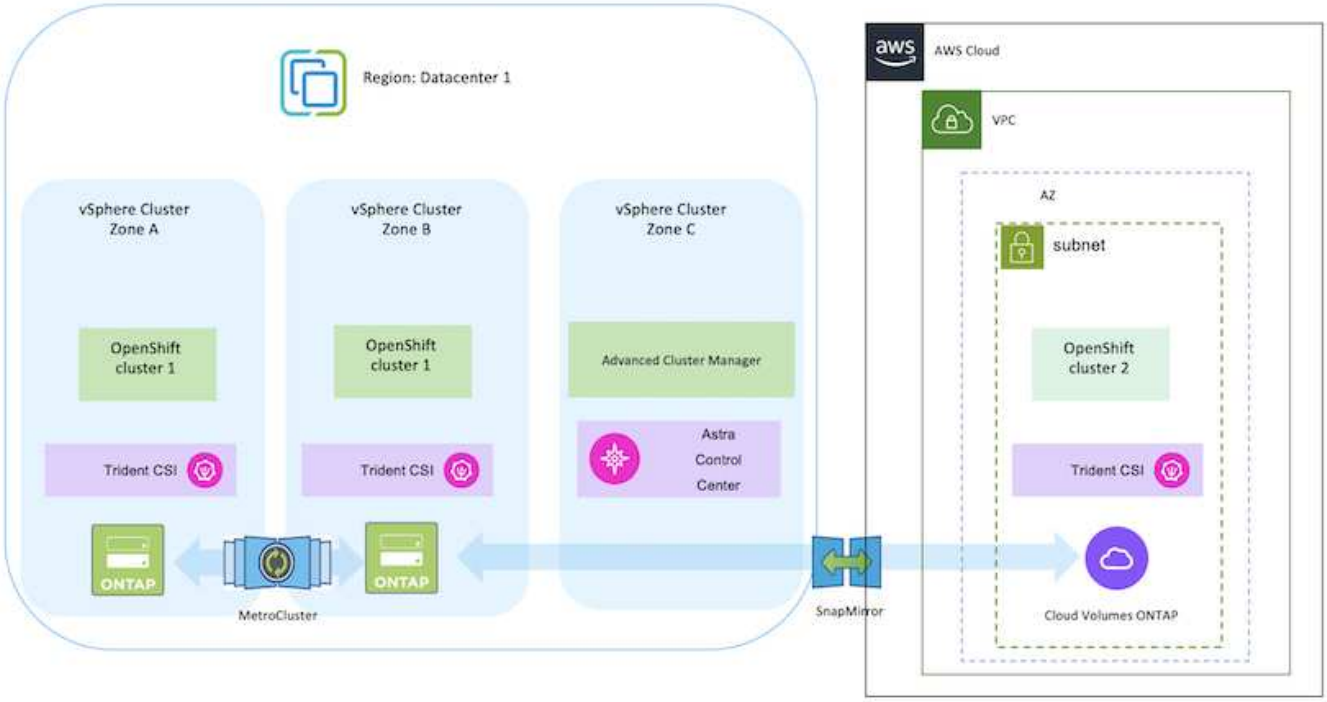
NetApp解決策 とRed Hat OpenShift Containerプラットフォームのワークロードをハイブリッドクラウドで運用

お客様は、一部の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た時点で、モダナイゼーションに移行する可能性があります。お客様は、さまざまな理由から、クラウドで自己管理型OpenShiftコンテナと自己管理型ネットアップストレージを使用することができます。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向け環境を成功させるには、Red Hat OpenShiftコンテナプラットフォーム（OCP）をクラウドに計画して導入する必要があります。OCPクラスタは、データセンターのVMwareまたはベアメタルに導入し、クラウド環境のAWS、Azure、Google Cloudに導入できます。

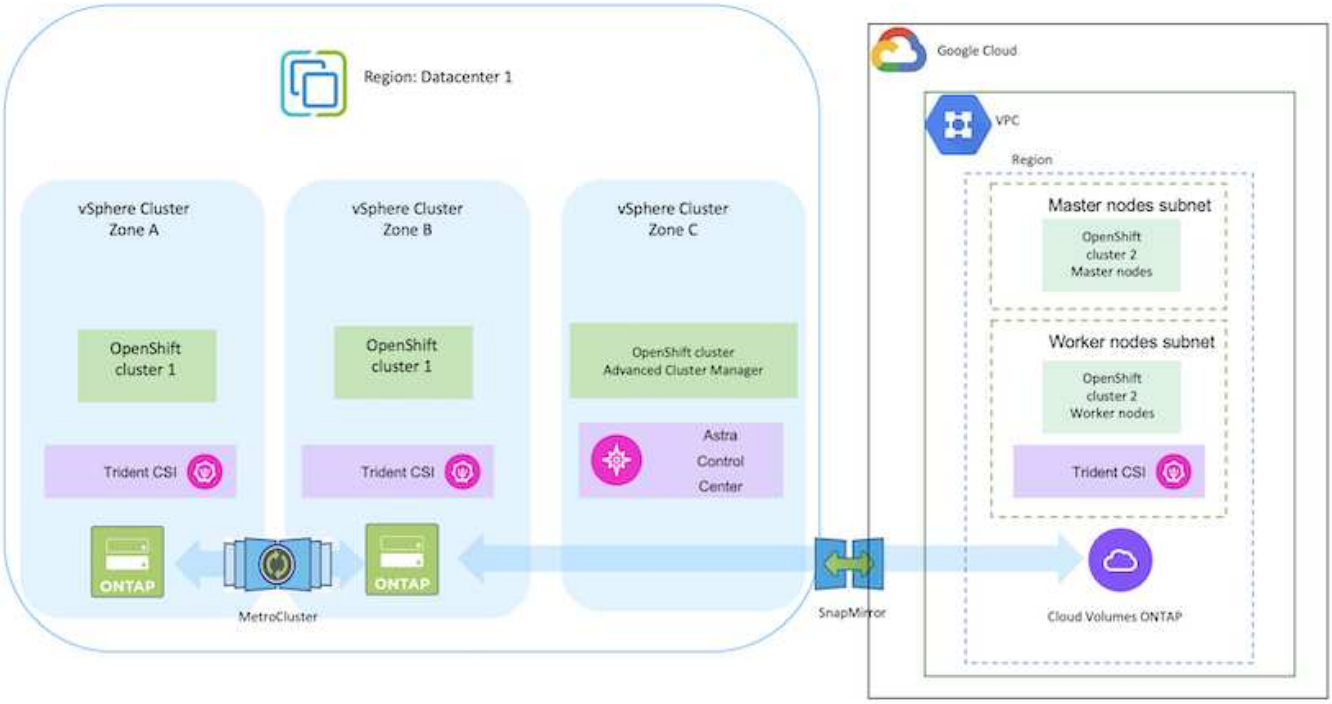
NetApp Cloud Volumes ONTAP ストレージは、AWS、Azure、Google Cloudでのコンテナ導入にデータ保護、信頼性、柔軟性を提供します。Astra Tridentは、お客様のステートフルアプリケーション向けに永続的Cloud Volumes ONTAP ストレージを利用するための動的ストレージプロビジョニングツールとして機能します。Astra Control Centerを使用すると、データ保護、移行、ビジネス継続性など、ステートフルアプリケーションに求められる多くのデータ管理要件をオーケストレーションできます。

Astra Control Centerを使用したハイブリッドクラウドでのOpenShiftコンテナワークロード向けのデータ保護と移行解決策

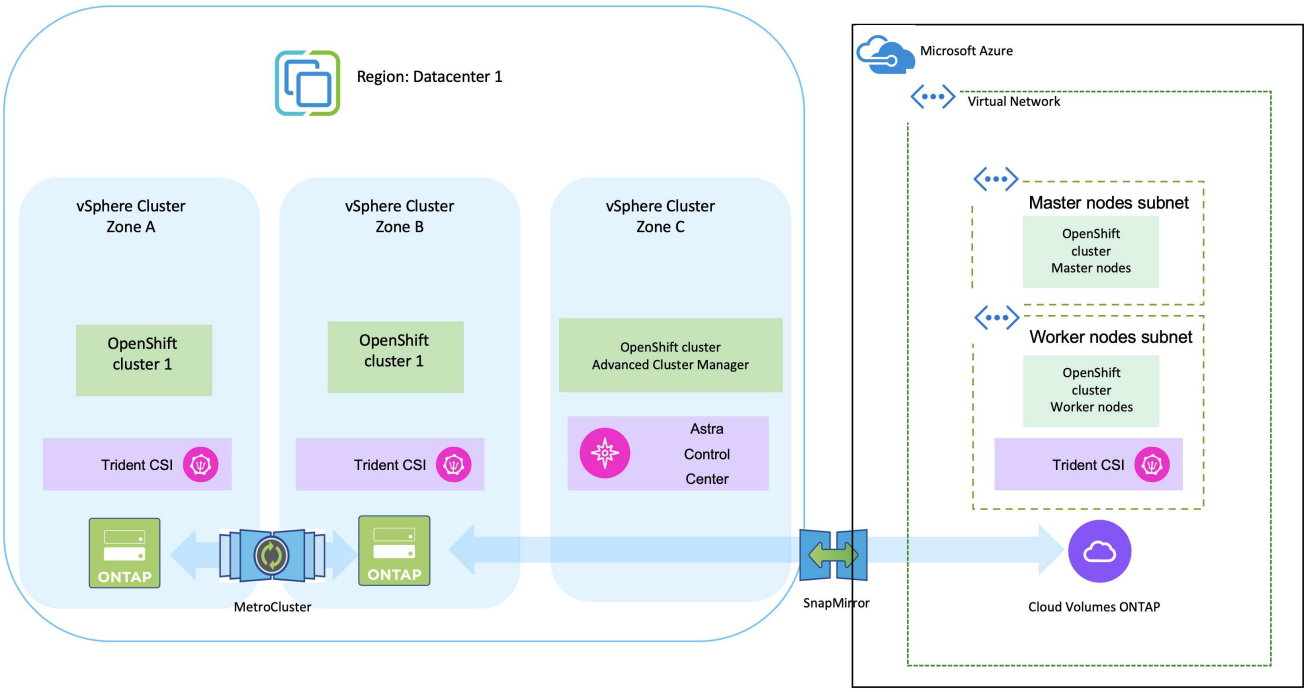
オンプレミスとAWS



オンプレミスとGoogle Cloud



オンプレミスとAzureクラウド

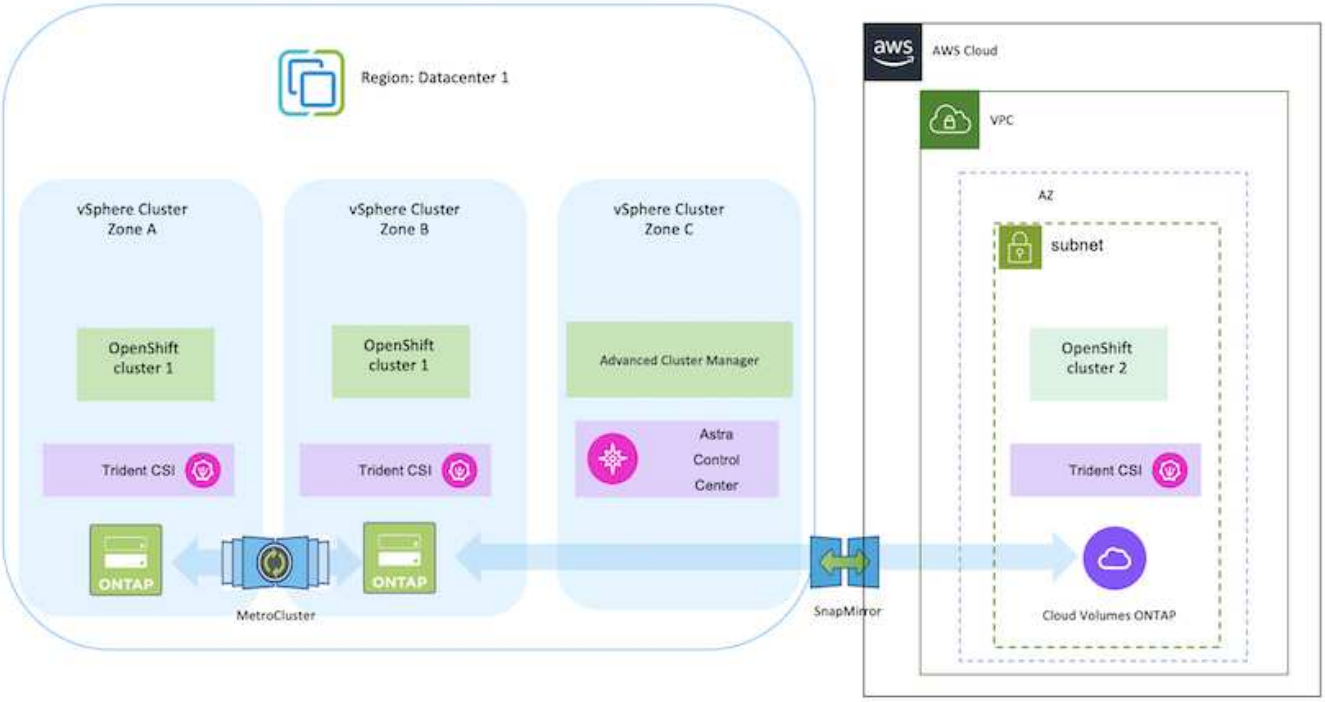


AWSにRed Hat OpenShift Containerプラットフォームを導入して設定します

このセクションでは、AWSでOpenShiftクラスタをセットアップおよび管理し、それらにステートフルアプリケーションを導入する方法の大まかなワークフローについて説明します。このスライドでは、Astra Tridentを使用してNetApp Cloud Volumes ONTAP ストレージを使用し、永続ボリュームを提供する方法を示しています。ステートフルアプリケーションに対してデータ保護と移行のアクティビティを実行するためのAstra Control Centerの使用方法について詳しく説明します。

> Red Hat OpenShift Containerプラットフォームクラスタを AWSに導入する方法はいくつかあります。このセットアップの概要概要 には、使用した具体的な方法のドキュメントへのリンクが記載されています。その他の方法については、に記載されている関連リンクを参照してください "リソースセクション"。

次の図は、AWSに導入され、VPNを使用してデータセンターに接続されたクラスタを示しています。



セットアッププロセスは、次の手順に分けることができます。

Advanced Cluster Managementから**AWS**に**OCP**クラスタをインストールします。

- サイト間VPN接続（pfsenseを使用）を使用してVPCを作成し、オンプレミスネットワークに接続します。
- オンプレミスネットワークはインターネットに接続されています。
- 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用にRoute 53プライベートホストゾーンとDNSリゾルバを作成します。

Advanced Cluster Management（ACM）ウィザードを使用して、AWSにOpenShiftクラスタを作成します。手順を参照してください "こちらをご覧ください"。

AWSでは、OpenShift Hybrid Cloudコンソールからクラスタを作成することもできます。を参照してください "こちらをご覧ください" 手順については、を参照し

ACMを使用してクラスタを作成する場合は、フォームビューで詳細を入力した後で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。クラスタが作成されたら、トラブルシューティングや追加の手動設定のために、クラスタのノードに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 を導入

- 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。手順を参照してください "こちらをご覧ください"。
- コネクタを使用してAWSにCVOインスタンスを導入します。手順を参照してください "こちらをご覧ください"。

> コネクタはクラウド環境にも設置できます。を参照してください "こちらをご覧ください" 追加情報 の場合。

OCPクラスタに**Astra Trident**をインストール

- Helmを使用してTrident Operatorを導入します。手順を参照してください "こちらをご覧ください"
- バックエンドとストレージクラスを作成手順を参照してください "こちらをご覧ください"。

AWSの**OCP**クラスタを**Astra Control Center**に追加します。

AWSのOCPクラスタをAstra Control Centerに追加します。

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

今日のクラウドプロバイダは、Kubernetes / OpenShiftのクラスタ管理者がゾーンベースのクラスタのノードを生成できるようにしています。ノードは、リージョンによって異なるアベイラビリティゾーンに配置することも、リージョンによって配置することもできます。マルチゾーンアーキテクチャでワークロード用のボリュームをプロビジョニングするために、 Astra 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、領域およびアベイラビリティゾーンに基づいて、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。を参照してください "こちらをご覧ください" を参照してください。

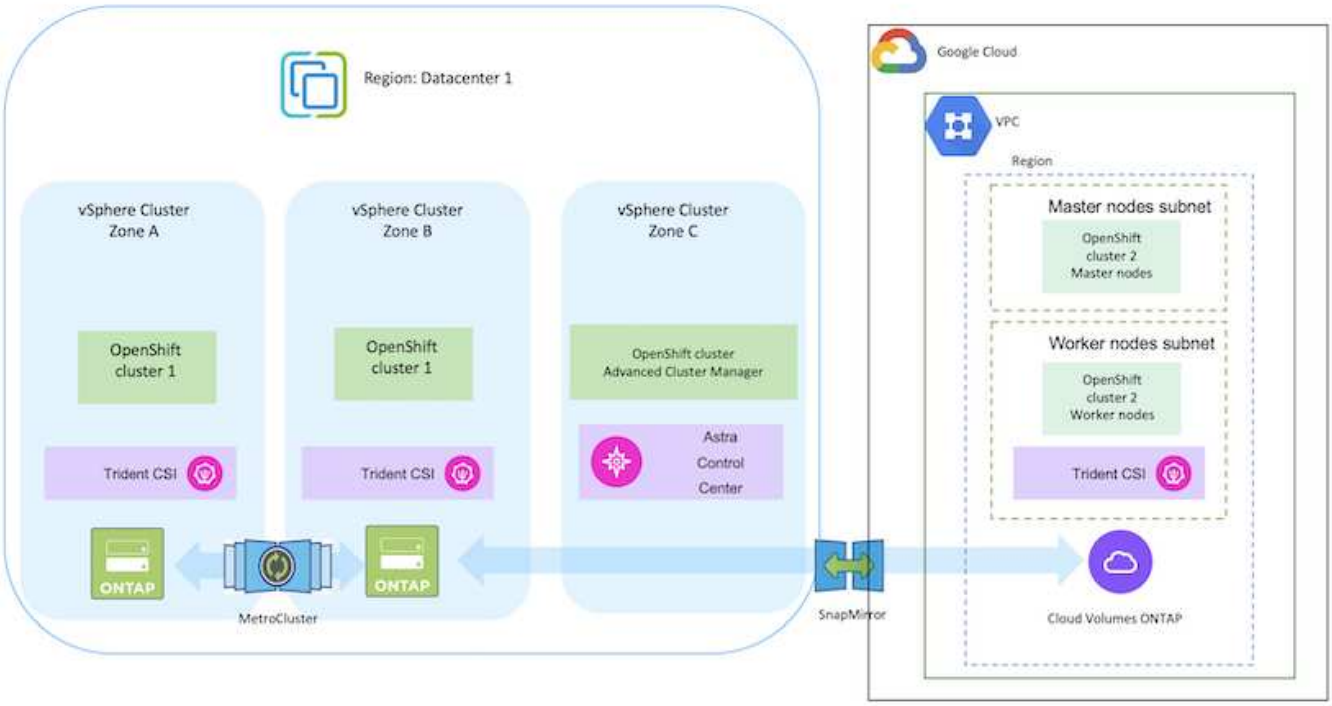
> Kubernetesでは2つのボリュームバインドモードがサポートされます。-***VolumeBindingMode_***が***_Immediate***（デフォルト）に設定されている場合、Astra Tridentはトポロジを認識せずにボリュームを作成します。永続ボリュームは、要求側ポッドのスケジュール要件に依存せずに作成されます。-***VolumeBindingMode_***が***_WaitForFirstConsumer***に設定されている場合、PVCの永続ボリュームの作成とバインドは、そのPVCを使用するポッドがスケジュールされて作成されるまで遅延します。これにより、トポロジの要件に応じたスケジュールの制約を満たすようにボリュームが作成されます。Astra Tridentのストレージバックエンドは、アベイラビリティゾーン（トポロジ対応バックエンド）に基づいて選択的にボリュームをプロビジョニングするように設計できます。ストレージクラスがそのようなバックエンドを使用する場合、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から要求された場合にのみ作成されます。（Topology-Aware StorageClass）を参照してください "こちらをご覧ください" を参照してください。

GCPでのRed Hat OpenShift Containerプラットフォームの導入と設定

GCPでのRed Hat OpenShift Containerプラットフォームの導入と設定

このセクションでは、GCPでOpenShiftクラスタをセットアップおよび管理し、それらにステートフルアプリケーションを導入する方法の概要的なワークフローについて説明します。このスライドでは、Astra Tridentを使用してNetApp Cloud Volumes ONTAP ストレージを使用し、永続ボリュームを提供する方法を示しています。ステートフルアプリケーションに対してデータ保護と移行のアクティビティを実行するためのAstra Control Centerの使用方法について詳しく説明します。

次の図は、GCPに導入され、VPNを使用してデータセンターに接続されたクラスタを示しています。



GCPにRed Hat OpenShift Containerプラットフォームクラスタを導入する方法はいくつかあります。このセットアップの概要概要 には、使用した具体的な方法のドキュメントへのリンクが記載されています。その他の方法については、に記載されている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、次の手順に分けることができます。

CLIから**GCP**に**OCP**クラスタ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ます。 "こちらをご覧ください"。
- オンプレミスとGCP間のVPN接続については、pfsense VMを作成して設定しました。手順については、を参照してください "こちらをご覧ください"。
  - 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設定できます。
  - フェーズ2のリモートネットワークIPアドレスは、OpenShiftクラスタインストールプログラムが実行され、クラスタ用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設定できます。
  - 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設定できます。
- 次に、GCPにOpenShiftクラスタ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入手し、ドキュメントに記載されている手順に従ってクラスタを導入する "こちらをご覧ください"。
  - インストールで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、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。
  - クラスタのインストールが完了し、クラスタのコンソールにログインするためのkubeconfigファイルとユーザ名とパスワードが表示されます。

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

- Google Cloudにコネクタをインストールします。手順を参照してください "こちらをご覧ください"。
- コネクタを使用してGoogle CloudにCVOインスタンスを導入します。手順については、こちら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**Astra Trident**をインストール

- 図に示すように、Astra Tridentにはさまざまな導入方法がある "こちらをご覧ください"。
- このプロジェクトでは、Astra Tridentのオペレータを手順に従って手動で導入し、Astra Tridentをインストールしました。 "こちらをご覧ください"。
- バックエンドとストレージクラスを作成手順を参照してください "こちらをご覧ください"。

GCPの**OCP**クラスタを**Astra Control Center**に追加します。

- クラスタの管理に必要な最小限の権限を含むクラスタロールを含むKubeConfigファイルを別途作成します。手順は次のとおりです。
  "こちらをご覧ください"。
- 手順に従ってクラスタをAstra Control Centerに追加
  "こちらをご覧ください"

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

今日のクラウドプロバイダは、Kubernetes / OpenShiftのクラスタ管理者がゾーンベースのクラスタのノードを生成できるようにしています。ノードは、リージョンによって異なるアベイラビリティゾーンに配置することも、リージョンによって配置することもできます。マルチゾーンアーキテクチャでワークロード用のボリュームをプロビジョニングするために、 Astra 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、領域およびアベイラビリティゾーンに基づいて、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。を参照してください "こちらをご覧ください" を参照してください。

> Kubernetesでは2つのボリュームバインドモードがサポートされます。-***VolumeBindingMode***_が***_Immediate***（デフォルト）に設定されている場合、Astra 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、要求側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の永続ボリュームの作成とバインドは、その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遅延します。これにより、トポロジの要件に応じたスケジュールの制約を満たすようにボリュームが作成されます。Astra Tridentのストレージバックエンドは、アベイラビリティゾーン（トポロジ対応バックエンド）に基づいて選択的にボリュームをプロビジョニングするように設計できます。ストレージクラスがそのようなバックエンドを使用する場合、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から要求された場合にのみ作成されます。（Topology-Aware StorageClass）を参照してください "こちらをご覧ください" を参照してください。

デモビデオ

Google Cloud PlatformへのOpenShiftクラスタのインストール

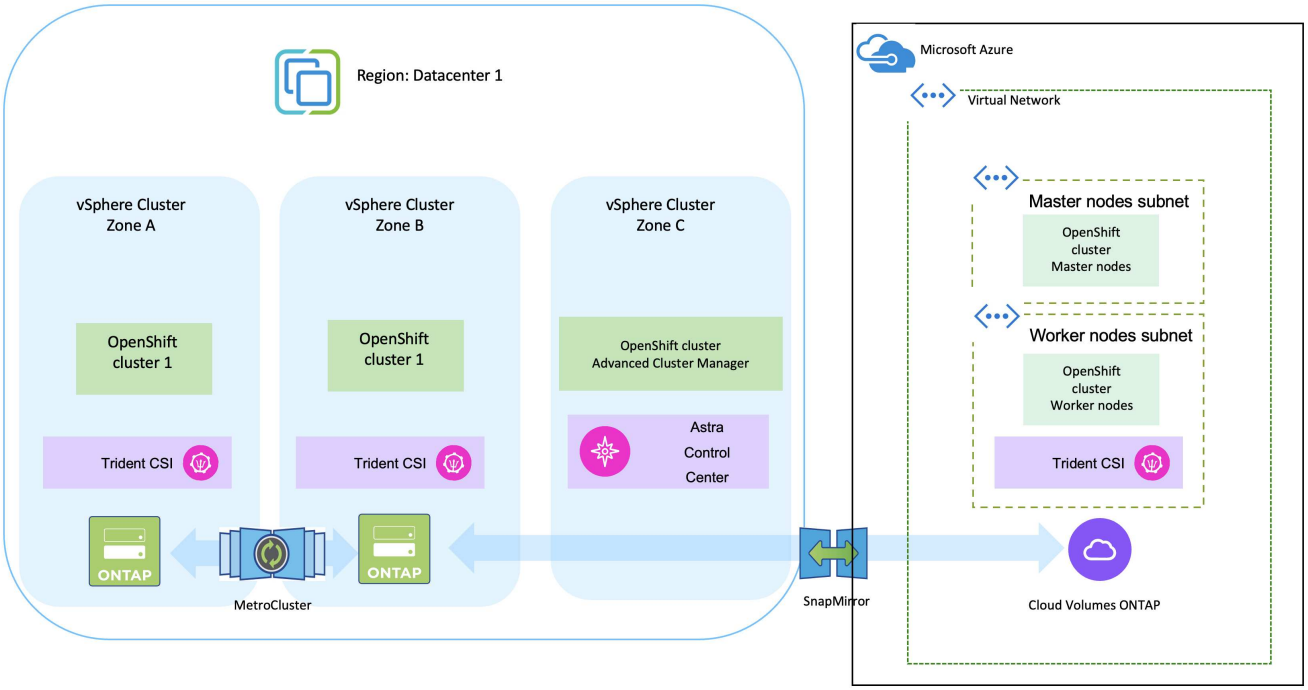
Astra Control CenterへのOpenShiftクラスタのインポート

Azureでの**Red Hat OpenShift Container**プラットフォームの導入と設定

Azureでの**Red Hat OpenShift Container**プラットフォームの導入と設定

このセクションでは、AzureでOpenShiftクラスタをセットアップおよび管理し、それらにステートフルアプリケーションを導入する方法の概要的なワークフローについて説明します。このスライドでは、Astra Trident / Astra Control Provisionerを使用して永続ボリュームを提供するNetApp Cloud Volumes ONTAPストレージを使用しています。ステートフルアプリケーションに対してデータ保護と移行のアクティビティを実行するためのAstra Control Centerの使用方法について詳しく説明します。

次の図は、Azureに導入され、VPNを使用してデータセンターに接続されたクラスタを示しています。



Red Hat OpenShift Containerプラットフォームクラスタを Azureに導入するには、いくつかの方法があります。このセットアップの概要概要 には、使用した具体的な方法のドキュメントへのリンクが記載されています。その他の方法については、に記載されている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、次の手順に分けることができます。

CLIを使用して**Azure**に**OCP**クラスタ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ます。 "こちらをご覧ください"。
- 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ゲートウェイおよびサイト間VPN接続を作成します。
- オンプレミスとAzure間のVPN接続のために、pfsense VMを作成して設定しました。手順については、を参照してください "こちらをご覧ください"。
- インストールプログラムとプルシークレットを入手し、ドキュメントに記載されている手順に従ってクラスタを導入する "こちらをご覧ください"。
- クラスタのインストールが完了し、クラスタのコンソールにログインするためのkubeconfigファイルとユーザ名とパスワードが表示されます。

install-config.yamlファイルの例を以下に示します。

```
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**を導入

- Azureにコネクタをインストールします。手順を参照してください "こちらをご覧ください"。
- コネクタを使用してAzureにCVOインスタンスを導入します。手順リンク：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。

AzureのOCPクラスタへのAstra Control Provisionerのインストール

- このプロジェクトでは、すべてのクラスタ（オンプレミスクラスタ、Astra Control Centerが導入されているオンプレミスクラスタ、およびAzureのクラスタ）にAstra Control Provisioner（ACP）をインストールしました。Astra Control Provisionerの詳細 "こちらをご覧ください"。
- バックエンドとストレージクラスを作成手順を参照してください "こちらをご覧ください"。

AzureのOCPクラスタをAstra Control Centerに追加します。

- クラスタの管理に必要な最小限の権限を含むクラスタロールを含むKubeConfigファイルを別途作成します。手順は次のとおりです。
  "こちらをご覧ください"。
- 手順に従ってクラスタをAstra Control Centerに追加
  "こちらをご覧ください"

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

今日のクラウドプロバイダは、Kubernetes / OpenShiftのクラスタ管理者がゾーンベースのクラスタのノードを生成できるようにしています。ノードは、リージョンによって異なるアベイラビリティゾーンに配置することも、リージョンによって配置することもできます。マルチゾーンアーキテクチャでワークロード用のボリュームをプロビジョニングするために、 Astra 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、領域およびアベイラビリティゾーンに基づいて、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。を参照してください "こちらをご覧ください" を参照してください。

> Kubernetesでは2つのボリュームバインドモードがサポートされます。-***VolumeBindingMode_***が***_Immediate***（デフォルト）に設定されている場合、Astra 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、要求側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の永続ボリュームの作成とバインドは、その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遅延します。これにより、トポロジの要件に応じたスケジュールの制約を満たすようにボリュームが作成されます。Astra Tridentのストレージバックエンドは、アベイラビリティゾーン（トポロジ対応バックエンド）に基づいて選択的にボリュームをプロビジョニングするように設計できます。ストレージクラスがそのようなバックエンドを使用する場合、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から要求された場合にのみ作成されます。（Topology-Aware StorageClass）を参照してください "こちらをご覧ください" を参照してください。

デモビデオ

Astra Controlを使用した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

Astra Control Centerを使用したデータ保護

このページには、VMware vSphereまたはAstra Control Center（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が表示されます。

ユーザがRed Hat OpenShiftを使用してアプリケーションを最新化する過程で、偶発的な削除やその他の人的エラーからユーザ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、データを管理か

ら保護するために、規制やコンプライアンスの目的で保護戦略が必要になります。

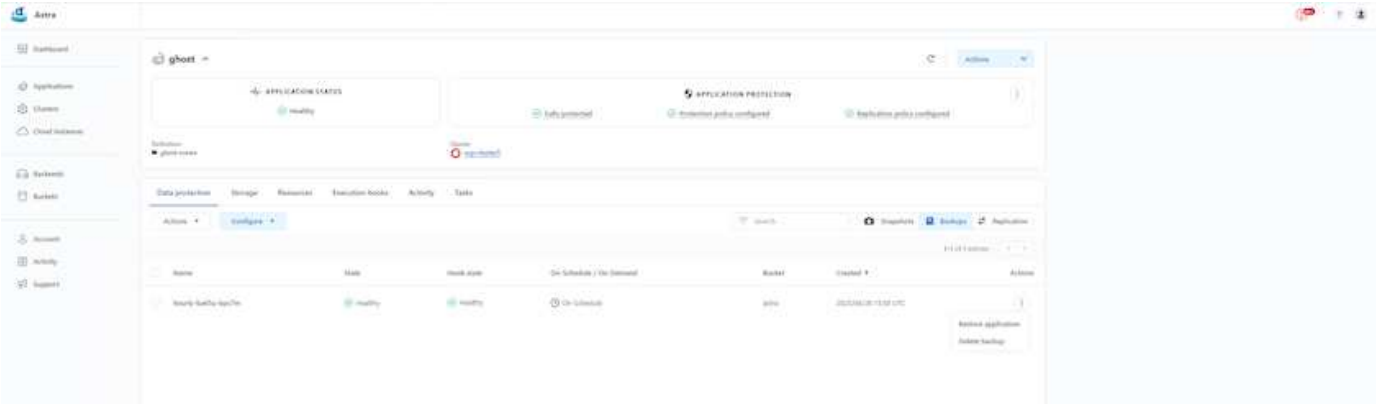
データ保護の要件は、ポイントインタイムコピーへのリバートから別の障害ドメインへの自動フェイルオーバーまで、人手を介さずにさまざまです。多くのお客様がONTAP をKubernetesアプリケーションに最適なストレージプラットフォームとして選択しています。その理由は、マルチテナンシー、マルチプロトコル、ハイパフォーマンスと容量のサービス、マルチサイト環境のレプリケーションとキャッシュ、セキュリティと柔軟性などの豊富な機能があるからです。

お客様は、データセンターの拡張機能としてクラウド環境を設定している場合があります。これにより、クラウドのメリット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ための適切な位置付けを得ることができます。このようなお客様にとって、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ません。その後、アプリケーションと関連データをクラウドまたはデータセンターのOpenShiftクラスタにリストアできます。

ACCを使用した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および更新できます。ACCはCSIを使用してSnapshotコピーを作成し、ポイントインタイムSnapshot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の保護ポリシーと保持するバックアップバージョンの数を設定できます。最小RPOは1時間です。

ACCを使用したバックアップからのアプリケーションのリストア

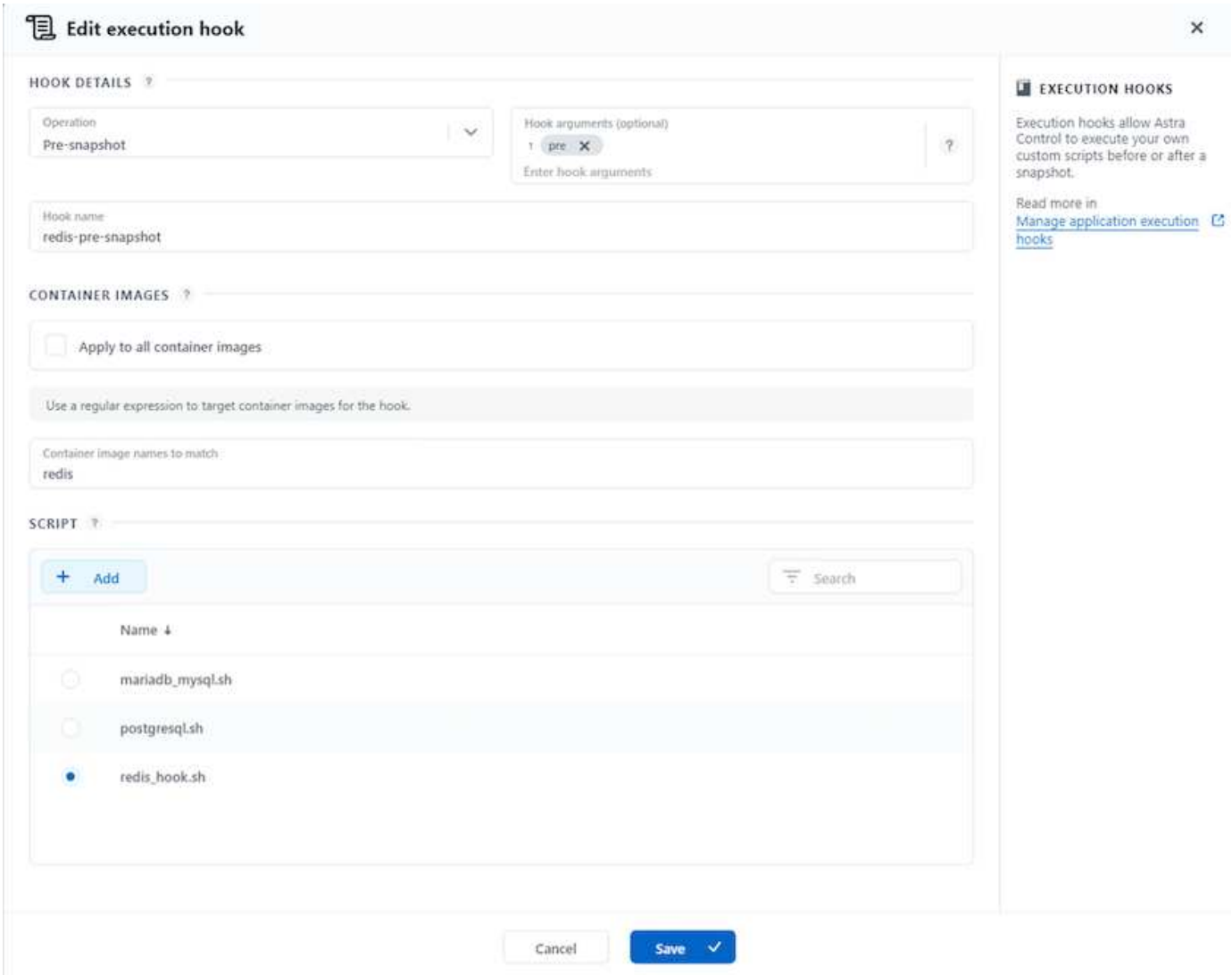


アプリケーション固有の実行フック

ストレージアレイレベルのデータ保護機能を使用できますが、アプリケーションのバックアップとリストアの整合性を確保するために追加の手順が必要になることがよくあります。アプリケーション固有の追加手順は次のとおりです。- Snapshotコピーの作成前または作成後。-バックアップの作成前または作成後。- Snapshotコピーまたはバックアップからリストアしたあと。Astra Controlでは、実行フックと呼ばれるカスタムスクリプトとしてコード化されたアプリケーション固有の手順を実行できます。

ネットアップの "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し、アプリケーションを簡単に保護し、堅牢で、オーケストレーションを容易にします。リポジトリにないアプリケーションに十分な情報がある場合は、そのプロジェクトに貢献してください。

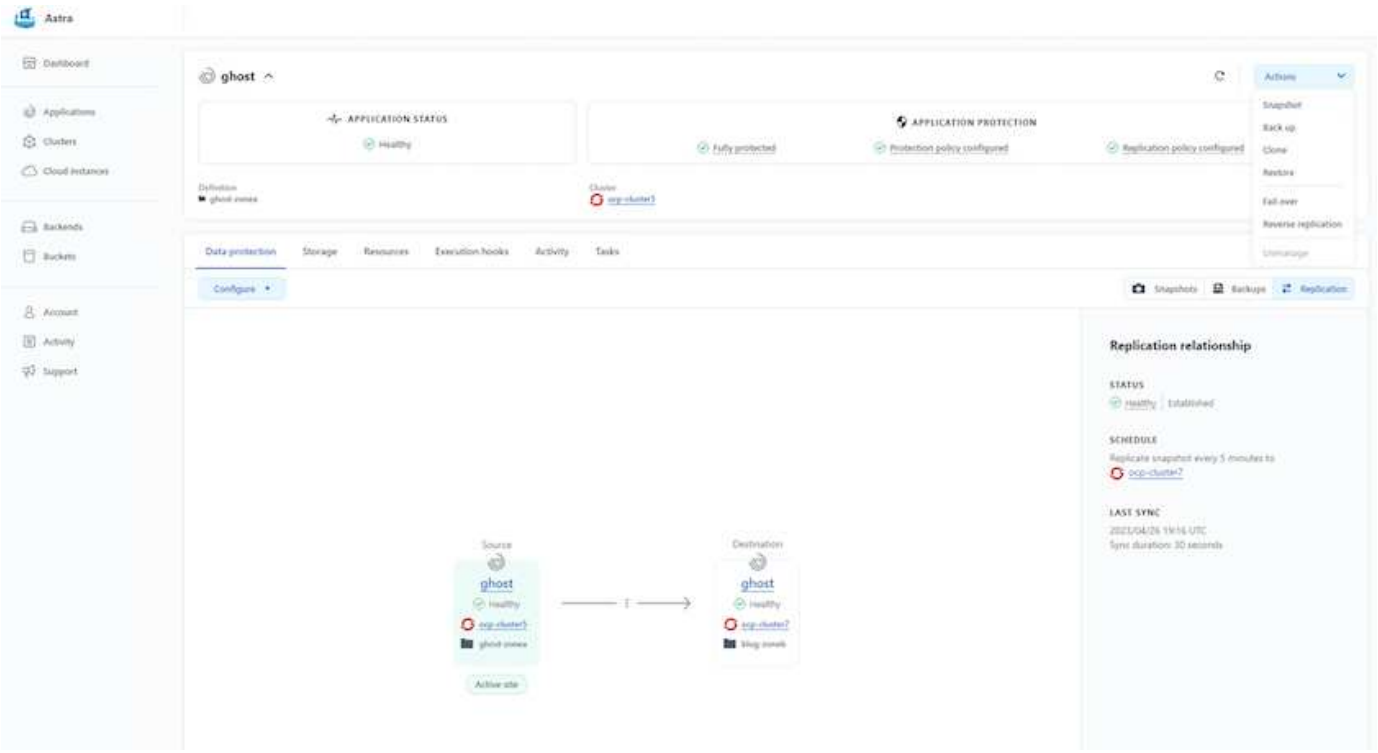
redisアプリケーションのpre-Snapshot用のサンプル実行フック。



ACCを使用したレプリケーション

リージョンを保護する場合や、RPOとRTOの低い解決策 を実現する場合は、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インスタンスにアプリケーションをレプリケートできます。ACCは、最短5分でRPOを実現するONTAP 非同期SnapMirrorを利用します。を参照してください "こちらをご覧ください" SnapMirrorのセットアップ手順を参照してください。

ACCを使用したSnapMirror



SANエコノミーおよびNASエコノミーのストレージドライバは、レプリケーション機能をサポートしていません。を参照してください "こちらをご覧ください" を参照してください。

デモビデオ：

"Astra Control Centerを使用したディザスタリカバリのデモビデオ"

Astra Control Centerによるデータ保護

Astra Control Centerのデータ保護機能の詳細を確認できます "こちらをご覧ください"

ACCを使用したディザスタリカバリ（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）

Astra Controlを使用した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

Astra Control Centerを使用したデータ移行

このページには、Astra Control Center（ACC）を使用したRed Hat OpenShiftクラスタ上のコンテナワークロードのデータ移行オプションが表示されます。具体的には、ACCを使用して、一部のワークロードまたはすべてのワークロードをオンプレミスのデータセンターからクラウドに移動したり、テスト目的でアプリケーションをクラウドにクローニングしたり、データセンターからクラウドに移行したりできます

データ移行

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の次の機能のいずれかを使用できます。

- レプリケーション
- バックアップとリストア
- クローン

を参照してください "データ保護セクション" レプリケーションおよびバックアップとリストアオプションの場合。を参照してください "こちらをご覧ください" クローン作成の詳細については、を参照してください。

> 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、NASエコノミードライバとSANエコノミードライバでは、レプリケーション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