



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	1
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	1
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	3
AWSにRed Hat OpenShift Containerプラットフォームを導入して設定します	5
GCPでのRed Hat OpenShift Containerプラットフォームの導入と設定	7
AzureでのRed Hat OpenShift Containerプラットフォームの導入と設定	10
Astra Control Centerを使用したデータ保護	14
Astra Control Centerを使用したデータ移行	17

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 <ul style="list-style-type: none"> Multi-tenancy FlexVol & FlexGroup LUN Quotas ONTAP CLI & API System Manager & BlueXP 	Performance & Scalability <ul style="list-style-type: none"> FlexCache FlexClone nconnect, session trunking, multipathing Scale-out clusters
Availability & Resilience <ul style="list-style-type: none"> Multi-AZ HA deployment (MetroCluster) SnapShot & SnapRestore SnapMirror SnapMirror Business Continuity (MetroCluster) SnapMirror Cloud 	Access Protocols <ul style="list-style-type: none"> NFS –v3, v4, v4.1, v4.2 SMB – v2, v3 iSCSI Multi-protocol access
Storage Efficiency <ul style="list-style-type: none"> Deduplication & Compression Compaction Thin provisioning Data Tiering (Fabric Pool) 	Security & Compliance <ul style="list-style-type: none"> 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 <ul style="list-style-type: none"> CSI NetApp® Snapshot™ copies and volume creation from CSI Snapshot copies CSI topology Volume expansion 	Security <ul style="list-style-type: none"> Dynamic-export policy management iSCSI initiator-groups dynamic management iSCSI bidirectional CHAP
Control <ul style="list-style-type: none"> Storage and performance consumption Monitoring Volume Import Cross Namespace Volume Access 	Installation methods <ul style="list-style-type: none"> Binary Helm chart Operator GitOps
Choose your access mode <ul style="list-style-type: none"> RWO (ReadWriteOnce, i.e 1↔1) RWX (ReadWriteMany, i.e 1↔n) ROX (ReadOnlyMany) RWOP (ReadWriteOnce POD) 	Choose your protocol <ul style="list-style-type: none"> 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。

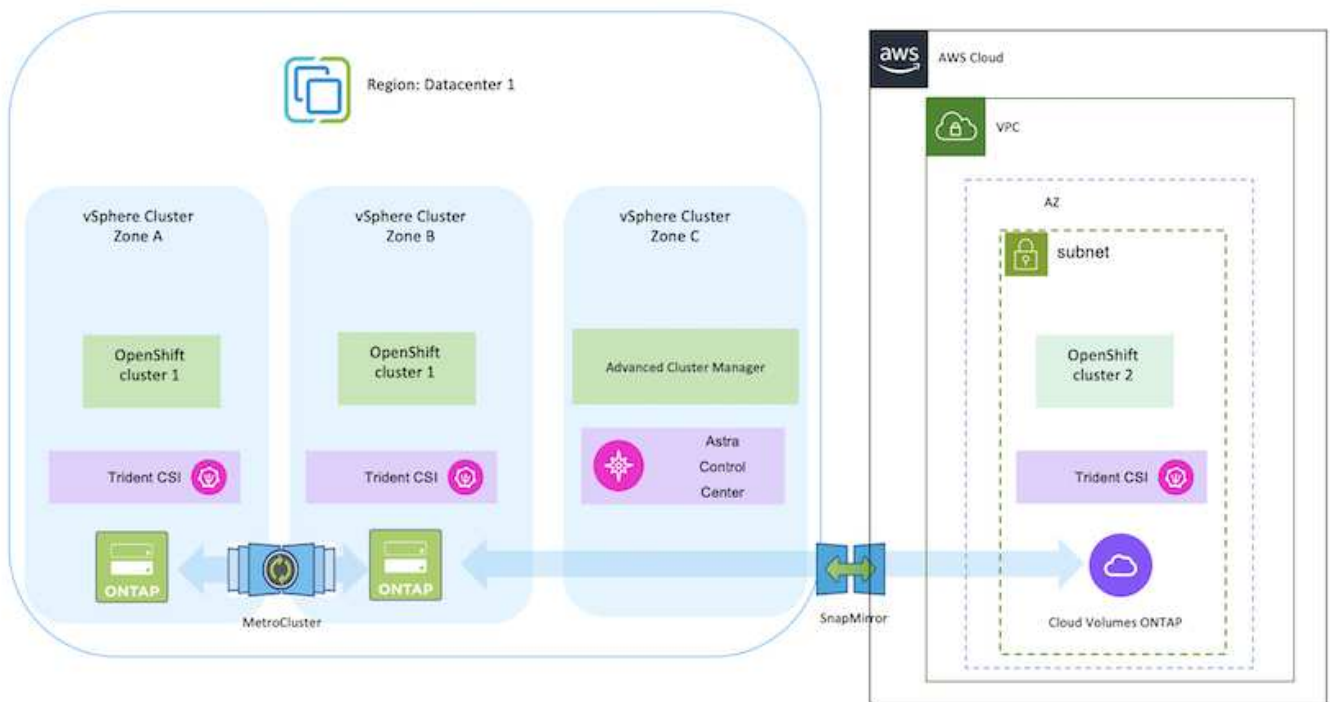
NetApp解決策 とRed Hat OpenShift Containerプラットフォームのワークロードをハイブリッドクラウドで運用

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。

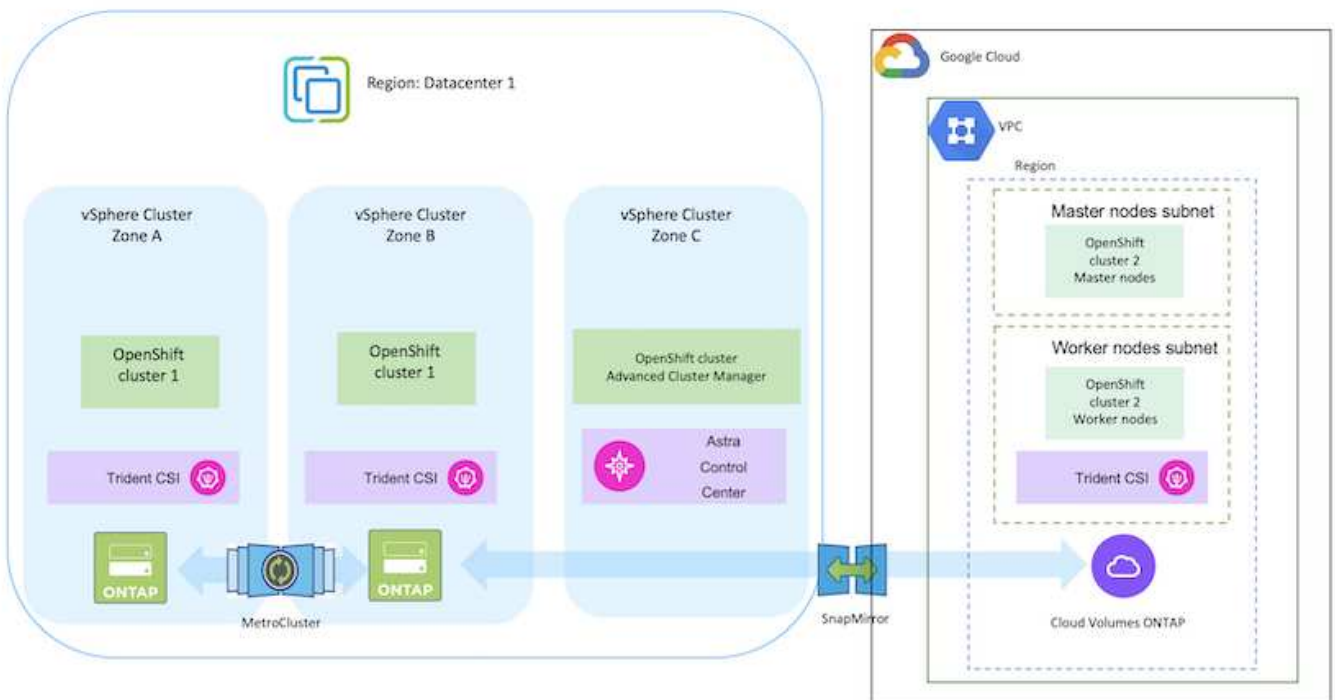
NetApp Cloud Volumes ONTAP ストレージは、AWS、Azure、Google Cloudでのコンテナ導入にデータ保護、信頼性、柔軟性を提供します。Astra Tridentは、お客様のステートフルアプリケーション向けに永続的Cloud Volumes ONTAP ストレージを利用するための動的ストレージプロビジョニングツールとして機能します。Astra Control Centerを使用すると、データ保護、移行、ビジネス継続性など、ステートフルアプリケーションに求められる多くのデータ管理要件をオーケストレーションできます。

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

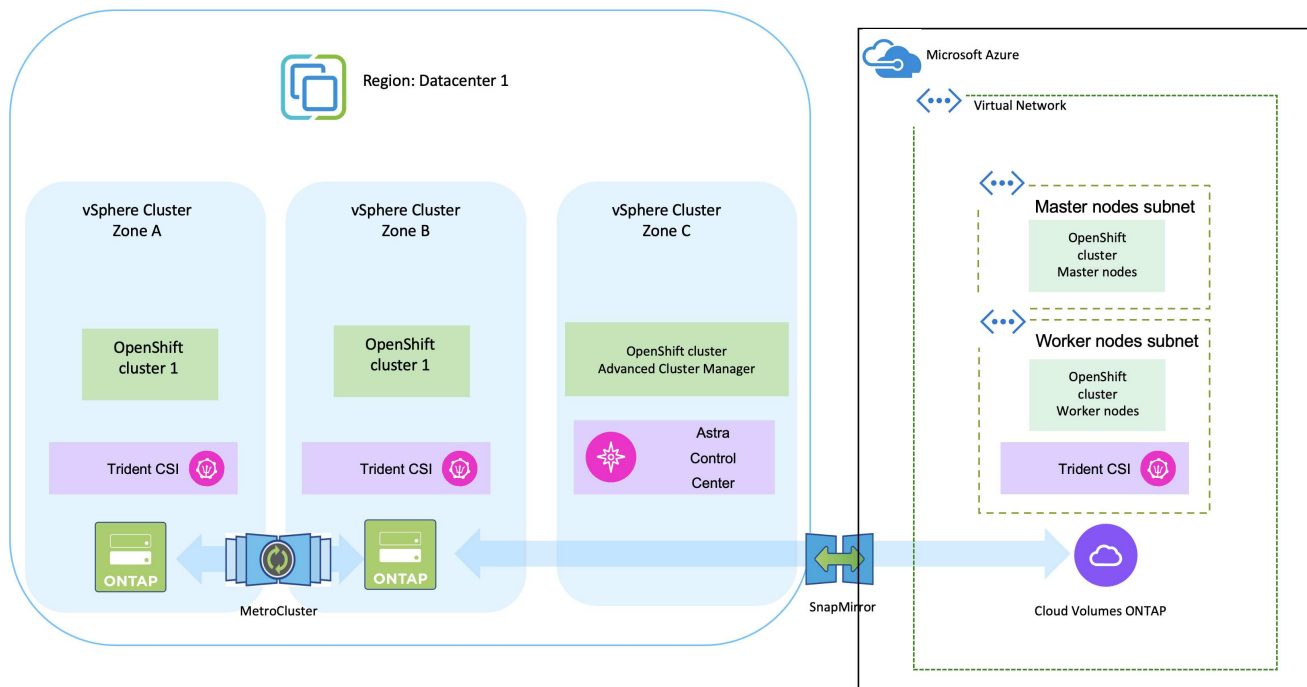
オンプレミスとAWS



オンプレミスとGoogle Cloud



オンプレミスとAzureクラウド



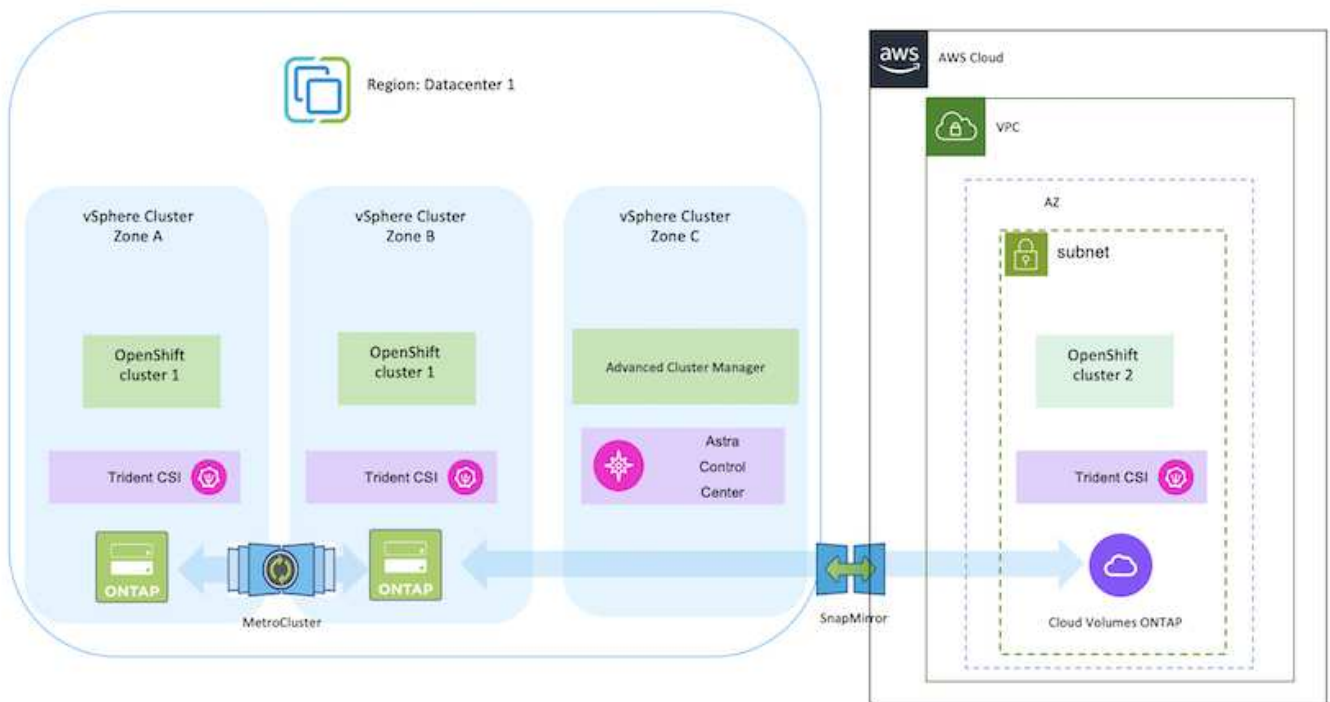
AWSにRed Hat OpenShift Containerプラットフォームを導入して設定します

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。



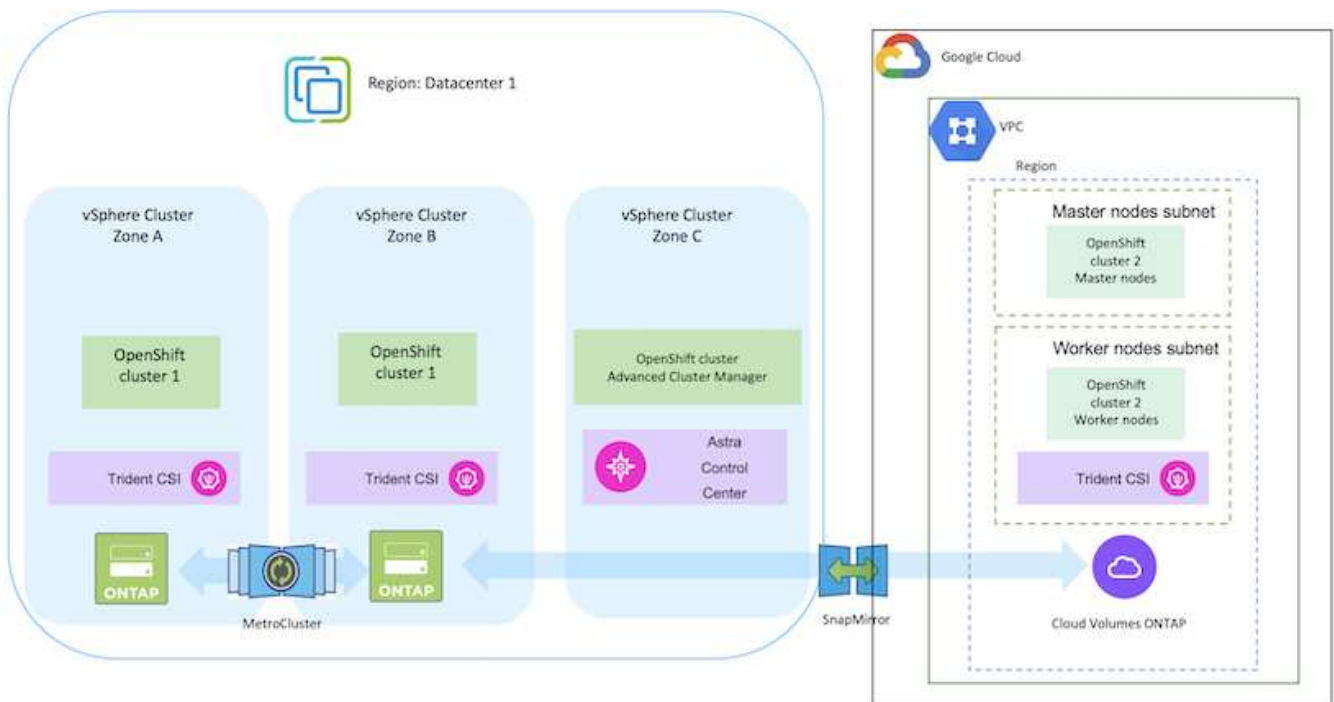
Kubernetesでは2つのボリュームバインドモードがサポートされます。**-VolumeBindingMode_**が **_Immediate** (デフォルト) に設定されている場合、Astra Tridentはトポロジを認識せずにボリュームを作成します。永続ボリュームは、要求側ポッドのスケジュール要件に依存せずに作成されます。**-VolumeBindingMode_**が **_WaitForFirstConsumer**に設定されている場合、PVCの永続ボリュームの作成とバインドは、そのPVCを使用するポッドがスケジュールされて作成されるまで遅延します。これにより、トポロジの要件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](#)

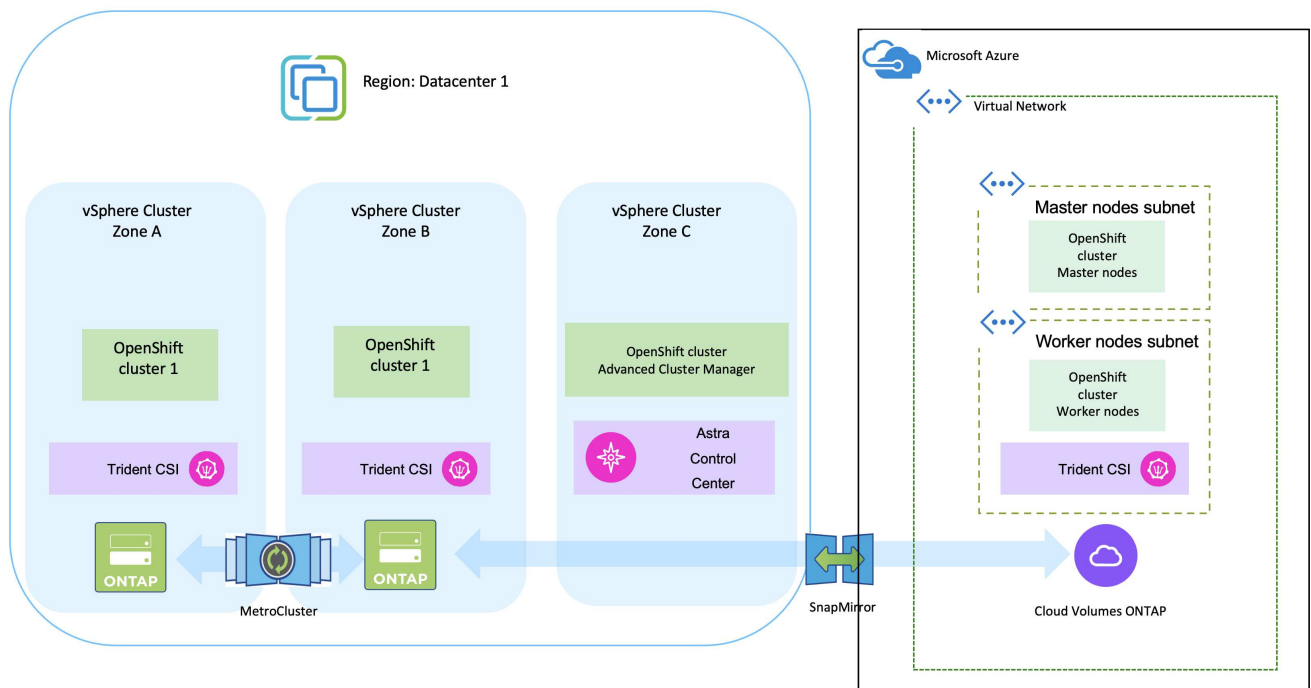
[Astra Control CenterへのOpenShiftクラスタのインポート](#)

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ーを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。

- 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、データを管理が

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。

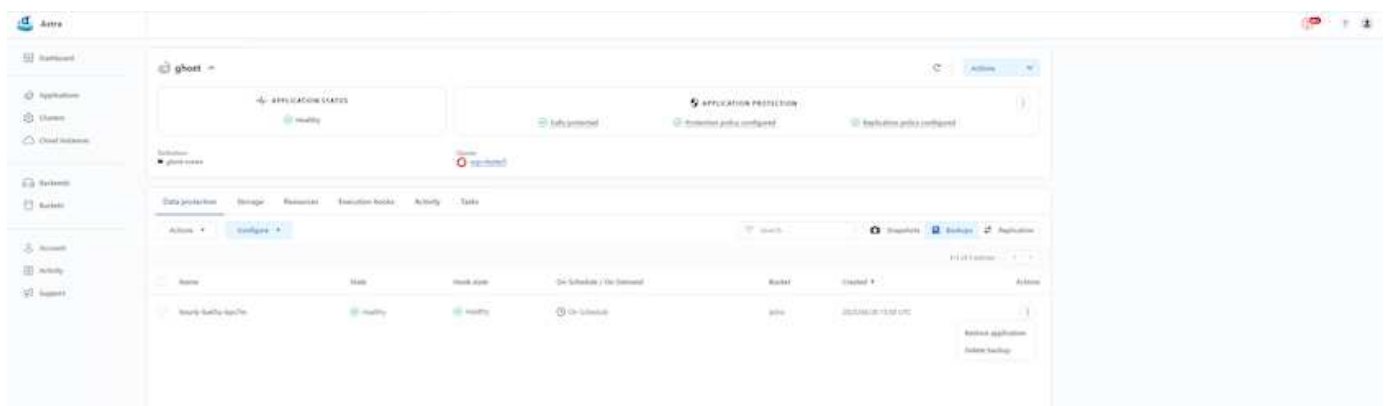
データ保護の要件は、ポイントインタイムコピーへのリバートから別の障害ドメインへの自動フェイルオーバーまで、人手を介さずにさまざまです。多くのお客様がONTAPをKubernetesアプリケーションに最適なストレージプラットフォームとして選択しています。その理由は、マルチテナンシー、マルチプロトコル、ハイパフォーマンスと容量のサービス、マルチサイト環境のレプリケーションとキャッシュ、セキュリティと柔軟性などの豊富な機能があるからです。

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。

Edit execution hook

HOOK DETAILS ?

Operation

Pre-snapshot

Hook arguments (optional)

1 pre X

Enter hook arguments

Hook name

redis-pre-snapshot

CONTAINER IMAGES ?

☐ Apply to all container images

Use a regular expression to target container images for the hook.

Container image names to match

redis

SCRIPT ?

+ Add

Search

Name ↓

☐ mariadb_mysql.sh

☐ postgresql.sh

☒ redis_hook.sh

EXECUTION HOOKS

Execution hooks allow Astra Control to execute your own custom scripts before or after a snapshot.

Read more in [Manage application execution hooks](#)

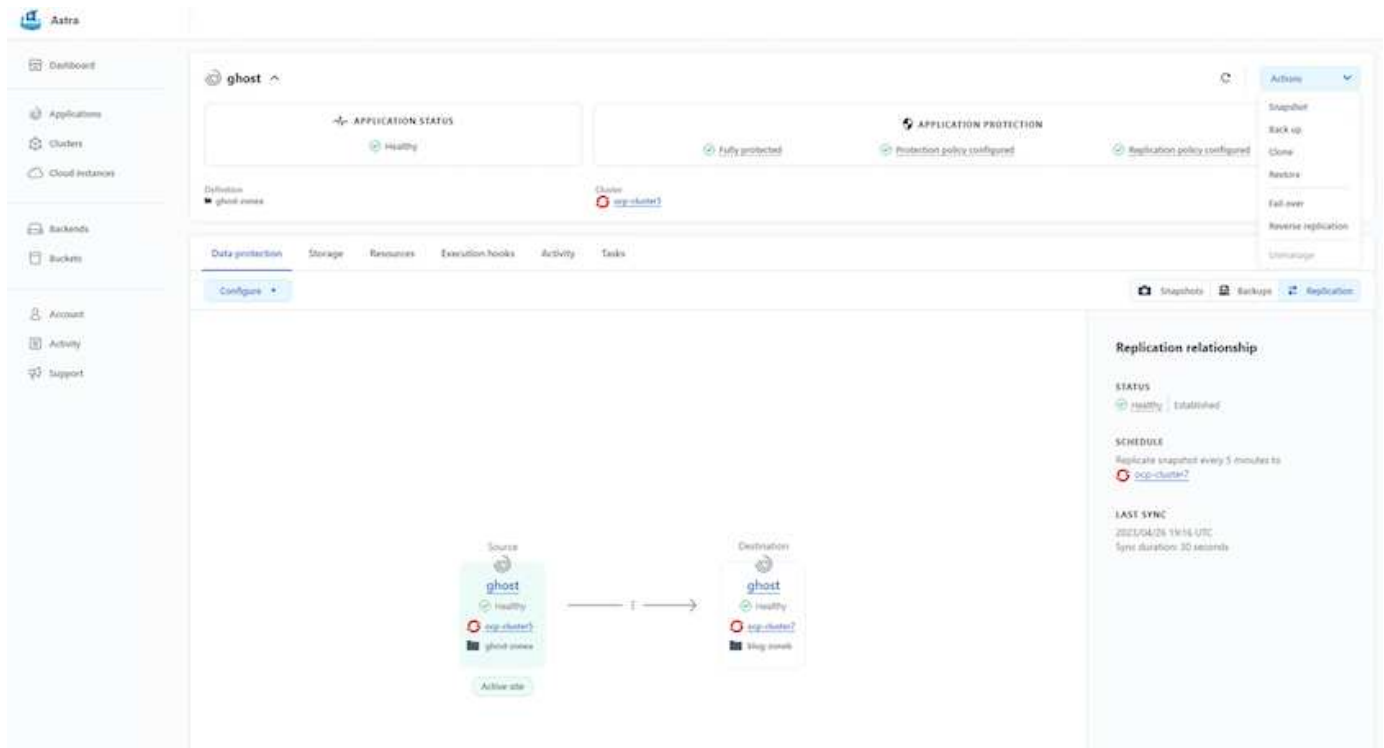
Cancel

Save ✓

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

The screenshot displays the Astra management console interface. On the left is a sidebar with navigation links: Dashboard, Applications, Clusters, Cloud instances, Backends, Buckets, Account, Activity, and Support. The main content area is titled 'ghost' and shows the 'APPLICATION STATUS' as 'Healthy'. Below this, it indicates the 'Destination' is 'ghost-zones' and the 'Cluster' is 'acc-cluster1'. A 'Configure' button is visible. The 'APPLICATION PROTECTION' section shows 'Fully protected', 'Protection policy configured', and 'Replication policy configured'. A 'Replication relationship' panel on the right shows the status as 'Healthy' and 'Established', with a schedule to 'Replicate snapshot every 5 minutes to acc-cluster2'. The 'LAST SYNC' timestamp is '2023/04/28 19:16 UTC' with a 'Sync duration: 30 seconds'. At the bottom, a diagram illustrates the replication relationship between a 'Source' cluster (ghost, acc-cluster1, ghost-zones, Active site) and a 'Destination' cluster (ghost, acc-cluster2, ghost-zones).

著作権に関する情報

Copyright © 2024 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。