Multicloud hybride NetApp avec Red Hat OpenShift

NetApp Solutions

NetApp
April 20, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions/rhhc/rhhc-value-prop.html on April 20, 2024. Always check docs.netapp.com for the latest.

Sommaire

Le multicloud hybride NetApp avec les workloads de conteneurs Red Hat OpenShift 1
Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift 1
Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift 15
Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift 26
Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift 43

Le multicloud hybride NetApp avec les workloads de conteneurs Red Hat OpenShift

Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

Présentation

NetApp constate une augmentation significative des clients qui modernisent leurs applications d'entreprise existantes et créent de nouvelles applications à l'aide de conteneurs et de plateformes d'orchestration basées sur Kubernetes. Nous avons adopté Red Hat OpenShift Container Platform comme bon nombre de nos clients.

Alors que les clients sont de plus en plus nombreux à adopter des conteneurs dans leur entreprise, NetApp est parfaitement positionné pour répondre aux besoins de stockage persistant de leurs applications avec état et aux besoins de gestion des données classiques, tels que la protection, la sécurité et la migration des données. Toutefois, ces besoins sont satisfaits à l'aide de stratégies, d'outils et de méthodes différents.

Les options de stockage basées sur NetApp ONTAP sont énumérées ci-dessous et offrent sécurité, protection des données, fiabilité et flexibilité pour les conteneurs et les déploiements Kubernetes.

- Stockage autogéré sur site :
  - Stockage FAS (Fabric Attached Storage), baies FAS 100 % Flash (AFF), baies SAN ASA (All SAN Array) et ONTAP Select
- Stockage géré par un fournisseur sur site :
  - NetApp Keystone fournit une solution de stockage en tant que service (STaaS)
- Stockage autogéré dans le cloud :
  - NetApp Cloud volumes ONTAP (CVO) fournit un stockage autogéré dans les hyperscalers
- Stockage géré par un fournisseur dans le cloud :
  - Cloud Volumes Service pour Google Cloud (CVS), Azure NetApp Files (ANF) et Amazon FSX pour NetApp ONTAP offrent un stockage entièrement géré dans les hyperscalers

ONTAP feature highlights

Storage Administration

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

Performance & Scalability

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

Availability & Resilience

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

Access Protocols

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

Storage Efficiency

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

Security & Compliance

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

NetApp BlueXP vous permet de gérer l'ensemble de vos ressources de stockage et de données à partir d'un seul plan de contrôle/interface.

Vous pouvez utiliser BlueXP pour créer et gérer du stockage cloud (par exemple, Cloud Volumes ONTAP et Azure NetApp Files), déplacer, protéger et analyser les données, et contrôler de nombreux systèmes de stockage sur site et en périphérie.

NetApp Astra Trident est un orchestrateur de stockage conforme à CSI qui permet de consommer rapidement et facilement du stockage persistant grâce à plusieurs options de stockage NetApp mentionnées ci-dessus. Il s'agit d'un logiciel open source géré et pris en charge par NetApp.

Astra Trident CSI feature highlights

CSI specific

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

Security

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

Control

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

Installation methods

- Binary
- Helm chart
- Operator
- GitOps

Choose your access mode

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

Choose your protocol

- NFS
- SMB
- iSCSI

Les workloads de conteneurs stratégiques requièrent bien plus que de simples volumes persistants. Leurs exigences de gestion des données requièrent également la protection et la migration des objets kubernetes applicatifs.

> Les données d'application incluent des objets kubernetes en plus des données utilisateur. Voici quelques exemples : - Objets kubernetes tels que les pods Specs, les PVC, les déploiements, les services - objets de configuration personnalisés tels que les cartes de configuration et les secrets - données persistantes telles que les copies Snapshot, les sauvegardes, les clones - ressources personnalisées telles que CRS et CRD

NetApp Astra Control, disponible en tant que logiciel entièrement géré et autogéré, assure l'orchestration pour une gestion robuste des données d'application. Reportez-vous à la "Documentation Astra" Pour en savoir plus sur la gamme de produits Astra.

Cette documentation de référence apporte la validation de la migration et de la protection des applications basées sur des conteneurs, déployées sur une plateforme de conteneurs RedHat OpenShift à l'aide de NetApp Astra Control Center. En outre, la solution fournit des détails généraux sur le déploiement et l'utilisation de Red Hat Advanced Cluster Management (ACM) pour la gestion des plateformes de conteneurs. Ce document détaille également les modalités d'intégration du stockage NetApp avec les plateformes de conteneurs Red Hat OpenShift à l'aide d'Astra Trident CSI Provisioner. ASTRA Control Center est déployé sur le cluster Hub et est utilisé pour gérer les applications de conteneur et leur cycle de vie de stockage persistant. Enfin, il fournit une solution de réplication, de basculement et de retour arrière pour les workloads de conteneurs sur des clusters Red Hat OpenShift gérés dans AWS (ROSA) utilisant Amazon FSX pour NetApp ONTAP (FSxN) en tant que stockage persistant.

Propositions de valeur des solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

La plupart des clients ne se contentent pas de créer des environnements Kubernetes sans infrastructure existante. Il s'agit peut-être d'un service INFORMATIQUE traditionnel qui exécute la plupart de ses applications d'entreprise sur des machines virtuelles (dans de grands environnements VMware, par exemple). Ils commencent ensuite à créer de petits environnements basés sur des conteneurs pour répondre aux besoins de leurs équipes de développement d'applications modernes. Ces initiatives commencent généralement à petite échelle et commencent à devenir plus omniprésentes lorsque les équipes apprennent ces nouvelles technologies et compétences, et commencent à reconnaître les nombreux avantages de leur adoption. La bonne nouvelle pour les clients est que NetApp répond aux besoins des deux environnements. Cet ensemble de solutions pour le multicloud hybride avec Red Hat OpenShift permettra aux clients NetApp d'adopter des technologies et des services cloud modernes sans avoir à remanier l'ensemble de leur infrastructure et de leur organisation. Que les applications et les données des clients soient hébergées sur site, dans le cloud, sur des machines virtuelles ou sur des conteneurs, NetApp offre des fonctionnalités cohérentes de gestion, de protection, de sécurité et de portabilité des données. Avec ces nouvelles solutions, la valeur ajoutée qu'offre NetApp dans les environnements de data Center sur site pendant des décennies sera disponible à l'échelle de l'entreprise à tous les niveaux, sans nécessiter d'investissements importants pour changer d'outil, acquérir de nouvelles compétences ou constituer de nouvelles équipes. NetApp est bien placé pour aider les clients à relever ces défis métier, quelle que soit l'étape de leur transition vers le cloud.

NetApp Hybrid Multi-Cloud avec Red Hat OpenShift :

- Fournit aux clients des conceptions et des pratiques validées qui démontrent la meilleure façon de gérer, protéger, sécuriser et migrer leurs données et applications lors de l'utilisation de Red Hat OpenShift avec les solutions de stockage NetApp.
- Présenter les meilleures pratiques pour les clients exécutant Red Hat OpenShift avec le stockage NetApp dans des environnements VMware, une infrastructure bare Metal ou une combinaison des deux.
- Présentez les stratégies et les options des environnements sur site et cloud, ainsi que des environnements hybrides dans lesquels les deux sont utilisés.

Solutions prises en charge de multicloud hybride NetApp pour les workloads de conteneurs Red Hat OpenShift

La solution teste et valide la migration et la protection centralisée des données avec OpenShift Container Platform (OCP), OpenShift Advanced Cluster Manager (ACM), NetApp ONTAP, NetApp BlueXP et NetApp Astra Control Center (ACC).

Pour cette solution, les scénarios suivants sont testés et validés par NetApp. La solution est divisée en plusieurs scénarios selon les caractéristiques suivantes :

- sur site
- le cloud
  - Clusters OpenShift autogérés et stockage NetApp autogéré
  - Clusters OpenShift gérés par le fournisseur et stockage NetApp géré par le fournisseur

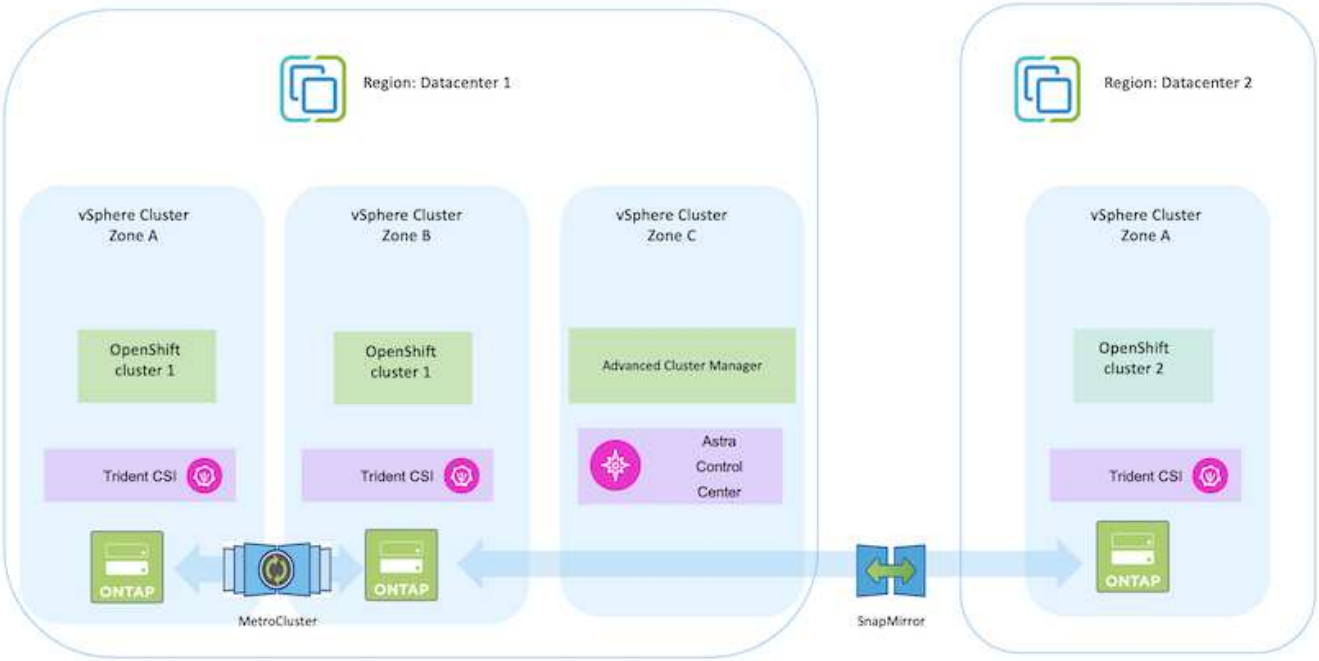
Nous élaborerons à l'avenir des solutions et des cas d'utilisation supplémentaires.

Scénario 1 : protection et migration des données au sein d'un environnement sur site avec ACC

Sur site : clusters OpenShift autogérés et stockage NetApp autogéré

- Avec ACC, créez des copies Snapshot, des sauvegardes et des restaurations pour protéger les données.
- Avec ACC, effectuer une réplication SnapMirror des applications de conteneur.

Scénario 1

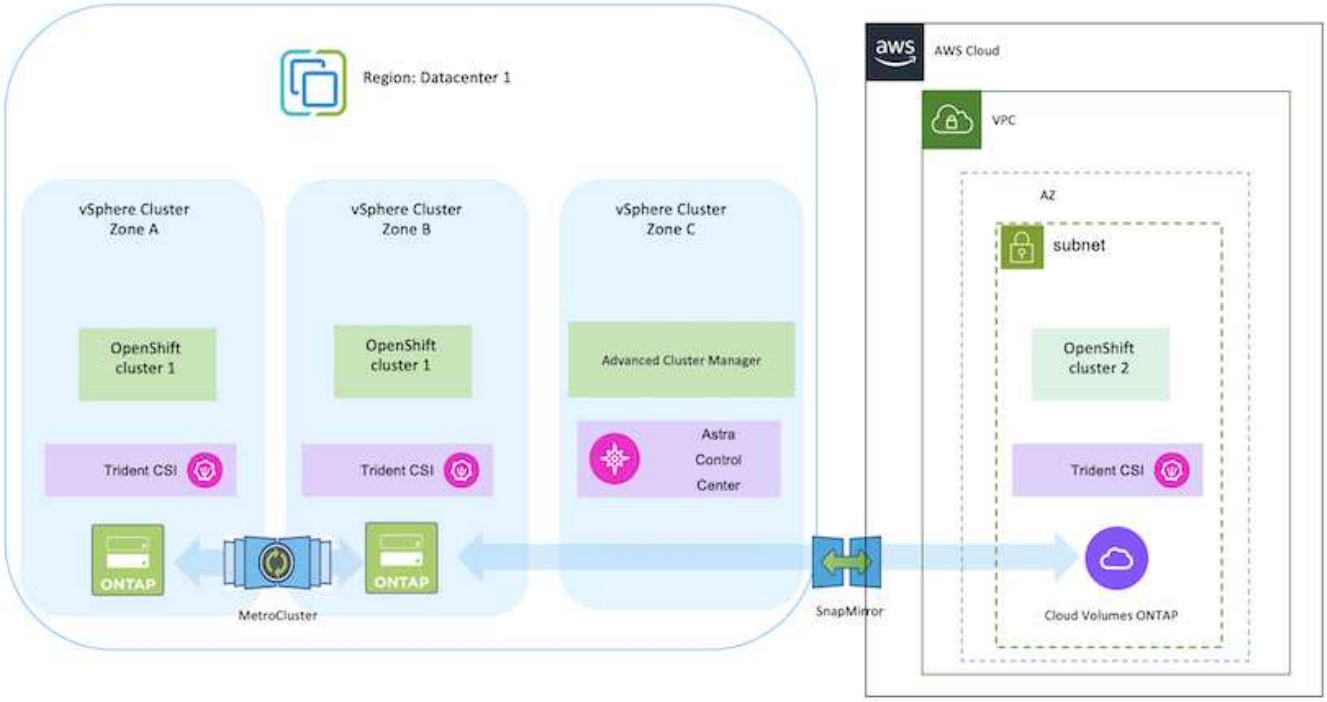


Scénario 2 : protection des données et migration d'un environnement sur site vers un environnement AWS à l'aide d'ACC

Sur site : cluster OpenShift autogéré et stockage autogéré AWS Cloud : cluster OpenShift autogéré et stockage autogéré

- Avec ACC, effectuez des sauvegardes et des restaurations pour protéger vos données.
- Avec ACC, effectuer une réplication SnapMirror des applications de conteneur.

Scénario 2

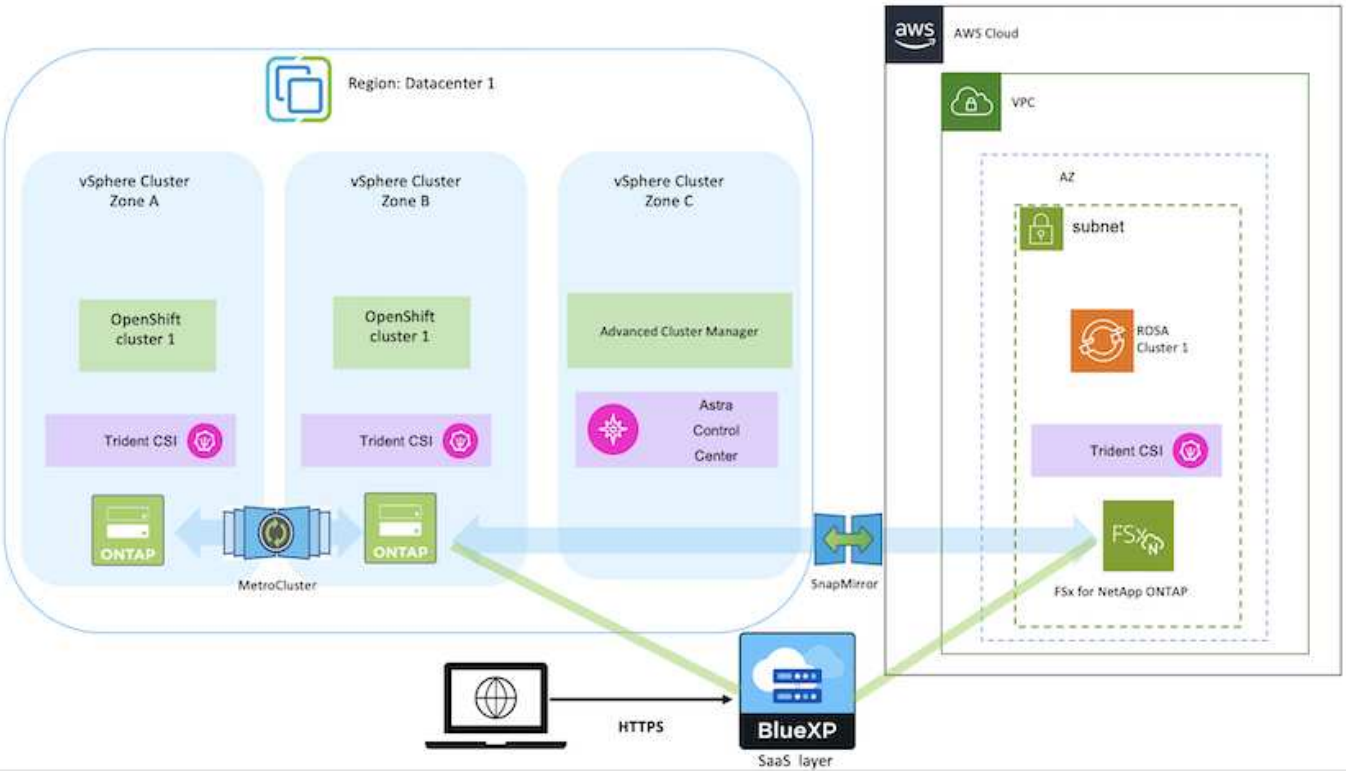


Scénario 3 : protection des données et migration d'un environnement sur site vers un environnement AWS

Sur site : cluster OpenShift autogéré et stockage autogéré AWS Cloud : cluster OpenShift géré par le fournisseur (ROSA) et stockage géré par le fournisseur (FSxN)

- Avec BlueXP, répliquez des volumes persistants (FSxN).
- À l'aide d'OpenShift GitOps, recréez les métadonnées de l'application.

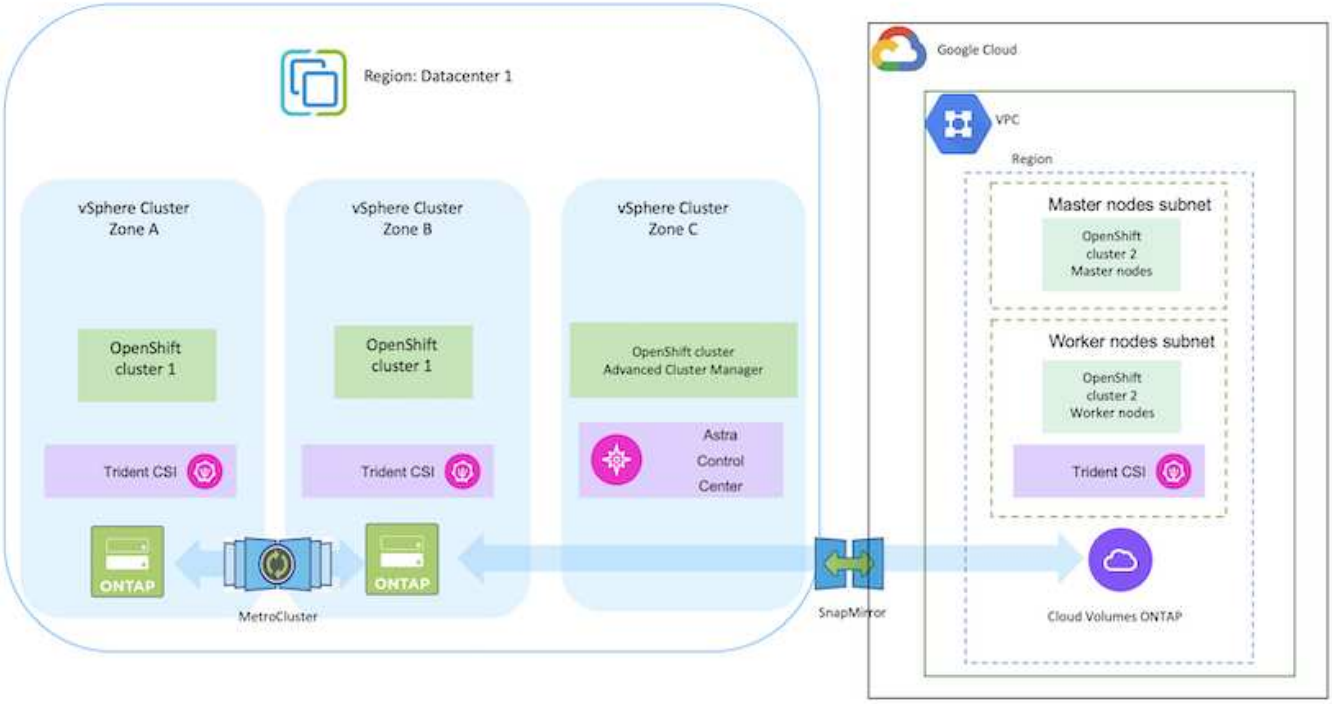
Scénario 3



Scénario 4 : protection des données et migration d'un environnement sur site vers un environnement GCP à l'aide d'ACC

Sur site : cluster OpenShift autogéré et stockage autogéré
Google Cloud : cluster OpenShift autogéré et stockage autogéré

- Avec ACC, effectuez des sauvegardes et des restaurations pour protéger vos données.
- Avec ACC, effectuer une réplication SnapMirror des applications de conteneur.

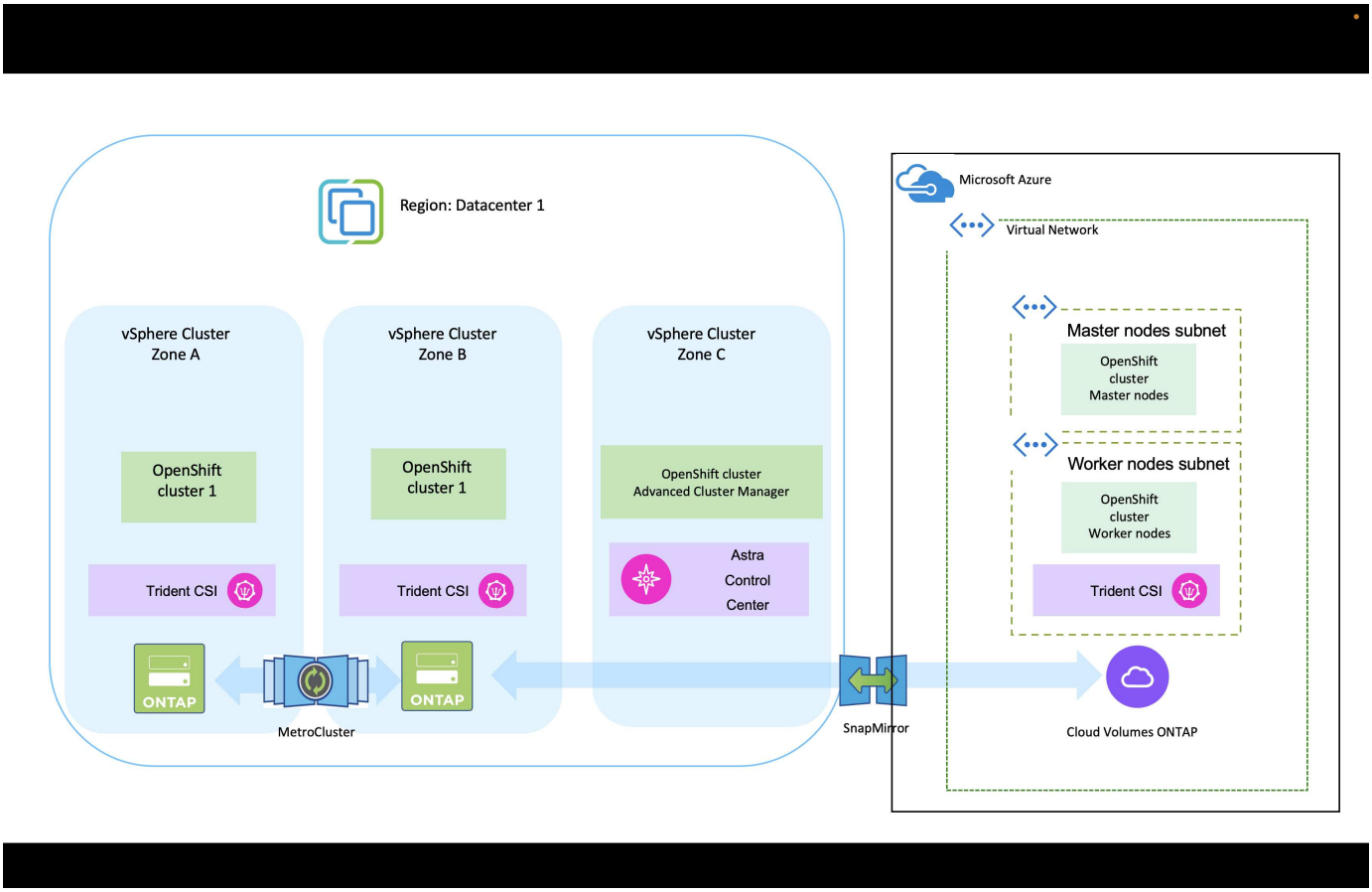


Pour connaître les points à prendre en compte lors de l'utilisation de ONTAP dans une configuration MetroCluster, reportez-vous à la section "ici".

Scénario 5 : protection des données et migration d'un environnement sur site vers un environnement Azure à l'aide d'ACC

Sur site : cluster OpenShift autogéré et stockage autogéré
Azure Cloud : cluster OpenShift autogéré et stockage autogéré

- Avec ACC, effectuez des sauvegardes et des restaurations pour protéger vos données.
- Avec ACC, effectuer une réplication SnapMirror des applications de conteneur.



Pour connaître les points à prendre en compte lors de l'utilisation de ONTAP dans une configuration MetroCluster, reportez-vous à la section "ici".

Versions des différents composants utilisés dans la validation de la solution

La solution teste et valide la migration et la protection centralisée des données avec OpenShift Container Platform, OpenShift Advanced Cluster Manager, NetApp ONTAP et NetApp Astra Control Center.

Les scénarios 1, 2 et 3 de la solution ont été validés à l'aide des versions indiquées dans le tableau ci-dessous :

Composant	Version
VMware	Client vSphere version 8.0.0.10200 VMware ESXi, 8.0.0, 20842819
Cluster Hub	OpenShift 4.11.34
Clusters source et de destination	OpenShift 4.12.9 sur site et dans AWS
NetApp Astra Trident	Serveur et client Trident 23.04.0
NetApp Astra Control Center	ACC 22.11.0-82
NetApp ONTAP	ONTAP 9.12.1

AWS FSX pour NetApp ONTAP	AZ unique

Le scénario 4 de la solution a été validé à l'aide des versions indiquées dans le tableau ci-dessous :

Composant	Version
VMware	Client vSphere version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Cluster Hub	OpenShift 4.13.13
Clusters source et de destination	OpenShift 4.13.12 Sur site et dans Google Cloud
NetApp Astra Trident	Serveur et client Trident 23.07.0
NetApp Astra Control Center	ACC 23.07.0-25
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	Disponibilité unique, nœud unique, 9.14.0

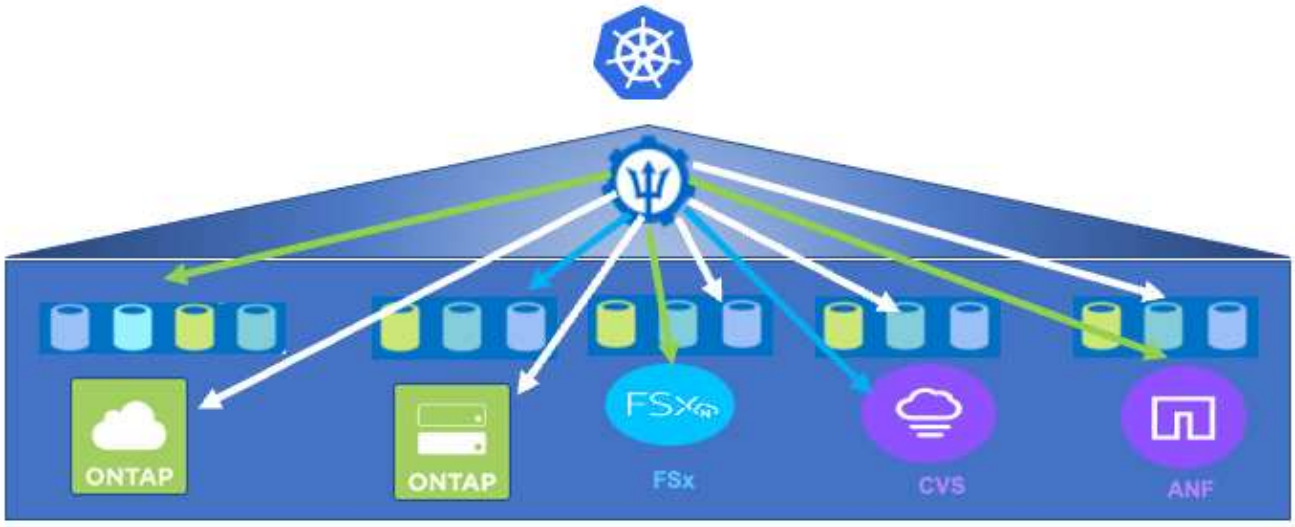
Le scénario 5 de la solution a été validé à l'aide des versions indiquées dans le tableau ci-dessous :

Composant	Version
VMware	Client vSphere version 8.0.2.00000 VMware ESXi, 8.0.2, 22380479
Clusters source et de destination	OpenShift 4.13.25 Sur site et dans Azure
NetApp Astra Trident	Serveur et client Trident et Astra Control Provisioner 23.10.0
NetApp Astra Control Center	ACC 23.10
NetApp ONTAP	ONTAP 9.12.1
Cloud Volumes ONTAP	Disponibilité unique, nœud unique, 9.14.0

Intégrations NetApp Storage prises en charge avec les conteneurs Red Hat Open Shift

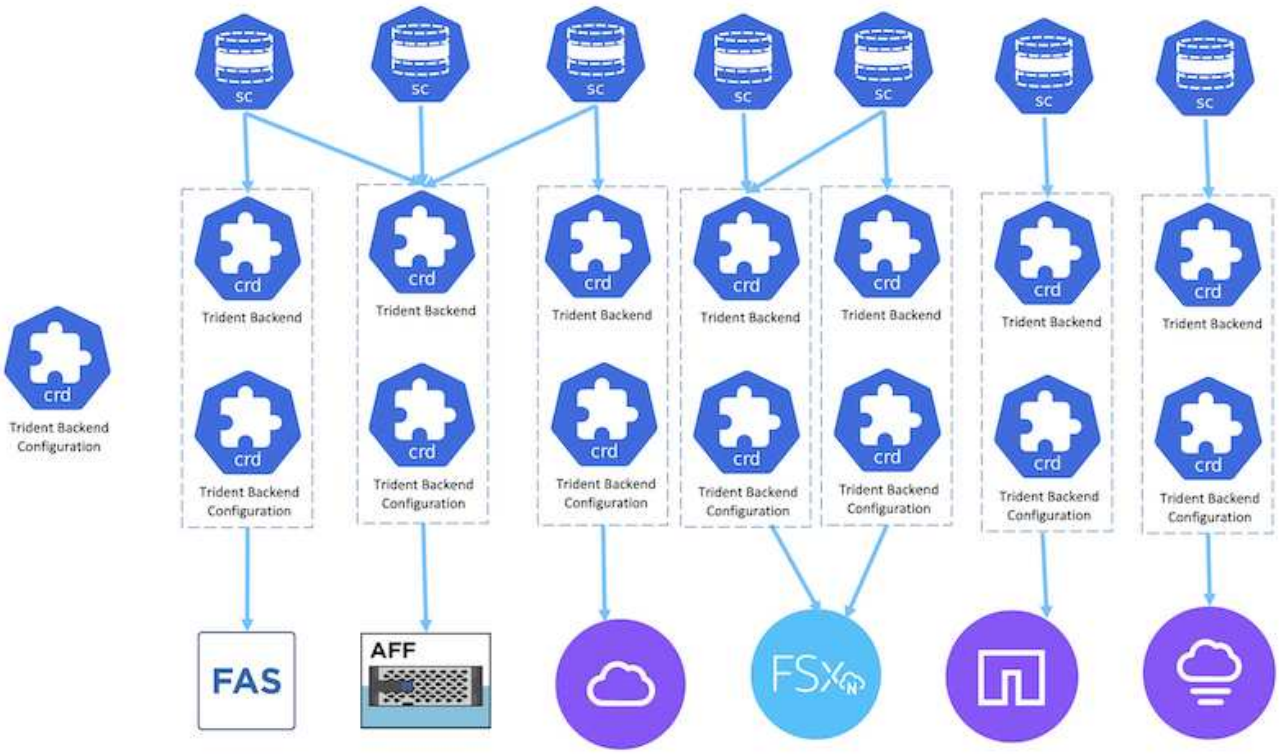
Que les conteneurs Red Hat Open Shift s'exécutent sur VMware ou dans les hyperscalers, NetApp Astra Trident peut être utilisé comme mécanisme de provisionnement CSI pour les différents types de stockage NetApp back-end pris en charge.

Le schéma suivant décrit les différents systèmes de stockage NetApp back-end pouvant être intégrés avec des clusters OpenShift à l'aide de NetApp Astra Trident.

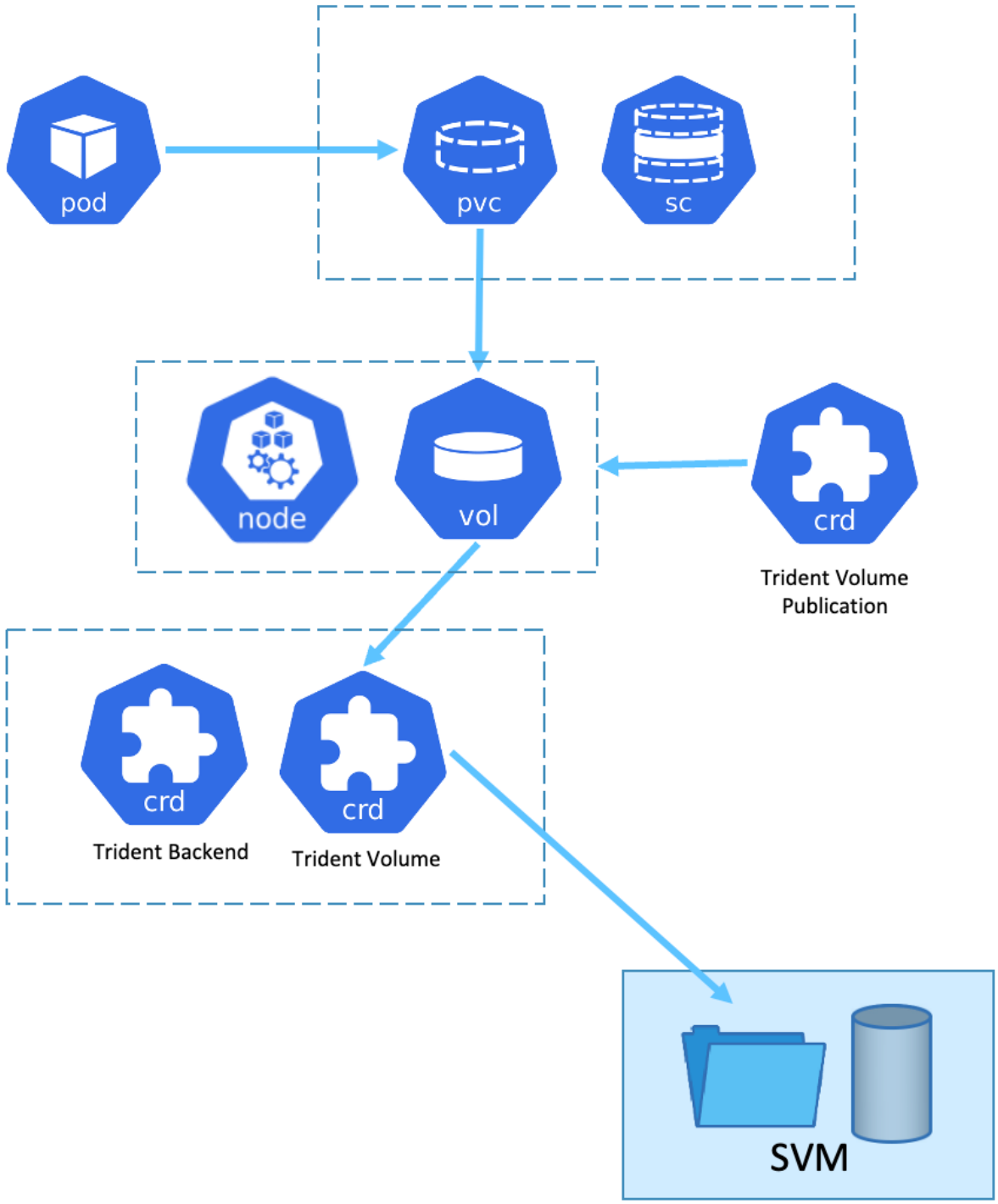


La SVM (Storage Virtual machine) de ONTAP assure une colocation sécurisée. Un cluster OpenShift peut se connecter à un seul SVM ou à plusieurs SVM, voire à plusieurs clusters ONTAP. Storage Class filtre le stockage back-end en fonction de paramètres ou de libellés. Les administrateurs du stockage définissent les paramètres de connexion au système de stockage à l'aide de la configuration back-end trident. Une fois la connexion établie, il crée le back-end trident et renseigne les informations que la classe de stockage peut filtrer.

La relation entre le storageclass et le backend est présentée ci-dessous.



Le propriétaire de l'application demande un volume persistant en utilisant la classe de stockage. La classe de stockage filtre le stockage back-end. La relation entre le pod et le système de stockage back-end est présentée ci-dessous.



Options Container Storage interface (CSI)

Sur les environnements vSphere, les clients peuvent choisir le pilote VMware CSI et/ou Astra Trident CSI pour s'intégrer à ONTAP. Avec VMware CSI, les volumes persistants sont utilisés en tant que disques SCSI locaux, tandis qu'avec Trident, ils sont utilisés avec le réseau. Étant donné que VMware CSI ne prend pas en charge les modes d'accès RWX avec ONTAP, les applications doivent utiliser Trident CSI si le mode RWX est requis. Pour les déploiements basés sur FC, VMware CSI est privilégié et SnapMirror Business Continuity (SMBC) offre une haute disponibilité au niveau de la zone.

Prise en charge de VMware CSI

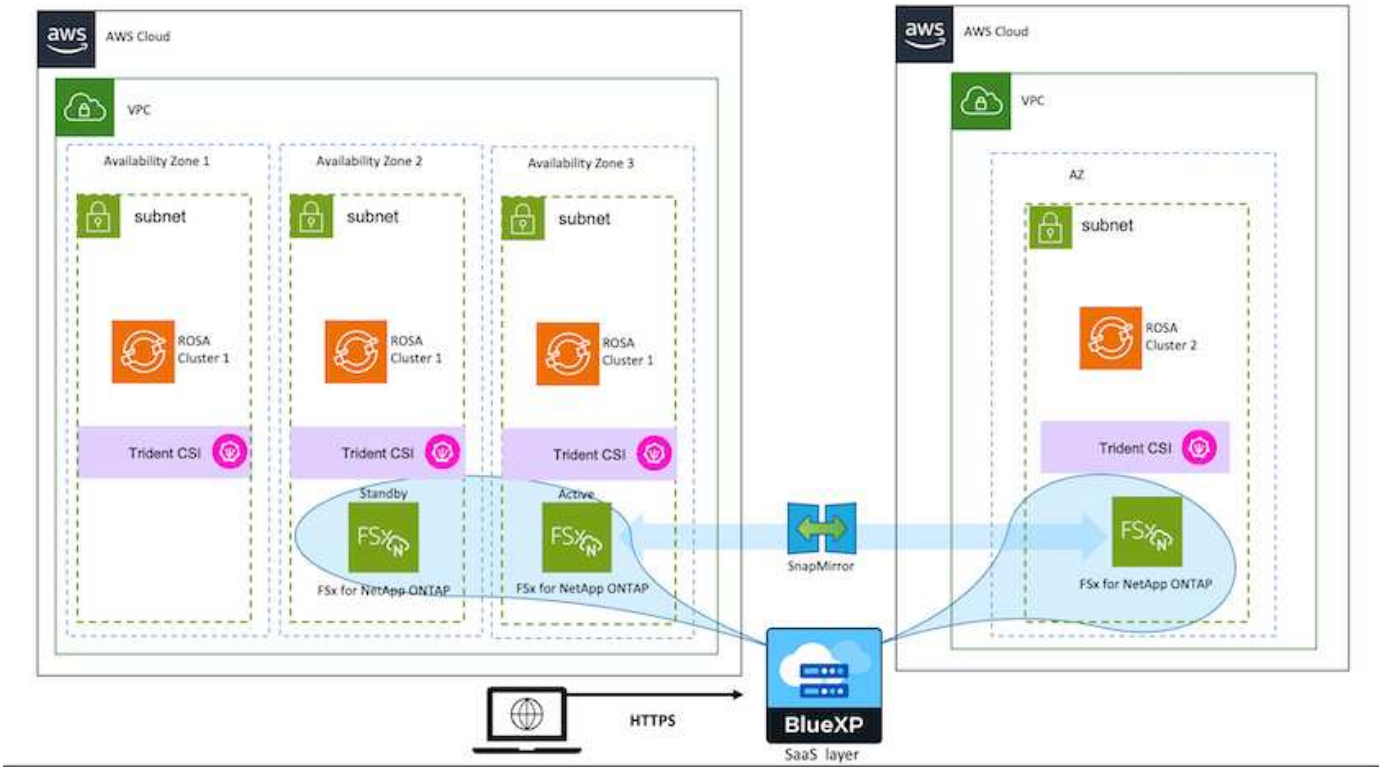
- Datastores basés sur des blocs principaux (FC, FCoE, iSCSI, NVMeoF)
- Datastores basés sur des fichiers principaux (NFS v3, v4)
- Datastores vVol (bloc et fichier)

Trident dispose des pilotes suivants pour prendre en charge ONTAP

- san ontap (volume dédié)
- ontap-san-economy (volume partagé)
- ontap-nas (volume dédié)
- ontap-nas-economy (volume partagé)
- ontap-nas-flexgroup (volume dédié à grande échelle)

Pour VMware CSI et Astra Trident CSI, ONTAP prend en charge nconnect, l'agrégation de sessions, kerberos, etc. Pour NFS et les chemins d'accès multiples, l'authentification chap, etc. Pour les protocoles en mode bloc.

Dans AWS, FSX pour NetApp ONTAP (FSxN) peut être déployé dans une zone de disponibilité unique (AZ) ou dans plusieurs zones de disponibilité. Pour les workloads de production qui nécessitent une haute disponibilité, plusieurs zones de disponibilité offrent une tolérance aux pannes de niveau zonal et un meilleur cache de lecture NVMe qu'une zone de disponibilité unique. Pour plus d'informations, consultez "Conseils sur les performances d'AWS".
Pour réduire les coûts sur le site de reprise après incident, un seul serveur AZ FSX ONTAP peut être utilisé.



Pour connaître le nombre de SVM pris en charge par FSX ONTAP, reportez-vous à la section "Gestion de la machine virtuelle de stockage FSX ONTAP"

Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

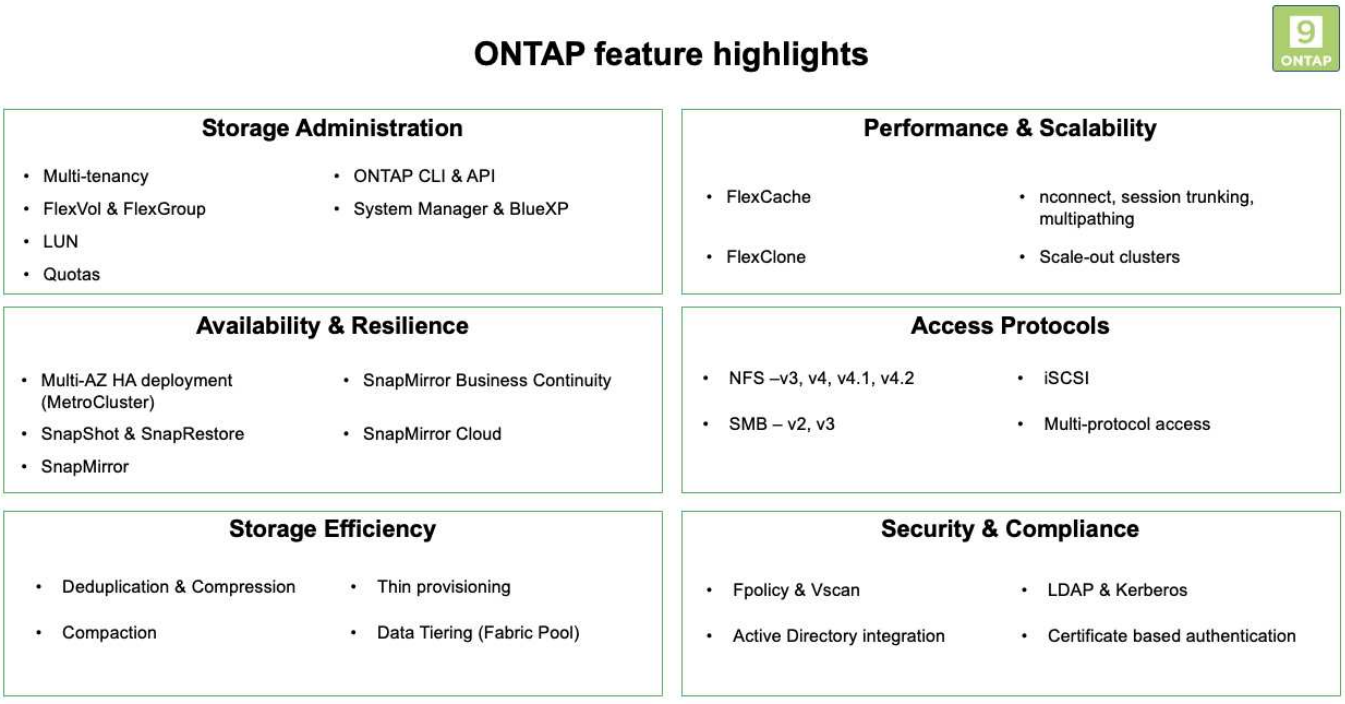
Présentation

NetApp constate une augmentation significative des clients qui modernisent leurs applications d'entreprise existantes et créent de nouvelles applications à l'aide de conteneurs et de plateformes d'orchestration basées sur Kubernetes. Nous avons adopté Red Hat OpenShift Container Platform comme bon nombre de nos clients.

Alors que les clients sont de plus en plus nombreux à adopter des conteneurs dans leur entreprise, NetApp est parfaitement positionné pour répondre aux besoins de stockage persistant de leurs applications avec état et aux besoins de gestion des données classiques, tels que la protection, la sécurité et la migration des données. Toutefois, ces besoins sont satisfaits à l'aide de stratégies, d'outils et de méthodes différents.

Les options de stockage basées sur NetApp ONTAP sont énumérées ci-dessous et offrent sécurité, protection des données, fiabilité et flexibilité pour les conteneurs et les déploiements Kubernetes.

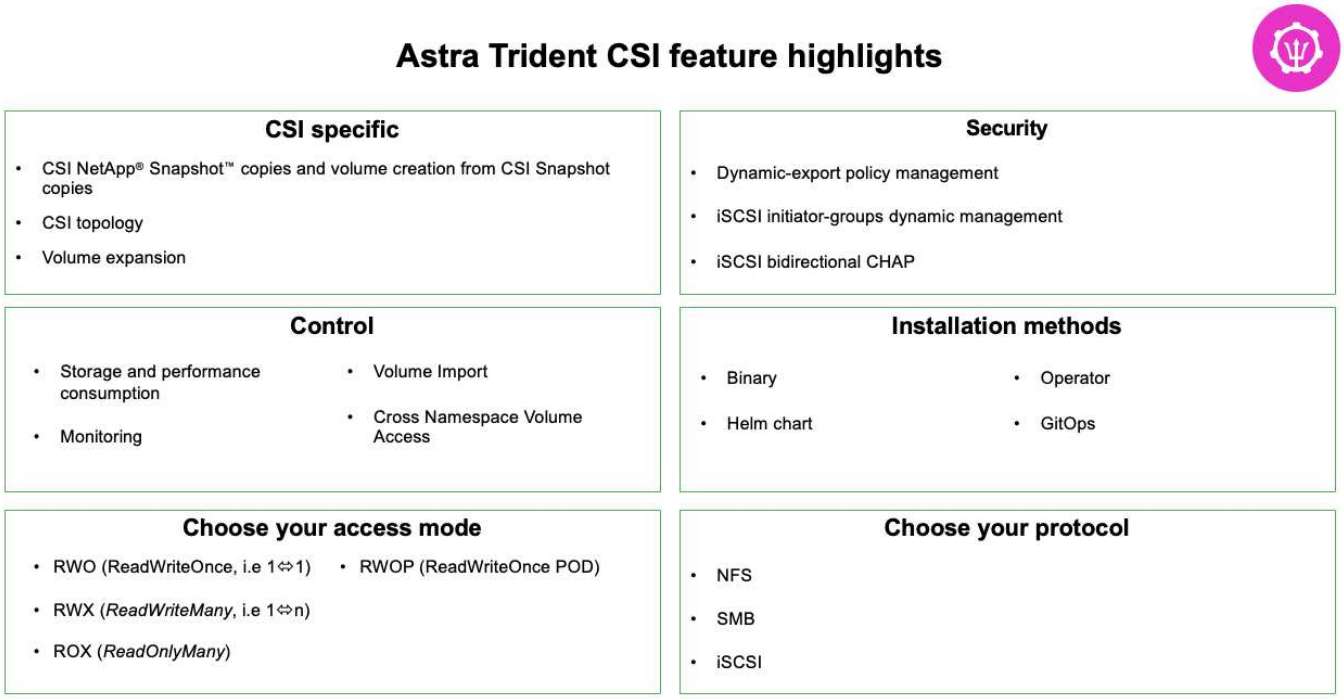
- Stockage autogéré sur site :
  - Stockage FAS (Fabric Attached Storage), baies FAS 100 % Flash (AFF), baies SAN ASA (All SAN Array) et ONTAP Select
- Stockage géré par un fournisseur sur site :
  - NetApp Keystone fournit une solution de stockage en tant que service (STaaS)
- Stockage autogéré dans le cloud :
  - NetApp Cloud volumes ONTAP (CVO) fournit un stockage autogéré dans les hyperscalers
- Stockage géré par un fournisseur dans le cloud :
  - Cloud Volumes Service pour Google Cloud (CVS), Azure NetApp Files (ANF) et Amazon FSX pour NetApp ONTAP offrent un stockage entièrement géré dans les hyperscalers



NetApp BlueXP vous permet de gérer l'ensemble de vos ressources de stockage et de données à partir d'un seul plan de contrôle/interface.

Vous pouvez utiliser BlueXP pour créer et gérer du stockage cloud (par exemple, Cloud Volumes ONTAP et Azure NetApp Files), déplacer, protéger et analyser les données, et contrôler de nombreux systèmes de stockage sur site et en périphérie.

NetApp Astra Trident est un orchestrateur de stockage conforme à CSI qui permet de consommer rapidement et facilement du stockage persistant grâce à plusieurs options de stockage NetApp mentionnées ci-dessus. Il s'agit d'un logiciel open source géré et pris en charge par NetApp.



Les workloads de conteneurs stratégiques requièrent bien plus que de simples volumes persistants. Leurs exigences de gestion des données requièrent également la protection et la migration des objets kubernetes applicatifs.

> Les données d'application incluent des objets kubernetes en plus des données utilisateur. Voici quelques exemples : - Objets kubernetes tels que les pods Specs, les PVC, les déploiements, les services - objets de configuration personnalisés tels que les cartes de configuration et les secrets - données persistantes telles que les copies Snapshot, les sauvegardes, les clones - ressources personnalisées telles que CRS et CRD

NetApp Astra Control, disponible en tant que logiciel entièrement géré et autogéré, assure l'orchestration pour une gestion robuste des données d'application. Reportez-vous à la "Documentation Astra" Pour en savoir plus sur la gamme de produits Astra.

Cette documentation de référence apporte la validation de la migration et de la protection des applications basées sur des conteneurs, déployées sur une plateforme de conteneurs RedHat OpenShift à l'aide de NetApp Astra Control Center. En outre, la solution fournit des détails généraux sur le déploiement et l'utilisation de Red Hat Advanced Cluster Management (ACM) pour la gestion des plateformes de conteneurs. Ce document détaille également les modalités d'intégration du stockage NetApp avec les plateformes de conteneurs Red Hat OpenShift à l'aide d'Astra Trident CSI Provisioner. ASTRA Control Center est déployé sur le cluster Hub et est utilisé pour gérer les applications de conteneur et leur cycle de vie de stockage persistant.

Enfin, il fournit une solution de réplication, de basculement et de retour arrière pour les workloads de conteneurs sur des clusters Red Hat OpenShift gérés dans AWS (ROSA) utilisant Amazon FSX pour NetApp ONTAP (FSxN) en tant que stockage persistant.

Solution NetApp avec les workloads de plateforme de conteneurs Red Hat OpenShift sur VMware

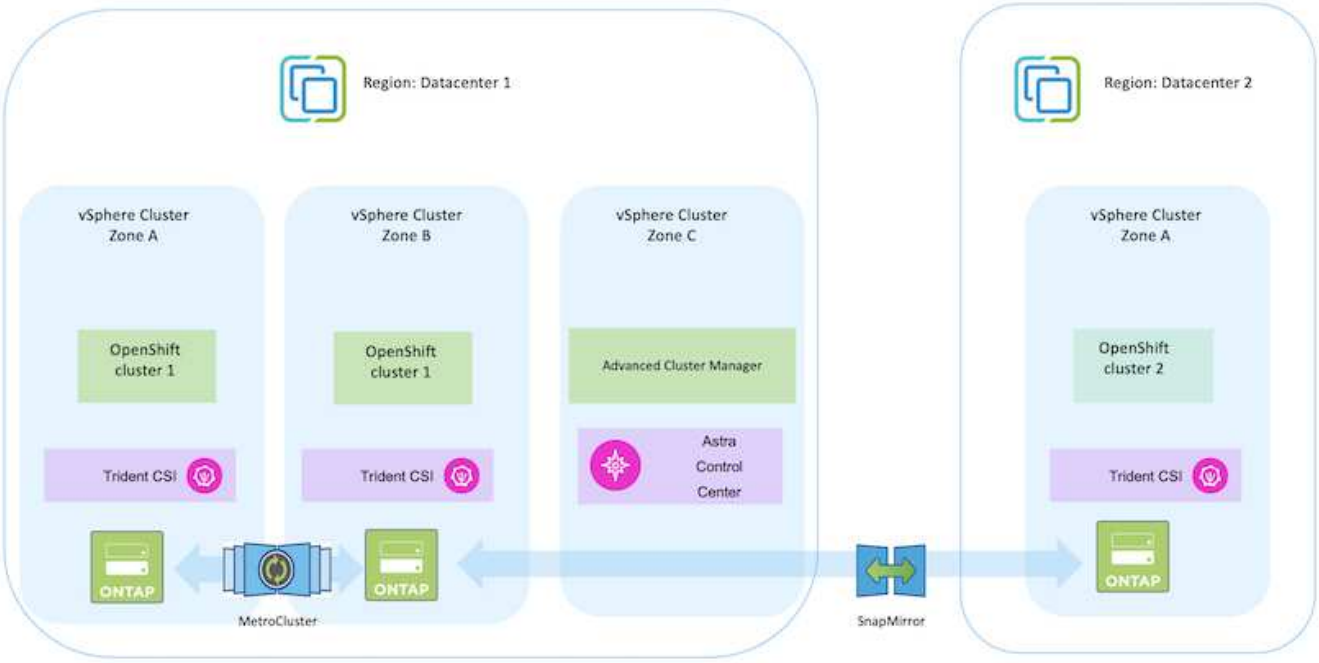
Si les clients ont besoin d'exécuter leurs applications conteneurisées modernes dans leur infrastructure dans leurs data centers privés, ils peuvent le faire. Ils doivent planifier et déployer Red Hat OpenShift Container Platform (OCP) pour que l'environnement de production soit prêt pour le déploiement de leurs workloads de conteneurs. Leurs clusters OCP peuvent être déployés sur VMware ou sur bare Metal.

Le stockage ONTAP de NetApp assure la protection, la fiabilité et la flexibilité des données pour les déploiements de conteneurs. ASTRA Trident sert de mécanisme de provisionnement de stockage dynamique pour consommer le stockage ONTAP persistant pour les applications avec état des clients. ASTRA Control Center peut être utilisé pour orchestrer les nombreuses exigences de gestion des données des applications avec état, telles que la protection des données, la migration et la continuité de l'activité.

Avec VMware vSphere, les outils NetApp ONTAP fournissent un plug-in vCenter qui peut être utilisé pour provisionner les datastores. Appliquez les balises et utilisez-les avec OpenShift pour stocker la configuration et les données des nœuds. Le stockage basé sur NVMe offre une latence faible et des performances élevées.

Cette solution fournit des informations détaillées sur la protection des données et la migration des workloads de conteneurs à l'aide d'Astra Control Center. Pour cette solution, les workloads de conteneurs sont déployés sur les clusters Red Hat OpenShift sur vSphere au sein de l'environnement sur site. REMARQUE : nous fournirons prochainement une solution pour les workloads de conteneurs sur des clusters OpenShift sur du serveur bare Metal.

Solution de protection et de migration des données pour les workloads de conteneurs OpenShift à l'aide d'Astra Control Center

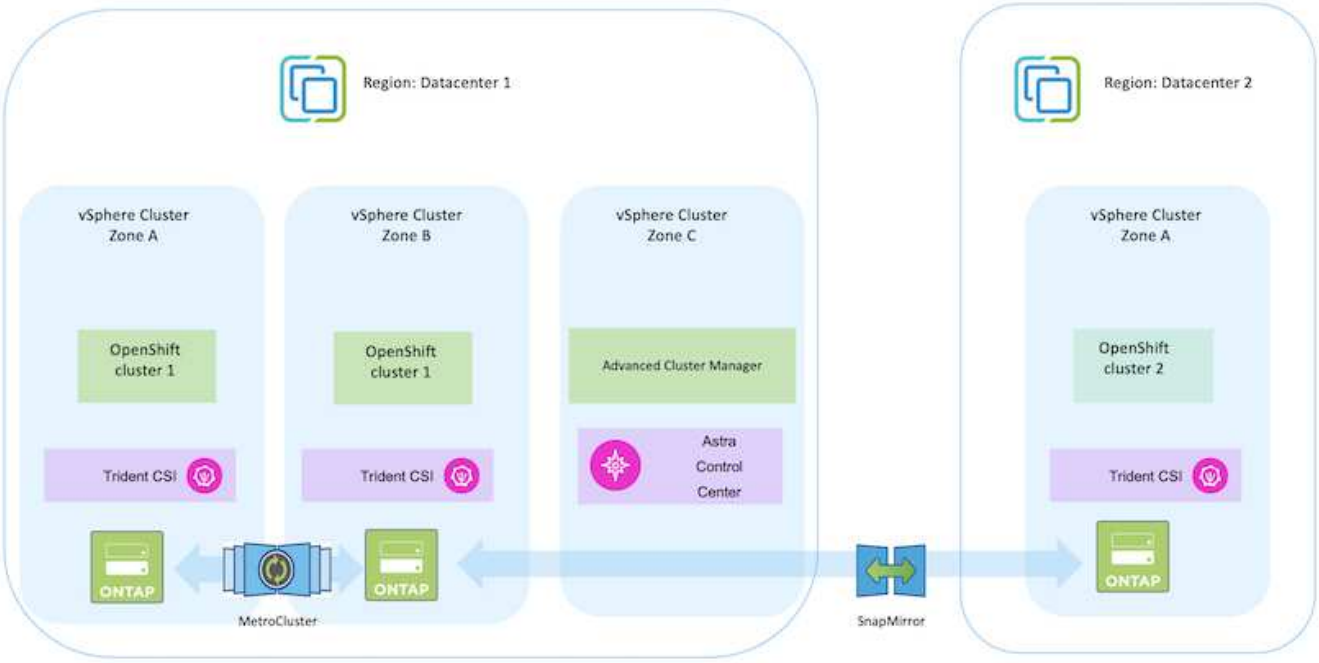


Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur VMware

Cette section décrit un workflow général expliquant comment configurer et gérer des clusters OpenShift et gérer des applications avec état sur ces clusters. Il présente l'utilisation des baies de stockage NetApp ONTAP à l'aide d'Astra Trident pour fournir des volumes persistants. Vous y trouverez des informations détaillées sur l'utilisation d'Astra Control Center pour effectuer les activités de protection des données et de migration des applications avec état.

> Il existe plusieurs façons de déployer les clusters de la plateforme de conteneurs Red Hat OpenShift. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Voici un diagramme illustrant les clusters déployés sur VMware dans un data Center.



Le processus de configuration peut être divisé en plusieurs étapes :

Déployez et configurez une machine virtuelle CentOS

- Elle est déployée dans l'environnement VMware vSphere.
- Cette VM sert à déployer certains composants, tels que NetApp Astra Trident et NetApp Astra Control Center, pour la solution.
- Un utilisateur root est configuré sur cette VM lors de l'installation.

Déploiement et configuration d'un cluster OpenShift Container Platform sur VMware vSphere (Hub Cluster)

Reportez-vous aux instructions du "Déploiement assisté" Méthode de déploiement d'un cluster OCP.

Souvenez-vous des éléments suivants : - Créez une clé publique et privée ssh à fournir au programme d'installation. Ces clés seront utilisées pour se connecter aux nœuds maître et worker si nécessaire. - Téléchargez le programme d'installation à partir de l'installateur assisté. Ce programme permet de démarrer les machines virtuelles que vous créez dans l'environnement VMware vSphere pour les nœuds maître et worker. - Les machines virtuelles doivent avoir la configuration minimale requise pour le processeur, la mémoire et le disque dur. (Reportez-vous aux commandes vm create sur "c'est ça" Pour les nœuds maître et worker qui fournissent ces informations) - l'UUID de disque doit être activé sur toutes les machines virtuelles. - Créer un minimum de 3 nœuds pour le maître et 3 nœuds pour le travailleur. - Une fois qu'ils sont découverts par le programme d'installation, activez le bouton bascule d'intégration de VMware vSphere.

Installez Advanced Cluster Management sur le cluster Hub

Ceci est installé à l'aide de l'opérateur de gestion avancée des clusters sur le cluster Hub. Reportez-vous aux instructions "ici".

Installez un registre Red Hat Quay interne sur le cluster Hub.

- Un registre interne est requis pour transmettre l'image Astra. Un registre interne Quay est installé à l'aide de l'opérateur dans le cluster Hub.
- Reportez-vous aux instructions "ici"

Installer deux clusters OCP supplémentaires (source et destination)

- Les clusters supplémentaires peuvent être déployés à l'aide de l'ACM sur le cluster Hub.
- Reportez-vous aux instructions "ici".

Configuration du stockage NetApp ONTAP

- Installez un cluster ONTAP connecté aux VM OCP dans un environnement VMware.
- Créer un SVM.
- Configurer la lif de données NAS pour accéder au stockage en SVM

Installez NetApp Trident sur les clusters OCP

- Installez NetApp Trident sur les trois clusters : concentrateur, source et destination
- Reportez-vous aux instructions "ici".
- Créez un système back-end de stockage pour ontap-nas .
- Créez une classe de stockage pour ontap-nas.
- Reportez-vous aux instructions "ici".

Installez NetApp Astra Control Center

- NetApp Astra Control Center est installé à l'aide d'Astra Operator sur le cluster Hub.
- Reportez-vous aux instructions "ici".

Points à retenir : * Téléchargez l'image NetApp Astra Control Center sur le site du support. * Poussez l'image dans un registre interne. * Reportez-vous aux instructions ici.

Déployer une application sur un cluster source

Déployez une application à l'aide d'OpenShift GitOps. (par ex. Postgres, fantôme)

Ajoutez les clusters source et cible dans Astra Control Center.

> Une fois que vous avez ajouté un cluster au système de gestion Astra Control, vous pouvez installer des applications sur le cluster (à l'extérieur d'Astra Control), puis accéder à la page applications dans Astra Control pour définir les applications et leurs ressources. Reportez-vous à la section "Commencez à gérer les applications d'Astra Control Center".

L'étape suivante consiste à utiliser Astra Control Center pour la protection des données et la migration des données du cluster source vers le cluster destination.

Protection des données avec Astra

Cette page présente les options de protection des données pour les applications basées sur des conteneurs Red Hat OpenShift qui s'exécutent sur VMware vSphere à l'aide d'Astra Control Center (ACC).

Au fur et à mesure que les utilisateurs s'engagent dans la modernisation de leurs applications avec Red Hat OpenShift, une stratégie de protection des données doit être mise en place pour les protéger contre toute suppression accidentelle ou toute autre erreur humaine. Souvent, une stratégie de protection est également nécessaire à des fins réglementaires ou de conformité afin de protéger leurs données contre les données d'un grand nombre.

Les exigences en matière de protection des données varient entre le retour à une copie instantanée et le basculement automatique vers un autre domaine de panne sans intervention humaine. De nombreux clients choisissent ONTAP comme plateforme de stockage préférée pour leurs applications Kubernetes en raison de ses nombreuses fonctionnalités, telles que la colocation, le multiprotocole, les performances et les capacités élevées, la réplication et la mise en cache pour les sites multisites, la sécurité et la flexibilité.

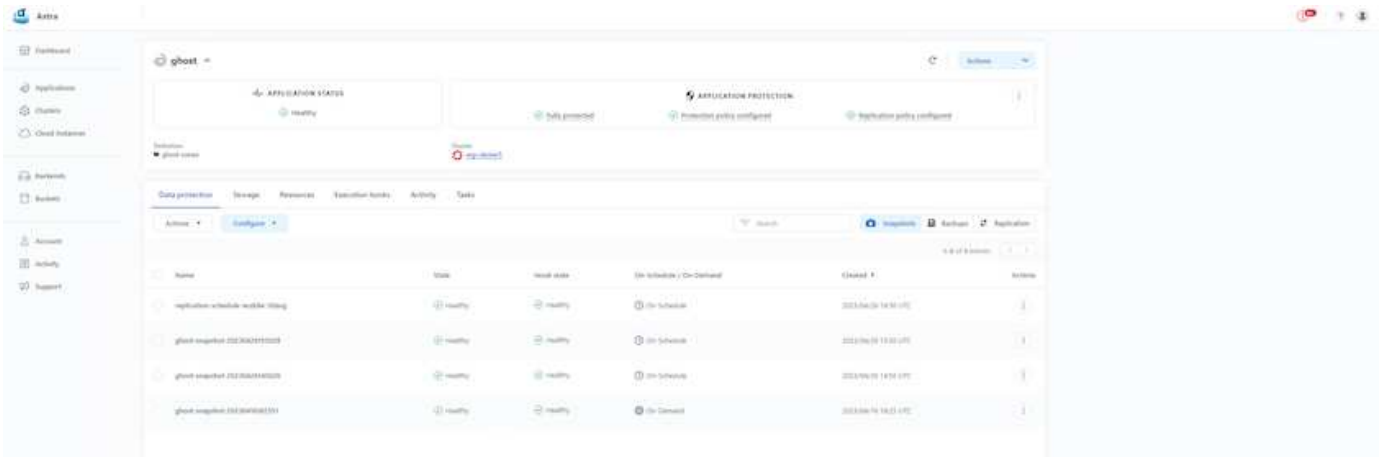
La protection des données dans ONTAP peut être obtenue en utilisant ad hoc ou contrôlé par des règles - **instantané** - **sauvegarde et restauration**

Les copies Snapshot et les sauvegardes protègent les types de données suivants : - **les métadonnées de l'application qui représentent l'état de l'application** - **tout volume de données persistantes associé à l'application** - **tout artefact de ressource appartenant à l'application**

Instantané avec ACC

Une copie instantanée des données peut être capturée à l'aide de Snapshot avec ACC. La règle de protection définit le nombre de copies Snapshot à conserver. L'option horaire minimum disponible est horaire. Les copies Snapshot manuelles à la demande peuvent être effectuées à tout moment et à intervalles plus courts que les copies Snapshot planifiées. Les copies Snapshot sont stockées sur le même volume provisionné que l'application.

Configuration de l'instantané avec ACC

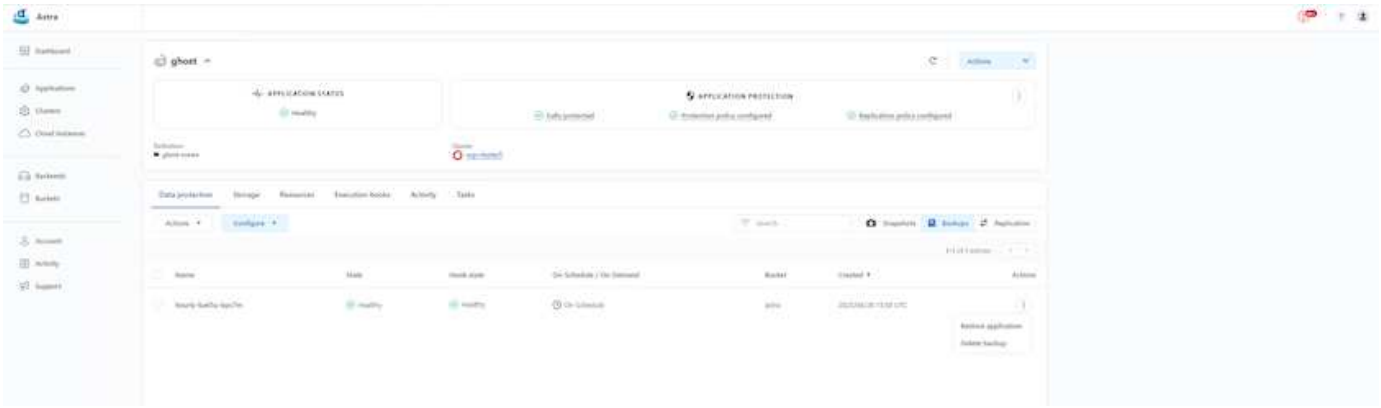


Sauvegarde et restauration avec ACC

Une sauvegarde est basée sur une copie Snapshot. ACC peut effectuer des copies Snapshot à l'aide de CSI et effectuer des sauvegardes à l'aide de la copie Snapshot instantanée. La sauvegarde est stockée dans un magasin d'objets externe (tout système s3 compatible avec ONTAP S3 à un emplacement différent). La règle de protection peut être configurée pour les sauvegardes planifiées et le nombre de versions de sauvegarde à conserver. L'objectif de point de récupération minimal est d'une heure.

Restauration d'une application à partir d'une sauvegarde à l'aide d'ACC

ACC restaure l'application à partir du compartiment S3 où sont stockées les sauvegardes.



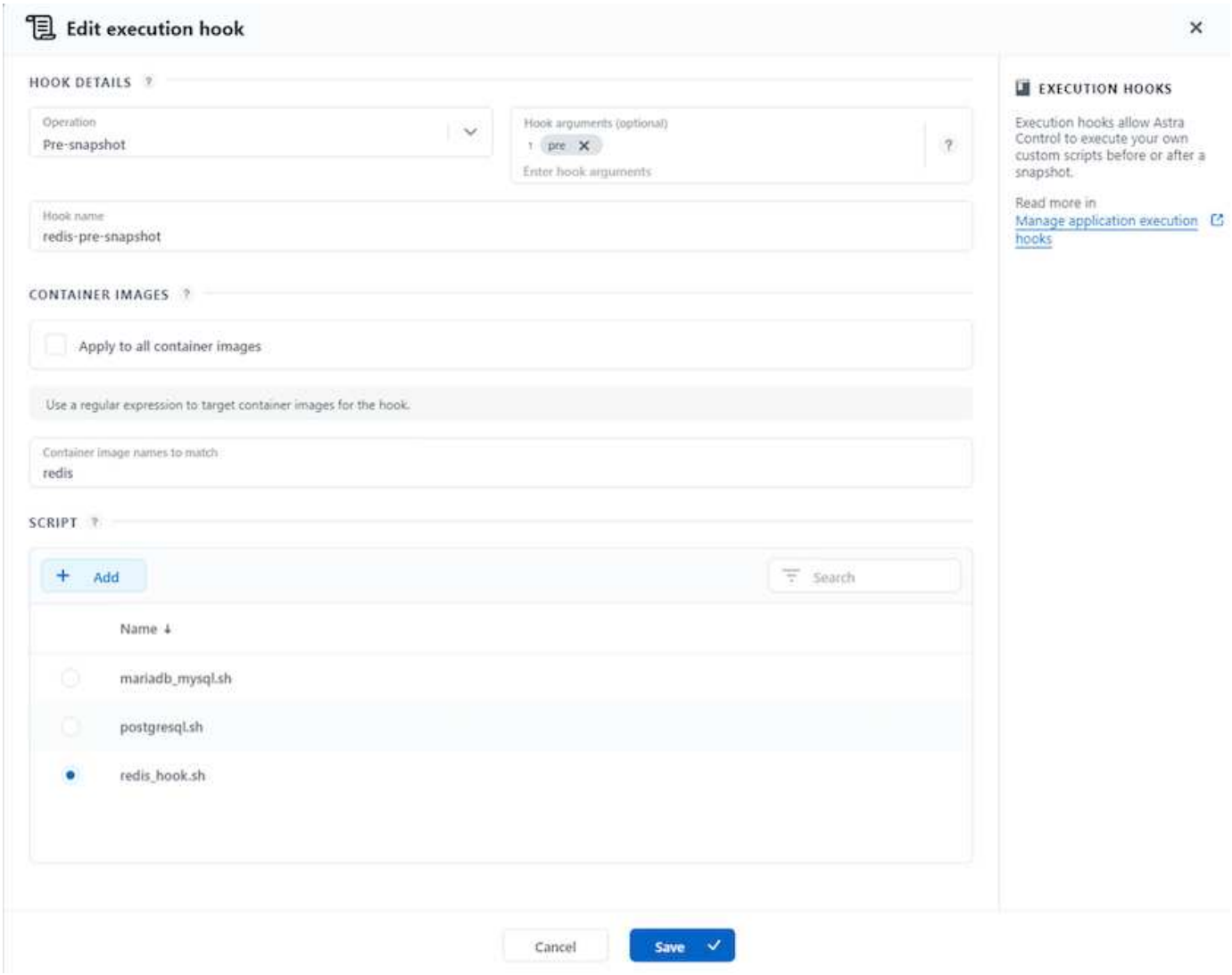
Crochets d'exécution spécifiques à l'application

En outre, vous pouvez configurer des crochets d'exécution pour qu'ils s'exécutent en conjonction avec une opération de protection des données d'une application gérée. Même si les fonctionnalités de protection des données au niveau des baies de stockage sont disponibles, il est souvent nécessaire de suivre des étapes supplémentaires pour rendre les sauvegardes et les restaurations cohérentes avec les applications. Les étapes supplémentaires spécifiques à l'application peuvent être : - avant ou après la création d'une copie Snapshot. - avant ou après la création d'une sauvegarde. - Après restauration à partir d'une copie Snapshot ou d'une sauvegarde.

ASTRA Control peut exécuter ces étapes spécifiques à l'application codées comme des scripts personnalisés appelés crochets d'exécution.

"Projet GitHub NetApp Verda" fournit des crochets d'exécution pour les applications cloud les plus courantes afin de simplifier, renforcer et orchestrer la protection des applications. N'hésitez pas à contribuer à ce projet si vous avez suffisamment d'informations pour une application qui ne se trouve pas dans le référentiel.

Exemple de crochet d'exécution pour pré-instantané d'une application redis.



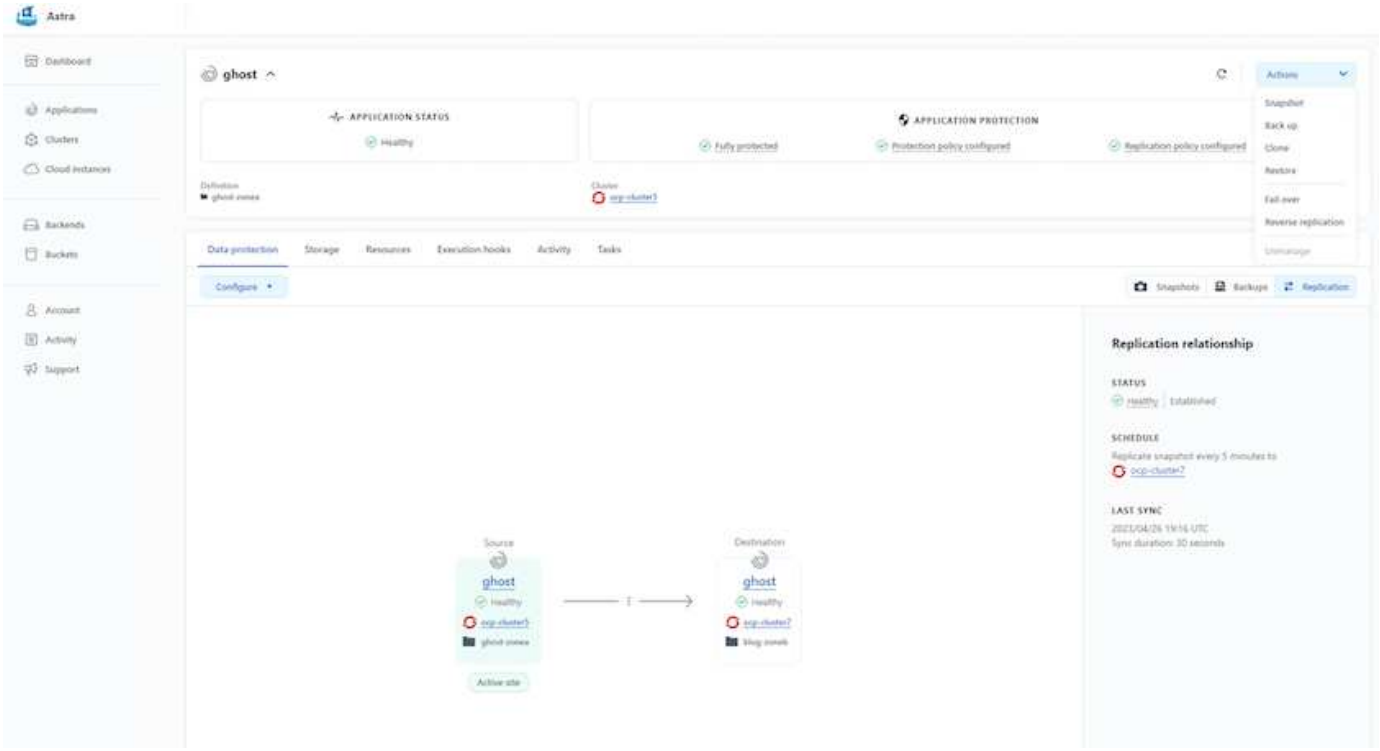
Réplication avec ACC

Pour la protection régionale ou pour une solution à faible RPO et RTO, une application peut être répliquée vers une autre instance Kubernetes s'exécutant sur un autre site, de préférence dans une autre région. ACC utilise ONTAP Async SnapMirror avec RPO à partir de 5 minutes. La réplication s'effectue par réplication dans ONTAP, puis un basculement crée les ressources Kubernetes dans le cluster de destination.

Notez que la réplication est différente de la sauvegarde et de la restauration où la sauvegarde est envoyée vers S3 et la restauration depuis S3. Pour plus d'informations sur les différences entre les deux types de protection des données, consultez le lien : here.

Reportez-vous à "ici" Pour obtenir les instructions d'installation de SnapMirror.

SnapMirror avec ACC



les pilotes de stockage san-economy et nas-economy ne prennent pas en charge la fonction de réplication. Reportez-vous à "ici" pour plus d'informations.

Vidéo de démonstration :

"Vidéo de démonstration de la reprise d'activité avec Astra Control Center"

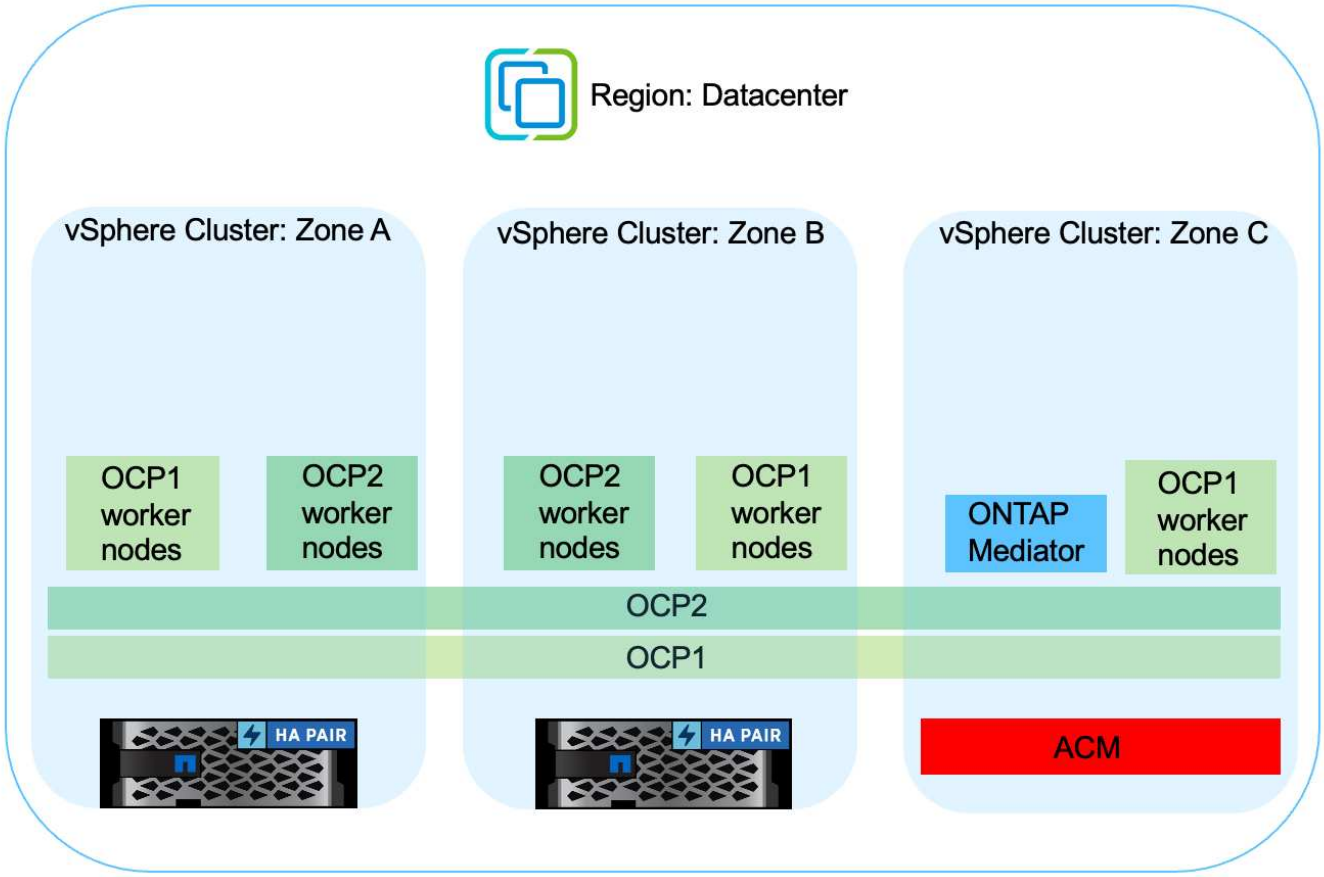
Protection des données avec Astra Control Center

Continuité de l'activité avec MetroCluster

La plupart de notre plate-forme matérielle pour ONTAP dispose de fonctionnalités de haute disponibilité pour se protéger contre les pannes de systèmes, ce qui évite d'avoir à effectuer des opérations de récupération à plat. Mais pour éviter les risques d'incendie ou de tout autre incident et pour poursuivre l'activité avec un RPO nul et un RTO faible, on utilise souvent une solution MetroCluster.

Les clients qui disposent actuellement d'un système ONTAP peuvent s'étendre à MetroCluster en ajoutant des systèmes ONTAP pris en charge dans les limites de distance pour fournir une reprise après incident au niveau de la zone. ASTRA Trident, le CSI (interface de stockage de conteneurs) prend en charge NetApp ONTAP, y compris la configuration MetroCluster, ainsi que d'autres options comme Cloud Volumes ONTAP, Azure NetApp Files, AWS FSX pour NetApp ONTAP, etc ASTRA Trident inclut cinq options de pilotes de stockage pour ONTAP et tous sont pris en charge pour la configuration MetroCluster. Reportez-vous à "ici" Pour en savoir plus sur les pilotes de stockage ONTAP pris en charge par Astra Trident.

La solution MetroCluster nécessite une extension réseau de couche 2 ou une capacité d'accès à la même adresse réseau à partir des deux domaines de défaillance. Une fois la configuration MetroCluster en place, la solution est transparente pour les propriétaires d'applications, puisque tous les volumes du svm MetroCluster sont protégés et profitent des avantages de SyncMirror (RPO nul).



Pour la configuration back-end Trident (TBC), ne spécifiez pas la dataLIF et le SVM lors de l'utilisation de la configuration MetroCluster. Spécifier l'IP de gestion du SVM pour la LIF managementLIF et utiliser les identifiants de rôle vsadmin

Des informations détaillées sur les fonctionnalités de protection des données d'Astra Control Center sont disponibles "ici"

Migration des données à l'aide d'Astra Control Center

Cette page présente les options de migration des données pour les workloads de conteneurs sur des clusters Red Hat OpenShift avec Astra Control Center (ACC).

Les applications Kubernetes doivent souvent être déplacées d'un environnement à un autre. Pour migrer une application et ses données persistantes, il est possible d'utiliser NetApp ACC.

Migration des données entre différents environnements Kubernetes

ACC prend en charge plusieurs versions de Kubernetes, notamment Google Anthos, Red Hat OpenShift, Tanzu Kubernetes Grid, Rancher Kubernetes Engine, Kubernetes en amont, etc Pour plus d'informations, reportez-vous à la section "ici".

Pour migrer une application d'un cluster à un autre, vous pouvez utiliser l'une des fonctions suivantes d'ACC :

- **réplication**
- **sauvegarde et restauration**

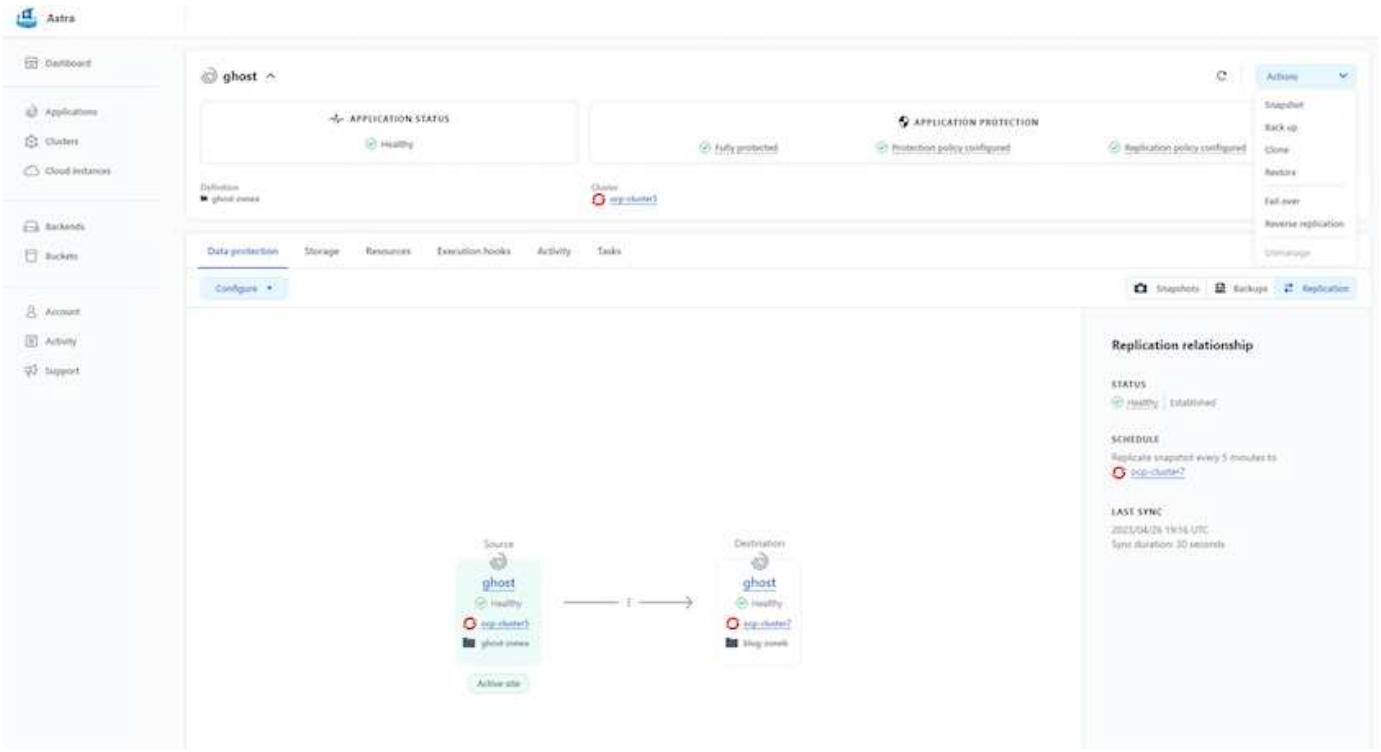
- **clone**

Reportez-vous à la "section sur la protection des données" pour les options **réplication et sauvegarde et restauration**.

Reportez-vous à "ici" pour plus de détails sur **clonage**.

> La fonctionnalité de réplication Astra n'est prise en charge qu'avec le plug-in Trident Container Storage interface (CSI). Cependant, la réplication n'est pas prise en charge par les pilotes NAS-Economy et san-Economy.

Réplication des données à l'aide d'ACC



Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

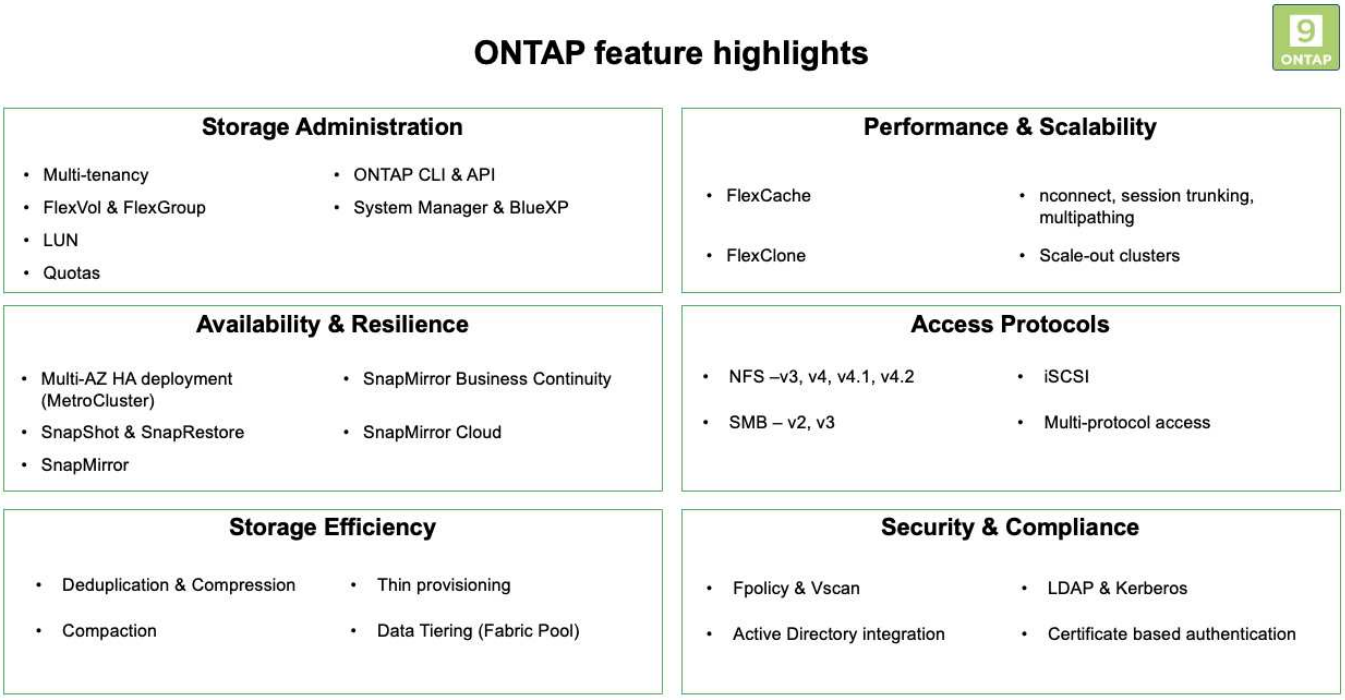
Présentation

NetApp constate une augmentation significative des clients qui modernisent leurs applications d'entreprise existantes et créent de nouvelles applications à l'aide de conteneurs et de plateformes d'orchestration basées sur Kubernetes. Nous avons adopté Red Hat OpenShift Container Platform comme bon nombre de nos clients.

Alors que les clients sont de plus en plus nombreux à adopter des conteneurs dans leur entreprise, NetApp est parfaitement positionné pour répondre aux besoins de stockage persistant de leurs applications avec état et aux besoins de gestion des données classiques, tels que la protection, la sécurité et la migration des données. Toutefois, ces besoins sont satisfaits à l'aide de stratégies, d'outils et de méthodes différents.

Les options de stockage basées sur NetApp ONTAP sont énumérées ci-dessous et offrent sécurité, protection des données, fiabilité et flexibilité pour les conteneurs et les déploiements Kubernetes.

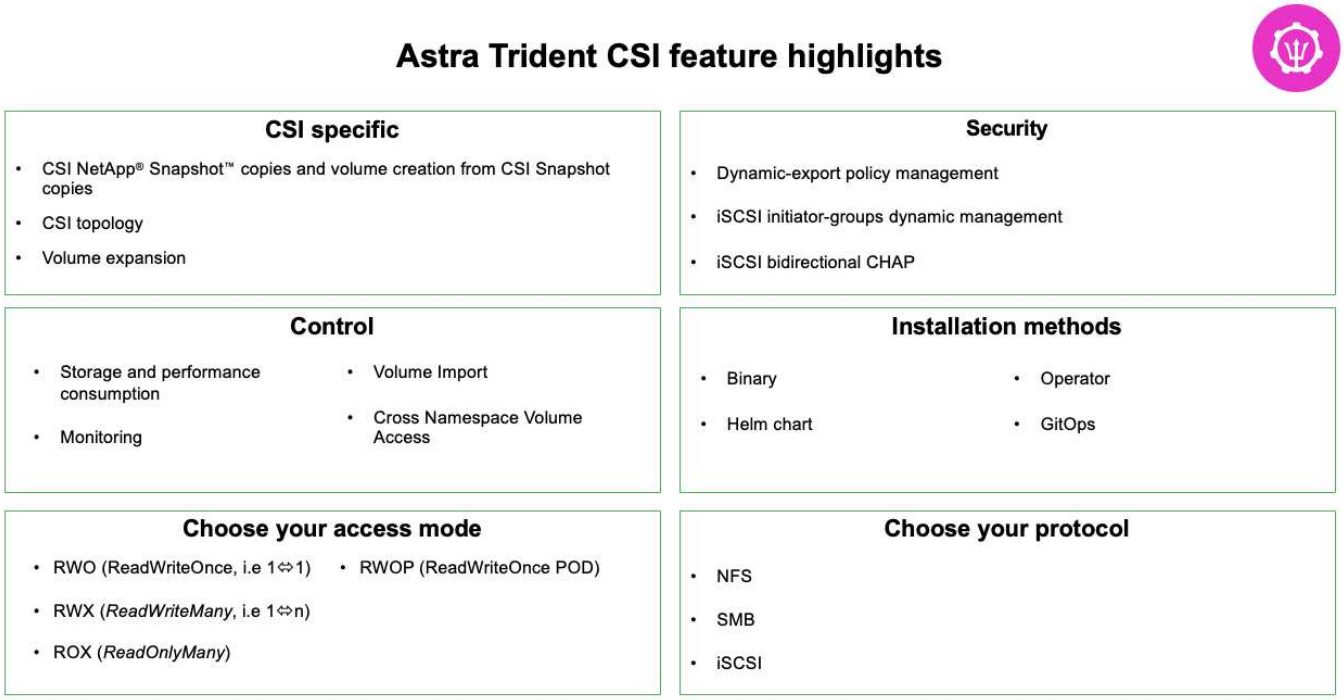
- Stockage autogéré sur site :
  - Stockage FAS (Fabric Attached Storage), baies FAS 100 % Flash (AFF), baies SAN ASA (All SAN Array) et ONTAP Select
- Stockage géré par un fournisseur sur site :
  - NetApp Keystone fournit une solution de stockage en tant que service (STaaS)
- Stockage autogéré dans le cloud :
  - NetApp Cloud volumes ONTAP (CVO) fournit un stockage autogéré dans les hyperscalers
- Stockage géré par un fournisseur dans le cloud :
  - Cloud Volumes Service pour Google Cloud (CVS), Azure NetApp Files (ANF) et Amazon FSX pour NetApp ONTAP offrent un stockage entièrement géré dans les hyperscalers



NetApp BlueXP vous permet de gérer l'ensemble de vos ressources de stockage et de données à partir d'un seul plan de contrôle/interface.

Vous pouvez utiliser BlueXP pour créer et gérer du stockage cloud (par exemple, Cloud Volumes ONTAP et Azure NetApp Files), déplacer, protéger et analyser les données, et contrôler de nombreux systèmes de stockage sur site et en périphérie.

NetApp Astra Trident est un orchestrateur de stockage conforme à CSI qui permet de consommer rapidement et facilement du stockage persistant grâce à plusieurs options de stockage NetApp mentionnées ci-dessus. Il s'agit d'un logiciel open source géré et pris en charge par NetApp.



Les workloads de conteneurs stratégiques requièrent bien plus que de simples volumes persistants. Leurs exigences de gestion des données requièrent également la protection et la migration des objets kubernetes applicatifs.

Les données d'application incluent des objets kubernetes en plus des données utilisateur. Voici quelques exemples : - Objets kubernetes tels que les pods Specs, les PVC, les déploiements, les services - objets de configuration personnalisés tels que les cartes de configuration et les secrets - données persistantes telles que les copies Snapshot, les sauvegardes, les clones - ressources personnalisées telles que CRS et CRD

NetApp Astra Control, disponible en tant que logiciel entièrement géré et autogéré, assure l'orchestration pour une gestion robuste des données d'application. Reportez-vous à la "Documentation Astra" Pour en savoir plus sur la gamme de produits Astra.

Cette documentation de référence apporte la validation de la migration et de la protection des applications basées sur des conteneurs, déployées sur une plateforme de conteneurs RedHat OpenShift à l'aide de NetApp Astra Control Center. En outre, la solution fournit des détails généraux sur le déploiement et l'utilisation de Red Hat Advanced Cluster Management (ACM) pour la gestion des plateformes de conteneurs. Ce document détaille également les modalités d'intégration du stockage NetApp avec les plateformes de conteneurs Red Hat OpenShift à l'aide d'Astra Trident CSI Provisioner. ASTRA Control Center est déployé sur le cluster Hub et est utilisé pour gérer les applications de conteneur et leur cycle de vie de stockage persistant. Enfin, il fournit une solution de réplication, de basculement et de retour arrière pour les workloads de conteneurs sur des clusters Red Hat OpenShift gérés dans AWS (ROSA) utilisant Amazon FSX pour NetApp ONTAP (FSxN) en tant que stockage persistant.

Solution NetApp avec les workloads de plateforme de conteneurs Red Hat OpenShift dans le cloud hybride

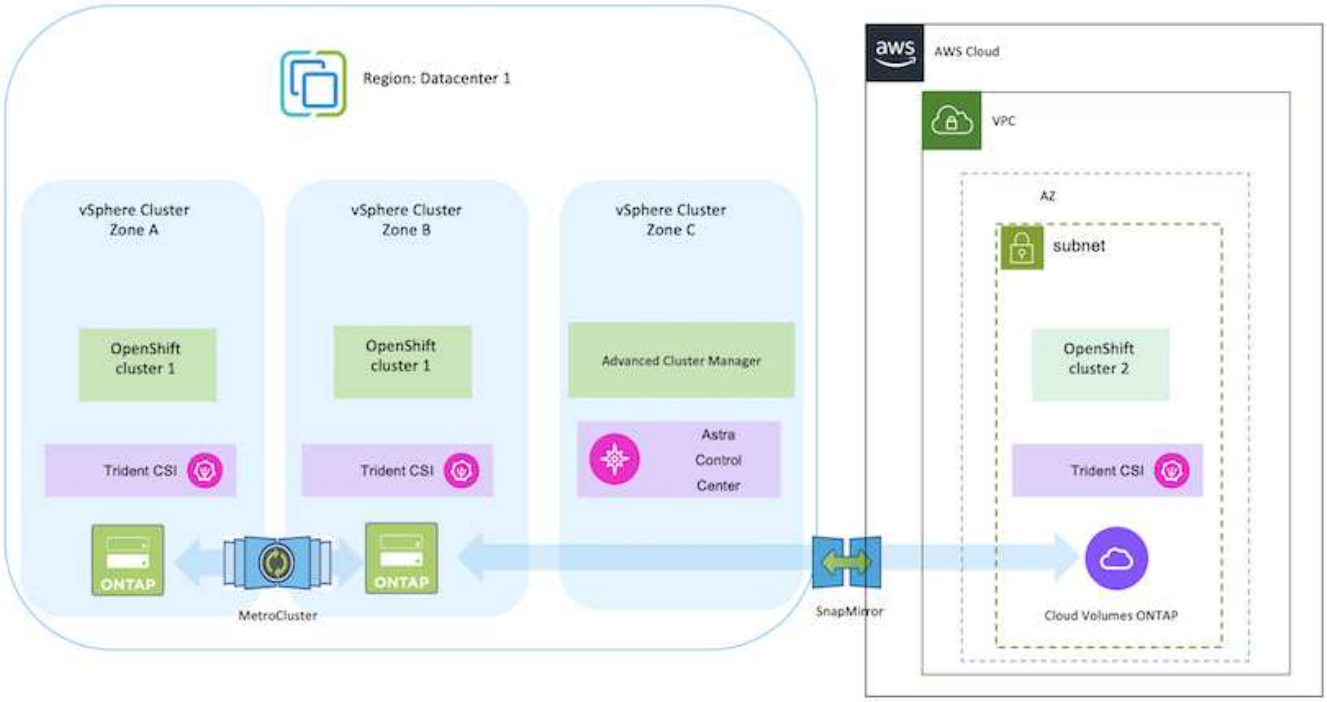
Les clients peuvent se trouver à un point de leur parcours de modernisation lorsqu'ils sont prêts à déplacer des workloads spécifiques ou tous les workloads de leurs data centers vers le cloud. Ils peuvent choisir d'utiliser des conteneurs OpenShift autogérés et

du stockage NetApp autogéré dans le cloud pour diverses raisons. Ils doivent planifier et déployer Red Hat OpenShift Container Platform (OCP) dans le cloud pour que l'environnement soit prêt à la production et puisse migrer les workloads de conteneurs depuis leurs data centers. Leurs clusters OCP peuvent être déployés sur VMware ou bare Metal dans leurs data centers, ainsi que sur AWS, Azure ou Google Cloud dans l'environnement cloud.

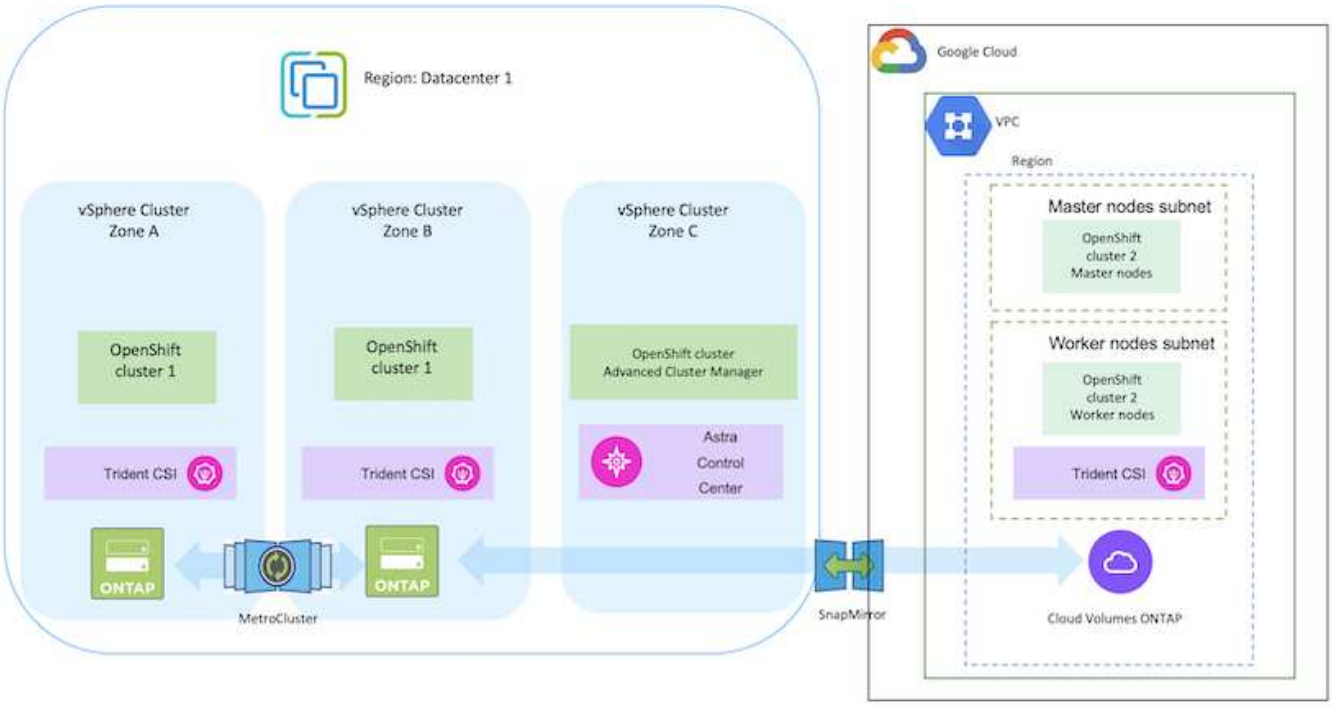
Le stockage NetApp Cloud Volumes ONTAP assure la protection, la fiabilité et la flexibilité des données pour les déploiements de conteneurs dans AWS, Azure et dans Google Cloud. ASTRA Trident sert de mécanisme de provisionnement de stockage dynamique pour consommer le stockage Cloud Volumes ONTAP persistant pour les applications avec état des clients. ASTRA Control Center peut être utilisé pour orchestrer les nombreuses exigences de gestion des données des applications avec état, telles que la protection des données, la migration et la continuité de l'activité.

Solution de protection et de migration des données pour les workloads de conteneurs OpenShift dans un cloud hybride via Astra Control Center

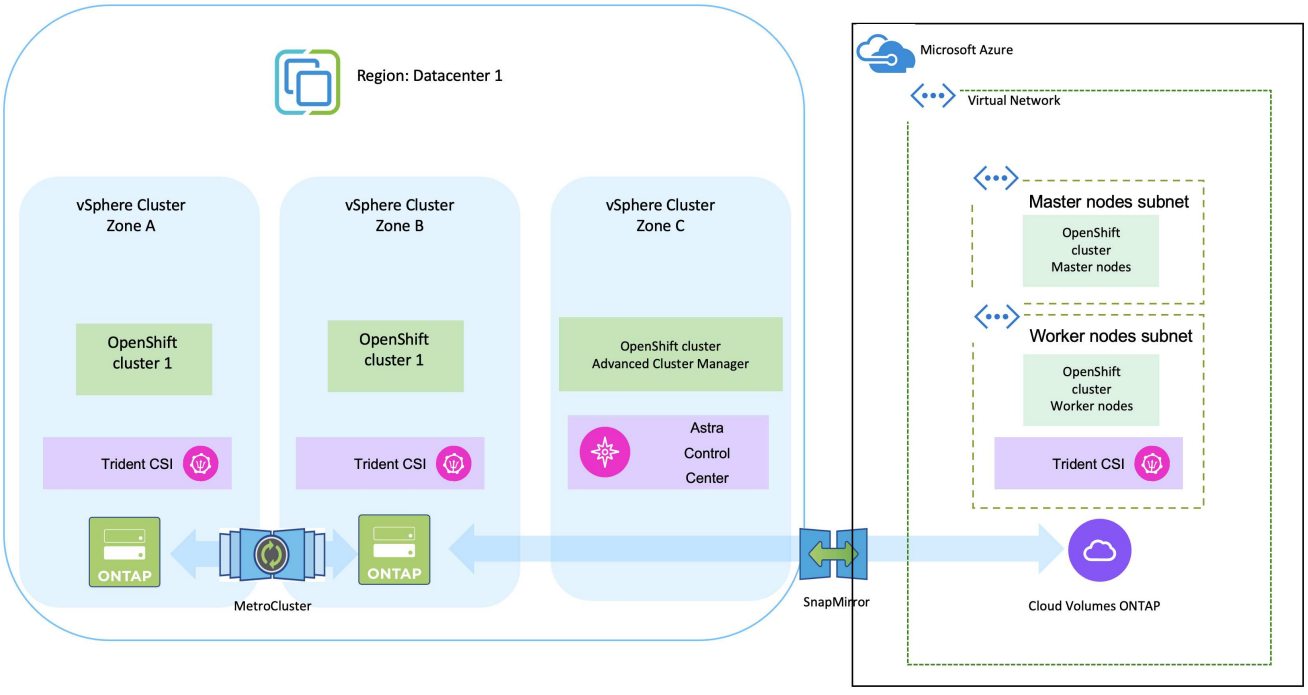
Sur site et AWS



Sur site et Google Cloud



Sur site et dans le cloud Azure

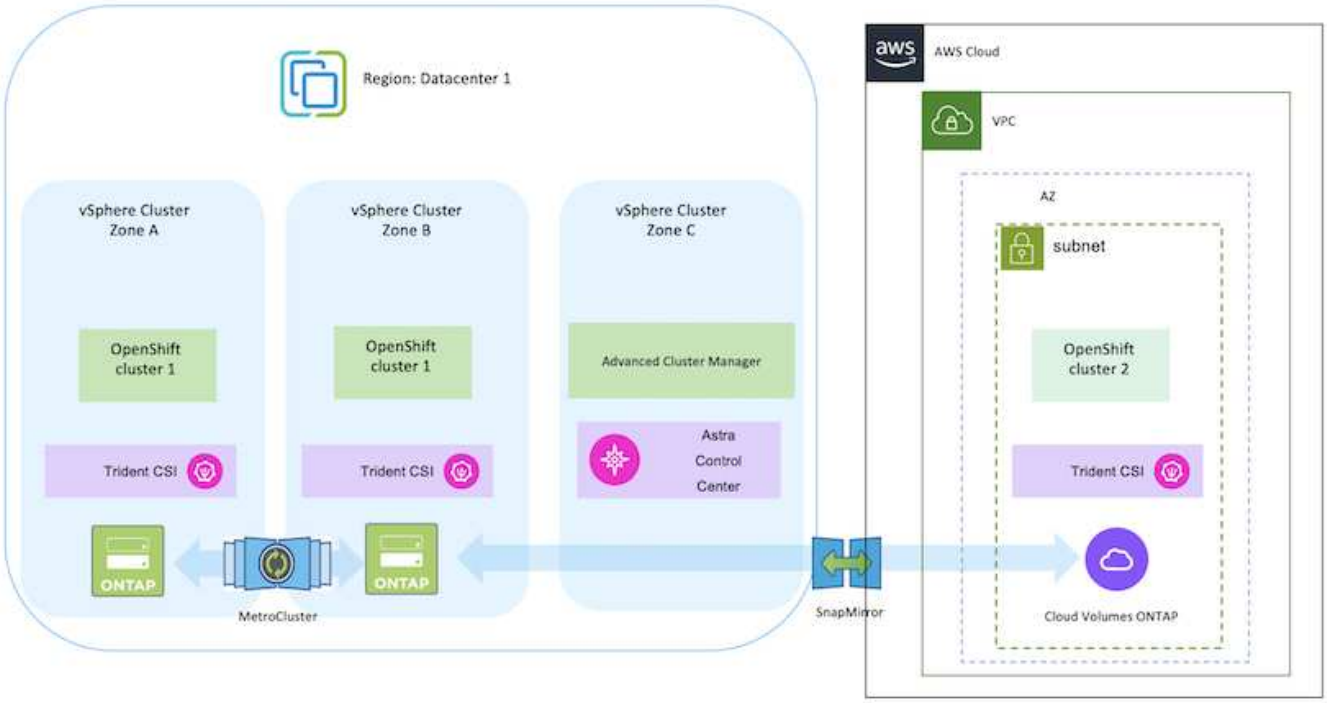


Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur AWS

Cette section décrit un workflow général expliquant comment configurer et gérer des clusters OpenShift dans AWS et comment déployer des applications avec état sur ces clusters. Il présente l'utilisation du stockage NetApp Cloud Volumes ONTAP à l'aide d'Astra Trident pour fournir des volumes persistants. Vous y trouverez des informations détaillées sur l'utilisation d'Astra Control Center pour effectuer les activités de protection des données et de migration des applications avec état.

Il existe plusieurs façons de déployer les clusters Red Hat OpenShift Container Platform sur AWS. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Voici un diagramme illustrant les clusters déployés sur AWS et connectés au data Center à l'aide d'un VPN.



Le processus de configuration peut être divisé en plusieurs étapes :

Installez un cluster OCP sur AWS à partir de Advanced Cluster Management.

- Créez un VPC avec une connexion VPN de site à site (à l'aide de pfsense) pour vous connecter au réseau sur site.
- Le réseau sur site dispose d'une connectivité Internet.
- Créez 3 sous-réseaux privés dans 3 zones de disponibilité différentes.
- Créez une zone hébergée privée route 53 et un résolveur DNS pour le VPC.

Créez OpenShift Cluster sur AWS à partir de l'assistant ACM (Advanced Cluster Management). Reportez-vous aux instructions "ici".

Vous pouvez également créer le cluster dans AWS à partir de la console OpenShift Hybrid Cloud. Reportez-vous à "ici" pour obtenir des instructions.

Lors de la création du cluster à l'aide de l'ACM, vous avez la possibilité de personnaliser l'installation en modifiant le fichier yaml après avoir rempli les détails dans la vue de formulaire. Une fois le cluster créé, vous pouvez vous connecter en ssh aux nœuds du cluster à des fins de dépannage ou à des fins de configuration manuelle supplémentaire. Utilisez la clé ssh que vous avez fournie lors de l'installation et le nom d'utilisateur core pour vous connecter.

Déployez Cloud Volumes ONTAP dans AWS à l'aide de BlueXP.

- Installez le connecteur dans un environnement VMware sur site. Reportez-vous aux instructions "ici".
- Déployez une instance CVO dans AWS à l'aide de Connector. Reportez-vous aux instructions "ici".

Le connecteur peut également être installé dans l'environnement cloud. Reportez-vous à "ici" pour plus d'informations.

Installer Astra Trident dans le cluster OCP

- Déployez l'opérateur Trident à l'aide d'Helm. Reportez-vous aux instructions "ici"
- Créez un back-end et une classe de stockage. Reportez-vous aux instructions "ici".

Ajoutez le cluster OCP sur AWS à Astra Control Center.

Ajoutez le cluster OCP dans AWS à Astra Control Center.

Utilisation de la fonctionnalité de topologie CSI de Trident pour les architectures multi-zones

Les fournisseurs de cloud permettent aujourd'hui aux administrateurs de clusters Kubernetes/OpenShift de frayer les nœuds des clusters basés sur les zones. Les nœuds peuvent se trouver dans différentes zones de disponibilité au sein d'une région ou entre différentes régions. Astra Trident utilise la topologie CSI pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multi-zones. Grâce à la fonction de topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Reportez-vous à "ici" pour plus d'informations.

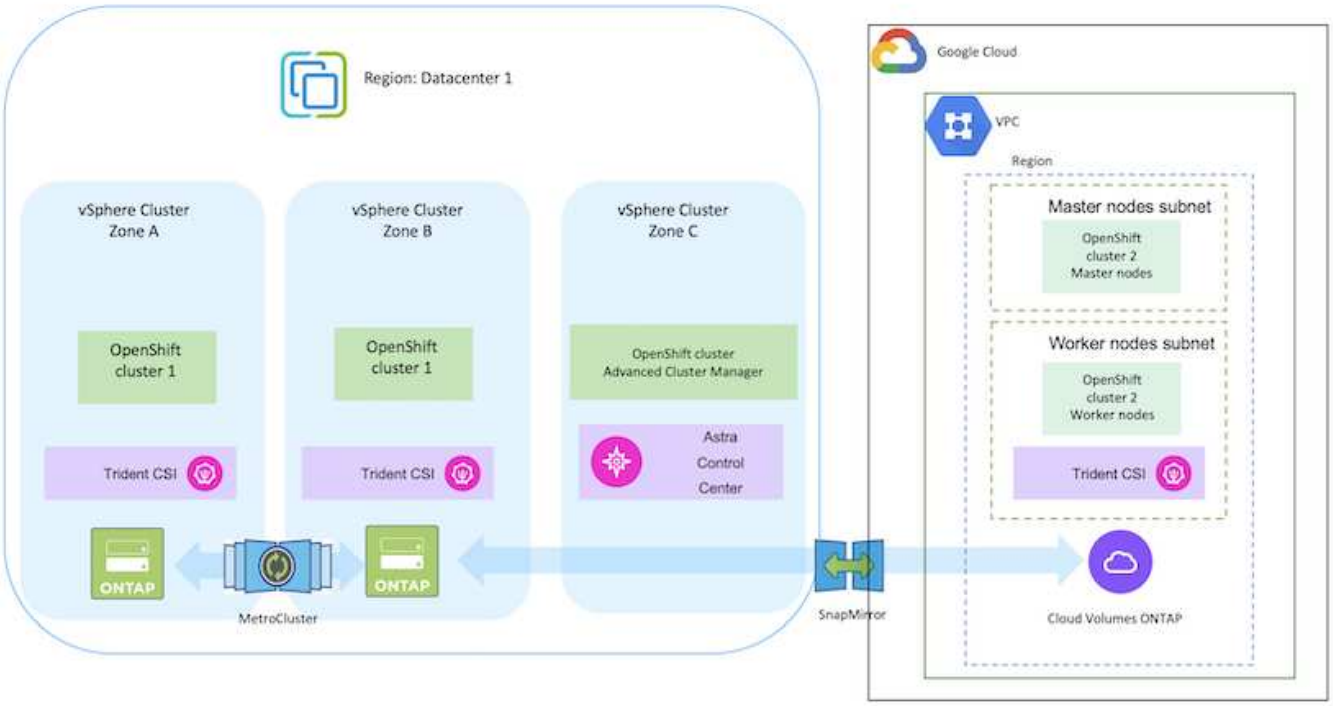
Kubernetes prend en charge deux modes de liaison de volume : - lorsque ***VolumeBindingMode*** **est défini sur** ***immédiat*** (par défaut), Astra Trident crée le volume sans sensibilisation à la topologie. Les volumes persistants sont créés sans dépendance vis-à-vis des exigences de planification du pod qui en fait la demande. - Lorsque ***VolumeBindingMode*** **est défini sur** ***WaitForFirstConsumer***, la création et la liaison d'un volume persistant pour une PVC est retardée jusqu'à ce qu'un pod qui utilise la PVC soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification appliquées en fonction des besoins de topologie. Les systèmes back-end de stockage Astra Trident peuvent être conçus pour provisionner de manière sélective des volumes en fonction des zones de disponibilité (back-end compatible avec la topologie). Pour les classes de stockage qui utilisent un tel backend, un volume ne sera créé que si une application est planifiée dans une région/zone prise en charge. (Classes de stockage orientées topologie) "ici" pour plus d'informations.

Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur GCP

Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur GCP

Cette section décrit un workflow de haut niveau expliquant comment configurer et gérer des clusters OpenShift dans GCP et déployer des applications avec état sur ces clusters. Il présente l'utilisation du stockage NetApp Cloud Volumes ONTAP à l'aide d'Astra Trident pour fournir des volumes persistants. Vous y trouverez des informations détaillées sur l'utilisation d'Astra Control Center pour effectuer les activités de protection des données et de migration des applications avec état.

La présente figure présente les clusters déployés sur GCP et connectés au data Center à l'aide d'un VPN.



Il existe plusieurs façons de déployer les clusters de plateforme de conteneurs Red Hat OpenShift dans GCP. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Le processus de configuration peut être divisé en plusieurs étapes :

Installez un cluster OCP sur GCP à partir de l'interface de ligne de commande.

- Assurez-vous que vous avez rempli toutes les conditions préalables indiquées "ici".
- Pour la connectivité VPN entre l'infrastructure sur site et GCP, une machine virtuelle pfsense a été créée et configurée. Pour obtenir des instructions, reportez-vous à la section "ici".
  - L'adresse de la passerelle distante dans pfsense ne peut être configurée qu'après avoir créé une passerelle VPN dans Google Cloud Platform.
  - Les adresses IP de réseau distant pour la phase 2 ne peuvent être configurées qu'après l'exécution du programme d'installation du cluster OpenShift et la création des composants d'infrastructure pour le cluster.
  - Le VPN dans Google Cloud ne peut être configuré qu'une fois que les composants de l'infrastructure du cluster ont été créés par le programme d'installation.
- Installez maintenant le cluster OpenShift sur GCP.
  - Obtenez le programme d'installation et le code Pull et déployez le cluster en suivant les étapes fournies dans la documentation "ici".
  - L'installation crée un réseau VPC dans Google Cloud Platform. Il crée également une zone privée dans Cloud DNS et ajoute Des enregistrements.
    - Utilisez l'adresse de bloc CIDR du réseau VPC pour configurer pfsense et établir la connexion VPN. Assurez-vous que les pare-feu sont correctement configurés.
    - Ajoutez des enregistrements dans le DNS de l'environnement sur site en utilisant l'adresse IP dans les enregistrements A du DNS Google Cloud.
  - L'installation du cluster est terminée et fournira un fichier kubeconfig ainsi qu'un nom d'utilisateur et un mot de passe pour vous connecter à la console du cluster.

Déployez Cloud Volumes ONTAP dans GCP à l'aide de BlueXP.

- Installez un connecteur dans Google Cloud. Reportez-vous aux instructions "ici".
- Déployez une instance CVO dans Google Cloud à l'aide de Connector. Reportez-vous aux instructions ici. https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-gcp.html

Installez Astra Trident dans le cluster OCP dans GCP

- Comme illustré, il existe de nombreuses méthodes de déploiement d'Astra Trident "ici".
- Pour ce projet, Astra Trident a été installé en déployant l'opérateur Astra Trident manuellement en utilisant les instructions "ici".
- Créez le back-end et des classes de stockage. Reportez-vous aux instructions "ici".

Ajoutez le cluster OCP sur GCP à Astra Control Center.

- Créez un fichier KubeConfig distinct avec un rôle de cluster qui contient les autorisations minimales nécessaires à la gestion d'un cluster par Astra Control. Les instructions sont disponibles "ici".
- Ajoutez le cluster à Astra Control Center en suivant les instructions "ici"

Utilisation de la fonctionnalité de topologie CSI de Trident pour les architectures multi-zones

Les fournisseurs de cloud permettent aujourd'hui aux administrateurs de clusters Kubernetes/OpenShift de frayer les nœuds des clusters basés sur les zones. Les nœuds peuvent se trouver dans différentes zones de disponibilité au sein d'une région ou entre différentes régions. Astra Trident utilise la topologie CSI pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multi-zones. Grâce à la fonction de topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Reportez-vous à "ici" pour plus d'informations.

> Kubernetes prend en charge deux modes de liaison de volume : - lorsque ***VolumeBindingMode*** **est défini sur** ***immédiat*** (par défaut), Astra Trident crée le volume sans sensibilisation à la topologie. Les volumes persistants sont créés sans dépendance vis-à-vis des exigences de planification du pod qui en fait la demande. - Lorsque ***VolumeBindingMode*** **est défini sur** ***WaitForFirstConsumer***, la création et la liaison d'un volume persistant pour une PVC est retardée jusqu'à ce qu'un pod qui utilise la PVC soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification appliquées en fonction des besoins de topologie. Les systèmes back-end de stockage Astra Trident peuvent être conçus pour provisionner de manière sélective des volumes en fonction des zones de disponibilité (back-end compatible avec la topologie). Pour les classes de stockage qui utilisent un tel backend, un volume ne sera créé que si une application est planifiée dans une région/zone prise en charge. (Classes de stockage orientées topologie) "ici" pour plus d'informations.

vidéo de démonstration

Installation d'OpenShift Cluster sur Google Cloud Platform

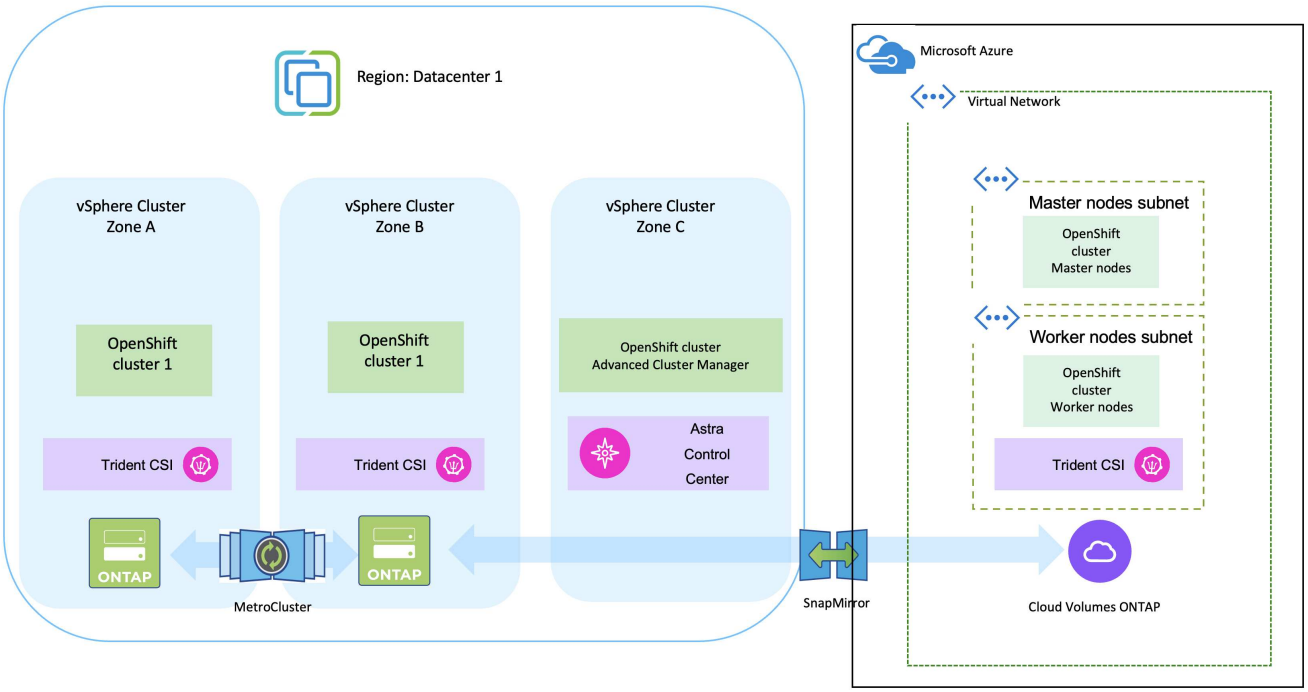
Importation de clusters OpenShift dans Astra Control Center

Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur Azure

Déploiement et configuration de la plateforme de conteneurs Red Hat OpenShift sur Azure

Cette section décrit un workflow général expliquant comment configurer et gérer des clusters OpenShift dans Azure et comment déployer des applications avec état sur ces clusters. Il présente l'utilisation du stockage NetApp Cloud Volumes ONTAP à l'aide d'Astra Trident/Astra Control Provisioner pour fournir des volumes persistants. Vous y trouverez des informations détaillées sur l'utilisation d'Astra Control Center pour effectuer les activités de protection des données et de migration des applications avec état.

Voici un diagramme illustrant les clusters déployés sur Azure et connectés au data Center à l'aide d'un VPN.



Il existe plusieurs façons de déployer les clusters de plateforme de conteneurs Red Hat OpenShift dans Azure. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Le processus de configuration peut être divisé en plusieurs étapes :

Installez un cluster OCP sur Azure à partir de l'interface de ligne de commande.

- Assurez-vous que vous avez rempli toutes les conditions préalables indiquées "ici".
- Créez un VPN, des sous-réseaux et des groupes de sécurité réseau, ainsi qu'une zone DNS privée. Créez une passerelle VPN et une connexion VPN de site à site.
- Pour la connectivité VPN entre les installations sur site et Azure, une machine virtuelle pfsense a été créée et configurée. Pour obtenir des instructions, reportez-vous à la section "ici".
- Obtenez le programme d'installation et le code Pull et déployez le cluster en suivant les étapes fournies dans la documentation "ici".
- L'installation du cluster est terminée et fournira un fichier kubeconfig ainsi qu'un nom d'utilisateur et un mot de passe pour vous connecter à la console du cluster.

Un exemple de fichier install-config.yaml est fourni ci-dessous.

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

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

Déployez Cloud Volumes ONTAP dans Azure à l'aide de BlueXP.

- Installez un connecteur dans Azure. Reportez-vous aux instructions "ici".
- Déployez une instance CVO dans Azure à l'aide de Connector. Reportez-vous au lien d'instructions :https://docs.netapp.com/us-en/bluexp-cloud-volumes-ontap/task-getting-started-azure.html [ici].

Installez Astra Control Provisioner dans le cluster OCP dans Azure

- Pour ce projet, Astra Control Provisioner (ACP) a été installé sur tous les clusters (cluster sur site, cluster sur site où Astra Control Center est déployé et le cluster dans Azure). En savoir plus sur Astra Control Provisioner "ici".
- Créez le back-end et des classes de stockage. Reportez-vous aux instructions "ici".

Ajoutez le cluster OCP sur Azure à Astra Control Center.

- Créez un fichier KubeConfig distinct avec un rôle de cluster qui contient les autorisations minimales nécessaires à la gestion d'un cluster par Astra Control. Les instructions sont disponibles "ici".
- Ajoutez le cluster à Astra Control Center en suivant les instructions "ici"

Utilisation de la fonctionnalité de topologie CSI de Trident pour les architectures multi-zones

Les fournisseurs de cloud permettent aujourd'hui aux administrateurs de clusters Kubernetes/OpenShift de frayer les nœuds des clusters basés sur les zones. Les nœuds peuvent se trouver dans différentes zones de disponibilité au sein d'une région ou entre différentes régions. Astra Trident utilise la topologie CSI pour faciliter le provisionnement des volumes pour les charges de travail dans une architecture multi-zones. Grâce à la fonction de topologie CSI, l'accès aux volumes peut être limité à un sous-ensemble de nœuds, en fonction des régions et des zones de disponibilité. Reportez-vous à "ici" pour plus d'informations.

> Kubernetes prend en charge deux modes de liaison de volume : - lorsque ***VolumeBindingMode*** **est défini sur** ***immédiat*** (par défaut), Astra Trident crée le volume sans sensibilisation à la topologie. Les volumes persistants sont créés sans dépendance vis-à-vis des exigences de planification du pod qui en fait la demande. - Lorsque ***VolumeBindingMode*** **est défini sur** ***WaitForFirstConsumer***, la création et la liaison d'un volume persistant pour une PVC est retardée jusqu'à ce qu'un pod qui utilise la PVC soit planifié et créé. De cette façon, les volumes sont créés pour répondre aux contraintes de planification appliquées en fonction des besoins de topologie. Les systèmes back-end de stockage Astra Trident peuvent être conçus pour provisionner de manière sélective des volumes en fonction des zones de disponibilité (back-end compatible avec la topologie). Pour les classes de stockage qui utilisent un tel backend, un volume ne sera créé que si une application est planifiée dans une région/zone prise en charge. (Classes de stockage orientées topologie) "ici" pour plus d'informations.

vidéo de démonstration

Utilisation d'Astra Control pour le basculement et le retour arrière des applications

Protection des données avec Astra Control Center

Cette page présente les options de protection des données pour les applications basées sur des conteneurs Red Hat OpenShift s'exécutant sur VMware vSphere ou dans le cloud via Astra Control Center (ACC).

Au fur et à mesure que les utilisateurs s'engagent dans la modernisation de leurs applications avec Red Hat OpenShift, une stratégie de protection des données doit être mise en place pour les protéger contre toute suppression accidentelle ou toute autre erreur humaine. Souvent, une stratégie de protection est également nécessaire à des fins réglementaires ou de conformité afin de protéger leurs données contre les données d'un grand nombre.

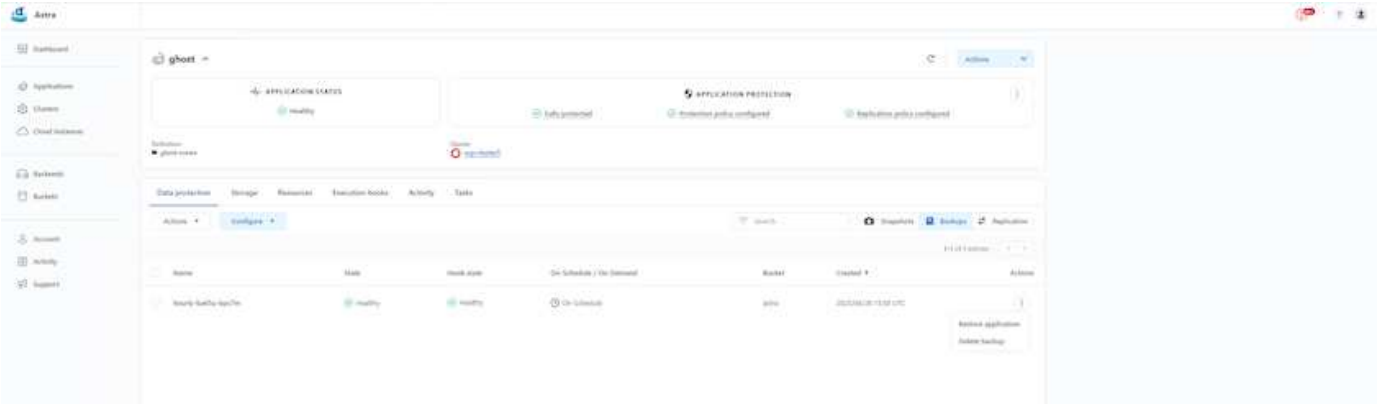
Les exigences en matière de protection des données varient entre le retour à une copie instantanée et le basculement automatique vers un autre domaine de panne sans intervention humaine. De nombreux clients choisissent ONTAP comme plateforme de stockage préférée pour leurs applications Kubernetes en raison de ses nombreuses fonctionnalités, telles que la colocation, le multiprotocole, les performances et les capacités élevées, la réplication et la mise en cache pour les sites multisites, la sécurité et la flexibilité.

Les clients peuvent disposer d'un environnement cloud pour étendre leur data Center, afin de bénéficier des avantages du cloud et de disposer d'un positionnement idéal pour déplacer leurs charges de travail à un moment ultérieur. Pour ces clients, la sauvegarde de leurs applications OpenShift et de leurs données dans l'environnement cloud devient un choix inévitable. Ils peuvent ensuite restaurer les applications et les données associées sur un cluster OpenShift dans le cloud ou dans leur data Center.

Sauvegarde et restauration avec ACC

Les propriétaires d'applications peuvent consulter et mettre à jour les applications découvertes par ACC. ACC peut effectuer des copies Snapshot à l'aide de CSI et effectuer des sauvegardes à l'aide de la copie Snapshot instantanée. La destination de la sauvegarde peut être un magasin d'objets dans l'environnement cloud. La règle de protection peut être configurée pour les sauvegardes planifiées et le nombre de versions de sauvegarde à conserver. L'objectif de point de récupération minimal est d'une heure.

Restauration d'une application à partir d'une sauvegarde à l'aide d'ACC

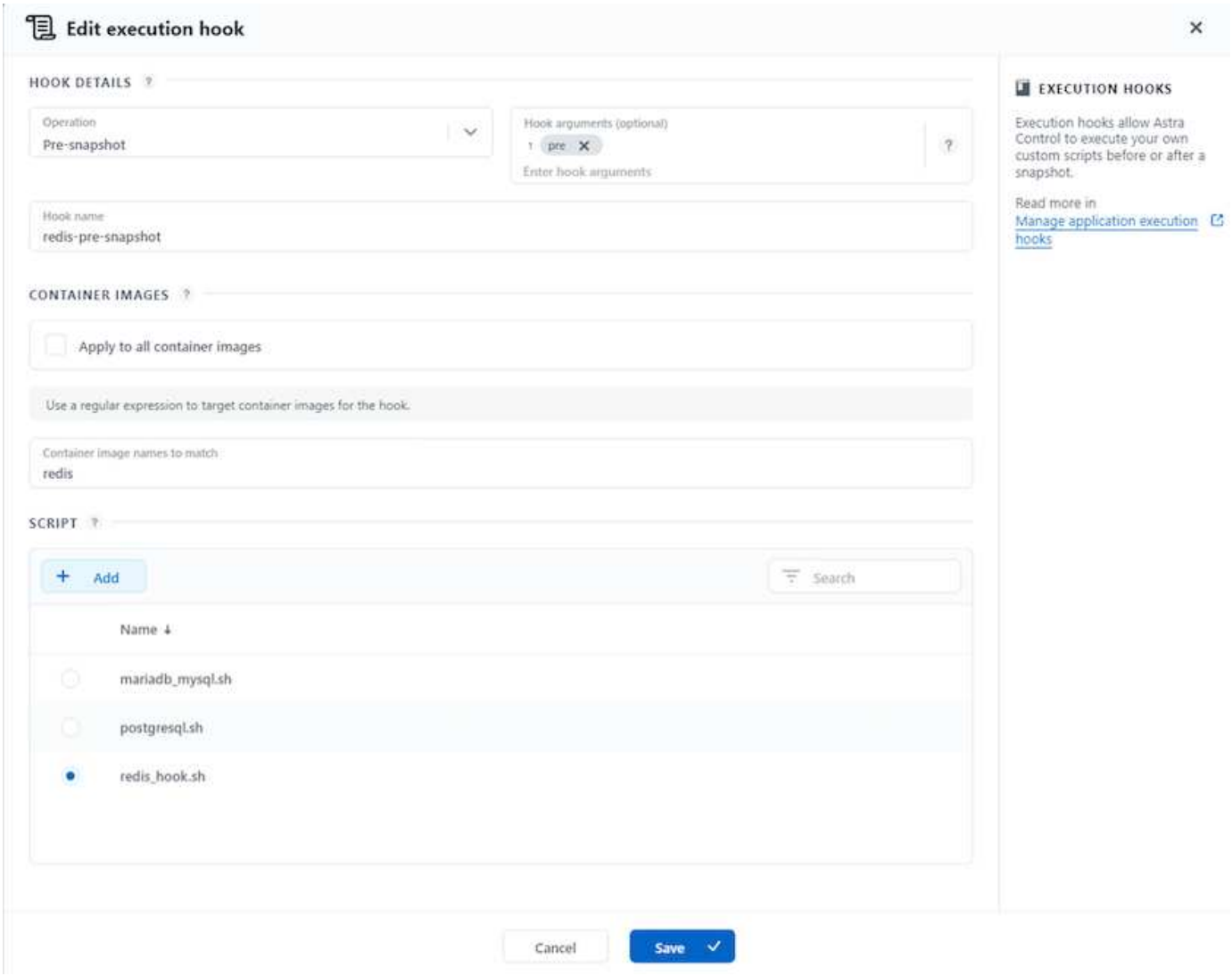


Crochets d'exécution spécifiques à l'application

Même si les fonctionnalités de protection des données au niveau des baies de stockage sont disponibles, des étapes supplémentaires sont souvent nécessaires pour assurer la cohérence des sauvegardes et des restaurations au niveau des applications. Les étapes supplémentaires spécifiques à l'application peuvent être : - avant ou après la création d'une copie Snapshot. - avant ou après la création d'une sauvegarde. - Après restauration à partir d'une copie Snapshot ou d'une sauvegarde. ASTRA Control peut exécuter ces étapes spécifiques à l'application codées comme des scripts personnalisés appelés crochets d'exécution.

NetApp "Projet open source Verda" fournit des crochets d'exécution pour les applications cloud les plus courantes afin de simplifier, renforcer et orchestrer la protection des applications. N'hésitez pas à contribuer à ce projet si vous avez suffisamment d'informations pour une application qui ne se trouve pas dans le référentiel.

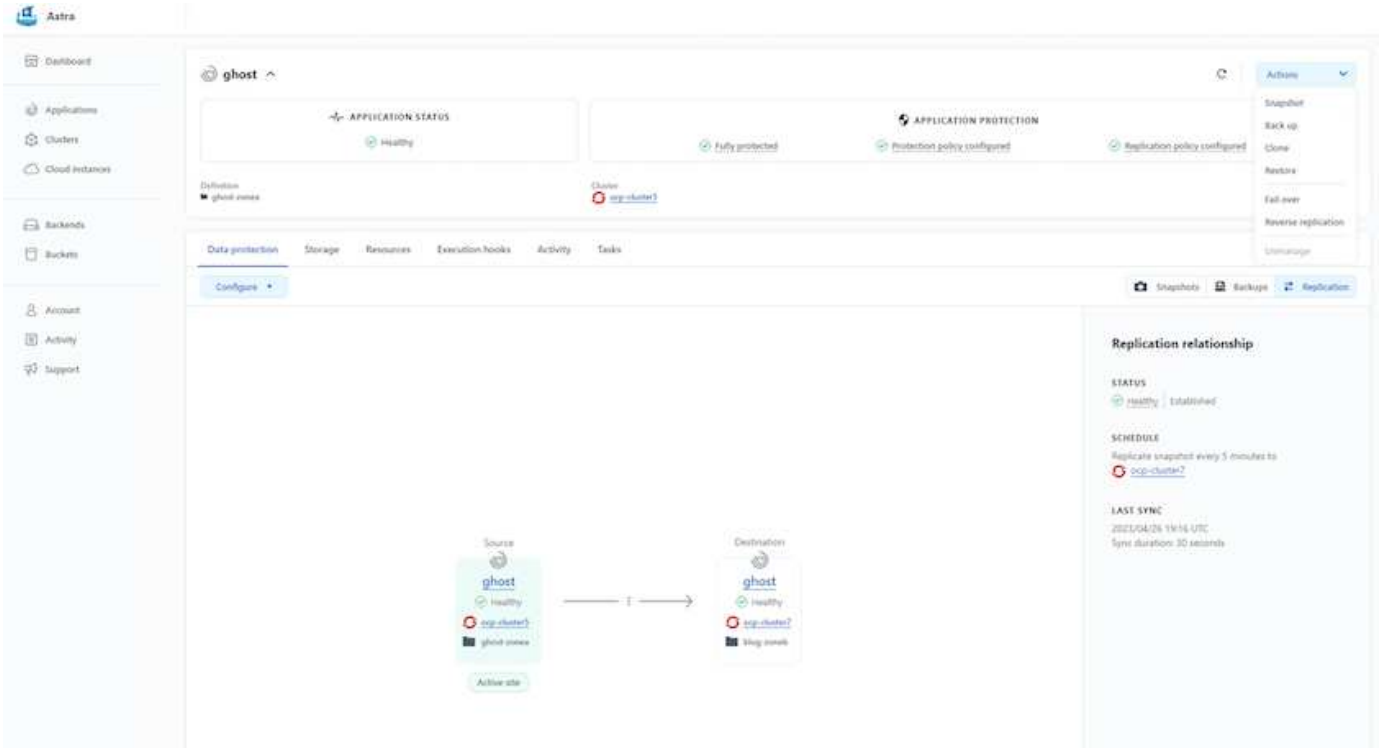
Exemple de crochet d'exécution pour pré-instantané d'une application redis.



Réplication avec ACC

Pour la protection régionale ou pour une solution à faible RPO et RTO, une application peut être répliquée vers une autre instance Kubernetes s'exécutant sur un autre site, de préférence dans une autre région. ACC utilise ONTAP Async SnapMirror avec RPO à partir de 5 minutes. Reportez-vous à "ici" Pour obtenir les instructions d'installation de SnapMirror.

SnapMirror avec ACC



les pilotes de stockage san-economy et nas-economy ne prennent pas en charge la fonction de réplication. Reportez-vous à "ici" pour plus d'informations.

Vidéo de démonstration :

"Vidéo de démonstration de la reprise d'activité avec Astra Control Center"

Protection des données avec Astra Control Center

Des informations détaillées sur les fonctionnalités de protection des données d'Astra Control Center sont disponibles "ici"

Reprise après incident (basculement et retour arrière avec réplication) avec ACC

Utilisation d'Astra Control pour le basculement et le retour arrière des applications

Migration des données à l'aide d'Astra Control Center

Cette page présente les options de migration des données pour les workloads de conteneurs sur des clusters Red Hat OpenShift avec Astra Control Center (ACC). Plus précisément, les clients peuvent utiliser ACC pour : déplacer des workloads sélectionnés ou tous les workloads de leurs data centers sur site vers le cloud ; cloner leurs applications vers le cloud à des fins de test ou passer du data Center au cloud

Migration des données

Pour migrer une application d'un environnement à un autre, vous pouvez utiliser l'une des fonctions suivantes d'ACC :

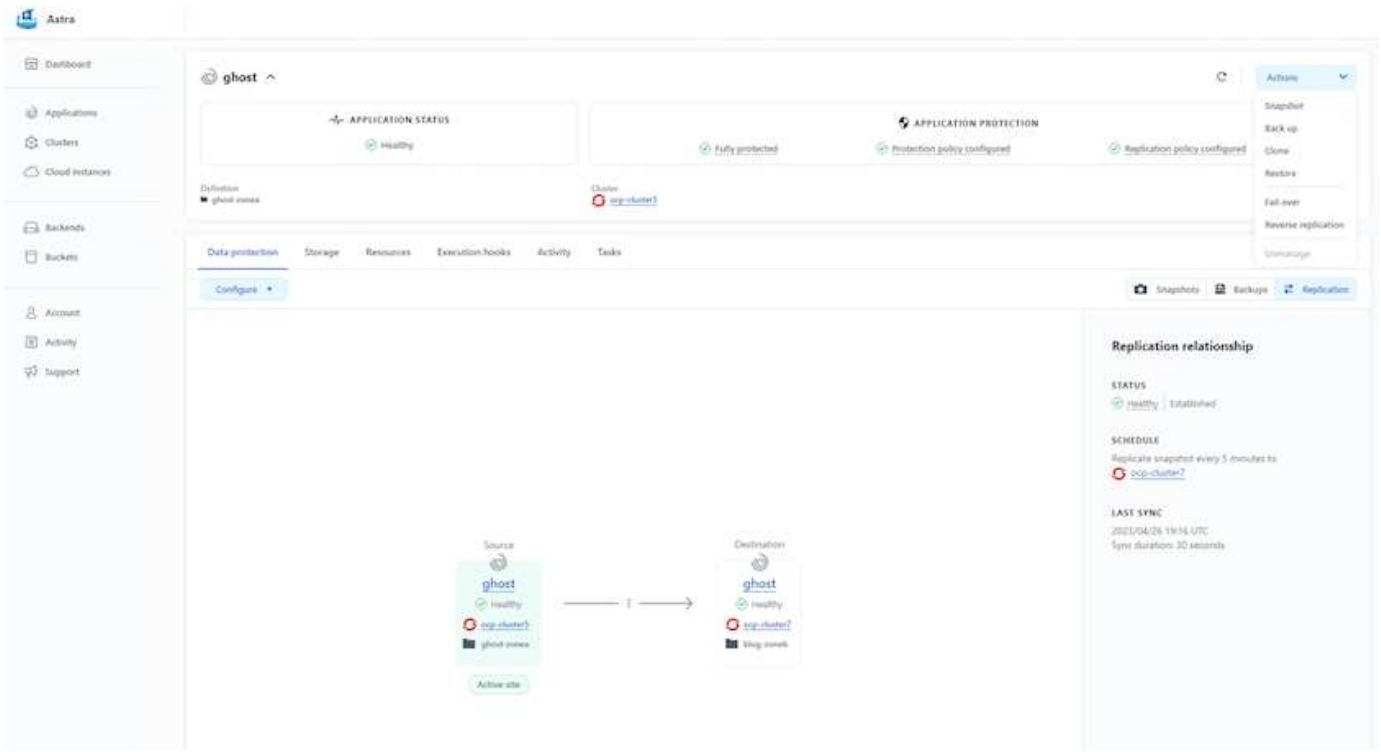
- **réplication**

- **sauvegarde et restauration**
- **clone**

Reportez-vous à la "section sur la protection des données" pour les options **réplication et sauvegarde et restauration**. Reportez-vous à "ici" pour plus de détails sur **clonage**.

La fonctionnalité de réplication Astra n'est prise en charge qu'avec le plug-in Trident Container Storage interface (CSI). Cependant, la réplication n'est pas prise en charge par les pilotes NAS-Economy et san-Economy.

Réplication des données à l'aide d'ACC



Solutions multicloud hybrides NetApp pour les workloads de conteneurs Red Hat OpenShift

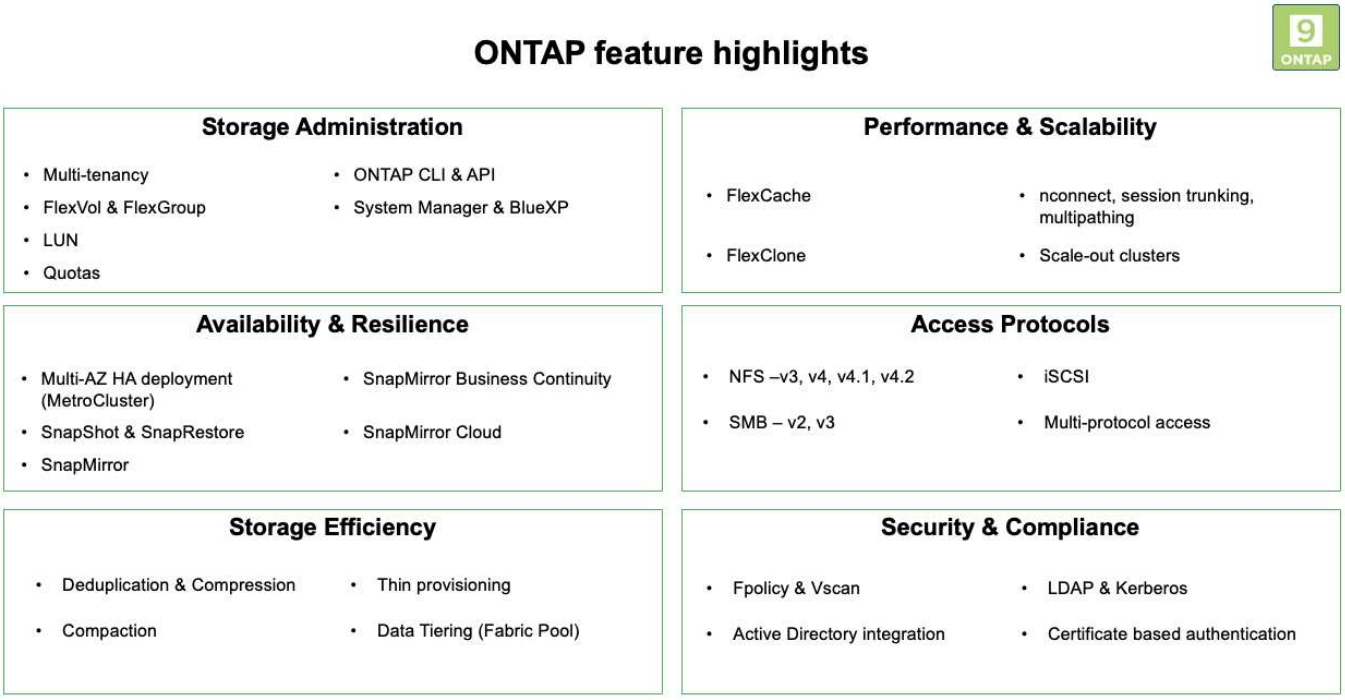
Présentation

NetApp constate une augmentation significative des clients qui modernisent leurs applications d'entreprise existantes et créent de nouvelles applications à l'aide de conteneurs et de plateformes d'orchestration basées sur Kubernetes. Nous avons adopté Red Hat OpenShift Container Platform comme bon nombre de nos clients.

Alors que les clients sont de plus en plus nombreux à adopter des conteneurs dans leur entreprise, NetApp est parfaitement positionné pour répondre aux besoins de stockage persistant de leurs applications avec état et aux besoins de gestion des données classiques, tels que la protection, la sécurité et la migration des données. Toutefois, ces besoins sont satisfaits à l'aide de stratégies, d'outils et de méthodes différents.

Les options de stockage basées sur NetApp ONTAP sont énumérées ci-dessous et offrent sécurité, protection des données, fiabilité et flexibilité pour les conteneurs et les déploiements Kubernetes.

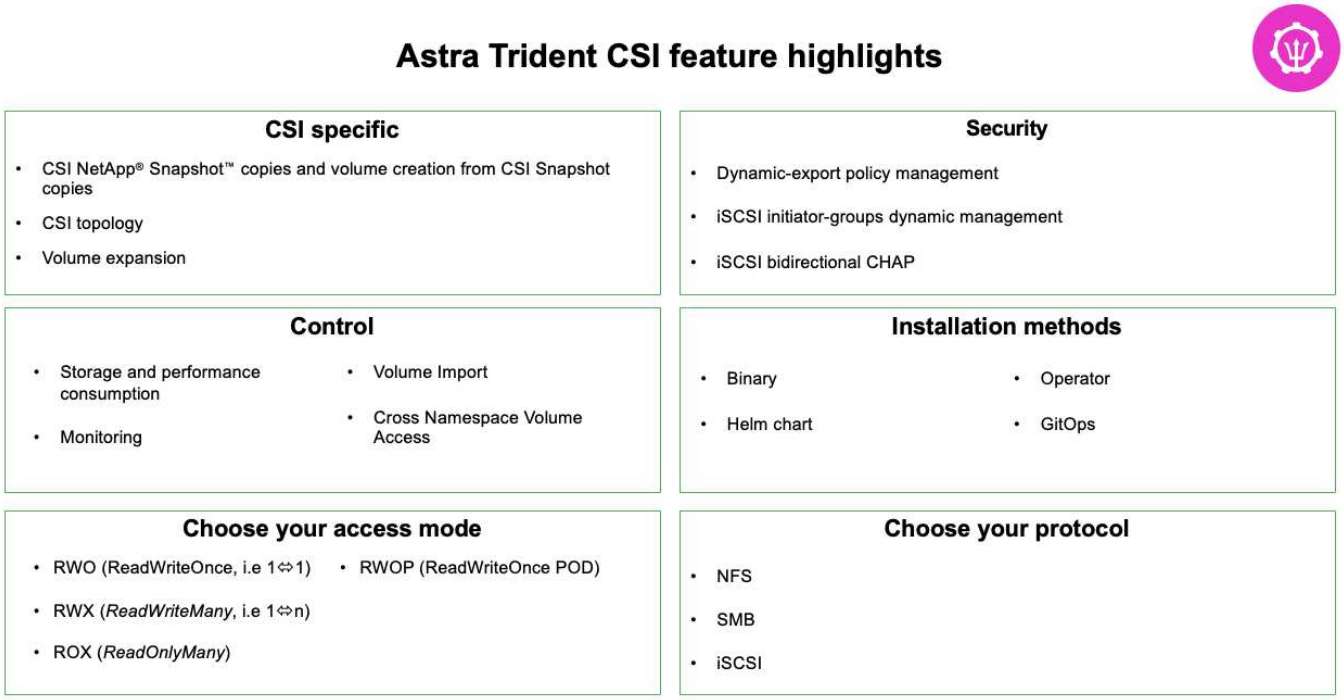
- Stockage autogéré sur site :
  - Stockage FAS (Fabric Attached Storage), baies FAS 100 % Flash (AFF), baies SAN ASA (All SAN Array) et ONTAP Select
- Stockage géré par un fournisseur sur site :
  - NetApp Keystone fournit une solution de stockage en tant que service (STaaS)
- Stockage autogéré dans le cloud :
  - NetApp Cloud volumes ONTAP (CVO) fournit un stockage autogéré dans les hyperscalers
- Stockage géré par un fournisseur dans le cloud :
  - Cloud Volumes Service pour Google Cloud (CVS), Azure NetApp Files (ANF) et Amazon FSX pour NetApp ONTAP offrent un stockage entièrement géré dans les hyperscalers



NetApp BlueXP vous permet de gérer l'ensemble de vos ressources de stockage et de données à partir d'un seul plan de contrôle/interface.

Vous pouvez utiliser BlueXP pour créer et gérer du stockage cloud (par exemple, Cloud Volumes ONTAP et Azure NetApp Files), déplacer, protéger et analyser les données, et contrôler de nombreux systèmes de stockage sur site et en périphérie.

NetApp Astra Trident est un orchestrateur de stockage conforme à CSI qui permet de consommer rapidement et facilement du stockage persistant grâce à plusieurs options de stockage NetApp mentionnées ci-dessus. Il s'agit d'un logiciel open source géré et pris en charge par NetApp.



Les workloads de conteneurs stratégiques requièrent bien plus que de simples volumes persistants. Leurs exigences de gestion des données requièrent également la protection et la migration des objets kubernetes applicatifs.

> Les données d'application incluent des objets kubernetes en plus des données utilisateur. Voici quelques exemples : - Objets kubernetes tels que les pods Specs, les PVC, les déploiements, les services - objets de configuration personnalisés tels que les cartes de configuration et les secrets - données persistantes telles que les copies Snapshot, les sauvegardes, les clones - ressources personnalisées telles que CRS et CRD

NetApp Astra Control, disponible en tant que logiciel entièrement géré et autogéré, assure l'orchestration pour une gestion robuste des données d'application. Reportez-vous à la "Documentation Astra" Pour en savoir plus sur la gamme de produits Astra.

Cette documentation de référence apporte la validation de la migration et de la protection des applications basées sur des conteneurs, déployées sur une plateforme de conteneurs RedHat OpenShift à l'aide de NetApp Astra Control Center. En outre, la solution fournit des détails généraux sur le déploiement et l'utilisation de Red Hat Advanced Cluster Management (ACM) pour la gestion des plateformes de conteneurs. Ce document détaille également les modalités d'intégration du stockage NetApp avec les plateformes de conteneurs Red Hat OpenShift à l'aide d'Astra Trident CSI Provisioner. ASTRA Control Center est déployé sur le cluster Hub et est utilisé pour gérer les applications de conteneur et leur cycle de vie de stockage persistant. Enfin, il fournit une solution de réplication, de basculement et de retour arrière pour les workloads de conteneurs sur des clusters Red Hat OpenShift gérés dans AWS (ROSA) utilisant Amazon FSX pour NetApp ONTAP (FSxN) en tant que stockage persistant.

Solution NetApp avec les workloads gérés de la plateforme de conteneurs Red Hat OpenShift sur AWS

Solution NetApp avec les workloads gérés de la plateforme de conteneurs Red Hat OpenShift sur AWS

Les clients peuvent être « nés dans le cloud » ou se trouver à un point de leur parcours

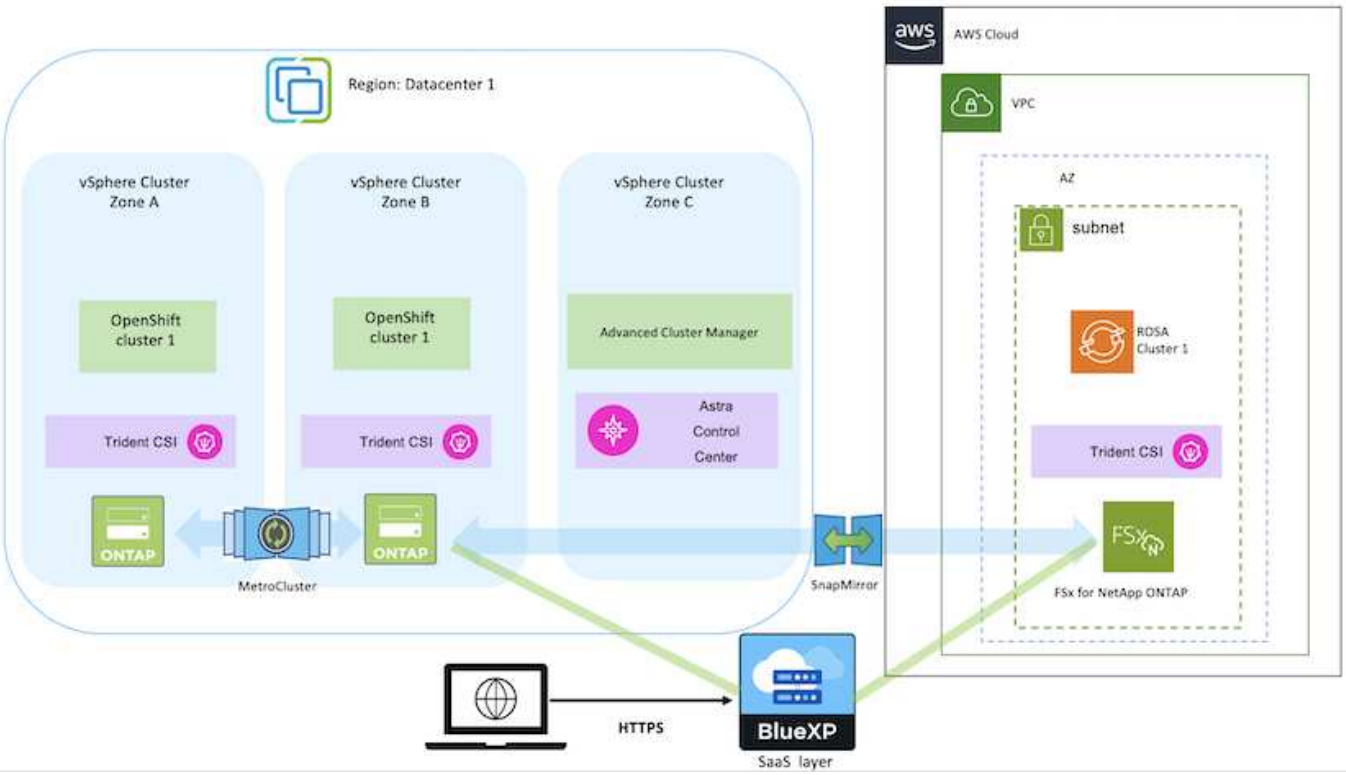
de modernisation lorsqu'ils sont prêts à déplacer des workloads spécifiques ou tous les workloads de leurs data centers vers le cloud. Ils peuvent choisir d'utiliser des conteneurs OpenShift gérés par un fournisseur et du stockage NetApp géré par un fournisseur dans le cloud pour exécuter leurs workloads. Ils doivent planifier et déployer les clusters de conteneurs Red Hat OpenShift (ROSA) gérés dans le cloud pour assurer la réussite de leur environnement de production pour leurs workloads de conteneurs. Dans le cloud AWS, ils peuvent également déployer FSX pour NetApp ONTAP pour répondre aux besoins en stockage.

FSX pour NetApp ONTAP assure la protection, la fiabilité et la flexibilité des données pour les déploiements de conteneurs dans AWS. ASTRA Trident sert de mécanisme de provisionnement de stockage dynamique pour consommer le stockage FSxN persistant pour les applications avec état des clients.

COMME ROSA peut être déployée en mode HA avec des nœuds de plan de contrôle répartis sur plusieurs zones de disponibilité, FSX ONTAP peut également être provisionné avec l'option multi-AZ qui assure la haute disponibilité et la protection contre les défaillances AZ.

L'accès à un système de fichiers Amazon FSX à partir de la zone de disponibilité préférée (AZ) du système de fichiers ne comporte aucun frais de transfert de données. Pour plus d'informations sur les prix, reportez-vous à la section "ici".

Solution de protection et de migration des données pour les workloads de conteneurs OpenShift

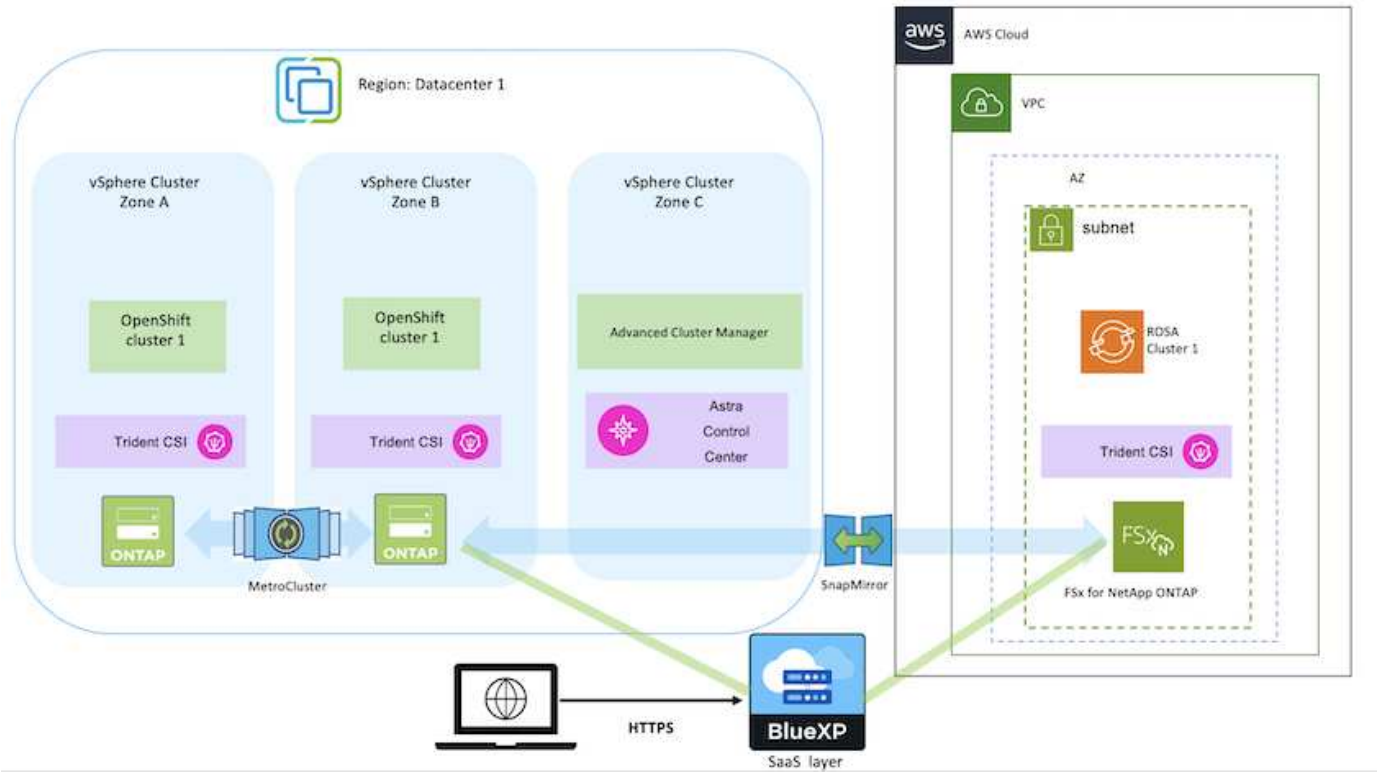


Déployez et configurez la plateforme de conteneurs Red Hat OpenShift gérée sur AWS

Cette section décrit un workflow général de configuration des clusters Red Hat OpenShift gérés sur AWS(ROSA). Il présente l'utilisation de FSX for NetApp ONTAP (FSxN) géré

en tant que back-end de stockage par Astra Trident pour fournir des volumes persistants. Vous trouverez des informations détaillées sur le déploiement de FSxN sur AWS à l'aide de BlueXP. Vous y trouverez également des informations détaillées sur l'utilisation de BlueXP et d'OpenShift GitOps (Argo CD) pour exécuter les activités de protection et de migration des données pour les applications avec état sur les clusters ROSA.

Voici un diagramme illustrant les clusters ROSA déployés sur AWS et utilisant FSxN comme stockage back-end.



Cette solution a été vérifiée en utilisant deux clusters ROSA dans deux VPC dans AWS. Chaque cluster ROSA a été intégré à FSxN à l'aide d'Astra Trident. IL existe plusieurs façons de déployer les clusters ROSA et FSxN dans AWS. Cette description de haut niveau de la configuration fournit des liens de documentation pour la méthode spécifique qui a été utilisée. Vous pouvez vous référer aux autres méthodes dans les liens pertinents fournis dans le "ressources".

Le processus de configuration peut être divisé en plusieurs étapes :

Installer les clusters ROSA

- Créez deux VPC et configurez la connectivité de peering VPC entre les VPC.
- Reportez-vous à "ici" Pour obtenir des instructions sur l'installation des clusters ROSA.

Installez FSxN

- Installez FSxN sur les VPC de BlueXP. Reportez-vous à "ici" Pour créer un compte BlueXP et démarrer. Reportez-vous à "ici" Pour l'installation de FSxN. Reportez-vous à "ici" Pour créer un connecteur dans AWS pour gérer le FSxN.
- Déploiement de FSxN à l'aide d'AWS Reportez-vous à "ici" Déploiement via la console AWS

Installation de Trident sur les clusters ROSA (à l'aide du graphique Helm)

- Utilisez le tableau Helm pour installer Trident sur les clusters ROSA. url du graphique Helm : https://netapp.github.io/trident-helm-chart

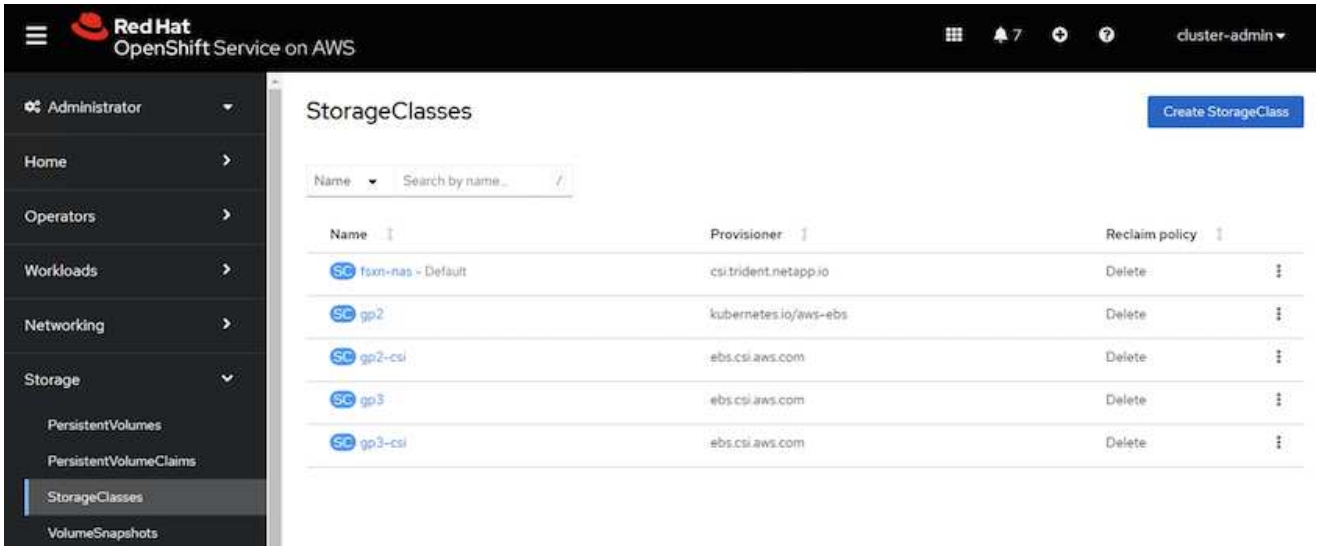
Intégration de FSxN avec Astra Trident pour les clusters ROSA

OpenShift GitOps peut être utilisé pour déployer Astra Trident CSI sur tous les clusters gérés lors de leur enregistrement sur ArgoCD à l'aide d'ApplicationSet.

```
apiVersion: argoproj.io/v1alpha1
kind: ApplicationSet
metadata:
  name: trident-operator
spec:
  generators:
  - clusters: {}
    # selector:
    #   matchLabels:
    #     tridentversion: '23.04.0'
  template:
    metadata:
      name: '{{nameNormalized}}-trident'
    spec:
      destination:
        namespace: trident
        server: '{{server}}'
      source:
        repoURL: 'https://netapp.github.io/trident-helm-chart'
        targetRevision: 23.04.0
        chart: trident-operator
      project: default
      syncPolicy:
        syncOptions:
          - CreateNamespace=true
```

Création de classes de stockage et de back-end à l'aide de Trident (pour FSxN)

- Reportez-vous à "ici" pour plus d'informations sur la création de systèmes back-end et de classes de stockage.
- Créez la classe de stockage créée pour FsxN avec Trident CSI par défaut depuis la console OpenShift. Voir la capture d'écran ci-dessous :



Déployer une application à l'aide d'OpenShift GitOps (Argo CD)

- Installez l'opérateur OpenShift GitOps sur le cluster. Reportez-vous aux instructions "ici".
- Configurez une nouvelle instance Argo CD pour le cluster. Reportez-vous aux instructions "ici".

Ouvrez la console du CD Argo et déployez une application. Par exemple, vous pouvez déployer une application Jenkins à l'aide du CD Argo avec Helm Chart. Lors de la création de l'application, les détails suivants ont été fournis : projet : cluster par défaut : https://kubernetes.default.svcEspace de noms : Jenkins l'url du graphique Helm : https://charts.bitnami.com/bitnami

Paramètres Helm : global.storageClass : fsxn-nas

Protection des données

Cette page présente les options de protection des données pour les clusters Red Hat OpenShift sur AWS (ROSA) gérés à l'aide d'Astra Control Service. ASTRA Control Service (ACS) est une interface utilisateur graphique simple d'utilisation qui vous permet d'ajouter des clusters, de définir des applications qui s'exécutent sur eux et d'effectuer des activités de gestion des données intégrant la cohérence applicative. Les fonctions ACS sont également accessibles via une API qui permet l'automatisation des flux de travail.

NetApp Astra Trident est le moteur d'Astra Control (ACS ou ACC). ASTRA Trident intègre plusieurs types de clusters Kubernetes tels que Red Hat OpenShift, EKS, AKS, SUSE Rancher, Anthos, etc. avec plusieurs versions de stockage NetApp ONTAP telles que FAS/AFF, ONTAP Select, CVO, Google Cloud Volumes Service, Azure NetApp Files et Amazon FSX pour NetApp ONTAP.

Cette section fournit des détails sur les options de protection des données suivantes à l'aide d'ACS :

- Vidéo montrant la sauvegarde et la restauration d'une application ROSA s'exécutant dans une région et la restauration dans une autre région.
- Vidéo présentant Snapshot et la restauration d'une application ROSA.
- Détails détaillés de l'installation d'un cluster ROSA, Amazon FSX pour NetApp ONTAP, à l'aide d'NetApp Astra Trident pour l'intégration au back-end de stockage, installation d'une application postgresql sur un cluster ROSA, utilisation d'ACS pour créer un snapshot de l'application et restaurer son application.
- Un blog montrant les détails pas à pas de la création et de la restauration à partir d'un snapshot pour une application mysql sur un cluster ROSA avec FSX pour ONTAP à l'aide d'ACS.

Sauvegarde/Restauration à partir de la sauvegarde

La vidéo suivante montre la sauvegarde d'une application ROSA s'exécutant dans une région et la restauration dans une autre région.

FSX NetApp ONTAP pour Red Hat OpenShift Service sur AWS

Snapshot/Restaurer à partir d'un snapshot

La vidéo suivante montre la prise d'un instantané d'une application ROSA et la restauration à partir de l'instantané après.

Snapshot/Restore pour les applications sur les clusters Red Hat OpenShift Service sur AWS (ROSA) avec le stockage Amazon FSX pour NetApp ONTAP

Blog

- "Utilisation d'Astra Control Service pour la gestion des données des applications sur des clusters ROSA avec le stockage Amazon FSX"

Détails détaillés étape par étape pour créer un snapshot et le restaurer à partir de celui-ci

Configuration des prérequis

- "Compte AWS"
- "Compte Red Hat OpenShift"
- Utilisateur IAM avec "autorisations appropriées" Pour créer et accéder au cluster ROSA
- "CLI AWS"
- "CLI ROSA"
- "Interface de ligne de commande OpenShift"(oc)
- VPC avec sous-réseaux et passerelles et routes appropriées
- "ROSA Cluster installée" Dans le VPC
- "Amazon FSX pour NetApp ONTAP" Créées dans le même VPC
- Accès au cluster ROSA depuis "OpenShift Hybrid Cloud Console"

Étapes suivantes

1. Créer un utilisateur admin et se connecter au cluster

2. Créez un fichier kubeconfig pour le cluster.
3. Installer Astra Trident sur le cluster.
4. Créez une configuration back-end, une classe de stockage et une classe Snapshot à l'aide du mécanisme de provisionnement Trident CSI.
5. Déployer une application postgresql sur le cluster.
6. Créez une base de données et ajoutez un enregistrement.
7. Ajoutez le cluster dans ACS.
8. Définissez l'application dans ACS.
9. Créez un instantané à l'aide d'ACS.
10. Supprimez la base de données dans l'application postgresql.
11. Restauration à partir d'un snapshot à l'aide d'ACS.
12. Vérifiez que votre application a été restaurée à partir de l'instantané.

1. Créer un utilisateur admin et se connecter au cluster

Accédez au cluster ROSA en créant un utilisateur admin avec la commande suivante : (vous devez créer un utilisateur admin uniquement si vous n'en avez pas créé un au moment de l'installation)

```
rosa create admin --cluster=<cluster-name>
```

La commande fournit une sortie qui ressemble à ce qui suit. Connectez-vous au cluster à l'aide de `oc login` commande fournie dans la sortie.

```
W: It is recommended to add an identity provider to login to this cluster.
See 'rosa create idp --help' for more information.
I: Admin account has been added to cluster 'my-rosa-cluster'. It may take up
to a minute for the account to become active.
I: To login, run the following command:
oc login https://api.my-rosa-cluster.abcd.p1.openshiftapps.com:6443 \
--username cluster-admin \
--password FWGYL-2mkJI-00000-00000
```

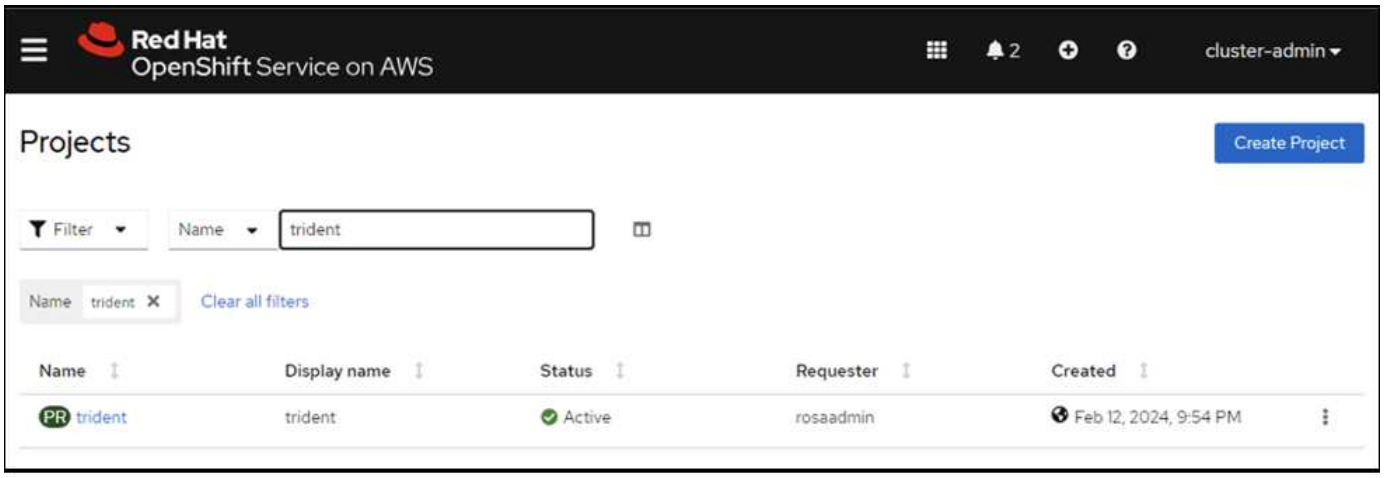
Vous pouvez également vous connecter au cluster à l'aide d'un jeton. Si vous avez déjà créé un administrateur au moment de la création du cluster, vous pouvez vous connecter au cluster depuis la console Red Hat OpenShift Hybrid Cloud à l'aide des informations d'identification de l'administrateur. Ensuite, en cliquant sur le coin supérieur droit où il affiche le nom de l'utilisateur connecté, vous pouvez obtenir le `oc login` commande (jeton de connexion) pour la ligne de commande.

2. Créez un fichier kubeconfig pour le cluster

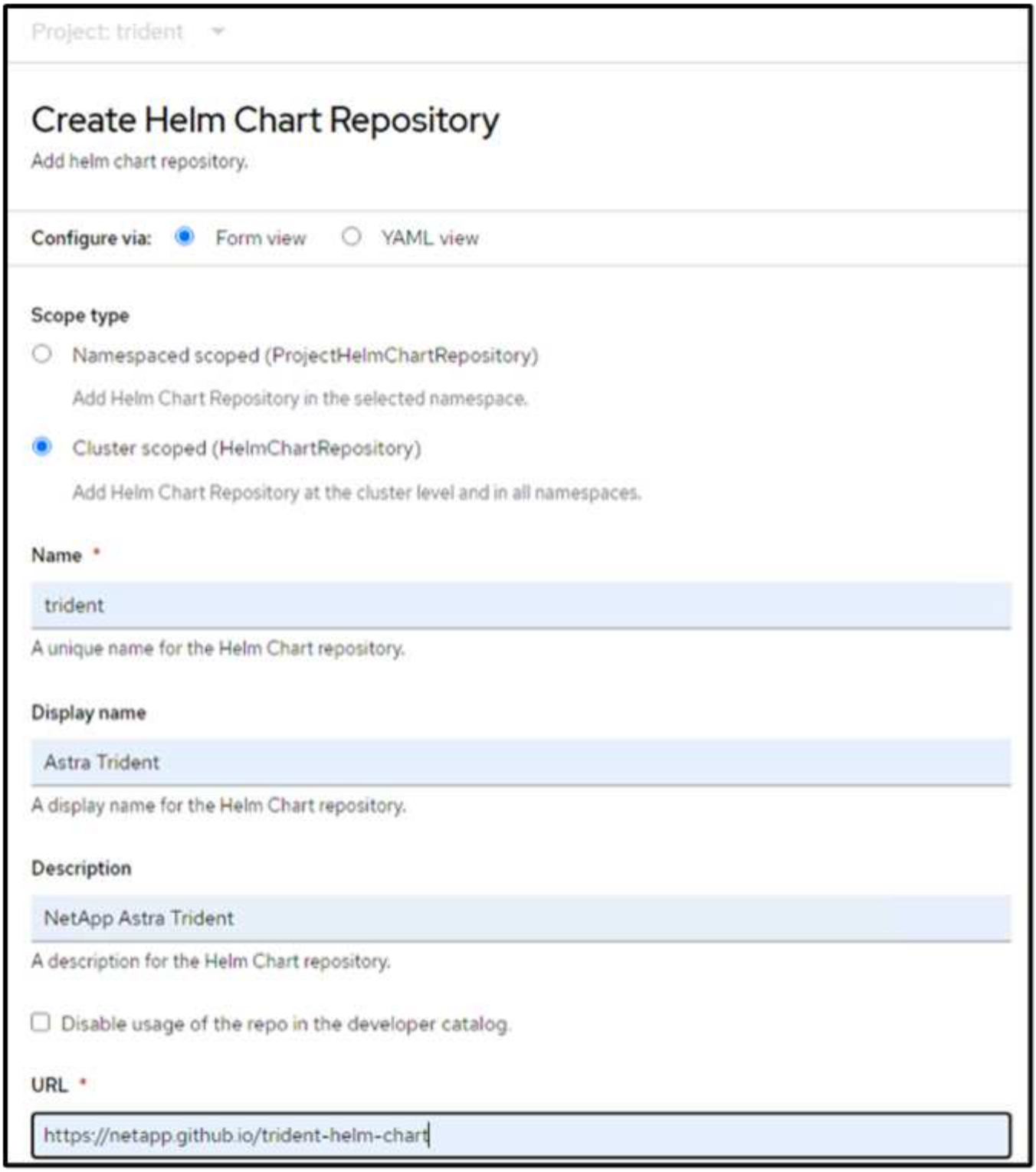
Suivre les procédures "ici" Pour créer un fichier kubeconfig pour le cluster ROSA. Ce fichier kubeconfig sera utilisé plus tard lorsque vous ajoutez le cluster dans ACS.

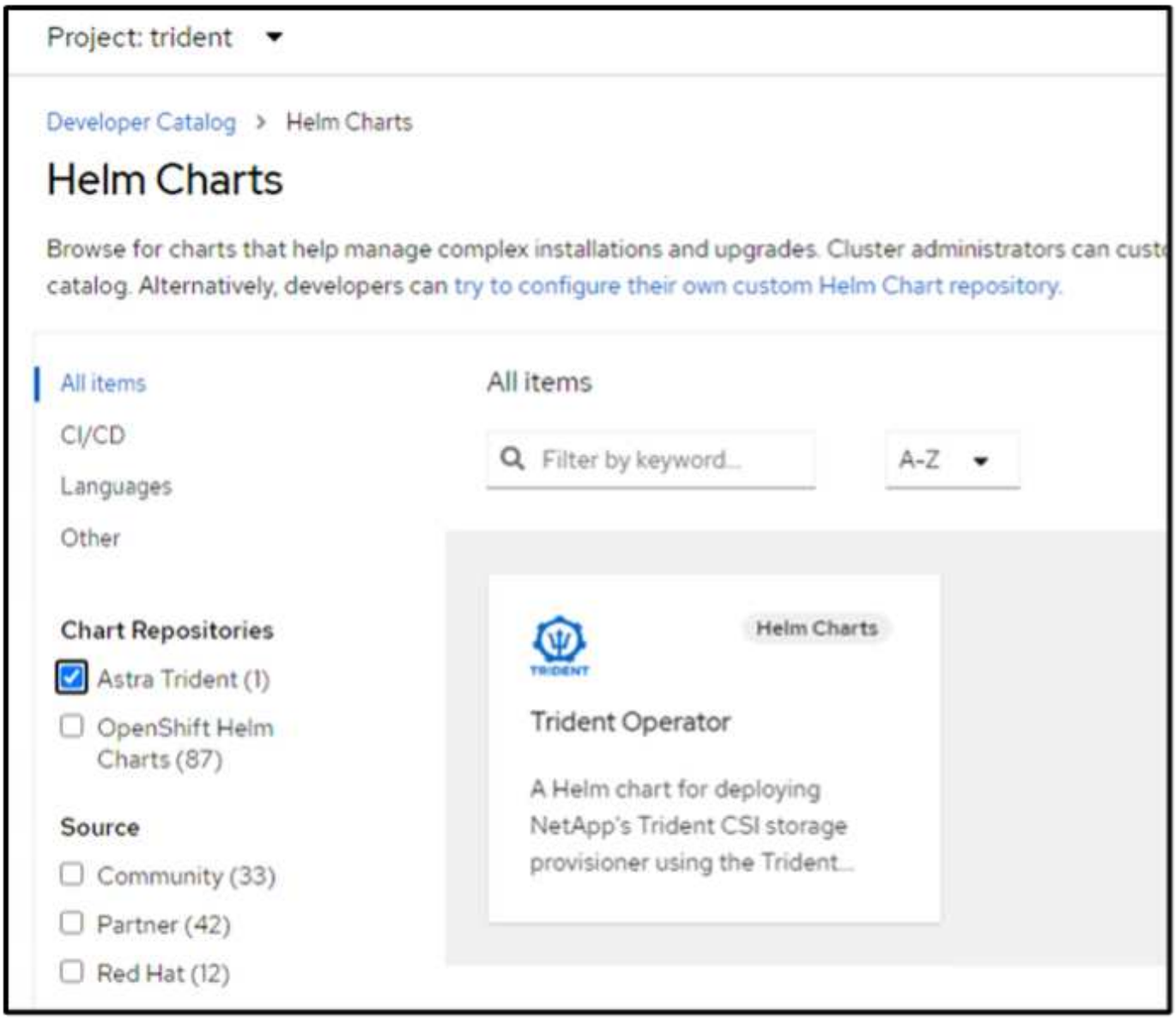
3. Installer Astra Trident sur le cluster

Installer Astra Trident (dernière version) sur le cluster ROSA. Pour ce faire, vous pouvez suivre l'une des procédures données "ici". Pour installer Trident à l'aide de Helm à partir de la console du cluster, commencez par créer un projet appelé Trident.

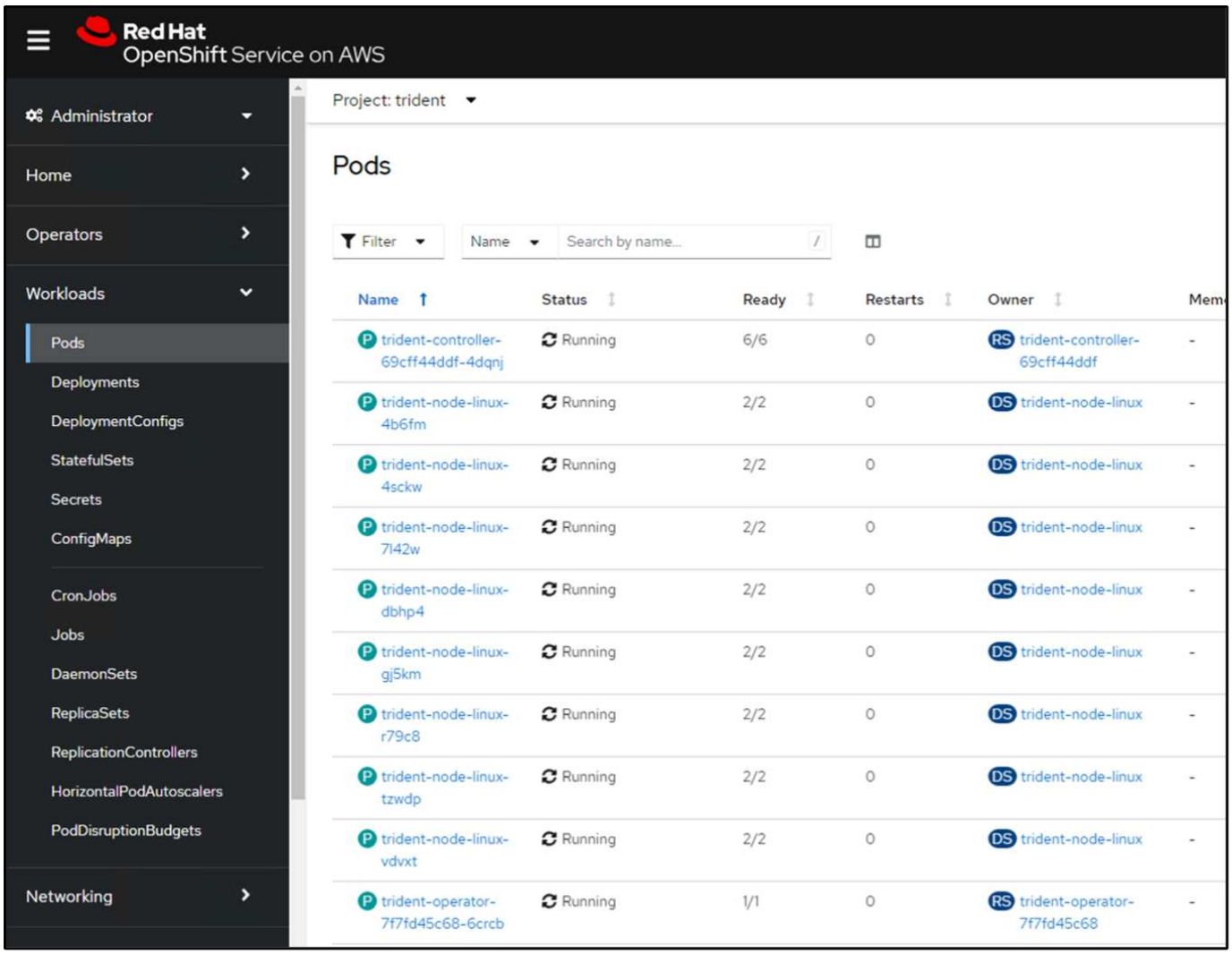


Ensuite, dans la vue Développeur, créez un référentiel de graphiques Helm. Pour le champ URL, utilisez `'https://netapp.github.io/trident-helm-chart'`. Créez ensuite une version de Helm pour l'opérateur Trident.


Project: trident
Create Helm Chart Repository
Add helm chart repository.
Configure via:
Form view
YAML view
Scope type
Namespaced scoped (ProjectHelmChartRepository)
Add Helm Chart Repository in the selected namespace.
Cluster scoped (HelmChartRepository)
Add Helm Chart Repository at the cluster level and in all namespaces.
Name *
trident
A unique name for the Helm Chart repository.
Display name
Astra Trident
A display name for the Helm Chart repository.
Description
NetApp Astra Trident
A description for the Helm Chart repository.
Disable usage of the repo in the developer catalog.
URL *
https://netapp.github.io/trident-helm-chart



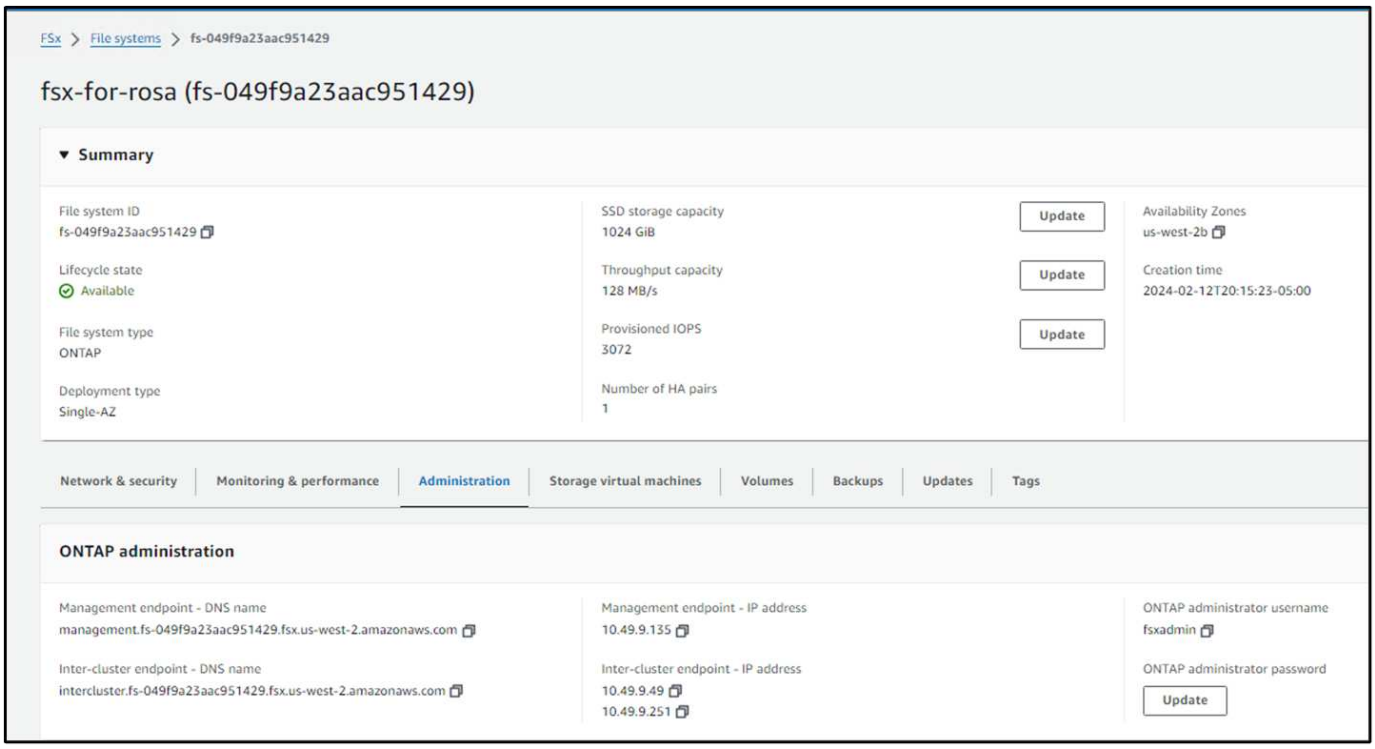
Vérifiez que tous les pods trident sont en cours d'exécution en revenant à la vue de l'administrateur de la console et en sélectionnant les pods dans le projet trident.



4. Créez une configuration backend, de classe de stockage et de classe de snapshots à l'aide du mécanisme de provisionnement Trident CSI

Utilisez les fichiers yaml illustrés ci-dessous pour créer un objet back-end trident, un objet classe de stockage et l'objet Volumesnapshot. Assurez-vous de fournir les informations d'identification de votre système de fichiers Amazon FSX for NetApp ONTAP que vous avez créé, la LIF de gestion et le nom de vServer de votre système de fichiers dans la configuration yaml pour le back-end. Pour obtenir ces informations, accédez à la console AWS pour Amazon FSX et sélectionnez le système de fichiers, accédez à l'onglet Administration. Cliquez également sur mettre à jour pour définir le mot de passe du `fsxadmin` utilisateur.

Vous pouvez utiliser la ligne de commande pour créer les objets ou les créer avec les fichiers yaml à partir de la console de cloud hybride.



Configuration back-end Trident

```
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-ontap-nas-secret
type: Opaque
stringData:
  username: fsxadmin
  password: <password>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: ontap-nas
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: <management lif>
  backendName: ontap-nas
  svm: fsx
  credentials:
    name: backend-tbc-ontap-nas-secret
```

Classe de stockage

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
  media: "ssd"
  provisioningType: "thin"
  snapshots: "true"
allowVolumeExpansion: true
```

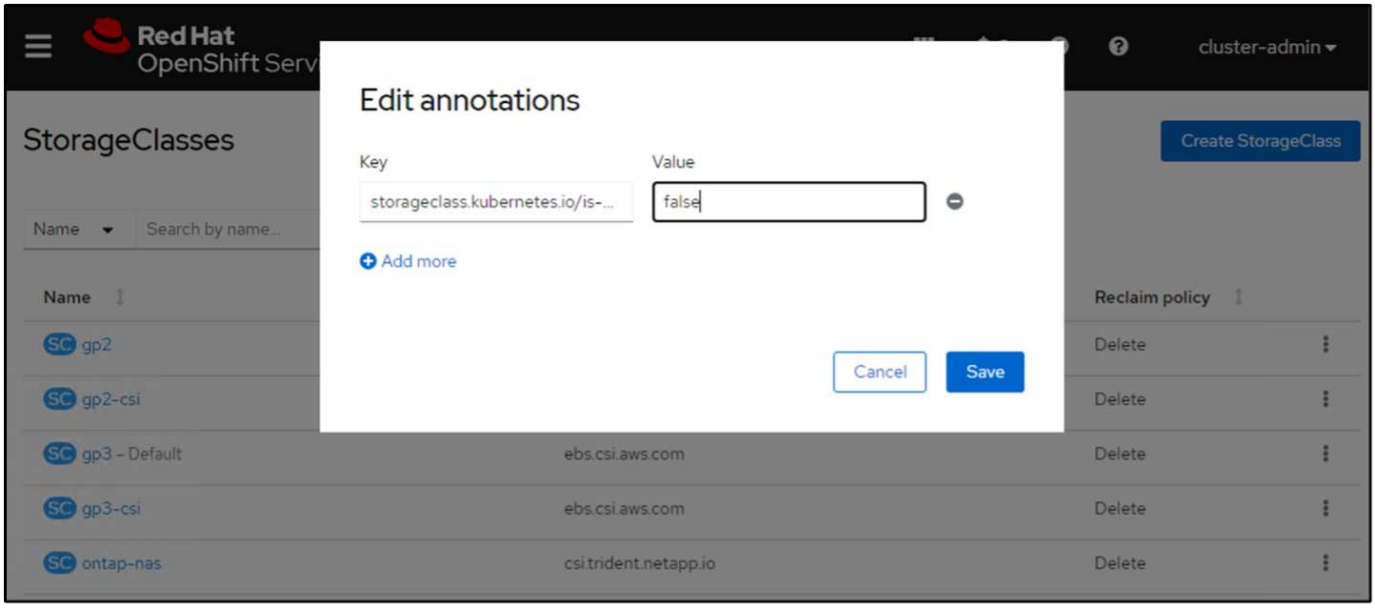
classe d'instantanés

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshotClass
metadata:
  name: trident-snapshotclass
driver: csi.trident.netapp.io
deletionPolicy: Delete
```

Vérifiez que le backend, la classe de stockage et les objets trident-snapshotclass sont créés à l'aide des commandes indiquées ci-dessous.

```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get tbc -n trident
NAME        BACKEND NAME   BACKEND UUID                           PHASE   STATUS
ontap-nas   ontap-nas      8a5e4583-2dac-46bb-b01e-fa7c3816f121   Bound   Success
[ec2-user@ip-10-49-11-132 storage]$ kubectl get sc
NAME            PROVISIONER             RECLAIMPOLICY   VOLUMEBINDINGMODE      ALLOWVOLUMEEXPANSION   AGE
gp2             kubernetes.io/aws-ebs   Delete          WaitForFirstConsumer   true                   3h23m
gp2-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
gp3 (default)   ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h23m
gp3-csi         ebs.csi.aws.com         Delete          WaitForFirstConsumer   true                   3h19m
ontap-nas       csi.trident.netapp.io   Delete          Immediate              true                   141m
[ec2-user@ip-10-49-11-132 storage]$ kubectl get Volumesnapshotclass
NAME                    DRIVER                  DELETIONPOLICY   AGE
csi-aws-vsc             ebs.csi.aws.com         Delete           3h19m
trident-snapshotclass   csi.trident.netapp.io   Delete           6m56s
[ec2-user@ip-10-49-11-132 storage]$
```

Vous devez à présent modifier de façon importante : définir ontap-nas comme classe de stockage par défaut au lieu de gp3 de sorte que l'application postgresql que vous déployez ultérieurement puisse utiliser la classe de stockage par défaut. Dans la console OpenShift de votre cluster, sous stockage, sélectionnez classes de stockage. Editez l'annotation de la classe par défaut actuelle à false et ajoutez l'annotation storageclass.kubernetes.io/is-default-class set à true pour la classe de stockage ontap-nas.



5. Déployer une application postgresql sur le cluster

Vous pouvez déployer l'application à partir de la ligne de commande comme suit :

```
helm install postgresql bitnami/postgresql -n postgresql --create-namespace
```

```
[ec2-user@ip-10-49-11-132 astra]$ helm install postgresql bitnami/postgresql -n postgresql --create-namespace
NAME: postgresql
LAST DEPLOYED: Tue Feb 13 14:46:16 2024
NAMESPACE: postgresql
STATUS: deployed
REVISION: 1
TEST SUITE: None
NOTES:
CHART NAME: postgresql
CHART VERSION: 14.0.4
APP VERSION: 16.2.0

** Please be patient while the chart is being deployed **

PostgreSQL can be accessed via port 5432 on the following DNS names from within your cluster:

    postgresql.postgresql.svc.cluster.local - Read/Write connection

To get the password for "postgres" run:

    export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="{.data.postgres-password}" | base64 -d)

To connect to your database run the following command:

    kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PG
PASSWORD=$POSTGRES_PASSWORD" \
      --command -- psql --host postgresql -U postgres -d postgres -p 5432

    > NOTE: If you access the container using bash, make sure that you execute "/opt/bitnami/scripts/postgresql/entrypoint.sh /bin/bash" in order to avoid
the error "psql: local user with ID 1001} does not exist"

To connect to your database from outside the cluster execute the following commands:

    kubectl port-forward --namespace postgresql svc/postgresql 5432:5432 &
    PGPASSWORD="$POSTGRES_PASSWORD" psql --host 127.0.0.1 -U postgres -d postgres -p 5432

WARNING: The configured password will be ignored on new installation in case when previous PostgreSQL release was deleted through the helm command. In that
 case, old PVC will have an old password, and setting it through helm won't take effect. Deleting persistent volumes (PVs) will solve the issue.
[ec2-user@ip-10-49-11-132 astra]$
```

Si vous ne voyez pas les modules d'application s'exécuter, une erreur peut survenir en raison de contraintes de contexte de sécurité.

```
[ec2-user@ip-10-49-11-132 astra]$ kubectl get all -n postgresql
NAME                     TYPE        CLUSTER-IP      EXTERNAL-IP   PORT(S)    AGE
service/postgresql       ClusterIP   172.30.245.50   <none>        5432/TCP   12m
service/postgresql-hl    ClusterIP   None            <none>        5432/TCP   12m

NAME                          READY   AGE
statefulset.apps/postgresql   0/1     12m
[ec2-user@ip-10-49-11-132 astra]$ kubectl get events -n postgresql
LAST SEEN   TYPE      REASON              OBJECT                                  MESSAGE
2m39s       Normal    WaitForFirstConsumer   persistentvolumeclaim/data-postgresql-0   waiting for first consumer to be created before binding
12m         Normal    SuccessfulCreate       statefulset/postgresql                  create Claim data-postgresql-0 Pod postgresql-0 in StatefulSet postg
resql success
107s        Warning   FailedCreate           statefulset/postgresql                  create Pod postgresql-0 in StatefulSet postgresql failed error: pods
 "postgresql-0" is forbidden: unable to validate against any security context constraint: [provider "trident-controller": Forbidden: not usable by user or
serviceaccount, provider "anyuid": Forbidden: not usable by user or serviceaccount, provider restricted-v2: .spec.securityContext.fsGroup: Invalid value: [
]int64{1001}: 1001 is not an allowed group, provider restricted-v2: .containers[0].runAsUser: Invalid value: 1001: must be in the ranges: [1001010000, 1001
019999], provider "restricted": Forbidden: not usable by user or serviceaccount, provider "nonroot-v2": Forbidden: not usable by user or serviceaccount, pr
ovider "nonroot": Forbidden: not usable by user or serviceaccount, provider "pcap-dedicated-admins": Forbidden: not usable by user or serviceaccount, provi
der "hostmount-anyuid": Forbidden: not usable by user or serviceaccount, provider "machine-api-termination-handler": Forbidden: not usable by user or servi
ceaccount, provider "hostnetwork-v2": Forbidden: not usable by user or serviceaccount, provider "hostnetwork": Forbidden: not usable by user or serviceacco
unt, provider "hostaccess": Forbidden: not usable by user or serviceaccount, provider "splunkforwarder": Forbidden: not usable by user or serviceaccount, p
rovider "trident-node-linux": Forbidden: not usable by user or serviceaccount, provider "node-exporter": Forbidden: not usable by user or serviceaccount, p
rovider "privileged": Forbidden: not usable by user or serviceaccount]
[ec2-user@ip-10-49-11-132 astra]$
```

Corrigez l'erreur en modifiant le `runAsUser` et `fsGroup` champs dans `statefuleset.apps/postgresql` objet avec l'uid qui se trouve dans la sortie du `oc get project` comme indiqué ci-dessous.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get project postgresql -o yaml | grep uid-range
    openshift.io/sa.scc.uid-range: 1001010000/10000
[ec2-user@ip-10-49-11-132 astra]$ oc edit -n postgresql statefulset.apps/postgresql
statefulset.apps/postgresql edited
[ec2-user@ip-10-49-11-132 astra]$
```

L'application postgresql doit être en cours d'exécution et utiliser des volumes persistants pris en charge par le stockage Amazon FSX pour NetApp ONTAP.

```
[ec2-user@ip-10-49-11-132 astra]$ oc get pods -n postgresql
NAME           READY   STATUS    RESTARTS   AGE
postgresql-0   1/1     Running   0          2m46s
[ec2-user@ip-10-49-11-132 astra]$
```

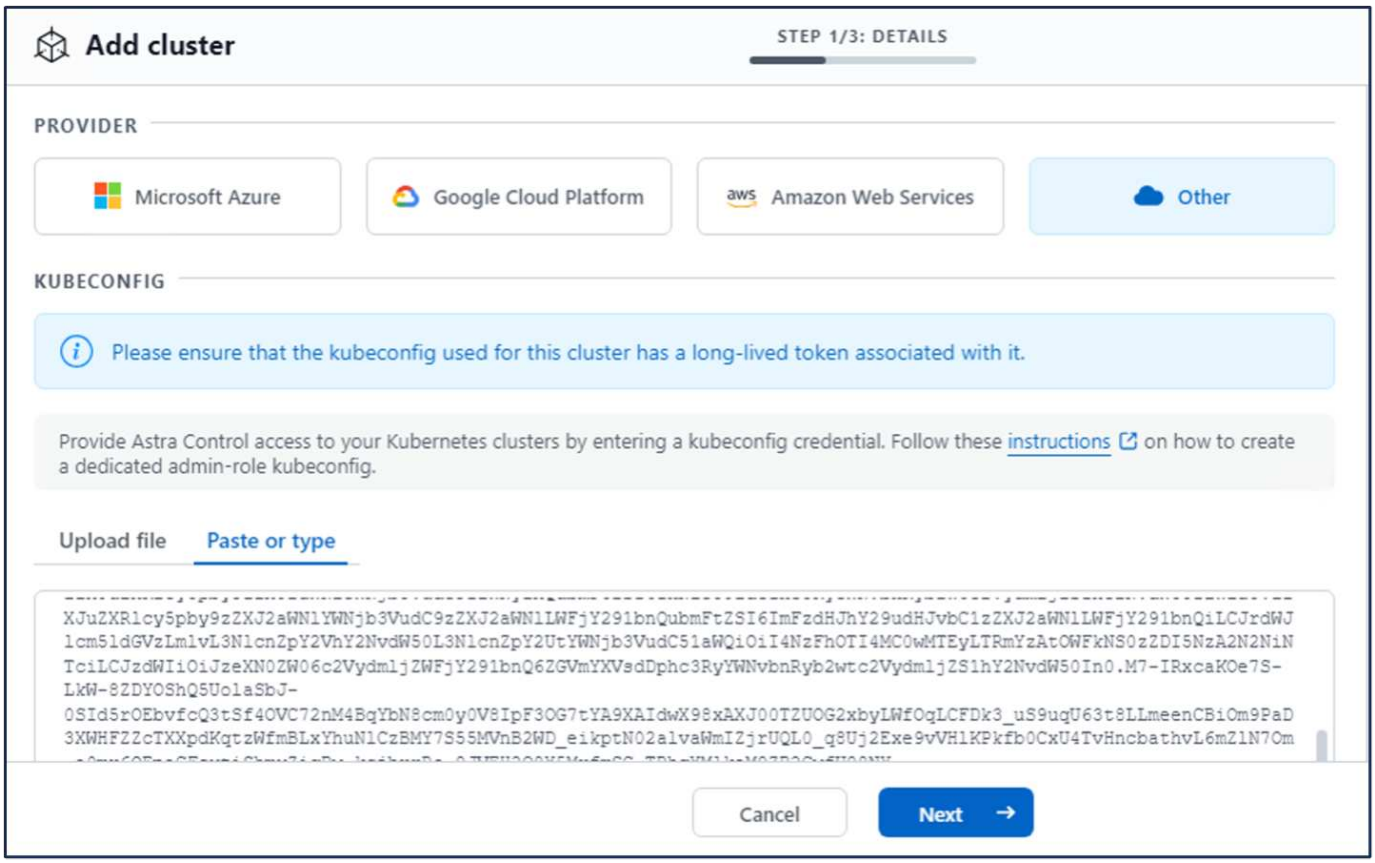
```
[ec2-user@ip-10-49-11-132 storage]$ kubectl get pvc -n postgresql
NAME               STATUS   VOLUME                                     CAPACITY   ACCESS MODES   STORAGECLASS   AGE
data-postgresql-0  Bound    pvc-dd09524a-de75-4825-9424-03a9b91195ca   8Gi        RWO            ontap-nas      4m2s
[ec2-user@ip-10-49-11-132 storage]$
```

6. Créer une base de données et ajouter un enregistrement

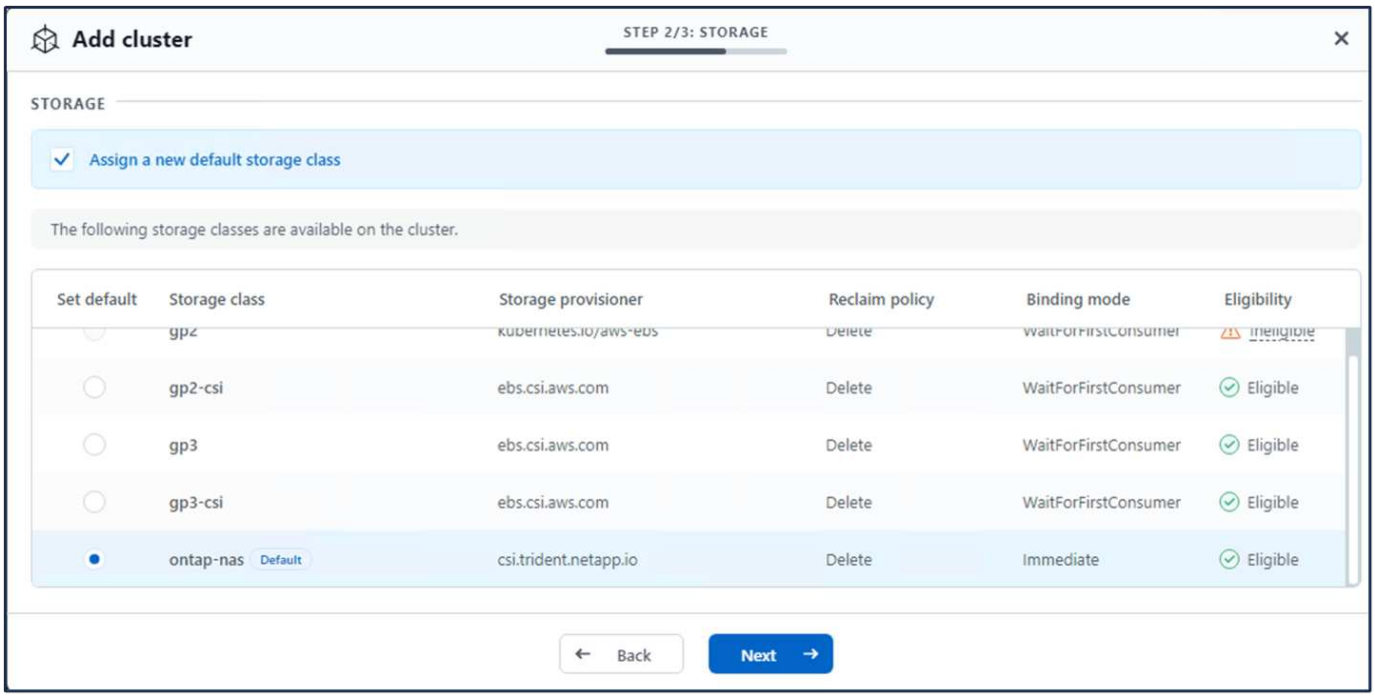
```
[ec2-user@ip-10-49-11-132 astra]$ export POSTGRES_PASSWORD=$(kubectl get secret --namespace postgresql postgresql -o jsonpath="
{.data.postgres-password}" | base64 -d)
[ec2-user@ip-10-49-11-132 astra]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image
docker.io/bitnami/postgresql:16.2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" \
> --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must se
t securityContext.allowPrivilegeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityCo
ntext.capabilities.drop=["ALL"]), runAsNonRoot != true (pod or container "postgresql-client" must set securityContext.runAsNonR
oot=true), seccompProfile (pod or container "postgresql-client" must set securityContext.seccompProfile.type to "RuntimeDefault
" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# CREATE DATABASE erp;
CREATE DATABASE
postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# CREATE TABLE PERSONS(ID INT PRIMARY KEY NOT NULL, FIRSTNAME TEXT NOT NULL, LASTNAME TEXT NOT NULL);
CREATE TABLE
erp=# INSERT INTO PERSONS VALUES(1,'John','Doe');
INSERT 0 1
erp=# \dt
          List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * FROM persons;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

7. Ajouter le cluster dans ACS

Connectez-vous à ACS. Sélectionnez cluster et cliquez sur Ajouter. Sélectionnez autre et téléchargez ou collez le fichier kubecconfig.



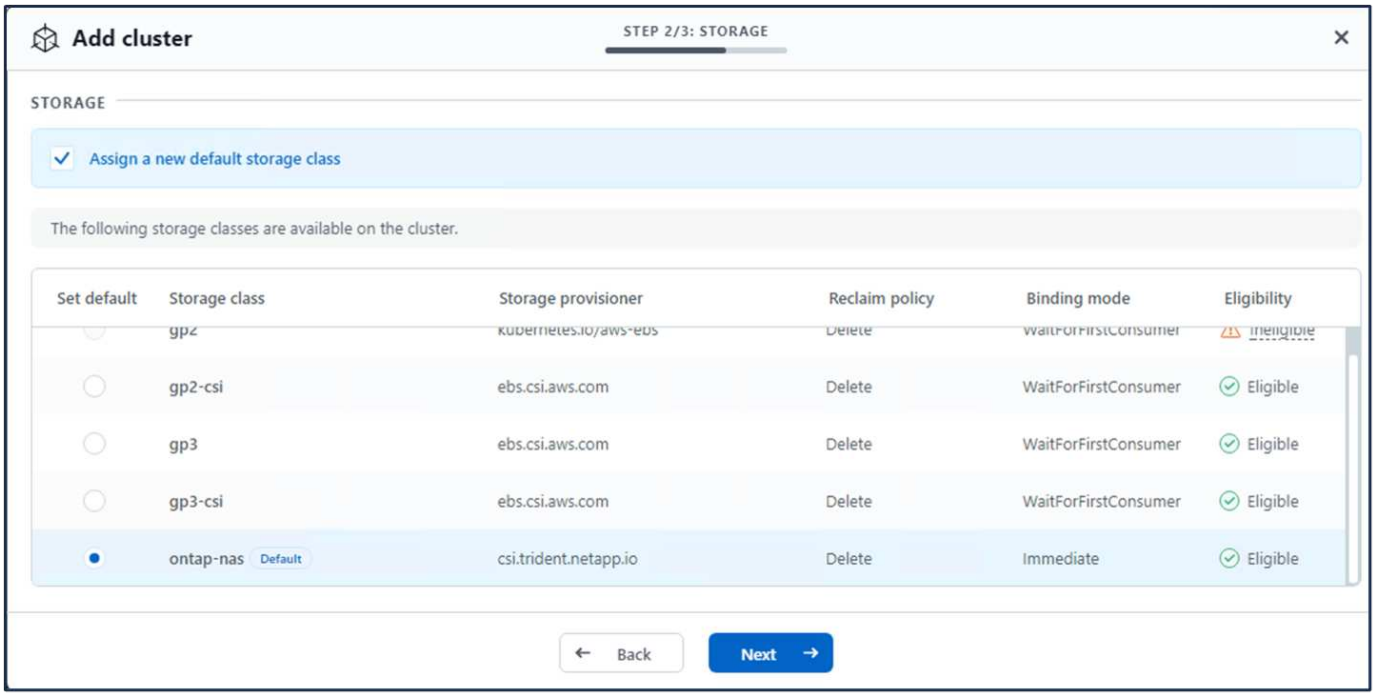
Cliquez sur **Suivant** et sélectionnez ontap-nas comme classe de stockage par défaut pour ACS. Cliquez sur **Suivant**, consultez les détails et **Ajouter** le cluster.



8. Définir l'application dans ACS

Définissez l'application postgresql dans ACS. Sur la page d'accueil, sélectionnez **applications**, **définir** et entrez les détails appropriés. Cliquez sur **Suivant** à plusieurs reprises, passez en revue les détails et cliquez

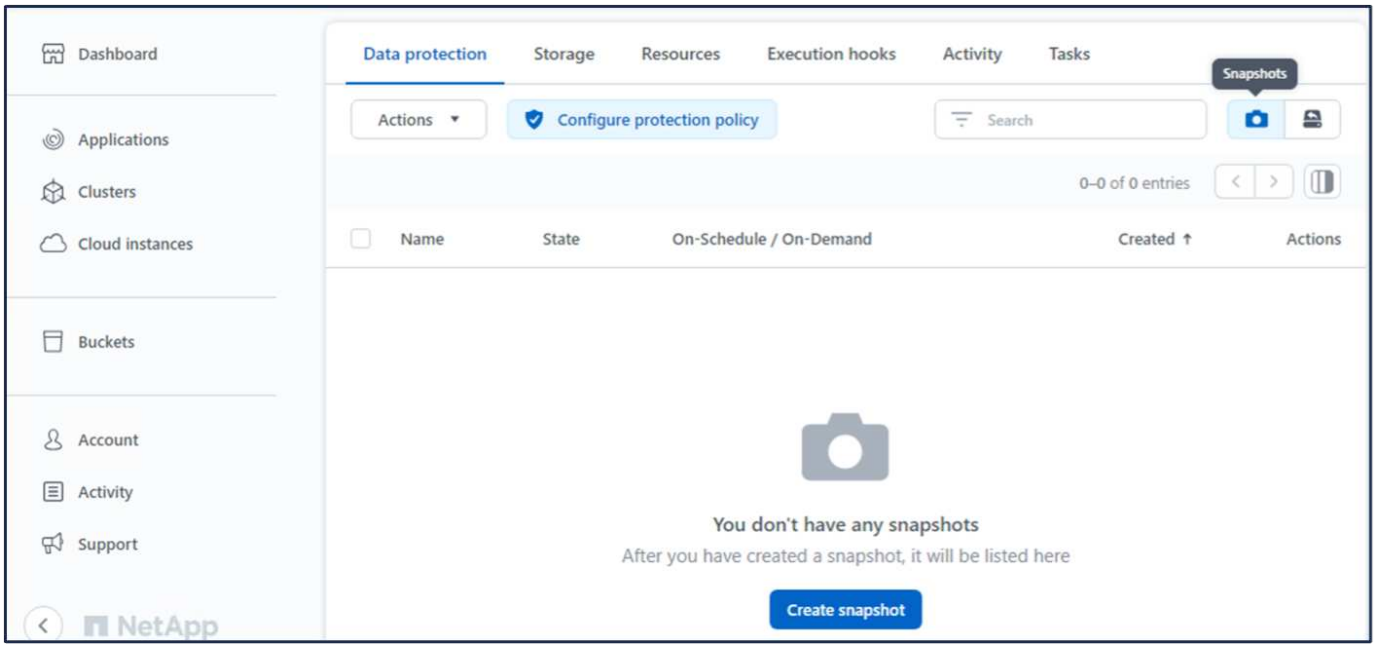
sur **définir**. L'application est ajoutée à ACS.

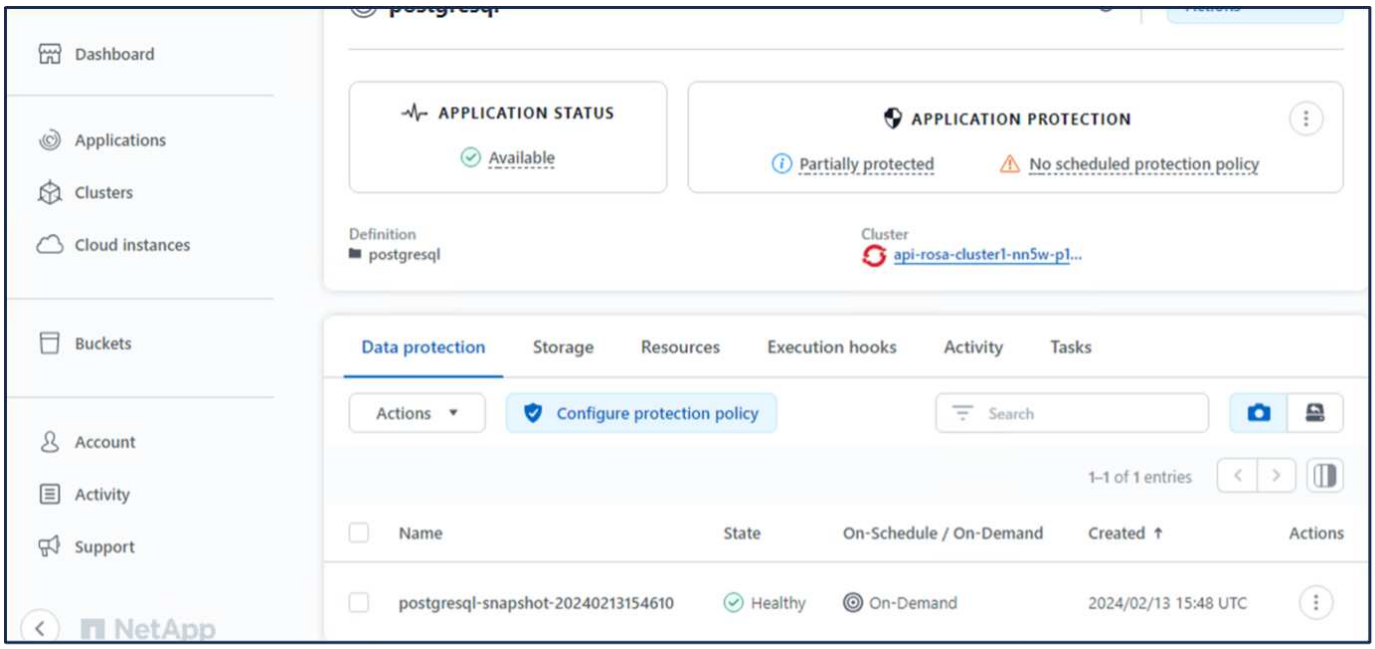


9. Créez un instantané à l'aide d'ACS

Il existe de nombreuses façons de créer un instantané dans ACS. Vous pouvez sélectionner l'application et créer un instantané à partir de la page qui affiche les détails de l'application. Vous pouvez cliquer sur Create snapshot pour créer un snapshot à la demande ou configurer une règle de protection.

Créez un instantané à la demande en cliquant simplement sur **Créer un instantané**, en fournissant un nom, en examinant les détails et en cliquant sur **instantané**. L'état de l'instantané passe à sain une fois l'opération terminée.





10. Supprimez la base de données dans l'application postgresql

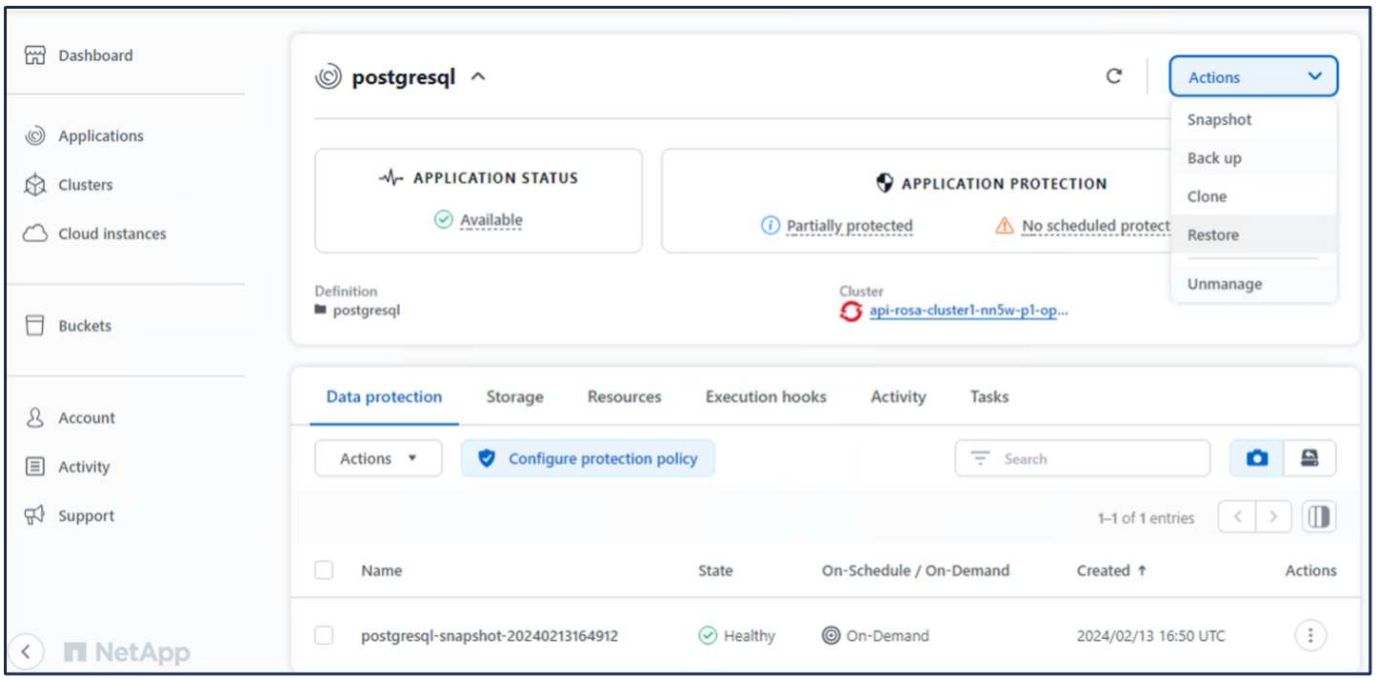
Reconnectez-vous à postgresql, répertoriez les bases de données disponibles, supprimez celle que vous avez créée précédemment et répertoriez à nouveau pour vous assurer que la base de données a été supprimée.

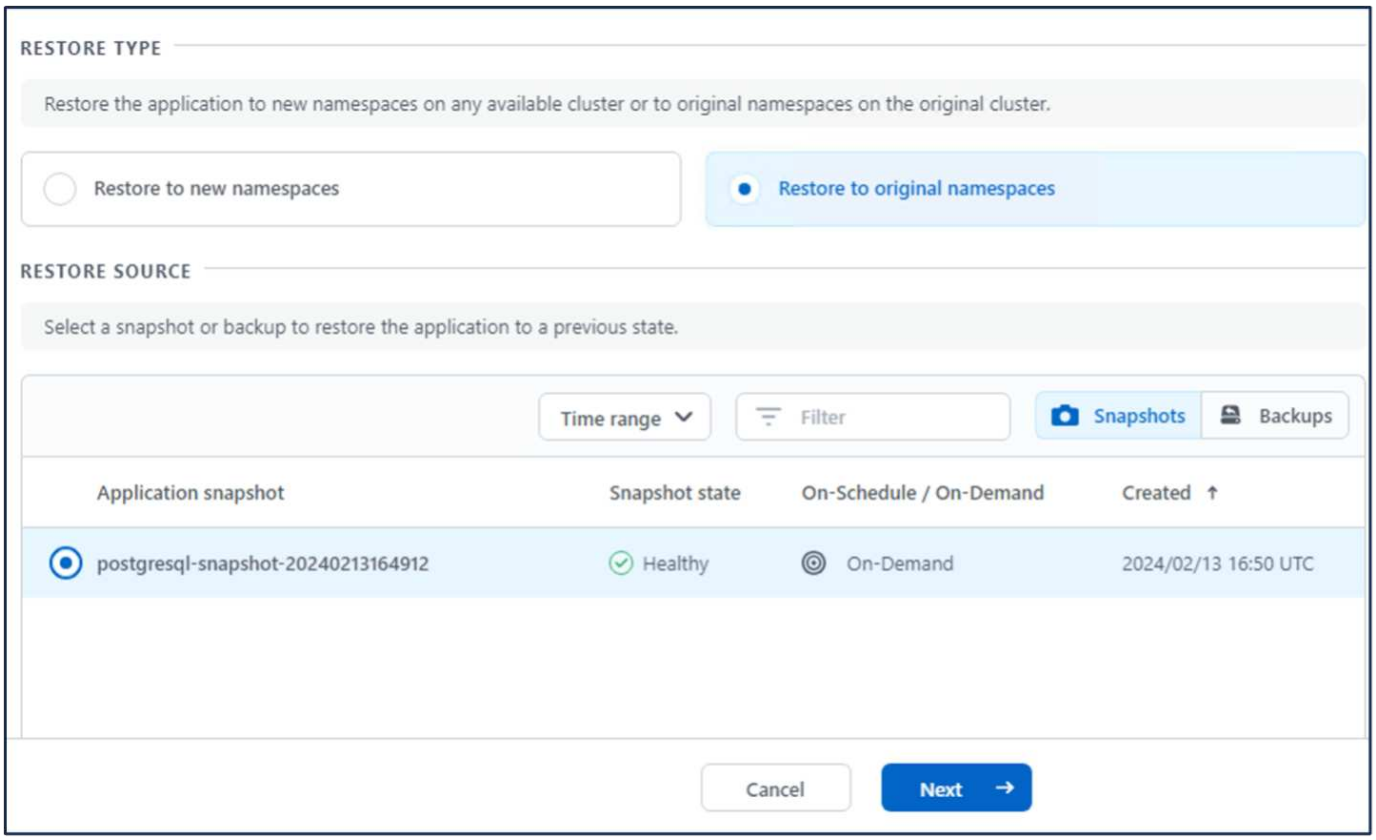
```
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+--------------
-
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(4 rows)

postgres=# DROP DATABASE erp;
DROP DATABASE
postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access priv
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+--------------
-
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres
+
           |          |          |                 |             |             |            |           | postgres=CTc/
(3 rows)
```

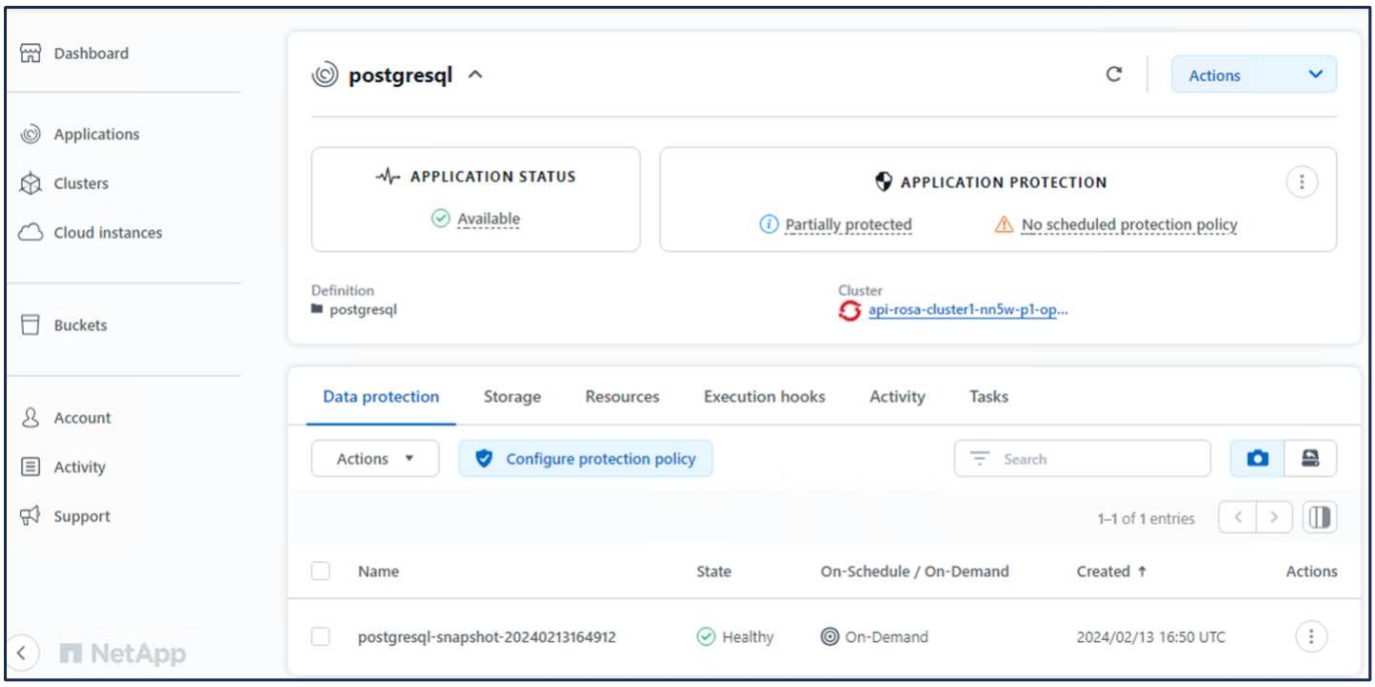
11. Restauration à partir d'un instantané à l'aide d'ACS

Pour restaurer l'application à partir d'un instantané, accédez à la page d'accueil de l'interface utilisateur ACS,

sélectionnez l'application et sélectionnez Restaurer. Vous devez choisir un snapshot ou une sauvegarde à partir de laquelle effectuer la restauration. (En général, plusieurs d'entre elles sont créées en fonction d'une règle que vous avez configurée). Faites les choix appropriés dans les deux écrans suivants, puis cliquez sur **Restaurer**. L'état de l'application passe de la restauration à disponible après sa restauration à partir de l'instantané.







12. Vérifiez que votre application a été restaurée à partir de l'instantané

Connectez-vous au client postgresql et vous devriez maintenant voir la table et l'enregistrement dans la table que vous aviez précédemment. C'est tout. En cliquant simplement sur un bouton, votre application a été restaurée à un état antérieur. C'est à ce niveau de simplicité que nous proposons à nos clients avec Astra Control.

```
[ec2-user@ip-10-49-11-132 ~]$ kubectl run postgresql-client --rm --tty -i --restart='Never' --namespace postgresql --image docker.io/bitnami/postgresql:16.
2.0-debian-11-r1 --env="PGPASSWORD=$POSTGRES_PASSWORD" --command -- psql --host postgresql -U postgres -d postgres -p 5432
Warning: would violate PodSecurity "restricted:v1.24": allowPrivilegeEscalation != false (container "postgresql-client" must set securityContext.allowPrivi
legeEscalation=false), unrestricted capabilities (container "postgresql-client" must set securityContext.capabilities.drop=["ALL"]), runAsNonRoot != true (
pod or container "postgresql-client" must set securityContext.runAsNonRoot=true), seccompProfile (pod or container "postgresql-client" must set securityCon
text.seccompProfile.type to "RuntimeDefault" or "Localhost")
If you don't see a command prompt, try pressing enter.

postgres=# \l
                                                 List of databases
   Name    |  Owner   | Encoding | Locale Provider |   Collate   |    Ctype    | ICU Locale | ICU Rules |   Access privileges
-----------+----------+----------+-----------------+-------------+-------------+------------+-----------+-----------------------
 erp       | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 postgres  | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           |
 template0 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
 template1 | postgres | UTF8     | libc            | en_US.UTF-8 | en_US.UTF-8 |            |           | =c/postgres          +
           |          |          |                 |             |             |            |           | postgres=CTc/postgres
(4 rows)

postgres=# \c erp
You are now connected to database "erp" as user "postgres".
erp=# \dt
          List of relations
 Schema |  Name   | Type  |  Owner
--------+---------+-------+----------
 public | persons | table | postgres
(1 row)

erp=# SELECT * from PERSONS;
 id | firstname | lastname
----+-----------+----------
  1 | John      | Doe
(1 row)
```

Activate Windows

Migration des données

Cette page présente les options de migration des données pour les workloads de conteneurs dans des clusters Red Hat OpenShift gérés à l'aide de FSX pour NetApp ONTAP pour le stockage persistant.

Migration des données

Les services Red Hat OpenShift sur AWS et FSX pour NetApp ONTAP (FSxN) font partie de leur portefeuille de services par AWS. FSxN est disponible avec les options Single AZ ou Multi-AZ. L'option Multi-Az assure la protection des données contre les défaillances de zone de disponibilité. FSxN peut être intégré à Astra Trident pour fournir un stockage persistant aux applications sur les clusters ROSA.

Intégration de FSxN avec Trident à l'aide de Helm Chart

Intégration de clusters ROSA avec Amazon FSX for ONTAP

La migration des applications de conteneurs implique :

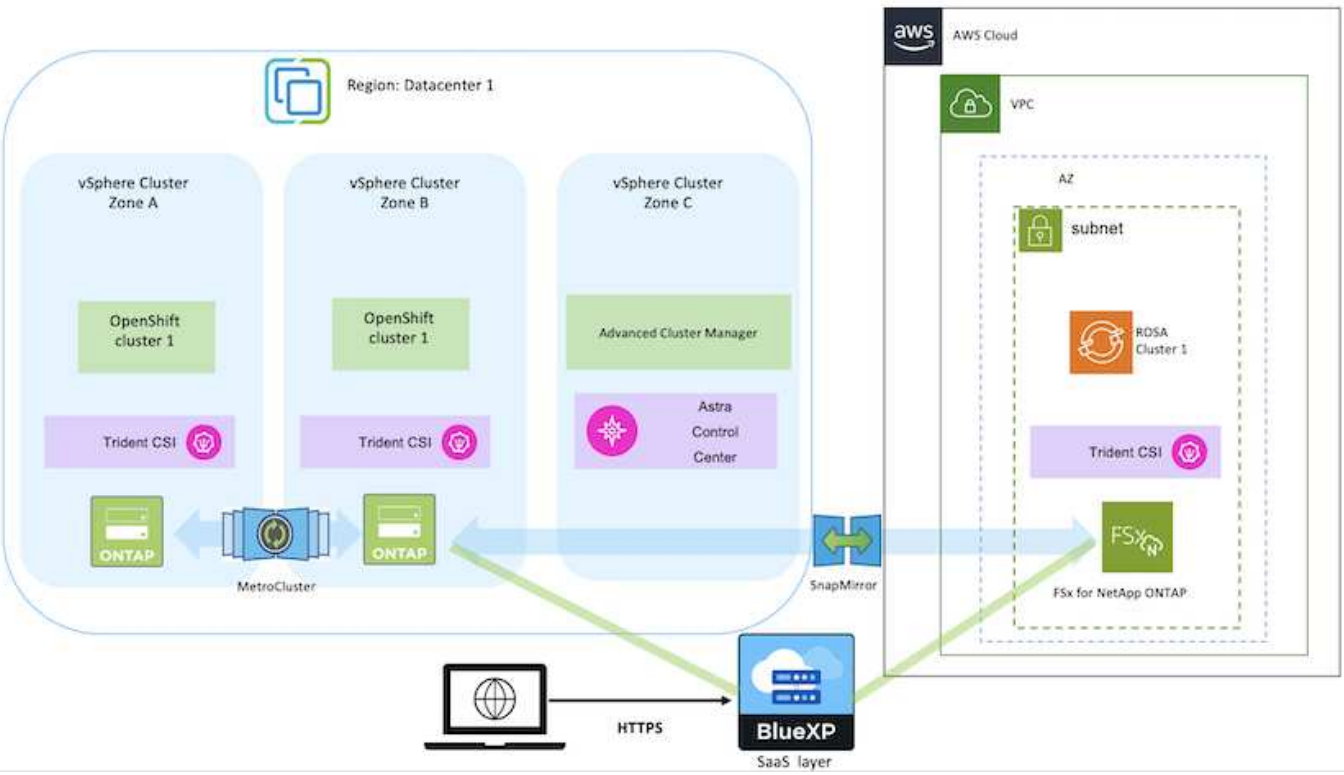
- Volumes persistants : cette opération peut être effectuée à l'aide de BlueXP. Une autre option consiste à utiliser Astra Control Center pour gérer les migrations d'applications de conteneurs d'un environnement sur site vers le cloud. L'automatisation peut être utilisée dans le même but.
- Métadonnées des applications : cette opération peut être réalisée à l'aide d'OpenShift GitOps (Argo CD).

Basculement et retour arrière des applications sur un cluster ROSA à l'aide de FSxN pour le stockage persistant

La vidéo suivante présente des scénarios de basculement et de retour arrière d'applications à l'aide de BlueXP et d'Argo CD.

Basculement et retour arrière des applications sur le cluster ROSA

Solution de protection et de migration des données pour les workloads de conteneurs OpenShift



Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.