



オンプレミス向け**OpenShift**

NetApp public and hybrid cloud solutions

NetApp
February 26, 2026

目次

オンプレミス向けOpenShift	1
VMware 上の Red Hat OpenShift Container プラットフォーム ワークロードを使用した NetAppソリューション	1
Trident Protect を使用した 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	1
VMware 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	2
Astraを使用したデータ保護	4
ACC によるスナップショット	4
ACC によるバックアップと復元	5
アプリケーション固有の実行フック	5
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。	6
ACCによるレプリケーション	6
MetroClusterによるビジネス継続性	7
Trident Protectを使用したデータ移行	8
異なるKubernetes環境間のデータ移行	8

オンプレミス向けOpenShift

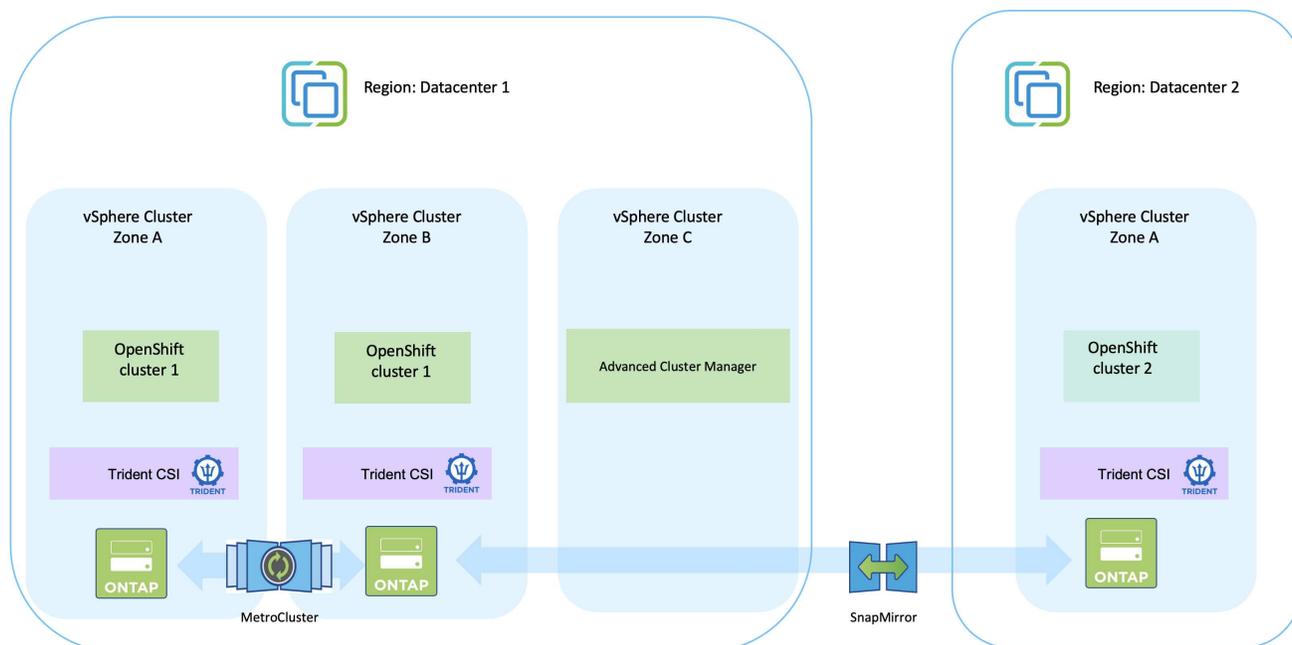
VMware 上の Red Hat OpenShift Container プラットフォーム ワークロードを使用したNetAppソリューション

お客様が最新のコンテナ化されたアプリケーションをプライベート データ センターのインフラストラクチャ上で実行する必要がある場合は、それを行うことができます。コンテナ ワークロードをデプロイするための本番環境を正常に構築するには、Red Hat OpenShift コンテナ プラットフォーム (OCP) を計画してデプロイする必要があります。OCP クラスタは、VMware またはベアメタル上に展開できます。

NetApp ONTAPストレージは、コンテナの導入においてデータ保護、信頼性、柔軟性を実現します。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。NetApp Trident Protect は、データ保護、移行、ビジネス継続性など、ステートフル アプリケーションのさまざまなデータ管理要件に使用できます。

VMware vSphere では、NetApp ONTAPツールは、データストアのプロビジョニングに使用できる vCenter プラグインを提供します。タグを適用し、OpenShift で使用してノード構成とデータを保存します。NVMe ベースのストレージは、低レイテンシと高パフォーマンスを実現します。

Trident Protect を使用した 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



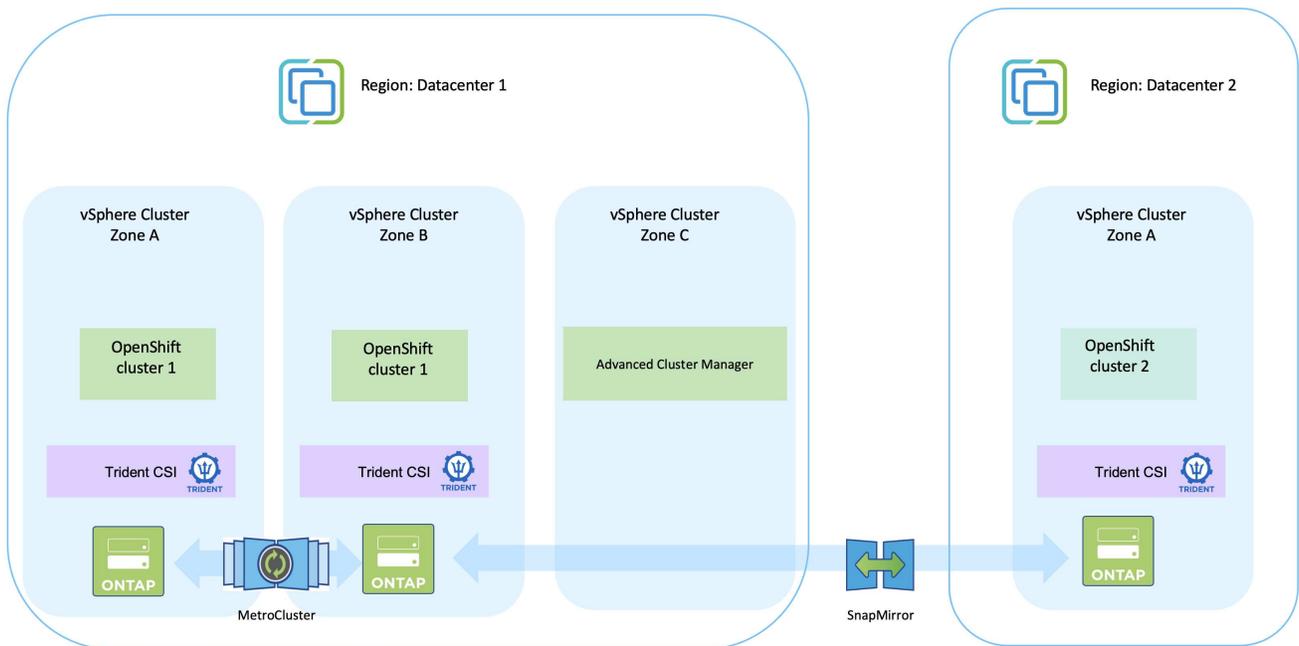
VMware 上で Red Hat OpenShift Container プラットフォームをデプロイおよび構成する

このセクションでは、OpenShift クラスターをセットアップおよび管理し、その上でステートフル アプリケーションを管理する方法の大き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 ONTAPストレージ アレイの使用法を示しています。



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、データセンター内の VMware に展開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。

CentOS VMのデプロイと構成

- VMware vSphere 環境に展開されます。
- この VM は、ソリューションのNetApp TridentやNetApp Trident Protect などのコンポーネントを展開するために使用されます。
- インストール中にこの VM にルート ユーザーが構成されます。

VMware vSphere (ハブ クラスター) 上に OpenShift Container Platform クラスターをデプロイして構成する

の説明書を参照してください["支援展開"](#)OCP クラスターをデプロイする方法。



次の点に注意してください: - インストーラーに提供する ssh 公開キーと秘密キーを作成します。これらのキーは、必要に応じてマスターノードとワーカーノードにログインするために使用されます。 - アシストインストーラーからインストーラー プログラムをダウンロードします。このプログラムは、マスター ノードとワーカー ノード用に VMware vSphere 環境で作成した VM を起動するために使用されます。 - VM には最低限の CPU、メモリ、ハード ディスクの要件が必要です。 (vm createコマンドについては、["事項を"](#)この情報を提供するマスター ノードとワーカー ノードのページ - すべての VM でディスク UUID を有効にする必要があります。 - マスター用に最低 3 つのノード、ワーカー用に最低 3 つのノードを作成します。 - インストーラーによって検出されたら、VMware vSphere 統合トグル ボタンをオンにします。

ハブクラスタに高度なクラスタ管理をインストールする

これは、ハブ クラスター上の Advanced Cluster Management Operator を使用してインストールされます。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。"](#)

2つの追加のOCPクラスタ（ソースと宛先）をインストールする

- 追加のクラスターは、ハブ クラスター上の ACM を使用してデプロイできます。
- 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。"](#)

NetApp ONTAPストレージを構成する

- VMWare 環境内の OCP VM に接続できるONTAPクラスターをインストールします。
- SVMを作成する
- SVM 内のストレージにアクセスできるように NAS データ ライフを設定します。

OCP クラスタにNetApp Tridentをインストールする

- ハブ、ソース、および宛先クラスタの3つのクラスタすべてにNetApp Trident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。"](#)
- ontap-nas のストレージ バックエンドを作成します。
- ontap-nas のストレージ 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。"](#)

ソースクラスタにアプリケーションをデプロイする

OpenShift GitOps を使用してアプリケーションをデプロイします。(例: Postgres、Ghost)

次のステップは、Trident Protect を使用してデータ保護と、ソース クラスタから宛先クラスタへのデータ移行を行うことです。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。

Astraを使用したデータ保護

このページでは、Trident Protect (ACC) を使用して VMware vSphere 上で実行されている 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。

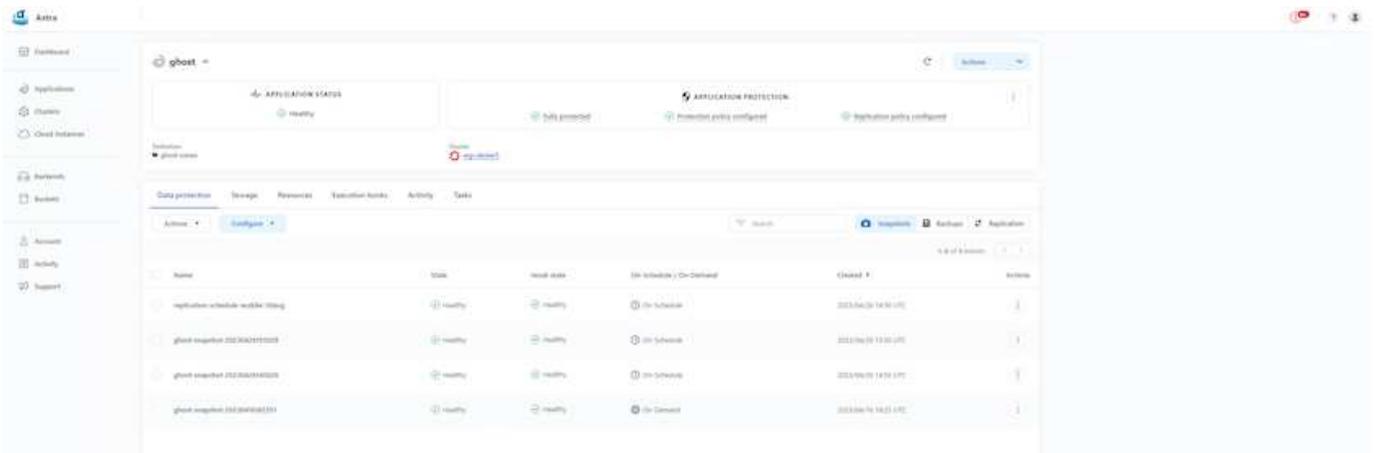
ONTAP のデータ保護は、アドホックまたはポリシー制御のスナップショット、バックアップとリストアを使用して実現できます。

スナップショット コピーとバックアップはどちらも、次の種類のデータを保護します: - アプリケーションの状態を表すアプリケーション メタデータ - アプリケーションに関連付けられた永続データ ボリューム - アプリケーションに属するリソース アーティファクト

ACC によるスナップショット

ACC を使用したスナップショットを使用して、データの特定期間のコピーをキャプチャできます。保護ポリシーは、保持するスナップショット コピーの数を定義します。利用可能な最小スケジュール オプションは時間単位です。手動のオンデマンド Snapshot コピーは、いつでも、スケジュールされた Snapshot コピーよりも短い間隔で作成できます。スナップショット コピーは、アプリと同じプロビジョニングされたボリュームに保存されます。

ACC を使用したスナップショットの設定

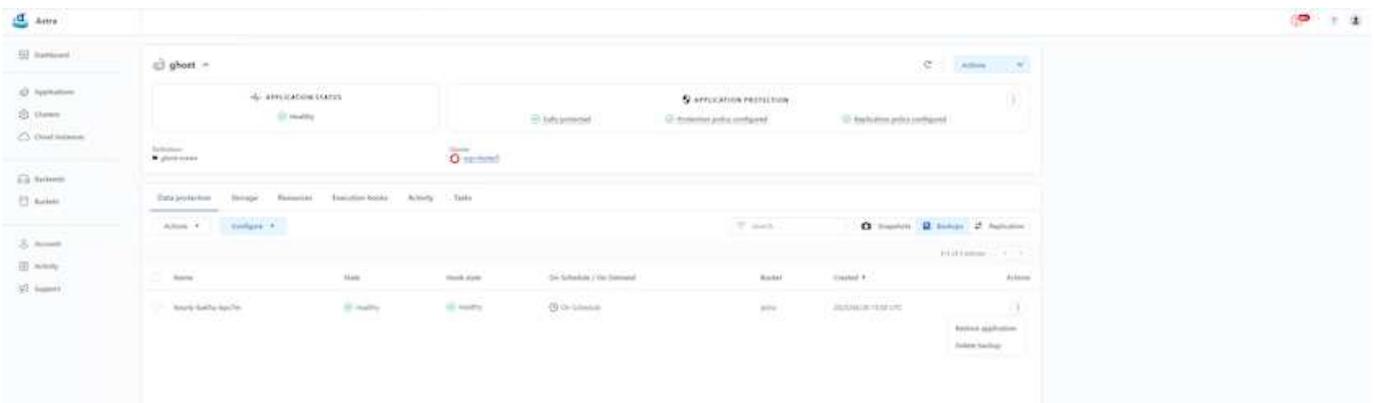


ACC によるバックアップと復元

バックアップはスナップショットに基づいています。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。バックアップは外部オブジェクト ストア (別の場所にあるONTAP S3 を含む、S3 と互換性のある任意のストア) に保存されます。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

ACC は、バックアップが保存されている S3 バケットからアプリケーションを復元します。



アプリケーション固有の実行フック

さらに、実行フックは、管理対象アプリのデータ保護操作と組み合わせて実行するように構成できます。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、アプリケーションの一貫性を保ちながらバックアップと復元を行うには、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としては、次のものが考えられます: - 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。

Astra Control 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 Verda GitHub プロジェクト"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。

Edit execution hook

HOOK DETAILS

Operation: Pre-snapshot

Hook arguments (optional): 1 pre

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
<input type="radio"/> mariadb_mysql.sh
<input type="radio"/> postgresql.sh
<input checked="" type="radio"/> redis_hook.sh

Cancel Save

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](#)

ACCによるレプリケーション

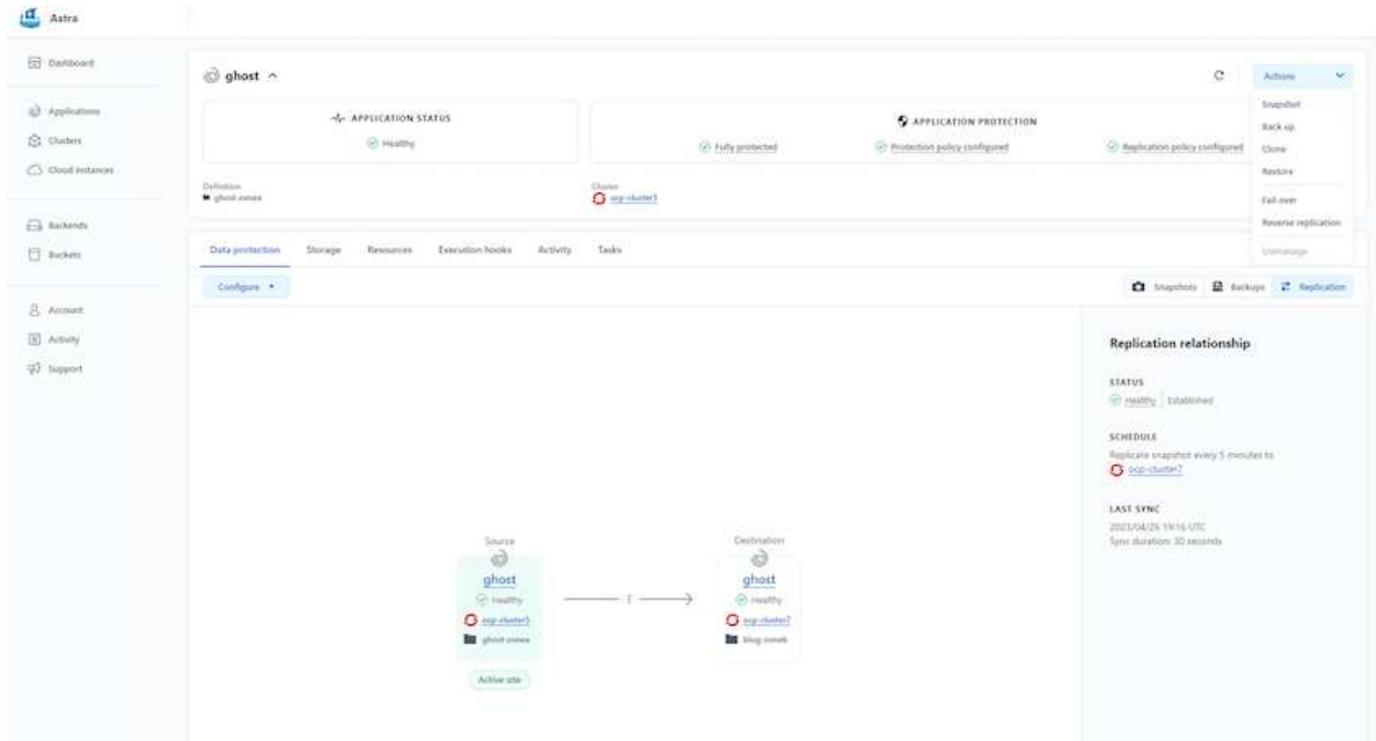
リージョン保護や RPO および RTO が低いソリューションの場合、アプリケーションを別のサイト (できれば別のリージョン) で実行されている別の Kubernetes インスタンスに複製できます。Trident Protect は、最短 5 分の RPO で ONTAP 非同期 SnapMirror を活用します。レプリケーションは ONTAP にレプリケートすることによって実行され、その後フェイルオーバーによって宛先クラスターに Kubernetes リソースが作成されます。



レプリケーションは、バックアップが S3 に保存され、復元が S3 から実行されるバックアップと復元とは異なることに注意してください。2種類のデータ保護の違いについての詳細は、<https://docs.netapp.com/us-en/astra-control-center/concepts/data-protection.html#replication-to-a-remote-cluster>[こちら]のリンクを参照してください。

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](#)

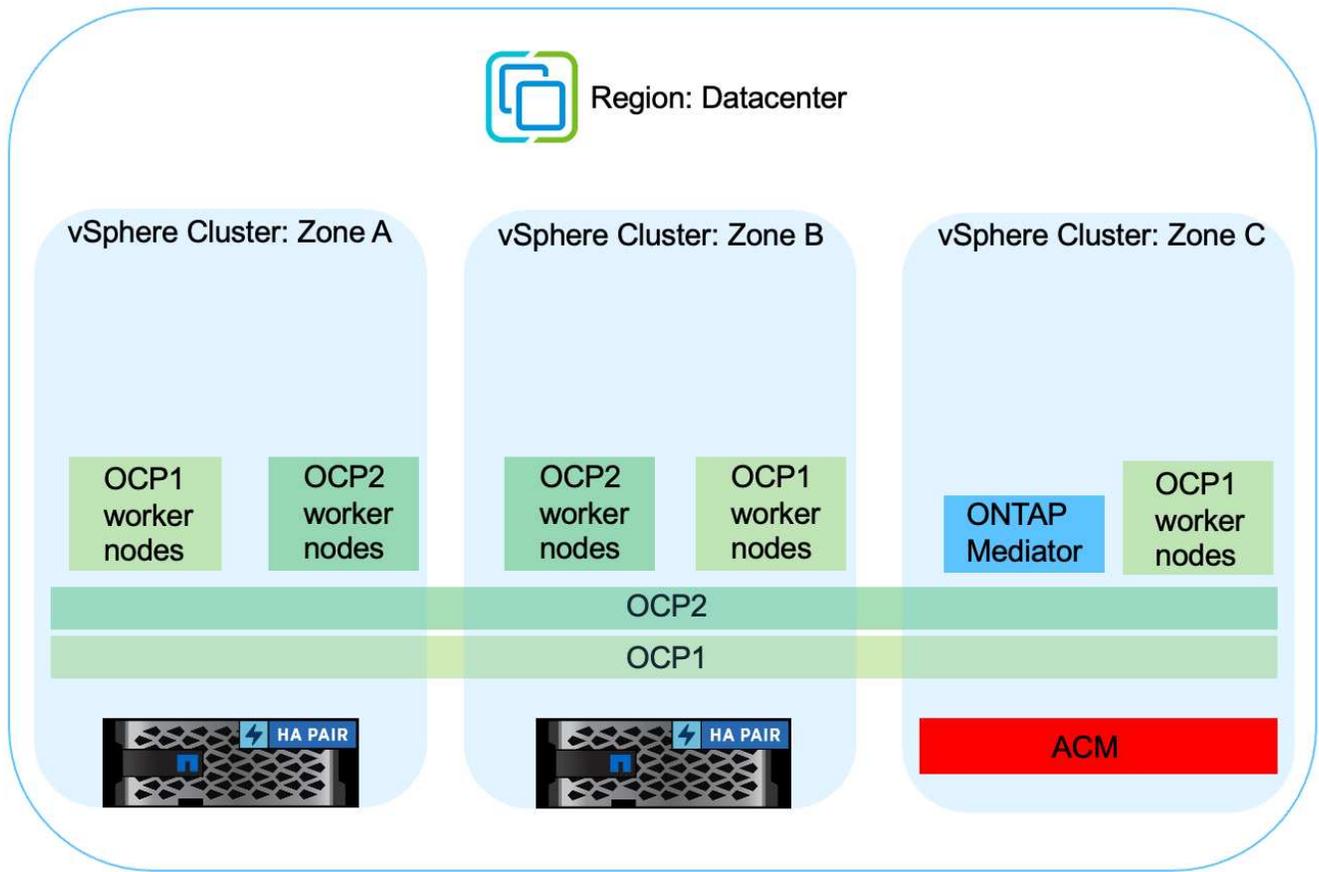
MetroClusterによるビジネス継続性

ONTAP向けの当社のハードウェア プラットフォームのほとんどには、デバイス障害から保護し、災害復旧を実行する必要性を回避する高可用性機能が備わっています。しかし、火災やその他の災害から保護し、RPO ゼロ、RTO の低さでビジネスを継続するために、MetroClusterソリューションが使用されることがよくあります。

現在ONTAPシステムをお持ちのお客様は、距離制限内でサポートされているONTAPシステムを追加することでMetroClusterに拡張し、ゾーン レベルの災害復旧を提供できます。Trident、CSI (Container Storage Interface) は、MetroCluster構成を含むNetApp ONTAPのほか、Cloud Volumes ONTAP、Azure NetApp Files、AWS FSx ONTAPなどのオプションもサポートします。TridentはONTAP用に5つのストレージ ドライバー オプションを提供し、すべてMetroCluster構成でサポートされています。参照する["ここをクリックしてください。"](#)TridentでサポートされているONTAPストレージ ドライバーの詳細については、[を参照してください。](#)

MetroClusterソリューションでは、レイヤー 2 ネットワーク拡張または両方の障害ドメインから同じネットワーク アドレスにアクセスする機能が必要です。MetroCluster構成が設定されると、MetroCluster SVM 内のすべてのボリュームが保護され、SyncMirror (ゼロ RPO) の利点を得られるため、ソリューションはアプリケー

ション所有者に対して透過的になります。



Tridentバックエンド構成 (TBC) の場合、MetroCluster構成を使用するときは、dataLIF と SVM を指定しないでください。管理LIF の SVM 管理 IP を指定し、vsadmin ロールの資格情報を使用します。

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。"](#)

Trident Protectを使用したデータ移行

このページでは、Trident Protect 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について説明します。

Kubernetes アプリケーションは、多くの場合、ある環境から別の環境に移動する必要があります。アプリケーションとその永続データを移行するには、NetApp Trident Protect を利用できます。

異なるKubernetes環境間のデータ移行

ACCは、Google Anthos、Red Hat OpenShift、Tanzu Kubernetes Grid、Rancher Kubernetes Engine、Upstream Kubernetesなど、さまざまなKubernetesフレーバーをサポートしています。詳細については、["ここをクリックしてください。"](#)

アプリケーションをあるクラスターから別のクラスターに移行するには、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-op-data-protection.html](https://docs.netapp.com/us-en/astra-control-center/use/clone-apps.html)**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>**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。**

ACC を使用したデータ複製の実行

The screenshot displays the Astra Control Center interface for an application named 'ghost'. The main view shows the 'Data protection' tab, which includes a 'Replication relationship' section. This section details the replication status and schedule. Below this, a diagram illustrates the replication relationship between two 'ghost' application instances, labeled 'Source' and 'Destination'. Both instances are shown as 'Healthy' and 'Established'. The 'Source' instance is associated with the cluster 'osp-cluster1' and the 'ghost' namespace. The 'Destination' instance is associated with the cluster 'osp-cluster2' and the 'ghost' namespace. The replication relationship is shown as a bidirectional arrow between the two instances.

Replication relationship

STATUS
Healthy | Established

SCHEDULE
Replicate snapshot every 5 minutes to
osp-cluster2

LAST SYNC
2023/04/26 19:14 UTC
Sync duration: 30 seconds

著作権に関する情報

Copyright © 2026 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。