Validation et utilisations des solutions

NetApp Solutions

NetApp
April 18, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/netapp-solutions/containers/rh-os-n_use_case_pipeline.html on April 18, 2024. Always check docs.netapp.com for the latest.

Sommaire

Validation et utilisations de la solution : Red Hat OpenShift avec NetApp 1
Déployez un pipeline ci/CD Jenkins avec le stockage persistant : Red Hat OpenShift avec NetApp 1
Configurer la colocation sur Red Hat OpenShift avec NetApp ONTAP 11
Red Hat OpenShift Virtualization avec NetApp ONTAP 31
Solution NetApp de gestion avancée des clusters pour Kubernetes sur Red Hat OpenShift 73

Validation et utilisations de la solution : Red Hat OpenShift avec NetApp

Les exemples présentés sur cette page sont les validations et les utilisations de Red Hat OpenShift avec NetApp.

- "Déployez un pipeline ci/CD Jenkins avec le stockage persistant"
- "Configurez la colocation sur Red Hat OpenShift avec NetApp"
- "Red Hat OpenShift Virtualization avec NetApp ONTAP"
- "Solution NetApp de gestion avancée des clusters pour Kubernetes sur Red Hat OpenShift"

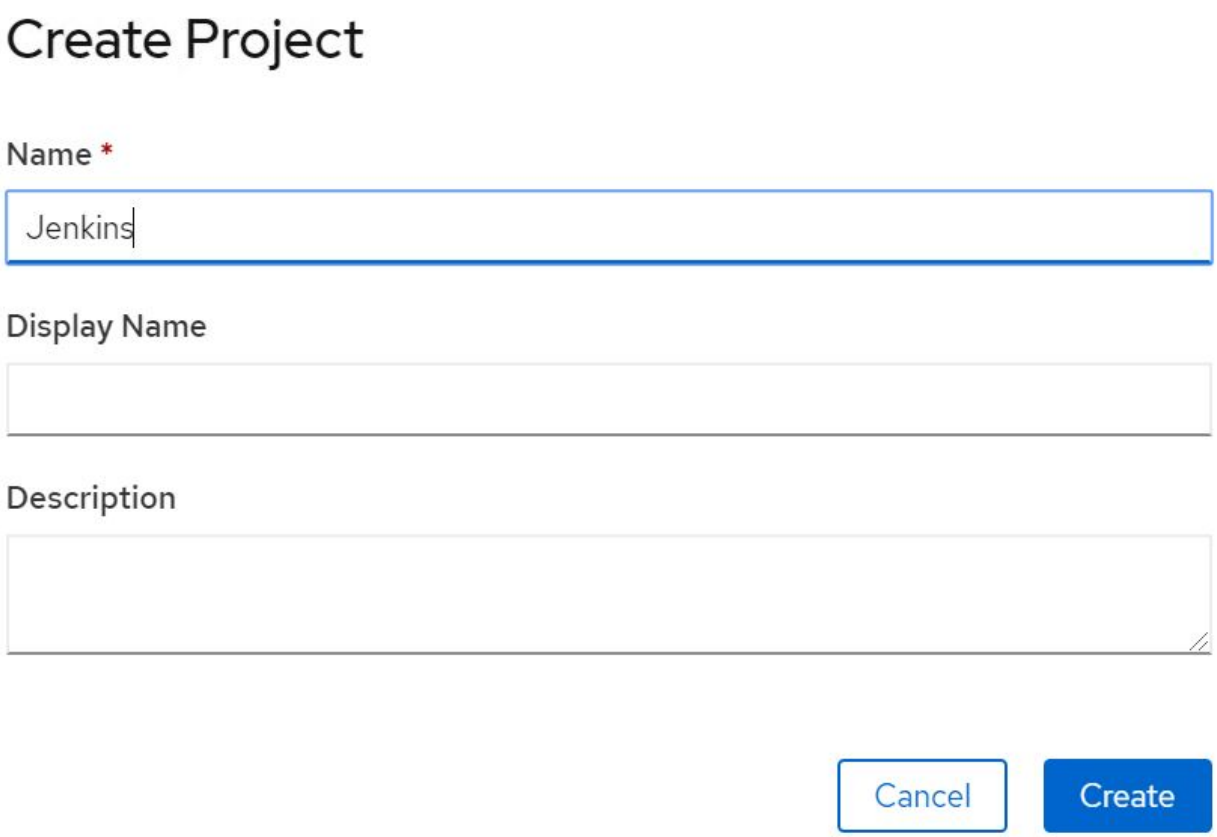
Déployez un pipeline ci/CD Jenkins avec le stockage persistant : Red Hat OpenShift avec NetApp

Cette section explique comment déployer un pipeline d'intégration/livraison continues ou de déploiement avec Jenkins pour valider le fonctionnement de la solution.

Créez les ressources requises pour le déploiement de Jenkins

Pour créer les ressources nécessaires au déploiement de l'application Jenkins, procédez comme suit :

1. Créez un nouveau projet appelé Jenkins.



2. Dans cet exemple, nous avons déployé Jenkins avec du stockage persistant. Pour prendre en charge la construction Jenkins, créez le PVC. Accédez à stockage > demandes de volume persistant et cliquez sur Créer une demande de volume persistant. Sélectionnez la classe de stockage créée, vérifiez que le nom de la demande de volume persistant est jenkins, sélectionnez la taille et le mode d'accès appropriés, puis cliquez sur Créer.

Project: jenkins

Create Persistent Volume Claim

Edit YAML

Storage Class

SC basic

Storage class for the new claim.

Persistent Volume Claim Name *

jenkins

A unique name for the storage claim within the project.

Access Mode *

Single User (RWO) Shared Access (RWX) Read Only (ROX)

Permissions to the mounted drive.

Size *

100 GiB

Desired storage capacity.

Use label selectors to request storage

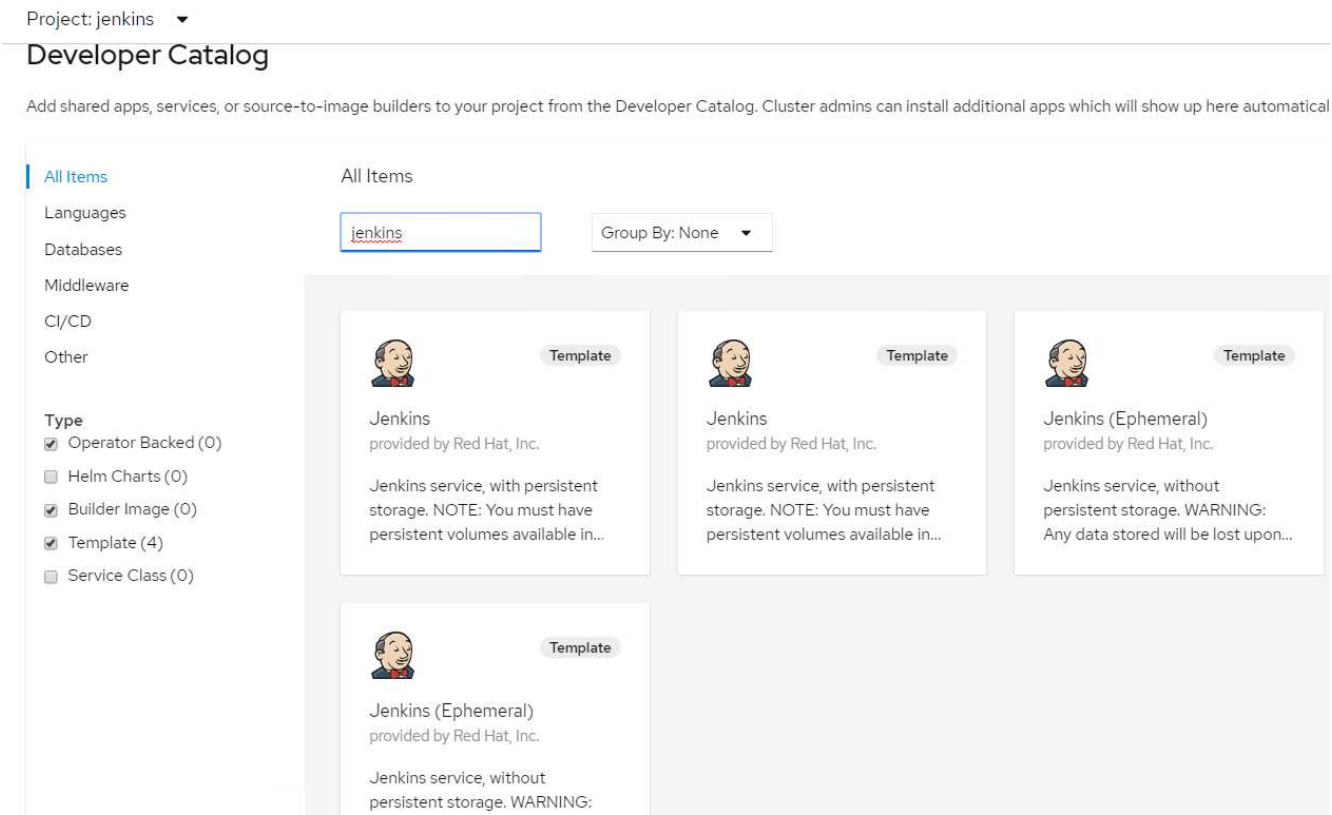
Use label selectors to define how storage is created.

Create Cancel

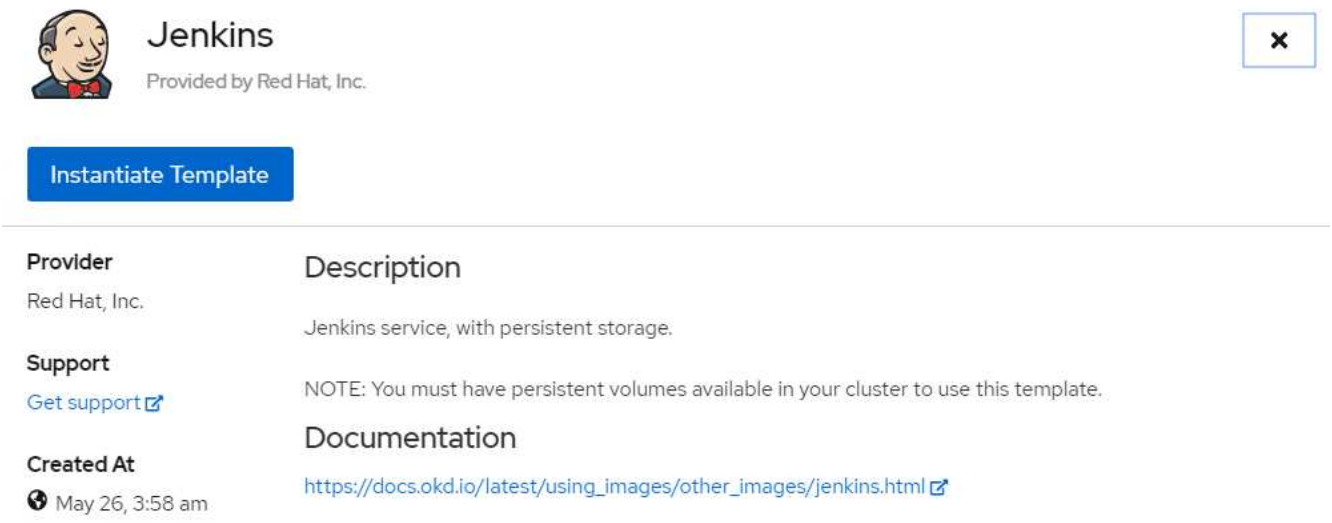
Déployez Jenkins avec le stockage persistant

Pour déployer Jenkins avec le stockage persistant, procédez comme suit :

1. Dans le coin supérieur gauche, modifiez le rôle de Administrateur à Développeur. Cliquez sur +Ajouter et sélectionnez à partir du catalogue. Dans la barre filtre par mot-clé, recherchez jenkins. Sélectionnez le service Jenkins avec le stockage persistant.

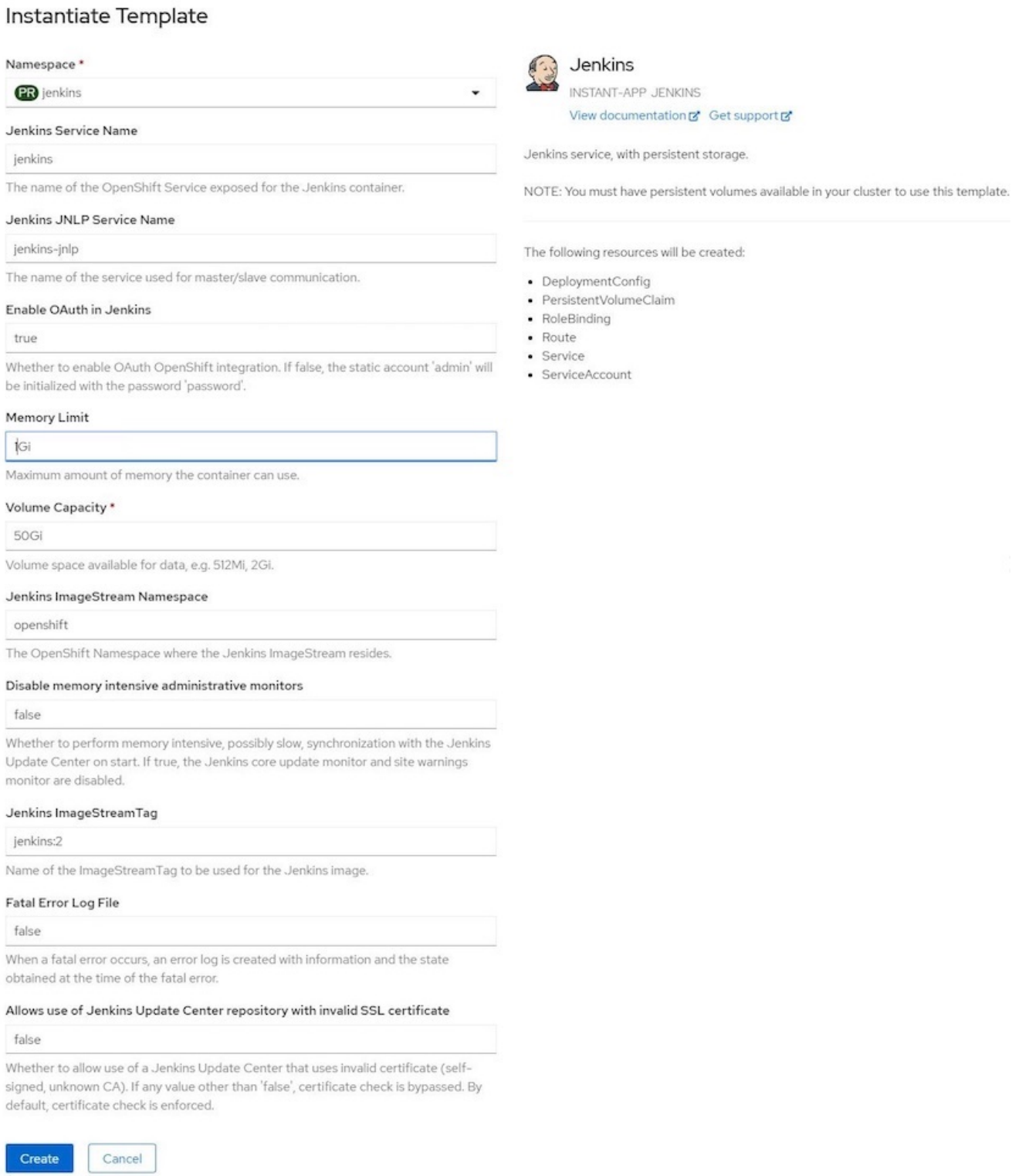


2. Cliquez sur `Instantiate Template`.



3. Par défaut, les détails de l'application Jenkins sont renseignés. En fonction de vos besoins, modifiez les paramètres et cliquez sur Créer. Ce processus crée toutes les ressources nécessaires pour prendre en

charge Jenkins sur OpenShift.



4. Les modules Jenkins prennent environ 10 à 12 minutes pour entrer en état « prêt ».

Project: jenkins

Pods

Create Pod

Filter by name...

1 Running | 0 Pending | 0 Terminating | 0 CrashLoopBackOff | 1 Completed | 0 Failed | 0 Unknown

Select all filters

1 of 2 Items

Name	Namespace	Status	Ready	Owner	Memory	CPU
P jenkins-1-c77n9	NS jenkins	Running	1/1	RC jenkins-1	-	0.004 cores

5. Une fois les pods instanciés, accédez à réseau > routes. Pour ouvrir la page Web Jenkins, cliquez sur l'URL fournie pour la route jenkins.

Project: jenkins

Routes

Create Route

Filter by name...

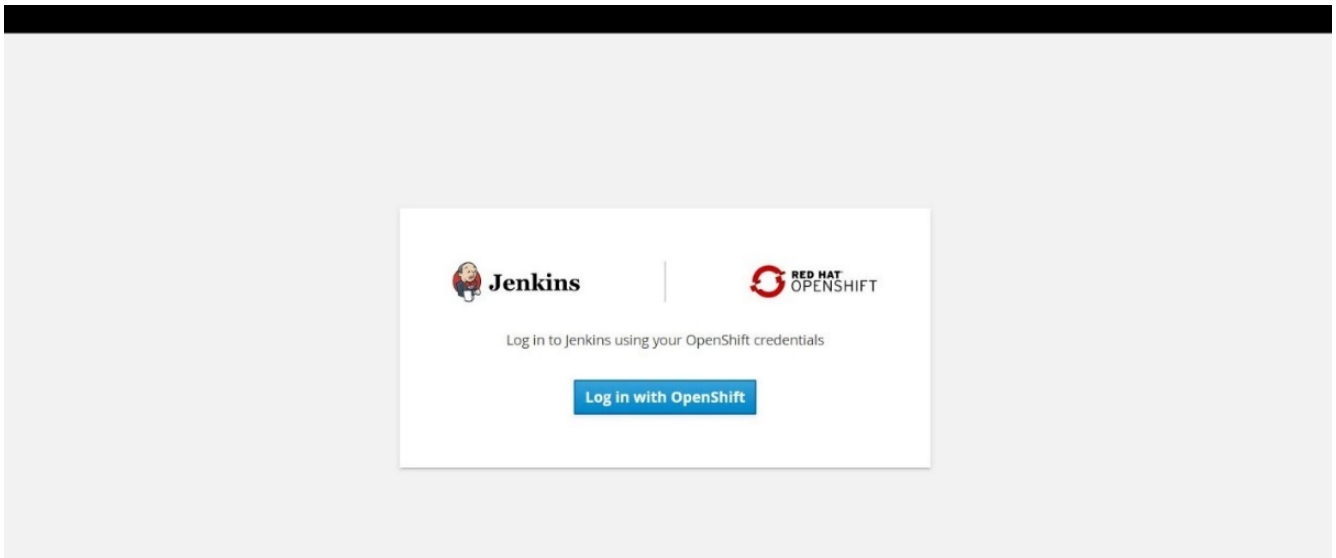
1 Accepted | 0 Rejected | 0 Pending

Select all filters

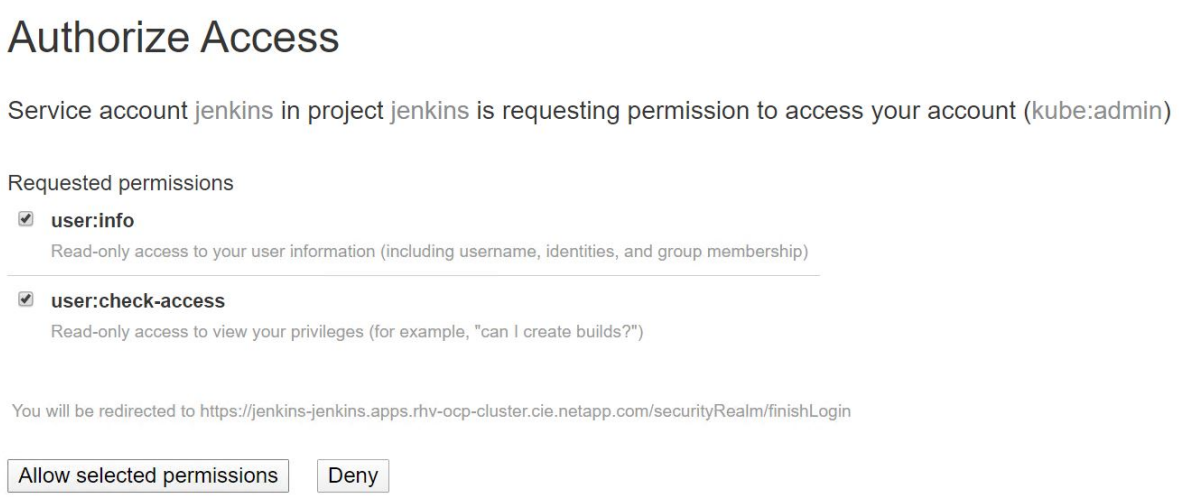
1 Item

Name	Namespace	Status	Location	Service
RT jenkins	NS jenkins	Accepted	https://jenkins-jenkins.apps.rhv-ocp-cluster.cie.netapp.com	S jenkins

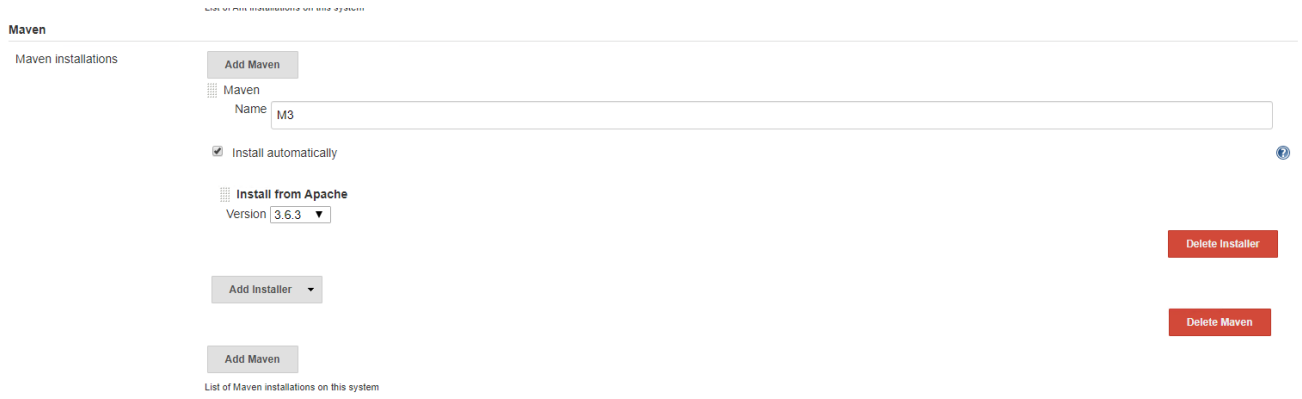
6. OpenShift OAuth a été utilisé lors de la création de l'application Jenkins, cliquez sur « se connecter avec OpenShift ».



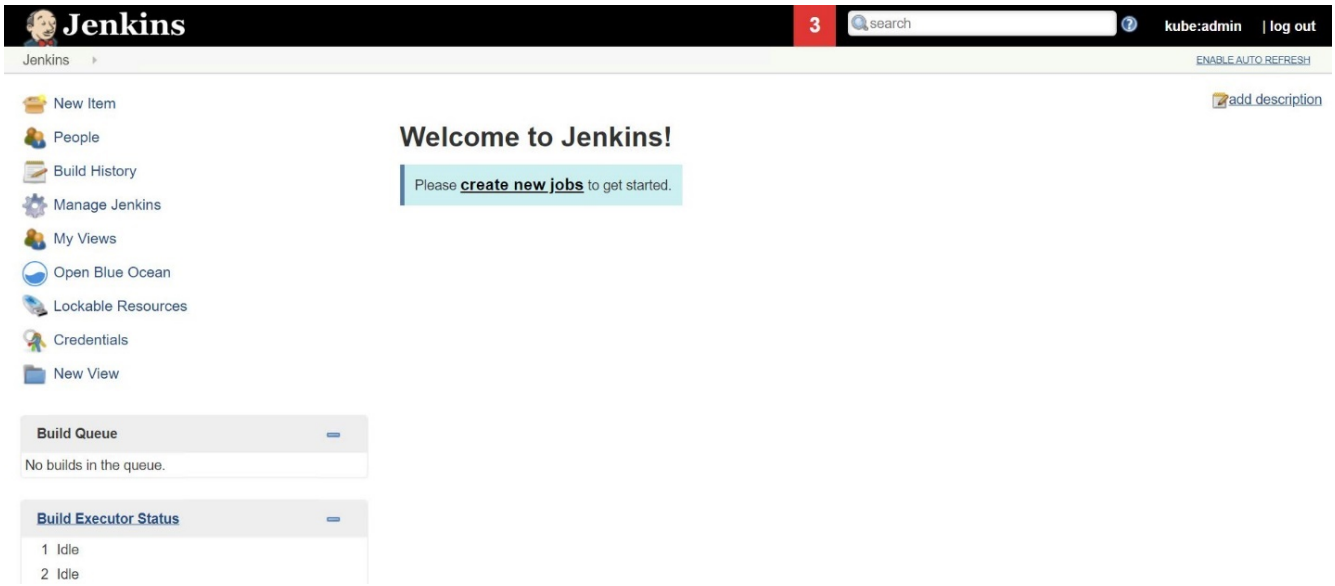
7. Autoriser le compte de service Jenkins à accéder aux utilisateurs OpenShift.



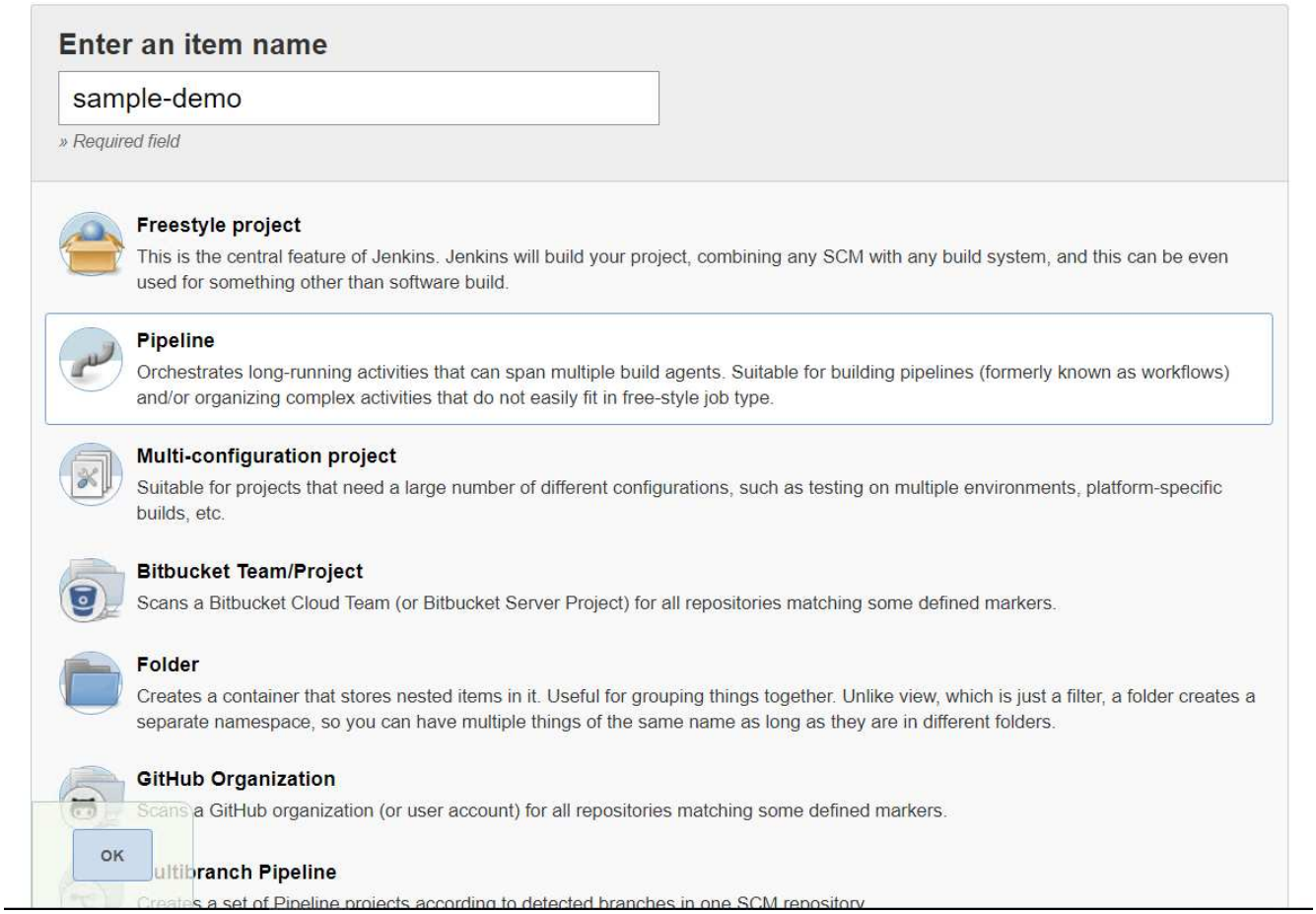
8. La page d’accueil de Jenkins s’affiche. Parce que nous utilisons une construction Maven, terminez d’abord l’installation Maven. Accédez à Manage Jenkins > Global Tool Configuration, puis, dans le sous-titre Maven, cliquez sur Add Maven. Entrez le nom de votre choix et assurez-vous que l’option installer automatiquement est sélectionnée. Cliquez sur Enregistrer.



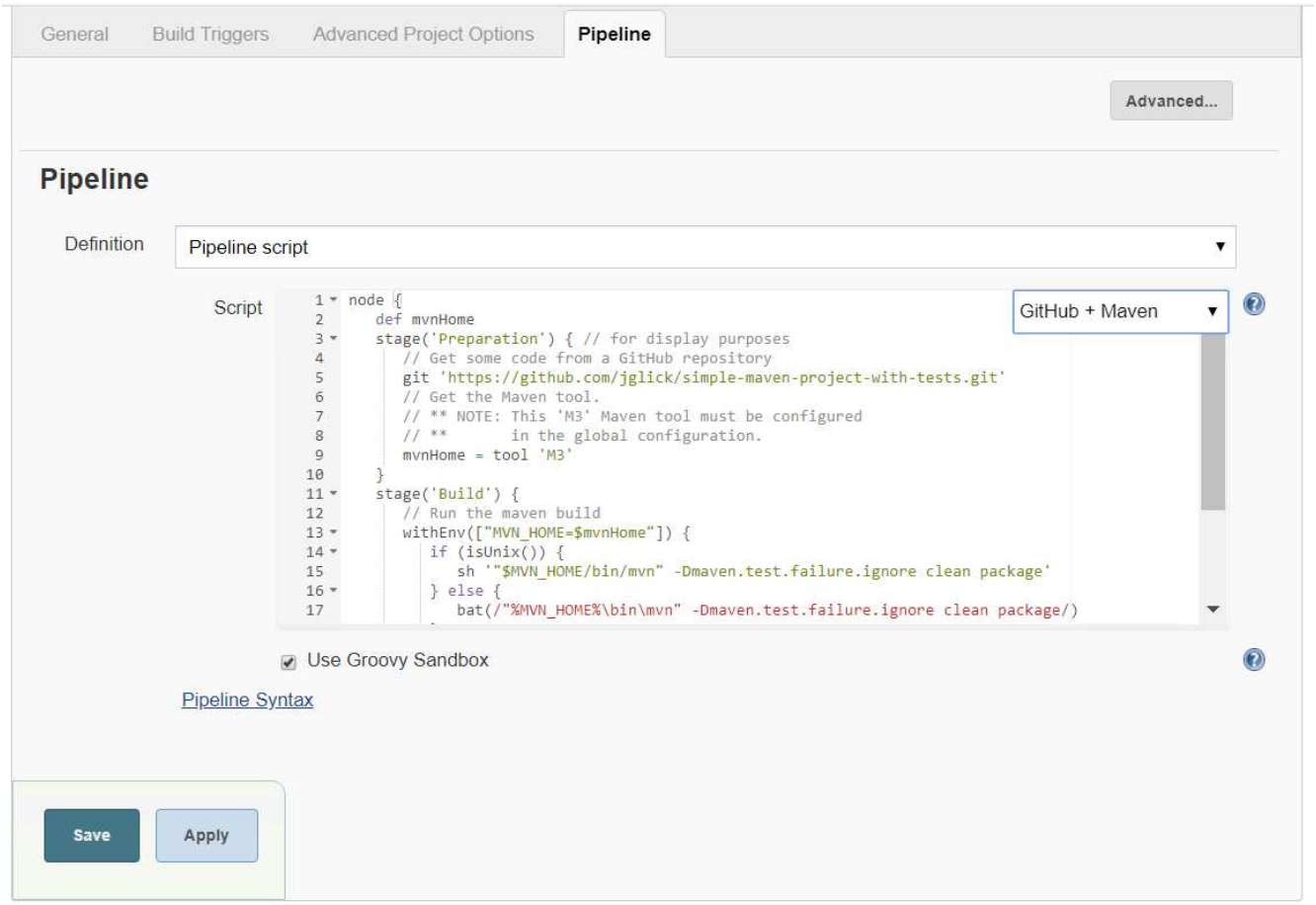
9. Vous pouvez désormais créer un pipeline pour démontrer le workflow ci/CD. Sur la page d'accueil, cliquez sur Créer de nouveaux travaux ou nouvel élément dans le menu de gauche.



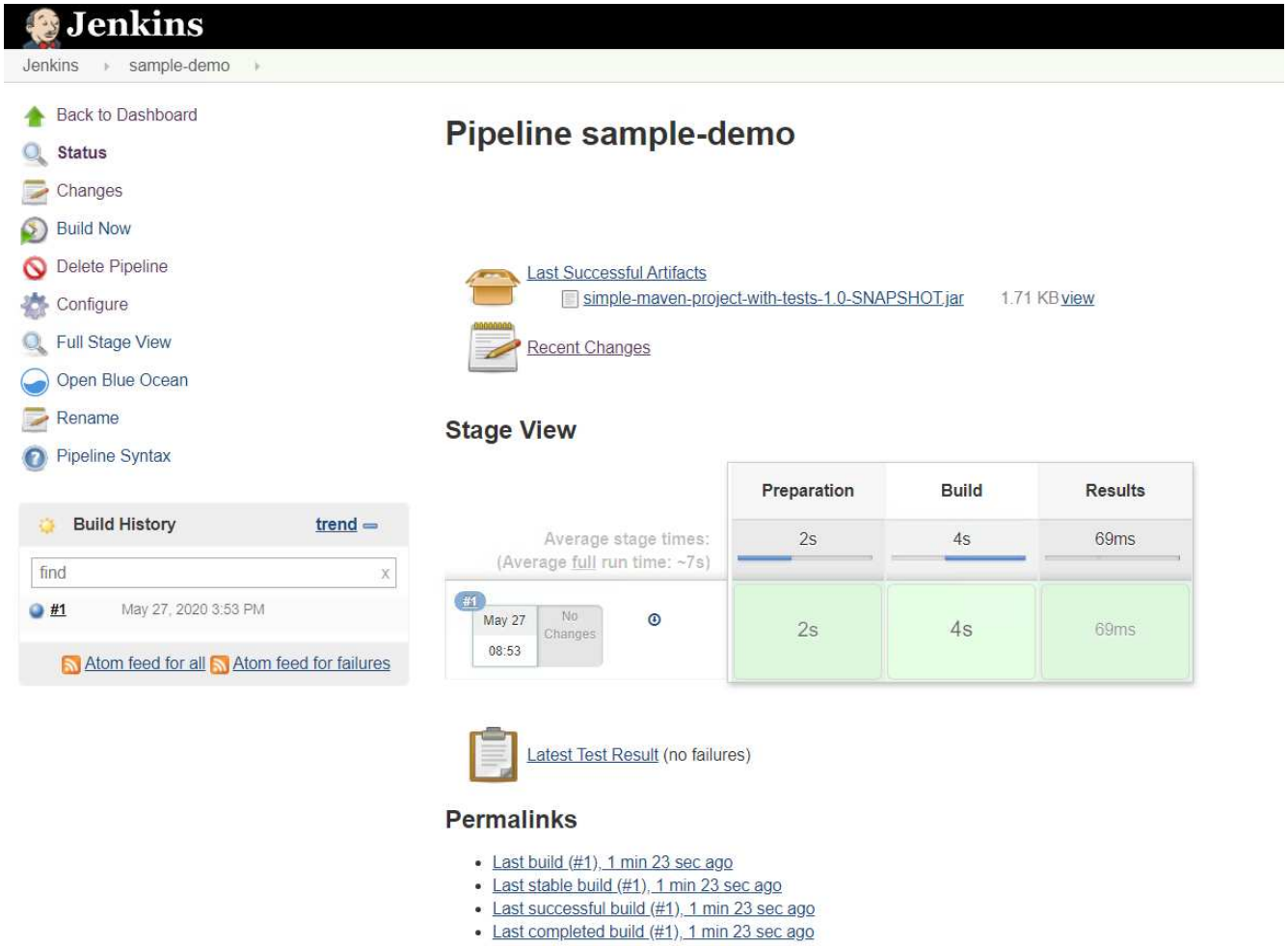
10. Sur la page Créer un élément, entrez le nom de votre choix, sélectionnez Pipeline, puis cliquez sur OK.



11. Sélectionnez l'onglet Pipeline. Dans le menu déroulant essayer un pipeline d'échantillon, sélectionnez Github + Maven. Le code est automatiquement renseigné. Cliquez sur Enregistrer.



12. Cliquez sur Créer maintenant pour déclencher le développement tout au long de la phase de préparation, de création et de test. Il peut prendre plusieurs minutes pour terminer l'ensemble du processus de construction et afficher les résultats de la construction.



13. Chaque fois que du code change, le pipeline peut être reconstruit pour corriger la nouvelle version du logiciel permettant l'intégration et la livraison continues. Cliquez sur modifications récentes pour suivre les modifications apportées à la version précédente.

Configurer la colocation sur Red Hat OpenShift avec NetApp ONTAP

Configuration d’une colocation sur Red Hat OpenShift avec NetApp

De nombreuses entreprises qui exécutent plusieurs applications ou charges de travail sur des conteneurs ont tendance à déployer un cluster Red Hat OpenShift par application ou par workload. Ils peuvent ainsi mettre en œuvre une isolation stricte pour l’application ou la charge de travail, optimiser les performances et réduire les vulnérabilités de sécurité. Toutefois, le déploiement d’un cluster Red Hat OpenShift distinct pour chaque application présente ses propres problèmes. Cette solution augmente les frais d’exploitation liés à la surveillance et à la gestion seule de chaque cluster, ce qui augmente les coûts du fait de ressources dédiées pour différentes applications et entrave l’évolutivité efficace.

Pour résoudre ces problèmes, il est possible d’exécuter toutes les applications ou charges de travail dans un seul cluster Red Hat OpenShift. Cependant, dans une telle architecture, l’isolement des ressources et les vulnérabilités liées à la sécurité des applications constituent l’un des défis majeurs. Toute vulnérabilité de sécurité dans une charge de travail pourrait naturellement se répandre sur une autre charge de travail, augmentant ainsi la zone d’impact. En outre, une application peut avoir une incidence soudaine et non contrôlée sur les performances d’une autre application, car il n’existe pas de stratégie d’allocation des ressources par défaut.

Les entreprises recherchent donc des solutions qui offrent les meilleures des deux mondes, par exemple, en leur permettant d'exécuter toutes leurs charges de travail dans un cluster unique, tout en offrant les avantages d'un cluster dédié pour chaque charge de travail.

L'une de ces solutions est utile : configurer la colocation sur Red Hat OpenShift. La colocation est une architecture qui permet à plusieurs locataires de coexister sur un même cluster avec une isolation appropriée des ressources, de la sécurité, etc. Dans ce contexte, un locataire peut être considéré comme un sous-ensemble des ressources du cluster qui sont configurées pour être utilisées par un groupe d'utilisateurs particulier à des fins exclusives. La configuration d'une colocation sur un cluster Red Hat OpenShift offre les avantages suivants :

- Réduction des dépenses d'investissement et d'exploitation en permettant le partage des ressources du cluster
- Réduisez les frais d'exploitation et de gestion
- Sécurisation des charges de travail contre toute contamination croisée des failles de sécurité
- Protection des charges de travail contre la dégradation inattendue des performances en raison des conflits des ressources

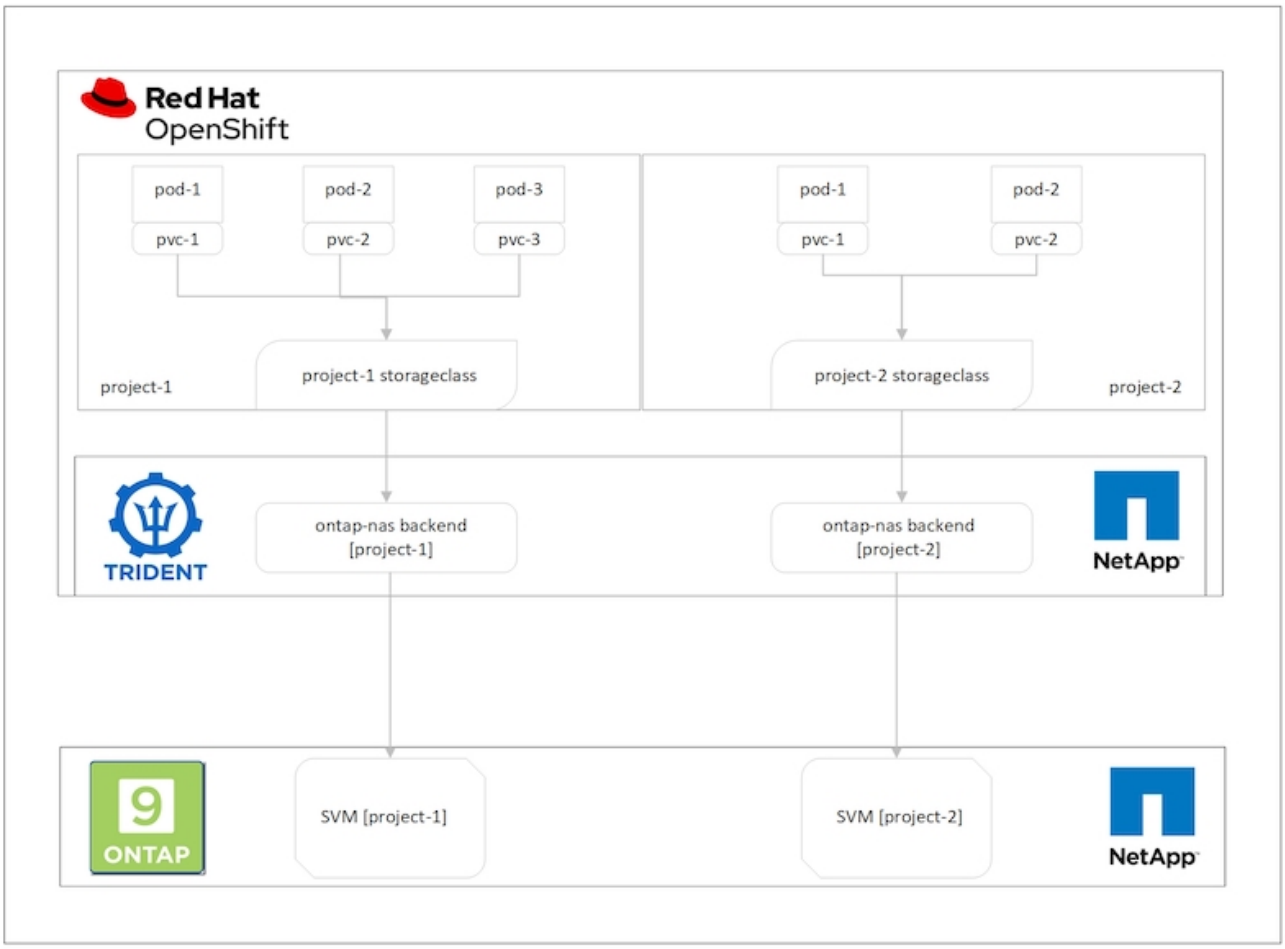
Pour un cluster OpenShift mutualisé entièrement réalisé, les quotas et les restrictions doivent être configurés pour les ressources de cluster appartenant à différents compartiments de ressources : calcul, stockage, réseau, sécurité, etc. Bien que nous aborderons certains aspects de toutes les ressources de cette solution, Nous mettons l'accent sur les bonnes pratiques d'isolation et de sécurisation des données servies ou consommées par plusieurs charges de travail sur le même cluster Red Hat OpenShift en configurant la colocation sur des ressources de stockage allouées de façon dynamique par Astra Trident et sauvegardé par NetApp ONTAP.

Architecture

Bien que Red Hat OpenShift et Astra Trident avec NetApp ONTAP ne assurent pas l'isolation des charges de travail par défaut, ils offrent un large éventail de fonctionnalités qui peuvent être utilisées pour configurer la colocation. Pour mieux comprendre comment concevoir une solution mutualisée sur un cluster Red Hat OpenShift avec Astra Trident basée sur NetApp ONTAP, nous examinons un exemple d'exigences et nous présente la configuration qui l'entoure.

Supposons qu'une entreprise exécute deux de ses charges de travail sur un cluster Red Hat OpenShift dans le cadre de deux projets sur lesquels deux équipes différentes travaillent. Les données de ces workloads résident sur des demandes de volume persistant qui sont provisionnées dynamiquement par Astra Trident sur un back-end NAS NetApp ONTAP. L'entreprise doit concevoir une solution mutualisée pour ces deux charges de travail et isoler les ressources utilisées pour ces projets afin de garantir la sécurité et la performance nécessaires. Elle est axée sur les données qui servent ces applications.

La figure suivante décrit la solution mutualisée sur un cluster Red Hat OpenShift avec Astra Trident et NetApp ONTAP.



Exigences technologiques

1. Cluster de stockage NetApp ONTAP
2. Cluster Red Hat OpenShift
3. Astra Trident

Ressources Red Hat OpenShift – Cluster

Du point de vue du cluster Red Hat OpenShift, la ressource de premier niveau à commencer est le projet. Un projet OpenShift peut être considéré comme une ressource de cluster qui divise l'ensemble du cluster OpenShift en plusieurs clusters virtuels. Ainsi, l'isolation au niveau du projet fournit une base pour la configuration de la colocation.

Ensuite, vous devez configurer RBAC dans le cluster. La meilleure pratique consiste à configurer tous les développeurs sur un seul projet ou charge de travail dans un seul groupe d'utilisateurs du fournisseur d'identités. Red Hat OpenShift permet l'intégration IDP et la synchronisation des groupes d'utilisateurs, ce qui permet d'importer les utilisateurs et les groupes du PDI dans le cluster. Les administrateurs du cluster peuvent ainsi isoler l'accès aux ressources du cluster dédiées à un projet à un ou plusieurs groupes d'utilisateurs travaillant sur ce projet, ce qui limite l'accès non autorisé aux ressources du cluster. Pour en savoir plus sur l'intégration IDP avec Red Hat OpenShift, consultez la documentation "ici".

NetApp ONTAP

Il est important d'isoler le service de stockage partagé en tant que fournisseur de stockage persistant pour un cluster Red Hat OpenShift afin de vérifier que les volumes créés sur le stockage pour chaque projet apparaissent aux hôtes comme s'ils sont créés sur un stockage distinct. Pour ce faire, créez autant de SVM (Storage Virtual machines) sur NetApp ONTAP que des projets ou des charges de travail et dédier chaque SVM à une charge de travail.

Astra Trident

Une fois que vous avez des SVM différents pour les projets créés sur NetApp ONTAP, vous devez mapper chaque SVM sur un back-end Trident différent. La configuration back-end de Trident entraîne l'allocation du stockage persistant aux ressources de cluster OpenShift, et elle requiert le mappage des détails de la SVM sur. Il doit s'agir du pilote de protocole pour le back-end au minimum. Vous pouvez également définir la manière dont les volumes sont provisionnés sur le stockage et définir des limites pour la taille des volumes ou l'utilisation des agrégats, etc. Vous trouverez des informations détaillées sur la définition des systèmes back-end Trident "ici".

Red Hat OpenShift – ressources de stockage

Une fois les systèmes back-end Trident configurés, l'étape suivante consiste à configurer les classes de stockage. Configurez autant de classes de stockage que les systèmes back-end, en donnant à chaque classe de stockage l'accès pour lancer des volumes sur un seul système back-end. Nous pouvons mapper la classe de stockage sur un back-end Trident en utilisant le paramètre storagePools lors de la définition de la classe de stockage. Les détails de la définition d'une classe de stockage sont disponibles "ici". Il existe donc un mappage un-à-un de StorageClass vers le backend Trident qui pointe vers un SVM. Ainsi, toutes les demandes de stockage traitées par la classe de stockage allouée à ce projet sont servies par la SVM dédiée à ce projet uniquement.

Comme les classes de stockage ne namesles ressources qui ne sont pas adaptées, comment pouvons-nous nous assurer que les déclarations de stockage présentées dans la classe d'un projet par des pods dans un autre espace de noms ou dans des projets sont rejetées ? La réponse est d'utiliser ResourceQuotas. ResourceQuotas sont des objets qui contrôlent l'utilisation totale des ressources par projet. Elle peut limiter le nombre ainsi que la quantité totale de ressources pouvant être consommées par des objets dans le projet. Presque toutes les ressources d'un projet peuvent être limitées à l'aide de ResourceQuotas et l'utilisation efficace de cette solution peut aider les entreprises à réduire les coûts et les pannes dus au sur-provisionnement ou à la sur-consommation des ressources. Reportez-vous à la documentation "ici" pour en savoir plus.

Pour ce cas d'utilisation, nous devons limiter les demandes de stockage provenant de classes de stockage qui ne sont pas dédiées à leur projet dans un projet particulier. Il nous faut donc limiter les demandes de volume persistant pour d'autres classes de stockage par paramètre `<storage-class-name>.storageclass.storage.k8s.io/persistentvolumeclaims` à 0. En outre, un administrateur de cluster doit s'assurer que les développeurs d'un projet ne doivent pas avoir accès pour modifier les ResourceQuotas.

Configuration

N'importe quelle solution mutualisée permet à aucun utilisateur d'accéder à davantage de ressources du cluster que nécessaire. Ainsi, l'ensemble des ressources à configurer dans le cadre de la configuration de colocation est divisé entre l'administrateur cluster, l'administrateur stockage et les développeurs travaillant sur chaque projet.

Le tableau suivant présente les différentes tâches à effectuer par différents utilisateurs :

Rôle	Tâches
Cluster-admin	Créez des projets pour différentes applications ou charges de travail
	Créez ClusterRoles et roles pour Storage-admin
	Créez des rôles et des roleliaisons pour les développeurs qui assignaient un accès à des projets spécifiques
	[Facultatif] configurez les projets pour planifier des pods sur des nœuds spécifiques
Storage-admin	Créez des SVM sur NetApp ONTAP
	Création des systèmes back-end Trident
	Créez des classes de stockage
	Créer des devis de ressources de stockage
Développeurs	Valider l'accès pour créer ou corriger des demandes de volume persistant ou des pods dans le projet affecté
	Valider l'accès pour créer ou corriger des demandes de volume persistant ou des pods dans un autre projet
	Validez l'accès pour afficher ou modifier des projets, des ResourceQuotas et des classes de stockage

Configuration

Prérequis

- Cluster NetApp ONTAP
- Cluster Red Hat OpenShift
- Trident est installé sur le cluster
- Station de travail Admin avec les outils tridentctl et oc installés et ajoutés à $PATH
- Accès administrateur à ONTAP
- L'accès cluster-admin au cluster OpenShift
- Le cluster est intégré avec Identity Provider
- Le fournisseur d'identités est configuré pour distinguer efficacement les utilisateurs de différentes équipes

Configuration : tâches d'administration du cluster

Les tâches suivantes sont réalisées par Red Hat OpenShift Cluster-admin :

1. Connectez-vous au cluster Red Hat OpenShift en tant qu'administrateur cluster.
2. Créer deux projets correspondant à différents projets.

```
oc create namespace project-1
oc create namespace project-2
```

3. Créer le rôle de développeur du projet-1.

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-1
  name: developer-project-1
rules:
  - verbs:
      - '*'
    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
  - verbs:
      - '*'
    apiGroups:
      - ''
    resources:
      - bindings
      - configmaps
      - endpoints
      - events
      - persistentvolumeclaims
      - pods
      - pods/log
      - pods/attach
      - podtemplates
      - replicationcontrollers
```

```
      - services
      - limitranges
      - namespaces
      - componentstatuses
      - nodes
  - verbs:
      - '*'
    apiGroups:
      - trident.netapp.io
    resources:
      - tridentsnapshots
EOF
```

La définition de rôle fournie dans cette section n'est qu'un exemple. Les rôles de développeur doivent être définis en fonction des exigences de l'utilisateur final.

1. De la même façon, créez des rôles de développement pour Project-2.
2. Toutes les ressources de stockage OpenShift et NetApp sont généralement gérées par un administrateur du stockage. L'accès pour les administrateurs du stockage est contrôlé par le rôle de l'opérateur trident créé lors de l'installation de Trident. En outre, l'administrateur du stockage nécessite également l'accès à ResourceQuotas pour contrôler la consommation du stockage.
3. Créez un rôle pour gérer ResourceQuotas dans tous les projets du cluster afin de le relier à l'administrateur de stockage.

```
cat << EOF | oc create -f -
kind: ClusterRole
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: resource-quotas-role
rules:
  - verbs:
      - '*'
    apiGroups:
      - ''
    resources:
      - resourcequotas
  - verbs:
      - '*'
    apiGroups:
      - quota.openshift.io
    resources:
      - '*'
EOF
```

4. Assurez-vous que le cluster est intégré au fournisseur d'identité de l'entreprise et que les groupes d'utilisateurs sont synchronisés avec les groupes de clusters. L'exemple suivant montre que le fournisseur d'identités a été intégré au cluster et synchronisé avec les groupes d'utilisateurs.

```
$ oc get groups
NAME                          USERS
ocp-netapp-storage-admins     ocp-netapp-storage-admin
ocp-project-1                 ocp-project-1-user
ocp-project-2                 ocp-project-2-user
```

1. Configurer les liaisons ClusterRoleBindages pour les administrateurs de stockage.

```
cat << EOF | oc create -f -
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-trident-operator
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: trident-operator
---
kind: ClusterRoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: netapp-storage-admin-resource-quotas-cr
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-netapp-storage-admins
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: resource-quotas-role
EOF
```

Pour les administrateurs du stockage, deux rôles doivent être liés : trident-Operator et Resource-quotas.

1. Créer des liaisons de type rôle pour les développeurs liant le rôle développeur-projet-1 au groupe correspondant (ocp-project-1) dans Project-1.

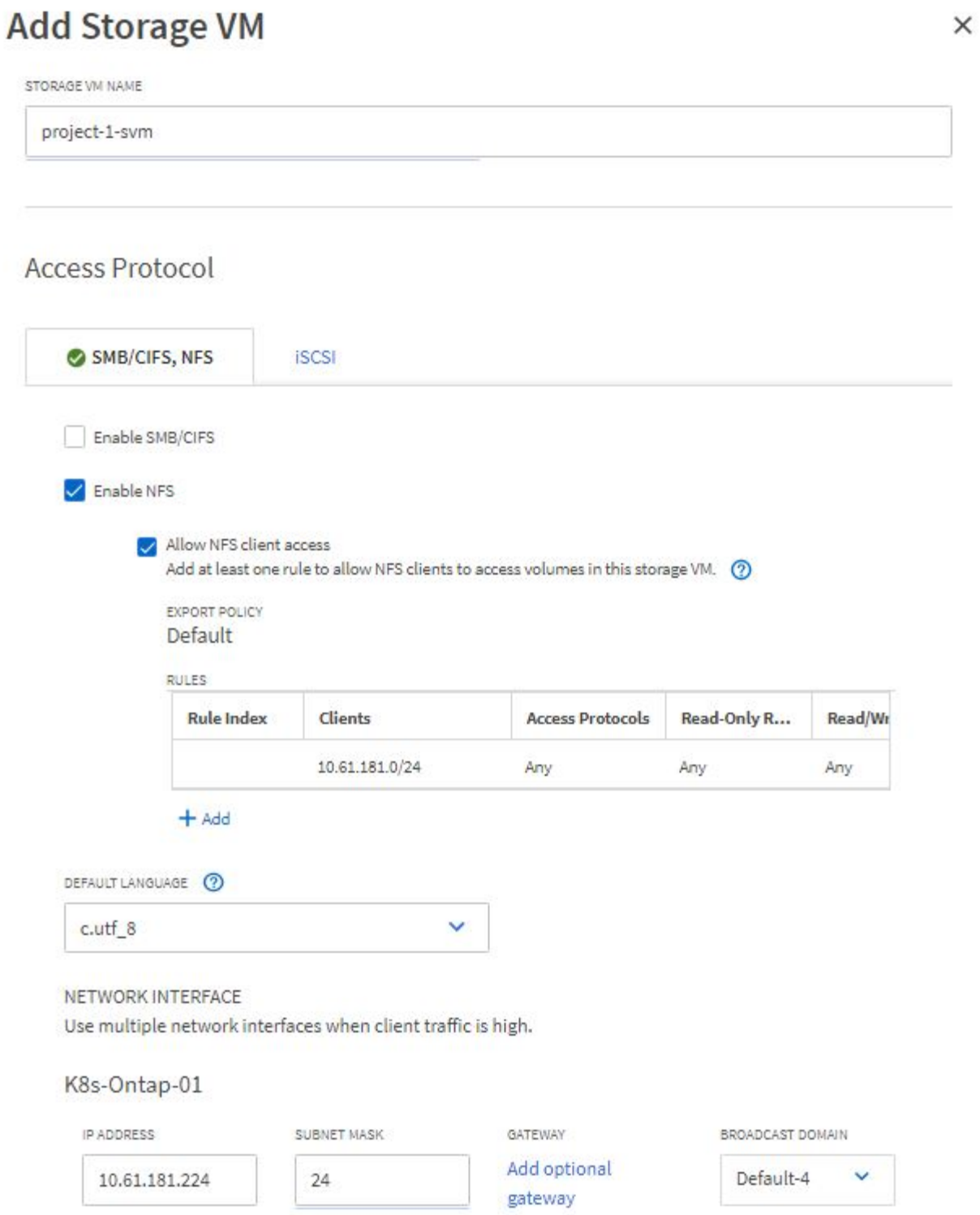
```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-1-developer
  namespace: project-1
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-project-1
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-1
EOF
```

2. De même, créez des liaisons de type rôle pour les développeurs qui lient les rôles de développeur au groupe d'utilisateurs correspondant dans Project-2.

Configuration : tâches d'administration du stockage

Les ressources suivantes doivent être configurées par un administrateur de stockage :

1. Connectez-vous au cluster NetApp ONTAP en tant qu'administrateur.
2. Accédez à Storage > Storage VM et cliquez sur Add. Créer deux SVM, un pour le projet-1 et l'autre pour le projet-2, en fournissant les détails requis. Créer également un compte vsadmin pour gérer le SVM et ses ressources



1. Connectez-vous au cluster Red Hat OpenShift en tant qu'administrateur du stockage.
2. Créer le backend pour projet-1 et le mapper au SVM dédié au projet NetApp recommande d'utiliser le compte vsadmin du SVM afin de connecter le backend au SVM au lieu d'utiliser l'administrateur du cluster ONTAP

```
cat << EOF | tridentctl -n trident create backend -f
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "nfs_project_1",
    "managementLIF": "172.21.224.210",
    "dataLIF": "10.61.181.224",
    "svm": "project-1-svm",
    "username": "vsadmin",
    "password": "NetApp123"
}
EOF
```

Nous utilisons le pilote ontap-nas dans cet exemple. Utilisez le pilote approprié lors de la création du back-end en fonction du cas d'utilisation.

Nous partons du principe que Trident est installé dans le projet trident.

1. Créer de la même manière le back-end Trident pour le projet-2 et le mapper sur le SVM dédié au projet-2.
2. Créez ensuite les classes de stockage. Créez la classe de stockage pour Project-1 et configurez-la pour utiliser les pools de stockage du back-end dédié au projet-1 en définissant le paramètre storagePools.

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-1-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_1:.*"
EOF
```

3. De même, créez une classe de stockage pour Project-2 et configurez-la pour utiliser les pools de stockage du système back-end dédié au projet-2.
4. Créer un Resourcequota pour limiter les ressources dans le projet-1 demandant le stockage de storageclasses dédiés à d'autres projets.

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-1-sc-rq
  namespace: project-1
spec:
  hard:
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

5. De même, créez un Resourcequota pour limiter les ressources du projet 2 demandant du stockage de storageclasses dédiés à d'autres projets.

Validation

Pour valider l'architecture mutualisée configurée lors des étapes précédentes, procédez comme suit :

Valider l'accès pour créer des demandes de volume persistant ou des pods dans le projet attribué

1. Connectez-vous en tant qu'utilisateur ocp-project-1, développeur dans Project-1.
2. Vérifiez l'accès pour créer un nouveau projet.

```
oc create ns sub-project-1
```

3. Créez un PVC dans Project-1 en utilisant le storageclass affecté au projet-1.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

4. Vérifiez le volume persistant associé à la demande de volume persistant.

```
oc get pv
```

5. Vérifiez que le volume persistant et son volume sont créés dans un SVM dédié à Project-1 sur NetApp ONTAP.

```
volume show -vserver project-1-svm
```

6. Créez un pod dans Project-1 et montez le PVC créé à l'étape précédente.

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  volumes:
    - name: test-pvc-project-1
      persistentVolumeClaim:
       claimName: test-pvc-project-1
  containers:
    - name: test-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
      volumeMounts:
        - mountPath: "/usr/share/nginx/html"
          name: test-pvc-project-1
EOF
```

7. Vérifiez si le pod est en cours d'exécution et si il a monté le volume.

```
oc describe pods test-pvc-pod -n project-1
```

Valider l'accès pour créer des demandes de volume persistant ou des pods dans un autre projet ou utiliser des ressources dédiées à un autre projet

1. Connectez-vous en tant qu'utilisateur ocp-project-1, développeur dans Project-1.
2. Créez un PVC dans Project-1 en utilisant le storageclass affecté au projet-2.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-1-sc-2
  namespace: project-1
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-2-sc
EOF
```

3. Création d'une demande de volume persistant dans Project-2.

```
cat << EOF | oc create -f -
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: test-pvc-project-2-sc-1
  namespace: project-2
  annotations:
    trident.netapp.io/reclaimPolicy: Retain
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: project-1-sc
EOF
```

4. Assurez-vous que les ESV `test-pvc-project-1-sc-2` et `test-pvc-project-2-sc-1` n'ont pas été créés.

```
oc get pvc -n project-1
oc get pvc -n project-2
```

5. Créez un pod dans Project-2.

```
cat << EOF | oc create -f -
kind: Pod
apiVersion: v1
metadata:
  name: test-pvc-pod
  namespace: project-1
spec:
  containers:
    - name: test-container
      image: nginx
      ports:
        - containerPort: 80
          name: "http-server"
EOF
```

Validez l’accès pour afficher et modifier les projets, ResourceQuotas et Storageclasses

1. Connectez-vous en tant qu’utilisateur ocp-project-1, développeur dans Project-1.
2. Vérifiez l’accès pour créer de nouveaux projets.

```
oc create ns sub-project-1
```

3. Valider l’accès pour afficher les projets.

```
oc get ns
```

4. Vérifiez si l’utilisateur peut afficher ou modifier ResourceQuotas dans Project-1.

```
oc get resourcequotas -n project-1
oc edit resourcequotas project-1-sc-rq -n project-1
```

5. Vérifiez que l’utilisateur a accès à l’affichage des données de stockage.

```
oc get sc
```

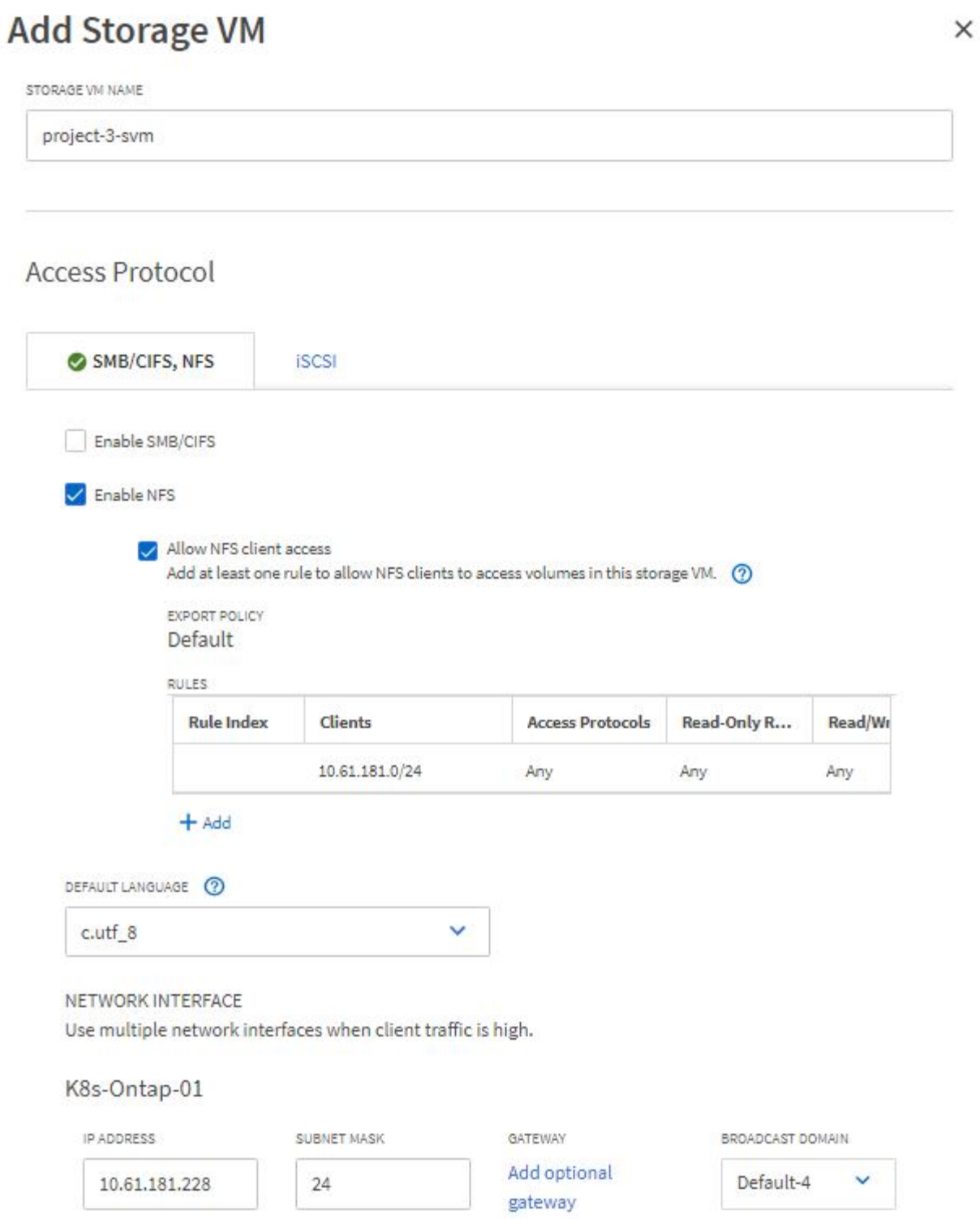
6. Vérifiez l’accès pour décrire les storageclasses.
7. Validez l’accès de l’utilisateur pour modifier les storageclasses.

```
oc edit sc project-1-sc
```

Évolutivité : ajout de projets

Dans une configuration mutualisée, l'ajout de nouveaux projets avec des ressources de stockage nécessite une configuration supplémentaire pour garantir que la colocation n'est pas respectée. Pour ajouter d'autres projets dans un cluster mutualisé, effectuez les opérations suivantes :

1. Connectez-vous au cluster NetApp ONTAP en tant qu'administrateur du stockage.
2. Accédez à `Storage → Storage VMs` et cliquez sur `Add`. Créez un nouveau SVM dédié au projet-3. Créer également un compte vsadmin pour gérer le SVM et ses ressources



1. Connectez-vous au cluster Red Hat OpenShift en tant qu'administrateur de cluster.
2. Créer un nouveau projet.

```
oc create ns project-3
```

3. Assurez-vous que le groupe d'utilisateurs du projet Project-3 est créé sur IDP et synchronisé avec le

cluster OpenShift.

```
oc get groups
```

4. Créer le rôle de développeur du projet-3.

```
cat << EOF | oc create -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: Role
metadata:
  namespace: project-3
  name: developer-project-3
rules:
  - verbs:
      - '*'
    apiGroups:
      - apps
      - batch
      - autoscaling
      - extensions
      - networking.k8s.io
      - policy
      - apps.openshift.io
      - build.openshift.io
      - image.openshift.io
      - ingress.operator.openshift.io
      - route.openshift.io
      - snapshot.storage.k8s.io
      - template.openshift.io
    resources:
      - '*'
  - verbs:
      - '*'
    apiGroups:
      - ''
    resources:
      - bindings
      - configmaps
      - endpoints
      - events
      - persistentvolumeclaims
      - pods
      - pods/log
      - pods/attach
      - podtemplates
```

```
      - replicationcontrollers
      - services
      - limitranges
      - namespaces
      - componentstatuses
      - nodes
  - verbs:
      - '*'
    apiGroups:
      - trident.netapp.io
    resources:
      - tridentsnapshots
EOF
```

> La définition de rôle fournie dans cette section n'est qu'un exemple. Le rôle de développeur doit être défini en fonction des exigences de l'utilisateur final.

1. Créer RoleBinding pour les développeurs dans projet-3 liant le rôle développeur-projet-3 au groupe correspondant (ocp-project-3) dans projet-3.

```
cat << EOF | oc create -f -
kind: RoleBinding
apiVersion: rbac.authorization.k8s.io/v1
metadata:
  name: project-3-developer
  namespace: project-3
subjects:
  - kind: Group
    apiGroup: rbac.authorization.k8s.io
    name: ocp-project-3
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: Role
  name: developer-project-3
EOF
```

2. Connectez-vous au cluster Red Hat OpenShift en tant qu'administrateur du stockage
3. Créer un système back-end Trident et le mapper sur le SVM dédié au projet-3. NetApp recommande d'utiliser le compte vsadmin du SVM afin de connecter le backend au SVM au lieu d'utiliser l'administrateur du cluster ONTAP

```
cat << EOF | tridentctl -n trident create backend -f
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "nfs_project_3",
    "managementLIF": "172.21.224.210",
    "dataLIF": "10.61.181.228",
    "svm": "project-3-svm",
    "username": "vsadmin",
    "password": "NetApp!23"
}
EOF
```

Nous utilisons le pilote ontap-nas dans cet exemple. Utilisez le pilote approprié pour créer le back-end en fonction du cas d'utilisation.

Nous partons du principe que Trident est installé dans le projet trident.

1. Créez la classe de stockage pour Project-3 et configurez-la pour qu'elle utilise les pools de stockage du système back-end dédié au projet-3.

```
cat << EOF | oc create -f -
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: project-3-sc
provisioner: csi.trident.netapp.io
parameters:
  backendType: ontap-nas
  storagePools: "nfs_project_3:.*"
EOF
```

2. Créer un Resourcequota pour limiter les ressources dans le projet-3 demandant du stockage de storageclasses dédié à d'autres projets.

```
cat << EOF | oc create -f -
kind: ResourceQuota
apiVersion: v1
metadata:
  name: project-3-sc-rq
  namespace: project-3
spec:
  hard:
    project-1-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
    project-2-sc.storageclass.storage.k8s.io/persistentvolumeclaims: 0
EOF
```

3. Patch des ResourceQuotas dans d'autres projets pour limiter les ressources de ces projets à l'accès au stockage depuis le storageclass dédié au projet-3.

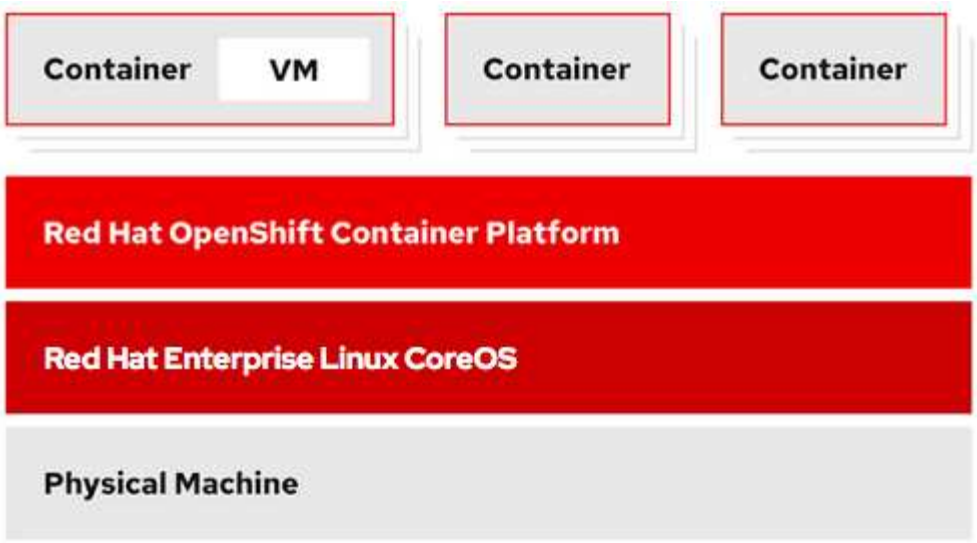
```
oc patch resourcequotas project-1-sc-rq -n project-1 --patch
'{"spec":{"hard":{ "project-3-
sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
oc patch resourcequotas project-2-sc-rq -n project-2 --patch
'{"spec":{"hard":{ "project-3-
sc.storageclass.storage.k8s.io/persistentvolumeclaims": 0}}}'
```

Red Hat OpenShift Virtualization avec NetApp ONTAP

Red Hat OpenShift Virtualization avec NetApp ONTAP

Selon l'utilisation, les conteneurs et les machines virtuelles peuvent servir de plateformes optimales pour différents types d'applications. Par conséquent, de nombreuses entreprises exécutent certaines de leurs workloads sur des conteneurs et certaines sur des VM. Les entreprises doivent souvent relever des challenges supplémentaires : la gestion de plateformes distinctes : un hyperviseur pour les machines virtuelles et un orchestrateur de conteneur pour les applications.

Pour relever ce défi, Red Hat a lancé OpenShift Virtualization (anciennement appelé Container Native Virtualization) à partir de la version 4.6 d'OpenShift. La fonction de virtualisation OpenShift vous permet d'exécuter et de gérer les machines virtuelles avec des conteneurs sur la même installation OpenShift Container Platform. Elle offre une fonctionnalité de gestion hybride permettant d'automatiser le déploiement et la gestion des machines virtuelles par l'intermédiaire des opérateurs. Outre la création de VM dans OpenShift, Red Hat prend également en charge l'importation de VM à partir de VMware vSphere, Red Hat Virtualization et Red Hat OpenStack Platform.



Certaines fonctionnalités comme la migration de VM en direct, le clonage de disques de VM, les snapshots de VM, etc. Sont également prises en charge par OpenShift Virtualization avec l'aide d'Astra Trident, avec le soutien de NetApp ONTAP. Des exemples de chacun de ces flux de travail sont présentés plus loin dans ce document dans leurs sections respectives.

Pour en savoir plus sur Red Hat OpenShift Virtualization, consultez la documentation "ici".

Déploiement pour OpenShift Virtualization

Déploiement de Red Hat OpenShift Virtualization avec NetApp ONTAP

Prérequis

- Un cluster Red Hat OpenShift (version ultérieure à la version 4.6) installé sur une infrastructure bare-Metal avec des nœuds worker RHCOS
- Le cluster OpenShift doit être installé via l'infrastructure provisionnée du programme d'installation (IPI).
- Déploiement de vérifications de l'état des machines pour garantir la haute disponibilité des machines virtuelles
- Un cluster NetApp ONTAP
- Astra Trident installé sur le cluster OpenShift
- Un système back-end Trident configuré avec un SVM sur le cluster ONTAP
- Classe de stockage configurée sur le cluster OpenShift avec Astra Trident en tant que mécanisme de provisionnement
- L'accès cluster-admin au cluster Red Hat OpenShift
- Accès au cluster NetApp ONTAP par administrateur
- Une station de travail d'administration avec des outils tridentctl et oc installés et ajoutés à $PATH

OpenShift Virtualization est gérée par un opérateur installé sur le cluster OpenShift et impose une surcharge supplémentaire pour la mémoire, le processeur et le stockage, ce qui doit être pris en compte lors de la planification des exigences matérielles du cluster. Voir la documentation "ici" pour en savoir plus.

Vous pouvez également spécifier un sous-ensemble des nœuds du cluster OpenShift pour héberger les opérateurs, contrôleurs et VM OpenShift Virtualization en configurant des règles de placement des nœuds.

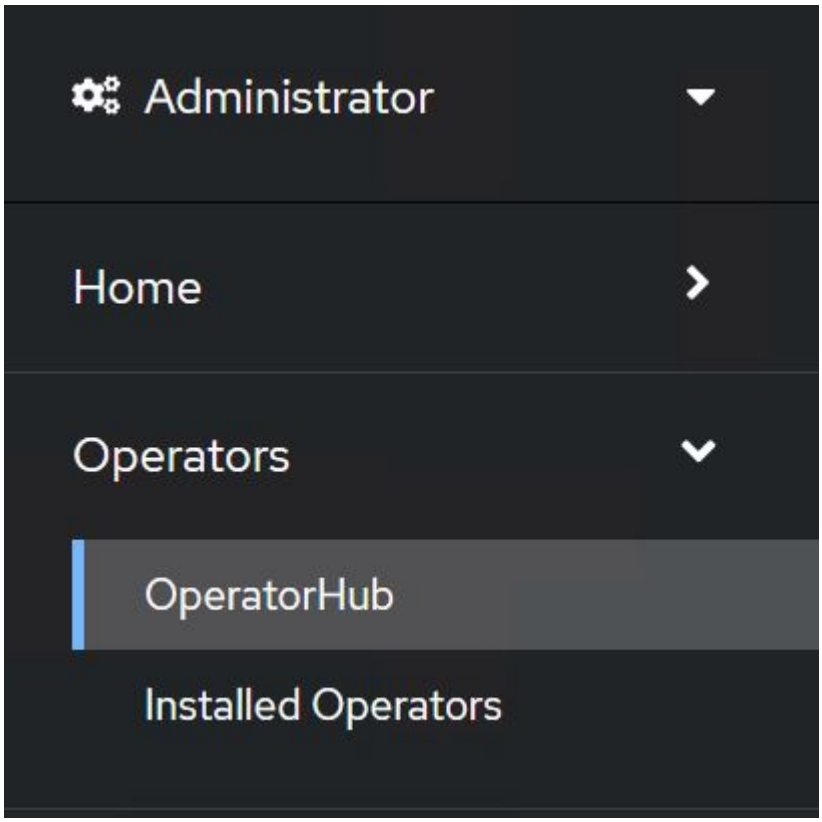
Pour configurer les règles de placement des nœuds pour OpenShift Virtualization, suivez la documentation "ici".

Pour la prise en charge du stockage d'OpenShift Virtualization, NetApp recommande d'utiliser une classe de stockage dédiée qui demande le stockage auprès d'un back-end Trident spécifique, qui est ensuite soutenue par un SVM dédié. Cela permet à un niveau d'architecture en colocation s'agissant des données servies aux charges de travail basées sur des VM du cluster OpenShift.

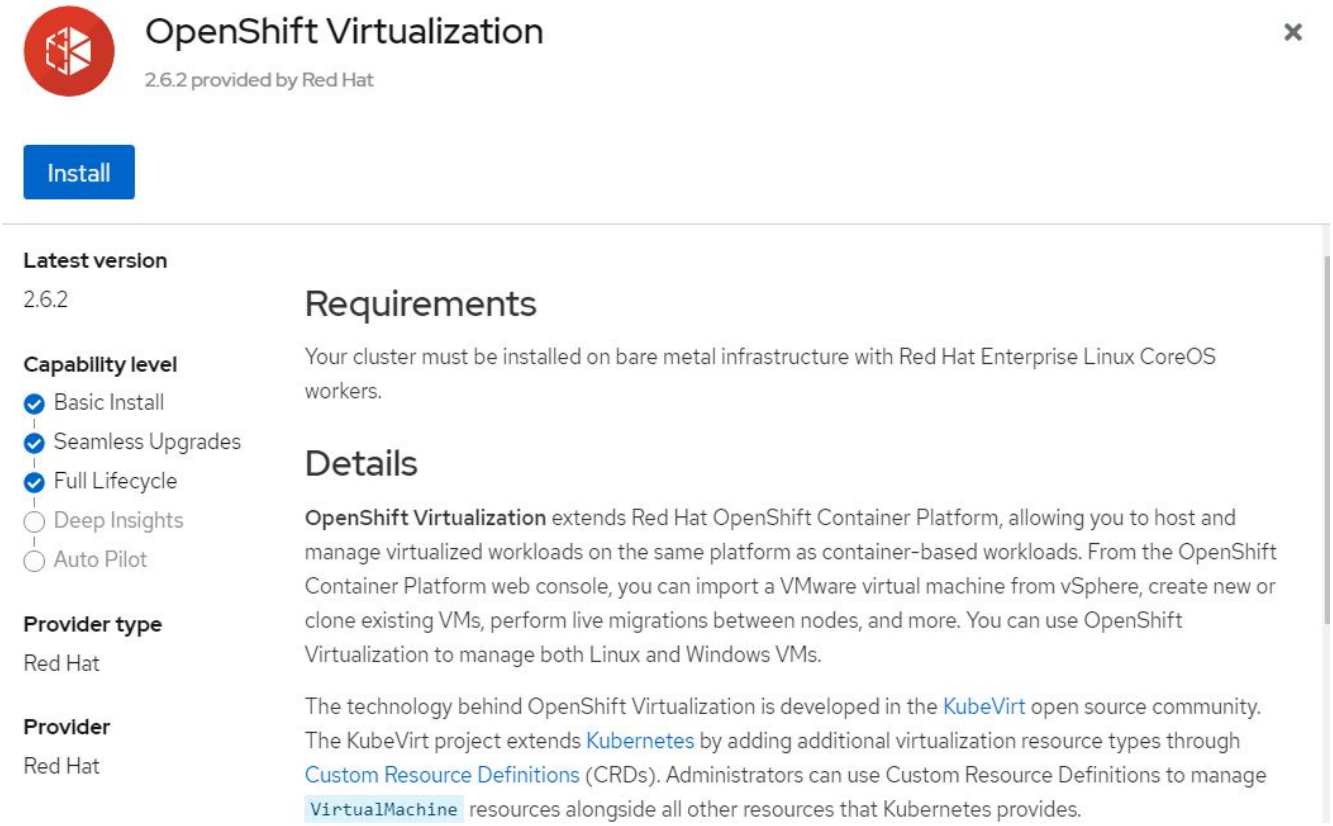
Déploiement de Red Hat OpenShift Virtualization avec NetApp ONTAP

Pour installer OpenShift Virtualization, procédez comme suit :

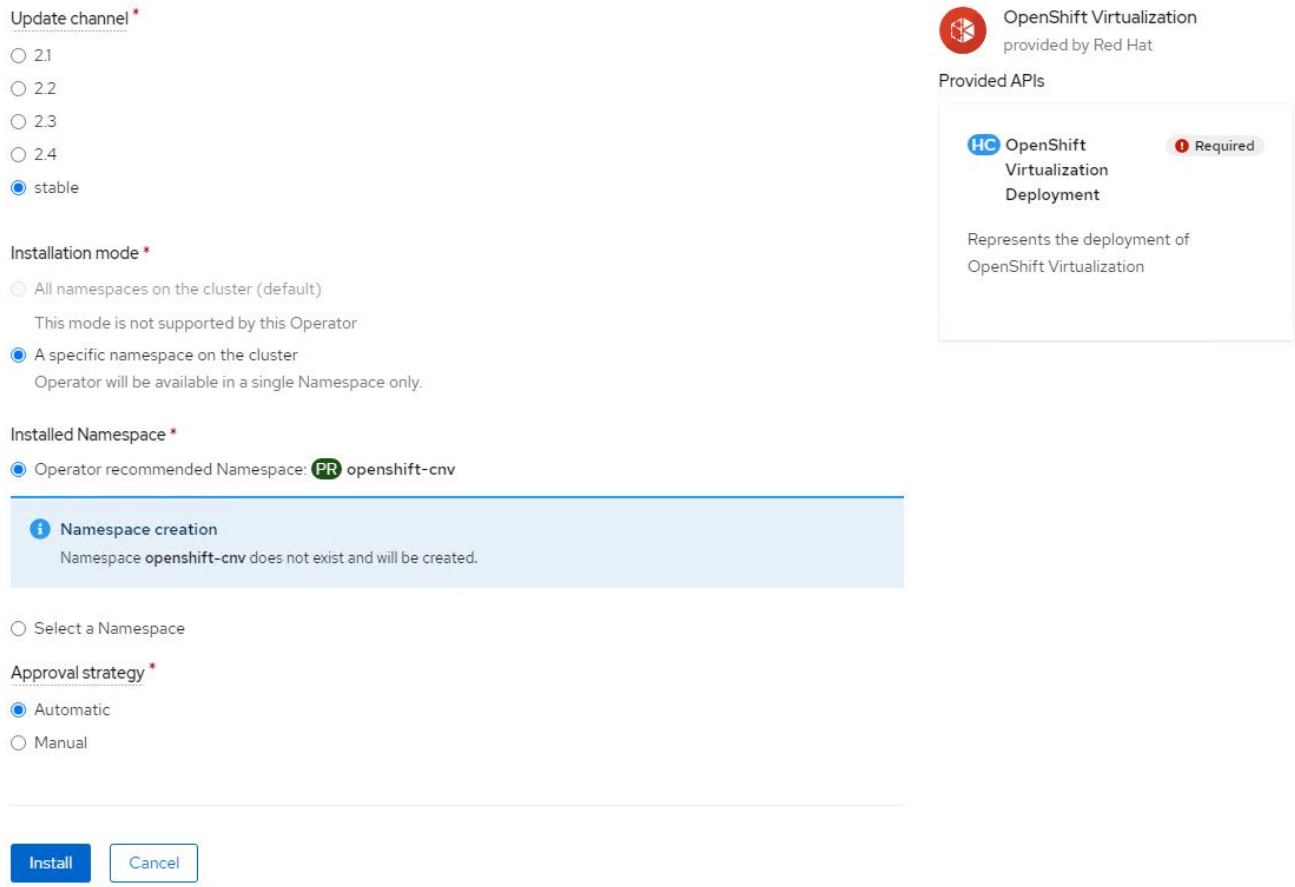
1. Connectez-vous au cluster sans système d'exploitation Red Hat OpenShift avec l'accès cluster-admin.
2. Sélectionnez Administrateur dans la liste déroulante perspective.
3. Accédez à Operators > OperatorHub et recherchez OpenShift Virtualization.



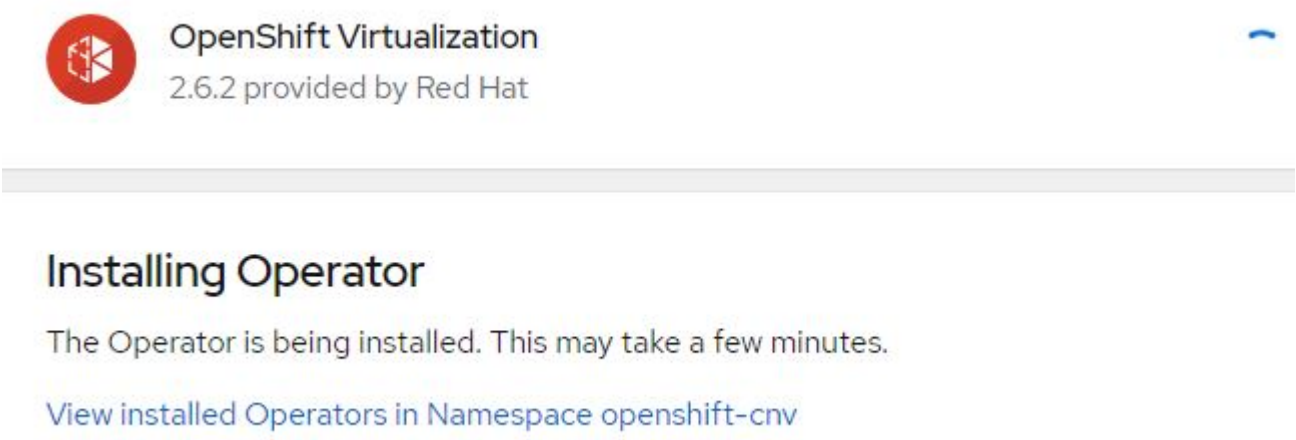
4. Sélectionnez la mosaïque OpenShift Virtualization et cliquez sur Install.



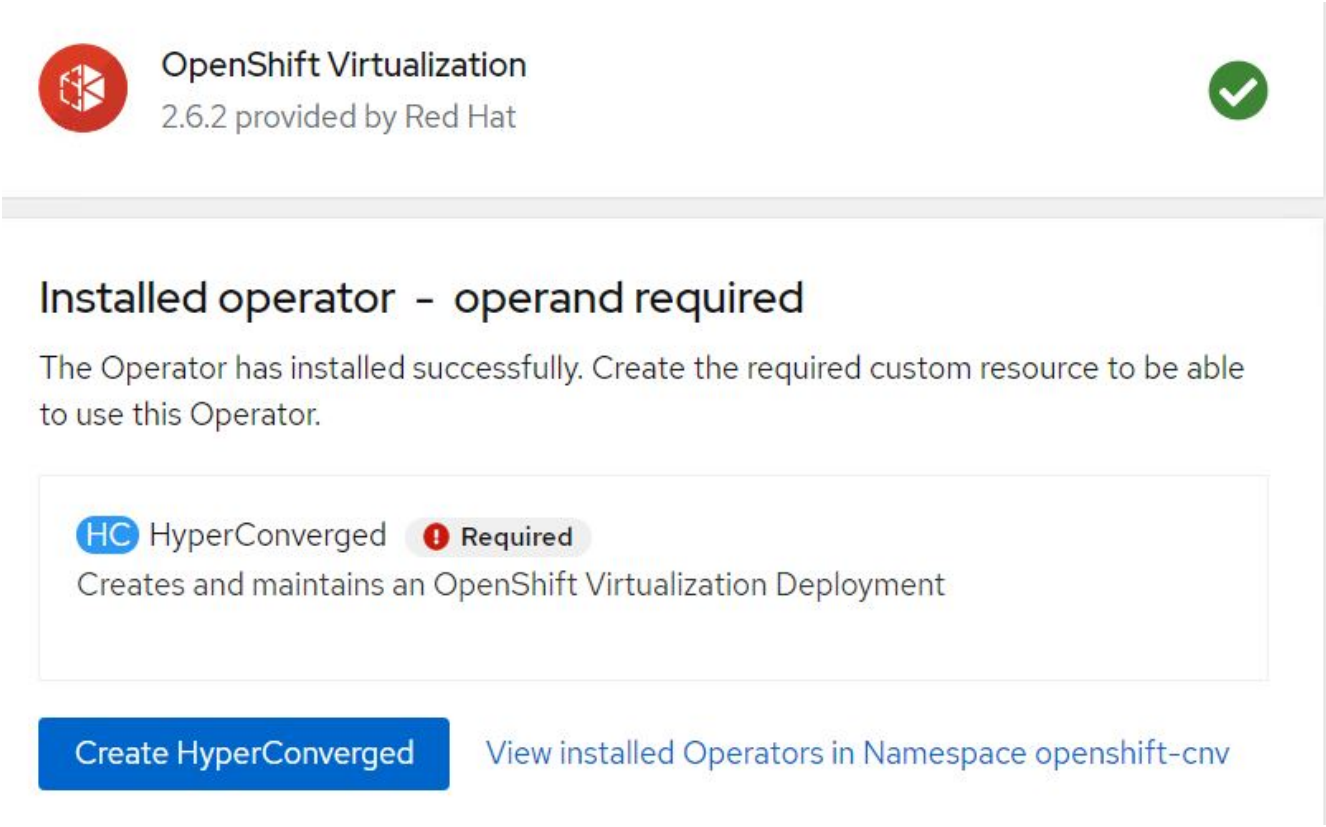
5. Sur l’écran installer l’opérateur, laissez tous les paramètres par défaut et cliquez sur installer.



6. Attendre la fin de l'installation par l'opérateur.



7. Une fois l'opérateur installé, cliquez sur Créer une Hyperconvergé.



8. Sur l'écran Créer une Hyperconvergeance, cliquez sur Créer, accepter tous les paramètres par défaut. Cette étape démarre l'installation d'OpenShift Virtualization.

Name *

kubevirt-hyperconverged

Labels

app=frontend

Infra

infra HyperConvergedConfig influences the pod configuration (currently only placement) for all the infra components needed on the virtualization enabled cluster but not necessarely directly on each node running VMs/VMIs.

Workloads

workloads HyperConvergedConfig influences the pod configuration (currently only placement) of components which need to be running on a node where virtualization workloads should be able to run. Changes to Workloads HyperConvergedConfig can be applied only without existing workload.

Bare Metal Platform

true

BareMetalPlatform indicates whether the infrastructure is baremetal.

Feature Gates

featureGates is a map of feature gate flags. Setting a flag to `true` will enable the feature. Setting `false` or removing the feature gate, disables the feature.

Local Storage Class Name

LocalStorageClassName the name of the local storage class.

Create Cancel

9. Une fois que tous les pods passent à l'état d'exécution dans l'espace de noms openshift-cnv et que l'opérateur OpenShift Virtualization est dans l'état « réussi », l'opérateur est prêt à l'emploi. Les VM peuvent désormais être créés sur le cluster OpenShift.

Project: openshift-cnv

Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation. Or create an Operator and ClusterServiceVersion using the Operator SDK.

Name Search by name...

Name	Managed Namespaces	Status	Last updated	Provided APIs
OpenShift Virtualization 2.6.2 provided by Red Hat	NS openshift-cnv	Succeeded Up to date	May 18, 8:02 pm	OpenShift Virtualization Deployment HostPathProvisioner deployment

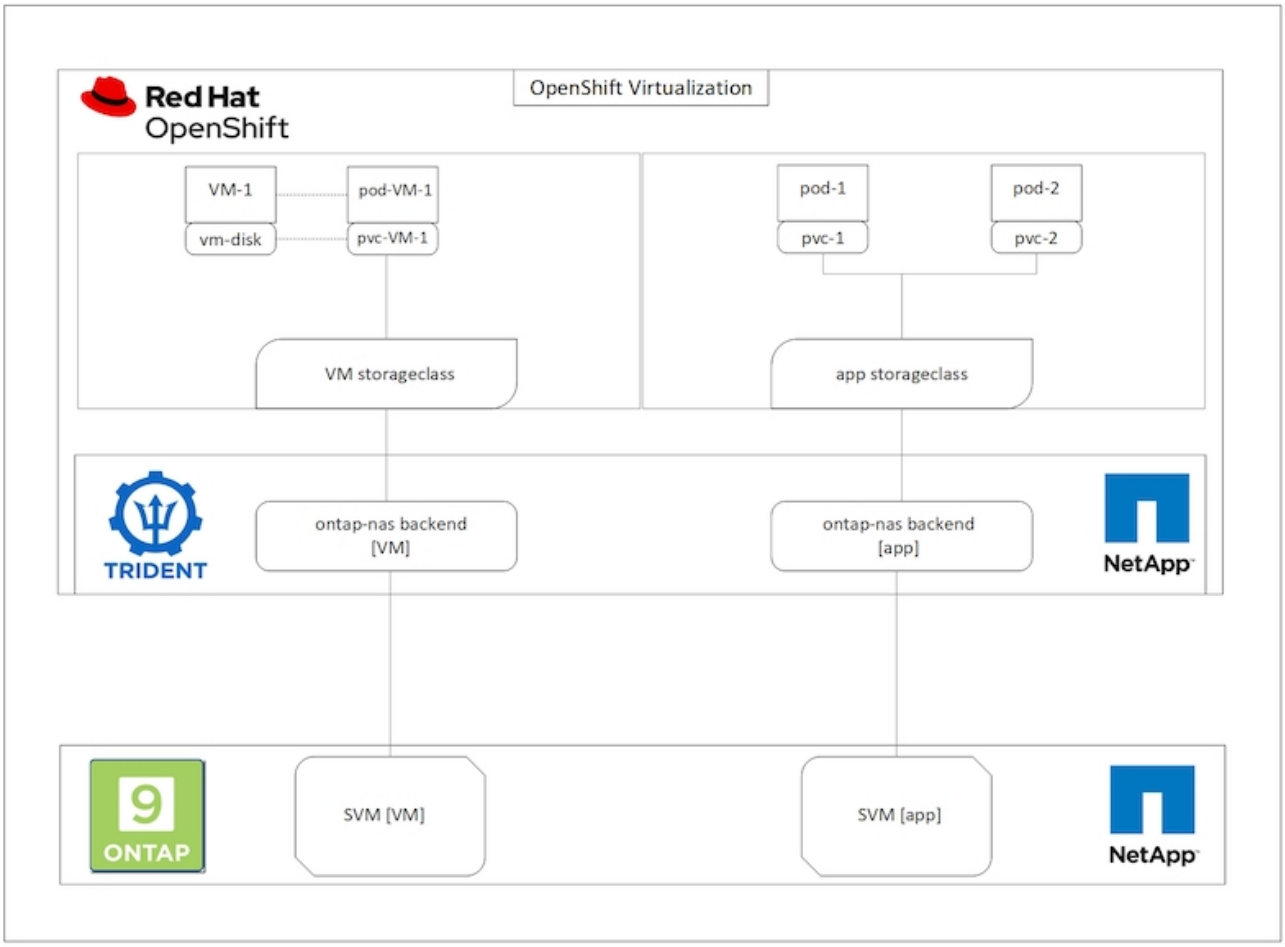
Flux de travail

Flux de travail : Red Hat OpenShift Virtualization avec NetApp ONTAP

Créer une machine virtuelle

Les machines virtuelles sont des déploiements avec état qui requièrent des volumes pour héberger le système d'exploitation et les données. Avec CNV, les machines virtuelles étant exécutées comme des pods, ces

dernières sont sauvegardées par des volumes persistants hébergés sur NetApp ONTAP via Trident. Ces volumes sont connectés en tant que disques et stockent l'intégralité du système de fichiers, y compris la source de démarrage de la machine virtuelle.



Pour créer un serveur virtuel sur le cluster OpenShift, effectuez les opérations suivantes :

1. Accédez à charges de travail > virtualisation > ordinateurs virtuels, puis cliquez sur Créer > avec l'assistant.
2. Sélectionnez le système d'exploitation souhaité et cliquez sur Suivant.
3. Si aucune source d'amorçage n'est configurée sur le système d'exploitation sélectionné, vous devez la configurer. Dans Source d'amorçage, indiquez si vous souhaitez importer l'image OS à partir d'une URL ou d'un registre et fournissez les détails correspondants. Développez Advanced et sélectionnez la classe de stockage sauvegardée par Trident. Cliquez ensuite sur Suivant.

Boot source

This template does not have a boot source. Provide a custom boot source for this **CentOS 8.0+ VM** virtual machine.

Boot source type *

Import via URL (creates PVC)

Import URL *

https://access.cdn.redhat.com/content/origin/files/sha256/58/588167f828001e57688ec4b9b31c11a59d532489f527488ebc89ac5e952...

Example: For RHEL, visit the **RHEL download page** (requires login) and copy the download link URL of the KVM guest image

☑ Mount this as a CD-ROM boot source

Persistent Volume Claim size *

5 GiB

Ensure your PVC size covers the requirements of the uncompressed image and any other space requirements. More storage can be added later.

Advanced

Storage class *

basic (default)

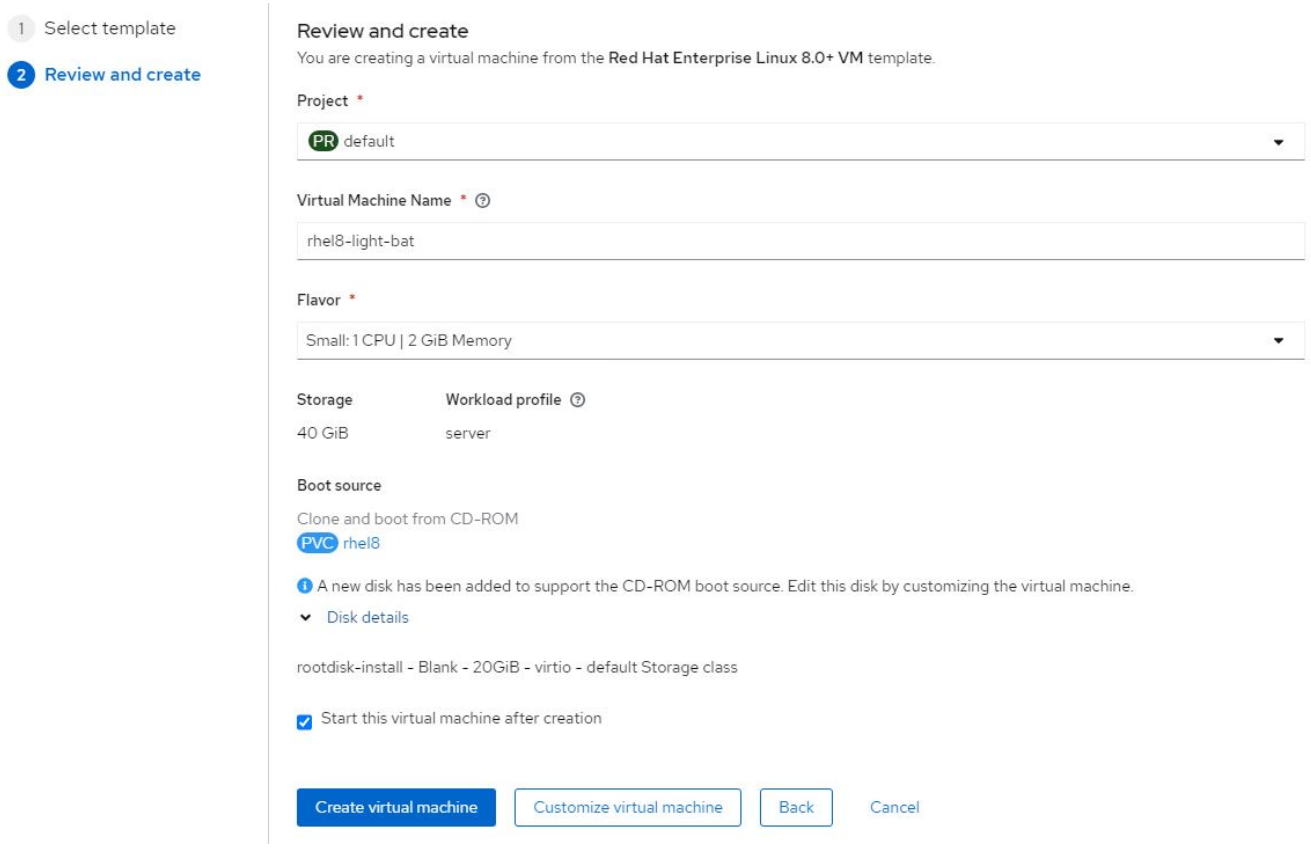
Access mode *

Single User (RWO)

Volume mode *

Filesystem

4. Si une source d'amorçage est déjà configurée sur le système d'exploitation sélectionné, l'étape précédente peut être ignorée.
5. Dans le volet révision et création, sélectionnez le projet dans lequel vous souhaitez créer la machine virtuelle et indiquez les détails de la machine virtuelle. Assurez-vous que la source de démarrage est sélectionnée pour être Clone et boot à partir du CD-ROM avec le PVC approprié affecté au système d'exploitation sélectionné.



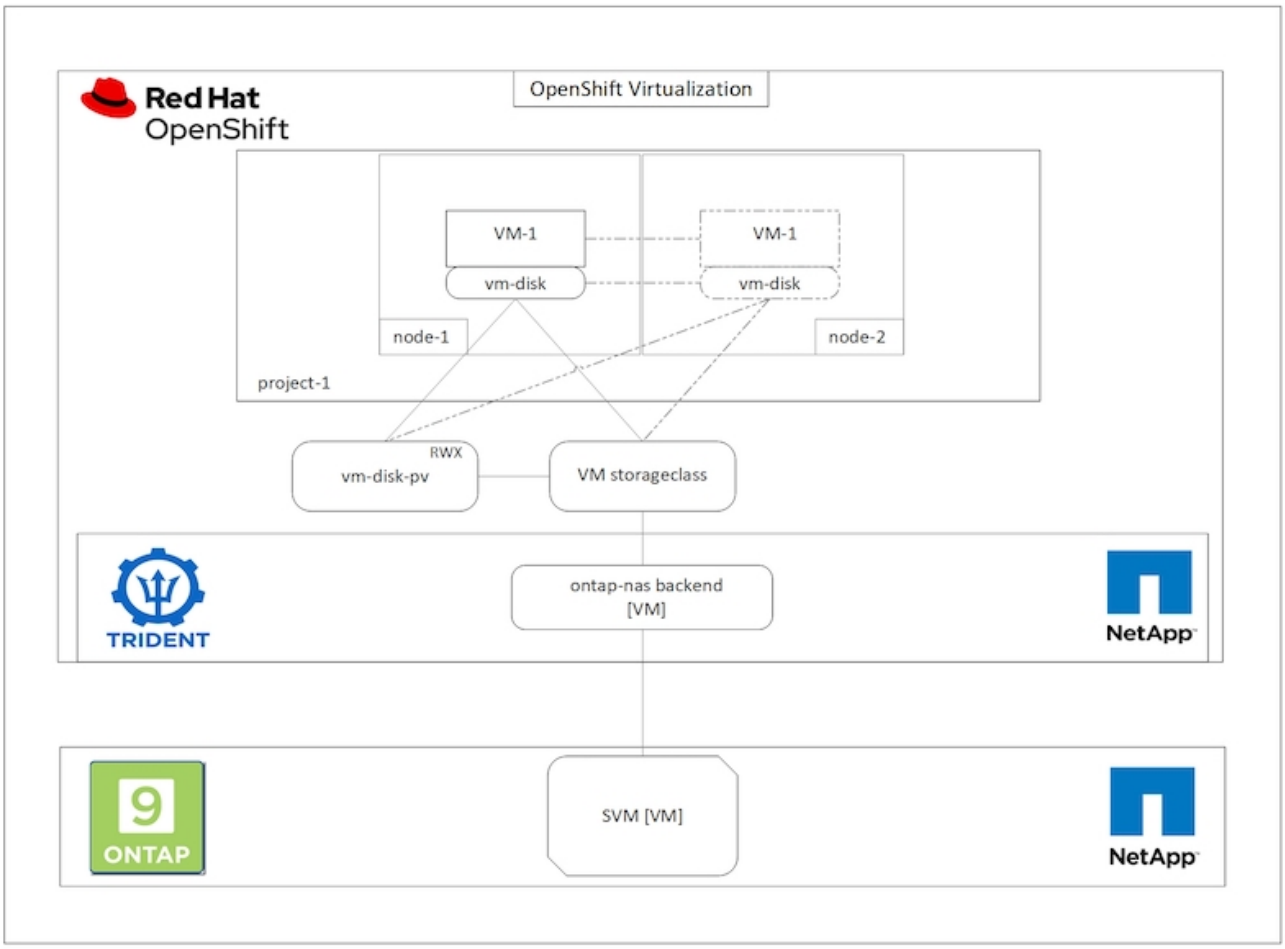
6. Si vous souhaitez personnaliser la machine virtuelle, cliquez sur Personnaliser la machine virtuelle et modifiez les paramètres requis.
7. Cliquez sur Créer une machine virtuelle pour créer la machine virtuelle ; le pod correspondant est alors pivotez en arrière-plan.

Lorsqu'une source d'amorçage est configurée pour un modèle ou un système d'exploitation à partir d'une URL ou d'un registre, elle crée une demande de volume persistant dans le `openshift-virtualization-os-images` Projetez et téléchargez l'image hôte KVM sur la demande de volume persistant. Vous devez vous assurer que les demandes de volume persistant du modèle disposent d'un espace provisionné suffisant pour prendre en charge l'image hôte KVM pour le système d'exploitation correspondant. Ces demandes de volume virtuel sont ensuite clonées et reliées en tant que rootdisks aux machines virtuelles lors de leur création à l'aide des modèles respectifs de n'importe quel projet.

Flux de travail : Red Hat OpenShift Virtualization avec NetApp ONTAP

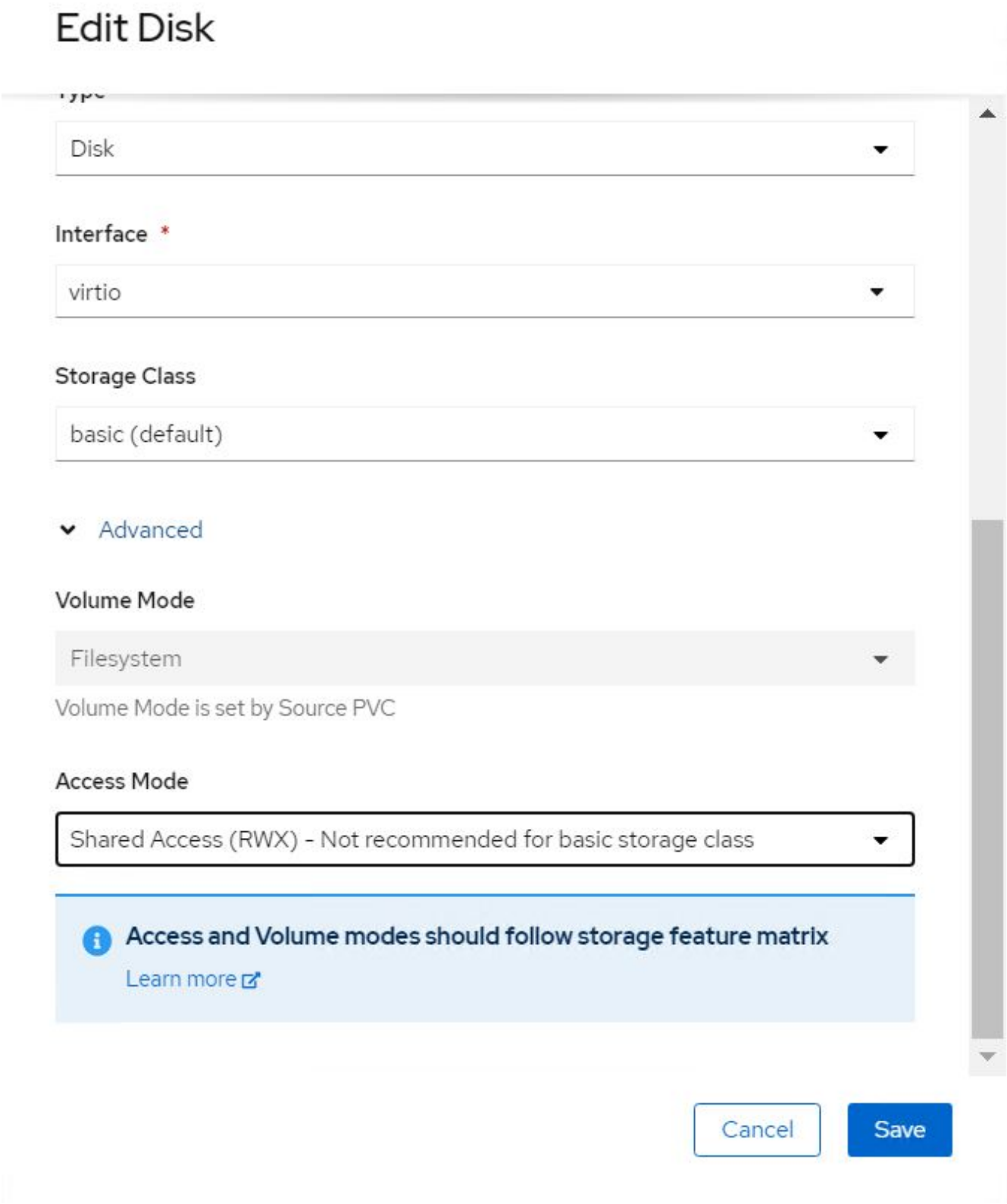
Migration en direct des machines virtuelles

Live migration est un processus de migration d'une instance de VM d'un nœud vers un autre dans un cluster OpenShift sans aucun temps d'indisponibilité. Pour que la migration en direct puisse fonctionner dans un cluster OpenShift, les VM doivent être liés aux demandes de volume virtuel avec le mode d'accès ReadWriteMany partagé. Le système back-end Astra Trident configuré avec un SVM sur un cluster NetApp ONTAP activé pour le protocole NFS prend en charge l'accès partagé ReadWriteMany pour les demandes de volume persistant. Par conséquent, les machines virtuelles avec des demandes de volume persistant demandées par les classes de stockage provisionnées par Trident à partir d'un SVM compatible NFS peuvent être migrées sans temps d'indisponibilité.



Pour créer une VM liée à des demandes de volume virtuel avec un accès ReadWriteMany partagé :

1. Accédez à charges de travail > virtualisation > ordinateurs virtuels, puis cliquez sur Créer > avec l'assistant.
2. Sélectionnez le système d'exploitation souhaité et cliquez sur Suivant. Supposons que l'OS sélectionné dispose déjà d'une source d'amorçage configurée avec celle-ci.
3. Dans le volet révision et création, sélectionnez le projet dans lequel vous souhaitez créer la machine virtuelle et indiquez les détails de la machine virtuelle. Assurez-vous que la source de démarrage est sélectionnée pour être Clone et boot à partir du CD-ROM avec le PVC approprié affecté au système d'exploitation sélectionné.
4. Cliquez sur Personnaliser l'ordinateur virtuel, puis sur stockage.
5. Cliquez sur les points de suspension en regard de rootdisk et assurez-vous que le storageclass provisionné à l'aide de Trident est sélectionné. Développez Avancé et sélectionnez accès partagé (RWX) pour le mode d'accès. Cliquez ensuite sur Enregistrer.



6. Cliquez sur vérifier et confirmer, puis sur Créer une machine virtuelle.

Pour migrer manuellement un VM vers un autre nœud du cluster OpenShift, procédez comme suit.

1. Accédez aux charges de travail > virtualisation > machines virtuelles.

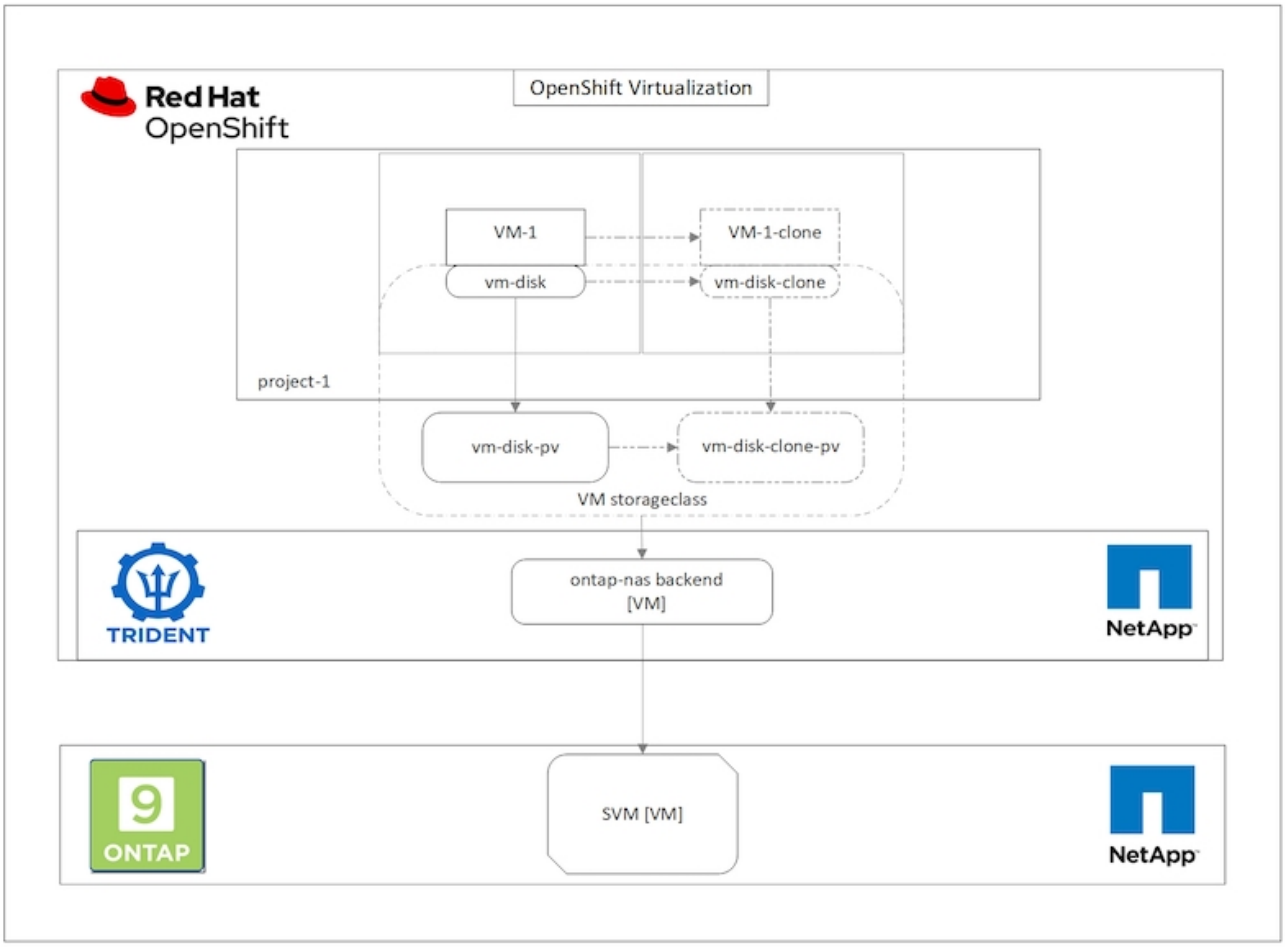
2. Pour la VM à migrer, cliquez sur les points de suspension, puis sur migrer la machine virtuelle.
3. Cliquez sur migrer lorsque le message s'affiche pour confirmer.

> Une instance de machine virtuelle d'un cluster OpenShift migre automatiquement vers un autre nœud lorsque le nœud d'origine est placé en mode maintenance si la stratégie d'éviction est définie sur LiveMigrate.

Flux de travail : Red Hat OpenShift Virtualization avec NetApp ONTAP

Clonage de VM

Le clonage d'une machine virtuelle existante dans OpenShift est réalisé avec la prise en charge de la fonctionnalité de clonage de volumes CSI d'Astra Trident. Le clonage de volumes CSI permet de créer une nouvelle demande de volume persistant en utilisant une demande de volume en tant que source de données en dupliquant son volume persistant. Une fois le nouveau PVC créé, il fonctionne comme une entité distincte et sans lien ou dépendance sur le PVC source.



Le clonage de volumes CSI peut prendre en compte certaines restrictions :

1. Le PVC source et le PVC de destination doivent être dans le même projet.
2. Le clonage est pris en charge au sein de la même classe de stockage.
3. Le clonage n'est possible que lorsque les volumes source et de destination utilisent le même paramètre

Volumemode. Par exemple, un volume de bloc ne peut être cloné que vers un autre volume de bloc.

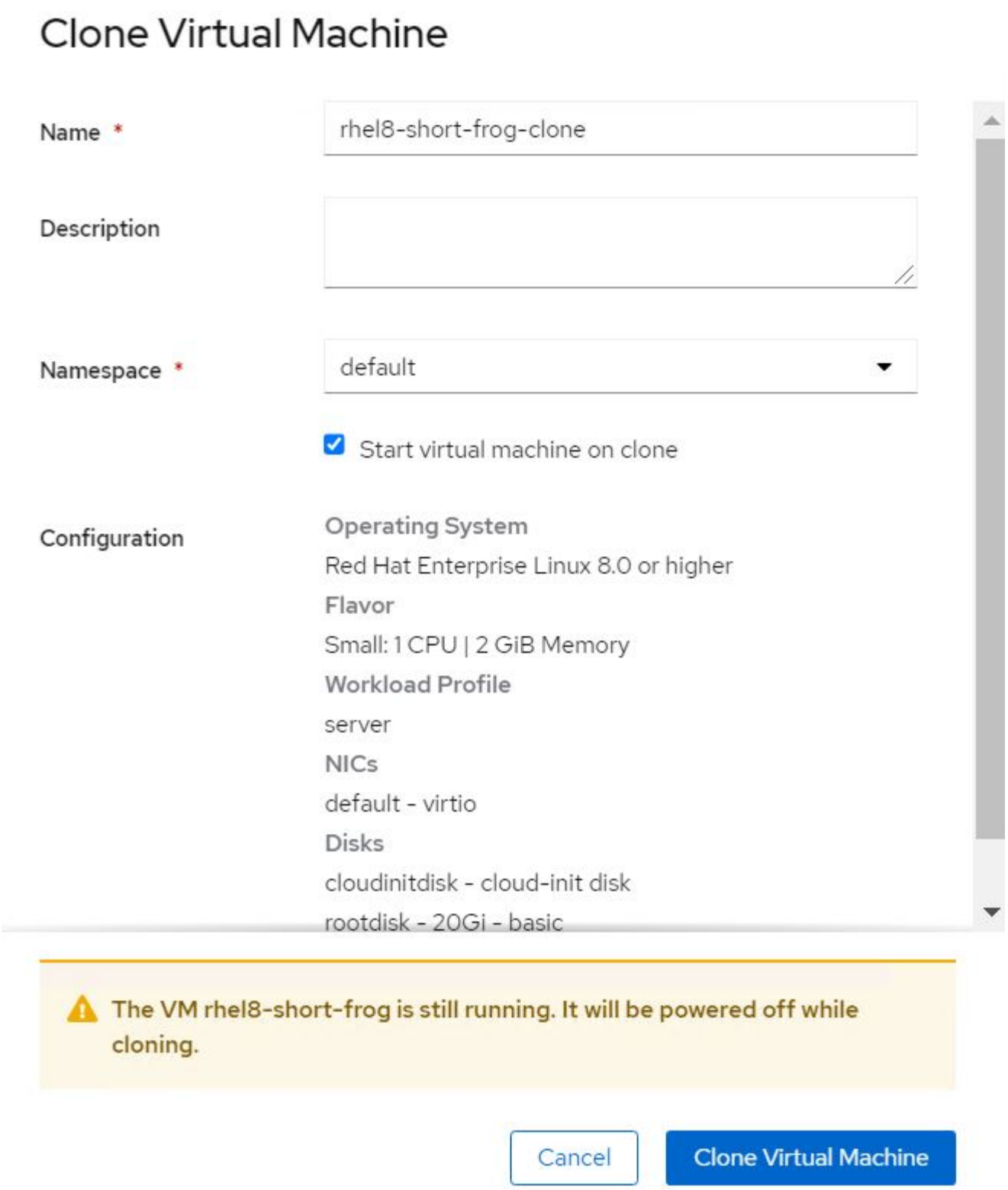
Les VM d'un cluster OpenShift peuvent être clonés de deux manières :

1. En cours d'arrêt de la machine virtuelle source
2. En conservant la machine virtuelle source en service

En cours d'arrêt de la machine virtuelle source

Le clonage d'une machine virtuelle existante en fermant cette machine virtuelle est une fonctionnalité OpenShift native prise en charge d'Astra Trident. Procédez comme suit pour cloner une machine virtuelle.

1. Accédez à charges de travail > virtualisation > machines virtuelles, puis cliquez sur les points de suspension situés à côté de la machine virtuelle que vous souhaitez cloner.
2. Cliquez sur Cloner l'ordinateur virtuel et fournissez les détails concernant la nouvelle machine virtuelle.

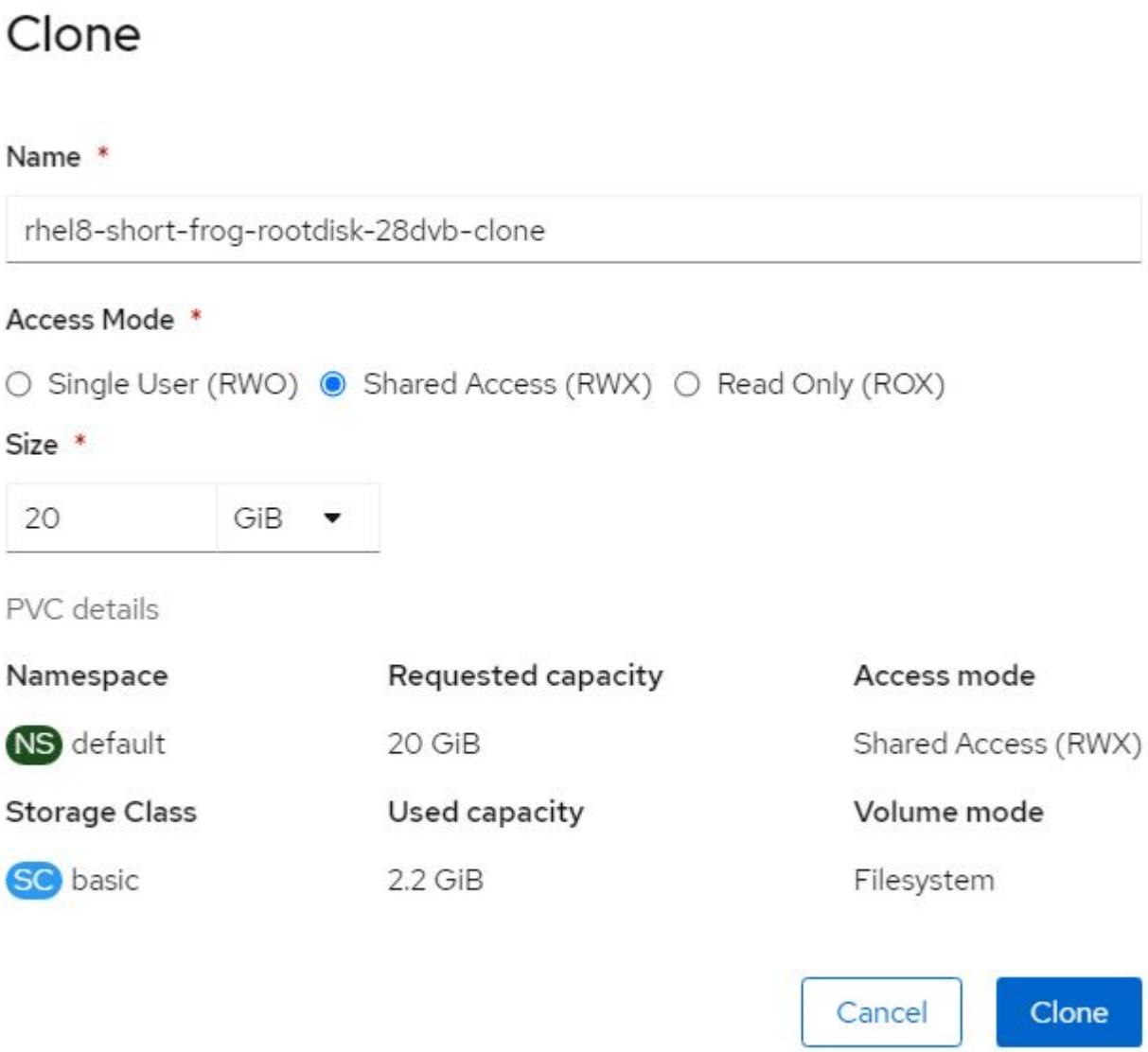


3. Cliquez sur Cloner l'ordinateur virtuel. La machine virtuelle source est arrêtée et commence la création de la machine virtuelle clone.
4. Une fois cette étape terminée, vous pouvez accéder au contenu de la machine virtuelle clonée et le vérifier.

En conservant la machine virtuelle source en service

Une machine virtuelle existante peut également être clonée en clonant le volume persistant existant de la machine virtuelle source, puis en créant une nouvelle machine virtuelle à l'aide du volume persistant cloné. Cette méthode n'exige pas l'arrêt de la machine virtuelle source. Procédez comme suit pour cloner une machine virtuelle sans la désactiver.

1. Accédez à Storage > PersistentVolumeClaims et cliquez sur les points de suspension en regard du volume persistant associé à la machine virtuelle source.
2. Cliquez sur Cloner le PVC et fournir les détails du nouveau PVC.



3. Cliquez ensuite sur Cloner. Cela crée une demande de volume persistant pour la nouvelle machine virtuelle.
4. Accédez à charges de travail > virtualisation > machines virtuelles, puis cliquez sur Créer > avec YAML.
5. Dans la section spécifications > modèle > spécifications > volumes, fixez le PVC cloné à la place du disque conteneur. Fournir tous les autres détails relatifs à la nouvelle machine virtuelle selon vos besoins.

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dvb-clone
```

6. Cliquez sur Créer pour créer la nouvelle machine virtuelle.
7. Une fois la machine virtuelle créée, accédez-y et vérifiez que la nouvelle machine virtuelle est un clone de la machine virtuelle source.

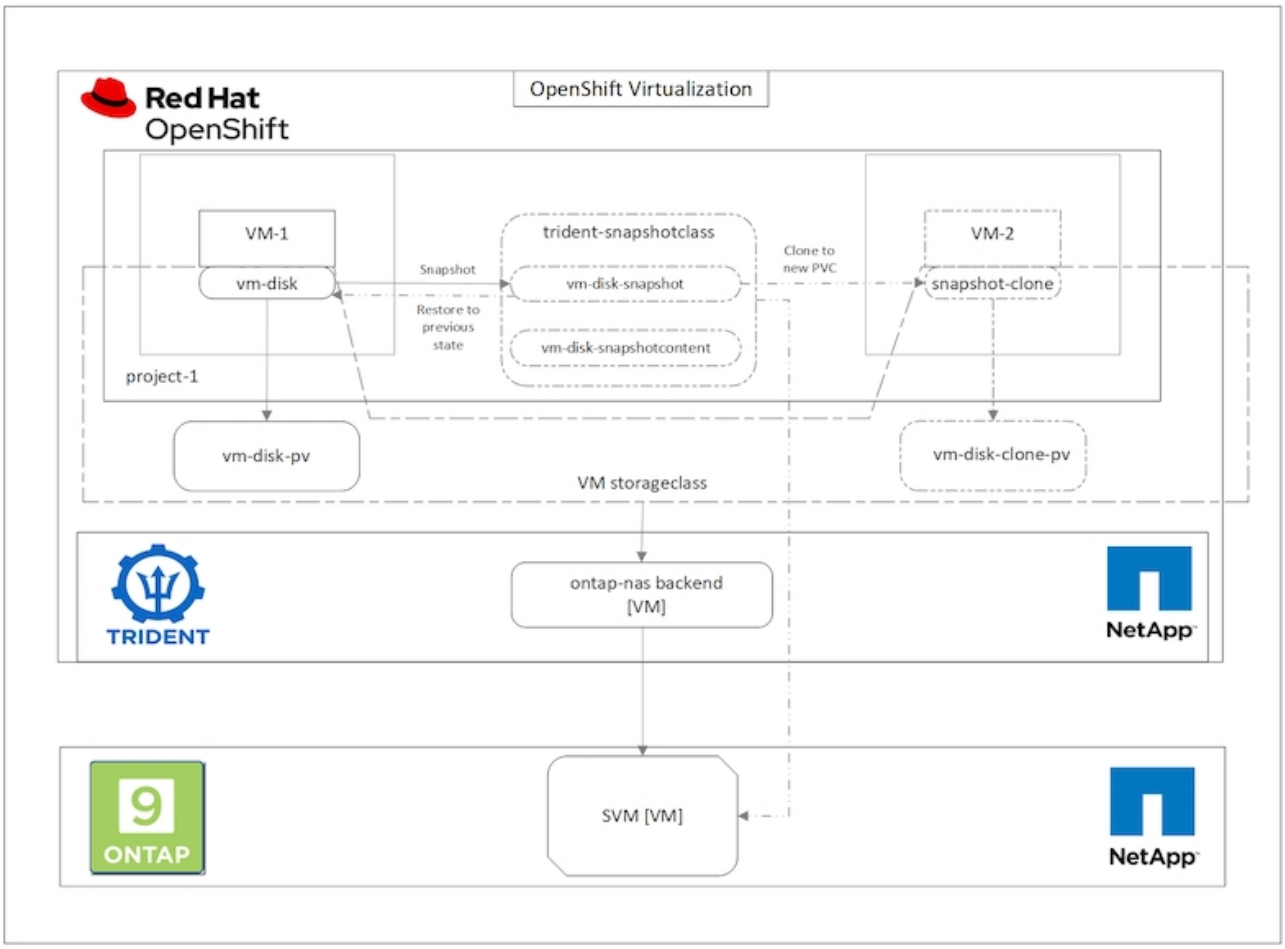
Flux de travail : Red Hat OpenShift Virtualization avec NetApp ONTAP

Créer un serveur virtuel à partir d'un Snapshot

Avec Astra Trident et Red Hat OpenShift, les utilisateurs peuvent créer un snapshot du volume persistant avec les classes de stockage provisionnées par celui-ci. Avec cette fonctionnalité, les utilisateurs peuvent effectuer une copie instantanée d'un volume et l'utiliser pour créer un nouveau volume ou restaurer le même volume à un état précédent. Cela permet d'activer ou de prendre en charge de nombreux cas d'utilisation, de la restauration aux clones en passant par la restauration des données.

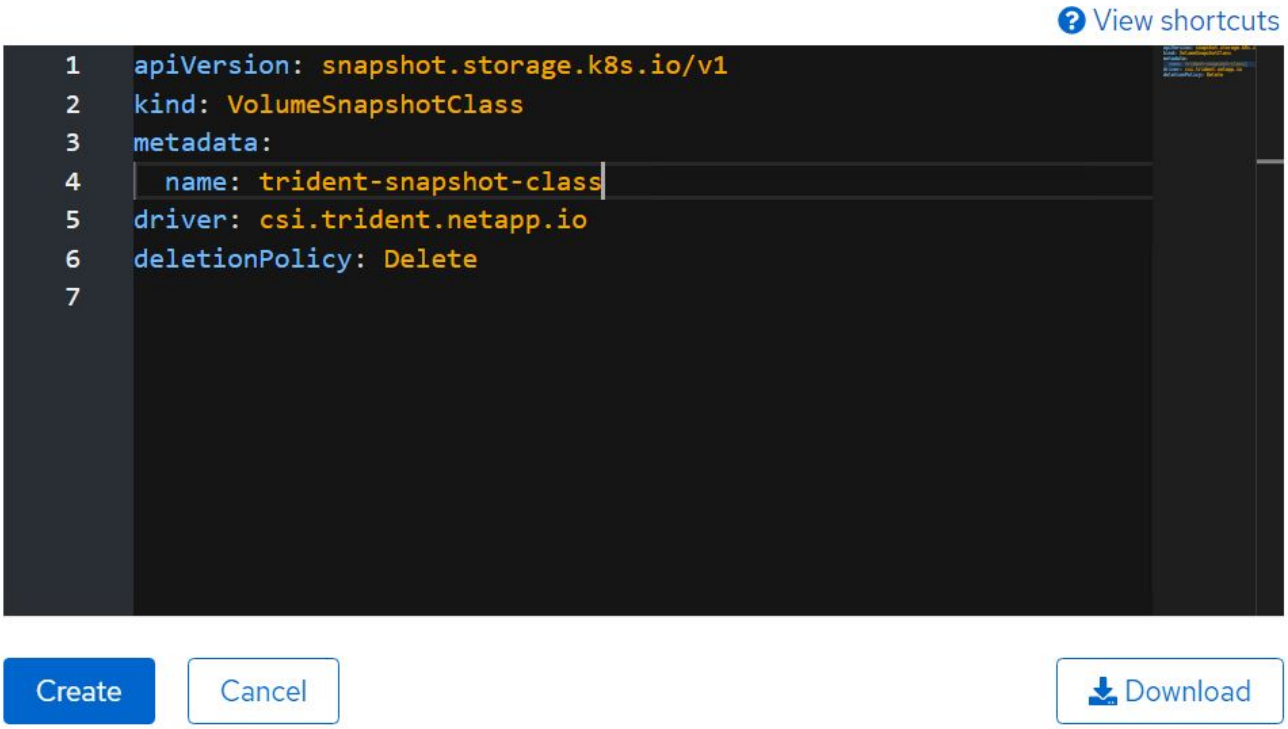
Pour les opérations Snapshot dans OpenShift, les ressources VolumeSnapshotClass, VolumeSnapshot et VolumeContent doivent être définies.

- Un VolumeSnapshotContent est le snapshot réellement pris à partir d'un volume du cluster. Il s'agit d'une ressource à l'échelle du cluster, semblable au volume persistant pour le stockage.
- Un VolumeSnapshot est une demande de création du snapshot d'un volume. Il est similaire à une demande de volume persistant.
- VolumeSnapshotClass permet à l'administrateur de spécifier différents attributs d'un VolumeSnapshot. Il vous permet d'avoir différents attributs pour les différents snapshots pris à partir du même volume.

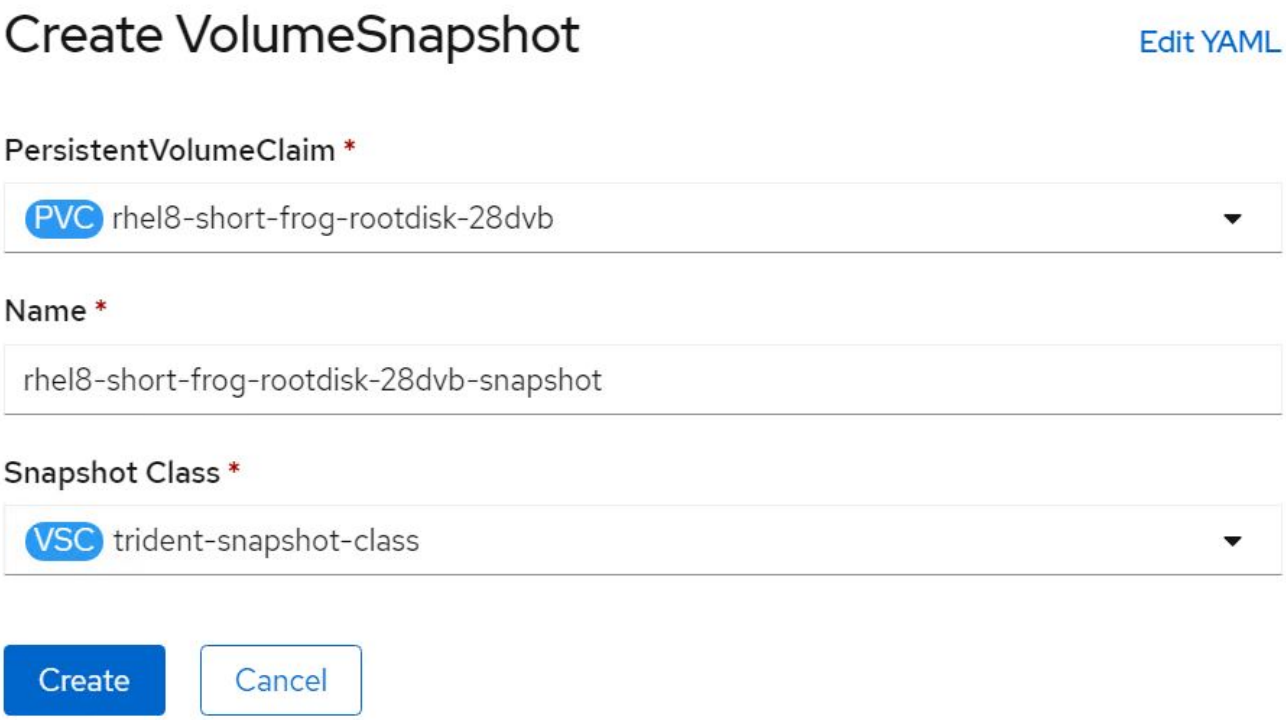


Pour créer le snapshot d'une machine virtuelle, effectuez la procédure suivante :

1. Créez une classe VolumeSnapshotClass qui peut ensuite être utilisée pour créer un Snapshot VolumeCas. Accédez à Storage > VolumeSnapshotclasses et cliquez sur Create VolumeSnapshotClass.
2. Entrez le nom de la classe d'instantanés, entrez csi.trident.netapp.io pour le pilote, puis cliquez sur Créer.



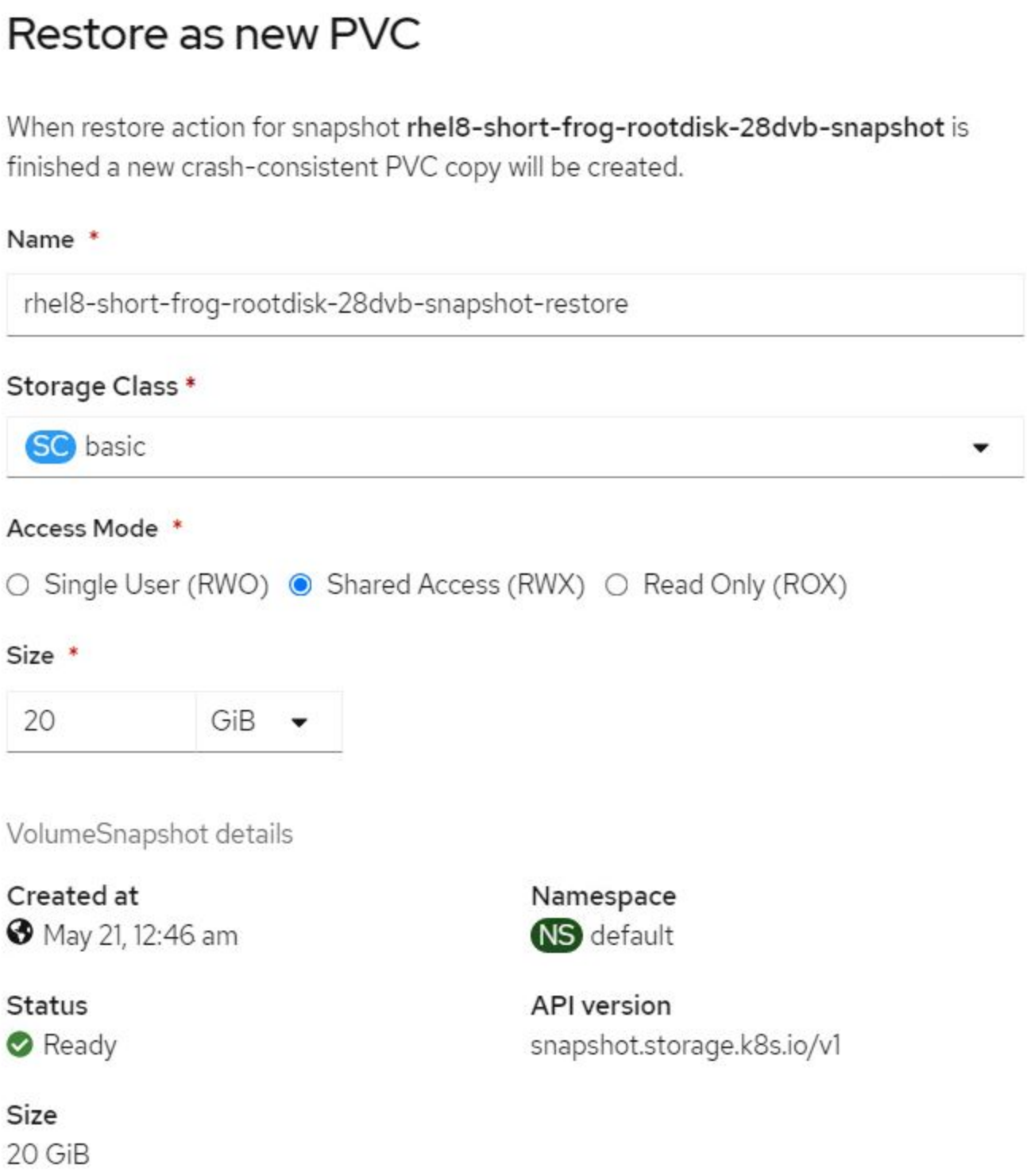
3. Identifiez le volume de volume persistant connecté à la machine virtuelle source, puis créez un Snapshot de cette demande de volume persistant. Accédez à `Storage > VolumeSnapshots` Puis cliquez sur Créer des copies Snapshot VolumeCas.
4. Sélectionnez la demande de volume persistant pour laquelle vous souhaitez créer l'instantané, entrez le nom de l'instantané ou acceptez la valeur par défaut, puis sélectionnez la classe VolumeSnapshotClass appropriée. Cliquez ensuite sur Créer.



5. La création du snapshot de la demande de volume persistant est alors possible.

Créer une nouvelle machine virtuelle à partir du snapshot

1. Tout d'abord, restaurez la copie Snapshot dans un nouveau volume persistant. Accédez à stockage > Volumesnapshots, cliquez sur les points de suspension situés à côté du Snapshot que vous souhaitez restaurer, puis cliquez sur Restaurer en tant que nouveau volume de volume persistant.
2. Entrez les détails du nouveau PVC et cliquez sur Restaurer. Cela crée un nouveau PVC.



3. Ensuite, créez une nouvelle machine virtuelle à partir de ce volume persistant. Accédez à charges de travail > virtualisation > machines virtuelles, puis cliquez sur Créer > avec YAML.

4. Dans la section spec > template > spec > volumes, spécifiez le nouveau PVC créé à partir de Snapshot au lieu du disque conteneur. Fournir tous les autres détails relatifs à la nouvelle machine virtuelle selon vos besoins.

```
- name: rootdisk
  persistentVolumeClaim:
    claimName: rhel8-short-frog-rootdisk-28dvb-snapshot-restore
```

5. Cliquez sur Créer pour créer la nouvelle machine virtuelle.
6. Une fois la machine virtuelle créée, accédez-y et vérifiez que la nouvelle machine virtuelle possède le même état que celle de la machine virtuelle dont le volume de demande de volume persistant a été utilisé pour créer le Snapshot au moment de la création du Snapshot.

Flux de travail : Red Hat OpenShift Virtualization avec NetApp ONTAP

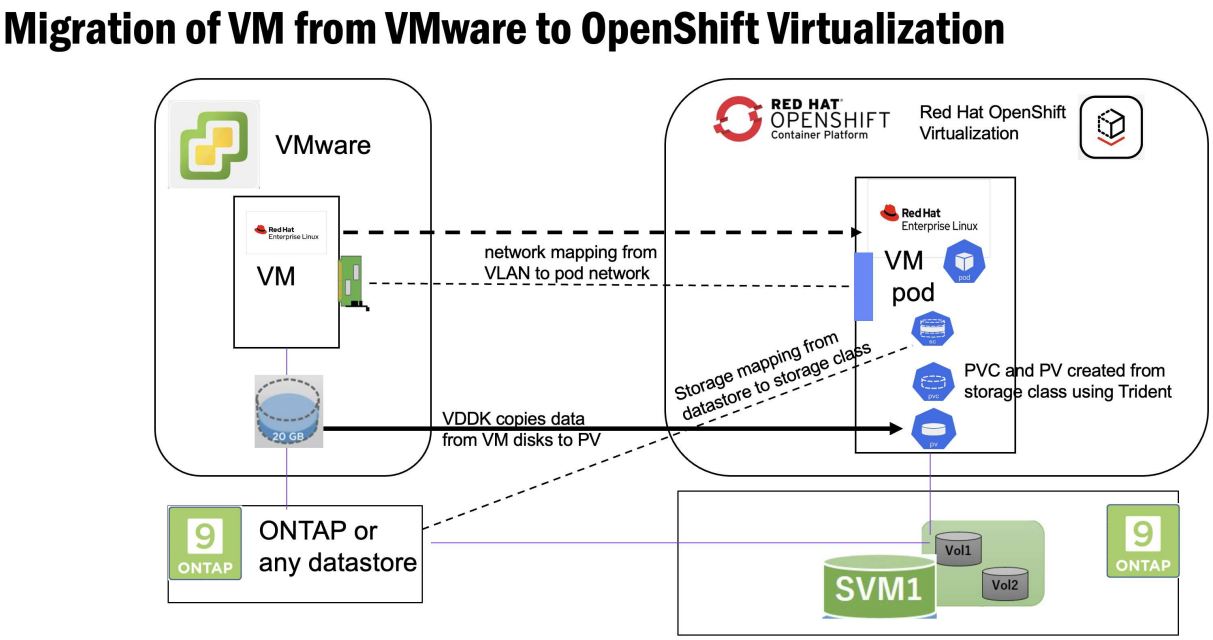
Migration de VM de VMware vers OpenShift Virtualization à l'aide de migration Toolkit pour la virtualisation

Dans cette section, nous allons voir comment utiliser le kit d'outils de migration pour la virtualisation (MTV) pour migrer des machines virtuelles de VMware vers OpenShift Virtualization s'exécutant sur OpenShift Container Platform et intégré avec le stockage NetApp ONTAP à l'aide d'Astra Trident.

La vidéo suivante montre une démonstration de la migration d'une machine virtuelle RHEL de VMware vers OpenShift Virtualization à l'aide d'ontap-san pour le stockage persistant.

Utilisation de Red Hat MTV pour migrer des machines virtuelles vers OpenShift Virtualization avec le stockage NetApp ONTAP

Le schéma suivant présente une vue d'ensemble de la migration d'une machine virtuelle de VMware vers Red Hat OpenShift Virtualization.



Conditions préalables pour l'exemple de migration

Sur VMware

- Une machine virtuelle RHEL 9 utilisant rhel 9.3 avec les configurations suivantes a été installée :
  - CPU: 2, mémoire: 20 Go, disque dur: 20 Go
  - informations d'identification de l'utilisateur : informations d'identification de l'utilisateur root et d'un utilisateur admin
- Une fois la machine virtuelle prête, le serveur postgresql a été installé.
  - le serveur postgresql a été démarré et activé pour démarrer au démarrage

```
systemctl start postgresql.service`
systemctl enable postgresql.service
The above command ensures that the server can start in the VM in
OpenShift Virtualization after migration
```

  - Ajout de 2 bases de données, 1 table et 1 ligne dans la table. Reportez-vous à "ici" Pour obtenir des instructions sur l'installation du serveur postgresql sur RHEL et la création d'entrées de base de données et de table.

> Assurez-vous que vous démarrez le serveur postgresql et que le service démarre au démarrage.

Sur OpenShift Cluster

Les installations suivantes ont été effectuées avant l'installation de MTV :

- OpenShift Cluster 4.13.34
- "ASTRA Trident 23.10"
- Chemins d'accès multiples sur les nœuds de cluster activés pour iSCSI (pour la classe de stockage ontap-san). Consultez le yaml fourni pour créer un jeu de démons qui active iSCSI sur chaque nœud du cluster.
- Système back-end Trident et classe de stockage pour SAN ONTAP utilisant iSCSI. Consultez les fichiers yaml fournis pour le back-end trident et la classe de stockage.
- "Virtualisation OpenShift"

Pour installer iscsi et le multipath sur les nœuds OpenShift Cluster, utilisez le fichier yaml indiqué ci-dessous
Préparation des nœuds de cluster pour iSCSI

```yaml
apiVersion: apps/v1
kind: DaemonSet
metadata:
  namespace: trident
  name: trident-iscsi-init
  labels:
    name: trident-iscsi-init
spec:
```

```
  selector:
    matchLabels:
      name: trident-iscsi-init
  template:
    metadata:
      labels:
        name: trident-iscsi-init
    spec:
      hostNetwork: true
      serviceAccount: trident-node-linux
      initContainers:
      - name: init-node
        command:
          - nsenter
          - --mount=/proc/1/ns/mnt
          - --
          - sh
          - -c
        args: ["$(STARTUP_SCRIPT)"]
        image: alpine:3.7
        env:
        - name: STARTUP_SCRIPT
          value: |
            #! /bin/bash
            sudo yum install -y lsscsi iscsi-initiator-utils sg3_utils
device-mapper-multipath
            rpm -q iscsi-initiator-utils
            sudo sed -i 's/^\(node.session.scan\).*/\1 = manual/'
/etc/iscsi/iscsid.conf
            cat /etc/iscsi/initiatorname.iscsi
            sudo mpathconf --enable --with_multipathd y --find_multipaths
n
            sudo systemctl enable --now iscsid multipathd
            sudo systemctl enable --now iscsi
        securityContext:
          privileged: true
      hostPID: true
      containers:
      - name: wait
        image: k8s.gcr.io/pause:3.1
      hostPID: true
      hostNetwork: true
      tolerations:
      - effect: NoSchedule
        key: node-role.kubernetes.io/master
  updateStrategy:
```

```
    type: RollingUpdate
```

Utilisez le fichier yaml suivant pour créer la configuration back-end trident pour l'utilisation du stockage san ONTAP

Back-end Trident pour iSCSI

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

Utilisez le fichier yaml suivant pour créer la configuration de classe de stockage trident pour l'utilisation du stockage san ONTAP

Classe de stockage Trident pour iSCSI

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

Installer MTV

Vous pouvez maintenant installer le kit d'outils de migration pour la virtualisation (MTV). Reportez-vous aux instructions fournies "ici" pour obtenir de l'aide lors de l'installation.

L'interface utilisateur MTV (migration Toolkit for Virtualization) est intégrée à la console Web OpenShift. Vous pouvez vous référer "ici" pour commencer à utiliser l'interface utilisateur pour différentes tâches.

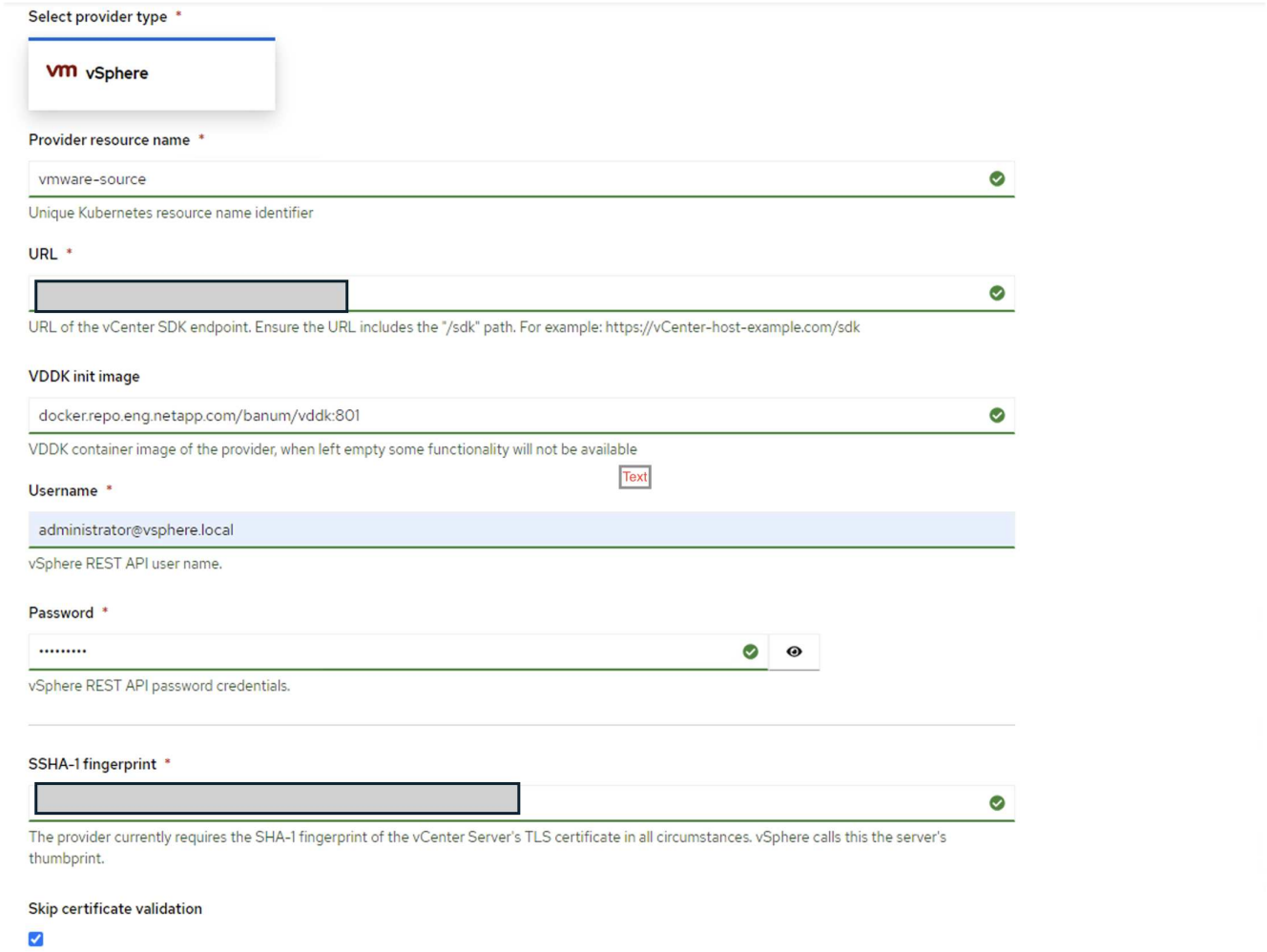
Créer un fournisseur source

Pour migrer la machine virtuelle RHEL de VMware vers OpenShift Virtualization, vous devez d'abord créer le fournisseur source pour VMware. Reportez-vous aux instructions "ici" pour créer le fournisseur source.

Vous avez besoin des éléments suivants pour créer votre fournisseur source VMware :

- url vCenter
- Informations d'identification vCenter
- Empreinte du serveur vCenter
- Image VDDK dans un référentiel

Exemple de création de fournisseur source :



> Le kit MTV (migration Toolkit for Virtualization) utilise le kit de développement de disques virtuels VMware (VDDK) pour accélérer le transfert des disques virtuels à partir de VMware vSphere. Par conséquent, la création d'une image VDDK, bien que facultative, est fortement recommandée.
> Pour utiliser cette fonction, vous téléchargez le kit de développement de disques virtuels VMware (VDDK), créez une image VDDK et envoyez l'image VDDK dans votre registre d'images.

Suivez les instructions fournies "ici" Pour créer et envoyer l'image VDDK vers un registre accessible à partir d'OpenShift Cluster.

Créer un fournisseur de destination

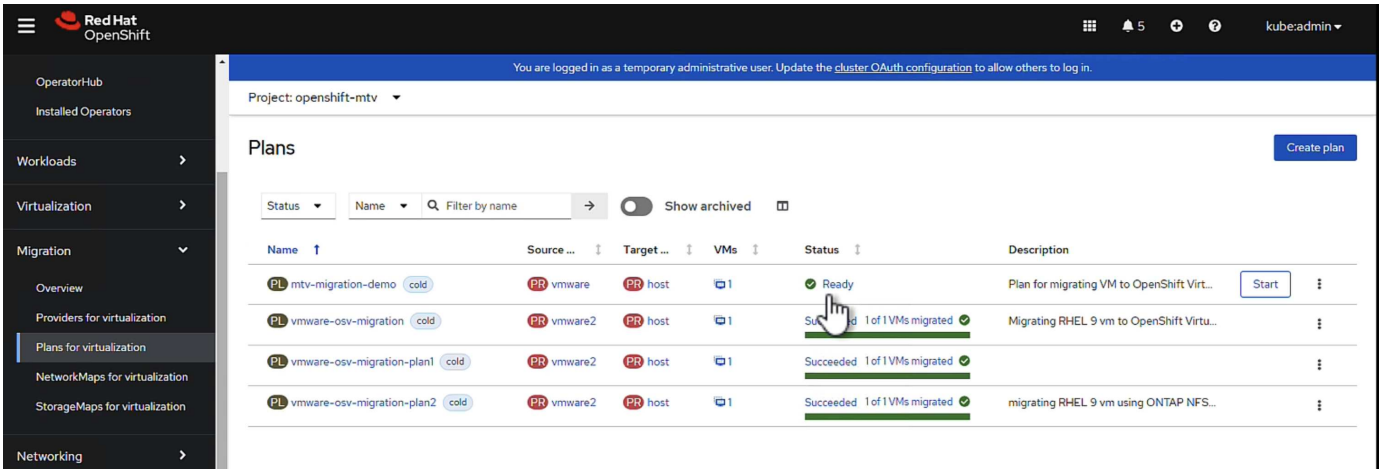
Le cluster hôte est automatiquement ajouté car le fournisseur de virtualisation OpenShift est le fournisseur source.

Créer un plan de migration

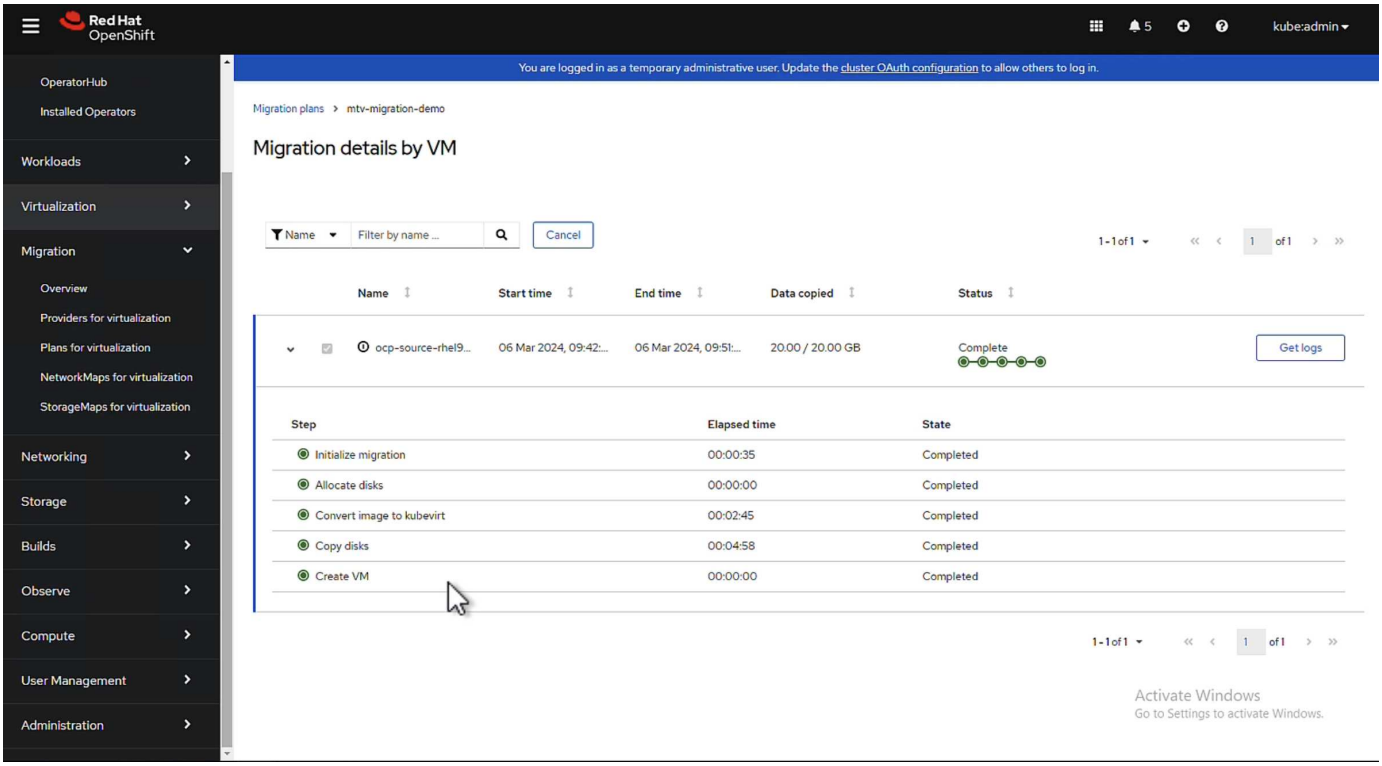
Suivez les instructions fournies "ici" pour créer un plan de migration.

Lors de la création d'un plan, vous devez créer les éléments suivants s'ils ne sont pas déjà créés :

- Mappage réseau pour mapper le réseau source au réseau cible.
- Un mappage de stockage pour mapper le datastore source à la classe de stockage cible. Pour cela, vous pouvez choisir la classe de stockage ontap-san.
  Une fois le plan de migration créé, le statut du plan doit indiquer **prêt** et vous devriez maintenant être en mesure de **démarrer** le plan.



Cliquez sur **Start** pour exécuter une séquence d'étapes pour terminer la migration de la machine virtuelle.



Lorsque toutes les étapes sont terminées, vous pouvez voir les VM migrés en cliquant sur les **machines virtuelles** sous **virtualisation** dans le menu de navigation de gauche.
Des instructions pour accéder aux machines virtuelles sont fournies "ici".

Vous pouvez vous connecter à la machine virtuelle et vérifier le contenu des bases de données postpostgresql. Les bases de données, les tables et les entrées de la table doivent être identiques à celles

créées sur la machine virtuelle source.

Protection des données pour OpenShift Virtualization

Protection des données pour les VM dans OpenShift Virtualization à l'aide d'OpenShift API for Data protection (OADP)

Auteur: Banu Sundhar, NetApp

Cette section du document de référence fournit des informations détaillées sur la création de sauvegardes de machines virtuelles à l'aide d'OpenShift API for Data protection (OADP) avec Velero sur NetApp ONTAP S3 ou NetApp StorageGRID S3. Les sauvegardes des volumes persistants (persistent volumes) des disques de la machine virtuelle sont créées à l'aide des snapshots CSI Astra Trident.

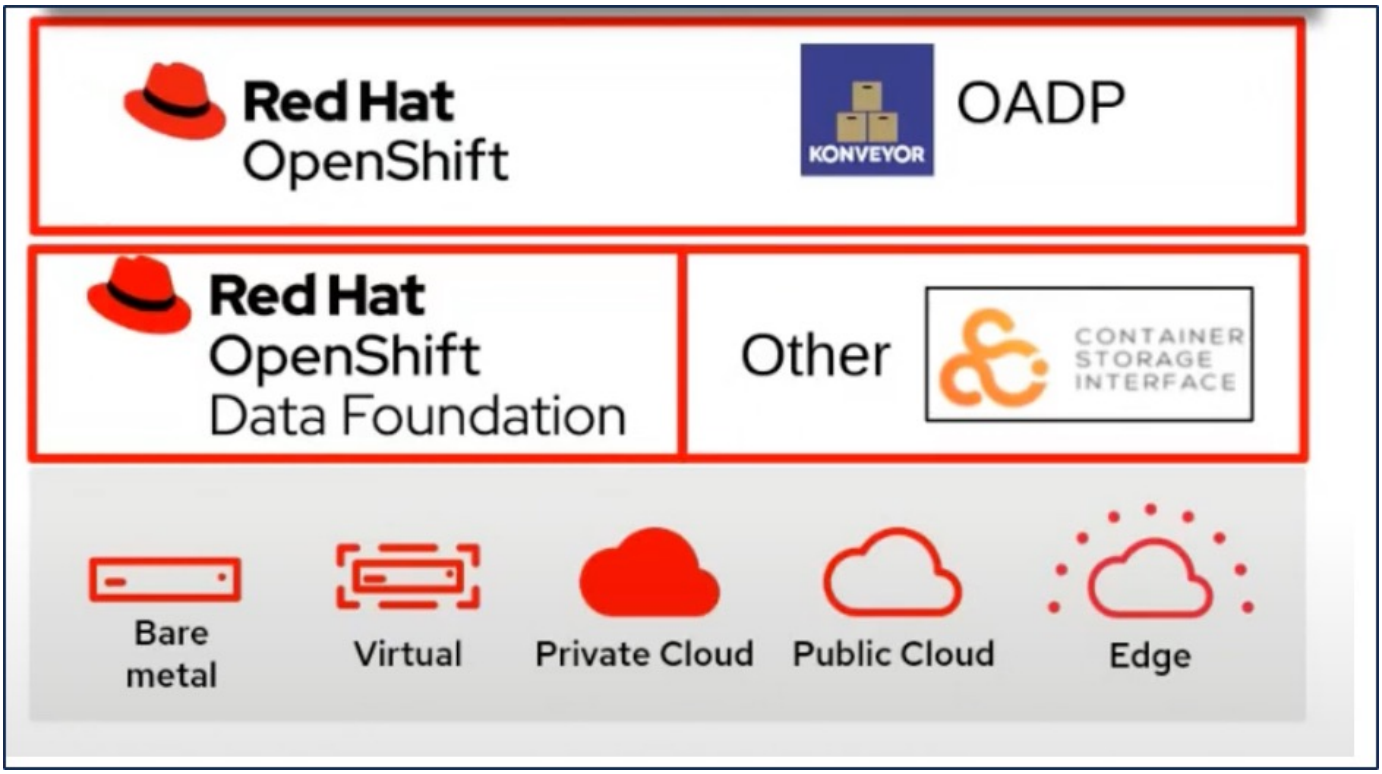
Les machines virtuelles de l'environnement OpenShift Virtualization sont des applications conteneurisées qui s'exécutent dans les nœuds workers de votre plateforme OpenShift Container. Il est important de protéger les métadonnées des machines virtuelles ainsi que les disques persistants des machines virtuelles, afin que vous puissiez les restaurer en cas de perte ou de corruption.

Les disques persistants des VM de virtualisation OpenShift peuvent être pris en charge par le stockage ONTAP intégré au cluster OpenShift à l'aide de "ASTRA Trident CSI". Dans cette section, nous utilisons "OpenShift API pour la protection des données (OADP)" Pour effectuer la sauvegarde des machines virtuelles, y compris leurs volumes de données vers

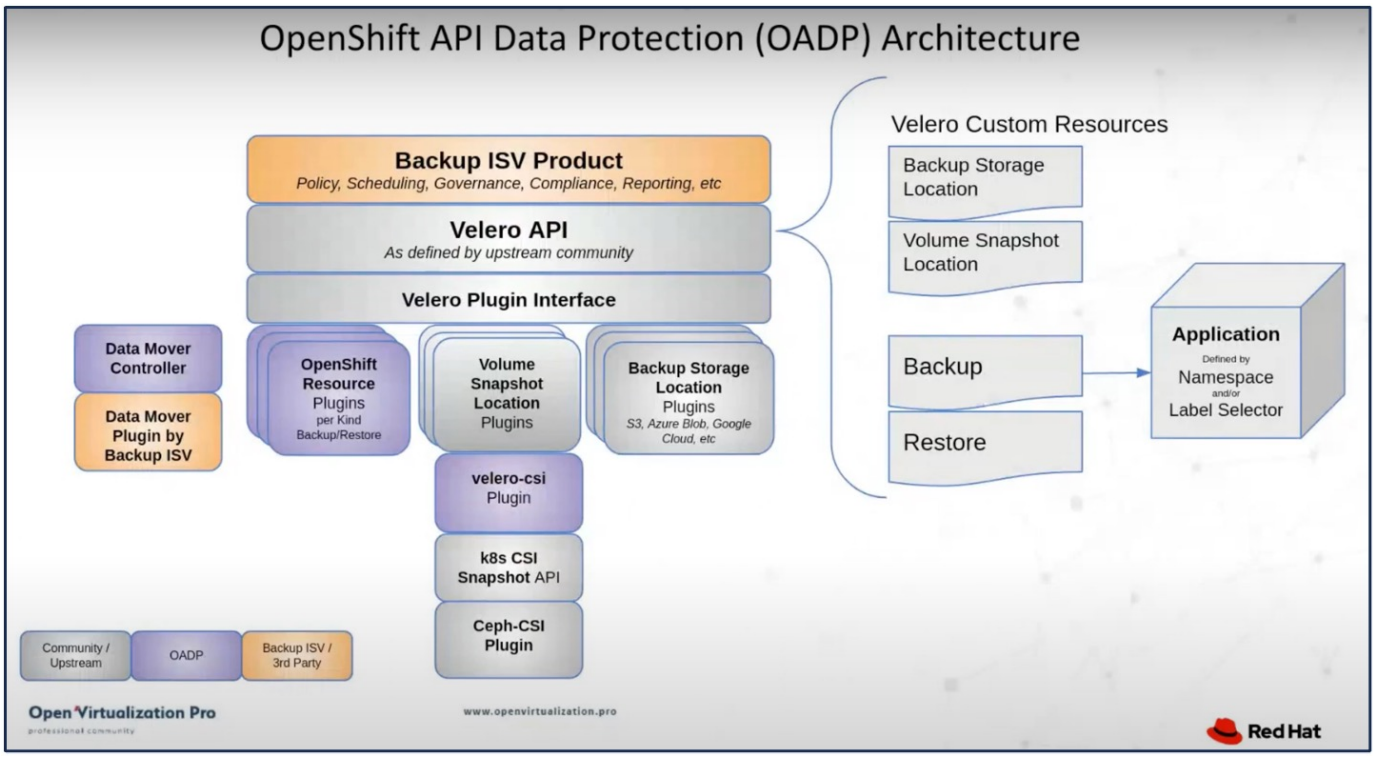
- Stockage objet ONTAP
- StorageGRID

Nous restaurons ensuite les données à partir de la sauvegarde si nécessaire.

OADP permet la sauvegarde, la restauration et la reprise après incident des applications sur un cluster OpenShift. Les données protégées avec OADP incluent les objets de ressource Kubernetes, les volumes persistants et les images internes.



Red Hat OpenShift a mis à profit les solutions développées par les communautés OpenSource pour la protection des données. "Velero" Est un outil open source qui permet de sauvegarder et de restaurer en toute sécurité, d'effectuer une reprise d'activité et de migrer les ressources de cluster Kubernetes et les volumes persistants. Pour utiliser Velero facilement, OpenShift a développé l'opérateur OADP et le plug-in Velero pour s'intégrer aux pilotes de stockage CSI. Les principales API OADP exposées sont basées sur les API Velero. Après l'installation de l'opérateur OADP et sa configuration, les opérations de sauvegarde/restauration qui peuvent être effectuées sont basées sur les opérations exposées par l'API Velero.



OADP 1.3 est disponible sur le hub opérateur d'OpenShift cluster 4.12 et versions ultérieures. Il est doté d'un

Data Mover intégré qui peut déplacer les instantanés de volume CSI vers un magasin d'objets distant. Ces fonctionnalités assurent la portabilité et la durabilité en déplaçant les snapshots vers un emplacement de stockage objet pendant la sauvegarde. Les snapshots sont ensuite disponibles pour la restauration après un incident.

Les versions suivantes des différents composants utilisés dans les exemples de cette section

- OpenShift Cluster 4.14
- OpenShift Virtualization installé via OperatorOpenShift Virtualization Operator fourni par Red Hat
- Opérateur OADP 1.13 fourni par Red Hat
- Velero CLI 1.13 pour Linux
- ASTRA Trident 24.02
- ONTAP 9.12

"ASTRA Trident CSI"
"OpenShift API pour la protection des données (OADP)"
"Velero"

Installation de l'opérateur OpenShift API for Data protection (OADP)

Prérequis

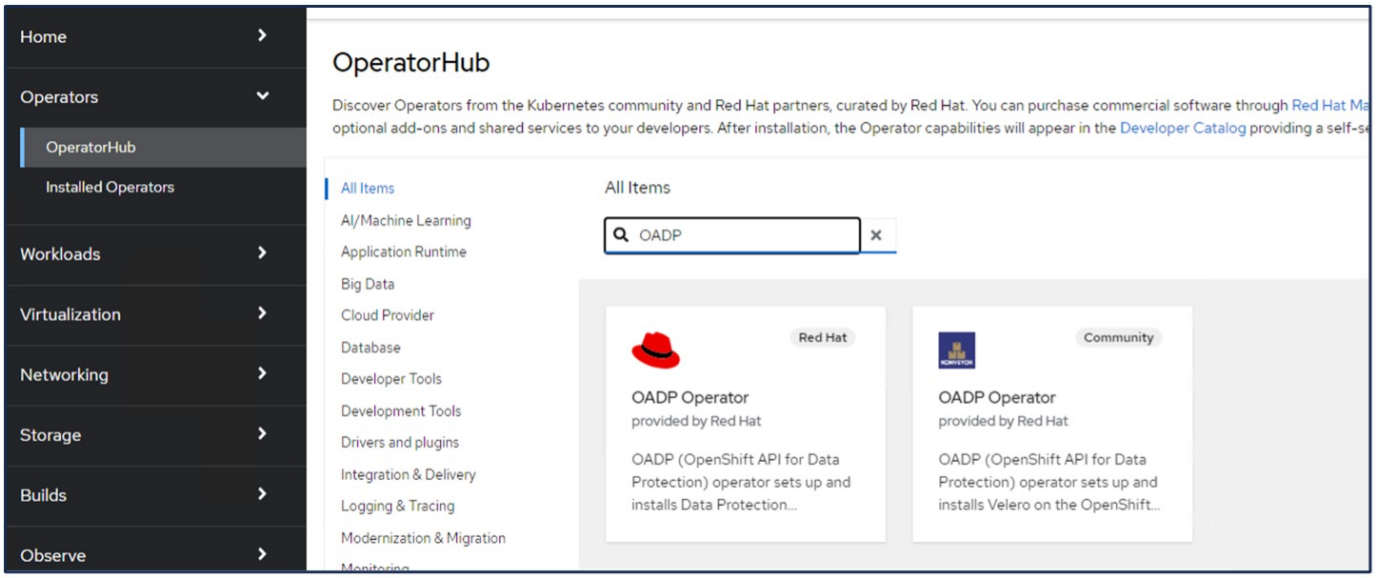
- Cluster Red Hat OpenShift (version ultérieure à la version 4.12) installé sur une infrastructure sans système d'exploitation avec des nœuds worker RHCOS
- Un cluster NetApp ONTAP intégré au cluster via Astra Trident
- Un système back-end Trident configuré avec un SVM sur le cluster ONTAP
- Classe de stockage configurée sur le cluster OpenShift avec Astra Trident en tant que mécanisme de provisionnement
- Classe Snapshot Trident créée sur le cluster
- L'accès cluster-admin au cluster Red Hat OpenShift
- Accès au cluster NetApp ONTAP par administrateur
- L'opérateur OpenShift Virtualization est installé et configuré
- VM déployées dans un espace de noms sur OpenShift Virtualization
- Une station de travail d'administration avec des outils tridentctl et oc installés et ajoutés à $PATH

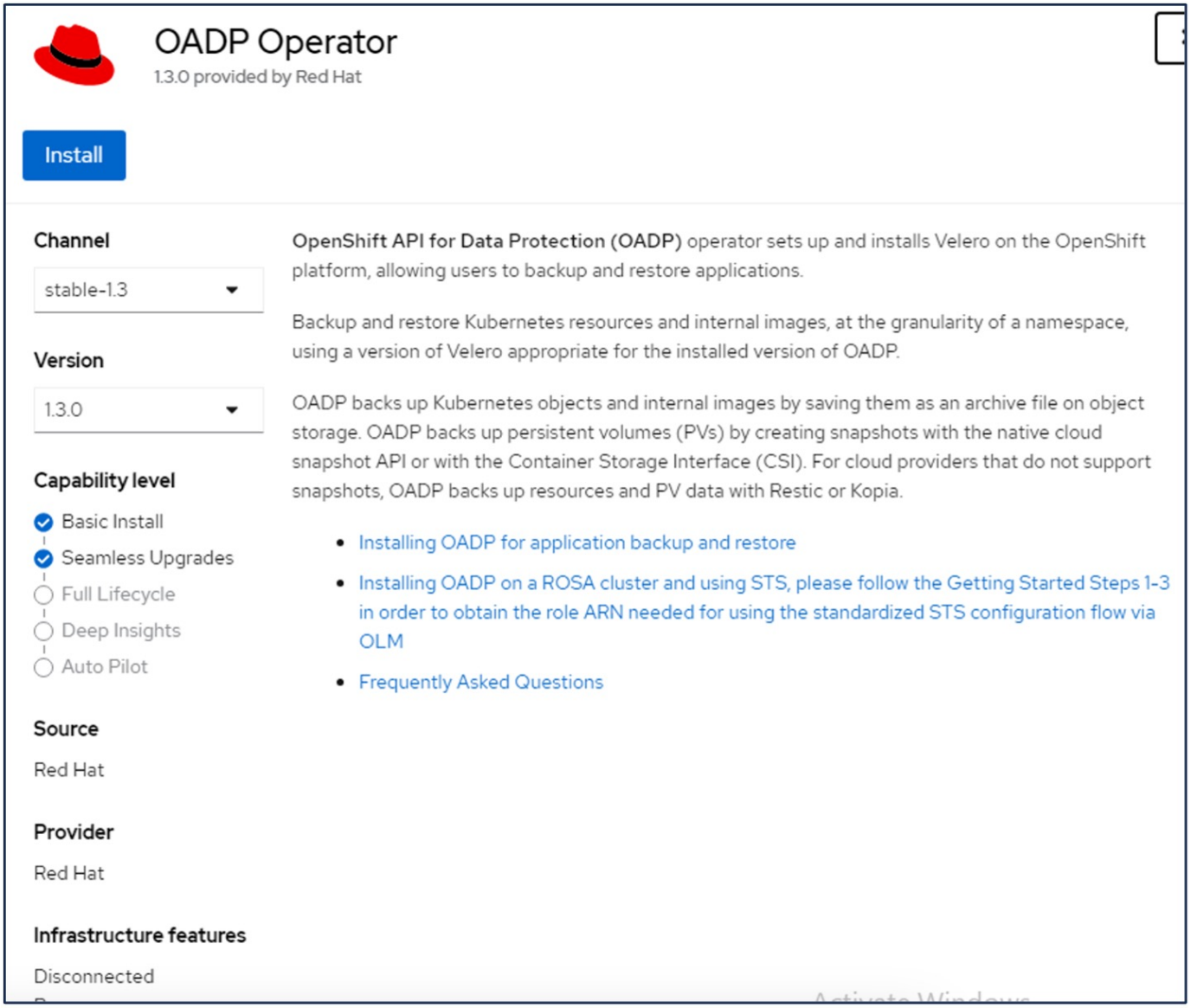
> Si vous souhaitez effectuer une sauvegarde d'une machine virtuelle alors qu'elle est en cours d'exécution, vous devez installer l'agent invité QEMU sur cette machine virtuelle. Si vous installez la machine virtuelle à l'aide d'un modèle existant, l'agent QEMU est automatiquement installé. QEMU permet à l'agent invité de suspendre les données en vol dans le système d'exploitation invité pendant le processus de snapshot et d'éviter toute corruption potentielle des données. Si QEMU n'est pas installé, vous pouvez arrêter la machine virtuelle avant d'effectuer une sauvegarde.

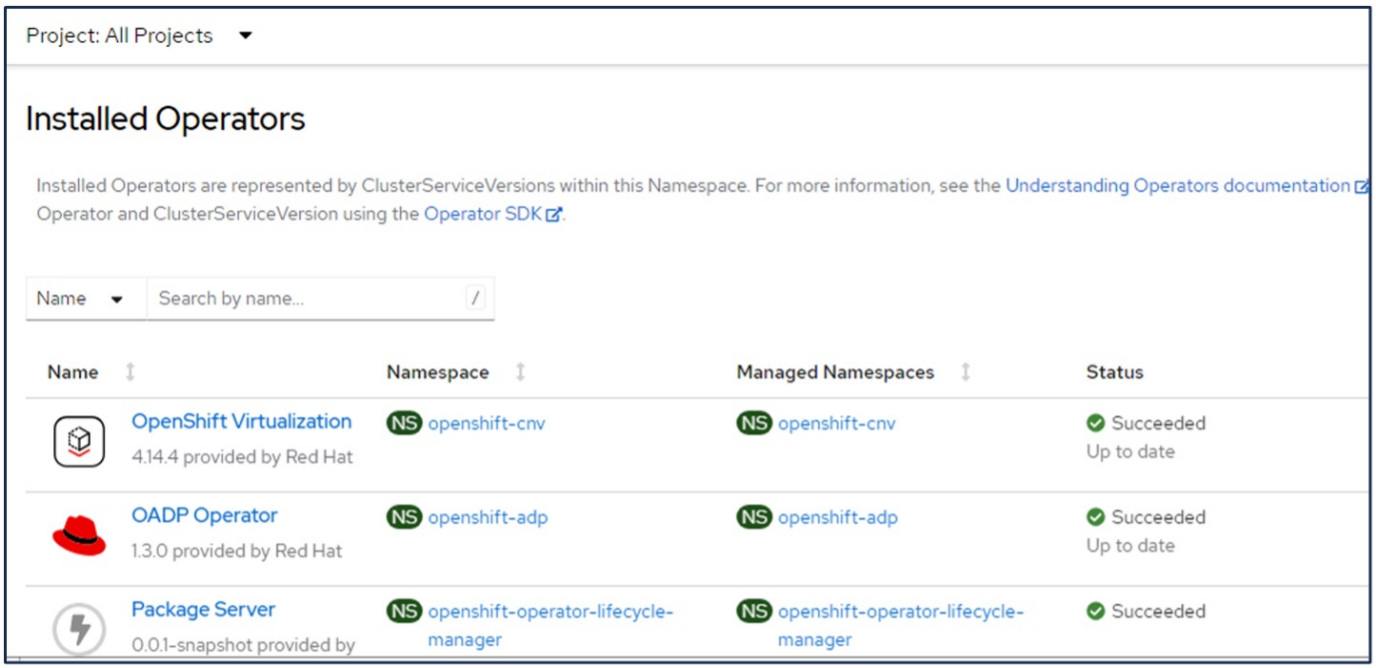
Procédure d'installation de l'opérateur OADP

1. Accédez au hub opérateur du cluster et sélectionnez opérateur OADP Red Hat. Dans la page installer, utilisez toutes les sélections par défaut et cliquez sur installer. Sur la page suivante, utilisez à nouveau toutes les valeurs par défaut et cliquez sur installer. L'opérateur OADP sera installé dans l'espace de noms

openshift-adp.







Conditions préalables pour la configuration Velero avec les détails de ONTAP S3

Une fois l'installation de l'opérateur réussie, configurez l'instance de Velero.
Velero peut être configuré pour utiliser le stockage objet compatible S3. Configurez ONTAP S3 à l'aide des procédures indiquées dans le "Section gestion du stockage objet de la documentation ONTAP". Pour l'intégration à Velero, vous aurez besoin des informations suivantes de votre configuration ONTAP S3.

- Une interface logique (LIF) qui peut être utilisée pour accéder à S3
- Informations d'identification de l'utilisateur pour accéder à S3, y compris la clé d'accès et la clé d'accès secrète
- Nom de compartiment dans S3 pour les sauvegardes avec des autorisations d'accès pour l'utilisateur
- Pour un accès sécurisé au stockage objet, le certificat TLS doit être installé sur le serveur de stockage objet.

Conditions préalables pour la configuration Velero avec les détails de StorageGRID S3

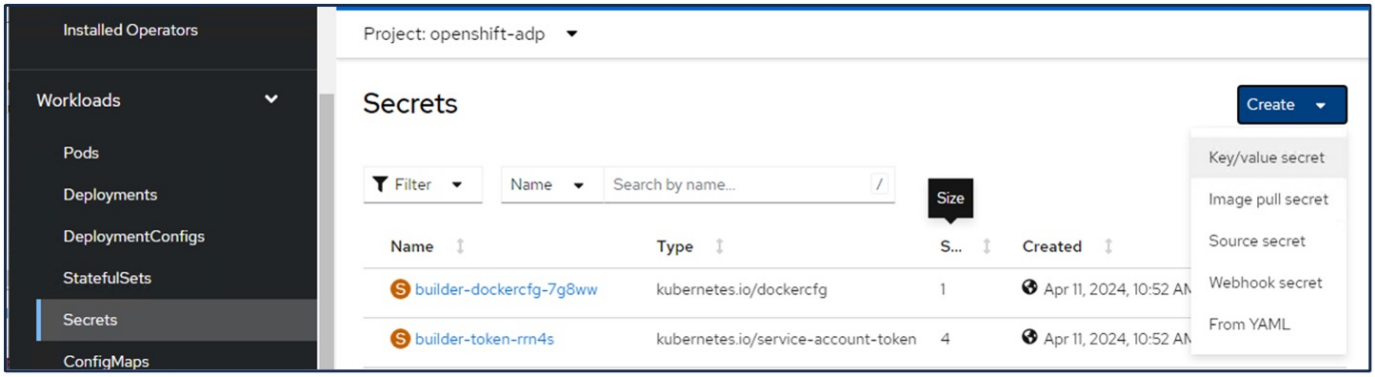
Velero peut être configuré pour utiliser le stockage objet compatible S3. Vous pouvez configurer StorageGRID S3 à l'aide des procédures indiquées dans le "Documentation StorageGRID". Pour l'intégration à Velero, vous aurez besoin des informations suivantes de votre configuration StorageGRID S3.

- Terminal pouvant être utilisé pour accéder à S3
- Informations d'identification de l'utilisateur pour accéder à S3, y compris la clé d'accès et la clé d'accès secrète
- Nom de compartiment dans S3 pour les sauvegardes avec des autorisations d'accès pour l'utilisateur
- Pour un accès sécurisé au stockage objet, le certificat TLS doit être installé sur le serveur de stockage objet.

Procédure de configuration de Velero

- Commencez par créer un secret pour les informations d'identification d'un utilisateur ONTAP S3 ou pour les informations d'identification d'un utilisateur de locataire StorageGRID. Ceci sera utilisé pour configurer

Velero ultérieurement. Vous pouvez créer un secret à partir de l'interface de ligne de commande ou de la console Web.
Pour créer un secret à partir de la console Web, sélectionnez secrets, puis cliquez sur clé/valeur Secret. Indiquez les valeurs pour le nom, la clé et la valeur des informations d'identification, comme indiqué. Assurez-vous d'utiliser l'ID de clé d'accès et la clé d'accès secrète de votre utilisateur S3. Nommez le secret de manière appropriée. Dans l'exemple ci-dessous, un code secret associé aux informations d'identification d'utilisateur ONTAP S3 nommées identifiants ontap-s3 est créé.



Project: openshift-adp

Create key/value secret

Key/value secrets let you inject sensitive data into your application as files or environment variables.

Secret name *

cloud-credentials

Unique name of the new secret.

Key *

cloud

Value

Browse...

Drag and drop file with your value here or browse to upload it.

```
[default]
aws_access_key_id=<Access Key Id of S3 user>
aws_secret_access_key=<Secret Access Key of S3 user>
```

Add key/value

Create Cancel

Pour créer un secret nommé sg-s3-credentials à partir de l'interface de ligne de commande, vous pouvez utiliser la commande suivante.
Image ::redhat_openshift_OADP_install_image6.jpg[Create Secret pour les informations d'identification de l'utilisateur S3 à l'aide de l'interface de ligne de commande]

- Ensuite, pour configurer Velero, sélectionnez opérateurs installés dans l'élément de menu sous opérateurs, cliquez sur opérateur OADP, puis sélectionnez l'onglet DataProtectionapplication. Image::redhat_openshift_OADP_install_image7.jpg[DataProtectionApplication]

Cliquez sur Create DataProtectionApplication. Dans la vue formulaire, indiquez un nom pour l'application Dataprotection ou utilisez le nom par défaut.
Image ::redhat_openshift_OADP_install_image8.jpg[Create application DataProtectionApplication]

Allez maintenant à la vue YAML et remplacez les informations de spécification comme indiqué dans les exemples de fichier yaml ci-dessous.

Exemple de fichier yaml pour la configuration de Velero avec ONTAP S3 comme emplacement de sauvegarde

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true' //use this for https communication
with ONTAP S3
          profile: default
          region: us-east
          s3ForcePathStyle: 'True' //This allows use of IP in s3URL
          s3Url: 'https://10.xx.xx.xx' //Ensure TLS certificate for S3 is
configured
        credential:
          key: cloud
          name: ontap-s3-credentials //previously created secret
        default: true
        objectStorage:
          bucket: velero //Your bucket name previously created in S3 for
backups
          prefix: demobackup //The folder that will be created in the
bucket
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
                    //default Data Mover uses Kopia to move snapshots to
Object  Storage
    velero:
      defaultPlugins:
        - csi //Add this plugin
        - openshift
        - aws
        - kubevirt //Add this plugin
```

Exemple de fichier yaml pour la configuration de Velero avec StorageGRID S3 comme backupLocation et snapshotLocation

```
spec:
  backupLocations:
    - velero:
        config:
          insecureSkipTLSVerify: 'true'
          profile: default
          region: us-east-1 // region of your StorageGrid system
          s3ForcePathStyle: 'True'
          s3Url: 'https://172.21.254.25:10443' //the IP used to access S3
        credential:
          key: cloud
          name: sg-s3-credentials //secret created earlier
        default: true
        objectStorage:
          bucket: velero
          prefix: demobackup
        provider: aws
  configuration:
    nodeAgent:
      enable: true
      uploaderType: kopia
    velero:
      defaultPlugins:
        - csi
        - openshift
        - aws
        - kubevirt
```

Les fichiers YAML ci-dessus ont les sections suivantes dans les spécifications configurées de manière appropriée, similaire aux exemples ci-dessus

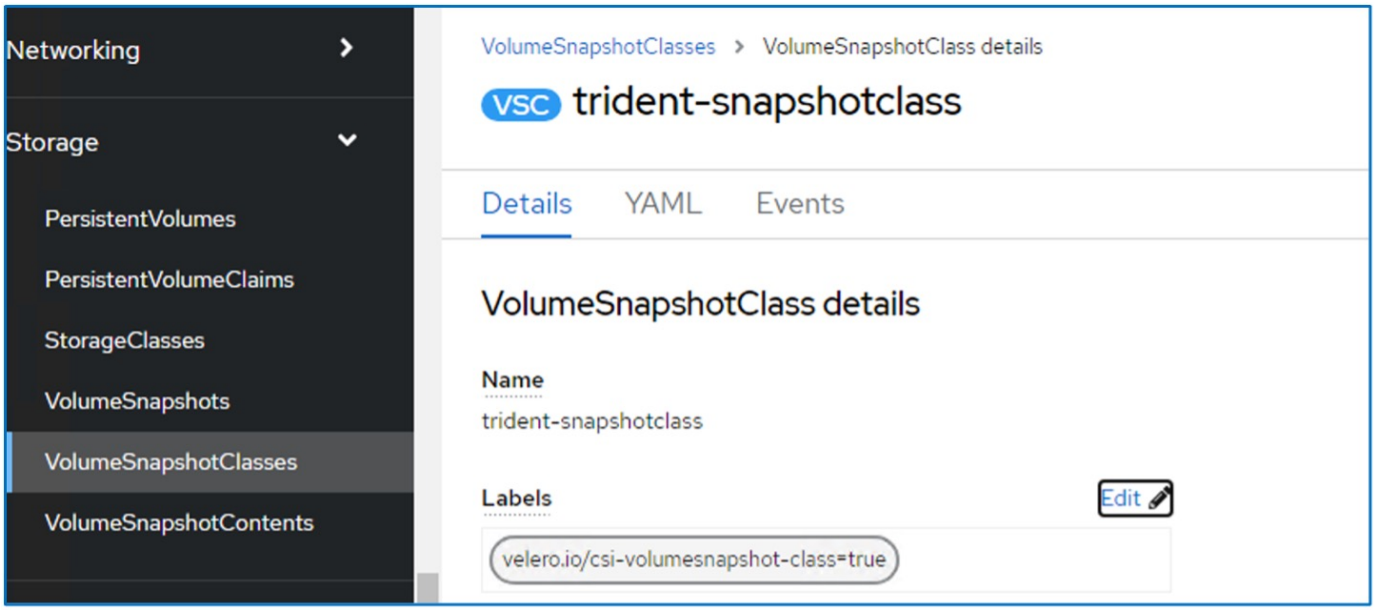
BackupLocation
ONTAP S3 ou StorageGRID S3 (avec ses informations d'identification et d'autres informations comme indiqué dans le yaml) est configuré comme emplacement de sauvegarde par défaut pour velero.

SnapshotLocation
Si vous utilisez des instantanés Container Storage interface (CSI), vous n'avez pas besoin de spécifier un emplacement de snapshot car vous allez créer un VolumeSnapshotClass CR pour enregistrer le pilote CSI. Dans cet exemple, vous utilisez Astra Trident CSI et vous avez déjà créé VolumeSnapShotClass CR à l'aide du pilote Trident CSI.

Activer CSI
Ajoutez csi aux plug-ins par défaut de Velero pour sauvegarder les volumes persistants avec des snapshots CSI.
Les plug-ins Velero CSI, pour sauvegarder les PVC CSI, choisiront le VolumeSnapshotClass dans le cluster qui a le label **velero.io/csi-volumesnapshot-class** sur celui-ci. Pour cela

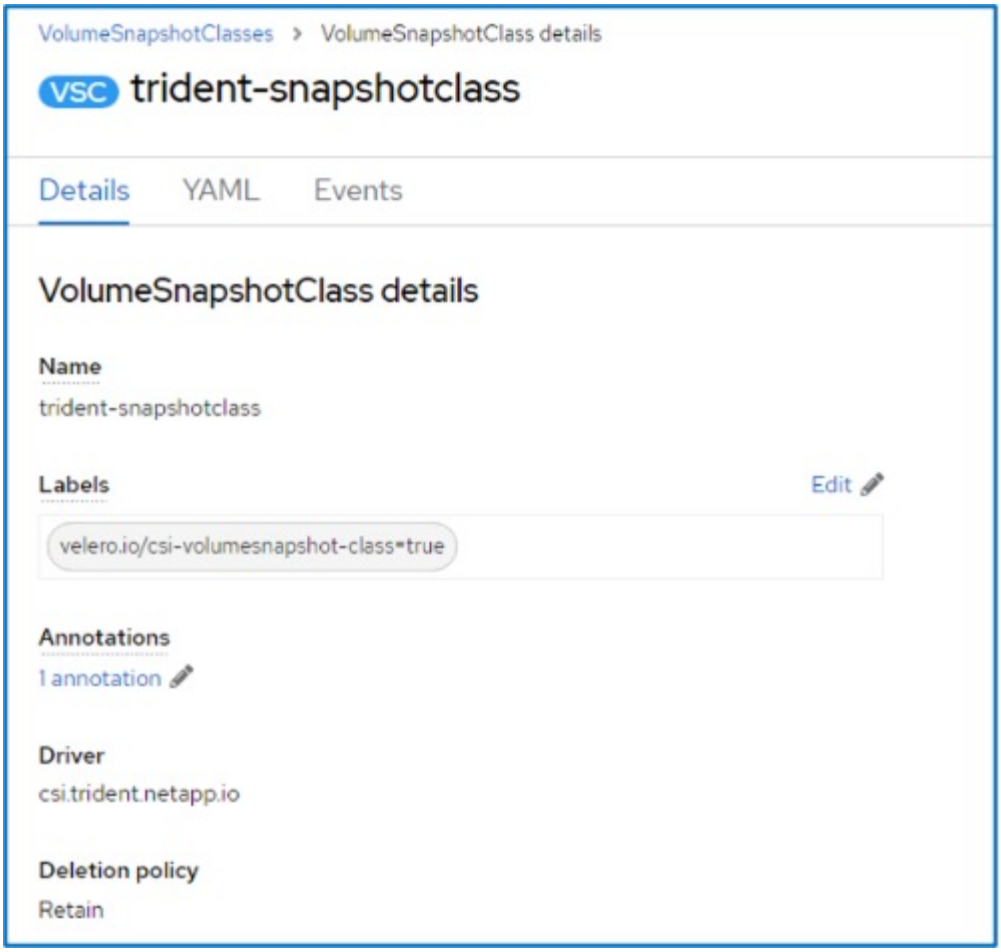
- Vous devez avoir créé la classe VolumeSnapshotClass.

- Modifiez le libellé de la classe trident-snapshotclass et définissez-le sur **velero.io/csi-volumesnapshot-class=true** comme indiqué ci-dessous.



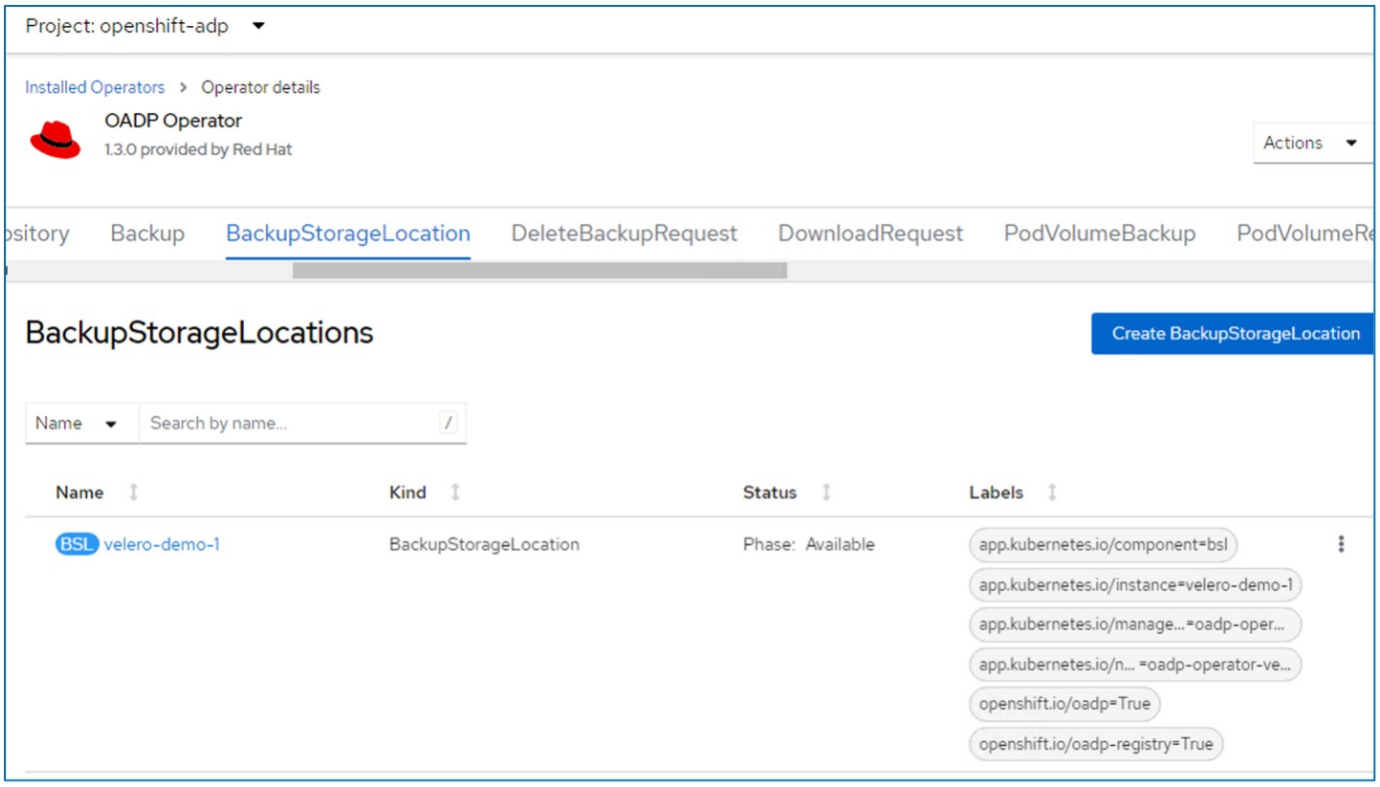
Assurez-vous que les snapshots peuvent persister même si les objets VolumeSnapshot sont supprimés. Pour ce faire, définissez la **deletionPolicy** à conserver. Si ce n'est pas le cas, la suppression d'un namespace perd complètement toutes les demandes de volume virtuels sauvegardées.

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



Assurez-vous que l'application DataProtectionApplication est créée et qu'elle est en condition:réconciliée. Image::redhat_openshift_OADP_install_image11.jpg[DataProtectionApplication l'objet est créé]

L'opérateur OADP va créer un BackupStorageLocation correspondant. Il sera utilisé lors de la création d'une sauvegarde.



Création d'une sauvegarde à la demande pour les machines virtuelles dans OpenShift Virtualization

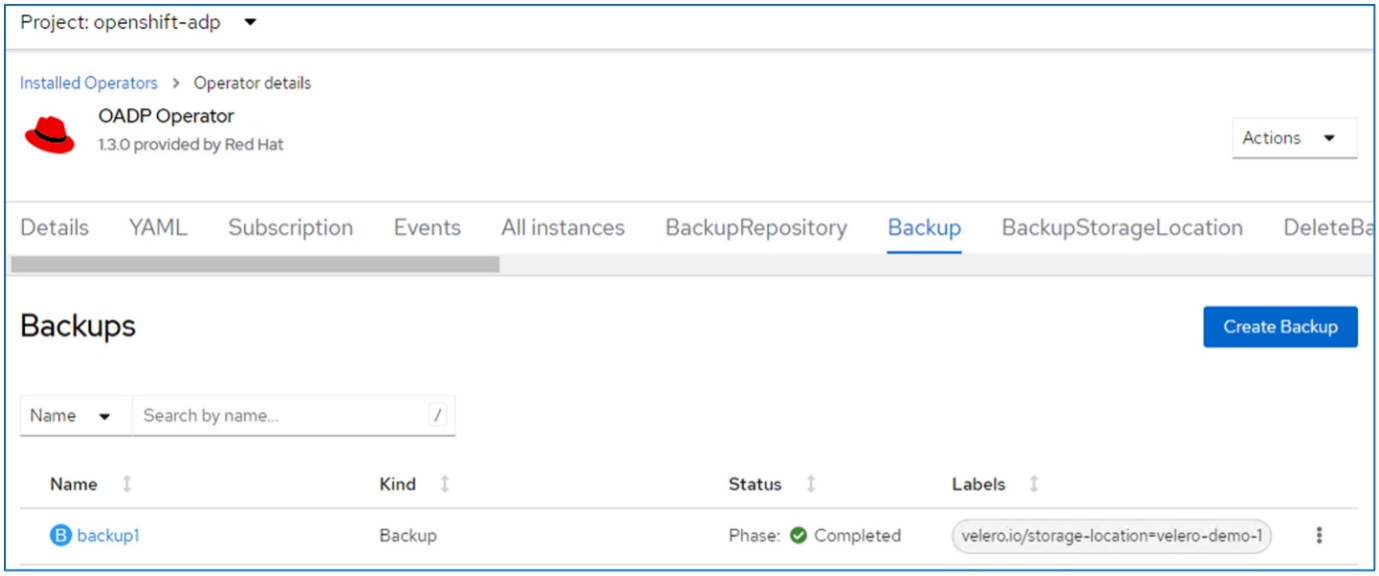
Étapes de création d'une sauvegarde d'une machine virtuelle

Pour créer une sauvegarde à la demande de l'ensemble de la machine virtuelle (métadonnées de la machine virtuelle et disques de la machine virtuelle), cliquez sur l'onglet **sauvegarde**. Cela crée une ressource personnalisée de sauvegarde (CR). Un exemple de yaml est fourni pour créer la CR de sauvegarde. En utilisant ce yaml, la machine virtuelle et ses disques dans l'espace de noms spécifié seront sauvegardés. Des paramètres supplémentaires peuvent être définis comme indiqué dans le "documentation".

Un instantané des volumes persistants qui soutiennent les disques sera créé par le CSI. Une sauvegarde de la machine virtuelle ainsi que l'instantané de ses disques sont créés et stockés dans l'emplacement de sauvegarde spécifié dans le yaml. La sauvegarde restera dans le système pendant 30 jours, comme spécifié dans le ttl.

```
apiVersion: velero.io/v1
kind: Backup
metadata:
  name: backup1
  namespace: openshift-adp
spec:
  includedNamespaces:
  - virtual-machines-demo
  snapshotVolumes: true
  storageLocation: velero-demo-1 //this is the backupStorageLocation
previously created
                                 //when Velero is configured.
  ttl: 720h0m0s
```

Une fois la sauvegarde terminée, sa phase s'affiche comme terminée.



Vous pouvez inspecter la sauvegarde dans le stockage objet à l'aide d'une application de navigateur S3. Le chemin de la sauvegarde s'affiche dans le compartiment configuré avec le préfixe nom (velero/démobilackup). Vous pouvez voir le contenu de la sauvegarde inclut les snapshots de volume, les journaux et d'autres métadonnées de la machine virtuelle.

> Dans StorageGRID, vous pouvez également utiliser la console S3 disponible dans le gestionnaire de locataires pour afficher les objets de sauvegarde.

Path: / demobackup/ backups/ backup1/

Name	Size	Type	Last Modified	Storage Class
..				
backup1.tar.gz	230.36 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
velero-backup.json	3.35 KB	JSON File	4/15/2024 10:26:29 PM	STANDARD
backup1-resource-list.json.gz	1.12 KB	GZ File	4/15/2024 10:26:29 PM	STANDARD
backup1-itemoperations.json.gz	600 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-volumesnapshots.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-podvolumebackups.json.gz	29 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-results.gz	49 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotclasses.json.gz	426 bytes	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshotcontents.json.gz	1.43 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-csi-volumesnapshots.json.gz	1.34 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD
backup1-logs.gz	13.49 KB	GZ File	4/15/2024 10:26:28 PM	STANDARD

Création de sauvegardes planifiées pour les machines virtuelles dans OpenShift Virtualization

Pour créer des sauvegardes sur un planning, vous devez créer une demande de modification d'horaires.

Le planning est simplement une expression cron qui vous permet de spécifier l'heure à laquelle vous souhaitez créer la sauvegarde. Un exemple de yaml pour créer une demande de modification d'horaire.

```
apiVersion: velero.io/v1
kind: Schedule
metadata:
  name: <schedule>
  namespace: openshift-adp
spec:
  schedule: 0 7 * * *
  template:
    hooks: {}
    includedNamespaces:
    - <namespace>
    storageLocation: velero-demo-1
    defaultVolumesToFsBackup: true
    ttl: 720h0m0s
```

L'expression Cron 0 7 * * * * signifie qu'une sauvegarde sera créée à 7:00 chaque jour.
Les espaces de noms à inclure dans la sauvegarde et l'emplacement de stockage de la sauvegarde sont également spécifiés. Par conséquent, au lieu d'une CR de sauvegarde, la CR de planification est utilisée pour créer une sauvegarde à l'heure et à la fréquence spécifiées.

Une fois le planning créé, il est activé.
Image ::redhat_openshift_OADP_backup_image3.jpg[Schedule créée]

Les sauvegardes seront créées en fonction de ce planning et peuvent être affichées à partir de l'onglet sauvegarde.
Image ::redhat_openshift_OADP_backup_image4.jpg[Schedule créée]

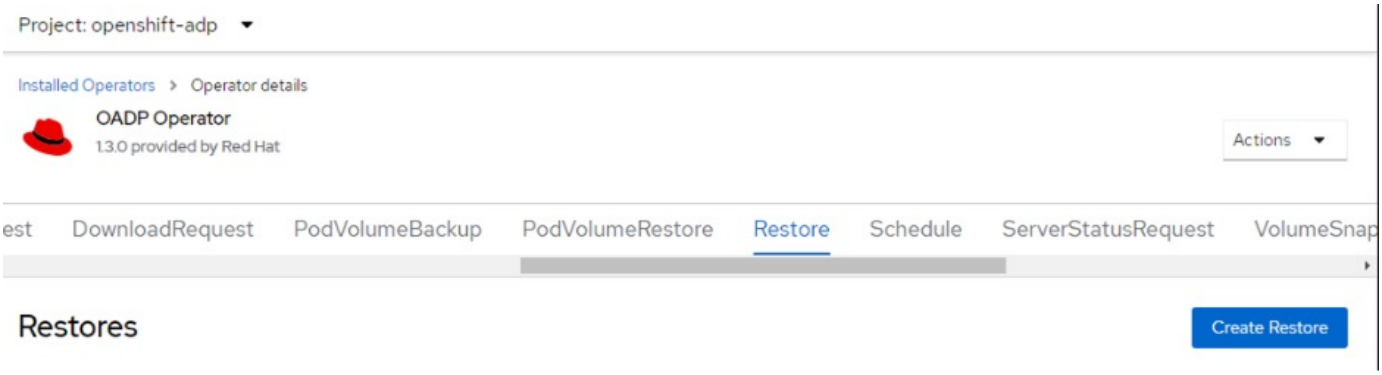
Restaurer une machine virtuelle à partir d'une sauvegarde

Prérequis

Pour effectuer une restauration à partir d'une sauvegarde, supposons que l'espace de noms dans lequel existait la machine virtuelle a été accidentellement supprimé.

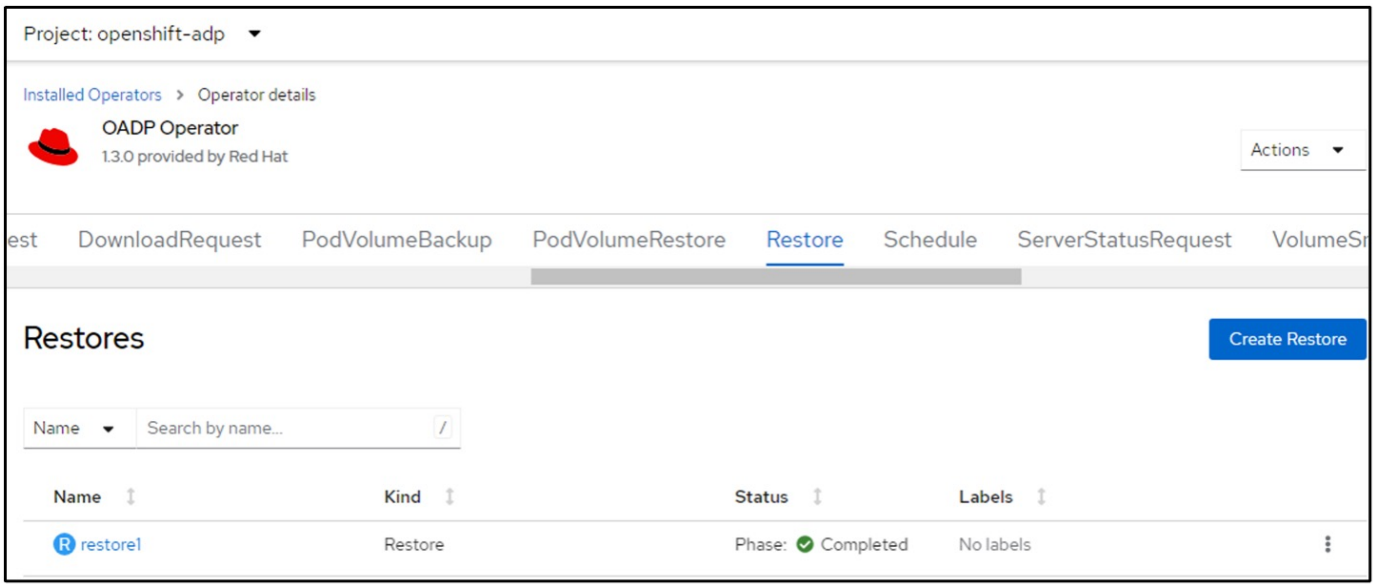
Restaurer dans le même espace de noms

Pour restaurer à partir de la sauvegarde que nous venons de créer, nous devons créer une ressource personnalisée de restauration (CR). Nous devons lui fournir un nom, fournir le nom de la sauvegarde à partir de laquelle nous voulons restaurer et définir les PV de restauration sur true. Des paramètres supplémentaires peuvent être définis comme indiqué dans le "documentation". Cliquez sur le bouton Créer.




```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore1
  namespace: openshift-adp
spec:
  backupName: backup1
  restorePVs: true
```

Lorsque la phase affiche terminé, vous pouvez voir que les machines virtuelles ont été restaurées à l'état au moment où l'instantané a été pris. (Si la sauvegarde a été créée lors de l'exécution de la machine virtuelle, la restauration de la machine virtuelle à partir de la sauvegarde démarre la machine virtuelle restaurée et la met en état d'exécution). La machine virtuelle est restaurée dans le même espace de noms.



Restauration dans un autre espace de noms

Pour restaurer la machine virtuelle dans un espace de noms différent, vous pouvez fournir un espace de noms dans la définition yaml de la CR de restauration.

L'exemple de fichier yaml suivant crée une CR de restauration pour restaurer une machine virtuelle et ses disques dans l'espace de nom de démonstration des machines virtuelles lorsque la sauvegarde a été effectuée dans l'espace de noms des machines virtuelles.

```
apiVersion: velero.io/v1
kind: Restore
metadata:
  name: restore-to-different-ns
  namespace: openshift-adp
spec:
  backupName: backup
  restorePVs: true
  includedNamespaces:
  - virtual-machines-demo
  namespaceMapping:
    virtual-machines-demo: virtual-machines
```

Lorsque la phase affiche terminé, vous pouvez voir que les machines virtuelles ont été restaurées à l'état au moment où l'instantané a été pris. (Si la sauvegarde a été créée lors de l'exécution de la machine virtuelle, la restauration de la machine virtuelle à partir de la sauvegarde démarre la machine virtuelle restaurée et la met en état d'exécution). La machine virtuelle est restaurée dans un espace de noms différent, comme spécifié dans le yaml.

Image::redhat_openshift_OADP_restore_image3.jpg[Restore terminé dans un nouvel espace de noms]%

Suppression des sauvegardes et des restaurations dans à l'aide de Velero

Suppression d'une sauvegarde

Vous pouvez supprimer une CR de sauvegarde sans supprimer les données de stockage d'objet à l'aide de l'outil CLI OC.

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

Si vous souhaitez supprimer la CR de sauvegarde et supprimer les données de stockage d'objets associées, vous pouvez le faire à l'aide de l'outil CLI de Velero.

Téléchargez l'interface de ligne de commande comme indiqué dans les instructions du "Documentation Velero".

Exécutez la commande DELETE suivante à l'aide de l'interface de ligne de commande Velero

```
velero backup delete <backup_CR_name> -n <velero_namespace>
```

Vous pouvez également supprimer la CR de restauration à l'aide de l'interface de ligne de commande Velero

```
velero restore delete restore --namespace openshift-adp
```

Vous pouvez utiliser la commande oc ainsi que l'interface utilisateur pour supprimer la CR de restauration

```
oc delete backup <backup_CR_name> -n <velero_namespace>
```

Solution NetApp de gestion avancée des clusters pour Kubernetes sur Red Hat OpenShift

Gestion avancée des clusters pour Kubernetes : Red Hat OpenShift avec NetApp

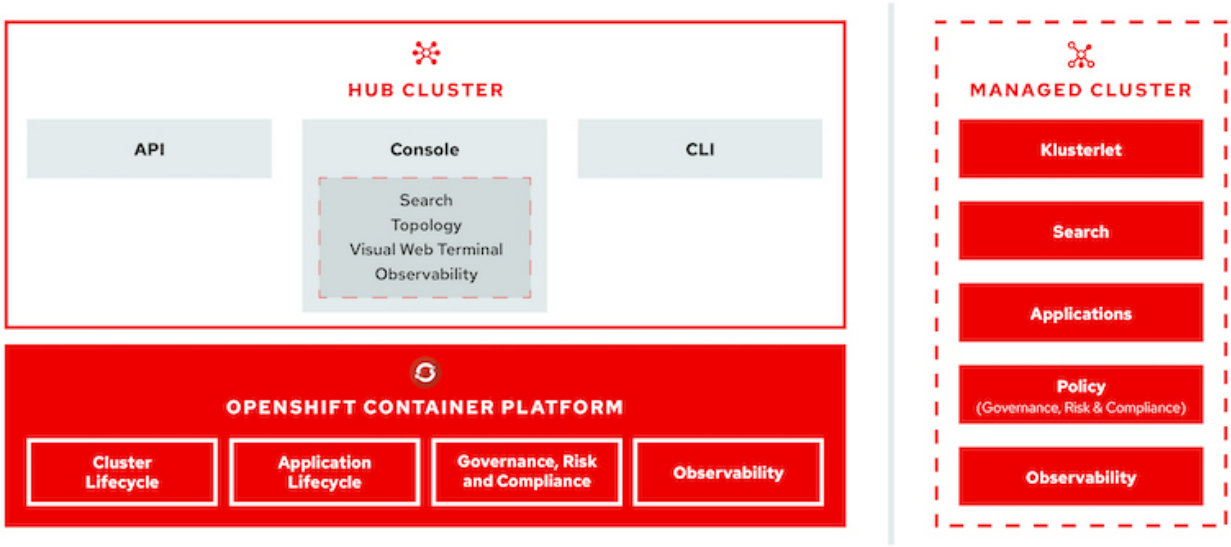
Lorsqu'une application conteneurisée passe du développement à la production, de nombreuses entreprises ont besoin de plusieurs clusters Red Hat OpenShift pour prendre en charge les tests et le déploiement de cette application. Parallèlement, les entreprises hébergent généralement plusieurs applications ou charges de travail sur les clusters OpenShift. Par conséquent, chaque entreprise finit par gérer un ensemble de clusters. Les administrateurs OpenShift doivent donc faire face au défi que représente la gestion et la maintenance de plusieurs clusters sur un large éventail d'environnements répartis sur plusieurs data centers sur site et clouds publics. Pour relever ces défis, Red Hat a introduit la solution avancée de gestion de clusters pour Kubernetes.

Red Hat Advanced Cluster Management pour Kubernetes vous permet d'effectuer les tâches suivantes :

1. Créez, importez et gérez plusieurs clusters entre les data centers et les clouds publics
2. Déployer et gérer des applications ou des charges de travail sur plusieurs clusters à partir d'une console unique

3. Contrôler et analyser l'état et l'état des différentes ressources du cluster
4. Surveillez et appliquez la conformité aux règles de sécurité dans plusieurs clusters

Red Hat Advanced Cluster Management pour Kubernetes est installé en tant qu'extension d'un cluster Red Hat OpenShift, et ce cluster est utilisé comme contrôleur central pour toutes ses opérations. Ce cluster est connu sous le nom de cluster de concentrateur et expose un plan de gestion permettant aux utilisateurs de se connecter à Advanced Cluster Management. Tous les autres clusters OpenShift importés ou créés via la console Advanced Cluster Management sont gérés par le cluster Hub et appelés clusters gérés. Il installe un agent appelé Klausterlet sur les clusters gérés afin de les connecter au cluster Hub et de répondre aux demandes différentes activités liées à la gestion du cycle de vie des clusters, à la gestion du cycle de vie des applications, à l'observabilité et à la conformité de la sécurité.



Pour plus d'informations, reportez-vous à la documentation "ici".

Déploiement

Déploiement de la gestion avancée des clusters pour Kubernetes

Prérequis

1. Un cluster Red Hat OpenShift (supérieur à la version 4.5) pour le cluster Hub
2. Clusters Red Hat OpenShift (supérieurs à la version 4.4.3) pour les clusters gérés
3. L'accès cluster-admin au cluster Red Hat OpenShift
4. Un abonnement Red Hat à Advanced Cluster Management pour Kubernetes

Advanced Cluster Management est un module complémentaire du cluster OpenShift. Il existe donc certaines conditions et restrictions sur les ressources matérielles en fonction des fonctionnalités utilisées sur le concentrateur et les clusters gérés. Vous devez tenir compte de ces problèmes lors du dimensionnement des clusters. Voir la documentation "ici" pour en savoir plus.

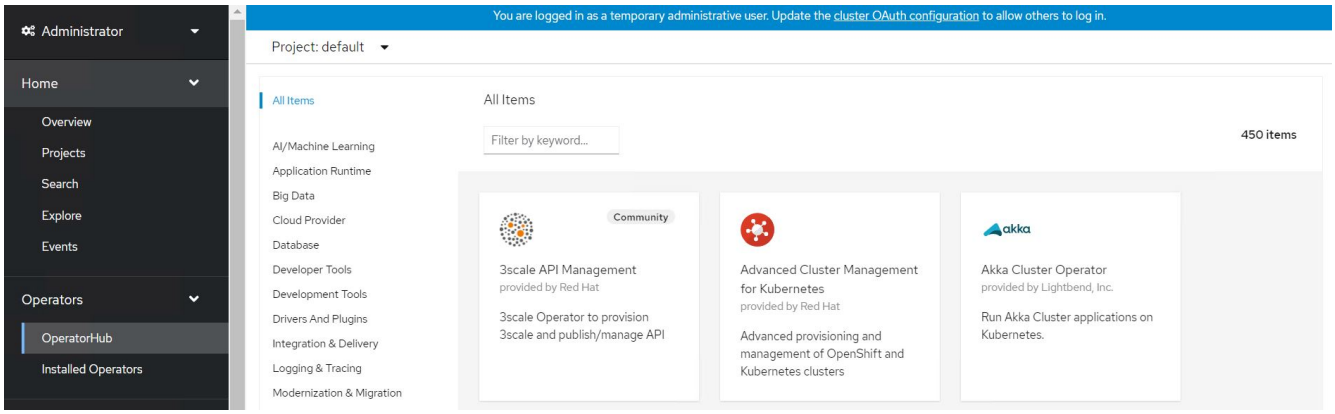
Si le cluster Hub dispose de nœuds dédiés pour héberger les composants de l'infrastructure et que vous souhaitez installer les ressources Advanced Cluster Management uniquement sur ces nœuds, vous devez ajouter des tolérances et des sélecteurs à ces nœuds en conséquence. Pour plus de détails, consultez la

documentation "ici".

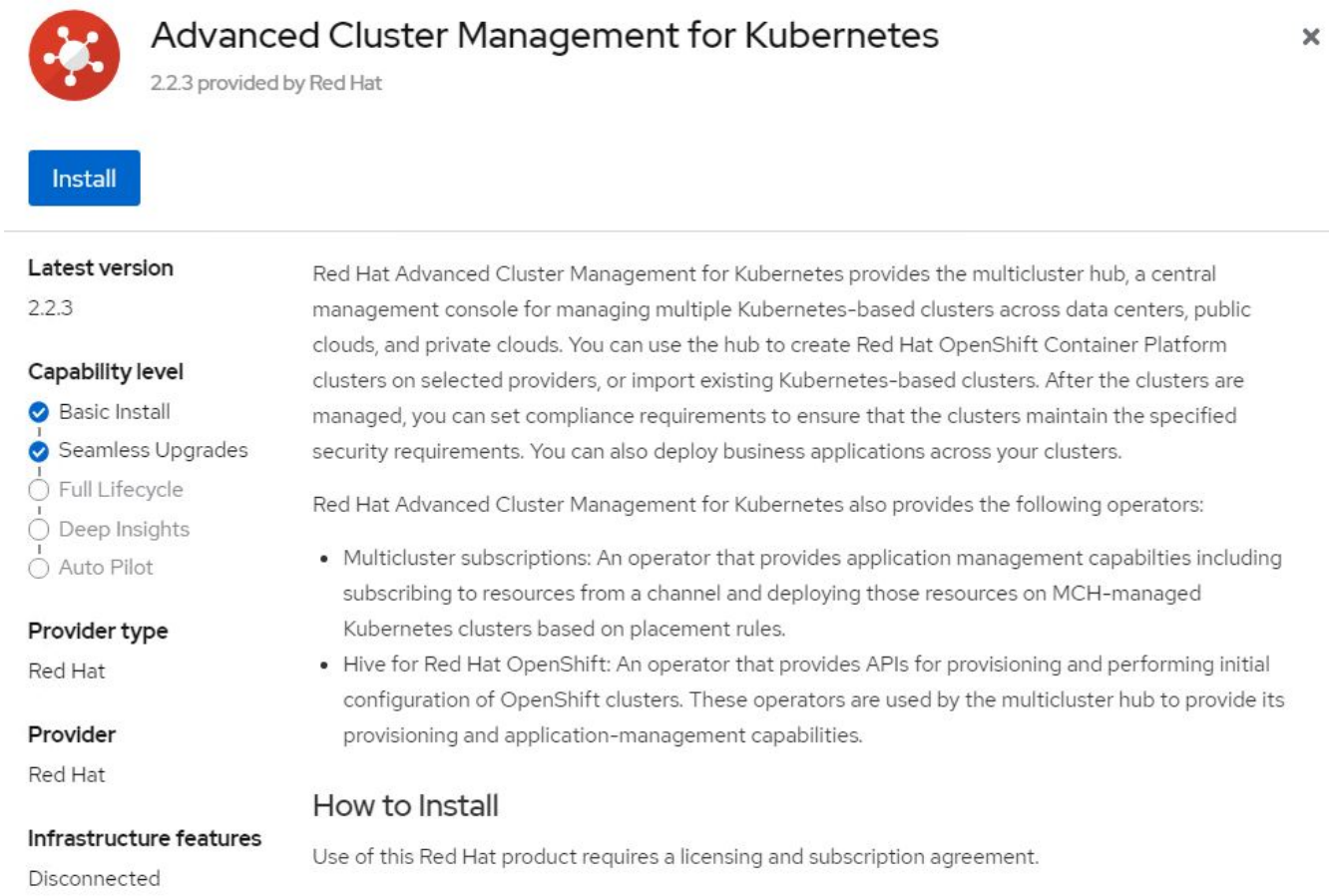
Déploiement de la gestion avancée des clusters pour Kubernetes

Pour installer Advanced Cluster Management pour Kubernetes sur un cluster OpenShift, effectuez les opérations suivantes :

1. Choisissez un cluster OpenShift en tant que cluster Hub et connectez-vous avec les privilèges cluster-admin.
2. Accédez à Operators > Operators Hub et recherchez Advanced Cluster Management pour Kubernetes.



3. Sélectionnez Advanced Cluster Management pour Kubernetes et cliquez sur Install.



4. Dans l'écran Install Operator, indiquez les détails nécessaires (NetApp recommande de conserver les

paramètres par défaut) et cliquez sur Install.

OperatorHub > Operator Installation

Install Operator

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

Update channel *

- release-2.0
- release-2.1
- release-2.2

Installation mode *

- All namespaces on the cluster (default)
  This mode is not supported by this Operator
- A specific namespace on the cluster
  Operator will be available in a single Namespace only.

Installed Namespace *

- Operator recommended Namespace: PR open-cluster-management

Namespace creation
Namespace **open-cluster-management** does not exist and will be created.

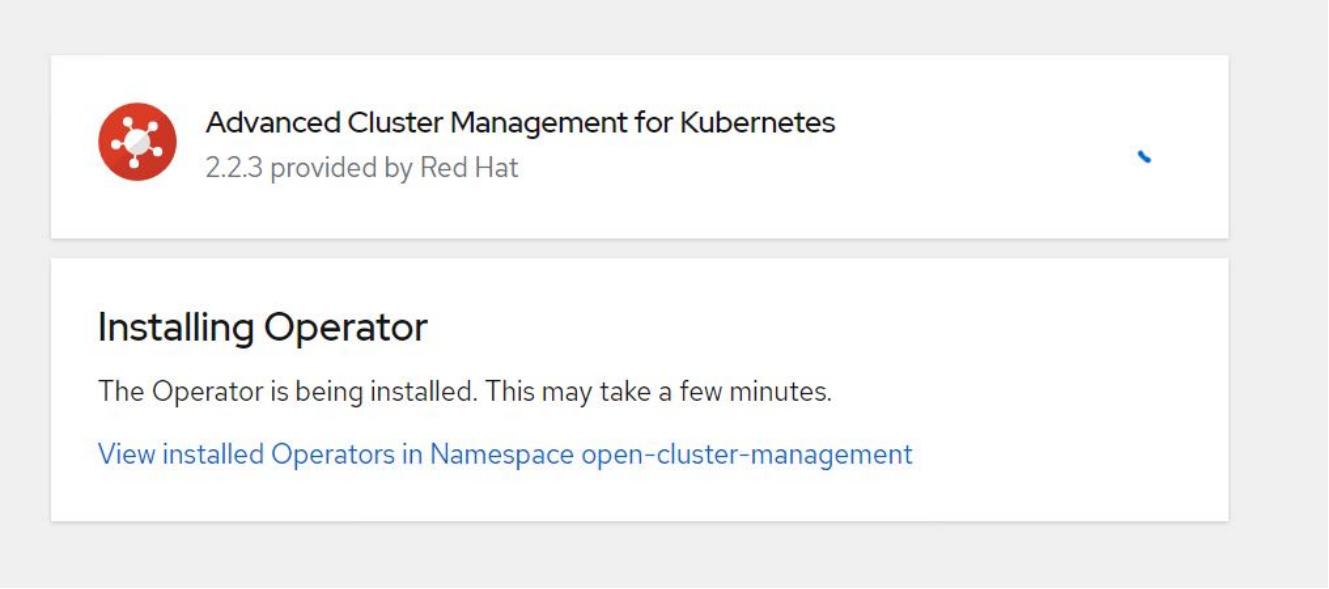
- Select a Namespace

Approval strategy *

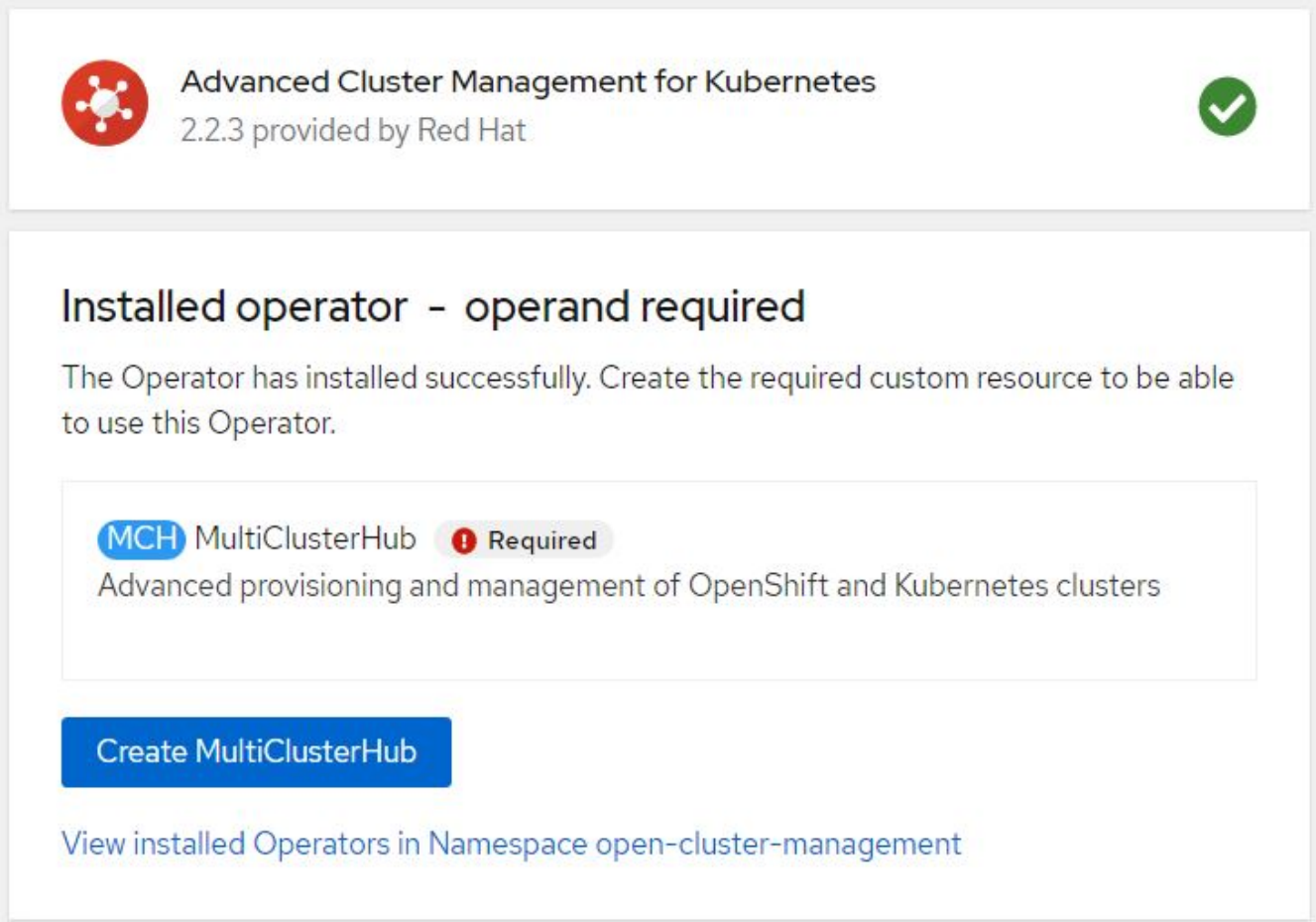
- Automatic
- Manual

Install Cancel

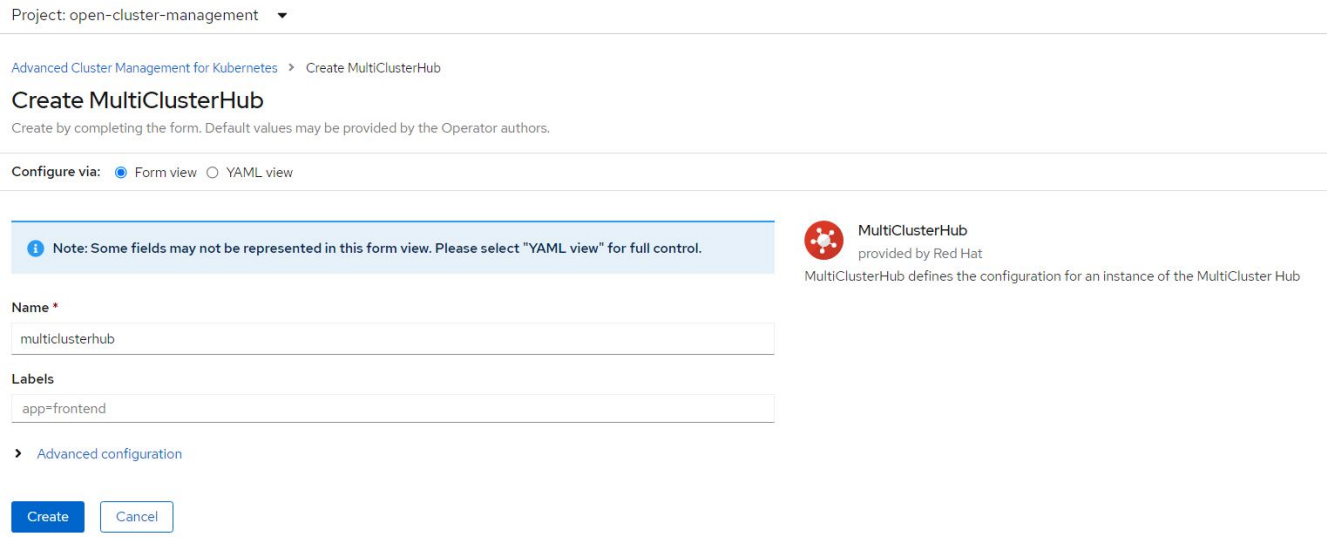
5. Attendre la fin de l'installation par l'opérateur.



6. Une fois l'opérateur installé, cliquez sur Créer MultiClusterHub.



7. Dans l'écran Créer MultiClusterHub, cliquez sur Créer après avoir donné les détails. Cela initie l'installation d'un hub multi-cluster.



8. Une fois que tous les pods passent à l'état d'exécution dans l'espace de noms d'open-cluster-management et que l'opérateur passe à l'état « réussi », Advanced Cluster Management pour Kubernetes est installé.

Project: open-cluster-management

Installed Operators

Installed Operators are represented by ClusterServiceVersions within this Namespace. For more information, see the Understanding Operators documentation. Or create an Operator and ClusterServiceVersion using the Operator SDK.

Name | Search by name...

Name	Managed Namespaces	Status	Provided APIs
Advanced Cluster Management for Kubernetes 2.2.3 provided by Red Hat	NS open-cluster-management	Succeeded Up to date	MultiClusterHub ClusterManager ClusterDeployment ClusterState View 25 more...

9. L'installation du concentrateur prend un certain temps et, une fois cette opération effectuée, le concentrateur MultiCluster passe à l'état d'exécution.

Installed Operators > Operator details

Advanced Cluster Management for Kubernetes
2.2.3 provided by Red Hat

Actions

Details | YAML | Subscription | Events | All instances | MultiClusterHub | ClusterManager | ClusterDeployment | ClusterSt

MultiClusterHubs

Create MultiClusterHub

Name | Search by name...

Name	Kind	Status	Labels
MCH multiclusterhub	MultiClusterHub	Phase: Running	No labels

10. Elle crée une route dans l'espace de noms Open-cluster-management. Connectez-vous à l'URL de la route pour accéder à la console Advanced Cluster Management.

Project: open-cluster-management

Routes

Create Route

Filter | Name | mul

Name mul ✕ | Clear all filters

Name	Status	Location	Service
RT multicloud-console	Accepted	https://multicloud-console.apps.ocp-vmware2.cie.netapp.com	S management-ingress

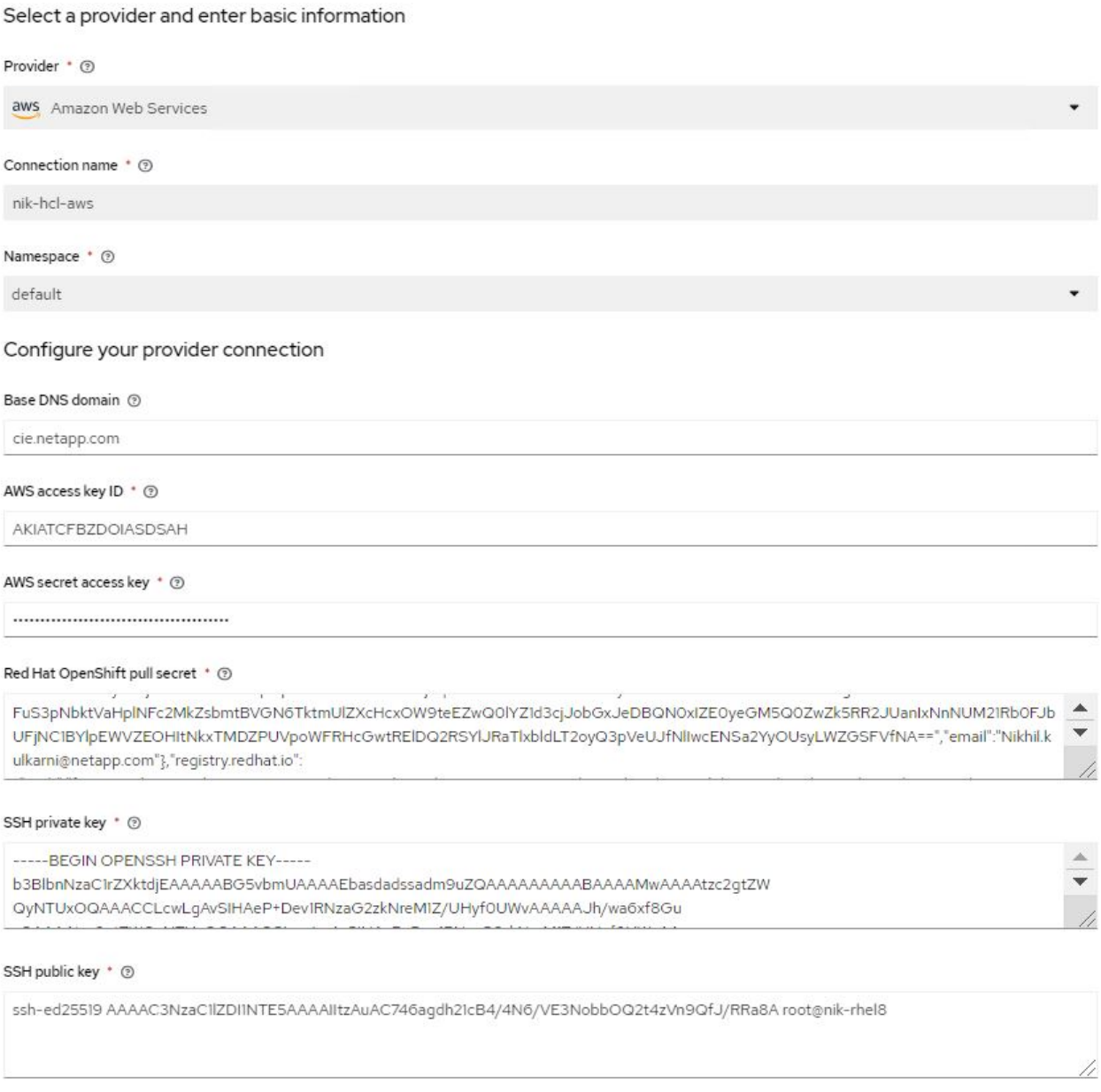
Caractéristiques

Fonctionnalités : gestion avancée des clusters pour Kubernetes sur Red Hat OpenShift avec NetApp

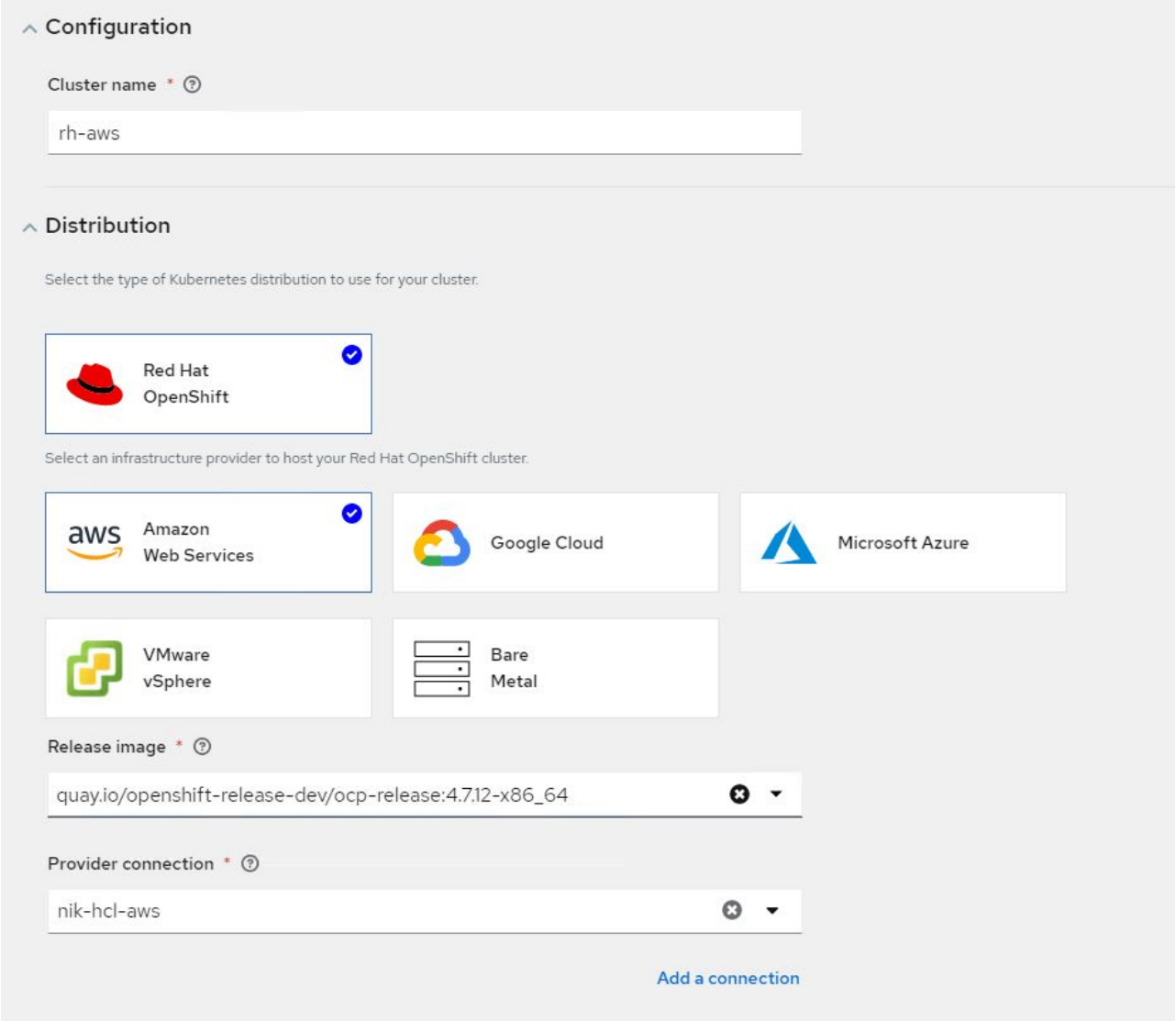
Gestion du cycle de vie des clusters

Pour gérer différents clusters OpenShift, vous pouvez les créer ou les importer dans Advanced Cluster Management.

1. Commencez par automatiser les infrastructures > clusters.
2. Pour créer un cluster OpenShift, effectuez les opérations suivantes :
   a. Créer une connexion fournisseur : accédez à connexions fournisseur et cliquez sur Ajouter une connexion, fournissez tous les détails correspondant au type de fournisseur sélectionné et cliquez sur Ajouter.

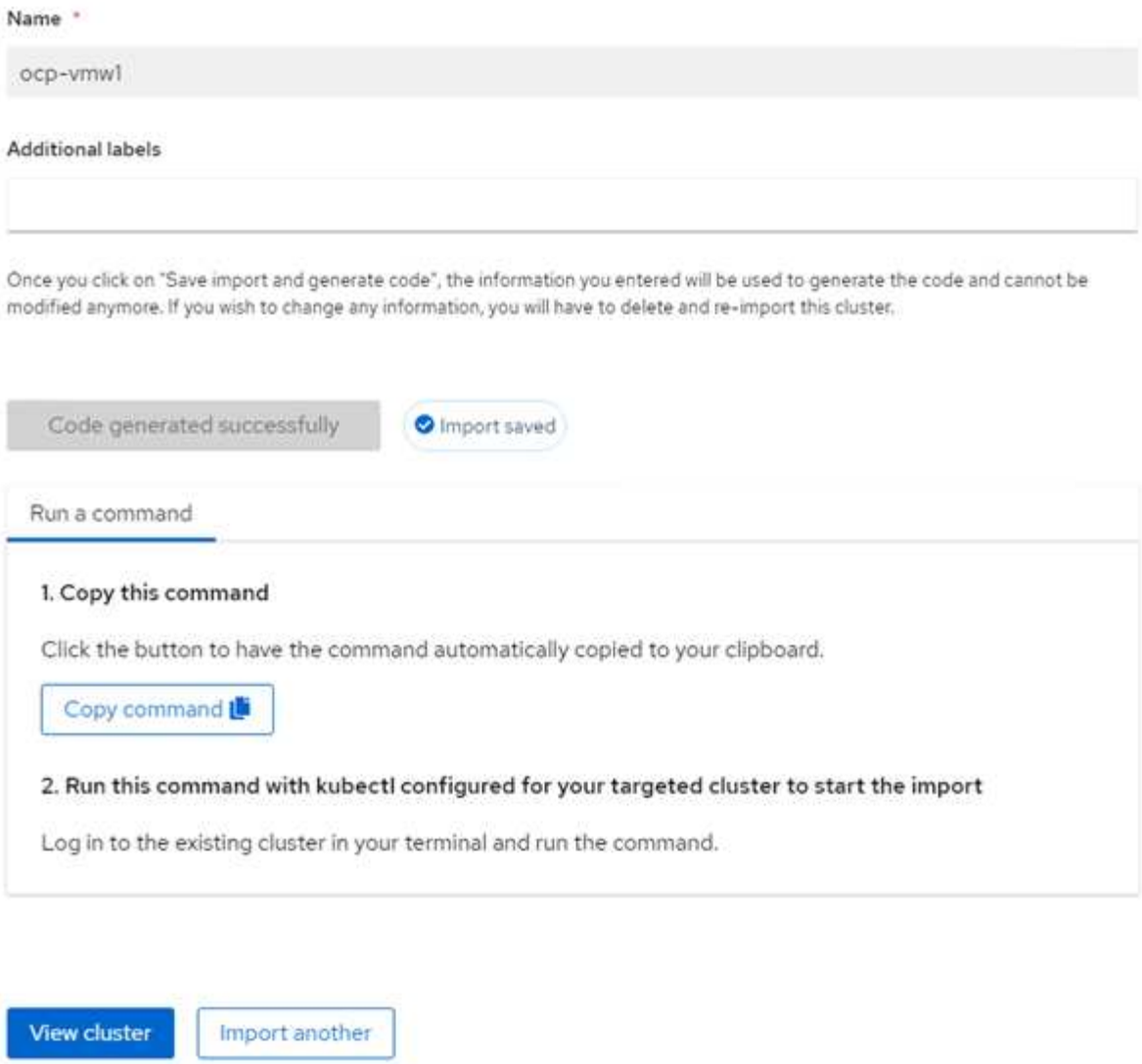


   b. Pour créer un nouveau cluster, accédez à clusters et cliquez sur Ajouter un cluster > Créer un cluster. Fournissez les détails du cluster et du fournisseur correspondant, puis cliquez sur Créer.



c. Une fois le cluster créé, il apparaît dans la liste des clusters avec l'état prêt.

3. Pour importer un cluster existant, procédez comme suit :
   a. Accédez à clusters et cliquez sur Ajouter un cluster > Importer un cluster existant.
   b. Entrez le nom du cluster, puis cliquez sur Enregistrer l'importation et générer le code. Une commande permettant d'ajouter le cluster existant est affichée.
   c. Cliquez sur Copy Command et exécutez la commande sur le cluster à ajouter au cluster Hub. Cette opération lance l'installation des agents nécessaires sur le cluster et, une fois ce processus terminé, le cluster apparaît dans la liste des clusters avec l'état prêt.



4. Une fois que vous avez créé et importé plusieurs clusters, vous pouvez les surveiller et les gérer à partir d'une seule console.

Fonctionnalités : gestion avancée des clusters pour Kubernetes sur Red Hat OpenShift avec NetApp

Gestion du cycle de vie des applications

Pour créer une application et la gérer dans un ensemble de clusters,

1. Accédez à gérer les applications dans la barre latérale et cliquez sur Créer une application. Indiquez les détails de l'application que vous souhaitez créer et cliquez sur Enregistrer.

Applications /

Create an application YAML: Off

Cancel Save

Name*

demo-app

Namespace*

default

Repository location for resources

Repository types

Select the type of repository where resources that you want to deploy are located

Git

URL*

https://github.com/open-cluster-management/acm-hive-openshift-releases.git

Branch

main

Path

clusterImageSets/fast/4.7

2. Une fois les composants de l'application installés, l'application apparaît dans la liste.

Applications

Refresh every 15s

Last update: 7:36:23 PM

Overview Advanced configuration

Create application

Search

Name	Namespace	Clusters	Resource	Time window	Created
demo-app	default	Local	Git		8 days ago

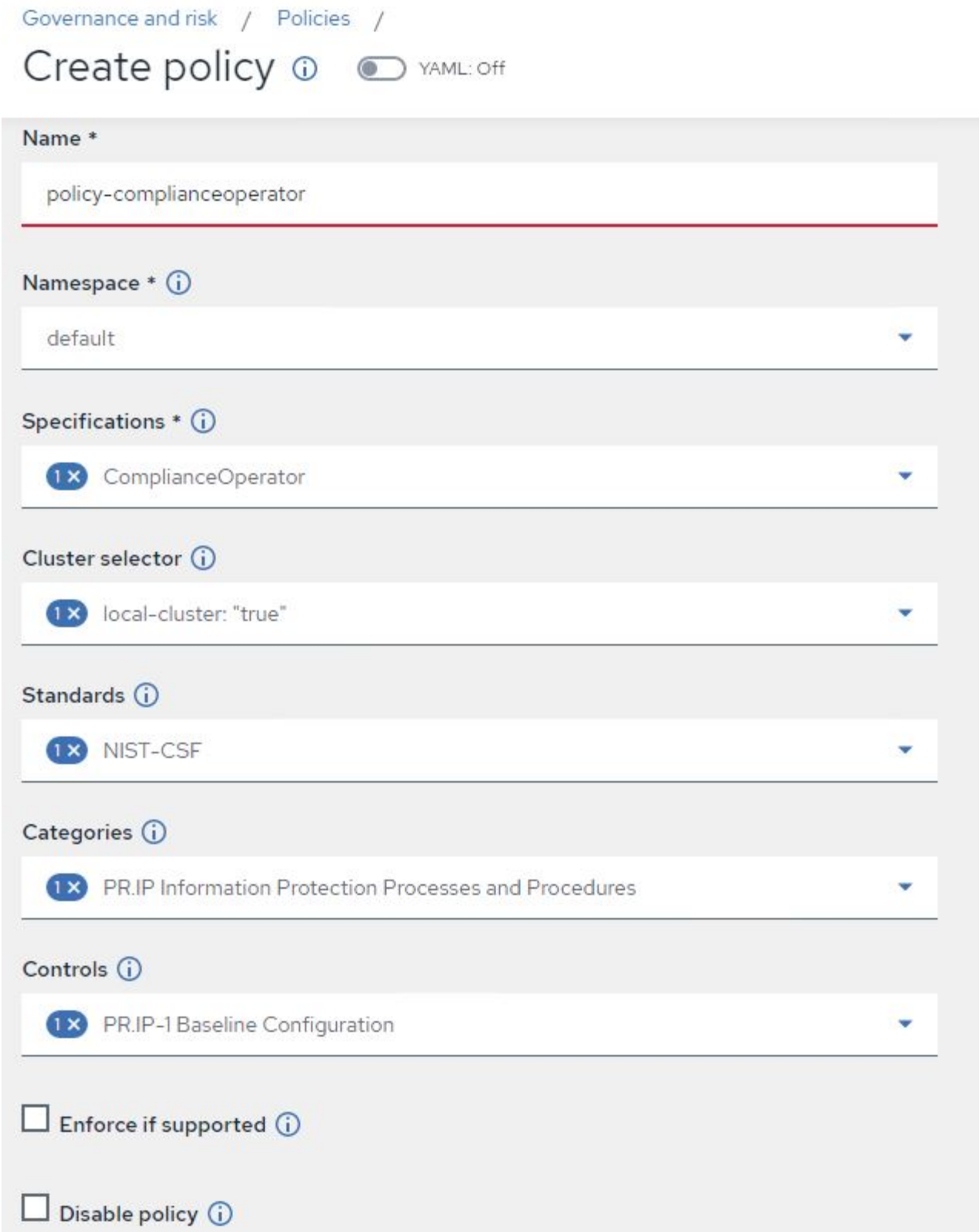
1 - 1 of 1 1 of 1

3. L'application peut désormais être contrôlée et gérée depuis la console.

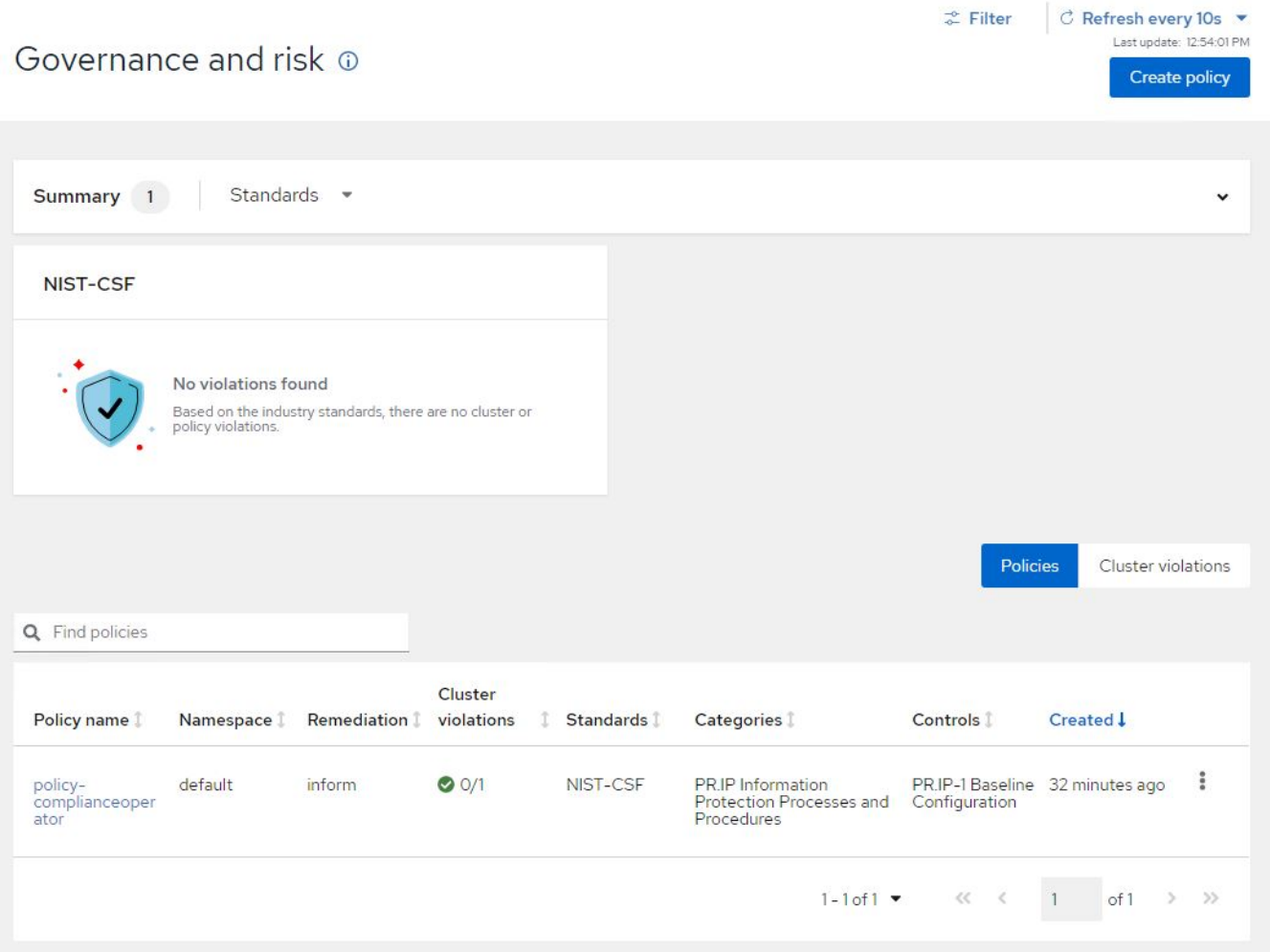
Gouvernance et risque

Cette fonctionnalité vous permet de définir les stratégies de conformité des différents clusters et de vous assurer que ces clusters l'adhèrent. Vous pouvez configurer les règles pour les informer ou corriger toute déviation ou violation des règles.

1. Accédez à gouvernance et risque depuis la barre latérale.
2. Pour créer des stratégies de conformité, cliquez sur Créer une stratégie, entrez les détails des normes de stratégie et sélectionnez les clusters qui doivent respecter cette stratégie. Si vous souhaitez corriger automatiquement les violations de cette stratégie, cochez la case appliquer si elle est prise en charge, puis cliquez sur Créer.



3. Une fois toutes les règles requises configurées, toutes les violations des règles ou des clusters peuvent être surveillées et remédier aux problèmes dans Advanced Cluster Management.

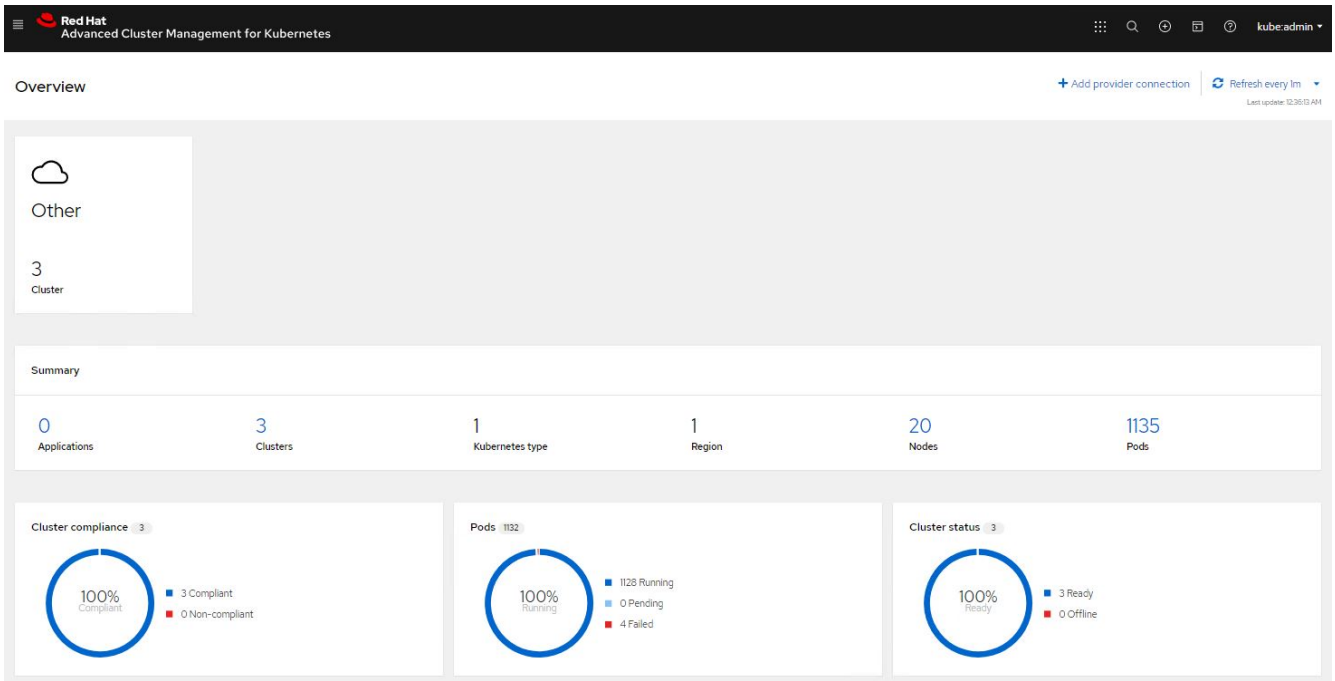


Fonctionnalités : gestion avancée des clusters pour Kubernetes sur Red Hat OpenShift avec NetApp

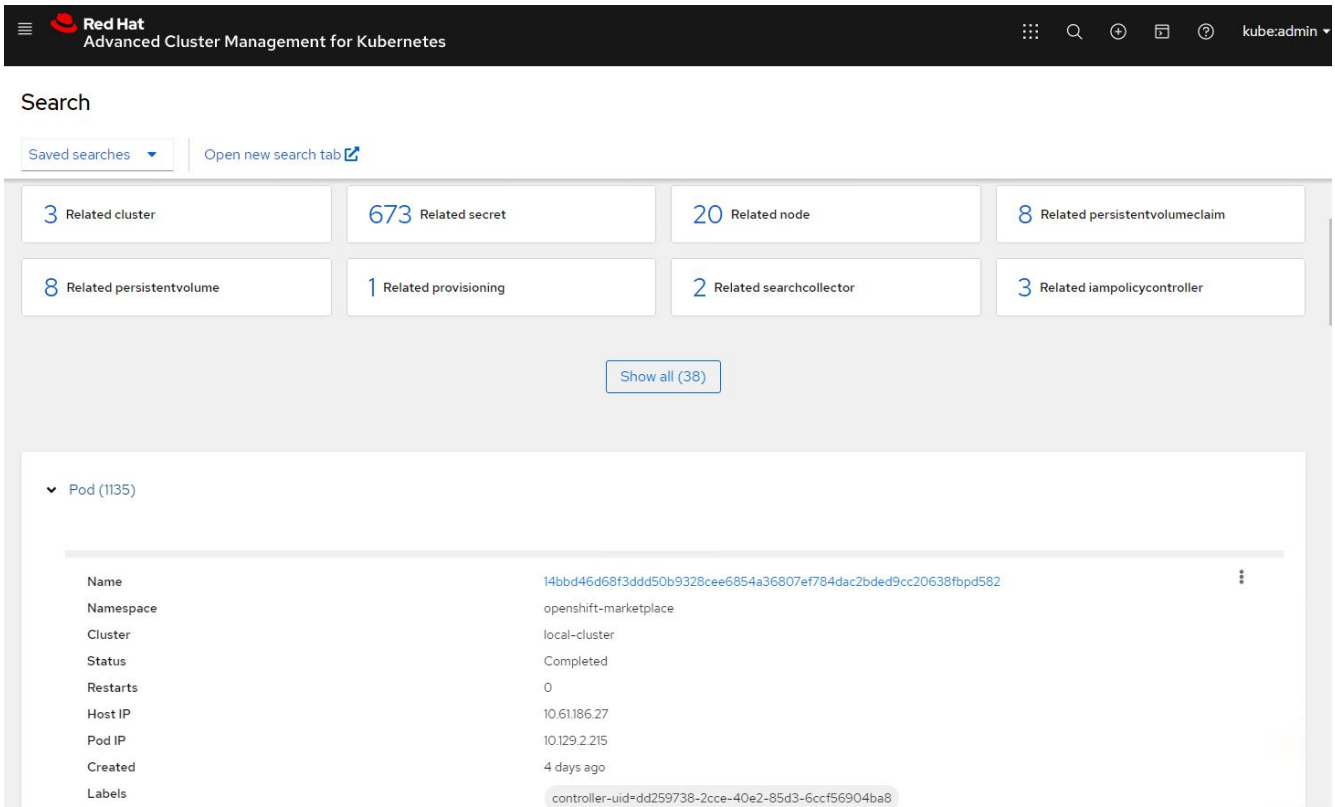
Observabilité

La solution Advanced Cluster Management pour Kubernetes fournit un moyen de surveiller les nœuds, les pods, les applications et les workloads dans l'ensemble des clusters.

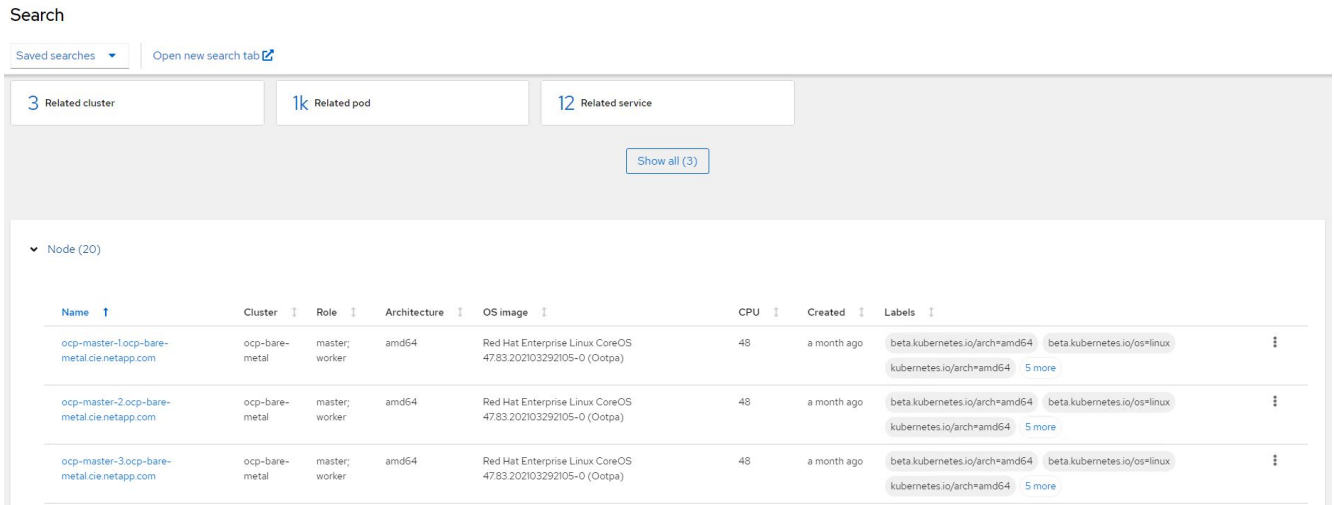
1. Naviguez jusqu'à observer les environnements > Présentation.



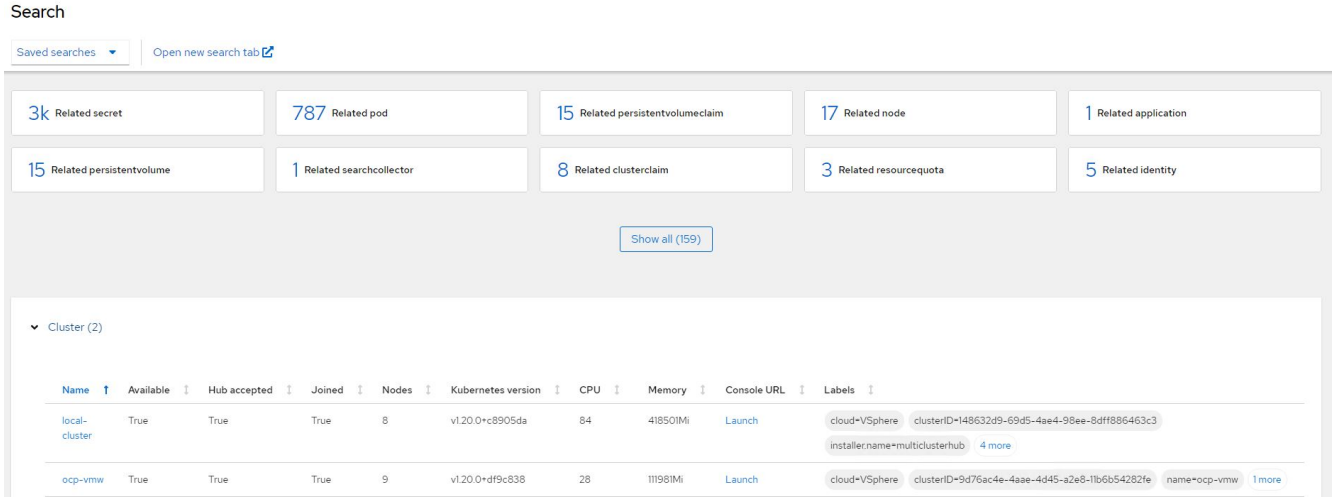
2. Tous les pods et les charges de travail dans tous les clusters sont surveillés et triés en fonction de différents filtres. Cliquez sur Pods pour afficher les données correspondantes.



3. Tous les nœuds des clusters sont surveillés et analysés en fonction de divers points de données. Cliquez sur nœuds pour obtenir plus d'informations sur les détails correspondants.



4. Tous les clusters sont surveillés et organisés en fonction de différents paramètres et ressources de cluster. Cliquez sur clusters pour afficher les détails du cluster.



Fonctionnalités : gestion avancée des clusters pour Kubernetes sur Red Hat OpenShift avec NetApp

Créer des ressources sur plusieurs clusters

La gestion avancée des clusters pour Kubernetes permet aux utilisateurs de créer des ressources sur un ou plusieurs clusters gérés simultanément à partir de la console. Par exemple, si vous disposez de clusters OpenShift sur différents sites et que ONTAP vous souhaitez provisionner des PVC sur les deux sites, vous pouvez cliquer sur le signe (+) de la barre d'onglets. Sélectionnez ensuite les clusters sur lesquels vous souhaitez créer la demande de volume persistant, collez la ressource YAML, puis cliquez sur Créer.

Create resource

Cancel | Create

Clusters | Select the clusters where the resource(s) will be deployed.

2 × local-cluster, ocp-vmw

Resource configuration | Enter the configuration manifest for the resource(s).

YAML

```yaml
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: demo-pvc
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ocp-trident
```

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.