Cloud hybride FlexPod avec NetApp Astra et Cisco Intersight pour Red Hat OpenShift

FlexPod

NetApp
October 30, 2025

Sommaire

Cloud hybride FlexPod avec NetApp Astra et Cisco Intersight pour Red Hat OpenShift . . . 1
Tr-4936 : cloud hybride FlexPod avec NetApp Astra et Cisco Intersight pour Red Hat OpenShift . . . 1
Introduction . . . 1
Public . . . 1
NetApp Astra Control – principales utilisations . . . 1
Composants de la solution . . . 3
FlexPod . . . 3
Contrôle Astra . . . 3
Astra Trident . . . 4
Système back-end . . . 5
NetApp Cloud Volumes ONTAP . . . 5
Cloud Central . . . 5
Le gestionnaire Cloud . . . 6
Connecteur . . . 6
NetApp Cloud Insights . . . 6
NetApp Active IQ Unified Manager . . . 6
Cisco Intersight . . . 6
Plateforme de conteneurs Red Hat OpenShift . . . 8
VMware vSphere 7.0 . . . 9
Révisions matérielles et logicielles . . . 9
Installation et configuration . . . 11
Installation de FlexPod pour OpenShift Container Platform 4 sans système d’exploitation . . . 11
Red Hat OpenShift sur AWS . . . 12
NetApp Cloud Volumes ONTAP . . . 13
Installation d’Astra Control Center sur OpenShift Container Platform . . . 13
Validation des solutions . . . 33
Présentation . . . 33
Restauration d’applications avec sauvegardes distantes . . . 33
Conclusion . . . 54
Dépannage . . . 55
Où trouver des informations complémentaires . . . 55
Historique des versions . . . 56

Cloud hybride FlexPod avec NetApp Astra et Cisco Intersight pour Red Hat OpenShift

Tr-4936 : cloud hybride FlexPod avec NetApp Astra et Cisco Intersight pour Red Hat OpenShift

Abhinav Singh

Introduction

Les conteneurs et Kubernetes s'imposent comme la solution idéale pour développer, déployer, exécuter, gérer et faire évoluer les applications conteneurisées, et les entreprises déploient de plus en plus d'applications stratégiques. Les applications stratégiques dépendent fortement de l'état des applications. Une application avec état possède des informations associées à l'état, aux données et à la configuration, et dépend des transactions de données précédentes pour exécuter sa logique applicative. Les applications stratégiques s'exécutant sur Kubernetes continuent de satisfaire aux exigences de disponibilité et de continuité de l'activité telles que les applications classiques. Une panne de service peut avoir des conséquences graves sur la perte de chiffre d'affaires, la productivité et la réputation de l'entreprise. Il est donc essentiel de protéger, restaurer et déplacer les workloads Kubernetes rapidement et facilement dans et entre les clusters, les data centers sur site et les environnements de cloud hybride. Les entreprises ont vu les avantages de basculer leur activité vers un modèle de cloud hybride et de moderniser leurs applications dans un format cloud natif.

Dans ce rapport technique, nous Unis d'un centre de contrôle NetApp Astra avec Red Hat OpenShift Container Platform sur une solution d'infrastructure convergée FlexPod. Il s'étend à Amazon Web Services (AWS) pour former un data Center de cloud hybride. Sur la base de la connaissance "FlexPod et Red Hat OpenShift", Ce document présente NetApp Astra Control Center, qui commence par l'installation, la configuration, les workflows de protection des applications et la migration des applications entre le site et le cloud. Il présente également les avantages des fonctionnalités de gestion des données intégrant la cohérence applicative (notamment la sauvegarde et la restauration, la continuité de l'activité) avec NetApp Astra Control Center pour les applications conteneurisées qui s'exécutent sur Red Hat OpenShift.

La figure suivante illustre la présentation de la solution.

[Erreur : image graphique manquante]

Public

Le public visé est composé de directeurs de la technologie (CTO), de développeurs d'applications, d'architectes de solutions cloud, d'ingénieurs de fiabilité des sites, d'ingénieurs DevOps, d'opérations IT et d'équipes de services professionnels axés sur la conception, l'hébergement et la gestion des applications conteneurisées.

NetApp Astra Control – principales utilisations

NetApp Astra Control vise à simplifier la protection des applications pour les clients qui gèrent des microservices cloud natifs :

- **Représentation d'application instantanée avec snapshots.** avec Astra Control, vous pouvez effectuer des snapshots de bout en bout de vos applications conteneurisées qui incluent les détails de configuration de l'application exécutée sur Kubernetes et le stockage persistant associé. En cas d'incident, les applications peuvent être restaurées à un état de fonctionnement connu en cliquant sur le bouton.

- **Sauvegarde complète de l'application de copie.** avec Astra Control, vous pouvez effectuer une sauvegarde complète de l'application selon un calendrier prédéfini qui peut être utilisé pour restaurer l'application vers le même cluster K8s ou vers un autre cluster à la demande de façon automatisée.
- **Portabilité des applications et migration avec des clones.** avec Astra Control, vous pouvez cloner une application entière avec ses données d'un cluster Kubernetes vers un autre cluster ou au sein d'un même cluster K8s. Cette fonction contribue également à déplacer ou migrer une application sur les clusters K8s, quel que soit l'emplacement des clusters (il suffit de supprimer l'instance d'application source après le clonage).
- **Personnaliser la cohérence des applications.** avec Astra Control, vous pouvez prendre le contrôle de la définition des États de mise en attente des applications en utilisant les crochets d'exécution. Lorsque vous placez les crochets d'exécution « pré » et « post » dans les flux de travail de snapshot et de sauvegarde, vos applications seront suspendues de votre manière avant qu'un snapshot ou une sauvegarde ne soit créé.
- **Automatisez la reprise après incident au niveau applicatif.** avec Astra Control, vous pouvez configurer un plan de reprise après incident pour la continuité de l'activité pour vos applications conteneurisées. NetApp SnapMirror est utilisé en back-end et la mise en œuvre complète du workflow de reprise après incident est automatisée.

Topologie de la solution

Cette section décrit la topologie logique de la solution.

L'illustration suivante représente la topologie de la solution, constituée de l'environnement FlexPod sur site exécutant des clusters OpenShift Container Platform et d'un cluster OpenShift Container Platform autogéré sur AWS avec NetApp Cloud Volumes ONTAP, Cisco Intersight et la plateforme NetApp Cloud Manager SaaS.

[Erreur : image graphique manquante]

Le premier cluster OpenShift Container Platform est une installation sans système d'exploitation sur FlexPod. Le second cluster OpenShift Container Platform est déployé sur VMware vSphere exécuté sur FlexPod, et le troisième cluster OpenShift Container Platform est déployé en tant que "cluster privé" Dans un cloud privé virtuel (VPC) existant sur AWS en tant qu'infrastructure autonome.

Avec cette solution, FlexPod est connecté à AWS par le biais d'un VPN site à site. Cependant, les clients peuvent également utiliser les implémentations de connexion directe pour s'étendre à un cloud hybride. Cisco Intersight permet de gérer les composants de l'infrastructure FlexPod.

Dans cette solution, Astra Control Center gère l'application conteneurisée hébergée sur le cluster OpenShift Container Platform qui s'exécute sur FlexPod et sur AWS. Astra Control Center est installé sur l'instance OpenShift bare-Metal qui s'exécute sur FlexPod. Astra Control communique avec l'api kube sur le nœud maître et surveille en permanence le cluster Kubernetes pour y apporter des modifications. Toutes les nouvelles applications ajoutées au cluster K8s sont automatiquement découvertes et mises à disposition pour la gestion.

La représentation des applications conteneurisées peut être capturée sous forme de copies Snapshot à l'aide d'Astra Control Center. Les snapshots d'applications peuvent être déclenchés par une stratégie de protection planifiée ou à la demande. Pour les applications prises en charge par Astra, le snapshot est cohérent en cas de panne. Un snapshot d'application constitue un snapshot des données d'application dans les volumes persistants, ainsi que des métadonnées d'application des différentes ressources Kubernetes associées à cette application.

Il est possible de créer une copie de sauvegarde complète d'une application à l'aide d'Astra Control avec un programme de sauvegarde prédéfini ou à la demande. Un stockage objet est utilisé pour stocker la

sauvegarde des données d'application. NetApp ONTAP S3, NetApp StorageGRID et toutes les implémentations S3 génériques peuvent être utilisées comme un magasin d'objets.

"Ensuite, les composants de la solution."

Composants de la solution

"Précédent : présentation de la solution."

FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp ONTAP, les réseaux Cisco Nexus, les réseaux de stockage Cisco MDS, Cisco Unified Computing System (Cisco UCS). La conception est suffisamment flexible pour que le réseau, le calcul et le stockage puissent s'intégrer dans un seul rack de data Center ou être déployés selon la conception du centre de données du client. La densité des ports permet aux composants réseau de prendre en charge plusieurs configurations.

Contrôle Astra

Astra Control propose des services de protection des données cohérents avec les applications cloud, hébergés dans des clouds publics et sur site. Astra Control assure la protection des données, la reprise d'activité et la migration de vos applications conteneurisées exécutées sur Kubernetes.

Caractéristiques

Astra Control offre des fonctionnalités stratégiques pour la gestion du cycle de vie des données d'application Kubernetes :

- Gérez automatiquement le stockage persistant
- Création de copies Snapshot et de sauvegardes cohérentes avec les applications à la demande
- Opérations de sauvegarde et de snapshots automatisées basées sur des règles
- Migrez des applications et des données associées d'un cluster Kubernetes vers un autre dans une configuration de cloud hybride
- Clonez une application sur le même cluster K8s ou sur un autre cluster K8s
- Visualisation de l'état de la protection des applications
- Fournit une interface utilisateur graphique et une liste exhaustive d'API REST permettant de mettre en œuvre tous les flux de travail de protection à partir des outils internes existants.

Astra Control offre une visualisation centralisée pour vos applications conteneurisées qui fournit un aperçu des ressources associées créées dans le cluster Kubernetes. Vous pouvez afficher tous vos clusters, toutes vos applications, dans tous les clouds ou dans tous les data centers à partir d'un portail unique. Vous pouvez utiliser les API de contrôle Astra dans tous les environnements (sur site ou dans des clouds publics) pour implémenter vos workflows de gestion des données.

Modèles de consommation Astra Control

Astra Control est disponible en deux modèles de consommation :

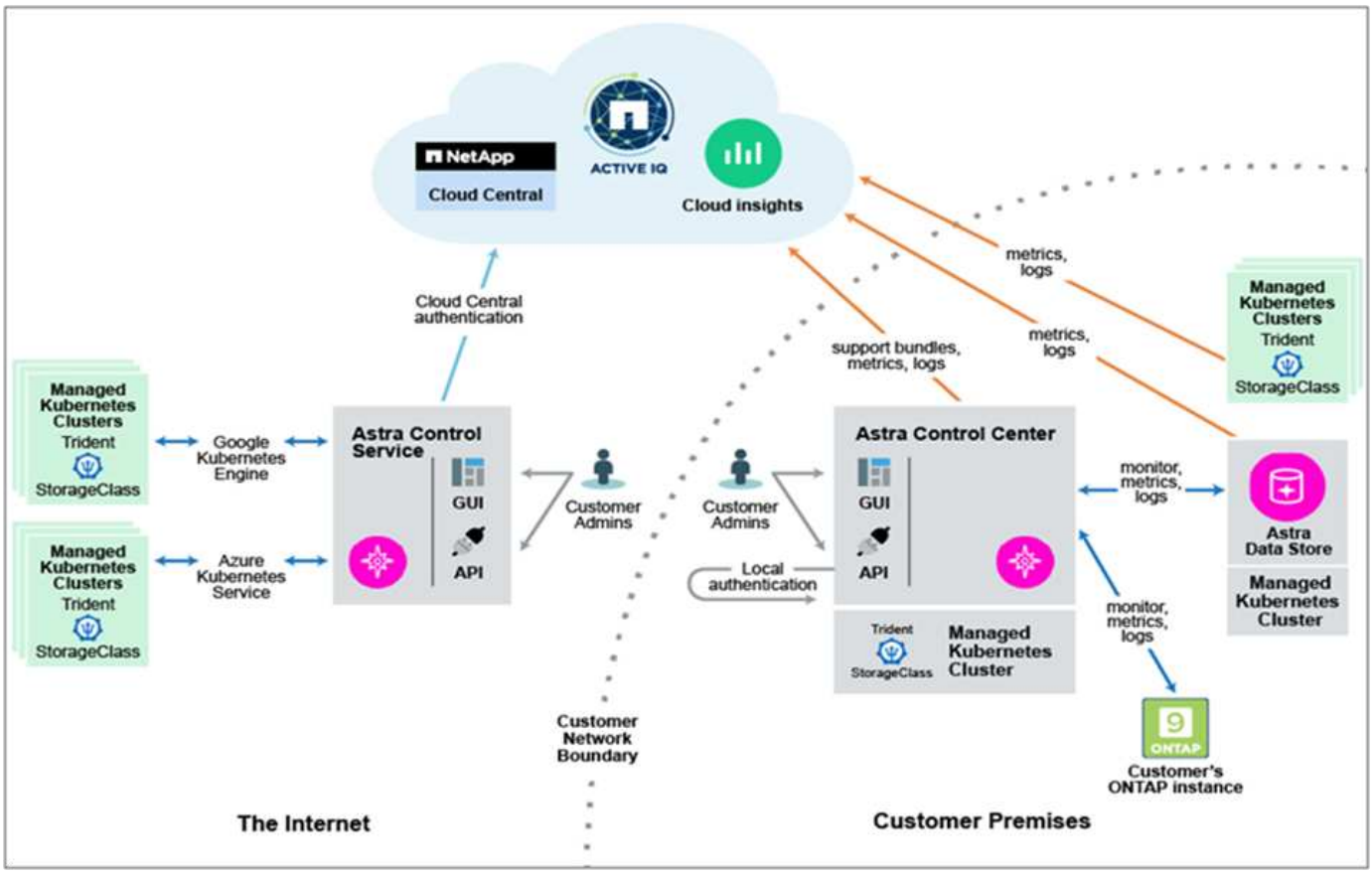
- **Astra Control Service.** Un service entièrement géré hébergé par NetApp qui permet la gestion des données intégrant la cohérence applicative des clusters Kubernetes dans Google Kubernetes Engine

(GKE), Azure Kubernetes Service (AKS).

- **Astra Control Center.** logiciel autogéré qui assure la gestion des données intégrant la cohérence applicative de clusters Kubernetes exécutés dans votre environnement sur site et de cloud hybride.

Dans ce rapport technique, Astra Control Center est utilisé pour la gestion des applications cloud natives qui s'exécutent sur Kubernetes.

L'image suivante montre l'architecture Astra Control.



Astra Trident

Astra Trident est un orchestrateur de stockage open source entièrement pris en charge pour les conteneurs et les distributions Kubernetes. Il a été conçu dès le départ pour vous aider à répondre aux exigences de persistance de vos applications conteneurisées à l'aide d'interfaces standard, telles que le "Interface de stockage de conteneurs (CSI)". Avec Astra Trident, les microservices et les applications conteneurisées peuvent bénéficier des services de stockage haute performance fournis par le portefeuille NetApp de systèmes de stockage.

Astra Trident est déployé sur les clusters Kubernetes sous forme de pods et fournit des services d'orchestration de stockage dynamique pour vos charges de travail Kubernetes. Il permet à vos applications conteneurisées de consommer rapidement et facilement le stockage persistant du vaste portefeuille de NetApp, qui comprend NetApp ONTAP (NetApp AFF, NetApp FAS, NetApp ONTAP Select, Cloud et Amazon FSx for NetApp ONTAP), le logiciel NetApp Element (NetApp SolidFire), ainsi que le service Azure NetApp Files . Dans un environnement FlexPod , Astra Trident est utilisé pour provisionner et gérer dynamiquement des volumes persistants pour les conteneurs qui sont pris en charge par des volumes NetApp FlexVol et des LUN hébergés sur une plateforme de stockage ONTAP telle que les systèmes NetApp AFF et FAS et Cloud Volumes ONTAP. Trident joue également un rôle clé dans la mise en œuvre des schémas de protection des applications fournis par Astra Control. Pour plus d'informations sur Astra Trident, consultez le "Documentation

Astra Trident."

Système back-end

Pour utiliser Astra Trident, vous avez besoin d'un système back-end de stockage pris en charge. Un système back-end Trident définit la relation entre Trident et un système de stockage. Il explique à Trident comment communiquer avec ce système de stockage et comment Trident doit provisionner les volumes à partir de celui-ci. Trident va automatiquement proposer des pools de stockage back-end correspondant aux exigences définies par une classe de stockage.

- Système back-end ONTAP AFF et FAS. En tant que plateforme matérielle et logicielle de stockage, ONTAP fournit des services de stockage de base, la prise en charge de plusieurs protocoles d'accès au stockage et des fonctionnalités de gestion du stockage, comme les copies Snapshot et la mise en miroir NetApp.
- Système back-end Cloud Volumes ONTAP
- "Magasin de données Astra" système back-end

NetApp Cloud Volumes ONTAP

NetApp Cloud Volumes ONTAP est une offre de stockage Software-defined qui offre des fonctionnalités avancées de gestion des données pour les workloads de fichiers et de blocs. Avec Cloud Volumes ONTAP, vous pouvez optimiser vos coûts de stockage cloud et augmenter les performances de vos applications tout en améliorant la protection des données, la sécurité et la conformité.

Parmi les principaux avantages :

- Exploitez les fonctionnalités intégrées de déduplication et de compression des données, de provisionnement fin et de clonage pour réduire les coûts de stockage.
- Fiabilité exceptionnelle et continuité de l'activité en cas de défaillances dans votre environnement cloud.
- Cloud Volumes ONTAP exploite SnapMirror, la technologie de réplication leader de NetApp, pour répliquer les données sur site dans le cloud de façon à pouvoir disposer de copies secondaires dans différents cas d'utilisation.
- Cloud Volumes ONTAP s'intègre également avec Cloud Backup Service pour fournir des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données cloud.
- Basculez entre pools de stockage hautes performances et faibles performances à la demande sans interrompre les applications.
- Cohérence des copies Snapshot avec NetApp SnapCenter
- Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.
- L'intégration avec Cloud Data SENSE vous aide à comprendre le contexte des données et à identifier les données sensibles.

Cloud Central

Cloud Central est une plateforme centralisée qui permet d'accéder aux services de données cloud NetApp et de les gérer. Ces services vous permettent d'exécuter des applications stratégiques dans le cloud, de créer des sites automatisés de reprise d'activité, de sauvegarder les données et de migrer et contrôler efficacement les données entre plusieurs clouds. Pour plus d'informations, voir "Cloud Central."

Le gestionnaire Cloud

Cloud Manager est une plateforme de gestion SaaS de grande qualité qui permet aux experts INFORMATIQUES et aux architectes clouds de gérer de manière centralisée leur infrastructure multicloud hybride à l'aide des solutions clouds NetApp. Cette solution offre un système centralisé pour afficher et gérer vos environnements de stockage sur site et cloud, prenant en charge des environnements de cloud hybride de plusieurs fournisseurs et comptes. Pour plus d'informations, voir "Le gestionnaire Cloud".

Connecteur

Connector est une instance qui permet à Cloud Manager de gérer les ressources et les processus dans un environnement de cloud public. Un connecteur est nécessaire pour utiliser de nombreuses fonctionnalités offertes par Cloud Manager. Un connecteur peut être déployé dans le cloud ou sur site.

Le connecteur est pris en charge aux emplacements suivants :

- AWS
- Microsoft Azure
- Google Cloud
- Sur site

Pour en savoir plus sur le connecteur, voir "ce lien."

NetApp Cloud Insights

Avec l'outil NetApp de surveillance de l'infrastructure cloud, Cloud Insights vous permet de surveiller la performance et l'utilisation de vos clusters Kubernetes gérés par Astra Control Center. Cloud Insights met en corrélation l'utilisation du stockage avec les charges de travail. Lorsque vous activez la connexion Cloud Insights dans le centre de contrôle Astra, les informations de télémétrie s'affichent dans les pages de l'interface utilisateur du centre de contrôle Astra.

NetApp Active IQ Unified Manager

Avec NetApp Active IQ Unified Manager, vous pouvez contrôler vos clusters de stockage ONTAP à partir d'une interface intuitive unique, reconçue pour exploiter les connaissances de la communauté et l'analytique d'IA. Elle fournit des informations opérationnelles, de performance et proactives sur l'environnement de stockage et les machines virtuelles qui s'exécutent sur celui-ci. Lorsqu'un problème survient sur l'infrastructure de stockage, Unified Manager vous informe des détails du problème pour vous aider à identifier la cause première. Le tableau de bord des machines virtuelles vous offre une vue détaillée des statistiques de performances de la machine virtuelle. Vous pouvez ainsi examiner l'ensemble du chemin d'E/S depuis l'hôte VMware vSphere, via le réseau et enfin vers le stockage. Certains événements fournissent également des mesures correctives qui peuvent être prises pour corriger le problème. Vous pouvez configurer des alertes personnalisées en cas d'événements afin que, lorsque des problèmes se produisent, vous soyez averti par e-mail et par des traps SNMP. Active IQ Unified Manager vous permet de planifier les besoins en stockage de vos utilisateurs en anticipant les besoins en stockage et en vous permettant d'anticiper les problèmes, ce qui évite de prendre des décisions réactives à court terme et même d'engendrer des problèmes supplémentaires à long terme.

Cisco Intersight

Cisco Intersight est une plateforme SaaS qui assure une automatisation, une observabilité et une optimisation intelligentes pour les applications et l'infrastructure classiques et cloud. La plateforme contribue aux

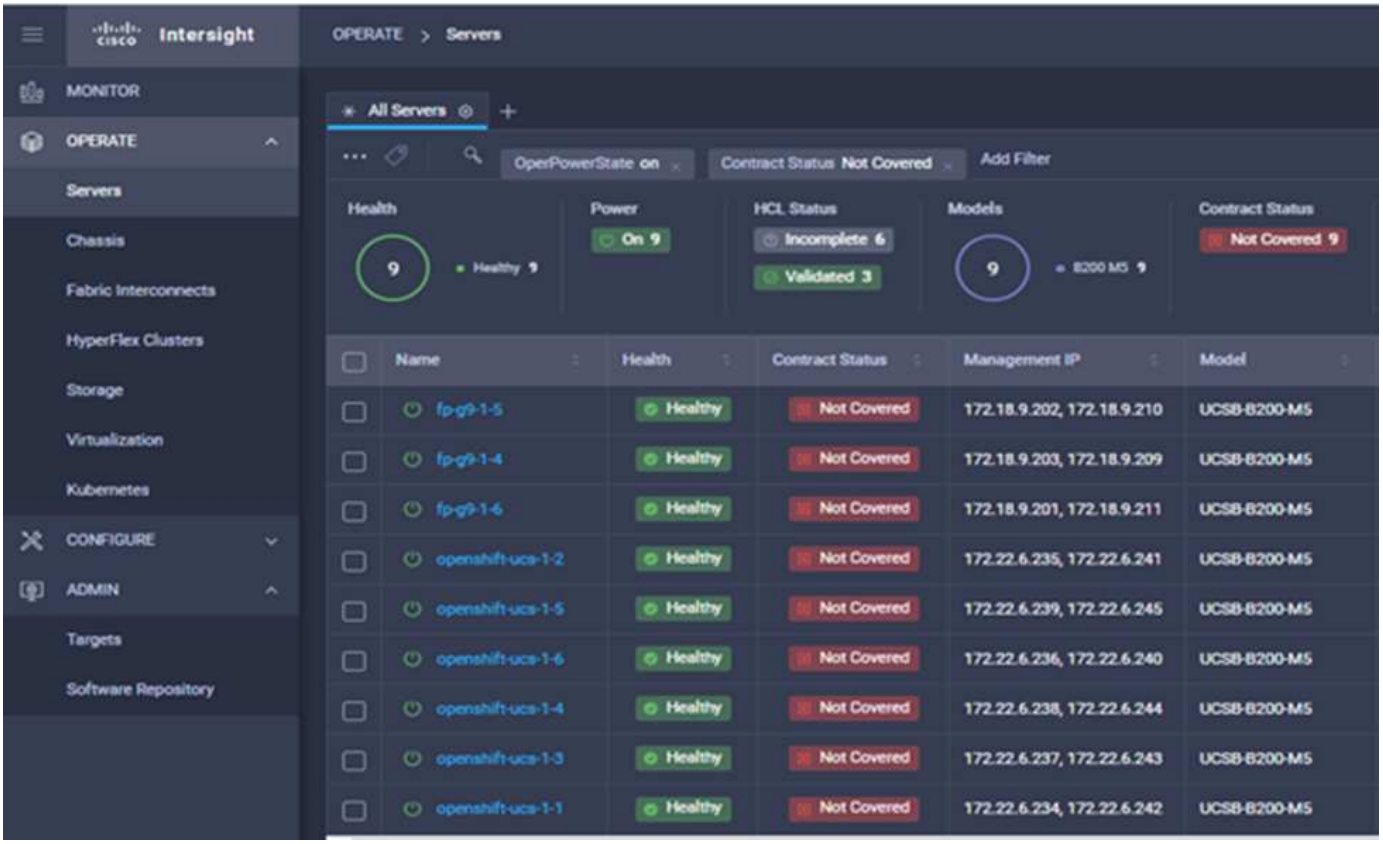
changements avec les équipes IT et propose un modèle d'exploitation conçu pour le cloud hybride.

Cisco Intersight offre les avantages suivants :

- **Livraison plus rapide.** livraison en tant que service depuis le cloud ou dans le centre de données du client avec des mises à jour fréquentes et une innovation continue, grâce à un modèle de développement logiciel agile. De cette façon, le client peut se concentrer sur l'accélération de la livraison pour le secteur d'activité.
- **Opérations simplifiées.** simplifier les opérations en utilisant un seul outil SaaS sécurisé avec inventaire, authentification et API communs pour travailler sur l'ensemble de la pile et tous les emplacements, éliminant ainsi les silos entre les équipes. De la gestion des serveurs physiques et des hyperviseurs sur site aux machines virtuelles, K8s, sans serveur, automatisation, l'optimisation et le contrôle des coûts à la fois sur site et dans les clouds publics.
- **Optimisation continue.** optimisation continue de votre environnement en utilisant l'intelligence fournie par Cisco Intersight sur chaque couche, ainsi que Cisco TAC. Cette intelligence est convertie en actions recommandées et automatisable, ce qui vous permet de vous adapter en temps réel à chaque changement : du déplacement des charges de travail et du contrôle de l'état des serveurs physiques, au dimensionnement automatique des clusters, aux recommandations de réduction des coûts des clouds publics avec lesquels vous travaillez.

Il existe deux modes d'opérations de gestion possibles avec Cisco Intersight : Umm (UCSM Managed mode) et IMM (Intersight Managed mode). Vous pouvez sélectionner l'UMM natif ou IMM pour les systèmes Cisco UCS reliés au fabric lors de la configuration initiale des interconnexions de fabric. Dans cette solution, l'UMM natif est utilisé.

L'image suivante montre le tableau de bord Cisco Intersight.

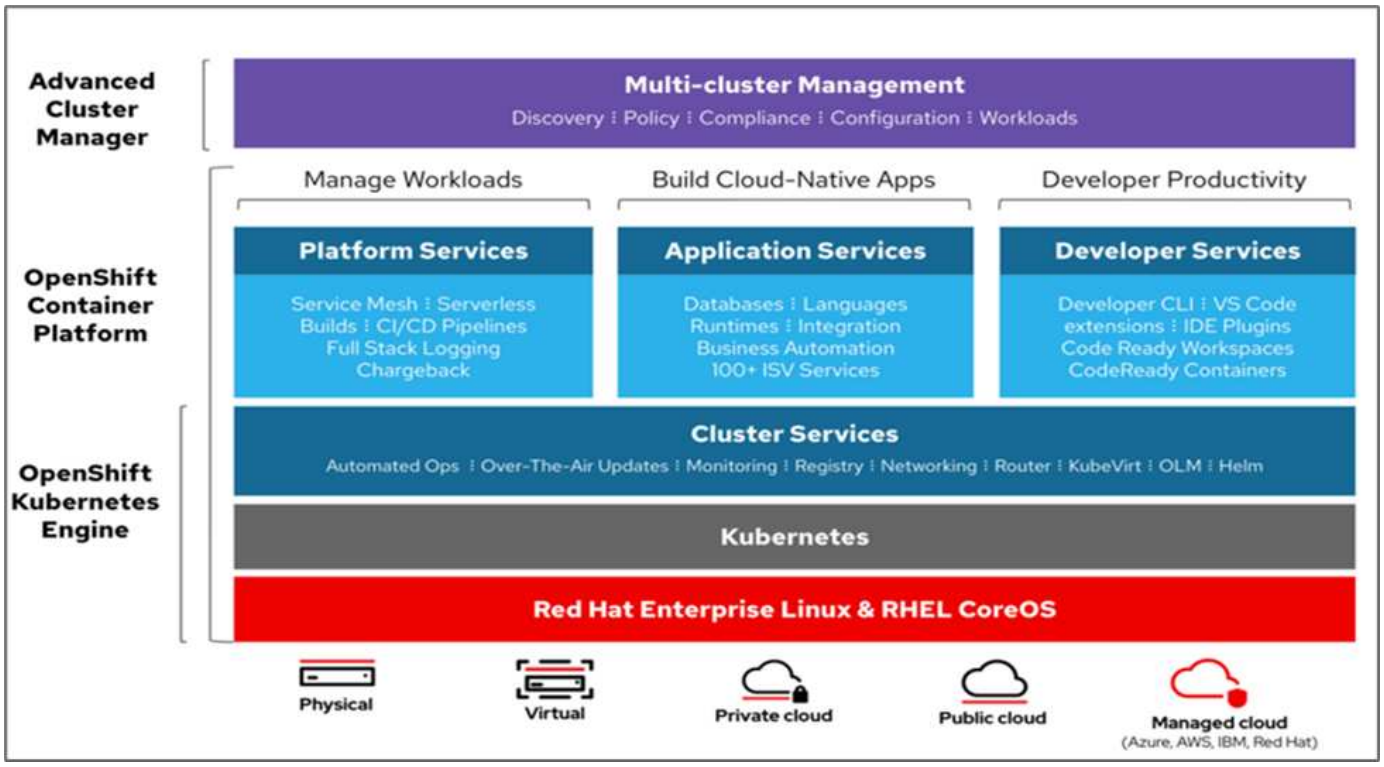


Plateforme de conteneurs Red Hat OpenShift

Red Hat OpenShift Container Platform est une plateforme applicative de conteneurs qui rassemble CRI-O et Kubernetes et qui fournit une API et une interface Web pour gérer ces services. CRI-O est une implémentation de l'interface d'exécution du conteneur Kubernetes (CRI) pour permettre l'utilisation des runtimes compatibles avec l'initiative OCI (Open Container Initiative). Il s'agit d'une alternative légère à l'utilisation de Docker en tant que composant d'exécution pour Kubernetes.

OpenShift Container Platform permet aux clients de créer et de gérer des conteneurs. Les conteneurs sont des processus autonomes qui s'exécutent dans leur propre environnement, indépendamment du système d'exploitation et de l'infrastructure sous-jacente. OpenShift Container Platform aide à développer, déployer et gérer les applications basées sur des conteneurs. Il offre une plateforme en libre-service pour créer, modifier et déployer des applications à la demande, ce qui accélère le développement et la commercialisation des cycles de vie. OpenShift Container Platform est dotée d'une architecture basée sur des microservices de petites unités découplées. Elle s'exécute sur un cluster Kubernetes, et les données relatives aux objets stockés dans ETCD, un magasin de clés à valeur ajoutée en cluster fiable.

L'image suivante présente la plateforme de conteneurs Red Hat OpenShift.



Infrastructure Kubernetes

Dans OpenShift Container Platform, Kubernetes gère les applications conteneurisées sur un ensemble d'hôtes d'exécution CRI-O, et fournit des mécanismes pour le déploiement, la maintenance et l'évolutivité des applications. Les packages de service CRI-O, instancient et exécutent des applications conteneurisées.

Un cluster Kubernetes comprend un ou plusieurs maîtres et un ensemble de nœuds workers. Cette solution intègre les fonctionnalités de haute disponibilité (HA) au niveau du matériel et de la pile logicielle. Un cluster Kubernetes est conçu pour s'exécuter en mode HA avec trois nœuds maîtres et au moins deux nœuds workers afin de vous aider à assurer que le cluster ne présente aucun point de défaillance unique.

Système d'exploitation Red Hat Core

OpenShift Container Platform exploite Red Hat Enterprise Linux CoreOS (RHCOS), un système d'exploitation orienté conteneurs qui combine les meilleures fonctionnalités des systèmes d'exploitation hôtes atomiques CoreOS et Red Hat. RHCOS est spécialement conçu pour exécuter des applications conteneurisées à partir d'OpenShift Container Platform et fonctionne avec de nouveaux outils pour permettre une installation rapide, une gestion basée sur l'opérateur et des mises à niveau simplifiées.

RHCOS inclut les fonctions suivantes :

- Ignition, qu'OpenShift Container Platform utilise comme première configuration de système de démarrage pour l'initialisation et la configuration des machines.
- CRI-O, implémentation d'un exécution de conteneurs natif Kubernetes qui s'intègre étroitement au système d'exploitation pour offrir une expérience Kubernetes efficace et optimisée. CRI-O permet de faire fonctionner, d'arrêter et de redémarrer les conteneurs. Elle remplace entièrement le moteur de conteneurs Docker, qui a été utilisé dans OpenShift Container Platform 3.
- Kubelet, l'agent de nœud principal pour Kubernetes, est responsable du lancement et de la surveillance des conteneurs.

VMware vSphere 7.0

VMware vSphere est une plateforme de virtualisation qui permet de gérer de manière holistique de vastes ensembles d'infrastructures (ressources notamment les processeurs, le stockage et le réseau), sous la forme d'un environnement d'exploitation transparent, polyvalent et dynamique. Contrairement aux systèmes d'exploitation traditionnels qui gèrent une machine individuelle, VMware vSphere agrège l'infrastructure d'un data Center dans son ensemble pour créer une seule puissance avec des ressources qui peuvent être allouées rapidement et dynamiquement à n'importe quelle application, selon les besoins.

Pour plus d'informations, voir "VMware vSphere".

VMware vSphere vCenter

VMware vCenter Server assure une gestion unifiée de tous les hôtes et machines virtuelles depuis une console unique et rassemble le contrôle des performances des clusters, des hôtes et des machines virtuelles. VMware vCenter Server offre aux administrateurs des informations détaillées sur l'état et la configuration des clusters de calcul, des hôtes, des VM, du stockage, du système d'exploitation invité, et autres composants essentiels d'une infrastructure virtuelle. VMware vCenter gère la richesse des fonctionnalités disponibles dans un environnement VMware vSphere.

Révisions matérielles et logicielles

Cette solution peut être étendue à tout environnement FlexPod qui exécute des versions logicielles, micrologicielles et matérielles prises en charge, telles que définies dans le "Matrice d'interopérabilité NetApp" et "Liste de compatibilité matérielle Cisco UCS." Le cluster OpenShift est installé sur FlexPod sans système d'exploitation, ainsi que sur VMware vSphere.

Une seule instance d'Astra Control Center est nécessaire pour gérer plusieurs clusters OpenShift (k8), tandis que Trident CSI est installé sur chaque cluster OpenShift. Astra Control Center peut être installé sur l'un de ces clusters OpenShift. Dans cette solution, Astra Control Center est installé sur le cluster OpenShift bare-Metal.

Le tableau suivant répertorie les révisions matérielles et logicielles FlexPod pour OpenShift.

Composant	Solution NetApp	Version
Calcul	Cisco UCS Fabric Interconnect 6454	4.1(3c)
	Serveurs Cisco UCS B200 M5	4.1(3c)
Le réseau	Cisco Nexus 9336C-FX2 NX-OS	9.3(8)
Stockage	NetApp AFF A700	9.11.1
	NetApp Astra Control Center	22.04.0
	Plug-in NetApp Astra Trident CSI	22.04.0
	NetApp Active IQ Unified Manager	9.11
Logiciel	Pilote Ethernet nenic VMware ESXi	1.0.35.0
	VSphere ESXi	7.0(U2)
	Appliance VMware vCenter	7.0 U2b
	Appliance virtuelle Cisco InterSight Assist	1.0.9-342
	Plateforme de conteneurs OpenShift	4.9
	Nœud principal OpenShift Container Platform	RHCOS 4.9
	Nœud de travail OpenShift Container Platform	RHCOS 4.9

Le tableau suivant répertorie les versions logicielles d'OpenShift sur AWS.

Composant	Solution NetApp	Version
Calcul	Type d'instance maître : m5.XLarge	s/o
	Type d'instance de travailleur : m5.large	s/o
Le réseau	Passerelle de transit du cloud privé virtuel	s/o
Stockage	NetApp Cloud Volumes ONTAP	9.11.1
	Plug-in NetApp Astra Trident CSI	22.04.0
Logiciel	Plateforme de conteneurs OpenShift	4.9
	Nœud principal OpenShift Container Platform	RHCOS 4.9
	Nœud de travail OpenShift Container Platform	RHCOS 4.9

"Suivant : installation de FlexPod pour OpenShift Container Platform 4 sans système d'exploitation."

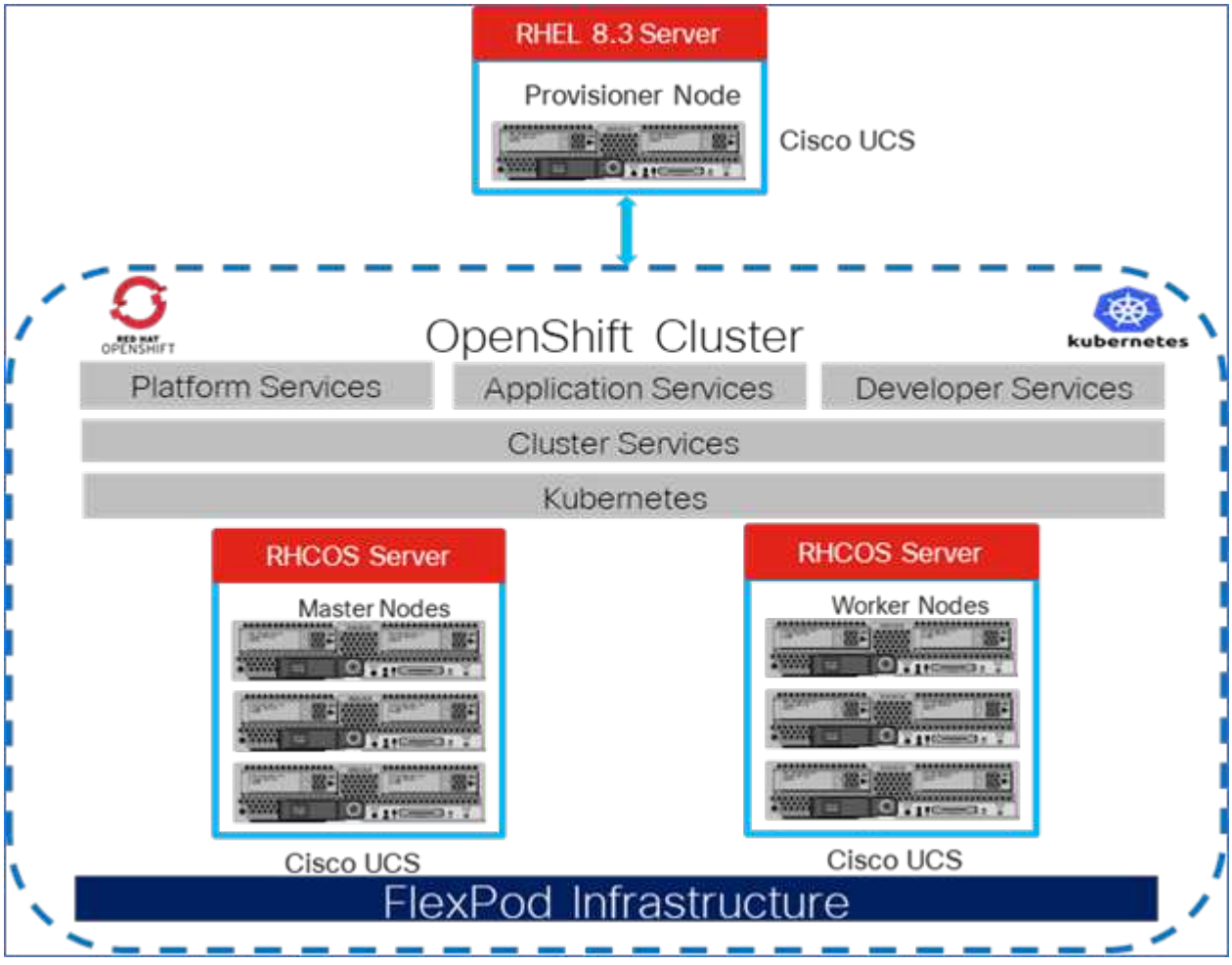
Installation et configuration

Installation de FlexPod pour OpenShift Container Platform 4 sans système d'exploitation

"Précédent : composants de la solution."

Pour comprendre la conception sans système d'exploitation FlexPod pour OpenShift Container Platform 4, les détails du déploiement et l'installation et la configuration de NetApp Astra Trident, consultez "Guide de déploiement et de conception validée par Cisco pour FlexPod avec OpenShift Cisco (CVD)". Ce CVD couvre le déploiement d'FlexPod et de OpenShift Container Platform avec Ansible. Le CVD fournit également des informations détaillées sur la préparation des nœuds de travail, de l'installation d'Astra Trident, du système de stockage back-end et des configurations de classes de stockage, qui sont les quelques prérequis au déploiement et à la configuration d'Astra Control Center.

La figure suivante illustre la plateforme de conteneurs OpenShift 4 sans système d'exploitation sur FlexPod.

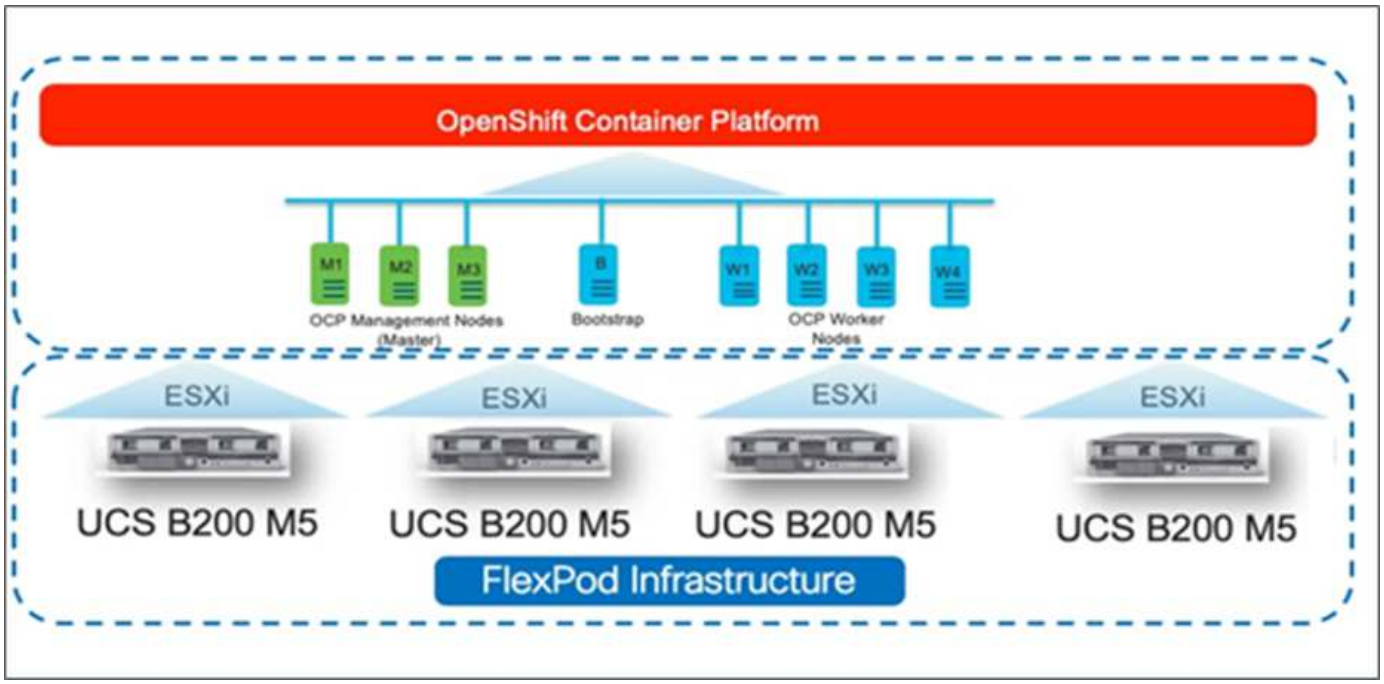


FlexPod pour OpenShift Container Platform 4 sur installation VMware

Pour en savoir plus sur le déploiement de Red Hat OpenShift Container Platform 4 sur un système FlexPod

exécutant VMware vSphere, consultez la page "FlexPod Datacenter pour OpenShift Container Platform 4".

La figure suivante illustre FlexPod pour OpenShift Container Platform 4 sur vSphere.

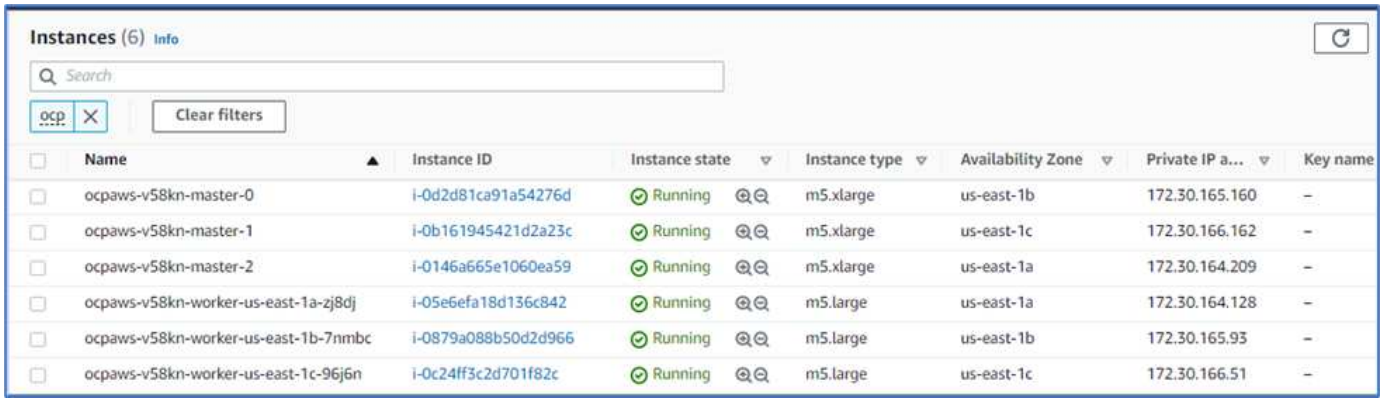


"Suivant : Red Hat OpenShift sur AWS."

Red Hat OpenShift sur AWS

"Précédent : installation de FlexPod pour OpenShift Container Platform 4 sans système d'exploitation."

Un cluster OpenShift Container Platform 4 autogéré est déployé sur AWS en tant que site de reprise après incident. Les nœuds maîtres et workers s'étendent sur trois zones de disponibilité pour une haute disponibilité.



```
[ec2-user@ip-172-30-164-92 ~]$ oc get nodes
NAME                                STATUS   ROLES    AGE   VERSION
ip-172-30-164-128.ec2.internal   Ready    worker   29m   v1.22.8+f34b40c
ip-172-30-164-209.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-165-160.ec2.internal   Ready    master   33m   v1.22.8+f34b40c
ip-172-30-165-93.ec2.internal    Ready    worker   30m   v1.22.8+f34b40c
ip-172-30-166-162.ec2.internal   Ready    master   36m   v1.22.8+f34b40c
ip-172-30-166-51.ec2.internal    Ready    worker   28m   v1.22.8+f34b40c
```

OpenShift est déployé en tant que A. "cluster privé" Dans un VPC existant sur AWS. Un cluster OpenShift Container Platform privé n'expose pas les terminaux externes. Il est accessible uniquement à partir d'un réseau interne et n'est pas visible sur Internet. NetApp Cloud Volumes ONTAP est déployé à un seul nœud à l'aide de NetApp Cloud Manager qui fournit un système back-end de stockage à Astra Trident.

Pour plus d'informations sur l'installation d'OpenShift sur AWS, consultez "Documentation OpenShift".

"Suivant : NetApp Cloud Volumes ONTAP."

NetApp Cloud Volumes ONTAP

"Précédent : Red Hat OpenShift sur AWS."

L'instance NetApp Cloud Volumes ONTAP est déployée sur AWS et sert de stockage back-end à Astra Trident. Avant d'ajouter un environnement de travail Cloud Volumes ONTAP, un connecteur doit être déployé. Cloud Manager vous invite à créer votre premier environnement de travail Cloud Volumes ONTAP sans connecteur. Pour déployer un connecteur dans AWS, voir "Créer un connecteur".

Pour déployer Cloud Volumes ONTAP sur AWS, consultez la section "Démarrage rapide pour AWS".

Une fois Cloud Volumes ONTAP déployé, vous pouvez installer Astra Trident et configurer le système de stockage back-end et la classe Snapshot sur le cluster OpenShift Container Platform.

"Suivant : installation d'Astra Control Center sur OpenShift Container Platform."

Installation d'Astra Control Center sur OpenShift Container Platform

"Précédent : NetApp Cloud Volumes ONTAP."

Vous pouvez installer Astra Control Center sur un cluster OpenShift qui s'exécute sur FlexPod ou sur AWS avec un système de stockage back-end Cloud Volumes ONTAP. Dans cette solution, Astra Control Center est déployé sur le cluster OpenShift bare-Metal.

Le centre de contrôle Astra peut être installé selon la procédure standard décrite "ici" Ou depuis Red Hat OpenShift OperatorHub. L'opérateur de contrôle Astra est un opérateur certifié Red Hat. Dans cette solution, Astra Control Center est installé à l'aide de Red Hat OperatorHub.

De l'environnement

- Astra Control Center prend en charge plusieurs distributions Kubernetes. Pour Red Hat OpenShift, les versions prises en charge incluent Red Hat OpenShift Container Platform 4.8 ou 4.9.
- Astra Control Center requiert les ressources suivantes en plus des exigences de l'environnement et de l'utilisateur final en matière de ressources applicatives :

Composants	Conditions requises
Capacité du système back-end	Au moins 500 Go disponibles
Nœuds worker	Au moins 3 nœuds workers et doté de 4 cœurs de processeurs et de 12 Go de RAM chacun
Adresse de nom de domaine complet (FQDN)	Une adresse FQDN pour Astra Control Center
Astra Trident	Astra Trident 21.04 ou plus récent installé et configuré
Contrôleur d'entrée ou équilibreur de charge	Configurez le contrôleur d'entrée pour exposer Astra Control Center avec un URL ou un équilibreur de charge afin de fournir une adresse IP qui sera définie pour le FQDN

- Vous devez disposer d'un registre d'images privées existant dans lequel vous pouvez pousser les images de création d'Astra Control Center. Vous devez fournir l'URL du registre d'images où vous téléchargez les images.

> Certaines images sont extraites lors de l'exécution de certains flux de travail et des conteneurs sont créés et détruits si nécessaire.

- Avec Astra Control Center, il est nécessaire de créer une classe de stockage et de la définir comme classe de stockage par défaut. Le centre de contrôle Astra prend en charge les pilotes ONTAP suivants fournis par Astra Trident :
  - ontap-nas
  - ontap-nas-flexgroup
  - ontap-san
  - ontap-san-économie

> Nous supposons qu'Astra Trident est installé et configuré avec un système back-end ONTAP, et qu'une classe de stockage par défaut est également définie.

- En ce qui concerne le clonage d'applications dans les environnements OpenShift, Astra Control Center doit permettre à OpenShift de monter des volumes et de modifier la propriété des fichiers. Pour modifier la export policy ONTAP pour permettre ces opérations, lancer les commandes suivantes :

```
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -superuser sys
export-policy rule modify -vserver <storage virtual machine name>
-policyname <policy name> -ruleindex 1 -anon 65534
```

Pour ajouter un deuxième environnement opérationnel OpenShift comme ressource de calcul gérée, assurez-vous que la fonctionnalité de snapshot de volume Astra Trident est activée. Pour activer et tester des copies Snapshot de volume avec Astra Trident, consultez le responsable "Instructions d'Astra Trident".

- A "Classe VolumeSnapClass" Doit être configuré sur tous les clusters Kubernetes à partir de l'emplacement de gestion des applications. Ceci peut également inclure le cluster K8s sur lequel Astra Control Center est installé. Astra Control Center peut gérer les applications du cluster K8s sur lequel il est exécuté.

De gestion des applications

- **Licence.** pour gérer des applications à l'aide d'Astra Control Center, vous avez besoin d'une licence Astra Control Center.
- **Espaces de noms.** Un espace de noms est la plus grande entité qui peut être gérée en tant qu'application par Astra Control Center. Vous pouvez choisir de filtrer les composants en fonction des étiquettes d'application et des étiquettes personnalisées dans un espace de noms existant et de gérer un sous-ensemble de ressources en tant qu'application.
- **StorageClass.** si vous installez une application avec une classe de stockage définie explicitement et que vous devez cloner l'application, le cluster cible pour l'opération de clonage doit avoir la classe de stockage spécifiée à l'origine. Le clonage d'une application avec une classe de stockage explicitement définie vers un cluster ne présentant pas la même classe de stockage échoue.
- **Ressources Kubernetes.** les applications qui utilisent des ressources Kubernetes non capturées par Astra Control peuvent ne pas disposer de fonctionnalités complètes de gestion des données d'application. Astra Control peut capturer les ressources Kubernetes suivantes :

Ressources Kubernetes		
ClusterRole	ClusterRoleBinding	ConfigMap
CustomResourceDefinition	Ressource CustomResource	Cronjob
Ensemble de démonstrations	HorizontalPodAutoscaler	Entrée
Déploiement.Config	MutatingWebhook	Demande de volume persistant
Pod	PodPetitionBudget	PodTemplate
Stratégie réseau	Et de réplication	Rôle
RoleBinding	Itinéraire	Secret
ValidétingWebhook		

Installez Astra Control Center à l'aide d'OpenShift OperatorHub

La procédure suivante permet d'installer Astra Control Center à l'aide de Red Hat OperatorHub. Dans cette solution, Astra Control Center est installé sur un cluster OpenShift bare-Metal exécuté sur FlexPod.

1. Téléchargez le pack Astra Control Center (`astra-control-center-[version].tar.gz`) du "Site de support NetApp".
2. Téléchargez le fichier .zip pour les certificats et clés Astra Control Center à partir du "Site de support NetApp".
3. Vérifiez la signature du lot.

```
openssl dgst -sha256 -verify astra-control-center[version].pub
-signature <astra-control-center[version].sig astra-control-
center[version].tar.gz
```

4. Extraire les images Astra.

```
tar -vxzf astra-control-center-[version].tar.gz
```

5. Passez au répertoire Astra.

```
cd astra-control-center-[version]
```

6. Ajoutez les images à votre registre local.

```
For Docker:
docker login [your_registry_path]OR
For Podman:
podman login [your_registry_path]
```

7. Utilisez le script approprié pour charger les images, les marquer et les pousser dans votre registre local.

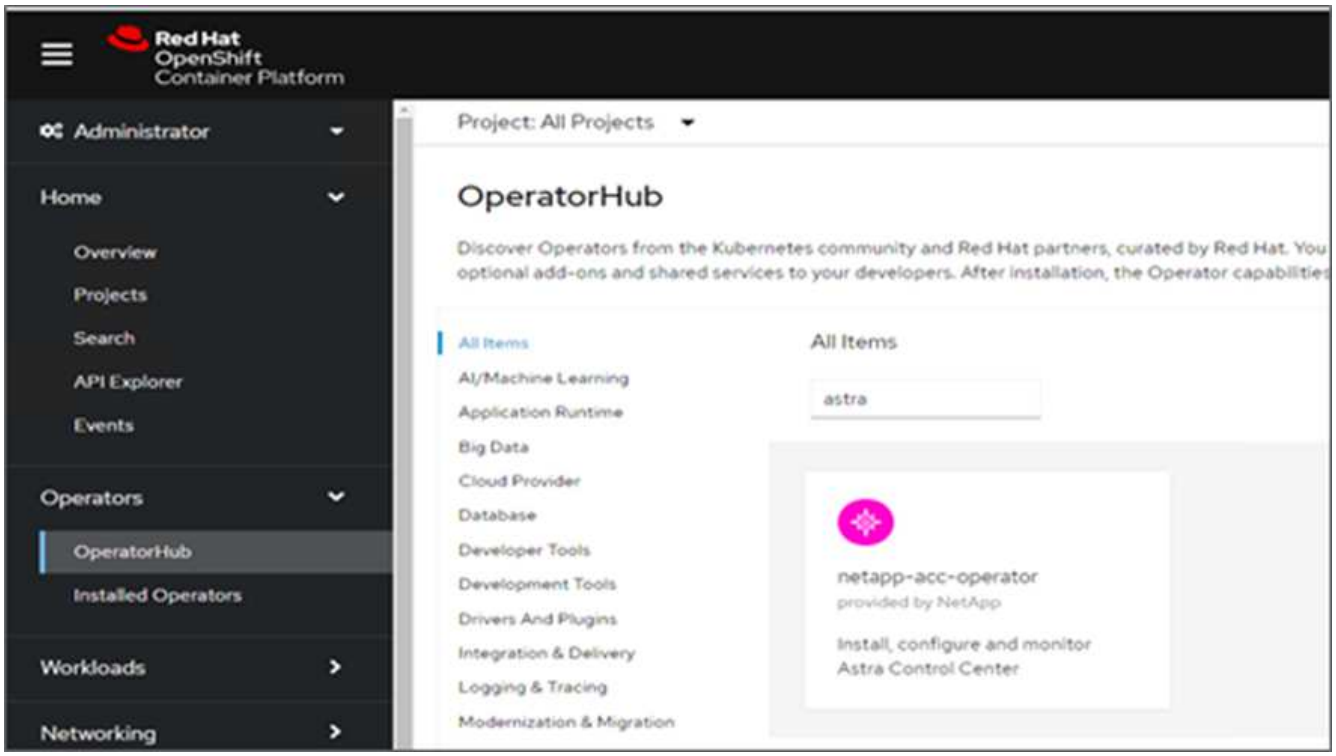
   Pour Docker :

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

   Pour Podman :

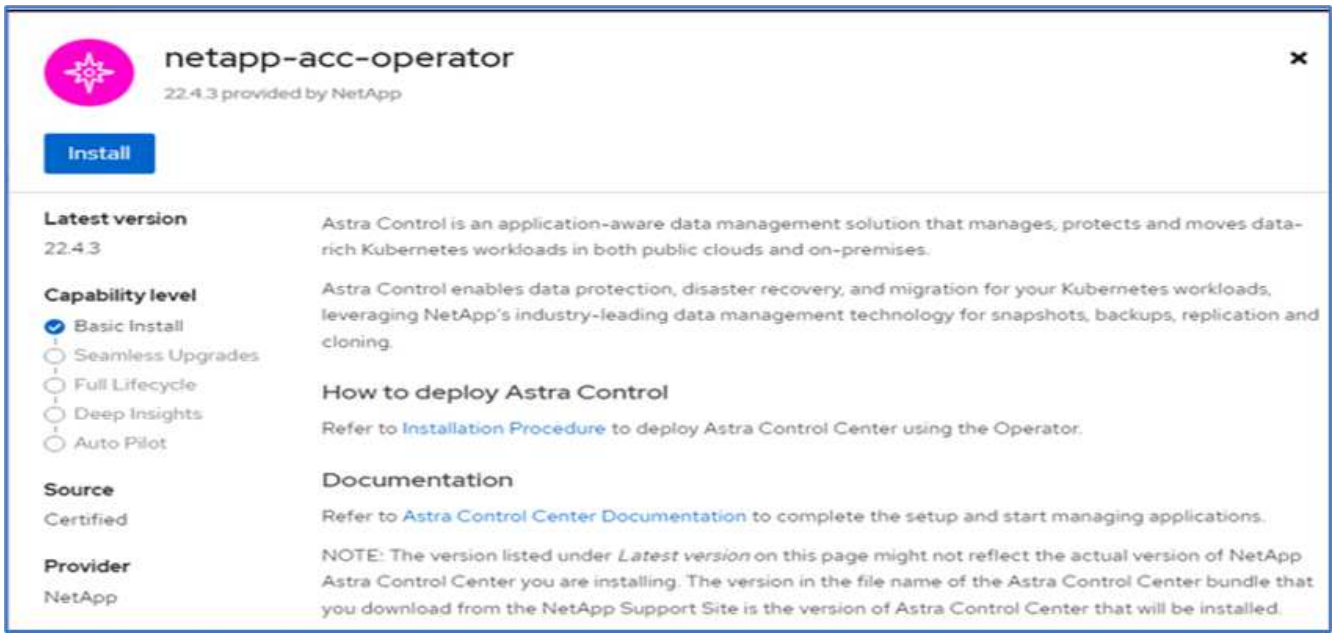
```
export REGISTRY=[Registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image trimming
the 'Loaded images: '
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')
  astraImage=$(echo ${astraImage} | sed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

8. Connectez-vous à la console web du cluster OpenShift sans système d'exploitation. Dans le menu latéral, sélectionnez opérateurs > OperatorHub. Entrez `astra` pour afficher la liste `netapp-acc-operator`.

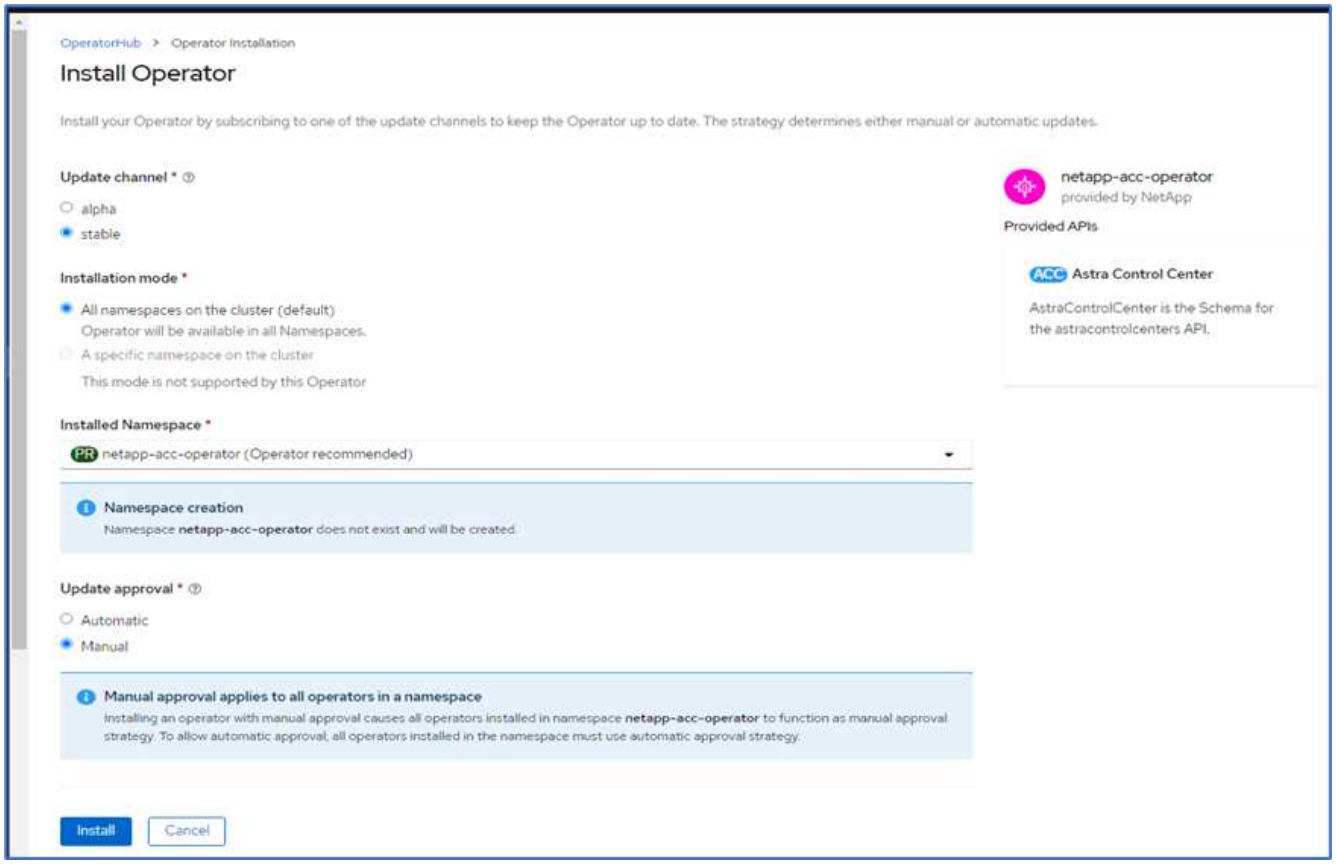


`netapp-acc-operator` Est un opérateur Red Hat OpenShift certifié. Il est répertorié dans le catalogue OperatorHub.

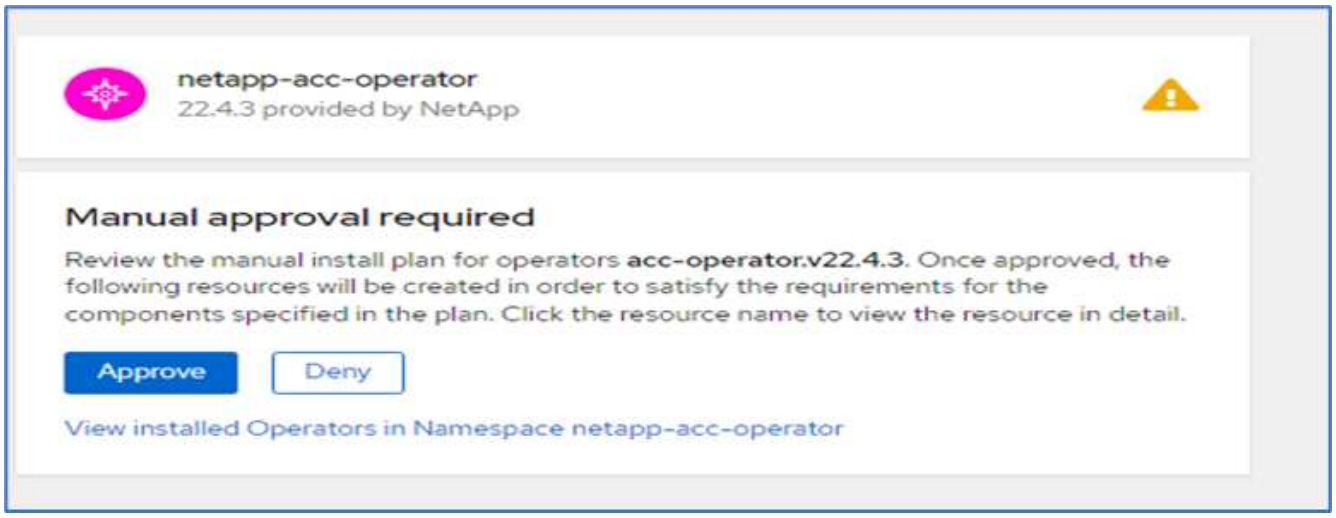
9. Sélectionnez `netapp-acc-operator` Cliquez ensuite sur installation.



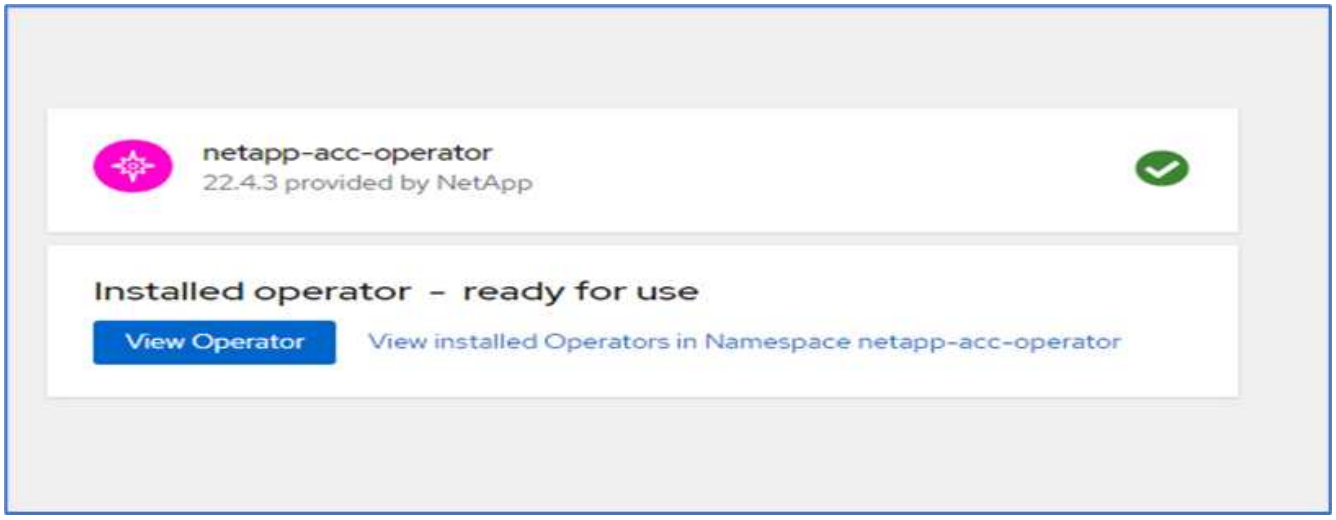
10. Sélectionnez les options appropriées et cliquez sur installer.



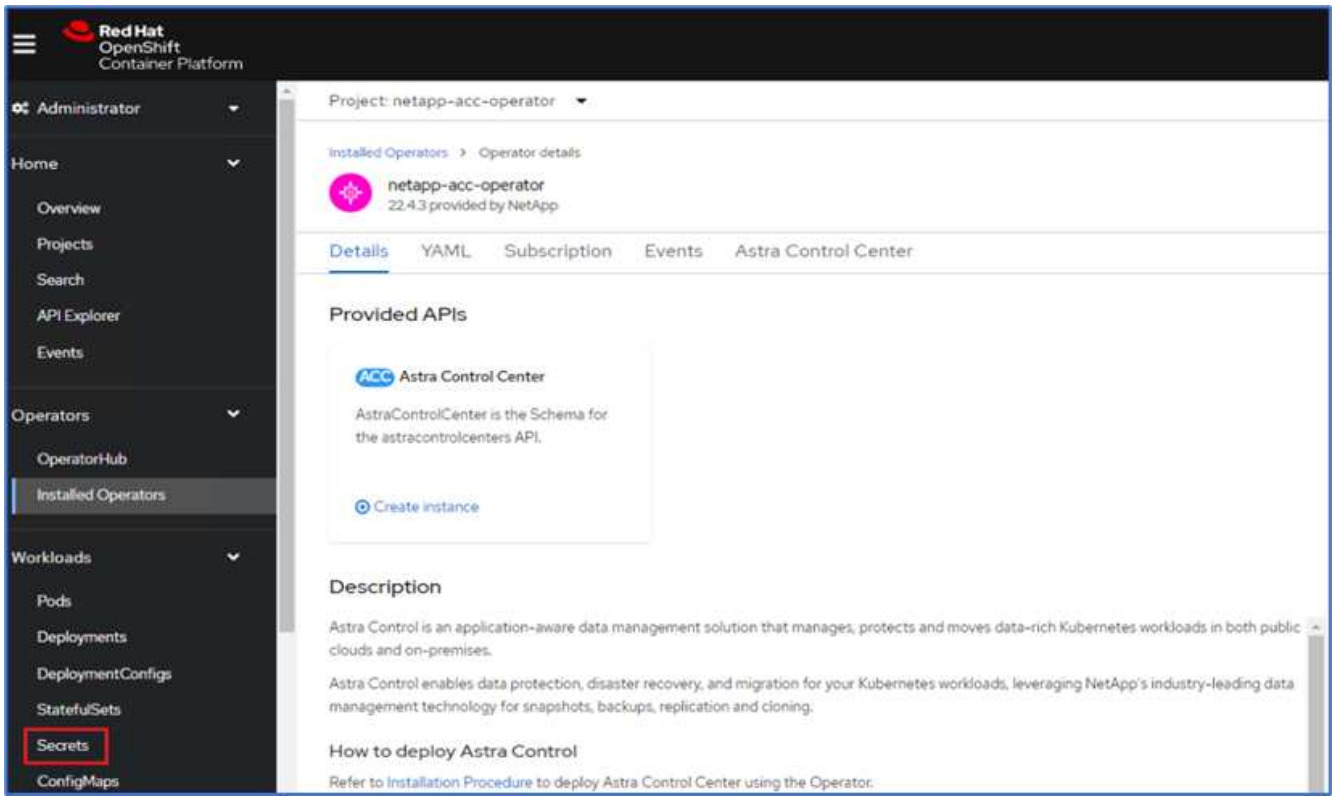
11. Approuver l'installation et attendre que l'opérateur soit installé.



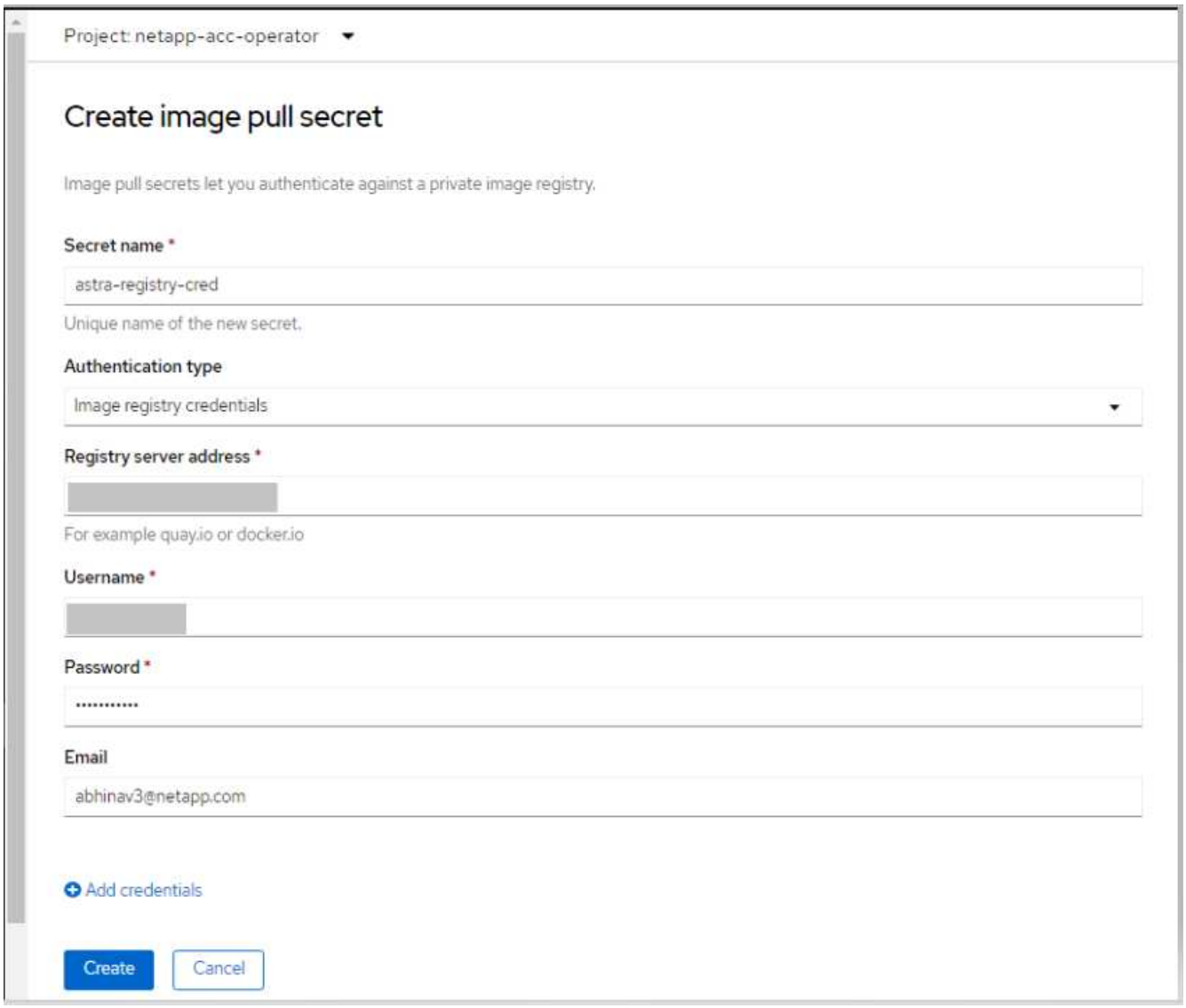
12. À ce stade, l'opérateur est installé avec succès et prêt à l'emploi. Cliquez sur Afficher l'opérateur pour démarrer l'installation du centre de contrôle Astra.



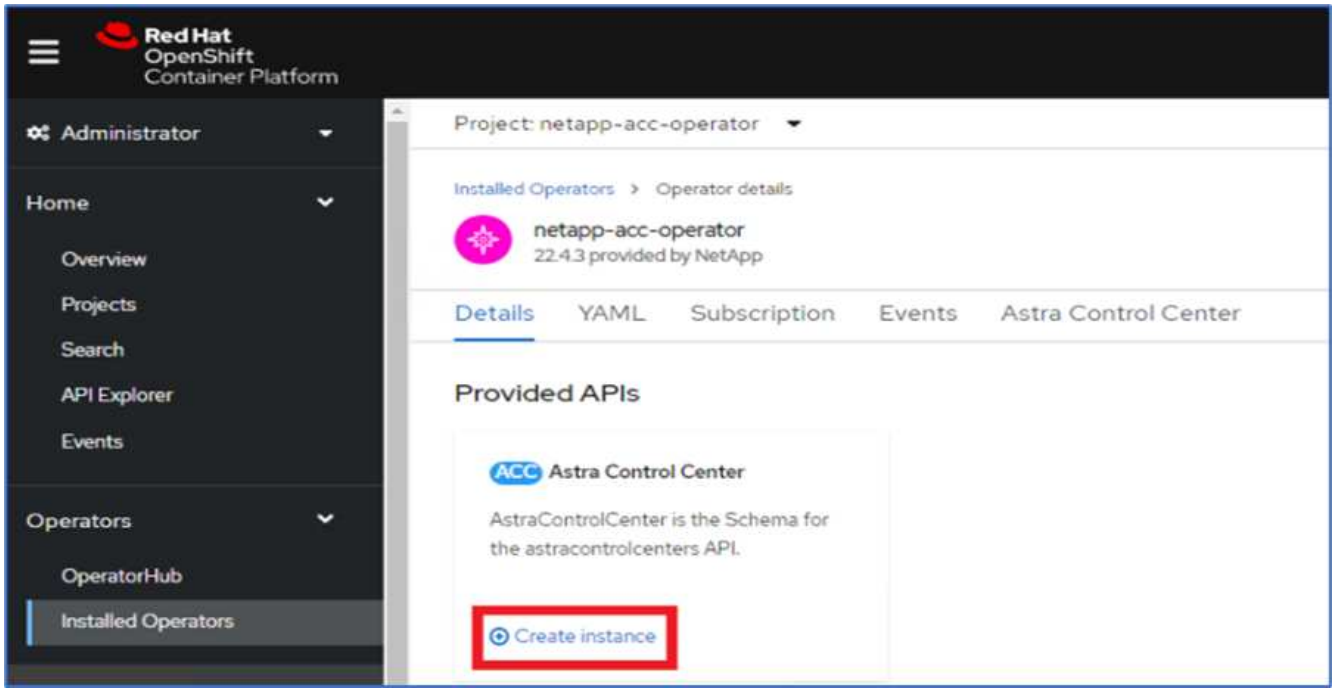
13. Avant d'installer Astra Control Center, créez le secret pour télécharger des images Astra à partir du registre Docker que vous avez poussé plus tôt.



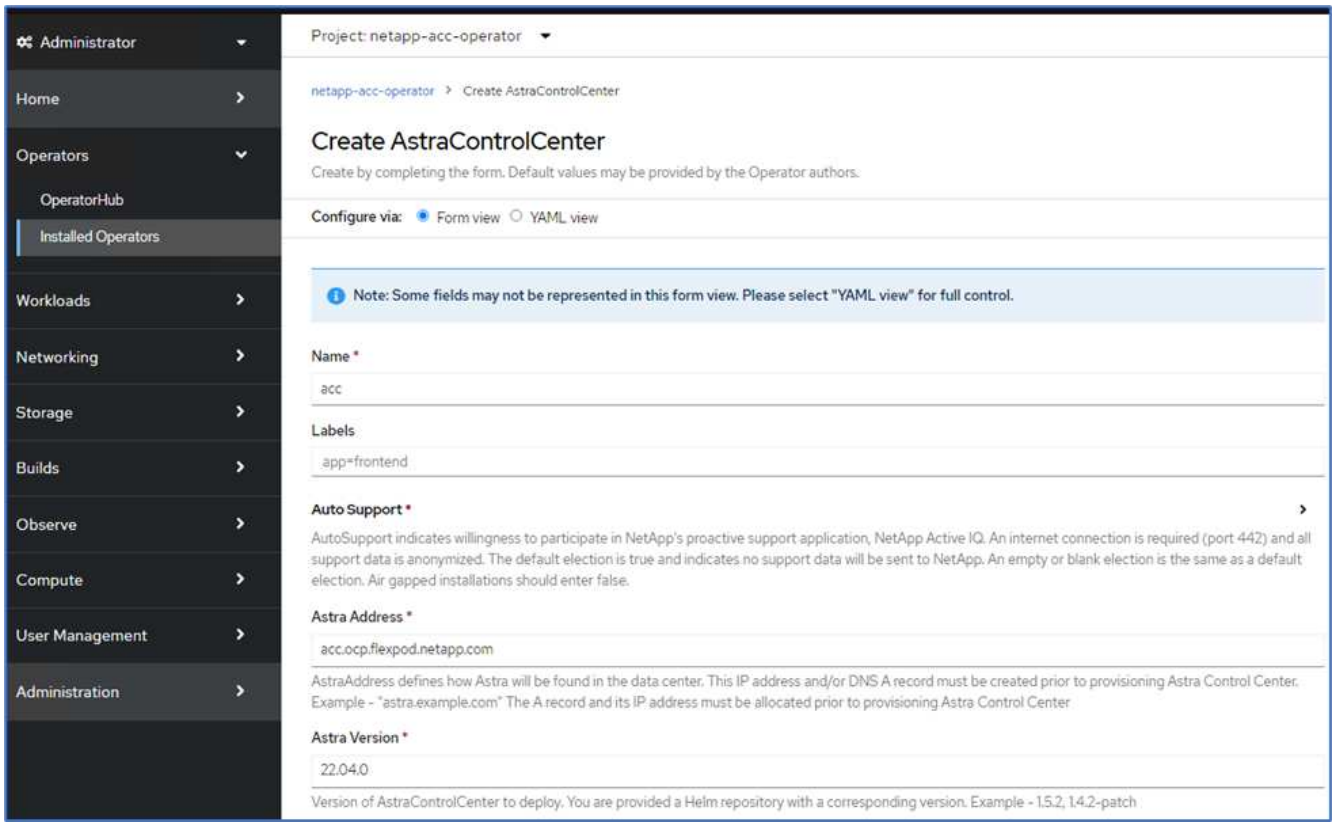
14. Pour extraire les images du centre de contrôle Astra de votre repo privé Docker, créez un secret dans le `netapp-acc-operator` espace de noms. Ce nom secret est fourni dans le manifeste YAML du Centre de contrôle Astra dans une étape ultérieure.



15. Dans le menu latéral, sélectionnez opérateurs > opérateurs installés et cliquez sur Créer une instance dans la section API fournie.



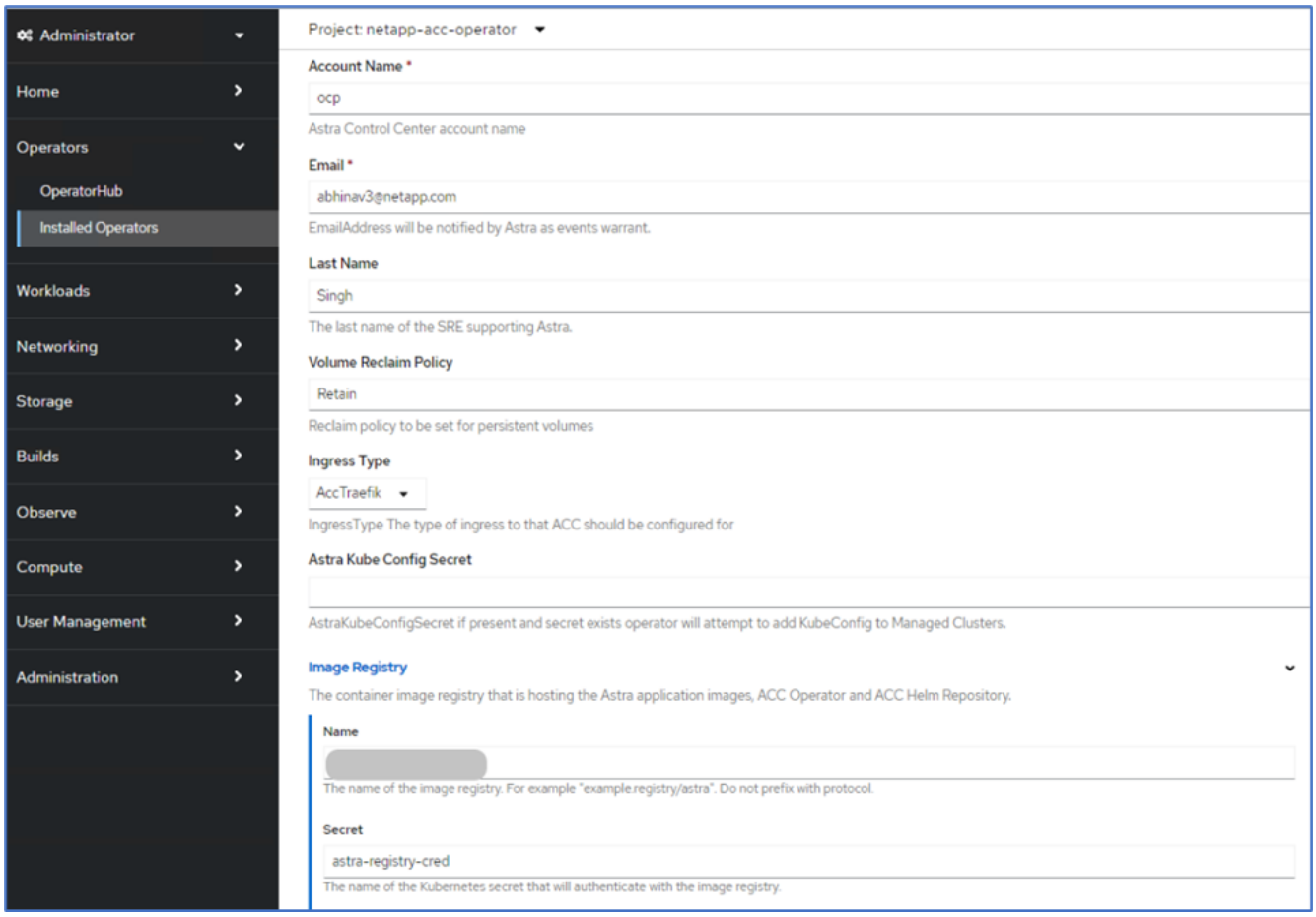
16. Remplissez le formulaire Create AstrakControlCenter. Indiquez le nom, l'adresse Astra et la version Astra.



Sous adresse Astra, indiquez l'adresse FQDN pour Astra Control Center. Cette adresse permet d'accéder à la console Web Astra Control Center. Le FQDN doit également se résoudre à un réseau IP accessible et doit être configuré dans le DNS.

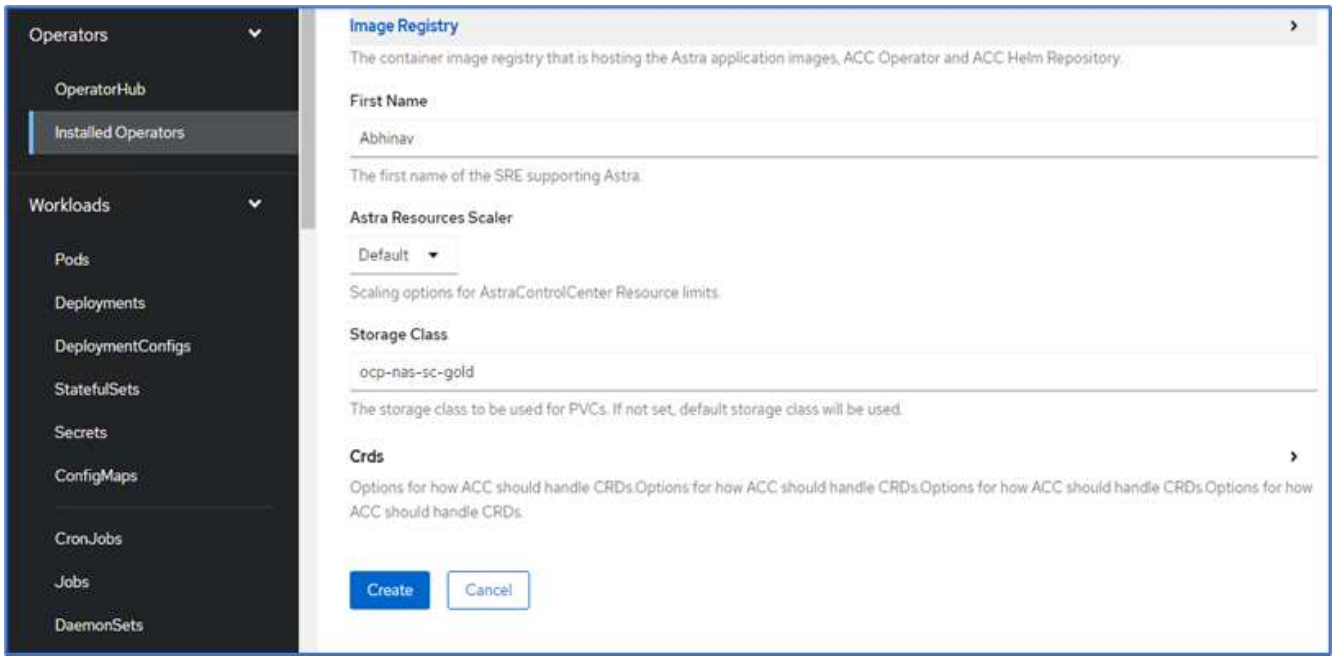
17. Entrez un nom de compte, une adresse e-mail, un nom d'administrateur et conservez la stratégie de récupération du volume par défaut. Si vous utilisez un équilibreur de charge, définissez le Type d'entrée

sur `AccTraefik`. Sinon, sélectionnez générique pour `Ingress.Controller`. Sous Registre d'images, entrez le chemin et le secret du registre d'images du conteneur.

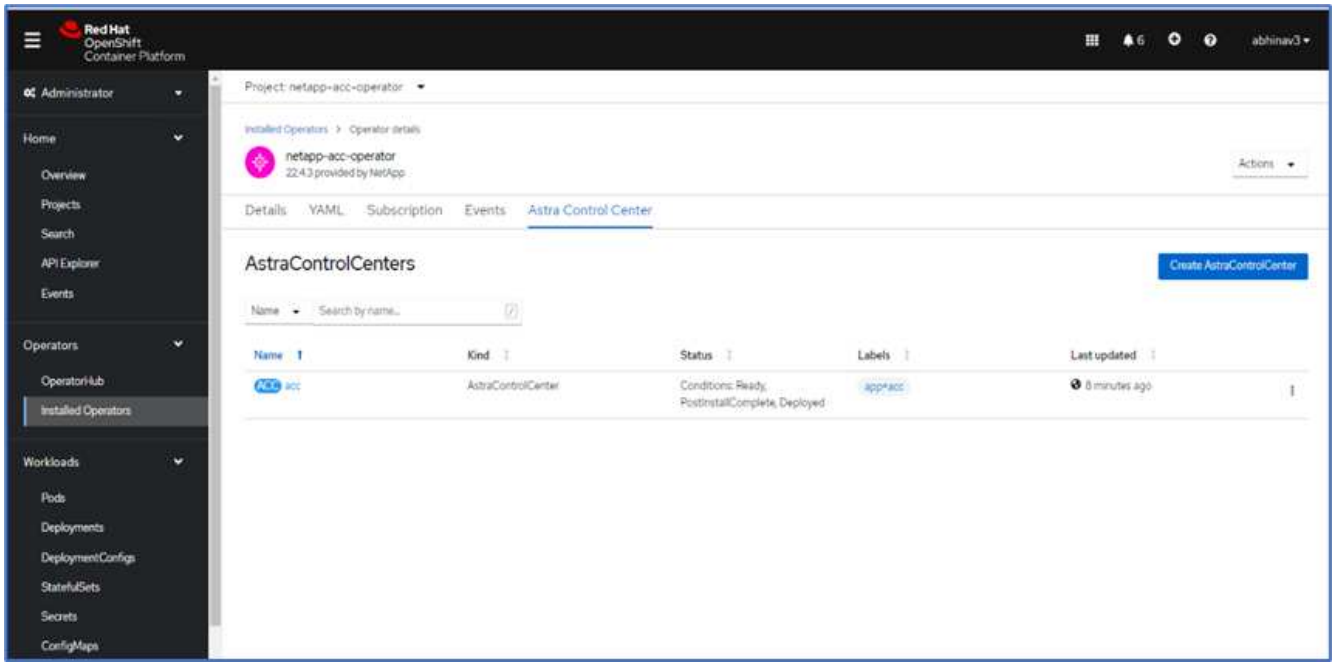


Dans cette solution, l'équilibreur de charge Metallb est utilisé. Par conséquent, le type d'entrée est AccTraefik. Cela expose la passerelle Ttrafik Astra Control Center en tant que service Kubernetes de type LoadBalancer.

18. Entrez le prénom de l'administrateur, configurez la mise à l'échelle des ressources et fournissez la classe de stockage. Cliquez sur Créer .



L'état de l'instance Astra Control Center doit passer de déploiement à prêt.



19. Vérifiez que tous les composants du système ont été correctement installés et que tous les modules fonctionnent.

```
root@abhinav-ansible# oc get pods -n netapp-acc-operator
NAME                                               READY   STATUS
RESTARTS   AGE
acc-helm-repo-77745b49b5-7zg2v                     1/1     Running   0
10m
acc-operator-controller-manager-5c656c44c6-tqnmn   2/2     Running   0
13m
```

```
activity-589c6d59f4-x2sfs                          1/1     Running   0
6m4s
api-token-authentication-4q5lj                     1/1     Running   0
5m26s
api-token-authentication-pzptd                     1/1     Running   0
5m27s
api-token-authentication-tbtg6                     1/1     Running   0
5m27s
asup-669df8d49-qps54                               1/1     Running   0
5m26s
authentication-5867c5f56f-dnpp2                    1/1     Running   0
3m54s
bucketservice-85495bc475-5zcc5                     1/1     Running   0
5m55s
cert-manager-67f486bbc6-txhh6                      1/1     Running   0
9m5s
cert-manager-cainjector-75959db744-4l5p5           1/1     Running   0
9m6s
cert-manager-webhook-765556b869-g6wdf              1/1     Running   0
9m6s
cloud-extension-5d595f85f-txrfl                    1/1     Running   0
5m27s
cloud-insights-service-674649567b-5s4wd            1/1     Running   0
5m49s
composite-compute-6b58d48c69-46vhc                 1/1     Running   0
6m11s
composite-volume-6d447fd959-chnrt                  1/1     Running   0
5m27s
credentials-66668f8ddd-8qc5b                       1/1     Running   0
7m20s
entitlement-fd6fc5c58-wxnmh                        1/1     Running   0
6m20s
features-756bbb7c7c-rgcrm                          1/1     Running   0
5m26s
fluent-bit-ds-278pg                                1/1     Running   0
3m35s
fluent-bit-ds-5pqc6                                1/1     Running   0
3m35s
fluent-bit-ds-8l7cq                                1/1     Running   0
3m35s
fluent-bit-ds-9qbft                                1/1     Running   0
3m35s
fluent-bit-ds-nj475                                1/1     Running   0
3m35s
fluent-bit-ds-x9pd8                                1/1     Running   0
3m35s
```

```
graphql-server-698d6f4bf-kftwc                    1/1     Running   0
3m20s
identity-5d4f4c87c9-wjz6c                         1/1     Running   0
6m27s
influxdb2-0                                       1/1     Running   0
9m33s
krakend-657d44bf54-8cb56                          1/1     Running   0
3m21s
license-594bbdc-rghdg                             1/1     Running   0
6m28s
login-ui-6c65fbbbd4-jg8wz                         1/1     Running   0
3m17s
loki-0                                            1/1     Running   0
9m30s
metrics-facade-75575f69d7-hnlk6                   1/1     Running   0
6m10s
monitoring-operator-65dff79cfb-z78vk              2/2     Running   0
3m47s
nats-0                                            1/1     Running   0
10m
nats-1                                            1/1     Running   0
9m43s
nats-2                                            1/1     Running   0
9m23s
nautilus-7bb469f857-4hlc6                         1/1     Running   0
6m3s
nautilus-7bb469f857-vz94m                         1/1     Running   0
4m42s
openapi-8586db4bcd-gwwvf                          1/1     Running   0
5m41s
packages-6bdb949cfb-nrq8l                         1/1     Running   0
6m35s
polaris-consul-consul-server-0                    1/1     Running   0
9m22s
polaris-consul-consul-server-1                    1/1     Running   0
9m22s
polaris-consul-consul-server-2                    1/1     Running   0
9m22s
polaris-mongodb-0                                 2/2     Running   0
9m22s
polaris-mongodb-1                                 2/2     Running   0
8m58s
polaris-mongodb-2                                 2/2     Running   0
8m34s
polaris-ui-5df7687dbd-trcnf                       1/1     Running   0
3m18s
```

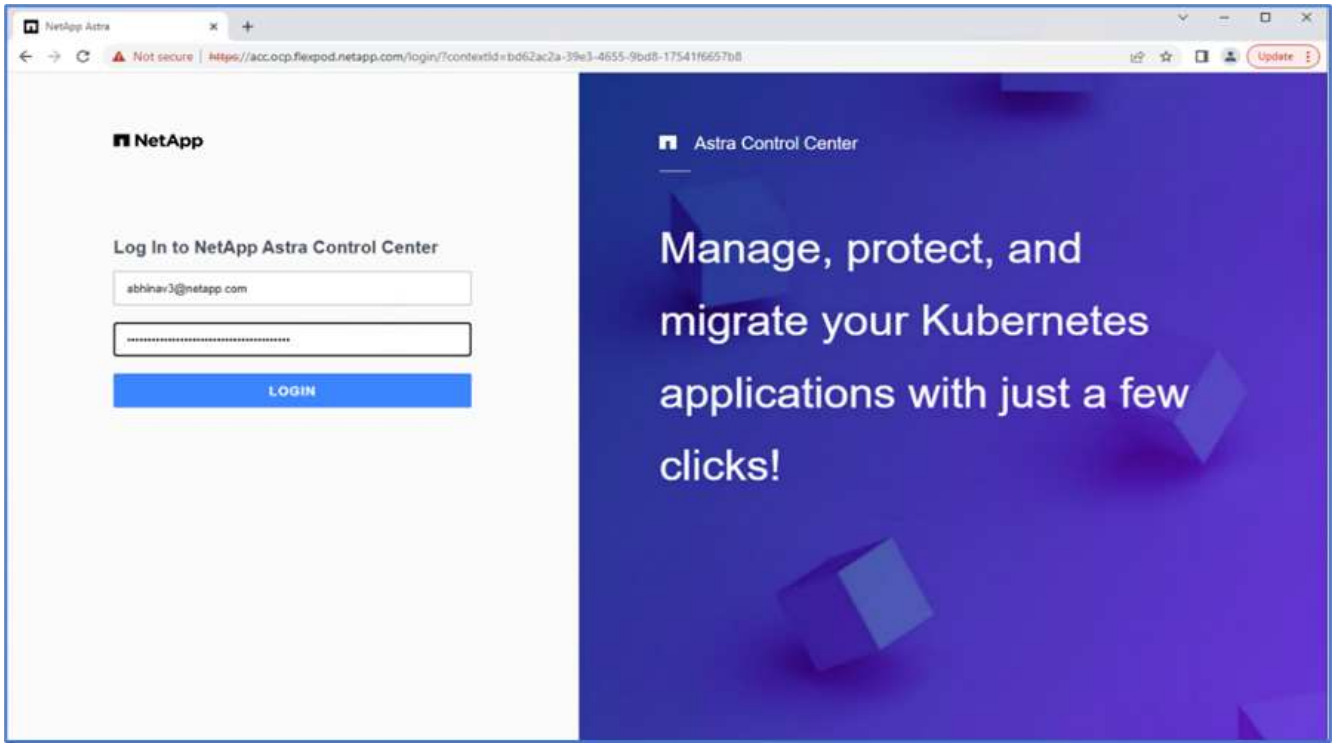
```
polaris-vault-0                                   1/1     Running   0
9m18s
polaris-vault-1                                   1/1     Running   0
9m18s
polaris-vault-2                                   1/1     Running   0
9m18s
public-metrics-7b96476f64-j88bw                   1/1     Running   0
5m48s
storage-backend-metrics-5fd6d7cd9c-vcb4j          1/1     Running   0
5m59s
storage-provider-bb85ff965-m7qrq                  1/1     Running   0
5m25s
telegraf-ds-4zqgz                                 1/1     Running   0
3m36s
telegraf-ds-cp9x4                                 1/1     Running   0
3m36s
telegraf-ds-h4n59                                 1/1     Running   0
3m36s
telegraf-ds-jnp2q                                 1/1     Running   0
3m36s
telegraf-ds-pdz5j                                 1/1     Running   0
3m36s
telegraf-ds-znqtp                                 1/1     Running   0
3m36s
telegraf-rs-rt64j                                 1/1     Running   0
3m36s
telemetry-service-7dd9c74bfc-sfkzt                1/1     Running   0
6m19s
tenancy-d878b7fb6-wf8x9                           1/1     Running   0
6m37s
traefik-6548496576-5v2g6                          1/1     Running   0
98s
traefik-6548496576-g82pq                          1/1     Running   0
3m8s
traefik-6548496576-psn49                          1/1     Running   0
38s
traefik-6548496576-qrkfd                          1/1     Running   0
2m53s
traefik-6548496576-srs6r                          1/1     Running   0
98s
trident-svc-679856c67-78kbt                       1/1     Running   0
5m27s
vault-controller-747d664964-xmn6c                 1/1     Running   0
7m37s
```

Chaque pod doit avoir l'état en cours d'exécution. Le déploiement des modules du système peut prendre plusieurs minutes.

20. Lorsque tous les pods s'exécutent, exécutez la commande suivante pour récupérer le mot de passe à une seule fois. Dans la version YAML de la sortie, vérifiez le `status.deploymentState` pour la valeur déployée, puis copiez le `status.uuid` valeur. Le mot de passe est `ACC-` Suivi de la valeur UUID. (ACC-[UUID]).

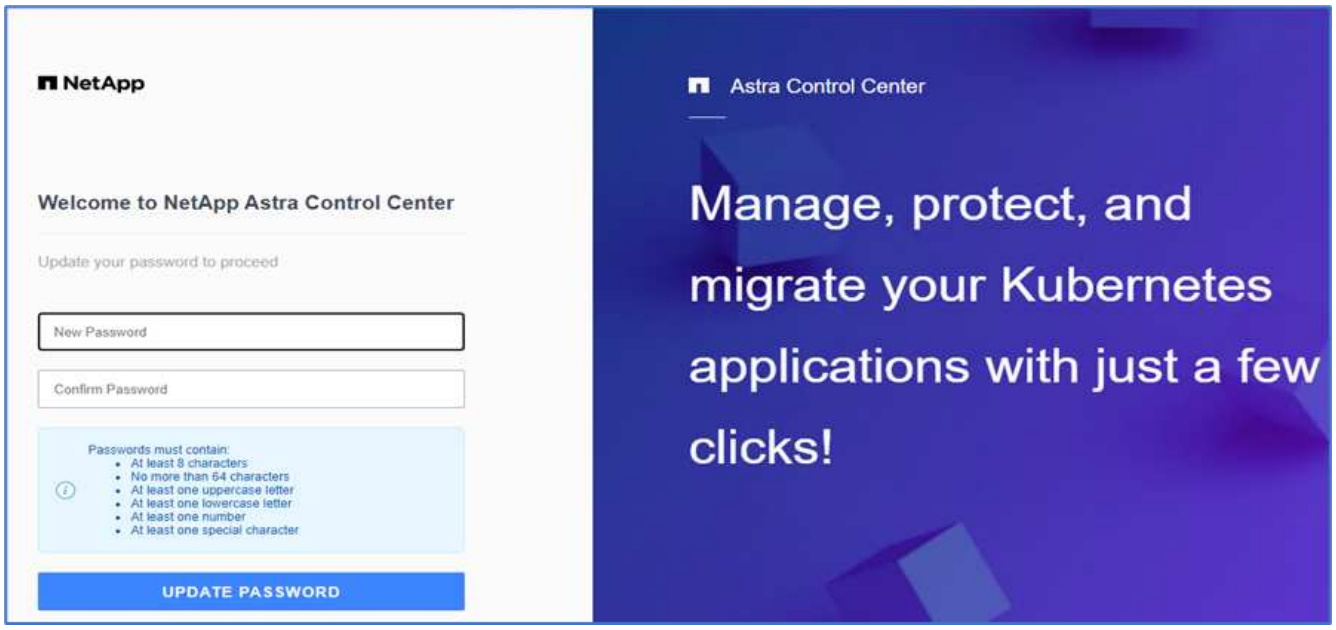
```
root@abhinav-ansible# oc get acc -o yaml -n netapp-acc-operator
```

21. Dans un navigateur, accédez à l'URL en utilisant le FQDN que vous avez fourni.
22. Connectez-vous à l'aide du nom d'utilisateur par défaut, à savoir l'adresse électronique fournie lors de l'installation et le mot de passe à usage unique ACC-[UUID].



Si vous saisissez trois fois un mot de passe incorrect, le compte administrateur est verrouillé pendant 15 minutes.

23. Modifiez le mot de passe et continuez.

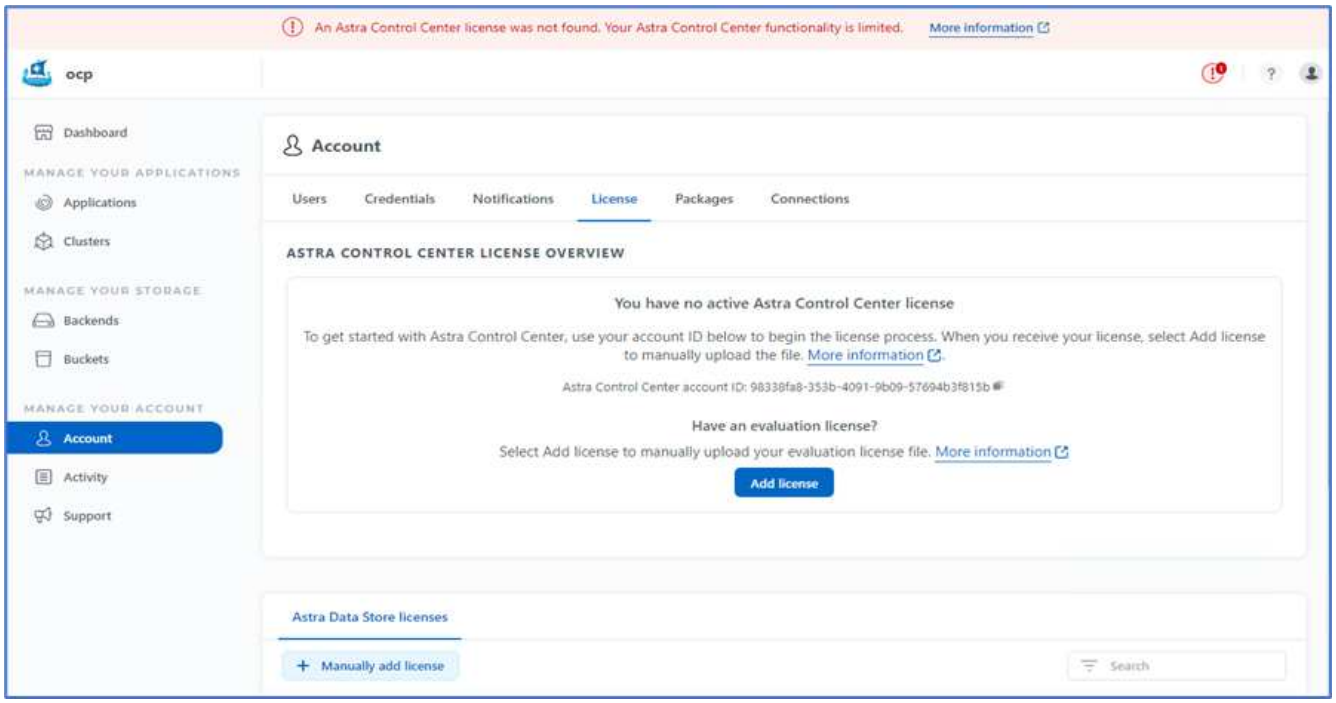


Pour en savoir plus sur l'installation du centre de contrôle Astra, consultez le "Présentation de l'installation du centre de contrôle Astra" page.

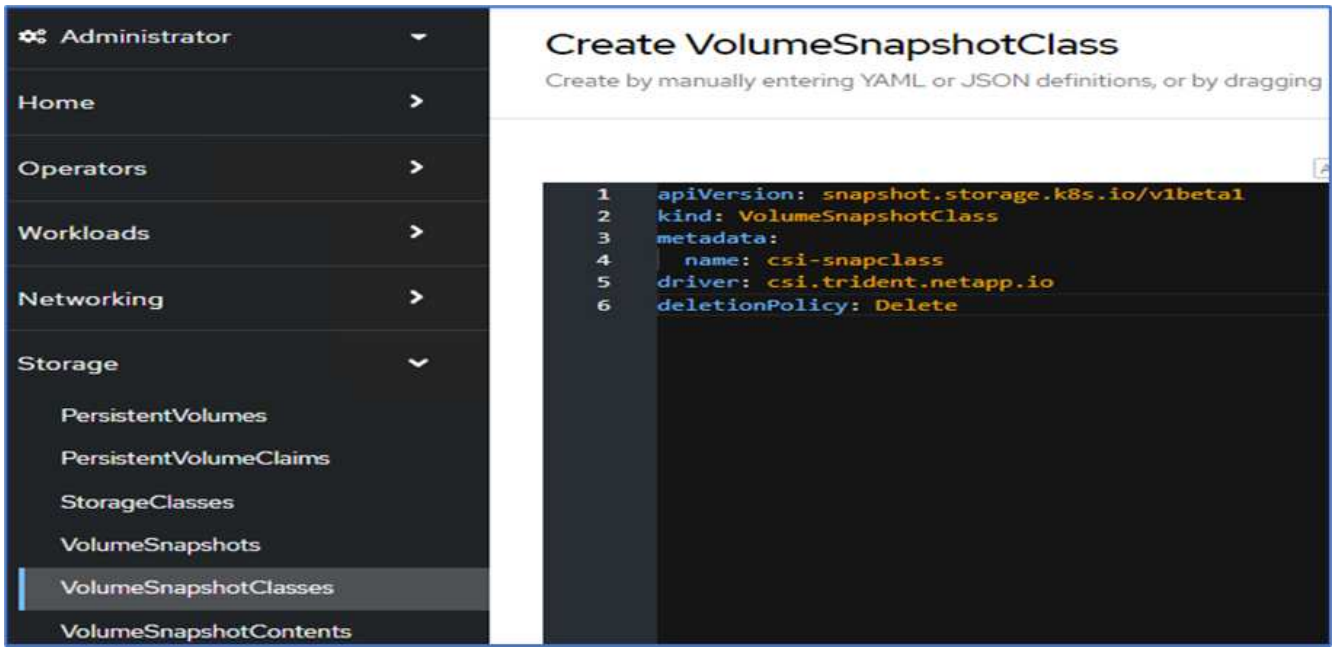
Configurer le centre de contrôle Astra

Une fois Astra Control Center installé, connectez-vous à l'interface utilisateur, téléchargez la licence, ajoutez des clusters, gérez le stockage et ajoutez des compartiments.

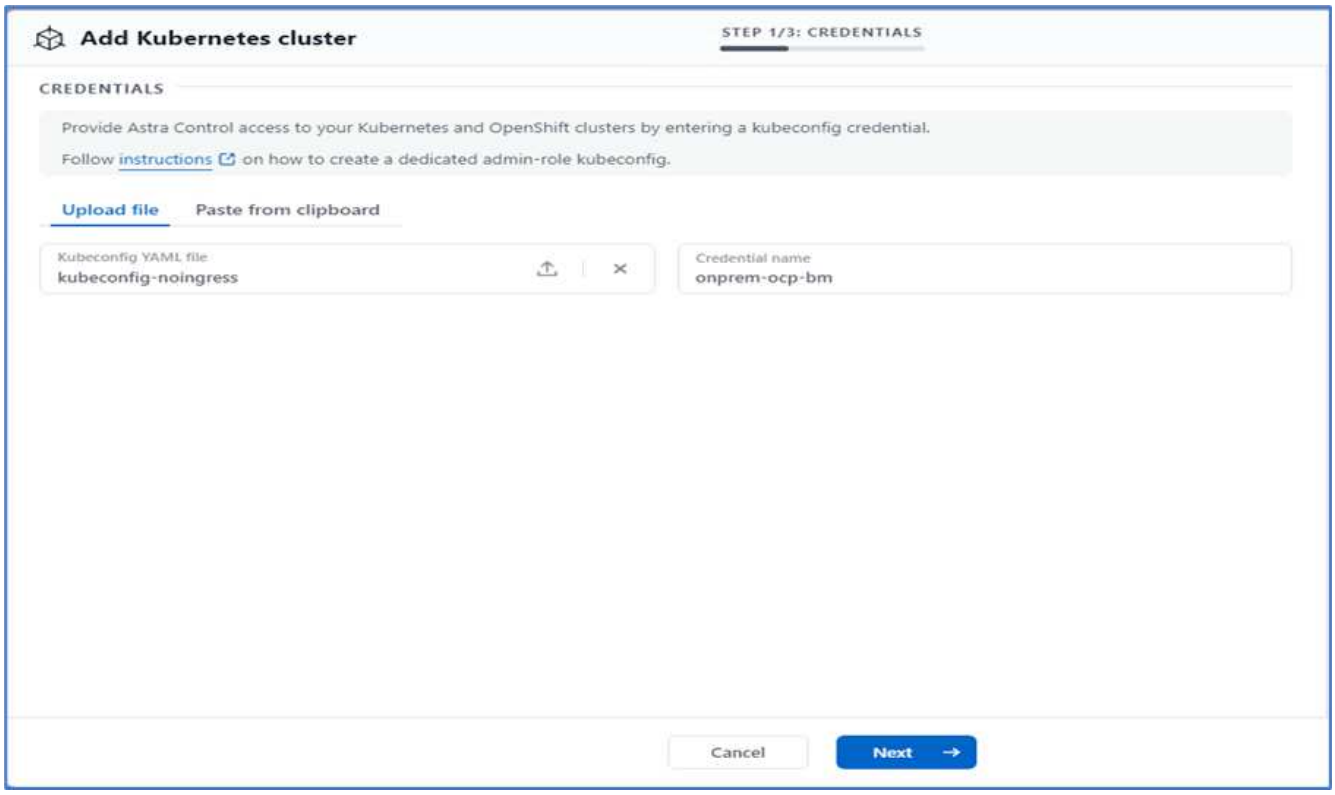
1. Sur la page d'accueil sous compte, accédez à l'onglet Licence et sélectionnez Ajouter une licence pour télécharger la licence Astra.



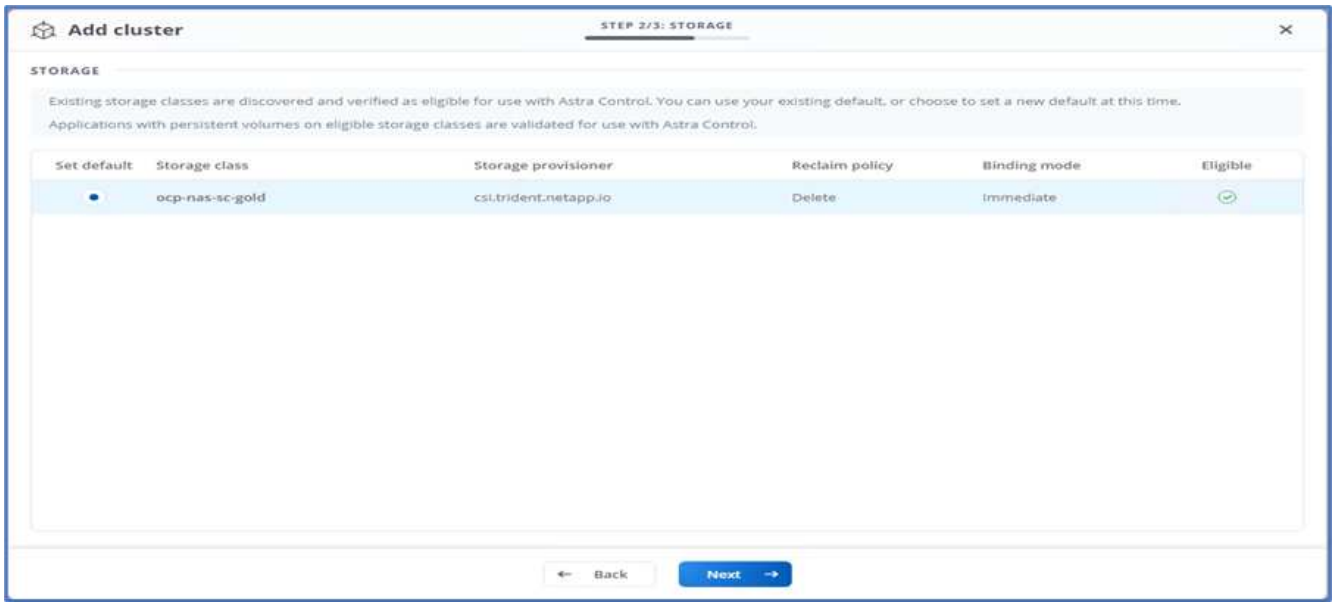
2. Avant d'ajouter le cluster OpenShift, créez une classe de snapshot de volume Astra Trident à partir de la console web OpenShift. La classe de snapshot de volume est configurée avec le `csi.trident.netapp.io` conducteur.



3. Pour ajouter le cluster Kubernetes, accédez à clusters sur la page d'accueil et cliquez sur Ajouter un cluster Kubernetes. Téléchargez ensuite le `kubeconfig` fichier du cluster et indiquez un nom d'identifiant. Cliquez sur Suivant.



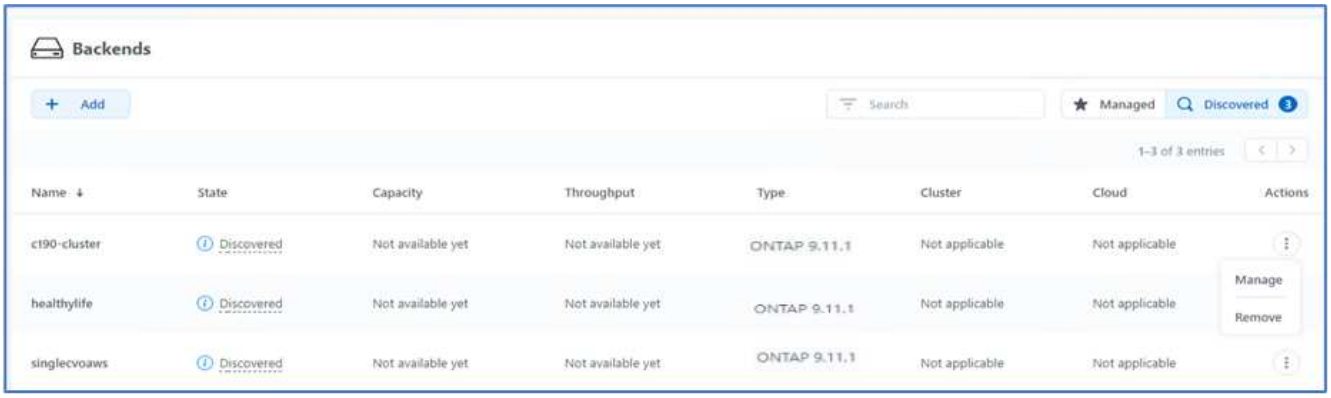
4. Les classes de stockage existantes sont automatiquement découvertes. Sélectionnez la classe de stockage par défaut, cliquez sur Suivant, puis sur Ajouter un cluster.



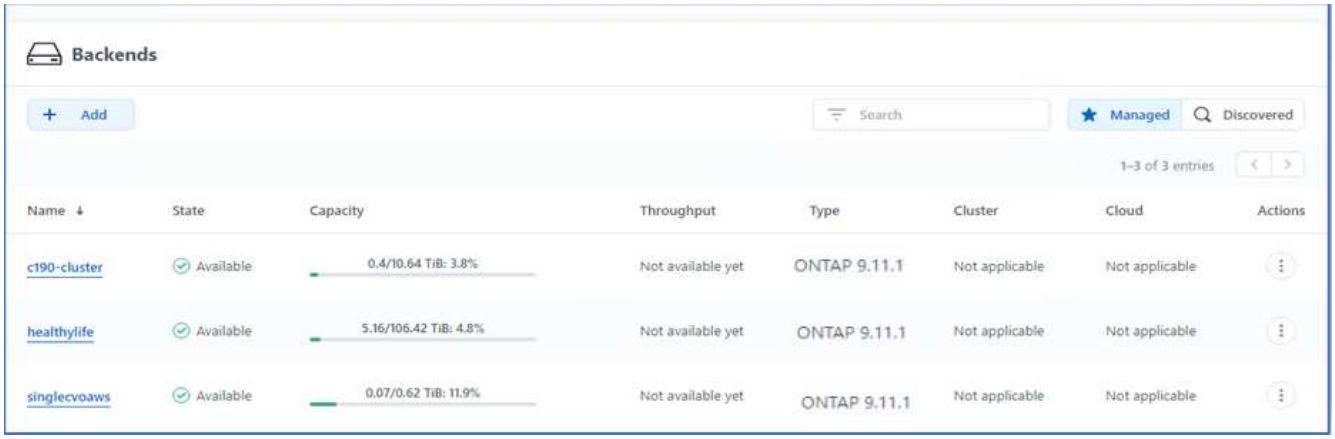
5. Le cluster est ajouté en quelques minutes. Pour ajouter d'autres clusters OpenShift Container Platform, répétez les étapes 1 à 4.

> Pour ajouter un environnement opérationnel OpenShift supplémentaire en tant que ressource de calcul gérée, assurez-vous qu'Astra Trident "Objets VolumeSnapshotClass" sont définis.

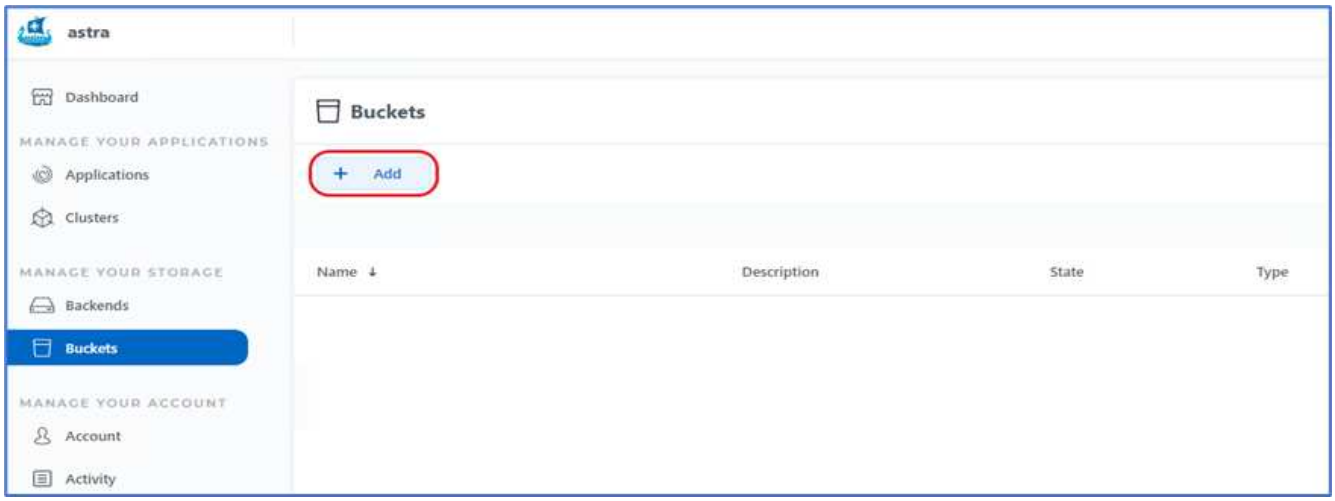
6. Pour gérer le stockage, accédez à Backends, cliquez sur les trois points sous actions par rapport au back-end que vous souhaitez gérer. Cliquez sur gérer.



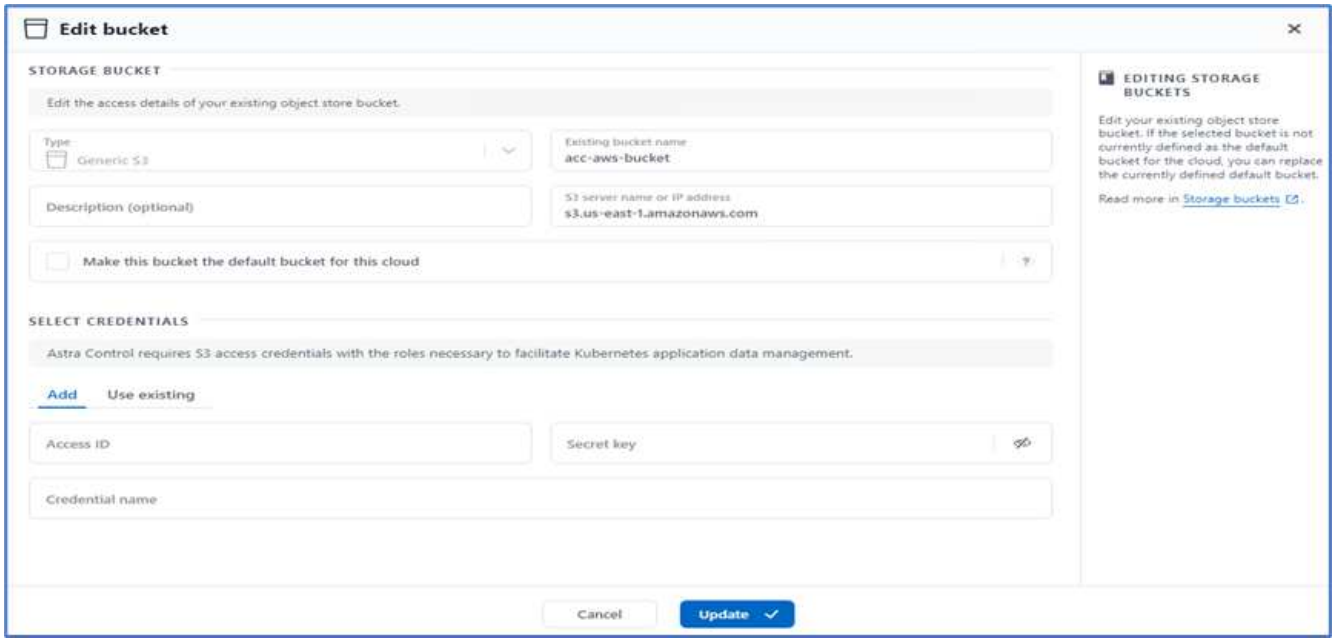
7. Indiquez les identifiants ONTAP et cliquez sur Next (Suivant). Vérifiez les informations et cliquez sur géré. Le système back-end doit être semblable à l'exemple suivant.



8. Pour ajouter un godet à la commande Astra, sélectionnez godets et cliquez sur Ajouter.

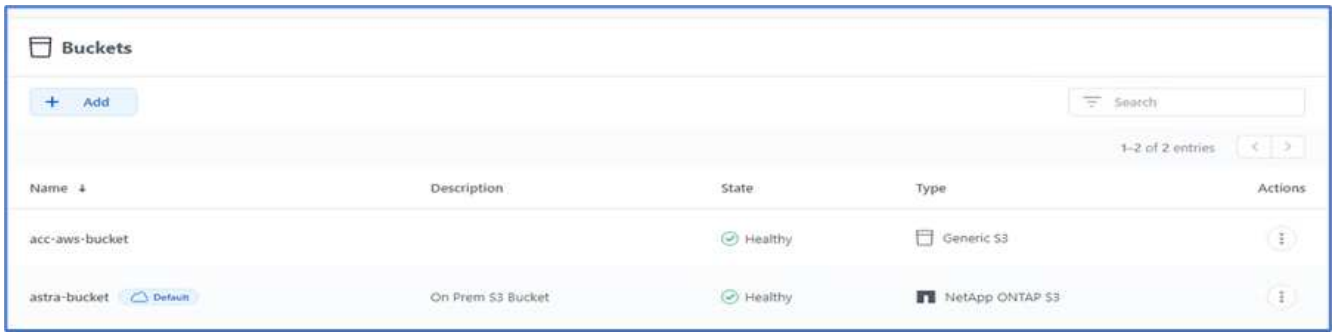


9. Sélectionnez le type de compartiment et indiquez le nom du compartiment, le nom du serveur S3 ou l'adresse IP et les identifiants S3. Cliquez sur mettre à jour.



Dans cette solution, des compartiments AWS S3 et ONTAP S3 sont tous deux utilisés. Vous pouvez également utiliser StorageGRID.

L'état du godet doit être sain.



Dans le cadre de l'enregistrement de clusters Kubernetes avec Astra Control Center pour la gestion des données intégrant la cohérence applicative, Astra Control crée automatiquement des liaisons de rôles et un espace de noms de contrôle NetApp qui contrôle la collecte de metrics et de journaux à partir des pods d'applications et des nœuds workers. Définir l'une des classes de stockage ONTAP par défaut prises en charge.

Après vous "Ajoutez un cluster à la gestion Astra Control", Vous pouvez installer des applications sur le cluster (en dehors d'Astra Control), puis aller à la page applications d'Astra Control pour gérer les applications et leurs ressources. Pour en savoir plus sur la gestion des applications avec Astra, consultez le "Besoins en termes de gestion des applications".

"Ensuite : présentation de la validation de la solution."

Validation des solutions

Présentation

"Précédent : installation d'Astra Control Center sur OpenShift Container Platform."

Dans cette section, nous revisiterons la solution en incluant quelques cas d'utilisation :

- Restauration d'une application avec état d'une sauvegarde à distance vers un autre cluster OpenShift exécuté dans le cloud.
- Restauration d'une application avec état dans le même espace de noms du cluster OpenShift
- Mobilité des applications par clonage d'un système FlexPod (OpenShift Container Platform bare Metal) vers un autre système FlexPod (OpenShift Container Platform sur VMware).

En particulier, seules quelques utilisations ont été validées dans cette solution. Cette validation ne correspond en aucune façon à l'ensemble des fonctionnalités d'Astra Control Center.

"Ensuite : restauration des applications avec sauvegardes distantes."

Restauration d'applications avec sauvegardes distantes

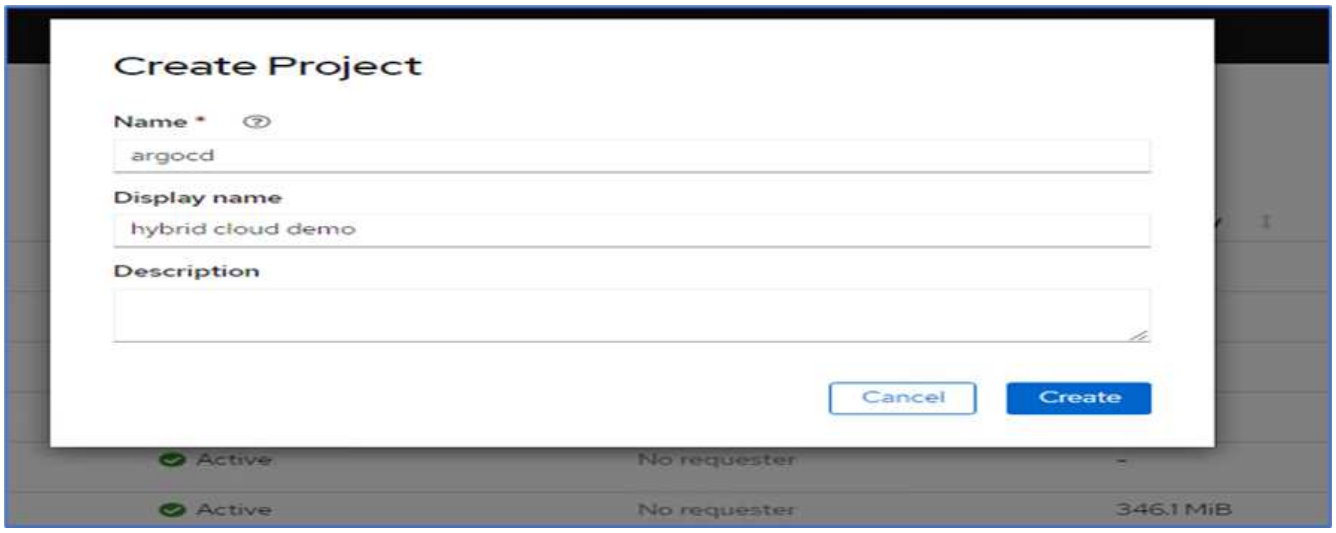
"Précédent : présentation de la validation de la solution."

Avec Astra, vous pouvez effectuer une sauvegarde complète et cohérente avec les applications qui permet de restaurer les données de votre application vers un autre cluster Kubernetes qui s'exécute dans un data Center sur site ou dans un cloud public.

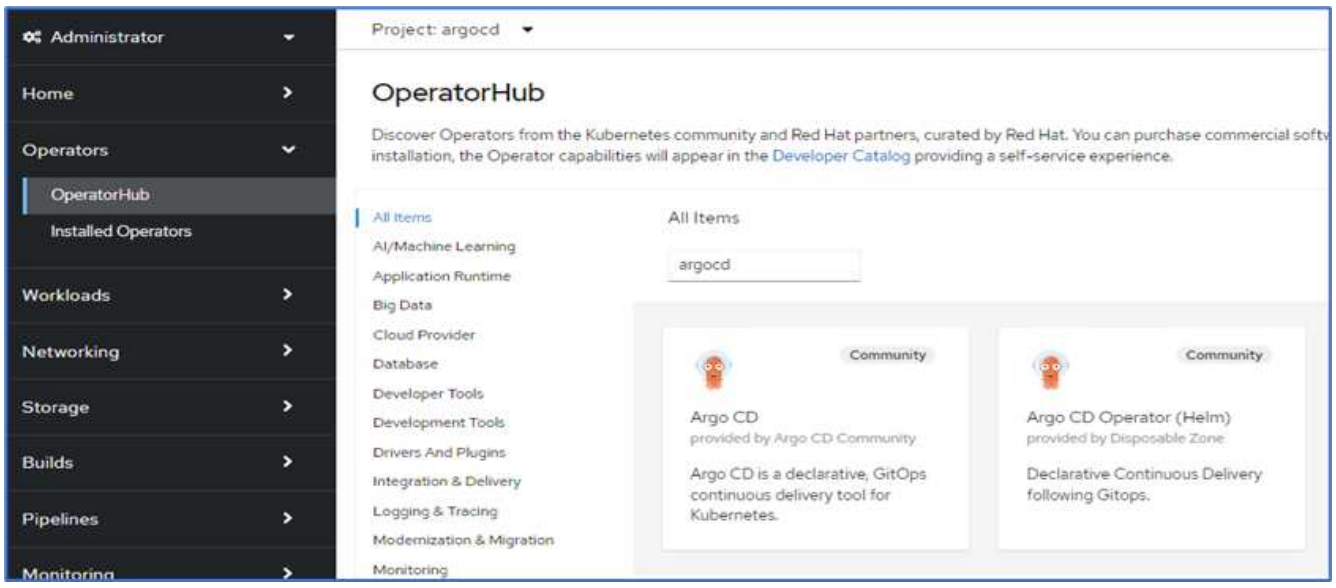
Pour valider la restauration d'application, simulez une défaillance sur site d'une application exécutée sur le système FlexPod et restaurez l'application sur un cluster K8s dans le cloud à l'aide d'une sauvegarde à distance.

L'exemple d'application est une application de liste de prix qui utilise MySQL pour la base de données. Pour automatiser le déploiement, nous avons utilisé le "CD Argo" outil. Argo CD est un outil de livraison continue déclaratif, GitOps.

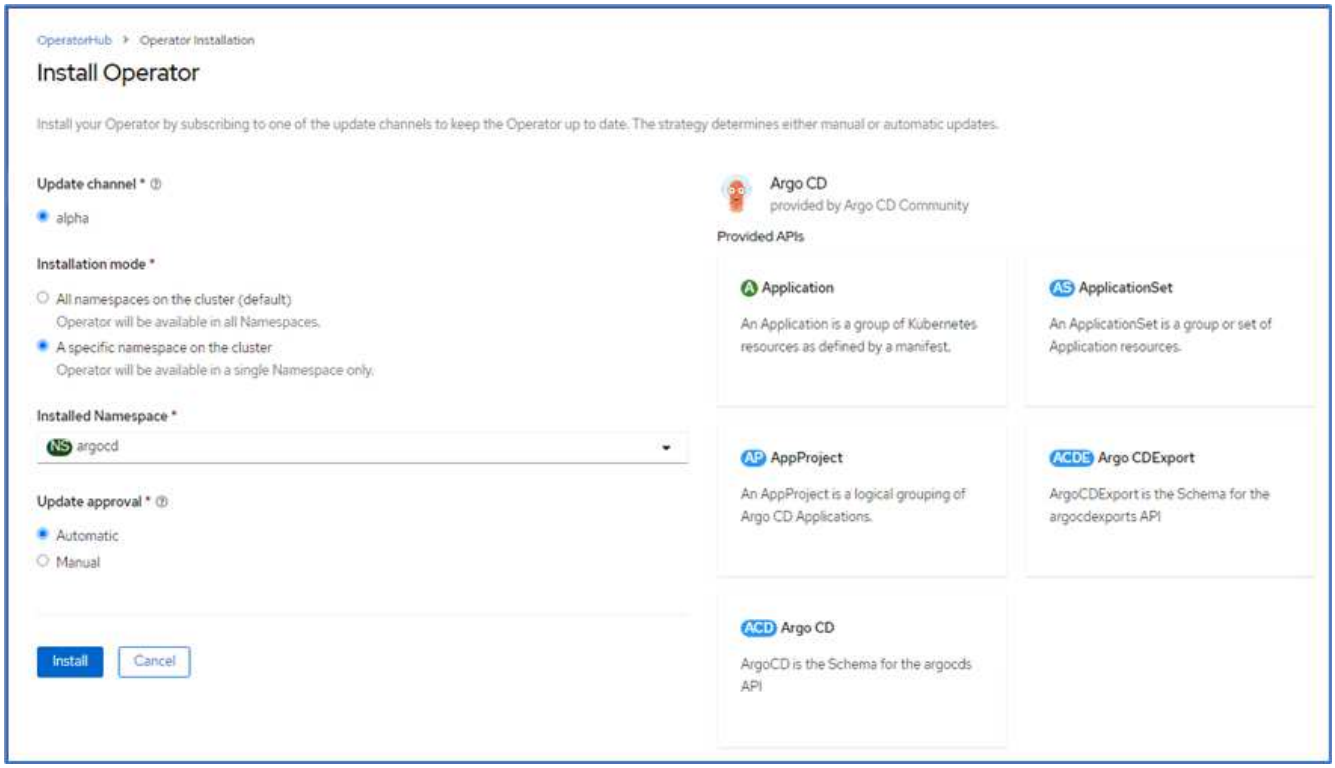
1. Connectez-vous au cluster OpenShift sur site et créez un nouveau projet sous son nom `argocd`.



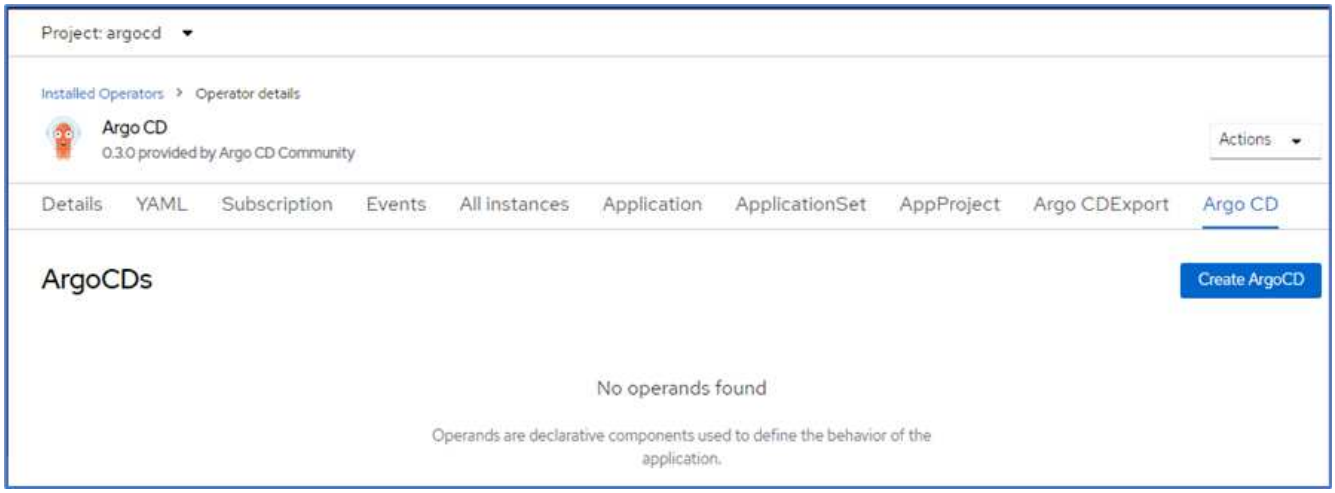
2. Dans OperatorHub, recherchez `argocd` Et sélectionnez opérateur du CD Argo.



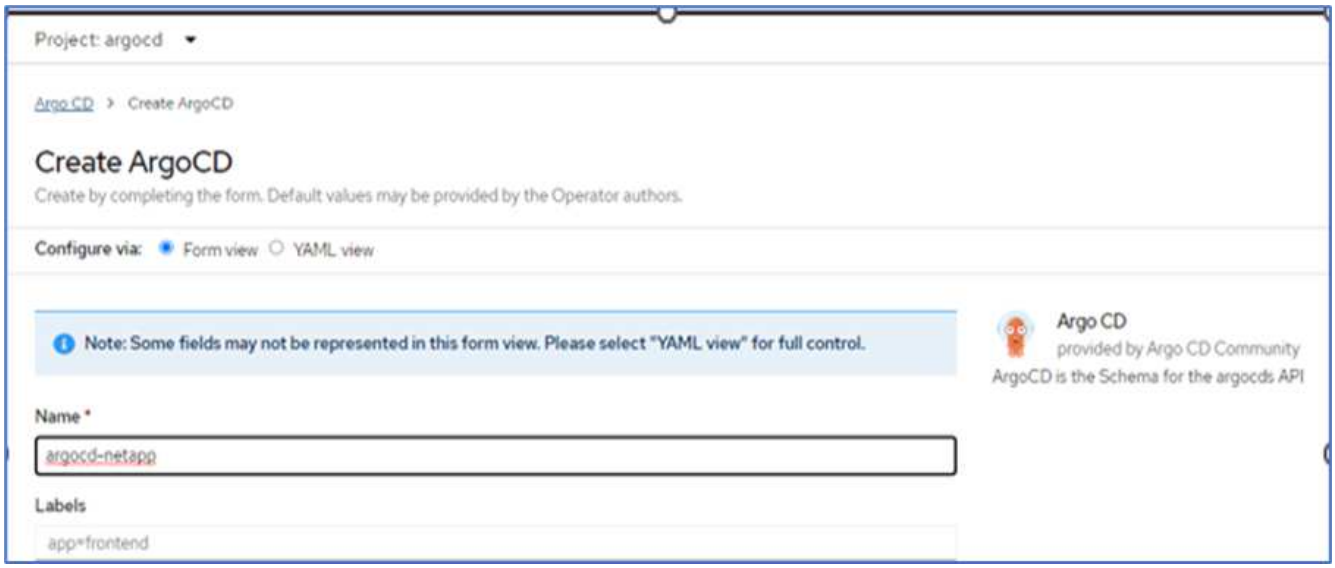
3. Installer l'opérateur dans le `argocd` espace de noms.



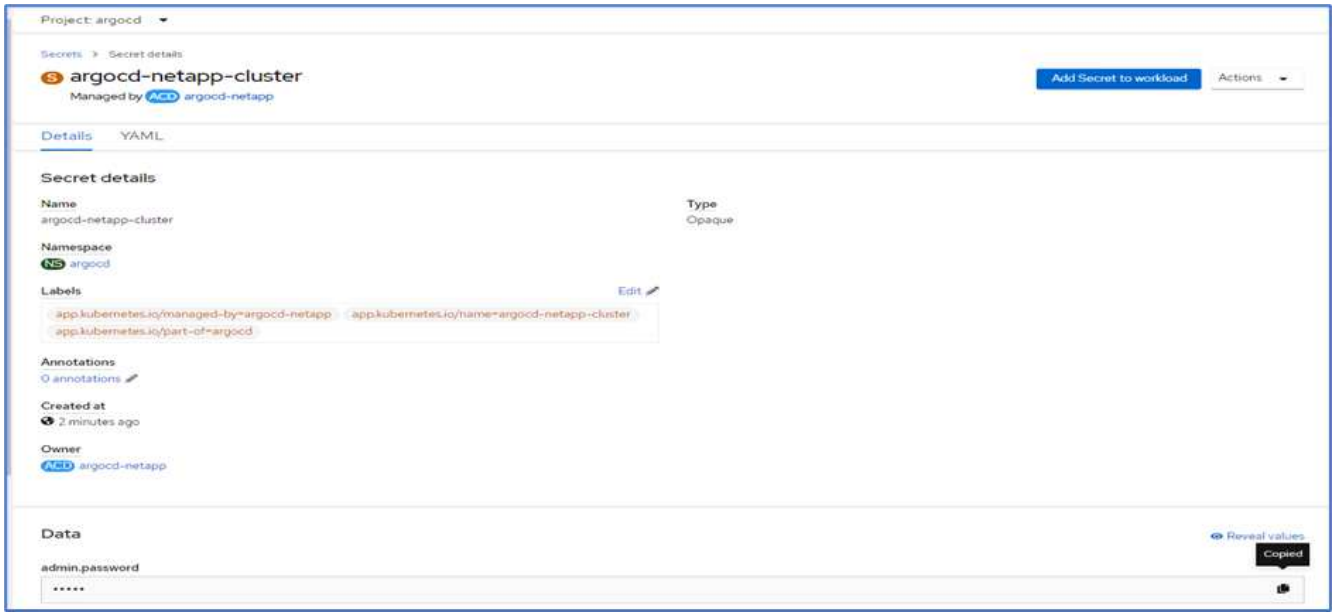
4. Accédez à l'opérateur et cliquez sur Créer un ArgoCD.



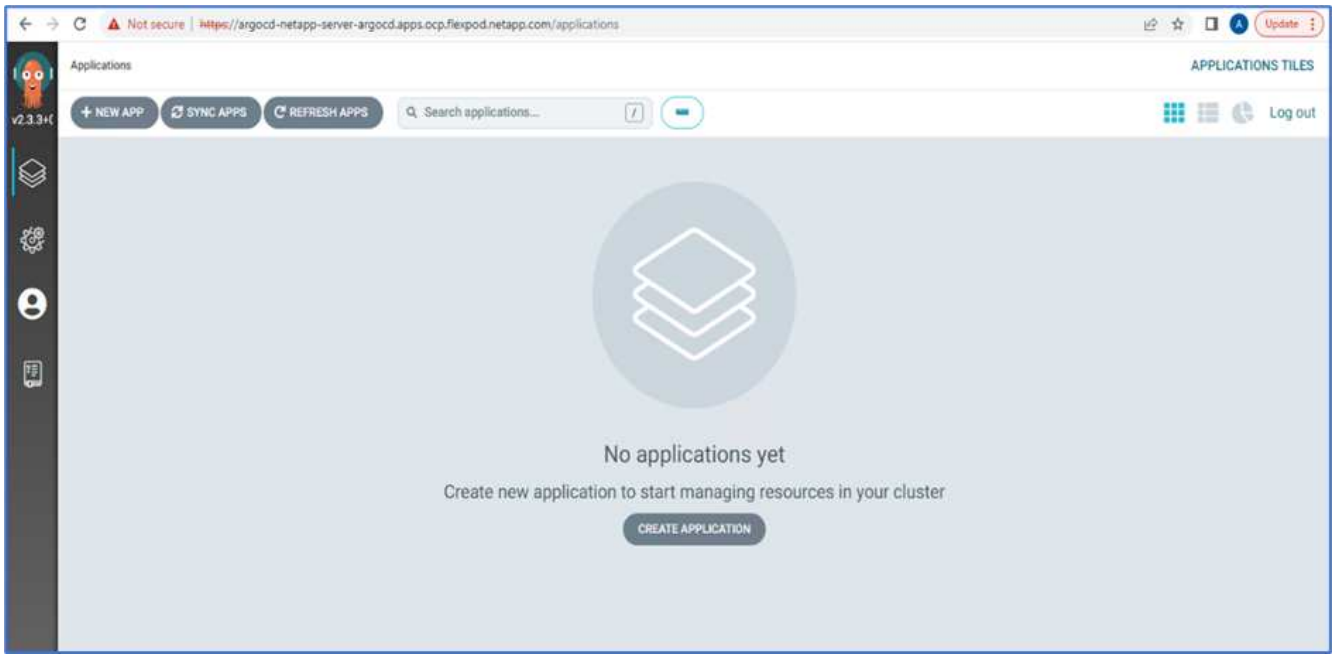
5. Pour déployer l'instance de CD Argo dans le `argocd` Donnez un nom au projet, puis cliquez sur Créer.



6. Pour vous connecter au CD Argo, l'utilisateur par défaut est admin et le mot de passe se trouve dans un fichier secret portant le nom `argocd-netapp-cluster`.



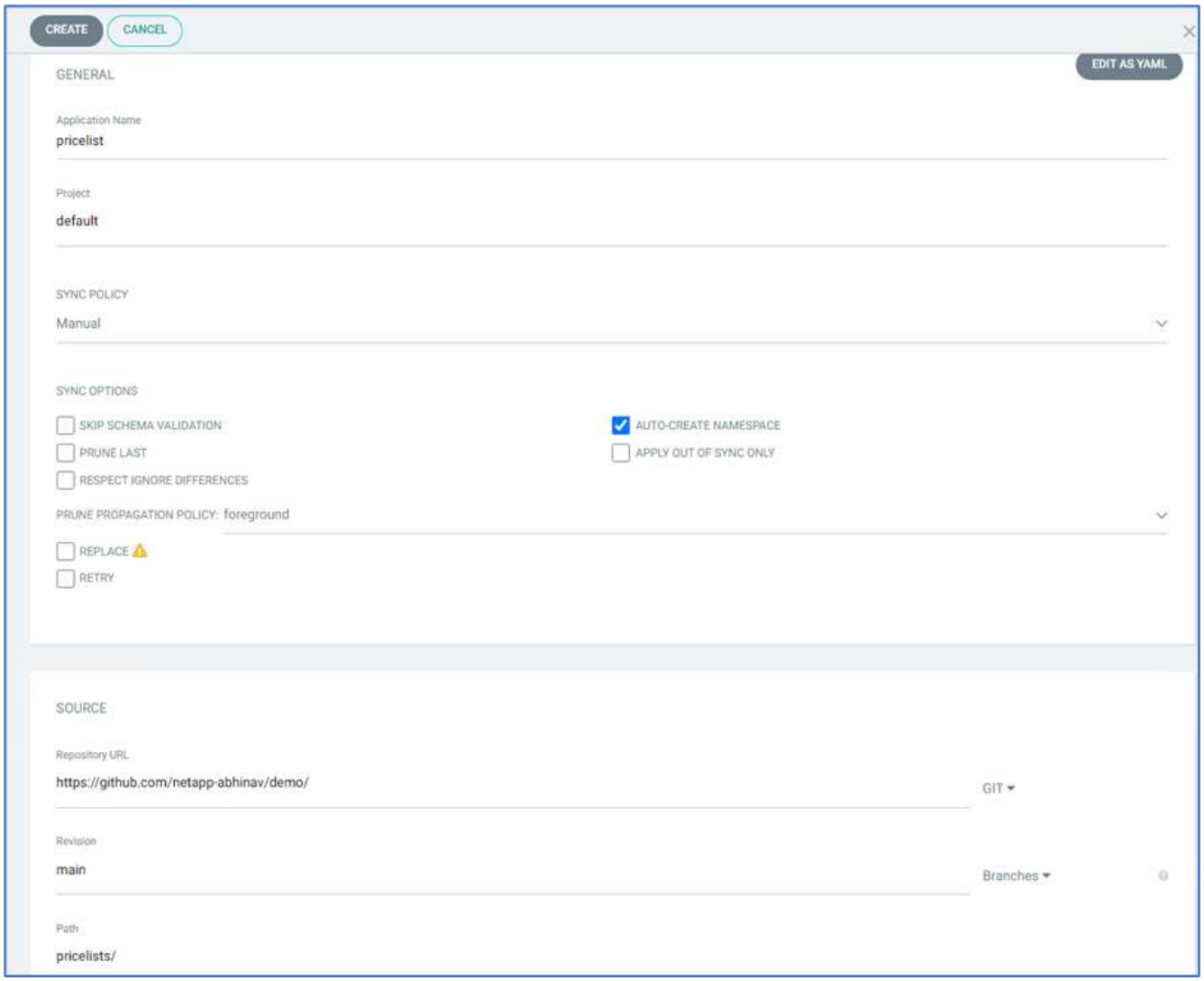
7. Dans le menu latéral, sélectionnez routes > emplacement et cliquez sur l'URL de l' `argocd` itinéraires. Entrez le nom d'utilisateur et le mot de passe.



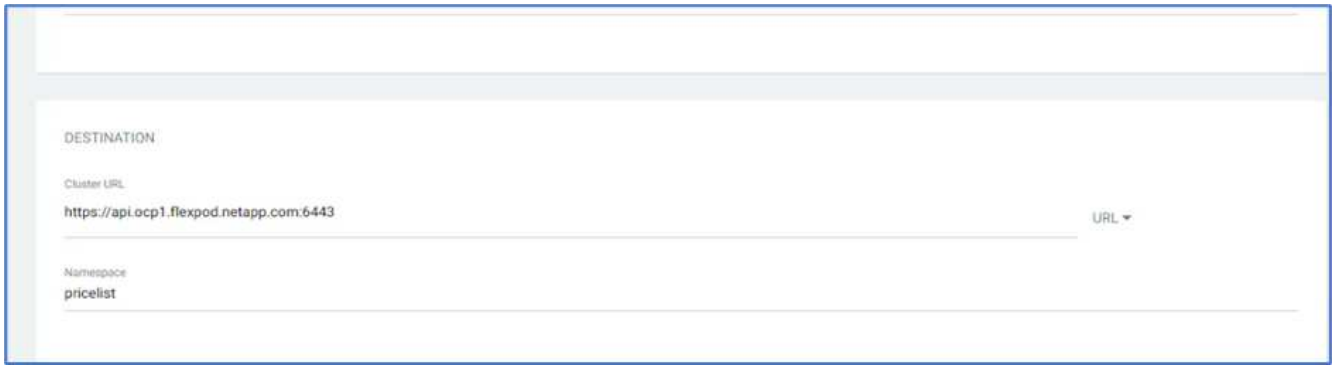
8. Ajoutez le cluster OpenShift sur site au CD Argo via l'interface de ligne de commande.

```
####Login to Argo CD####
abhinav3@abhinav-ansible$ argocd-linux-amd64 login argocd-netapp-server-
argocd.apps.ocp.flexpod.netapp.com --insecure
Username: admin
Password:
'admin:login' logged in successfully
Context'argocd-netapp-server-argocd.apps.ocp.flexpod.netapp.com' updated
####List the On-Premises OpenShift cluster####
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add
ERRO[0000] Choose a context name from:
CURRENT  NAME
CLUSTER              SERVER
*        default/api-ocp-flexpod-netapp-com:6443/abhinav3
api-ocp-flexpod-netapp-com:6443
https://api.ocp.flexpod.netapp.com:6443
         default/api-ocp1-flexpod-netapp-com:6443/abhinav3
api-ocp1-flexpod-netapp-com:6443
https://api.ocp1.flexpod.netapp.com:6443
####Add On-Premises OpenShift cluster###
abhinav3@abhinav-ansible$ argocd-linux-amd64 cluster add default/api-
ocp1-flexpod-netapp-com:6443/abhinav3
WARNING: This will create a service account `argocd-manager` on the
cluster referenced by context `default/api-ocp1-flexpod-netapp-
com:6443/abhinav3` with full cluster level admin privileges. Do you want
to continue [y/N]? y
INFO[0002] ServiceAccount "argocd-manager" already exists in namespace
"kube-system"
INFO[0002] ClusterRole "argocd-manager-role" updated
INFO[0002] ClusterRoleBinding "argocd-manager-role-binding" updated
Cluster 'https://api.ocp1.flexpod.netapp.com:6443' added
```

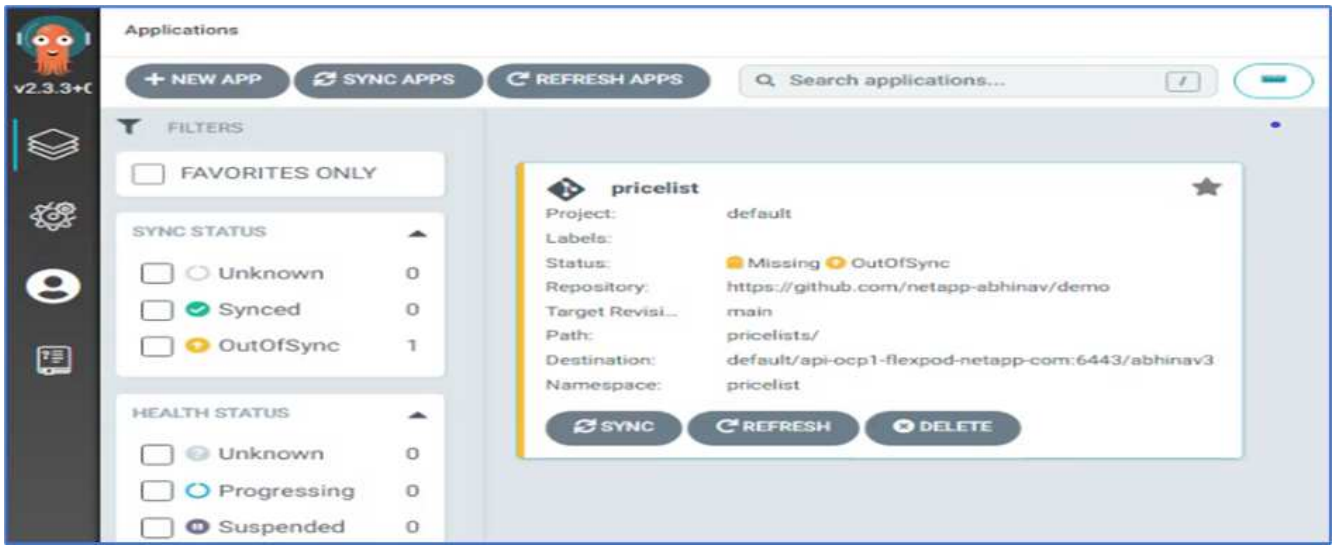
9. Dans l’interface utilisateur ArgoCD, cliquez sur NOUVELLE APPLICATION et entrez les détails du nom de l’application et du référentiel de code.



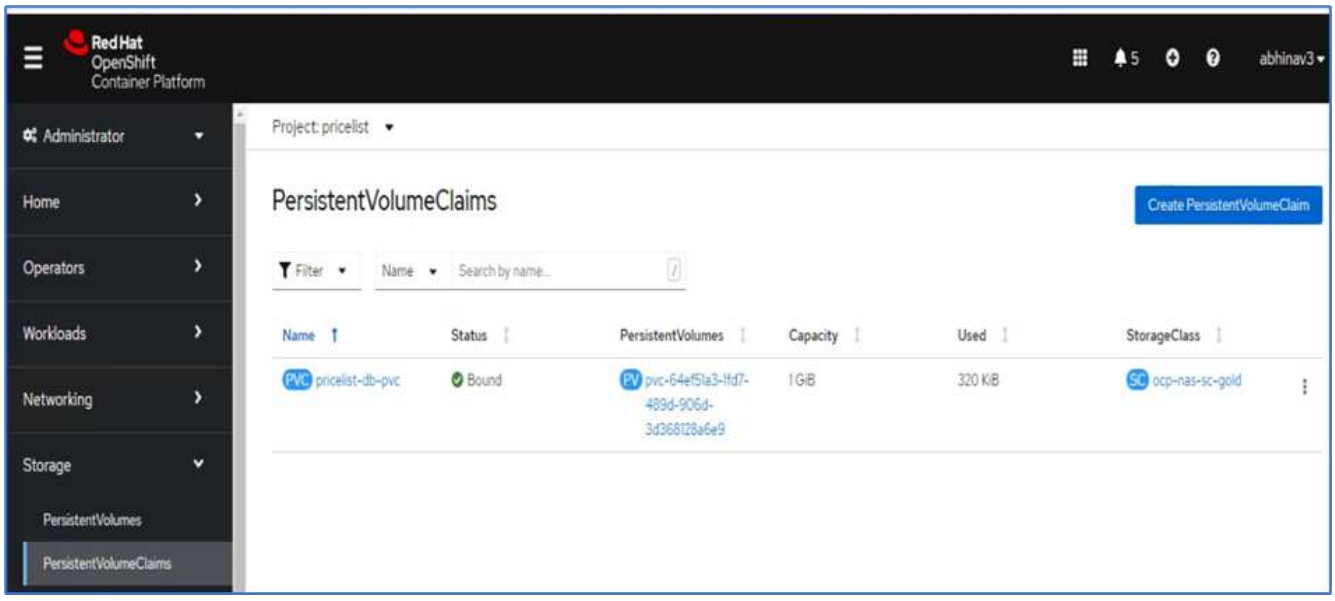
10. Entrez le cluster OpenShift où l'application sera déployée avec le namespace.



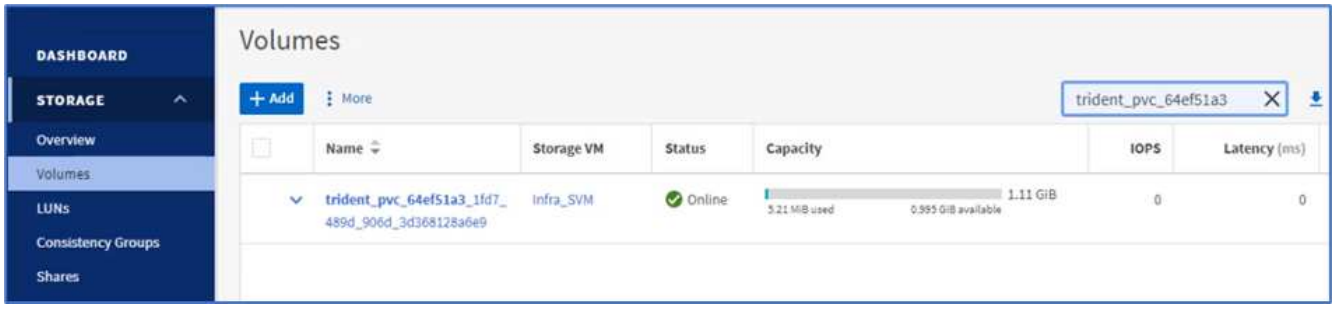
11. Pour déployer l'application sur le cluster OpenShift sur site, cliquez sur SYNC.



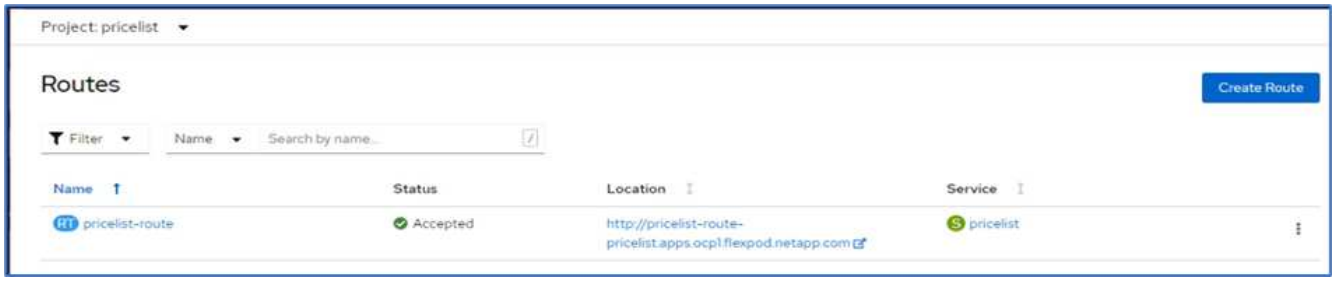
12. Dans la console OpenShift Container Platform, accédez à la liste des tarifs du projet et, sous Storage, vérifiez le nom et la taille de la demande de volume persistant.



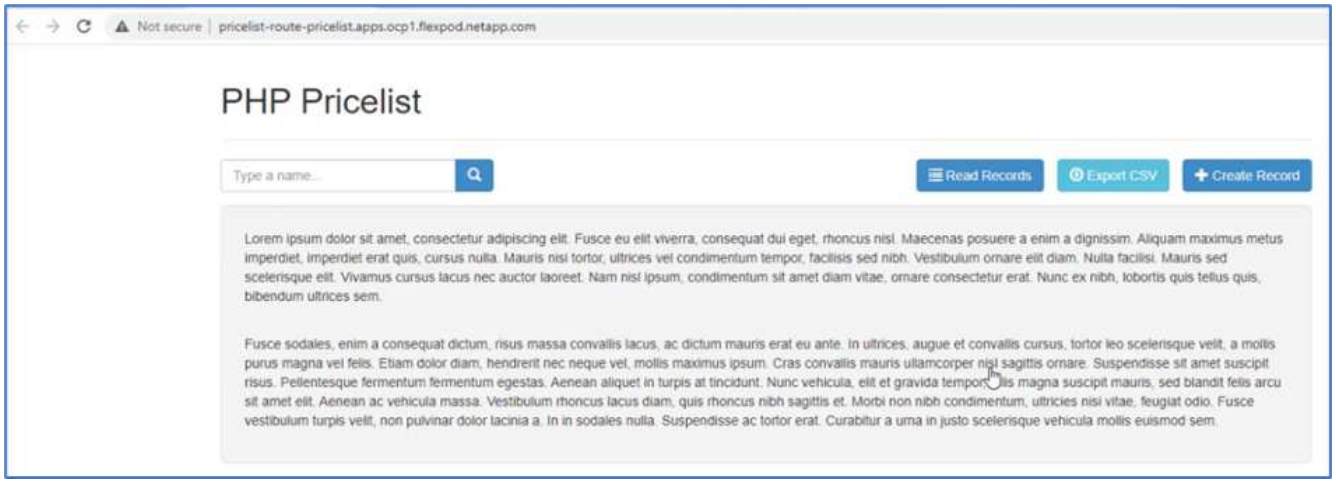
13. Connectez-vous à System Manager et vérifiez le volume persistant.



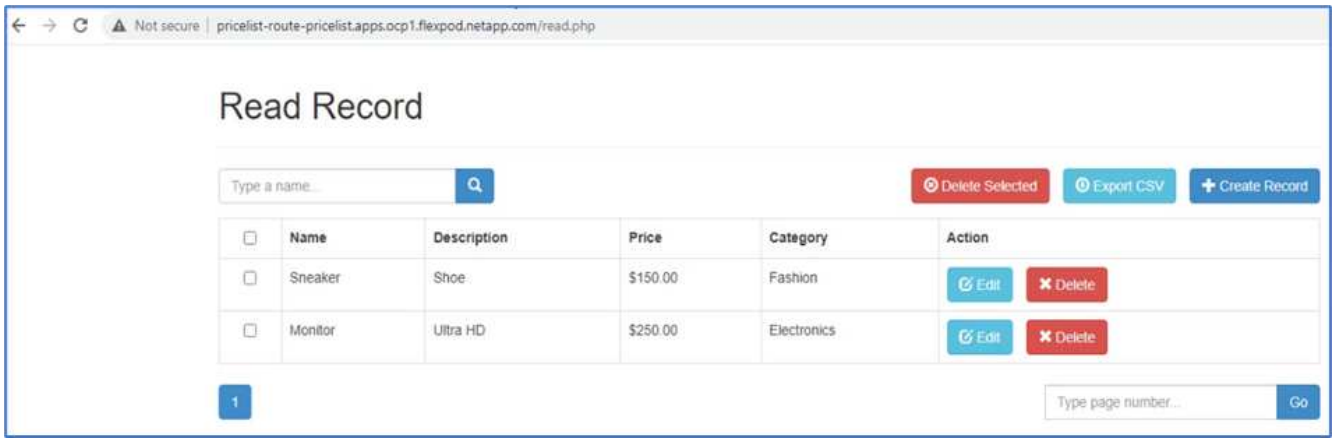
14. Une fois les pods en cours d'exécution, sélectionnez réseau > routes dans le menu latéral, puis cliquez sur l'URL sous emplacement.



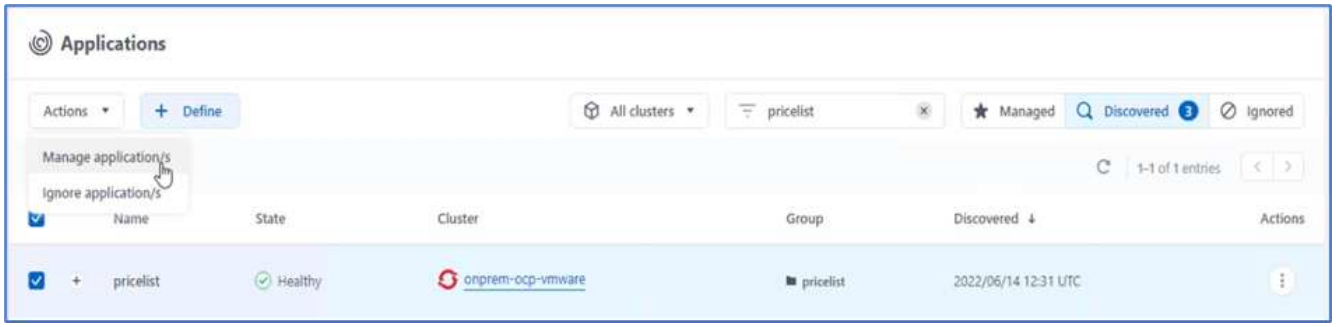
15. La page d'accueil de l'application Tarifs s'affiche.



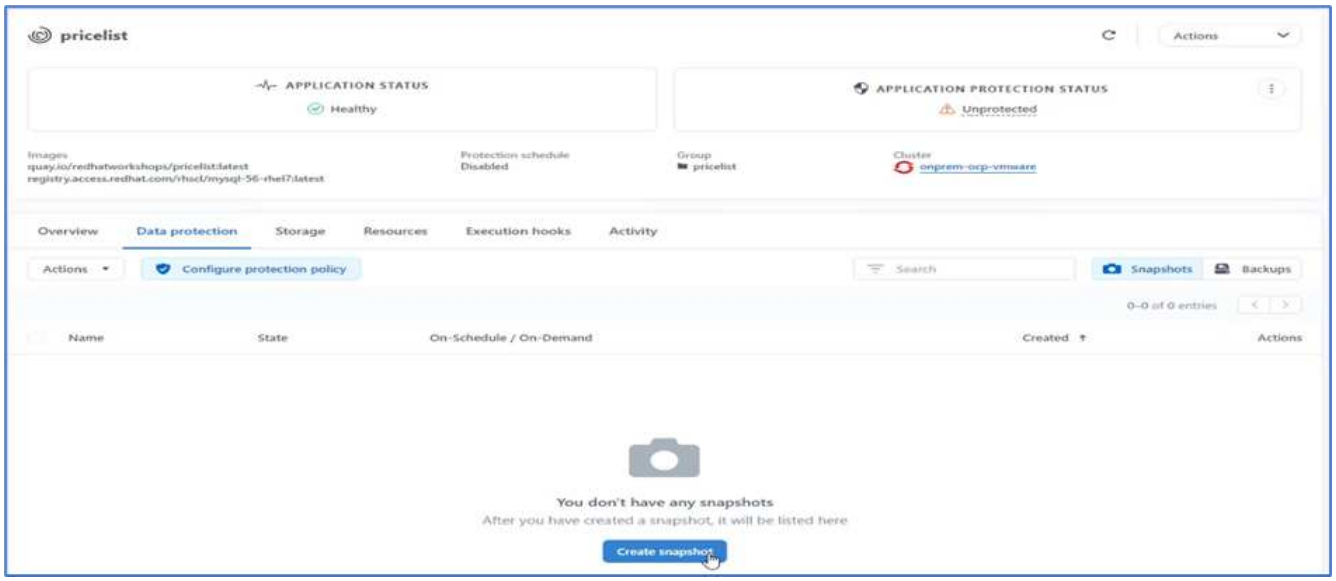
16. Créez quelques enregistrements sur la page Web.



17. L'application est découverte dans Astra Control Center. Pour gérer l'application, accédez à applications > découverte, sélectionnez l'application Barème des prix, puis cliquez sur gérer les applications sous actions.

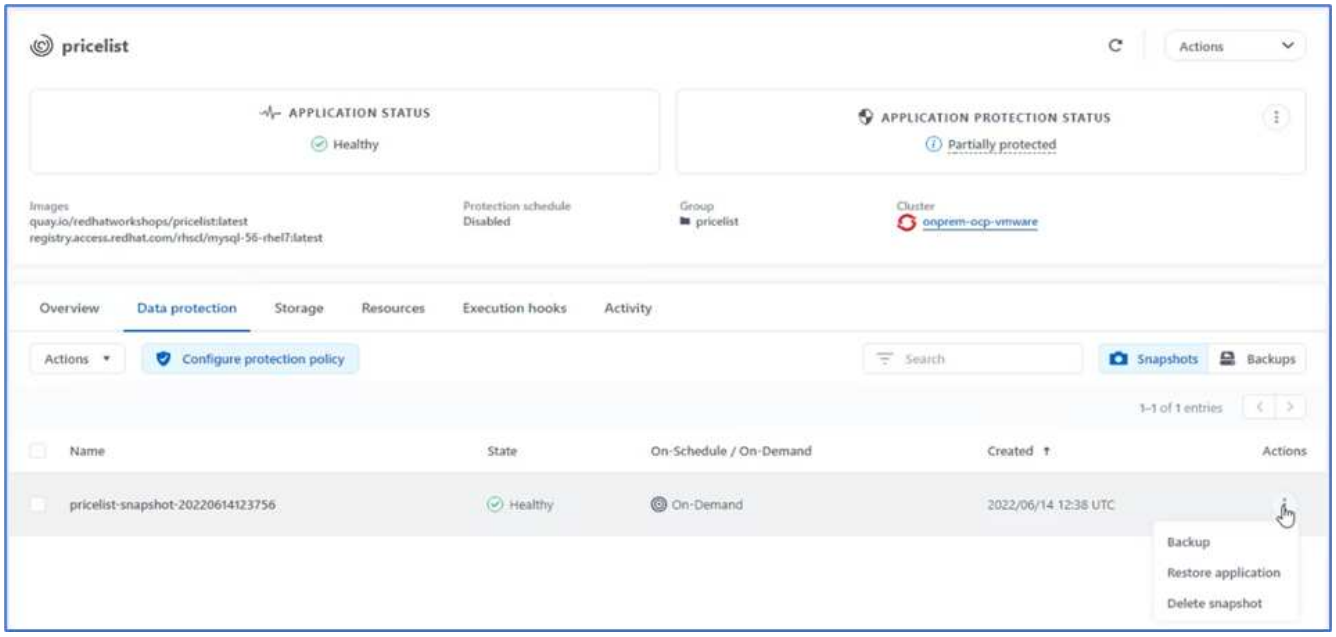


18. Cliquez sur l'application Barème des prix et sélectionnez protection des données. À ce stade, il ne doit y avoir aucun Snapshot ni aucune sauvegarde. Cliquez sur Créer un snapshot pour créer un snapshot à la demande.

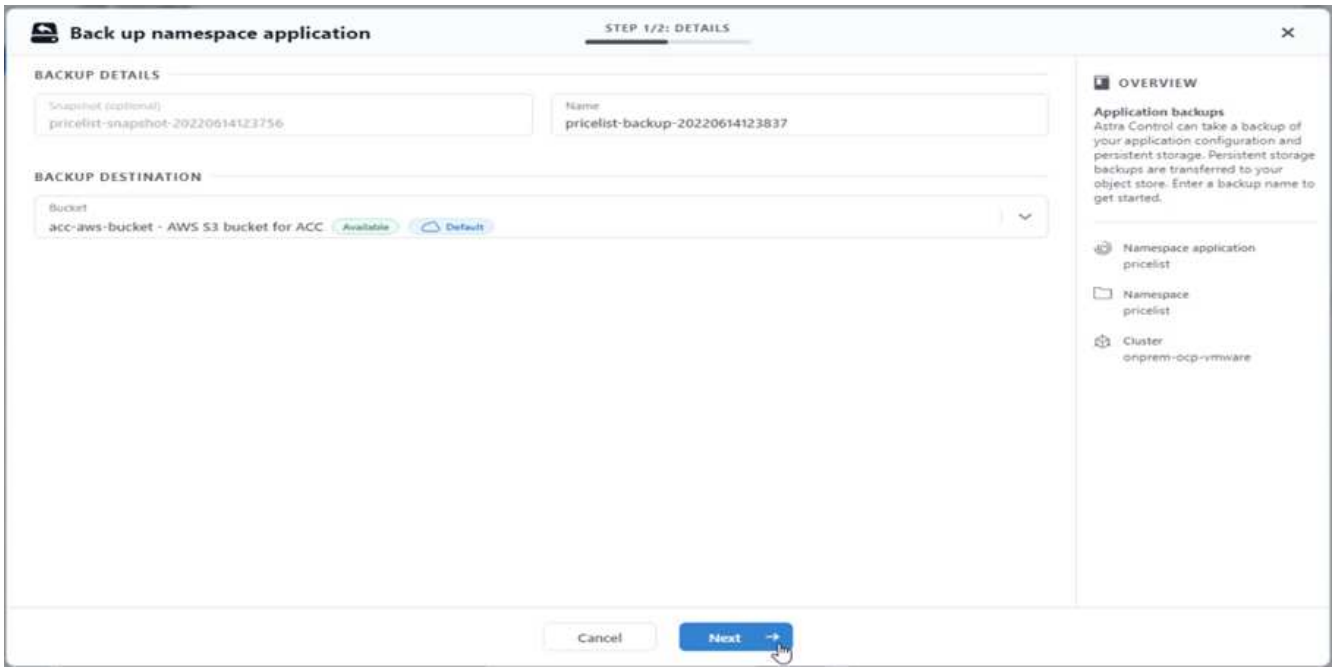


Le NetApp Astra Control Center prend en charge à la demande et les sauvegardes Snapshot et planifiées.

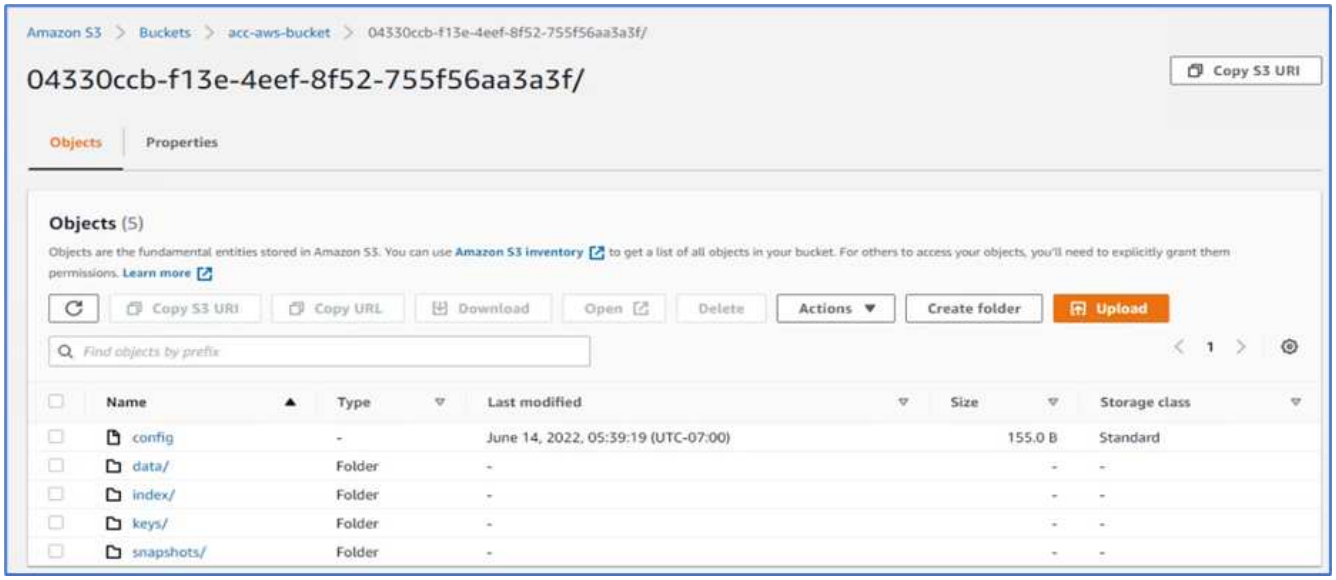
19. Une fois le snapshot créé et l'état fonctionnel, créez une sauvegarde à distance à l'aide de ce snapshot. Cette sauvegarde est stockée dans le compartiment S3.



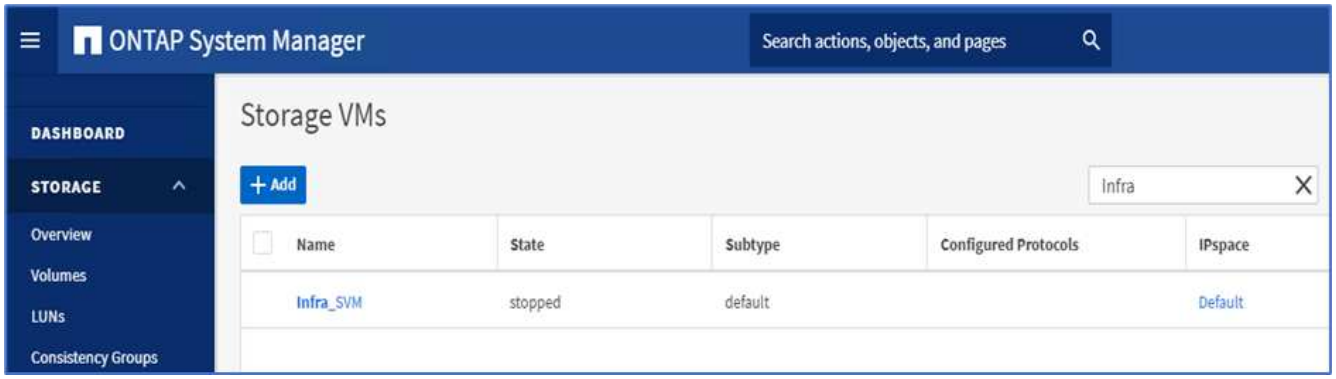
20. Sélectionnez le compartiment AWS S3 et lancez l'opération de sauvegarde.



21. L'opération de sauvegarde doit créer un dossier contenant plusieurs objets dans le compartiment AWS S3.



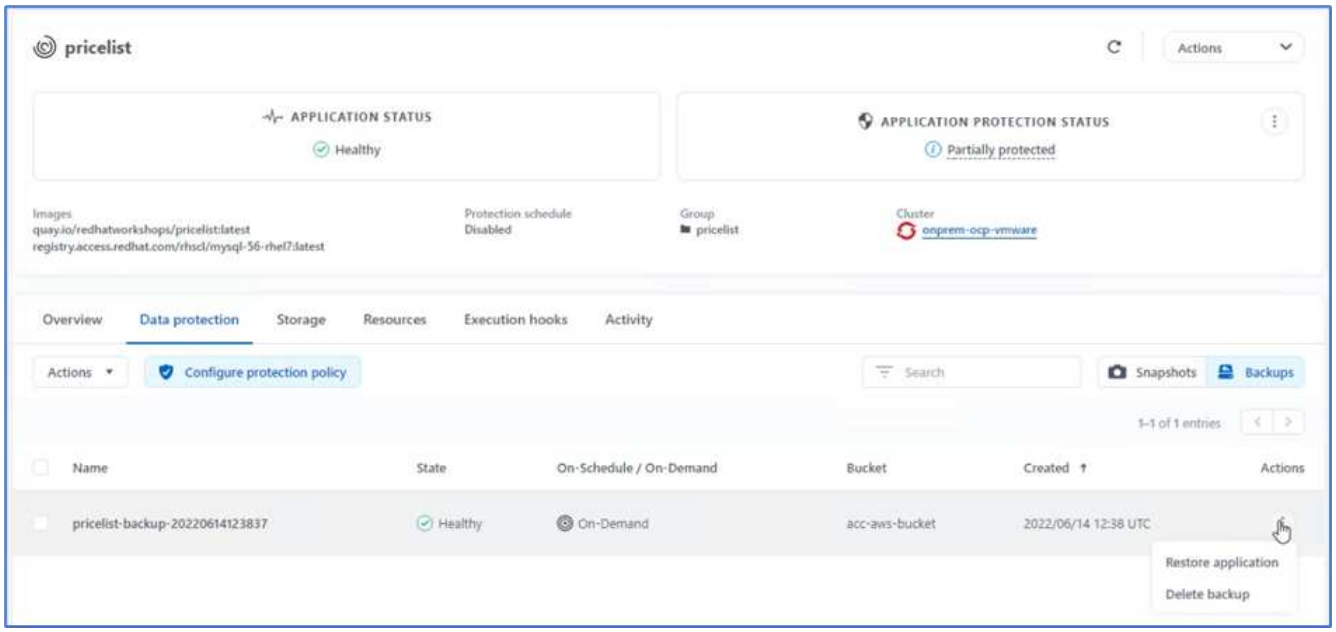
22. Une fois la sauvegarde à distance terminée, simulez un incident sur site en arrêtant la machine virtuelle de stockage (SVM) qui héberge le volume de support du volume persistant.



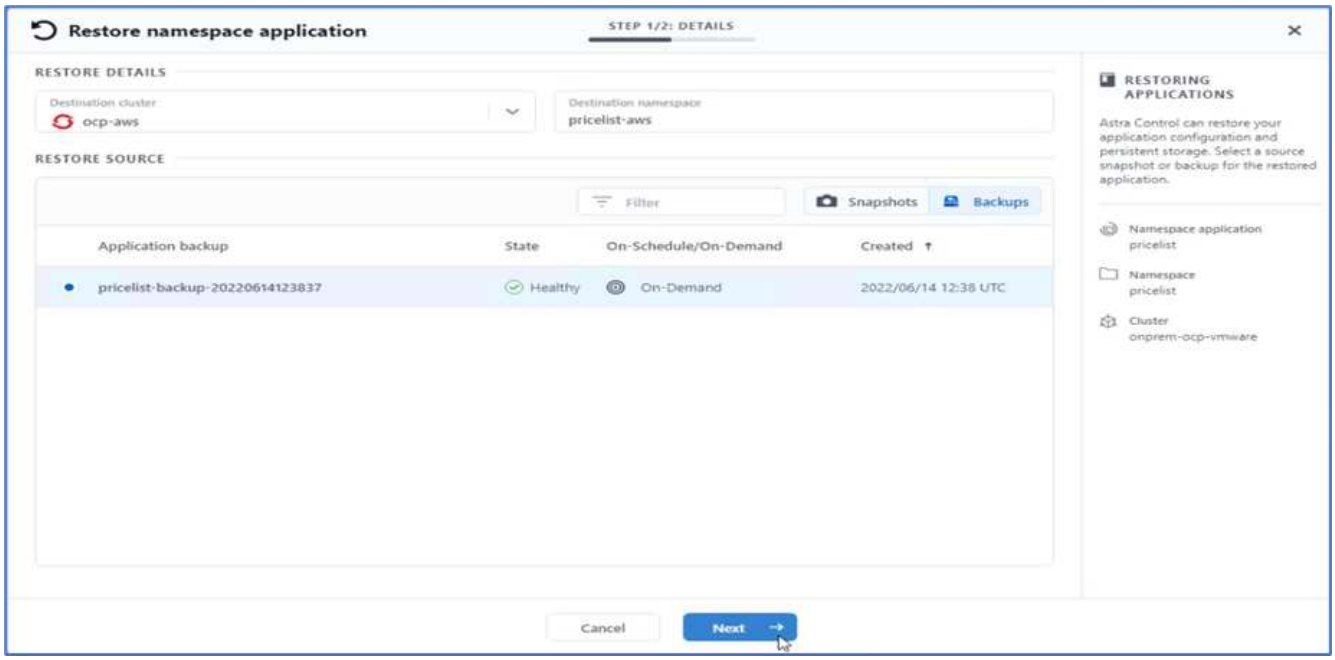
23. Actualisez la page Web pour confirmer l'interruption. La page Web n'est pas disponible.

Comme on pouvait s'y attendre, le site Web est en panne. Restaurez rapidement l'application à partir de la sauvegarde à distance en utilisant Astra vers le cluster OpenShift exécuté dans AWS.

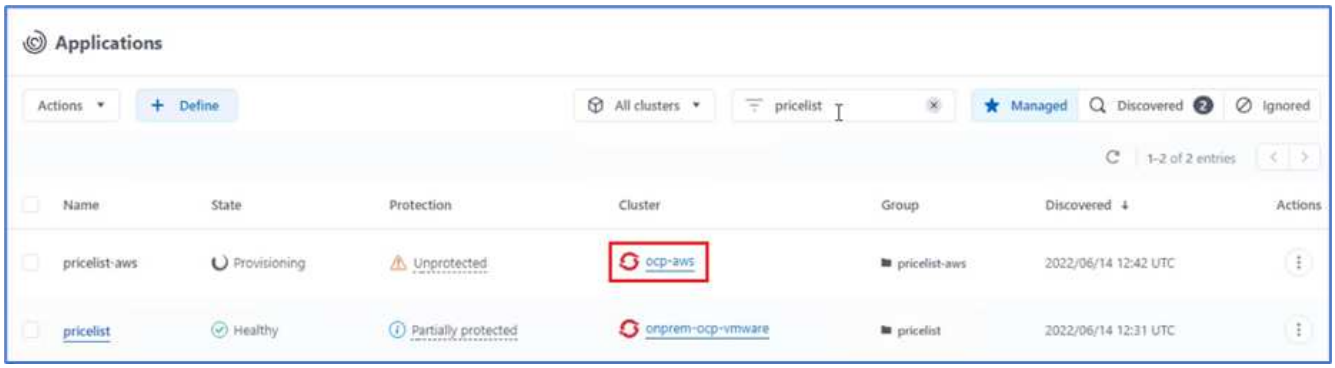
24. Dans Astra Control Center, cliquez sur l'application Pricelist et sélectionnez protection des données > sauvegardes. Sélectionnez la sauvegarde, puis cliquez sur Restaurer l'application sous action.



25. Sélectionnez `ocp-aws` comme cluster de destination et donner un nom au namespace. Cliquez sur sauvegarde à la demande, puis sur Suivant, puis sur Restaurer.

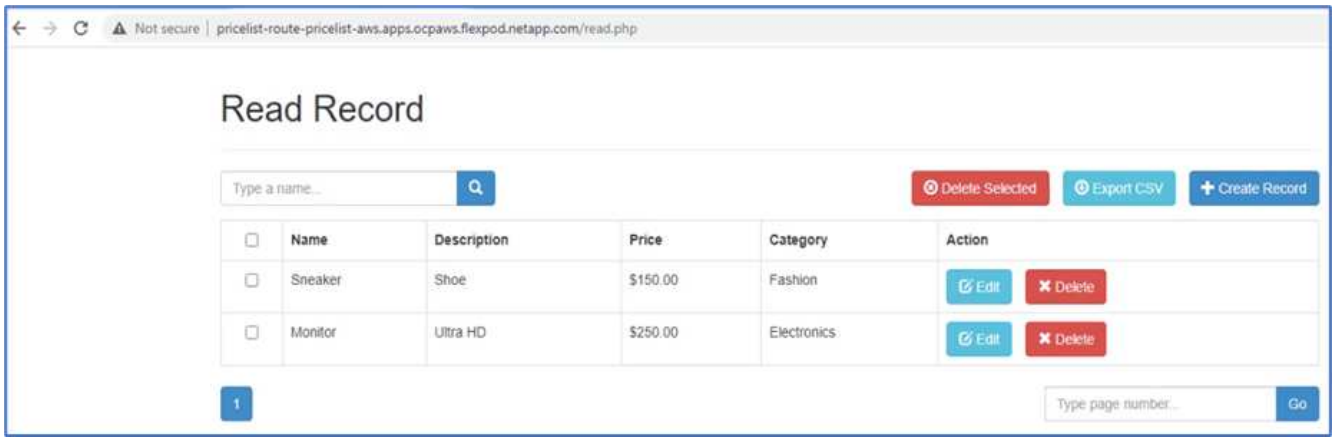


26. Une nouvelle application portant le nom `pricelist-app` Est mise à la disposition du cluster OpenShift exécuté dans AWS.



27. Vérifiez la même chose dans la console web OpenShift.

28. Après toutes les gousses sous le `pricelist-aws` Le projet est en cours d'exécution, accédez aux itinéraires et cliquez sur l'URL pour lancer la page Web.



Ce processus valide la restauration de l'application prichère et le maintien de l'intégrité des données sur le cluster OpenShift fonctionnant de façon transparente sur AWS avec l'aide d'Astra Control Center.

Protection des données avec les copies Snapshot et mobilité des applications pour DevTest

Ce cas d'utilisation se compose de deux parties, comme décrit dans les sections suivantes.

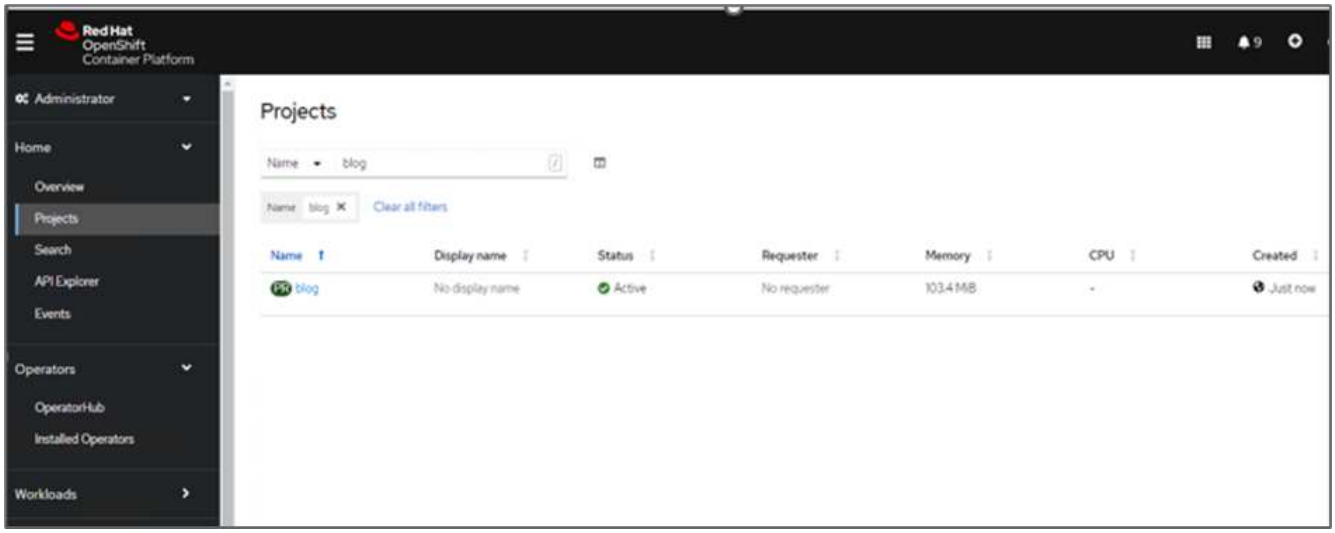
Partie 1

Avec Astra Control Center, vous pouvez créer des snapshots respectueux des applications pour une protection locale des données. Si vous supprimez ou corrompre accidentellement vos données, vous pouvez restaurer vos applications et les données associées à un état correct connu à l'aide d'un instantané précédemment enregistré.

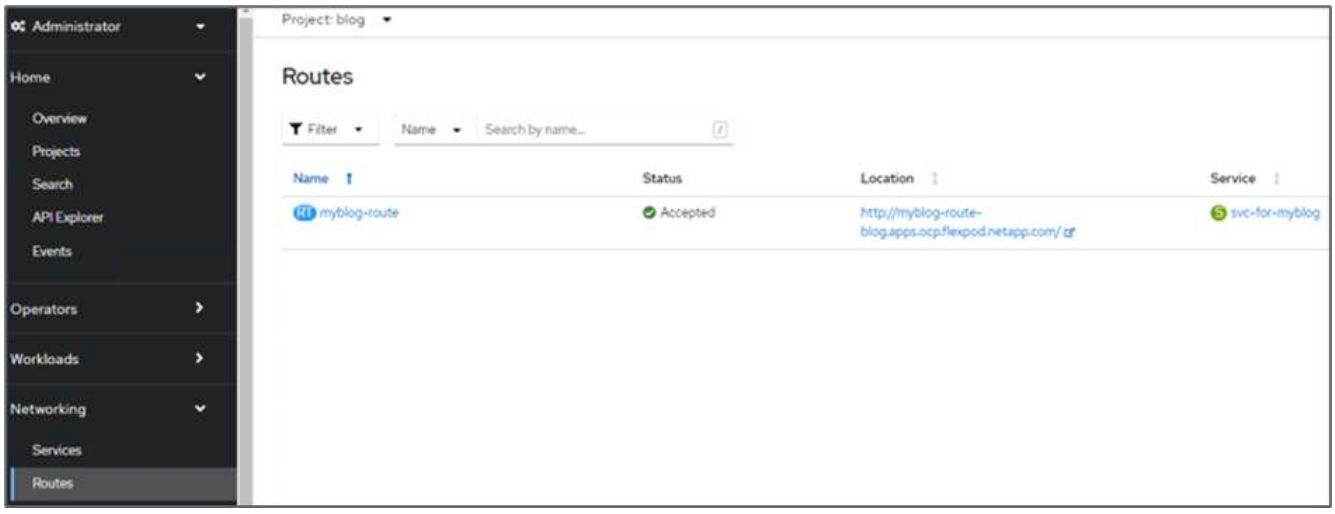
Dans ce scénario, une équipe de développement et de test (DevTest) déploie un exemple d'application avec état (site de blog) qui est une application de blog Ghost, ajoute du contenu et met à niveau l'application vers la dernière version disponible. L'application Ghost utilise SQLite pour la base de données. Avant de mettre à niveau l'application, un snapshot (à la demande) est utilisé avec Astra Control Center pour la protection des données. Les étapes détaillées sont les suivantes :

1. Déployez l'application exemple de blogging et synchronisez-la à partir d'ArgoCD.

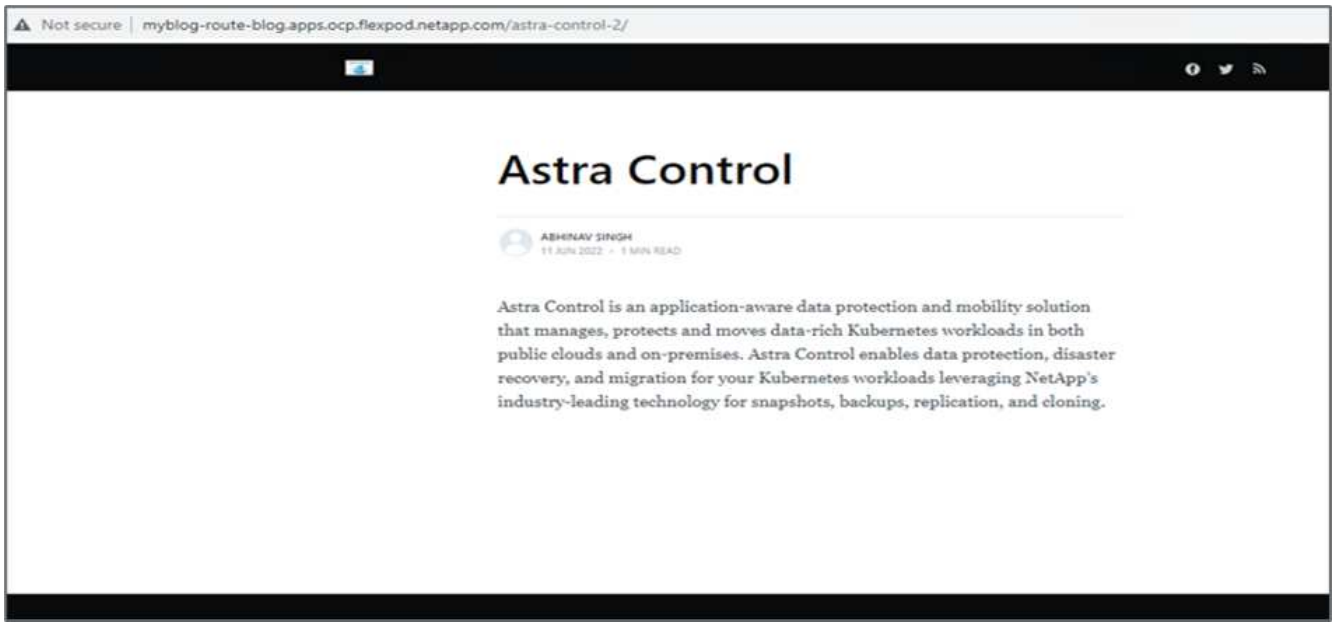
2. Connectez-vous au premier cluster OpenShift, accédez à Project et entrez Blog dans la barre de recherche.



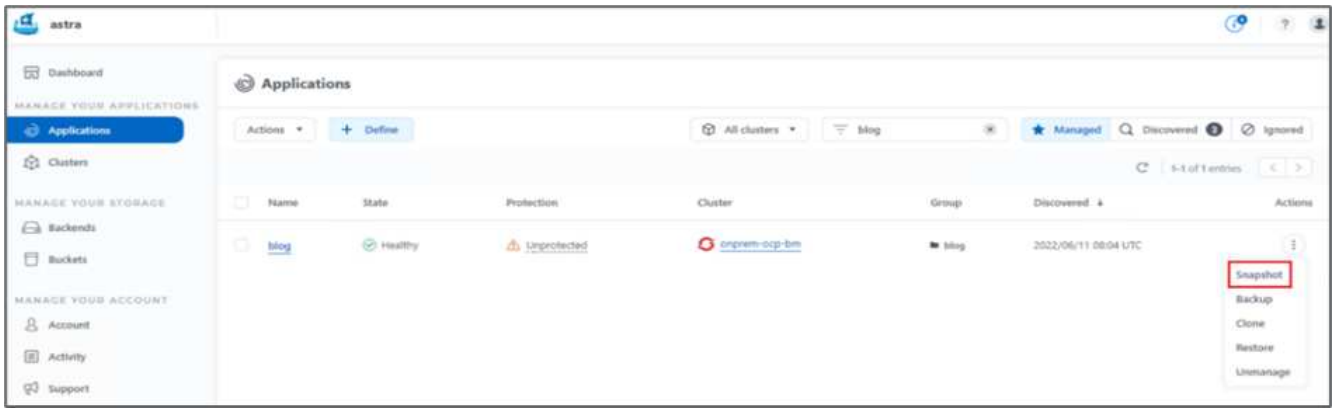
3. Dans le menu latéral, sélectionnez réseau > routes et cliquez sur l'URL.



4. La page d'accueil du blog s'affiche. Ajoutez du contenu au site du blog et publiez-le.



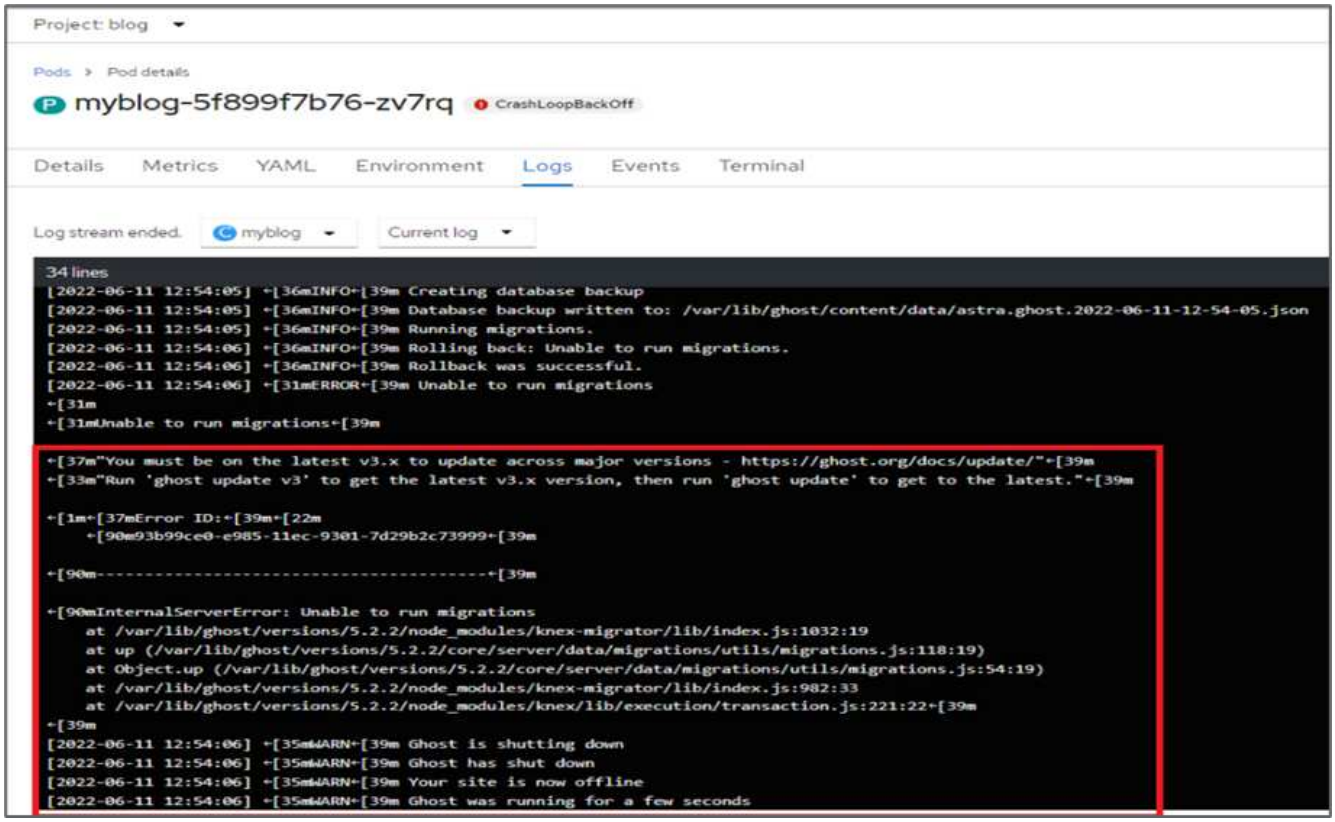
5. Rendez-vous à Astra Control Center. Commencez par gérer l'application à partir de l'onglet découverte, puis effectuez une copie Snapshot.



Vous pouvez également protéger vos applications en créant des snapshots, des sauvegardes ou les deux à un calendrier défini. Pour plus d'informations, voir "Protéger les applications avec les snapshots et les sauvegardes".

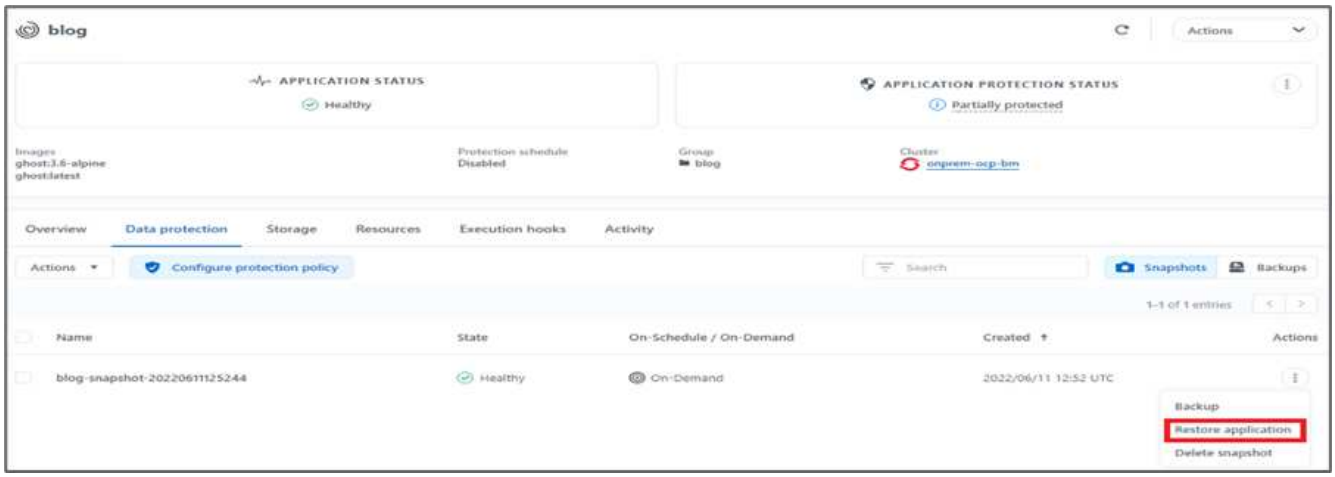
6. Une fois le snapshot à la demande créé, mettez l'application à niveau vers la dernière version. La version actuelle de l'image est `ghost: 3.6-alpine` et la version cible est `ghost:latest`. Pour mettre à niveau l'application, apportez directement des modifications au référentiel Git et synchronisez-les sur le CD Argo.

7. Vous pouvez voir que la mise à niveau directe vers la dernière version n'est pas prise en charge car le site du blog est en panne et l'application entière est corrompue.

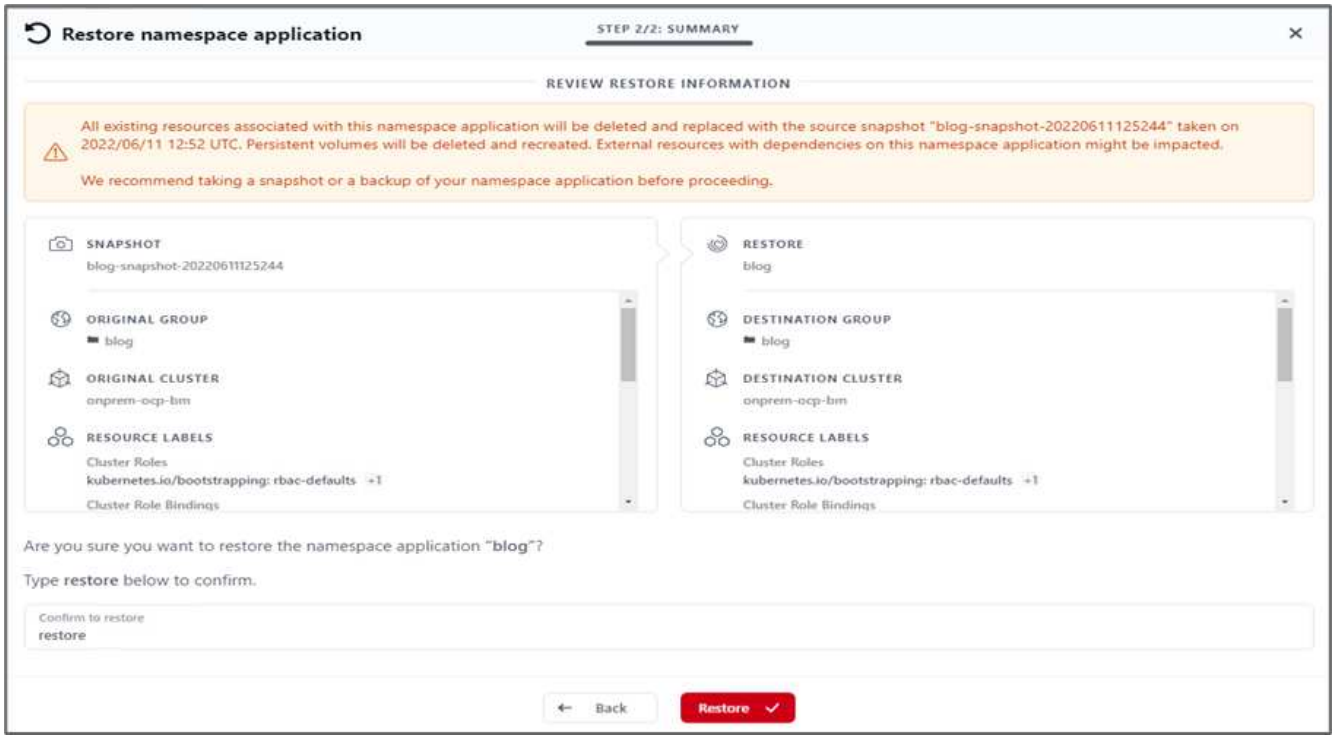


8. Pour confirmer l’indisponibilité du site du blog, actualisez l’URL.

9. Restaurez l’application à partir du snapshot.



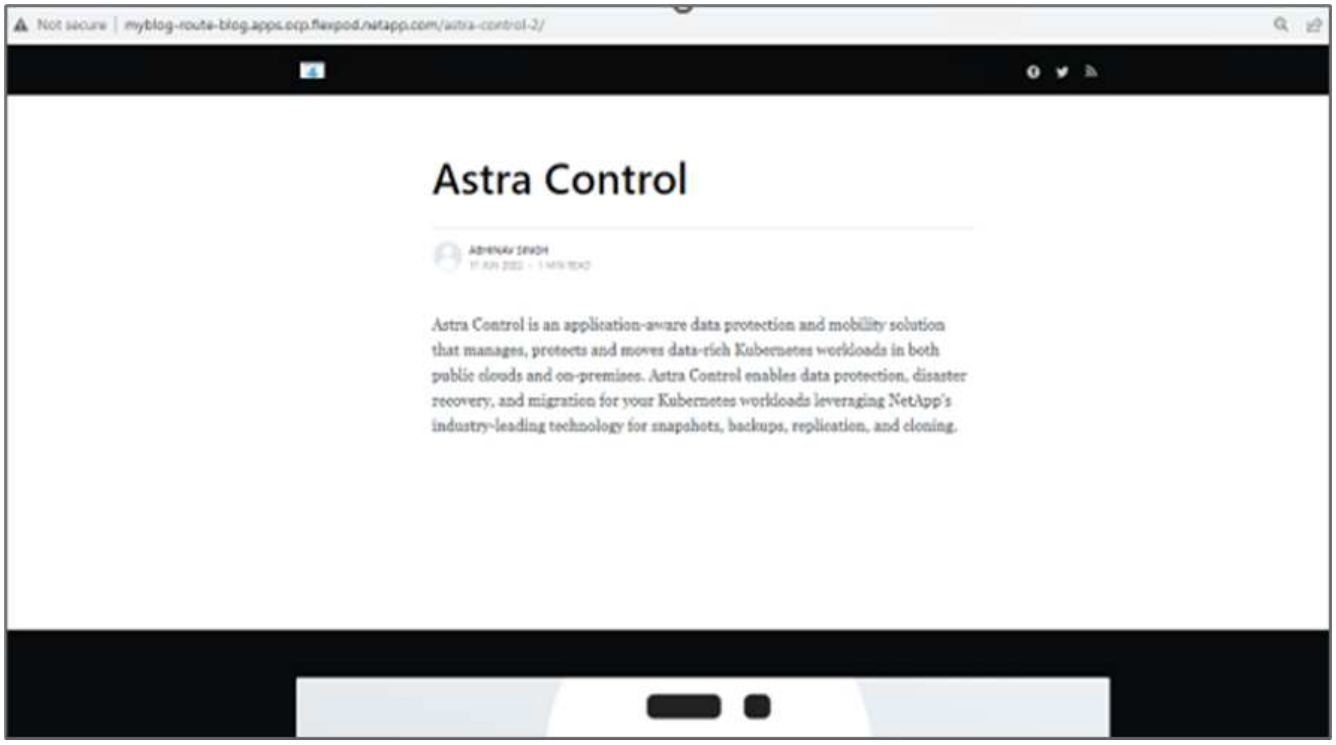
10. L'application est restaurée sur le même cluster OpenShift.



11. Le processus de restauration des applications démarre immédiatement.

12. En quelques minutes, l'application est restaurée à partir du snapshot disponible.

13. Pour voir si la page Web est disponible, actualisez l'URL.

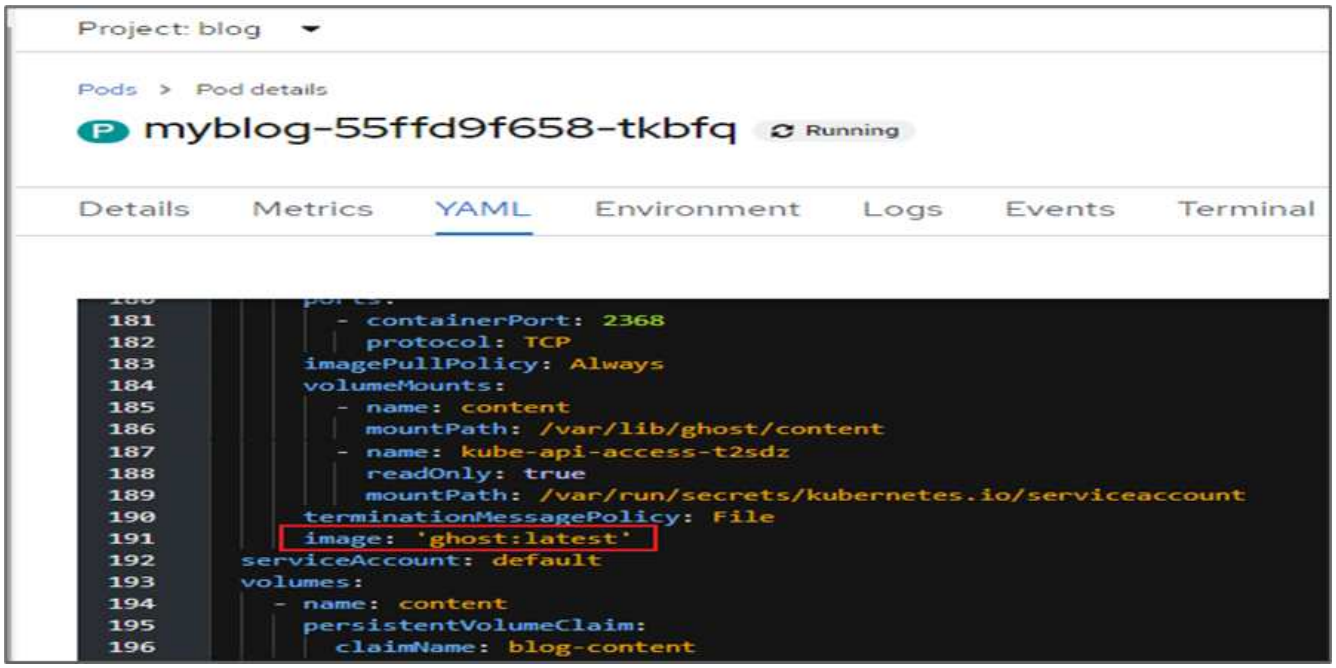


Avec l'aide d'Astra Control Center, une équipe DevTest peut réussir la récupération d'une application de blog et de ses données associées à l'aide de la capture d'écran.

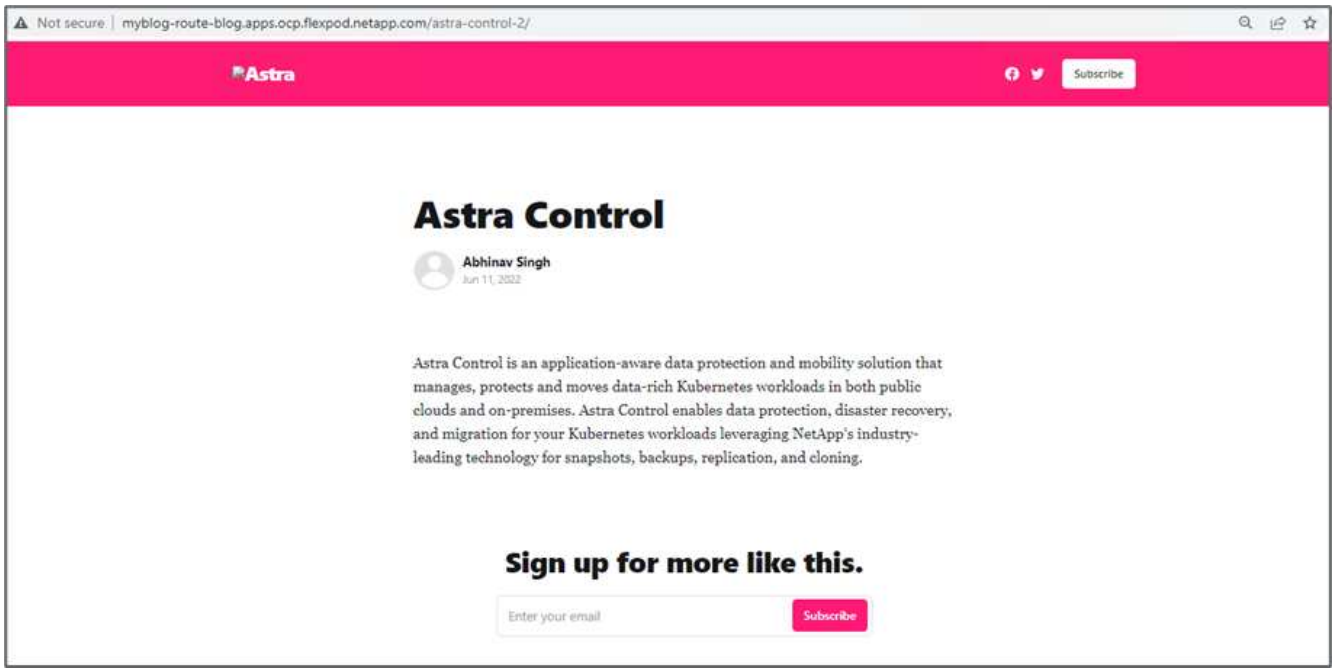
Partie 2

Avec Astra Control Center, vous pouvez déplacer l'ensemble d'une application avec ses données d'un cluster Kubernetes vers un autre, quel que soit l'emplacement des clusters (sur site ou dans le cloud).

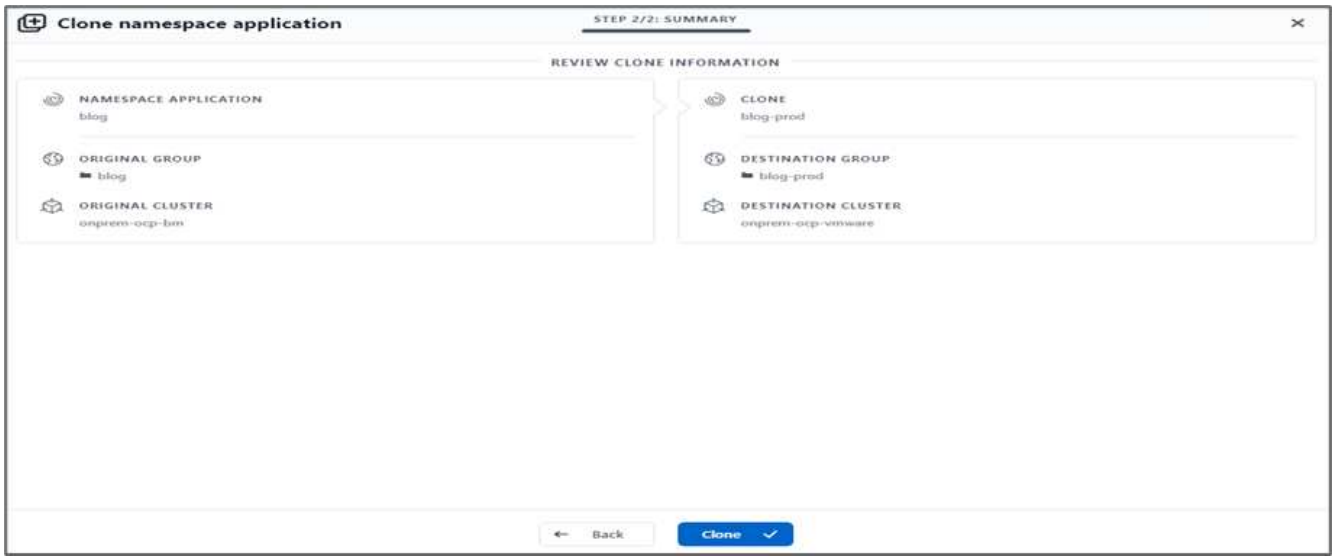
1. L'équipe DevTest met initialement à niveau l'application vers la version prise en charge (`ghost-4.6-alpine`) avant la mise à niveau vers la version finale (`ghost-latest`) pour la préparer à la production. Ils publient ensuite une mise à niveau de l'application clonée vers le cluster OpenShift de production s'exécutant sur un autre système FlexPod.
2. À ce stade, l'application est mise à niveau vers la dernière version et prête à être clonée sur le cluster de production.



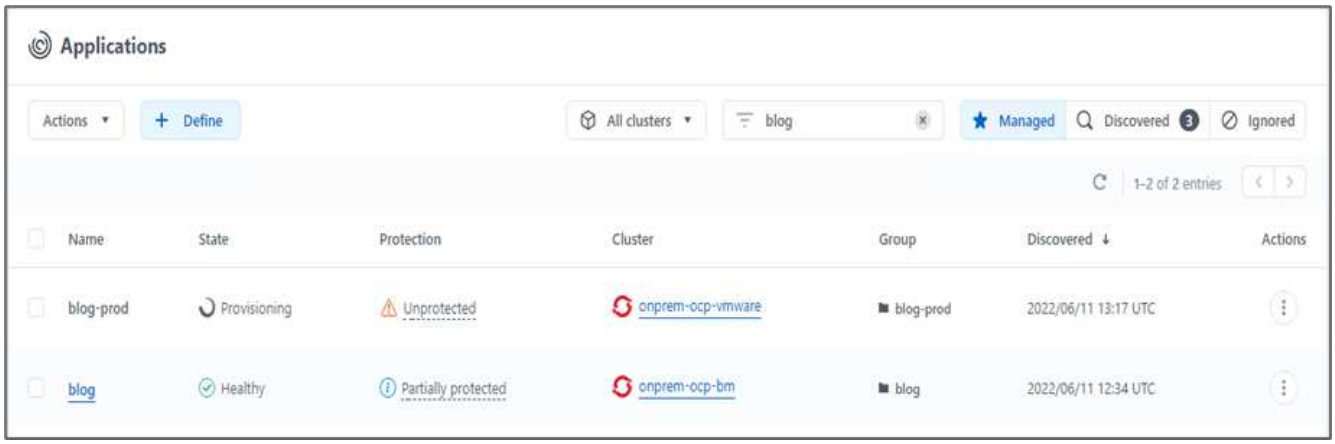
3. Pour vérifier le nouveau thème, actualisez le site du blog.



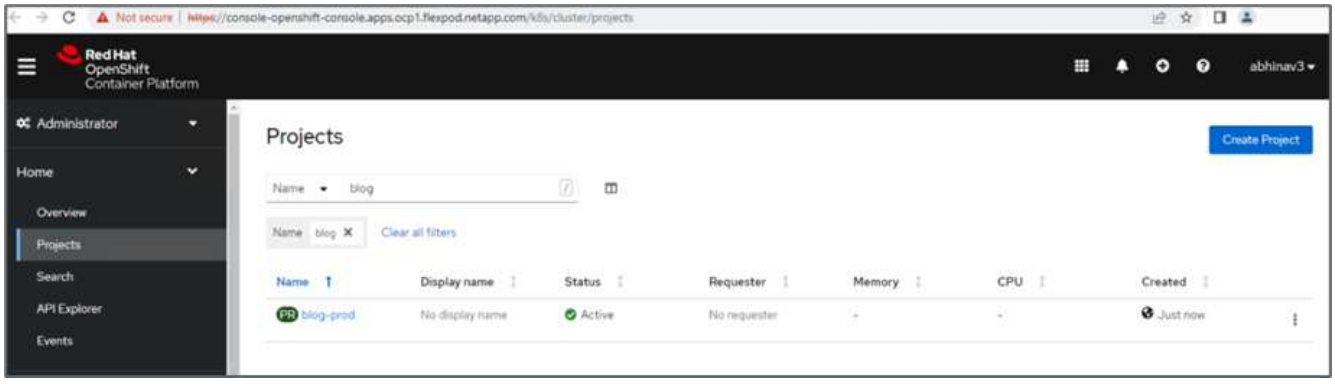
4. À partir d'Astra Control Center, clonez l'application vers l'autre cluster OpenShift de production qui s'exécute sur VMware vSphere.



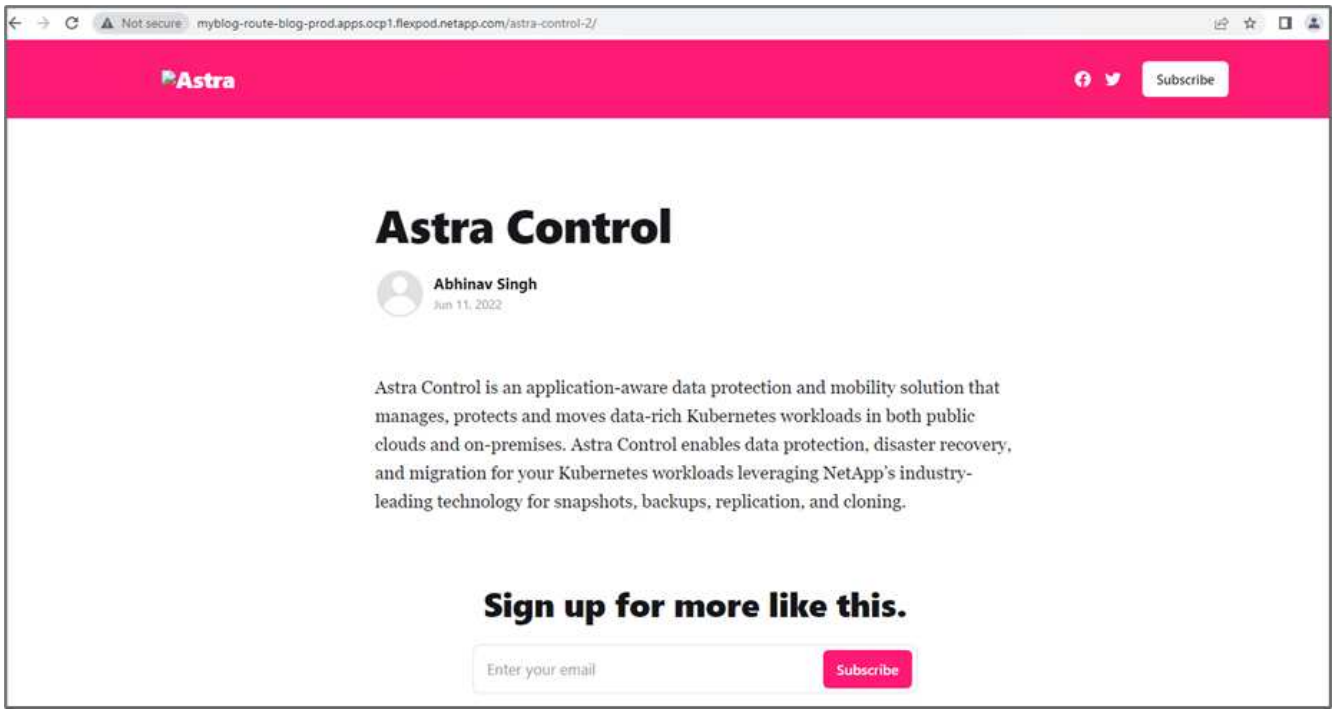
Un nouveau clone d'application est désormais provisionné dans le cluster OpenShift de production.



5. Connectez-vous au cluster OpenShift de production et recherchez le blog du projet.



6. Dans le menu latéral, sélectionnez réseau > itinéraires et cliquez sur l'URL sous emplacement. La même page d'accueil avec le contenu s'affiche.



La validation de la solution Astra Control Center est maintenant terminée. Vous pouvez désormais cloner une application et ses données d'un cluster Kubernetes à un autre, quel que soit l'emplacement du cluster Kubernetes.

"Suivant: Conclusion."

Conclusion

"Précédente : restauration d'applications avec sauvegardes distantes."

Avec cette solution, nous avons mis en œuvre un plan de protection pour les applications conteneurisées qui sont exécutées sur FlexPod et AWS à l'aide du portefeuille NetApp Astra. NetApp Astra Control Center et Astra Trident, ainsi que Cloud Volumes ONTAP, Red Hat OpenShift et l'infrastructure FlexPod, ont constitué les principaux composants de cette solution.

Nous avons démontré la protection des applications en capturant des snapshots et en exécutant des sauvegardes complètes afin de restaurer les applications sur différents clusters K8s exécutés sur les environnements cloud et sur site.

Nous avons également démontré le clonage des applications sur les clusters K8s, afin de permettre aux clients de migrer leurs applications vers les clusters K8s de leur choix.

FlexPod a constamment évolué pour permettre à ses clients de moderniser leurs applications et leurs processus de fourniture d'informations. Avec cette solution, les clients de FlexPod peuvent créer en toute confiance leur plan de reprise après incident BCDR pour leurs applications cloud natives, en utilisant le cloud public comme emplacement dans le cadre d'un plan de reprise après incident transitoire ou à temps complet, tout en conservant le coût de la solution le plus bas.

Astra Control vous permet de déplacer une application avec ses données d'un cluster Kubernetes vers un autre, quel que soit l'emplacement des clusters. Elle accélère également le déploiement, les opérations et la

protection de vos applications cloud.

Dépannage

Pour obtenir des conseils de dépannage, reportez-vous à la section "documentation en ligne".

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

- Page d'accueil de FlexPod

  "https://www.flexpod.com"

- Guides de conception et de déploiement validés par Cisco pour FlexPod

  "https://www.cisco.com/c/en/us/solutions/design-zone/data-center-design-guides/flexpod-design-guides.html"

- Déploiement de FlexPod avec Infrastructure as code pour VMware avec Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_m6_esxi7u2.html#AnsibleAutomationWorkflowandSolutionDeployment"

- Déploiement de FlexPod avec Infrastructure as code pour Red Hat OpenShift bare Metal avec Ansible

  "https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_iac_redhat_openshift.html"

- Outil d'interopérabilité matérielle et logicielle Cisco UCS

  "http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"

- Fiche technique Cisco Intersight

  "https://intersight.com/help/saas/home"

- Documentation NetApp Astra

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Control Center

  "https://docs.netapp.com/us-en/astra-control-center/index.html"

- NetApp Astra Trident

  "https://docs.netapp.com/us-en/trident/index.html"

- NetApp Cloud Manager

  "https://docs.netapp.com/us-en/occm/concept_overview.html"

- NetApp Cloud Volumes ONTAP

"https://docs.netapp.com/us-en/occm/task_getting_started_aws.html"

- Red Hat OpenShift

  "https://www.openshift.com/"

- Matrice d'interopérabilité NetApp

  "http://support.netapp.com/matrix/"

Historique des versions

Version	Date	Historique des versions du document
Version 1.0	Juillet 2022	Lancement de l'ACC 22.04.0.