



コンテナ NetApp Solutions

NetApp
September 10, 2024

目次

ネットアップのコンテナソリューション	1
NVA-1165：ネットアップを使用したAnthos	1
TR-4919：『DevOps with NetApp Astra』	34
NVA-1160：ネットアップでの Red Hat OpenShift	63
NVA-1166：ネットアップを使用したVMware Tanzuの評価	266
アーカイブされたソリューション	312

ネットアップのコンテナソリューション

NVA-1165：ネットアップを使用したAnthos

ネットアップBanu SundharとSuresh Thoppay

このリファレンスガイドで解決策は、ネットアップとエンジニアリングパートナーの協力のもと、Anthosを複数のデータセンター環境に導入する際の検証について説明します。また、ネットアップストレージシステムとのストレージ統合の詳細についても、Astra Tridentストレージオーケストレーションツールを使用して永続的ストレージを管理する方法を紹介しています。最後に、解決策 検証と実際のユースケースをいくつか確認して文書化します。

ユースケース

NetApp解決策 を搭載したAnthosは、以下のユースケースでお客様に卓越した価値を提供するように設計されています。

- ベアメタル上の「bmctl」ツールまたはVMware vSphere上の「gkectl」ツールを使用して展開されたAnthos環境の導入と管理が容易になります。
- エンタープライズコンテナと仮想化ワークロードのパワーを、vSphere上またはベアメタル上に仮想的に導入されたAnthosで活用できます ["Kubevirt"](#)。
- ネットアップストレージとKubernetes向けオープンソースストレージオーケストレーションツールであるAstra Tridentとともに使用されるAnthosの特徴を強調した実際の構成とユースケース

ビジネスバリュー

企業は、新しい製品の作成、リリースサイクルの短縮、新機能の迅速な追加を目的として、DevOps の手法を採用する傾向に迫られています。即応性に優れた本来の性質から、コンテナやマイクロサービスは、DevOps の実践を支援するうえで重要な役割を果たします。しかし、エンタープライズ環境で本番環境規模でDevOps を実践する場合、独自の課題が生じ、基盤となるインフラに次のような一定の要件が課せられます。

- スタック内のすべてのレイヤで高可用性を実現します
- 導入手順の簡易化
- ノンストップオペレーションとアップグレード
- API ベースのプログラム可能なインフラで、マイクロサービスの即応性を維持します
- パフォーマンスを保証するマルチテナンシー
- 仮想ワークロードとコンテナ化されたワークロードを同時に実行できます
- ワークロードのニーズに応じてインフラを個別に拡張できること

NetApp解決策 を搭載したAnthosは、このような課題に対応し、お客様のデータセンター環境にオンプレミス環境に完全に自動化された導入を実装することで、それぞれの問題に対処できる解決策 を提供します。

テクノロジーの概要

NetApp解決策 を搭載したAnthosは、以下の主要コンポーネントで構成されています。

オンプレミスのAnthos

オンプレミスのAnthosは、VMware vSphereハイパーバイザーや、選択したベアメタルインフラに導入可能な、完全にサポートされているエンタープライズ向けKubernetesプラットフォームです。

Anthos の詳細については、Anthos の Web サイトを参照してください "[こちらをご覧ください](#)"。

ネットアップストレージシステム

ネットアップには、エンタープライズデータセンターやハイブリッドクラウド環境に最適なストレージシステムが複数あります。ネットアップのポートフォリオには、NetApp ONTAP ストレージシステム用のNetApp ONTAP、Cloud Volumes ONTAP、Cloud Volumes Service、Azure NetApp Files、FSxNが含まれており、いずれもコンテナ化されたアプリケーション用の永続的ストレージを提供できます。

詳細については、ネットアップの Web サイトをご覧ください "[こちらをご覧ください](#)"。

ネットアップとストレージの統合

Astra Tridentは、オープンソースで、Anthosを含むコンテナやKubernetesディストリビューション向けの完全にサポートされているストレージオーケストレーションツールです。

詳細については、Astra Trident の Web サイトをご覧ください "[こちらをご覧ください](#)"。

Advanced Configuration Options（詳細設定オプション）

このセクションは、実環境のユーザがこの解決策を本番環境に導入するときに実行する必要があるカスタマイズ（専用のプライベートイメージレジストリの作成やカスタムロードバランサインスタンスの導入など）に特化したものです。

検証済みリリースの現在のサポートマトリックスです

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。

Anthosの概要

ネットアップのAnthosは、信頼性に優れた信頼性の高い方法でオンプレミスのGoogle Kubernetes Engine（GKE）環境を導入するための、検証済みのベストプラクティスに基づくハイブリッドクラウドアーキテクチャです。このNetApp Verified Architectureリファレンスドキュメントは、NetApp解決策 をベアメタル環境と仮想環境に導入した場合のAnthosの設計ガイドと導入検証の両方を対象としています。本ドキュメントで説明しているアーキテクチャは、ネットアップとGoogle Cloudのエキスパートによる検証を受けたもので、エンタープライズデータセンター環境でAnthosを実行するメリットを提供します。

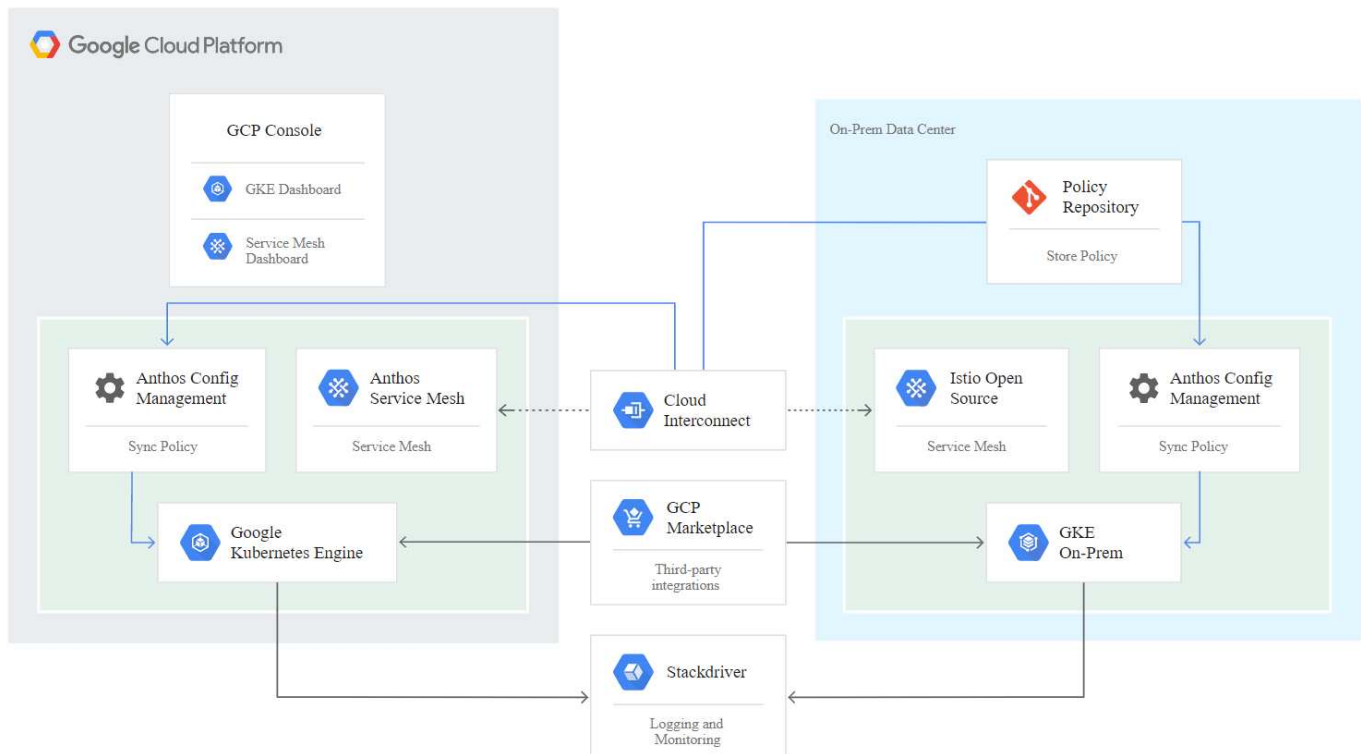
Anthos の場合

Anthosは、Kubernetesを使用したハイブリッドクラウド対応データセンター解決策です。最新のハイブリッドクラウドインフラを構築、管理しつつ、アプリケーション開発に重点を置いた即応性に優れたワークフローを採用できます。オープンソーステクノロジーを基盤とした解決策を基盤とする Anthos は、VMware vSphere ベースのインフラにオンプレミスで稼働し、Google Cloud の Anthos GKE との接続と相互運用が可能です。コンテナ、サービスメッシュ、その他の変革テクノロジーを採用することで、ローカルおよびクラウドベースの環境で一貫したアプリケーション開発サイクルと本番環境対応のワークロードを体験できるようになります。次の図は、Anthos 解決策と、オンプレミスのデータセンターに導入し、クラウドのインフラと相互接続する方法を示しています。

Anthos の詳細については、Anthos の Web サイトを参照してください ["こちらをご覧ください"](#)。

Anthos には次のような機能があります。

- * Anthos の構成管理。* ハイブリッド Kubernetes 環境のポリシーとセキュリティを自動化します。
- * Anthos サービスメッシュ * は、Istio 電源のサービスメッシュにより、アプリケーションのオブザーバビリティ、セキュリティ、および制御を強化します。
- * Google Cloud Marketplace for Kubernetes Applications 。* キュレーションされたコンテナアプリケーションのカタログを利用して、簡単に導入できます。
- * Anthos * に移行。オンプレミスからクラウドへの物理サービスと VM の自動移行を実現します。
- * Stackdriver. * クラウド・インスタンスのロギングと監視のために Google が提供する管理サービス。



Anthosの導入方法

VMware上のAnthosクラスタ

VMware vSphere環境に導入されるAnthosクラスタは、ほとんどのエンドユーザー向けKubernetesワークロード

の導入、保守、拡張が容易です。

ネットアップとともに導入されるVMware上のAnthosクラスタの詳細については、このページを参照してください ["こちらをご覧ください"](#)。

ベアメタルの Anthos

ベアメタルサーバに導入されたAnthosクラスタはハードウェアに依存しないため、お客様に合わせて最適化されたコンピューティングプラットフォームを選択できます。

ネットアップとともに導入されたベアメタルクラスタ上のAnthosの詳細については、を参照してください ["こちらをご覧ください"](#)。

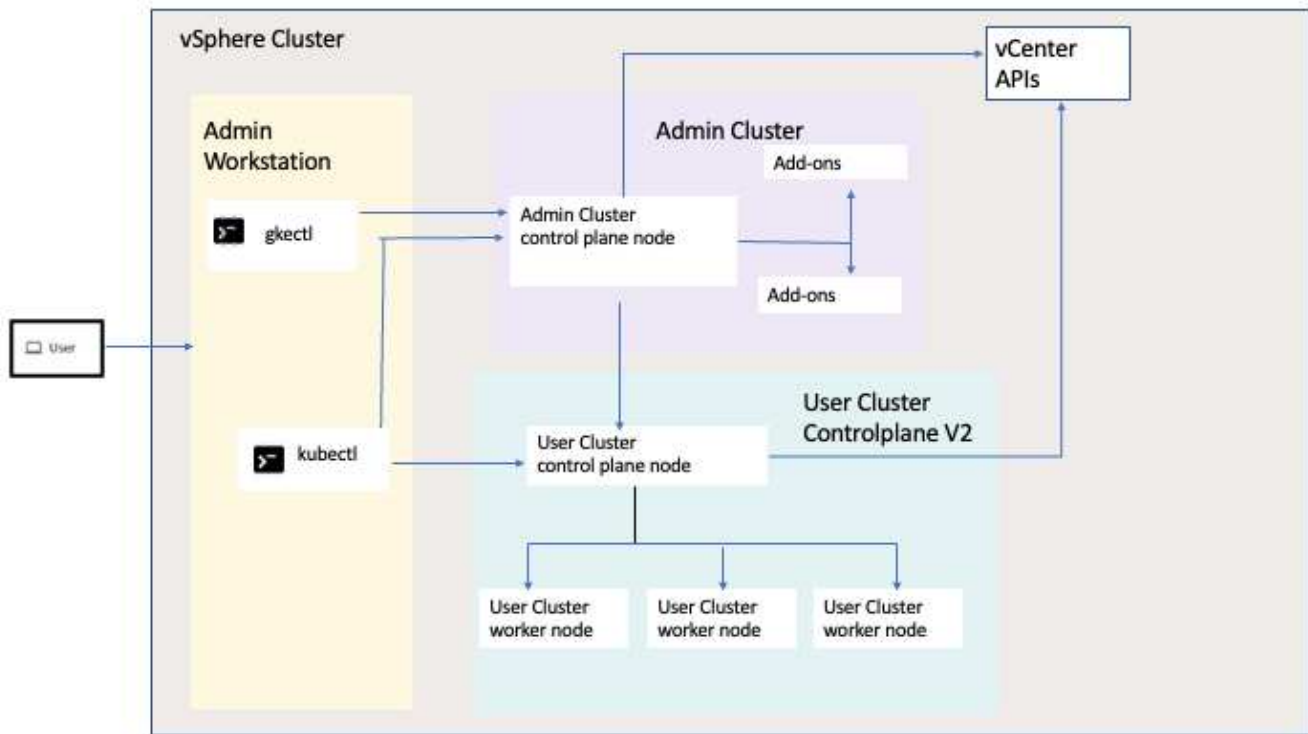
VMware上のAnthosクラスタ

VMware上のAnthosクラスタは、エンドユーザのプライベートデータセンターに導入されているGoogle Kubernetes Engineの拡張機能です。組織は、オンプレミスのKubernetesクラスタ内のGoogle Cloud内のコンテナで実行するように設計されたものと同じアプリケーションを導入できます。VMware上のAnthosクラスタは、データセンター内の既存のVMware vSphere環境に導入できます。これにより、資本コストを削減し、導入と拡張の処理をより迅速に実行できます。

VMware環境にAnthosクラスタを導入するには、次のコンポーネントが必要です。

- *Anthos管理ワークステーション*`gkectl`および`kubectl`コマンドを実行してAnthos展開を展開および操作できる配置ホスト
- 管理クラスタ。VMware上でAnthosクラスタをセットアップする際に最初に導入されたクラスタ。このクラスタは、導入、拡張、アップグレードなど、下位のユーザクラスタ操作をすべて管理します。
- *ユーザクラスタ。*各ユーザクラスタには独自のロードバランサインスタンスまたはパーティションが導入されているため、ユーザまたはグループごとにスタンドアロンのKubernetesクラスタとして機能し、マルチテナンシーを完全に実現できます。

次の図は、VMware環境のAnthos-clusters-onの概要を示しています。



利点

VMware上のAnthosクラスタには次のようなメリットがあります。

- *高度なマルチテナンシー。*各エンドユーザには、独自の開発環境に必要な仮想リソースを使用して、独自のユーザクラスタを割り当てることができます。
- *コスト削減。*エンドユーザーは、複数のユーザークラスタを同じ物理環境に導入し、Google Cloud環境や大規模なベアメタルクラスタにリソースをプロビジョニングする代わりに、アプリケーション導入に独自の物理リソースを使用することで、大幅なコスト削減を実現できます。
- *開発して公開。*アプリケーションの開発中にオンプレミス環境を使用できます。これにより、ローカルデータセンターのプライバシーでアプリケーションをテストしてから、クラウドで公開することができます。
- *セキュリティ要件。*セキュリティの懸念が高まるお客様や、パブリッククラウドに保存できない機密データセットをお持ちのお客様は、自社のデータセンターのセキュリティからアプリケーションを実行できるため、組織の要件を満たすことができます。

VMware vSphere の場合

VMware vSphere は、ESXi ハイパーバイザー上で実行される多数の仮想サーバとネットワークを一元管理するための仮想化プラットフォームです。

VMware vSphere の詳細については、を参照してください ["VMware vSphere の Web サイト"](#)。

VMware vSphere には次の機能があります。

- * VMware vCenter Server*。 VMware vCenter Server は、1つのコンソールからすべてのホストと VM を統合管理し、クラスタ、ホスト、VM のパフォーマンス監視を集約します。
- * VMware vSphere vMotion。* VMware vCenterでは、要求に応じて、無停止でクラスタ内のノード間

でVMをホット移行できます。

- * vSphere High Availability。*ホスト障害時のシステム停止を避けるため、VMware vSphereを使用すると、ホストをクラスタ化して高可用性を構成することができます。ホストの障害によってシステムが停止した VM は、クラスタ内の他のホストでまもなくリブートされ、サービスがリストアされます。
- * DRS （ Distributed Resource Scheduler ） 。 * VMware vSphere クラスタは、ホストしている VM のリソースニーズを負荷分散するように構成できます。リソース競合のある VM は、十分なリソースを使用できるように、クラスタ内の他のノードにホット移行できます。

ハードウェア要件

コンピューティング

Google Cloudは、Anthos Readyプラットフォームパートナープログラムを通じて、新しいリリースのAnthosを使用したパートナーサーバプラットフォームの更新検証を定期的に要求しています。現在検証済みのサーバプラットフォームとサポートされているAnthosのバージョンの一覧が表示されます "[こちらをご覧ください](#)"。

オペレーティングシステム

VMware上のAnthosクラスタは、お客様の現在のデータセンターインフラに合わせて、vSphere 7環境とvSphere 8環境のどちらにも導入できます。

次の表に、ネットアップとパートナーが解決策 の検証に使用したvSphereのバージョンを示します。

オペレーティングシステム	リリース。	Anthosのバージョン
vCenter	8.0.1	1.28

追加のハードウェア

ネットアップをフル検証済みの解決策 として導入したAnthosには、ネットアップとパートナーのエンジニアによって、ネットワークとストレージ用のデータセンターコンポーネントが追加でテストされています。

次の表に、これらの追加インフラコンポーネントに関する情報を示します。

製造元	ハードウェアコンポーネント
Mellanoxのサイト	スイッチ（データネットワーク）
シスコ	スイッチ（管理ネットワーク）
ネットアップ	AFF ストレージシステム

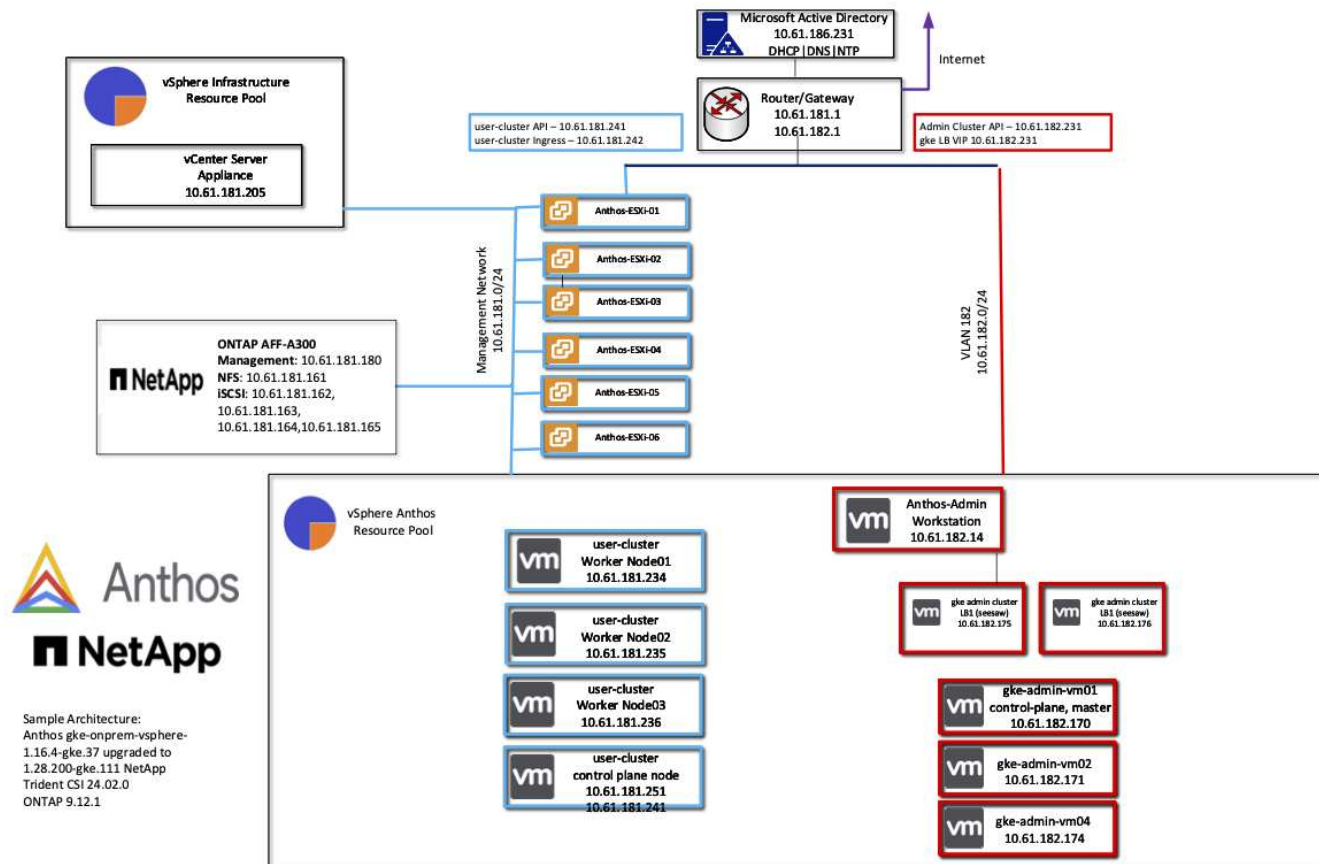
追加のソフトウェア

次の表に、検証環境で導入されたソフトウェアバージョンの一覧を示します。

製造元	Software Name（ソフトウェア名）	バージョン
ネットアップ	ONTAP	9.12.1:
ネットアップ	Astra Trident	24.02.0

ネットアップが実施したAnthos Readyプラットフォームの検証では、次の図に基づいてラボ環境を構築し、

さまざまなNetApp ONTAP ストレージバックエンドを使用して複数のシナリオをテストできました。



ネットワークインフラストラクチャサポートリソース

Anthosを導入する前に、以下のインフラを導入する必要があります。

- ・インバンド管理ネットワークと VM ネットワークからアクセス可能な完全なホスト名解決を提供する DNS サーバが少なくとも 1 台必要です。
- ・インバンド管理ネットワークおよび VM ネットワークからアクセスできる NTP サーバが少なくとも 1 台必要です。
- ・クラスタを動的に拡張する必要がある場合に、ネットワークアドレスのリースをオンデマンドで提供するために使用できる DHCP サーバ。
- ・（オプション）インバンド管理ネットワークと VM ネットワークの両方のアウトバウンドインターネット接続。

本番環境の導入に関するベストプラクティス

このセクションでは、この解決策を本番環境に導入する前に考慮する必要があるベストプラクティスをいくつか紹介します。

Anthosは、3ノード以上の**ESXi**クラスタに導入します

Anthosは、デモや評価用に3ノード未満のvSphereクラスタにインストールすることは可能ですが、本番環境のワークロードには推奨されません。2つのノードでは基本的なHAとフォールトトレランスを実現できます

が、デフォルトのホストアフィニティを無効にするようにAnthosクラスタ構成を変更する必要があります。
この導入方法はGoogle Cloudではサポートされていません。

仮想マシンとホストのアフィニティを設定します

Anthosクラスタノードを複数のハイパーバイザーノードに分散するには、VMとホストのアフィニティを有効にします。

アフィニティまたは非アフィニティは、VM やホストのセットに対してルールを定義する方法で、グループ内の同じホストまたはホスト上で VM を一緒に実行するか、別のホスト上で実行するかを決定します。VM とホストで構成されるアフィニティグループを作成することで、VM に適用されます。このアフィニティグループには同じパラメータと条件が設定されます。アフィニティグループ内の VM がグループ内の同じホストで実行されているのか、または別々のホストで実行されているのかに応じて、アフィニティグループのパラメータでは正のアフィニティまたは負のアフィニティを定義できます。

アフィニティグループを設定するには、使用しているVMware vSphereのバージョンに応じた以下の該当するリンクを参照してください。

"vSphere 6.7 ドキュメント：「DRS アフィニティルールの使用」。 <https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.resmgmt.doc/GUID-FF28F29C-8B67-4EFF-A2EF-63B3537E6934.html>["vSphere 7.0のドキュメント：「Using DRS Affinity Rules""]。



Anthosには'cluster.yamlファイルごとに構成オプションがあり'環境内のESXiホストの数に基づいて有効または無効にできるノードアフィニティルールが自動的に作成されます

ベアメタルの Anthos

ハードウェアに依存しないベアメタル上のAnthos機能により、お客様に合わせて最適化されたコンピューティングプラットフォームを選択でき、さらに多くのメリットがあります。

利点

ハードウェアに依存しないベアメタル上のAnthos機能により、お客様に合わせて最適化されたコンピューティングプラットフォームを選択でき、さらに多くのメリットがあります。

たとえば、次のようなものです。

- *既存のインフラストラクチャに対応したサーバを使用して、設備投資と管理コストを削減できます。
- 独自の**Linux OS**をお持ちください。Anthosオンベアメタル環境を導入するLinux OSを選択することで、Anthos環境を既存のインフラストラクチャと管理スキームに適切に適合させることができます。
- *パフォーマンスの向上とコストの削減*ハイパーバイザを必要としないAnthosオンベアメタルクラスタは、GPUなどのパフォーマンスに最適化されたハードウェアデバイスを含むサーバハードウェアリソースへの直接アクセスを求めています。
- ネットワークパフォーマンスの向上とレイテンシの低減 Anthos-ベア メタルサーバノードは仮想抽象化レイヤーを使用せずに直接ネットワークに接続されているため、低レイテンシと低パフォーマンスを実現するように最適化できます。

ハードウェア要件

コンピューティング

Google Cloudは、Anthos Readyプラットフォームパートナープログラムを通じて、新しいリリースのAnthosを使用したパートナーサーバプラットフォームの更新検証を定期的に要求しています。現在検証済みのサーバプラットフォームとサポートされているAnthosのバージョンの一覧が表示されます "[こちらをご覧ください](#)"。

以下の表は、ネットアップとネットアップパートナーのエンジニアが、ベアメタル環境でのAnthosの検証にテストしたサーバプラットフォームを示しています。

製造元	メーカー	モデル
シスコ	UCS	B200 M5
HPE	ProLiant	DL360

オペレーティングシステム

Anthosオンベアメタルノードには、現在のデータセンターインフラに合わせて、お客様が選択した複数のLinuxディストリビューションを構成できます。

次の表に、ネットアップとパートナー各社が解決策の検証に使用してきたLinuxオペレーティングシステムをまとめます。

オペレーティングシステム	リリース。	Anthosのバージョン
CentOS の場合	8.4.2105	1.14
Red Hat Enterprise Linux の場合	8/4	1.14
Ubuntu	18.04.5 LTS (カーネル5.4.0-81-generic)	1.14
Ubuntu	20.04.2 LTS	1.14

追加のハードウェア

ネットアップとパートナーのエンジニアは、検証済みの解決策としてベアメタルにAnthosを導入するために、ネットアップとストレージ用のデータセンターコンポーネントを追加でテストしました。

次の表に、これらの追加インフラコンポーネントに関する情報を示します。

製造元	Hardware Nameの略	モデル
シスコ	Nexus社	C9336C-FX2
ネットアップ	AFF	A250、A220

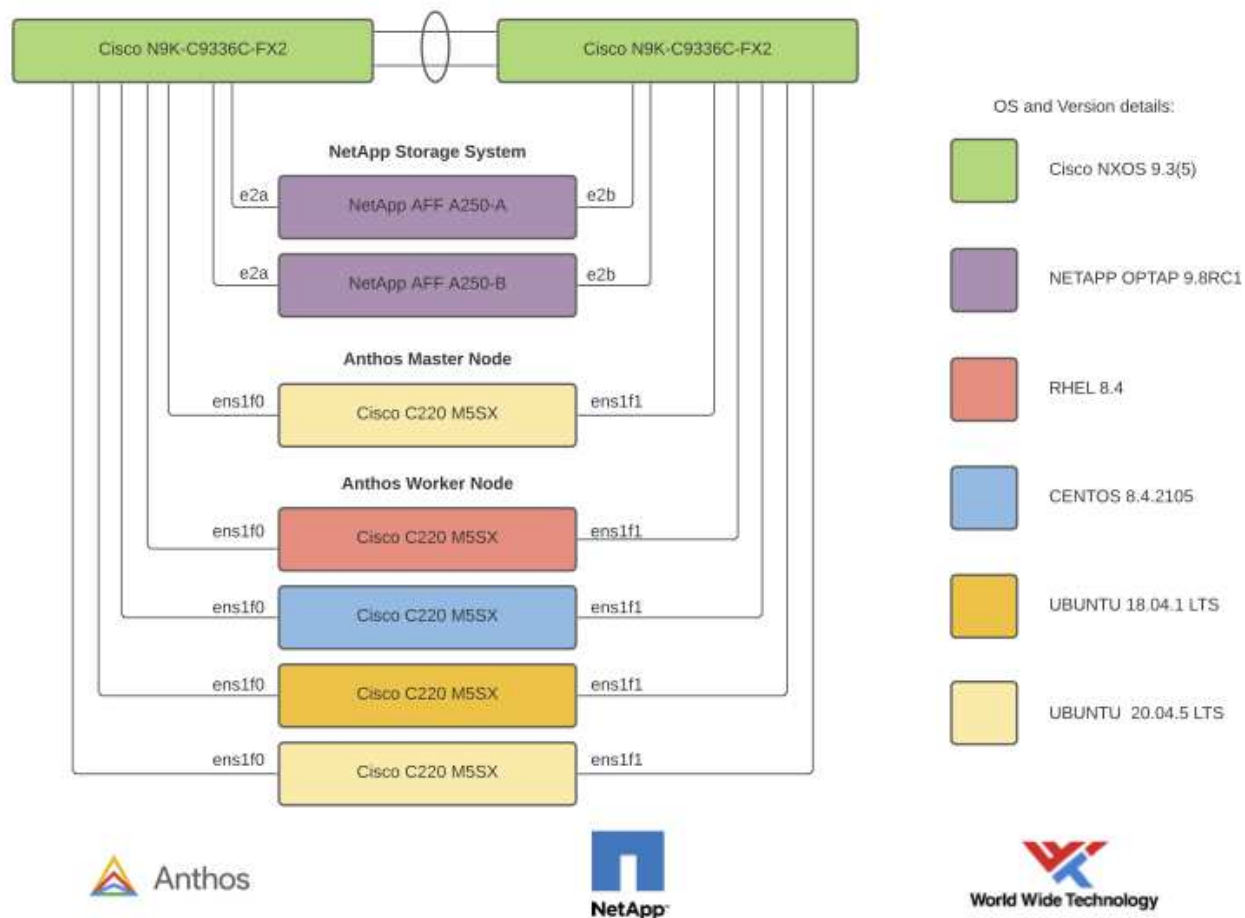
追加のソフトウェア

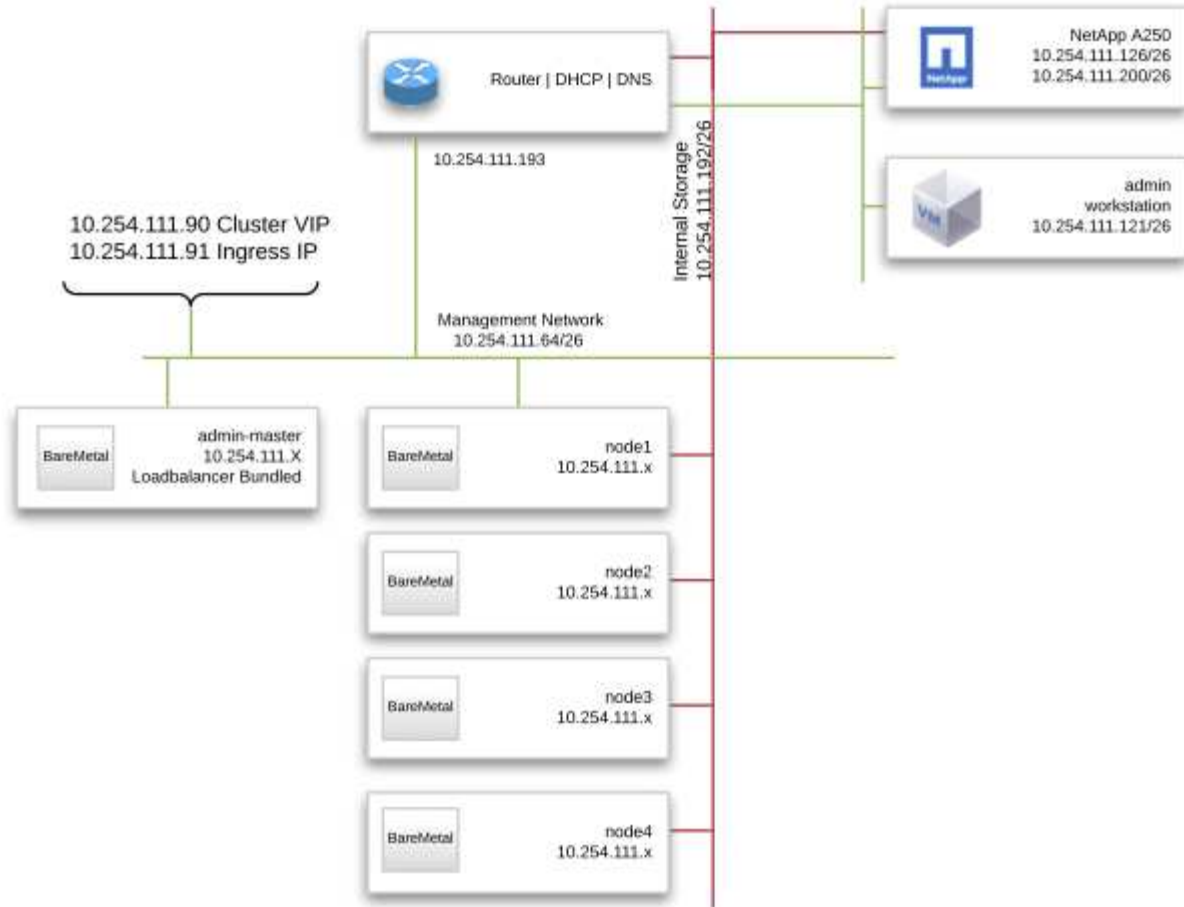
次の表に、検証環境に導入されているその他のソフトウェアバージョンを示します。

製造元	ソフトウェア名	バージョン
シスコ	NXOS	9.3 (5)
ネットアップ	ONTAP	9.11.1P4.
ネットアップ	Astra Trident	23.01.0

Anthos Readyプラットフォームの検証では、ネットアップとパートナーチームがWorld Wide Technology (WWT) を担当し、以下の図に基づいてラボ環境を構築しました。この図を参考に、サーバタイプ、オペレーティングシステム、ネットワークデバイス、 および解決策 に導入されているストレージシステム。

Anthos BareMetal Physical Hardware and Network Diagram





このマルチOS環境では、Anthos-On-by-Metal解決策 でサポートされているOSバージョンとの相互運用性が示されています。導入のために、お客様が1つまたは一部のオペレーティングシステムを標準化することを期待しています。

インフラサポートリソース

Anthosをベアメタルに導入する前に、以下のインフラを導入する必要があります。

- 管理ネットワークからアクセス可能な完全なホスト名解決を提供するDNSサーバが少なくとも1つ必要です。
- 管理ネットワークからアクセスできるNTPサーバが少なくとも1台必要です。
- (任意) インバンド管理ネットワークの両方のアウトバウンドインターネット接続。



本ドキュメントの「ビデオとデモ」セクションには、ベアメタル環境に導入されたAnthosのデモビデオがあります。

ネットアップストレージの概要

ネットアップには、Astra Trident Storage Orchestratorで認定された複数のストレージプラットフォームがあり、コンテナとして導入されるアプリケーション用のストレージをプロビジョニングできます。



- AFF システムと FAS システムは、NetApp ONTAP を実行し、ファイルベース（NFS）とブロックベース（iSCSI）の両方のユースケースにストレージを提供します。
- Cloud Volumes ONTAP と ONTAP Select は、それぞれクラウドと仮想スペースに同じメリットをもたらします。
- NetApp Cloud Volumes Service（GCP）と Azure NetApp Files は、クラウドでファイルベースストレージを提供します。
- Amazon FSx for NetApp ONTAP は、AWS上で提供されるフルマネージドサービスで、ファイルベースのユースケースにストレージを提供します。



ネットアップのポートフォリオに含まれる各ストレージシステムでは、オンプレミスサイトとクラウド間でのデータ管理と移動の両方を容易に行えるため、データがアプリケーションの配置場所にあることを保証できます。

NetApp ONTAP

NetApp ONTAP は、わかりやすい GUI、自動化統合機能を備えた REST API、AI に基づく予測分析と修正措置、ハードウェアの無停止アップグレード、ストレージ間インポートなどの機能を備えた強力なストレージソフトウェアツールです。

NetApp ONTAP ストレージシステムの詳細については、を参照してください ["ネットアップの ONTAP Web サイト"](#)。

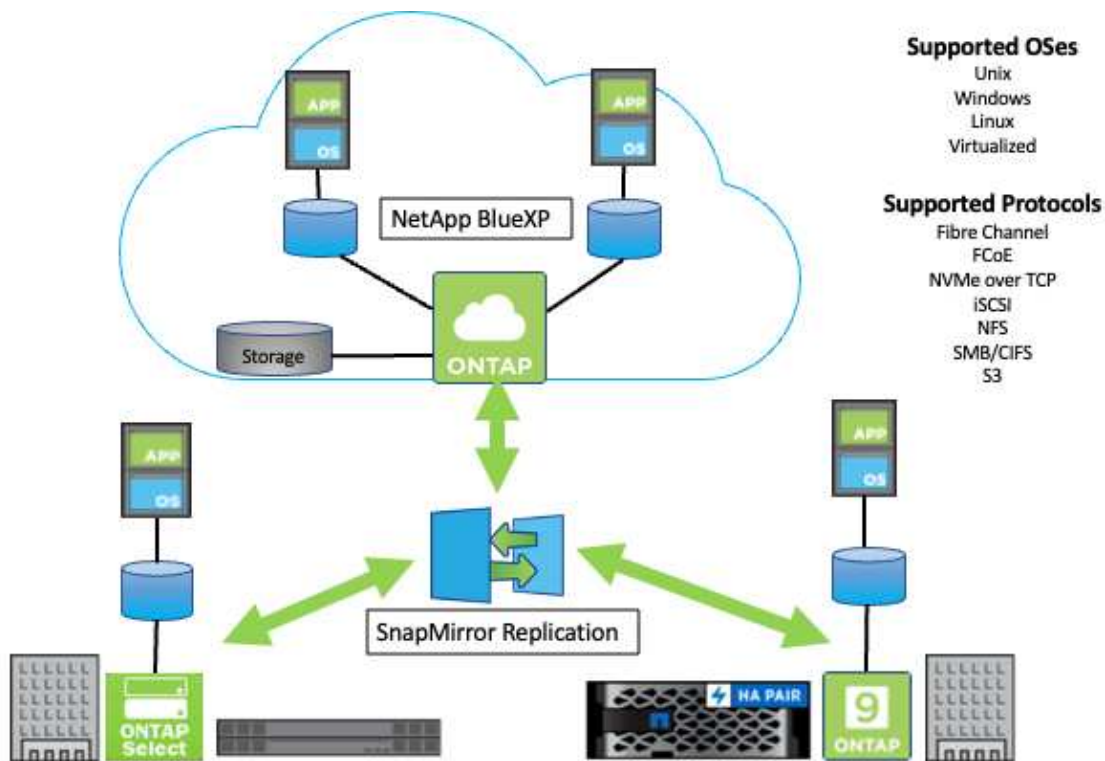
ONTAP は以下の機能を提供します。

- NFS、CIFS、iSCSI、FC、FCoE を同時にデータアクセスと管理できるユニファイドストレージシステム FC-NVMe プロトコルが必要です。
- 導入モデルには、オンプレミスのオールフラッシュ、ハイブリッド、オール HDD のハードウェア構成、ONTAP Select などのサポートされるハイパーバイザーを使用する VM ベースのストレージプラットフォーム、Cloud Volumes ONTAP などのクラウドがあります。
- ONTAP システムでは、データの自動階層化、インラインデータ圧縮、重複排除、コンパクションがサポートされ、データストレージ効率が向上しています。
- ワークロードベースの QoS 制御ストレージ：
- パブリッククラウドとのシームレスな統合により、データの階層化と保護を実現 ONTAP は、あらゆる環境に対応する堅牢なデータ保護機能も備えています。
 - * NetApp Snapshot コピー。* 最小限のディスク・スペースでデータをポイント・イン・タイムで高速バックアップし、パフォーマンス・オーバーヘッドを追加する必要はありません。
 - * NetApp SnapMirror。* 1 つのストレージ・システムから別のストレージ・システムへデータの Snapshot コピーをミラーリングします。ONTAP では、他の物理プラットフォームやクラウドネイティブのサービスへのデータのミラーリングもサポートされています。
 - * NetApp SnapLock。* 指定された期間にわたって上書きまたは消去できない特殊なボリュームに書き込むことにより、書き換え不可能なデータを効率的に管理します。
 - * NetApp SnapVault。* は、複数のストレージ・システムのデータを、指定されたすべてのシステムのバックアップとして機能する中央の Snapshot コピーにバックアップします。
 - * NetApp SyncMirror。* 同じコントローラに物理的に接続された 2 つの異なるディスクプレックスに対して、データをリアルタイムで RAID レベルでミラーリングします。
 - * NetApp SnapRestore * を使用すると、Snapshot コピーからオンデマンドでバックアップされたデータを迅速にリストアできます。
 - * NetApp FlexClone。* Snapshot コピーに基づいて、ネットアップボリュームの読み書き可能なフルコピーを瞬時にプロビジョニングできます。

ONTAP の詳細については、を参照してください ["ONTAP 9 ドキュメンテーション・センター"](#)。



NetApp ONTAP は、オンプレミス、仮想環境、クラウド環境で利用できます。



ネットアップのプラットフォーム

NetApp AFF/FAS

ネットアップは、堅牢なオールフラッシュ（AFF）およびスケールアウトハイブリッド（FAS）ストレージプラットフォームを提供し、低レイテンシのパフォーマンス、統合データプロテクション、マルチプロトコルのサポートを通じて、お客様のニーズに合わせてカスタマイズします。

どちらのシステムも、NetApp ONTAP データ管理ソフトウェアを搭載しています。NetApp Data Management ソフトウェアは、可用性が高く、クラウドと統合されたシンプルなストレージ管理を実現する業界最先端のデータ管理ソフトウェアで、データファブリックのニーズに合わせてエンタープライズクラスのスピード、効率性、セキュリティを提供します。

ネットアップのAFF プラットフォームとFAS プラットフォームの詳細については、[をクリックしてください](#) "[こちらをご覧ください](#)"。

ONTAP Select の場合

ONTAP Select は、お客様の環境のハイパーバイザーに導入できる、ソフトウェアで定義された NetApp ONTAP の導入です。VMware vSphere または KVM にインストールでき、ハードウェアベースの ONTAP システムの全機能とエクスペリエンスを提供します。

ONTAP Select の詳細については、[をクリックしてください](#) "[こちらをご覧ください](#)"。

Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP は、クラウドで導入される NetApp ONTAP のバージョンで、Amazon AWS、Microsoft Azure、Google Cloud などのさまざまなパブリッククラウドに導入できます。

Cloud Volumes ONTAP の詳細については、[をクリックしてください](#) "[こちらをご覧ください](#)"。

ネットアップストレージ統合の概要

ネットアップは、Anthosなどのコンテナベース環境における永続的データのオーケストレーションや管理を支援する製品を多数提供しています。

Anthos Readyストレージパートナープログラム：

Google Cloudは、Anthos Readyストレージパートナープログラムを通じて、パートナー様のストレージ統合とAnthosの新しいリリースの統合に関する最新検証を定期的にリクエストしています。現在検証済みのストレージソリューション、CSIドライバ、使用可能な機能、サポートされているAnthosのバージョンのリストが見つかります ["こちらをご覧ください"](#)。

ネットアップは、Astra Trident CSIに準拠したストレージオーケストレーションツールとONTAP ストレージシステムをAnthosのバージョンで検証するよう求められ、四半期ごとに定期的にコンプライアンスを維持しています。

次の表に、ネットアップおよびネットアップパートナーのエンジニアが、Anthos Readyストレージパートナープログラムの一環としてNetApp Astra CSIドライバおよび機能セットの検証にテストしたAnthosのバージョンを示します。

展開タイプ	バージョン	ストレージシステム	Astra Tridentバージョン	プロトコル	の機能
VMware	1.28	ONTAP 9.12.1	24.02	NAS	マルチライター、ボリューム拡張、スナップショット、PVCDataSource
VMware	1.28	ONTAP 9.12.1	24.02	SAN	rawブロック、ボリューム拡張、スナップショット、PVCDataSource
VMware	1.15	ONTAP 9.12.1	23.04	NAS	マルチライター、ボリューム拡張、スナップショット、PVCDataSource
VMware	1.15	ONTAP 9.12.1	23.04	SAN	rawブロック、ボリューム拡張、スナップショット、PVCDataSource

VMware	1.14	ONTAP 9.12.1	23.01.	NAS	マルチライター、ボリューム拡張、スナップショット、PVCDatSource
VMware	1.14	ONTAP 9.12.1	23.01.	SAN	rawブロック、ボリューム拡張、スナップショット、PVCDatSource
VMware	1.13	ONTAP 9.12.1	22.10	NAS	マルチライター、ボリューム拡張、スナップショット、PVCDatSource
VMware	1.13	ONTAP 9.12.1	22.10	SAN	rawブロック、ボリューム拡張、スナップショット、PVCDatSource
VMware	1.11	ONTAP 9.9.1	22.04	NAS	マルチライター、ボリューム拡張、スナップショット
VMware	1.11	ONTAP 9.9.1	22.04	SAN	Raw Block、Volume Expansion、Snapshot
VMware	1.11	Element 12.3	22.04	SAN	Raw Block、Volume Expansion、Snapshot
ベアメタル	1.10	ONTAP 9.8	22.01	NAS	マルチライター、ボリューム拡張、スナップショット
ベアメタル	1.10	ONTAP 9.8	22.01	SAN	Raw Block、Volume Expansion、Snapshot

ネットアップとストレージの統合

ネットアップは、Anthosなどのコンテナベース環境における永続的データのオーケストレーションと管理に役立つ製品を多数提供しています。

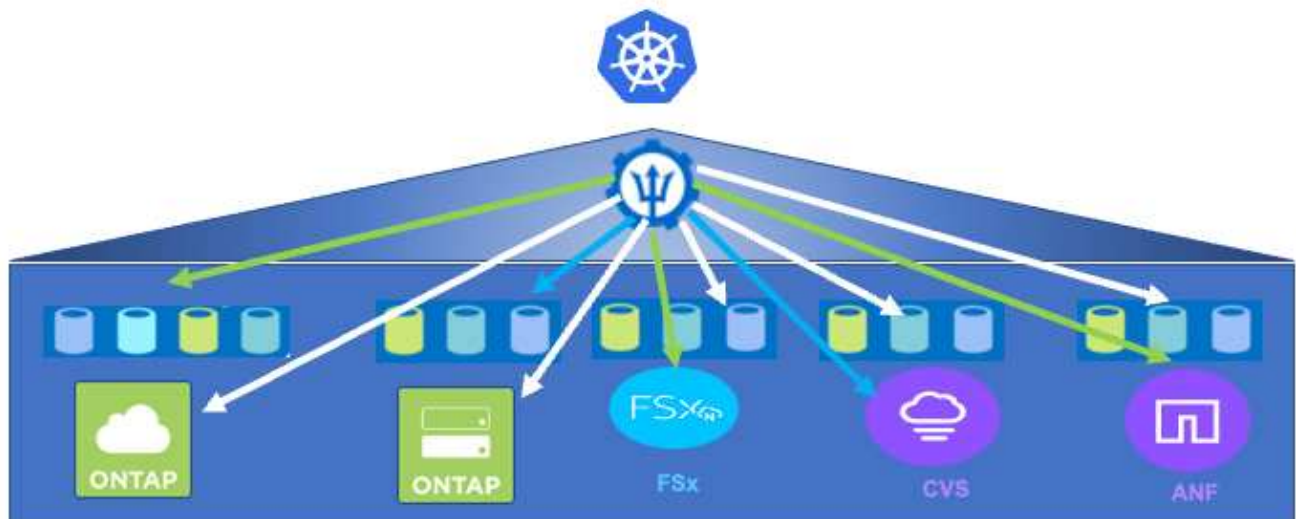
NetApp Astra Tridentは、オープンソースで、Anthosを含むコンテナやKubernetesディストリビューション向けの完全にサポートされているストレージオーケストレーションツールです。詳細については、Astra Trident の Web サイトをご覧ください ["こちらをご覧ください"](#)。

以下のページでは、追加情報 解決策 を使用したAnthosでアプリケーションおよび永続的ストレージの管理向けに検証されたネットアップ製品について説明します。

Astra Trident の概要

Astra Tridentは、Anthosを含むコンテナとKubernetesディストリビューション向けの、完全サポートされたオープンソースストレージオーケストレーションツールです。Tridentは、NetApp ONTAP を含むネットアップのストレージポートフォリオ全体と連携し、NFS接続とiSCSI接続もサポートします。Trident を使用すると、ストレージ管理者の手を煩わせることなく、エンドユーザがネットアップストレージシステムからストレージをプロビジョニングして管理できるため、DevOps ワークフローが高速化されます。

管理者は、プロジェクトのニーズとストレージシステムモデルに基づいて複数のストレージバックエンドを構成し、圧縮、特定のディスクタイプ、QoSレベルなどの高度なストレージ機能を有効にして一定のレベルのパフォーマンスを保証できます。定義されたバックエンドは、プロジェクトの開発者が永続的ボリューム要求（PVC）を作成し、永続的ストレージをオンデマンドでコンテナに接続するために使用できます。



Astra Tridentは、迅速な開発サイクルを実現し、Kubernetesと同様、年間4回リリースされます。

Astra Tridentの最新バージョンに関するドキュメントを参照できます ["こちらをご覧ください"](#)。Trident のどのバージョンがサポートされているかを確認できます Kubernetes ディストリビューションのテストに使用 ["こちらをご覧ください"](#)。

20.04 リリース以降、Trident のセットアップは Trident オペレータによって実行されます。オペレータが大規

模な導入を容易にし、Trident インストールの一部として導入されたポッドの自己修復などの追加サポートを提供します。

22.04リリースでは、Trident Operatorのインストールを容易にするためにHelmチャートを使用できるようになりました。

Astra Tridentのインストールの詳細については、を参照してください ["こちらをご覧ください"](#)。

ストレージ・システム・バックエンドを作成します

Astra Trident Operator のインストールが完了したら、使用するネットアップストレージプラットフォームに合わせてバックエンドを設定する必要があります。Astra Tridentのセットアップと設定を続行するには、次のリンクを参照してください。 ["バックエンドを作成します。"](#)

ストレージクラスを作成する。

バックエンドを作成したら、Kubernetesユーザがボリュームを作成するタイミングを指定するストレージクラスを作成する必要があります。Kubernetesユーザは、ストレージクラスを名前で指定する永続的ボリューム要求（PVC）を使用してボリュームをプロビジョニングします。ストレージクラスを作成するには、次のリンクをクリックしてください。 ["ストレージクラスを作成する。"](#)

ボリュームを動的にプロビジョニングします

ボリュームを動的にプロビジョニングするには、ストレージクラスを使用してKubernetesの永続的ボリューム要求（PVC）オブジェクトを作成する必要があります。PVCオブジェクトを作成するには、次のリンクをクリックしてください。 ["PVCを作成します"](#)

ボリュームを使用します

上記の手順でプロビジョニングしたボリュームは、ポッドにボリュームをマウントすることでアプリケーションで使用できます。下のリンクは例を示しています。 ["ボリュームをポッドにマウントします"](#)

Advanced Configuration Options （詳細設定オプション）

一般的には、最も簡単に導入できる解決策が最適ですが、場合によっては、特定のアプリケーションまたは解決策の導入先環境の要件または仕様を満たすために、高度なカスタマイズが必要になります。そのため、NetApp 解決策を使用した Red Hat OpenShift では、これらのニーズに合わせて次のカスタマイズを行うことができます。



このセクションでは、サードパーティ製のロードバランサを使用するか、カスタマイズしたコンテナイメージをホストするプライベートレジストリを作成するなど、いくつかの高度な設定オプションについて説明しました。どちらも NetApp Astra Control Center をインストールするための前提条件です。

以下のページでは、解決策追加情報を使用した Red Hat OpenShift で検証済みの高度な構成オプションについて説明します。

ロードバランサのオプションを確認する

Anthosに導入されたアプリケーションは、オンプレミス環境のAnthosに導入されたロードバランサによって提供されるサービスによって世界に公開されます。

以下のページでは、NetApp解決策 を搭載したAnthosで検証済みのロードバランサオプションについて、追加情報を紹介します。

- ["F5 BIG-IPロードバランサのインストール"](#)
- ["MetalLBロードバランサをインストールしています"](#)
- ["Seesawロードバランサをインストールしています"](#)

F5 BIG-IPロードバランサのインストール

F5 BIG-IPは、L4-L7ロードバランシング、SSL/TLSオフロード、DNS、ファイアウォールなど、高度な本番環境レベルのトラフィック管理およびセキュリティサービスを幅広く提供するApplication Delivery Controller（ADC）です。これらのサービスにより、アプリケーションの可用性、セキュリティ、パフォーマンスが大幅に向上します。

F5 BIG-IPは、専用ハードウェア、クラウド、オンプレミスの仮想アプライアンスなど、さまざまな方法で導入、使用できます。F5 BIG-IPの詳細と導入方法については、ここで説明しているドキュメントを参照してください。

F5 BIG-IPは、オンプレミスのAnthosで最初に提供されているロードバランサソリューションの1つで、NetApp解決策 を搭載したAnthosの初期のReadyパートナー検証で使用されていました。



F5 BIG-IPは、スタンドアロンモードまたはクラスタモードで導入できます。この検証のために、F5 BIG-IPはスタンドアロンモードで導入されました。ただし本番環境では、単一点障害を避けるために、ビッグIPインスタンスで構成されるクラスタを作成することを推奨します。



F5 BIG-IP システムは、専用のハードウェア、クラウド、またはオンプレミスの仮想アプライアンスとして、バージョンが 12.x よりも大きいオンプレミスに導入でき、F5 CIS と統合できます。このドキュメントでは、BIG-IP VE エディションなどを使用して、F5 BIG-IP システムを仮想アプライアンスとして検証しました。

検証済みのリリース

この解決策 は、VMware vSphereに導入された仮想アプライアンスを使用します。F5 BIG-IP 仮想アプライアンスのネットワークは、ネットワーク環境に基づいて、2 アームまたは3 アームの構成で設定できます。本ドキュメントでの導入は、2 つの設定に基づいています。Anthosで仮想アプライアンスを使用するための構成方法については、こちらをご覧ください ["こちらをご覧ください"](#)。

ネットアップのソリューションエンジニアリングチームでは、今回のラボの以下の表に示すリリースを、オンプレミスのAnthos環境で機能することを検証しました。

メーカー	を入力します	バージョン
F5キー	BIG-IP VE	15.0.1-0.0.11
F5キー	BIG-IP VE	16.1.0-0.0.19

インストール

F5 BIG-IPをインストールするには、次の手順を実行します。

1. から Virtual Application Open Virtual Appliance （OVA；仮想アプリケーションオープン仮想アプライアンス）ファイルをダウンロードします F5 キー ["こちらをご覧ください"](#)。



アプライアンスをダウンロードするには、F5 に登録する必要があります。これらは、Big IP Virtual Edition ロードバランサ用の 30 日間のデモライセンスを提供します。アプライアンスを本番環境に導入するには、10Gbps の永続的ライセンスを推奨します。

2. インフラストラクチャリソースプールを右クリックし、[Deploy OVF Template]を選択します。手順 1 でダウンロードした OVA ファイルを選択するためのウィザードが起動します。次へをクリックします。

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

[http](#) | [https://remoteserver-address/filetoinstall.ovf](#) | .ova

☒ Local file

BIGIP-15.0.1-0.....ALL-vmware.ova

[CANCEL](#)

[BACK](#)

[NEXT](#)

3. [次へ] をクリックして各手順を続行し、ストレージ選択画面に達するまで表示される各画面のデフォルト値を受け入れます。仮想マシンを導入する VM_Datastore を選択し、Next をクリックします。
4. ウィザードの次の画面では、環境で使用する仮想ネットワークをカスタマイズできます。[External] フィールドに VM_Network を選択し、[Management] フィールドに [Management_Network] を選択します。内部および HA は、F5 BIG-IP アプライアンスの高度な設定に使用され、設定されていません。これらのパラメータは単独で使用することも、インフラストラクチャ以外の分散ポートグループに接続するように設定することもできます。次へをクリックします。

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- 8 Select networks**
- 9 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
Internal	BIG-IP-Internal
External	VM_Network
HA	BIG-IP-HA
Management	Management_Network

4 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL

BACK

NEXT

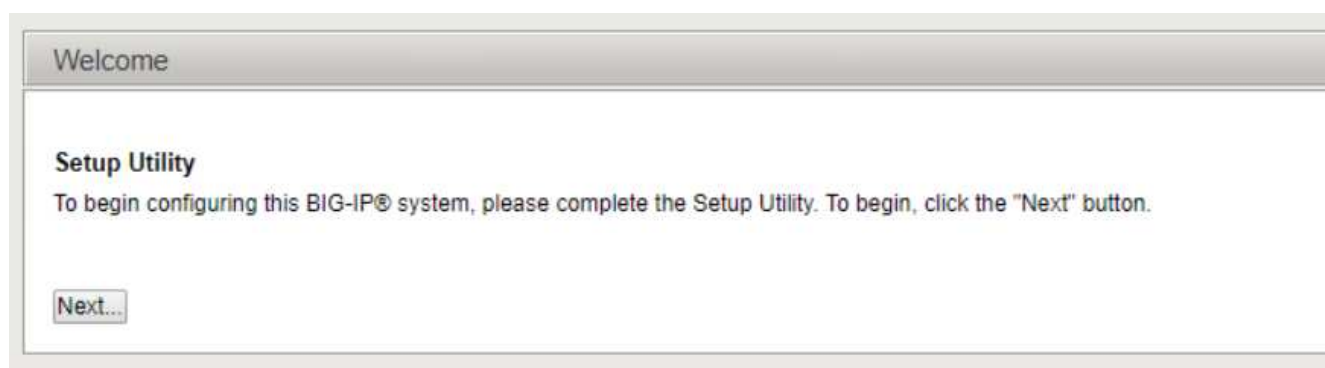
5. アプライアンスの概要画面を確認し、すべての情報が正しい場合は、Finish をクリックして展開を開始します。
6. 仮想アプライアンスを導入したら、右クリックして電源をオンにします。管理ネットワークで DHCP アドレスが割り当てられている必要があります。アプライアンスはLinuxベースで、VMware Toolsが導入されているため、vSphereクライアントで受信したDHCPアドレスを表示できます。

The screenshot shows the vSphere VM Summary view for a virtual machine named 'BIGIP-15.0.1-0.0.11-vmware-B'. The VM is powered on. The summary includes details about the Guest OS (CentOS 4/5 or later (64-bit)), Compatibility (ESXi 5.5 and later (VM version 10)), and VMware Tools (Running, version:10245 (Guest Managed)). It also shows the DNS Name (localhost.localdomain), IP Addresses (127.20.0.254), and Host (172.21.224.101). A tooltip is visible showing the IP Addresses: 127.20.0.254, 127.1.1.254, and 172.21.224.20.

7. Web ブラウザを開き、前の手順で確認した IP アドレスでアプライアンスに接続します。デフォルトのログインは admin/admin で、初回ログイン後はすぐに admin パスワードを変更するように要求されます。新しいクレデンシャルでログインする必要がある画面に戻ります。



8. 最初の画面で、セットアップユーティリティを完了するように指示されます。[次へ]をクリックして'ユーティリティを開始します



9. 次の画面では、アプライアンスのライセンスを有効にするよう求められます。Activate をクリックして開始します。次のページでメッセージが表示されたら、ダウンロード用に登録したときに受け取った 30 日間の評価ライセンスキーか、アプライアンスの購入時に取得した永久ライセンスのいずれかを貼り付けます。次へをクリックします。

General Properties	
Base Registration Key	BFXBY-PVROQ-QIHCH-NZGSZ-AZCFDPX Revert
Add-On Registration Key List	Add-On Key <input type="text"/> Add
	<div></div>
	Edit Delete
Activation Method	<input checked="" type="radio"/> Automatic (requires outbound connectivity) <input type="radio"/> Manual
Outbound Interface	mgmt ▼
License Comparison	<input type="checkbox"/> Enable License Comparison
Next...	



デバイスがアクティベーションを実行するには、管理インターフェイスで定義されたネットワークがインターネットに接続できる必要があります。

10. 次の画面では、エンドユーザライセンス契約（EULA）が表示されます。ライセンスの条件に同意する場合は、[同意する]をクリックします。
11. 次の画面では、これまでに行われた設定変更を確認するまでの経過時間がカウントされます。Continue（続行）をクリックして、初期設定を再開します。

BIG-IP system configuration has changed

Tue Nov 05 2019 18:10:20

The configuration for this device has been updated. Consequently, the features and functionality previously available on the BIG-IP system might have changed.

Elapsed Time: 49 seconds

✓ Please wait while the configuration changes are verified...
The BIG-IP Configuration utility will be updated momentarily.

✓ Configuration changes have been verified
You may now continue using the BIG-IP Configuration utility.

Continue

12. 設定変更ウィンドウが閉じ、セットアップユーティリティにリソースプロビジョニングメニューが表示されます。このウィンドウには、現在ライセンスされている機能、および仮想アプライアンスと各実行サービスの現在のリソース割り当てが表示されます。

Current Resource Allocation				
CPU	MGMT TMM:85%			
Disk (24GB)	MGMT			
Memory (3.8GB)	MGMT TMM			
Module	Provisioning	License Status	Required Disk (GB)	Required Memory (MB)
Management (MGMT)	Small	N/A	0	1070
Local Traffic (LTM)	Nominal	Licensed	0	854
Application Security (ASM)	None	Licensed	20	1492
Fraud Protection Service (FPS)	None	N/A	12	544
Global Traffic (DNS)	None	Licensed	0	148
Link Controller (LC)	None	Unlicensed	0	148
Access Policy (APM)	None	Limited	12	494
Application Visibility and Reporting (AVR)	None	Licensed	16	576
Policy Enforcement (PEM)	None	Unlicensed	16	1223
Advanced Firewall (AFM)	None	Licensed	16	1058
Application Acceleration Manager (AAM)	None	Unlicensed	32	2050
Secure Web Gateway (SWG)	None	Unlicensed	24	4096
iRules Language Extensions (iRulesLX)	None	Licensed	0	748
URLDB Minimal (URLDB)	None	Unlicensed	36	2048
SSL Orchestrator (SSLO)	None	Unlicensed	0	128
Carrier Grade NAT (CGNAT)	None	Licensed	16	336

13. 左側の [プラットフォーム (Platform)] メニューオプションをクリックすると、プラットフォームをさらに変更できます。変更内容には、DHCP を使用して設定された管理 IP アドレスの設定、アプライアンスをインストールするホスト名とタイムゾーンの設定、SSH からのアクセスの保護などがあります。

General Properties	
Management Config IPv4	<input checked="" type="radio"/> Automatic (DHCP) <input type="radio"/> Manual
Management Config IPv6	<input checked="" type="radio"/> Automatic (DHCP) <input type="radio"/> Manual
Host Name	<input type="text" value="Anthos-F5-Big-IP"/>
Host IP Address	<input type="text" value="Use Management Port IP Address"/>
Time Zone	<input type="text" value="America/New York"/>
User Administration	
Root Account	<input type="checkbox"/> Disable login Password: <input type="text"/> Confirm: <input type="text"/>
SSH Access	<input checked="" type="checkbox"/> Enabled
SSH IP Allow	<input type="text" value="* All Addresses"/>

14. 次に、標準ネットワーク機能を設定できる [ネットワーク] メニューをクリックします。[次へ] をクリックして、標準ネットワーク構成ウィザードを開始します。

Standard Network Configuration
Create a standard network configuration by configuring these features:

- Redundancy
- VLANs
- NTP
- DNS
- Config Sync
- Failover
- Mirroring
- Peer Device Discovery (for Redundant Configurations)

Next...

Advanced Network Configuration
Create advanced device configurations by clicking **Finished** and navigating to the Main tab of the Configuration Utility.

Finished

15. ウィザードの最初のページでは冗長性が設定されます。デフォルトのままで Next（次へ）をクリックします。次のページでは、ロードバランサに内部インターフェイスを設定できます。インターフェイス1.1は、OVF DeploymentウィザードでInternalというラベルの付いたVMNICにマッピングされます。

Internal Network Configuration

Self IP	Address: 192.168.1.11 Netmask: 255.255.255.0 Port Lockdown: Allow Default ▼
Floating IP	Address: 192.168.1.10 Port Lockdown: Allow Default ▼

Internal VLAN Configuration

VLAN Name	internal
VLAN Tag ID	auto
VLAN Interfaces	1.1 ▼
Tagging	Select... ▼
Interfaces	<div>Add</div> <div>Edit Delete</div>

Cancel Next...



このページの「自己IPアドレス」、「ネットマスク」、「フローティング」の各IPアドレスには、プレースホルダとして使用するルーティング不可のIPを入力できます。また、3段階の設定を導入する場合は、仮想ゲスト用の分散ポートグループとして設定された内部ネットワークにも接続できます。ウィザードを続行するには、これらの手順を完了する必要があります。

16. 次のページでは、Kubernetes で導入されたポッドにサービスをマッピングするために使用する外部ネットワークを設定できます。VM_Network の範囲内の静的 IP、適切なサブネットマスク、および同じ範囲のフローティング IP を選択します。インターフェイス1.2は、OVF導入ウィザードでExternalというラベルのVMNICにマッピングされます。

External Network Configuration	
External VLAN	<input checked="" type="radio"/> Create VLAN external <input type="radio"/> Select existing VLAN
Self IP	Address: <input type="text" value="10.63.172.101"/> Netmask: <input type="text" value="255.255.255.0"/> Port Lockdown: <input type="text" value="Allow None"/>
Default Gateway	<input type="text" value="10.63.172.1"/>
Floating IP	Address: <input type="text" value="10.63.172.100"/> Port Lockdown: <input type="text" value="Allow None"/>

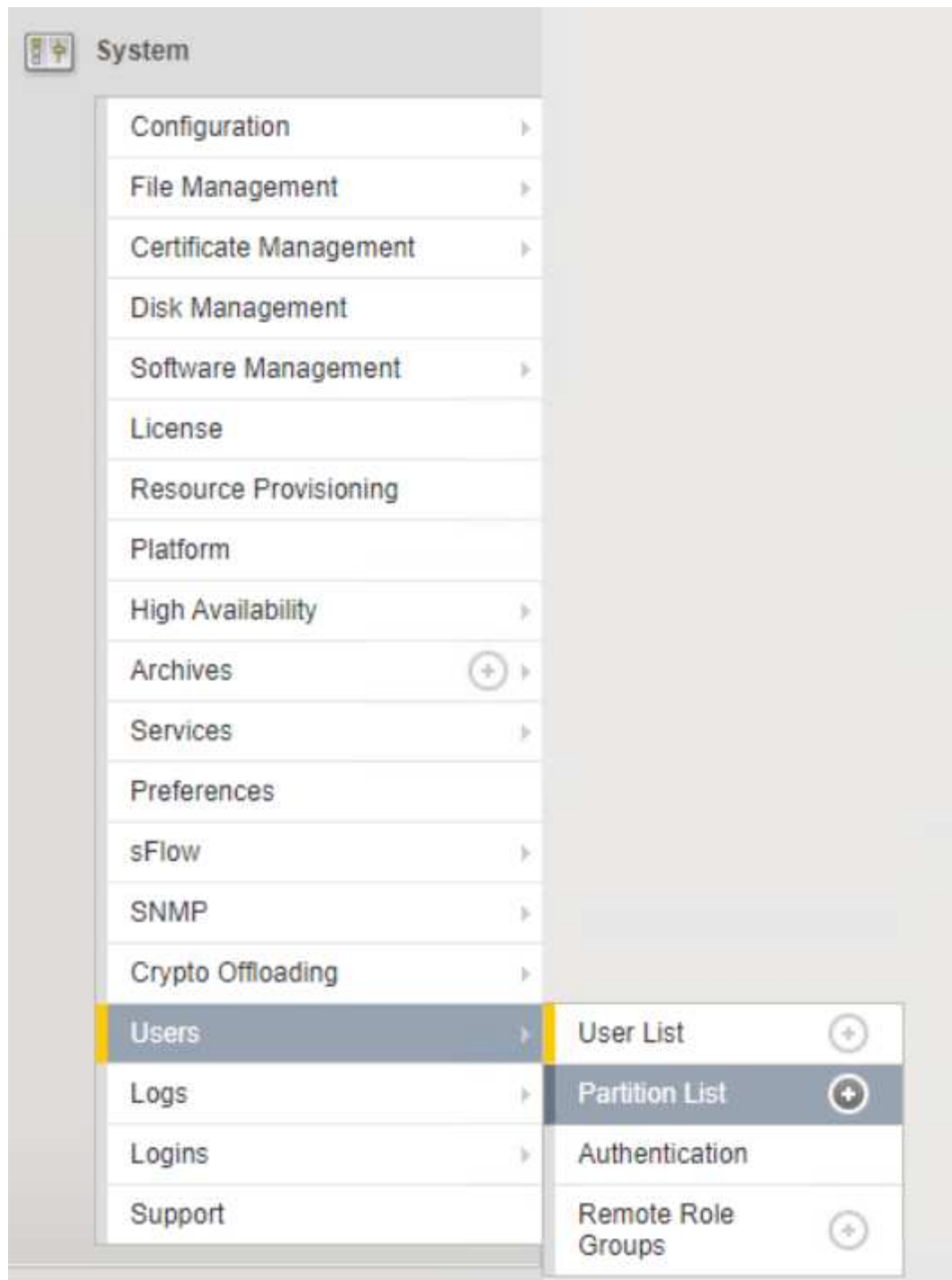
External VLAN Configuration	
VLAN Name	<input type="text" value="external"/>
VLAN Tag ID	<input type="text" value="auto"/>
Interfaces	VLAN Interfaces: <input type="text" value="1.2"/> Tagging: <input type="text" value="Select..."/> <input type="button" value="Add"/> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

17. 環境に複数の仮想アプライアンスを導入する場合は、次のページで内部 HA ネットワークを設定できます。続行するには、Self-IP Address フィールドと Netmask フィールドに値を入力し、VLAN インターフェイスとしてインターフェイス 1.3 を選択し、OVF テンプレートウィザードで定義された HA ネットワークにマッピングする必要があります。

High Availability Network Configuration	
High Availability VLAN	<input checked="" type="radio"/> Create VLAN HA <input type="radio"/> Select existing VLAN
Self IP	Address: <input type="text" value="192.168.2.11"/> Netmask: <input type="text" value="255.255.255.0"/>

High Availability VLAN Configuration	
VLAN Name	<input type="text" value="HA"/>
VLAN Tag ID	<input type="text" value="auto"/>
Interfaces	VLAN Interfaces: <input type="text" value="1.3"/> Tagging: <input type="text" value="Select..."/> <input type="button" value="Add"/> <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

18. 次のページでは、NTP サーバを設定できます。次へをクリックして、DNS セットアップに進みます。DNS サーバとドメインの検索リストは、DHCP サーバによってすでに入力されている必要があります。[次へ]をクリックしてデフォルトを受け入れ、続行します。
19. ウィザードの残りの部分については、[Next] をクリックして、詳細なピアリング設定を行います。この設定は、このマニュアルでは説明していません。完了をクリックしてウィザードを終了します。
20. Anthos 管理クラスタと環境内に導入されているユーザクラスタごとに、個別のパーティションを作成します。左側のメニューで [システム] をクリックし、[ユーザー] に移動して、[パーティションリスト] をクリックします。



21. 表示される画面には、現在の共通パーティションのみが表示されます。右側の[作成]をクリックして最初の追加パーティションを作成し、「GKE-ADMIN」という名前を付けます。[繰り返し]をクリックし、パーティションにUser-Cluster-1という名前を付けます[繰り返し]ボタンをもう一度クリックして次のパーティションにUser-Cluster-2という名前を付けます最後に、[終了]をクリックしてウィザードを完了します。パーティションリスト画面が表示され、すべてのパーティションが表示されます。

Search		Create...
<input checked="" type="checkbox"/> Name	Partition	Default Route Domain
<input type="checkbox"/> Anthos-Admin		0
<input type="checkbox"/> Anthos-Cluster1		0
<input type="checkbox"/> Anthos-Cluster2		0
<input type="checkbox"/> Common		0
Delete...		

Anthosとの統合

管理クラスタ用の各構成ファイルにはセクションがあり、導入するユーザクラスタごとにロードバランサを設定し、オンプレミスのAnthosで管理されるようにします。

次のスクリプトは、GKE-Adminクラスタ用パーティションの設定例です。コメントを解除して変更する必要がある値は、次の太字で表示されます。

```
# (Required) Load balancer configuration
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.230"
    # # (Optional) Used for admin cluster addons (needed for multi cluster
features). Must
    # # be the same across clusters
    # # addonsVIP: ""
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" or
"ManualLB". Uncomment
  # the corresponding field below to provide the detailed spec
  kind: F5BigIP
  # # (Required when using "ManualLB" kind) Specify pre-defined nodeports
  # manualLB:
  #   # NodePort for ingress service's http (only needed for user cluster)
  #   ingressHTTPNodePort: 0
  #   # NodePort for ingress service's https (only needed for user
cluster)
  #   ingressHTTPSNodePort: 0
  #   # NodePort for control plane service
  #   controlPlaneNodePort: 30968
  #   # NodePort for addon service (only needed for admin cluster)
  #   addonsNodePort: 31405
  # # (Required when using "F5BigIP" kind) Specify the already-existing
partition and
  # # credentials
  f5BigIP:
    address: "172.21.224.21"
    credentials:
      username: "admin"
      password: "admin-password"
    partition: "GKE-Admin"
  #   # # (Optional) Specify a pool name if using SNAT
  #   # snatPoolName: ""
  # (Required when using "Seesaw" kind) Specify the Seesaw configs
  # seesaw:
  # (Required) The absolute or relative path to the yaml file to use for
```

```

IP allocation
# for LB VMs. Must contain one or two IPs.
# ipBlockFilePath: ""
# (Required) The Virtual Router Identifier of VRRP for the Seesaw
group. Must
# be between 1-255 and unique in a VLAN.
# vrid: 0
# (Required) The IP announced by the master of Seesaw group
# masterIP: ""
# (Required) The number CPUs per machine
# cpus: 4
# (Required) Memory size in MB per machine
# memoryMB: 8192
# (Optional) Network that the LB interface of Seesaw runs in (default:
cluster
# network)
# vCenter:
# vSphere network name
# networkName: VM_Network
# (Optional) Run two LB VMs to achieve high availability (default:
false)
# enableHA: false

```

MetalLBロードバランサをインストールしています

このページでは、**MetalLB**管理対象ロードバランサのインストールおよび設定手順を示します。

MetalLB ロードバランサをインストールします

MetalLBロードバランサは、VMware上のAnthosクラスタと完全に統合されており、1.11リリース以降のAdminおよびUserクラスタセットアップの一部として自動展開を実行しています。ロード・バランサ情報を提供するために変更する必要がある'対応する'cluster.yamlの構成ファイル内にテキストのブロックがありますサポートされている他のロードバランサソリューションのような外部リソースの導入を必要とするのではなく、Anthosクラスタで自己ホストされます。また、IPプールを作成し、クラウドプロバイダで実行されていないクラスタでロードバランサタイプのKubernetesサービスの作成時にアドレスを自動的に割り当てることもできます。

Anthosとの統合

Anthos管理用の**MetalLB**ロードバランサをイネーブルにする場合、「admin-cluster.yaml」ファイルにある「Loadbalancer:」セクションの一部の行を変更する必要があります。変更する必要がある値は、「controlPlaneVip:」アドレスを設定し、「kind:」を**MetalLB**として設定することだけです。例については、次のコードスニペットを参照してください。

```
# (Required) Load balancer configuration
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.230"
    # # (Optional) Used for admin cluster addons (needed for multi cluster
    # # features). Must
    # # be the same across clusters
    # addonsVIP: ""
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" "ManualLB" or
  # "MetalLB".
  # Uncomment the corresponding field below to provide the detailed spec
  kind: MetalLB
```

AnthosユーザクラスタでMetalLBロードバランサをイネーブルにする場合、更新が必要な「user-cluster.yaml」ファイルごとに2つの領域があります。まず「admin-cluster.yaml」ファイルと同様に「controlPlaneVip:」と「ingressVip:」の値をLoadbalancerの「」セクションで変更する必要があります例については、次のコードスニペットを参照してください。

```
loadBalancer:
  # (Required) The VIPs to use for load balancing
  vips:
    # Used to connect to the Kubernetes API
    controlPlaneVIP: "10.61.181.240"
    # Shared by all services for ingress traffic
    ingressVIP: "10.61.181.244"
  # (Required) Which load balancer to use "F5BigIP" "Seesaw" "ManualLB" or
  # "MetalLB".
  # Uncomment the corresponding field below to provide the detailed spec
  kind: MetalLB
```



設定の後半で、MetalLBロードバランサに割り当てられたIPアドレスのプール内に、ingressVIP IPアドレスが存在している必要があります。

次に「metalLB:」サブセクションに移動し「addressPools:」セクションを修正して「-name:」変数にプールの名前を付けますまた、MetalLBが「address:」変数に範囲を提供することで、LoadBalancer型のサービスに割り当てることができるIPアドレスのプールを作成する必要があります。

```
# # (Required when using "MetalLB" kind in user clusters) Specify the
MetalLB config
  metalLB:
    # # (Required) A list of non-overlapping IP pools used by load balancer
typed services.
    # # Must include ingressVIP of the cluster.
    addressPools:
      # # (Required) Name of the address pool
      - name: "default"
      # # (Required) The addresses that are part of this pool. Each address
must be either
      # # in the CIDR form (1.2.3.0/24) or range form (1.2.3.1-1.2.3.5).
      addresses:
        - "10.61.181.244-10.61.181.249"
```



この例のような範囲を指定すると、特定のサブネット内のアドレス数に制限することも、サブネット全体が使用可能になった場合にCIDR表記として指定することもできます。

1. LoadBalancerタイプのKubernetesサービスが作成されると、MetalLBは自動的にそのサービスに外部IPを割り当て、ARP要求に応答してIPアドレスをアドバタイズします。

Seesawロードバランサをインストールしています

このページには、**Seesaw**管理対象ロードバランサのインストールおよび設定手順がリストされています。

Seesawは、VMware環境のAnthosクラスタにインストールされているデフォルトのマネージドネットワークロードバランサで、バージョン1.6～1.10です。

シーソーロードバランサの取り付け

Seesawロードバランサは、VMware上のAnthosクラスタと完全に統合されており、AdminクラスタとUserクラスタセットアップの一部として自動で導入されています。'cluster.yaml'コンフィギュレーションファイルには'ロード・バランサ情報を提供するために変更する必要があるテキストのブロックがあります次に'組み込みのgkectl'ツールを使用してロード・バランサを導入するためのクラスタ配備の前に'追加のステップがあります



シーソーロードバランサは、HAモードまたは非HAモードで展開できます。この検証の目的で、シーソーロードバランサはデフォルト設定である非HAモードで展開されました。本番環境では、フォールトトレランスと信頼性を確保するために、HA構成でシーソーを導入することを推奨します。

Anthosとの統合

管理クラスタ用の各構成ファイルと、オンプレミスのAnthosで管理されるようにロードバランサを構成するために導入するユーザクラスタごとにセクションがあります。

次のテキストは、GKE-Adminクラスタ用パーティションの設定例です。コメントを解除して変更する必要がある値は、次の太字で表示されます。

loadBalancer:

(Required) The VIPs to use for load balancing

vips:

Used to connect to the Kubernetes API

controlPlaneVIP: "10.61.181.230"

(Optional) Used for admin cluster addons (needed for multi cluster features). Must

be the same across clusters

addonsVIP: ""

(Required) Which load balancer to use "F5BigIP" "Seesaw" or "ManualLB". Uncomment

the corresponding field below to provide the detailed spec

kind: Seesaw

(Required when using "ManualLB" kind) Specify pre-defined nodeports

manualLB:

NodePort for ingress service's http (only needed for user cluster)

ingressHTTPTNodePort: 0

NodePort for ingress service's https (only needed for user

cluster)

ingressHTTPSNodePort: 0

NodePort for control plane service

controlPlaneNodePort: 30968

NodePort for addon service (only needed for admin cluster)

addonsNodePort: 31405

(Required when using "F5BigIP" kind) Specify the already-existing partition and

credentials

f5BigIP:

address:

credentials:

username:

password:

partition:

(Optional) Specify a pool name if using SNAT

snatPoolName: ""

(Required when using "Seesaw" kind) Specify the Seesaw configs

seesaw:

(Required) The absolute or relative path to the yaml file to use for IP allocation

for LB VMs. Must contain one or two IPs.

ipBlockFilePath: "admin-seesaw-block.yaml"

(Required) The Virtual Router Identifier of VRRP for the Seesaw group. Must

be between 1-255 and unique in a VLAN.

vrid: 100

```
# (Required) The IP announced by the master of Seesaw group
masterIP: "10.61.181.236"
# (Required) The number CPUs per machine
cpus: 1
# (Required) Memory size in MB per machine
memoryMB: 2048
# (Optional) Network that the LB interface of Seesaw runs in (default:
cluster
# network)
vCenter:
# vSphere network name
networkName: VM_Network
# (Optional) Run two LB VMs to achieve high availability (default:
false)
enableHA: false
```

Seesawロードバランサには、クラスタの展開ごとに提供する必要のある個別の静的な「seesaw-block.yaml」ファイルもあります。このファイルは'cluster.yaml'配備ファイルと同じディレクトリに配置する必要がありますまたは'上記のセクションでフルパスを指定する必要があります

「admin-seesa-block.yaml」ファイルのサンプルは、次のスクリプトのようになります。

```
blocks:
- netmask: "255.255.255.0"
  gateway: "10.63.172.1"
  ips:
  - ip: "10.63.172.152"
    hostname: "admin-seesaw-vm"
```



このファイルは、ロードバランサが基盤となるクラスタに提供するネットワークのゲートウェイとネットマスク、およびロードバランサを実行するために導入された仮想マシンの管理IPとホスト名を提供します。

解決策の検証とユースケース

このページには、ネットアップを使用したAnthosでの解決策 の検証とユースケースが含まれています。

["Google Cloud Consoleを使用してアプリケーションをインストールします"](#)

ビデオとデモ

次のビデオでは、このドキュメントで説明している機能の一部を紹介します。

[ベアメタルへのAnthosの導入- NetAppを使用したAnthos](#)

追加情報の参照先

このドキュメントに記載されている情報の詳細については、次の Web サイトを参照してください。

- NetApp のドキュメント

["https://docs.netapp.com/"](https://docs.netapp.com/)

- ネットアップAstra Tridentドキュメント

["https://docs.netapp.com/us-en/trident/index.html"](https://docs.netapp.com/us-en/trident/index.html)

- NetApp Astra Control Center のドキュメント

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- VMwareドキュメントのAnthosクラスタ

["https://cloud.google.com/anthos/clusters/docs/on-prem/latest/overview"](https://cloud.google.com/anthos/clusters/docs/on-prem/latest/overview)

- 『Anthos on bare metal Documentation』

["https://cloud.google.com/anthos/clusters/docs/bare-metal/latest"](https://cloud.google.com/anthos/clusters/docs/bare-metal/latest)

- VMware vSphere のドキュメント

["https://docs.vmware.com/"](https://docs.vmware.com/)

TR-4919 : 『DevOps with NetApp Astra』

このテクニカルレポートでは、コンテナ化されたアプリケーションを使用する場合に、ネットアップがDevOpsのユースケースを複数の面で簡単かつ効率的に作成する方法を説明します。まずは、ネットアップのストレージシステムの詳細と、ネットアップのKubernetesプラットフォームとの統合を紹介するAstraポートフォリオを活用します。最後に、解決策検証と実際の使用事例をいくつか確認して文書化します。

ネットアップ、Alan Cowles 氏と Nikhil M Kulkarni 氏

ユースケース

ネットアップのAstra解決策を使用したDevOpsは、次のユースケースにおいて、卓越した価値をお客様に提供するように設計されています。

- サポートされているKubernetesディストリビューションに導入されたアプリケーションや開発環境の導入と管理が容易です。
- DevOpsワークフローの実際のユースケースと、ネットアップが提供するツールやメソッドの例について説明し、これらの手法の採用や利用を簡易化する方法を紹介します。

- アプリケーションと整合性のあるSnapshot、バックアップ、クローンを使用してDevOpsエクスペリエンスを向上する方法をご紹介します。

ビジネスバリュー

企業は、新しい製品の作成、リリースサイクルの短縮、新機能の迅速な追加を目的として、DevOpsの手法を採用する傾向に迫られています。即応性に優れた本来の性質から、コンテナやマイクロサービスは、DevOpsの実践を支援するうえで重要な役割を果たします。しかし、エンタープライズ環境で本番環境規模でDevOpsを実践する場合、独自の課題が生じ、基盤となるインフラに次のような一定の要件が課せられます。

- ワークフローが中断されないように、スタック内のすべてのレイヤで高可用性を実現します。
- エンドユーザ向けの導入と管理の手順が簡単です。
- APIベースのプログラム可能なインフラで、マイクロサービスや開発者の即応性に対応します。
- ワークロードのニーズに基づいて、インフラを個別に、自動化された方法で拡張できます。
- DevOpsワークフロー向けの永続的データセットと並行してアプリケーションを保護することで、再導入や手動によるデータコピーに頼ることなく、製品化サイクルを短縮できます。

このテクニカルレポートでは、これらの機能と課題を認識し、さまざまなネットアップ製品ポートフォリオを使用してコンテナ化されたアプリケーションのDevOpsユースケースを改善、簡易化するプロセスについて説明します。

テクノロジーの概要

NetApp解決策を使用したDevOpsには、次の主要コンポーネントが含まれています。

DevOpsの手法

DevOpsの手法は、自動化され、反復可能で容易に管理できる運用に重点が置かれます。この運用では、開発ワークフローが強化され、エンドユーザがコードを開発する環境を制御できるようになります。この解決策には、ネットアップテクノロジーがこのような運用の最大のメリットになる例とユースケースがいくつかあります。

コンテナオーケストレーション

現在、多数のコンテナオーケストレーションプラットフォームが使用されています。これらのプラットフォームのほとんどはKubernetesをベースにしていますが、それぞれに長所と短所があります。そのため、DevOpsワークフロー用のコンテナオーケストレーションプラットフォームを選択する際には、機能セットと統合について理解することが重要です。ネットアップは、NetApp Astra製品スイートを通じて、本格的なDevOpsユースケース向けに次のプラットフォームをサポートしています。

- ["Red Hat OpenShift のサービスです"](#) 4.6.8以降
- ["ランチマー"](#) 2.5以上
- ["Kubernetes"](#) 1.20以降
- ["VMware Tanzu Kubernetesグリッド"](#) 1.4以降
- ["VMware Tanzu Kubernetes Grid統合エディション"](#) 1.12.2+

ネットアップストレージシステム

ネットアップには、エンタープライズデータセンターやハイブリッドクラウド環境に最適なストレージシステムが複数あります。ネットアップのポートフォリオには、コンテナ化されたアプリケーションに永続的ストレージを提供できる NetApp ONTAP、NetApp Element、および NetApp E シリーズストレージシステムが含まれています。

詳細については、ネットアップのWebサイトを参照してください "[こちらをご覧ください](#)"。

ネットアップとストレージの統合

NetApp Astra Control Centerは、オンプレミス環境に導入され、信頼性の高いネットアップのデータ保護テクノロジーを基盤とするステートフルKubernetesワークロード向けに、豊富なストレージサービスとアプリケーション対応データ管理サービスを提供します。

詳細については、NetApp Astra の Web サイトをご覧ください "[こちらをご覧ください](#)"。

Astra Tridentは、コンテナやKubernetesディストリビューション向けの、完全にサポートされているオープンソースのストレージオーケストレーションツールです。 {k8s_distribution_name} などが挙げられます。

詳細については、Astra Trident の Web サイトをご覧ください "[こちらをご覧ください](#)"。

DevOpsの概要

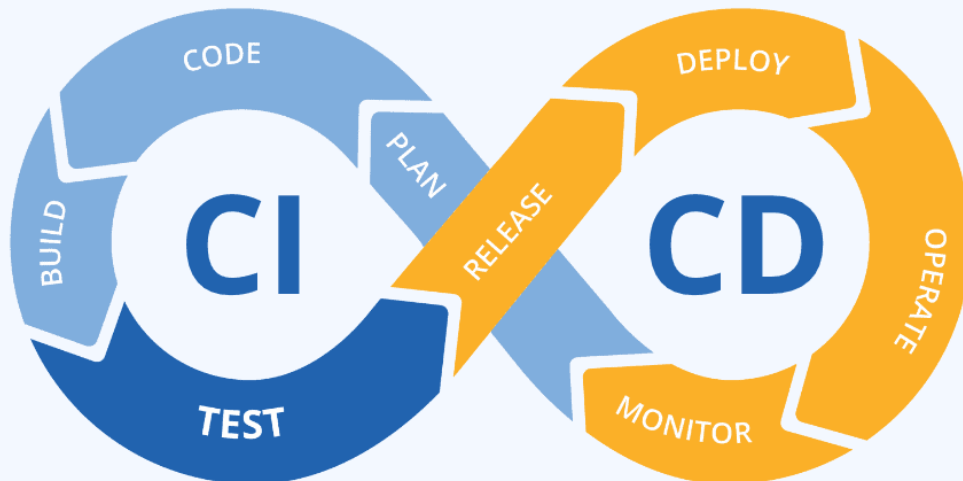
ここ数年、ソフトウェアを開発している組織がDevOpsの概念をすでに採用しています。DevOpsの手法は組織の壁を取り払い、開発チームと運用チームをより緊密に連携させます。DevOpsの手法は、サービス提供の高速化、可用性の向上、サービスとアプリケーションの安定化を可能にし、チームの生産性を向上させます。また、自動化フレームワークの採用は、大規模なアプリケーションの構築、テスト、運用、完全に自動化されたインフラプラットフォームやスタックの管理など、成功の鍵となる要素でもあります。以下に、DevOpsの一般的なユースケースをいくつか紹介します。DevOpsの実践で実践している実践的な経験を強化するために、ネットアップのソリューションを導入することができます。

DevOpsのユースケース

DevOpsには普遍的に受け入れられている単一の定義はありませんが、DevOps実践者向けのソリューションには、大規模な実装、繰り返し、管理を容易に行える同様の構造やイデオロギーが含まれています。以降のセクションでは、ネットアップのソリューションで実現するDevOpsワークフローのユースケースについて説明します。

継続的統合、継続的導入、継続的導入（CI / CD）

継続的統合、継続的導入、継続的導入（CI / CD）は、コードの更新、テスト、導入を一貫して自動化する方法を確立することで、コーディング手法の実装と変革を開発者に奨励するコーディング哲学です。ほとんどのDevOpsワークフローでCI / CDを実装する最も一般的な方法は、CI / CDパイプラインを使用する方法であり、この方法を実現するために役立つサードパーティ製のソフトウェアアプリケーションがいくつかあります。



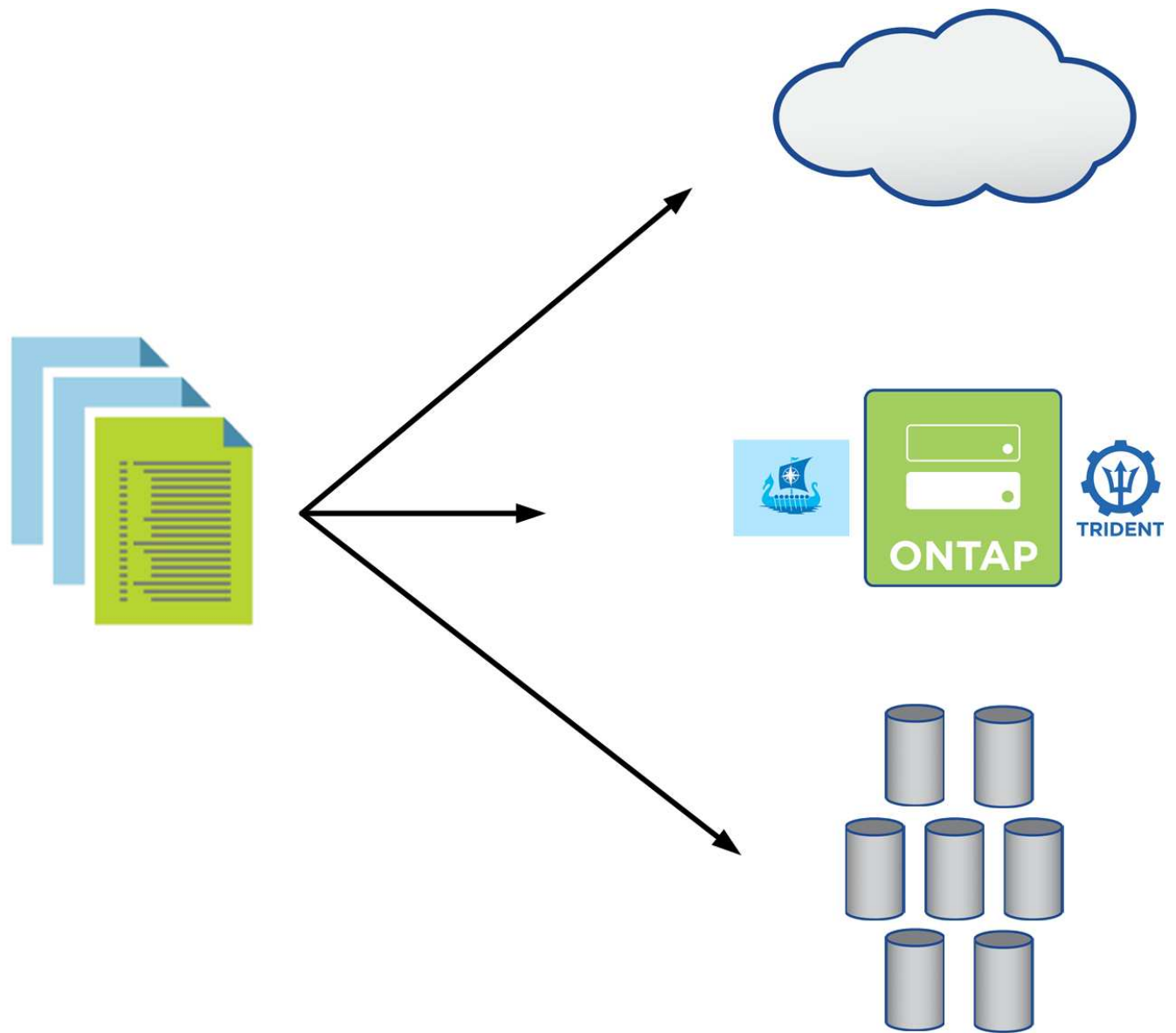
CI / CDタイプのワークフローに役立つ一般的なアプリケーションの例を次に示します。

"アルゴCD"
"Jenkins"
"テクトン"

このテクニカルレポートの後半で紹介するユースケースの中には、Jenkinsで紹介したものもありますが、CI / CDの主な原理は、組織が独自の方法で実装したどのツールにも適用できます。

コードとしてのインフラ

Infrastructure as codeは、自動化されたコマンド、API、およびソフトウェア開発キット（SDK）を通じてITリソースのプロビジョニングと管理を支援します。この概念は、開発者が目標を達成できなくなる可能性のある物理データセンターやリソースの制限を取り除くことで、DevOpsエクスペリエンスを大幅に向上させます。



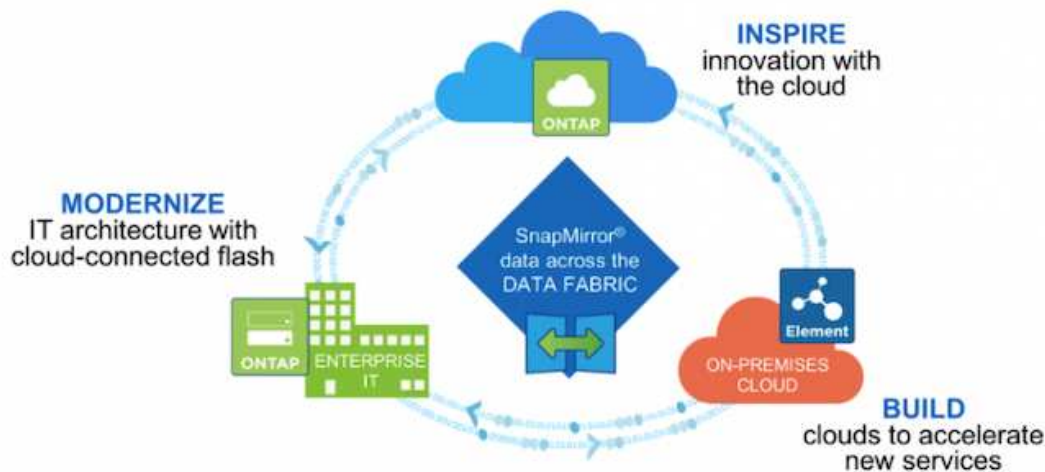
エンドユーザーは、などのプログラミング言語を頻繁に使用します "Python" などの自動化ツールを使用できます "Ansible" または "パペット" 必要に応じて開発者が呼び出すことができる、自動化された反復可能なインフラ拡張アクションを作成するため。

NetApp ONTAP と Astra Control には、パブリック向けの API と Ansible モジュールまたはソフトウェア開発ツールキットが含まれているため、運用を自動化しやすく、DevOps プロセスへの統合が容易です。

ネットアップストレージシステムの概要

ネットアップには、Astra Trident と Astra Control で認定された複数のストレージプラットフォームがあり、コンテナ化されたアプリケーションのデータをプロビジョニング、保護、管理し、DevOps のスループットを定義して最大化するのに役立ちます。

ネットアップには、Astra Trident と Astra Control で認定された複数のストレージプラットフォームがあり、コンテナ化されたアプリケーションのデータをプロビジョニング、保護、管理できます。



- AFF システムと FAS システムは、NetApp ONTAP を実行し、ファイルベース（NFS）とブロックベース（iSCSI）の両方のユースケースにストレージを提供します。
- Cloud Volumes ONTAP と ONTAP Select は、それぞれクラウドと仮想スペースに同じメリットをもたらします。
- NetApp Cloud Volumes Service（AWS / GCP）と Azure NetApp Files は、クラウドでファイルベースのストレージを提供します。



ネットアップのポートフォリオに含まれる各ストレージシステムでは、データ管理とオンプレミスサイトとクラウド間の移動の両方を容易に行えるため、データはアプリケーションの配置場所になります。

次のページでは、{solution_name} 解決策 で検証されたネットアップストレージシステムに関する追加情報を使用しています。

- ["NetApp ONTAP"](#)

NetApp ONTAP

NetApp ONTAP は、わかりやすい GUI、自動化統合機能を備えた REST API、AI に基づく予測分析と修正措置、無停止のハードウェアアップグレード、ストレージ間インポートなどの機能を備えた強力なストレージソフトウェアツールです。

NetApp ONTAP は、わかりやすい GUI、自動化統合機能を備えた REST API、AI に基づく予測分析と修正措置、無停止のハードウェアアップグレード、ストレージ間インポートなどの機能を備えた強力なストレージソフトウェアツールです。

NetApp ONTAP ストレージシステムの詳細については、を参照してください ["ネットアップの ONTAP Web サイト"](#)。

ONTAP は以下の機能を提供します。

- NFS、CIFS、iSCSI、FC、FCoE を同時にデータアクセスと管理できるユニファイドストレージシステム FC-NVMe プロトコルが必要です。
- 導入モデルには、オンプレミスのオールフラッシュ、ハイブリッド、オール HDD のハードウェア構成、ONTAP Select などのサポートされるハイパーバイザーを使用する VM ベースのストレージプラットフォーム、Cloud Volumes ONTAP などのクラウドがあります。
- ONTAP システムでは、データの自動階層化、インラインデータ圧縮、重複排除、コンパクションがサポートされ、データストレージ効率が向上しています。
- ワークロードベースの QoS 制御ストレージ：
- パブリッククラウドとのシームレスな統合により、データの階層化と保護を実現 ONTAP は、あらゆる環境に対応する堅牢なデータ保護機能も備えています。
 - * NetApp Snapshot コピー。* 最小限のディスク・スペースでデータをポイント・イン・タイムで高速バックアップし、パフォーマンス・オーバーヘッドを追加する必要はありません。
 - * NetApp SnapMirror。* 1 つのストレージ・システムから別のストレージ・システムへデータの Snapshot コピーをミラーリングします。ONTAP では、他の物理プラットフォームやクラウドネイティブのサービスへのデータのミラーリングもサポートされています。
 - * NetApp SnapLock。* 指定された期間にわたって上書きまたは消去できない特殊なボリュームに書き込むことにより、書き換え不可能なデータを効率的に管理します。
 - * NetApp SnapVault。* は、複数のストレージ・システムのデータを、指定されたすべてのシステムのバックアップとして機能する中央の Snapshot コピーにバックアップします。
 - * NetApp SyncMirror。* 同じコントローラに物理的に接続された 2 つの異なるディスクプレックスに対して、データをリアルタイムで RAID レベルでミラーリングします。
 - * NetApp SnapRestore * を使用すると、Snapshot コピーからオンデマンドでバックアップされたデータを迅速にリストアできます。
 - * NetApp FlexClone。* Snapshot コピーに基づいて、ネットアップボリュームの読み書き可能なフルコピーを瞬時にプロビジョニングできます。

ONTAP の詳細については、を参照してください ["ONTAP 9 ドキュメンテーション・センター"](#)。



NetApp ONTAP は、オンプレミス、仮想環境、クラウド環境で利用できます。



ネットアップのプラットフォーム

NetApp AFF/FAS

ネットアップは、堅牢なオールフラッシュ（AFF）およびスケールアウトハイブリッド（FAS）ストレージプラットフォームを提供し、低レイテンシのパフォーマンス、統合データプロテクション、マルチプロトコルのサポートのそれぞれに合わせてカスタマイズします。

どちらのシステムも、NetApp ONTAP データ管理ソフトウェアを搭載しています。NetAppは、シンプルで可用性の高いクラウド統合ストレージ管理を実現する業界最先端のデータ管理ソフトウェアで、データファブリックのニーズに合わせてエンタープライズクラスのスピード、効率性、セキュリティを提供します。

NetApp AFF / FAS プラットフォームの詳細については、をクリックしてください ["こちらをご覧ください"](#)。

ONTAP Select の場合

ONTAP Select は、お客様の環境のハイパーバイザーに導入できる、ソフトウェアで定義された NetApp ONTAP の導入です。VMware vSphereまたはKVMにインストールでき、ハードウェアベースのONTAP システムの全機能とエクスペリエンスを提供します。

ONTAP Select の詳細については、をクリックしてください ["こちらをご覧ください"](#)。

ロード向けに、充実したストレージサービスとアプリケーション対応データ管理サービスを提供します。Astra Control Service は、クラウドネイティブの Kubernetes 環境でステートフルワークロードをサポートするために利用できます。Astra Control Centerは、 {k8s_distribution_name} などのエンタープライズKubernetes プラットフォームをオンプレミスで導入する場合に、ステートフルワークロードをサポートするために使用できます。詳細については、NetApp Astra Control の Web サイトをご覧ください ["こちらをご覧ください"](#)。

NetApp Astra Tridentは、コンテナ向けのオープンソースで完全にサポートされているストレージオーケストレーションツールであり、 {k8s_distribution_name} などのKubernetesディストリビューションに対応しています。詳細については、Astra Trident の Web サイトをご覧ください ["こちらをご覧ください"](#)。

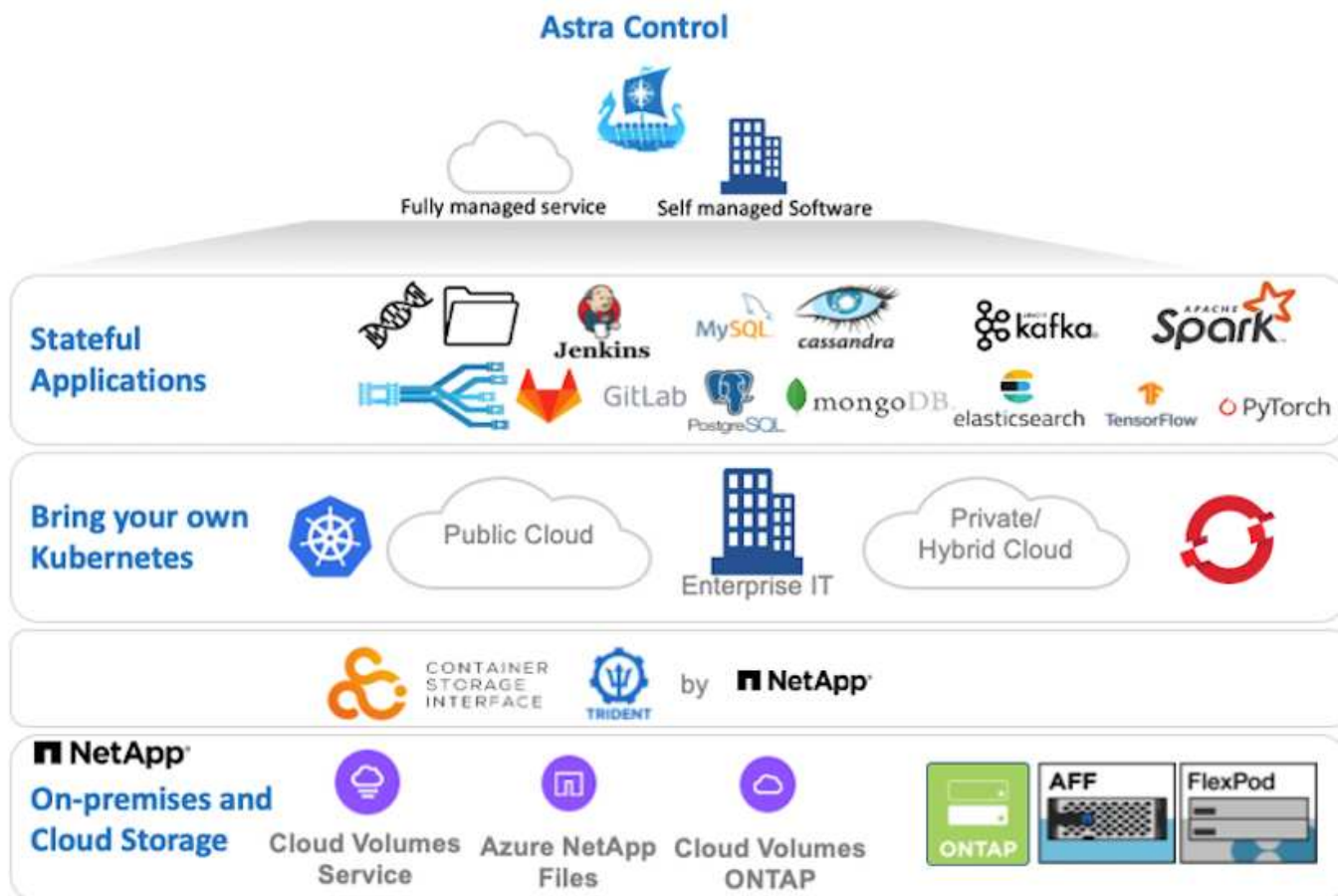
次のページには、 {solution_name} 解決策 でアプリケーションおよび永続的ストレージの管理用に検証されたネットアップ製品に関する追加情報 があります。

- ["ネットアップアストラコントロールセンター"](#)
- ["ネットアップアストラ Trident"](#)

NetApp Astra Controlの概要

NetApp Astra Control Center は、NetApp の信頼できるデータ保護テクノロジーを基盤とするオンプレミス環境に導入された、ステートフル Kubernetes ワークロード向けの豊富なストレージおよびアプリケーション対応データ管理サービスを提供します。

NetApp Astra Control Center は、オンプレミス環境に導入され、ネットアップのデータ保護テクノロジーを基盤とするステートフル Kubernetes ワークロード向けの充実したストレージサービスとアプリケーション対応データ管理サービスを提供します。



NetApp Astra Control Centerは、Astra Tridentストレージオーケストレーションツールを導入して、NetApp ONTAP ストレージシステムにストレージクラスとストレージバックエンドで構成されている {k8s_distribution_name} クラスタにインストールできます。

Astra Tridentの詳細については、を参照してください ["このドキュメントはこちら"](#)。

クラウド接続環境では、Cloud Insights を使用して高度なモニタリングとテレメトリを提供します。Cloud Insights 接続がない場合は、限定的な監視と計測（7日間の指標）を使用でき、オープン指標エンドポイントを通じてKubernetesの標準の監視ツール（PrometheusとGrafana）にエクスポートされます。

Astra Control Centerは、NetApp AutoSupportとActive IQのデジタルアドバイザー（デジタルアドバイザーとも呼ばれます）エコシステムに完全に統合されており、ユーザのサポート、トラブルシューティングの支援、使用状況の統計の表示を提供します。

支払い済みのAstra Control Centerに加えて、90日間の評価ライセンスも利用できます。評価版は、EメールとSlackコミュニティチャンネルを通じてサポートされます。お客様は、これらのリソース、その他のナレッジベース記事、および製品サポートダッシュボードから入手できるドキュメントにアクセスできます。

Astraポートフォリオの詳細については、を参照してください ["Astra の Web サイト"](#)。

Astra Control Centerのインストールと操作の詳細については、のマニュアルを参照してください ["こちらをご覧ください"](#)。

Astra Control Center自動化

Astra Control Centerには、プログラム経由でアクセスするための完全に機能するREST APIが用意されています。任意のプログラミング言語またはユーティリティを使用して、Astra Control REST APIエンドポイントとやり取りできます。このAPIの詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。

すぐに利用できる、Astra Control REST APIと連携するためのソフトウェア開発ツールキットを探している場合、ネットアップはAstra Control Python SDKツールキットを提供しています。このツールキットはこちらからダウンロードできます ["こちらをご覧ください"](#)。

環境に適したプログラミングでない場合に構成管理ツールを使用するには、ネットアップが公開しているAnsibleプレイブックのクローンを作成して実行します ["こちらをご覧ください"](#)。

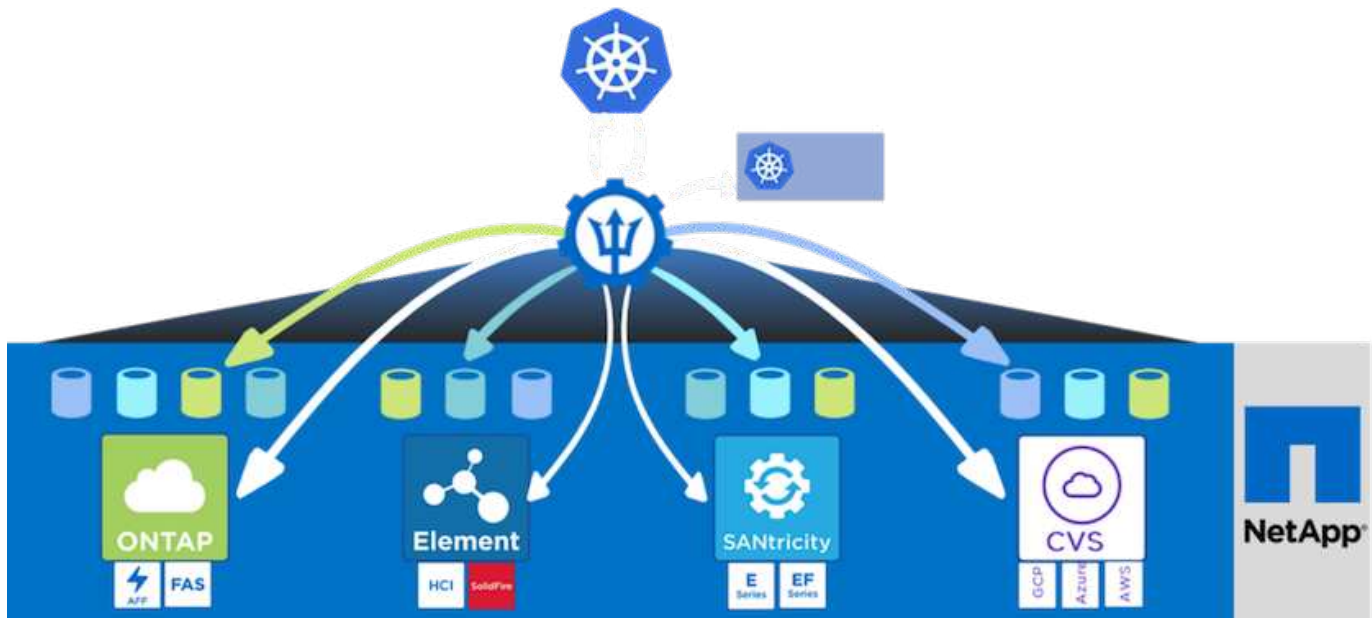
Astra Trident の概要

Astra Trident は、コンテナやKubernetes ディストリビューション向けの、Red Hat OpenShift などのオープンソースで完全にサポートされているストレージオーケストレーションツールです。

Astra Tridentは、コンテナやKubernetesディストリビューション向けの、完全にサポートされているオープンソースのストレージオーケストレーションツールです。 {k8s_distribution_name} などが挙げられます。Trident は、NetApp ONTAP や Element ストレージシステムを含むネットアップストレージポートフォリオ全体と連携し、NFS 接続と iSCSI 接続もサポートします。Trident を使用すると、ストレージ管理者の手を煩わせることなく、エンドユーザがネットアップストレージシステムからストレージをプロビジョニングして管理できるため、DevOps ワークフローが高速化されます。

管理者は、プロジェクトのニーズやストレージシステムモデルに基づいて複数のストレージバックエンドを構成し、圧縮、特定のディスクタイプ、QoS レベルなどの高度なストレージ機能を有効にして一定のレベルのパフォーマンスを保証できます。定義されたバックエンドは、プロジェクトの開発者が永続的ボリューム要求

(PVC) を作成し、永続的ストレージをオンデマンドでコンテナに接続するために使用できます。



Astra Tridentは、迅速な開発サイクルを実現し、Kubernetesと同様、年間4回リリースされます。

Tridentの最新バージョンは2022年4月に22.04にリリースされました。Trident のどのバージョンがサポートされているかを確認できます [Kubernetes ディストリビューションのテストに使用 "こちらをご覧ください"](#)。

20.04 リリース以降、Trident のセットアップはTrident オペレータによって実行されます。オペレータが大規模な導入を容易にし、Tridentのインストールの一部として導入されるポッドの自己修復などの追加サポートを提供します。

21.01 リリースでは、Trident Operator のインストールを容易にするために Helm チャートを使用できるようになりました。

のドキュメントを参照してください ["こちらをご覧ください"](#) Astra Tridentの導入と使用方法

ユースケースの検証：ネットアップAstraを使用したDevOps

ネットアップAstraを使用してDevOps向けに検証されたユースケースは次のとおりです。

- ["NetApp Astra Controlにより、CI / CDパイプラインへの保護を統合"](#)
- ["アストラ制御を活用して、事後分析とアプリケーションの復元を容易にします"](#)
- ["ネットアップのFlexCloneでソフトウェア開発を高速化"](#)

NetApp Astra Controlにより、**CI / CD**パイプラインへの保護を統合

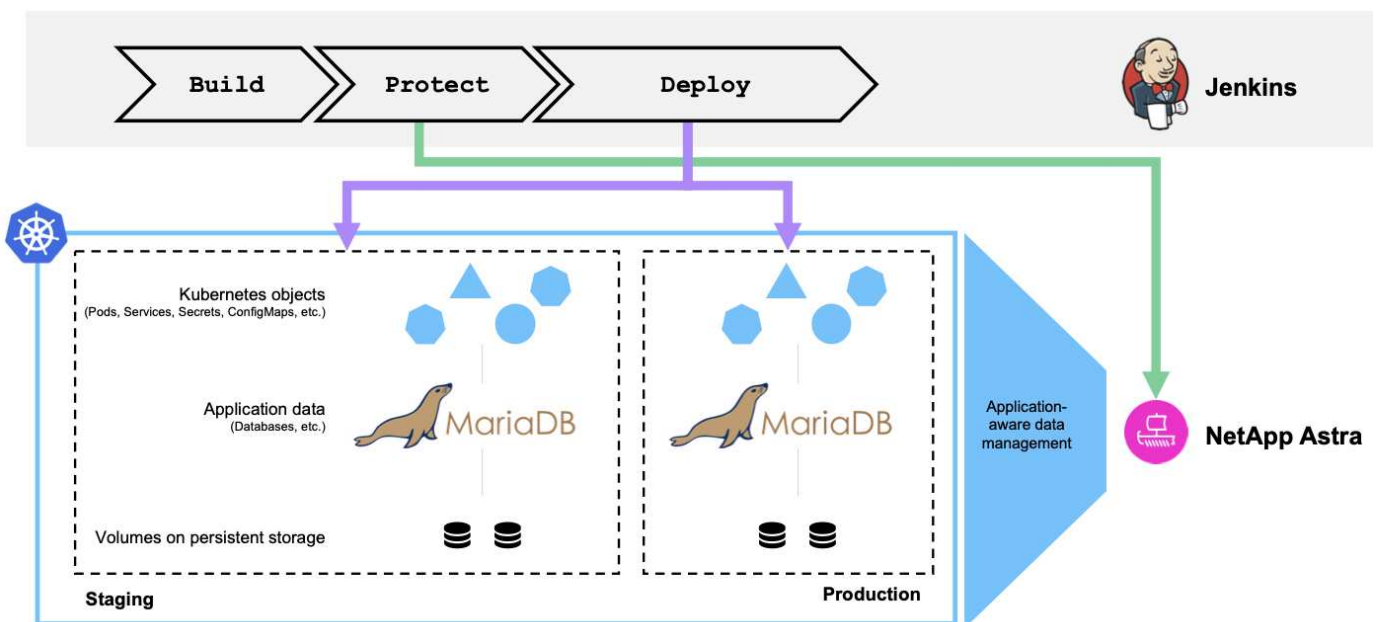
NetApp Astra Control Center は、NetApp の信頼できるデータ保護テクノロジーを基盤とするオンプレミス環境に導入された、ステータフル Kubernetes ワークロード向けの豊富なストレージおよびアプリケーション対応データ管理サービスを提供します。

概要

DevOpsワークフローの最も一般的な用途の1つは、継続的統合と継続的導入（CI / CD）パイプラインです。開発者が新しいコードをコミットする際に、アプリケーションでテストスイートの自動構築、統合、実行を行うことができます。通常、DevOpsエンジニアやサイト信頼性エンジニア（SRE）は、新機能の開発、回帰テスト、バグ修正、品質エンジニアリングなど、開発プロセスのさまざまな機能に特化したパイプラインを備えています。

チームの自動化レベルが上がると、本番環境のアプリケーションの変化のペースが圧倒的に高まります。そのため、一部のチームは、本番環境のアプリケーションやサービスの保護を希望しています。コードおよびコンテナイメージを保護するだけでなく、アプリケーションの状態、構成データ（アプリケーションに関連付けられたKubernetesオブジェクトやリソースなど）、およびアプリケーションの永続データも保護したいと考えています。

このユースケースでは、まず新しいバージョンのアプリケーションをステージング環境に導入してから本番環境に導入する、本番への昇格パイプラインについて詳しく見ていきます。この例は、主要なパブリッククラウドとオンプレミス環境に同様に当てはまります。アプリケーションの1つのバージョンの展開を示していますが、パイプラインは、青/緑、カナリアデプロイメントなどの他の戦略でも使用できます。CI/CDパイプラインの一部として、アプリケーションの完全なバックアップを作成してアプリケーションを保護します。本番環境のアプリケーションと、そのデータ、状態、設定をアプリケーションに対応したバックアップでバックアップすると、多数のDevOpsワークフローに役立ちます。



このユースケースの検証に使用したアプリケーションはです **"Magento"**は、Webベースのフロントエンドを備えたEコマース解決策、検索および分析機能用のElasticsearchインスタンス、ショッピングインベントリとトランザクションの詳細をすべて追跡するMariaDBデータベースです。このコンテナ化されたアプリケーションは、Red Hat OpenShiftクラスタにインストールされました。アプリケーション内のすべてのポッドで、永続ボリュームを使用してデータを格納しました。永続ボリュームは、コンテナストレージインターフェイスに準拠したKubernetes向けストレージオーケストレーションツールであるNetApp Astra Tridentによって自動的に作成され、ネットアップストレージシステムでストレージをプロビジョニングできるようになりました。さらに、Astra Control Centerのアプリケーション保護機能を利用するために、問題のアプリケーションはAstra Controlによって管理されました。Astra Controlは、永続的ボリュームに保存されたデータとともに、アプリケーションの状態を保存したアプリケーションのバックアップをトリガするために使用されました。使用した **"NetApp Astra Control Python SDK"** アプリケーションのバックアップを開始するプロセスを自動化するために、CI / CDパイプラインに導入されました。このパイプラインは、という一般的なCI / CDツールを使用して作成、実行されました **"Jenkins"**を選択すると、アプリケーションの構築、保護、導入のためのフローが自

動化されます。

CI/CDパイプラインに保護機能を導入するための前提条件と手順 について説明します。

ユースケースの検証の前提条件

前提条件として、次のツールまたはプラットフォームを導入および設定しました。

1. Red Hat OpenShift Container Platform
2. ネットアップのOpenShiftにTridentをインストールし、バックエンドからNetApp ONTAP システムを構成
3. NetApp ONTAP バックエンドをポイントするデフォルトのストレージクラスが設定されている
4. OpenShiftクラスタにNetApp Astraコントロールセンターをインストール
5. OpenShiftクラスタをAstra Control Centerにマネージドクラスタとして追加
6. JenkinsをOpenShiftクラスタにインストールし、Dockerエンジンがインストールされたエージェントノードで構成します

アプリケーションをインストールしています

まず、ステージング環境と本番環境にアプリケーションを最初にインストールします。このユースケースでは、この手順が前提条件となるため、手動で実行します。CI / CDパイプラインは、アプリケーションの新しいバージョンリリースの結果として、以降のビルドおよび導入ワークフローに使用されます。

この使用事例の本番環境は「Magent-prod」という名前のネームスペースであり、対応するステージング環境はRed Hat OpenShiftクラスタ上で構成される「Magent-staging」という名前のネームスペースです。アプリケーションをインポートするには、次の手順を実行します。

1. bitnami helmチャートを使用して、生産環境にMagentoアプリケーションをインストールします。ジェントポッドとMariaDBポッドにRWX PVSを使用します。

```
[netapp-user@rhel7 na_astra_control_suite]$ helm install --version 14
magento bitnami/magento -n magento-prod --create-namespace --set
image.tag=2.4.1-debian-10-
r11,magentoHost=10.63.172.243,persistence.magento.accessMode=ReadWriteMa
ny,persistence.apache.accessMode=ReadWriteMany,mariadb.master.persistenc
e.accessModes[0]=ReadWriteMany
```



Magento bitnami Helmチャートには、Magento GUIサービスを公開するためのロードバランササービスが必要です。使用しました **"MetalLB"** この例では、オンプレミスのロードバランササービスを提供します。

2. 数分後に、すべてのポッドとサービスが実行されていることを確認します。

```
[netapp-user@rhel7 na_astra_control_suite]$ oc get pods -n magento-prod
NAME                                READY   STATUS
RESTARTS   AGE
magento-9d658fd96-grxmt            1/1     Running
0         49m
magento-elasticsearch-coordinating-only-69869cc5-768rm  1/1     Running
0         49m
magento-elasticsearch-data-0       1/1     Running
0         49m
magento-elasticsearch-master-0     1/1     Running
0         49m
magento-mariadb-0                  1/1     Running
0         49m
```

3. ステージング環境についても同じ手順 を繰り返します。

Astra Control Centerで**Magento**アプリケーションを管理します

1. [アプリケーション]に移動し、[検出されたアプリケーション]タブを選択します。
2. 本番環境でMagentoアプリケーション(「Magent-prod」)の省略記号をクリックし、「管理」をクリックします。
3. Magentoアプリケーションは、Astra Control Centerによって管理されるようになりました。Astra Controlでサポートされているすべての操作をアプリケーションで実行できます。アプリケーションのバージョンも記録します。

 **magento-prod**

Available ▼

App status

Healthy

App protection status

Partially Protected

Images

docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16
docker.io/bitnami/magento:2.4.1-debian-10-r11
docker.io/bitnami/mariadb:10.3.23-debian-10-r38


Protection schedule

Disabled

Group

■ magento-prod

Cluster

 ocp-vmw

4. ステージング環境でMagentoアプリケーションを管理するための手順を繰り返します(「Magent-staging」)。

保護機能を統合した**CI / CD**パイプライン

新しいバージョンのアプリケーションを使用する場合は、CI / CDパイプラインを使用してコンテナイメージを作成し、ステージング環境と本番環境の両方のバックアップを作成し、新しいバージョンのアプリケーションをステージング環境に導入し、本番環境への昇格の承認を待ちます。その後、新しいバージョンのアプリケーションを本番環境に導入します。CI / CDパイプラインを使用するには、次の手順を実行します。

1. Jenkinsにログインし、必要なクレデンシャルを作成します。Magento作成する場合は1つ、MariaDB管理作成する場合は1つ、MariaDBルート作成する場合は3つ目です。

2. Manage Jenkins > Manage Credentialsと進み、適切なドメインをクリックします。
3. [資格情報の追加]をクリックし、[種類]を[パスワードと有効範囲を使用するユーザー名]に設定して[グローバル]に設定します。ユーザー名、パスワード、および資格情報のIDを入力し、[OK]をクリックします。

Dashboard > Credentials > System > Global credentials (unrestricted)

Back to credential domains

Add Credentials

Kind
Username with password

Scope
Global (Jenkins, nodes, items, all child items, etc)

Username
admin

☐ Treat username as secret

Password

ID
magento-cred

Description

OK

4. 他の2つのクレデンシャルについても同じ手順を繰り返します。
5. ダッシュボードに戻り、[新しいアイテム]をクリックしてパイプラインを作成し、[パイプライン]をクリックします。
6. Jenkinsfileからパイプラインをコピーします ["こちらをご覧ください"](#)。
7. パイプラインをJenkinsパイプラインセクションに貼り付け、保存をクリックします。
8. Helmチャートバージョン、アップグレード先のMagentoアプリケーションバージョン、Astraツールキットバージョン、Astra Control Center FQDN、APIトークン、インスタンスIDなど、Jenkinsパイプラインのパラメータをそれぞれの詳細に入力します。本番環境とステージング環境の両方でDockerレジストリ、ネームスペース、MagentoのIPを指定し、作成したクレデンシャルのクレデンシャルIDも指定します。

```
MAGENTO_VERSION = '2.4.1-debian-10-r14'
CHART_VERSION = '14'
RELEASE_TYPE = 'MINOR'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxxxxxx'
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'
DOCKER_REGISTRY = 'docker.io/netapp-solutions-cicd'
PROD_NAMESPACE = 'magento-prod'
PROD_MAGENTO_IP = 'x.x.x.x'
STAGING_NAMESPACE = 'magento-staging'
STAGING_MAGENTO_IP = 'x.x.x.x'
MAGENTO_CREDS = credentials('magento-cred')
MAGENTO_MARIADB_CREDS = credentials('magento-mariadb-cred')
MAGENTO_MARIADB_ROOT_CREDS = credentials('magento-mariadb-root-cred')
```


9. [今すぐ構築]をクリックしますパイプラインが実行を開始し'ステップを進めますアプリケーションイメージは最初にビルドされ、コンテナレジストリにアップロードされます。


Build & Publish Segment	Build Docker Image	Publish Image to Registry	Protect & Deploy Segment	Install & Configure Pre-requisites	Download & Configure Astra Toolkit	Backup Tasks	Backup of Staging Env	Backup of Production Env	Deploy to Staging environment [Minor/Patch]	Deploy to Staging environment [Major]	Promote to Production?	Deploy to Production environment [Minor/Patch]	Deploy to Production environment [Major]	Delete temporary files
4s	24s	5s	213ms	40s	2s	290ms	1min 38s	1min 2s	6min 29s	229ms	361ms	2min 57s	200ms	850ms
3s														
18min 29s														


10. アプリケーションのバックアップは、Astra Controlを使用して開始します。

The screenshot shows the Astra Control Center interface for an application named 'magento-prod'. At the top, the application status is 'Available'. Below this, there are two main sections: 'App status' showing 'Healthy' and 'App protection status' showing 'Partially Protected'. Under 'App status', a list of images is provided: 'docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16', 'docker.io/bitnami/magento:2.4.1-debian-10-r11', and 'docker.io/bitnami/mariadb:10.3.23-debian-10-r38'. The 'Protection schedule' is 'Disabled'. The 'Group' is 'magento-prod' and the 'Cluster' is 'ocp-vmw'. Below this, there is a tabbed interface with 'Data protection' selected. It shows a table of backup entries. The first entry is 'upgrade-prod-2-4-1-debian-10-r20', which is 'Ready', 'On-Schedule/On-Demand', created on '2021/10/29 14:43 UTC', and is currently 'Running'.

11. バックアップステージが正常に完了したら、Astra Control Centerからのバックアップを確認します。


magento-prod
Available



App status
Healthy


App protection status
Partially Protected

Images
 docker.io/bitnami/elasticsearch:6.8.10-debian-10-r16
 docker.io/bitnami/magento:2.4.1-debian-10-r11
 docker.io/bitnami/mariadb:10.3.23-debian-10-r38

Protection schedule
 Disabled

Group
 magento-prod

Cluster
 ocp-vmw

Overview

Data protection

Storage

Resources

Activity

Actions

Configure protection policy

Search

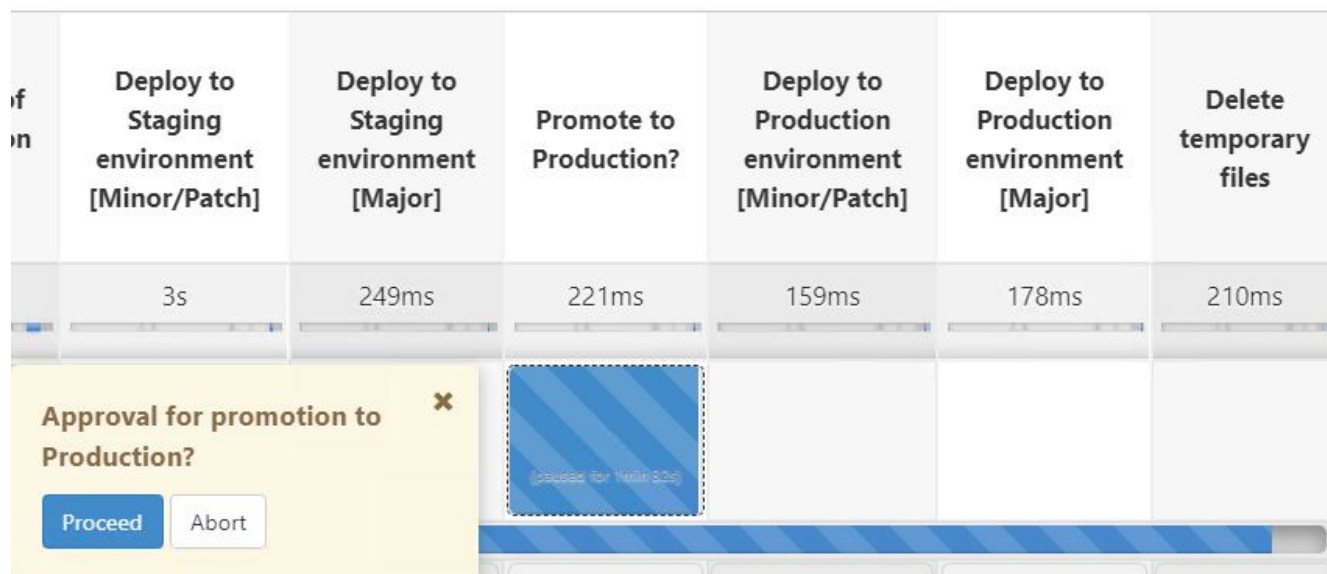
1-8 of 8 entries

Name	Ready	On-Schedule/On-Demand	Created	Actions
upgrade-prod-2-4-1-debian-10-r20	Healthy	On-Demand	2021/10/29 14:43 UTC	Available

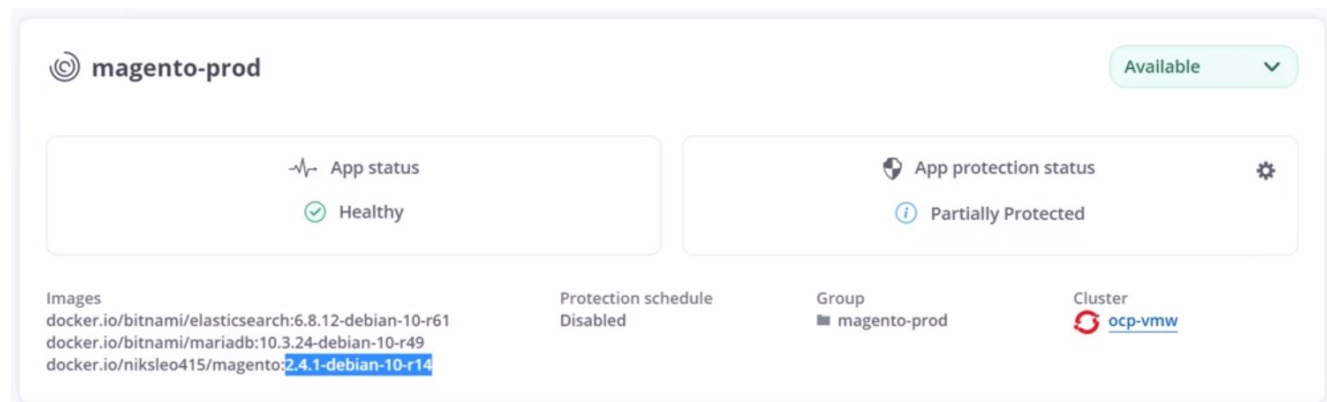
12. 新しいバージョンのアプリケーションがステージング環境に展開されます。

Build & Publish Segment	Build Docker Image	Publish Image to Registry	Protect & Deploy Segment	Install & Configure Pre-requisites	Download & Configure Astra Toolkit	Backup Tasks	Backup of Staging Env	Backup of Production Env	Deploy to Staging environment [Minor/Patch]	Deploy to Staging environment [Major]	Promote to Production?	Deploy to Production environment [Minor/Patch]	Deploy to Production environment [Major]	Delete temporary files
4s	47s	7s	238ms	1min 25s	2s	273ms	1min 53s	1min 18s	5min 20s	211ms	337ms	2min 39s	187ms	780ms
3s	4min 16s	30s	485ms	7s	3s	153ms	6min 9s	5min 9s						
7min 1s														

13. この手順が完了すると、ユーザが本番環境への導入を承認するまで待機します。この段階では、QAチームがいくつかの手動テストを実行し、本番環境を承認すると仮定します。次に、[承認]をクリックして、新しいバージョンのアプリケーションを本番環境に展開できます。



14. 本番アプリケーションが目的のバージョンにアップグレードされていることも確認します。



CI / CDパイプラインの一環として、アプリケーションに対応した完全なバックアップを作成してアプリケーションを保護できることを実証しました。アプリケーション全体が本番への昇格パイプラインの一部としてバックアップされているため、高度に自動化されたアプリケーションの導入について、自信を持って実行できます。アプリケーションのデータ、状態、設定を含むこのアプリケーション対応バックアップは、多数のDevOpsワークフローに役立ちます。予期しない問題が発生した場合は、アプリケーションの前のバージョンにロールバックすることが重要なワークフローとなります。

Jenkinsツールを使用してCI / CDワークフローをデモしましたが、コンセプトはさまざまなツールや戦略に簡単かつ効率的に外挿できます。このユースケースの実際の動作を確認するには、以下のビデオをご覧ください。

Astra Control Centerを使用したCI / CDパイプラインのデータ保護

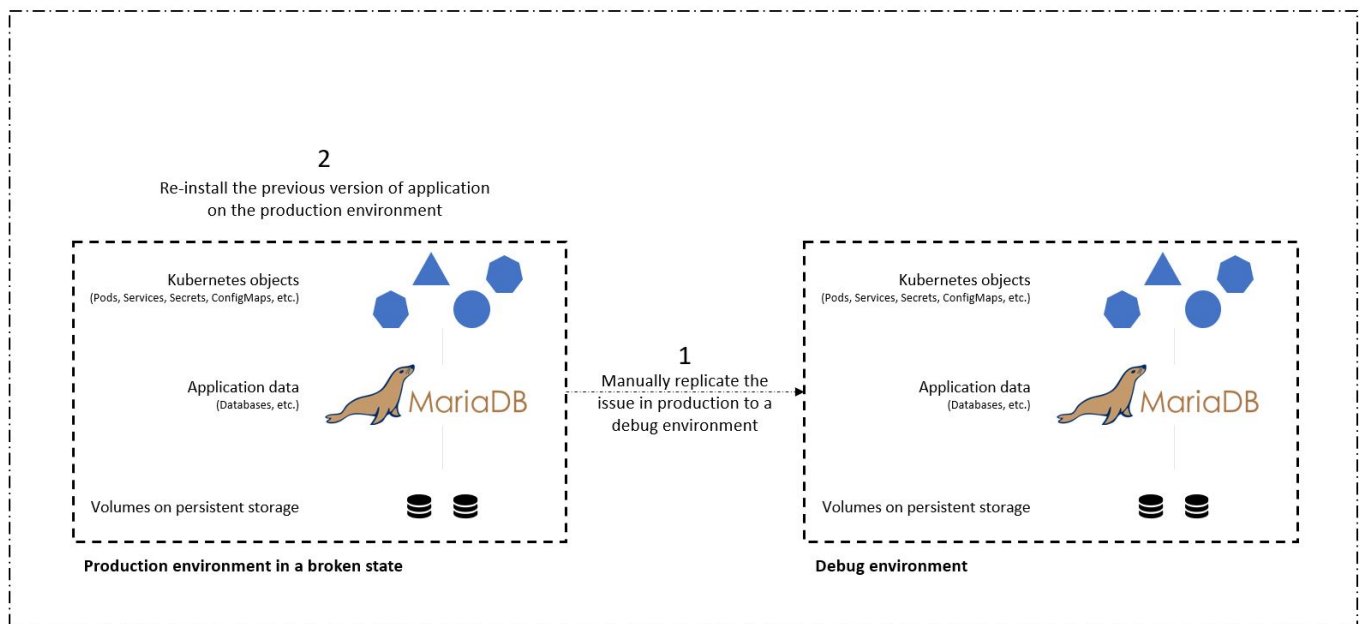
アストラ制御を使用すると、事後分析やアプリケーションのリストアが容易になります

NetApp Astra Control Center は、NetApp の信頼できるデータ保護テクノロジーを基盤とするオンプレミス環境に導入された、ステートフル Kubernetes ワークロード向けの豊富なストレージおよびアプリケーション対応データ管理サービスを提供します。

概要

を参照してください。"最初のユースケース"では、ネットアップのAstra Control Centerを使用してKubernetesでアプリケーションを保護する方法を紹介しました。このセクションでは、NetApp AstraツールキットのPython SDKを使用して、Astra Controlを介したアプリケーションバックアップを開発ワークフローに直接統合する方法について説明します。このアプローチにより、継続的統合/継続的導入（CI / CD）プロセスでオンデマンドバックアップを自動化することで、開発環境と本番環境の保護が可能になります。アプリケーションと整合性のあるデータ保護のこの追加レイヤーがCI / CDパイプラインと本番アプリケーションに追加されたことで、プロセスに何か問題が発生しても開発プロセスは安全になり、ビジネス継続性のプラクティスが促進されます。

従来のワークフローでは、アプリケーションを新しいバージョンにアップグレードするときにエラーが発生した場合、開発チームはお客様から提供されたバグレポートに基づいて問題のトラブルシューティングをリアルタイムで試みます。また、最初に問題が発生したときに、チームはアプリケーションを並列デバッグ環境に再配置して、そのプロセスをオフラインにすることもできます。以前のバージョンの古いコードベースを本番環境に再導入することで、アプリケーションを作業順序に復元できます。

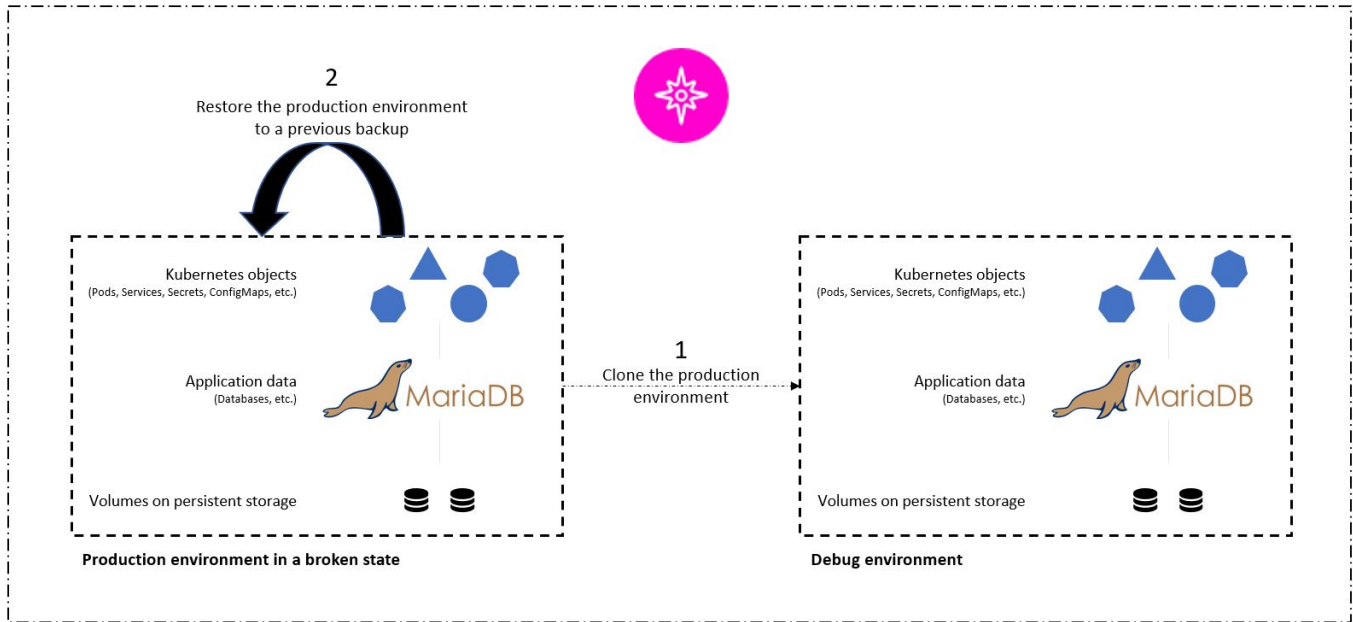


このアプローチは機能しますが、問題が発生したときに本番環境で使用されていたバージョンと破損した本番アプリケーションの状態が一致していることを確認する必要があります。また、リポジトリからコードを取得し、マシンイメージを再展開してアプリケーションを良好な稼働状態に復元することで、動作確認済みビルドを本番環境にプロモートするための時間も必要になります。また、このシナリオでは、本番環境のデータベース自体が、障害のあるコードによって破損していないかどうかを考慮しませんでした。データベースデータのバックアッププロセスが別に用意されているのは理想的ですが、公開時にアプリケーションの状態と整合性があると仮定する必要があります。ここでは、Astra Controlを使用して、ステートフルでアプリケーションと整合性のあるバックアップ、リストア、クローンを作成することのメリットが、まさにその価値を示しています。

まず、アストラ制御を使用して、アプリケーションの状態に関する事後分析を容易に行うことができます。そのためには、アプリケーションと整合性のある方法で、バグのある本番バージョンを並行テスト環境にクローニングします。この環境をバグ非表示状態にしておくと、リアルタイムで問題のトラブルシューティングを行うことができます。

さらに、Astra Controlでは、インプレースリストア機能がサポートされているため、本番アプリケーションを最後の許容可能なバックアップ（コードのバージョンが古い場合）にリストアできます。復元されたバージョンは、以前に割り当てられた入力IPを含む、アプリケーションと一貫性のあるステートフルな方法で、以前の

バグのある本番アプリケーションの位置を想定しています。そのため、フロントエンドにアクセスするお客様は、バックアップバージョンへの移行を認識しません。



ユースケースの検証の前提条件

前提条件として、次のツールまたはプラットフォームを導入および設定しました。

- Red Hat OpenShift Container Platform :
- NetApp ONTAP システムにバックエンドを設定して、OpenShiftにNetApp Astra Tridentをインストールします。
- NetApp ONTAP バックエンドをポイントするデフォルトのストレージクラスが設定されている
- OpenShiftクラスタにNetApp Astraコントロールセンターをインストール。
- OpenShiftクラスタをAstra Control Centerにマネージドクラスタとして追加。
- OpenShiftクラスタにJenkinsをインストールしました。
- 本番環境にインストールされたMagentoアプリケーション。このユースケースの本番環境は、Red Hat OpenShiftクラスタで「ジェント本番環境」という名前のネームスペースです。
- 本番アプリケーションはAstra Control Centerによって管理されます。
- Astra Controlでキャプチャされた、本番アプリケーションの正常なバックアップ。

クローニングとリストアのパイプライン

アプリケーションが新しいバージョンにアップグレードされたことを考慮して、本番環境のアプリケーション（「Magent-prod」）はアップグレード後に意図したとおりに動作しません。フロントエンドクエリから返されるデータがリクエストと一致しないか、データベースが実際に破損しているとします。パイプラインをクローニングしてリストアするには、次の手順を実行します。



This site can't be reached

10.63.172.243 took too long to respond.

Try:

- Checking the connection
- [Checking the proxy and the firewall](#)
- [Running Windows Network Diagnostics](#)

ERR_CONNECTION_TIMED_OUT

Reload

Details

1. Jenkinsにログインし、[新しいアイテム]、[パイプライン]の順にクリックしてパイプラインを作成します。
2. Jenkinsfileからパイプラインをコピーします "[こちらをご覧ください](#)".
3. パイプラインをJenkinsパイプラインセクションに貼り付け、保存をクリックします。
4. Jenkinsパイプラインのパラメータに、本番環境の現在のMagentoアプリケーションバージョン、Astra Control Center FQDN、APIトークン、本番環境とデバッグ環境のインスタンスIDとアプリケーション名またはネームスペース、ソースクラスタ名とデスティネーションクラスタ名など、それぞれの詳細を入力します。このユースケースのために、本番環境は「メント本番」と呼ばれるネームスペースであり、デバッグ環境はRed Hat OpenShiftクラスタで構成される「メントデバッグ」と呼ばれるネームスペースです。

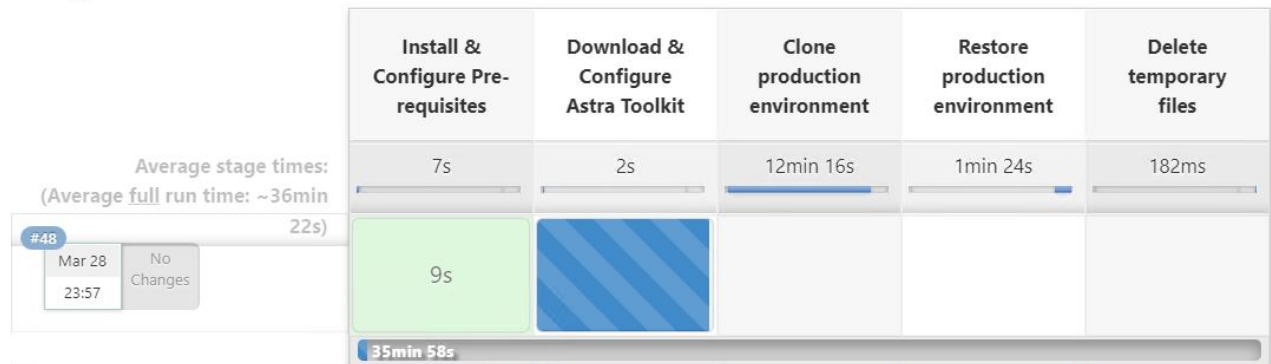
```
MAGENTO_VERSION = '2.4.1-debian-10-r14'
ASTRA_TOOLKIT_VERSION = '2.0.2'
ASTRA_API_TOKEN = 'xxxxxx'
ASTRA_INSTANCE_ID = 'xxx-xxx-xxx-xxx-xxx'
ASTRA_FQDN = 'netapp-astra-control-center.org.example.com'
PROD_APP_NAME = 'magento-prod'
DEBUG_APP_NAME = 'magento-debug'
DEBUG_NAMESPACE = 'magento-debug'
PROD_KUBERNETES_CLUSTER = 'ocp-vmw'
DEBUG_KUBERNETES_CLUSTER = 'ocp-vmw'
```

5. [今すぐ構築]をクリックしますパイプラインが実行を開始し'ステップを進めますアプリケーションは、最初に現在の状態でデバッグ環境にクローニングされ、その後、動作確認済みのバックアップにリストアされます。

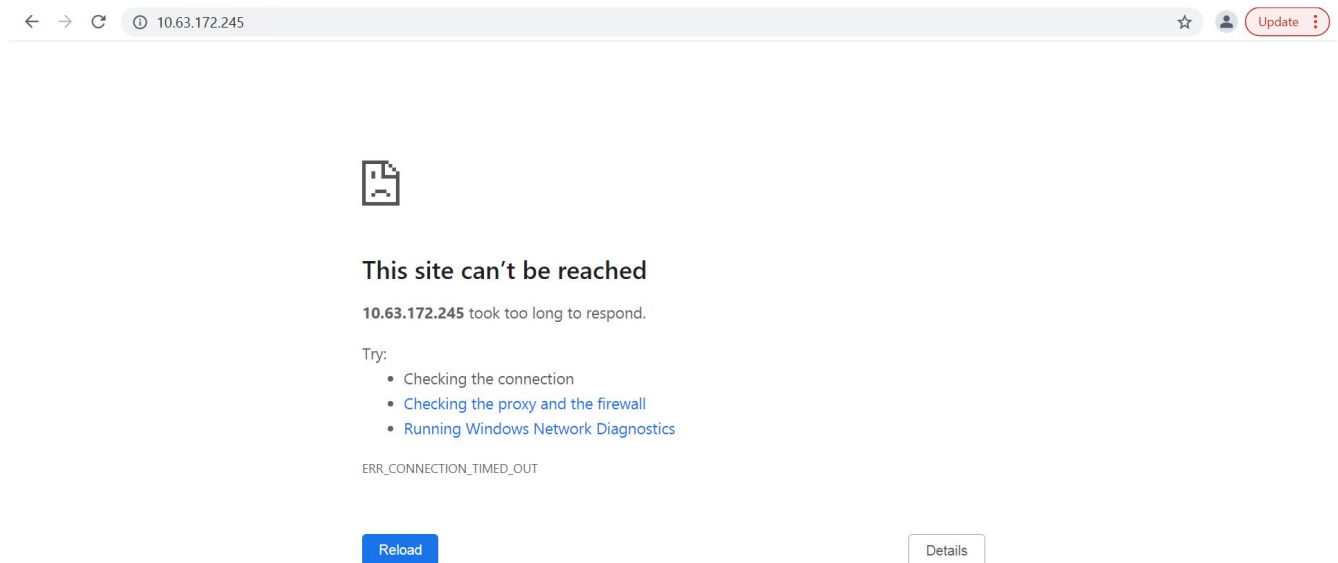
Pipeline magento_clone-for-triage_restore-from-backup



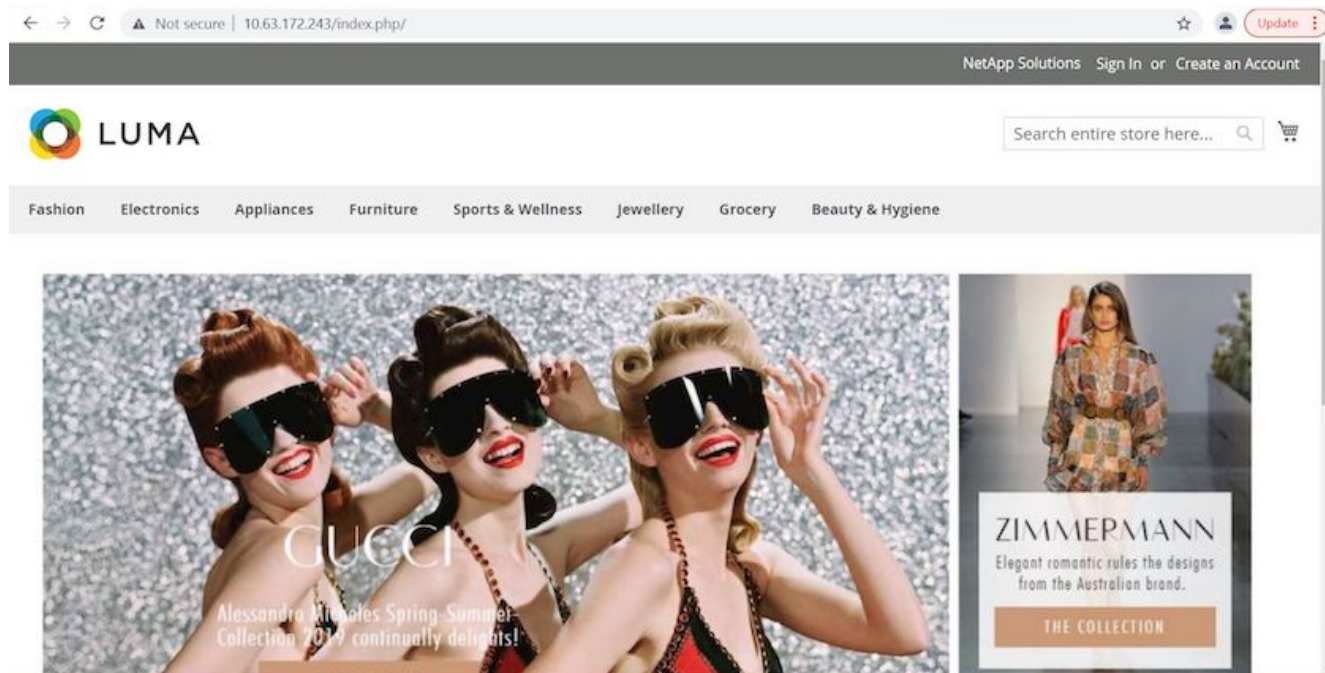
Stage View



6. クローニングしたアプリケーションのバージョンがバグを含むことを確認します。



7. 本番環境が稼働中のバックアップにリストアされ、本番環境のアプリケーションが想定どおりに動作することを確認します。



これら2つのオペレーションを同時に行うことで、通常の業務に迅速に復帰できます。このユースケースの実際の動作を確認するには、以下のビデオをご覧ください。

[NetApp Astra Control を活用して、事後分析とアプリケーションのリストアを実行](#)

NetApp FlexCloneテクノロジーでソフトウェア開発を高速化

このセクションでは、NetApp FlexCloneテクノロジーを使用して解決策を迅速に導入する方法について説明します。

概要

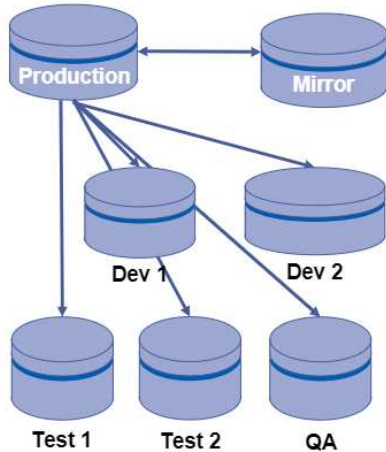
Kubernetesクラスタに導入されたアプリケーションをクローニングすると、開発者は、パートナーと環境を共有したり、現在作業しているバージョンを妨げずに開発環境で新しいバージョンのコードをテストしたりすることで、ワークフローを迅速化したいと考えています。これは非常に便利なツールです。Kubernetesアプリケーションのステートフルでアプリケーションと整合性のあるクローニングは、NetApp Astra Controlに含まれる主要な機能であり、アプリケーションのバックアップとリストアに加えて提供されます。さらに、同じストレージバックエンドを使用して同じKubernetesクラスタ内でアプリケーションをクローニングした場合、Astra Controlでは、永続的データボリュームの重複に対してNetApp FlexCloneテクノロジーがデフォルトで使用されるため、処理時間が大幅に短縮されます。このプロセスを短縮することで、クローニングした環境のプロビジョニングが完了し、数秒で使用できるようになります。そのため、開発者はテスト環境や開発環境を再導入する場合と比べて、作業を一時的に中断することなく再開できます。さらに、NetApp Astra Controlで使用するすべての機能をAPIで呼び出すことができるため、Ansibleなどの自動フレームワークに簡単に統合できます。このため、クローニング手順を開始するためにプレイブックまたはロールに必要な変更はわずかなため、環境のステージング時間をさらに短縮できます。

NetApp FlexCloneテクノロジーとは

NetApp FlexCloneテクノロジーは、NetApp FlexVol の書き込み可能なポイントインタイムSnapshotベースのコピーです。ほぼ瞬時にプロビジョニングされ、ソースボリュームのデータがすべて含まれます。新しいボリュームのデータがソースボリュームと異なる状態になるまで、追加のストレージスペースは消費されません。ステージング目的でデータの複数のコピーが有用で、ストレージシステムでボリュームのプロビジョニングに使

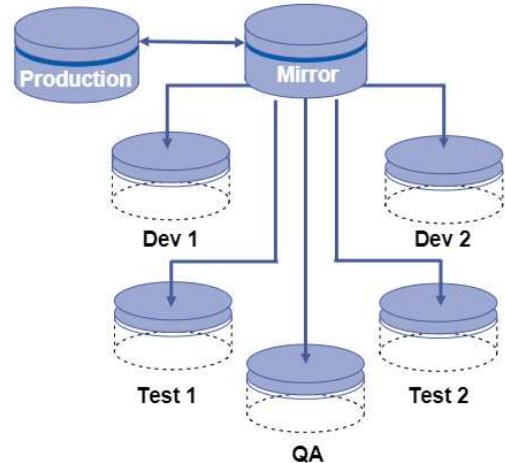
用できるリソースが限られている場合、開発環境やテンプレートベースの環境でよく使用されます。従来のストレージシステムではデータを何度もコピーする必要があるため、ストレージスペースや時間が大幅に消費されるため、NetApp FlexCloneテクノロジーを使用するとストレージに依存するタスクを高速化できます。

Traditional Data Copies



Traditional physical copies take additional time and consume additional storage space

NetApp FlexClone Copies



NetApp FlexClone copies are near instantaneous and only consume space when written to

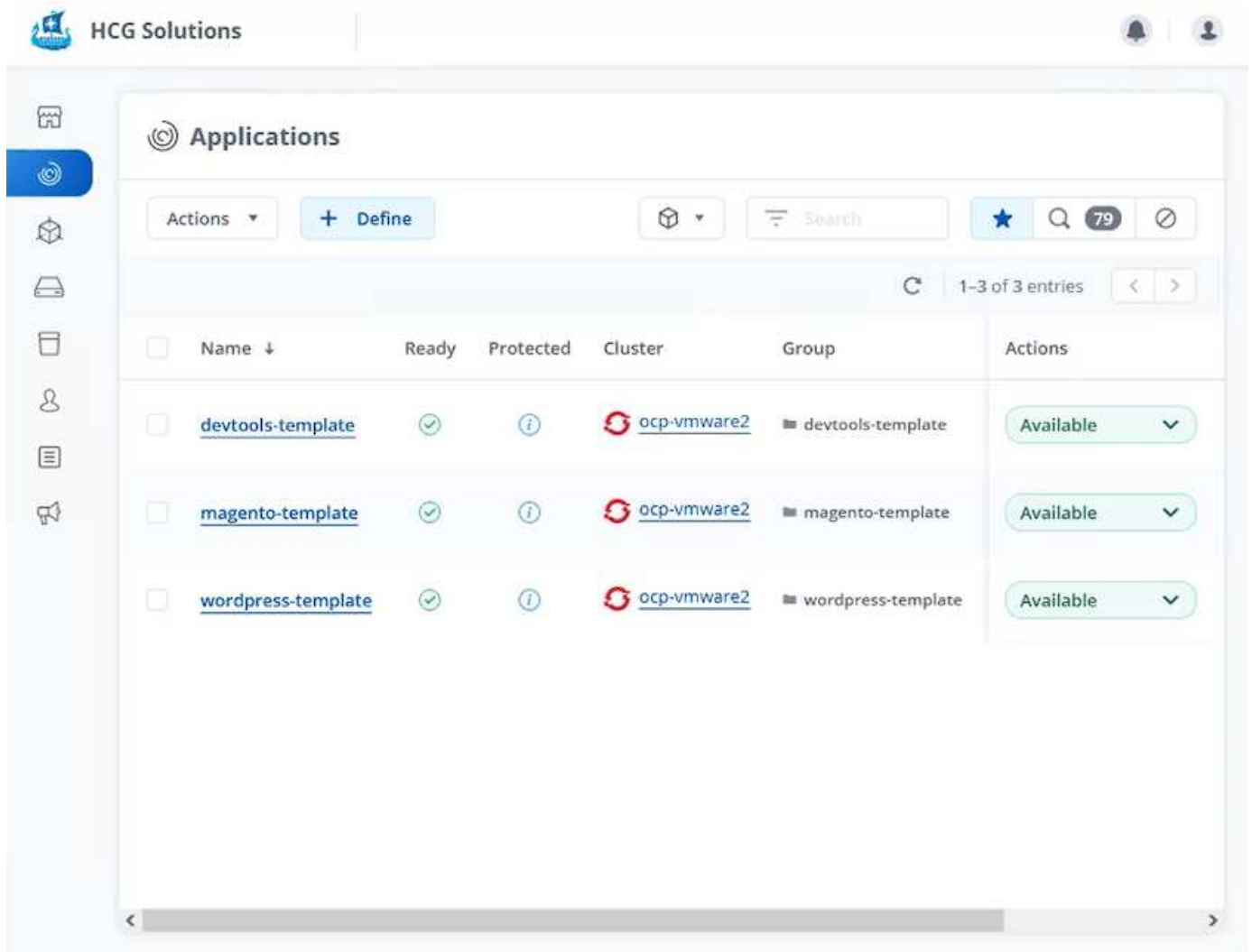
NetApp FlexCloneテクノロジーの詳細については、のページを参照してください ["ネットアップのドキュメント"](#)。

前提条件

1. Red Hat OpenShift 4.6.8+、Rancher 2.5+、Kubernetes 1.19+などのサポートされるKubernetesディストリビューション。
2. ネットアップアストラコントロールセンター21.12以降
3. NetApp ONTAP システム。ネットアップのTrident経由でストレージバックエンドを設定します。
4. Ansible 2.9以降
5. NetApp Astra Controlの管理対象アプリケーションとしてクローニングする環境用のテンプレート。

ユースケースの概要

このユースケースでは、次のワークフローのような情報が表示されます。



各環境はNetApp Astra制御によって管理され、ネットアップONTAP ストレージシステムに現在格納されている永続的ボリュームは、ネットアップAstra Tridentが提供するNFSバックエンドを使用している。

ユースケースの検証

1. ネットアップのソリューションエンジニアリングチームが提供するAnsibleツールキットをクローニングします。これには、クローニングのルールとアプリケーションの更新に関するプレイブックが含まれます。

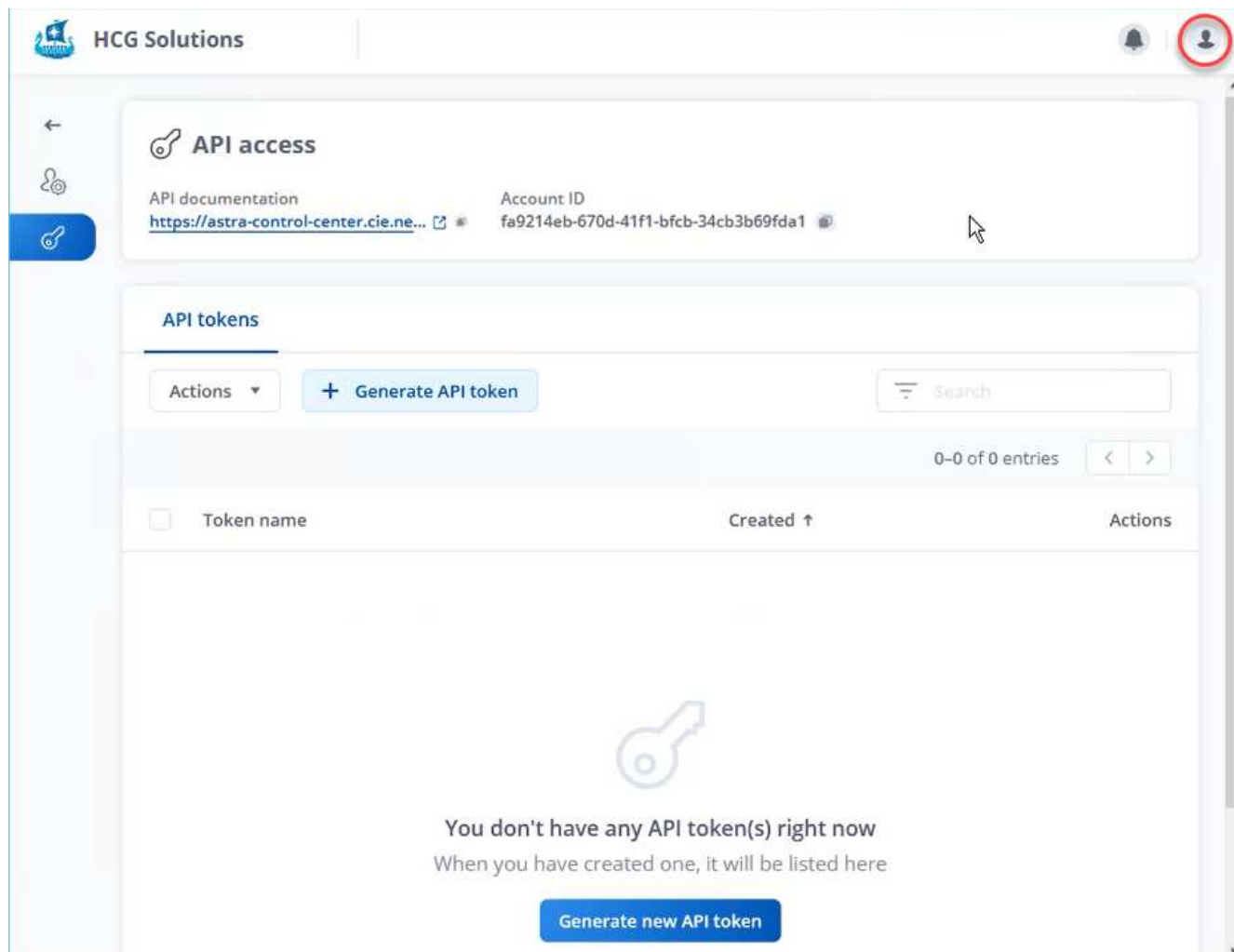
```
[netapp-user@rhel7 ~]$ git clone https://github.com/NetApp-Automation/na_astra_control_suite.git
[netapp-user@rhel7 ~]$ cd na_astra_control_suite
```

2. 'vars/clone_vars.yml'を編集し、Astra Control環境に適したグローバル値を入力します。

```
astra_control_fqdn: astra-control-center.example.com
astra_control_account_id: "xxxx-xxxx-xxxx-xxxx-xxxx"
astra_control_api_token: "xxxxx"
```




入力する必要があるグローバル環境値は、NetApp Astra ControlのAPIアクセスメニューにあるユーザプロフィールアイコンで確認できます。



3. グローバル変数が完成したら、複製する特定のアプリケーションの値を選択できます。DevTools環境を'Alan - DevTools'という個人環境にクローンを作成するには'次の手順を実行します

```
clone_details:
- clone_name: alan-devtools
  destination_namespace: alan-dev-namespace
  source_cluster_name: ocp-vmware2
  destination_cluster_name: ocp-vmware2
  source_application_name: devtools-template
```



クローン作成プロセスでNetApp FlexCloneテクノロジーを活用するには'src-cluster'と'dest-cluster'を同じにする必要があります

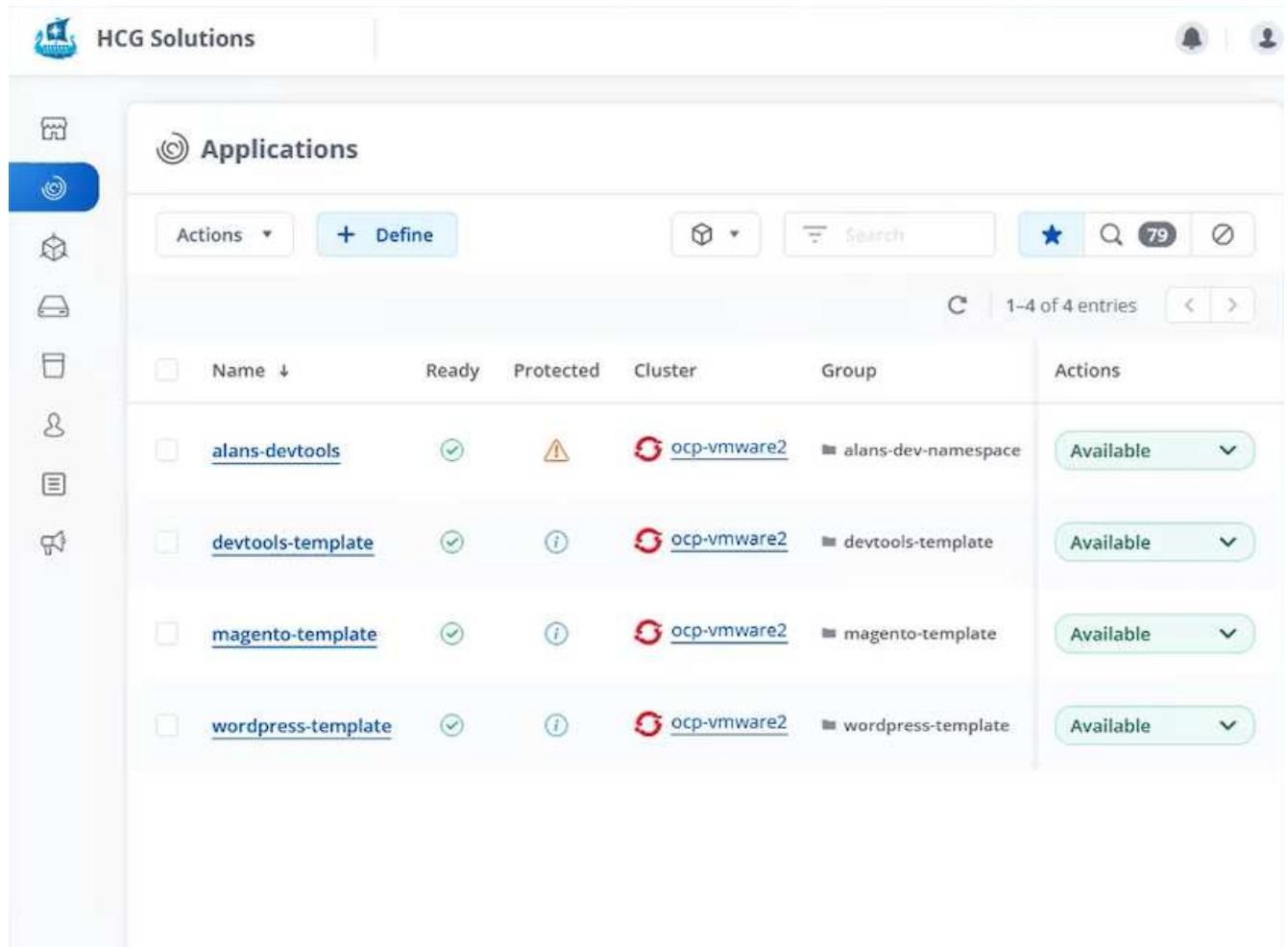
4. プレイブックを実行してアプリケーションをクローニングできるようになりました。

```
[netapp-user@rhel7 na_astra_control_suite]$ ansible-playbook -K clone_app_playbook.yml]
```



記載されたプレイブックは、rootユーザ、またはsudoプロセスを介して「-K」引数を渡してエスカレーションできるユーザが実行する必要があります。

5. プレイブックの実行が完了すると、クローニングされたアプリケーションがAstra Control Centerコンソールに表示されます。



6. ユーザは、アプリケーションが導入されたKubernetes環境にログインし、アプリケーションが新しいIPアドレスで公開されていることを確認して、開発作業を開始できます。

この使用例のデモとアプリケーションのアップグレード例については、以下のビデオをご覧ください。

[Astra ControlとNetApp FlexCloneテクノロジーでソフトウェア開発を高速化](#)

ビデオとデモ：NetApp Astraを使用したDevOps

次のビデオでは、このドキュメントで説明する機能の一部を紹介します。

[Astra Control Centerを使用したCI / CDパイプラインのデータ保護](#)

NetApp Astra Control を活用して、事後分析とアプリケーションのリストアを実行

Astra ControlとNetApp FlexCloneテクノロジーでソフトウェア開発を高速化

追加情報：ネットアップのAstraを使用したDevOps

このドキュメントに記載されている情報の詳細については、次の Web サイトを参照してください。

- NetApp のドキュメント

["https://docs.netapp.com/"](https://docs.netapp.com/)

- Astra Trident のドキュメント

["https://docs.netapp.com/us-en/trident/"](https://docs.netapp.com/us-en/trident/)

- NetApp Astra Control Center のドキュメント

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- Ansibleのドキュメント

["https://docs.ansible.com/"](https://docs.ansible.com/)

- Red Hat OpenShift のドキュメント

["https://access.redhat.com/documentation/en-us/openshift_container_platform/4.8/"](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.8/)

- Rancherドキュメント

["https://rancher.com/docs/"](https://rancher.com/docs/)

- Kubernetesのドキュメント

["https://kubernetes.io/docs/home/"](https://kubernetes.io/docs/home/)

NVA-1160：ネットアップでの Red Hat OpenShift

ネットアップ、Alan Cowles 氏と Nikhil M Kulkarni 氏

このリファレンスドキュメントでは、ネットアップによって検証済みの複数の異なるデータセンター環境に Installer Provisioned Infrastructure（IPI）を通じて導入された Red Hat OpenShift 解決策の導入を検証します。また、ネットアップストレージシステムとの統合についても、Astra Trident ストレージオーケストレーションツールを使用して永続的ストレージを管理することで詳しく説明します。最後に、解決策検証と実際の使用事例をいくつか確認して文書化します。

ユースケース

ネットアップ解決策を使用した Red Hat OpenShift は、次のユースケースでお客様に卓越した価値を提供するように設計されています。

- ベアメタル、Red Hat OpenStack Platform、Red Hat Virtualization、VMware vSphere に IPI（インストーラでプロビジョニングされたインフラ）を使用して導入した Red Hat OpenShift の導入と管理が容易です。
- OSP、RHV、vSphere、または OpenShift Virtualization を使用したベアメタルに導入された Red Hat OpenShift を使用して、エンタープライズコンテナと仮想化ワークロードのパワーを組み合わせたもの。
- ネットアップストレージと Kubernetes 向けオープンソースストレージオーケストレーションツールである Astra Trident とともに使用される Red Hat OpenShift の機能を紹介する実際の構成とユースケース。

ビジネスバリュー

企業は、新しい製品の作成、リリースサイクルの短縮、新機能の迅速な追加を目的として、DevOps の手法を採用する傾向に迫られています。即応性に優れた本来の性質から、コンテナやマイクロサービスは、DevOps の実践を支援するうえで重要な役割を果たします。しかし、エンタープライズ環境で本番環境規模で DevOps を実践する場合、独自の課題が生じ、基盤となるインフラに次のような一定の要件が課せられます。

- スタック内のすべてのレイヤで高可用性を実現します
- 導入手順の簡易化
- ノンストップオペレーションとアップグレード
- API ベースのプログラム可能なインフラで、マイクロサービスの即応性を維持します
- パフォーマンスを保証するマルチテナンシー
- 仮想ワークロードとコンテナ化されたワークロードを同時に実行できます
- ワークロードのニーズに応じてインフラを個別に拡張できる

ネットアップとともに Red Hat OpenShift を導入することで、これらの課題に対応し、お客様が選択したデータセンター環境に Red Hat OpenShift IPI を完全に自動で導入できるようになり、それぞれの問題に対処できる解決策が提供されます。

テクノロジーの概要

NetApp 解決策を使用した Red Hat OpenShift は、次の主要コンポーネントで構成されています。

Red Hat OpenShift Container Platform

Red Hat OpenShift Container Platform は、完全にサポートされているエンタープライズ向け Kubernetes プラットフォームです。Red Hat は、オープンソースの Kubernetes をいくつか強化して、コンテナ化されたアプリケーションの構築、導入、管理を完全に統合したすべてのコンポーネントを備えたアプリケーションプラットフォームを提供します。

詳細については、OpenShift の Web サイトを参照してください ["こちらをご覧ください"](#)。

ネットアップストレージシステム

ネットアップには、エンタープライズデータセンターやハイブリッドクラウド環境に最適なストレージシステ

ムが複数あります。ネットアップのポートフォリオには、コンテナ化されたアプリケーションに永続的ストレージを提供できる NetApp ONTAP、NetApp Element、および NetApp E シリーズストレージシステムが含まれています。

詳細については、ネットアップの Web サイトをご覧ください ["こちらをご覧ください"](#)。

ネットアップとストレージの統合

NetApp Astra Controlは、オンプレミス環境に導入され、信頼性の高いNetAppデータ保護テクノロジーを基盤とする、ステートフルなKubernetesワークロード向けのストレージとアプリケーション対応のデータ管理サービスの豊富なセットを提供します。

詳細については、NetApp Astra の Web サイトをご覧ください ["こちらをご覧ください"](#)。

Astra Trident は、コンテナや Kubernetes ディストリビューション向けの、Red Hat OpenShift などのオープンソースで完全にサポートされているストレージオーケストレーションツールです。

詳細については、Astra Trident の Web サイトをご覧ください ["こちらをご覧ください"](#)。

Advanced Configuration Options（詳細設定オプション）

このセクションは、実環境のユーザがこの解決策を本番環境に導入するときに実行する必要があるカスタマイズ（専用のプライベートイメージレジストリの作成やカスタムロードバランサインスタンスの導入など）に特化したものです。

検証済みリリースの現在のサポートマトリックスです

テクノロジー	目的	ソフトウェアのバージョン
NetApp ONTAP	ストレージ	9.8、9.9.1、9.12.1
NetApp Element	ストレージ	12.3
ネットアップアストラコントロール	アプリケーション対応データ管理	21.12.60、23.04、23.07、23.10、24.02
ネットアップアストラ Trident	ストレージオーケストレーション	22.01.0、23.04、23.07、23.10、24.02
Red Hat OpenShift のサービスです	コンテナオーケストレーション	4.6 EUS、4.7、4.8、4.10、4.11、4.12、4.13、4.14
VMware vSphere の場合	データセンターの仮想化	7.0、8.0.2

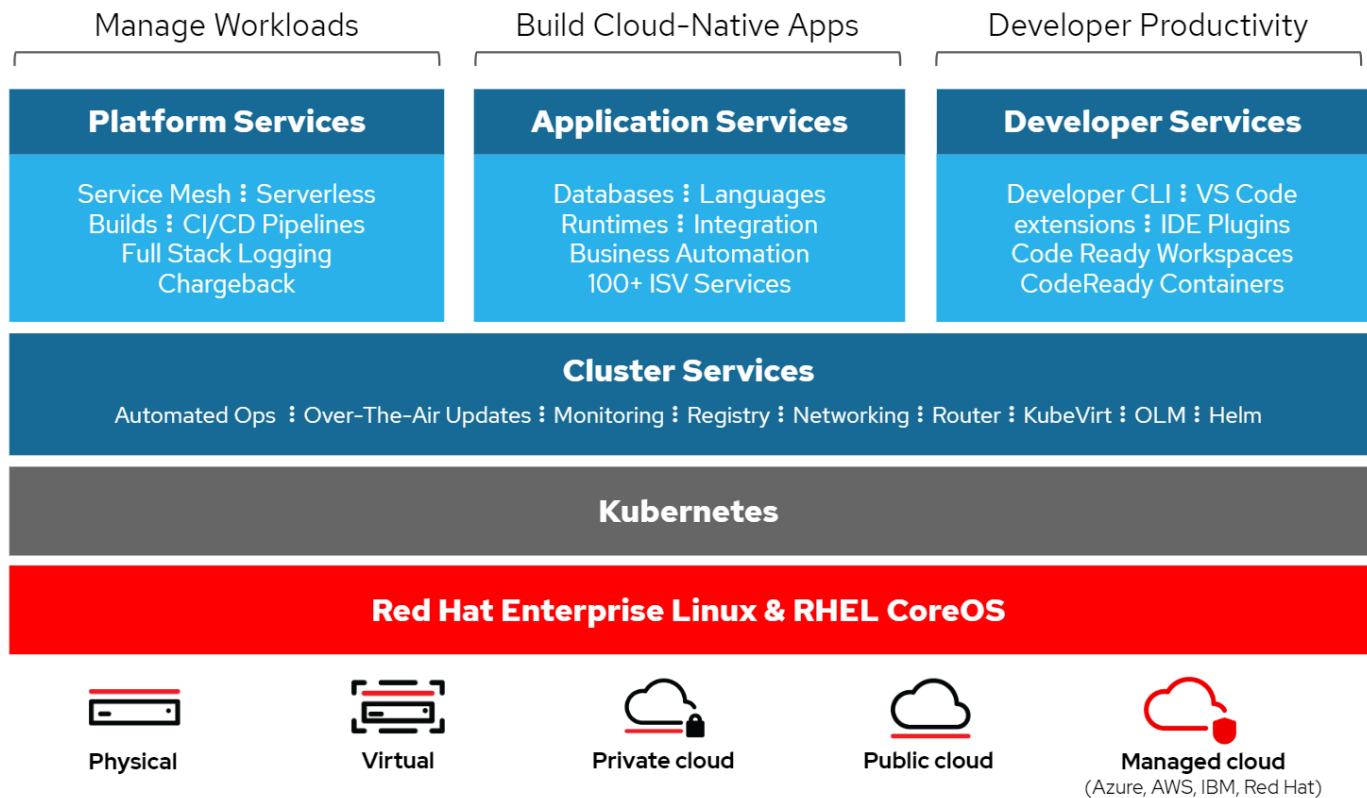
OpenShift の概要

Red Hat OpenShift Container Platform は、開発と IT の運用を単一のプラットフォーム上に統合し、オンプレミスとハイブリッドクラウドのインフラ全体でアプリケーションを一貫して構築、導入、管理します。Red Hat OpenShift は、コンテナベースのワークロード向けに設計された、世界をリードするエンタープライズ Linux ディストリビューションである Kubernetes や Red Hat Enterprise Linux CoreOS など、オープンソースのイノベーションと業界標準に基づいて構築されています。OpenShift は Cloud Native Computing Foundation（CNCF）認定 Kubernetes プログラムの一部であり、コンテナ

ワークロードの移植性と相互運用性を提供します。

Red Hat OpenShift には次の機能があります。

- ***セルフサービスプロビジョニング***開発者は、最も頻繁に使用するツールを使用して、必要に応じてアプリケーションをすばやく簡単に作成できます。また、運用担当者は、環境全体を完全に制御できます。
- **永続的ストレージ** OpenShift Container Platformは、永続的ストレージをサポートすることで、ステートフルアプリケーションとクラウドネイティブのステートレスアプリケーションの両方を実行できます。
- ***継続的統合および継続的開発 (CI/CD) ***このソースコードプラットフォームは、大規模なビルドおよび展開イメージを管理します。
- ***オープンソース標準***これらの標準には、他のオープンソーステクノロジーに加えて、コンテナオーケストレーションのための Open Container Initiative (OCI) と Kubernetes が組み込まれています。お客様は、特定のベンダーのテクノロジーやビジネスロードマップに制限されることはありません。
- ***CI/CDパイプライン*** OpenShiftは、CI/CDパイプラインを即座にサポートします。これにより、開発チームはアプリケーション配信プロセスのすべてのステップを自動化し、アプリケーションのコードまたは構成に加えられたすべての変更に対して確実に実行できるようになります。
- ***ロールベースアクセス制御(RBAC)***この機能は、チームとユーザーの追跡を提供し、大規模な開発者グループを編成するのに役立ちます。
- **ビルドとデプロイの自動化** OpenShiftを使用すると、開発者は、コンテナ化されたアプリケーションをビルドしたり、アプリケーションのソースコードやバイナリからコンテナをプラットフォームにビルドさせることができます。プラットフォームは、アプリケーションに定義された特性に基づいて、これらのアプリケーションのインフラストラクチャへの導入を自動化します。たとえば、割り当てられるリソースの量や、サードパーティのライセンスに準拠するために導入するインフラストラクチャ上の場所などです。
- **一貫した環境** OpenShiftにより、開発者向けにプロビジョニングされた環境が、オペレーティングシステム、ライブラリ、ランタイムバージョン（Javaランタイムなど）、アプリケーションのライフサイクル全体にわたって一貫していることが保証されます。また、一貫性のない環境に起因するリスクを排除するために使用されているアプリケーションランタイム（Tomcatなど）でも使用されています。
- ***構成管理***構成と機密データ管理がプラットフォームに組み込まれているため、アプリケーションの構築に使用されるテクノロジーや環境に依存しない一貫したアプリケーション構成がアプリケーションに提供されます。
導入済み：
- ***アプリケーションのログとメトリック。***迅速なフィードバックは、アプリケーション開発の重要な側面です。OpenShift に統合された監視機能とログ管理機能により、開発者はアプリケーションがどのように変化しても動作しているかを調査し、アプリケーションのライフサイクルの早い段階で問題を修正できるようになります。
- **セキュリティとコンテナカタログ** OpenShiftはマルチテナンシーを提供し、Security-Enhanced Linux (SELinux)、cgroups、Secure Computing Mode (seccomp) で確立されたセキュリティを使用してコンテナを分離および保護することで、有害なコード実行からユーザーを保護します。また、さまざまなサブシステム用の TLS 証明書による暗号化、およびエンドユーザーに認証済みの信頼できるセキュアなアプリケーションコンテナを提供するためにセキュリティを重視してスキャンおよび採点される Red Hat 認定コンテナ（access.redhat.com/containers）へのアクセスも提供します。



Red Hat OpenShift の導入方法

Red Hat OpenShift 4 以降、OpenShift の導入方法には、高度にカスタマイズされた導入に User Provisioned Infrastructure（UPI；ユーザプロビジョニングインフラ）を使用する手動導入、または Installer Provisioned Infrastructure（IPI）を使用した完全に自動化された導入が含まれます。

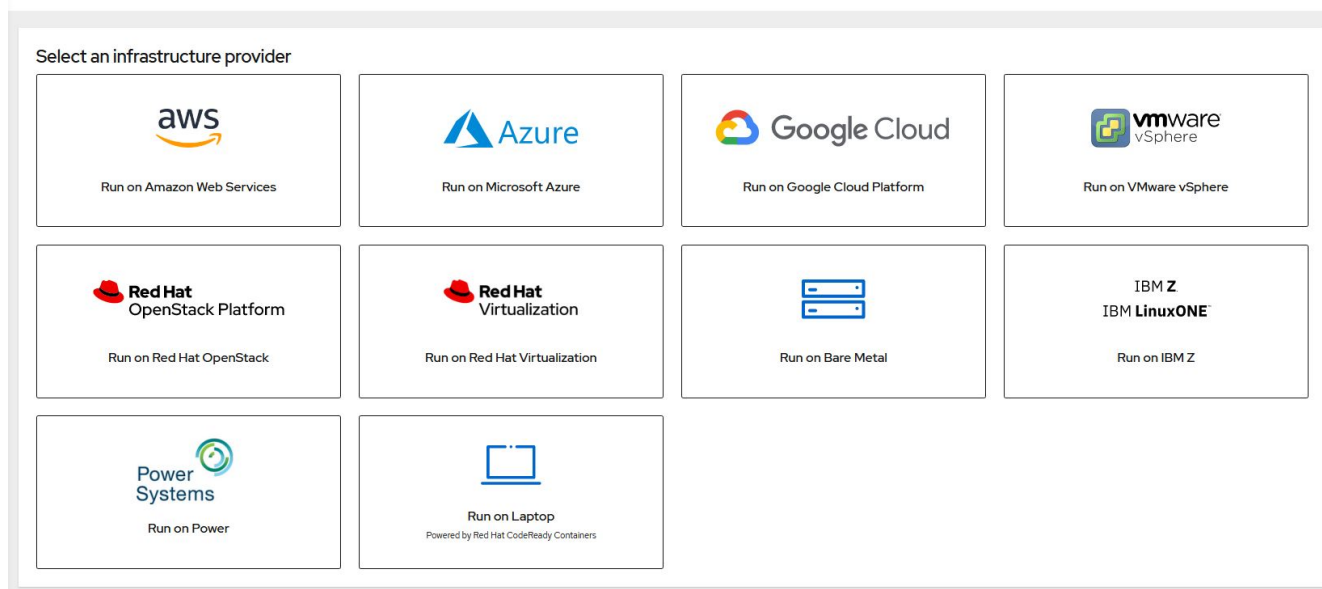
開発、テスト、本番環境向けにOpenShiftクラスタを迅速に導入できるため、ほとんどの場合、IPIのインストール方法が推奨されます。

Red Hat OpenShift の IPI インストール

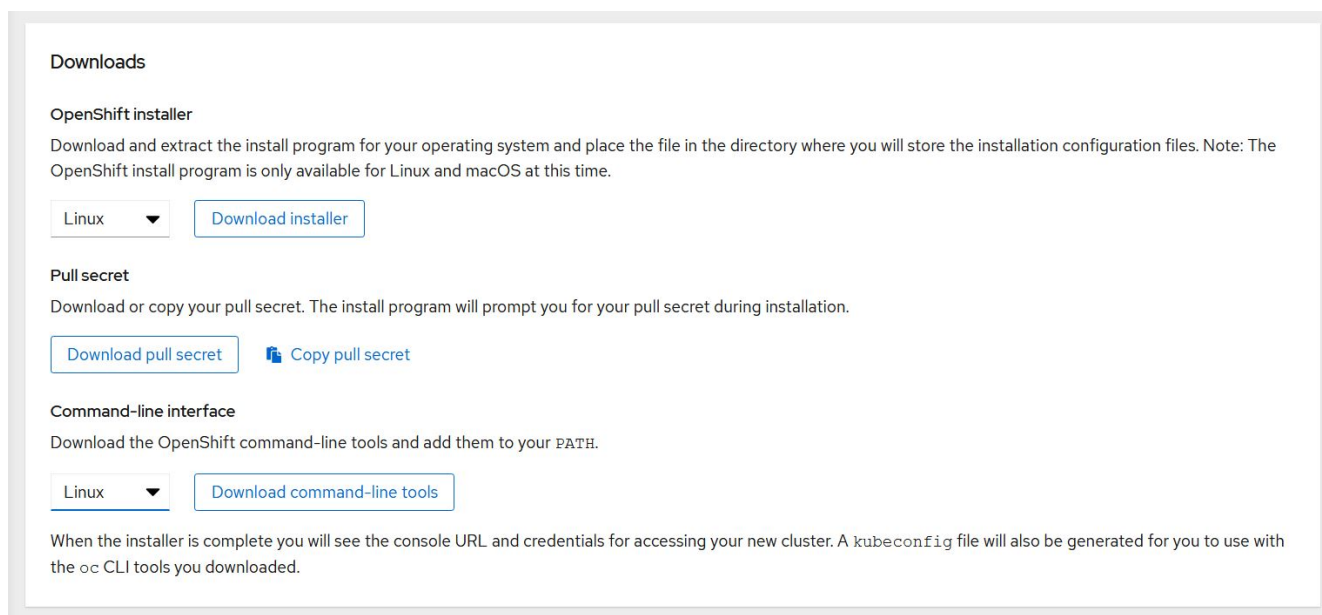
OpenShift の Installer Provisioned Infrastructure（IPI）導入には、次の高度な手順が含まれます。

1. Red Hat OpenShift をご覧ください "[Web サイト](#)" SSO クレデンシャルでログインします。
2. Red Hat OpenShift を導入する環境を選択します。

Install OpenShift Container Platform 4



3. 次の画面で、インストーラ、独自のプルシークレット、および管理用の CLI ツールをダウンロードします。



4. に従ってください **"インストール手順"** Red Hat が提供する、お客様の環境への導入サービスです。

ネットアップが検証済みの **OpenShift** 環境

ネットアップでは、以下の各データセンター環境で Installer Provisioned Infrastructure (IPI) 導入方法を使用して、Red Hat OpenShift のラボへの導入をテストし、検証しています。

- **"ベアメタルで実装された OpenShift"**
- **"Red Hat OpenStack Platform 上の OpenShift"**
- **"Red Hat 仮想化を基盤とした OpenShift"**

- ["VMware vSphere 上の OpenShift"](#)

ベアメタルで実装された OpenShift

ベアメタル上の OpenShift では、コモディティサーバ上に OpenShift Container Platform を自動で導入できます。

ベアメタル上の OpenShift は、コンテナ化の準備ができていないアプリケーションの仮想ワークロードをサポートしながら、OpenShift クラスタの導入、迅速なプロビジョニング、拡張を容易にする OpenShift の仮想導入に似ています。ベアメタルに導入することで、OpenShift 環境に加えてホストハイパーバイザー環境の管理に必要な追加のオーバーヘッドを必要としません。ベアメタルサーバに直接導入することで、ホストと OpenShift 環境間でリソースを共有する必要がある物理的なオーバーヘッドの制限を軽減できます。

ベアメタル上の OpenShift には次の機能があります。

- *** IPIまたはAssisted Installer Deployment * Installer Provisioned Infrastructure (IPI)** によってベアメタルサーバにOpenShiftクラスタを導入すると、ハイパーバイザーレイヤを管理することなく、汎用性が高く拡張性の高いOpenShift環境を汎用サーバに直接導入できます。
- ***コンパクトなクラスタ設計***ハードウェア要件を最小限に抑えるために、OpenShiftをベアメタルで使用すると、OpenShiftコントロールプレーンノードがワーカーノードおよびホストコンテナとしても機能するため、わずか3ノードのクラスタを導入できます。
- *** OpenShift仮想化*** OpenShiftは、OpenShift仮想化を使用して、コンテナ内で仮想マシンを実行できます。このコンテナネイティブの仮想化では、コンテナ内で KVM ハイパーバイザーを実行し、VM ストレージ用の永続ボリュームを接続します。
- *** AI / MLに最適化されたインフラ*** GPUベースのワーカーノードをOpenShift環境に組み込み、OpenShift Advanced Schedulingを活用することで、Kubeflowなどのアプリケーションを機械学習アプリケーションに導入できます。

ネットワーク設計

NetApp 解決策上の Red Hat OpenShift では、2 つのデータスイッチを使用して 25Gbps でプライマリデータ接続を提供します。また、ストレージノードのインバンド管理用に 1Gbps で接続を提供する管理スイッチを 2 台使用し、IPMI 機能のアウトオブバンド管理も使用します。

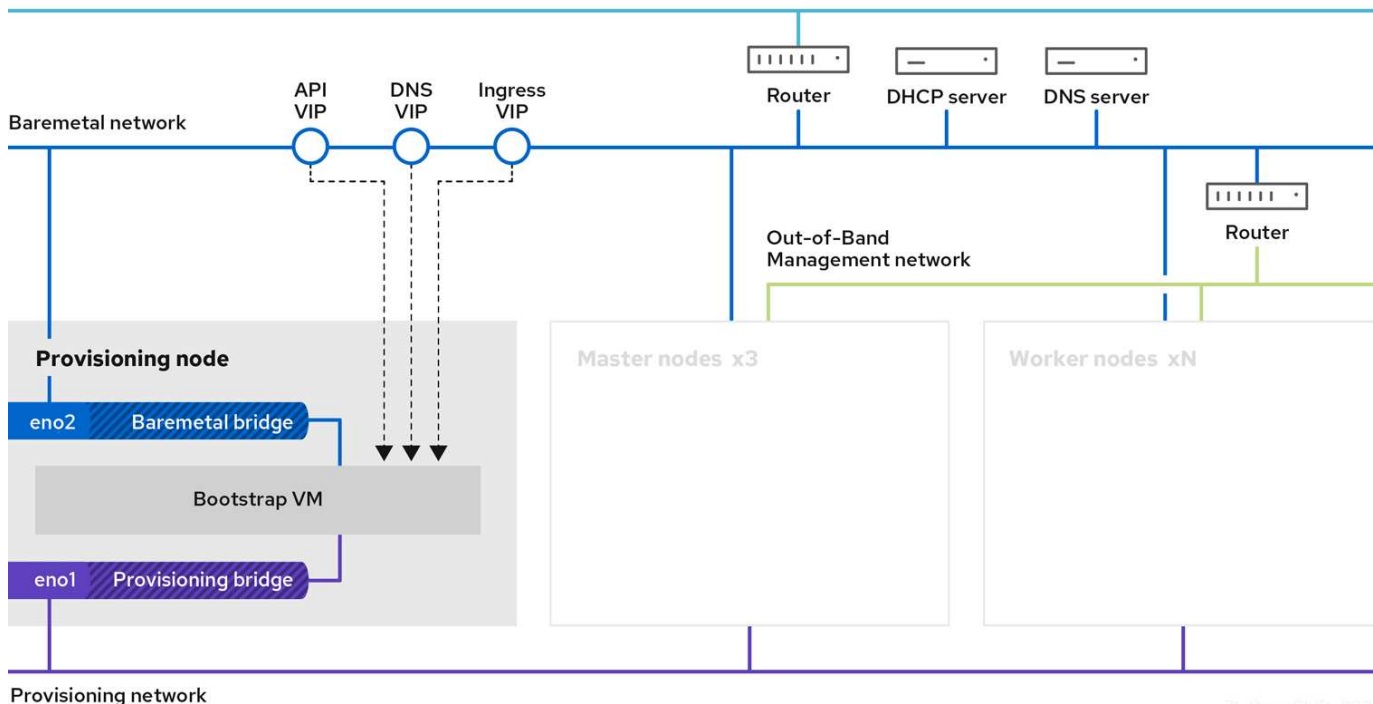
OpenShift ベアメタル IPI 環境では、プロビジョニングノード、つまりネットワークインターフェイスが別々のネットワークに接続されている Red Hat Enterprise Linux 8 マシンを作成する必要があります。

- ***プロビジョニングネットワーク***このネットワークは、ベアメタルノードをブートし、OpenShiftクラスタの導入に必要なイメージとパッケージをインストールするために使用されます。
- ***ベアメタルネットワーク***このネットワークは、クラスタ導入後のパブリック側通信に使用されます。

プロビジョニングノードをセットアップするために、お客様は、トラフィックをノード自体と、導入用にプロビジョニングされたブートストラップ VM に適切にルーティングできるようにするブリッジインターフェイスを作成します。クラスタが導入されると、API および入力 VIP アドレスがブートストラップノードから新しく導入されたクラスタに移行されます。

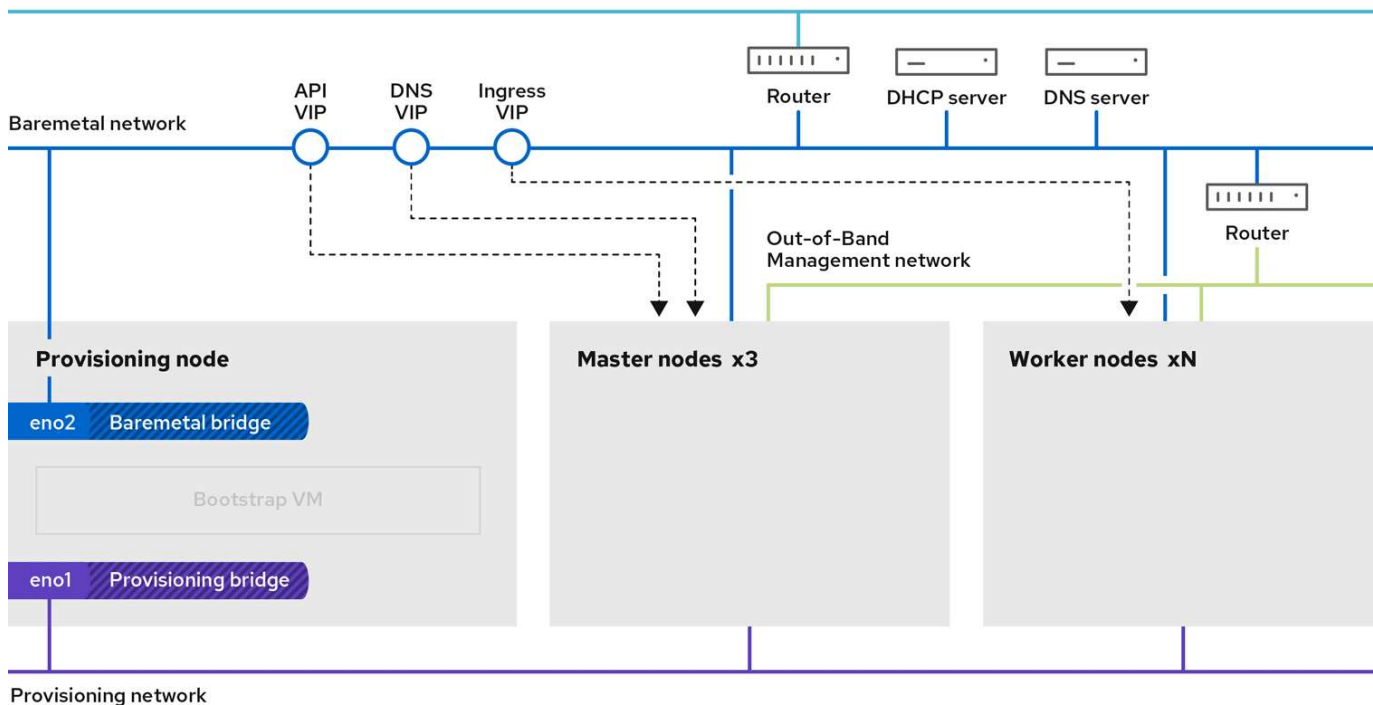
次の図は、IPI の導入時と導入の完了後の環境を示しています。

Internet access



7L_OpenShift_0320

Internet access



VLAN の要件

ネットアップ解決策を使用した Red Hat OpenShift は、仮想ローカルエリアネットワーク（VLAN）を使用して、ネットワークトラフィックを論理的に分離するように設計されています。

VLAN	目的	VLAN ID
アウトオブバンド管理ネットワーク	ベアメタルノードと IPMI の管理	16
ベアメタルネットワーク	クラスタが使用可能になると、OpenShift サービス用のネットワーク	181
プロビジョニングネットワーク	Network for PXE boot and installation of bare metal nodes (ベアメタルノードの PXE ブートおよびインストール用ネットワーク IPI を使用)	3485



これらの各ネットワークは仮想的に VLAN で分離されますが、PXE ブートシーケンス中に VLAN タグを渡す方法がないため、各物理ポートをプライマリ VLAN が割り当てられたアクセスモードで設定する必要があります。

ネットワークインフラストラクチャサポートリソース

OpenShift Container Platform を導入する前に、次のインフラを用意する必要があります。

- インバンド管理ネットワークと VM ネットワークからアクセス可能な完全なホスト名解決を提供する DNS サーバが少なくとも 1 台必要です。
- インバンド管理ネットワークおよび VM ネットワークからアクセスできる NTP サーバが少なくとも 1 台必要です。
- (オプション) インバンド管理ネットワークと VM ネットワークの両方のアウトバウンドインターネット接続。

Red Hat OpenStack Platform 上の OpenShift

Red Hat OpenStack Platform は、セキュアで信頼性の高いプライベート OpenStack クラウドの構築、導入、拡張を行うための統合基盤を提供します。

OSP は、コンピューティング、ストレージ、ネットワークリソースを管理する一連の制御サービスによって実装される IaaS (インフラサービス) クラウドです。この環境の管理には Web ベースのインターフェイスを使用します。このインターフェイスを使用すると、管理者とユーザは OpenStack リソースの制御、プロビジョニング、自動化を行うことができます。さらに、OpenStack インフラは、広範なコマンドラインインターフェイスと API を通じて管理者とエンドユーザにフルオートメーション機能を提供します。

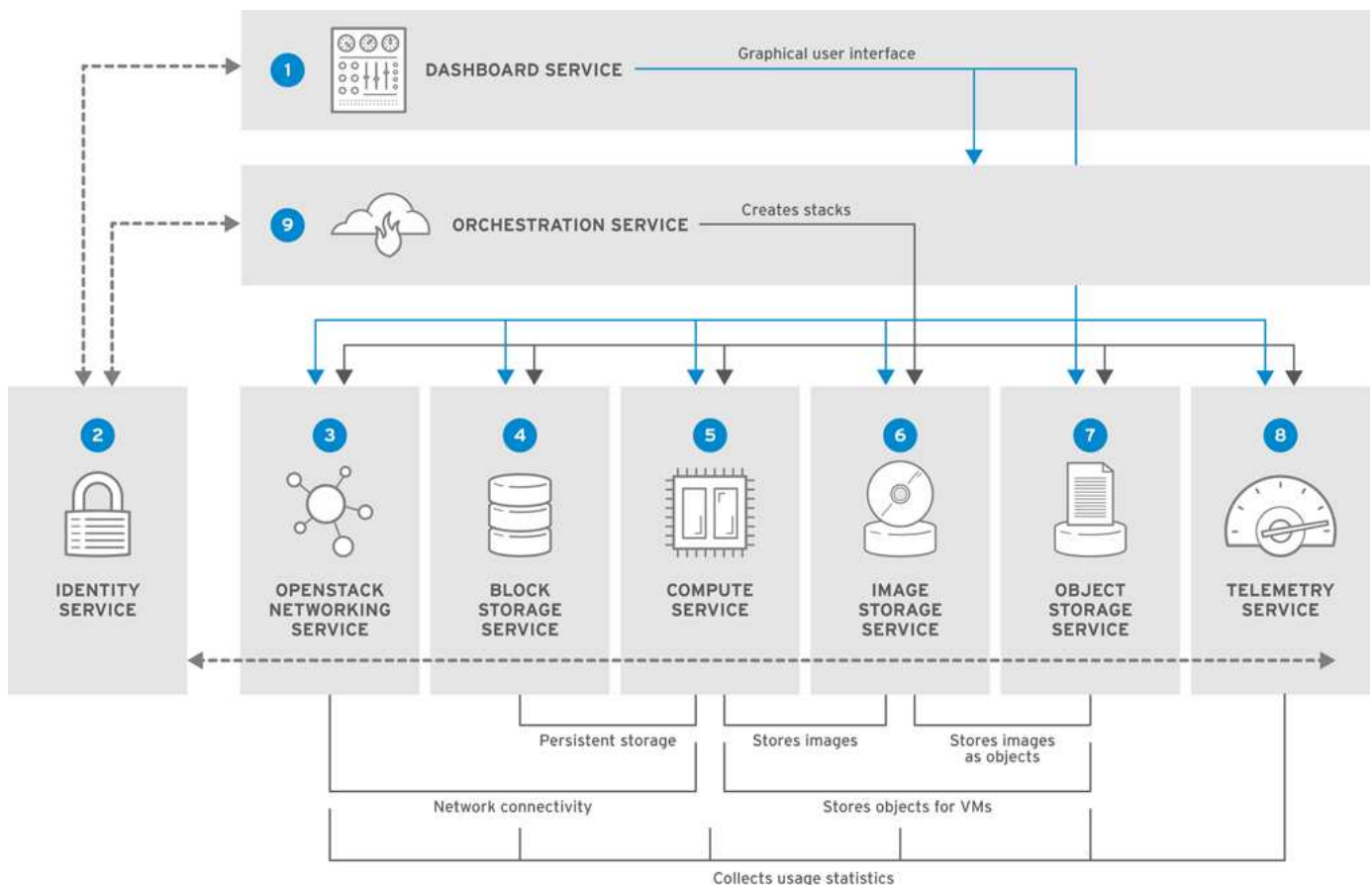
OpenStack プロジェクトは、短期間で開発されたコミュニティプロジェクトで、6 カ月ごとに更新リリースを提供します。最初の Red Hat OpenStack Platform は、すべてのアップストリームリリースに加えて新しいリリースを公開することで、このリリースサイクルのペースを維持していました。また、3 回目のリリースごとに長期的なサポートを提供します。最近、OpenStack Train をベースとした OSP リリース 16.0 ではリリース番号に対応しないことが選択されましたが、新しい機能はサブリリースにバックポートされています。最新のリリースは Red Hat OpenStack Platform 16.1 です。これには、アップストリームの Usuri および Victoria リリースからバックポートされた高度な機能が含まれています。

OSP の詳細については、を参照してください ["Red Hat OpenStack Platform の Web サイト"](#)。

OpenStack サービス

OpenStack Platform サービスはコンテナとして導入されます。コンテナはサービスを分離するため、アップグレードも簡単です。OpenStack Platform は、Kolla によって構築、管理された一連のコンテナを使用しま

す。サービスの導入は、Red Hat Custom Portal からコンテナイメージを取得することによって行われます。これらのサービスコンテナは、Podman コマンドを使用して管理され、Red Hat OpenStack Director で導入、設定、および管理されます。



サービス	プロジェクト名	説明
ダッシュボード	地平線	OpenStack サービスの管理に使用する Web ブラウザベースのダッシュボード。
ID	Keystone	OpenStack サービスの認証と許可、およびユーザ、プロジェクト、ロールの管理を一元化するサービスです。
OpenStack ネットワーク	中性子	OpenStack サービスのインターフェイス間の接続を提供します。
ブロックストレージ	Cinder の場合	仮想マシン（VM）の永続的なブロックストレージボリュームを管理します。
コンピューティング	ノバ	コンピューティングノードで実行されている VM を管理およびプロビジョニングします。
イメージ（Image）	Glance	VM イメージやボリューム Snapshot などのリソースを格納するためのレジストリサービス。
オブジェクトストレージ	Swift	ユーザにファイルおよび任意のデータの格納および取得を許可します。
テレメータ	Ceilometer	クラウドリソースの使用状況を測定できます。

サービス	プロジェクト名	説明
オーケストレーション	熱	リソーススタックの自動作成をサポートする、テンプレートベースのオーケストレーションエンジン。

ネットワーク設計

NetApp 解決策を使用した Red Hat OpenShift では、2 つのデータスイッチを使用して 25Gbps でプライマリデータ接続を提供します。また、ストレージノードのインバンド管理用に 1Gbps で接続を提供する管理スイッチをさらに 2 台使用し、IPMI 機能のアウトオブバンド管理も行います。

Red Hat OpenStack Director では、皮肉なベアメタルプロビジョニングサービスを使用して Red Hat OpenStack Platform を導入するために、IPMI 機能が必要です。

VLAN の要件

ネットアップとともに Red Hat OpenShift を実装することで、仮想ローカルエリアネットワーク（VLAN）を使用してネットワークトラフィックを論理的に分離するように設計されています。この構成は、お客様のニーズに合わせて拡張することも、特定のネットワークサービスをさらに分離することもできます。次の表に、ネットアップで解決策を検証する際に解決策を実装するために必要な VLAN を示します。

VLAN	目的	VLAN ID
アウトオブバンド管理ネットワーク	物理ノードの管理に使用するネットワークと、皮肉なことに IPMI サービス。	16
ストレージインフラ	Swift などのインフラサービスをサポートするためにボリュームを直接マッピングするためのコントローラノードのネットワーク。	201
ストレージ Cinder	環境に導入された仮想インスタンスにブロックボリュームを直接マッピングして接続するためのネットワーク。	202.
内部 API	API 通信、RPC メッセージ、データベース通信を使用する OpenStack サービス間の通信に使用するネットワーク。	301
テナント	Neutron は、VXLAN を介したトンネリングによって、各テナントに独自のネットワークを提供します。ネットワークトラフィックは、各テナントネットワーク内で分離されます。各テナントネットワークには IP サブネットが関連付けられており、ネットワークネームスペースとは、複数のテナントネットワークで同じアドレス範囲を使用しても競合が発生することを意味します	302
ストレージ管理	OpenStack Object Storage（Swift）は、このネットワークを使用して、対象のレプリカノード間でデータオブジェクトを同期します。プロキシサービスは、ユーザ要求と基盤となるストレージレイヤの中間インターフェイスとして機能します。プロキシは受信要求を受信し、要求されたデータを取得するために必要なレプリカを検索します。	303
PXE	OpenStack Director は、OSP Overcloud のインストールをオーケストレーションするための、皮肉なベアメタルプロビジョニングサービスの一部として PXE ブートを提供します。	3484
外部	OpenStack Dashboard（Horizon）をグラフィカルに管理するためにホストする、公開されているネットワーク。OpenStack サービスを管理するためのパブリック API 呼び出しが可能です。	3485

VLAN	目的	VLAN ID
インバンド管理ネットワーク	SSH アクセス、DNS トラフィック、ネットワークタイムプロトコル（NTP）トラフィックなど、システム管理機能へのアクセスを提供します。このネットワークは、コントローラ以外のノードのゲートウェイとしても機能します。	3486

ネットワークインフラストラクチャサポートリソース

OpenShift Container Platform を導入する前に、次のインフラを用意する必要があります。

- ホスト名の完全な解決を可能にする DNS サーバが少なくとも 1 つ必要です。
- 解決策内のサーバの時刻を同期できる NTP サーバが 3 台以上ある。
- （オプション）OpenShift 環境でのアウトバウンドのインターネット接続。

本番環境の導入に関するベストプラクティス

このセクションでは、この解決策を本番環境に導入する前に考慮する必要があるベストプラクティスをいくつか紹介します。

少なくとも **3** つのコンピューティングノードで構成された **OSP** プライベートクラウドに **OpenShift** を導入します。

このドキュメントで説明する検証済みのアーキテクチャでは、3 つの OSP コントローラノードと 2 つの OSP コンピューティングノードを導入して、HA 運用に適した最小限のハードウェアを導入します。このアーキテクチャにより、耐障害性を備えた構成が実現し、両方のコンピューティングノードで仮想インスタンスを起動し、導入した VM を 2 つのハイパーバイザー間で移行できます。

Red Hat OpenShift 原因では最初に 3 つのマスターノードを導入するため、2 ノード構成では少なくとも 2 つのマスターが同じノードを占有する可能性があり、その特定のノードが使用できなくなった場合には OpenShift が停止する可能性があります。そのため、Red Hat では、少なくとも 3 つの OSP コンピューティングノードを導入して、OpenShift マスターを均等に分散させ、解決策にフォールトトレランスを強化することをベストプラクティスとして推奨します。

仮想マシンとホストのアフィニティを設定します

仮想マシンとホストのアフィニティを有効にすると、複数のハイパーバイザーノードに OpenShift マスターを分散できます。

アフィニティとは、VM やホストのセットに対してルールを定義する方法で、グループ内の同じホストで複数の VM が実行されるか、別々のホストで実行されるかを決定します。VM とホストで構成されるアフィニティグループを作成することで、VM に適用されます。このアフィニティグループには同じパラメータと条件が設定されます。アフィニティグループ内の VM がグループ内の同じホストで実行されているのか、または別々のホストで実行されているのかに応じて、アフィニティグループのパラメータでは正のアフィニティまたは負のアフィニティを定義できます。Red Hat OpenStack Platform では、サーバグループを作成し、Nova で導入されたインスタンスが異なるコンピューティングノードに導入されるようにフィルタを設定することで、ホストアフィニティルールと非アフィニティルールを作成して適用することができます。

サーバグループには、配置を管理できる最大 10 個の仮想インスタンスがデフォルトで存在します。Nova のデフォルトクォータを更新することで変更できます。



OSP サーバグループには、特定のハードアフィニティや非アフィニティの制限があります。ノードを共有するために十分なリソースが別々のノードに導入できない場合や、リソースが不足している場合は、VM をブートできません。

アフィニティグループを設定するには、を参照してください ["OpenStack インスタンス用にアフィニティおよび非アフィニティを設定するにはどうすればよいですか？"](#)。

OpenShift 環境にカスタムインストールファイルを使用します

IPI を使用すると、このドキュメントで前述した対話型ウィザードを使用して、OpenShift クラスタを簡単に導入できます。ただし、クラスタ導入の一環として、一部のデフォルト値の変更が必要になる場合があります。

このような場合は、クラスタをすぐに導入せずにウィザードを実行してタスクを実行できます。代わりに、あとでクラスタを導入できる構成ファイルを作成します。これは、IPI のデフォルト値を変更する必要がある場合や、マルチテナンシーなどの他の用途のために環境内に同一のクラスタを複数導入する必要がある場合に非常に便利です。OpenShift 用にカスタマイズされたインストール構成の作成の詳細については、を参照してください ["Red Hat OpenShift カスタマイズを使用した OpenStack へのクラスタのインストール"](#)。

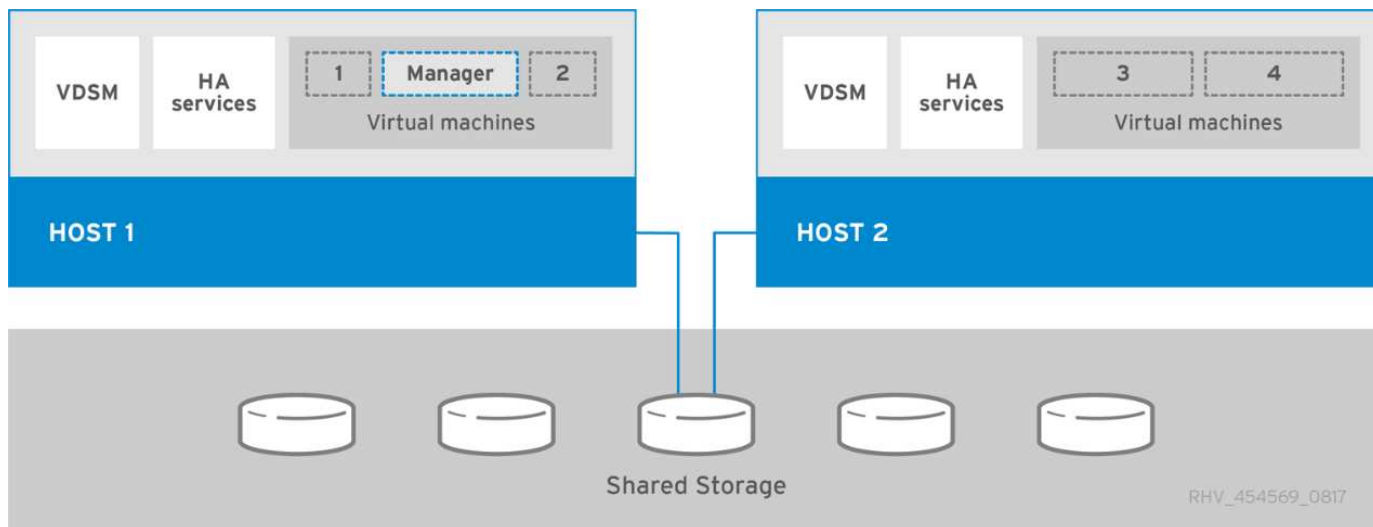
Red Hat 仮想化を基盤とした OpenShift

Red Hat Virtualization (RHV) は、Red Hat Enterprise Linux (RHEL) で実行され、KVM ハイパーバイザーを使用するエンタープライズ仮想データセンタープラットフォームです。

RHV の詳細については、を参照してください ["Red Hat Virtualization の Web サイト"](#)。

RHV は以下の機能を提供します。

- 仮想マシンとホストの一元管理 RHV マネージャは、導入環境内で物理マシンまたは仮想マシン (VM) として実行され、中央インターフェイスから解決策を管理するための Web ベースの GUI を提供します。
- *自己ホスト型エンジン*ハードウェア要件を最小限に抑えるために、RHV Manager (RHV-M) をゲスト VM を実行するホスト上に VM として導入できます。
- *高可用性*ホストで障害が発生した場合の中断を回避するために、RHV では VM を高可用性用に構成できます。高可用性 VM は、耐障害性ポリシーを使用してクラスタレベルで制御されます。
- 高い拡張性 1 つの RHV クラスタに最大 200 のハイパーバイザホストを配置できるため、IT 部門は大規模な VM の要件をサポートし、リソースを大量に消費するエンタープライズクラスのワークロードをホストできます。
- 強化されたセキュリティ RHV から継承された、Secure Virtualization (sVirt) および Security Enhanced Linux (SELinux) テクノロジーは、ホストおよび VM の高度なセキュリティと強化を目的として、RHV に採用されています。これらの機能の主なメリットは、VM とそれに関連するリソースを論理的に分離できることです。



ネットワーク設計

NetApp 解決策上の Red Hat OpenShift では、2つのデータスイッチを使用して 25Gbps でプライマリデータ接続を提供します。また、ストレージノードのインバンド管理用に 1Gbps で接続を提供する管理スイッチを 2 台追加し、IPMI 機能用にアウトオブバンド管理を使用します。OCP は、クラスタ管理に RHV 上の仮想マシン論理ネットワークを使用します。このセクションでは、解決策で使用される各仮想ネットワークセグメントの配置と目的について説明し、解決策を導入するための前提条件について説明します。

VLAN の要件

RHV 上の Red Hat OpenShift は、仮想ローカルエリアネットワーク（VLAN）を使用して、さまざまな目的でネットワークトラフィックを論理的に分離するように設計されています。この構成は、お客様のニーズに合わせて拡張することも、特定のネットワークサービスをさらに分離することもできます。次の表に、ネットアップで解決策を検証する際に解決策を実装するために必要な VLAN を示します。

VLAN	目的	VLAN ID
アウトオブバンド管理ネットワーク	物理ノードと IPMI の管理	16
VM ネットワーク	仮想ゲストネットワークアクセス	1172
インバンド管理ネットワーク	RHV-H ノード、RHV-Manager、および ovirtmgmt ネットワークの管理	3343
ストレージネットワーク	NetApp Element iSCSI 用のストレージネットワーク	344
移行用ネットワーク	仮想ゲスト移行用のネットワーク	3345

ネットワークインフラストラクチャサポートリソース

OpenShift Container Platform を導入する前に、次のインフラを用意する必要があります。

- インバンド管理ネットワークと VM ネットワークからアクセス可能な完全なホスト名解決を提供する DNS サーバが少なくとも 1 台必要です。
- インバンド管理ネットワークおよび VM ネットワークからアクセスできる NTP サーバが少なくとも 1 台必要です。
- （オプション）インバンド管理ネットワークと VM ネットワークの両方のアウトバウンドインターネット

接続。

本番環境の導入に関するベストプラクティス

このセクションでは、この解決策を本番環境に導入する前に考慮する必要があるベストプラクティスをいくつか紹介します。

少なくとも **3 つの RHV クラスタに OpenShift を導入します ノード**

このドキュメントで説明する検証済みのアーキテクチャは、2 つの RHV-H ハイパーバイザーノードを導入し、ホスト型エンジンと導入済み VM を両方のホストで管理して 2 つのハイパーバイザー間で移行できるフォールトトレラントな構成を確保することによって、HA 処理に適した最小限のハードウェア導入を示しています。

Red Hat OpenShift は最初に 3 つのマスターノードで導入するため、2 ノード構成で少なくとも 2 つのマスターが同じノードを占有します。そのため、特定のノードが使用できなくなった場合に OpenShift が停止する可能性があります。そのため、解決策の一部として少なくとも 3 つの RHV - H ハイパーバイザーノードを導入して、OpenShift マスターを均等に分散できるようにし、解決策にさらにフォールトトレランスを追加することが Red Hat のベストプラクティスです。

仮想マシンとホストのアフィニティを設定します

VM とホストのアフィニティを有効にすると、OpenShift マスターを複数のハイパーバイザーノードに分散できます。

アフィニティとは、VM やホストのセットに対してルールを定義する方法で、グループ内の同じホストで複数の VM が実行されるか、別々のホストで実行されるかを決定します。VM とホストで構成されるアフィニティグループを作成することで、VM に適用されます。このアフィニティグループには同じパラメータと条件が設定されます。アフィニティグループ内の VM がグループ内の同じホストで実行されているのか、または別々のホストで実行されているのかに応じて、アフィニティグループのパラメータでは正のアフィニティまたは負のアフィニティを定義できます。

パラメータに定義された条件は、強制またはソフト強制のいずれかです。強制をハードに行うことで、アフィニティグループ内の VM は、外部条件に関係なく常に正または負のアフィニティに従って配置されます。ソフトな適用では、可能なかぎり、アフィニティグループ内の VM に対して肯定的または否定的なアフィニティに従って高い優先度が設定されます。このドキュメントで説明する 2 つまたは 3 つのハイパーバイザー構成では、ソフトアフィニティが推奨される設定です。大規模なクラスタでは、ハードアフィニティによって OpenShift ノードを適切に分散できます。

アフィニティグループを設定するには、を参照してください ["Red Hat 6.11アフィニティグループのドキュメント"](#)。

OpenShift 環境にカスタムインストールファイルを使用します

IPI を使用すると、このドキュメントで前述した対話型ウィザードを使用して、OpenShift クラスタを簡単に導入できます。ただし、一部のデフォルト値については、クラスタの導入時に変更が必要になる場合があります。

このような場合は、クラスタをすぐに導入せずにウィザードを実行してタスクを実行できます。クラスタの導入に使用する構成ファイルが作成されます。これは、IPI のデフォルト値を変更する場合や、マルチテナンシーなどの他の用途のために環境内に同一のクラスタを複数導入する場合に非常に便利です。OpenShift 用にカスタマイズされたインストール構成の作成の詳細については、を参照してください ["Red Hat OpenShift カスタマイズを使用した RHV へのクラスタのインストール"](#)。

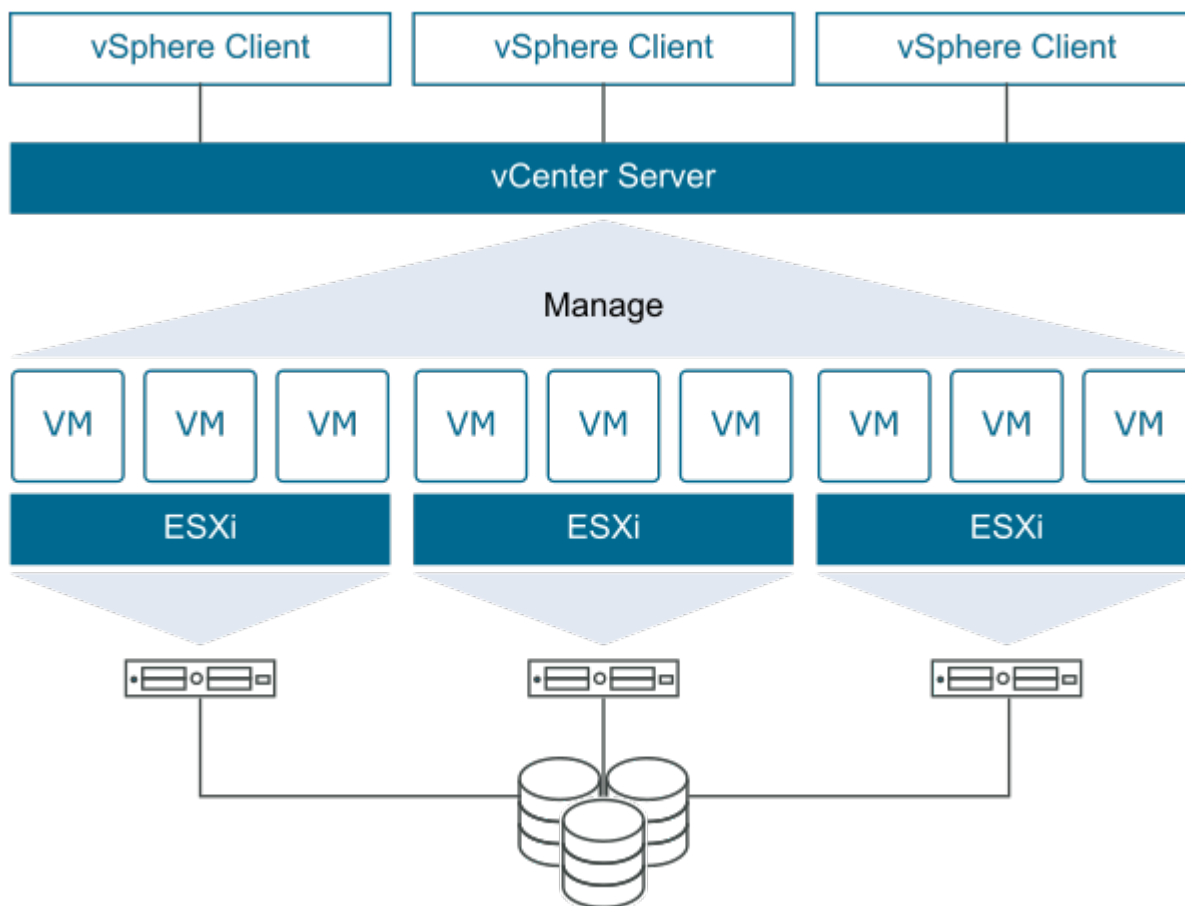
VMware vSphere 上の OpenShift

VMware vSphere は、ESXi ハイパーバイザー上で実行される多数の仮想サーバとネットワークを一元管理するための仮想化プラットフォームです。

VMware vSphere の詳細については、を参照してください "[VMware vSphere の Web サイト](#)".

VMware vSphere には次の機能があります。

- * VMware vCenter Server* VMware vCenter Server は、1つのコンソールからすべてのホストと VM を統合管理し、クラスタ、ホスト、VM のパフォーマンス監視を集約します。
- * VMware vSphere vMotion * VMware vCenterを使用すると、要求に応じて、システムを停止せずにクラスタ内のノード間でVMをホット移行できます。
- * vSphere High Availability *ホスト障害時のシステム停止を回避するために、VMware vSphereではホストをクラスタ化し、高可用性を実現できるように構成できます。ホストの障害によってシステムが停止した VM は、クラスタ内の他のホストでまもなくリブートされ、サービスがリストアされます。
- * Distributed Resource Scheduler (DRS) * VMware vSphereクラスタは、ホストしているVMのリソースニーズを負荷分散するように設定できます。リソース競合のある VM は、十分なリソースを使用できるように、クラスタ内の他のノードにホット移行できます。



ネットワーク設計

NetApp 解決策上の Red Hat OpenShift では、2つのデータスイッチを使用して 25Gbps でプライマリデータ接続を提供します。また、ストレージノードのインバンド管理用に 1Gbps で接続を提供する管理スイッチを

さらに 2 台使用し、IPMI 機能のアウトオブバンド管理も行います。OCP のクラスタ管理には、VMware vSphere 上の VM 論理ネットワークが使用されます。このセクションでは、解決策で使用される各仮想ネットワークセグメントの配置と目的について説明し、解決策を導入するための前提条件について説明します。

VLAN の要件

VMware vSphere 上の Red Hat OpenShift は、仮想ローカルエリアネットワーク（VLAN）を使用して、ネットワークトラフィックを論理的に分離するように設計されています。この構成は、お客様のニーズに合わせて拡張することも、特定のネットワークサービスをさらに分離することもできます。次の表に、ネットアップで解決策を検証する際に解決策を実装するために必要な VLAN を示します。

VLAN	目的	VLAN ID
アウトオブバンド管理ネットワーク	物理ノードと IPMI の管理	16
VM ネットワーク	仮想ゲストネットワークアクセス	181
ストレージネットワーク	ONTAP NFS 用のストレージネットワーク	184
ストレージネットワーク	ONTAP iSCSI 用のストレージネットワーク	185
インバンド管理ネットワーク	ESXi ノード、vCenter Server、ONTAP Select の管理	3480
ストレージネットワーク	NetApp Element iSCSI 用のストレージネットワーク	3481
移行用ネットワーク	仮想ゲスト移行用のネットワーク	3487

ネットワークインフラストラクチャサポートリソース

OpenShift Container Platform を導入する前に、次のインフラを用意する必要があります。

- ・インバンド管理ネットワークと VM ネットワークからアクセス可能な完全なホスト名解決を提供する DNS サーバが少なくとも 1 台必要です。
- ・インバンド管理ネットワークおよび VM ネットワークからアクセスできる NTP サーバが少なくとも 1 台必要です。
- ・（オプション）インバンド管理ネットワークと VM ネットワークの両方のアウトバウンドインターネット接続。

本番環境の導入に関するベストプラクティス

このセクションでは、この解決策を本番環境に導入する前に考慮する必要があるベストプラクティスをいくつか紹介します。

少なくとも 3 つのボリュームからなる ESXi クラスタに OpenShift を導入します ノード

本ドキュメントで説明する検証済みのアーキテクチャには、VMware vSphere HA と VMware vMotion を有効にして、2 つの ESXi ハイパーバイザーノードを導入し、フォールトトレラント構成を確保することで、HA 処理に適した最小限のハードウェア環境が示されています。この構成では、導入した VM を 2 つのハイパーバイザー間で移行し、1 つのホストが使用できなくなった場合にリブートすることができます。

Red Hat OpenShift では最初に 3 つのマスターノードを導入するため、2 ノード構成の少なくとも 2 つのマスターが同じノードを占有することがあります。その場合、特定のノードが使用できなくなったときに

OpenShift が停止する可能性があります。そのため、Red Hat のベストプラクティスでは、OpenShift マスターを均等に分散してフォールトトレランスを高めるために、少なくとも 3 つの ESXi ハイパーバイザーノードを導入する必要があります。

仮想マシンとホストのアフィニティを設定します

VM とホストのアフィニティを有効にすることで、複数のハイパーバイザーノードに OpenShift マスターを確実に分散させることができます。

アフィニティまたは非アフィニティは、VM やホストのセットに対してルールを定義する方法で、グループ内の同じホストまたはホスト上で VM を一緒に実行するか、別のホスト上で実行するかを決定します。VM とホストで構成されるアフィニティグループを作成することで、VM に適用されます。このアフィニティグループには同じパラメータと条件が設定されます。アフィニティグループ内の VM がグループ内の同じホストで実行されているのか、または別々のホストで実行されているのかに応じて、アフィニティグループのパラメータでは正のアフィニティまたは負のアフィニティを定義できます。

アフィニティグループを設定するには、を参照してください ["vSphere 6.7 ドキュメント：「DRS アフィニティルール」の使用](#)。

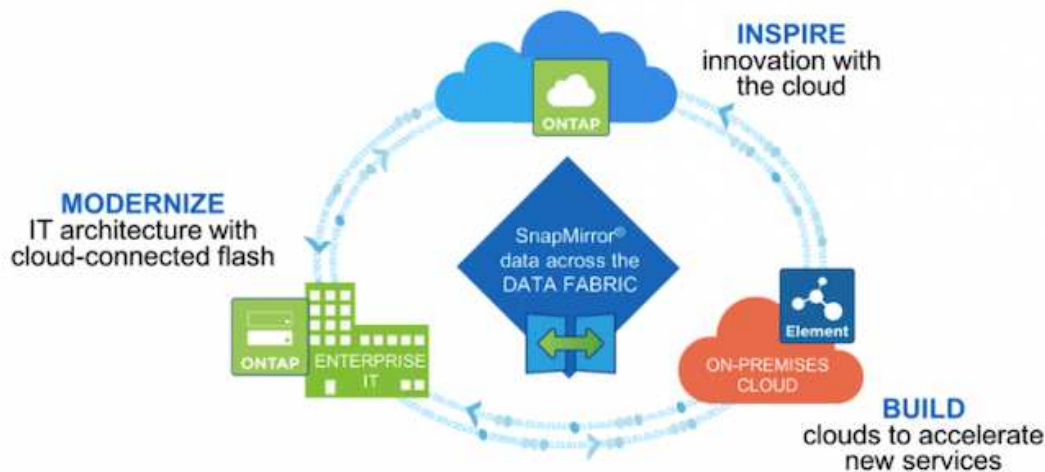
OpenShift 環境にカスタムインストールファイルを使用します

IPI を使用すると、このドキュメントで前述した対話型ウィザードを使用して、OpenShift クラスタを簡単に導入できます。ただし、クラスタ導入の一環として、一部のデフォルト値の変更が必要になる場合があります。

このような場合は、クラスタをすぐに導入せずにウィザードを実行してタスクを実行できますが、代わりに、あとでクラスタを導入できる構成ファイルが作成されます。これは、IPI のデフォルトを変更する必要がある場合や、マルチテナンシーなどの他の用途のために環境内に同一のクラスタを複数導入する場合に非常に便利です。OpenShift 用にカスタマイズされたインストール構成の作成の詳細については、を参照してください ["Red Hat OpenShift カスタマイズを使用して vSphere にクラスタをインストールします"](#)。

ネットアップストレージの概要

ネットアップには、Red Hat OpenShift に導入されたアプリケーション用のストレージをプロビジョニングするための、ネットアップの Astra Trident ストレージオーケストレーションツールで認定されているストレージプラットフォームが複数あります。



- AFF システムと FAS システムは、NetApp ONTAP を実行し、ファイルベース（NFS）とブロックベース（iSCSI）の両方のユースケースにストレージを提供します。
- Cloud Volumes ONTAP と ONTAP Select は、それぞれクラウドと仮想スペースに同じメリットをもたらします。
- NetApp Cloud Volumes Service（AWS / GCP）と Azure NetApp Files は、クラウドでファイルベースのストレージを提供します。
- NetApp Element ストレージシステムは、拡張性に優れた環境でブロックベース（iSCSI）のユースケースに対応します。



ネットアップのポートフォリオに含まれる各ストレージシステムでは、オンプレミスサイトとクラウド間でのデータ管理と移動の両方を容易に行えるため、データがアプリケーションの配置場所にあることを保証できます。

以下のページでは、Red Hat OpenShift with NetApp 解決策で検証されたネットアップストレージシステムに関する追加情報について説明します。

- ["NetApp ONTAP"](#)
- ["NetApp Element"](#)

NetApp ONTAP

NetApp ONTAP は、わかりやすい GUI、自動化統合機能を備えた REST API、AI に基づく予測分析と修正措置、無停止のハードウェアアップグレード、ストレージ間インポートなどの機能を備えた強力なストレージソフトウェアツールです。

NetApp ONTAP ストレージシステムの詳細については、を参照してください ["ネットアップの ONTAP Web サイト"](#)。

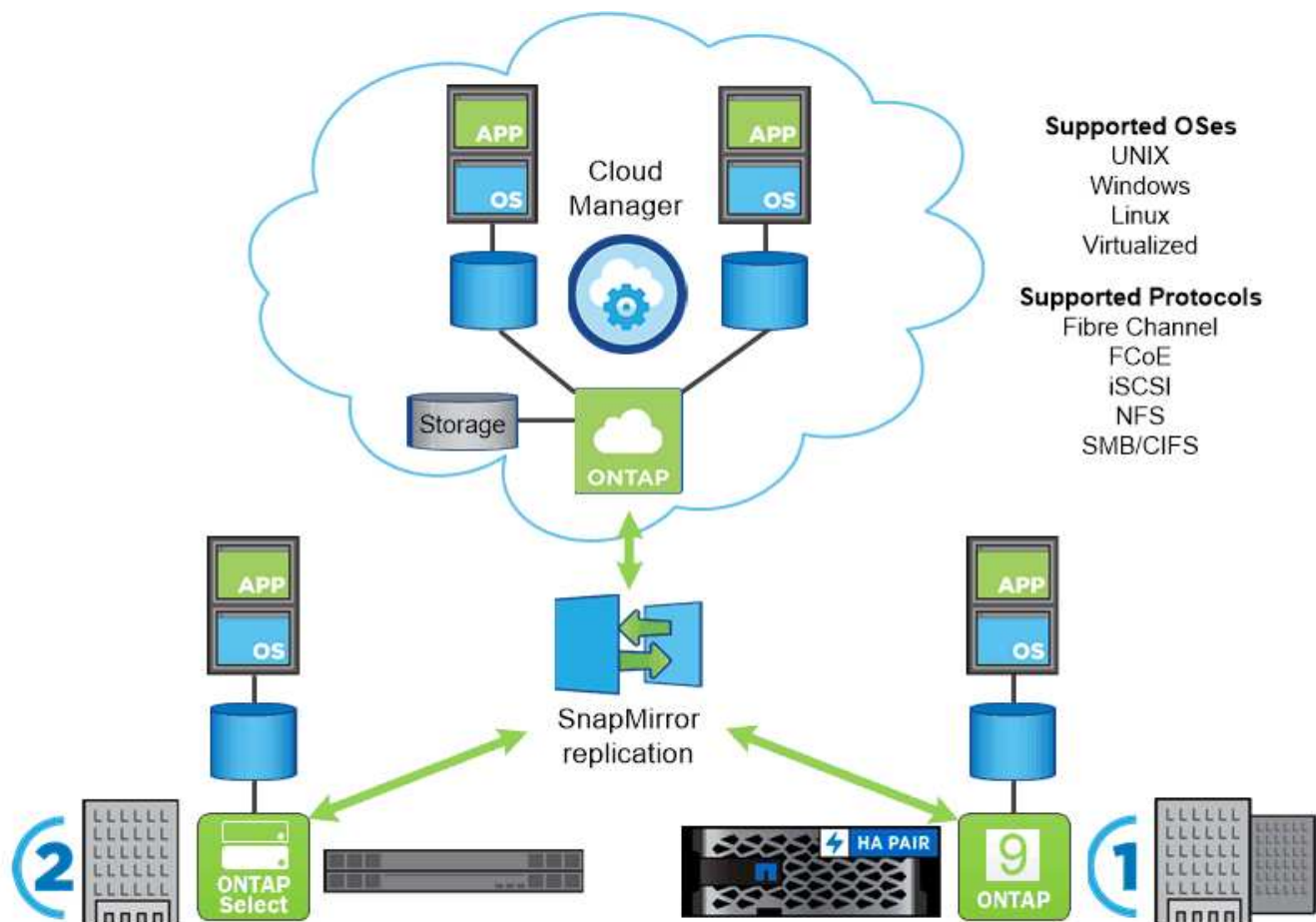
ONTAP は以下の機能を提供します。

- NFS、CIFS、iSCSI、FC、FCoE を同時にデータアクセスと管理できるユニファイドストレージシステム FC-NVMe プロトコルが必要です。
- 導入モデルには、オンプレミスのオールフラッシュ、ハイブリッド、オール HDD のハードウェア構成、ONTAP Select などのサポートされるハイパーバイザーを使用する VM ベースのストレージプラットフォーム、Cloud Volumes ONTAP などのクラウドがあります。
- ONTAP システムでは、データの自動階層化、インラインデータ圧縮、重複排除、コンパクションがサポートされ、データストレージ効率が向上しています。
- ワークロードベースの QoS 制御ストレージ：
- パブリッククラウドとのシームレスな統合により、データの階層化と保護を実現 ONTAP は、あらゆる環境に対応する堅牢なデータ保護機能も備えています。
 - * NetApp Snapshot コピー。* 最小限のディスク・スペースでデータをポイント・イン・タイムで高速バックアップし、パフォーマンス・オーバーヘッドを追加する必要はありません。
 - * NetApp SnapMirror。* 1 つのストレージ・システムから別のストレージ・システムへデータの Snapshot コピーをミラーリングします。ONTAP では、他の物理プラットフォームやクラウドネイティブのサービスへのデータのミラーリングもサポートされています。
 - * NetApp SnapLock。* 指定された期間にわたって上書きまたは消去できない特殊なボリュームに書き込むことにより、書き換え不可能なデータを効率的に管理します。
 - * NetApp SnapVault。* は、複数のストレージ・システムのデータを、指定されたすべてのシステムのバックアップとして機能する中央の Snapshot コピーにバックアップします。
 - * NetApp SyncMirror。* 同じコントローラに物理的に接続された 2 つの異なるディスクプレックスに対して、データをリアルタイムで RAID レベルでミラーリングします。
 - * NetApp SnapRestore * を使用すると、Snapshot コピーからオンデマンドでバックアップされたデータを迅速にリストアできます。
 - * NetApp FlexClone。* Snapshot コピーに基づいて、ネットアップボリュームの読み書き可能なフルコピーを瞬時にプロビジョニングできます。

ONTAP の詳細については、を参照してください ["ONTAP 9 ドキュメンテーション・センター"](#)。



NetApp ONTAP は、オンプレミス、仮想環境、クラウド環境で利用できます。



ネットアップのプラットフォーム

NetApp AFF/FAS

ネットアップは、堅牢なオールフラッシュ（AFF）およびスケールアウトハイブリッド（FAS）ストレージプラットフォームを提供し、低レイテンシのパフォーマンス、統合データプロテクション、マルチプロトコルのサポートのそれぞれに合わせてカスタマイズします。

どちらのシステムも、NetApp ONTAP データ管理ソフトウェアを搭載しています。NetApp は、可用性が高く、クラウドと統合されたシンプルなストレージ管理を実現する業界最先端のデータ管理ソフトウェアで、データファブリックのニーズに応じたエンタープライズクラスのスピード、効率性、セキュリティを提供します。

NetApp AFF / FAS プラットフォームの詳細については、をクリックしてください ["こちらをご覧ください"](#)。

ONTAP Select の場合

ONTAP Select は、お客様の環境のハイパーバイザーに導入できる、ソフトウェアで定義された NetApp ONTAP の導入です。VMware vSphere または KVM にインストールでき、ハードウェアベースの ONTAP システムの全機能とエクスペリエンスを提供します。

ONTAP Select の詳細については、をクリックしてください ["こちらをご覧ください"](#)。

Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP は、クラウドで導入される NetApp ONTAP のバージョンで、Amazon AWS、Microsoft Azure、Google Cloud などのさまざまなパブリッククラウドに導入できます。

Cloud Volumes ONTAP の詳細については、をクリックしてください ["こちらをご覧ください"](#)。

NetApp ONTAP 対応の Amazon FSx

Amazon FSx for NetApp ONTAPは、ONTAPの一般的なデータアクセス機能と管理機能を使用して、AWSクラウドでフルマネージドの共有ストレージを提供します。Amazon FSx for NetApp ONTAPの詳細については、"[こちらをご覧ください](#)"。

Azure NetApp Files の特長

Azure NetApp Filesは、Azureネイティブのファーストパーティ機能を備えたエンタープライズクラスのハイパフォーマンスファイルストレージサービスです。NetAppアカウント、容量プール、ボリュームを作成できるボリュームサービスを提供します。また、サービスレベルとパフォーマンスレベルを選択し、データ保護を管理することもできます。使い慣れたオンプレミスと同じプロトコルとツールを使用して、ハイパフォーマンス、可用性、拡張性に優れたファイル共有を作成、管理できます。Azure NetApp Filesの詳細については、"[こちらをご覧ください](#)"。

Google Cloud NetAppボリューム

Google Cloud NetApp Volumesは、高度なデータ管理機能と拡張性に優れたパフォーマンスを提供する、フルマネージドのクラウドベースデータストレージサービスです。ファイルベースのアプリケーションをGoogle Cloudに移行できます。Network File System (NFSv3およびNFSv4.1) プロトコルとServer Message Block (SMB; サーバメッセージブロック) プロトコルを標準でサポートしているため、アプリケーションを再設計する必要がなく、アプリケーションに永続的ストレージを引き続き使用できます。Google Cloud NetApp VolumesPの詳細については、"[こちらをご覧ください](#)"。

NetApp Element : ネットアップを使用した Red Hat OpenShift

NetApp Element ソフトウェアは、拡張性に優れたモジュラ型のパフォーマンスを提供し、ストレージノードごとに容量とスループットを保証します。NetApp Element システムは、1つのクラスタで4~100 ノードまで拡張でき、高度なストレージ管理機能も多数備えています。



NetApp Element ストレージ・システムの詳細については、を参照してください ["ネットアップの SolidFire Web サイト"](#)。

NetApp Element ソフトウェアは、iSCSI ストレージプロトコルを利用します。これは、従来の TCP/IP ネットワーク上で SCSI コマンドをカプセル化する標準的な方法です。SCSI 標準が変更された場合や、イーサネットネットワークのパフォーマンスが向上した場合、iSCSI ストレージプロトコルには変更は必要ありません。

すべてのストレージノードには管理 IP とストレージ IP が設定されますが、NetApp Element ソフトウェアは、クラスタ内のすべてのストレージトラフィックについて、ストレージ仮想 IP アドレス（SVIP アドレス）を 1 つアドバタイズします。iSCSI のログインプロセスでは、ストレージはターゲットボリュームが別のアドレスに移動されたことを応答するため、ネゴシエーションプロセスを続行できません。その後、ホスト側の再設定を必要としないプロセスで、ホストはログイン要求を新しいアドレスに再発行します。このプロセスは、iSCSI ログインリダイレクトと呼ばれます。

iSCSI ログインリダイレクトは、NetApp Element ソフトウェアクラスタの重要な要素です。ホストログイン要求を受信すると、ノードは、IOPS とボリュームの容量要件に基づいて、トラフィックを処理するクラスタのメンバーを決定します。ボリュームは NetApp Element ソフトウェアクラスタ全体に分散され、単一のノードがボリュームのトラフィックを大量に処理している場合や新しいノードが追加された場合に再配置されます。特定のボリュームの複数のコピーがアレイ全体に割り当てられます。

この方法では、ノード障害のあとにボリュームの再配分が発生しても、ログアウトして新しい場所にリダイレクトしてログインした場合を超えてホスト接続には影響はありません。iSCSI ログインリダイレクションを使用する NetApp Element ソフトウェアクラスタは、無停止のアップグレードと運用が可能な自己回復型のスケールアウトアーキテクチャです。

NetApp Element ソフトウェアクラスタの QoS

NetApp Element ソフトウェアクラスタでは、QoS をボリューム単位で動的に設定できます。ボリュームごとの QoS 設定を使用して、定義した SLA に基づいてストレージパフォーマンスを制御できます。QoS は、次の 3 つの設定可能なパラメータで定義されます。

- * 最小 IOPS 。 * NetApp Element ソフトウェアクラスタがボリュームに提供する平常時の最小 IOPS 。ボリュームに設定された最小 IOPS は、そのボリュームに対して最低限保証されるパフォーマンスレベルです。ボリュームごとのパフォーマンスがこのレベルを下回ることはありません。
- * 最大 IOPS 。 * NetApp Element ソフトウェアクラスタが特定のボリュームに提供する平常時の最大 IOPS 。
- * Burst IOPS 。 * 短時間のバースト時に許容される最大 IOPS 。バースト期間の設定は、デフォルトの 1 分に設定できます。ボリュームが最大 IOPS レベル未満で動作しているときは、バーストクレジットが蓄積されます。パフォーマンスレベルが非常に高くなってプッシュされると、ボリュームで IOPS が最大 IOPS を超えた短時間のバーストが許容されます。

マルチテナンシー

セキュアマルチテナンシーには、次の機能があります。

- * セキュアな認証。 * Challenge Handshake Authentication Protocol （ CHAP ； チャレンジハンドシェイク認証プロトコル）は、ボリュームへのセキュアなアクセスに使用されます。Lightweight Directory Access Protocol （ LDAP ）は、管理とレポートのためのクラスタへのセキュアなアクセスに使用されます。
- * ボリュームアクセスグループ（ VAG ） 。 * 必要に応じて、任意の数の iSCSI イニシエータ固有の iSCSI Qualified Name （ IQN ）を 1 つ以上のボリュームにマッピングし、認証の代わりに VAG を使用できます。VAG 内のボリュームにアクセスするには、イニシエータの IQN がボリュームグループの許可された IQN リストに含まれている必要があります。

- * テナント仮想 LAN（VLAN）。* ネットワークレベルでは、iSCSI イニシエータと NetApp Element ソフトウェアクラスタ間のエンドツーエンドのネットワークセキュリティは、VLAN を使用することで容易になります。ワークロードまたはテナントを分離するために作成された VLAN については、NetApp Element ソフトウェアが、特定の VLAN 経由でのみアクセス可能な iSCSI ターゲット SVIP アドレスを別途作成します。
- * VRF 対応 VLAN。* データセンターのセキュリティと拡張性をさらにサポートするため、NetApp Element ソフトウェアを使用すると、VRF に似た機能を持つテナント VLAN を有効にできます。この機能には、次の 2 つの主要機能が追加されて
 - * テナント SVIP アドレスへの L3 ルーティング。* この機能を使用すると、iSCSI イニシエータを、NetApp Element ソフトウェアクラスタとは別のネットワークまたは VLAN に配置できます。
 - * IP サブネットの重複または重複 *。この機能を使用すると、テナント環境にテンプレートを追加し、各テナント VLAN に同じ IP サブネットから IP アドレスを割り当てることができます。この機能は、IPspace の拡張と保持が重要なサービスプロバイダ環境に役立ちます。

エンタープライズクラスのストレージ効率化

NetApp Element ソフトウェアクラスタを使用すると、全体的なストレージ効率とパフォーマンスが向上します。次の機能はインラインで実行されます。常時有効であり、ユーザによる手動設定は必要ありません。

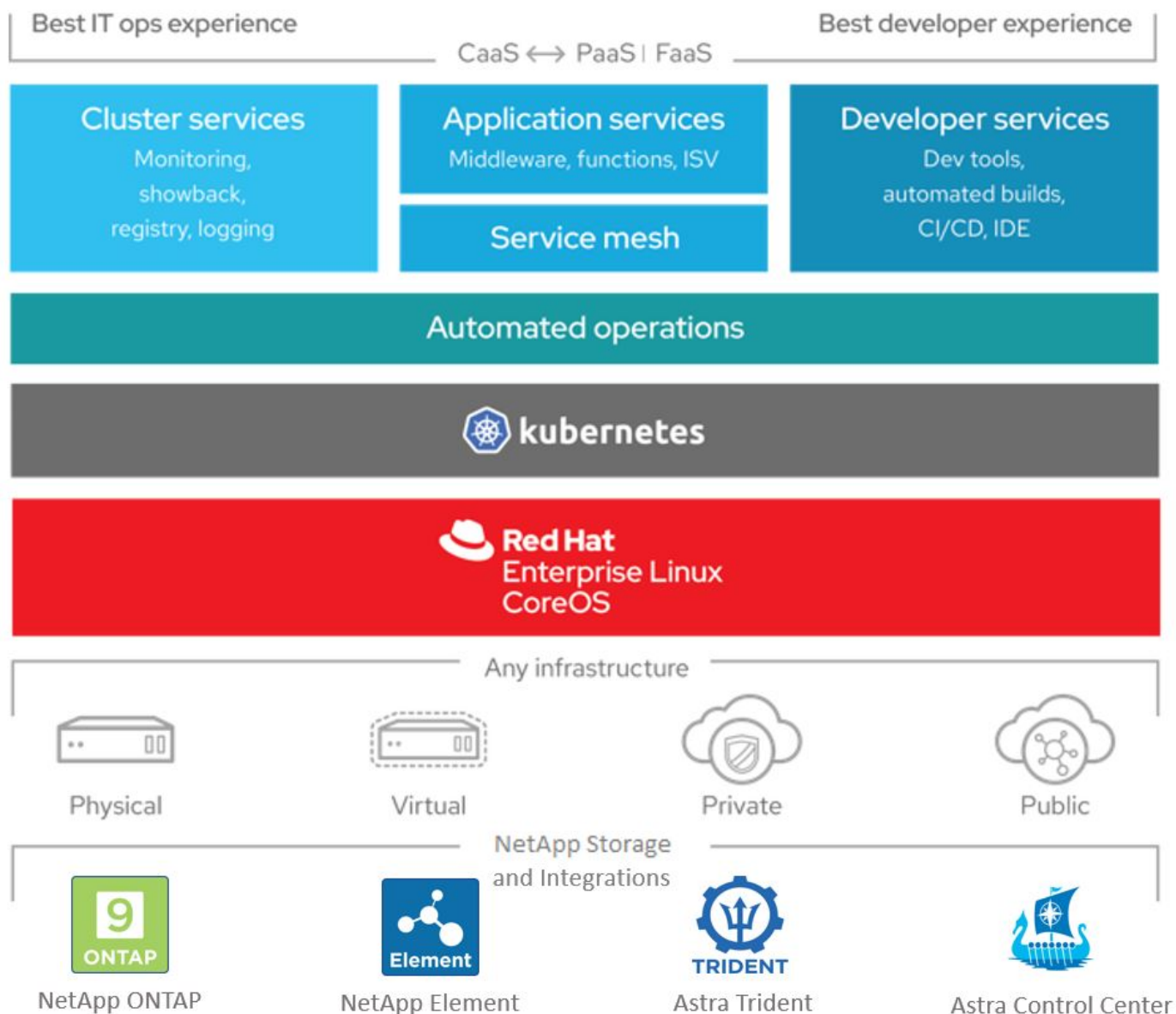
- * 重複排除。* システムには、一意の 4K ブロックのみが保存されます。重複する 4K ブロックは格納済みのデータバージョンに自動的に関連付けられます。データはブロックドライブに格納され、NetApp Element ソフトウェアの Helix データ保護を使用してミラーリングされます。このシステムは、システム内の容量消費と書き込み処理数を大幅に削減します。
- * 圧縮。* 圧縮は、データが NVRAM に書き込まれる前にインラインで実行されます。データは 4K ブロック単位で圧縮され、システム内で圧縮されたままとなります。この圧縮により、クラスタ全体での容量消費、書き込み処理数、および帯域幅消費が大幅に削減されます。
- * シンプロビジョニング。* この機能は、必要なときに必要な量のストレージを提供し、オーバープロビジョニングされたボリュームや利用率の低いボリュームによる容量消費を排除します。
- * Helix。* 個々のボリュームのメタデータはメタデータドライブに格納され、セカンダリメタデータドライブにレプリケートされて冗長性が確保されます。



Element は自動化を目的として設計されました。ストレージ機能はすべて API を使用して利用できます。これらの API は、システムの制御に UI で使用される唯一のメソッドです。

ネットアップストレージ統合の概要

ネットアップは、Red Hat OpenShift などのコンテナベースの環境における永続的データのオーケストレーションと管理に役立つさまざまな製品を提供します。



NetApp Astra Control は、ネットアップのデータ保護テクノロジーを基盤とするステートフル Kubernetes ワークロード向けの充実したストレージサービスとアプリケーション対応データ管理サービスを提供します。Astra Control Service は、クラウドネイティブの Kubernetes 環境でステートフルワークロードをサポートするために利用できます。Astra Control Center は、Red Hat OpenShift などのオンプレミス環境でステートフルワークロードをサポートするために使用できます。詳細については、NetApp Astra Control の Web サイトをご覧ください ["こちらをご覧ください"](#)。

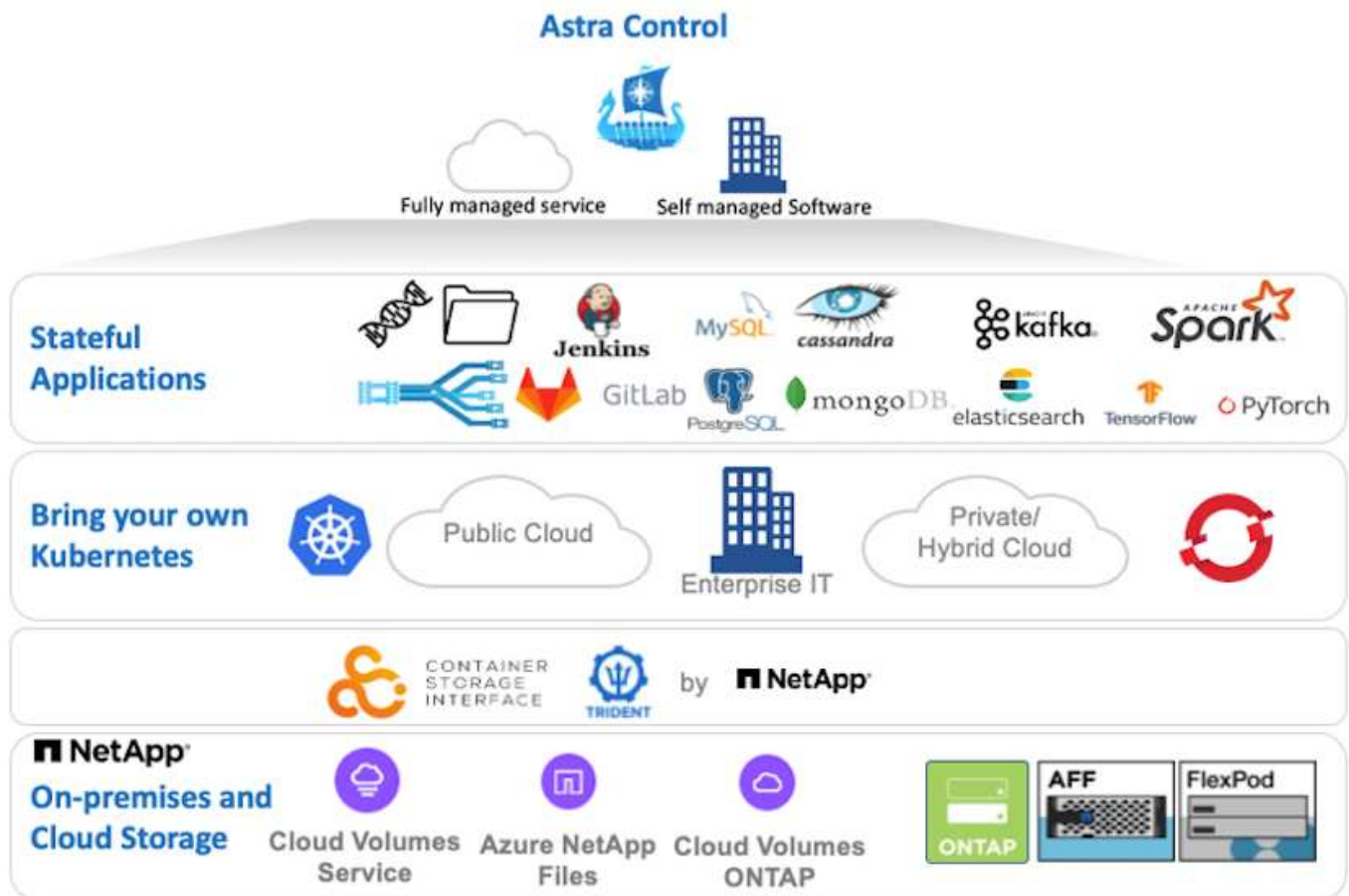
NetApp Astra Trident は、コンテナや Kubernetes ディストリビューション向けの、Red Hat OpenShift などのオープンソースで完全にサポートされているストレージオーケストレーションツールです。詳細については、Astra Trident の Web サイトをご覧ください ["こちらをご覧ください"](#)。

以下のページには、解決策追加情報に実装された Red Hat OpenShift でアプリケーションおよび永続的ストレージ管理のために検証されたネットアップ製品に関する があります。

- ["ネットアップアストラコントロールセンター"](#)
- ["ネットアップアストラ Trident"](#)

NetApp Astra Control Center の概要

NetApp Astra Control Center は、オンプレミス環境に導入され、ネットアップのデータ保護テクノロジーを基盤とするステートフル Kubernetes ワークロード向けの充実したストレージサービスとアプリケーション対応データ管理サービスを提供します。



NetApp Astra Control Center は、Astra Trident ストレージオーケストレーションツールを導入し、NetApp ONTAP ストレージシステムにストレージクラスとストレージバックエンドを使用して構成した Red Hat OpenShift クラスタにインストールできます。

Astra Trident のインストールと設定を行い、Astra Control Center をサポートするには、[を参照してください "このドキュメントはこちら"](#)。

クラウド接続環境では、Cloud Insights を使用して高度なモニタリングとテレメトリを提供します。Cloud Insights 接続がない場合は、限定的な監視と計測（7 日間相当の指標）を使用でき、オープン指標エンドポイントを介して Kubernetes の標準の監視ツール（Prometheus および Grafana）にエクスポートされます。

Astra Control Center は、NetApp AutoSupport と Active IQ のデジタルアドバイザー（デジタルアドバイザーとも呼ばれます）エコシステムに完全に統合されており、ユーザのサポート、トラブルシューティングの支援、使用状況の統計の表示を提供します。

Astra Control Center の有料版に加え、90 日間の評価ライセンスも提供されています。評価版は、E メールとコミュニティ（Slack チャンネル）を通じてサポートされています。お客様は、これらの記事やその他のナレッジベース記事、および製品サポートダッシュボードから入手可能なドキュメントにアクセスできます。

ネットアップアストラコントロールセンターの利用を開始するには、[にアクセスしてください "Astra の Web](#)

サイト"。

Astra Control Center のインストールの前提条件

1. 1 つ以上の Red Hat OpenShift クラスタ。バージョン 4.6 EUS および 4.7 が現在サポートされています。
2. 各 Red Hat OpenShift クラスタに Astra Trident をインストールして設定しておく必要があります。
3. ONTAP 9.5 以降を実行している NetApp ONTAP ストレージシステムが 1 つ以上必要です。



サイトに各 OpenShift インストールを実装し、永続的ストレージ専用の SVM を用意することがベストプラクティスです。マルチサイト環境では、追加のストレージシステムが必要です。

4. Trident ストレージバックエンドは、ONTAP クラスタがサポートする SVM を含む各 OpenShift クラスタで設定する必要があります。
5. ストレージプロビジョニングツールとして Astra Trident を使用し、各 OpenShift クラスタに設定されたデフォルトのストレージクラス。
6. ロードバランシングや OpenShift Services の公開のために、各 OpenShift クラスタにロードバランサをインストールして構成する必要があります。



リンクを参照してください ["こちらをご覧ください"](#) この目的で検証済みのロードバランサに関する情報。

7. NetApp アストラ Control Center イメージをホストするには、プライベートイメージのレジストリを設定する必要があります。



リンクを参照してください ["こちらをご覧ください"](#) この目的のために OpenShift プライベートレジストリをインストールして構成します。

8. Red Hat OpenShift クラスタにクラスタ管理者アクセス権限が必要です。
9. NetApp ONTAP クラスタへの管理者アクセスが必要です。
10. Docker または podman 、 tridentctl 、 OC または kubectl ツールがインストールされ、\$path に追加された管理ワークステーション。



Docker をインストールする場合は、20.10 よりも前のバージョンの Docker 、 Podman をインストールする場合は、バージョン 3.0 よりも前の podman が必要です。

Astra Control Center をインストールします

OperatorHub を使用する

1. ネットアップサポートサイトにログインし、最新バージョンの NetApp Astra Control Center をダウンロードします。そのためには、ネットアップアカウントにライセンスを関連付ける必要があります。tarball をダウンロードしたら、admin ワークステーションに転送します。



Astra Control の試用版ライセンスの使用を開始するには、にアクセスしてください "[Astra 登録サイト](#)"。

2. tar ボールを開梱し、作業ディレクトリを作成されたフォルダに変更します。

```
[netapp-user@rhel7 ~]$ tar -vxzf astra-control-center-21.12.60.tar.gz
[netapp-user@rhel7 ~]$ cd astra-control-center-21.12.60
```

3. インストールを開始する前に、Astra Control Center イメージをイメージレジストリにプッシュします。この手順では、Docker または Podman のいずれかを使用して実行します。両方の手順については、この手順で説明します。

ポドマン

- a. レジストリ FQDN を、組織 / 名前空間 / プロジェクト名とともに環境変数「管理」としてエクスポートします。

```
[netapp-user@rhel7 ~]$ export REGISTRY=astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra
```

- b. レジストリにログインします。

```
[netapp-user@rhel7 ~]$ podman login -u ocp-user -p password --tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com
```



「kubeadmin」ユーザを使用してプライベートレジストリにログインしている場合は、「podman login -u OCP -user -p token --tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com」の代わりにトークンを使用します。



または、サービスアカウントのトークンを使用して、サービスアカウントを作成し、（プッシュアクセスまたはプルアクセスが必要かどうかに応じて）レジストリエディタまたはレジストリビューアロールを割り当て、レジストリにログインすることもできます。

- c. シェルスクリプトファイルを作成し、次の内容を貼り付けます。

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh

for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded
  image trimming the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image(s): //' )
  astraImage=$(echo ${astraImage} | sed 's!localhost/!!!')
  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/${astraImage}
  # Push to the local repo.
  podman push ${REGISTRY}/${astraImage}
done
```



レジストリに信頼されていない証明書を使用している場合は、シェルスクリプトを編集し、podman push コマンドに「--tls-verify=false」を使用します。「podman push \$registry/\$」（echo \$astraallImage | sed's ^\V\W"/--tls-verify=false」）。

- d. ファイルを実行可能にします

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

e. シェルスクリプトを実行します。

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```


Docker です

- a. レジストリ FQDN を、組織 / 名前空間 / プロジェクト名とともに環境変数「管理」としてエクスポートします。

```
[netapp-user@rhel7 ~]$ export REGISTRY=astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra
```

- b. レジストリにログインします。

```
[netapp-user@rhel7 ~]$ docker login -u ocp-user -p password astra-registry.apps.ocp-vmw.cie.netapp.com
```



「kubeadmin」ユーザを使用してプライベートレジストリにログインする場合は、「password -d Occker login -u OCP-user-p token astra-registry.apps.ocp-vmw.cie.netapp.com」の代わりにトークンを使用します。



または、サービスアカウントのトークンを使用して、サービスアカウントを作成し、（プッシュアクセスまたはプルアクセスが必要かどうかに応じて）レジストリエディタまたはレジストリビューアロールを割り当て、レジストリにログインすることもできます。

- c. シェルスクリプトファイルを作成し、次の内容を貼り付けます。

```
[netapp-user@rhel7 ~]$ vi push-images-to-registry.sh

for astraImageFile in $(ls images/*.tar) ; do
    # Load to local cache. And store the name of the loaded
    image trimming the 'Loaded images: '
    astraImage=$(docker load --input ${astraImageFile} | sed
's/Loaded image: //' )
    astraImage=$(echo ${astraImage} | sed 's!localhost/!!')
    # Tag with local image repo.
    docker tag ${astraImage} ${REGISTRY}/${astraImage}
    # Push to the local repo.
    docker push ${REGISTRY}/${astraImage}
done
```

- d. ファイルを実行可能にします

```
[netapp-user@rhel7 ~]$ chmod +x push-images-to-registry.sh
```

- e. シェルスクリプトを実行します。

```
[netapp-user@rhel7 ~]$ ./push-images-to-registry.sh
```

4. 公開されていないプライベートイメージレジストリを使用する場合は、イメージレジストリ TLS 証明書を OpenShift ノードにアップロードします。そのためには、TLS 証明書を使用して OpenShift -config ネームスペースに ConfigMap を作成し、クラスタイメージ構成にパッチを適用して証明書を信頼できるようにします。

```
[netapp-user@rhel7 ~]$ oc create configmap default-ingress-ca -n
openshift-config --from-file=astra-registry.apps.ocp
-vmw.cie.netapp.com=tls.crt

[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster
--patch '{"spec":{"additionalTrustedCA":{"name":"default-ingress-
ca"}}}' --type=merge
```



ルートとともに入力オペレータからのデフォルト TLS 証明書を含む OpenShift 内部レジストリを使用している場合は、前の手順に従って、ルートホスト名に証明書をパッチする必要があります。入力オペレータから証明書を抽出するには、コマンド「`oc extract secret/router-ca --keys=tls.crt-n OpenShift ingress-operator`」を使用します。

5. Astra Control Center 用の名前空間 NetApp-acc-operator' を作成します

```
[netapp-user@rhel7 ~]$ oc create ns netapp-acc-operator

namespace/netapp-acc-operator created
```

6. NetApp-acc-operator ネームスペースのイメージレジストリにログインするためのクレデンシャルを含むシークレットを作成します。


```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-
registry-cred --docker-server=astra-registry.apps.ocp
-vmw.cie.netapp.com --docker-username=ocp-user --docker
-password=password -n netapp-acc-operator

secret/astra-registry-cred created
```

7. クラスタ管理者アクセスで Red Hat OpenShift GUI コンソールにログインします。
8. Perspective ドロップダウンから Administrator を選択します。
9. [演算子]>[演算子ハブ] の順に移動し、Astra を検索します。



10. NetApp-acc-operator' タイルを選択し、[インストール] をクリックします。



netapp-acc-operator
21.12.63-1 provided by NetApp

✕

Install

Latest version
21.12.63-1

Capability level
☒ Basic Install
☐ Seamless Upgrades
☐ Full Lifecycle
☐ Deep Insights
☐ Auto Pilot

Provider type
Certified

Provider
NetApp

Astra Control is an application-aware data management solution that manages, protects and moves data-rich Kubernetes workloads in both public clouds and on-premises.

Astra Control enables data protection, disaster recovery, and migration for your Kubernetes workloads, leveraging NetApp's industry-leading data management technology for snapshots, backups, replication and cloning.

How to deploy Astra Control

Refer to [Installation Procedure](#) to deploy Astra Control Center using the Operator.

Documentation

Refer to [Astra Control Center Documentation](#) to complete the setup and start managing applications.

11. インストールオペレータ画面で、デフォルトのパラメータをすべて受け入れて、「インストール」をクリックします。

Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

Update channel *

- ☐ alpha
☒ stable

Installation mode *

- ☒ All namespaces on the cluster (default)
Operator will be available in all Namespaces.
- ☐ A specific namespace on the cluster
This mode is not supported by this Operator

Installed Namespace *

PR netapp-acc-operator (Operator recommended)

⚠ Namespace already exists


Namespace **netapp-acc-operator** already exists and will be used. Other users can already have access to this namespace.

Approval strategy *

- ☒ Automatic
☐ Manual

Install

Cancel

 **netapp-acc-operator**
provided by NetApp

Provided APIs

 **Astra Control Center**

AstraControlCenter is the Schema for the astracontrolcenters API

12. オペレータによるインストールが完了するまで待ちます。



netapp-acc-operator
21.12.63-1 provided by NetApp



Installing Operator

InstallWaiting: installing: waiting for deployment acc-operator-controller-manager to become ready: Waiting for rollout to finish: 0 of 1 updated replicas are available...

The Operator is being installed. This may take a few minutes.

[View installed Operators in Namespace netapp-acc-operator](#)

13. オペレータのインストールが完了したら、[View Operator] をクリックします。



netapp-acc-operator
21.12.63-1 provided by NetApp



Installed operator - ready for use

[View Operator](#)

[View installed Operators in Namespace netapp-acc-operator](#)

14. 次に、オペレーターの Astra Control Center タイルで [Create Instance] をクリックします。

[Installed Operators](#) > [Operator details](#)



netapp-acc-operator
21.12.63-1 provided by NetApp

[Details](#)

[YAML](#)

[Subscription](#)

[Events](#)

[Astra Control Center](#)

Provided APIs

ACC Astra Control Center

AstraControlCenter is the Schema for the astracontrolcenters API

[+ Create instance](#)

15. [Create AstraControl] フォームフィールドに入力し [Create] をクリックします
- 必要に応じて、Astra Control Center インスタンス名を編集します。
 - 必要に応じて、AutoSupport を有効または無効にします。Auto Support 機能の保持を推奨します。
 - Astra Control Center の FQDN を入力します。
 - Astra Control Center のバージョンを入力します。デフォルトで最新のバージョンが表示されま

す。

- e. Astra Control Center のアカウント名を入力し、管理者の詳細（名、姓、メールアドレスなど）を入力します。
- f. ボリューム再利用ポリシーを入力します。デフォルトは Retain です。
- g. Image Registry に、レジストリの FQDN と、イメージをレジストリにプッシュする際に指定した組織名を入力します（この例では「astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra」）。
- h. 認証が必要なレジストリを使用する場合は、[イメージレジストリ] セクションにシークレット名を入力します。
- i. Astra Control Center のリソース制限のスケーリングオプションを設定します。
- j. デフォルト以外のストレージクラスに PVC を配置する場合は、ストレージクラス名を入力します。
- k. CRD 処理の環境設定を定義します。

Project: netapp-acc-operator ▼

Name *

Labels

Account Name *

Astra Control Center account name

Astra Address *

AstraAddress defines how Astra will be found in the data center. This IP address and/or DNS A record must be created prior to provisioning Astra Control Center. Example - "astra.example.com" The A record and its IP address must be allocated prior to provisioning Astra Control Center

Astra Version *

Version of AstraControlCenter to deploy. You are provided a Helm repository with a corresponding version. Example - 1.5.2, 1.4.2-patch

Email *

EmailAddress will be notified by Astra as events warrant.

Auto Support * >

AutoSupport indicates willingness to participate in NetApp's proactive support application, NetApp Active IQ. The default election is true and indicates support data will be sent to NetApp. An empty or blank election is the same as a default election. Air gapped installations should enter false.

First Name

The first name of the SRE supporting Astra.

Last Name

Admin

The last name of the SRE supporting Astra.

Image Registry

The container image registry that is hosting the Astra application images, ACC Operator and ACC Helm Repository.

Name

astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra

The name of the image registry. For example "example.registry/astra". Do not prefix with protocol.

Secret

astra-registry-cred

The name of the Kubernetes secret that will authenticate with the image registry.

Volume Reclaim Policy

Retain

Reclaim policy to be set for persistent volumes

Astra Resources Scaler

Default

Scaling options for AstraControlCenter Resource limits.

Storage Class

The storage class to be used for PVCs. If not set, default storage class will be used.

Crds

Options for how ACC should handle CRDs.

Create

Cancel

自動化された [Ansible]

1. Ansibleプレイブックを使用してAstra Control Centerを導入するには、AnsibleがインストールされたUbuntu / RHELマシンが必要です。手順に従います ["こちらをご覧ください"](#) UbuntuおよびRHELの場合。
2. Ansible コンテンツをホストする GitHub リポジトリをクローニングします。

```
git clone https://github.com/NetApp-
Automation/na_astra_control_suite.git
```

3. ネットアップサポートサイトにログインし、最新バージョンのNetApp Astra Control Centerをダウンロードします。そのためには、ネットアップアカウントにライセンスを関連付ける必要があります。tar ファイルをダウンロードしたら、ワークステーションに転送します。



Astra Control の試用版ライセンスの使用を開始するには、にアクセスしてください ["Astra 登録サイト"](#)。

4. Astra Control CenterをインストールするOpenShiftクラスタにadminとしてアクセスし、kubeconfig

ファイルを作成または取得します。

5. ディレクトリを `na_Astra_control_site` に変更します。

```
cd na_astra_control_suite
```

6. 「vars/vars.yml」 ファイルを編集し、必要な情報を変数に入力します。

```
#Define whether or not to push the Astra Control Center images to
your private registry [Allowed values: yes, no]
push_images: yes

#The directory hosting the Astra Control Center installer
installer_directory: /home/admin/

#Specify the ingress type. Allowed values - "AccTraefik" or
"Generic"
#"AccTraefik" if you want the installer to create a LoadBalancer
type service to access ACC, requires MetallB or similar.
#"Generic" if you want to create or configure ingress controller
yourself, installer just creates a ClusterIP service for traefik.
ingress_type: "AccTraefik"

#Name of the Astra Control Center installer (Do not include the
extension, just the name)
astra_tar_ball_name: astra-control-center-22.04.0

#The complete path to the kubeconfig file of the
kubernetes/openshift cluster Astra Control Center needs to be
installed to.
hosting_k8s_cluster_kubeconfig_path: /home/admin/cluster-
kubeconfig.yml

#Namespace in which Astra Control Center is to be installed
astra_namespace: netapp-astra-cc

#Astra Control Center Resources Scaler. Leave it blank if you want
to accept the Default setting.
astra_resources_scaler: Default

#Storageclass to be used for Astra Control Center PVCs, it must be
created before running the playbook [Leave it blank if you want the
PVCs to use default storageclass]
astra_trident_storageclass: basic

#Reclaim Policy for Astra Control Center Persistent Volumes [Allowed
```

```

values: Retain, Delete]
storageclass_reclaim_policy: Retain

#Private Registry Details
astra_registry_name: "docker.io"

#Whether the private registry requires credentials [Allowed values:
yes, no]
require_reg_creds: yes

#If require_reg_creds is yes, then define the container image
registry credentials
#Usually, the registry namespace and usernames are same for
individual users
astra_registry_namespace: "registry-user"
astra_registry_username: "registry-user"
astra_registry_password: "password"

#Kuberenets/OpenShift secret name for Astra Control Center
#This name will be assigned to the K8s secret created by the
playbook
astra_registry_secret_name: "astra-registry-credentials"

#Astra Control Center FQDN
acc_fqdn_address: astra-control-center.cie.netapp.com

#Name of the Astra Control Center instance
acc_account_name: ACC Account Name

#Administrator details for Astra Control Center
admin_email_address: admin@example.com
admin_first_name: Admin
admin_last_name: Admin

```

7. プレイブックを実行して Astra Control Center を導入します。Playbookには、特定の構成用のroot権限が必要です。

このプレイブックを実行しているユーザがrootである場合、またはパスワードを使用しないsudoが設定されている場合は、次のコマンドを実行してプレイブックを実行します。

```

ansible-playbook install_acc_playbook.yml

```

ユーザにパスワードベースのsudoアクセスが設定されている場合は、次のコマンドを実行してこのPlaybookを実行し、sudoパスワードを入力します。

```
ansible-playbook install_acc_playbook.yml -K
```

インストール後の手順

1. インストールが完了するまでに数分かかることがあります。NetApp-AstrA-cc' ネームスペース内のすべてのポッドとサービスが稼働していることを確認します

```
[netapp-user@rhel7 ~]$ oc get all -n netapp-astra-cc
```

2. 「acc-operator-controller-manager」ログをチェックし、インストールが完了したことを確認します。

```
[netapp-user@rhel7 ~]$ oc logs deploy/acc-operator-controller-manager -n  
netapp-acc-operator -c manager -f
```



次のメッセージは、Astra Control Center のインストールが正常に完了したことを示します。

```
{"level":"info","ts":1624054318.029971,"logger":"controllers.AstraControlCenter","msg":"Successfully Reconciled AstraControlCenter in [seconds]s","AstraControlCenter":"netapp-astra-cc/astra","ae.Version":"[21.12.60]"}
```

3. Astra Control Center にログインするためのユーザ名は、CRD ファイルに提供された管理者の電子メールアドレスで、パスワードは Astra Control Center UUID に付加された文字列「ACC-」です。次のコマンドを実行します。

```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc  
NAME      UUID  
astra     345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```



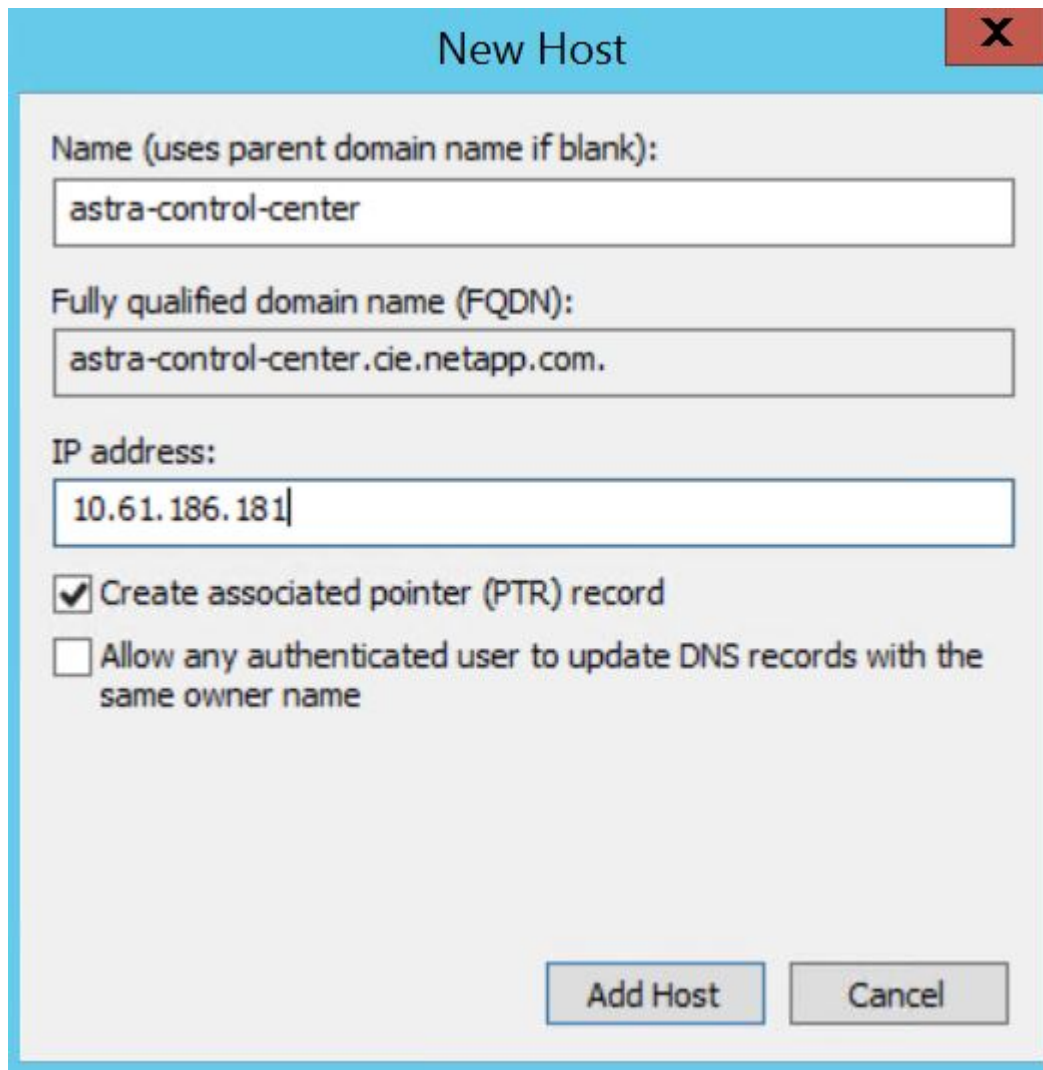
この例では、パスワードは「ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f」です。

4. traefik サービスのロードバランサ IP を取得します。

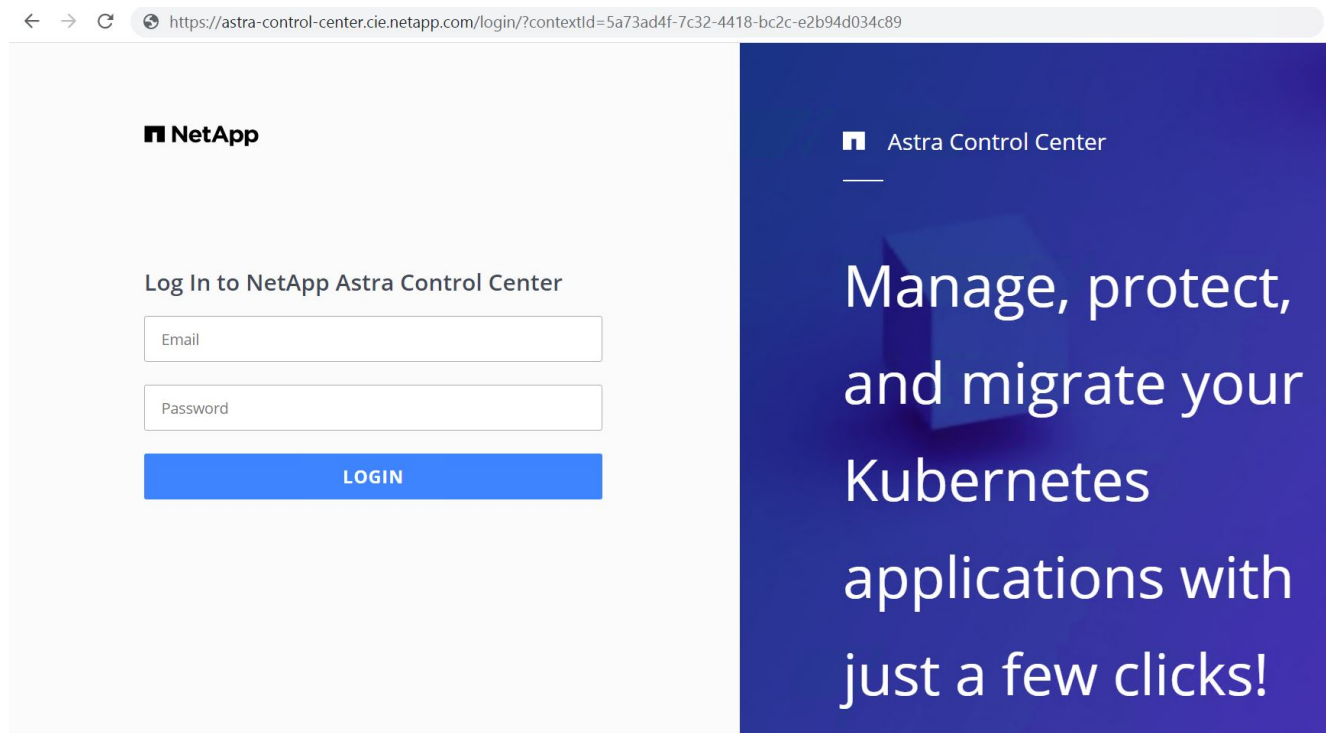
```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep  
'EXTERNAL|traefik'
```

NAME	EXTERNAL-IP	PORT(S)	TYPE	CLUSTER-IP
traefik	10.61.186.181	80:30343/TCP, 443:30060/TCP	LoadBalancer	172.30.99.142
AGE 16m				

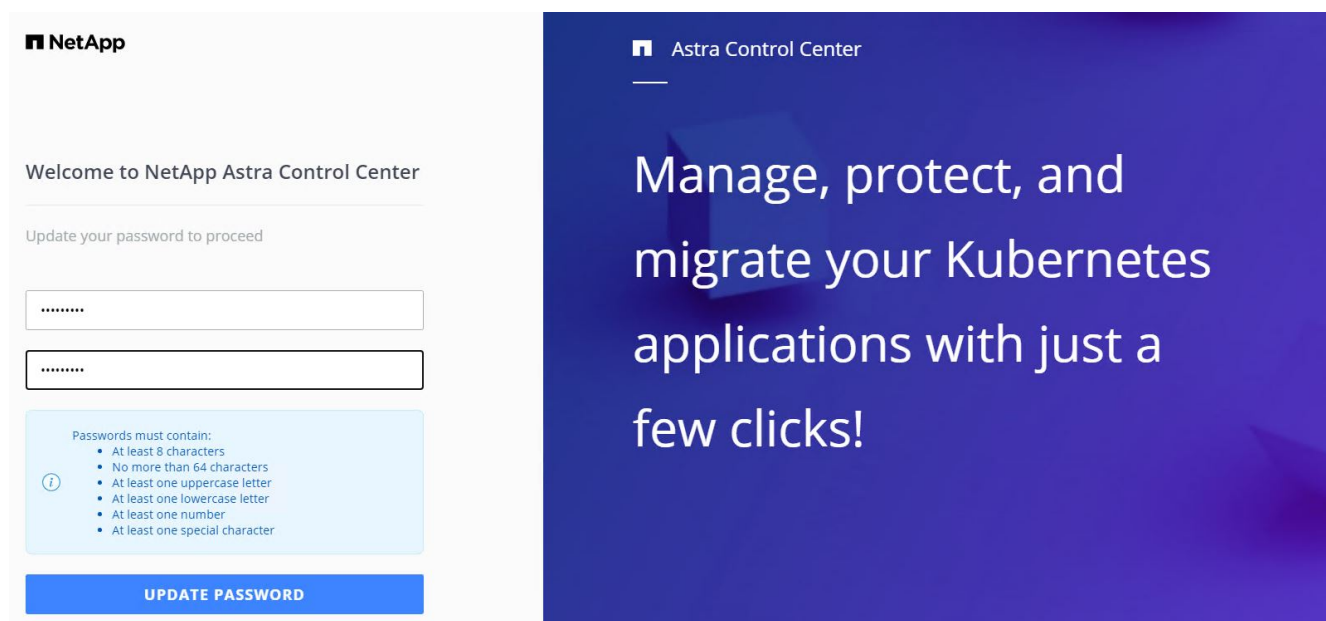
5. Astra Control Center CRD ファイルに指定された FQDN を指す DNS サーバーのエントリを、traefik サービスの「external-IP」に追加します。



6. Astra Control Center GUI に、FQDN を参照してログインします。



7. CRD で提供された管理者メールアドレスを使用して初めて Astra Control Center GUI にログインする場合は、パスワードを変更する必要があります。



8. ユーザーを Astra Control Center に追加する場合は、[アカウント]>[ユーザー] の順に選択し、[追加] をクリックしてユーザーの詳細を入力し、[追加] をクリックします。

Add user

USER DETAILS

First name: Nikhil

Last name: Kulkarni

Email address: tme_nik@netapp.com

PASSWORD

Temporary password: *****

Confirm temporary password: *****

Passwords must contain:

- At least 8 characters
- No more than 64 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character

USER ROLE

Role: Owner

Cancel Add ✓

ADD NEW USER

Add new user

Add a new user to your Astra Control Center account. New users will be prompted to update their password the first time they log in to Astra Control Center. They will also inherit access to account-wide credentials according to their role. Read more in [users](#).

9. Astra Control Center では、すべての機能が動作するためにライセンスが必要です。ライセンスを追加するには、[アカウント] > [ライセンス] の順に選択し、[ライセンスの追加] をクリックして、ライセンスファイルをアップロードします。

Account

Users Credentials Notifications **License** Connections

ASTRA CONTROL CENTER LICENSE

To get started with Astra Control Center, select Add license to manually upload the file.

ADD LICENSE

Select and add a license file.

License file: EvalNLF-AstraControlCenter-480Cores(vCPU)-100000002-ACC60f19...

Cancel Add

Add license




NetApp Astra Control Center のインストールまたは設定で問題が発生した場合は、既知の問題のナレッジベースを利用できます ["こちらをご覧ください"](#)。

Red Hat OpenShift クラスタを Astra Control Center に登録します


Astra Control Center でワークロードを管理できるようにするには、まず Red Hat OpenShift クラスタを登録する必要があります。

Red Hat OpenShift クラスタを登録します

1. 最初のステップでは、OpenShift クラスタを Astra Control Center に追加して管理します。クラスタに移動してクラスタの追加をクリックし、OpenShift クラスタの kubeconfig ファイルをアップロードして、ストレージの選択をクリックします。

 **Add cluster**

STEP 1/3: CREDENTIALS





CREDENTIALS

Provide Astra Control access to your Kubernetes and OpenShift clusters by entering a kubeconfig credential.

Follow [instructions](#) on how to create a dedicated admin-role kubeconfig.

[Upload file](#) [Paste from clipboard](#)

Kubeconfig YAML file
ocp-vmw kubeconfig.txt

Credential name
ocp-vmw

ADDING A CLUSTER

Adding a cluster is needed for Astra Control to discover your Kubernetes applications.

Select a cloud provider and input credentials to get started.

Read more in [Clusters](#).

Cancel

Configure storage →



ユーザ名とパスワードまたはトークンを使用して認証するために kubeconfig ファイルを生成できます。トークンが期限切れになるまでの時間は制限されており、登録されたクラスタに到達できなくなる可能性があります。ネットアップでは、OpenShift クラスタを Astra Control Center に登録するために、ユーザ名とパスワードを付けた kubeconfig ファイルを使用することを推奨します。

2. Astra Control Center で、対象となるストレージクラスが検出される。次に、ストレージクラスが NetApp ONTAP 上の SVM がサポートする Trident を使用してボリュームをプロビジョニングする方法を選択し、Review（確認）をクリックします。次のペインで詳細を確認し、Add Cluster をクリックします。

STORAGE

Existing storage classes are discovered and verified as eligible for use with Astra Control. You can use your existing default, or choose to set a new default at this time.
Applications with persistent volumes on eligible storage classes are validated for use with Astra Control.

Set default	Storage class	Storage provisioner	Reclaim policy	Binding mode	Eligible
<input checked="" type="radio"/>	ocp-trident <small>Default</small>	csi.trident.netapp.io	Delete	Immediate	✓
<input type="radio"/>	ocp-trident-iscsi	csi.trident.netapp.io	Delete	Immediate	✓
<input type="radio"/>	project-1-sc	csi.trident.netapp.io	Delete	Immediate	⚠
<input type="radio"/>	thin	kubernetes.io/vsphere-volume	Delete	Immediate	⚠

← Select credentials

Review →

3. 手順 1 の説明に従って、両方の OpenShift クラスタを登録します。追加すると、Astra Control Center がクラスタを検査して必要なエージェントをインストールしながら、クラスタは Discovering ステータスに移行します。クラスタが登録されると、クラスタのステータスが「Running」に変わります。

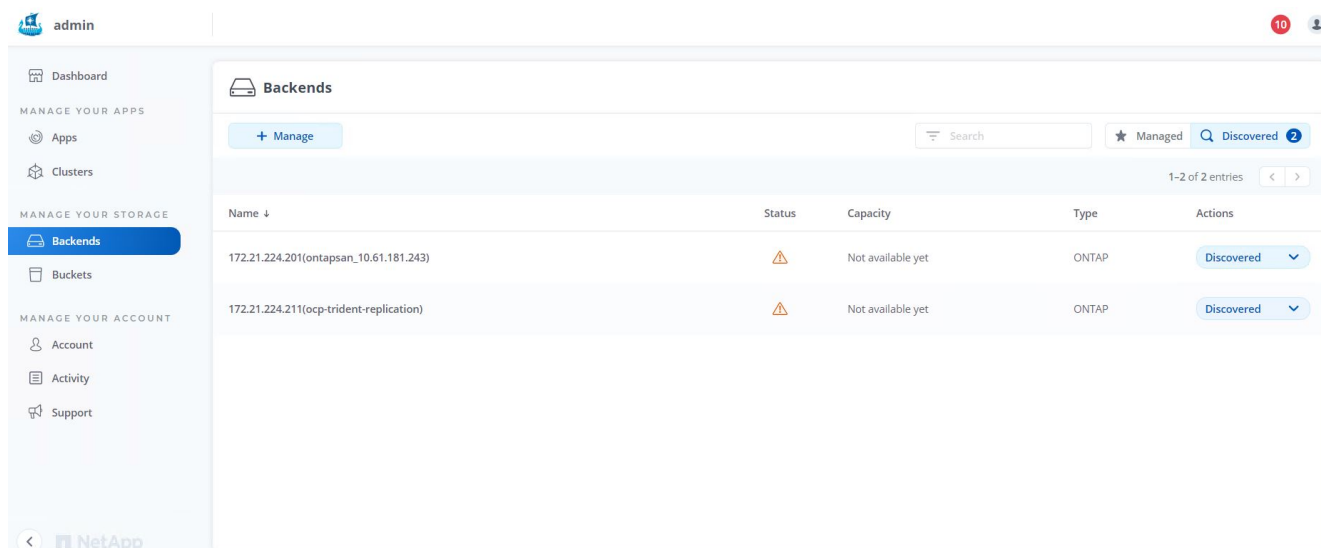
The screenshot shows the Astra Control Center interface. The left sidebar has a 'Clusters' section highlighted. The main content area displays a table titled 'Clusters' with the following data:

Name	Ready	Type	Version	Actions
ocp-vmw	✓	Red Hat OpenShift	v1.20.0+df9c838	Running
ocp-vmware2	✓	Red Hat OpenShift	v1.20.0+c8905da	Running



Astra Control Center で管理するすべての Red Hat OpenShift クラスタは、管理対象クラスタにインストールされたエージェントとしてインストールに使用されたイメージレジストリにアクセスする必要があります。このレジストリからイメージがプルされます。

4. ONTAP クラスタをストレージリソースとして Astra Control Center でバックエンドとして管理するようにインポートします。ストレージクラスが設定されている Astra に OpenShift クラスタが追加されると、ストレージクラスをサポートする ONTAP クラスタが自動的に検出されて検査されますが、Astra コントロールセンターにインポートされて管理されません。



5. ONTAP クラスタをインポートするには、バックエンドに移動し、ドロップダウンをクリックして、管理対象の ONTAP クラスタの横にある Manage を選択します。ONTAP クラスタの資格情報を入力し、[情報の確認] をクリックして、[ストレージバックエンドのインポート] をクリックします。

6. バックエンドを追加すると、ステータスが Available に変わります。このバックエンドには、OpenShift クラスタ内の永続ボリュームと ONTAP システム上の対応するボリュームに関する情報が含まれます。

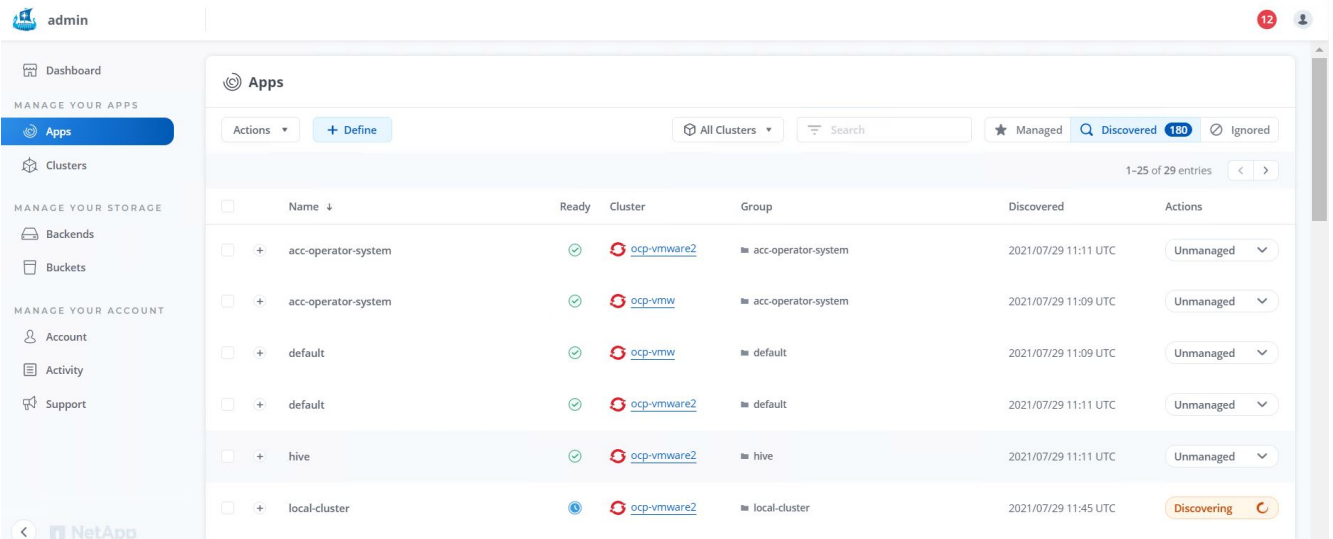


保護するアプリケーションを選択します

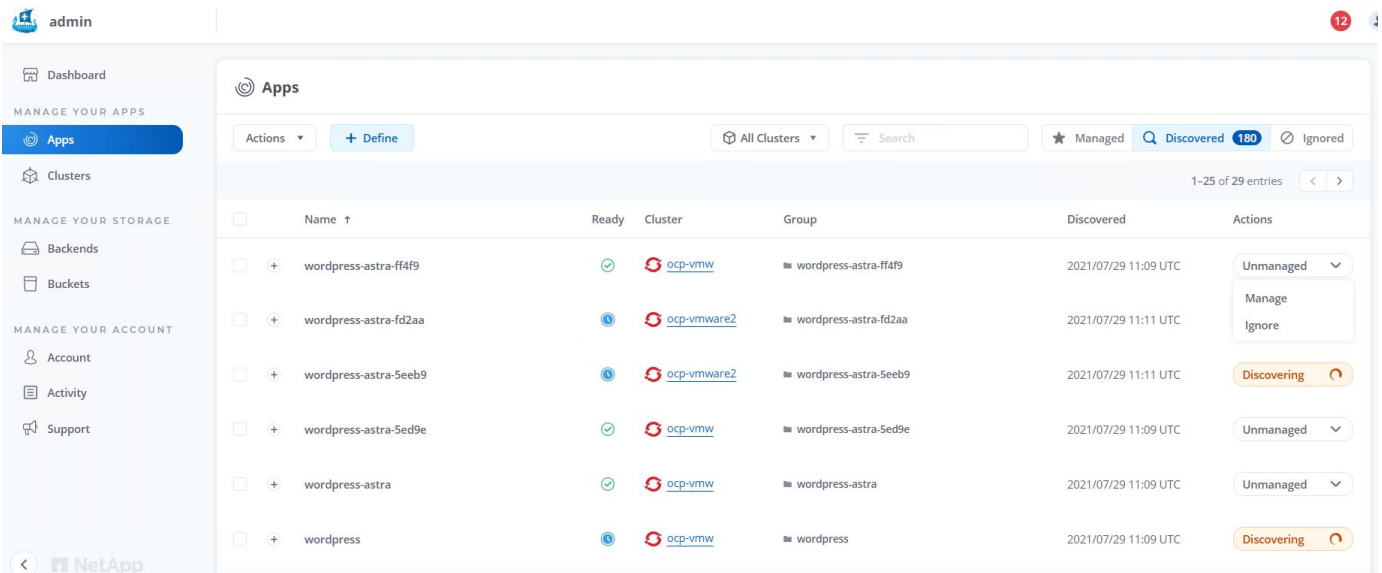
109

アプリケーションを管理します

1. OpenShift クラスタと ONTAP バックエンドが Astra Control Center に登録されると、コントロールセンターは、指定した ONTAP バックエンドで構成されたストレージクラスを使用するすべてのネームスペース内のアプリケーションを自動的に検出します。



2. [アプリケーション]>[検出済み]の順に移動し、Astra を使用して管理するアプリケーションの横にあるドロップダウンメニューをクリックします。[管理]をクリックします。



1. アプリケーションが[使用可能 (Available)] 状態になり、[アプリケーション (Apps)] セクションの[管理 (Managed)] タブで表示できます。

Apps							
Actions ▾		+ Define		All Clusters ▾		Search	
				★ Managed		Q Discovered 175	
						Ignored	
1-1 of 1 entries < >							
<input type="checkbox"/>	Name ↓	Ready	Protected	Cluster	Group	Discovered	Actions
<input type="checkbox"/>	wordpress-astra-ff4f9	✓	?	ocp-vmw	■ wordpress-astra-ff4f9	2021/07/29 11:09 UTC	Available ▾

アプリケーションを保護

アプリケーションワークロードを Astra Control Center で管理した後、それらのワークロードの保護設定を構成できます。

アプリケーションスナップショットを作成しています

アプリケーションの Snapshot コピーを作成すると、ONTAP Snapshot コピーが作成されます。Snapshot コピーに基づいて、アプリケーションを特定の時点にリストアまたはクローニングできます。

1. アプリケーションのスナップショットを作成するには、[アプリ] > [管理] タブに移動し、Snapshot コピーを作成するアプリケーションをクリックします。アプリケーション名の横にあるドロップダウンメニューをクリックし、Snapshot をクリックします。

APPLICATION STATUS

✓ Healthy

Images

docker.io/bitnami/mariadb:10.5.13-debian-10-r58

docker.io/bitnami/wordpress:5.9.0-debian-10-r1

APPLICATION PROTECTION STATUS

⚠ Unprotected

Protection schedule

Disabled

Group

■ wp

Running ▾

Snapshot

Backup

Clone

Restore

Unmanage

2. スナップショットの詳細を入力し、[次へ] をクリックして、[スナップショット] をクリックします。Snapshot の作成には約 1 分かかり、作成が完了するとステータスを確認できるようになります。

SNAPSHOT DETAILS

Name
wp-snapshot-20220228185949

CREATING APPLICATION SNAPSHOTS

Astra Control can take a quick snapshot of your application configuration and persistent storage. Enter a snapshot name to get started.

Read more in [Protect apps](#).

Application
wp

Namespace
wp

Cluster
ocp-vmw

Cancel

Next →

アプリケーションのバックアップを作成しています

アプリケーションのバックアップは、アプリケーションのアクティブな状態とそのリソースの設定をキャプチャしてファイルに変換し、リモートのオブジェクトストレージバケットに格納します。

Astra Control Center で管理対象アプリケーションのバックアップとリストアを行うには、バックアップ ONTAP システムのスーパーユーザ設定を前提条件として設定する必要があります。そのためには、次のコマンドを入力します。

```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1 -anon
65534 -vserver ocp-trident
```

1. Astra Control Center で管理対象アプリケーションのバックアップを作成するには、[アプリ] > [管理] タブに移動し、バックアップを作成するアプリケーションをクリックします。アプリケーション名の横にあるドロップダウンメニューをクリックし、[バックアップ] をクリックします。

wp

Running

APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Unprotected

Images
docker.io/bitnami/mariadb:10.5.13-debian-10-r58
docker.io/bitnami/wordpress:5.9.0-debian-10-r1

Protection schedule
Disabled

Group
wp

Cluster
ocp-vmw

Snapshot
Backup
Clone
Restore
Unmanage

2. バックアップの詳細を入力し、バックアップファイルを保存するオブジェクトストレージバケットを選択して次へをクリックします。詳細を確認したら、バックアップをクリックします。アプリケーションのサイズとデータによっては、バックアップに数分かかることがあり、バックアップが正常に完了したあとでバックアップのステータスを確認できるようになります。

Backup application

STEP 1/2: DETAILS

X

BACKUP DETAILS

Name

wp-backup

☐ Backup from an existing snapshot

BACKUP DESTINATION

Bucket

na-ocp-astra/na-ocp-acc Available

CREATING APPLICATION BACKUPS

Astra Control can take a backup of your application configuration and persistent storage. Persistent storage backups are transferred to your object store. Enter a backup name to get started.

Read more in [Application backups](#).

Application

wp

Namespace

wp

Cluster

ocp-vmw

Cancel

Next →

アプリケーションのリストア

ボタンを押すだけで、アプリケーションを同じクラスタ内の元のネームスペースまたはリモートクラスタにリストアし、アプリケーションを保護してディザスタリカバリに使用できます。

1. アプリケーションを復元するには、[アプリ]>[管理]タブに移動し、該当するアプリをクリックします。アプリケーション名の横にあるドロップダウン・メニューをクリックし「リストア」をクリックします

wp

Running

APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Partially protected

Images

docker.io/bitnami/mariadb:10.5.13-debian-10-r58

docker.io/bitnami/wordpress:5.9.0-debian-10-r1

Protection schedule

Disabled

Group

wp

Cluster

ocp-vmw

Snapshot

Backup

Clone

Restore

Unmanage

2. リストアネームスペースの名前を入力し、リストア先のクラスタを選択して、既存の Snapshot からリストアするかアプリケーションのバックアップからリストアするかを選択します。次へをクリックします。

Restore application

STEP 1/2: DETAILS

RESTORE DETAILS

Destination cluster

ocp-vmw

Destination namespace

wp

RESTORE SOURCE

Filter

SnapshotsBackups

Application backup	Ready	On-Schedule/On-Demand	Created ↑
wp-backup	✓	On-Demand	2022/02/28 18:54 UTC

RESTORING APPLICATIONS

Astra Control can restore your application configuration and persistent storage. Select a source snapshot or backup for the restored application.

- Application wp
- Namespace wp
- Cluster ocp-vmw

Cancel

Next →

- レビューペインで「restore」と入力し、詳細を確認した後で「Restore」をクリックします。

Restore application

STEP 2/2: SUMMARY

REVIEW RESTORE INFORMATION

All existing resources associated with this application will be deleted and replaced with the source backup "wp-backup" taken on 2022/02/28 18:54 UTC. Persistent volumes will be deleted and recreated. External resources with dependencies on this application may be impacted.

We recommend taking a snapshot or a backup of your application before proceeding.

BACKUP

wp-backup

ORIGINAL GROUP

wp

ORIGINAL CLUSTER

ocp-vmw

RESOURCE LABELS

ClusterRole

kubernetes.io/bootstrapping: rbac-defaults +1

ClusterRoleBinding

RESTORE

wp

DESTINATION GROUP

wp

DESTINATION CLUSTER

ocp-vmw

RESOURCE LABELS

ClusterRole

kubernetes.io/bootstrapping: rbac-defaults +1

ClusterRoleBinding

Are you sure you want to restore the application "wp"?

Type **restore** below to confirm.













Confirm to restore

restore

← Back

Restore ✓


- 新しいアプリケーションは、Astra Control Center が選択したクラスタ上のアプリケーションを復元している間、Restoring 状態になります。アプリケーションのすべてのリソースが Astra によってインストールおよび検出されると、アプリケーションは Available 状態になります。



Actions ▾	+ Define	 ▾	<input type="text" value="Search"/>			110	
<div>  1-1 of 1 entries <div>   </div> </div>							
<input type="checkbox"/>	Name ↓	Ready	Protected	Cluster	Group	Discovered	Actions
<input type="checkbox"/>	wp			 ocp-vmw	 wp	2022/02/28 18:34 UTC	Available 



アプリケーションのクローニング

アプリケーションは、開発 / テストやアプリケーションの保護およびディザスタリカバリ目的で、元のクラスタまたはリモートクラスタにクローニングできます。同じストレージバックエンドで同じクラスタ内にあるアプリケーションをクローニングする場合、NetApp FlexClone テクノLOGYを使用します。FlexClone テクノLOGYを使用すると、PVC のクローンを瞬時に作成し、ストレージスペースを節約できます。

1. アプリケーションをクローンするには、[アプリケーション (Apps)] > [管理 (Managed)] タブに移動し、該当するアプリケーションをクリックします。アプリケーション名の横にあるドロップダウンメニューをクリックし、Clone をクリックします。


 wp


 APPLICATION STATUS
 Healthy

 APPLICATION PROTECTION STATUS
 Partially protected

Images
docker.io/bitnami/mariadb:10.5.13-debian-10-r58
docker.io/bitnami/wordpress:5.9.0-debian-10-r1


Protection schedule
Disabled

Group
 wp

Cluster
 ocp-vmw

Running ▾
Snapshot
Backup
Clone
Restore
Unmanage

2. 新しいネームスペースの詳細を入力し、クローニング先のクラスタを選択します。クローンを既存の Snapshot、バックアップ、またはアプリケーションの現在の状態から作成するかどうかを選択します。詳細を確認したら、[次へ] をクリックして、[レビューペインに複製] をクリックします。

 Clone application


STEP 1/2: DETAILS


✕

CLONE DETAILS

Clone name
wp-clone

Clone namespace
wp-clone


Destination cluster
 ocp-vmw ▾


☐ Clone from an existing snapshot or backup 


CLONING APPLICATIONS

Astra Control can create a clone of your application configuration and persistent storage. Persistent storage backups are transferred from your object store, so choosing a clone from an existing backup will complete the fastest. Enter a clone name to get started.

Read more in [Clone applications](#)

 Application
wp

 Namespace
wp

 Cluster
ocp-vmw

Cancel

Next →

- 新しいアプリケーションは Discovering 状態になり、Astra Control Center は選択したクラスタにアプリケーションを作成します。アプリケーションのすべてのリソースが Astra によってインストールおよび検出されると、アプリケーションは Available 状態になります。

Applications

Actions ▾

+ Define

📦 ▾

🔍 Search

★ 🔍 110 🔍

🔄

1-2 of 2 entries

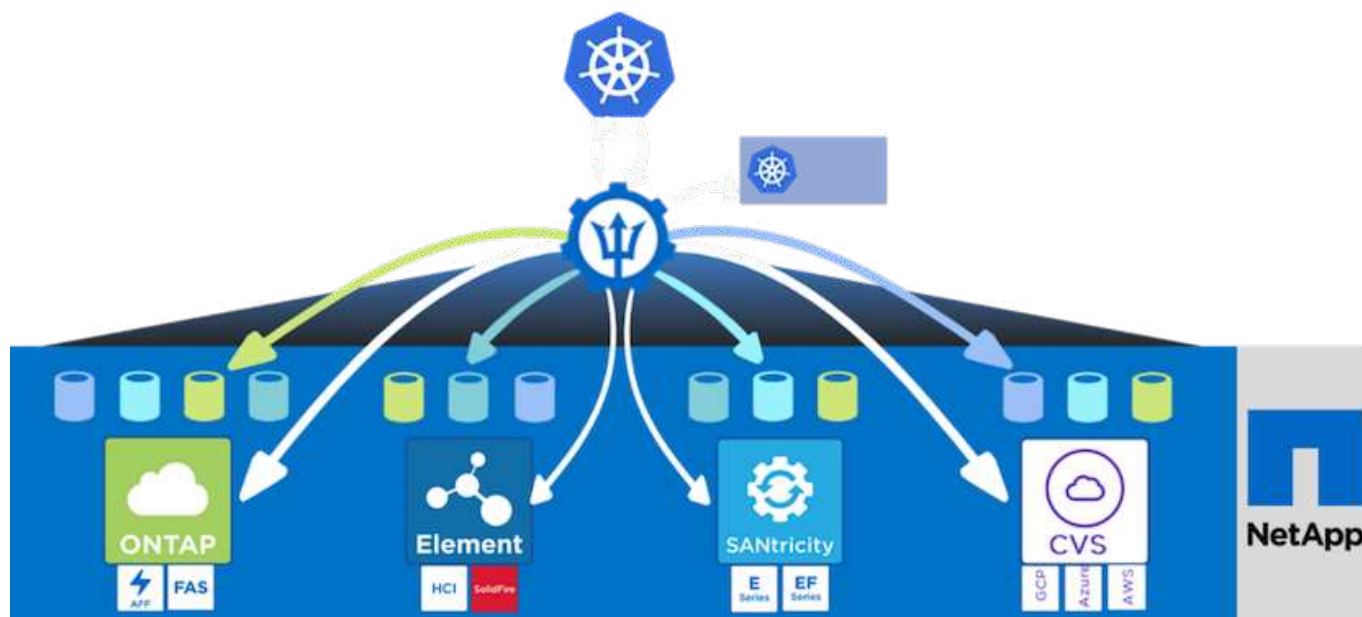
< >

<input type="checkbox"/>	Name ↓	Ready	Protected	Cluster	Group	Discovered	Actions
<input type="checkbox"/>	wp	✓	ℹ️	ocp-vmw	wp	2022/02/28 18:34 UTC	Available ▾
<input type="checkbox"/>	wp-clone	✓	⚠️	ocp-vmw	wp-clone	2022/02/28 19:21 UTC	Available ▾

Astra Trident の概要

Astra Trident は、コンテナや Kubernetes ディストリビューション向けの、Red Hat OpenShift などのオープンソースで完全にサポートされているストレージオーケストレーションツールです。Trident は、NetApp ONTAP や Element ストレージシステムを含むネットアップストレージポートフォリオ全体と連携し、NFS 接続と iSCSI 接続もサポートします。Trident を使用すると、ストレージ管理者の手を煩わせることなく、エンドユーザがネットアップストレージシステムからストレージをプロビジョニングして管理できるため、DevOps ワークフローが高速化されます。

管理者は、プロジェクトのニーズやストレージシステムモデルに基づいて複数のストレージバックエンドを構成し、圧縮、特定のディスクタイプ、QoS レベルなどの高度なストレージ機能を有効にして一定のレベルのパフォーマンスを保証できます。定義されたバックエンドは、プロジェクトの開発者が永続的ボリューム要求（PVC）を作成し、永続的ストレージをオンデマンドでコンテナに接続するために使用できます。



Astra Trident は、Kubernetes と同様、迅速な開発サイクルを 1 年に 4 回リリースしています。

2022 年 1 月にリリースされた最新バージョンの Astra Trident は 22.01 です。Trident のどのバージョンがサポートされているかを確認できます Kubernetes ディストリビューションのテストに使用 ["こちらをご覧ください"](#)。

20.04 リリース以降、Trident のセットアップは Trident オペレータによって実行されます。オペレータが大規模な導入を容易にし、Trident インストールの一部として導入されたポッドの自己修復などの追加サポートを提供します。

21.01 リリースでは、Trident Operator のインストールを容易にするために Helm チャートを使用できるようになりました。

Astra Trident をダウンロード

導入したユースケースに Trident をインストールし、永続ボリュームをプロビジョニングするには、次の手順を実行します。

1. インストールアーカイブを管理ワークステーションにダウンロードし、内容を展開します。Trident の最新バージョンは 22.01 で、ダウンロードできます ["こちらをご覧ください"](#)。

```
[netapp-user@rhel7 ~]$ wget
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
--2021-05-06 15:17:30--
https://github.com/NetApp/trident/releases/download/v22.01.0/trident-
installer-22.01.0.tar.gz
Resolving github.com (github.com)... 140.82.114.3
Connecting to github.com (github.com)|140.82.114.3|:443... connected.
HTTP request sent, awaiting response... 302 Found
Location: https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
Amz-
Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
content-disposition=attachment%3B%20filename%3Dtrident-installer-
22.01.0.tar.gz&response-content-type=application%2Foctet-stream
[following]
--2021-05-06 15:17:30-- https://github-
releases.githubusercontent.com/77179634/a4fa9f00-a9f2-11eb-9053-
98e8e573d4ae?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=AKIAIWNJYAX4CSVEH53A%2F20210506%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20210506T191643Z&X-Amz-Expires=300&X-
Amz-
```



```

Signature=8a49a2a1e08c147d1ddd8149ce45a5714f9853fee19bb1c507989b9543eb36
30&X-Amz-
SignedHeaders=host&actor_id=0&key_id=0&repo_id=77179634&response-
content-disposition=attachment%3B%20filename%3Dtrident-installer-
22.01.0.tar.gz&response-content-type=application%2Foctet-stream
Resolving github-releases.githubusercontent.com (github-
releases.githubusercontent.com)... 185.199.108.154, 185.199.109.154,
185.199.110.154, ...
Connecting to github-releases.githubusercontent.com (github-
releases.githubusercontent.com)|185.199.108.154|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 38349341 (37M) [application/octet-stream]
Saving to: 'trident-installer-22.01.0.tar.gz'

100%[=====
=====>] 38,349,341  88.5MB/s
in 0.4s

2021-05-06 15:17:30 (88.5 MB/s) - 'trident-installer-22.01.0.tar.gz'
saved [38349341/38349341]

```

2. ダウンロードしたバンドルから Trident のインストールを解凍します。

```

[netapp-user@rhel7 ~]$ tar -xzf trident-installer-22.01.0.tar.gz
[netapp-user@rhel7 ~]$ cd trident-installer/
[netapp-user@rhel7 trident-installer]$

```

Helm を使用して **Trident Operator** をインストールします

1. Trident にはこのファイルを渡すオプションがないため、まず、ユーザクラスタの「kubeconfig」ファイルの場所を環境変数として設定します。

```

[netapp-user@rhel7 trident-installer]$ export KUBECONFIG=~/.ocp-
install/auth/kubeconfig

```

2. Helm コマンドを実行し、ユーザクラスタに trident 名前空間を作成しながら、Helball ディレクトリ内の tarball から Trident 演算子をインストールします。

```
[netapp-user@rhel7 trident-installer]$ helm install trident
helm/trident-operator-22.01.0.tgz --create-namespace --namespace trident
NAME: trident
LAST DEPLOYED: Fri May  7 12:54:25 2021
NAMESPACE: trident
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
Thank you for installing trident-operator, which will deploy and manage
NetApp's Trident CSI
storage provisioner for Kubernetes.

Your release is named 'trident' and is installed into the 'trident'
namespace.
Please note that there must be only one instance of Trident (and
trident-operator) in a Kubernetes cluster.

To configure Trident to manage storage resources, you will need a copy
of tridentctl, which is
available in pre-packaged Trident releases. You may find all Trident
releases and source code
online at https://github.com/NetApp/trident.

To learn more about the release, try:

$ helm status trident
$ helm get all trident
```

3. Trident が正しくインストールされていることを確認するには、ネームスペースで実行されているポッドを確認するか、tridentctl バイナリを使用してインストールされているバージョンを確認します。

```
[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
```

NAME	READY	STATUS	RESTARTS	AGE
trident-csi-5z451	1/2	Running	2	30s
trident-csi-696b685cf8-htdb2	6/6	Running	0	30s
trident-csi-b74p2	2/2	Running	0	30s
trident-csi-lrw4n	2/2	Running	0	30s
trident-operator-7c748d957-gr2gw	1/1	Running	0	36s

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident version
```

SERVER VERSION	CLIENT VERSION
22.01.0	22.01.0



場合によっては、お客様の環境で Trident の導入のカスタマイズが必要になることもあります。このような場合は、Trident のオペレータを手動でインストールし、含まれているマニフェストを更新して配置をカスタマイズすることもできます。

Trident Operator を手動でインストールします

1. Trident にはこのファイルを渡すオプションがないため、まず、ユーザクラスタの「kubeconfig」ファイルの場所を環境変数として設定します。

```
[netapp-user@rhel7 trident-installer]$ export KUBECONFIG=~/.ocp-  
install/auth/kubeconfig
```

2. 'trident-installer' ディレクトリには '必要なすべてのリソースを定義するマニフェストが含まれています適切なマニフェストを使用して、「TridentOrchestrator」カスタムリソース定義を作成します。

```
[netapp-user@rhel7 trident-installer]$ oc create -f  
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.yaml  
customresourcedefinition.apiextensions.k8s.io/tridentorchestrators.tride  
nt.netapp.io created
```

3. 存在しない場合は、指定されたマニフェストを使用して、クラスタ内に Trident ネームスペースを作成します。

```
[netapp-user@rhel7 trident-installer]$ oc apply -f deploy/namespace.yaml  
namespace/trident created
```

4. トライデントオペレータの配備に必要なリソースを作成しますたとえば 'オペレータ用のサービスアカウン

ント 'ClusterRole' および 'ClusterRoleBind' を 'ServiceAccount' 専用の 'PodSecurityPolicy' またはオペレータ自体に割り当てます

```
[netapp-user@rhel7 trident-installer]$ oc create -f deploy/bundle.yaml
serviceaccount/trident-operator created
clusterrole.rbac.authorization.k8s.io/trident-operator created
clusterrolebinding.rbac.authorization.k8s.io/trident-operator created
deployment.apps/trident-operator created
podsecuritypolicy.policy/tridentoperatorpods created
```

5. 次のコマンドを使用すると、展開後にオペレータのステータスを確認できます。

```
[netapp-user@rhel7 trident-installer]$ oc get deployment -n trident
NAME                READY    UP-TO-DATE    AVAILABLE    AGE
trident-operator    1/1      1              1             23s
[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                                READY    STATUS    RESTARTS    AGE
trident-operator-66f48895cc-lzczk    1/1      Running    0            41s
```

6. オペレータが導入したら、Trident をインストールできます。これには 'TridentOrchestrator' を作成する必要があります

```
[netapp-user@rhel7 trident-installer]$ oc create -f
deploy/crds/tridentorchestrator_cr.yaml
tridentorchestrator.trident.netapp.io/trident created
[netapp-user@rhel7 trident-installer]$ oc describe torc trident
Name:                trident
Namespace:
Labels:               <none>
Annotations:          <none>
API Version:          trident.netapp.io/v1
Kind:                 TridentOrchestrator
Metadata:
  Creation Timestamp:  2021-05-07T17:00:28Z
  Generation:          1
  Managed Fields:
    API Version:        trident.netapp.io/v1
    Fields Type:         FieldsV1
    fieldsV1:
      f:spec:
        .:
        f:debug:
        f:namespace:
  Manager:              kubect1-create
```

```

Operation:      Update
Time:           2021-05-07T17:00:28Z
API Version:    trident.netapp.io/v1
Fields Type:    FieldsV1
fieldsV1:
  f:status:
    .:
  f:currentInstallationParams:
    .:
    f:IPv6:
    f:autosupportHostname:
    f:autosupportimage:
    f:autosupportProxy:
    f:autosupportSerialNumber:
    f:debug:
    f:enableNodePrep:
    f:imagePullSecrets:
    f:imageRegistry:
    f:k8sTimeout:
    f:kubeletDir:
    f:logFormat:
    f:silenceAutosupport:
    f:tridentimage:
  f:message:
  f:namespace:
  f:status:
  f:version:
Manager:        trident-operator
Operation:      Update
Time:           2021-05-07T17:00:28Z
Resource Version: 931421
Self Link:
/apis/trident.netapp.io/v1/tridentorchestrators/trident
UID:            8a26a7a6-dde8-4d55-9b66-a7126754d81f
Spec:
  Debug:        true
  Namespace:    trident
Status:
  Current Installation Params:
    IPv6:                false
    Autosupport Hostname:
    Autosupport image:    netapp/trident-autosupport:21.01
    Autosupport Proxy:
    Autosupport Serial Number:
    Debug:                true
    Enable Node Prep:     false

```

```

Image Pull Secrets:
Image Registry:
k8sTimeout:          30
Kubelet Dir:          /var/lib/kubelet
Log Format:           text
Silence Autosupport:  false
Trident image:       netapp/trident:22.01.0
Message:             Trident installed
Namespace:           trident
Status:              Installed
Version:             v22.01.0
Events:
  Type    Reason          Age   From                      Message
  ----    -
  Normal  Installing      80s   trident-operator.netapp.io Installing
  Trident
  Normal  Installed       68s   trident-operator.netapp.io Trident
  installed

```

7. Trident が正しくインストールされていることを確認するには、ネームスペースで実行されているポッドを確認するか、tridentctl バイナリを使用してインストールされているバージョンを確認します。

```

[netapp-user@rhel7 trident-installer]$ oc get pods -n trident
NAME                                READY   STATUS    RESTARTS   AGE
trident-csi-bb64c6cb4-lmd6h        6/6     Running   0           82s
trident-csi-gn59q                   2/2     Running   0           82s
trident-csi-m4szj                   2/2     Running   0           82s
trident-csi-sb9k9                   2/2     Running   0           82s
trident-operator-66f48895cc-lzczk   1/1     Running   0           2m39s

[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident version
+-----+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+-----+
| 22.01.0       | 22.01.0       |
+-----+-----+

```

ワーカーノードをストレージ用に準備する

NFS

ほとんどの Kubernetes ディストリビューションには、Red Hat OpenShift など、デフォルトでインストールされる NFS バックエンドをマウントするパッケージとユーティリティが付属しています。

ただし NFSv3 については、クライアントとサーバ間の同時処理をネゴシエートするメカニズムはありません。したがって 'サーバが接続のウィンドウ・サイズを小さくしなくても NFS 接続の最適なパフォーマンス

を確保できるように 'クライアント側 sunrpc スロット・テーブル・エントリーの最大数は' サーバ上でサポートされている値と手動で同期する必要があります

ONTAP でサポートされる sunrpcslot table エントリーの最大数は 128 です。つまり、ONTAP は、一度に 128 個の NFS 要求を同時に処理できます。ただし、Red Hat CoreOS / Red Hat Enterprise Linux では、接続ごとに最大 65、536 の sunrpc スロットテーブルエントリがデフォルトでサポートされます。この値を 128 に設定する必要があります。これは OpenShift のマシン構成オペレータ (MCO) を使用して実行できます。

OpenShift ワーカーノードで最大 sunrpc スロットテーブルエントリを変更するには、次の手順を実行します。

1. OCP Web コンソールにログインし、[計算]>[マシン構成] に移動します。[マシン構成の作成] をクリックします。YAML ファイルをコピーして貼り付け、[作成] をクリックします。

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  name: 98-worker-nfs-rpc-slot-tables
  labels:
    machineconfiguration.openshift.io/role: worker
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
        - contents:
            source: data:text/plain;charset=utf-8;base64,b3B0aW9ucyBzdW5ycGMgdGNwX21heF9zbG90X3RhYmxlX2VudHJpZXM9MTI4Cg==
            filesystem: root
            mode: 420
            path: /etc/modprobe.d/sunrpc.conf
```

2. MCO が作成されたら、すべてのワーカーノードに設定を適用し、1 つずつ再起動する必要があります。プロセス全体には約 20~30 分かかります。「OC GET MCP」を使用してマシン構成が適用されているかどうかを確認し、ワーカーのマシン構成プールが更新されていることを確認します。

```
[netapp-user@rhel7 openshift-deploy]$ oc get mcp
```

NAME	CONFIG	UPDATED	UPDATING
DEGRADED			
master	rendered-master-a520ae930e1d135e0dee7168	True	False
False			
worker	rendered-worker-de321b36eeba62df41feb7bc	True	False
False			

iSCSI

iSCSI プロトコルによるブロックストレージボリュームのマッピングを許可するようにワーカーノードを準備するには、その機能をサポートするために必要なパッケージをインストールする必要があります。

Red Hat OpenShift では、MCO（マシン構成オペレータ）を展開後にクラスタに適用することによって処理されます。

ワーカーノードで iSCSI サービスを実行するように設定するには、次の手順を実行します。

1. OCP Web コンソールにログインし、[計算] > [マシン構成] に移動します。[マシン構成の作成] をクリックします。YAML ファイルをコピーして貼り付け、[作成] をクリックします。

マルチパスを使用しない場合：

```
apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  labels:
    machineconfiguration.openshift.io/role: worker
  name: 99-worker-element-iscsi
spec:
  config:
    ignition:
      version: 3.2.0
    systemd:
      units:
        - name: iscsid.service
          enabled: true
          state: started
  osImageURL: ""
```

マルチパスを使用する場合：

```

apiVersion: machineconfiguration.openshift.io/v1
kind: MachineConfig
metadata:
  name: 99-worker-ontap-iscsi
  labels:
    machineconfiguration.openshift.io/role: worker
spec:
  config:
    ignition:
      version: 3.2.0
    storage:
      files:
      - contents:
          source: data:text/plain;charset=utf-8;base64,ZGVmYXVsdHMgewogICAgICAgIHVzZXJfZnJpZW5kbHlfbmFtZXMgYm8KICAgICAgICBmaW5kX211bHRpcGF0aHMGbm8KfQoKYmxhY2tsaXN0X2V4Y2VwdGlvbnMGewogICAgICAgIHByb3BlcnR5ICIoU0NTSV9JREVOVF98SURfV1dOKSfQoKYmxhY2tsaXN0IHsKfQoK
          verification: {}
        filesystem: root
        mode: 400
        path: /etc/multipath.conf
    systemd:
      units:
      - name: iscsid.service
        enabled: true
        state: started
      - name: multipathd.service
        enabled: true
        state: started
  osImageURL: ""

```

2. 構成の作成後、約 20~30 分で設定がワーカーノードに適用され、再ロードされます。「OC GET MCP」を使用してマシン構成が適用されているかどうかを確認し、ワーカーのマシン構成プールが更新されていることを確認します。ワーカーノードにログインして、iscsid サービスが実行されている（マルチパスを使用している場合、multipathd サービスが実行されている）ことを確認することもできます。

```
[netapp-user@rhel7 openshift-deploy]$ oc get mcp
NAME          CONFIG                                UPDATED    UPDATING
DEGRADED
master        rendered-master-a520ae930e1d135e0dee7168    True       False
False
worker        rendered-worker-de321b36eeba62df41feb7bc    True       False
False

[netapp-user@rhel7 openshift-deploy]$ ssh core@10.61.181.22 sudo
systemctl status iscsid
● iscsid.service - Open-iSCSI
   Loaded: loaded (/usr/lib/systemd/system/iscsid.service; enabled;
   vendor preset: disabled)
   Active: active (running) since Tue 2021-05-26 13:36:22 UTC; 3 min ago
     Docs: man:iscsid(8)
           man:iscsiadm(8)
  Main PID: 1242 (iscsid)
    Status: "Ready to process requests"
     Tasks: 1
  Memory: 4.9M
     CPU: 9ms
   CGroup: /system.slice/iscsid.service
           └─1242 /usr/sbin/iscsid -f

[netapp-user@rhel7 openshift-deploy]$ ssh core@10.61.181.22 sudo
systemctl status multipathd
● multipathd.service - Device-Mapper Multipath Device Controller
   Loaded: loaded (/usr/lib/systemd/system/multipathd.service; enabled;
   vendor preset: enabled)
   Active: active (running) since Tue 2021-05-26 13:36:22 UTC; 3 min ago
  Main PID: 918 (multipathd)
    Status: "up"
     Tasks: 7
  Memory: 13.7M
     CPU: 57ms
   CGroup: /system.slice/multipathd.service
           └─918 /sbin/multipathd -d -s
```



また、適切なフラグを指定して「OC debug」コマンドを実行することにより、MachineConfig が正常に適用され、サービスが正常に開始されたことを確認することもできます。

ストレージシステムバックエンドを作成

Astra Trident Operator のインストールが完了したら、使用するネットアップストレージプラットフォームに

合わせてバックエンドを設定する必要があります。Astra Trident のセットアップと設定を続行するには、次のリンクを参照してください。

- ["NetApp ONTAP NFS"](#)
- ["NetApp ONTAP iSCSI の略"](#)
- ["NetApp Element iSCSI の略"](#)

NetApp ONTAP の NFS 構成

Trident を NetApp ONTAP ストレージシステムと統合するには、ストレージシステムとの通信を可能にするバックエンドを作成する必要があります。

1. ダウンロードしたインストールアーカイブのサンプルバックエンドファイルは、「sample-input」フォルダ階層にあります。NFS を提供している NetApp ONTAP システムの場合は、「backend-ontap/nas.json」ファイルを作業ディレクトリにコピーし、ファイルを編集します。

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-samples/ontap-nas/backend-ontap-nas.json ./
[netapp-user@rhel7 trident-installer]$ vi backend-ontap-nas.json
```

2. backendName、managementLIF、dataLIF、SVM、ユーザ名を編集します。パスワードの値を入力します。

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap-nas+10.61.181.221",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.221",
  "svm": "trident_svm",
  "username": "cluster-admin",
  "password": "password"
}
```



カスタムの backendName 値は、簡単に識別できるように NFS を提供するストレージ DriverName とデータ LIF を組み合わせて定義することを推奨します。

3. このバックエンドファイルを設定した状態で、次のコマンドを実行して最初のバックエンドを作成します。

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-nas.json
```

NAME	STATE	VOLUMES	STORAGE DRIVER	UUID
ontap-nas+10.61.181.221	online	0	ontap-nas	be7a619d-c81d-445c-b80c-5c87a73c5b1e

4. バックエンドを作成したら、次にストレージクラスを作成する必要があります。バックエンドと同様に、sample_inputs フォルダにある環境用に編集可能なサンプルのストレージクラスファイルがあります。作業ディレクトリにコピーし、作成したバックエンドを反映するために必要な編集を行います。

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

5. このファイルに対して行う必要がある唯一の編集は 'バックエンドタイプの値を '新しく作成されたバックエンドのストレージドライバの名前に定義することですまた、名前フィールドの値もメモしておきます。この値は、以降の手順で参照する必要があります。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
```



このファイルに定義されているオプションのフィールド「fsType」があります。この行は NFS バックエンドで削除できます。

6. oc コマンドを実行して 'ストレージ・クラスを作成します

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-
basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

7. ストレージクラスを作成したら、最初の永続的ボリューム要求（PVC）を作成する必要があります。sample_inputs にもあるこのアクションを実行するために使用できるサンプルの 'pvc-basicy.yaml' ファイルがあります

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

8. このファイルに対して行う必要がある唯一の編集は 'storageClassName' フィールドが作成したものと同じであることを確認することですプロビジョニングするワークロードによって必要に応じて、PVC 定義をさらにカスタマイズできます。

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

9. 「OC」コマンドを発行して、PVC を作成します。作成中の元のボリュームのサイズによっては作成にしばらく時間がかかることがあるため、作成が完了した時点でこのプロセスを監視できます。

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME      STATUS    VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS  AGE
basic      Bound       pvc-b4370d37-0fa4-4c17-bd86-94f96c94b42d  1Gi
RWO                                     basic-csi      7s
```

NetApp ONTAP iSCSI 構成

Trident を NetApp ONTAP ストレージシステムと統合するには、ストレージシステムとの通信を可能にするバックエンドを作成する必要があります。

1. ダウンロードしたインストールアーカイブのサンプルバックエンドファイルは、「sample-input」フォルダ階層にあります。iSCSI を提供している NetApp ONTAP システムの場合は、「backend-ontap-san.json」ファイルを作業ディレクトリにコピーし、ファイルを編集します。

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-
samples/ontap-san/backend-ontap-san.json ./
[netapp-user@rhel7 trident-installer]$ vi backend-ontap-san.json
```

2. このファイルで管理 LIF、データ LIF、SVM、ユーザ名、パスワードの値を編集します。

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.240",
  "svm": "trident_svm",
  "username": "admin",
  "password": "password"
}
```

3. このバックエンドファイルを設定した状態で、次のコマンドを実行して最初のバックエンドを作成します。

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-san.json
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE | VOLUMES | |          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontapsan_10.61.181.241 | ontap-san      | 6788533c-7fea-4a35-b797-
fb9bb3322b91 | online |      0 |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

4. バックエンドを作成したら、次にストレージクラスを作成する必要があります。バックエンドと同様に、sample_inputs フォルダにある環境用に編集可能なサンプルのストレージクラスファイルがあります。作業ディレクトリにコピーし、作成したバックエンドを反映するために必要な編集を行います。

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-
samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

5. このファイルに対して行う必要がある唯一の編集は 'バックエンドタイプの値を '新しく作成されたバックエンドのストレージドライバの名前に定義することですまた、名前フィールドの値もメモしておきます。この値は、以降の手順で参照する必要があります。


```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"

```



このファイルに定義されているオプションのフィールド「fsType」があります。iSCSI バックエンドでは、この値を特定の Linux ファイルシステムタイプ（XFS、ext4 など）に設定することも、OpenShift が使用するファイルシステムを決定できるようにするために削除することもできます。

6. oc コマンドを実行して 'ストレージ・クラス' を作成します

```

[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-basic.yaml
storageclass.storage.k8s.io/basic-csi created

```

7. ストレージクラスを作成したら、最初の永続的ボリューム要求（PVC）を作成する必要があります。sample_inputs にもあるこのアクションを実行するために使用できるサンプルの 'pvc-basicy.yaml' ファイルがあります

```

[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml

```

8. このファイルに対して行う必要がある唯一の編集は 'storageClassName' フィールドが作成したものと同じであることを確認することですプロビジョニングするワークロードによって必要に応じて、PVC 定義をさらにカスタマイズできます。

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi

```

9. 「OC」コマンドを発行して、PVCを作成します。作成中の元のボリュームのサイズによっては作成にしばらく時間がかかることがあるため、作成が完了した時点でこのプロセスを監視できます。

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME      STATUS    VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS  AGE
basic       Bound       pvc-7ceac1ba-0189-43c7-8f98-094719f7956c  1Gi
RWO                               basic-csi          3s
```

NetApp Element iSCSI 構成

Trident を NetApp Element ストレージシステムと統合するには、iSCSI プロトコルを使用してストレージシステムと通信できるバックエンドを作成する必要があります。

1. ダウンロードしたインストールアーカイブのサンプルバックエンドファイルは、「sample-input」フォルダ階層にあります。iSCSI を提供している NetApp Element システムの場合、「backend-solidfire.json」ファイルを作業ディレクトリにコピーし、ファイルを編集します。

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/backends-
samples/solidfire/backend-solidfire.json ./
[netapp-user@rhel7 trident-installer]$ vi ./backend-solidfire.json
```

- a. エンドポイント行のユーザ、パスワード、および MVIP 値を編集します。
- b. 「仮想 IP」の値を編集します。

```
{
  "version": 1,
  "storageDriverName": "solidfire-san",
  "Endpoint": "https://trident:password@172.21.224.150/json-
rpc/8.0",
  "SVIP": "10.61.180.200:3260",
  "TenantName": "trident",
  "Types": [{"Type": "Bronze", "Qos": {"minIOPS": 1000, "maxIOPS":
2000, "burstIOPS": 4000}},
            {"Type": "Silver", "Qos": {"minIOPS": 4000, "maxIOPS":
6000, "burstIOPS": 8000}},
            {"Type": "Gold", "Qos": {"minIOPS": 6000, "maxIOPS":
8000, "burstIOPS": 10000}}]
}
```

2. このバックエンドファイルを設定したら、次のコマンドを実行して最初のバックエンドを作成します。

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-solidfire.json
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE | VOLUMES |          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| solidfire_10.61.180.200 | solidfire-san  | b90783ee-e0c9-49af-8d26-3ea87ce2efdf |
| online |          0 |          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

3. バックエンドを作成したら、次にストレージクラスを作成する必要があります。バックエンドと同様に、sample_inputs フォルダにある環境用に編集可能なサンプルのストレージクラスファイルがあります。作業ディレクトリにコピーし、作成したバックエンドを反映するために必要な編集を行います。

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/storage-class-samples/storage-class-csi.yaml.templ ./storage-class-basic.yaml
[netapp-user@rhel7 trident-installer]$ vi storage-class-basic.yaml
```

4. このファイルに対して行う必要がある唯一の編集は 'バックエンドタイプの値を '新しく作成されたバックエンドのストレージドライバの名前に定義することですまた、名前フィールドの値もメモしておきます。この値は、以降の手順で参照する必要があります。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: basic-csi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "solidfire-san"
```



このファイルに定義されているオプションのフィールド「fsType」があります。iSCSI バックエンドでは、この値を特定の Linux ファイルシステムタイプ（XFS、ext4 など）に設定するか、OpenShift で使用するファイルシステムを決定できるようにするためにこの値を削除できます。

5. oc コマンドを実行して 'ストレージ・クラスを作成します

```
[netapp-user@rhel7 trident-installer]$ oc create -f storage-class-basic.yaml
storageclass.storage.k8s.io/basic-csi created
```

6. ストレージクラスを作成したら、最初の永続的ボリューム要求（PVC）を作成する必要があります。sample_inputs にもあるこのアクションを実行するために使用できるサンプルの 'pvc-basic.yaml' ファイルがあります

```
[netapp-user@rhel7 trident-installer]$ cp sample-input/pvc-samples/pvc-basic.yaml ./
[netapp-user@rhel7 trident-installer]$ vi pvc-basic.yaml
```

7. このファイルに対して行う必要がある唯一の編集は 'storageClassName' フィールドが作成したものと同じであることを確認することです。プロビジョニングするワークロードによって必要に応じて、PVC 定義をさらにカスタマイズできます。

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: basic-csi
```

8. 「OC」コマンドを発行して、PVC を作成します。作成中の元のボリュームのサイズによっては作成にしばらく時間がかかることがあるため、作成が完了した時点でこのプロセスを監視できます。

```
[netapp-user@rhel7 trident-installer]$ oc create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ oc get pvc
NAME      STATUS    VOLUME                                     CAPACITY
ACCESS MODES  STORAGECLASS  AGE
basic      Bound       pvc-3445b5cc-df24-453d-a1e6-b484e874349d  1Gi
RWO          basic-csi     5s
```

Advanced Configuration Options（詳細設定オプション）

ロードバランサのオプションの確認：ネットアップを使用した **Red Hat OpenShift**

ほとんどの場合、Red Hat OpenShift は、ルートを介してアプリケーションを外部で利用できるようにします。サービスは、外部からアクセス可能なホスト名を付与することで公開されます。定義されたルートおよびサービスによって識別されるエンドポイントは、OpenShift ルータによって使用され、外部クライアントにこの名前付き接続を提供できます。

ただし、アプリケーションでは、適切なサービスを公開するために、カスタマイズしたロードバランサの導入と設定が必要になる場合があります。その一例が、ネットアップアストラコントロールセンターです。このニーズを満たすために、いくつかのカスタムロードバランサオプションを評価しました。このセクションでは、これらのインストールと設定について説明します。

以下のページでは、解決策追加情報を搭載した Red Hat OpenShift で検証済みのロードバランサオプションについて説明します。

- ["MetalLB"](#)
- ["F5 BIG-IP"](#)

MetalLB ロードバランサのインストール：ネットアップでの **Red Hat OpenShift**

このページでは、MetalLB ロードバランサのインストールおよび設定手順を示します。

MetalLB は、OpenShift クラスタにインストールされた自己ホスト型ネットワークロードバランサであり、クラウドプロバイダで実行されないクラスタでタイプロードバランサの OpenShift サービスを作成できます。LoadBalancer サービスをサポートするために連携する MetalLB の 2 つの主な機能は、アドレス割り当てと外部アナウンスメントです。

MetalLB 設定オプション

MetalLB が OpenShift クラスタの外部でロードバランササービスに割り当てられた IP アドレスをどのようにアナウンスするかに基づいて、次の 2 つのモードで動作します。

- **レイヤ 2 モード。** * このモードでは、OpenShift クラスタ内の 1 つのノードがサービスの所有権を取得し、その IP の ARP 要求に応答して、OpenShift クラスタ外で到達可能にします。IP をアドバタイズするのはノードだけなので、帯域幅のボトルネックと低速フェールオーバーの制限があります。詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。
- * このモードでは、OpenShift クラスタ内のすべてのノードがルータとの BGP ピアリングセッションを確立し、トラフィックをサービス IP に転送するためにルータをアドバタイズします。このための前提条件は、MetalLB をそのネットワーク内のルータと統合することです。BGP のハッシュメカニズムにより、サービスの IP-to-Node マッピングが変更されることがあります。詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。



このマニュアルでは、レイヤ 2 モードで MetalLB を設定します。

MetalLB ロードバランサをインストールします

1. MetalLB リソースをダウンロードします。

```
[netapp-user@rhel7 ~]$ wget
https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/namespace.yaml
[netapp-user@rhel7 ~]$ wget
https://raw.githubusercontent.com/metallb/metallb/v0.10.2/manifests/metallb.yaml
```

2. ファイル「metallb.yaml」を編集し、「pec.template.spec.securityContext」をコントローラ展開とスピーカー DemonSet から削除します。

◦ 削除する行数： *

```
securityContext:
  runAsNonRoot: true
  runAsUser: 65534
```

3. 「metallb-system」ネームスペースを作成します。

```
[netapp-user@rhel7 ~]$ oc create -f namespace.yaml
namespace/metallb-system created
```

4. MetalLB CR を作成します。

```
[netapp-user@rhel7 ~]$ oc create -f metallb.yaml
podsecuritypolicy.policy/controller created
podsecuritypolicy.policy/speaker created
serviceaccount/controller created
serviceaccount/speaker created
clusterrole.rbac.authorization.k8s.io/metallb-system:controller created
clusterrole.rbac.authorization.k8s.io/metallb-system:speaker created
role.rbac.authorization.k8s.io/config-watcher created
role.rbac.authorization.k8s.io/pod-lister created
role.rbac.authorization.k8s.io/controller created
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:controller
created
clusterrolebinding.rbac.authorization.k8s.io/metallb-system:speaker
created
rolebinding.rbac.authorization.k8s.io/config-watcher created
rolebinding.rbac.authorization.k8s.io/pod-lister created
rolebinding.rbac.authorization.k8s.io/controller created
daemonset.apps/speaker created
deployment.apps/controller created
```

5. MetalLB スピーカを設定する前に、スピーカ DemonSet の昇格特権を与えて、ロードバランサを動作させるために必要なネットワーク設定を実行できるようにします。

```
[netapp-user@rhel7 ~]$ oc adm policy add-scc-to-user privileged -n metallb-system -z speaker
clusterrole.rbac.authorization.k8s.io/system:openshift:scc:privileged
added: "speaker"
```

6. 「metallb - システム」ネームスペースに「ConfigMap」を作成して、MetalLB を設定します。

```
[netapp-user@rhel7 ~]$ vim metallb-config.yaml

apiVersion: v1
kind: ConfigMap
metadata:
  namespace: metallb-system
  name: config
data:
  config: |
    address-pools:
    - name: default
      protocol: layer2
      addresses:
      - 10.63.17.10-10.63.17.200

[netapp-user@rhel7 ~]$ oc create -f metallb-config.yaml
configmap/config created
```

7. これで、ロードバランササービスが作成されると、MetalLB は外部 IP をサービスに割り当て、ARP 要求に応答して IP アドレスをアドバタイズします。



BGP モードで MetalLB を設定する場合は、上記の手順 6 を省略し、MetalLB マニュアルの手順に従います ["こちらをご覧ください"](#)。

F5 BIG-IP ロードバランサのインストール

F5 BIG-IP は、L4-L7 ロードバランシング、SSL/TLS オフロード、DNS、ファイアウォールなど、高度な運用レベルのトラフィック管理およびセキュリティサービスを幅広く提供する Application Delivery Controller（ADC; アプリケーションデリバリーコントローラ）です。これらのサービスにより、アプリケーションの可用性、セキュリティ、パフォーマンスが大幅に向上します。

F5 BIG-IP は、専用ハードウェア、クラウド、またはオンプレミスの仮想アプライアンスに、さまざまな方法で導入、使用できます。要件に応じて F5 BIG-IP を調査し、導入するには、ここで説明しているドキュメントを参照してください。

F5 BIG-IP サービスを Red Hat OpenShift と効率的に統合するために、F5 は BIG-IP Container Ingress Service (CIS) を提供します。CI は、特定のカスタムリソース定義 (CRD) の OpenShift API を監視し、F5 BIG-IP システム構成を管理するコントローラポッドとしてインストールされます。F5 BIG-IP CIS は、OpenShift でサービスタイプ Loadancers とルートを制御するように構成できます。

さらに、タイプ LoadBalancer にサービスを提供するための自動 IP アドレス割り当てには、F5 IPAM コントローラを使用できます。F5 IPAM コントローラは、LoadBalancer サービスの OpenShift API を ipamLabel 注釈で監視し、事前構成済みプールから IP アドレスを割り当てるコントローラポッドとしてインストールされます。

このページには、F5 BIG-IP CIS および IPAM コントローラのインストールおよび設定手順がリストされています。前提条件として、F5 BIG-IP システムを導入し、ライセンスを取得しておく必要があります。また、デフォルトでは BIG-IP VE 基本ライセンスに含まれている SDN サービスのライセンスも必要です。



F5 BIG-IP は、スタンドアロンモードまたはクラスタモードで導入できます。この検証の目的上、F5 BIG-IP はスタンドアロンモードで導入されましたが、本番環境では、単一点障害を避けるために、大量の IP で構成されたクラスタを使用することを推奨します。



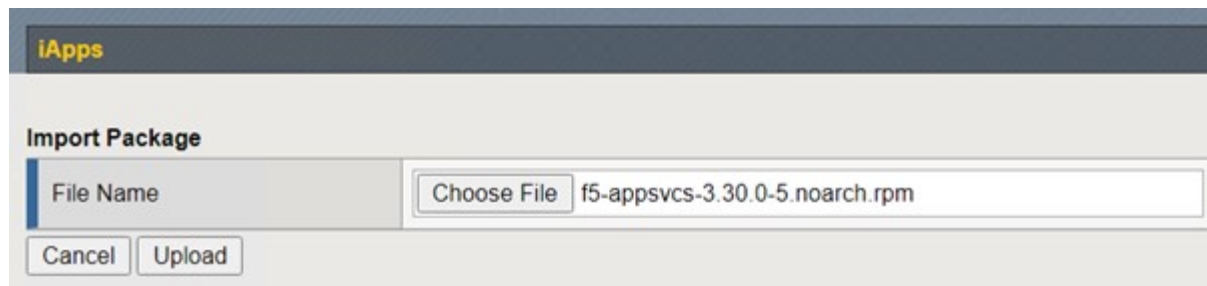
F5 BIG-IP システムは、専用のハードウェア、クラウド、またはオンプレミスの仮想アプライアンスとして、バージョンが 12.x よりも大きいオンプレミスに導入でき、F5 CIS と統合できます。このドキュメントでは、BIG-IP VE エディションなどを使用して、F5 BIG-IP システムを仮想アプライアンスとして検証しました。

検証済みのリリース

テクノロジー	ソフトウェアのバージョン
Red Hat OpenShift のサービスです	4.6 EUS 、 4.7
F5 BIG-IP VE エディション	16.1.0
F5 Container Ingress Service の略	2.5.1
F5 IPAM コントローラ	0.1.4
F5 AS3	3.30.0

インストール

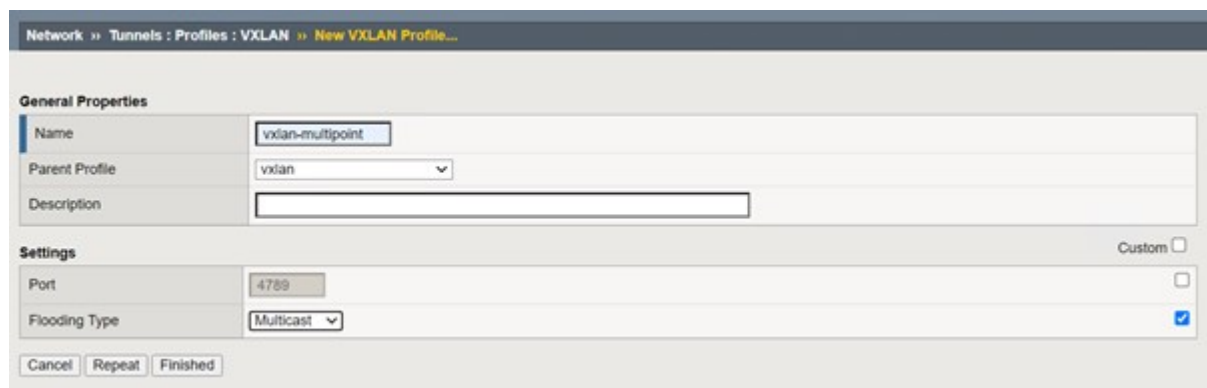
1. F5 Application Services 3 拡張機能をインストールして、big-IP システムが命令コマンドではなく JSON で構成を受け入れるようにします。に進みます ["F5 AS3 GitHub リポジトリ"](#) をクリックし、最新の RPM ファイルをダウンロードします。
2. F5 BIG-IP システムにログインし、iApps > Package Management LX に移動して、Import (インポート) をクリックします。
3. [ファイルの選択] をクリックして、ダウンロードした AS3 RPM ファイルを選択し、[OK] をクリックして、[アップロード] をクリックします。



4. AS3 拡張機能が正常にインストールされたことを確認します。



5. 次に、OpenShift システムと BIG-IP システム間の通信に必要なリソースを構成します。まず、OpenShift SDN のための BIG-IP システムに VXLAN トンネルインターフェイスを作成し、OpenShift と BIG-IP サーバ間にトンネルを作成します。Network > Tunnels > Profiles と進み、Create をクリックして Parent Profile を VXLAN に設定し、フラッディング Type を Multicast に設定します。プロファイルの名前を入力し、[完了] をクリックします。



6. Network > Tunnels > Tunnel List と進み、Create をクリックして、トンネルの名前とローカル IP アドレスを入力します。前の手順で作成したトンネルプロファイルを選択し、[完了] をクリックします。

Network » Tunnels : Tunnel List » New Tunnel...

Configuration	
Name	openshift_vxlan
Description	
Key	0
Profile	vxlan-multipoint ▼
Local Address	10.63.172.239
Secondary Address	Any ▼
Remote Address	Any ▼
Mode	Bidirectional ▼
MTU	0
Use PMTU	<input checked="" type="checkbox"/> Enabled
TOS	Preserve ▼
Auto-Last Hop	Default ▼
Traffic Group	None ▼

Cancel Repeat Finished

7. クラスタ管理者権限で Red Hat OpenShift クラスタにログインします。
8. F5 BIG-IP サーバの OpenShift にホストサブネットを作成します。このサブネットは、OpenShift クラスタから F5 BIG-IP サーバに拡張します。ホストサブネット YAML 定義をダウンロードします。

```
wget https://github.com/F5Networks/k8s-bigip-ctlr/blob/master/docs/config_examples/openshift/f5-kctlr-openshift-hostsubnet.yaml
```

9. ホストサブネットファイルを編集し、OpenShift SDN の BIG-IP VTEP （VXLAN トンネル） IP を追加します。

```
apiVersion: v1
kind: HostSubnet
metadata:
  name: f5-server
  annotations:
    pod.network.openshift.io/fixed-vnid-host: "0"
    pod.network.openshift.io/assign-subnet: "true"
# provide a name for the node that will serve as BIG-IP's entry into the
cluster
host: f5-server
# The hostIP address will be the BIG-IP interface address routable to
the
# OpenShift Origin nodes.
# This address is the BIG-IP VTEP in the SDN's VXLAN.
hostIP: 10.63.172.239
```



ご使用の環境に応じて、hostIP などの詳細情報を変更します。

10. HostSubnet リソースを作成します。

```
[admin@rhel-7 ~]$ oc create -f f5-kctlr-openshift-hostsubnet.yaml

hostsubnet.network.openshift.io/f5-server created
```

11. F5 BIG-IP サーバ用に作成されたホストサブネットのクラスタ IP サブネット範囲を取得します。

```
[admin@rhel-7 ~]$ oc get hostssubnet
```

NAME	HOST	HOST IP
SUBNET	EGRESS CIDRS	EGRESS IPS
f5-server	f5-server	10.63.172.239
10.131.0.0/23		
ocp-vmw-nszws-master-0	ocp-vmw-nszws-master-0	10.63.172.44
10.128.0.0/23		
ocp-vmw-nszws-master-1	ocp-vmw-nszws-master-1	10.63.172.47
10.130.0.0/23		
ocp-vmw-nszws-master-2	ocp-vmw-nszws-master-2	10.63.172.48
10.129.0.0/23		
ocp-vmw-nszws-worker-r8fh4	ocp-vmw-nszws-worker-r8fh4	10.63.172.7
10.130.2.0/23		
ocp-vmw-nszws-worker-tvr46	ocp-vmw-nszws-worker-tvr46	10.63.172.11
10.129.2.0/23		
ocp-vmw-nszws-worker-wdxhg	ocp-vmw-nszws-worker-wdxhg	10.63.172.24
10.128.2.0/23		
ocp-vmw-nszws-worker-wg8r4	ocp-vmw-nszws-worker-wg8r4	10.63.172.15
10.131.2.0/23		
ocp-vmw-nszws-worker-wtgfw	ocp-vmw-nszws-worker-wtgfw	10.63.172.17
10.128.4.0/23		

12. F5 BIG-IP サーバに対応する OpenShift のホストサブネット範囲の IP を使用して、VXLAN OpenShift 上に自己 IP を作成します。F5 BIG-IP システムにログインし、[ネットワーク]>[自己 IP] の順に選択し、[作成] をクリックします。F5 BIG-IP ホストサブネット用に作成されたクラスタ IP サブネットから IP を入力し、VXLAN トンネルを選択して、その他の詳細を入力します。[完了] をクリックします。

Network » Self IPs » New Self IP...

Configuration

Name	10.131.0.60
IP Address	10.131.0.60
Netmask	255.252.0.0
VLAN / Tunnel	openshift_vxla ▾
Port Lockdown	Allow All ▾
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating) ▾
Service Policy	None ▾

Cancel Repeat Finished

13. CIS で設定および使用する F5 BIG-IP システムにパーティションを作成します。[システム]>[ユーザ]>[パーティションリスト] の順に選択し、[作成] をクリックして詳細を入力します。[完了] をクリックします。

System » Users : Partition List » New Partition...

Properties

Partition Name	<input type="text" value="ocp-vmw"/>
Partition Default Route Domain	<input type="text" value="0"/>
Description	<div></div> <div><input type="checkbox"/> Extend Text Area <input type="checkbox"/> Wrap Text</div>

Redundant Device Configuration

Device Group	<input checked="" type="checkbox"/> Inherit device group from root folder <input type="text" value="None"/>
Traffic Group	<input checked="" type="checkbox"/> Inherit traffic group from root folder <input type="text" value="traffic-group-1 (floating)"/>



CIS で管理されるパーティションでは手動で設定しないことをお勧めします。

14. OperatorHub のオペレータを使用して F5 BIG-IP CIS をインストールします。cluster-admin 権限を持つ Red Hat OpenShift クラスタにログインし、F5 BIG-IP システムログインクレデンシャルを使用してシークレットを作成します。これはオペレータの前提条件です。

```
[admin@rhel-7 ~]$ oc create secret generic bigip-login -n kube-system
--from-literal=username=admin --from-literal=password=admin

secret/bigip-login created
```

15. F5 CIS CRD をインストールします。

```
[admin@rhel-7 ~]$ oc apply -f
https://raw.githubusercontent.com/F5Networks/k8s-bigip-
ctrlr/master/docs/config_examples/crd/Install/customresourcedefinitions.y
ml

customresourcedefinition.apiextensions.k8s.io/virtualservers.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/tlsprofiles.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/transportservers.cis.f5.co
m created
customresourcedefinition.apiextensions.k8s.io/externaldnss.cis.f5.com
created
customresourcedefinition.apiextensions.k8s.io/ingresslinks.cis.f5.com
created
```


16. [演算子]>[演算子ハブ] に移動し、キーワード F5 を検索して、F5 Container Ingress Service タイルをクリックします。

OperatorHub

Discover Operators from the Kubernetes community and Red Hat partners, curated by Red Hat. You can purchase commercial software through [Red Hat Marketplace](#). You can install Operators on your clusters to provide optional add-ons and shared services to your developers. After installation, the Operator capabilities will appear in the [Developer Catalog](#) providing a self-service experience.

The screenshot shows the OperatorHub interface. On the left is a sidebar with categories like 'AI/Machine Learning', 'Application Runtime', 'Big Data', 'Cloud Provider', 'Database', 'Developer Tools', 'Development Tools', 'Drivers And Plugins', 'Integration & Delivery', 'Logging & Tracing', 'Modernization & Migration', and 'Monitoring'. The main area is titled 'All Items' and has a search bar containing 'F5'. To the right of the search bar, it says '1 items'. Below the search bar, a single result is displayed as a card. The card features the F5 logo, the text 'F5 Container Ingress Services provided by F5 Networks Inc.', and 'Operator to install F5 Container Ingress Services (CIS) for BIG-IP.'

17. オペレータ情報を読み、[インストール]をクリックします。

 **F5 Container Ingress Services** 1.8.0 provided by F5 Networks Inc. ×

Install

Latest version
1.8.0

Capability level
☒ Basic Install
☐ Seamless Upgrades
☐ Full Lifecycle
☐ Deep Insights
☐ Auto Pilot

Provider type
Certified

Provider
F5 Networks Inc.

Repository
<https://github.com/F5Networks/k8s-bigip-ctlr>

Container image
registry.connect.redhat.com/f5networks/k8s-bigip-ctlr

Introduction
This Operator installs F5 Container Ingress Services (CIS) for BIG-IP in your Cluster. This enables to configure and deploy CIS using Helm Charts.

F5 Container Ingress Services for BIG-IP
F5 Container Ingress Services (CIS) integrates with container orchestration environments to dynamically create L4/L7 services on F5 BIG-IP systems, and load balance network traffic across the services. Monitoring the orchestration API server, CIS is able to modify the BIG-IP system configuration based on changes made to containerized applications.

Documentation
Refer to F5 documentation

- CIS on OpenShift (<https://clouddocs.f5.com/containers/latest/userguide/openshift/>) - OpenShift Routes (<https://clouddocs.f5.com/containers/latest/userguide/routes.html>)

Prerequisites
Create BIG-IP login credentials for use with Operator Helm charts. A basic way be,

```
oc create secret generic <SECRET-NAME> -n kube-system --from-literal=username=<USERNAME> --from-literal=password=<PASSWORD>
```

18. Install Operator（オペレータのインストール）画面で、デフォルトのパラメータをすべてそのままにして、Install（インストール）をクリックします。

Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

Update channel *

☒ beta

Installation mode *

- ☒ All namespaces on the cluster (default)
Operator will be available in all Namespaces.
- ☐ A specific namespace on the cluster
Operator will be available in a single Namespace only.

Installed Namespace *

PR openshift-operators

Approval strategy *

- ☒ Automatic
- ☐ Manual

Install Cancel



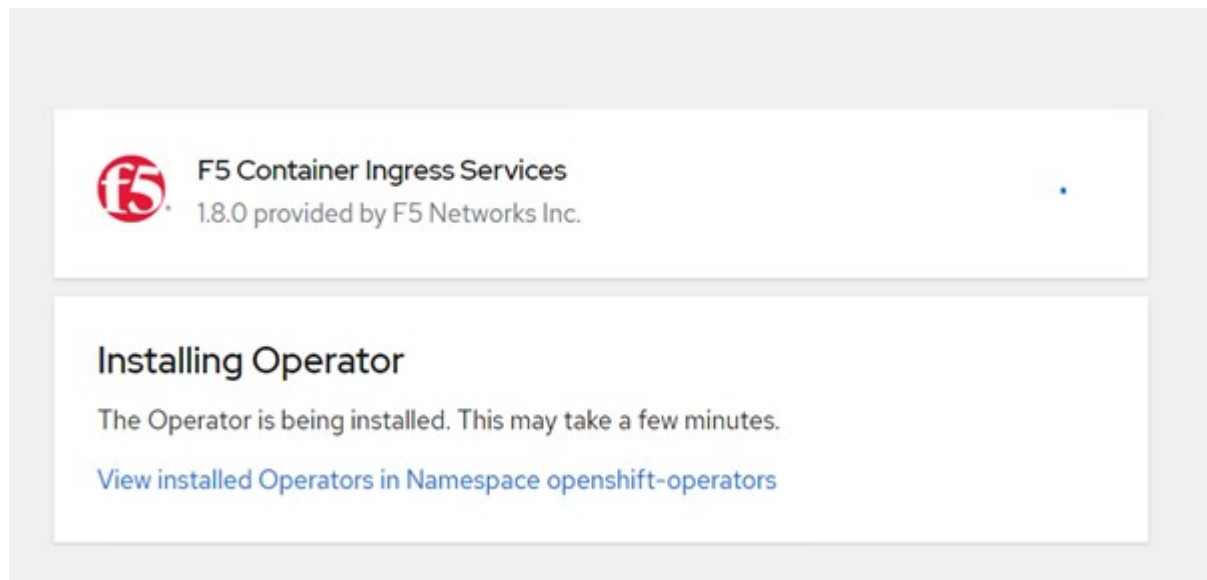
F5 Container Ingress Services
provided by F5 Networks Inc.

Provided APIs

FBIC F5BigIpCtrlr

This CRD provides kind **F5BigIpCtrlr** to configure and deploy F5 BIG-IP Controller.

19. オペレータのインストールには時間がかかります。



20. オペレータがインストールされると、「Installation Successful」というメッセージが表示されます。

21. [演算子]>[インストールされている演算子]に移動し、[F5BigIpCtrlr] タイルの下にある [F5 Container Ingress Service] をクリックして、[インスタンスの作成] をクリックします。

[Installed Operators](#) > Operator details



F5 Container Ingress Services
1.8.0 provided by F5 Networks Inc.

[Details](#)

[YAML](#)

[Subscription](#)

[Events](#)

[F5BigIpCtrlr](#)

Provided APIs

FBIC F5BigIpCtrlr

This CRD provides kind `F5BigIpCtrlr` to configure and deploy F5 BIG-IP Controller.

[+ Create instance](#)

22. YAML View をクリックし、必要なパラメータを更新した後で次の内容を貼り付けます。



以下のパラメータ「bigip_dpartition」、「OpenShift」SDN_NAME」、「bigip_url」、「bigip_login_secret」を更新して、内容をコピーする前にセットアップの値を反映させます。

```




apiVersion: cis.f5.com/v1
kind: F5BigIpCtlr
metadata:
  name: f5-server
  namespace: openshift-operators
spec:
  args:
    log_as3_response: true
    agent: as3
    log_level: DEBUG
    bigip_partition: ocp-vmw
    openshift_sdn_name: /Common/openshift_vxlan
    bigip_url: 10.61.181.19
    insecure: true
    pool-member-type: cluster
    custom_resource_mode: true
    as3_validation: true
    ipam: true
    manage_configmaps: true
  bigip_login_secret: bigip-login
  image:
    pullPolicy: Always
    repo: f5networks/cntr-ingress-svcs
    user: registry.connect.redhat.com
  namespace: kube-system
  rbac:
    create: true
  resources: {}
  serviceAccount:
    create: true
  version: latest

```

23. このコンテンツを貼り付けたら、[作成]をクリックします。これにより、CIS ポッドが kube-system 名前空間にインストールされます。

Pods Create Pod

Filter Name Search by name...

Name ↑	Status ↓	Ready ↓	Restarts ↓	Owner ↓	Memory ↓	CPU ↓
 f5-server-f5-bigip-ctlr-5d7578667d-qxdgj	 Running	1/1	0	 f5-server-f5-bigip-ctlr-5d7578667d	61.1 MiB	0.003 cores



Red Hat OpenShift は、デフォルトで、L7 ロードバランシングのルートを紹介してサービスを公開する方法を提供します。組み込みの OpenShift ルータは、これらのルートのトラフィックのアドバタイズと処理を行います。ただし、外部 F5 BIG-IP システムを紹介してルートをサポートするように F5 CIS を構成することもできます。このシステムは、補助ルータとして実行することも、自己ホスト型 OpenShift ルータに代わるものでもあります。CIS は、OpenShift ルートのルータとして機能する BIG-IP システムに仮想サーバを作成し、BIG-IP はアドバタイズメントとトラフィックルーティングを処理します。この機能を有効にするためのパラメータについては、次のドキュメントを参照してください。これらのパラメータは、APPS/v1 API の OpenShift Deployment リソースに対して定義されています。したがって、F5BigIpCtrl リソース cis.f5.com/v1 API でこれらを使用する場合は、パラメータ名にハイフン (-) をアンダースコア (_) に置き換えます。

24. CIS リソースの作成に渡される引数には 'IPAM:true' と 'custom_resource_mode:true' がありますこれらのパラメータは 'IPAM コントローラとの CIS 統合を有効にするために必要ですF5 IPAM リソースを作成して 'CIS で IPAM 統合が有効になっていることを確認します

```
[admin@rhel-7 ~]$ oc get f5ipam -n kube-system
```

NAMESPACE	NAME	AGE
kube-system	ipam.10.61.181.19.ocp-vmw	43s

25. F5 IPAM コントローラに必要なサービスアカウント、ロール、およびロールバインドを作成します。YAML ファイルを作成し、次の内容を貼り付けます。

```
[admin@rhel-7 ~]$ vi f5-ipam-rbac.yaml

kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctrl-clusterrole
rules:
  - apiGroups: ["fic.f5.com"]
    resources: ["ipams","ipams/status"]
    verbs: ["get", "list", "watch", "update", "patch"]
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: ipam-ctrl-clusterrole-binding
  namespace: kube-system
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: ipam-ctrl-clusterrole
subjects:
  - apiGroup: ""
    kind: ServiceAccount
    name: ipam-ctrl
    namespace: kube-system
---
apiVersion: v1
kind: ServiceAccount
metadata:
  name: ipam-ctrl
  namespace: kube-system
```

26. リソースを作成します。

```
[admin@rhel-7 ~]$ oc create -f f5-ipam-rbac.yaml

clusterrole.rbac.authorization.k8s.io/ipam-ctrl-clusterrole created
clusterrolebinding.rbac.authorization.k8s.io/ipam-ctrl-clusterrole-
binding created
serviceaccount/ipam-ctrl created
```

27. YAML ファイルを作成し、下記の F5 IPAM 展開定義を貼り付けます。



以下の spec.template.spec.containers [0] の ip-range パラメータを更新して、設定に対応する ipamLabel と IP アドレス範囲を反映させます。



IPAM コントローラが定義された範囲から IP アドレスを検出して割り当てるには 'ipamLabels[range1' および range2 を以下の例に示します] が 'LoadBalancer 型のサービスに注釈を付ける必要があります

```
[admin@rhel-7 ~]$ vi f5-ipam-deployment.yaml

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    name: f5-ipam-controller
    name: f5-ipam-controller
    namespace: kube-system
spec:
  replicas: 1
  selector:
    matchLabels:
      app: f5-ipam-controller
  template:
    metadata:
      creationTimestamp: null
      labels:
        app: f5-ipam-controller
    spec:
      containers:
      - args:
        - --orchestration=openshift
        - --ip-range='{ "range1": "10.63.172.242-10.63.172.249",
"range2": "10.63.170.111-10.63.170.129"}'
        - --log-level=DEBUG
        command:
        - /app/bin/f5-ipam-controller
        image:: registry.connect.redhat.com/f5networks/f5-ipam-
controller:latest
        imagePullPolicy: IfNotPresent
        name: f5-ipam-controller
        dnsPolicy: ClusterFirst
        restartPolicy: Always
        schedulerName: default-scheduler
        securityContext: {}
        serviceAccount: ipam-ctrlr
        serviceAccountName: ipam-ctrlr
```


28. F5 IPAM コントローラ配置を作成します。

```
[admin@rhel-7 ~]$ oc create -f f5-ipam-deployment.yaml  
  
deployment/f5-ipam-controller created
```

29. F5 IPAM コントローラポッドが実行されていることを確認します。

```
[admin@rhel-7 ~]$ oc get pods -n kube-system
```

NAME	READY	STATUS	RESTARTS
f5-ipam-controller-5986cff5bd-2bvn6	1/1	Running	0
f5-server-f5-bigip-ctlr-5d7578667d-qxdgj	1/1	Running	0

30. F5 IPAM スキーマを作成します。

```
[admin@rhel-7 ~]$ oc create -f  
https://raw.githubusercontent.com/F5Networks/f5-ipam-  
controller/main/docs/_static/schemas/ipam_schema.yaml  
  
customresourcedefinition.apiextensions.k8s.io/ipams.fic.f5.com
```

検証

1. LoadBalancer タイプのサービスを作成します

```
[admin@rhel-7 ~]$ vi example_svc.yaml
```

```
apiVersion: v1
kind: Service
metadata:
  annotations:
    cis.f5.com/ipamLabel: range1
  labels:
    app: f5-demo-test
  name: f5-demo-test
  namespace: default
spec:
  ports:
  - name: f5-demo-test
    port: 80
    protocol: TCP
    targetPort: 80
  selector:
    app: f5-demo-test
  sessionAffinity: None
  type: LoadBalancer
```

```
[admin@rhel-7 ~]$ oc create -f example_svc.yaml
```

```
service/f5-demo-test created
```

2. IPAM コントローラが外部 IP を割り当ててるかどうかを確認します。

```
[admin@rhel-7 ~]$ oc get svc
```

NAME	TYPE	CLUSTER-IP	EXTERNAL-IP
f5-demo-test	LoadBalancer	172.30.210.108	10.63.172.242
80:32605/TCP	27s		

3. 導入環境を作成し、作成した LoadBalancer サービスを使用します。

```
[admin@rhel-7 ~]$ vi example_deployment.yaml
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    app: f5-demo-test
  name: f5-demo-test
spec:
  replicas: 2
  selector:
    matchLabels:
      app: f5-demo-test
  template:
    metadata:
      labels:
        app: f5-demo-test
    spec:
      containers:
      - env:
        - name: service_name
          value: f5-demo-test
        image: nginx
        imagePullPolicy: Always
        name: f5-demo-test
        ports:
        - containerPort: 80
          protocol: TCP
```

```
[admin@rhel-7 ~]$ oc create -f example_deployment.yaml
```

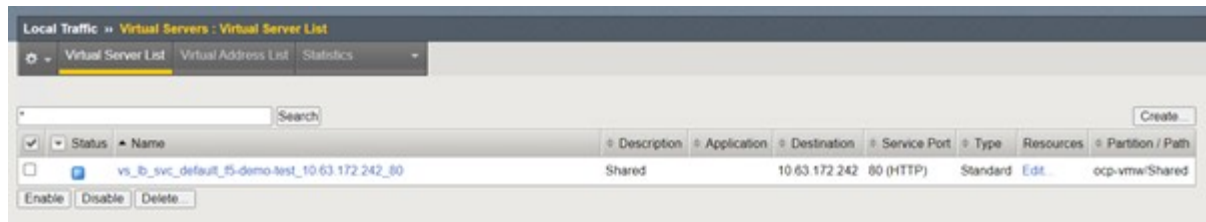
```
deployment/f5-demo-test created
```

4. ポッドが実行されているかどうかを確認します。

```
[admin@rhel-7 ~]$ oc get pods
```

NAME	READY	STATUS	RESTARTS	AGE
f5-demo-test-57c46f6f98-47wwp	1/1	Running	0	27s
f5-demo-test-57c46f6f98-cl2m8	1/1	Running	0	27s

5. 対応する仮想サーバが、OpenShift の LoadBalancer タイプのサービス用に BIG-IP システムに作成されているかどうかを確認します。Local Traffic > Virtual Servers > Virtual Server List の順に選択します。



プライベートイメージレジストリを作成しています

Red Hat OpenShift の導入では、のようなパブリックレジストリを使用します **"キー・IO"** または **"DockerHub"** お客様のほとんどのニーズに対応ただし、お客様が独自のプライベートイメージまたはカスタマイズされたイメージをホストしたい場合があります。

この手順ドキュメントでは、Astra Trident と NetApp ONTAP が提供する永続的ボリュームを使用して作成された、プライベートイメージレジストリを作成しています。



Astra Control Center では、Astra コンテナに必要なイメージをホストするためにレジストリが必要です。次のセクションでは、Red Hat OpenShift クラスタにプライベートレジストリをセットアップし、Astra Control Center のインストールをサポートするために必要なイメージをプッシュする手順について説明します。

プライベートイメージレジストリを作成しています

1. 現在のデフォルトストレージクラスからデフォルトのアノテーションを削除し、OpenShift クラスタの Trident バック対象ストレージクラスをデフォルトとしてアノテートします。

```
[netapp-user@rhel7 ~]$ oc patch storageclass thin -p '{"metadata": {"annotations": {"storageclass.kubernetes.io/is-default-class": "false"}}}'
storageclass.storage.k8s.io/thin patched

[netapp-user@rhel7 ~]$ oc patch storageclass ocp-trident -p '{"metadata": {"annotations": {"storageclass.kubernetes.io/is-default-class": "true"}}}'
storageclass.storage.k8s.io/ocp-trident patched
```

2. 「PEC」セクションに以下の保管パラメータを入力して、imagegeistry のオペレータを編集します。

```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

storage:
  pvc:
    claim:
```

3. カスタムホスト名を使用して OpenShift ルートを作成するには、「PEC」セクションに次のパラメータ

を入力します。保存して終了します。

```
routes:
- hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
  name: netapp-astra-route
```



上記のルート設定は、ルートのカスタムホスト名が必要な場合に使用されます。OpenShift でデフォルトのホスト名を持つルートを作成するには、「PEC」セクションに「defaultRoute : true」というパラメータを追加します。

カスタム TLS 証明書

ルートにカスタムホスト名を使用している場合、デフォルトでは、OpenShift 入力オペレータのデフォルトの TLS 設定が使用されます。ただし、カスタム TLS 設定をルートに追加することはできません。これには、次の手順を実行します。

- a. ルートの TLS 証明書とキーを使用して秘密を作成します。

```
[netapp-user@rhel7 ~]$ oc create secret tls astra-route-tls -n
openshift-image-registry -cert/home/admin/netapp-astra/tls.crt
--key=/home/admin/netapp-astra/tls.key
```

- b. imageregistry 演算子を編集して 'PEC' セクションに次のパラメータを追加します

```
[netapp-user@rhel7 ~]$ oc edit
configs.imageregistry.operator.openshift.io

routes:
- hostname: astra-registry.apps.ocp-vmw.cie.netapp.com
  name: netapp-astra-route
  secretName: astra-route-tls
```

4. このような場合は、すべての管理者をもう一度編集し、管理状態を「管理状態」に変更してください。保存して終了します。

```
oc edit configs.imageregistry/cluster

managementState: Managed
```

5. すべての前提条件を満たしている場合は、プライベートイメージレジストリに PVC、ポッド、およびサービスが作成されます。数分後にレジストリが起動します。

```
[netapp-user@rhel7 ~]$oc get all -n openshift-image-registry
```

NAME	READY	STATUS
pod/cluster-image-registry-operator-74f6d954b6-rb7zr	1/1	Running
3		90d
pod/image-pruner-1627257600-f5cpj	0/1	Completed
0		2d9h
pod/image-pruner-1627344000-swqx9	0/1	Completed
0		33h
pod/image-pruner-1627430400-rv5nt	0/1	Completed
0		9h
pod/image-registry-6758b547f-6pnj8	1/1	Running
0		76m
pod/node-ca-bwb5r	1/1	Running
0		90d
pod/node-ca-f8w54	1/1	Running
0		90d
pod/node-ca-gjx7h	1/1	Running
0		90d
pod/node-ca-lcx4k	1/1	Running
0		33d
pod/node-ca-v7zmx	1/1	Running
0		7d21h
pod/node-ca-xpppp	1/1	Running
0		89d

NAME	TYPE	CLUSTER-IP	EXTERNAL-
IP PORT(S) AGE			
service/image-registry	ClusterIP	172.30.196.167	<none>
5000/TCP 15h			
service/image-registry-operator	ClusterIP	None	<none>
60000/TCP 90d			

NAME	DESIRED	CURRENT	READY	UP-TO-DATE
AVAILABLE NODE SELECTOR		AGE		
daemonset.apps/node-ca	6	6	6	6
kubernetes.io/os=linux	90d			

NAME	READY	UP-TO-DATE
AVAILABLE AGE		
deployment.apps/cluster-image-registry-operator	1/1	1
90d		
deployment.apps/image-registry	1/1	1
15h		

NAME	DESIRED
CURRENT READY AGE	
replicaset.apps/cluster-image-registry-operator-74f6d954b6	1 1
1 90d	
replicaset.apps/image-registry-6758b547f	1 1
1 76m	
replicaset.apps/image-registry-78bfbd7f59	0 0
0 15h	
replicaset.apps/image-registry-7fcc8d6cc8	0 0
0 80m	
replicaset.apps/image-registry-864f88f5b	0 0
0 15h	
replicaset.apps/image-registry-cb47fffb	0 0
0 10h	

NAME	COMPLETIONS	DURATION	AGE
job.batch/image-pruner-1627257600	1/1	10s	2d9h
job.batch/image-pruner-1627344000	1/1	6s	33h
job.batch/image-pruner-1627430400	1/1	5s	9h

NAME	SCHEDULE	SUSPEND	ACTIVE	LAST
SCHEDULE AGE				
cronjob.batch/image-pruner	0 0 * * *	False	0	9h
90d				

NAME	HOST/PORT
PATH SERVICES PORT TERMINATION WILDCARD	
route.route.openshift.io/public-routes	astra-registry.apps.ocp-vmw.cie.netapp.com
image-registry	<all> reencrypt None

6. 入力オペレータ OpenShift レジストリルートにデフォルトの TLS 証明書を使用している場合は、次のコマンドを使用して TLS 証明書を取得できます。

```
[netapp-user@rhel7 ~]$ oc extract secret/router-ca --keys=tls.crt -n openshift-ingress-operator
```

7. OpenShift ノードがレジストリにアクセスしてイメージをプルできるようにするには、OpenShift ノード上の Docker クライアントに証明書を追加します。TLS 証明書を使用して「OpenShift -config」ネームスペースに ConfigMap を作成し、証明書を信頼できるようにクラスティメージ設定にパッチします。


```
[netapp-user@rhel7 ~]$ oc create configmap astra-ca -n openshift-config
--from-file=astra-registry.apps.ocp-vmw.cie.netapp.com=tls.crt

[netapp-user@rhel7 ~]$ oc patch image.config.openshift.io/cluster
--patch '{"spec":{"additionalTrustedCA":{"name":"astra-ca"}}}'
--type=merge
```

8. OpenShift の内部レジストリは認証によって制御されます。OpenShift ユーザはすべて OpenShift レジストリにアクセスできますが、ログインユーザが実行できる操作はユーザ権限によって異なります。

- a. ユーザーまたはユーザーのグループがレジストリから画像をプルできるようにするには、ユーザーにレジストリビューアの役割が割り当てられている必要があります。

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-viewer
ocp-user

[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-viewer
ocp-user-group
```

- b. ユーザーまたはユーザーグループにイメージの書き込みまたはプッシュを許可するには、ユーザーにレジストリエディタの役割が割り当てられている必要があります。

```
[netapp-user@rhel7 ~]$ oc policy add-role-to-user registry-editor
ocp-user

[netapp-user@rhel7 ~]$ oc policy add-role-to-group registry-editor
ocp-user-group
```

9. OpenShift ノードがレジストリにアクセスし、イメージをプッシュまたはプルするには、プルシークレットを設定する必要があります。

```
[netapp-user@rhel7 ~]$ oc create secret docker-registry astra-registry-
credentials --docker-server=astra-registry.apps.ocp-vmw.cie.netapp.com
--docker-username=ocp-user --docker-password=password
```

10. このプルシークレットは、サービスアカウントにパッチを適用するか、対応するポッド定義で参照できます。

- a. サービスアカウントにパッチを適用するには、次のコマンドを実行します。

```
[netapp-user@rhel7 ~]$ oc secrets link <service_account_name> astra-
registry-credentials --for=pull
```

- b. ポッド定義でプルシークレットを参照するには、「PEC」セクションに次のパラメータを追加します。

```
imagePullSecrets:
  - name: astra-registry-credentials
```

11. OpenShift ノードとは別にワークステーションからイメージをプッシュまたはプルするには、次の手順を実行します。

- a. TLS 証明書を Docker クライアントに追加します。

```
[netapp-user@rhel7 ~]$ sudo mkdir /etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com

[netapp-user@rhel7 ~]$ sudo cp /path/to/tls.crt
/etc/docker/certs.d/astra-registry.apps.ocp-vmw.cie.netapp.com
```

- b. OC ログインコマンドを使用して OpenShift にログインします。

```
[netapp-user@rhel7 ~]$ oc login --token=sha256~D49SpB_lesSrJYwrM0LIO-VRcjWHu0a27vKa0 --server=https://api.ocp-vmw.cie.netapp.com:6443
```

- c. podman/docker コマンドで OpenShift ユーザクレデンシャルを使用してレジストリにログインします。

ポッドマン

```
[netapp-user@rhel7 ~]$ podman login astra-registry.apps.ocp-vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t) --tls
--verify=false
```

+ 注: 「kubeadmin」ユーザを使用してプライベートレジストリにログインする場合は、パスワードの代わりにトークンを使用します。

Docker です

```
[netapp-user@rhel7 ~]$ docker login astra-registry.apps.ocp-vmw.cie.netapp.com -u kubeadmin -p $(oc whoami -t)
```

+ 注: 「kubeadmin」ユーザを使用してプライベートレジストリにログインする場合は、パスワードの代わりにトークンを使用します。

- d. 画像を押したり引いたりします。

ポッドマン

```
[netapp-user@rhel7 ~]$ podman push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest  
[netapp-user@rhel7 ~]$ podman pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

Docker です

```
[netapp-user@rhel7 ~]$ docker push astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest  
[netapp-user@rhel7 ~]$ docker pull astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra/vault-controller:latest
```

解決策の検証とユースケース：ネットアップを使用した **Red Hat OpenShift**

このページに記載する例は、ネットアップでの Red Hat OpenShift の解決策の検証と使用事例です。

- ["永続的ストレージを使用した Jenkins CI/CD パイプラインの導入"](#)
- ["ネットアップを使用して Red Hat OpenShift でマルチテナンシーを構成します"](#)
- ["NetApp ONTAP を使用した Red Hat OpenShift Virtualization"](#)
- ["ネットアップを使用した Red Hat OpenShift での Kubernetes 向けの高度なクラスタ管理"](#)

永続的ストレージを使用した **Jenkins CI / CD** パイプラインの導入：ネットアップでの **Red Hat OpenShift**

このセクションでは、Jenkins との継続的統合 / 継続的配信または導入（CI / CD）パイプラインを導入して解決策の動作を検証する手順について説明します。

Jenkins の導入に必要なリソースを作成します

Jenkins アプリケーションの導入に必要なリソースを作成するには、次の手順に従います。

1. Jenkins という名前の新しいプロジェクトを作成します。

Create Project

Name *

Jenkins

Display Name

Description

Cancel

Create

2. この例では、永続的ストレージを使用して Jenkins を導入しています。Jenkins ビルドをサポートするには、PVC を作成します。[ストレージ]>[永続的ボリューム要求]の順に選択し、[永続的ボリューム要求の作成]をクリックします。作成したストレージクラスを選択し、永続ボリューム要求名が Jenkins であることを確認し、適切なサイズとアクセスモードを選択して、作成をクリックします。

Create Persistent Volume Claim

[Edit YAML](#)

Storage Class

 basic ▼

Storage class for the new claim.

Persistent Volume Claim Name *

jenkins

A unique name for the storage claim within the project.

Access Mode *

☒ Single User (RWO) ☐ Shared Access (RWX) ☐ Read Only (ROX)

Permissions to the mounted drive.

Size *

100 GiB ▼

Desired storage capacity.

☐ Use label selectors to request storage

Use label selectors to define how storage is created.

[Create](#) [Cancel](#)

永続的ストレージを使用して **Jenkins** を導入する

永続ストレージを使用して Jenkins を導入するには、次の手順を実行します。

1. 左上隅で、ロールを Administrator から Developer に変更します。+ 追加をクリックし、カタログからを選択します。キーワードでフィルターバーで Jenkins を検索します。永続的ストレージを使用する Jenkins Service を選択します。

Developer Catalog

Add shared apps, services, or source-to-image builders to your project from the Developer Catalog. Cluster admins can install additional apps which will show up here automatically.

All Items
Languages
Databases
Middleware
CI/CD
Other

Type
☒ Operator Backed (0)
☐ Helm Charts (0)
☒ Builder Image (0)
☒ Template (4)
☐ Service Class (0)

All Items
Group By: None ▼


Template

Jenkins
provided by Red Hat, Inc.

Jenkins service, with persistent storage. NOTE: You must have persistent volumes available in...


Template

Jenkins
provided by Red Hat, Inc.

Jenkins service, with persistent storage. NOTE: You must have persistent volumes available in...


Template

Jenkins (Ephemeral)
provided by Red Hat, Inc.

Jenkins service, without persistent storage. WARNING: Any data stored will be lost upon...


Template

Jenkins (Ephemeral)
provided by Red Hat, Inc.

Jenkins service, without persistent storage. WARNING:

- 「テンプレートをインスタンス化」をクリックします。



Jenkins

Provided by Red Hat, Inc.



Instantiate Template

Provider

Red Hat, Inc.

Support

[Get support](#)

Created At

 May 26, 3:58 am

Description

Jenkins service, with persistent storage.

NOTE: You must have persistent volumes available in your cluster to use this template.

Documentation


https://docs.okd.io/latest/using_images/other_images/jenkins.html

- デフォルトでは、Jenkins アプリケーションの詳細が入力されます。要件に基づいてパラメータを変更し、[作成 (Create)] をクリックします。このプロセスでは、OpenShift で Jenkins をサポートするた

めに必要なリソースがすべて作成されます。

Instantiate Template

Namespace *

 jenkins

Jenkins Service Name

jenkins

The name of the OpenShift Service exposed for the Jenkins container.

Jenkins JNLP Service Name

jenkins-jnlp

The name of the service used for master/slave communication.

Enable OAuth in Jenkins

true

Whether to enable OAuth OpenShift integration. If false, the static account 'admin' will be initialized with the password 'password'.

Memory Limit

1Gi

Maximum amount of memory the container can use.

Volume Capacity *

50Gi

Volume space available for data, e.g. 512Mi, 2Gi.

Jenkins ImageStream Namespace

openshift

The OpenShift Namespace where the Jenkins ImageStream resides.

Disable memory intensive administrative monitors

false

Whether to perform memory intensive, possibly slow, synchronization with the Jenkins Update Center on start. If true, the Jenkins core update monitor and site warnings monitor are disabled.

Jenkins ImageStreamTag

jenkins:2

Name of the ImageStreamTag to be used for the Jenkins image.

Fatal Error Log File

false

When a fatal error occurs, an error log is created with information and the state obtained at the time of the fatal error.

Allows use of Jenkins Update Center repository with invalid SSL certificate

false

Whether to allow use of a Jenkins Update Center that uses invalid certificate (self-signed, unknown CA). If any value other than 'false', certificate check is bypassed. By default, certificate check is enforced.

[Create](#) [Cancel](#)



Jenkins

INSTANT-APP JENKINS

[View documentation](#) [Get support](#)

Jenkins service, with persistent storage.

NOTE: You must have persistent volumes available in your cluster to use this template.

The following resources will be created:





- DeploymentConfig
- PersistentVolumeClaim
- RoleBinding
- Route
- Service
- ServiceAccount

4. Jenkins ポッドが「Ready」状態になるまでに約 10 ～ 12 分かかります。

Pods

[Create Pod](#)

1 Running	0 Pending	0 Terminating	0 CrashLoopBackOff	1 Completed	0 Failed	0 Unknown
Select all filters						1 of 2 Items





Name ↑	Namespace ↓	Status ↓	Ready ↓	Owner ↓	Memory ↓	CPU ↓
 jenkins-l-c77n9	 jenkins	 Running	1/1	 jenkins-1	-	0.004 cores

5. ポッドがインスタンス化されたら、ネットワーキング > ルートと進みます。Jenkins の Web ページを開くには、Jenkins ルート用の URL をクリックします。

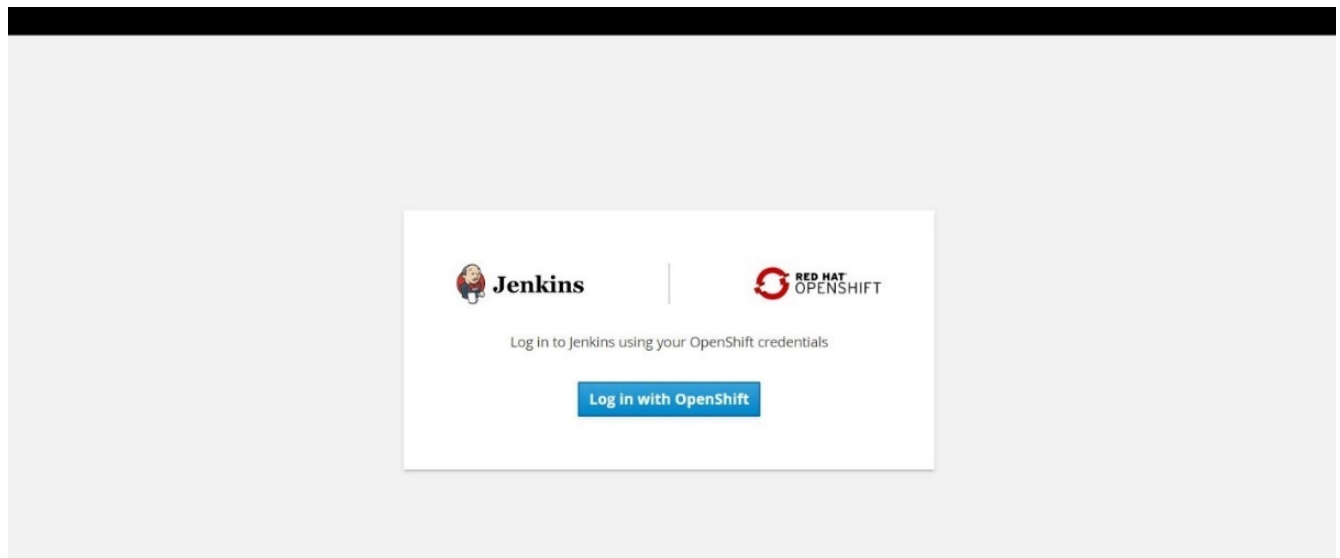
Routes

[Create Route](#)

1 Accepted	0 Rejected	0 Pending	Select all filters	1 Item
------------	------------	-----------	------------------------------------	--------

Name ↓	Namespace ↓	Status	Location ↓	Service ↓
 jenkins	 jenkins	 Accepted	https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com	 jenkins

6. Jenkins アプリケーションの作成時に OpenShift OAuth が使用されていたため、「OpenShift でログイン」をクリックします。



7. Jenkins サービスアカウントに OpenShift ユーザへのアクセスを許可します。

Authorize Access

Service account `jenkins` in project `jenkins` is requesting permission to access your account (`kube:admin`)

Requested permissions

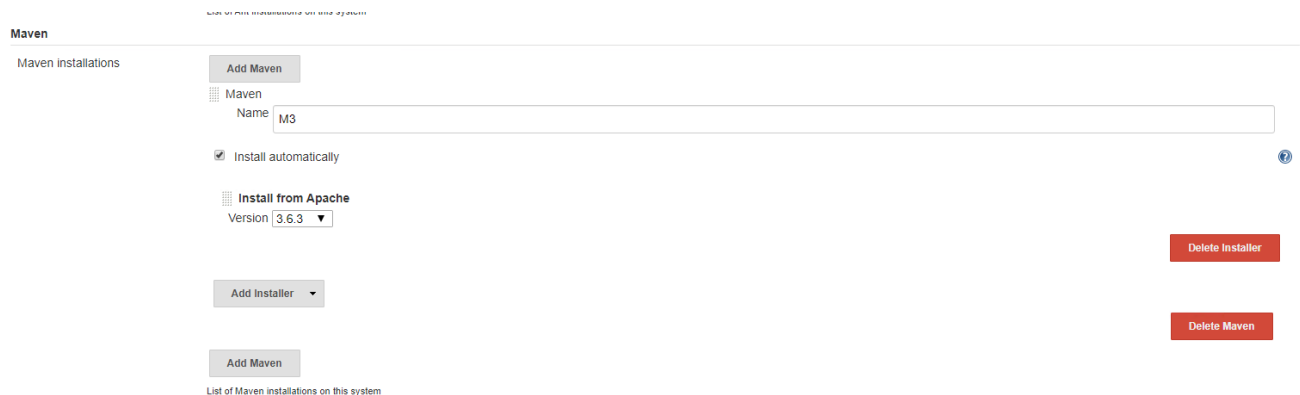
- ☒ **user:info**
Read-only access to your user information (including username, identities, and group membership)
- ☒ **user:check-access**
Read-only access to view your privileges (for example, "can I create builds?")

You will be redirected to <https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com/securityRealm/finishLogin>

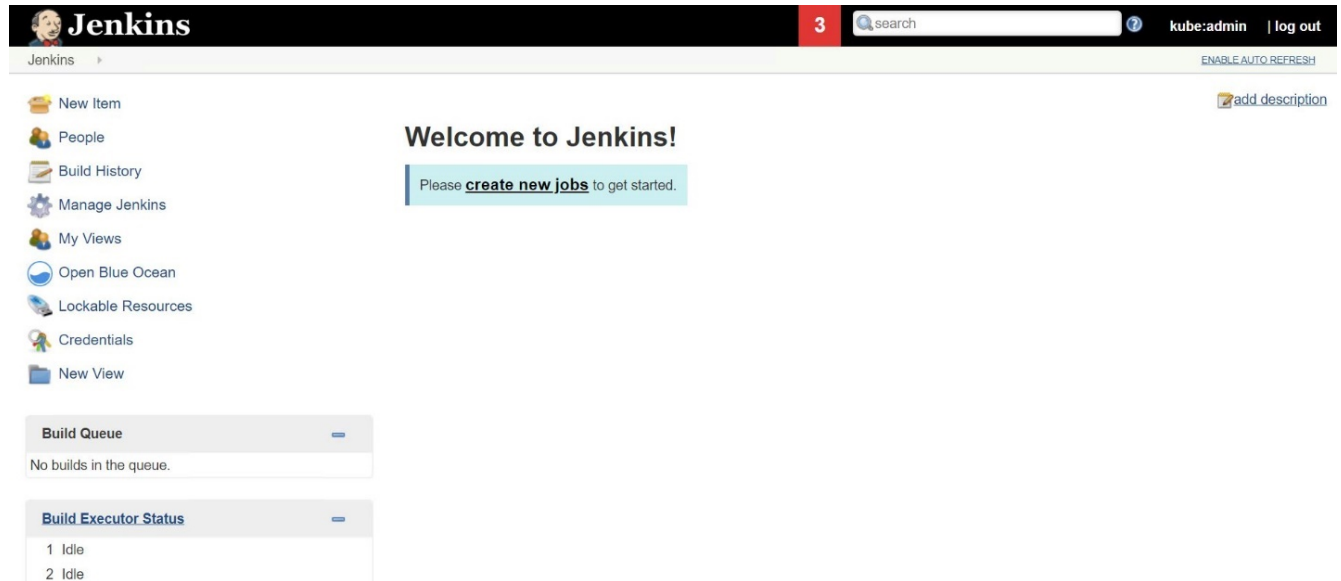
Allow selected permissions

Deny

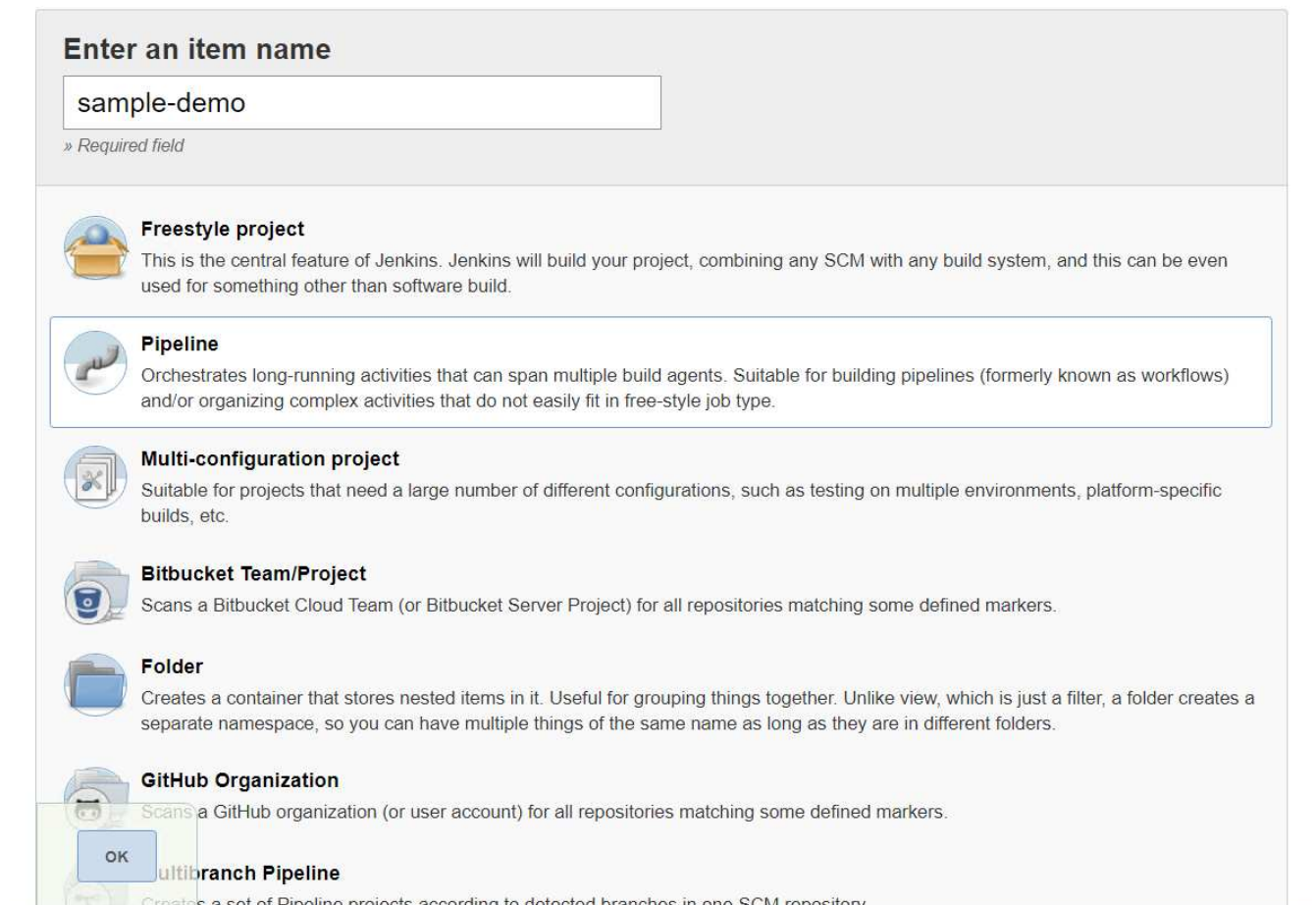
8. Jenkins のようこそページが表示されます。Maven ビルドを使用しているので、まず Maven のインストールを完了します。Manage Jenkins > Global Tool Configuration に移動し、Maven サブヘッドで Add Maven をクリックします。任意の名前を入力し、[自動的にインストール] オプションが選択されていることを確認します。[保存] をクリックします。



9. CI / CD のワークフローを示すパイプラインを作成できるようになりました。ホームページで、左側のメニューから [新規ジョブの作成] または [新規アイテム] をクリックします。



10. [項目の作成] ページで、任意の名前を入力し、[パイプライン] を選択して、[OK] をクリックします。



11. パイプライン (Pipeline) タブを選択します。サンプルパイプラインを試すドロップダウンメニューから、Github + Maven を選択します。コードが自動的に入力されます。[保存] をクリックします。

GeneralBuild TriggersAdvanced Project OptionsPipeline

Advanced...

Pipeline

DefinitionPipeline script

Script

```
1 node {
2   def mvnHome
3   stage('Preparation') { // for display purposes
4     // Get some code from a GitHub repository
5     git 'https://github.com/jglick/simple-maven-project-with-tests.git'
6     // Get the Maven tool.
7     // ** NOTE: This 'M3' Maven tool must be configured
8     // **       in the global configuration.
9     mvnHome = tool 'M3'
10  }
11  stage('Build') {
12    // Run the maven build
13    withEnv(["MVN_HOME=$mvnHome"]) {
14      if (isUnix()) {
15        sh "$MVN_HOME/bin/mvn" -Dmaven.test.failure.ignore clean package
16      } else {
17        bat ("%MVN_HOME%\bin\mvn" -Dmaven.test.failure.ignore clean package/)
18      }
19    }
20  }
21 }
```

GitHub + Maven

☒ Use Groovy Sandbox

[Pipeline Syntax](#)

SaveApply

12. 「今すぐビルド」をクリックして、準備、ビルド、テストの各フェーズで開発を開始します。ビルドプロセス全体が完了してビルドの結果が表示されるまでに数分かかることがあります。

Jenkins

[Jenkins](#)
[sample-demo](#)

[Back to Dashboard](#)
[Status](#)
[Changes](#)
[Build Now](#)
[Delete Pipeline](#)
[Configure](#)
[Full Stage View](#)
[Open Blue Ocean](#)
[Rename](#)
[Pipeline Syntax](#)

Pipeline sample-demo

[Last Successful Artifacts](#)

[Recent Changes](#)

[simple-maven-project-with-tests-1.0-SNAPSHOT.jar](#)
1.71 KB
[view](#)

Stage View

#1

May 27 08:53

No Changes

Average stage times:

(Average full run time: ~7s)

Preparation	Build	Results
2s	4s	69ms

[Latest Test Result \(no failures\)](#)

Permalinks

- [Last build \(#1\), 1 min 23 sec ago](#)
- [Last stable build \(#1\), 1 min 23 sec ago](#)
- [Last successful build \(#1\), 1 min 23 sec ago](#)
- [Last completed build \(#1\), 1 min 23 sec ago](#)

13. コードが変更された場合は、必ずパイプラインを再構築して新しいバージョンのソフトウェアにパッチを適用することで、継続的な統合と継続的な提供を実現できます。[最近の変更] をクリックして、前のバージョンからの変更を追跡します。

171

Back to Dashboard

Status

Changes

Build Now

Delete Pipeline

Configure

Full Stage View

Open Blue Ocean

Rename

Pipeline Syntax

Pipeline sample-demo

Last Successful Artifacts

simple-maven-project-with-tests-1.0-SNAPSHOT.jar 1.71 KB view

Recent Changes

Stage View

Build History

find

#2 May 27, 2020 3:56 PM

#1 May 27, 2020 3:53 PM

Atom feed for all Atom feed for failures

Average stage times:

(Average full run time: ~6s)

#2 May 27 08:56 No Changes

#1 May 27 08:53 No Changes

Preparation	Build	Results
2s	4s	86ms
1s	4s	104ms
2s	4s	69ms

Latest Test Result (no failures)

Permalinks

- Last build (#2). 19 sec ago
- Last stable build (#2). 19 sec ago
- Last successful build (#2). 19 sec ago
- Last completed build (#2). 19 sec ago

NetApp ONTAP を使用して Red Hat OpenShift にマルチテナンシーを設定します

ネットアップを使用した Red Hat OpenShift でのマルチテナンシーの構成

コンテナで複数のアプリケーションやワークロードを実行する多くの組織は、アプリケーションやワークロードごとに 1 つの Red Hat OpenShift クラスタを導入する傾向にあります。これにより、アプリケーションやワークロードを厳密に分離し、パフォーマンスを最適化し、セキュリティの脆弱性を軽減できます。ただし、アプリケーションごとに独立した Red Hat OpenShift クラスタを導入するには、独自の問題が発生します。これにより、各クラスタを個別に監視および管理する必要がある運用上のオーバーヘッドが増大し、さまざまなアプリケーションに専用リソースを使用することでコストが増大し、効率的な拡張性が妨げられます。

この問題を解決するには、すべてのアプリケーションまたはワークロードを 1 つの Red Hat OpenShift クラスタで実行することを検討します。しかし、このようなアーキテクチャでは、リソースの分離とアプリケーションセキュリティの脆弱性が大きな課題の 1 つとなっています。あるワークロードのセキュリティの脆弱性は、自然に別のワークロードにオーバーフローする可能性があるため、影響ゾーンが増加します。また、あるアプリケーションによる突然の制御されないリソース使用率は、デフォルトではリソース割り当てポリシーがないため、別のアプリケーションのパフォーマンスに影響を与える可能性があります。

172

そのため、組織は、たとえば、すべてのワークロードを単一のクラスタで実行しながら、各ワークロードに専用のクラスタのメリットを提供することで、両方の世界で最も優れたソリューションを見つけることができます。

このように効果的な解決策の 1 つは、Red Hat OpenShift でマルチテナンシーを構成することです。マルチテナンシーは、複数のテナントを同じクラスタ上に共存させ、リソースやセキュリティなどを適切に分離できるアーキテクチャです。この場合、テナントは、特定のユーザグループが専用として使用するよう設定されたクラスタリソースのサブセットとみなすことができます。Red Hat OpenShift クラスタでマルチテナンシーを設定する利点は次のとおりです。

- クラスタリソースを許可することで設備投資と運用コストを削減を共有します
- 運用と管理のオーバーヘッドを軽減
- セキュリティ侵害のクロスコンタミネーションからワークロードを保護
- リソースの競合による予期しないパフォーマンスの低下からワークロードを保護

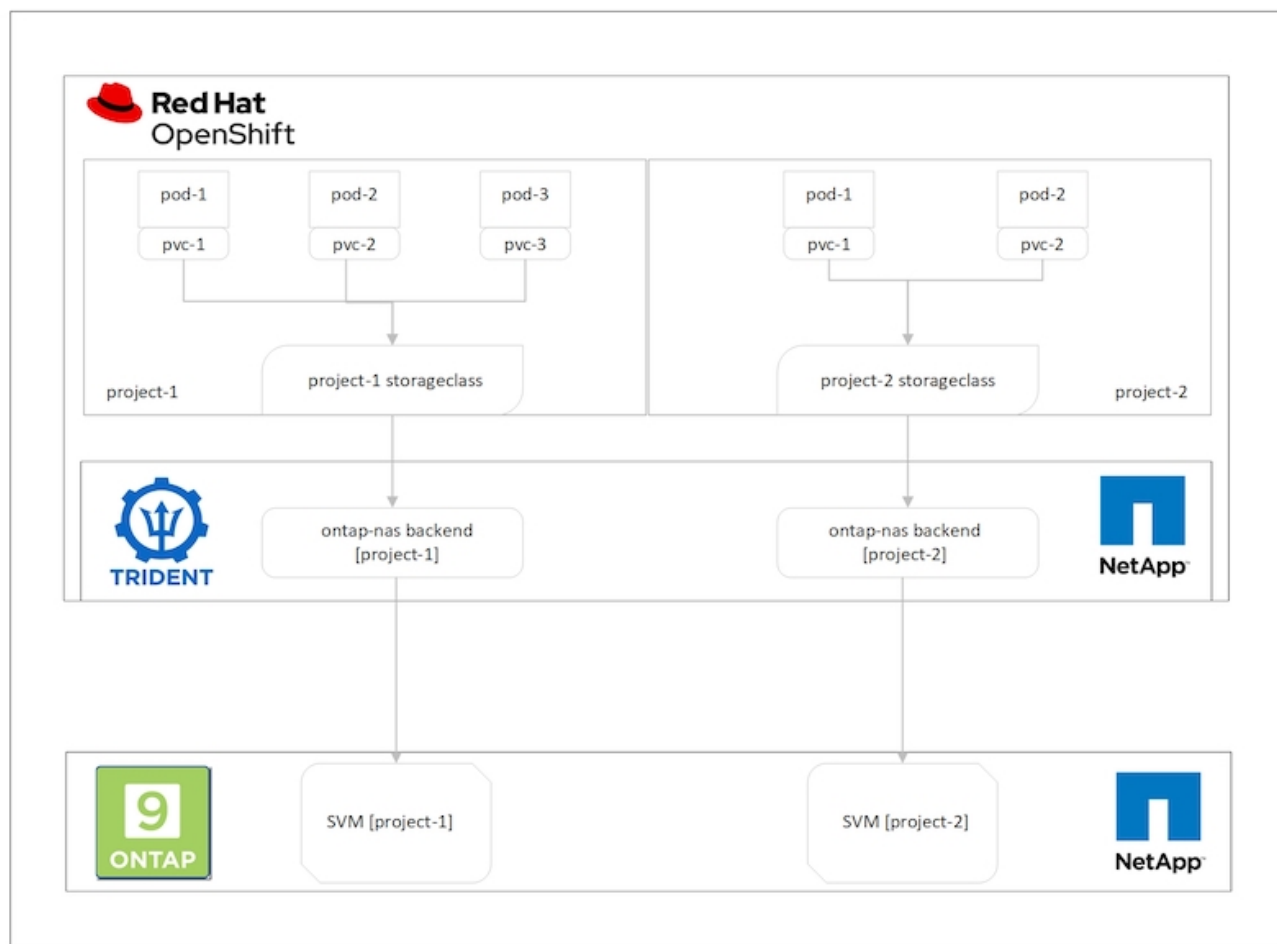
マルチテナント OpenShift クラスタを完全に実現するには、コンピューティング、ストレージ、ネットワーク、セキュリティなど、異なるリソースバケットに属するクラスタリソースにクォータと制限を設定する必要があります。この解決策のすべてのリソースバケットの特定の側面について説明しますが、ネットアップでは、NetApp ONTAP を基盤とする Astra Trident によって動的に割り当てられるストレージリソースにマルチテナンシーを設定することで、複数のワークロードで提供または消費されるデータを分離し、保護するためのベストプラクティスに焦点を当てています。

アーキテクチャ

ネットアップ ONTAP を基盤とする Red Hat OpenShift と Astra Trident は、デフォルトでワークロードを分離する機能を提供していませんが、マルチテナンシーの設定に使用できる幅広い機能を備えています。ネットアップ ONTAP を基盤とする Astra Trident を使用した Red Hat OpenShift クラスタでのマルチテナント解決策の設計について理解を深めるために、一連の要件を含む例を検討し、その構成について概説します。

2 つの異なるチームが取り組んでいる 2 つのプロジェクトの一環として、組織が Red Hat OpenShift クラスタ上で 2 つのワークロードを実行するとします。こうしたワークロードのデータは、NetApp ONTAP NAS バックエンドの Astra Trident によって動的にプロビジョニングされる PVC 上に存在します。組織では、この 2 つのワークロードに対応するマルチテナント解決策を設計し、これらのプロジェクトに使用されるリソースを分離して、セキュリティとパフォーマンスを維持することが求められています。主に、これらのアプリケーションを提供するデータに重点が置かれています。

次の図は、ネットアップ ONTAP を基盤とする Astra Trident を使用した Red Hat OpenShift クラスタ上のマルチテナント解決策を示しています。



テクノロジー要件

1. NetApp ONTAP ストレージクラス
2. Red Hat OpenShift クラス
3. Astra Trident

Red Hat OpenShift –クラスタリソース

Red Hat OpenShift クラスターの観点からは、最初に最上位のリソースがプロジェクトです。OpenShift プロジェクトは、OpenShift クラスター全体を複数の仮想クラスターに分割するクラスタリソースと見なすことができます。したがって、プロジェクトレベルでの分離によって、マルチテナンシーの設定の基盤が提供されます。

次に、クラスターで RBAC を設定します。ベストプラクティスとして、すべての開発者が 1 つのプロジェクトまたはワークロードを担当し、アイデンティティプロバイダ (IdP) 内の単一のユーザグループに設定することを推奨します。Red Hat OpenShift では、IdP の統合とユーザグループの同期が可能なため、IdP のユーザとグループをクラスターにインポートできるようになります。これにより、クラスター管理者は、プロジェクト専用のクラスタリソースへのアクセスをそのプロジェクトに使用するユーザグループまたはグループに分離して、クラスタリソースへの不正アクセスを制限できます。Red Hat OpenShift への IdP の統合の詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。

NetApp ONTAP

Red Hat OpenShift クラスタの永続的ストレージプロバイダとして機能している共有ストレージを分離し、各プロジェクト用にストレージ上に作成されたボリュームが、別々のストレージ上に作成されたものと同じようにホストに表示されるようにすることが重要です。そのためには、プロジェクトやワークロードに応じて Storage Virtual Machine (SVM) を NetApp ONTAP 上に作成し、各 SVM をワークロード専用にします。

Astra Trident

NetApp ONTAP で作成されたプロジェクトごとに異なる SVM が作成されたら、各 SVM を異なる Trident バックエンドにマッピングする必要があります。Trident のバックエンド構成は、OpenShift クラスタリソースへの永続的ストレージの割り当てを促進します。また、マッピング先の SVM の詳細が必要です。これは、バックエンドのプロトコルドライバである必要があります。必要に応じて、ストレージでのボリュームのプロビジョニング方法を定義したり、ボリュームのサイズやアグリゲートの使用などを制限したりできます。Trident バックエンドの定義に関する詳細はこちらをご覧ください ["こちらをご覧ください"](#)。

Red Hat OpenShift –ストレージリソース

Trident バックエンドを設定したら、次の手順として StorageClasses を設定します。バックエンドと同じ数のストレージクラスを構成して、各ストレージクラスが 1 つのバックエンドにしかボリュームをスピニングできない。ストレージクラスを定義する際に StoragePools パラメータを使用して、ストレージクラスを特定の Trident バックエンドにマッピングできます。ストレージクラスを定義する詳細については、[こちらをご覧ください](#)。そのため、StorageClass から Trident バックエンドへの 1 対 1 のマッピングで、1 つの SVM をポイントします。これにより、そのプロジェクトに割り当てられた StorageClass を経由するすべてのストレージ要求が、そのプロジェクト専用の SVM によって処理されます。

ストレージクラスにネームスペースリソースが含まれていないため、あるプロジェクトのストレージクラスに対するストレージ要求を別のネームスペースまたはプロジェクトのポッドで拒否するにはどうすればよいですか？回答では、ResourceQuotas を使用します。ResourceQuotas は、プロジェクトごとのリソースの合計使用量を制御するオブジェクトです。プロジェクト内のオブジェクトで消費できるリソースの合計量だけでなく、リソースの数も制限できます。ほとんどの場合、ResourceQuotas を使用してプロジェクトのリソースを制限することができます。この機能を効率的に使用することで、リソースのオーバプロビジョニングや過剰消費によるコストやシステム停止を削減できます。のドキュメント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。

このユースケースでは、特定のプロジェクトのポッドが、プロジェクト専用ではないストレージクラスのストレージを要求しないように制限する必要があります。これを行うには '`<storage-class-name>.storageclass.storage0.k8sio/persistentvolumeclaims'0` を設定して '他のストレージ・クラスに対する永続的ボリューム要求を制限する必要がありますさらに、クラスタ管理者は、プロジェクト内の開発者が ResourceQuotas を変更するためのアクセス権を持っていないことを確認する必要があります。

設定

マルチテナント解決策では、必要以上に多くのクラスタリソースにアクセスすることはできません。つまり、マルチテナンシー構成の一部として構成するリソースセット全体が、クラスタ管理者、ストレージ管理者、および各プロジェクトに取り組む開発者に分けられます。

次の表に、各ユーザが実行する各タスクを示します。

ロール	タスク
* Cluster-admin*	さまざまなアプリケーションやワークロード用のプロジェクトを作成できます
	Storage Admin 用の ClusterRoles および RoleBindings を作成します
	ロールとロールの作成特定のアクセス権を割り当てる開発者のためのバインド プロジェクト
	[オプション] 特定のノードでポッドをスケジュールするようにプロジェクトを設定します
* ストレージ管理者 *	NetApp ONTAP に SVM を作成する
	Trident バックエンドを作成
	ストレージクラスを作成します
	ストレージリソースクォータを作成します
* 開発者 *	割り当てられたプロジェクトで PVC またはポッドを作成またはパッチするためのアクセスを検証します
	アクセスを検証して、別のプロジェクトで PVC またはポッドを作成またはパッチします
	アクセス権を検証して、プロジェクト、リソースクォータ、ストレージクラスを表示または編集します

設定

NetAppを使用したRed Hat OpenShiftでマルチテナンシーを設定するための前提条件を次に示します。

前提条件

- NetApp ONTAP クラスタ：
- Red Hat OpenShift クラスタ
- Trident がクラスタにインストールされている。
- tridentctl および OC ツールがインストールされ、\$PATH に追加された管理ワークステーション。
- ONTAP への管理アクセス。
- OpenShift クラスタへのクラスタ管理者アクセス。
- クラスタがアイデンティティプロバイダに統合されました。
- アイデンティティプロバイダは、異なるチームのユーザを効率的に区別するように設定されています。

Configuration ：クラスタ管理者のタスク

Red Hat OpenShift cluster-admin によって次のタスクが実行されます。

1. Red Hat OpenShift クラスタに cluster-admin としてログインします。

2. 異なるプロジェクトに対応する 2 つのプロジェクトを作成します。

```
oc create namespace project-1
oc create namespace project-2
```

3. project-1 の開発者ロールを作成します。

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-1
  name: developer-project-1
rules:
  - verbs:
      - '*'
    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
  - verbs:
      - '*'
    apiGroups:
      - ''
    resources:
      - bindings
      - configmaps
      - endpoints
      - events
      - persistentvolumeclaims
      - pods
      - pods/log
      - pods/attach
```

```
- podtemplates
- replicationcontrollers
- services
- limitranges
- namespaces
- componentstatuses
- nodes
- verbs:
  - '*'
apiGroups:
  - trident.netapp.io
resources:
  - trident snapshots
EOF
```



ここで説明するロール定義は単なる例です。エンドユーザの要件に基づいて開発者の役割を定義する必要があります。

1. 同様に、project-2 の開発者ロールを作成します。
2. すべての OpenShift およびネットアップストレージリソースは、通常はストレージ管理者が管理します。ストレージ管理者向けのアクセスは、Trident のインストール時に作成された Trident オペレータロールによって制御されます。これに加えて、ストレージ管理者は ResourceQuotas にアクセスして、ストレージの消費方法を制御する必要があります。
3. クラスタ内のすべてのプロジェクトの ResourceQuotas を管理する役割を作成して、ストレージ管理者に割り当てます。

```
cat << EOF | oc create -f -
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: resource-quotas-role
rules:
  - verbs:
    - '*'
    apiGroups:
    - ''
    resources:
    - resourcequotas
  - verbs:
    - '*'
    apiGroups:
    - quota.openshift.io
    resources:
    - '*'
EOF
```

4. クラスタが組織のアイデンティティプロバイダと統合され、ユーザグループがクラスタグループと同期されていることを確認します。次の例は、アイデンティティプロバイダがクラスタに統合され、ユーザグループと同期されていることを示しています。

```
$ oc get groups
NAME                                USERS
ocp-netapp-storage-admins          ocp-netapp-storage-admin
ocp-project-1                      ocp-project-1-user
ocp-project-2                      ocp-project-2-user
```

1. ストレージ管理者用の ClusterRoleBindings を設定します。

```

cat << EOF | oc create -f -
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-trident-operator
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-operator
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-resource-quotas-cr
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: resource-quotas-role
EOF

```



ストレージ管理者の場合は、Trident オペレータとリソースクォータの 2 つのロールにバインドする必要があります。

1. ロールの作成 - developer-project-1 のロールを project-1 の対応するグループ (OCP-project-1) にバインドする開発者のバインディング。

```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-1-developer
  namespace: project-1
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-project-1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-1
EOF
```

2. 同様に、開発者の役割を project-2 の対応するユーザーグループにバインドする開発者の RoleBindings を作成します。

設定：ストレージ管理者のタスク

ストレージ管理者が次のリソースを設定する必要があります。

1. NetApp ONTAP クラスタに admin としてログインします。
2. Storage > Storage VMs と進み、Add をクリックします。必要な詳細を指定して、プロジェクト 1 用とプロジェクト 2 用に 1 つずつ、2 つの SVM を作成します。また、SVM とそのリソースを管理するには vsadmin アカウントを作成します。

Add Storage VM



STORAGE VM NAME

project-1-svm

Access Protocol



SMB/CIFS, NFS

iSCSI



Enable SMB/CIFS



Enable NFS



Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

Rule Index	Clients	Access Protocols	Read-Only R...	Read/Wr
	10.61.181.0/24	Any	Any	Any

[+ Add](#)

DEFAULT LANGUAGE [?](#)

c.utf_8



NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

10.61.181.224

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN

Default-4



1. ストレージ管理者として Red Hat OpenShift クラスタにログインします。
2. project-1 のバックエンドを作成し、プロジェクト専用の SVM にマッピングします。ONTAP クラスタ管理者を使用する代わりに、SVM の vsadmin アカウントを使用してバックエンドを SVM に接続することを推奨します。


```
cat << EOF | tridentctl -n trident create backend -f
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "nfs_project_1",
  "managementLIF": "172.21.224.210",
  "dataLIF": "10.61.181.224",
  "svm": "project-1-svm",
  "username": "vsadmin",
  "password": "NetApp123"
}
EOF
```



この例では ONTAP と NAS のドライバを使用しています。ユースケースに基づいてバックエンドを作成する場合は、適切なドライバを使用します。



Trident が Trident プロジェクトにインストールされているとします。

1. 同様に、project-2 の Trident バックエンドを作成し、project-2 に専用の SVM にマッピングします。
2. 次に、ストレージクラスを作成します。StoragePools パラメータを設定して、project-1 専用のバックエンドのストレージプールを使用するように project-1 のストレージクラスを作成し、これを設定します。

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-1-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_1:.*"
EOF
```

3. 同様に、project-2 に対してストレージクラスを作成し、project-2 に専用のバックエンドのストレージプールを使用するように設定します。
4. ResourceQuota を作成して 'プロジェクト 1 内のリソースを制限し' 他のプロジェクト専用のストレージを要求します

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-1-sc-rq
  namespace: project-1
spec:
  hard:
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

5. 同様に 'ResourceQuota を作成して 'project-2 内のリソースを制限し ' 他のプロジェクト専用のストレージを要求します

検証

前の手順で設定したマルチテナントアーキテクチャを検証するには、次の手順を実行します。

割り当てられたプロジェクトで **PVC** またはポッドを作成するためのアクセスを検証します

1. OCP-project-1-user として、 project-1 の開発者としてログインします。
2. アクセス権をチェックして新しいプロジェクトを作成してください

```
oc create ns sub-project-1
```

3. project-1 に割り当てられたストレージクラスを使用して 'project-1 に PVC を作成します

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
    storageClassName: project-1-sc
EOF
```

4. PVC に関連付けられている PV を確認します

```
oc get pv
```

5. PV とそのボリュームが、NetApp ONTAP 上のプロジェクト 1 専用の SVM に作成されていることを確認します。

```
volume show -vserver project-1-svm
```

6. project-1 にポッドを作成し、前の手順で作成した PVC をマウントします。

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  volumes:
    - name: test-pvc-project-1
      persistentVolumeClaim:
        claimName: test-pvc-project-1
  containers:
    - name: test-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/usr/share/nginx/html"
          name: test-pvc-project-1
EOF
```

7. ポッドが実行中かどうか、およびボリュームがマウントされているかどうかを確認します。

```
oc describe pods test-pvc-pod -n project-1
```

アクセスを検証して別のプロジェクトに **PVC** またはポッドを作成するか、別のプロジェクト専用のリソースを使用します

1. OCP-project-1-user として、project-1 の開発者としてログインします。
2. project-2 に割り当てられたストレージクラスを使用して 'project-1 に PVC を作成します

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1-sc-2
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-2-sc
EOF
```

3. PROJECT-2 で PVC を作成します。

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-2-sc-1
  namespace: project-2
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

4. PVC 「test-pvc-project-1-sc-2」 および 「test-pvc-project-2-ssc-1」 が作成されていないことを確認します。

```
oc get pvc -n project-1
oc get pvc -n project-2
```

5. プロジェクト 2 でポッドを作成します。

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  containers:
  - name: test-container
    image: nginx
    ports:
    - containerPort: 80
      name: "http-server"
EOF
```

アクセス権を検証して、プロジェクト、リソースクォータ、ストレージクラスを表示および編集します

1. OCP-project-1-user として、project-1 の開発者としてログインします。
2. アクセス権をチェックして新しいプロジェクトを作成してください。

```
oc create ns sub-project-1
```

3. アクセスを検証してプロジェクトを表示します

```
oc get ns
```

4. ユーザーが ResourceQuotas を表示または編集できるかどうかを確認します プロジェクト 1

```
oc get resourcequotas -n project-1
oc edit resourcequotas project-1-sc-rq -n project-1
```

5. ユーザーがストレージクラスを表示するためのアクセス権を持っていることを確認します

```
oc get sc
```

6. ストレージクラスについては 'アクセスを確認してください
7. ストレージクラスを編集するためにユーザーのアクセス権を検証します

```
oc edit sc project-1-sc
```

拡張：プロジェクトの追加

マルチテナント構成でストレージリソースを使用する新しいプロジェクトを追加する場合、マルチテナンシーを違反しないように追加の設定が必要になります。マルチテナントクラスタでプロジェクトを追加するには、次の手順を実行します。

1. NetApp ONTAP クラスタにストレージ管理者としてログインします。
2. 「ストレージ → ストレージ VM」に移動し、「追加」をクリックします。project-3 専用の新しい SVM を作成します。また、SVM とそのリソースを管理するには vsadmin アカウントを作成します。

Add Storage VM



STORAGE VM NAME

project-3-svm

Access Protocol

☒ SMB/CIFS, NFS

iSCSI

☐ Enable SMB/CIFS

☒ Enable NFS

☒ Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

Rule Index	Clients	Access Protocols	Read-Only R...	Read/Wr
	10.61.181.0/24	Any	Any	Any

[+ Add](#)

DEFAULT LANGUAGE [?](#)

c.utf_8

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

10.61.181.228

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN

Default-4

1. Red Hat OpenShift クラスタにクラスタ管理者としてログインします
2. 新しいプロジェクトを作成します。

```
oc create ns project-3
```


3. IdP に project-3 のユーザグループが作成され、 OpenShift クラスタと同期されていることを確認してください。

```
oc get groups
```

4. project-3 の開発者ロールを作成します。

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-3
  name: developer-project-3
rules:
  - verbs:
    - '*'
    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
  - verbs:
    - '*'
    apiGroups:
      - ''
    resources:
      - bindings
      - configmaps
      - endpoints
      - events
      - persistentvolumeclaims
      - pods
      - pods/log
      - pods/attach
```

```

- podtemplates
- replicationcontrollers
- services
- limitranges
- namespaces
- componentstatuses
- nodes
- verbs:
  - '*'
apiGroups:
- trident.netapp.io
resources:
- trident snapshots
EOF

```



ここで説明するロール定義は単なる例です。開発者ロールは、エンドユーザの要件に基づいて定義する必要があります。

1. プロジェクト 3 の開発者用に RoleBinding を作成します。これは、developer-project-3 の役割を、project-3 の対応するグループ (OCP-project-3) にバインドします。

```

cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-3-developer
  namespace: project-3
subjects:
- kind: Group
  apiGroup: rbac.authorization.k8s.io
  name: ocp-project-3
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-3
EOF

```

2. Red Hat OpenShift クラスタにストレージ管理者としてログインします
3. Trident バックエンドを作成し、project-3 専用の SVM にマッピングします。ONTAP クラスタ管理者を使用する代わりに、SVM の vsadmin アカウントを使用してバックエンドを SVM に接続することを推奨します。

```
cat << EOF | tridentctl -n trident create backend -f
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "nfs_project_3",
  "managementLIF": "172.21.224.210",
  "dataLIF": "10.61.181.228",
  "svm": "project-3-svm",
  "username": "vsadmin",
  "password": "NetApp!23"
}
EOF
```



この例では ONTAP と NAS のドライバを使用しています。ユースケースに基づいてバックエンドを作成するための適切なドライバを使用します。



Trident が Trident プロジェクトにインストールされているとします。

1. project-3 用のストレージクラスを作成し、project-3 専用のバックエンドのストレージプールを使用するように設定します。

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-3-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_3:.*"
EOF
```

2. ResourceQuota を作成して 'プロジェクト 3 のリソースを制限しますストレージを要求するストレージは '他のプロジェクト専用のストレージになります

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-3-sc-rq
  namespace: project-3
spec:
  hard:
    project-1-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

3. 他のプロジェクトの ResourceQuotas にパッチを適用して 'プロジェクト内のリソースがプロジェクト 3 専用のストレージからストレージにアクセスするのを制限します

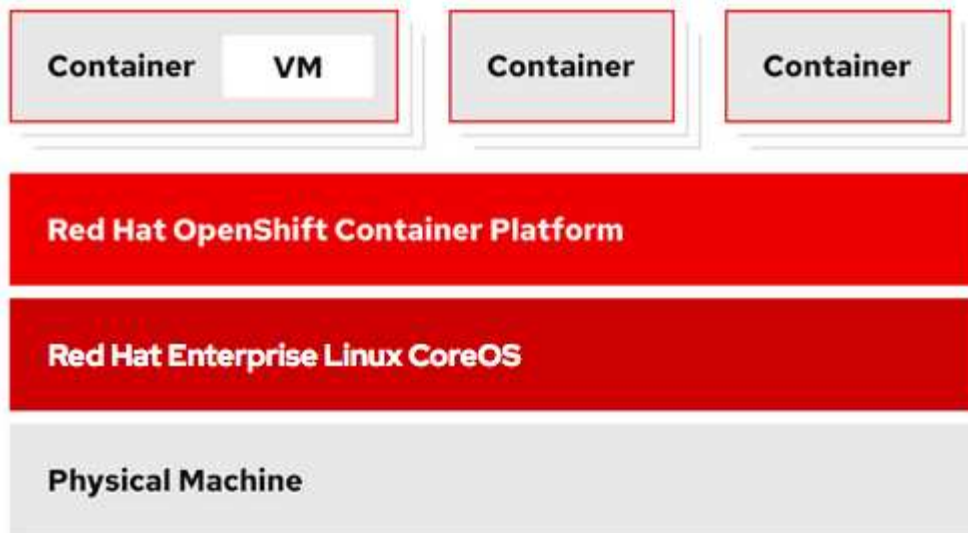
```
oc patch resourcequotas project-1-sc-rq -n project-1 --patch
'{"spec":{"hard":{"project-3-sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
oc patch resourcequotas project-2-sc-rq -n project-2 --patch
'{"spec":{"hard":{"project-3-sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
```

NetApp ONTAP を使用した Red Hat OpenShift Virtualization

NetApp ONTAP を使用した Red Hat OpenShift Virtualization

それぞれのユースケースに応じて、コンテナと仮想マシン（VM）はどちらも、さまざまなタイプのアプリケーションに最適なプラットフォームとして機能します。そのため、多くの組織では、ワークロードの一部をコンテナで実行し、一部を VM で実行しています。そのため多くの場合、VM 用のハイパーバイザーとアプリケーション用のコンテナオーケストレーションツールという別々のプラットフォームを管理する必要があり、組織はさらに多くの課題に直面します。

この課題に対処するために、Red Hat は OpenShift バージョン 4.6 から始まる OpenShift Virtualization（以前のコンテナネイティブ仮想化）を導入しました。OpenShift Virtualization 機能を使用すると、同じ OpenShift Container Platform インストール上でコンテナとともに仮想マシンを実行および管理できるため、オペレータを介して VM の導入と管理を自動化するハイブリッド管理機能が提供されます。OpenShift Virtualization では、OpenShift で VM を作成するだけでなく、VMware vSphere、Red Hat Virtualization、Red Hat OpenStack Platform の各環境からの VM のインポートもサポートします。



NetApp ONTAP をベースにした OpenShift Virtualization では、ライブ VM 移行、VM ディスククローニング、VM スナップショットなどの一部の機能がサポートされており、Astra Trident の支援を受けています。それぞれのセクションで、このドキュメントの後半で各ワークフローの例について説明します。

Red Hat OpenShift Virtualization の詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。

OpenShift 仮想化の導入

NetApp ONTAP を使用して **Red Hat OpenShift Virtualization** を導入します

このセクションでは、NetApp ONTAP を使用した Red Hat OpenShift Virtualization の導入方法について説明します。

前提条件

- Red Hat OpenShift クラスタ（バージョン 4.6 以降） RHCOS ワーカーノードを使用するベアメタルインフラストラクチャにインストールします
- OpenShift クラスタは、インストーラでプロビジョニングされたインフラを介してインストールする必要があります（IPI）
- VM の HA を維持するには、マシンの健全性チェックを導入します
- NetApp ONTAP クラスタ
- OpenShift クラスタに Trident の Astra をインストール
- ONTAP クラスタの SVM で設定された Trident バックエンド
- OpenShift クラスタ上でストレージクラスを構成し、Astra Trident をプロビジョニングツールとして提供
- Red Hat OpenShift クラスタへのクラスタ管理者アクセス
- NetApp ONTAP クラスタへの管理者アクセス
- tridentctl および OC ツールがインストールされている管理ワークステーション \$PATH に追加されました

OpenShift Virtualization は、OpenShift クラスタにインストールされたオペレータによって管理されるため、メモリ、CPU、およびストレージに追加のオーバーヘッドが発生します。このオーバーヘッドは、クラスタ

のハードウェア要件を計画する際に考慮する必要があります。のドキュメントを参照してください "[こちらをご覧ください](#)" 詳細：

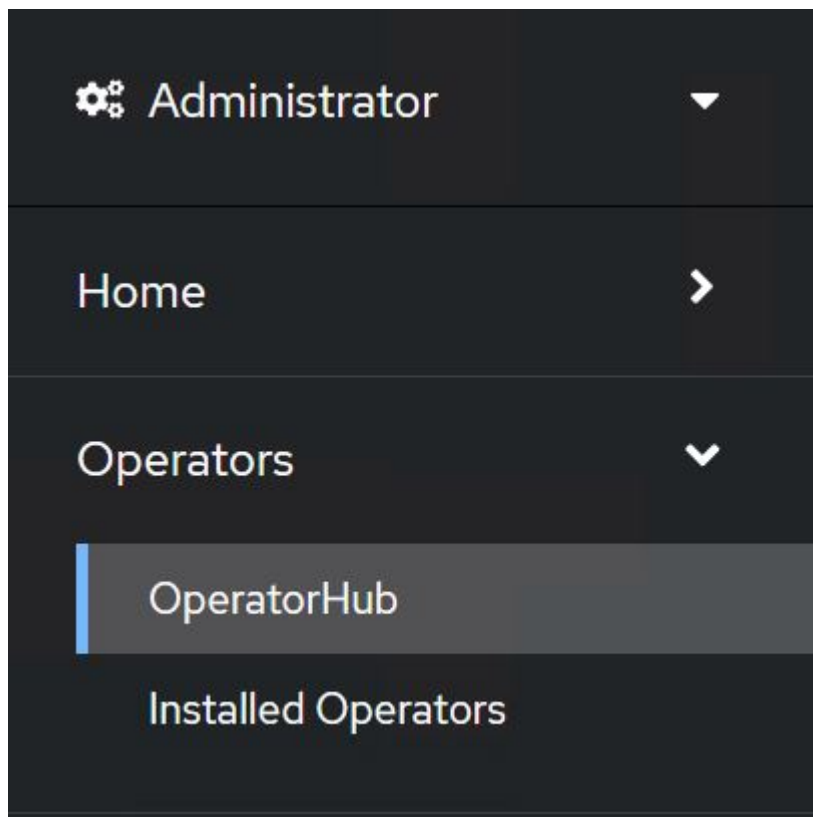
ノード配置ルールを設定して、OpenShift Virtualization オペレータ、コントローラ、VM をホストする OpenShift クラスタノードのサブセットを指定することもできます。OpenShift Virtualization のノード配置ルールを設定するには、のドキュメントに従ってください "[こちらをご覧ください](#)"。

OpenShift Virtualization を基盤とするストレージについては、特定の Trident バックエンドからストレージを要求する専用のストレージクラスを用意し、そのストレージクラスを専用の SVM でバックアップすることを推奨します。これにより、OpenShift クラスタ上で VM ベースのワークロードに提供されるデータに関して、レベルのマルチテナンシーが維持されます。

NetApp ONTAP を使用して **Red Hat OpenShift Virtualization** を導入します

OpenShift Virtualization をインストールするには、次の手順を実行します。

1. クラスタ管理者アクセス権を持つ Red Hat OpenShift ベアメタルクラスタにログインします。
2. Perspective ドロップダウンから Administrator を選択します。
3. Operators > OperatorHub に移動して、OpenShift Virtualization を検索します。



4. OpenShift Virtualization タイルを選択し、Install をクリックします。



Install

Latest version

2.6.2

Capability level

- ☒ Basic Install
- ☒ Seamless Upgrades
- ☒ Full Lifecycle
- ☐ Deep Insights
- ☐ Auto Pilot

Provider type

Red Hat

Provider

Red Hat

Requirements

Your cluster must be installed on bare metal infrastructure with Red Hat Enterprise Linux CoreOS workers.

Details

OpenShift Virtualization extends Red Hat OpenShift Container Platform, allowing you to host and manage virtualized workloads on the same platform as container-based workloads. From the OpenShift Container Platform web console, you can import a VMware virtual machine from vSphere, create new or clone existing VMs, perform live migrations between nodes, and more. You can use OpenShift Virtualization to manage both Linux and Windows VMs.

The technology behind OpenShift Virtualization is developed in the [KubeVirt](#) open source community. The KubeVirt project extends [Kubernetes](#) by adding additional virtualization resource types through [Custom Resource Definitions](#) (CRDs). Administrators can use Custom Resource Definitions to manage [VirtualMachine](#) resources alongside all other resources that Kubernetes provides.

5. Install Operator（オペレータのインストール）画面で、デフォルトのパラメータをすべてそのままにして、Install（インストール）をクリックします。

Update channel *

- ☐ 2.1
- ☐ 2.2
- ☐ 2.3
- ☐ 2.4
- ☒ stable

Installation mode *

- ☐ All namespaces on the cluster (default)
This mode is not supported by this Operator
- ☒ A specific namespace on the cluster
Operator will be available in a single Namespace only.

Installed Namespace *

- ☒ Operator recommended Namespace: **PR** openshift-cnv



Namespace creation

Namespace **openshift-cnv** does not exist and will be created.

- ☐ Select a Namespace

Approval strategy *

- ☒ Automatic
- ☐ Manual

Install

Cancel



OpenShift Virtualization
provided by Red Hat

Provided APIs



OpenShift
Virtualization
Deployment

Required

Represents the deployment of
OpenShift Virtualization

6. オペレータによるインストールが完了するまで待ちます。



OpenShift Virtualization

2.6.2 provided by Red Hat



Installing Operator

The Operator is being installed. This may take a few minutes.

[View installed Operators in Namespace openshift-cnv](#)

7. オペレータがインストールされたら、Create HyperConverged をクリックします。



OpenShift Virtualization

2.6.2 provided by Red Hat



Installed operator – operand required

The Operator has installed successfully. Create the required custom resource to be able to use this Operator.

HC HyperConverged **Required**

Creates and maintains an OpenShift Virtualization Deployment

Create HyperConverged

[View installed Operators in Namespace openshift-cnv](#)

8. [Create HyperConverged (ハイパーコンバージドの作成)] 画面で、[Create (作成)] をクリックし、すべてのデフォルトパラメータを受け入れます。このステップでは、OpenShift Virtualization のインストールを開始します。

Name *

kubevirt-hyperconverged

Labels

app=frontend

Infra >

infra HyperConvergedConfig influences the pod configuration (currently only placement) for all the infra components needed on the virtualization enabled cluster but not necessarily directly on each node running VMs/VMLs.

Workloads >

workloads HyperConvergedConfig influences the pod configuration (currently only placement) of components which need to be running on a node where virtualization workloads should be able to run. Changes to Workloads HyperConvergedConfig can be applied only without existing workload.

Bare Metal Platform

☒ true

BareMetalPlatform indicates whether the infrastructure is baremetal.

Feature Gates >

featureGates is a map of feature gate flags. Setting a flag to `true` will enable the feature. Setting `false` or removing the feature gate, disables the feature.

Local Storage Class Name

LocalStorageClassName the name of the local storage class.




Create **Cancel**

9. OpenShift CNV ネームスペースですべてのポッドが running 状態に移行し、OpenShift Virtualization オペレータが Succeeded 状態になると、オペレータは使用可能な状態になります。これで、OpenShift クラスタで VM を作成できるようになります。

Project: openshift-cnv ▾

Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#). Or create an Operator and ClusterServiceVersion using the [Operator SDK](#).

Name ▾	Managed Namespaces ▴	Status	Last updated	Provided APIs
 OpenShift Virtualization 2.6.2 provided by Red Hat	NS openshift-cnv	 Succeeded Up to date	 May 18, 8:02 pm	OpenShift Virtualization Deployment HostPathProvisioner deployment

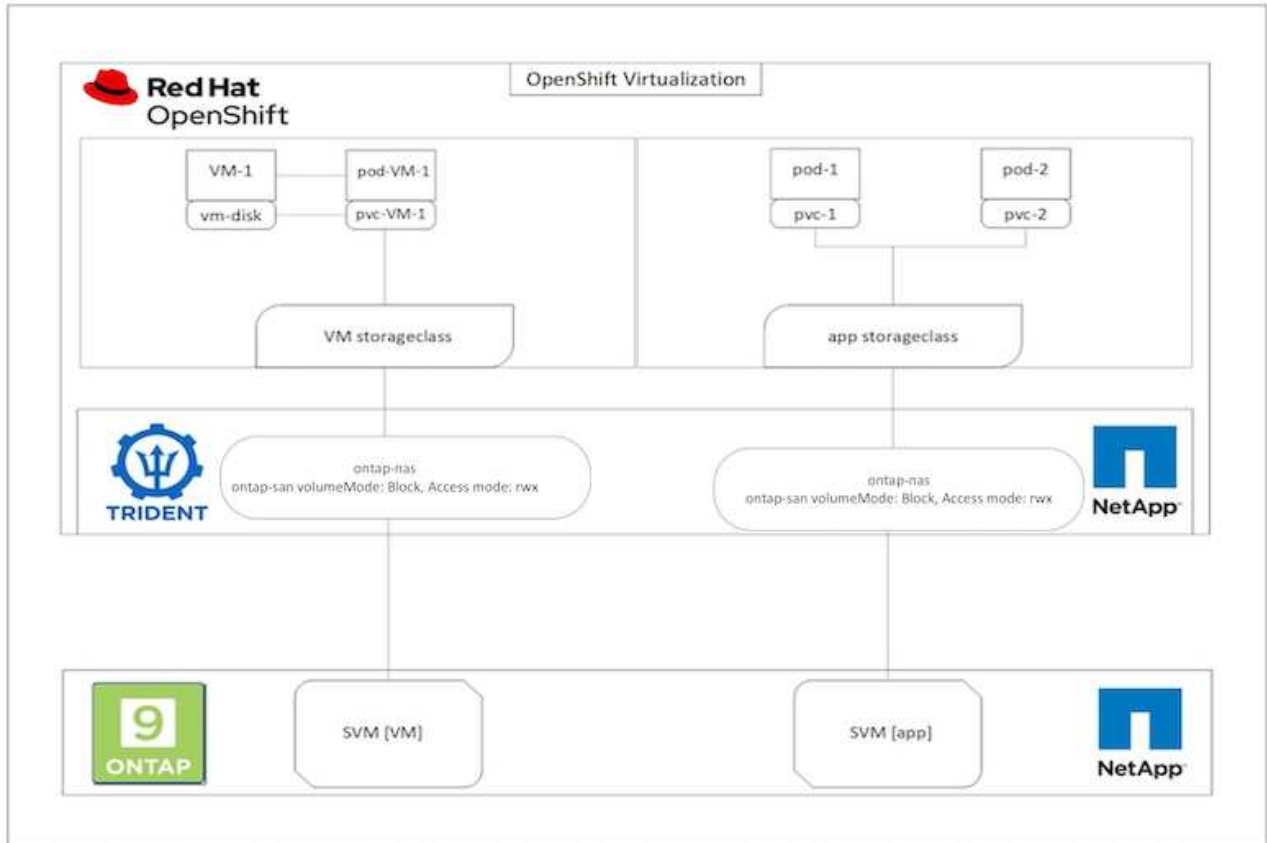
ワークフロー

ワークフロー：NetApp ONTAP を使用した Red Hat OpenShift Virtualization

このセクションでは、Red Hat OpenShift Virtualizationを使用して仮想マシンを作成する方法について説明します。

VM を作成します

VM は、オペレーティングシステムとデータをホストするボリュームを必要とするステートフルな導入です。CNV では、VM がポッドとして実行されるため、VM は Trident 経由で NetApp ONTAP にホストされた PVS によってバックアップされます。これらのボリュームはディスクとして接続され、VM のブートソースを含むファイルシステム全体が格納されます。



OpenShift クラスタに仮想マシンを簡単に作成するには、次の手順を実行します。

1. [仮想化]>[仮想マシン]に移動し、[作成]をクリックします。
2. テンプレートから選択します。
3. 起動ソースが使用可能なオペレーティングシステムを選択します。
4. [Start the VirtualMachine after creation]チェックボックスをオンにします。
5. [Quick create VirtualMachine]をクリックします。

仮想マシンが作成されて起動し、* running *状態になります。デフォルトのストレージクラスを使用して、ブートディスク用にPVCと対応するPVが自動的に作成されます。将来VMをライブマイグレーションできるようにするには、ディスクに使用するストレージクラスがRWXボリュームをサポートできることを確認する必要があります。これはライブマイグレーションの要件です。ONTAP-NASとONTAP-SAN（iSCSIプロトコルとNVMe/TCPプロトコルのvolumeModeブロック）では、それぞれのストレージクラスを使用して作成されたボリュームのRWXアクセスモードがサポートされます。

クラスタでONTAP-SANストレージクラスを設定するには、を参照してください。 ["VMwareからOpenShiftによる仮想化へのVMの移行に関するセクション"](#)。



ONTAP NASまたはiSCSIをクラスタのデフォルトのストレージクラスとしてセットアップできます。[Quick create VirtualMachine]をクリックすると、デフォルトのストレージクラスを使用して、VMのブート可能なルートディスク用のPVCとPVが作成されます。デフォルトのストレージクラスがONTAP-NASまたはONTAP-SANでない場合は、[Customize VirtualMachine]>[Customize VirtualMachine parameters]>[Disks]を選択し、必要なストレージクラスを使用するようにディスクを編集して、ディスクのストレージクラスを選択できます。

通常、VMディスクのプロビジョニング時には、ファイルシステムよりもブロックアクセスモードが推奨されます。

OSテンプレートを選択した後で仮想マシンの作成をカスタマイズするには、[クイック作成]ではなく[仮想マシンのカスタマイズ]をクリックします。

1. 選択したオペレーティングシステムにブートソースが設定されている場合は、*[仮想マシンパラメータのカスタマイズ]*をクリックします。
2. 選択したオペレーティングシステムにブートソースが設定されていない場合は、設定する必要があります。手順の詳細については、"[ドキュメント](#)"。
3. 起動ディスクを設定したら、*[仮想マシンパラメータのカスタマイズ]*をクリックします。
4. このページのタブからVMをカスタマイズできます。例：タブをクリックし、[ディスクの追加]*をクリックしてVMに別のディスクを追加します。
5. [仮想マシンの作成]をクリックして仮想マシンを作成します。これにより、対応するポッドがバックグラウンドでスピンアップされます。



ブートソースがURLまたはレジストリからテンプレートまたはオペレーティングシステム用に設定されている場合、openshift-virtualization-os-images KVMゲストイメージをPVCに投影してダウンロードします。テンプレート PVC に、対応する OS の KVM ゲストイメージを格納できるだけの十分なプロビジョニングスペースがあることを確認する必要があります。これらのPVCは、任意のプロジェクトでそれぞれのテンプレートを使用して作成されると、クローニングされて仮想マシンにルートディスクとして接続されます。

The screenshot shows the OpenShift Virtualization console interface. On the left is a sidebar with navigation links: Administrator, Home, Operators, Workloads, Virtualization (selected), Overview, Catalog, VirtualMachines (active), Templates, and Instance Types. The main panel displays a table of Virtual Machines under the heading 'VirtualMachines'. The table has columns for Name, Status, Conditions, Node, and IP address. There are four VMs listed, all with a status of 'Running'. A 'Create' button is located in the top right corner of the table area, and a dropdown menu is open below it, showing three options: 'From template', 'From volume', and 'With YAML'.

Name	Status	Conditions	Node	IP address
VM centos-stream9-hissing-anteater	Running		ocp-worker3	10.130.0.143
VM centos-stream9-improved-kill	Running		ocp-worker3	10.130.0.145
VM centos-stream9-weary-toucan	Running		ocp-worker3	10.130.0.123
VM centos-stream9-zealous-anaconda	Running		ocp-worker3	10.130.0.117

Create new VirtualMachine

Select an option to create a VirtualMachine from.

Template catalog

InstanceTypes

Template project

All projects

All items

Default templates

User templates

Boot source available

Operating system

CentOS

Fedora

Other

RHEL

Windows

Workload

Desktop

High performance


Server

Default templates

Q Filter by keyword...

13 items

Source available



CentOS Stream 8 VM

centos-stream8-server-small

Project openshift


Boot source PVC (auto import)

Workload Server

CPU 1

Memory 2 GiB

Source available



CentOS Stream 9 VM

centos-stream9-server-small

Project openshift


Boot source PVC (auto import)

Workload Server

CPU 1

Memory 2 GiB

Source available



CentOS 7 VM

centos7-server-small

Project openshift


Boot source PVC (auto import)

Workload Server

CPU 1

Memory 2 GiB

Source available



Fedora VM

fedora-server-small

Project openshift


Boot source PVC (auto import)

Workload Server

CPU 1

Memory 2 GiB

Source available



Red Hat Enterprise Linux 7 VM

rhel7-server-small

Project openshift


Boot source PVC (auto import)

Workload Server

CPU 1

Memory 2 GiB

Source available



Red Hat Enterprise Linux 8 VM

rhel8-server-small

Project openshift


Boot source PVC (auto import)

Workload Server

CPU 1

Memory 2 GiB

Source available



Red Hat Enterprise Linux 9 VM

rhel9-server-small

Project openshift


Boot source PVC (auto import)

Workload Server

CPU 1

Memory 2 GiB

Source available



Microsoft Windows 10 VM

windows10-desktop-medium

Project openshift


Boot source PVC

Workload Desktop

CPU 1

Memory 4 GiB

Source available



Microsoft Windows 11 VM

windows11-desktop-medium

Project openshift


Boot source PVC

Workload Desktop

CPU 2

Memory 4 GiB

Source available



Microsoft Windows Server 2012 R2 VM

windows2k12r2-server-medium

Project openshift

Boot source PVC

Workload Server

CPU 1

Memory 4 GiB

202



CentOS Stream 9 VM

centos-stream9-server-small



Template info

Operating system

CentOS Stream 9 VM

Workload type

Server (default)

Description

Template for CentOS Stream 9 VM or newer. A PVC with the CentOS Stream disk image must be available.

Documentation

[Refer to documentation](#)

CPU | Memory

1 CPU | 2 GiB Memory

Network interfaces (1)

Name	Network	Type
default	Pod networking	Masquerade

Disks (2)

Name	Drive	Size
rootdisk	Disk	30 GiB
cloudinitdisk	Disk	-

Hardware devices (0)

GPU devices

Not available

Host devices

Not available

Quick create VirtualMachine

VirtualMachine name *

centos-stream9-pleased-ham...

Project

openshift-virtualization-os-images

☒ Start this VirtualMachine after creation

Quick create VirtualMachine

Customize VirtualMachine

Cancel

Activate Windows

Go to Settings to activate Windows.

Project: openshift-virtualization-os-images

Catalog > Customize template parameters > Customize VirtualMachine

Customize and create VirtualMachine

Template: CentOS Stream 9 VM

Overview YAML Scheduling Environment Network interfaces Disks Scripts Metadata

Name
centos-stream9-pleased-hamster

Namespace
openshift-virtualization-os-images

Description
Not available

Operating system
CentOS Stream 9 VM

CPU | Memory
1 CPU | 2 GiB Memory

Machine type
pc-q35-rhel9.2.0

Boot mode
BIOS

Start in pause mode
☐

Workload profile
Server

Network interfaces (1)

Name	Network	Type
default	Pod networking	Masquerade

Disks (2)

Name	Drive	Size
rootdisk	Disk	30 GiB
cloudinitdisk	Disk	-

Hardware devices

GPU devices
Not available

Host devices
Not available

Headless mode
☐

Hostname
centos-stream9-pleased-hamster

☒ Start this VirtualMachine after creation

Create VirtualMachine Cancel

VirtualMachines > VirtualMachine details

VM centos-stream9-zealous-anaconda Running YAML Actions

Overview Details Metrics **Configuration** Events Console Snapshots Diagnostics

Disks +

Add disk

Filter Search by name... Mount Windows drivers disk

Name	Source	Size	Drive	Interface	Storage class
cloudinitdisk	Other	-	Disk	virtio	-
data-disk Persistent Hotplug	PVC centos-stream9-zealous-anaconda-data-disk	30.00 GiB	Disk	SCSI	ontap-san-block
rootdisk bootable	PVC centos-stream9-zealous-anaconda	30.00 GiB	Disk	virtio	ontap-san-block

File systems

Name	File system type	Mount point	Total bytes	Used bytes
vdal	xfs	/	29.94 GiB	1.30 GiB

ワークフロー：NetApp ONTAP を使用した Red Hat OpenShift Virtualization

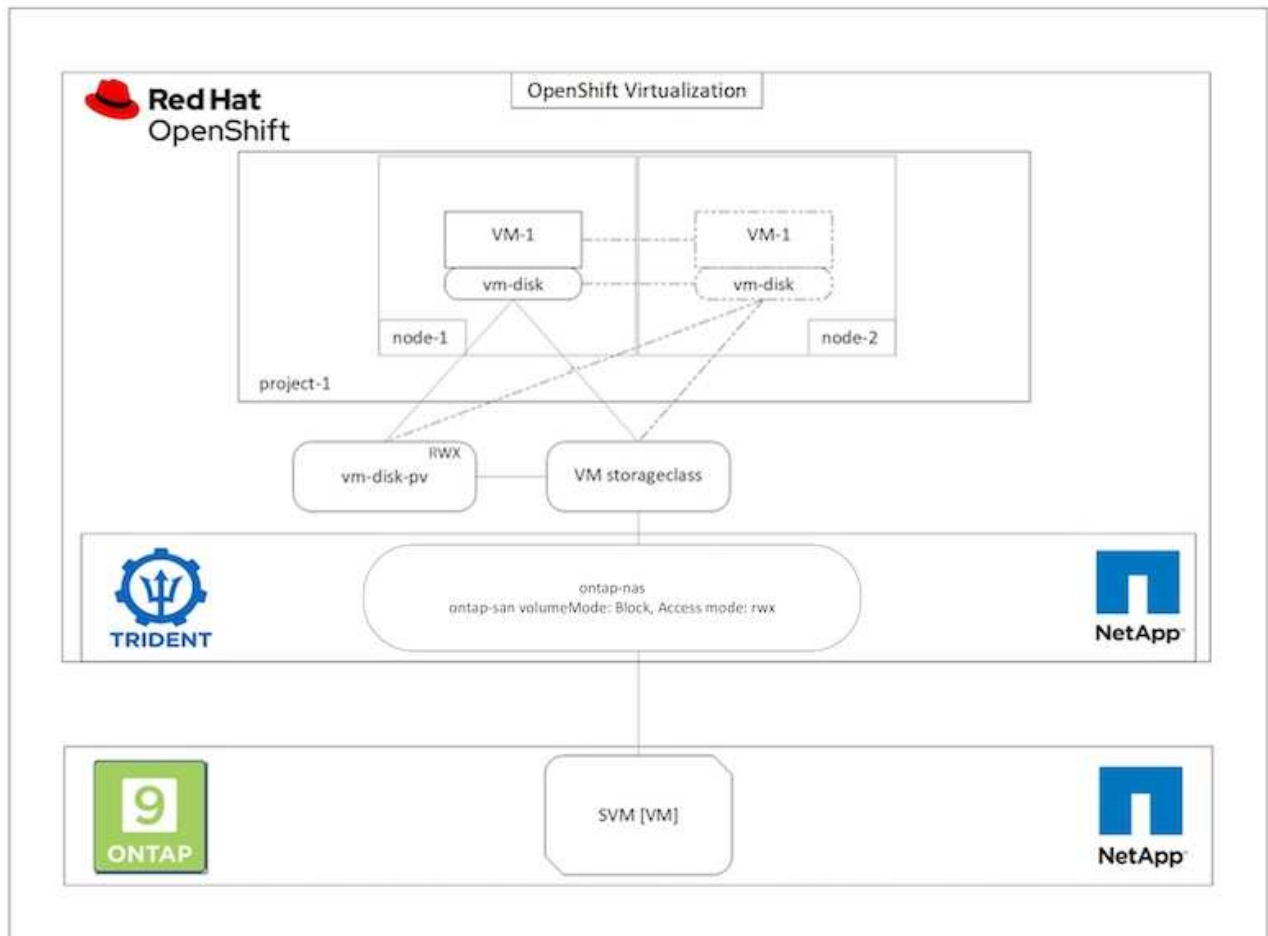
このセクションでは、クラスタ内のノード間でOpenShift Virtualizationで仮想マシンを移行する方法を説明します。

VM ライブマイグレーション

ライブマイグレーションは、OpenShift クラスタ内の 1 つのノードから別のノードに VM インスタンスをダ

ウンタイムなしで移行するプロセスです。OpenShift クラスターでライブマイグレーションを実行するには、VM を共有 ReadWriteAny アクセスモードの PVC にバインドする必要があります。ONTAPを使用して構成されたAstra Tridentバックエンド- NASドライバは、ファイルシステムプロトコルNFSとSMBのRWXアクセスモードをサポートします。のドキュメントを参照してください ["こちらをご覧ください"](#)。ONTAP SANドライバを使用して構成されたAstra Tridentバックエンドは、iSCSIプロトコルとNVMe/TCPプロトコルでブロックボリュームモードのRWXアクセスモードをサポートします。のドキュメントを参照してください ["こちらをご覧ください"](#)。

そのため、ライブマイグレーションを成功させるには、ONTAP-NASまたはONTAP-SAN（volumeMode：Block）ストレージクラスを使用して、PVCを含むVMをディスク（ブートディスクと追加のホットプラグディスク）でプロビジョニングする必要があります。PVCが作成されると、TridentはNFS対応またはiSCSI対応のSVMにONTAPボリュームを作成します。



以前に作成され、実行中の状態にあるVMのライブマイグレーションを実行するには、次の手順を実行します。

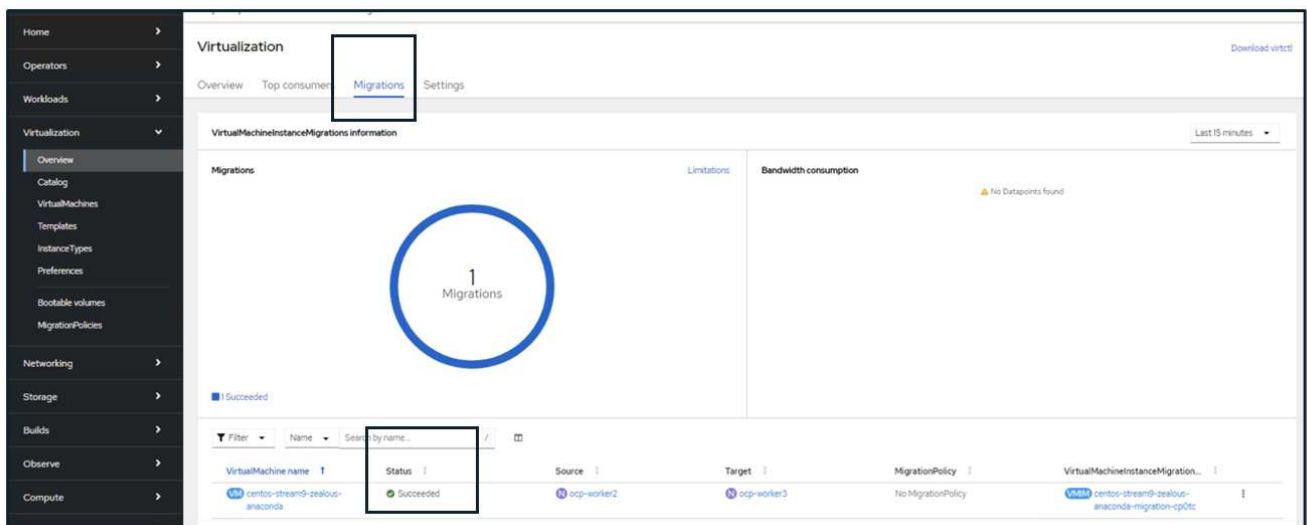
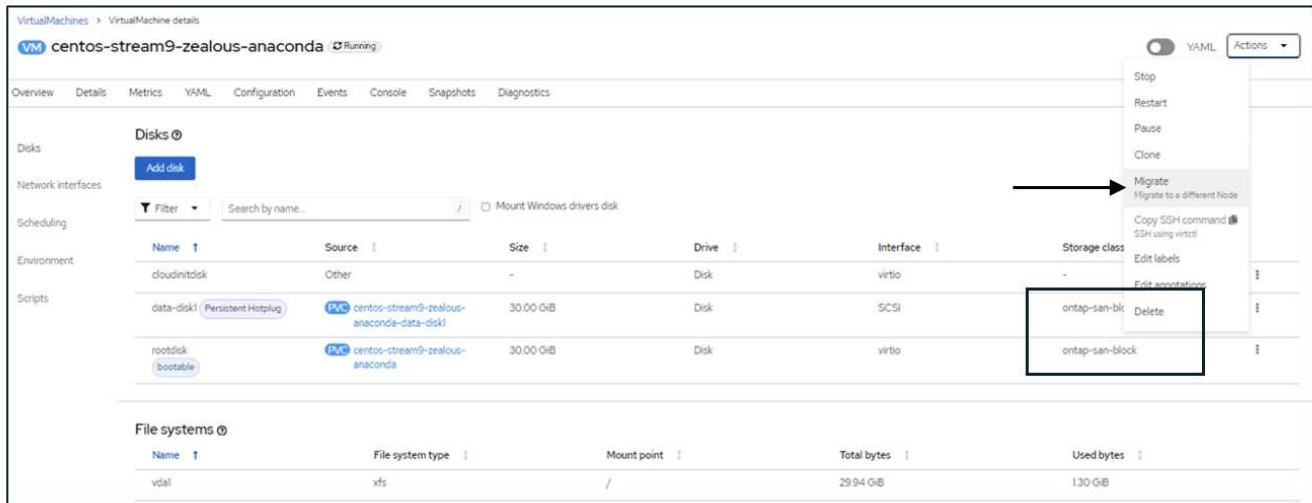
1. ライブマイグレーションするVMを選択します。
2. [Configuration]*タブをクリックします。
3. RWXアクセスモードをサポートできるストレージクラスを使用して、VMのすべてのディスクが作成されていることを確認します。
4. 右隅の*をクリックし、[Migrate]*を選択します。

5. 移行の進行状況を確認するには、左側のメニューで[Virtualization]>[Overview]に移動し、*[Migrations]タブをクリックします。

VMの移行は、*保留中*から*スケジュール設定*に*成功*に移行します。



OpenShift クラスタ内の VM インスタンスは、evictionStrategy が LiveMigrate に設定されている場合、元のノードがメンテナンスモードになると、自動的に別のノードに移行します。



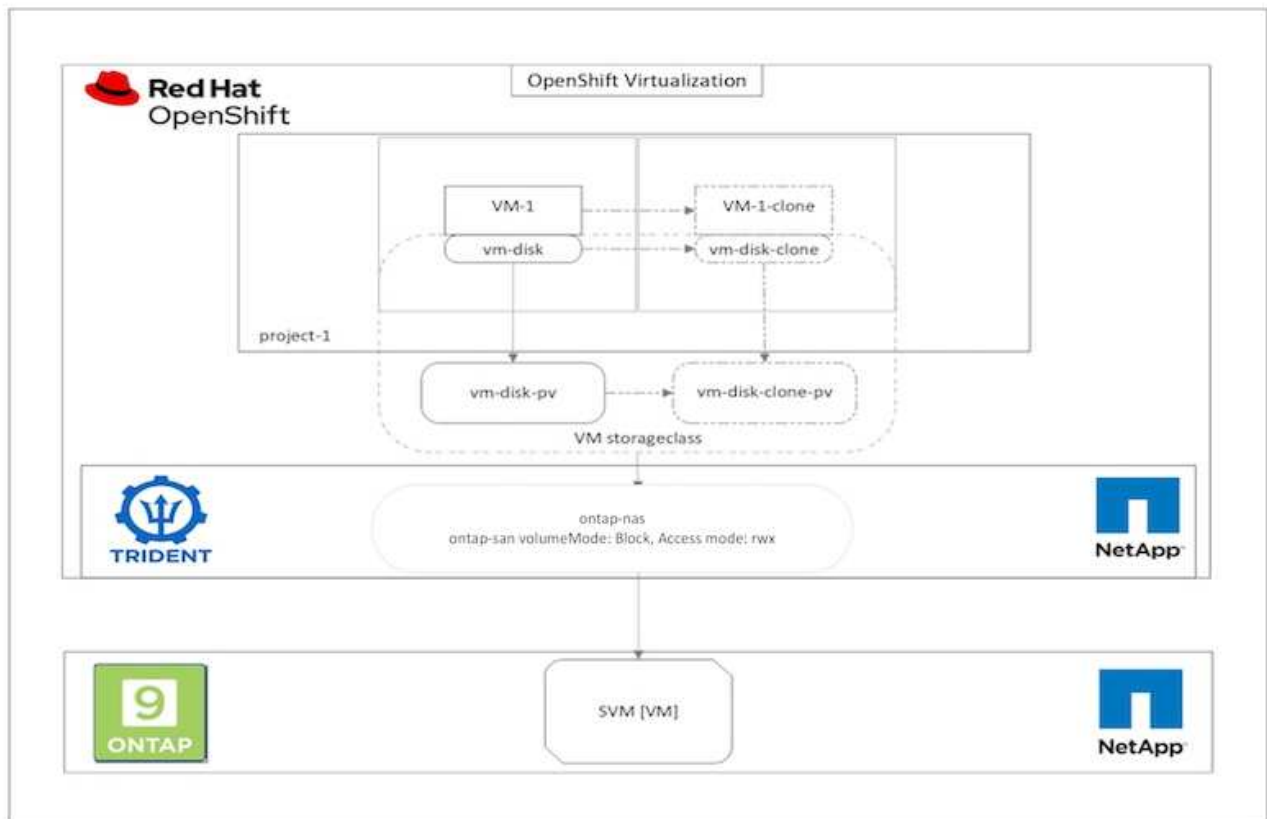
ワークフロー：NetApp ONTAP を使用した Red Hat OpenShift Virtualization

このセクションでは、Red Hat OpenShift Virtualizationを使用して仮想マシンをクローニングする方法について説明します。

VM のクローニング

OpenShift で既存の VM をクローニングするには、Astra Trident の Volume CSI クローニング機能をサポートします。CSI ボリュームクローニングでは、PV を複製することによって、既存の PVC をデータソースとし

て使用して新しい PVC を作成できます。新しい PVC が作成されると、その PVC は独立したエンティティとして機能し、送信元 PVC へのリンクや依存関係はありません。



CSI ボリュームクローニングには、次のような一定の制限事項があります。

1. 送信元 PVC と宛先 PVC は同じプロジェクト内に存在する必要があります。
2. クローニングは、同じストレージクラス内でサポートされます。
3. クローニングを実行できるのは、ソースボリュームとデスティネーションボリュームで同じボリュームモード設定を使用している場合のみです。たとえば、ブロックボリュームは別のブロックボリュームにしかクローニングできません。

OpenShift クラスタ内の VM は、次の 2 つの方法でクローニングできます。

1. ソース VM をシャットダウンします
2. ソース VM を稼働させます

ソース **VM** をシャットダウンします

VM をシャットダウンして既存の VM をクローニングすることは、Astra Trident のサポートとともに実装されるネイティブの OpenShift 機能です。VM をクローニングするには、次の手順を実行します。

1. [Workloads (ワークロード)] > [Virtualization (仮想化)] > [Virtual Machines (仮想マシン)] に移動し、クローンを作成する仮想マシンの横にある省略記号をクリックします。
2. Clone Virtual Machine をクリックして、新しい VM の詳細を指定します。

Clone Virtual Machine

Name *

rhel8-short-frog-clone

Description

Namespace *

default

☒ Start virtual machine on clone

Configuration

Operating System

Red Hat Enterprise Linux 8.0 or higher

Flavor

Small: 1 CPU | 2 GiB Memory

Workload Profile

server

NICs

default - virtio

Disks

cloudinitdisk - cloud-init disk

rootdisk - 20Gi - basic



The VM rhel8-short-frog is still running. It will be powered off while cloning.

Cancel

Clone Virtual Machine

3. Clone Virtual Machine をクリックします。これにより、ソース VM がシャットダウンされ、クローン VM の作成が開始されます。
4. この手順が完了すると、クローニングした VM のコンテンツにアクセスして確認できるようになります。

ソース VM を稼働させます

既存の VM は、ソース VM の既存の PVC をクローニングしてから、クローン PVC を使用して新しい VM を作成することによってもクローニングできます。この方法では、ソース VM をシャットダウンする必要はありません。シャットダウンせずに VM をクローニングするには、次の手順を実行します。

1. Storage > PersistentVolume要求 と進み、ソース VM に接続されている PVC の横にある省略記号をクリックします。
2. Clone PVC をクリックして、新しい PVC の詳細を提供します。

Clone

Name *

rhel8-short-frog-rootdisk-28dvv-clone

Access Mode *

☐ Single User (RWO) ☒ Shared Access (RWX) ☐ Read Only (ROX)


Size *

20

GiB

PVC details

Namespace

 default

Requested capacity

20 GiB

Access mode

Shared Access (RWX)

Storage Class

 basic

Used capacity

2.2 GiB

Volume mode

Filesystem

Cancel

Clone

3. 次に、Clone をクリックします。これにより、新しい VM の PVC が作成されます。
4. [Workloads (ワークロード)] > [Virtualization (仮想化)] > [Virtual Machines (仮想マシン)] に移動し、[Create (作成)]
5. spec> template> spec> volumes セクションで、コンテナディスクではなく、クローン PVC を接続します。新しい VM について、要件に応じてその他の詳細をすべて指定します。

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dvvb-clone
```

6. Create をクリックして、新しい VM を作成します。
7. VM が作成されたら、にアクセスし、新しい VM がソース VM のクローンであることを確認します。

ワークフロー： NetApp ONTAP を使用した Red Hat OpenShift Virtualization

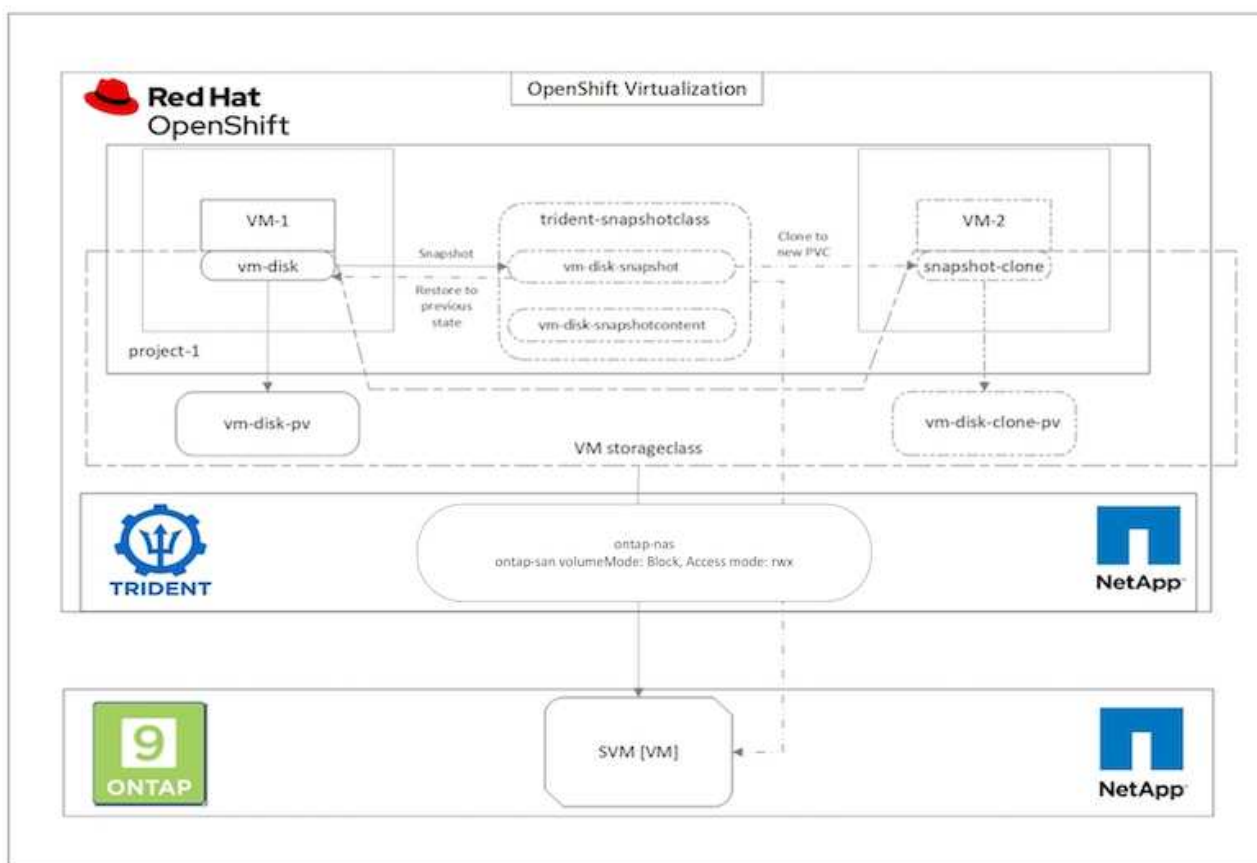
このセクションでは、Red Hat OpenShift Virtualizationを使用してSnapshotから仮想マシンを作成する方法を説明します。

Snapshot から VM を作成します

Astra Trident と Red Hat OpenShift を使用すると、ユーザは、プロビジョニングされたストレージクラス上の永続的ボリュームのスナップショットを作成できます。この機能を使用すると、ボリュームのポイントインタイムコピーを作成して、そのコピーを使用して新しいボリュームを作成したり、同じボリュームを以前の状態にリストアしたりできます。これにより、ロールバックからクローン、データリストアまで、さまざまなユースケースを実現またはサポートできます。

OpenShift で Snapshot 処理を実行するには、リソース VolumeSnapshotClass、VolumeSnapshot、および VolumeSnapshotContent を定義する必要があります。

- VolumeSnapshotContent は、クラスタ内のボリュームから作成された実際の Snapshot です。このデータストアは、Storage 用の PersistentVolume に似た、クラスタ全体のリソースです。
- ボリューム Snapshot は、ボリュームの Snapshot 作成要求です。これは、PersistentVolumeClaim に似ています。
- VolumeSnapshotClass を使用すると、管理者はボリューム Snapshot のさまざまな属性を指定できます。これにより、同じボリュームから作成された異なる Snapshot に対して異なる属性を設定できます。



VM の Snapshot を作成するには、次の手順を実行します。

1. ボリューム Snapshot を作成するために使用できるボリューム Snapshot クラスを作成します。Storage > VolumeSnapshotClasses の順に移動し、Create VolumeSnapshotClass をクリックします。
2. スナップショットクラスの名前を入力し、ドライバの `csi.trident.netapp.io` を入力して、Create をクリックします。

```
1  apiVersion: snapshot.storage.k8s.io/v1
2  kind: VolumeSnapshotClass
3  metadata:
4    name: trident-snapshot-class
5  driver: csi.trident.netapp.io
6  deletionPolicy: Delete
7
```

[Create](#)[Cancel](#)[Download](#)

3. ソース VM に接続されている PVC を特定し、その PVC の Snapshot を作成します。「ストレージ」>「ボリュームスナップショット」と選択し、「ボリュームスナップショットの作成」をクリックします。
4. Snapshot を作成する PVC を選択し、Snapshot の名前を入力するか、デフォルトを受け入れて、適切な VolumeSnapshotClass を選択します。[作成] をクリックします。

Create VolumeSnapshot

[Edit YAML](#)

PersistentVolumeClaim *

PVC rhel8-short-frog-rootdisk-28dvb ▼

Name *

rhel8-short-frog-rootdisk-28dvb-snapshot

Snapshot Class *

VSC trident-snapshot-class ▼

[Create](#)[Cancel](#)

5. これにより、その時点で PVC のスナップショットが作成されます。

スナップショットから新しい **VM** を作成します

1. 最初に、スナップショットを新しい PVC に復元します。Storage > VolumeSnapshots と進み、リストアする Snapshot の横にある省略記号をクリックして、Restore as new PVC（新しい PVC として復元）をクリックします。
2. 新しい PVC の詳細を入力し、Restore をクリックします。これにより、新しい PVC が作成されます。

Restore as new PVC

When restore action for snapshot **rhel8-short-frog-rootdisk-28dvb-snapshot** is finished a new crash-consistent PVC copy will be created.

Name *

rhel8-short-frog-rootdisk-28dvb-snapshot-restore

Storage Class *

 basic

Access Mode *

☐ Single User (RWO) ☒ Shared Access (RWX) ☐ Read Only (ROX)

Size *

20

GiB

VolumeSnapshot details

Created at

 May 21, 12:46 am

Namespace

 default

Status

 Ready

API version

snapshot.storage.k8s.io/v1

Size

20 GiB

3. 次に、この PVC から新しい VM を作成します。[Virtualization]>[Virtual Machines]に移動し、[Create]>[With YAML]をクリックします。

4. `spec>template>spec>volumes` セクションで、コンテナディスクからではなく、スナップショットから作成された新しい PVC を指定します。新しい VM について、要件に応じてその他の詳細をすべて指定します。

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dvv-snapshot-restore
```

5. Create をクリックして、新しい VM を作成します。
6. VM が正常に作成されたら、にアクセスして、新しい VM の状態が、スナップショット作成時に PVC を使用してスナップショットを作成した VM の状態と同じであることを確認します。

ワークフロー：NetApp ONTAP を使用した Red Hat OpenShift Virtualization

このセクションでは、Red Hat OpenShift Virtualizationマイグレーションツールキットを使用して、VMwareからOpenShiftクラスタに仮想マシンを移行する方法について説明します。

仮想化向け移行ツールキットを使用したVMwareからOpenShiftによる仮想化へのVMの移行

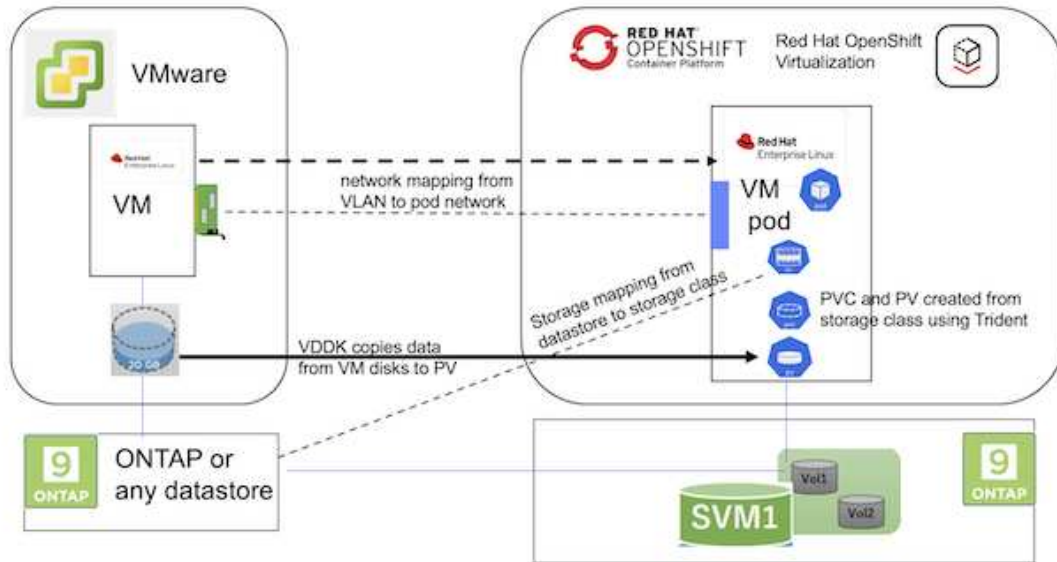
このセクションでは、仮想化向け移行ツールキット（MTV）を使用して、VMwareからOpenShift Containerプラットフォームで実行されるOpenShift仮想化に仮想マシンを移行し、Astra Tridentを使用してNetApp ONTAPストレージと統合する方法を説明します。

次のビデオでは、永続的ストレージ用のONTAP-SANストレージクラスを使用して、VMwareからOpenShiftによる仮想化にRHEL VMを移行するデモを示します。

Red Hat MTVを使用したNetApp ONTAPストレージによるOpenShift仮想化へのVMの移行

次の図は、VMwareからRed Hat OpenShift VirtualizationへのVMの移行の概要を示しています。

Migration of VM from VMware to OpenShift Virtualization



サンプル移行の前提条件

VMware環境

- 次の構成のRHEL 9.3を使用するRHEL 9 VMをインストールしました。
 - CPU：2、メモリ：20 GB、ハードディスク：20 GB
 - ユーザクレデンシャル：rootユーザとadminユーザのクレデンシャル
- VMの準備が完了したら、PostgreSQLサーバがインストールされました。
 - PostgreSQLサーバが起動され、起動時に起動できるようになりました

```
systemctl start postgresql.service`  
systemctl enable postgresql.service  
The above command ensures that the server can start in the VM in  
OpenShift Virtualization after migration
```

- 2つのデータベース、1つのテーブル、および1つの行が追加されました。を参照してください "[こちらをご覧ください](#)" RHELにPostgreSQLサーバをインストールし、データベースエントリとテーブルエントリを作成する手順については、を参照してください。



PostgreSQLサーバを起動し、起動時にサービスを開始できるようにしてください。

OpenShiftクラスタ上

MTVをインストールする前に、次のインストールが完了しました。

- OpenShiftクラスタ4.13.34

- ["Astra Trident 23.10"](#)
- クラスタノードのマルチパスがiSCSIに対して有効になっている（ONTAP-SANストレージクラス用）。クラスタ内の各ノードでiSCSIを有効にするデーモンセットを作成するには、提供されているYAMLを参照してください。
- iSCSIを使用するONTAP SAN向けのTridentバックエンドおよびストレージクラス。Tridentバックエンドとストレージクラス用に提供されているYAMLファイルを参照してください。
- ["OpenShift 仮想化"](#)

OpenShiftクラスタノードにiSCSIとマルチパスをインストールするには、以下のYAMLファイルを使用します。
クラスタノードを**iSCSI**用に準備しています

```
apiVersion: apps/v1
kind: DaemonSet
metadata:
  namespace: trident
  name: trident-iscsi-init
  labels:
    name: trident-iscsi-init
spec:
  selector:
    matchLabels:
      name: trident-iscsi-init
  template:
    metadata:
      labels:
        name: trident-iscsi-init
    spec:
      hostNetwork: true
      serviceAccount: trident-node-linux
      initContainers:
        - name: init-node
          command:
            - nsenter
            - --mount=/proc/1/ns/mnt
            - --
            - sh
            - -c
          args: ["$(STARTUP_SCRIPT)"]
          image: alpine:3.7
          env:
            - name: STARTUP_SCRIPT
              value: |
                #!/bin/bash
                sudo yum install -y lsscsi iscsi-initiator-utils sg3_utils
                device-mapper-multipath
```

```

        rpm -q iscsi-initiator-utils
        sudo sed -i 's/^\(node.session.scan\).*\/\1 = manual/'
/etc/iscsi/iscsid.conf
        cat /etc/iscsi/initiatorname.iscsi
        sudo mpathconf --enable --with_multipathd y --find_multipaths
n
        sudo systemctl enable --now iscsid multipathd
        sudo systemctl enable --now iscsi

securityContext:
  privileged: true
hostPID: true
containers:
- name: wait
  image: k8s.gcr.io/pause:3.1
hostPID: true
hostNetwork: true
tolerations:
- effect: NoSchedule
  key: node-role.kubernetes.io/master
updateStrategy:
  type: RollingUpdate

```

次のYAMLファイルを使用して、ONTAP SANストレージを使用するためのTridentバックエンド構成を作成
iSCSI向けTridentバックエンド

```

apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-san-secret
type: Opaque
stringData:
  username: <username>
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-san
spec:
  version: 1
  storageDriverName: ontap-san
  managementLIF: <management LIF>
  backendName: ontap-san
  svm: <SVM name>
  credentials:
    name: backend-tbc-ontap-san-secret

```

次のYAMLファイルを使用して、ONTAP SANストレージを使用するためのTridentストレージクラス構成を作成

iSCSI用のTridentストレージクラス

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-san
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true

```

* MTVのインストール*

これで、Migration Toolkit for Virtualization (MTV) をインストールできます。付属の説明書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。

Migration Toolkit for Virtualization (MTV) ユーザーインターフェイスは、OpenShift Webコンソールに統合されています。

次を参照できます。 ["こちらをご覧ください"](#) さまざまなタスクのユーザーインターフェイスの使用を開始します。

ソースプロバイダの作成

RHEL VMをVMwareからOpenShift Virtualizationに移行するには、まずVMwareのソースプロバイダを作成する必要があります。手順を参照してください ["こちらをご覧ください"](#) ソースプロバイダを作成します。

VMwareソースプロバイダを作成するには、次のものがが必要です。

- vCenter URL
- vCenterクレデンシャル
- vCenter Serverサムプリント
- リポジトリ内のVDDKイメージ

ソースプロバイダの作成例：

The screenshot displays the 'Add provider' configuration page for a VMware source. The 'Select provider type' dropdown is set to 'vSphere'. The 'Provider resource name' is 'vmware-source'. The 'URL' field is empty, with a note that it should include the '/sdk' path. The 'VDDK init image' is 'docker.repo.eng.netapp.com/banum/vddk:601'. The 'Username' is 'administrator@vsphere.local' and the 'Password' is masked. The 'SSHA-1 fingerprint' field is empty. The 'Skip certificate validation' checkbox is checked.

Select provider type *

vm vSphere

Provider resource name *

vmware-source

Unique Kubernetes resource name identifier

URL *

URL of the vCenter SDK endpoint. Ensure the URL includes the "/sdk" path. For example: https://vCenter-host-example.com/sdk

VDDK init image

docker.repo.eng.netapp.com/banum/vddk:601

VDDK container image of the provider, when left empty some functionality will not be available

Username *

administrator@vsphere.local

vSphere REST API user name.

Password *

.....

vSphere REST API password credentials.

SSHA-1 fingerprint *

The provider currently requires the SHA-1 fingerprint of the vCenter Server's TLS certificate in all circumstances. vSphere calls this the server's thumbprint.

Skip certificate validation

☒



Migration Toolkit for Virtualization (MTV) では、VMware Virtual Disk Development Kit (VDDK) SDKを使用して、VMware vSphereからの仮想ディスクの転送を高速化します。そのため、VDDKイメージはオプションですが作成することを強くお勧めします。この機能を使用するには、VMware Virtual Disk Development Kit (VDDK) をダウンロードし、VDDKイメージをビルドして、VDDKイメージをイメージレジストリにプッシュします。

表示される指示に従います。"こちらをご覧ください" VDDKイメージを作成して、OpenShiftクラスタからアクセス可能なレジストリにプッシュします。

送信先プロバイダの作成

OpenShift仮想化プロバイダがソースプロバイダであるため、ホストクラスタが自動的に追加されます。

移行計画の作成

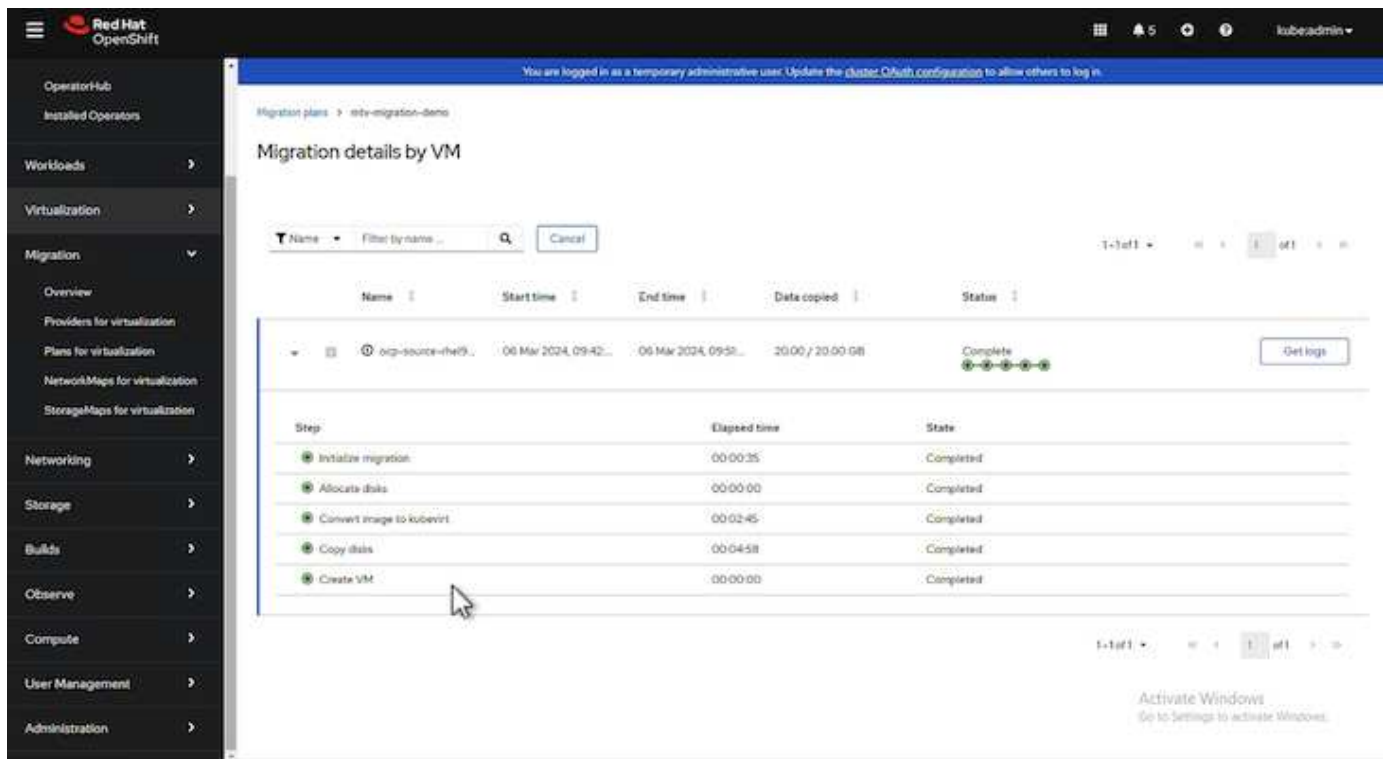
表示される指示に従います。"こちらをご覧ください" をクリックして移行計画を作成します。

まだ計画を作成していない場合は、計画の作成時に次のものを作成する必要があります。

- ソースネットワークをターゲットネットワークにマッピングするネットワークマッピング。
 - ソースデータストアをターゲットストレージクラスにマッピングするストレージマッピング。このためには、ONTAP-SANストレージクラスを選択できます。
- 移行計画が作成されると、計画のステータスが*準備完了*と表示され、計画を*開始*できるようになります。

Name	Source	Target	VMs	Status	Description
mtv-migration-demo	vmware	host	1	Ready	Plan for migrating VM to OpenShift Virt...
vmware-osv-migration	vmware2	host	1	Succeeded 1 of 1 VMs migrated	Migrating RHEL 9 vm to OpenShift Virtu...
vmware-osv-migration-plan1	vmware2	host	1	Succeeded 1 of 1 VMs migrated	
vmware-osv-migration-plan2	vmware2	host	1	Succeeded 1 of 1 VMs migrated	migrating RHEL 9 vm using ONTAP NFS...

[Start]*をクリックすると、VMの移行が完了するまでの一連の手順が実行されます。



すべての手順が完了したら、左側のナビゲーションメニューの*[仮想マシン]*をクリックすると、移行されたVMが表示されます。

仮想マシンへのアクセス手順が記載されています。 ["こちらをご覧ください"](#)。

仮想マシンにログインして、postgresqlデータベースの内容を検証できます。データベース、テーブル、およびテーブル内のエントリは、ソースVMで作成されたものと同じである必要があります。

サードパーティツールを使用したVMのデータ保護

OpenShift API for Data Protection (OADP) を使用した**OpenShift Virtualization**でのVMのデータ保護

作成者：Banu Sundhar、NetApp

このセクションでは、NetApp ONTAP S3またはNetApp StorageGRID S3上のVeleroでOpenShift API for Data Protection (OADP) を使用してVMのバックアップを作成する方法について詳しく説明します。VMディスクの永続的ボリューム (PV) のバックアップは、CSIのAstra Trident Snapshotを使用して作成されます。

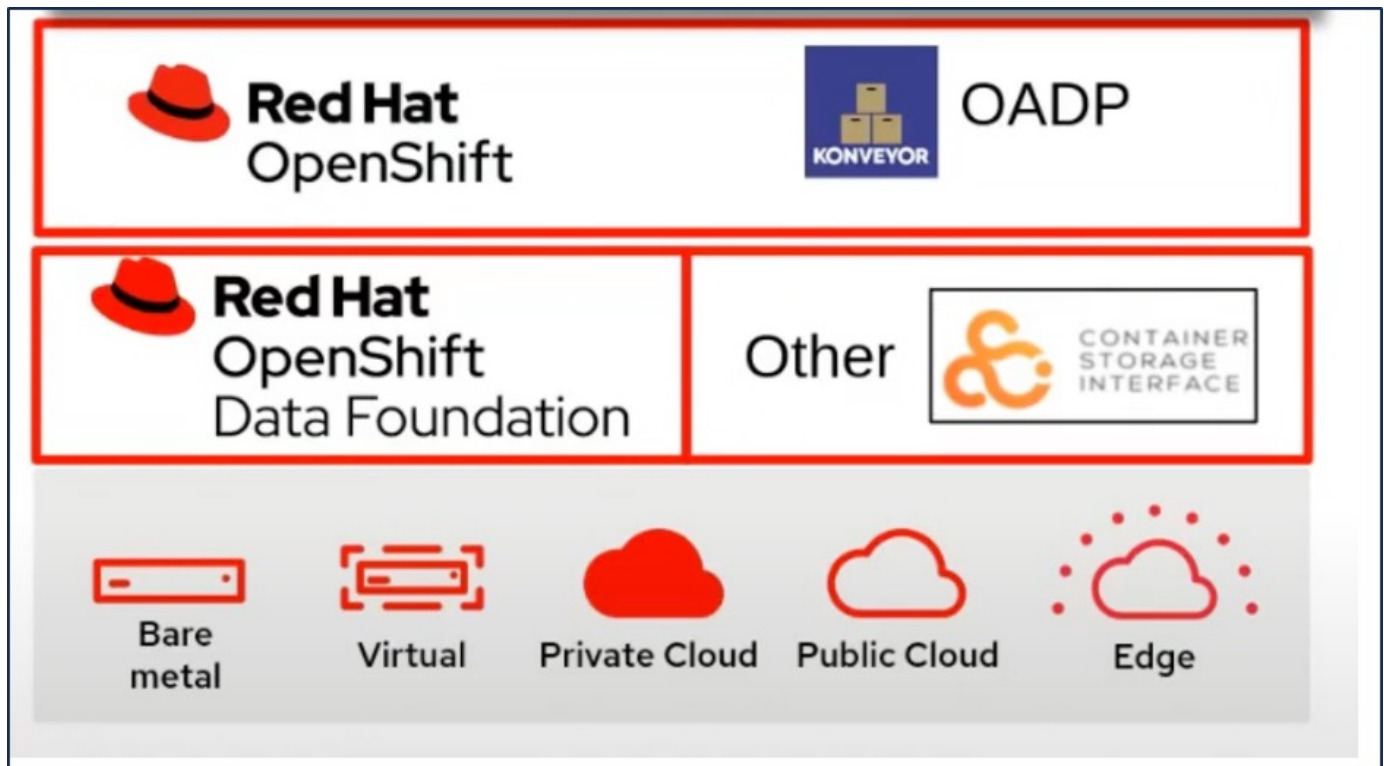
OpenShift仮想化環境の仮想マシンは、OpenShift Containerプラットフォームのワーカーノードで実行されるコンテナ化されたアプリケーションです。VMメタデータとVMの永続ディスクを保護して、VMが失われたり破損したりした場合にリカバリできるようにすることが重要です。

OpenShift仮想化VMの永続ディスクは、次のコマンドを使用してOpenShiftクラスタに統合されたONTAPストレージによってバックアップできます。 ["Astra Trident CSI"](#)。このセクションでは、 ["OpenShift API for Data Protection \(OADP\)"](#) データボリュームを含むVMのバックアップを

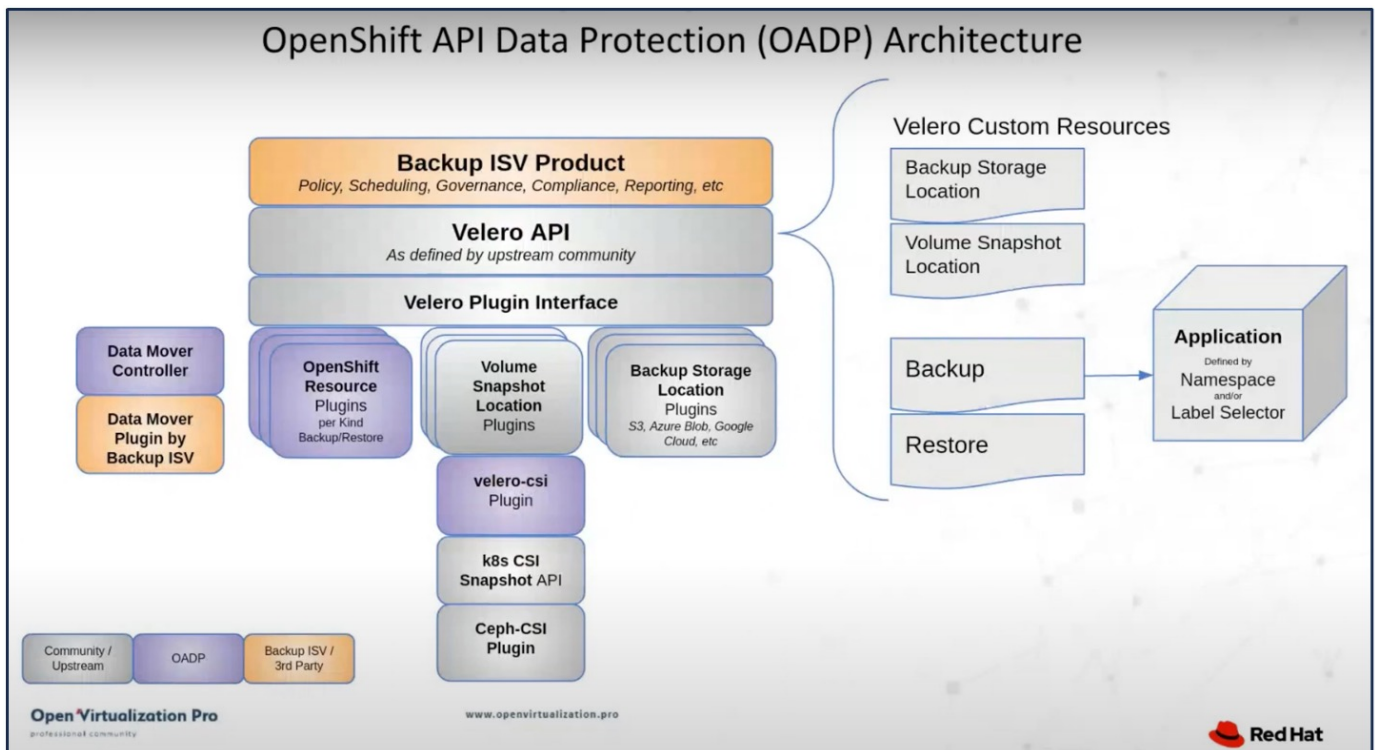
- ONTAPオブジェクトストレージ
- StorageGRID

その後、必要に応じてバックアップからリストアします。

OADPを使用すると、OpenShiftクラスタ上のアプリケーションのバックアップ、リストア、ディザスタリカバリを実行できます。OADPで保護できるデータには、Kubernetesリソースオブジェクト、永続ボリューム、内部イメージなどがあります。



Red Hat OpenShiftは、OpenSourceコミュニティが開発したソリューションをデータ保護に活用しています。["ベレロカプセル"](#) は、安全なバックアップとリストア、ディザスタリカバリの実行、Kubernetesクラスタリソースと永続ボリュームの移行を行うためのオープンソースツールです。Veleroを簡単に使用するために、OpenShiftはCSIストレージドライバーと統合するためのOADPオペレーターとVeleroプラグインを開発しました。公開されるOADP APIのコアは、Velero APIに基づいています。OADPオペレータをインストールして設定すると、Velero APIで公開されている操作に基づいて実行できるバックアップ/リストア操作が実行されます。



OADP 1.3は、OpenShiftクラスタ4.12以降のOperator Hubから利用できます。CSIボリュームのスナップショットをリモートオブジェクトストアに移動できるData Moverが組み込まれています。これにより、バックアップ時にSnapshotをオブジェクトストレージの場所に移動することで、データのモビリティと保持性が向上します。作成したSnapshotは、災害後のリストアに使用できます。

このセクションの例で使用されている各種コンポーネントのバージョンは次のとおりです

- OpenShiftクラスタ4.14
- OpenShift VirtualizationをOperator経由でインストールRed Hatが提供するOpenShift Virtualization Operator
- Red Hatが提供するOADP Operator 1.13
- Linux版Velero CLI 1.13
- Astra Trident 24.02
- ONTAP 9.12

"Astra Trident CSI"

"OpenShift API for Data Protection (OADP) "

"ベレロカプセル"

OpenShift API for Data Protection (OADP) Operatorのインストール

このセクションでは、OpenShift API for Data Protection (OADP) Operatorのインストールについて説明します。

前提条件

- RHCOSワーカーノードを含むベアメタルインフラにインストールされたRed Hat OpenShiftクラスタ（バージョン4.12以降）

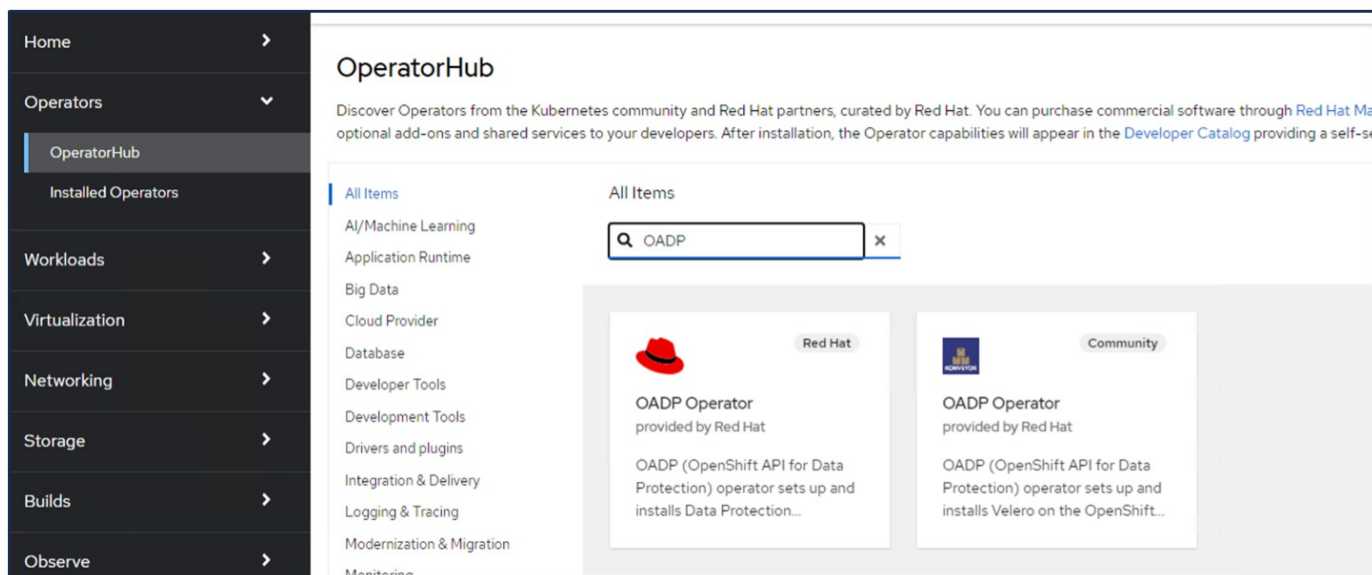
- Astra Tridentを使用してクラスタと統合されるNetApp ONTAPクラスタ
- ONTAP クラスタの SVM で設定された Trident バックエンド
- OpenShift クラスタ上でストレージクラスを構成し、Astra Trident をプロビジョニングツールとして提供
- クラスタに作成されたTrident Snapshotクラス
- Red Hat OpenShift クラスタへのクラスタ管理者アクセス
- NetApp ONTAP クラスタへの管理者アクセス
- OpenShift仮想化オペレータのインストールと設定
- OpenShift仮想化のネームスペースに導入されたVM
- tridentctl および OC ツールがインストールされている管理ワークステーション \$PATH に追加されました



実行状態のVMのバックアップを作成する場合は、その仮想マシンにQEMUゲストエージェントをインストールする必要があります。既存のテンプレートを使用してVMをインストールすると、QEMUエージェントが自動的にインストールされます。QEMUを使用すると、ゲストエージェントは、スナップショットプロセス中にゲストOSの転送中データを休止し、データの破損を回避できます。QEMUがインストールされていない場合は、バックアップを作成する前に仮想マシンを停止できます。

OADP Operatorのインストール手順

1. クラスタのOperator Hubに移動し、Red Hat OADP operatorを選択します。[Install]ページで、デフォルトの設定をすべて使用し、[install]をクリックします。次のページで、すべてのデフォルト値を使用して[インストール]をクリックします。OADP演算子は、ネームスペースOpenShift-ADPにインストールされます。





OADP Operator

1.3.0 provided by Red Hat

Install

Channel

stable-1.3

Version

1.3.0

Capability level

- ☒ Basic Install
- ☒ Seamless Upgrades
- ☐ Full Lifecycle
- ☐ Deep Insights
- ☐ Auto Pilot

Source

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected

OpenShift API for Data Protection (OADP) operator sets up and installs Velero on the OpenShift platform, allowing users to backup and restore applications.

Backup and restore Kubernetes resources and internal images, at the granularity of a namespace, using a version of Velero appropriate for the installed version of OADP.

OADP backs up Kubernetes objects and internal images by saving them as an archive file on object storage. OADP backs up persistent volumes (PVs) by creating snapshots with the native cloud snapshot API or with the Container Storage Interface (CSI). For cloud providers that do not support snapshots, OADP backs up resources and PV data with Restic or Kopia.






- [Installing OADP for application backup and restore](#)
- [Installing OADP on a ROSA cluster and using STS, please follow the Getting Started Steps 1-3 in order to obtain the role ARN needed for using the standardized STS configuration flow via OLM](#)
- [Frequently Asked Questions](#)

Project: All Projects

Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#) Operator and ClusterServiceVersion using the [Operator SDK](#).

Name Search by name...

Name	Namespace	Managed Namespaces	Status
 OpenShift Virtualization 4.14.4 provided by Red Hat	 openshift-cnv	 openshift-cnv	 Succeeded Up to date
 OADP Operator 1.3.0 provided by Red Hat	 openshift-adp	 openshift-adp	 Succeeded Up to date
 Package Server 0.0.1-snapshot provided by	 openshift-operator-lifecycle- manager	 openshift-operator-lifecycle- manager	 Succeeded

ONTAP S3を使用したVelero構成の前提条件

オペレータのインストールが成功したら、Veleroのインスタンスを設定します。

VeleroはS3互換オブジェクトストレージを使用するように設定できます。に示す手順に従って、ONTAP S3を設定します。"[ONTAPドキュメントのオブジェクトストレージの管理に関するセクション](#)"。Veleroと統合するには、ONTAP S3構成から次の情報が必要です。

- S3へのアクセスに使用できる論理インターフェイス（LIF）
- アクセスキーとシークレットアクセスキーを含むS3にアクセスするためのユーザクレデンシャル
- ユーザのアクセス権限があるバックアップ用のS3のバケット名
- オブジェクトストレージへのセキュアなアクセスを実現するには、TLS証明書をオブジェクトストレージサーバにインストールする必要があります。

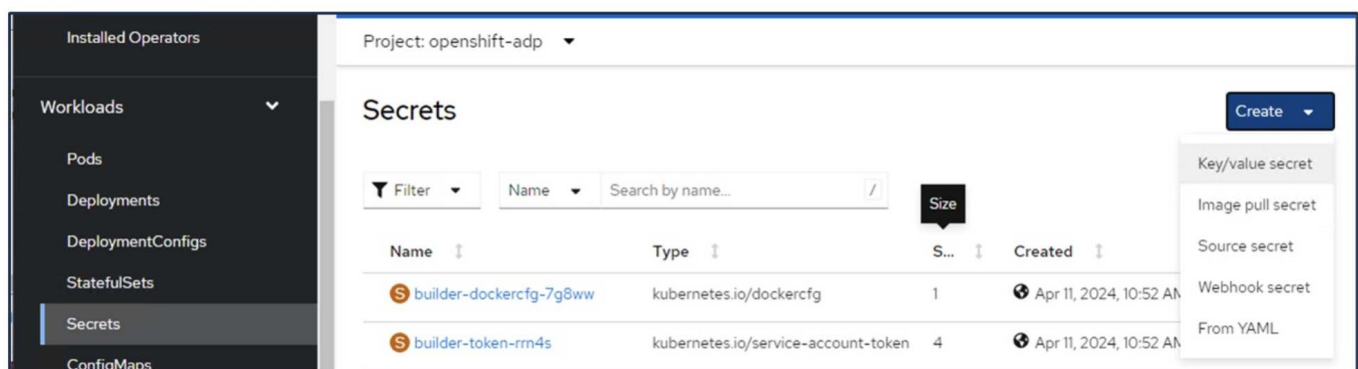
StorageGRID S3を使用したVelero構成の前提条件

VeleroはS3互換オブジェクトストレージを使用するように設定できます。StorageGRID S3は、の手順に従って設定できます。"[StorageGRIDのドキュメント](#)"。Veleroと統合するには、StorageGRID S3構成から次の情報が必要です。

- S3へのアクセスに使用できるエンドポイント
- アクセスキーとシークレットアクセスキーを含むS3にアクセスするためのユーザクレデンシャル
- ユーザのアクセス権限があるバックアップ用のS3のバケット名
- オブジェクトストレージへのセキュアなアクセスを実現するには、TLS証明書をオブジェクトストレージサーバにインストールする必要があります。

Veleroの設定手順

- 最初に、ONTAP S3ユーザクレデンシャルまたはStorageGRIDテナントユーザクレデンシャルのシークレットを作成します。これは、後でVeleroを設定するために使用します。シークレットは、CLIまたはWebコンソールから作成できます。
Webコンソールからシークレットを作成するには、[Secrets]を選択し、[Key/Value Secret]をクリックします。次の図に示すように、クレデンシャル名、キー、および値を指定します。必ずS3ユーザのアクセスキーIDとシークレットアクセスキーを使用してください。秘密に適切な名前を付けます。次の例では、ontap-s3-credentialsという名前のONTAP S3ユーザクレデンシャルを含むシークレットが作成されています。



Project: openshift-adp ▼

Edit key/value secret

Key/value secrets let you inject sensitive data into your application as files or environment variables.

Secret name *

ontap-s3-credentials

Unique name of the new secret.

Key *

cloud

Value

Drag and drop file with your value here or browse to upload it.

```
[default]
aws_access_key_id=
aws_secret_access_key=
```

[+ Add key/value](#)

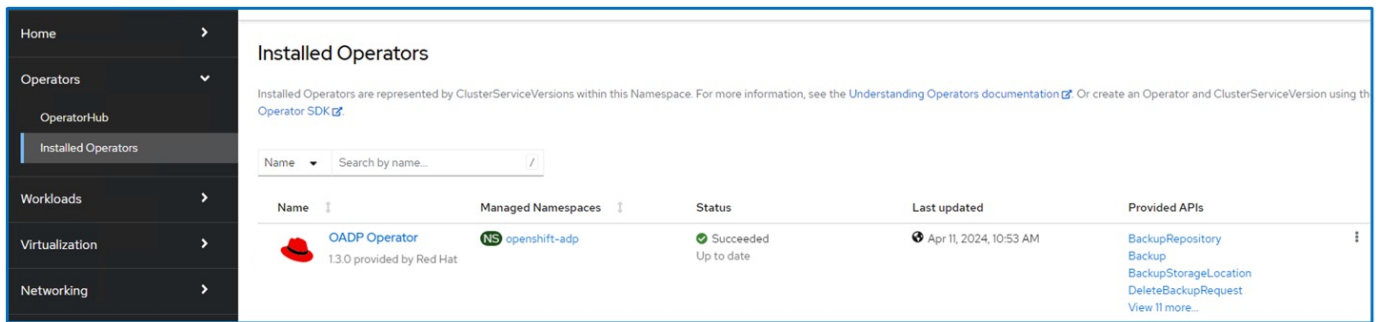
CLIからsg-s3-credentialsという名前のシークレットを作成するには、次のコマンドを使用します。

```
# oc create secret generic sg-s3-credentials --namespace openshift-adp --from-file
cloud=cloud-credentials.txt
```

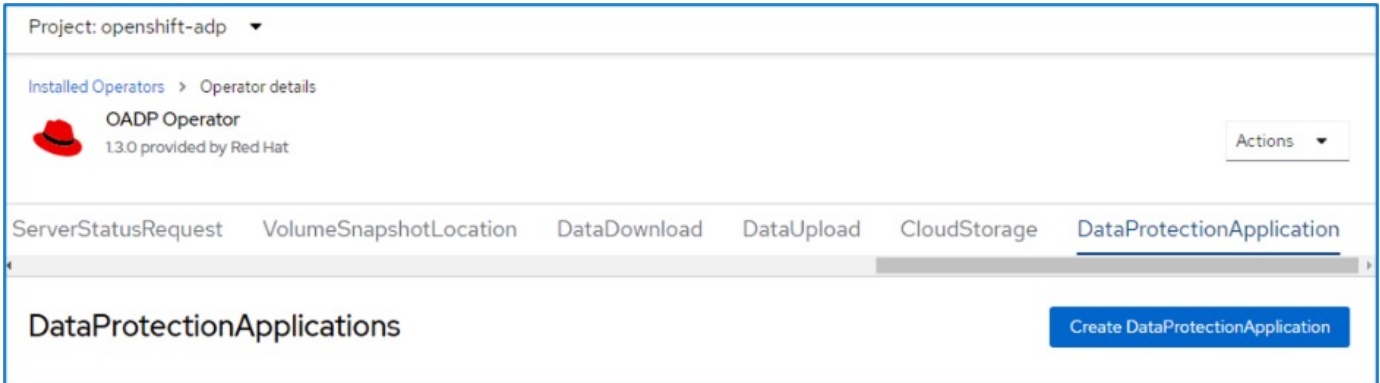
Where credentials.txt file contains the Access Key Id and the Secret Access Key of the S3 user in the following format:

```
[default]
aws_access_key_id=< Access Key ID of S3 user>
aws_secret_access_key=<Secret Access key of S3 user>
```

- 次に、Veleroを設定するには、[Operators]の下メニュー項目から[Installed Operators]を選択し、[OADP Operator]をクリックして、[DataProtectionApplication]タブを選択します。



[Create DataProtectionApplication]をクリックします。フォームビューで、DataProtectionアプリケーションの名前を指定するか、デフォルトの名前を使用します。



次に、YAMLビューに移動し、以下のYAMLファイルの例に示すように仕様情報を置き換えます。

バックアップの場所として**ONTAP S3**を使用して**Velero**を構成するためのサンプルYAMLファイル

```

spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'false' ->use this for https
communication with ONTAP S3
          profile: default
          region: us-east-1
          s3ForcePathStyle: 'True' ->This allows use of IP in s3URL
          s3Url: 'https://10.xx.xx.xx' ->LIF to access S3. Ensure TLS
certificate for S3 is configured
          credential:
            key: cloud
            name: ontap-s3-credentials ->previously created secret
          default: true
          objectStorage:
            bucket: velero ->Your bucket name previously created in S3 for
backups
            prefix: demobackup ->The folder that will be created in the
bucket
            provider: aws
          configuration:
            nodeAgent:
              enable: true
              uploaderType: kopia
              #default Data Mover uses Kopia to move snapshots to Object Storage
            velero:
              defaultPlugins:
                - csi ->Add this plugin
                - openshift
                - aws
                - kubevirt ->Add this plugin

```

- StorageGRID S3をBackupLocationおよびsnapshotLocationとして設定するためのサンプルYAMLファイル**


```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 ->region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' ->the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials ->secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

YAMLファイルのspecセクションは、上記の例のように、次のパラメータに対して適切に設定する必要があります。

バックアップの場所

ONTAP S3またはStorageGRID S3（クレデンシャルおよびYAMLに表示されるその他の情報）は、veleroのデフォルトのBackupLocationとして設定されます。

スナップショットの場所

Container Storage Interface（CSI）スナップショットを使用する場合は、CSIドライバを登録するためにVolumeSnapshotClass CRを作成するため、スナップショットの場所を指定する必要はありません。この例では、Astra Trident CSIを使用し、Trident CSIドライバを使用してVolumeSnapshotClass CRを作成しています。

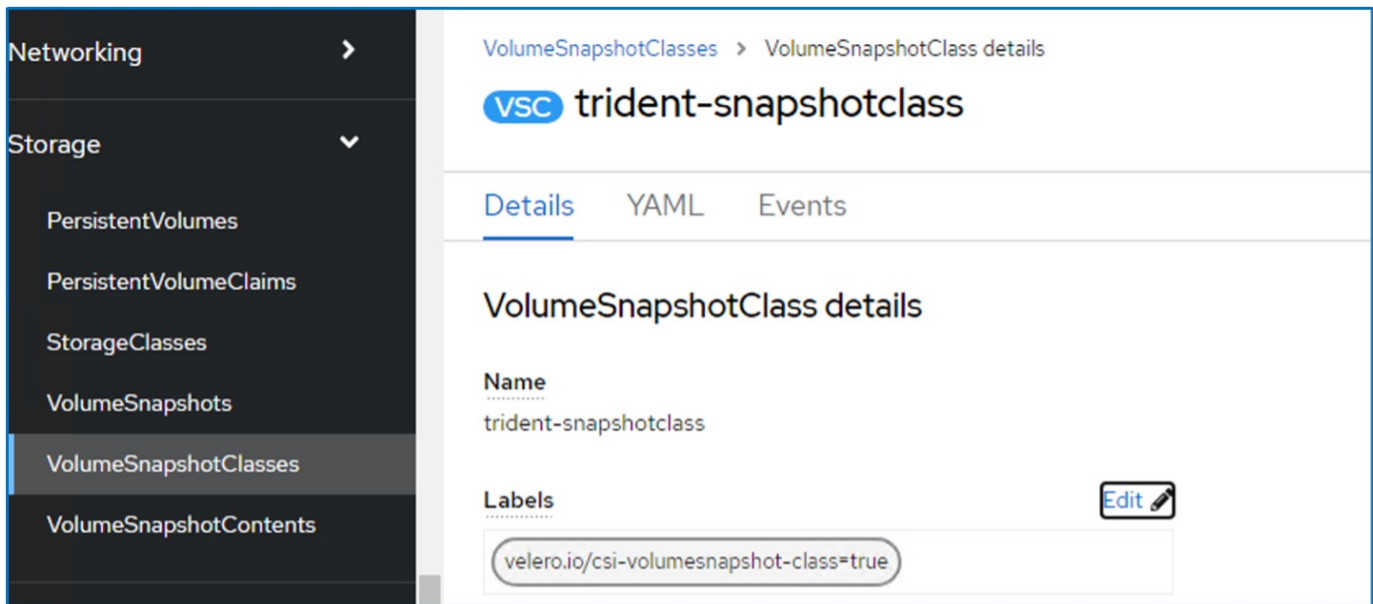
• CSIプラグインを有効にする

CSIスナップショットを使用して永続ボリュームをバックアップするには、**Velero**の**defaultPlugins**に**CSI**を追加します。

Velero CSIプラグインは、**CSI**ベースの**PVC**をバックアップするために、velero.io/CSI-volumesnapshot-class**ラベルが設定されているクラスタ内のVolumeSnapshotClassを選択します。このために

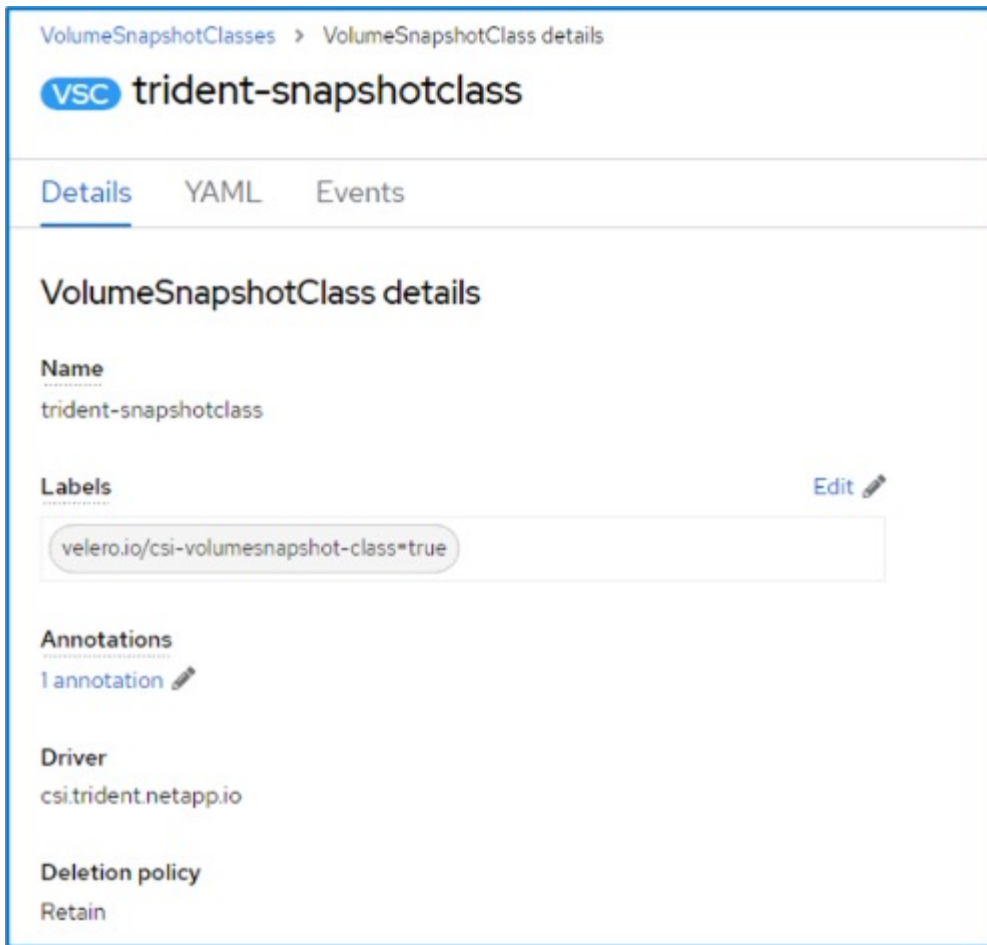
- Trident VolumeSnapshotClassを作成しておく必要があります。

- trident-snapshotclassのラベルを編集し、
- `velero.io/csi-volumesnapshot-class=true` **を参照してください。

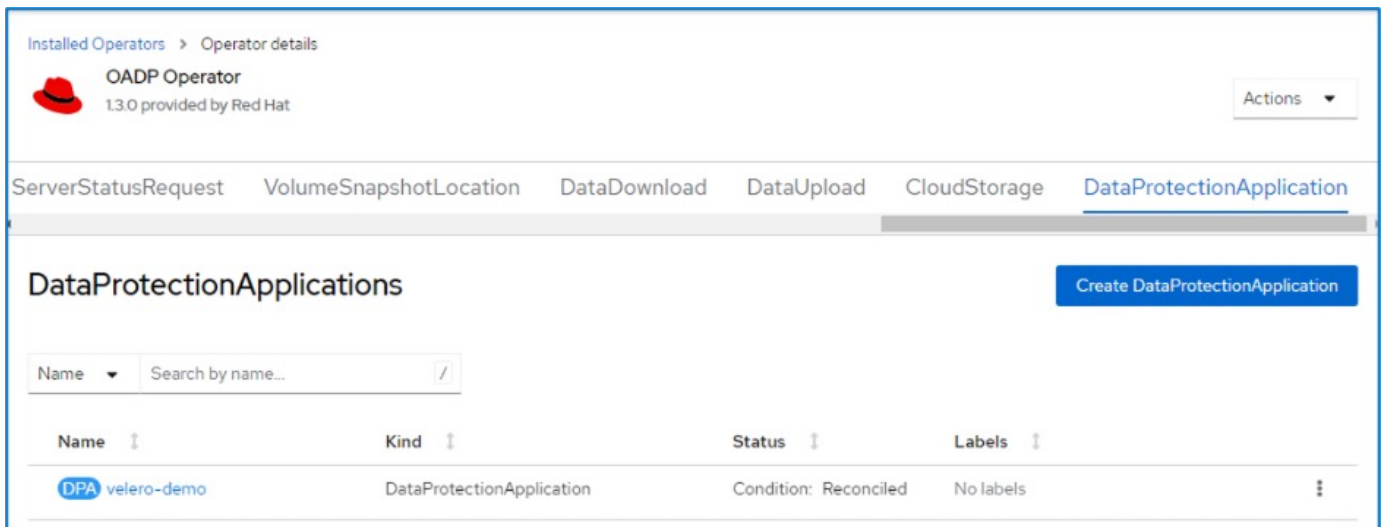


VolumeSnapshotオブジェクトが削除された場合でも、Snapshotが保持されることを確認します。これを行うには、* deletionPolicy *をRetainに設定します。そうでない場合、ネームスペースを削除すると、そのネームスペースにバックアップされたすべてのPVCが完全に失われます。

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Retain
```




DataProtectionApplicationが作成され、Conciled状態になっていることを確認します。



OADPオペレータが対応するBackupStorageLocationを作成します。これはバックアップの作成時に使用されます。

Project: openshift-adp ▾

Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat


Actions ▾

Repository Backup BackupStorageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRecovery

BackupStorageLocations

Create BackupStorageLocation

Name ▾ Search by name... /

Name ▴ ▾	Kind ▴ ▾	Status ▴ ▾	Labels ▴ ▾
 velero-demo-1	BackupStorageLocation	Phase: Available	<div>app.kubernetes.io/component=bsl</div> <div>app.kubernetes.io/instance=velero-demo-1</div> <div>app.kubernetes.io/managed-by=oadp-operator</div> <div>app.kubernetes.io/name=oadp-operator-velero</div> <div>openshift.io/oadp=True</div> <div>openshift.io/oadp-registry=True</div>

OpenShift仮想化でのVMのオンデマンドバックアップの作成

このセクションでは、OpenShift VirtualizationでVMのオンデマンドバックアップを作成する方法について説明します。

VMのバックアップの作成手順

VM全体（VMメタデータとVMディスク）のオンデマンドバックアップを作成するには、[* **Backup**]タブをクリックします。これにより、バックアップカスタムリソース（CR）が作成されます。バックアップCRを作成するためのサンプルYAMLが用意されています。このYAMLを使用すると、指定したネームスペース内のVMとそのディスクがバックアップされます。追加のパラメータは、"[ドキュメント](#)"。

CSIによって、ディスクをバックアップする永続ボリュームのスナップショットが作成されます。VMのバックアップとそのディスクのスナップショットが作成され、YAMLで指定されたバックアップの場所に格納されます。バックアップは、ttlで指定された30日間システムに残ります。

```

apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 -->this is the backupStorageLocation
  previously created
                                when Velero is configured.

  ttl: 720h0m0s

```

バックアップが完了すると、[Phase]に[Completed]と表示されます。

Project: openshift-adp ▾

Installed Operators > Operator details

OADP Operator
1.3.0 provided by Red Hat

Actions ▾

Details YAML Subscription Events All instances BackupRepository **Backup** BackupStorageLocation DeleteBa

Backups Create Backup

Name ▾ Search by name... /

Name ↕	Kind ↕	Status ↕	Labels ↕
backup1	Backup	Phase: Completed	velero.io/storage-location=velero-demo-1

S3ブラウザアプリケーションを使用して、オブジェクトストレージ内のバックアップを確認できます。バックアップのパスは、設定されたバケット内でプレフィックス名（velero/demobackup）で表示されます。バックアップの内容（ボリュームSnapshot、ログ、仮想マシンのその他のメタデータなど）を確認できます。



StorageGRIDでは、Tenant ManagerのS3コンソールを使用してバックアップオブジェクトを表示することもできます。

Path: / demobackup/ backups/ backup1/				
Name	Size	Type	Last Modified	Storage Class
..				
backup1.tar.gz	230.36 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
velero-backup.json	3.35 KB	JSON File	4/15/2024 10:26:29 PM	STANDARD
backup1-resource-list.json.gz	1.12 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
backup1-itemoperations.json.gz	600 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-volumesnapshots.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-podvolumebackups.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-results.gz	49 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotclasses.json.gz	426 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotcontents.json.gz	1.43 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshots.json.gz	1.34 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-logs.gz	13.49 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD

OpenShift VirtualizationでのVMのスケジュールバックアップの作成

スケジュールに従ってバックアップを作成するには、スケジュールCRを作成する必要があります。スケジュールは、単にバックアップを作成する時刻を指定できるcron式です。スケジュールCRを作成するためのサンプルYAML。

```

apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s


```

cron式0 7 ***は、バックアップが毎日7時に作成されることを意味します。バックアップに含めるネームスペースとバックアップの格納場所も指定されます。そのため、バックアップCRではなく、スケジュールCRを使用して、指定した時刻と頻度でバックアップを作成します。

作成したスケジュールは有効になります。

Project: openshift-adp ▾



Installed Operators > Operator details

 **OADP Operator**
1.3.0 provided by Red Hat

storageLocation DeleteBackupRequest DownloadRequest PodVolumeBackup PodVolumeRestore Restore **Schedule**

Schedules


Name ▾ Search by name... /

Name ▴ ▾	Kind ▴ ▾	Status ▴ ▾	Labels ▴ ▾
 schedule1	Schedule	Phase:  Enabled	No labels

バックアップはこのスケジュールに従って作成され、[Backup]タブで確認できます。

Project: openshift-adp ▾

Installed Operators > Operator details


 **OADP Operator**
1.3.0 provided by Red Hat

Events All instances BackupRepository **Backup** BackupStorageLocation DeleteBackupRequest DownloadRequest

Backups

Create Backup

Name ▾ Search by name... /

Name ▴ ▾	Kind ▴ ▾	Status ▴ ▾	Labels ▴ ▾
 schedule1-20240416140507	Backup	Phase: InProgress	velero.io/schedule-name=schedule1 velero.io/storage-location=velero-demo-1

バックアップからのVMのリストア

このセクションでは、バックアップから仮想マシンをリストアする方法について説明します。


前提条件

バックアップからリストアする場合は、仮想マシンが存在していた名前スペースが誤って削除されたと仮定します。

作成したバックアップからリストアするには、Restore Custom Resource (CR) を作成する必要があります。名前とリストア元のバックアップの名前を指定し、restorePVをtrueに設定する必要があります。追加のパラメータは、"[ドキュメント](#)"。[作成]ボタンをクリックします。

Project: openshift-adp

Installed Operators > Operator details


OADP Operator
1.3.0 provided by Red Hat

Actions

[DownloadRequest](#)
[PodVolumeBackup](#)
[PodVolumeRestore](#)
[Restore](#)
[Schedule](#)
[ServerStatusRequest](#)
[VolumeSnap](#)

Restores

[Create Restore](#)

```


apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore1
  namespace: openshift-adp
spec:
  backupName: backup1
  restorePVs: true

```

フェーズが完了と表示されると、仮想マシンがスナップショット作成時の状態にリストアされたことがわかります。（VMの実行中にバックアップが作成された場合、バックアップからVMをリストアすると、リストアされたVMが起動して実行状態になります）。VMが同じネームスペースにリストアされます。

Project: openshift-adp

Installed Operators > Operator details


OADP Operator
1.3.0 provided by Red Hat



Actions

[DownloadRequest](#)
[PodVolumeBackup](#)
[PodVolumeRestore](#)
[Restore](#)
[Schedule](#)
[ServerStatusRequest](#)
[VolumeSn](#)

Restores

[Create Restore](#)

Name Search by name...

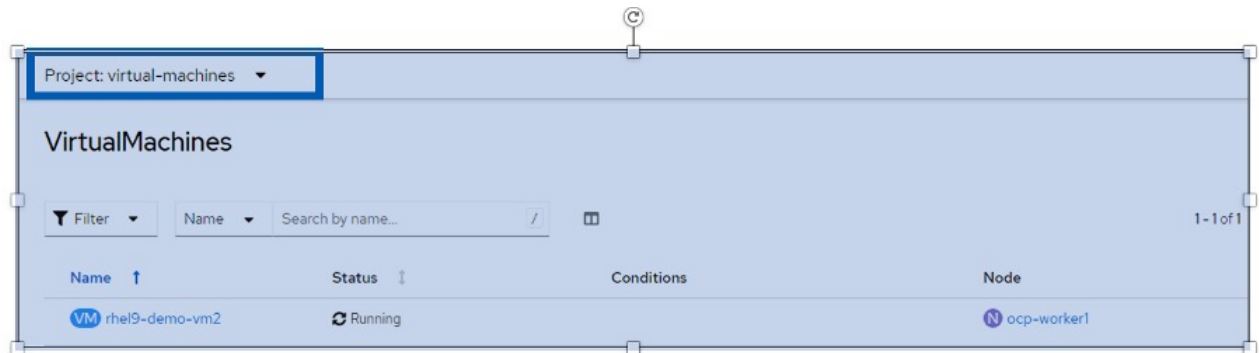
Name	Kind	Status	Labels
 restore1	Restore	Phase:  Completed	No labels

VMを別のネームスペースにリストアするには、Restore CRのYAML定義でnamespaceMappingを指定します。

次のYAMLファイルの例では、バックアップがvirtual-machines-demoネームスペースに作成されたときに、VMとそのディスクをvirtual-machines-demoネームスペースにリストアするためのRestore CRが作成されます。

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup
  restorePVs: true
  includedNamespaces:
  - virtual-machines-demo
  namespaceMapping:
    virtual-machines-demo: virtual-machines
```

フェーズが完了と表示されると、仮想マシンがスナップショット作成時の状態にリストアされたことがわかります。（VMの実行中にバックアップが作成された場合、バックアップからVMをリストアすると、リストアされたVMが起動して実行状態になります）。YAMLで指定された別のネームスペースにVMがリストアされます。



別のストレージクラスへのリストア

Veleroには、JSONパッチを指定してリストア時にリソースを変更する一般的な機能が用意されています。JSONのパッチは、リストア前にリソースに適用されます。JSONパッチはConfigMapで指定され、ConfigMapはrestoreコマンドで参照されます。この機能を使用すると、別のストレージクラスを使用してリストアを実行できます。

次の例では、仮想マシンの作成時にONTAP-NASをディスクのストレージクラスとして使用しています。backup1という名前の仮想マシンのバックアップが作成されます。

The screenshot shows the 'Configuration' tab for a virtual machine named 'rhel9-demo-vm1'. Under the 'Disks' section, there is a table listing the disks:

Name	Source	Size	Drive	Interface	Storage class
cloudinitdisk	Other	-	Disk	virtio	-
disk1	PVC rhel9-demo-vm1-disk1	31.75 GiB	Disk	virtio	ontap-nas
rootdisk	PVC rhel9-demo-vm1	31.75 GiB	Disk	virtio	ontap-nas

The screenshot shows the 'Backup' tab for the 'OADP Operator'. It displays a table of backups:

Name	Kind	Status
backup1	Backup	Phase: Completed

VMを削除して、VMの損失をシミュレートします。

別のストレージクラス（ontap-nas-ecoストレージクラスなど）を使用してVMをリストアするには、次の2つの手順を実行する必要があります。

ステップ1

次のように、OpenShift-ADP名前スペースに構成マップ（コンソール）を作成します。スクリーンショットのように詳細を入力します。
名前スペースを選択：OpenShift-ADP

name: change-storage-class-config (任意の名前を指定できます)

キー: change-storage-class-config.yaml:

値:

```
version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
    resourceNameRegex: "^rhel*"
    namespaces:
    - virtual-machines-demo
patches:
- operation: replace
  path: "/spec/storageClassName"
  value: "ontap-nas-eco"
```

Project: openshift-adp ▼

Edit ConfigMap

Config maps hold key-value pairs that can be used in pods to read application configuration.

Configure via: ☒ Form view ☐ YAML view

Name *

change-storage-class-config

A unique name for the ConfigMap within the project

☐ Immutable

Immutable, if set to true, ensures that data stored in the ConfigMap cannot be updated

Data

Data contains the configuration data that is in UTF-8 range

Key *

change-storage-class-config.yaml

Value

Browse...

Drag and drop file with your value here or browse to upload it.

```
version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
```

+ Add key/value

- Remove key/value

設定マップオブジェクトは次のようになります (CLI)。

```
# kubectl describe cm/change-storage-class-config -n openshift-
adp
Name:          change-storage-class-config
Namespace:     openshift-adp
Labels:        velero.io/change-storage-class=RestoreItemAction
                velero.io/plugin-config=
Annotations:   <none>

Data
====
change-storage-class-config.yaml:
----
version: v1
resourceModifierRules:
- conditions:
    groupResource: persistentvolumeclaims
    resourceNameRegex: "^rhel*"
    namespaces:
      - virtual-machines-demo
  patches:
    - operation: replace
      path: "/spec/storageClassName"
      value: "ontap-nas-eco"

BinaryData
====

Events:   <none>
```

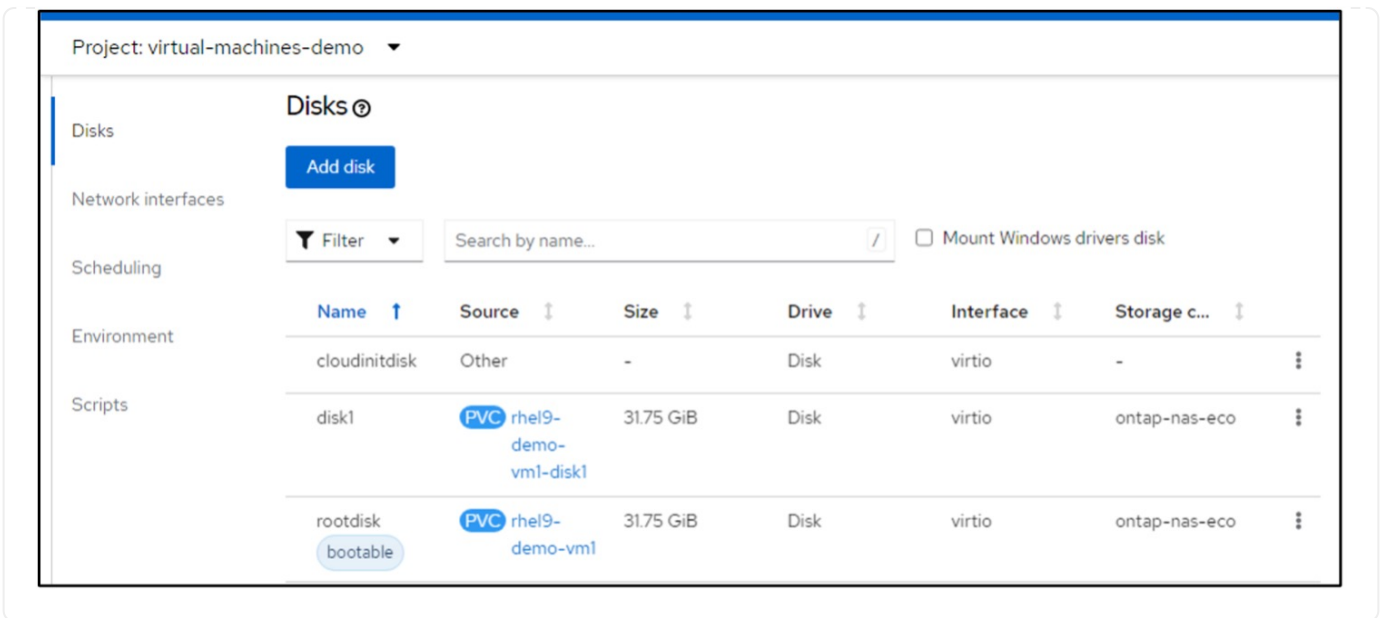
この設定マップは、リストアの作成時にリソース修飾子ルールを適用します。RHELで始まるすべての永続ボリューム要求に対して、ストレージクラス名をontap-nas-ecoに置き換えるパッチを適用します。

ステップ2

VMをリストアするには、Velero CLIから次のコマンドを使用します。

```
#velero restore create restore1 --from-backup backup1 --resource
-modifier-configmap change-storage-class-config -n openshift-adp
```

VMが、ストレージクラスontap-nas-ecoを使用して作成されたディスクと同じネームスペースにリストアされます。



Veleroを使用したバックアップとリストアの削除

このセクションでは、Veleroを使用したOpenShift VirtualizationでVMのバックアップとリストアを削除する方法について説明します。

バックアップを削除します

OC CLIツールを使用して、オブジェクトストレージデータを削除せずにバックアップCRを削除できます。

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

バックアップCRを削除し、関連するオブジェクトストレージデータを削除するには、Velero CLIツールを使用します。

の手順に従ってCLIをダウンロードします。"[Veleroドキュメント](#)"。

Velero CLIを使用して、次のDELETEコマンドを実行します。

```
velero backup delete <backup_CR_name> -n <velero_namespace>
```

リストアの削除

Velero CLIを使用してリストアCRを削除できます。

```
velero restore delete restore --namespace openshift-adp
```

OCコマンドとUIを使用してリストアCRを削除できます。

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

Cloud Insightsを使用した監視

Red Hat OpenShift仮想化でのVMに対するCloud Insightsを使用した監視

作成者：Banu Sundhar、NetApp

このセクションでは、NetApp Cloud InsightsとRed Hat OpenShiftクラスタを統合してOpenShift仮想化VMを監視する方法について詳しく説明します。

NetApp Cloud Insights は、インフラ全体を可視化できるクラウドインフラ監視ツールです。Cloud Insights を使用すると、パブリッククラウドやプライベートデータセンターなど、すべてのリソースの監視、トラブルシューティング、最適化を行うことができます。NetApp Cloud Insightsの詳細については、"[Cloud Insights のドキュメント](#)"。

Cloud Insightsの使用を開始するには、NetApp BlueXPポータルで登録する必要があります。詳細については、[を参照してください "Cloud Insights オンボーディング"](#)

Cloud Insightsには、データの迅速かつ簡単な検索、問題のトラブルシューティング、環境に関する分析情報の提供を可能にする複数の機能があります。強力なクエリを使用してデータを簡単に検索したり、ダッシュボードでデータを視覚化したり、設定したデータのしきい値に関するEメールアラートを送信したりできます。を参照してください "[ビデオチュートリアル](#)" これらの機能を理解するのに役立ちます。

Cloud Insightsでデータの収集を開始するには、次の情報が必要です。

データコレクタ

データコレクタには、次の3種類があります。

*インフラストラクチャ（ストレージデバイス、ネットワークスイッチ、コンピューティングインフラストラクチャ）

*オペレーティング・システム（VMwareやWindowsなど）

*サービス（Kafkaなど）

データコレクタは、ONTAPストレージデバイス（インフラストラクチャデータコレクタ）などのデータソースから情報を検出します。収集された情報は、分析、検証、監視、トラブルシューティングに使用されます。

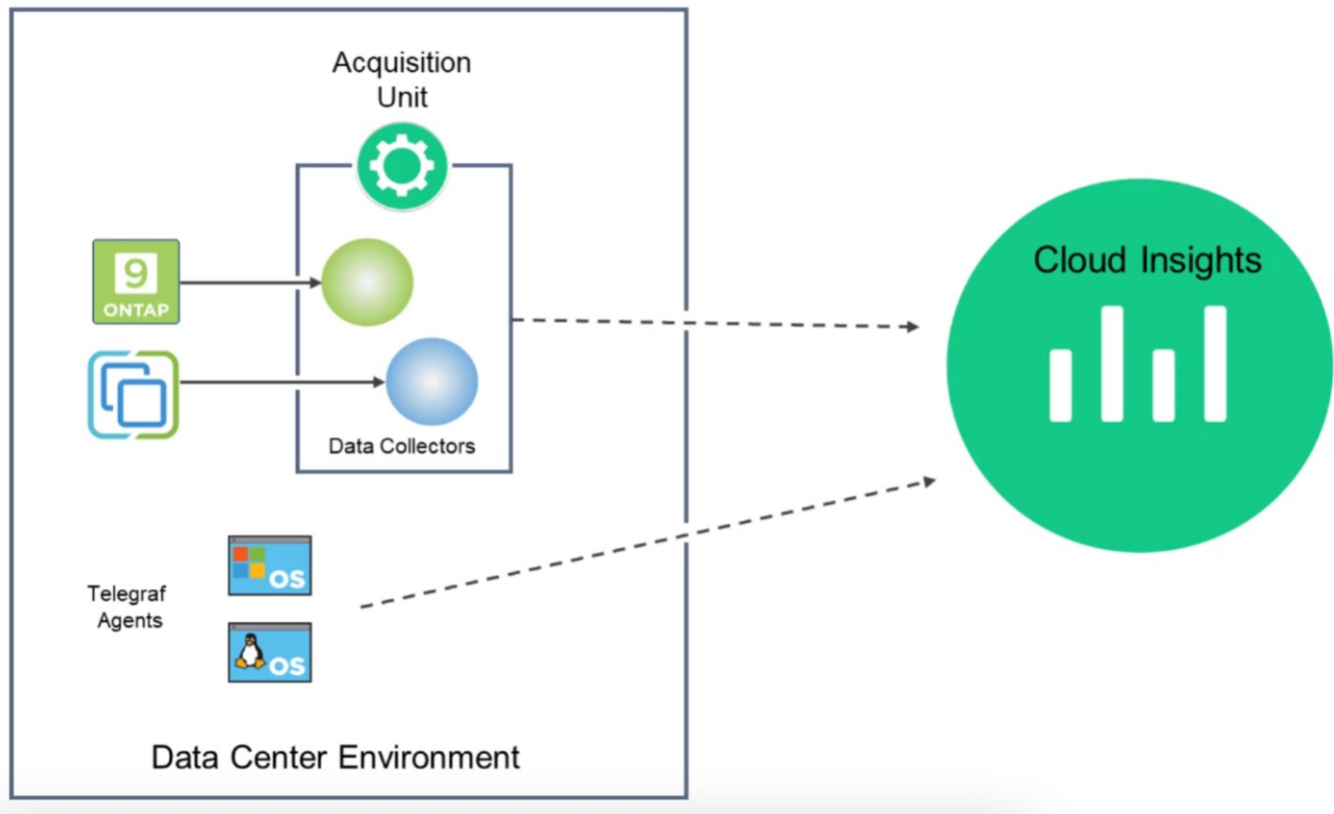
• Acquisition Unit **

インフラストラクチャData Collectorを使用している場合は、Cloud Insightsにデータを注入するAcquisition Unitも必要です。Acquisition Unitは、データコレクタ（通常は仮想マシン）をホストする専用のコンピュータです。このコンピュータは通常、監視対象項目と同じデータセンター/VPCに配置されます。

テレグラフエージェント

Cloud Insightsは、統合データ収集のエージェントとしてTelegrafもサポートしています。Telegraf はプラグインベースのサーバエージェントで、指標、イベント、ログの収集とレポートに使用できます。

Cloud Insightsのアーキテクチャ



Red Hat OpenShiftによる仮想化でのVM向けCloud Insightsとの統合

OpenShift VirtualizationでVMのデータ収集を開始するには、以下をインストールする必要があります。

1. Kubernetesの監視オペレータとデータコレクタでKubernetesデータを収集
詳細な手順については、"[ドキュメント](#)"。
2. VMディスクに永続的ストレージを提供するONTAPストレージからデータを収集するAcquisition Unit。
詳細な手順については、"[ドキュメント](#)"。
3. ONTAPのデータコレクタ
詳細な手順については、"[ドキュメント](#)"

また、VMバックアップにStorageGRIDを使用している場合は、StorageGRIDのデータコレクタも必要です。

Red Hat OpenShift仮想化でのVMの監視機能の例

このセクションでは、Red Hat OpenShift VirtualizationでのVMのCloud Insightsを使用した監視について説明します。

イベントに基づく監視とアラートの作成

ここでは、OpenShift VirtualizationでVMを含むネームスペースがイベントに基づいて監視される例を示します。この例では、クラスタ内の指定されたネームスペースの **logs.kubernetes.event** に基づいてモニタが作成されます。

Observability

Explore

Alerts

Collectors

Log Queries

Enrich

Reporting

Kubernetes

Workload Security

ONTAP Essentials

Admin

NetApp PCS Sandbox / Observability / Alerts / Manage Monitors / Monitor virtual-machines-demo-ns

Edit log monitor

Filter/Advanced Query and Group by in section 1 must not be empty. If alert resolution is based on log entry, section 3 filter/advanced query also must not be empty.

Select the log to monitor

Log Source logs.kubernetes.event

Filter By

kubernetes_cluster ocp-cluster4

involvedobject.namespace virtual-machines-demo

Advanced Query

Group By

reason

27 items found

timestamp ↓	type	source	message
04/19/2024 10:31:18 AM	logs.kubernetes.event	kubernetes_cluster:ocp-cluster4;namespace:cloudi	VirtualMachineInstance started.
04/19/2024 10:31:18 AM	logs.kubernetes.event	kubernetes_cluster:ocp-cluster4;namespace:cloudi	VirtualMachineInstance defined.

Define alert behavior

Create an alert at severity

Warning

when the conditions above occur

1

time

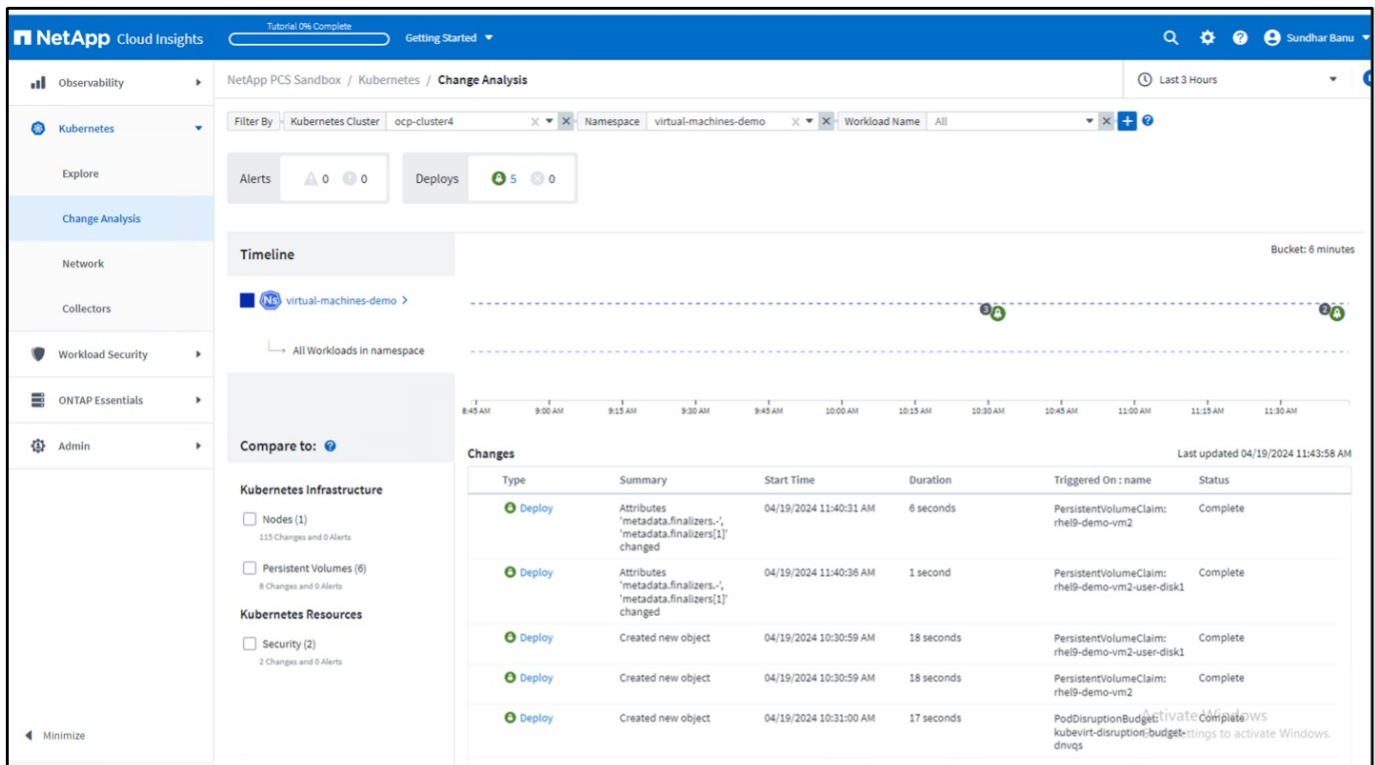
このクエリは、ネームスペース内の仮想マシンのすべてのイベントを提供します。（ネームスペースに仮想マシンが1つしかありません）。高度なクエリを作成して、理由が「failed」または「FailedMount」のイベントに基づいてフィルタリングすることもできます。これらのイベントは通常、PVの作成時またはポッドへのPVのマウント時に問題が存在し、永続的プロビジョニングツールを作成するための動的プロビジョニングツールで問題を示す場合に作成されます。VMのボリューム。

上記のようにアラートモニターを作成するときに、受信者への通知を設定することもできます。エラーの解決に役立つ対処方法や追加情報を指定することもできます。上記の例では、追加情報がTridentバックエンド構成とストレージクラスの定義を調べて問題を解決できます。

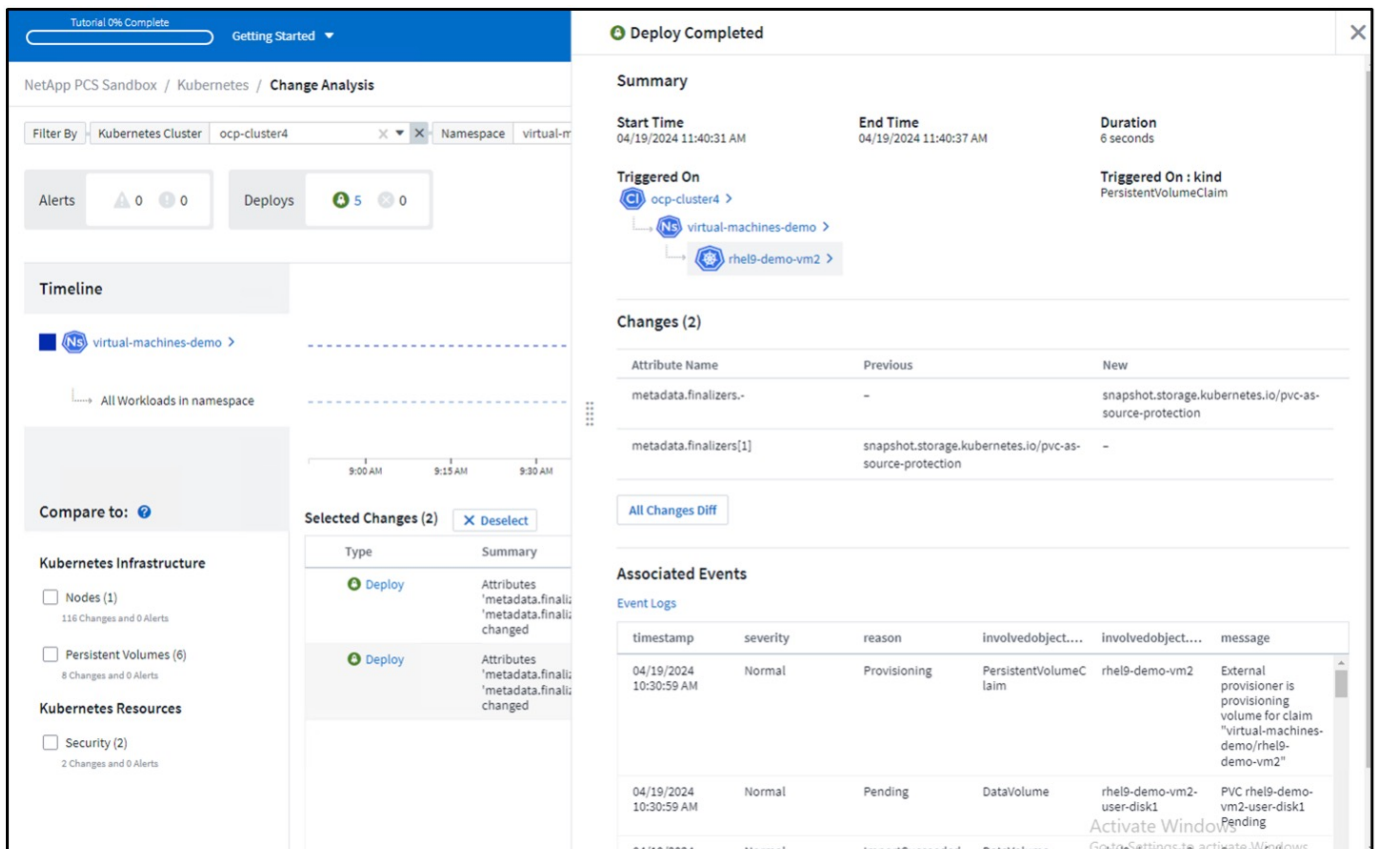
分析の変更

Change Analyticsを使用すると、クラスタの状態で何が変更されたかを確認できます。これには、変更を行ったユーザーも含まれます。これは、問題のトラブルシューティングに役立ちます。

245



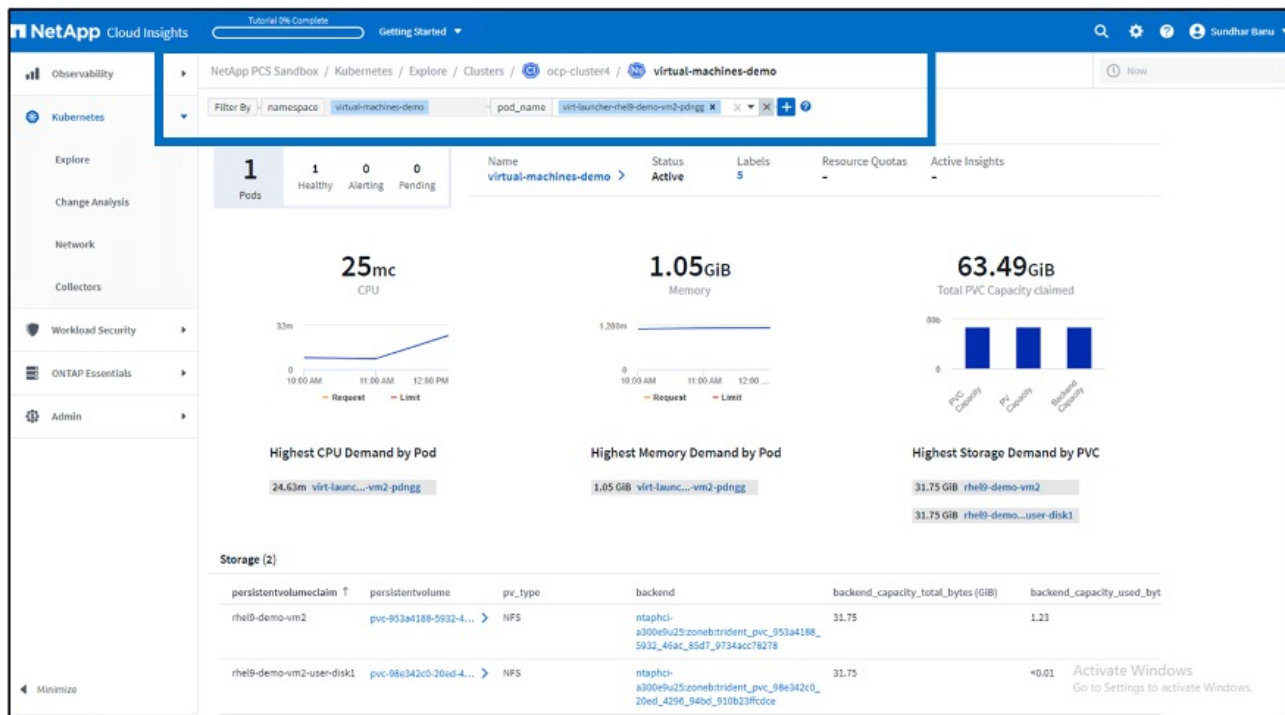
上記の例では、OpenShift仮想化VMを含むネームスペースのOpenShiftクラスターで変更分析が構成されています。ダッシュボードには、タイムラインに対する変更が表示されます。変更内容をドリルダウンして確認し、[すべての変更の相違]をクリックしてマニフェストの相違を確認できます。マニフェストから、永続ディスクの新しいバックアップが作成されたことを確認できます。



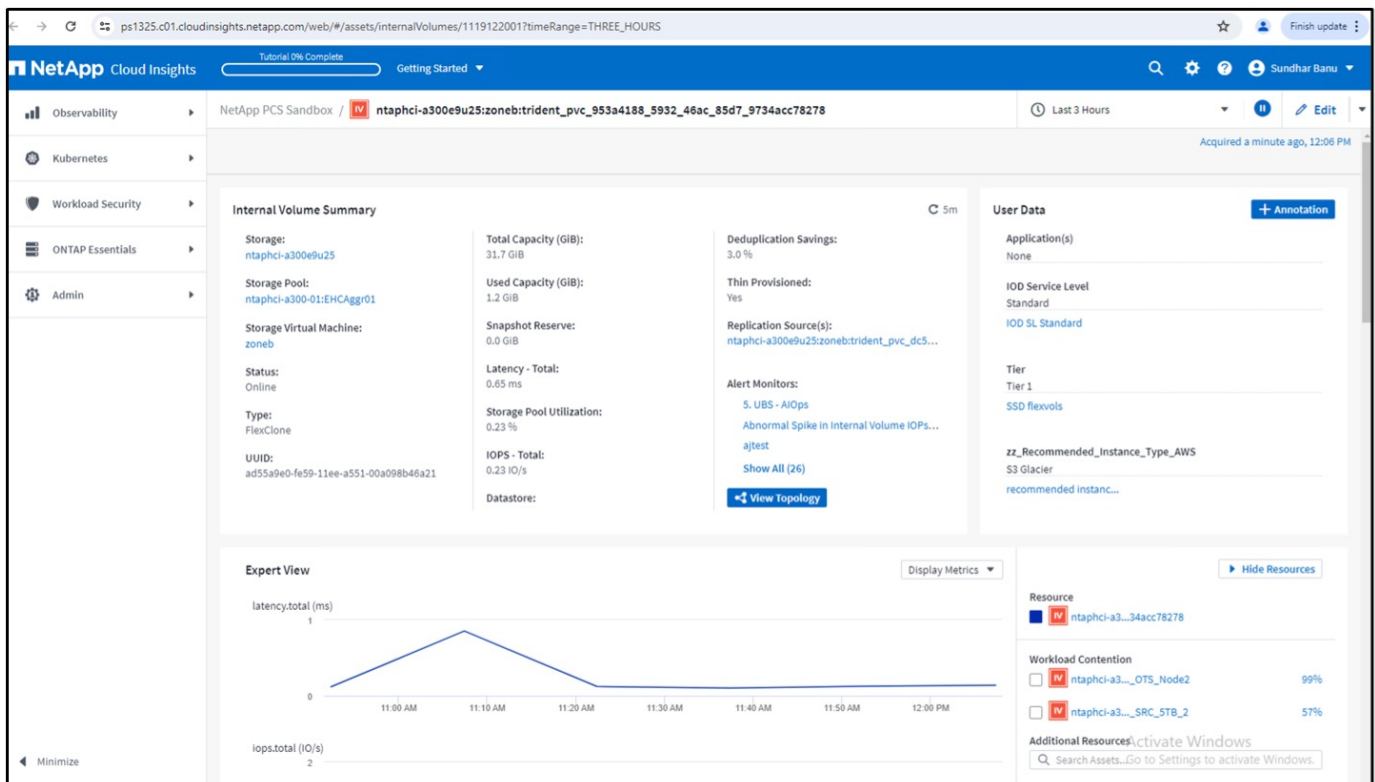
All Changes Diff			
Previous		New	
Expand 45 lines ...			
46	kind: DataVolume	46	kind: DataVolume
47	name: rhel9-demo-vm2	47	name: rhel9-demo-vm2
48	uid: dc93b7a-71bc-409b-ad12-4916d05e0980	48	uid: dc93b7a-71bc-409b-ad12-4916d05e0980
49	- resourceVersion: "8569671"	49	+ resourceVersion: "8619670"
50	uid: 953a4188-5932-46ac-85d7-9734acc78278	50	uid: 953a4188-5932-46ac-85d7-9734acc78278
51	spec:	51	spec:
52	accessModes:	52	accessModes:
Expand 15 lines ...			

バックエンドストレージマッピング

Cloud Insightsを使用すると、VMディスクのバックエンドストレージとPVCに関するいくつかの統計を簡単に確認できます。



[Backend]列の下リンクをクリックすると、バックエンドONTAPストレージからデータが直接取得されます。



すべてのポッドとストレージのマッピングを確認するもう1つの方法は、[Explore]の[Observability]メニューで[All Metrics]クエリを作成することです。

Explore

Object: kubernetes.pod_to_storage

Filter by Attribute: kubernetes_cluster

Filter by Metric

Group By: kubernetes.pod_to_storage

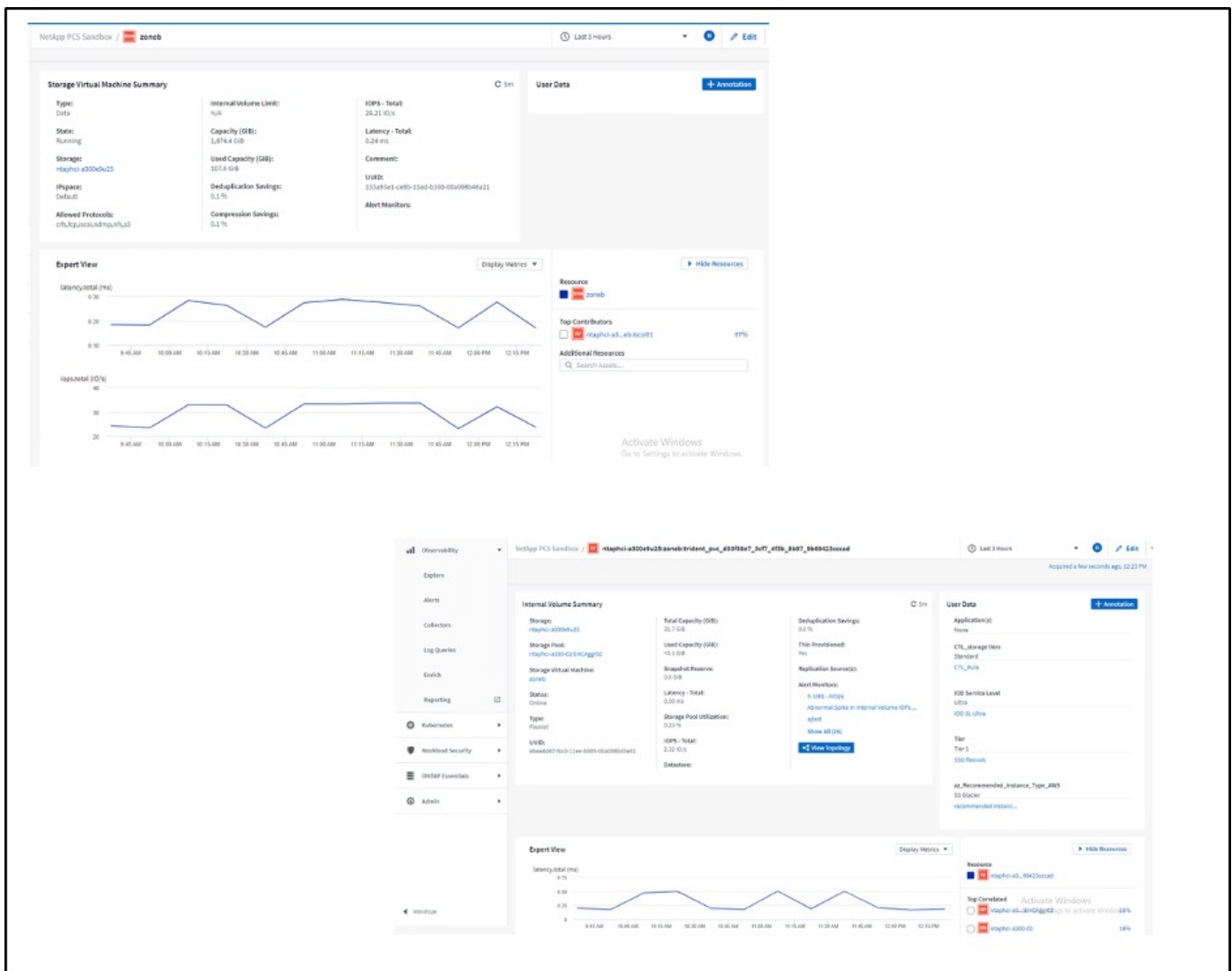
Formattings: Show Expanded Details Conditional Formatting Background Color Show In Range as green

6 items found

Table Row Grouping	Metrics & Attributes
kubernetes.pod_to_storage	persisten... workload...
importer-prime-4f1b6351-2678-4295-b9db-64...	pvc-d4ccec2c-24b openshift-virtualization-os-image zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 0.16
importer-prime-8f792a39-02bb-4e86-a8a8-d6...	pvc-d50f58e7-3c7f openshift-virtualization-os-image zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 0.16
virt-launcher-rhel9-demo-vm2-pdngg	pvc-98e342c0-20e virtual-machines-demo zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 0.00
virt-launcher-rhel9-demo-vm2-pdngg	pvc-953a4188-5932 virtual-machines-demo zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 3.88
virt-launcher-rhel9-demo-vm2-rnztj	pvc-fad1adc3-314 virtual-machines zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 3.88
virt-launcher-rhel9-demo-vm2-rnztj	pvc-ad805a7b-4a virtual-machines zoneb ntaphci-a300e9u25 3d72704c-6108-11e 0.00 0.00

いずれかのリンクをクリックすると、ONTAPストレージに対応する詳細情報が表示されます。たとえば、storageVirtualMachine列でSVM名をクリックすると、SVMに関する詳細がONTAPから取得されます。内部ボリューム名をクリックすると、そのボリュームに関する詳細がONTAPに表示されます。

	storageVirtualMachin...	internalVolume.name	volume.na..
zation-os-image	zoneb		ntaphci-a300e9u25:zoneb:trident_p
zation-os-image	zoneb		ntaphci-a300e9u25:zoneb:trident_p
demo	zoneb		ntaphci-a300e9u25:zoneb:trident_p
demo	zoneb		ntaphci-a300e9u25:zoneb:trident_p
	zoneb		ntaphci-a300e9u25:zoneb:trident_p
	zoneb		ntaphci-a300e9u25:zoneb:trident_p



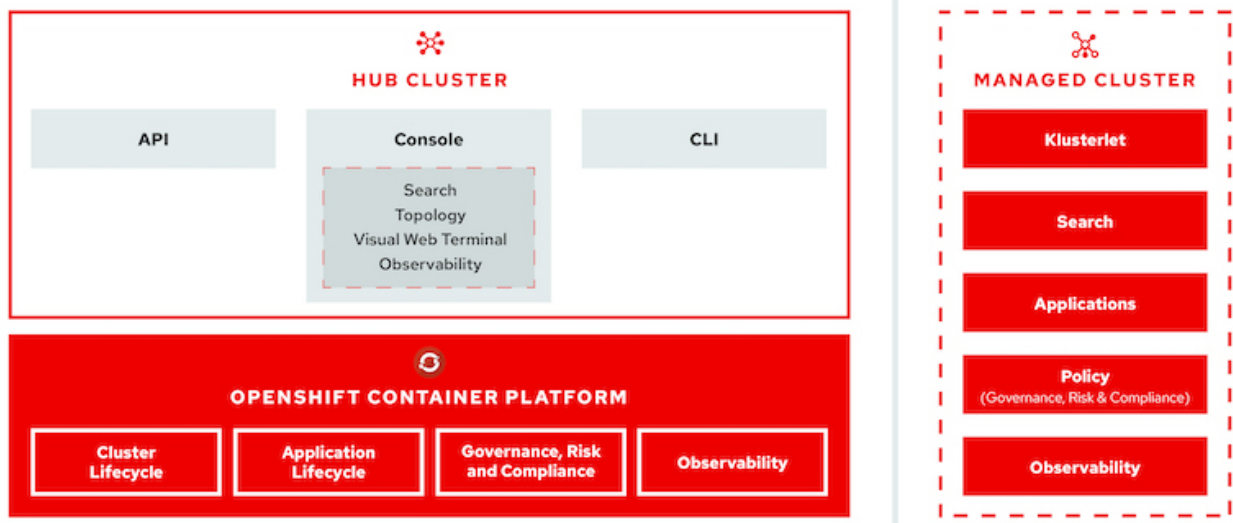
Kubernetes向けの高度なクラスタ管理：NetAppを使用したRed Hat OpenShift -概要

コンテナ化されたアプリケーションを開発環境から本番環境に移行する際、多くの組織では、そのアプリケーションのテストと導入をサポートするために複数の Red Hat OpenShift クラスタが必要になります。この機能を利用することで、多くの組織は、OpenShift クラスタ上で複数のアプリケーションやワークロードをホストしています。そのため、組織ごとにクラスタのセットを管理する必要があり、OpenShift の管理者は、複数のオンプレミスデータセンターとパブリッククラウドにまたがるさまざまな環境で複数のクラスタを管理および管理するという新たな課題に直面する必要があります。これらの課題に対処するために、Red Hat は Kubernetes 向けの高度なクラスタ管理機能を導入しました。

Kubernetes 向けの Red Hat Advanced Cluster Management では、次のタスクを実行できます。

1. 複数のデータセンターとパブリッククラウドにわたって、複数のクラスタを作成、インポート、管理できます。
2. 1つのコンソールから複数のクラスタにアプリケーションやワークロードを導入して管理
3. さまざまなクラスタリソースの健全性とステータスを監視および分析できます
4. 複数のクラスタにわたってセキュリティコンプライアンスを監視し、実施できます。

Red Hat OpenShift クラスタに Red Hat Advanced Cluster Management for Kubernetes をアドオンとしてインストールし、このクラスタをすべての処理の中央コントローラとして使用します。このクラスタはハブクラスタと呼ばれ、ユーザが Advanced Cluster Management に接続するための管理プレーンを公開します。Advanced Cluster Management コンソールからインポートまたは作成されたその他のすべての OpenShift クラスタは、ハブクラスタによって管理され、管理対象クラスタと呼ばれます。Klusterlet というエージェントを管理対象クラスタにインストールし、ハブクラスタに接続し、クラスタライフサイクル管理、アプリケーションライフサイクル管理、オペレータビリティ、およびセキュリティコンプライアンスに関連するさまざまなアクティビティの要求を処理します。



詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。

導入

Kubernetes 向けの高度なクラスタ管理機能を導入

このセクションでは、NetAppを使用したRed Hat OpenShiftでのKubernetes向けの高度なクラスタ管理について説明します。

前提条件

1. ハブクラスタには Red Hat OpenShift クラスタ（バージョン 4.5 以降）が必要です
2. 管理対象クラスタの Red Hat OpenShift クラスタ（バージョン 4.4.4 よりも大きい）
3. Red Hat OpenShift クラスタへのクラスタ管理者アクセス
4. Kubernetes 向けの Advanced Cluster Management 向けの Red Hat サブスクリプション

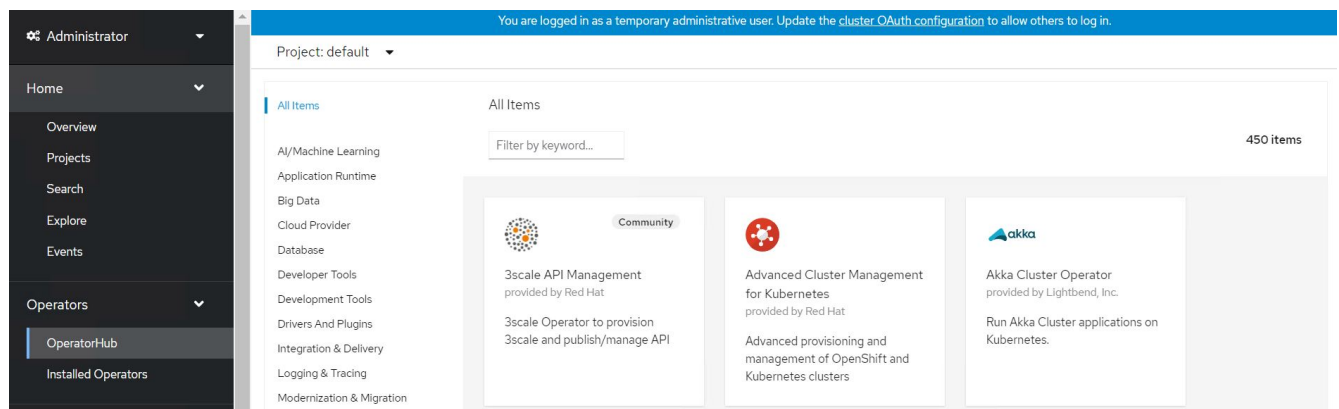
高度なクラスタ管理は OpenShift クラスタのアドオンであるため、ハブクラスタと管理対象クラスタで使用される機能に基づいて、ハードウェアリソースには一定の要件と制限があります。クラスタのサイジングを行う際は、これらの問題について考慮する必要があります。のドキュメントを参照してください ["こちらをご覧ください"](#) 詳細：

オプションで、ハブクラスタにインフラストラクチャコンポーネントをホストする専用ノードがあり、それらのノードにのみ Advanced Cluster Management リソースをインストールする場合は、それに応じてそれらのノードに公差とセレクトラを追加する必要があります。詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。

Kubernetes 向けの高度なクラスタ管理機能を導入

OpenShift クラスタに Kubernetes 向けの高度なクラスタ管理をインストールするには、次の手順を実行します。

1. OpenShift クラスタをハブクラスタとして選択し、cluster-admin 権限でログインします。
2. Operators > Operators Hub に移動し、Kubernetes の Advanced Cluster Management を検索します。



3. Kubernetes の高度なクラスタ管理を選択し、インストールをクリックします。



Advanced Cluster Management for Kubernetes

2.2.3 provided by Red Hat



Install

Latest version

2.2.3

Capability level

- ☒ Basic Install
- ☒ Seamless Upgrades
- ☐ Full Lifecycle
- ☐ Deep Insights
- ☐ Auto Pilot

Provider type

Red Hat

Provider

Red Hat

Infrastructure features

Disconnected

Red Hat Advanced Cluster Management for Kubernetes provides the multicluster hub, a central management console for managing multiple Kubernetes-based clusters across data centers, public clouds, and private clouds. You can use the hub to create Red Hat OpenShift Container Platform clusters on selected providers, or import existing Kubernetes-based clusters. After the clusters are managed, you can set compliance requirements to ensure that the clusters maintain the specified security requirements. You can also deploy business applications across your clusters.

Red Hat Advanced Cluster Management for Kubernetes also provides the following operators:

- Multicluster subscriptions: An operator that provides application management capabilities including subscribing to resources from a channel and deploying those resources on MCH-managed Kubernetes clusters based on placement rules.
- Hive for Red Hat OpenShift: An operator that provides APIs for provisioning and performing initial configuration of OpenShift clusters. These operators are used by the multicluster hub to provide its provisioning and application-management capabilities.

How to Install

Use of this Red Hat product requires a licensing and subscription agreement.

4. Install Operator 画面で、必要な詳細情報を入力し（デフォルトのパラメータをそのまま使用することを推奨）、Install をクリックします。

Install Operator

Install your Operator by subscribing to one of the update channels to keep the Operator up to date. The strategy determines either manual or automatic updates.

Update channel *

- ☐ release-2.0
- ☐ release-2.1
- ☒ release-2.2

Installation mode *

- ☐ All namespaces on the cluster (default)
This mode is not supported by this Operator
- ☒ A specific namespace on the cluster
Operator will be available in a single Namespace only.

Installed Namespace *

- ☒ Operator recommended Namespace: **PR** open-cluster-management



Namespace creation

Namespace **open-cluster-management** does not exist and will be created.

- ☐ Select a Namespace

Approval strategy *

- ☒ Automatic
- ☐ Manual

Install

Cancel

5. オペレータによるインストールが完了するまで待ちます。



Advanced Cluster Management for Kubernetes

2.2.3 provided by Red Hat

Installing Operator

The Operator is being installed. This may take a few minutes.

[View installed Operators in Namespace open-cluster-management](#)

6. オペレータがインストールされたら、Create MultiClusterHub (MultiClusterHub の作成) をクリックします。



Advanced Cluster Management for Kubernetes

2.2.3 provided by Red Hat



Installed operator - operand required

The Operator has installed successfully. Create the required custom resource to be able to use this Operator.

MCH MultiClusterHub **Required**

Advanced provisioning and management of OpenShift and Kubernetes clusters

Create MultiClusterHub

[View installed Operators in Namespace open-cluster-management](#)

7. Create MultiClusterHub（マルチクラスタハブの作成）画面で、詳細を提供した後に Create（作成）をクリックします。これにより、マルチクラスタハブのインストールが開始されます。

Project: open-cluster-management ▾

[Advanced Cluster Management for Kubernetes](#) > [Create MultiClusterHub](#)

Create MultiClusterHub

Create by completing the form. Default values may be provided by the Operator authors.

Configure via: ☒ Form view ☐ YAML view

Note: Some fields may not be represented in this form view. Please select "YAML view" for full control.



MultiClusterHub

provided by Red Hat

MultiClusterHub defines the configuration for an instance of the MultiCluster Hub

Name *

multiclusterhub

Labels

app=frontend

> [Advanced configuration](#)



Create

Cancel

8. すべてのポッドがオープンクラスタ管理Namespaceの running 状態に移行し、オペレータが Succeeded 状態に移行すると、Kubernetes の Advanced Cluster Management がインストールされます。


Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the [Understanding Operators documentation](#). Or create an Operator and ClusterServiceVersion using the [Operator SDK](#).

Name	Managed Namespaces	Status	Provided APIs
 Advanced Cluster Management for Kubernetes 2.2.3 provided by Red Hat	NS open-cluster-management	 Succeeded Up to date	MultiClusterHub ClusterManager ClusterDeployment ClusterState View 25 more...

9. ハブのインストールが完了するまでにはしばらく時間がかかり、完了すると、マルチクラスタハブは running 状態に移行します。

Installed Operators > Operator details



Advanced Cluster Management for Kubernetes
 2.2.3 provided by Red Hat

Actions

[Details](#)
[YAML](#)
[Subscription](#)
[Events](#)
[All instances](#)
[MultiClusterHub](#)
[ClusterManager](#)
[ClusterDeployment](#)
[ClusterState](#)

MultiClusterHubs

[Create MultiClusterHub](#)

Name	Kind	Status	Labels
MCH multiclusterhub	MultiClusterHub	Phase:  Running	No labels

10. オープンクラスタ管理ネームスペースにルートが作成されます。ルートの URL に接続して、Advanced Cluster Management コンソールにアクセスします。



Project: open-cluster-management

Routes

[Create Route](#)

Filter Name mul

Name mul Clear all filters

Name	Status	Location	Service
RT multcloud-console	 Accepted	https://multicloud-console.apps.ocp-vmware2.cie.netapp.com	 management-ingress

クラスタのライフサイクル管理

さまざまな OpenShift クラスタを管理するには、クラスタを作成するか、Advanced Cluster Management にインポートします。

1. 最初に、[インフラストラクチャの自動化]、[クラスタ] の順に移動
2. 新しい OpenShift クラスタを作成するには、次の手順を実行します。
 - a. プロバイダ接続の作成：[プロバイダ接続] に移動して [接続の追加] をクリックし、選択したプロバイダタイプに対応するすべての詳細を入力して [追加] をクリックします。

Select a provider and enter basic information

Provider * ⓘ

aws Amazon Web Services

Connection name * ⓘ

nik-hcl-aws

Namespace * ⓘ

default

Configure your provider connection

Base DNS domain ⓘ

cie.netapp.com

AWS access key ID * ⓘ

AKIATCFBZDOIASDSA

AWS secret access key * ⓘ

.....

Red Hat OpenShift pull secret * ⓘ

```
FuS3pNbktVaHplNFc2MkZsbmtBVG6TktmUIZxcHcxOW9teEZwQ0lYzld3cjJobGxJeDBQON0xlZE0yeGM5Q0ZwZk5RR2JUanlxNnNUM2I1RbOJFb
UFjNCIBYlpEWVZEOHItNkxTMDZPUVpoWFRHcGwtRElDQ2RSYlJRaTlxblDLT2oyQ3pVeUJfNllwcENSa2YyOU5yLWZGSFVfNA==", "email": "Nikhil.k
ulkarni@netapp.com"}, "registry.redhat.io":
```

SSH private key * ⓘ

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BilbnNzaClrZXktdjEAAAAABG5vbmUAAAAEbasdadssadm9uZQAAAAAAAAABAAAAAMwAAAAAtzc2gtZW
QyNTUxOQAAACCLcwLgAvSlHAeP+DevIRNzaG2zkNreMIZ/UHyfOUWwAAAAAJhy/wa6xf8Gu
```

SSH public key * ⓘ

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIltzAuAC746agdh2lcB4/4N6/VE3NobbOQ2t4zVn9QfJ/RRa8A root@nik-rhel8
```

- b. 新しいクラスタを作成するには、クラスタに移動し、クラスタの追加 > クラスタの作成をクリックし
ます。クラスタと対応するプロバイダの詳細を指定し、Create をクリックします。

Configuration

Cluster name * ⓘ

rh-aws

Distribution

Select the type of Kubernetes distribution to use for your cluster.

Red Hat OpenShift

Select an infrastructure provider to host your Red Hat OpenShift cluster.

aws Amazon Web Services

Google Cloud

Microsoft Azure

VMware vSphere

Bare Metal

Release image * ⓘ

quay.io/openshift-release-dev/ocp-release:4.7.12-x86_64

Provider connection * ⓘ

nik-hcl-aws

Add a connection

- c. 作成されたクラスタは、クラスタのリストに Ready ステータスで表示されます。
3. 既存のクラスタをインポートするには、次の手順を実行します。
 - a. クラスタに移動し、クラスタの追加 > 既存クラスタのインポートをクリックします。
 - b. クラスタの名前を入力し、[インポートしてコードを生成して保存]をクリックします。既存のクラスタを追加するコマンドが表示されます。
 - c. Copy コマンドをクリックし、ハブクラスタに追加するクラスタ上でコマンドを実行します。これにより、必要なエージェントのクラスタへのインストールが開始され、このプロセスが完了すると、クラスタがクラスタリストに「Ready」と表示されます。

Name *

ocp-vmw1

Additional labels

Once you click on "Save import and generate code", the information you entered will be used to generate the code and cannot be modified anymore. If you wish to change any information, you will have to delete and re-import this cluster.

Code generated successfully Import saved

Run a command

1. Copy this command

Click the button to have the command automatically copied to your clipboard.

Copy command

2. Run this command with kubectl configured for your targeted cluster to start the import

Log in to the existing cluster in your terminal and run the command.

View cluster Import another

- 複数のクラスタを作成してインポートしたら、1つのコンソールからクラスタを監視および管理できます。

アプリケーションのライフサイクル管理

アプリケーションのライフサイクル管理

アプリケーションを作成して一連のクラスタ全体で管理するには、

- サイドバーから Manage Applications に移動し、Create Application をクリックします。作成するアプリケーションの詳細を入力し、[保存] をクリックします。

Create an application YAML: Off

Cancel

Save


Name* ⓘ
demo-app

Namespace* ⓘ
default X ▾

^ **Repository location for resources**

^ **Repository types**

Select the type of repository where resources that you want to deploy are located

 Git ✓

URL* ⓘ
https://github.com/open-cluster-management/acm-hive-openshift-releases.git X ▾

Branch ⓘ
main X ▾

Path ⓘ
clusterImageSets/fast/4.7 X ▾

- アプリケーションコンポーネントがインストールされると、アプリケーションがリストに表示されます。

Applications


Refresh every 15s ▾

Last update: 7:36:23 PM

Overview

Advanced configuration

Create application

Search						
Name ▴ ▾	Namespace ▴ ▾	Clusters ▴ ▾ ⓘ	Resource ▴ ▾ ⓘ	Time window ▴ ▾ ⓘ	Created ▴ ▾	
demo-app	default	Local	Git 		8 days ago	⋮
1 - 1 of 1 ▾ << < 1 of 1 > >>						

- これで、アプリケーションをコンソールから監視および管理できるようになります。

この機能を使用すると、異なるクラスタのコンプライアンスポリシーを定義し、それらのクラスタが準拠していることを確認できます。ポリシーを設定して、ルールの逸脱や違反について通知したり修正したりできます。

1. サイドバーから「ガバナンスとリスク」に移動します。
2. コンプライアンスポリシーを作成するには、Create Policy（ポリシーの作成）をクリックし、ポリシー標準の詳細を入力して、このポリシーに準拠するクラスタを選択します。このポリシーの違反を自動的に修正するには、[サポートされている場合に適用] チェックボックスをオンにして、[作成] をクリックします。

Create policy ⓘ

YAML: Off

Name *

policy-complianceoperator

Namespace * ⓘ

default ▼

Specifications * ⓘ

1 x ComplianceOperator ▼

Cluster selector ⓘ

1 x local-cluster: "true" ▼

Standards ⓘ

1 x NIST-CSF ▼

Categories ⓘ

1 x PR.IP Information Protection Processes and Procedures ▼

Controls ⓘ

1 x PR.IP-1 Baseline Configuration ▼

☐ Enforce if supported ⓘ☐ Disable policy ⓘ

3. 必要なポリシーをすべて設定したら、Advanced Cluster Management でポリシーやクラスタの違反を監視して修正できます。

Summary 1

Standards ▼

NIST-CSF



No violations found

Based on the industry standards, there are no cluster or policy violations.

Policies

Cluster violations

Find policies

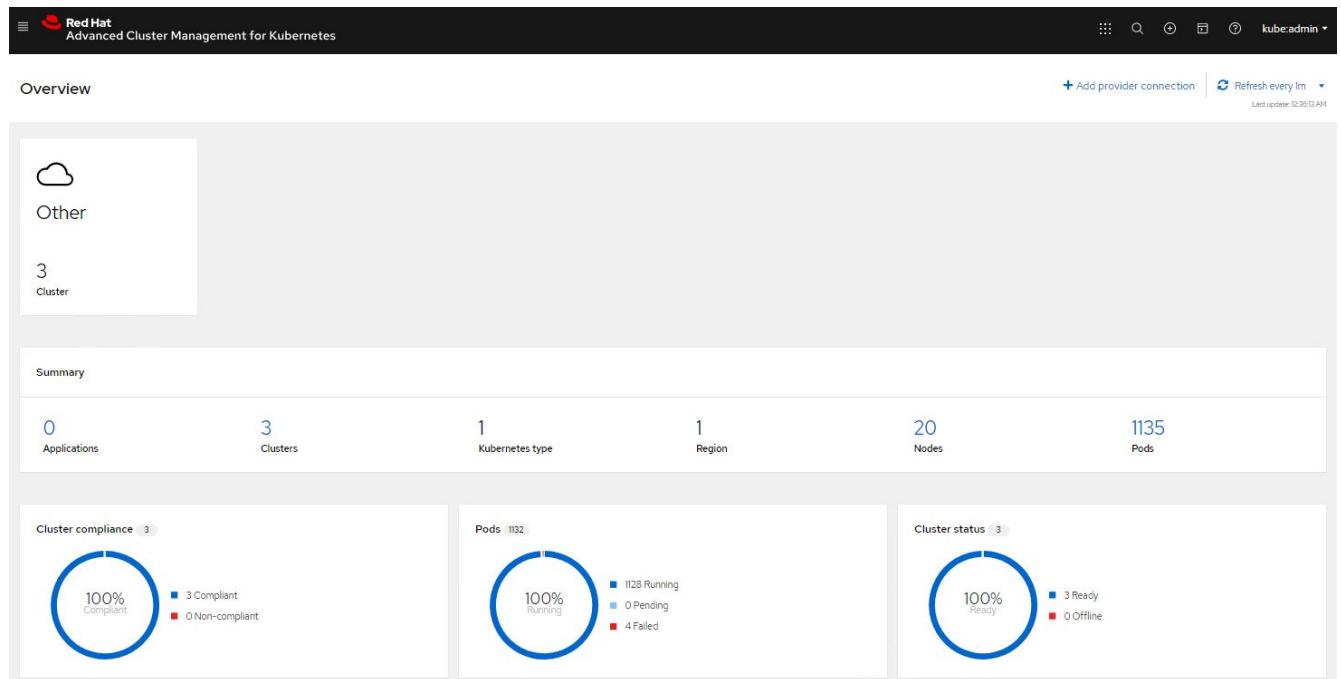
Policy name ↑	Namespace ↑	Remediation ↑	Cluster violations	Standards ↑	Categories ↑	Controls ↑	Created ↓
policy-complianceoperator	default	inform	✓ 0/1	NIST-CSF	PR.IP Information Protection Processes and Procedures	PR.IP-1 Baseline Configuration	32 minutes ago ⋮

1 - 1 of 1 ▼ << < 1 of 1 > >>

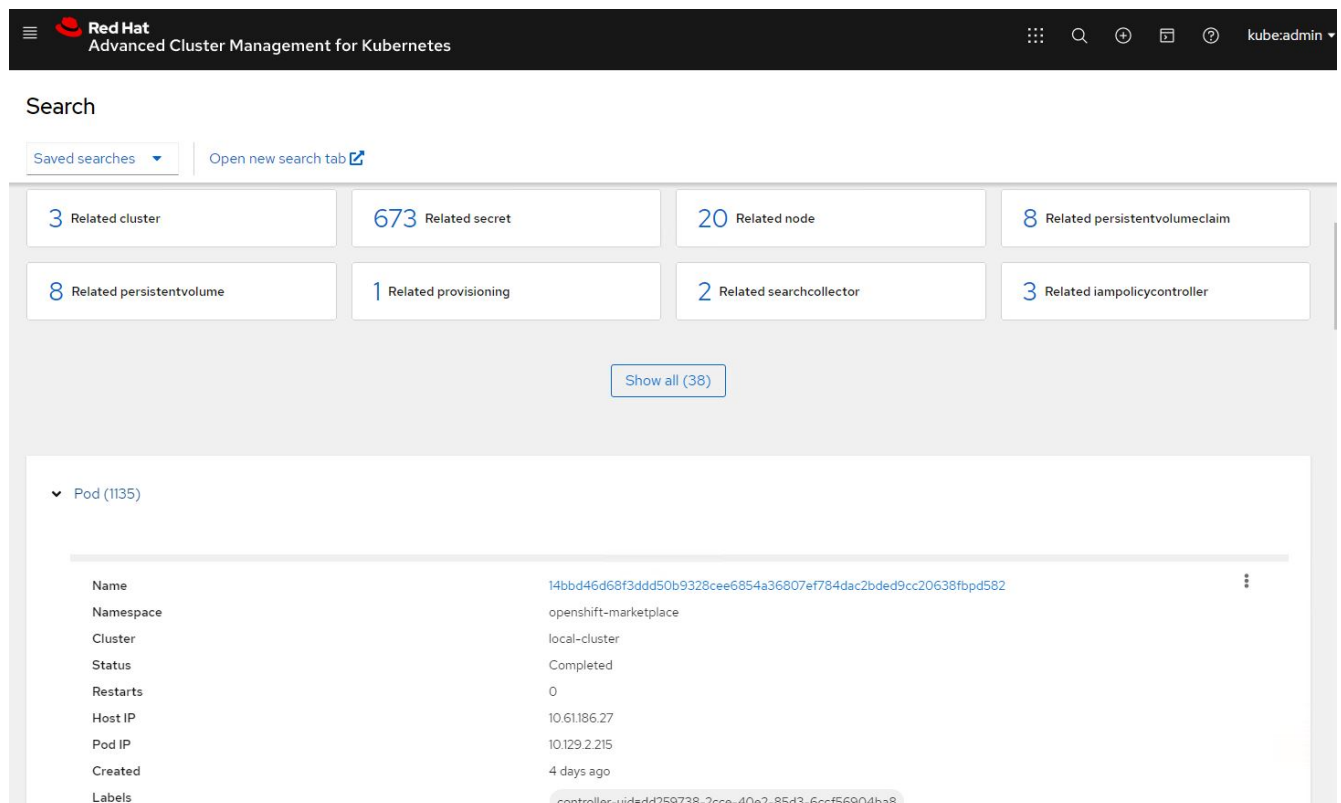
オブザーバビリティ

Kubernetes 向けの高度なクラスタ管理機能を使用すると、ノード、ポッド、およびすべてのクラスタのアプリケーションとワークロードを監視できます。

1. [環境の監視] > [概要] に移動します。



- すべてのクラスタのすべてのポッドとワークロードが監視され、さまざまなフィルタに基づいてソートされます。ポッドをクリックすると、対応するデータが表示されます。



- クラスタ内のすべてのノードが、さまざまなデータポイントに基づいて監視および分析されます。ノードをクリックすると、対応する詳細が表示されます。

Search

[Saved searches](#)
[Open new search tab](#)

3 Related cluster

1k Related pod

12 Related service

Show all (3)

▼ Node (20)

Name	Cluster	Role	Architecture	OS image	CPU	Created	Labels
ocp-master-1.ocp-bare-metal.cie.netapp.com	ocp-bare-metal	master; worker	amd64	Red Hat Enterprise Linux CoreOS 47.83.202103292105-0 (Ootpa)	48	a month ago	beta.kubernetes.io/arch=amd64 beta.kubernetes.io/os=linux kubernetes.io/arch=amd64 5 more
ocp-master-2.ocp-bare-metal.cie.netapp.com	ocp-bare-metal	master; worker	amd64	Red Hat Enterprise Linux CoreOS 47.83.202103292105-0 (Ootpa)	48	a month ago	beta.kubernetes.io/arch=amd64 beta.kubernetes.io/os=linux kubernetes.io/arch=amd64 5 more
ocp-master-3.ocp-bare-metal.cie.netapp.com	ocp-bare-metal	master; worker	amd64	Red Hat Enterprise Linux CoreOS 47.83.202103292105-0 (Ootpa)	48	a month ago	beta.kubernetes.io/arch=amd64 beta.kubernetes.io/os=linux kubernetes.io/arch=amd64 5 more

4. クラスタはすべて、クラスタのリソースとパラメータに基づいて監視および整理されます。クラスタをクリックしてクラスタの詳細を表示します。

Search

[Saved searches](#)
[Open new search tab](#)

3k Related secret

787 Related pod

15 Related persistentvolumeclaim

17 Related node

1 Related application

15 Related persistentvolume

1 Related searchcollector

8 Related clusterclaim

3 Related resourcequota

5 Related identity

Show all (159)

▼ Cluster (2)

Name	Available	Hub accepted	Joined	Nodes	Kubernetes version	CPU	Memory	Console URL	Labels
local-cluster	True	True	True	8	v1.20.0+c8905da	84	418501Mi	Launch	cloud=VSphere clusterID=148632d9-69d5-4ae4-98ee-8df1886463c3 installer.name=multiclusterhub 4 more
ocp-vmw	True	True	True	9	v1.20.0+df9c838	28	111981Mi	Launch	cloud=VSphere clusterID=9d76ac4e-4aae-4d45-a2e8-11b6b54282fe name=ocp-vmw 1 more

複数のクラスタにリソースを作成する

Kubernetes 向けの高度なクラスタ管理機能を使用すると、ユーザはコンソールから 1 つ以上の管理対象クラスタ上にリソースを同時に作成できます。たとえば、異なる NetApp ONTAP クラスタでサポートされている異なるサイトに OpenShift クラスタがあり、両方のサイトで PVC をプロビジョニングする場合は、上部バーの（+）記号をクリックします。次に、PVC を作成するクラスタを選択し、リソース YAML を貼り付けて、Create をクリックします。

Create resource

[Cancel](#)[Create](#)

Clusters | Select the clusters where the resource(s) will be deployed.

2 x local-cluster,
ocp-vmw

Resource configuration | Enter the configuration manifest for the resource(s).

YAML

```
1 kind: PersistentVolumeClaim
2 apiVersion: v1
3 metadata:
4   name: demo-pvc
5 spec:
6   accessModes:
7     - ReadWriteOnce
8   resources:
9     requests:
10      storage: 1Gi
11   storageClassName: ocp-trident
```

サードパーティツールを使用したコンテナアプリケーションとVMのデータ保護

このソリューションでは、Red Hat OpenShift ContainerプラットフォームのOADPオペレータと統合されているVeleroを使用して、コンテナとVMのデータ保護処理を実行する方法を説明します。

1. OpenShift Containerプラットフォームでのコンテナアプリケーションのバックアップの作成とリストアの詳細については、[を参照してください "こちらをご覧ください"](#)。
2. OpenShift Containerプラットフォームに導入されたOpenShift VirtualizationでVMのバックアップの作成とリストアの詳細については、[を参照してください "こちらをご覧ください"](#)。

ビデオとデモ：ネットアップを使用した Red Hat OpenShift

次のビデオでは、このドキュメントで説明している機能の一部を紹介します。

[Cloud InsightsとOpenShift仮想化の統合](#)

[Red Hat MTVを使用したNetApp ONTAPストレージによるOpenShift仮想化へのVMの移行](#)

[Astra ControlとNetApp FlexCloneテクノロジーでソフトウェア開発を高速化- Red Hat OpenShift with NetApp](#)

[NetApp Astra Control を活用して、事後分析とアプリケーションのリストアを実行](#)

[Astra Control Centerを使用したCI / CDパイプラインのデータ保護](#)

[Astra Control Center - Red Hat OpenShiftとNetAppを使用したワークロードの移行](#)

[ワークロードの移行 - ネットアップを使用した Red Hat OpenShift](#)

OpenShift Virtualizationのインストール-ネットアップでRed Hat OpenShiftを実装します

OpenShift仮想化を使用した仮想マシンの導入-ネットアップでRed Hat OpenShiftを実装します

Red Hat 仮想化での NetApp HCI for Red Hat OpenShift

追加情報：ネットアップを使用した **Red Hat OpenShift**

このドキュメントに記載されている情報の詳細については、次の Web サイトを参照してください。

- NetApp のドキュメント

["https://docs.netapp.com/"](https://docs.netapp.com/)

- Astra Trident のドキュメント

["https://docs.netapp.com/us-en/trident/index.html"](https://docs.netapp.com/us-en/trident/index.html)

- NetApp Astra Control Center のドキュメント

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- Red Hat OpenShift のドキュメント

["https://access.redhat.com/documentation/en-us/openshift_container_platform/4.7/"](https://access.redhat.com/documentation/en-us/openshift_container_platform/4.7/)

- Red Hat OpenStack Platform のドキュメント

["https://access.redhat.com/documentation/en-us/red_hat_opensstack_platform/16.1/"](https://access.redhat.com/documentation/en-us/red_hat_opensstack_platform/16.1/)

- Red Hat Virtualization のドキュメント

["https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.4/"](https://access.redhat.com/documentation/en-us/red_hat_virtualization/4.4/)

- VMware vSphere のドキュメント

["https://docs.vmware.com/"](https://docs.vmware.com/)

NVA-1166：ネットアップを使用したVMware Tanzuの評価

ネットアップ、Alan Cowles 氏と Nikhil M Kulkarni 氏

このリファレンスガイドでは、Tanzu Kubernetes Grid (TKG)、Tanzu Kubernetes Grid Service (TKGS)、またはTanzu Kubernetes Grid Integrated (TKGI) のいずれかとして、ネットアップによって検証済みの複数のデータセンター環境に導入された、さまざまなVMware Tanzu Kubernetesソリューションの導入方法を検証します。また、ネットアップストレージシステムとAstra Tridentストレージオーケストレーションツールとのストレージ統合についても説明します。Tridentストレージオーケストレーションツールを使用して永続的ストレージを管理し、Astra Control Centerで、永続的ストレージを使

用してステートフルアプリケーションのバックアップとクローニングを実行できます。最後に、解決策 の統合と検証のビデオデモを紹介します。

ユースケース

NetApp解決策 を搭載したVMware Tanzuは、次のユースケースにおいて、お客様に卓越した価値を提供するように設計されています。

- VMware vSphereに導入され、ネットアップストレージシステムと統合されたVMware Tanzu Kubernetes Gridサービスの導入と管理が簡単です。
- VMware Tanzu Kubernetes Gridソリューションは、エンタープライズコンテナと仮想化ワークロードの機能を統合したものです。
- VMware Tanzuの機能にネットアップのストレージやネットアップのAstra製品スイートを使用した実際の構成とユースケース
- VMware Tanzu Kubernetes Gridクラスタに導入されたコンテナ化ワークロードを、Astra Control Centerを使用してネットアップストレージシステムにアプリケーションと整合性のある方法で保護または移行

ビジネスバリュー

企業は、新しい製品の作成、リリースサイクルの短縮、新機能の迅速な追加を目的として、DevOps の手法を採用する傾向に迫られています。即応性に優れた本来の性質から、コンテナやマイクロサービスは、DevOps の実践を支援するうえで重要な役割を果たします。しかし、エンタープライズ環境で本番環境規模でDevOps を実践する場合、独自の課題が生じ、基盤となるインフラに次のような一定の要件が課せられます。

- スタック内のすべてのレイヤで高可用性を実現します
- 導入手順の簡易化
- ノンストップオペレーションとアップグレード
- API ベースのプログラム可能なインフラで、マイクロサービスの即応性を維持します
- パフォーマンスを保証するマルチテナンシー
- 仮想ワークロードとコンテナ化されたワークロードを同時に実行できます
- ワークロードのニーズに応じてインフラを個別に拡張できる
- オンプレミスのデータセンターとクラウドの両方でコンテナを実行するハイブリッドクラウドモデルに導入できます。

ネットアップのVMware Tanzuにはこのような課題があることを認め、お客様が選択したハイブリッドクラウド環境にVMware Tanzu Kubernetesソリューションを導入することで、それぞれの問題に対処できる解決策が示されています。

テクノロジーの概要

NetApp解決策 を搭載したVMware Tanzuは、次の主要コンポーネントで構成されています。

VMware Tanzu Kubernetesプラットフォーム

VMware Tanzuには、ネットアップのソリューションエンジニアリングチームがラボで検証したさまざまなフレーバーがあります。各Tanzuリリースはネットアップのストレージポートフォリオと正常に統合されてお

り、各リリースが特定のインフラ要件を満たすのに役立ちます。次の各バージョンのTanzuの特徴と機能については、このドキュメントで説明します。

- VMware Tanzu Kubernetes Grid (TKG)*
- VMware vSphere環境に展開される標準のアップストリームKubernetes環境。
- 以前はEssential PKSと呼ばれていました（Heptio買収により、2019年2月に取得）。
- TKGは、vSphere 6.7U3以降でサポートされる独立した管理クラスティンスタンスとともに導入されています。
- TKGの導入は、AWSやAzureと同様にクラウドにも導入できます。
- WindowsまたはLinuxのワーカーノード（Ubuntu / Photon）を使用できます。
- NSXとT、HA Proxy、AVIネットワーク、またはロードバランサをコントロールプレーンに使用できます。
- TKGはアプリケーション/データプレーンでMetalLBをサポートしています。
- vSphere CSIおよびNetApp Astra TridentなどのサードパーティCSISを使用可能

* 『VMware Tanzu Kubernetes Grid Service (TKGS) 』

- VMware vSphere環境に展開される標準のアップストリームKubernetes環境。
- 以前はEssential PKSと呼ばれていました（Heptio買収により、2019年2月に取得）。
- TKGSは、vSphere 7.0U1以降でのみスーパーバイザクラスタおよびワークロードクラスタとともに配置されます。
- WindowsまたはLinuxのワーカーノード（Ubuntu / Photon）を使用できます。
- NSXとT、HA Proxy、AVIネットワーク、またはロードバランサをコントロールプレーンに使用できます。
- TKGSはアプリケーション/データプレーンでMetalLBをサポートしています。
- vSphere CSIおよびNetApp Astra TridentなどのサードパーティCSISを使用可能
- は、Tanzuを使用したvSphereポッドのサポートを提供し、環境内の有効なESXiホストでポッドを直接実行できるようにします。
- VMware Tanzu Kubernetes Grid Integrated (TKGI) *
- 以前の名称はEnterprise PKS（Heptio取得、2019年2月）です。
- NSXとT、HAプロキシ、AVIのいずれかを使用できます。独自のロードバランサを指定することもできます。
- vSphere 6.7U3以降、およびAWS、Azure、GCPでサポートされます。
- ウィザードを使用してセットアップすると、導入が簡単になります。
- BOSHが管理する変更不可の制御VMでTanzuを実行します。
- NetApp Astra Tridentのように、vSphere CSIやサードパーティのCSISを利用できる（一部の条件が適用される）

* 「vSphereポッド」 (Tanzu (vSphereポッド) を使用したvSphere *

- vSphereネイティブのポッドは、完全な分離のために、処方された仮想ハードウェアを使用して、薄い光子ベースのレイヤで実行されます。

- NSXは必須ですがHarborイメージレジストリなどの追加機能をサポートできます
- TKGSなどの仮想スーパーバイザークラスタを使用して、vSphere 7.0U1以降に導入および管理されます。ポッドをESXiノードで直接実行します。
- vSphere管理により、vSphereと完全に統合され、最高レベルの可視性と制御を実現します。
- 独立したCRXベースのポッドにより、最高レベルのセキュリティを実現。
- vSphere CSIの永続的ストレージのみをサポートします。サードパーティ製ストレージオーケストレーションツールはサポートされていません。

ネットアップストレージシステム

ネットアップには、エンタープライズデータセンターやハイブリッドクラウド環境に最適なストレージシステムが複数あります。ネットアップのポートフォリオには、コンテナ化されたアプリケーションに永続的ストレージを提供できる NetApp ONTAP、NetApp Element、および NetApp E シリーズストレージシステムが含まれています。

詳細については、ネットアップのWebサイトを参照してください ["こちらをご覧ください"](#)。

ネットアップとストレージの統合

NetApp Astra Control Centerは、ステートフルKubernetesワークロード向けの充実したストレージおよびアプリケーション対応のデータ管理サービスを提供します。オンプレミス環境に導入され、信頼できるネットアップのデータ保護テクノロジーを基盤としています。

詳細については、NetApp Astra の Web サイトをご覧ください ["こちらをご覧ください"](#)。

Astra Tridentは、コンテナやKubernetesディストリビューション向けの、VMware Tanzuなどのオープンソースの完全サポートされたストレージオーケストレーションツールです。

詳細については、Astra Trident の Web サイトをご覧ください ["こちらをご覧ください"](#)。

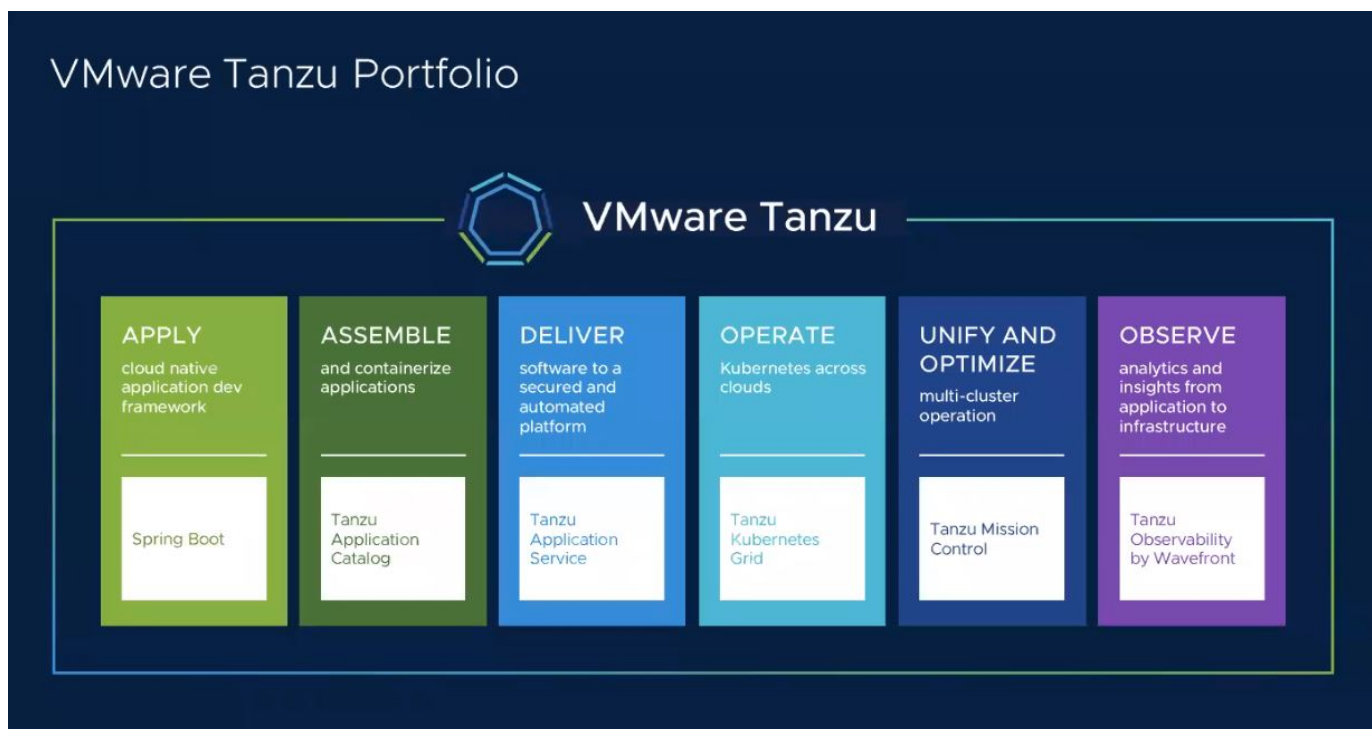
検証済みリリースの現在のサポートマトリックスです

テクノロジー	目的	ソフトウェアのバージョン
NetApp ONTAP	ストレージ	9.9.1
ネットアップアストラコントロールセンター	アプリケーション対応データ管理	22.04
ネットアップアストラ Trident	ストレージオーケストレーション	22.04.0
VMware Tanzu Kubernetesグリッド	コンテナオーケストレーション	1.4以降
VMware Tanzu Kubernetes Gridサービス	コンテナオーケストレーション	0.0.15 [vSphere名前空間]
		1.22.6 [スーパーバイザークラスタのKubernetes]
VMware Tanzu Kubernetes Grid統合	コンテナオーケストレーション	1.13.3
VMware vSphere の場合	データセンターの仮想化	7.0U3

VMware NSX -Tデータセンター	ネットワークとセキュリティ	3.1.3
VMware NSX Advanced Load Balancerの略	ロードバランサ	20.1.3

VMware Tanzuの概要

VMware Tanzuは、企業がアプリケーションおよび実行するインフラストラクチャを最新化できるようにする製品ポートフォリオです。VMware Tanzuの機能の完全なスタックにより、開発チームとIT運用チームが1つのプラットフォーム上に統合され、オンプレミスとハイブリッドクラウド環境全体でアプリケーションとインフラストラクチャの両方の最新化を一貫して活用し、継続的に優れたソフトウェアを本番環境に提供します。



Tanzuポートフォリオのさまざまなサービスとその機能の詳細については、ドキュメントを参照してください ["こちらをご覧ください"](#)。

TanzuのKubernetes Operationsカタログについて、VMwareはTanzu Kubernetes Gridのためのさまざまな実装を提供しています。これらはすべて、さまざまなプラットフォームでTanzu Kubernetesクラスタのライフサイクルをプロビジョニングおよび管理します。Tanzu Kubernetesクラスタは、VMwareによって構築およびサポートされる本格的なKubernetesディストリビューションです。

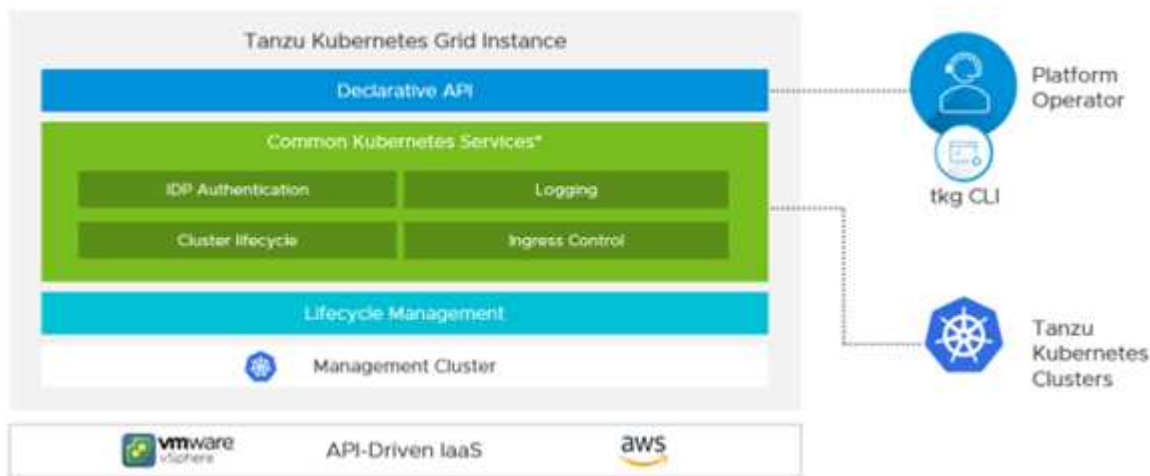
ネットアップでは、VMware Tanzuポートフォリオに含まれる次の製品の導入と相互運用性について、ラボでテストを実施して検証しています。

- "VMware Tanzu Kubernetes Grid (TKG) "
- "VMware Tanzu Kubernetes Grid Service (TKGS) "
- "VMware Tanzu Kubernetes Grid Integrated (TKGI) "
- "VMware vSphereとTanzu (vSphereポッド) "

VMware Tanzu Kubernetes Grid (TKG) の概要

TKGとも呼ばれるVMware Tanzu Kubernetes Gridを使用すると、ハイブリッドクラウド環境やパブリッククラウド環境にTanzu Kubernetesクラスタを導入できます。TKGはKubernetesクラスタそのものである管理クラスタとしてインストールされ、Tanzu Kubernetesクラスタを導入および運用します。これらのTanzu Kubernetesクラスタは、実際のワークロードが導入されているワークロードのKubernetesクラスタです。

Tanzu Kubernetes Gridは、いくつかの有望なアップストリームコミュニティプロジェクトに基づいて構築され、VMwareが開発、販売、サポートするKubernetesプラットフォームを提供します。Kubernetesディストリビューションに加え、Tanzu Kubernetes Gridには、レジストリ、ロードバランシング、認証などの重要な本番環境クラスのサービスであるアドオンが追加されています。管理クラスタを備えたVMware TKGはvSphere 6.7環境で広く使用されていますが、それがサポートされていても、TKGSにはvSphere 7とのネイティブ統合機能があるため、vSphere 7環境への導入は推奨されません。



Tanzu Kubernetes Gridの詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。

Tanzu Kubernetes GridがvSphereクラスタまたはクラウド環境にインストールされているかどうかに応じて、インストールガイドに従ってTanzu Kubernetes Gridを準備して導入します ["こちらをご覧ください"](#)。

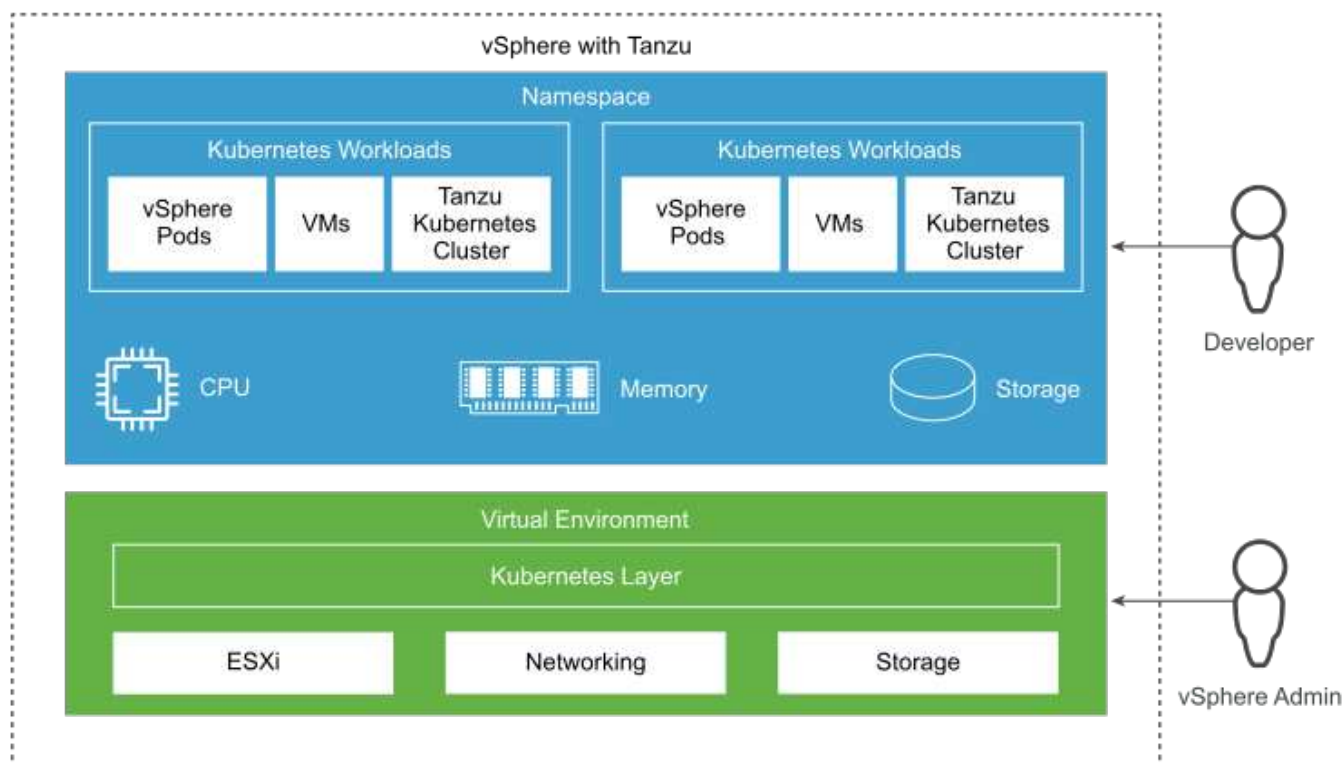
Tanzu Kubernetes Gridの管理クラスタをインストールしたら、のドキュメントに従って、必要に応じてユーザクラスタまたはワークロードクラスタを導入します ["こちらをご覧ください"](#)。VMware TKG管理クラスタでは、Tanzu Kubernetesクラスタのインストールと運用にSSHキーが必要です。このキーは'capv'ユーザを使用してクラスタ・ノードにログインするために使用できます

VMware Tanzu Kubernetes Grid Service (TKGS) の概要

VMware Tanzu Kubernetes Grid Service (別名「Tanzu」) を使用すると、Tanzu KubernetesクラスタをvSphereでネイティブに作成および運用できます。また、一部の小規模なワークロードをESXiホストで直接実行することもできます。vSphereをプラットフォームに変換して、コンテナ化されたワークロードをハイパーバイザーレイヤでネイティブに実行できます。Tanzu Kubernetes Grid Serviceは、ワークロードに必要なクラスタを導入および運用することを有効にすると、vSphereにスーパーバイザクラスタを導入します。vSphere 7とネイティブに統合されており、vCenter SSO、コンテンツライブラリ、vSphereネットワーク、vSphereストレージ、vSphere HAおよびDRS

、vSphereセキュリティなど、信頼性の高いvSphereの機能を活用して、Kubernetesのシームレスなエクスペリエンスを実現します。

Tanzuを搭載したvSphereは、ハイブリッドアプリケーション環境向けの単一プラットフォームを提供します。このプラットフォームでは、コンテナ内またはVM内でアプリケーションコンポーネントを実行できるため、開発者、DevOpsエンジニア、およびvSphere管理者はより可視性が高く、運用が容易になります。VMware TKGSはvSphere 7環境でのみサポートされており、Tanzu Kubernetes運用ポートフォリオの中で、ESXiホストでポッドを直接実行できる唯一の製品です。



Tanzu Kubernetes Grid Serviceの詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。

機能セットやネットワークなどに関するアーキテクチャ上の考慮事項は多数あります。選択したアーキテクチャによっては、Tanzu Kubernetes Grid Serviceの前提条件と導入プロセスが異なります。このガイドに従って、環境にTanzu Kubernetes Grid Serviceを導入および設定してください ["こちらをご覧ください"](#)。さらに、TKGS経由で導入されたTanzu Kubernetesクラスタノードにログインするには、このに記載されている手順に従ってください ["リンク"](#)。

必要なワークロードの要件を満たすためには、ワーカーノードの構成を選択して、複数のマスター環境にすべての本番環境を導入してフォールトトレランスを実現することを推奨します。したがって、負荷の高いワークロードに推奨されるVMクラスには、少なくとも4つのvCPUと12GBのRAMがあります。

Tanzu Kubernetesクラスタがネームスペース内に作成されると、「owner」または「edit」権限を持つユーザーは、ユーザーアカウントを使用してポッドを任意のネームスペース内に直接作成できます。これは所有者または編集権限を持つユーザーにはクラスタ管理者の役割が割り当てられているためですただし、展開、デモンセツト、ステートフルセツト、またはその他の名前空間を作成する場合は、対応するサービスアカウントに必要な権限を持つロールを割り当てる必要があります。これは、展開またはデモンセツトがサービスアカウントを使用してポッドを展開するために必要です。

ClusterRoleBindingの次の例を参照して、クラスタ内のすべてのサービスアカウントにクラスタ管理者ロール

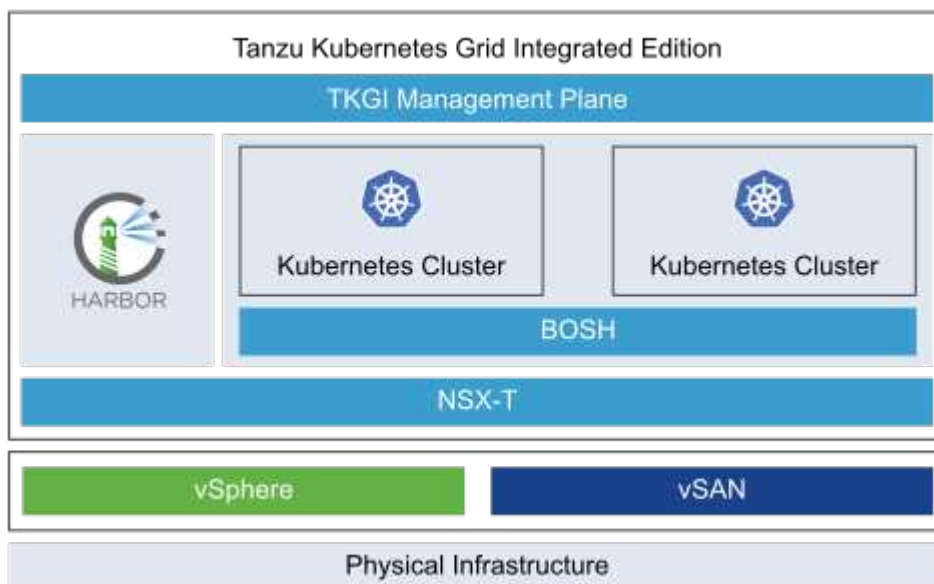
を割り当てます。

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: all_sa_ca
subjects:
- kind: Group
  name: system:serviceaccounts
  namespace: default
roleRef:
  kind: ClusterRole
  name: psp:vmware-system-privileged
  apiGroup: rbac.authorization.k8s.io
```

VMware Tanzu Kubernetes Grid Integrated Edition (TKGI) の概要

VMware Tanzu Kubernetes Grid Integrated (TKGI) Editionは、従来のVMware Enterprise PKSと呼ばれていた、スタンドアロンのコンテナオーケストレーションプラットフォームであり、ライフサイクル管理、クラスタの健全性監視、高度なネットワーク、コンテナレジストリなどの機能を備えています。TKGIは、BOSHとOps Managerで構成されるTKGIコントロールプレーンを使用してKubernetesクラスタをプロビジョニングおよび管理します。

TKGIは、オンプレミスのvSphere環境またはOpenStack環境、あるいは各IaaSサービス上の主要なパブリッククラウドのいずれかにインストールして操作できます。さらに、TKGIとNSXおよびNSXとの統合により、エンタープライズワークロードの幅広いユースケースが可能になります。TKGIとその機能の詳細については、のマニュアルを参照してください ["こちらをご覧ください"](#)。



TKGIは、さまざまなユースケースとデザインに基づいて、さまざまなプラットフォームにさまざまな構成で

インストールされています。ガイドに従ってください "[こちらをご覧ください](#)" TKGIとその前提条件をインストールおよび構成するには、次の手順に従います。TKGIは、改ざん不可の構成イメージを実行するTanzu Kubernetesクラスタのノードとして、Bosh VMを使用します。また、Bosh VMに対する手動変更は、リブート後も維持されません。

重要事項：

- NetApp Tridentでは、特権コンテナへのアクセスが必要です。そのため、TKGIのインストール中に、Tanzu Kubernetesクラスタノードプランを構成する手順でEnable Privileged Containers（特権コンテナを有効にする）チェックボックスを選択してください。

The screenshot displays the configuration page for TKGI worker nodes. It includes several sections with dropdown menus and checkboxes:

- Worker Node Instances:** Set to 3.
- Worker Persistent Disk Size:** Set to 50 GB.
- Worker Availability Zones:** Set to az (checked).
- Worker VM Type:** Set to medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB).
- Max Worker Node Instances:** Set to 50.
- Errand VM Type:** Set to medium.disk (cpu: 2, ram: 4 GB, disk: 32 GB).
- Enable Privileged Containers (Use with caution):** Checked.
- Admission Plugins:** PodSecurityPolicy and SecurityContextDeny are both unchecked.
- Cluster Services:** Four options are listed, all of which are checked:
 - Force node to drain even if it has running pods not managed by a ReplicationController, ReplicaSet, Job, DaemonSet or Stateful Set
 - Force node to drain even if it has running DaemonSet managed pods
 - Force node to drain even if it has running pods using emptyDir
 - Force node to drain even if pods are still running after timeout
- Node Drain Timeout (minutes, min: 0, max: 1440):** Set to 0.
- Pod Shutdown Grace Period (seconds, min: -1, max: 86400):** Set to 10.

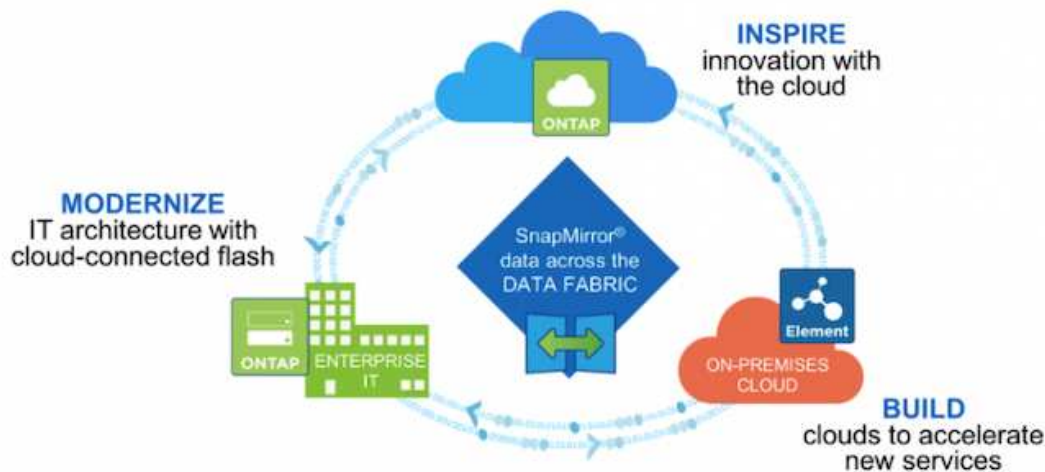
At the bottom, there are two buttons: "SAVE PLAN" and "DELETE".

- ワークロードの要件を満たすようにワーカーノードの構成を選択し、すべての本番環境を複数のマスター環境に導入してフォールトトレランスを実現することを推奨します。したがって、推奨されるTKGIクラスタ計画は、少なくとも3つのマスターと、少なくとも4つのvCPUと12GBのRAMを持つ3人のワーカーで構成され、負荷の高いワークロードを実現します。

ネットアップストレージシステムの概要

ネットアップには、Astra TridentとAstra Controlで認定された複数のストレージプラットフォームがあり、コンテナ化されたアプリケーションのデータをプロビジョニング、保護、管理し、DevOpsのスループットを定義して最大化するのに役立ちます。

ネットアップには、Astra TridentとAstra Controlで認定された複数のストレージプラットフォームがあり、コンテナ化されたアプリケーションのデータをプロビジョニング、保護、管理できます。



- AFF システムと FAS システムは、NetApp ONTAP を実行し、ファイルベース（NFS）とブロックベース（iSCSI）の両方のユースケースにストレージを提供します。
- Cloud Volumes ONTAP と ONTAP Select は、それぞれクラウドと仮想スペースに同じメリットをもたらします。
- NetApp Cloud Volumes Service（AWS / GCP）と Azure NetApp Files は、クラウドでファイルベースのストレージを提供します。



ネットアップのポートフォリオに含まれる各ストレージシステムでは、データ管理とオンプレミスサイトとクラウド間の移動の両方を容易に行えるため、データはアプリケーションの配置場所になります。

次のページでは、{solution_name} 解決策 で検証されたネットアップストレージシステムに関する追加情報を使用しています。

- ["NetApp ONTAP"](#)

NetApp ONTAP

NetApp ONTAP は、わかりやすい GUI、自動化統合機能を備えた REST API、AI に基づく予測分析と修正措置、無停止のハードウェアアップグレード、ストレージ間インポートなどの機能を備えた強力なストレージソフトウェアツールです。

NetApp ONTAP は、わかりやすい GUI、自動化統合機能を備えた REST API、AI に基づく予測分析と修正措置、無停止のハードウェアアップグレード、ストレージ間インポートなどの機能を備えた強力なストレージソフトウェアツールです。

NetApp ONTAP ストレージシステムの詳細については、を参照してください ["ネットアップの ONTAP Web サイト"](#)。

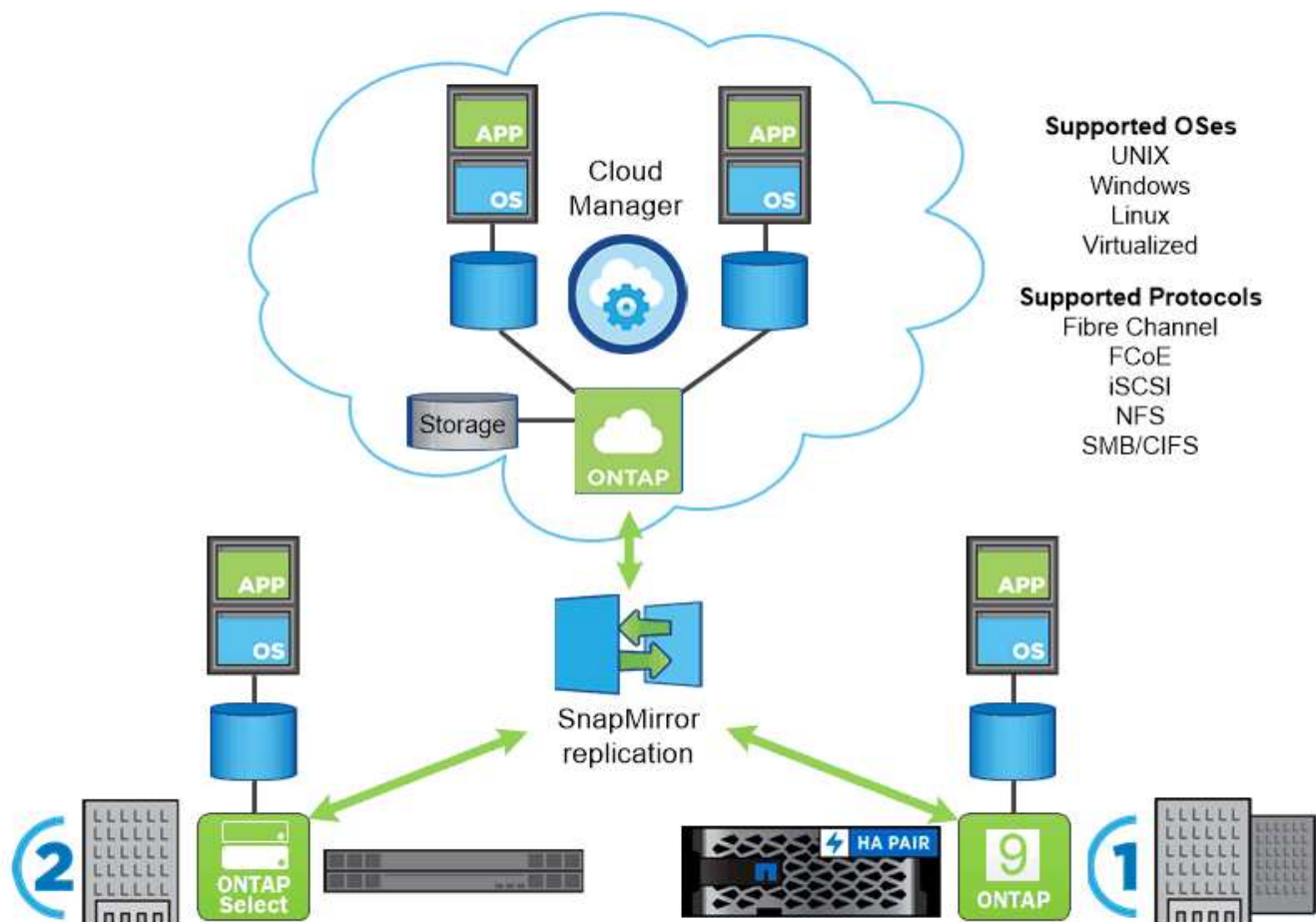
ONTAP は以下の機能を提供します。

- NFS、CIFS、iSCSI、FC、FCoE を同時にデータアクセスと管理できるユニファイドストレージシステム FC-NVMe プロトコルが必要です。
- 導入モデルには、オンプレミスのオールフラッシュ、ハイブリッド、オール HDD のハードウェア構成、ONTAP Select などのサポートされるハイパーバイザーを使用する VM ベースのストレージプラットフォーム、Cloud Volumes ONTAP などのクラウドがあります。
- ONTAP システムでは、データの自動階層化、インラインデータ圧縮、重複排除、コンパクションがサポートされ、データストレージ効率が向上しています。
- ワークロードベースの QoS 制御ストレージ：
- パブリッククラウドとのシームレスな統合により、データの階層化と保護を実現 ONTAP は、あらゆる環境に対応する堅牢なデータ保護機能も備えています。
 - * NetApp Snapshot コピー。* 最小限のディスク・スペースでデータをポイント・イン・タイムで高速バックアップし、パフォーマンス・オーバーヘッドを追加する必要はありません。
 - * NetApp SnapMirror。* 1 つのストレージ・システムから別のストレージ・システムへデータの Snapshot コピーをミラーリングします。ONTAP では、他の物理プラットフォームやクラウドネイティブのサービスへのデータのミラーリングもサポートされています。
 - * NetApp SnapLock。* 指定された期間にわたって上書きまたは消去できない特殊なボリュームに書き込むことにより、書き換え不可能なデータを効率的に管理します。
 - * NetApp SnapVault。* は、複数のストレージ・システムのデータを、指定されたすべてのシステムのバックアップとして機能する中央の Snapshot コピーにバックアップします。
 - * NetApp SyncMirror。* 同じコントローラに物理的に接続された 2 つの異なるディスクプレックスに対して、データをリアルタイムで RAID レベルでミラーリングします。
 - * NetApp SnapRestore * を使用すると、Snapshot コピーからオンデマンドでバックアップされたデータを迅速にリストアできます。
 - * NetApp FlexClone。* Snapshot コピーに基づいて、ネットアップボリュームの読み書き可能なフルコピーを瞬時にプロビジョニングできます。

ONTAP の詳細については、を参照してください ["ONTAP 9 ドキュメンテーション・センター"](#)。



NetApp ONTAP は、オンプレミス、仮想環境、クラウド環境で利用できます。



ネットアップのプラットフォーム

NetApp AFF/FAS

ネットアップは、堅牢なオールフラッシュ（AFF）およびスケールアウトハイブリッド（FAS）ストレージプラットフォームを提供し、低レイテンシのパフォーマンス、統合データプロテクション、マルチプロトコルのサポートのそれぞれに合わせてカスタマイズします。

どちらのシステムも、NetApp ONTAP データ管理ソフトウェアを搭載しています。NetAppは、シンプルで可用性の高いクラウド統合ストレージ管理を実現する業界最先端のデータ管理ソフトウェアで、データファブリックのニーズに合わせてエンタープライズクラスのスピード、効率性、セキュリティを提供します。

NetApp AFF / FAS プラットフォームの詳細については、をクリックしてください ["こちらをご覧ください"](#)。

ONTAP Select の場合

ONTAP Select は、お客様の環境のハイパーバイザーに導入できる、ソフトウェアで定義された NetApp ONTAP の導入です。VMware vSphereまたはKVMにインストールでき、ハードウェアベースのONTAP システムの全機能とエクスペリエンスを提供します。

ONTAP Select の詳細については、をクリックしてください ["こちらをご覧ください"](#)。

Cloud Volumes ONTAP

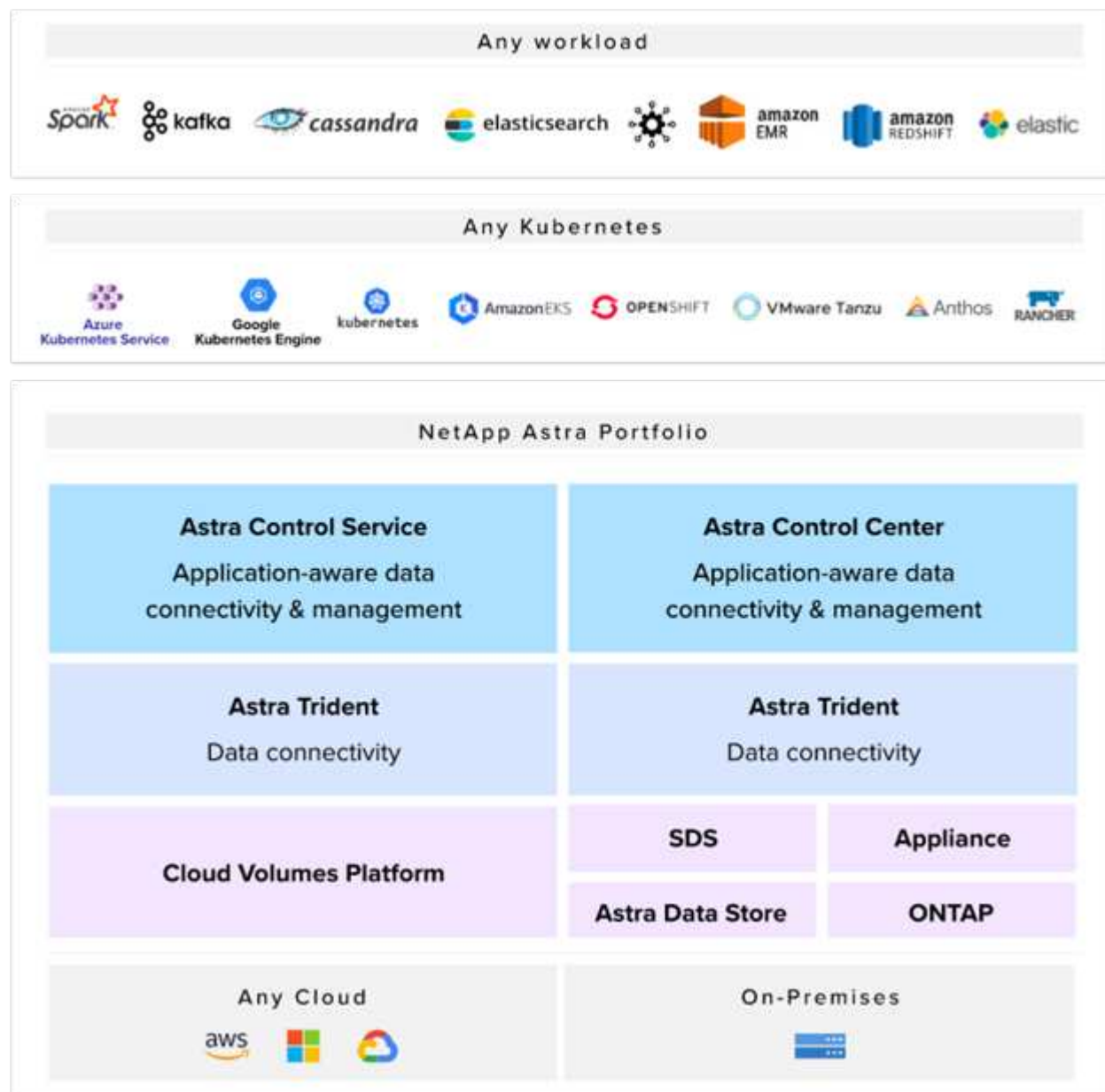
NetApp Cloud Volumes ONTAP は、クラウドで導入されるNetApp ONTAP のバージョンで、Amazon AWS、Microsoft Azure、Google Cloudなどのさまざまなパブリッククラウドに導入できます。

Cloud Volumes ONTAP の詳細については、をクリックしてください ["こちらをご覧ください"](#)。

ネットアップストレージ統合の概要

NetApp provides a number of products which assist our customers with orchestrating and managing persistent data in container based environments.

ネットアップは、ステートフルなコンテナ化アプリケーションとそのデータのオーケストレーション、管理、保護、移行を支援するための製品を多数提供しています。



NetApp Astra Controlは、ネットアップのデータ保護テクノロジーを基盤とするステートフルKubernetesワークロード向けに、充実したストレージサービスとアプリケーション対応データ管理サービスを提供します。Astra Control Service は、クラウドネイティブの Kubernetes 環境でステートフルワークロードをサポートするために利用できます。Astra Control Centerは、 {k8s_distribution_name} などのエンタープライズKubernetesプラットフォームをオンプレミスで導入する場合に、ステートフルワークロードをサポートするために使用できます。詳細については、NetApp Astra Control の Web サイトをご覧ください "[こちらをご覧ください](#)"。

NetApp Astra Tridentは、コンテナ向けのオープンソースで完全にサポートされているストレージオーケストレーションツールであり、 {k8s_distribution_name} などのKubernetesディストリビューションに対応しています。詳細については、Astra Trident の Web サイトをご覧ください "[こちらをご覧ください](#)"。

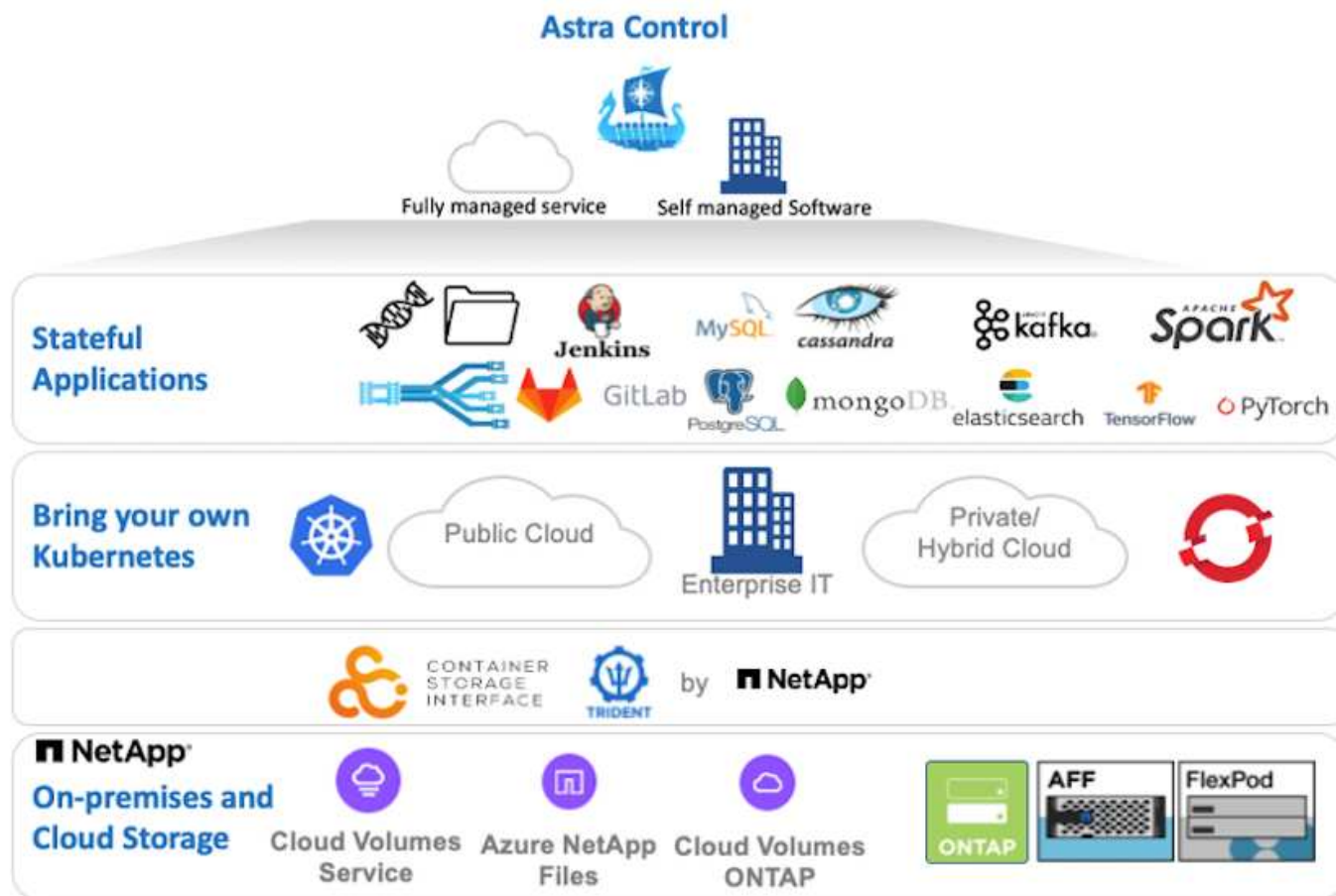
次のページには、 {solution_name} 解決策 でアプリケーションおよび永続的ストレージの管理用に検証されたネットアップ製品に関する追加情報 があります。

- "[ネットアップアストラコントロールセンター](#)"
- "[ネットアップアストラ Trident](#)"

NetApp Astra Controlの概要

NetApp Astra Control Centerは、ネットアップの信頼できるデータ保護テクノロジーを基盤とするオンプレミス環境に導入された、ステートフルKubernetesワークロード向けの豊富なストレージサービスとアプリケーション対応データ管理サービスを提供します。

NetApp Astra Control Center は、オンプレミス環境に導入され、ネットアップのデータ保護テクノロジーを基盤とするステートフル Kubernetes ワークロード向けの充実したストレージサービスとアプリケーション対応データ管理サービスを提供します。



NetApp Astra Control Centerは、Astra Tridentストレージオーケストレーションツールを導入して、NetApp ONTAP ストレージシステムにストレージクラスとストレージバックエンドで構成されている {k8s_distribution_name} クラスタにインストールできます。

Astra Tridentの詳細については、を参照してください ["このドキュメントはこちら"](#)。

クラウド接続環境では、Cloud Insights を使用して高度なモニタリングとテレメトリを提供します。Cloud Insights 接続がない場合は、限定的な監視と計測（7日間の指標）を使用でき、オープン指標エンドポイントを介してKubernetesの標準の監視ツール（PrometheusとGrafana）にエクスポートされます。

Astra Control Centerは、NetApp AutoSupportとActive IQのデジタルアドバイザー（デジタルアドバイザーとも呼ばれます）エコシステムに完全に統合されており、ユーザのサポート、トラブルシューティングの支援、使用状況の統計の表示を提供します。

支払い済みのAstra Control Centerに加えて、90日間の評価ライセンスも利用できます。評価版は、EメールとSlackコミュニティチャンネルを通じてサポートされます。お客様は、これらのリソース、その他のナレッジベース記事、および製品サポートダッシュボードから入手できるドキュメントにアクセスできます。

Astraポートフォリオの詳細については、を参照してください ["Astra の Web サイト"](#)。

Astra Control Center自動化

Astra Control Centerには、プログラム経由でアクセスするための完全に機能するREST APIが用意されています。任意のプログラミング言語またはユーティリティを使用して、Astra Control REST APIエンドポイントとやり取りできます。このAPIの詳細については、のドキュメントを参照してください ["こちらをご覧ください"](#)。

すぐに利用できる、Astra Control REST APIと連携するためのソフトウェア開発ツールキットを探している場合、ネットアップはAstra Control Python SDKのツールキットを提供しています。このツールキットはダウンロードが可能です ["こちらをご覧ください"](#)。

プログラミングが適していない状況で構成管理ツールを使用する場合は、ネットアップが公開しているAnsibleプレイブックをクローニングして実行できます ["こちらをご覧ください"](#)。

Astra Control Center のインストールの前提条件

Astra Control Centerのインストールには、次の前提条件が必要です。

- 1つ以上のTanzu Kubernetesクラスタは、管理クラスタまたはTKGSまたはTKGIによって管理されます。TKGワークロードクラスタ1.4 +およびTKGIユーザークラスタ1.12.2+がサポートされています。
- 各Tanzu KubernetesクラスタにAstra Tridentがインストールおよび設定されている必要があります。
- ONTAP 9.5 以降を実行している NetApp ONTAP ストレージシステムが 1 つ以上必要です。



サイトにある各Tanzu Kubernetesインストールでは、永続的ストレージ用の専用SVMを使用することを推奨します。マルチサイト環境では、追加のストレージシステムが必要です。

- Tridentストレージバックエンドは、ONTAP クラスタから作成されたSVMを含む各Tanzu Kubernetesクラスタで設定する必要があります。
- 各Tanzu Kubernetesクラスタに設定されたデフォルトのStorageClassには、Astra Tridentをストレージプロビジョニングツールとして使用します。
- ingressType 「AccTraefik」を使用している場合は、ロードバランシングとアストラコントロールセンターの公開のために、各Tanzu Kubernetesクラスタにロードバランサをインストールし、設定する必要があります。
- ingressType 「Generic」を使用している場合は、Astra Control Centerを公開するために、各Tanzu Kubernetesクラスタに入力コントローラをインストールし、設定する必要があります。
- NetApp アストラ Control Center イメージをホストするには、プライベートイメージのレジストリを設定する必要があります。
- Astra Control CenterをインストールしているTanzu Kubernetesクラスタにクラスタ管理者としてアクセスできる必要があります。
- NetApp ONTAP クラスタへの管理者アクセスが必要です。
- RHELまたはUbuntuの管理ワークステーション。

Astra Control Center をインストールします

この解決策 では、Ansibleプレイブックを使用してAstra Control Centerをインストールするための自動手順について説明します。手順を手動でインストールしてAstra Control Centerをインストールする場合は、詳細なインストールと操作のガイドに従ってください ["こちらをご覧ください"](#)。

1. Astra Control Centerを導入するAnsibleプレイブックを使用するには、AnsibleがインストールされたUbuntu / RHELマシンが必要です。手順に従います ["こちらをご覧ください"](#) UbuntuおよびRHELの場合。
2. Ansible コンテンツをホストする GitHub リポジトリをクローニングします。

```
git clone https://github.com/NetApp-
Automation/na_astra_control_suite.git
```

3. ネットアップサポートサイトにログインし、最新バージョンの NetApp Astra Control Center をダウンロードします。そのためには、ネットアップアカウントにライセンスを関連付ける必要があります。tar ファイルをダウンロードしたら、ワークステーションに転送します。



Astra Control の試用版ライセンスの使用を開始するには、にアクセスしてください "[Astra 登録サイト](#)"。

4. Astra Control CenterをインストールするユーザまたはワークロードのTanzu Kubernetesクラスタに管理者アクセスでkubeconfigファイルを作成または取得します。
5. ディレクトリを'na_Astra_control_site'に変更します

```
cd na_astra_control_suite
```

6. 「vars/vars.yml」 ファイルを編集し、必要な情報を変数に入力します。

```
#Define whether or not to push the Astra Control Center images to your
private registry [Allowed values: yes, no]
push_images: yes

#The directory hosting the Astra Control Center installer
installer_directory: /home/admin/

#Specify the ingress type. Allowed values - "AccTraefik" or "Generic"
#"AccTraefik" if you want the installer to create a LoadBalancer type
service to access ACC, requires MetalLB or similar.
#"Generic" if you want to create or configure ingress controller
yourself, installer just creates a ClusterIP service for traefik.
ingress_type: "AccTraefik"

#Name of the Astra Control Center installer (Do not include the
extension, just the name)
astra_tar_ball_name: astra-control-center-22.04.0

#The complete path to the kubeconfig file of the kubernetes/openshift
cluster Astra Control Center needs to be installed to.
hosting_k8s_cluster_kubeconfig_path: /home/admin/cluster-kubeconfig.yml

#Namespace in which Astra Control Center is to be installed
astra_namespace: netapp-astra-cc

#Astra Control Center Resources Scaler. Leave it blank if you want to
```

```

accept the Default setting.
astra_resources_scaler: Default

#Storageclass to be used for Astra Control Center PVCs, it must be
created before running the playbook [Leave it blank if you want the PVCs
to use default storageclass]
astra_trident_storageclass: basic

#Reclaim Policy for Astra Control Center Persistent Volumes [Allowed
values: Retain, Delete]
storageclass_reclaim_policy: Retain

#Private Registry Details
astra_registry_name: "docker.io"

#Whether the private registry requires credentials [Allowed values: yes,
no]
require_reg_creds: yes

#If require_reg_creds is yes, then define the container image registry
credentials
#Usually, the registry namespace and usernames are same for individual
users
astra_registry_namespace: "registry-user"
astra_registry_username: "registry-user"
astra_registry_password: "password"

#Kuberenets/OpenShift secret name for Astra Control Center
#This name will be assigned to the K8s secret created by the playbook
astra_registry_secret_name: "astra-registry-credentials"

#Astra Control Center FQDN
acc_fqdn_address: astra-control-center.cie.netapp.com

#Name of the Astra Control Center instance
acc_account_name: ACC Account Name

#Administrator details for Astra Control Center
admin_email_address: admin@example.com
admin_first_name: Admin
admin_last_name: Admin

```

7. プレイブックを実行して Astra Control Center を導入します。Playbookには、特定の構成用のroot権限が必要です。

プレイブックを実行しているユーザがrootである場合、またはパスワードなしのsudoが設定されている場合は、次のコマンドを実行してプレイブックを実行します。

```
ansible-playbook install_acc_playbook.yml
```

ユーザにパスワードベースのsudoアクセスが設定されている場合は、次のコマンドを実行してこのPlaybookを実行し、sudoパスワードを入力します。

```
ansible-playbook install_acc_playbook.yml -K
```

インストール後の手順

1. インストールが完了するまでに数分かかることがあります。NetApp-Astra-cc' ネームスペース内のすべてのポッドとサービスが稼働していることを確認します

```
[netapp-user@rhel7 ~]$ kubectl get all -n netapp-astra-cc
```

2. 「acc-operator-controller-manager」ログをチェックし、インストールが完了したことを確認します。

```
[netapp-user@rhel7 ~]$ kubectl logs deploy/acc-operator-controller-  
manager -n netapp-acc-operator -c manager -f
```



次のメッセージは、Astra Control Center のインストールが正常に完了したことを示します。

```
{"level":"info","ts":1624054318.029971,"logger":"controllers.AstraControlCenter","msg":"Successfully Reconciled AstraControlCenter in [seconds]s","AstraControlCenter":"netapp-astra-cc/astra","ae.Version":"[22.04.0]"}
```

3. Astra Control Center にログインするためのユーザ名は、CRD ファイルに提供された管理者の電子メールアドレスで、パスワードは Astra Control Center UUID に付加された文字列「ACC-」です。次のコマンドを実行します。

```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc  
NAME      UUID  
astra     345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```



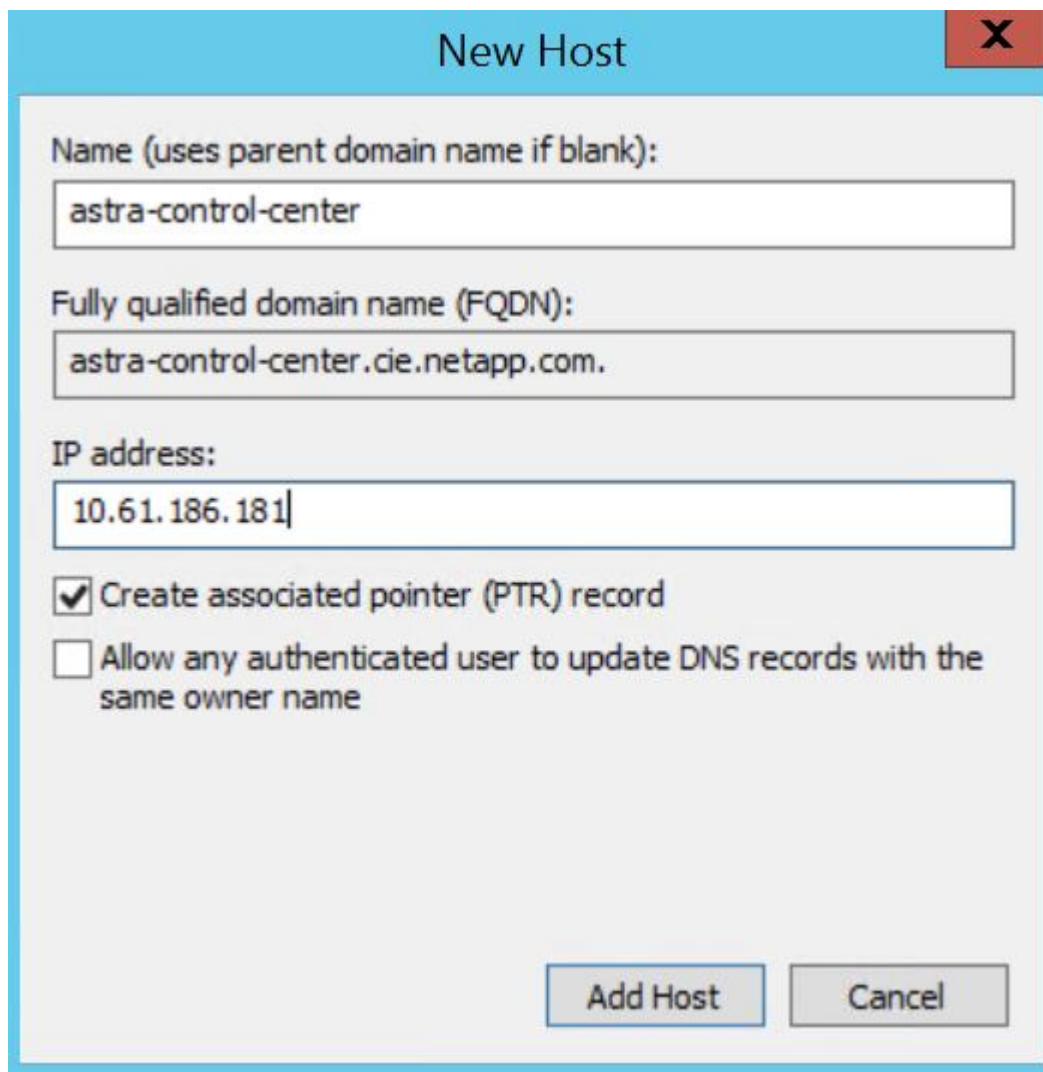
この例では、パスワードは「ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f」です。

4. ingressTypeがAccTraefikの場合は、traefikサービスロードバランサIPを取得します。

```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep  
'EXTERNAL|traefik'
```

NAME	EXTERNAL-IP	PORT(S)	TYPE	CLUSTER-IP
traefik	10.61.186.181	80:30343/TCP, 443:30060/TCP	LoadBalancer	172.30.99.142
AGE 16m				

5. Astra Control Center CRD ファイルに指定された FQDN を指す DNS サーバーのエントリを、traefik サービスの「external-IP」に追加します。



New Host

Name (uses parent domain name if blank):
astra-control-center

Fully qualified domain name (FQDN):
astra-control-center.cie.netapp.com.

IP address:
10.61.186.181

☒ Create associated pointer (PTR) record

☐ Allow any authenticated user to update DNS records with the same owner name

Add Host Cancel

6. Astra Control Center GUI に、FQDN を参照してログインします。

NetApp

Astra Control Center

Log In to NetApp Astra Control Center

Email

Password

LOGIN

Manage, protect,
and migrate your
Kubernetes
applications with
just a few clicks!

7. CRD で提供された管理者メールアドレスを使用して初めて Astra Control Center GUI にログインする場合は、パスワードを変更する必要があります。

NetApp

Astra Control Center

Welcome to NetApp Astra Control Center

Update your password to proceed

.....

.....

Passwords must contain:

- At least 8 characters
- No more than 64 characters
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

UPDATE PASSWORD

Manage, protect, and
migrate your Kubernetes
applications with just a
few clicks!

8. ユーザーを Astra Control Center に追加する場合は、[アカウント]>[ユーザー] の順に選択し、[追加] をクリックしてユーザーの詳細を入力し、[追加] をクリックします。

Add user

USER DETAILS

First name: Nikhil

Last name: Kulkarni

Email address: tme_nik@netapp.com

PASSWORD

Temporary password:

Confirm temporary password:

Passwords must contain:

- At least 8 characters
- No more than 64 characters
- At least one lowercase letter
- At least one uppercase letter
- At least one number
- At least one special character

USER ROLE

Role: Owner

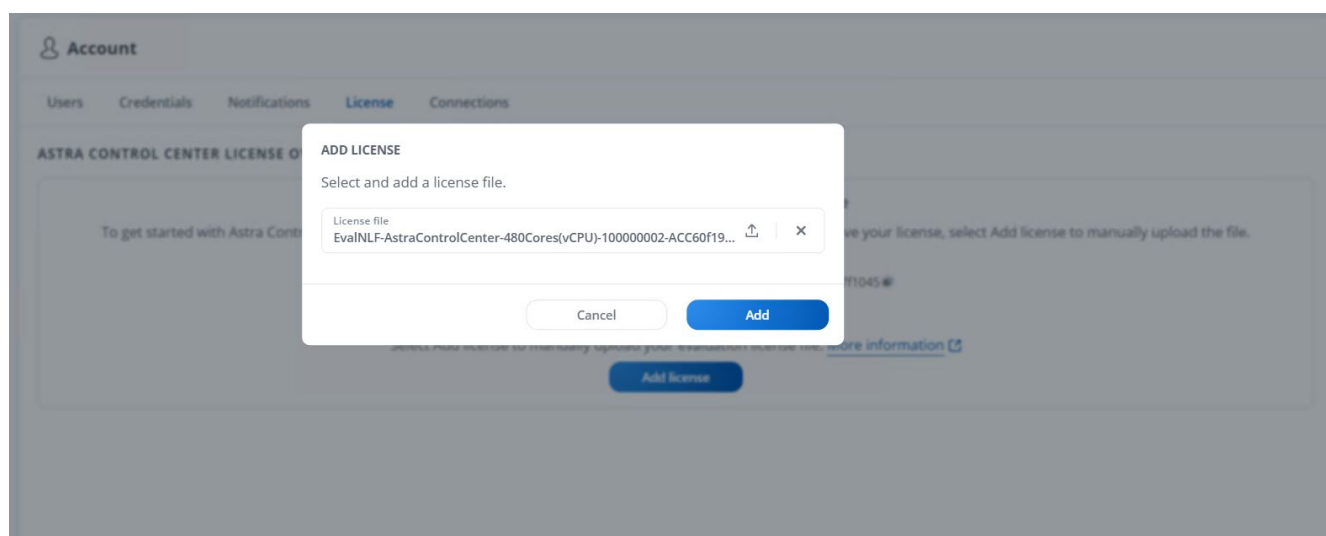
Buttons: Cancel, Add

ADD NEW USER

Add new user

Add a new user to your Astra Control Center account. New users will be prompted to update their password the first time they log in to Astra Control Center. They will also inherit access to account-wide credentials according to their role. Read more in [users](#).

9. Astra Control Centerのすべての機能が動作するには、ライセンスが必要です。ライセンスを追加するには、[アカウント] > [ライセンス] の順に選択し、[ライセンスの追加] をクリックして、ライセンスファイルをアップロードします。




NetApp Astra Control Center のインストールまたは設定で問題が発生した場合は、既知の問題のナレッジベースを利用できます ["こちらをご覧ください"](#)。

VMware Tanzu Kubernetes クラスタを **Astra Control Center** に登録します

Astra Control Center でワークロードを管理できるようにするには、まず Tanzu Kubernetes クラスタを登録する必要があります。

VMware Tanzu Kubernetes クラスタを登録します

1. 最初の手順は、Tanzu Kubernetes クラスタを Astra Control Center に追加して管理することです。[クラスタ] に移動して [クラスタの追加] をクリックし、Tanzu Kubernetes クラスタの kubeconfig ファイルをアップロードして、[ストレージの選択] をクリックします。

 **Add Kubernetes cluster**

STEP 1/3: CREDENTIALS

×

CREDENTIALS

Provide Astra Control access to your Kubernetes and OpenShift clusters by entering a kubeconfig credential.

Follow [instructions](#) on how to create a dedicated admin-role kubeconfig.

[Upload file](#) [Paste from clipboard](#)

Kubeconfig YAML file
tkgi-kubeconfig.txt

↑ ×

Credential name
tkgi-acc

ADDING CLUSTERS

Adding a cluster allows Astra Control to install its storage services, and enable data management operations on your containerized applications.


For more details on required versions or cloud specific setup refer to the documentation.

Read more in [Adding clusters](#).

Cancel

Next →

2. Astra Control Center で、対象となるストレージクラスが検出される。次に、ストレージクラスが NetApp ONTAP 上の SVM がサポートする Trident を使用してボリュームをプロビジョニングする方法を選択し、Review（確認）をクリックします。次のペインで詳細を確認し、Add Cluster をクリックします。
3. クラスタが追加されると、Astra Control Center がクラスタを検査し、必要なエージェントをインストールしながら、クラスタは Discovering ステータスに移行します。正常に登録されると、クラスタ・ステータスは「Healthy」に変わります。



 **Clusters**

Actions ▾

+ Add Kubernetes cluster

Search

1-1 of 1 entries < >

<input type="checkbox"/>	Name ↓	State	Type	Version	Actions
<input type="checkbox"/>	tkgi-acc	Healthy	 Kubernetes	v1.22.6+vmware.1	



Astra Control Center で管理するすべての Tanzu Kubernetes クラスタは、管理対象クラスタにインストールされたエージェントとしてそのインストールに使用されたイメージレジストリにアクセスする必要があります。このレジストリからイメージがプルされます。

4. ONTAP クラスタをストレージリソースとして Astra Control Center でバックエンドとして管理するようにインポートします。Tanzu Kubernetes クラスタが Astra に追加され、ストレージクラスが設定されている

場合、ストレージクラスをサポートするONTAP クラスタは自動的に検出されて検査されますが、管理対象のAstraコントロールセンターにはインポートされません。

Backends

+ Add

Search

★

🔍

1

1-1 of 1 entries

Name ↓	State	Capacity	Throughput	Type	Cluster	Cloud	Actions
172.21.224.201(trident)	<div><div></div><div>Discovered</div></div>	Not available yet	Not available yet	ONTAP	Not applicable	Not applicable	<div><div></div></div>

5. ONTAP クラスタをインポートするには、バックエンドに移動し、ドロップダウンをクリックして、管理対象のONTAP クラスタの横にあるManageを選択します。ONTAP クラスタの資格情報を入力し、[情報の確認] をクリックして、[ストレージバックエンドのインポート] をクリックします。

Manage ONTAP storage backend

STEP 1/2: CREDENTIALS

CREDENTIALS

Enter cluster administrator credentials for the ONTAP storage backend you want to manage.

Cluster management IP address

172.21.224.201

User name

admin

Password

MANAGING STORAGE BACKENDS

Storage backends provide storage to your Kubernetes applications.

Managing storage clusters in Astra Control as a storage backend will allow you to get linkages between PVs and the storage backend. You will also see capacity and health details of the storage backend, including performance metrics if Astra Control is connected to Cloud Insights.

Read more in [Storage type](#) .

ONTAP

Cancel

Next →


6. バックエンドを追加すると、ステータスが Available に変わります。これらのバックエンドには、Tanzu Kubernetesクラスタ内の永続ボリュームおよびONTAP システム上の対応するボリュームに関する情報が含まれるようになりました。

289

Backends


</

7. Astra Control Centerを使用してTanzu Kubernetesクラスタ間でバックアップおよびリストアを実行するには、S3プロトコルをサポートするオブジェクトストレージバケットをプロビジョニングする必要があります。現在サポートされているオプションは、ONTAP S3、StorageGRID、AWS S3、およびMicrosoft Azure Blob Storageです。このインストールのために、AWS S3 バケットを設定します。バケットに移動し、バケットの追加をクリックして、汎用 S3 を選択します。S3バケットとクレデンシャルの詳細を入力してアクセスし、Make this Bucket the Default Bucket for the Cloud（このバケットをクラウドのデフォルトバケットにする）チェックボックスをオンにして、Add（追加）をクリックします。

 **Add bucket**

Enter the access details of your existing object store bucket to allow Astra Control to store your application backups.

Type

 Generic S3

Existing bucket name

na-tanzu-astra/na-astra-tkgi

Description (optional)

S3 server name or IP address

s3.us-east-1.amazonaws.com

☒ Make this bucket the default bucket for this cloud

?

SELECT CREDENTIALS

Astra Control requires S3 access credentials with the roles necessary to facilitate Kubernetes application data management.


Add

Use existing

Select credential

AWS Creds

Cancel

Add 

BUCKETS

Astra Control stores backups in your existing object store buckets. The first bucket added for a selected cloud will be designated as the default bucket for backup and clone operations.

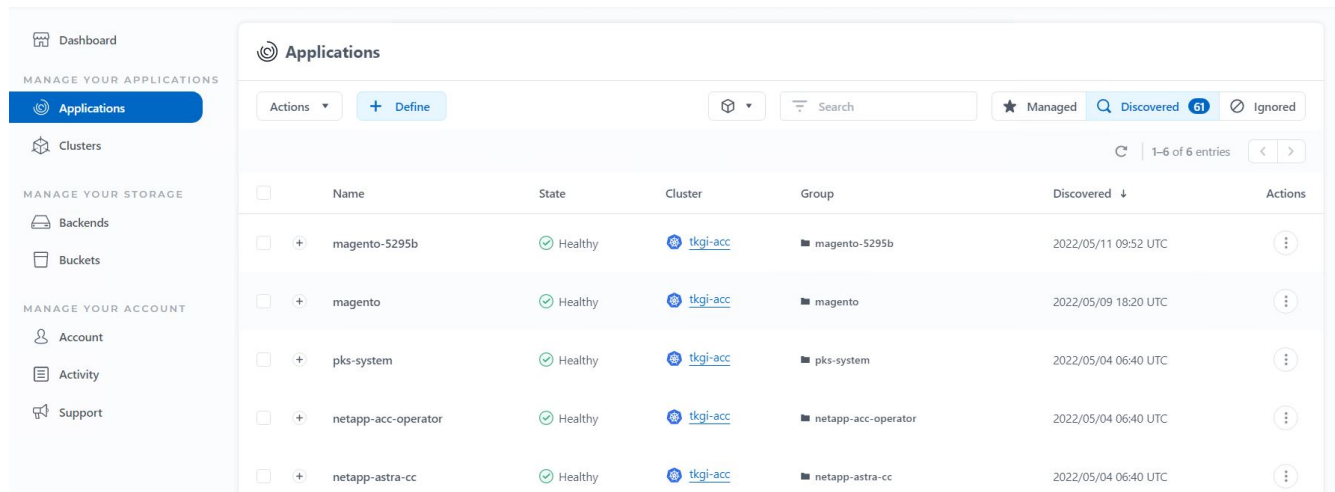
Read more in [Storage buckets](#).

保護するアプリケーションを選択します

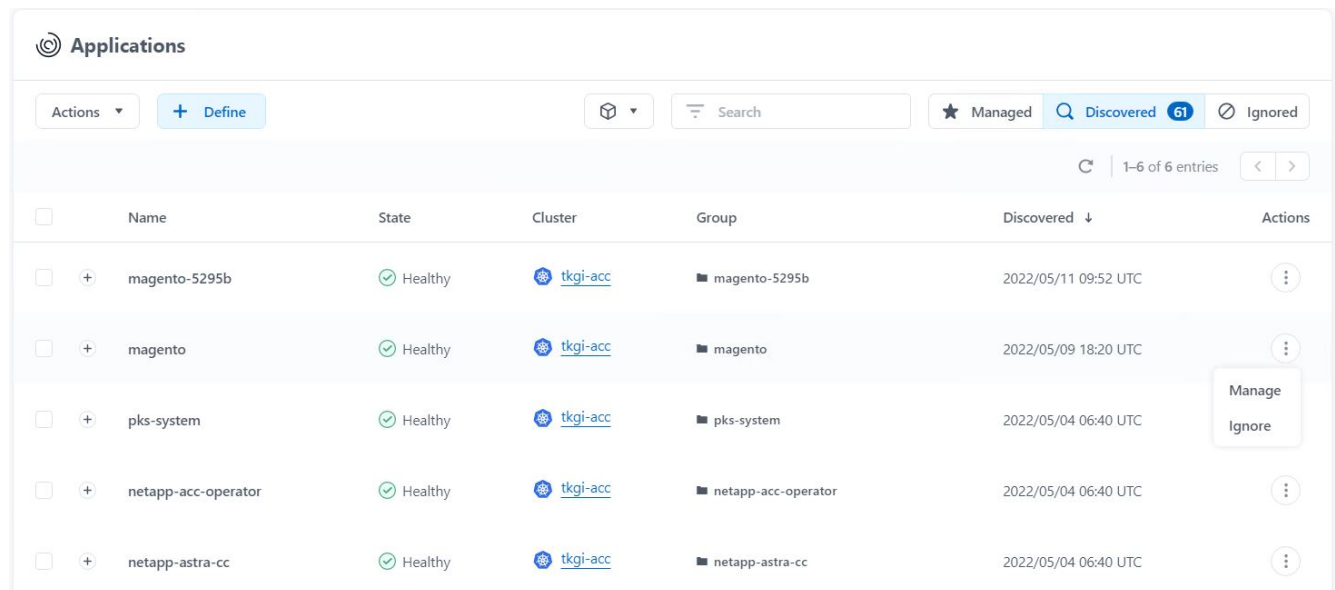
Tanzu Kubernetesクラスタを登録したら、Astra Control Centerを使用して導入および管理されているアプリケーションを検出できます。

アプリケーションを管理します

1. Tanzu KubernetesクラスタとONTAP バックエンドがAstraコントロールセンターに登録されると、コントロールセンターは指定されたONTAP バックエンドで構成されたストレージクラスを使用しているすべてのネームスペース内のアプリケーションを自動的に検出します。



2. [アプリケーション] > [検出済み] の順に移動し、Astra を使用して管理するアプリケーションの横にあるドロップダウンメニューをクリックします。[管理] をクリックします。



3. アプリケーションが[使用可能 (Available)] 状態になり、[アプリケーション (Apps)] セクションの[管理 (Managed)] タブで表示できます。

Applications

Actions ▾

+ Define

All clusters ▾

Search

★ Managed

Q

Discovered60

⌕

Ignored

↺

1-1 of 1 entries

⏪

⏩

<input type="checkbox"/>	Name	State	Protection	Cluster	Group	Discovered ↓	Actions
<input type="checkbox"/>	magento	<div>✓ Healthy</div>	<div>⚠ Unprotected</div>	<div>tkgi-acc</div>	<div>📁 magento</div>	2022/05/09 18:20 UTC	<div>⋮</div>

アプリケーションを保護

アプリケーションワークロードを Astra Control Center で管理した後、それらのワークロードの保護設定を構成できます。

アプリケーションスナップショットを作成します

アプリケーションのSnapshotコピーを作成すると、ONTAP Snapshotコピーとアプリケーションメタデータのコピーが作成されます。このコピーを使用して、アプリケーションを特定の時点の状態にリストアまたはクローニングできます。

1. アプリケーションのスナップショットを作成するには、[アプリ] > [管理] タブに移動し、Snapshot コピーを作成するアプリケーションをクリックします。アプリケーション名の横にあるドロップダウンメニューをクリックし、Snapshot をクリックします。

APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Unprotected

Images

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61
 docker.io/bitnami/magento:2.4.1-debian-10-r14
 docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule

Disabled

Group

magento

Cluster

tkgi-acc

Actions ▾

Snapshot

Backup

Clone

Restore

Unmanage

2. スナップショットの詳細を入力し、[次へ] をクリックして、[スナップショット] をクリックします。Snapshot の作成には約 1 分かかり、作成が完了するとステータスを確認できるようになります。

Snapshot namespace application

STEP 1/2: DETAILS

✕

SNAPSHOT DETAILS

Name

magento-snapshot-20220516212403

CREATING APPLICATION SNAPSHOTS

Astra Control can take a quick snapshot of your application configuration and persistent storage. Enter a snapshot name to get started.

Read more in [Protect apps](#)

Namespace application
magento

Namespace
magento

Cluster
tkgi-acc

Cancel

Next →

アプリケーションのバックアップを作成します

アプリケーションのバックアップは、アプリケーションのアクティブな状態とそのリソースの設定をキャプチャしてファイルに変換し、リモートのオブジェクトストレージバケットに格納します。

1. Astra Control Center で管理対象アプリケーションのバックアップとリストアを行うには、バックアップ ONTAP システムのスーパーユーザ設定を前提条件として設定する必要があります。そのためには、次のコマンドを入力します。

```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1
-anon 65534 -vserver ocp-trident
```

2. Astra Control Center で管理対象アプリケーションのバックアップを作成するには、[アプリ] > [管理] タブに移動し、バックアップを作成するアプリケーションをクリックします。アプリケーション名の横にあるドロップダウンメニューをクリックし、[バックアップ] をクリックします。

magento

Actions

Snapshot

Backup

Clone

Restore

Unmanage

APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Unprotected

Images
docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61
docker.io/bitnami/magento:2.4.1-debian-10-r14
docker.io/bitnami/mariadb:10.3.24-debian-10-r49


Protection schedule
Disabled

Group
 magento

Cluster
 tkgi-acc

3. バックアップの詳細を入力し、バックアップファイルを保存するオブジェクトストレージバケットを選択して次へをクリックします。詳細を確認したら、バックアップをクリックします。アプリケーションのサイズとデータによっては、バックアップに数分かかることがあり、バックアップが正常に完了したあとで

バックアップのステータスを確認できるようになります。

 **Back up namespace application**

STEP 1/2: DETAILS

×

BACKUP DETAILS

Name
magento-backup-20220516212622

☐ Back up from an existing snapshot ?

BACKUP DESTINATION

Bucket
na-tanzu-astro/na-astro-tkgi Available Default

CREATING APPLICATION BACKUPS

Astra Control can take a backup of your application configuration and persistent storage. Persistent storage backups are transferred to your object store. Enter a backup name to get started.

Read more in [Application backups](#).

Namespace application
magento

Namespace
magento

Cluster
tkgi-acc


Cancel

Next →

アプリケーションのリストア


ボタンを押すだけで、アプリケーションを同じクラスタ内の元のネームスペースまたはリモートクラスタにリストアし、アプリケーションを保護してディザスタリカバリに使用できます。


1. アプリケーションを復元するには、[アプリ]>[管理]タブに移動し、該当するアプリをクリックします。アプリケーション名の横にあるドロップダウンメニューをクリックし、[復元]をクリックします。

 **magento**

🔄

Actions ▼

 **APPLICATION STATUS**
Healthy

 **APPLICATION PROTECTION STATUS**
Unprotected

Images
docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61
docker.io/bitnami/magento:2.4.1-debian-10-r14
docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule
Disabled

Group
magento

Cluster
tkgi-acc

2. リストアネームスペースの名前を入力し、リストア先のクラスタを選択して、既存の Snapshot からリストアするかアプリケーションのバックアップからリストアするかを選択します。次へをクリックします。

Restore namespace application

STEP 1/2: DETAILS

✕

RESTORE DETAILS

Destination cluster

tkgi-acc

Destination namespace

magento

RESTORE SOURCE

Filter

Snapshots

Backups

Application backup	State	On-Schedule/On-Demand	Created ↑
<input type="radio"/> <div>magento-backup-20220516212730</div>	<div>✓</div> <div>Healthy</div>	<div>🕒</div> <div>On-Demand</div>	2022/05/16 21:27 UTC

RESTORING APPLICATIONS

Astra Control can restore your application configuration and persistent storage. Select a source snapshot or backup for the restored application.

🕒 Namespace application

magento

📁 Namespace

magento

🌐 Cluster

tkgi-acc

Cancel

Next →

- レビューペインで「restore」と入力し、詳細を確認した後で「Restore」をクリックします。

Restore namespace application

STEP 2/2: SUMMARY

✕

REVIEW RESTORE INFORMATION

⚠️

All existing resources associated with this namespace application will be deleted and replaced with the source backup "magento-backup-20220516212730" taken on 2022/05/16 21:27 UTC. Persistent volumes will be deleted and recreated. External resources with dependencies on this namespace application might be impacted.

We recommend taking a snapshot or a backup of your namespace application before proceeding.

🕒 BACKUP

magento-backup-20220516212730

📁 ORIGINAL GROUP

■ magento

🌐 ORIGINAL CLUSTER

tkgi-acc

🔗 RESOURCE LABELS

Config Maps

app.kubernetes.io/name: elasticsearch +9

Deployments

🕒 RESTORE

magento

📁 DESTINATION GROUP

■ magento

🌐 DESTINATION CLUSTER

tkgi-acc

🔗 RESOURCE LABELS

Config Maps

app.kubernetes.io/name: elasticsearch +9

Deployments

Are you sure you want to restore the namespace application "magento"?

Type restore below to confirm.

Confirm to restore

restore

← Back

Restore ✓

- 新しいアプリケーションは、Astra Control Center が選択したクラスタ上のアプリケーションを復元している間、Restoring 状態になります。アプリケーションのすべてのリソースが Astra によってインストールおよび検出されると、アプリケーションは Available 状態になります。

Applications

Actions

+ Define

All clusters

Search

Managed

Discovered 60

Ignored

1-1 of 1 entries

<input type="checkbox"/>	Name	State	Protection	Cluster	Group	Discovered ↓	Actions
<input type="checkbox"/>	magento	Healthy	Unprotected	tkgi-acc	magento	2022/05/09 18:20 UTC	

アプリケーションのクローニング

アプリケーションは、開発 / テストやアプリケーションの保護およびディザスタリカバリ目的で、元のクラスタまたはリモートクラスタにクローニングできます。同じストレージバックエンドで同じクラスタ内にあるアプリケーションをクローニングする場合、NetApp FlexClone テクノロジを使用します。FlexClone テクノロジを使用すると、PVC のクローンを瞬時に作成し、ストレージスペースを節約できます。

1. アプリケーションをクローンするには、[アプリケーション (Apps)] > [管理 (Managed)] タブに移動し、該当するアプリケーションをクリックします。アプリケーション名の横にあるドロップダウンメニューをクリックし、Clone をクリックします。

APPLICATION STATUS

Healthy

APPLICATION PROTECTION STATUS

Unprotected

Images

docker.io/bitnami/elasticsearch:6.8.12-debian-10-r61
docker.io/bitnami/magento:2.4.1-debian-10-r14
docker.io/bitnami/mariadb:10.3.24-debian-10-r49

Protection schedule

Disabled

Group

magento

Cluster

tkgi-acc

Actions

Snapshot
Backup
Clone
Restore
Unmanage

2. 新しいネームスペースの詳細を入力し、クローニング先のクラスタを選択します。クローンを既存のSnapshotから作成するか、バックアップから作成するか、アプリケーションの現在の状態から作成するかを選択します。詳細を確認したら、[次へ]をクリックし、確認ペインの[複製]をクリックします。

Clone namespace application

STEP 1/2: DETAILS

×

CLONE DETAILS

Clone namespace
magento-bef7f

Destination cluster
tkgi-acc

☐ Clone from an existing snapshot or backup

Cancel

Next →

CLONING APPLICATIONS

Astra Control can create a clone of your application configuration and persistent storage. Persistent storage backups are transferred from your object store, so choosing a clone from an existing backup will complete the fastest. Enter a clone name to get started.

Not all applications may support cloning.

Read more in [Clone applications](#).

Namespace application
magento

Namespace
magento

Cluster
tkgi-acc

3. 新しいアプリケーションは Discovering 状態になり、Astra Control Center は選択したクラスタにアプリケーションを作成します。アプリケーションのすべてのリソースが Astra によってインストールおよび検出されると、アプリケーションは Available 状態になります。

Applications

Actions ▾

+ Define

All clusters ▾

Search

★ Managed

Q Discovered 60

Ignored

1-2 of 2 entries

< >

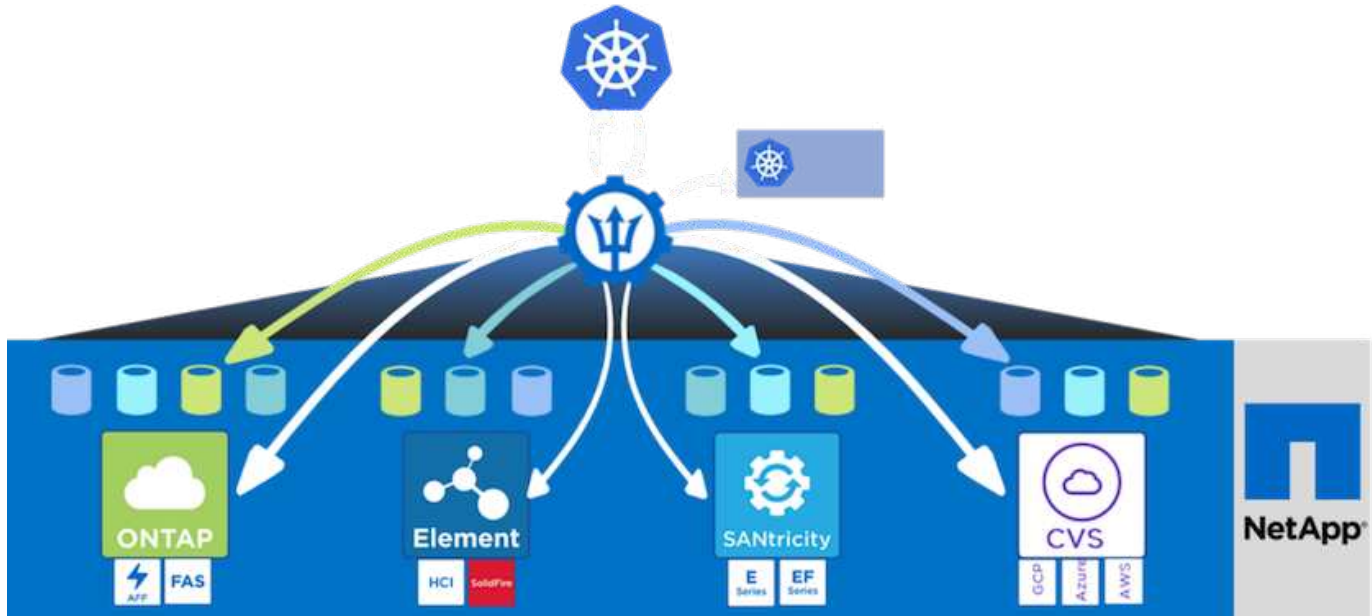
<input type="checkbox"/>	Name	State	Protection	Cluster	Group	Discovered ↓	Actions
<input type="checkbox"/>	magento-bef7f	Healthy	Unprotected	tkgi-acc	magento-bef7f	2022/05/16 21:31 UTC	⋮
<input type="checkbox"/>	magento	Healthy	Partially protected	tkgi-acc	magento	2022/05/09 18:20 UTC	⋮

Astra Tridentの概要

Astra Tridentは、VMware TanzuなどのコンテナやKubernetesディストリビューション向けの、オープンソースで完全にサポートされているストレージオーケストレーションツールです。

Astra Tridentは、コンテナやKubernetesディストリビューション向けの、完全にサポートされているオープンソースのストレージオーケストレーションツールです。{k8s_distribution_name}などが挙げられます。Tridentは、NetApp ONTAPやElementストレージシステムを含むネットアップストレージポートフォリオ全体と連携し、NFS接続とiSCSI接続もサポートします。Tridentを使用すると、ストレージ管理者の手を煩わせることなく、エンドユーザがネットアップストレージシステムからストレージをプロビジョニングして管理できるため、DevOpsワークフローが高速化されます。

管理者は、プロジェクトのニーズやストレージシステムモデルに基づいて複数のストレージバックエンドを構成し、圧縮、特定のディスクタイプ、QoS レベルなどの高度なストレージ機能を有効にして一定のレベルのパフォーマンスを保証できます。定義されたバックエンドは、プロジェクトの開発者が永続的ボリューム要求（PVC）を作成し、永続的ストレージをオンデマンドでコンテナに接続するために使用できます。



Astra Tridentは、迅速な開発サイクルを実現し、Kubernetesと同様、年間4回リリースされます。

Tridentの最新バージョンは2022年4月に22.04にリリースされました。Trident のどのバージョンがサポートされているかを確認できます Kubernetes ディストリビューションのテストに使用 [こちらをご覧ください](#)。

20.04 リリース以降、Trident のセットアップは Trident オペレータによって実行されます。オペレータが大規模な導入を容易にし、Tridentのインストールの一部として導入されるポッドの自己修復などの追加サポートを提供します。

21.01 リリースでは、Trident Operator のインストールを容易にするために Helm チャートを使用できるようになりました。

Helmを使用してTridentオペレータを導入

1. Trident にはこのファイルを渡すオプションがないため、まず、ユーザクラスタの「kubeconfig」ファイルの場所を環境変数として設定します。

```
[netapp-user@rhel7]$ export KUBECONFIG=~/.tanzu-install/auth/kubeconfig
```

2. NetApp Astra Trident Helmリポジトリを追加

```
[netapp-user@rhel7]$ helm repo add netapp-trident  
https://netapp.github.io/trident-helm-chart  
"netapp-trident" has been added to your repositories
```

3. Helmリポジトリを更新します。

```
[netapp-user@rhel7]$ helm repo update
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "netapp-trident" chart repository
...Successfully got an update from the "bitnami" chart repository
Update Complete. ☐Happy Helming!☐
```

4. Tridentをインストールするための新しいネームスペースを作成します。

```
[netapp-user@rhel7]$ kubectl create ns trident
```

5. DockerHubのクレデンシャルを使用してシークレットを作成し、Astra Tridentイメージをダウンロードします。

```
[netapp-user@rhel7]$ kubectl create secret docker-registry docker-registry-cred --docker-server=docker.io --docker-username=netapp-solutions-tme --docker-password=xxxxxxx -n trident
```

6. TKGS (vSphere with Tanzu) またはTKG (管理クラスタを含む) で管理されるユーザまたはワークロードクラスタの場合、次の手順 を実行してAstra Tridentをインストールします。
- ログインしているユーザに、tridentネームスペースにサービスアカウントを作成する権限があり、tridentネームスペースのサービスアカウントにポッドを作成する権限があることを確認します。
 - 以下のHelmコマンドを実行し、作成したネームスペースにTridentオペレータをインストールします。

```
[netapp-user@rhel7]$ helm install trident netapp-trident/trident-operator -n trident --set imagePullSecrets[0]=docker-registry-cred
```

7. TKGI導入によって管理されるユーザまたはワークロードクラスタの場合は、次のHelmコマンドを実行して、作成されたネームスペースにTridentオペレータをインストールします。

```
[netapp-user@rhel7]$ helm install trident netapp-trident/trident-operator -n trident --set imagePullSecrets[0]=docker-registry-cred,kubeletDir="/var/vcap/data/kubelet"
```

8. Tridentポッドが稼働中であることを確認します。

NAME	READY	STATUS	RESTARTS
AGE			
trident-csi-6vv62	2/2	Running	0
14m			
trident-csi-cfd844bcc-sqhcg	6/6	Running	0
12m			
trident-csi-dfcmz	2/2	Running	0
14m			
trident-csi-pb2n7	2/2	Running	0
14m			
trident-csi-qsw6z	2/2	Running	0
14m			
trident-operator-67c94c4768-xw978	1/1	Running	0
14m			

```
[netapp-user@rhel7]$ ./tridentctl -n trident version
+-----+
| SERVER VERSION | CLIENT VERSION |
+-----+
| 22.04.0        | 22.04.0        |
+-----+
```

ストレージシステムバックエンドを作成

Astra Trident Operator のインストールが完了したら、使用するネットアップストレージプラットフォームに合わせてバックエンドを設定する必要があります。次のリンクに従って、Astra Tridentのセットアップと設定を続けてください。

- ["NetApp ONTAP NFS"](#)
- ["NetApp ONTAP iSCSI の略"](#)

NetApp ONTAP の NFS 構成

TridentをNFS経由でNetApp ONTAP ストレージシステムと統合するには、ストレージシステムとの通信を可能にするバックエンドを作成する必要があります。この解決策では基本的なバックエンドを設定しますが、よりカスタマイズされたオプションを探している場合は、のマニュアルを参照してください ["こちらをご覧ください"](#)。

ONTAP でSVMを作成します

1. ONTAP System Managerにログインし、Storage > Storage VMの順に選択し、Addをクリックします。
2. SVMの名前を入力し、NFSプロトコルを有効にし、NFSクライアントアクセスを許可チェックボックスをオンにして、ワークロードクラス内でボリュームをPVSとしてマウントできるように、ワーカーノードがオンになっているサブネットをエクスポートポリシールールに追加します。

Add Storage VM



STORAGE VM NAME

trident_svm

Access Protocol

☒ SMB/CIFS, NFS, S3

iSCSI

☐ Enable SMB/CIFS

☒ Enable NFS

☒ Allow NFS client access

Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

RULES

Rule Index	Clients	Access Protocols	Read-Only Rule	Read/Wr
	0.0.0.0/0	Any	Any	Any



NSX -Tを使用したユーザクラスタまたはワークロードクラスタのNAT配置を使用する場合は、出力サブネット（TKGS0の場合はフローティングIPサブネット（TKGIの場合））をエクスポートポリシールールに追加する必要があります。

3. データLIFの詳細とSVM管理アカウントの詳細を指定し、保存をクリックします。

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

K8s-Ontap-01

IP ADDRESS

172.21.252.180

SUBNET MASK

24

GATEWAY

172.21.252.1



BROADCAST DOMAIN

Default



Storage VM Administration

☒ Manage administrator account

USER NAME

vsadmin

PASSWORD

.....

CONFIRM PASSWORD

.....

☐ Add a network interface for storage VM management.

4. アグリゲートをSVMに割り当てます。Storage > Storage VMsと進み、新しく作成したSVMの横にある省略記号をクリックして、Editをクリックします。ボリュームの作成を優先ローカル階層に制限するチェックボックスをオンにして、必要なアグリゲートを関連付けます。

Edit Storage VM



STORAGE VM NAME

trident_svm

DEFAULT LANGUAGE

c.utf_8



DELETED VOLUME RETENTION PERIOD 

12

HOURS

Resource Allocation



Limit volume creation to preferred local tiers

LOCAL TIERS

K8s_Ontap_01_SSD_1 ×

Cancel

Save

5. Tridentをインストールするユーザまたはワークロードクラスタに対してNATを使用して配置した場合、ストレージマウント要求はSNATのために非標準ポートから到達する可能性があります。デフォルトでは、ONTAP は、ルートポートから作成されたボリュームマウント要求のみを許可します。したがっ

て、ONTAP CLIにログインし、非標準ポートからのマウント要求を許可する設定を変更してください。

```
ontap-01> vservers nfs modify -vservers tanzu_svm -mount-rootonly disabled
```

バックエンドとStorageClassesを作成します

1. NFSを提供しているNetApp ONTAP システムの場合は、backendName、managementLIF、dataLIF、SVM、ユーザ名を指定してjumpshotでバックエンド構成ファイルを作成します。パスワードなどの詳細情報。

```
{
  "version": 1,
  "storageDriverName": "ontap-nas",
  "backendName": "ontap-nas+10.61.181.221",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.221",
  "svm": "trident_svm",
  "username": "admin",
  "password": "password"
}
```



カスタムの backendName 値は、簡単に識別できるように NFS を提供するストレージ DriverName とデータ LIF を組み合わせて定義することを推奨します。

2. 次のコマンドを実行してTridentバックエンドを作成します。

```
[netapp-user@rhel7]$ ./tridentctl -n trident create backend -f backend-ontap-nas.json
+-----+-----+
+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE | VOLUMES |          |
+-----+-----+-----+
+-----+-----+-----+
| ontap-nas+10.61.181.221 | ontap-nas      | be7a619d-c81d-445c-b80c-5c87a73c5b1e |
| online |          | 0 |
+-----+-----+-----+
+-----+-----+-----+
```

3. バックエンドを作成したら、次にストレージクラスを作成する必要があります。次のストレージクラス定義の例では、必須フィールドと基本フィールドが強調表示されています。パラメータbackendTypeは新しく作成されたTridentバックエンドのストレージ・ドライバを反映する必要があります

```

apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"

```

4. kubectlコマンドを実行して、ストレージクラスを作成します。

```

[netapp-user@rhel7 trident-installer]$ kubectl create -f storage-class-nfs.yaml
storageclass.storage.k8s.io/ontap-nfs created

```

5. ストレージクラスを作成したら、最初の永続的ボリューム要求（PVC）を作成する必要があります。PVC定義の例を次に示します。[storageClassName](ストレージクラス名)フィールドが作成したストレージクラスの名前と一致していることを確認しますプロビジョニングするワークロードに応じて、PVC定義を必要に応じてさらにカスタマイズできます。

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-nfs

```

6. kubectlコマンドを発行して、PVCを作成します。作成中の元のボリュームのサイズによっては作成にしばらく時間がかかることがあるため、作成が完了した時点でこのプロセスを監視できます。

```

[netapp-user@rhel7 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ kubectl get pvc

```

NAME	STATUS	VOLUME	CAPACITY
basic	Bound	pvc-b4370d37-0fa4-4c17-bd86-94f96c94b42d	1Gi
ACCESS MODES		STORAGECLASS	AGE
RWO		ontap-nfs	7s

NetApp ONTAP ストレージシステムをiSCSI経由で永続ボリューム用のVMware Tanzu Kubernetesクラスタと統合するには、まず各ノードにログインし、iSCSIボリュームをマウントするためのiSCSIユーティリティまたはパッケージを設定してノードを準備します。そのためには、この『手順』に記載されている手順に従ってください "[リンク](#)"。



NATによるVMware Tanzu Kubernetesクラスタの導入には、この手順 は推奨されません。



TKGIは、変更不可の構成イメージを実行するTanzu Kubernetesクラスタのノードとして、Bosh VMを使用します。また、Bosh VMでiSCSIパッケージを手動で変更しても、リブート後も維持されません。そのため、TKGIによって導入、運用されているTanzu Kubernetesクラスタの永続ストレージにはNFSボリュームを使用することを推奨します。

iSCSIボリュームのクラスタノードの準備が完了したら、ストレージシステムとの通信を可能にするバックエンドを作成する必要があります。この解決策 では基本的なバックエンドを設定しましたが、よりカスタマイズ可能なオプションを探している場合は、のドキュメントを参照してください "[こちらをご覧ください](#)"。

ONTAP でSVMを作成します

ONTAP でSVMを作成するには、次の手順を実行します。

1. ONTAP System Managerにログインし、Storage > Storage VMの順に選択し、Addをクリックします。
2. SVMの名前を入力し、iSCSIプロトコルを有効にして、データLIFの詳細を指定します。

Add Storage VM



STORAGE VM NAME

trident_svm_iscsi

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

☒ Enable iSCSI

NETWORK INTERFACE

K8s-Ontap-01

IP ADDRESS

10.61.181.231

SUBNET MASK

24

GATEWAY

10.61.181.1

BROADCAST DOMAIN

Defa...

☐ Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

10.61.181.232

SUBNET MASK

24

GATEWAY

10.61.181.1

BROADCAST DOMAIN

Defa...

3. SVM管理アカウントの詳細を入力し、保存をクリックします。

Storage VM Administration

☒ Manage administrator account

USER NAME

vsadmin

PASSWORD

.....

CONFIRM PASSWORD

.....

☐ Add a network interface for storage VM management.

Save

Cancel

4. アグリゲートをSVMに割り当てるには、Storage > Storage VMに移動し、新しく作成したSVMの横にある省略記号をクリックしてEditをクリックします。ボリュームの作成を優先ローカル階層に制限するチェックボックスをオンにし、必要なアグリゲートを関連付けます。

Edit Storage VM



STORAGE VM NAME

trident_svm_iscsi

DEFAULT LANGUAGE

c.utf_8



DELETED VOLUME RETENTION PERIOD 

12

HOURS

Resource Allocation

☒ Limit volume creation to preferred local tiers

LOCAL TIERS

K8s_Ontap_01_SSD_1 ✕

Cancel

Save

バックエンドと**StorageClasses**を作成します

1. NFSを提供しているNetApp ONTAP システムの場合は、backendName、managementLIF、dataLIF、SVM、ユーザ名を指定してjumpshotでバックエンド構成ファイルを作成します。 パスワードなどの詳細情報。

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap-san+10.61.181.231",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.231",
  "svm": "trident_svm_iscsi",
  "username": "admin",
  "password": "password"
}
```

2. 次のコマンドを実行してTridentバックエンドを作成します。

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-san.json
+-----+-----+
+-----+-----+-----+-----+
|          NAME          | STORAGE DRIVER |          UUID          |
| STATE | VOLUMES | |          |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
| ontap-san+10.61.181.231 | ontap-san      | 6788533c-7fea-4a35-b797- |
| fb9bb3322b91 | online |          0 |          |
+-----+-----+-----+-----+
+-----+-----+-----+-----+
```

3. バックエンドを作成したら、次にストレージクラスを作成する必要があります。次のストレージクラス定義の例では、必須フィールドと基本フィールドが強調表示されています。パラメータbackendTypeは'新しく作成されたTridentバックエンドのストレージ・ドライバを反映する必要がありますまた、名前フィールドの値もメモしておきます。この値は、以降の手順で参照する必要があります。

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-iscsi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
```



このファイルに定義されているオプションのフィールド「fsType」があります。iSCSIバックエンドでは、この値を特定のLinuxファイルシステムタイプ（XFS、ext4など）に設定するか、またはTanzu Kubernetesクラスタが使用するファイルシステムを決定できるようにするために削除できます。

4. kubectlコマンドを実行して、ストレージクラスを作成します。

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f storage-class-iscsi.yaml
storageclass.storage.k8s.io/ontap-iscsi created
```

5. ストレージクラスを作成したら、最初の永続的ボリューム要求（PVC）を作成する必要があります。PVC定義の例を次に示します。[storageClassName](ストレージクラス名)フィールドが作成したストレージクラスの名前と一致していることを確認します。プロビジョニングするワークロードに応じて、PVC定義を必要に応じてさらにカスタマイズできます。

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-iscsi
```

6. kubectlコマンドを発行して、PVCを作成します。作成中の元のボリュームのサイズによっては作成にしばらく時間がかかることがあるため、作成が完了した時点でこのプロセスを監視できます。

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created
```

```
[netapp-user@rhel7 trident-installer]$ kubectl get pvc
```

NAME	STATUS	VOLUME	CAPACITY
basic	Bound	pvc-7ceac1ba-0189-43c7-8f98-094719f7956c	1Gi
		ontap-iscsi	3s

ビデオとデモ：VMware Tanzu with NetApp

次のビデオでは、このドキュメントで説明する機能の一部を紹介します。

[Astra Tridentを使用してVMware Tanzuで永続的ストレージをプロビジョニング- VMware TanzuとNetApp](#)

[Astra Control Centerを使用して、VMware Tanzu - VMware TanzuとNetAppのアプリケーションをクローニングします](#)



これらのデモは、TKGのバージョン1.3.1とAstra Control Centerのバージョン21.12を使用した技術プレビューとして記録されています。サポートされている公式バージョンについては、サポートマトリックスを参照してください。

追加情報：ネットアップを使用した**VMware**の**Tanzu**の紹介

このドキュメントに記載されている情報の詳細については、次の Web サイトを参照してください。

- NetApp のドキュメント

["https://docs.netapp.com/"](https://docs.netapp.com/)

- Astra Trident のドキュメント

["https://docs.netapp.com/us-en/trident/"](https://docs.netapp.com/us-en/trident/)

- NetApp Astra Control Center のドキュメント

["https://docs.netapp.com/us-en/astra-control-center/"](https://docs.netapp.com/us-en/astra-control-center/)

- Ansibleのドキュメント

["https://docs.ansible.com/"](https://docs.ansible.com/)

- VMware Tanzuのドキュメント

["https://docs.vmware.com/en/VMware-Tanzu/index.html"](https://docs.vmware.com/en/VMware-Tanzu/index.html)

- VMware Tanzu Kubernetes Gridのドキュメント

["https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmware-tanzu-kubernetes-grid-15/GUID-index.html"](https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid/1.5/vmware-tanzu-kubernetes-grid-15/GUID-index.html)

- VMware Tanzu Kubernetes Grid Serviceに関するドキュメント

["https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-152BE7D2-E227-4DAA-B527-557B564D9718.html"](https://docs.vmware.com/en/VMware-vSphere/7.0/vmware-vsphere-with-tanzu/GUID-152BE7D2-E227-4DAA-B527-557B564D9718.html)

- VMware Tanzu Kubernetes Grid Integrated Editionのドキュメント

["https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid-Integrated-Edition/index.html"](https://docs.vmware.com/en/VMware-Tanzu-Kubernetes-Grid-Integrated-Edition/index.html)

アーカイブされたソリューション

ベアメタルの **Anthos**

=
:allow-uri-read:

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。