Présentation de NetApp Astra Control Center

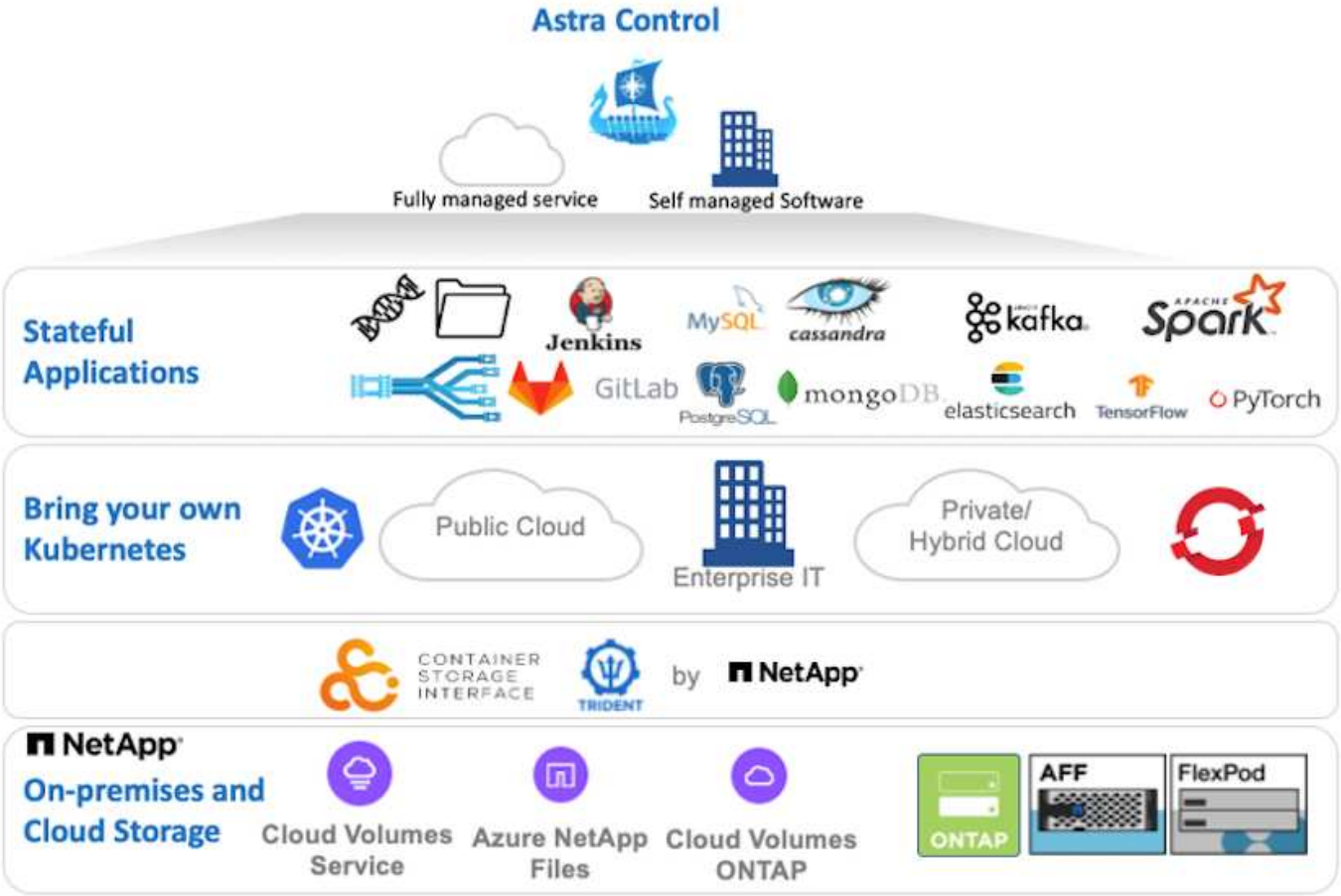
NetApp Solutions

NetApp
April 26, 2024

Sommaire

Présentation de NetApp Astra Control Center

NetApp Astra Control Center propose un ensemble complet de services de gestion du stockage et des données respectueuse des applications pour les workloads Kubernetes avec état, déployés dans un environnement sur site et optimisé par les technologies NetApp de protection des données.



NetApp Astra Control Center peut être installé sur un cluster Red Hat OpenShift que l'orchestrateur de stockage Astra Trident est déployé et configuré avec des classes de stockage et des systèmes back-end de stockage dans des systèmes de stockage NetApp ONTAP.

Pour l'installation et la configuration d'Astra Trident pour prendre en charge Astra Control Center, voir "ce document ici".

Dans un environnement connecté au cloud, Astra Control Center utilise Cloud Insights pour fournir des fonctionnalités avancées de surveillance et de télémétrie. En l'absence de connexion Cloud Insights, un contrôle limité et une télémétrie (valeurs de metrics de 7 jours) sont disponibles et exportés vers les outils de contrôle natifs Kubernetes (Prometheus et Grafana) via des terminaux ouverts.

Le centre de contrôle Astra est entièrement intégré à l'écosystème NetApp AutoSupport et Active IQ qui fournit un soutien aux utilisateurs, fournit des conseils pour la résolution de problèmes et affiche des statistiques d'utilisation.

En plus de la version payante d'Astra Control Center, une licence d'évaluation de 90 jours est disponible. La version d'évaluation est prise en charge par e-mail et par la communauté (Channel Slack). Les clients ont accès à ces articles, ainsi qu'à d'autres articles de la base de connaissances, et à la documentation disponible dans le tableau de bord de support des produits.

Pour commencer avec NetApp Astra Control Center, rendez-vous sur le "Site Web d'Astra".

Conditions préalables à l'installation d'Astra Control Center

1. Un ou plusieurs clusters Red Hat OpenShift. Les versions 4.6 EUS et 4.7 sont actuellement prises en charge.
2. Astra Trident doit déjà être installé et configuré sur chaque cluster Red Hat OpenShift.
3. Un ou plusieurs systèmes de stockage NetApp ONTAP exécutant ONTAP 9.5 ou version ultérieure.

   > Il est recommandé que chaque installation OpenShift sur un site dispose d'un SVM dédié pour le stockage persistant. Les déploiements multisites requièrent des systèmes de stockage supplémentaires.

4. Un système back-end de stockage Trident doit être configuré sur chaque cluster OpenShift avec un SVM sauvegardé par un cluster ONTAP.
5. Classe de stockage par défaut configurée sur chaque cluster OpenShift avec Astra Trident comme provisionneur de stockage.
6. Un équilibreur de charge doit être installé et configuré sur chaque cluster OpenShift pour équilibrer les charges et exposer les services OpenShift.

   > Voir le lien "ici" pour plus d'informations sur les équilibreurs de charge qui ont été validés à cet effet.

7. Un registre d'images privées doit être configuré pour héberger les images du NetApp Astra Control Center.

   > Voir le lien "ici" Pour installer et configurer un registre privé OpenShift à cet effet.

8. Vous devez disposer d'un accès Cluster Admin au cluster Red Hat OpenShift.
9. Vous devez disposer d'un accès d'administration aux clusters NetApp ONTAP.
10. Une station de travail d'administration avec docker ou podman, tridentctl et oc ou kubectl a été installée et ajoutée à votre $PATH

    > Les installations Docker doivent avoir une version docker supérieure à 20.10 et les installations Podman doivent avoir une version podman supérieure à 3.0.

Poser le centre de contrôle Astra

Utilisation de OperatorHub

1. Connectez-vous au site de support NetApp et téléchargez la dernière version de NetApp Astra Control Center. Une licence associée à votre compte NetApp est requise. Après avoir téléchargé le fichier tarball, transférez-le sur le poste de travail d'administration.

   Pour commencer avec une licence d'essai d'Astra Control, visitez le "Site d'inscription à Astra".

2. Déballez la boule tar et remplacez le répertoire de travail par le dossier obtenu.

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

3. Avant de commencer l'installation, poussez les images du centre de contrôle Astra vers un registre d'images. Vous pouvez choisir de le faire avec Docker ou Podman, les instructions pour les deux sont fournies dans cette étape.

Podman

a. Exportez le FQDN du Registre avec le nom de l'organisation/espace de noms/projet comme variable d'environnement 'regiant'.

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

b. Connectez-vous au registre.

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

> Si vous utilisez `kubeadmin` l'utilisateur doit se connecter au registre privé, puis utiliser un jeton au lieu du mot de passe - `podman login -u ocp-user -p token --tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com`.

> Vous pouvez également créer un compte de service, attribuer un rôle d'éditeur de registre et/ou de visualiseur de registre (selon que vous avez besoin d'un accès Push/Pull) et vous connecter au registre à l'aide du jeton du compte de service.

c. Créez un fichier de script shell et collez le contenu suivant dans celui-ci.

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

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

> Si vous utilisez des certificats non approuvés pour votre registre, modifiez le script de shell et utilisez-le `--tls-verify=false` pour la commande push podman `podman push $REGISTRY/$(echo $astraImage | sed 's/[\/]\+\///') --tls-verify=false`.

d. Rendre le fichier exécutable.

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

e. Exécutez le script de shell.

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

Docker

a. Exportez le FQDN du Registre avec le nom de l'organisation/espace de noms/projet comme variable d'environnement 'regiant'.

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

b. Connectez-vous au registre.

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

> Si vous utilisez `kubeadmin` l'utilisateur doit se connecter au registre privé, puis utiliser un jeton au lieu du mot de passe - `docker login -u ocp-user -p token astra-registry.apps.ocp-vmw.cie.netapp.com`.

> Vous pouvez également créer un compte de service, attribuer un rôle d'éditeur de registre et/ou de visualiseur de registre (selon que vous avez besoin d'un accès Push/Pull) et vous connecter au registre à l'aide du jeton du compte de service.

c. Créez un fichier de script shell et collez le contenu suivant dans celui-ci.

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

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

d. Rendre le fichier exécutable.

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

e. Exécutez le script de shell.

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

4. Lorsque vous utilisez des registres d'images privés qui ne sont pas de confiance publique, chargez les certificats TLS du registre d'images sur les nœuds OpenShift. Pour ce faire, créez une config map dans l'espace de noms openshift-config à l'aide des certificats TLS et installez-la sur la configuration d'images du cluster pour que le certificat soit fiable.

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

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

> Si vous utilisez un registre interne OpenShift avec des certificats TLS par défaut de l'opérateur d'entrée portant une route, vous devez suivre l'étape précédente pour corriger le nom d'hôte de la route. Pour extraire les certificats de l'opérateur Ingress, vous pouvez utiliser la commande `oc extract secret/router-ca --keys=tls.crt -n openshift-ingress-operator`.

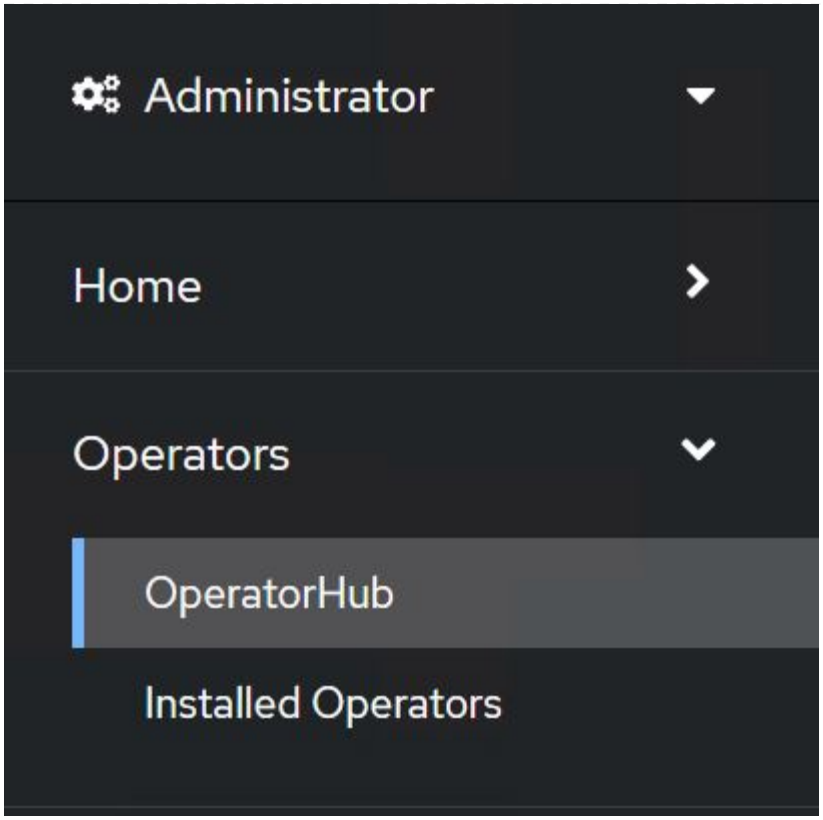
5. Créer un espace de noms `netapp-acc-operator` Pour Astra Control Center.

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

namespace/netapp-acc-operator created
```

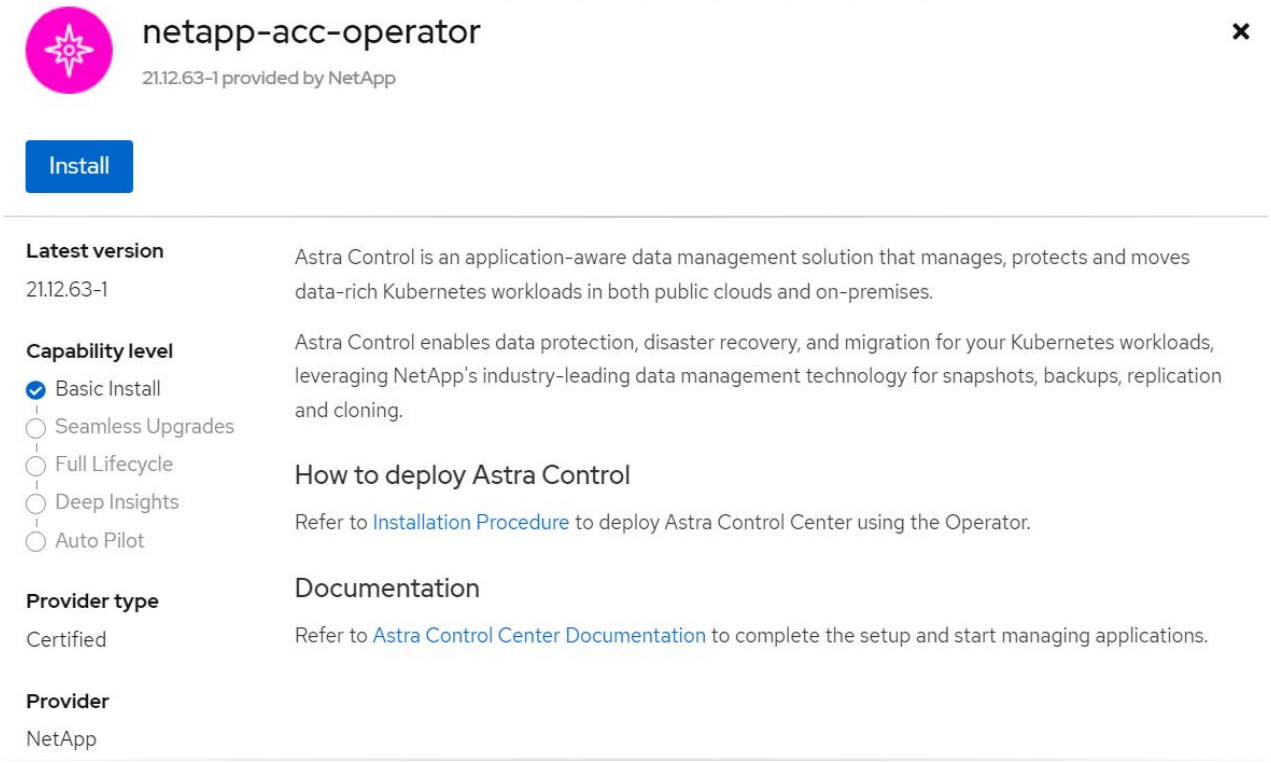
6. Créez un secret avec des informations d'identification pour vous connecter au registre d'images dans `netapp-acc-operator` espace de noms.

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

secret/astra-registry-cred created
```

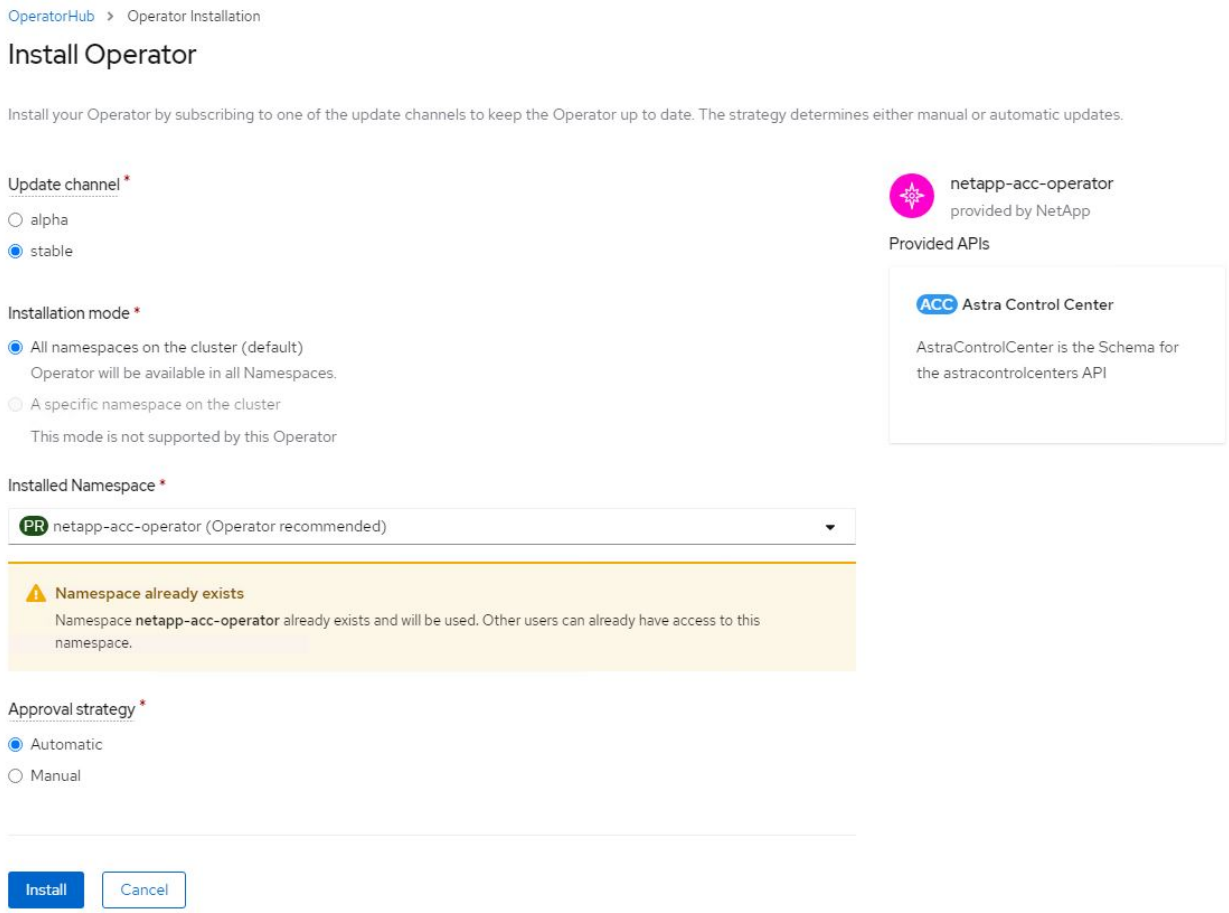
7. Connectez-vous à la console IUG de Red Hat OpenShift avec un accès cluster-admin.
8. Sélectionnez Administrateur dans la liste déroulante perspective.
9. Accédez à Operators > OperatorHub et recherchez Astra.



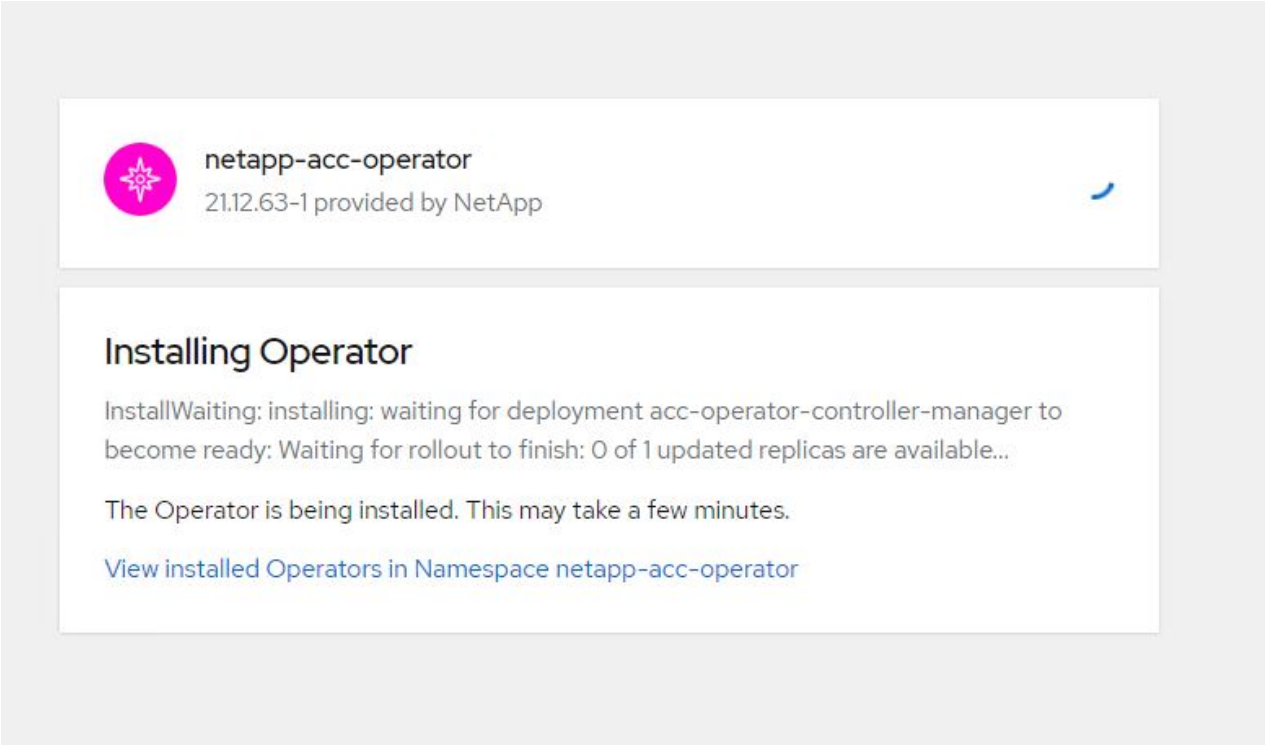
10. Sélectionnez `netapp-acc-operator` mosaïque et clic `Install`.



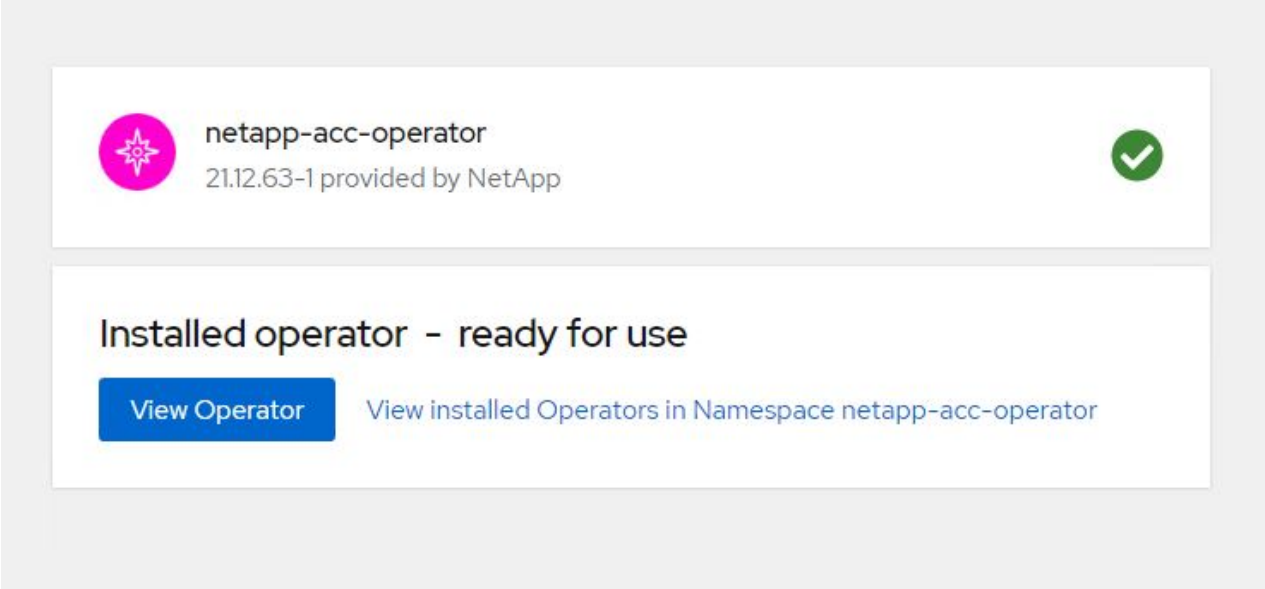
11. Sur l'écran installer l'opérateur, acceptez tous les paramètres par défaut et cliquez sur `Install`.



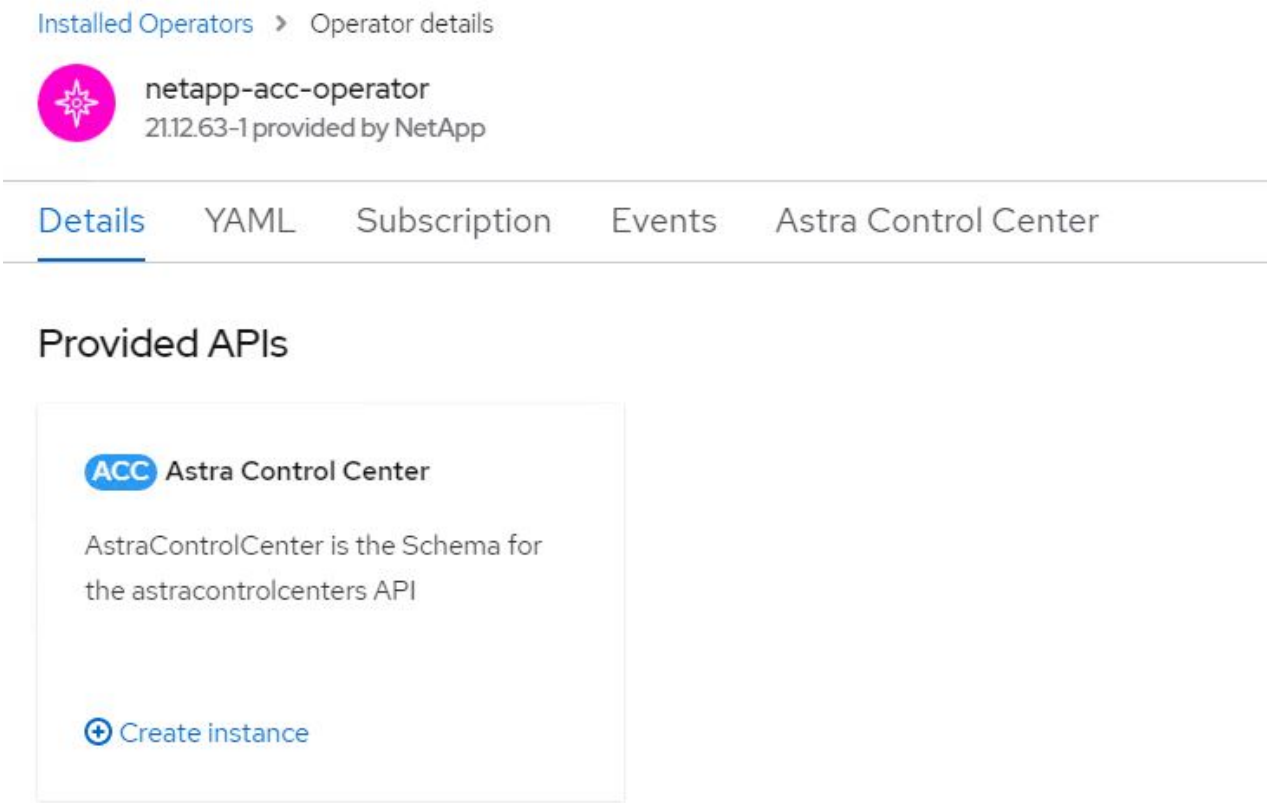
12. Attendre la fin de l'installation par l'opérateur.



13. Une fois l'installation de l'opérateur réussie, cliquez sur `View Operator`.



14. Cliquez ensuite sur `Create Instance` Dans la mosaïque Astra Control Center du conducteur.



15. Remplissez le `Create AstraControlCenter` et cliquez sur `Create`.

    a. Vous pouvez modifier le nom de l'instance du Centre de contrôle Astra.
    b. Vous pouvez éventuellement activer ou désactiver Auto support. Il est recommandé de conserver la fonctionnalité Auto support.
    c. Saisissez le nom de domaine complet pour Astra Control Center.
    d. Accédez à la version du Centre de contrôle Astra ; la dernière est affichée par défaut.

e. Entrez un nom de compte pour le centre de contrôle Astra et des détails d'administrateur tels que le prénom, le nom et l'adresse e-mail.

f. Entrez la règle de récupération du volume. La valeur par défaut est conservation.

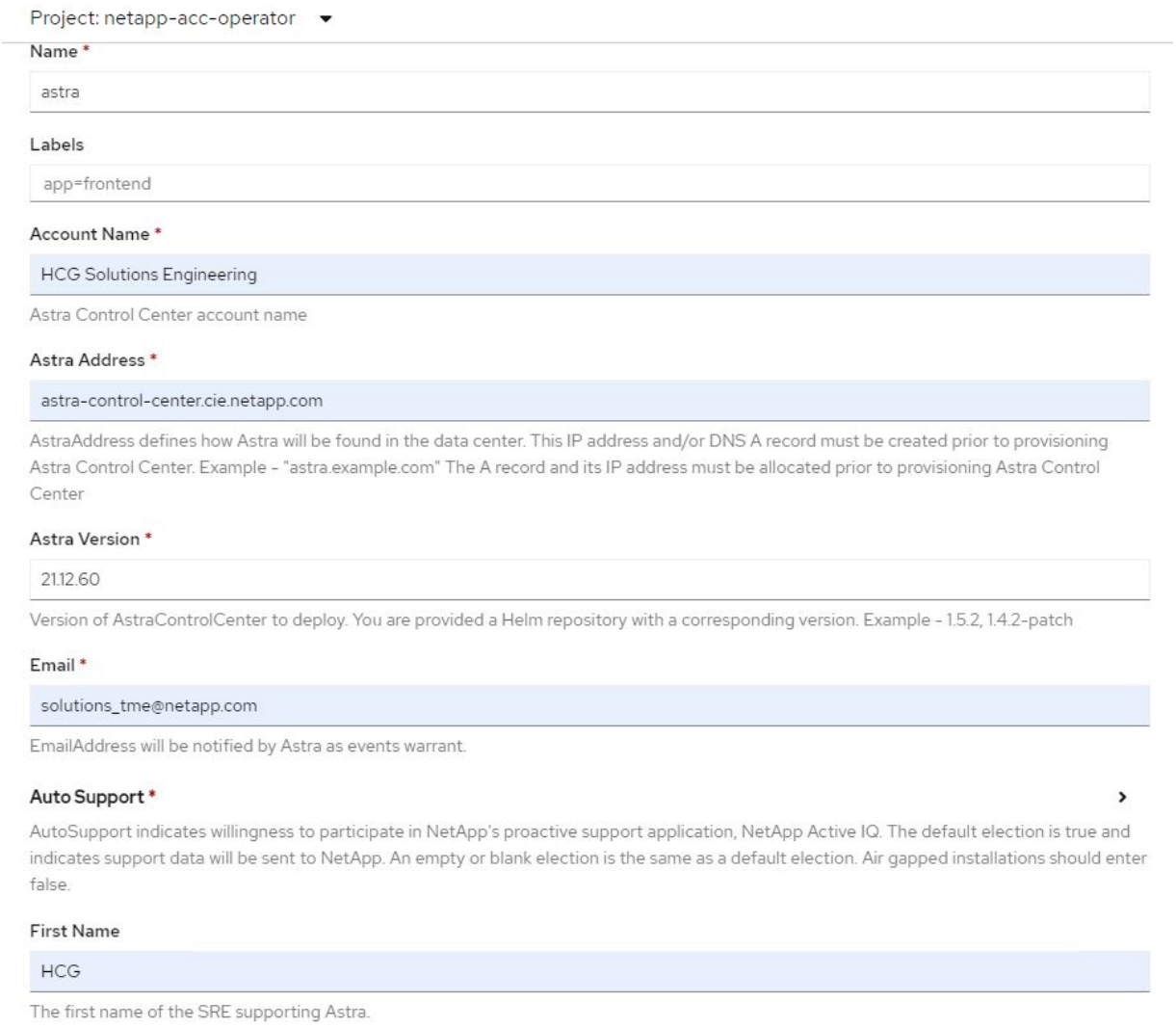
g. Dans le Registre d'images, entrez le FQDN de votre registre ainsi que le nom d'organisation tel qu'il a été donné lors de l'envoi des images au Registre (dans cet exemple, `astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra`)

h. Si vous utilisez un registre qui nécessite une authentification, entrez le nom secret dans la section Registre d'images.

i. Configurez les options d'échelle pour les limites de ressources Astra Control Center.

j. Entrez le nom de la classe de stockage si vous souhaitez placer des ESV sur une classe de stockage non-défaut.

k. Définissez les préférences de gestion de CRD.



Last Name

Admin

The last name of the SRE supporting Astra.

Image Registry

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

Name

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

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

Secret

astra-registry-cred

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

Volume Reclaim Policy

Retain

Reclaim policy to be set for persistent volumes

Astra Resources Scaler

Default

Scaling options for AstraControlCenter Resource limits.

Storage Class

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

Crds

Options for how ACC should handle CRDs.

Create Cancel

Automatisation [Ansible]

1. Pour déployer Astra Control Center sur un playbooks Ansible, vous devez utiliser un ordinateur Ubuntu/RHEL avec Ansible installé. Suivre les procédures "ici" Pour Ubuntu et RHEL.
2. Clonez le référentiel GitHub qui héberge le contenu Ansible.

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

3. Connectez-vous au site de support NetApp et téléchargez la dernière version de NetApp Astra Control Center. Une licence associée à votre compte NetApp est requise. Après avoir téléchargé le tarball, transférez-le sur le poste de travail.

> Pour commencer avec une licence d'essai d'Astra Control, visitez le "Site d'inscription à Astra".

4. Créez ou obtenez le fichier kubeconfig avec un accès administrateur au cluster OpenShift sur lequel vous devez installer Astra Control Center.

5. Remplacez le répertoire par na_astra_control_suite.

```
cd na_astra_control_suite
```

6. Modifiez le `vars/vars.yml` et remplissez les variables avec les informations requises.

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

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

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

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

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

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

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

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

#Reclaim Policy for Astra Control Center Persistent Volumes [Allowed
values: Retain, Delete]
```

```
storageclass_reclaim_policy: Retain

#Private Registry Details
astra_registry_name: "docker.io"

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

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

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

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

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

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

7. Utilisez le PlayBook pour déployer le centre de contrôle Astra. Le PlayBook requiert des privilèges root pour certaines configurations.

   Si l'utilisateur exécutant le PlayBook est root ou a configuré un sudo sans mot de passe, exécutez la commande suivante pour exécuter le PlayBook.

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

   Si l'accès sudo basé sur un mot de passe est configuré, exécutez la commande suivante pour exécuter le PlayBook, puis saisissez le mot de passe sudo.

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

Après l'installation

1. L'installation peut prendre plusieurs minutes. Vérifier que tous les pods et services dans le `netapp-astra-cc` les espaces de noms sont opérationnels.

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

2. Vérifier le `acc-operator-controller-manager` journaux pour vérifier que l'installation est terminée.

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

> Le message suivant indique que le centre de contrôle Astra a été installé avec succès.

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

3. Le nom d'utilisateur pour la connexion à Astra Control Center est l'adresse électronique de l'administrateur fournie dans le fichier CRD et le mot de passe est une chaîne `ACC-` Joint à l'UUID du centre de contrôle Astra. Exécutez la commande suivante :

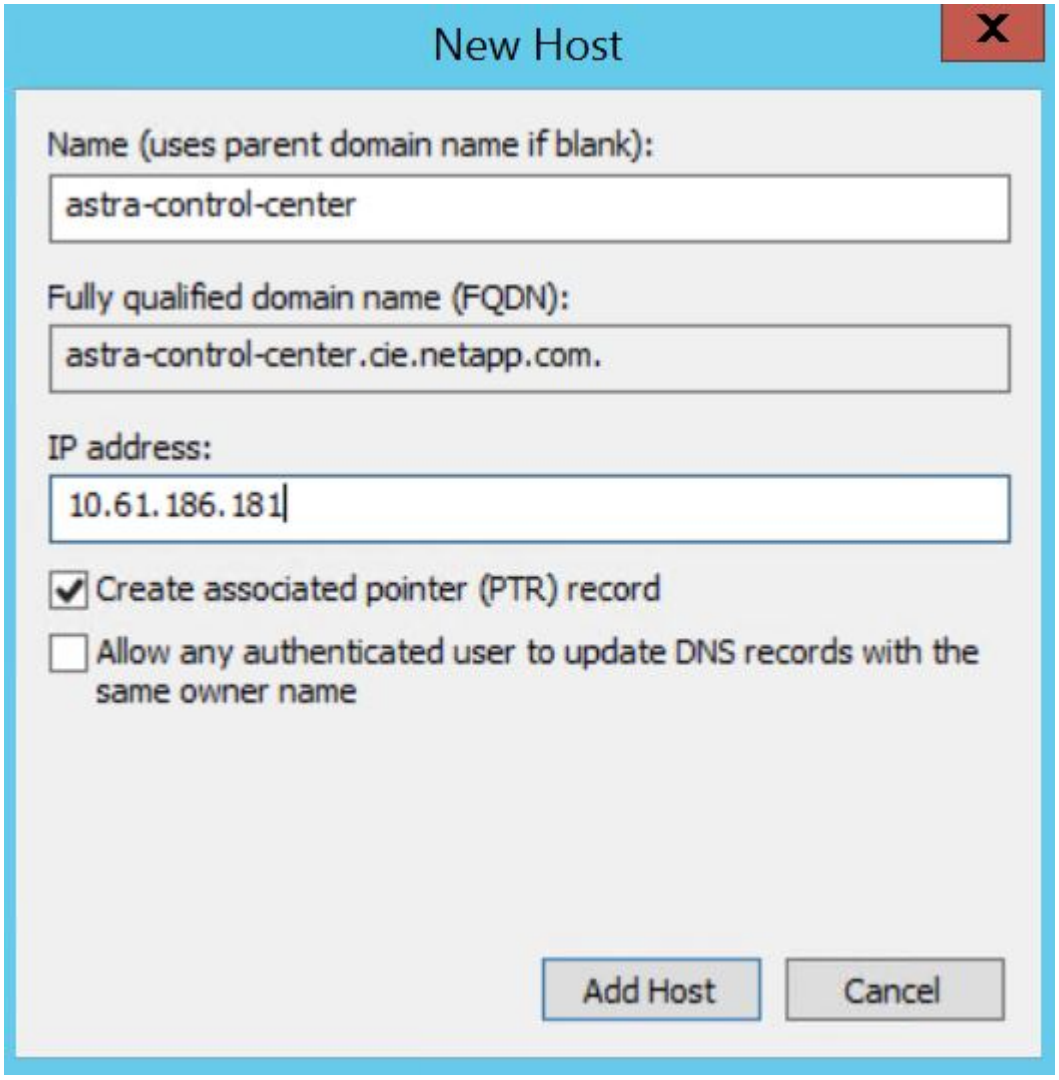
```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc
NAME    UUID
astra   345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```

> Dans cet exemple, le mot de passe est `ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f`.

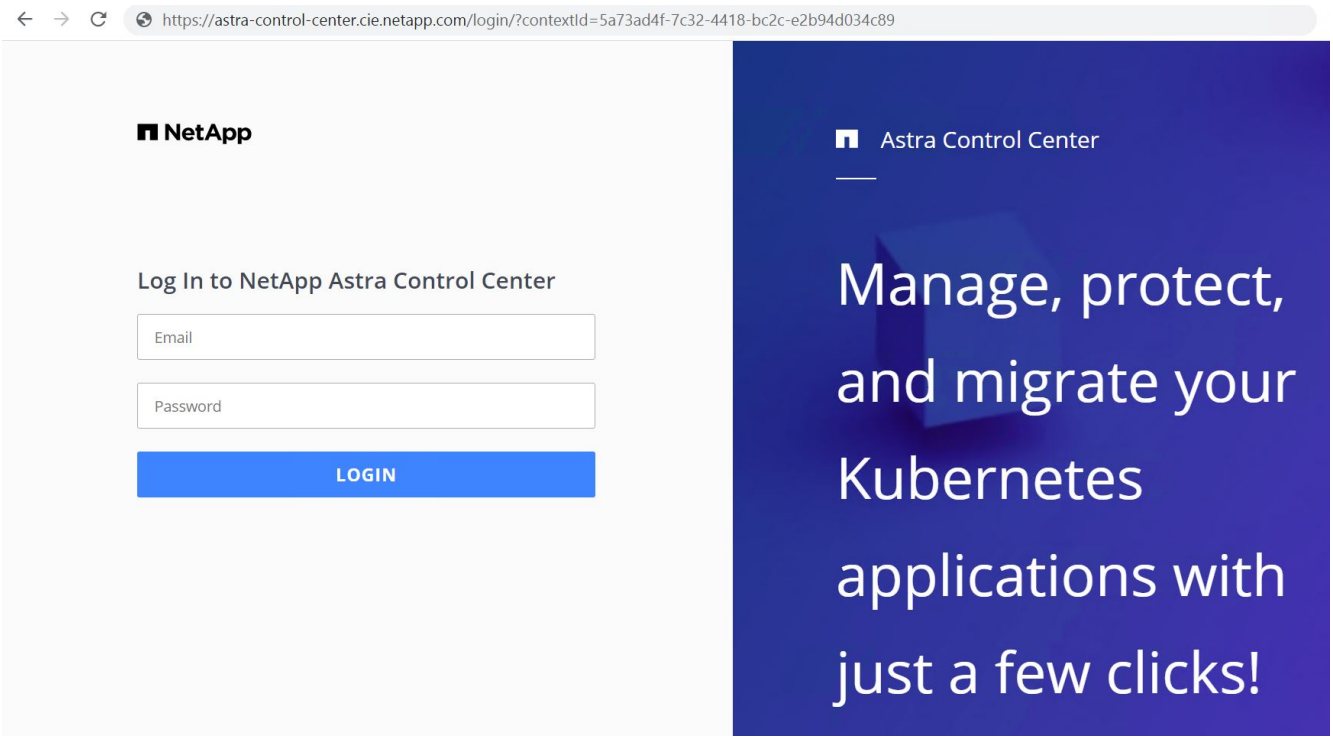
4. Procurez-vous l'IP d'équilibrage de charge du service traefik.

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

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

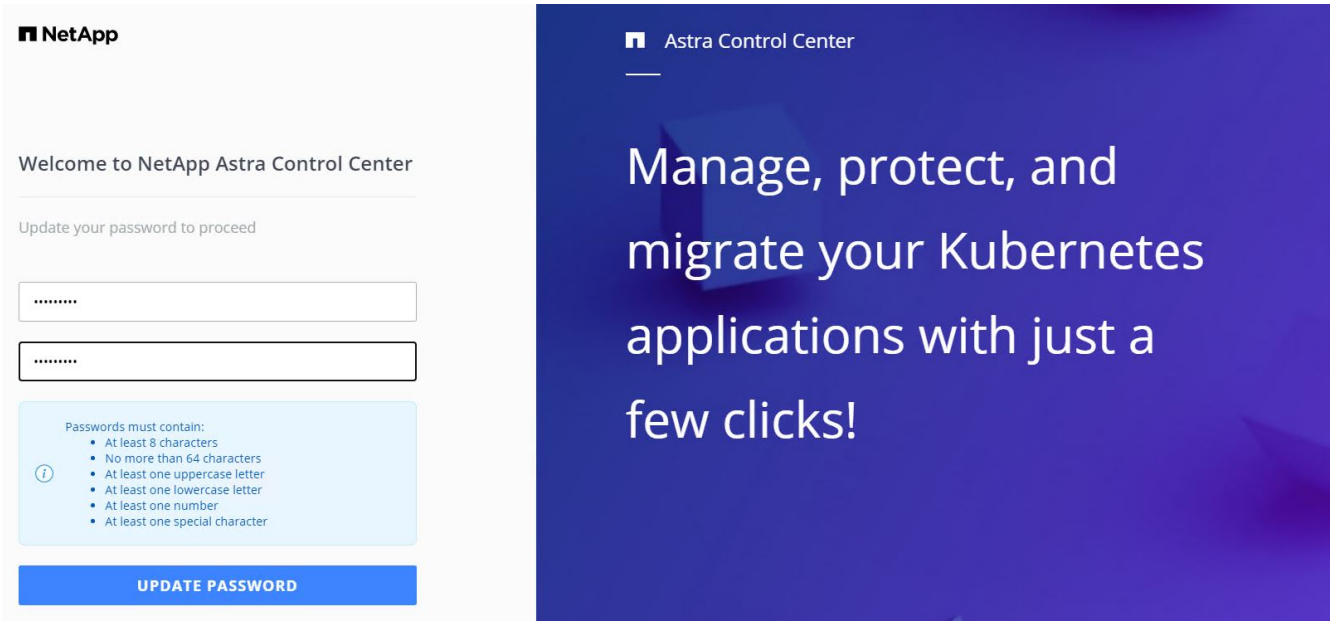
5. Ajoutez une entrée dans le serveur DNS pointant le FQDN fourni dans le fichier CRD Astra Control Center vers le `EXTERNAL-IP` du service de trafik.



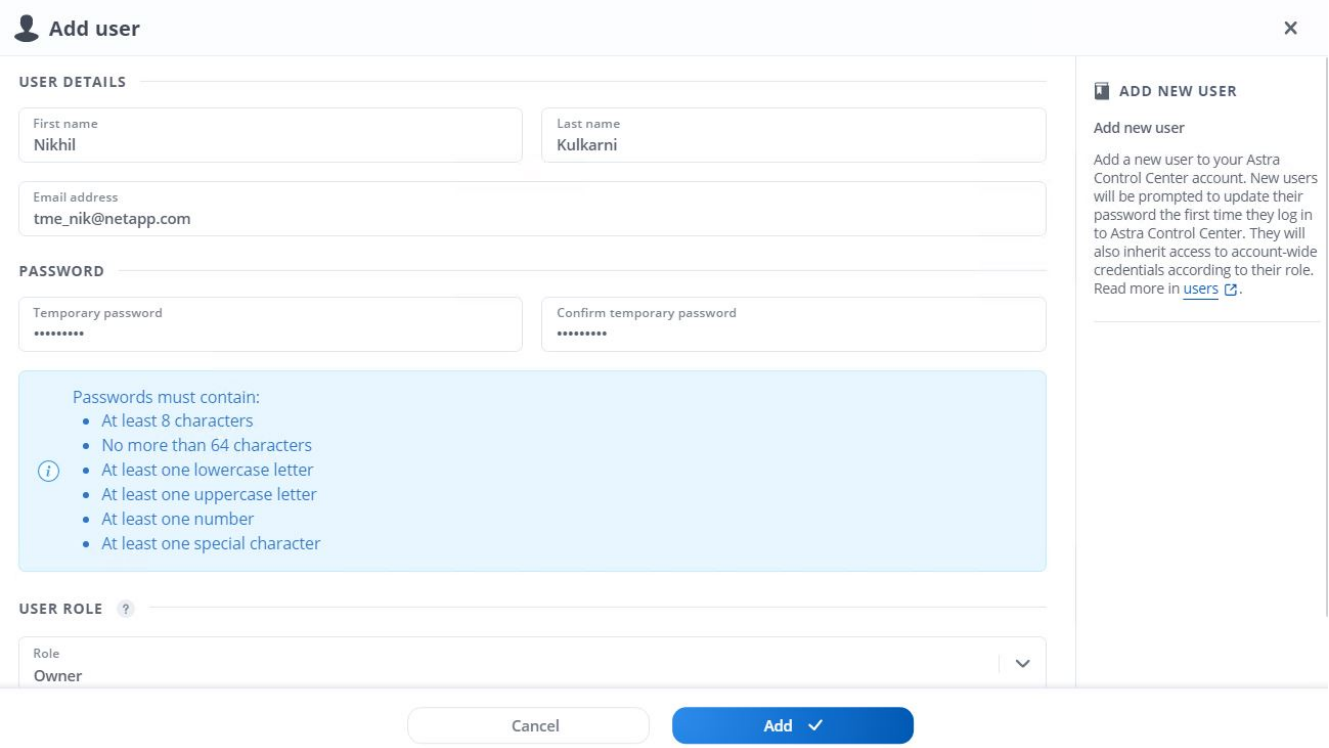
6. Connectez-vous à l'interface graphique d'Astra Control Center en parcourant son FQDN.



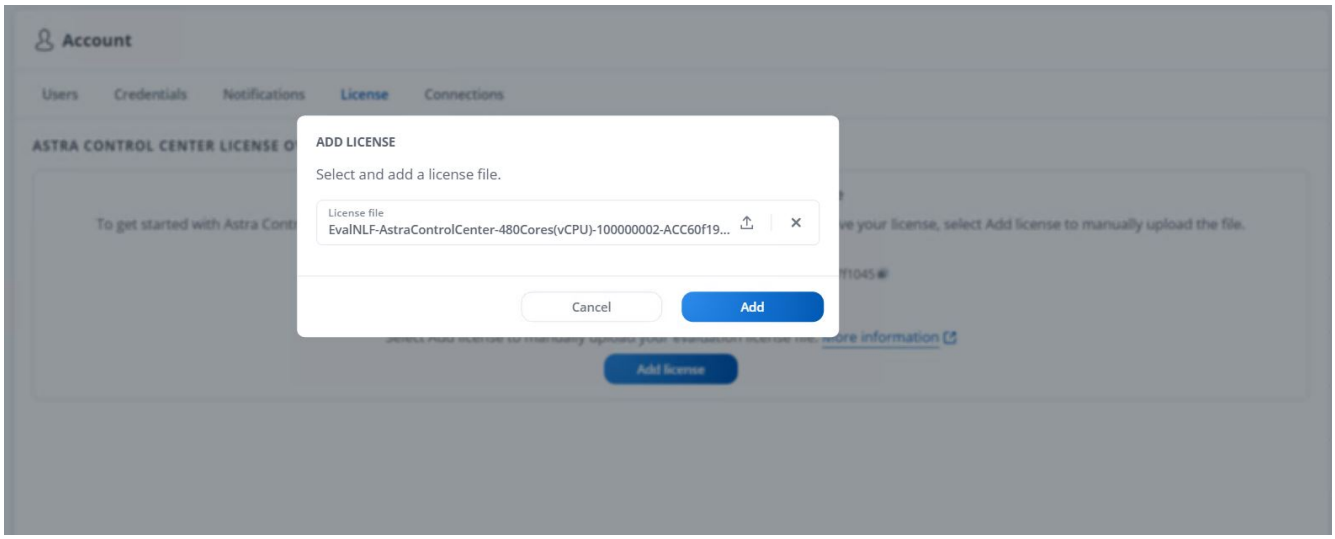
7. Lorsque vous vous connectez à l'interface graphique d'Astra Control Center pour la première fois à l'aide de l'adresse e-mail d'administration fournie dans CRD, vous devez modifier le mot de passe.



8. Si vous souhaitez ajouter un utilisateur au Centre de contrôle Astra, accédez à compte > utilisateurs, cliquez sur Ajouter, entrez les détails de l'utilisateur et cliquez sur Ajouter.



9. Astra Control Center requiert une licence pour toutes ses fonctionnalités. Pour ajouter une licence, accédez à compte > Licence, cliquez sur Ajouter une licence et téléchargez le fichier de licence.



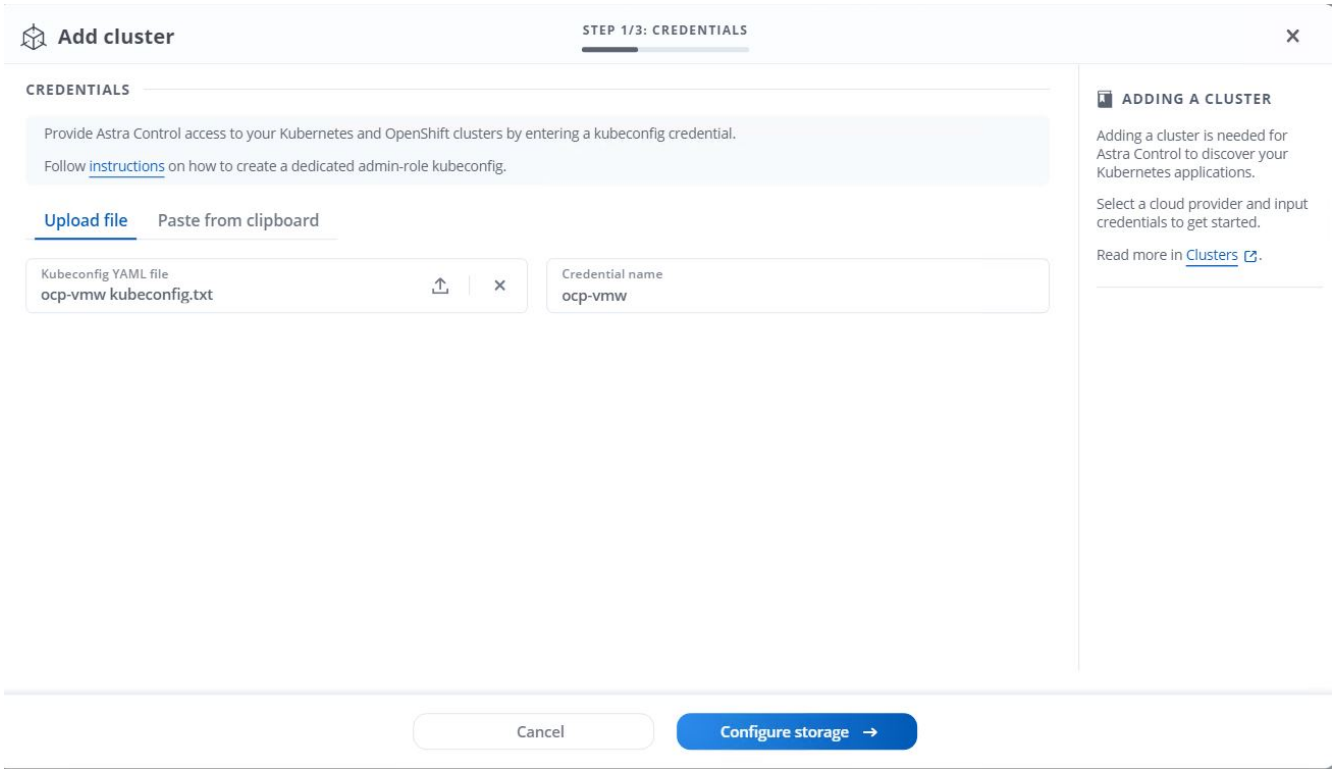
En cas de problème avec l'installation ou la configuration de NetApp Astra Control Center, la base de connaissances des problèmes connus est disponible "ici".

Enregistrez vos clusters Red Hat OpenShift avec Astra Control Center

Pour permettre à Astra Control Center de gérer vos charges de travail, vous devez d'abord enregistrer votre cluster Red Hat OpenShift.

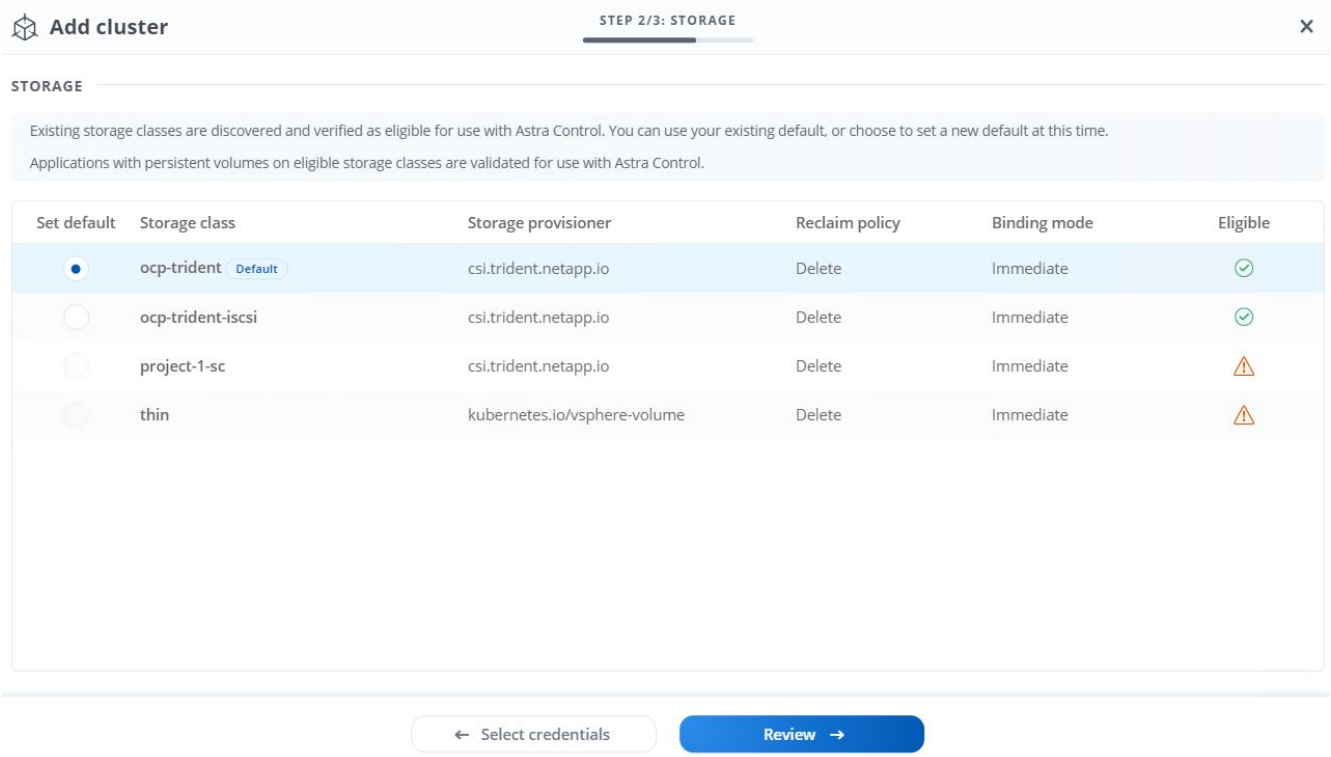
Enregistrez les clusters Red Hat OpenShift

1. La première étape consiste à ajouter les clusters OpenShift au Centre de contrôle Astra et à les gérer. Accédez aux clusters et cliquez sur Ajouter un cluster, téléchargez le fichier kubeconfig pour le cluster OpenShift, puis cliquez sur Sélectionner un stockage.

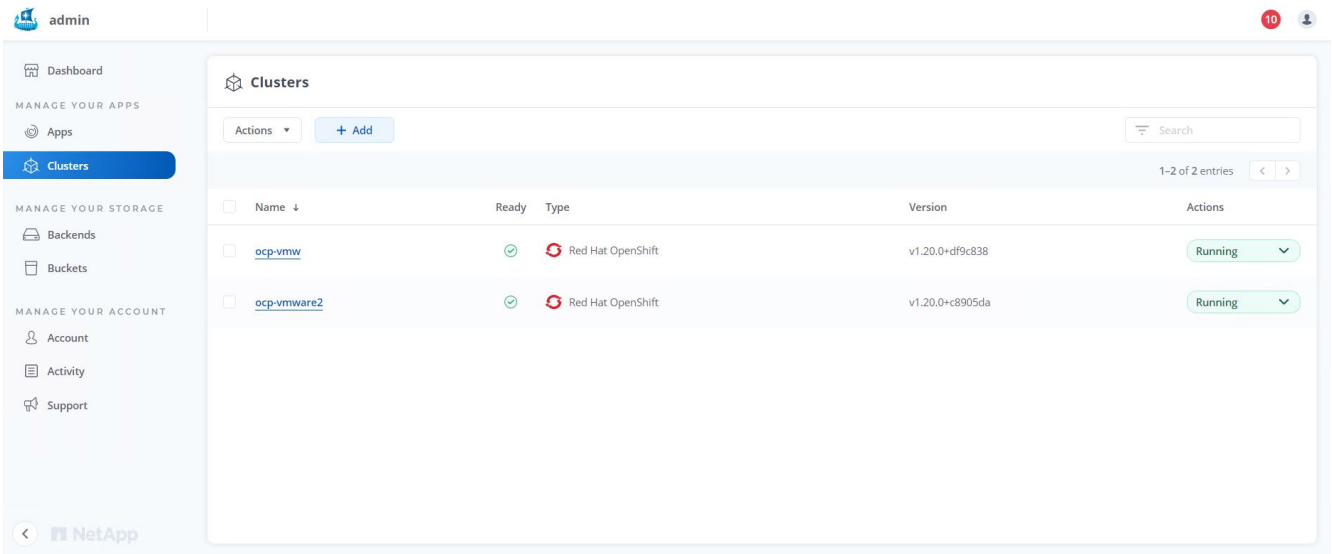


> Le fichier kubeconfig peut être généré pour s'authentifier avec un nom d'utilisateur et un mot de passe ou un jeton. Les jetons expirent après un délai limité et peuvent laisser le cluster enregistré inaccessible. NetApp recommande d'utiliser un fichier kubeconfig avec un nom d'utilisateur et un mot de passe pour enregistrer vos clusters OpenShift sur Astra Control Center.

2. Astra Control Center détecte les classes de stockage admissibles. Maintenant, sélectionnez la façon dont storageclass provisionne les volumes en utilisant Trident sauvegardé par un SVM sur NetApp ONTAP et Click Review. Dans le volet suivant, vérifiez les détails et cliquez sur Ajouter un cluster.

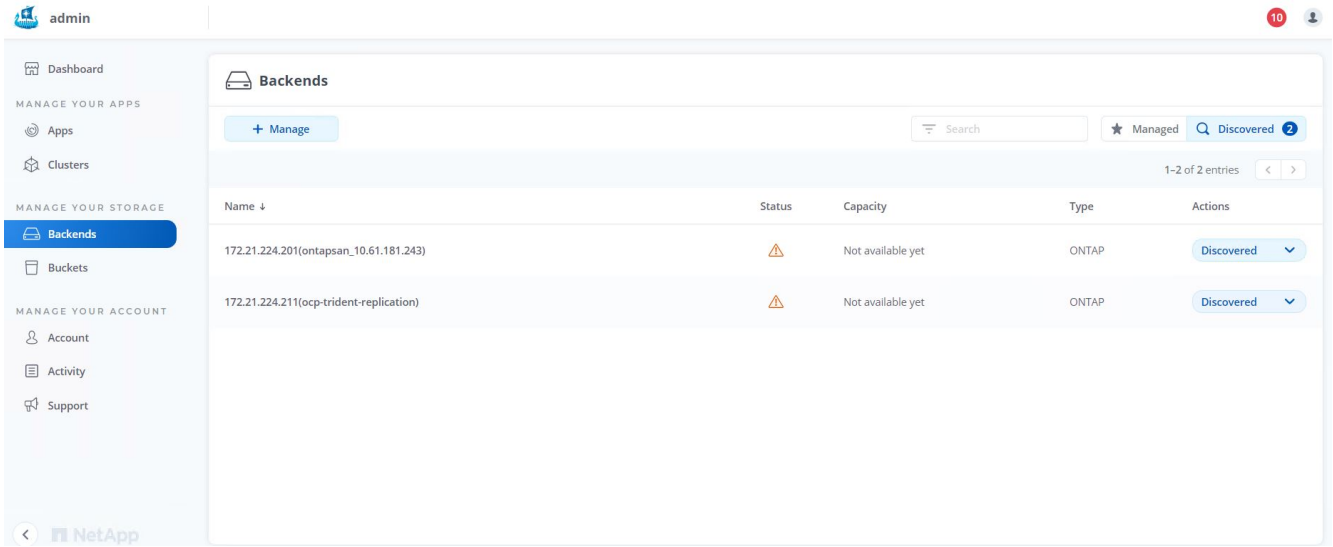


3. Enregistrez les deux clusters OpenShift comme décrit à l'étape 1. Lorsqu'elles sont ajoutées, les clusters passent à l'état découverte pendant qu'Astra Control Center les inspecte et installe les agents nécessaires. L'état du cluster est modifié en cours d'exécution après son enregistrement.

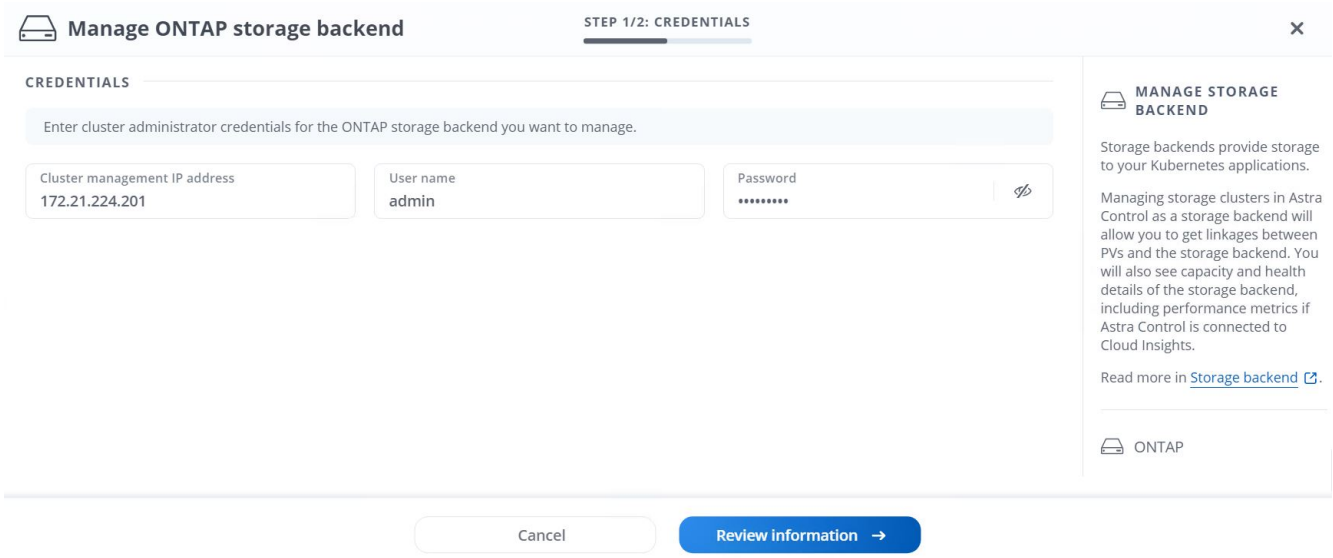


> Tous les clusters Red Hat OpenShift devant être gérés par Astra Control Center doivent avoir accès au registre d'images utilisé pour son installation lorsque les agents installés sur les clusters gérés extraient les images de ce registre.

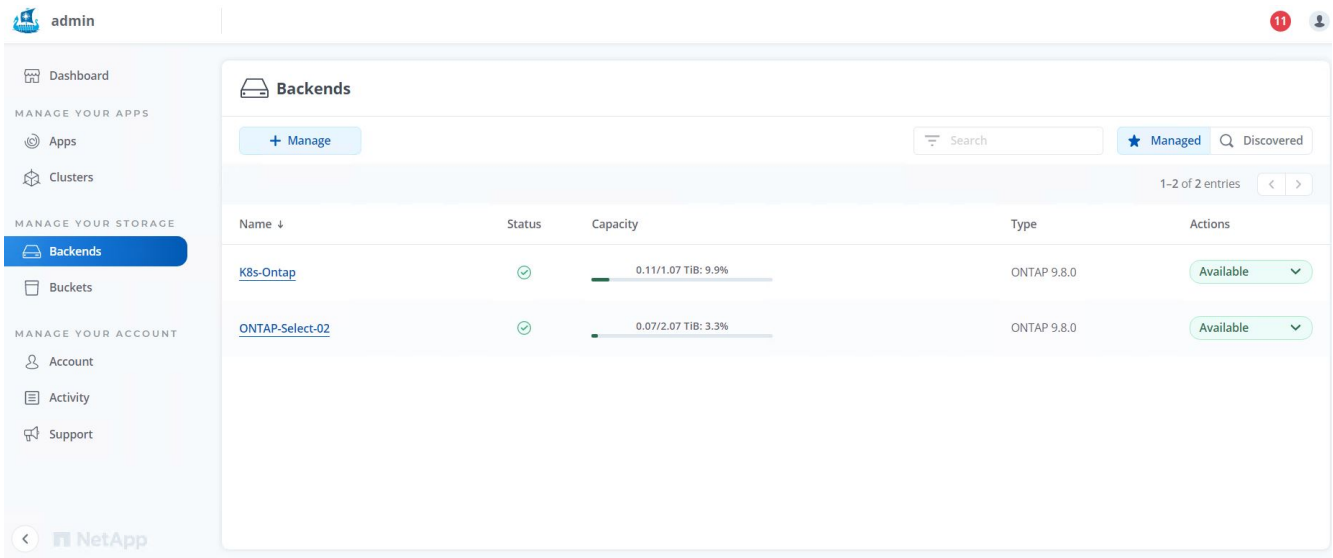
4. Importation de clusters ONTAP comme ressources de stockage à gérer en tant que système back-end par Astra Control Center. Lorsque des clusters OpenShift sont ajoutés à Astra et qu'un storageclass est configuré, il détecte et inspecte automatiquement le cluster ONTAP qui soutient le storageclass, mais ne l'importe pas dans le Control Center Astra à gérer.



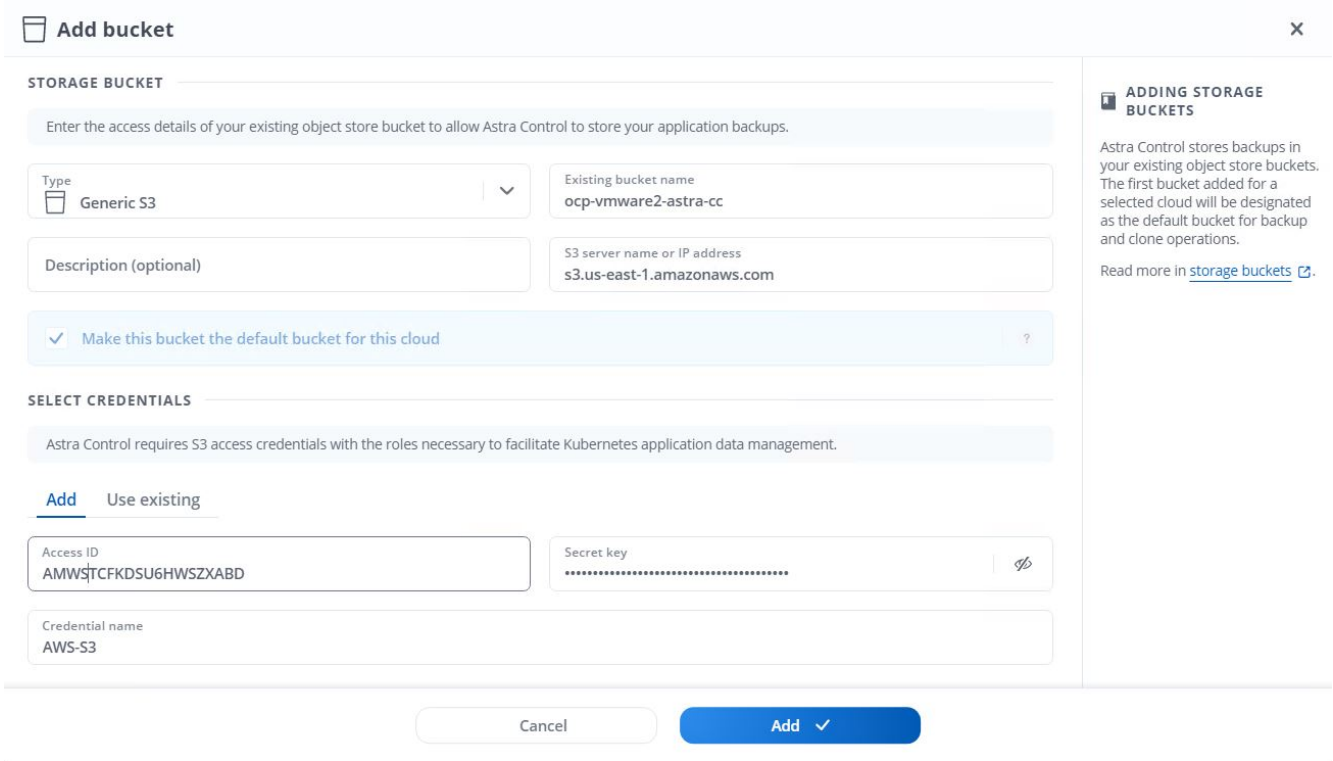
5. Pour importer les clusters ONTAP, accédez aux systèmes back-end, cliquez sur la liste déroulante et sélectionnez gérer en regard du cluster ONTAP à gérer. Entrez les informations d'identification du cluster ONTAP, cliquez sur vérifier les informations, puis sur Importer le stockage back-end.



6. Une fois que le système back-end est ajouté, le statut devient disponible. Ces systèmes back-end disposent désormais d'informations sur les volumes persistants dans le cluster OpenShift et sur les volumes correspondants sur le système ONTAP.



7. Pour la sauvegarde et la restauration entre les clusters OpenShift avec Astra Control Center, vous devez provisionner un compartiment de stockage objet qui prend en charge le protocole S3. Les options ONTAP S3, StorageGRID et AWS S3 sont actuellement prises en charge. Pour les besoins de cette installation, nous allons configurer un compartiment AWS S3. Accédez à godets, cliquez sur Ajouter un compartiment et sélectionnez Generic S3. Entrez les informations d'identification du compartiment S3 et des informations d'identification pour y accéder, cochez la case « définir ce compartiment par défaut pour le cloud », puis cliquez sur Ajouter.

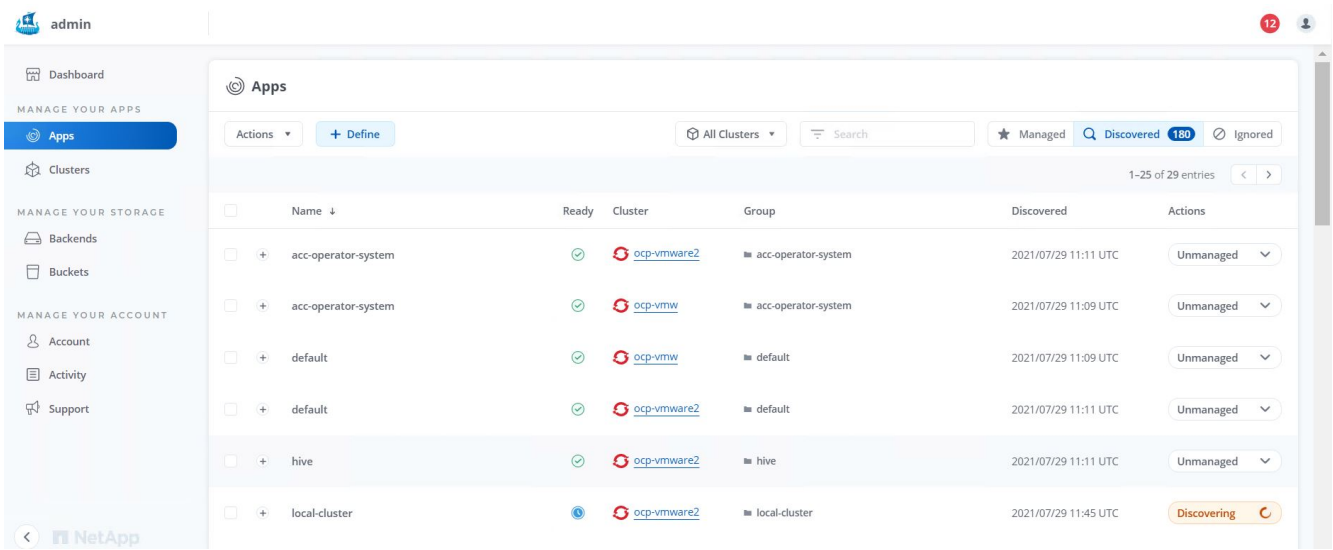


Choisissez les applications à protéger

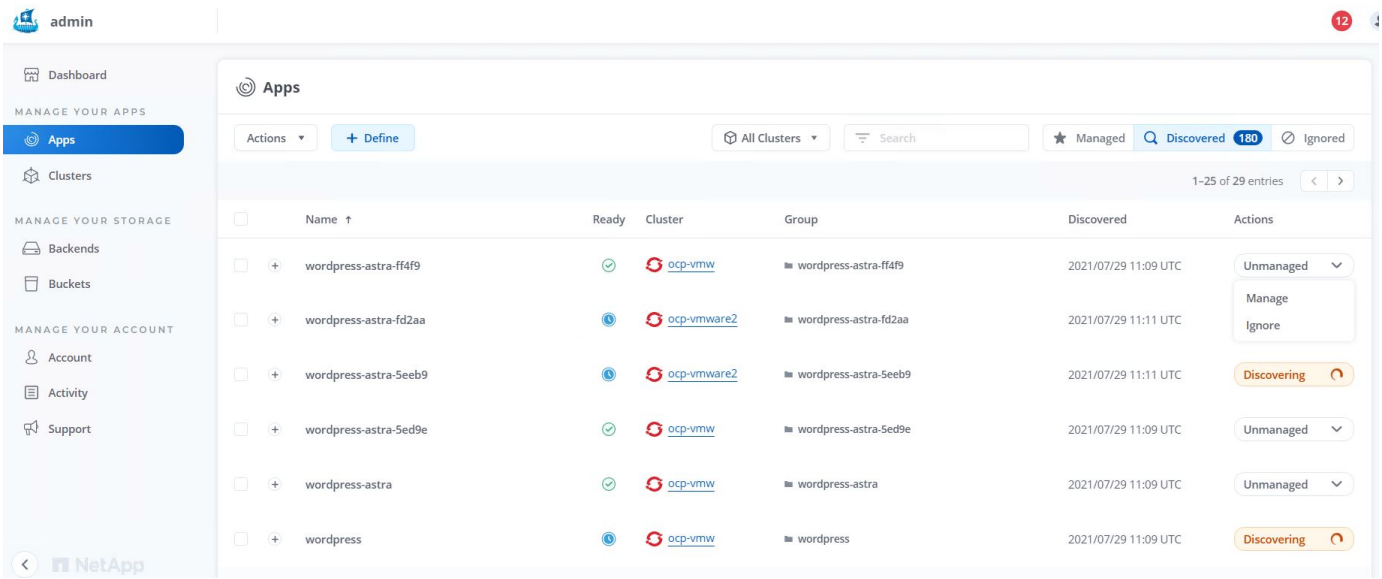
Une fois vos clusters Red Hat OpenShift enregistrés, vous pouvez détecter les applications déployées et les gérer via Astra Control Center.

Gestion des applications

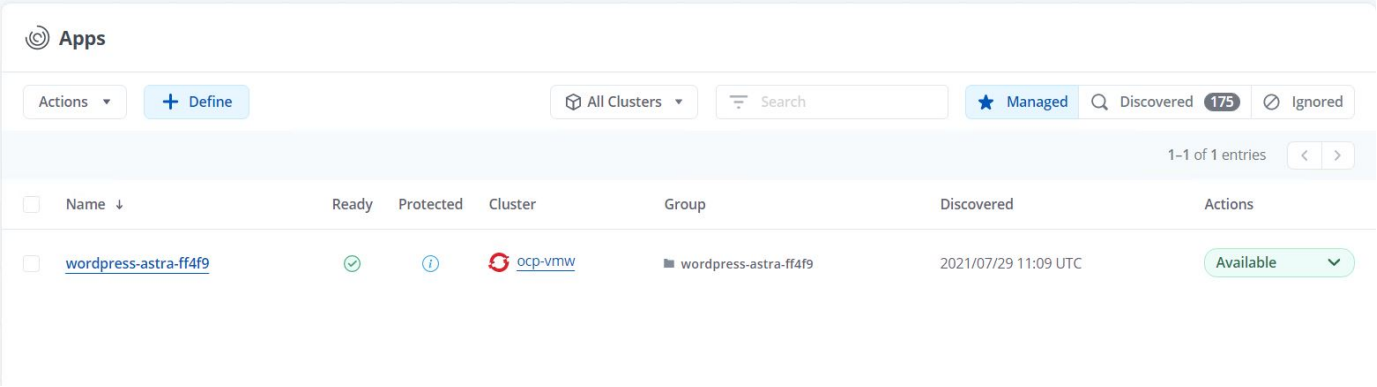
1. Une fois les clusters OpenShift et les systèmes back-end ONTAP enregistrés auprès de l'Astra Control Center, le centre de contrôle démarre automatiquement la détection des applications dans tous les namespaces qui utilisent le storageclass configuré avec le back-end ONTAP spécifié.



2. Accédez à applications > découverte et cliquez sur le menu déroulant en regard de l'application que vous souhaitez gérer à l'aide d'Astra. Cliquez ensuite sur gérer.



1. L'application passe à l'état disponible et peut être affichée sous l'onglet géré de la section applications.



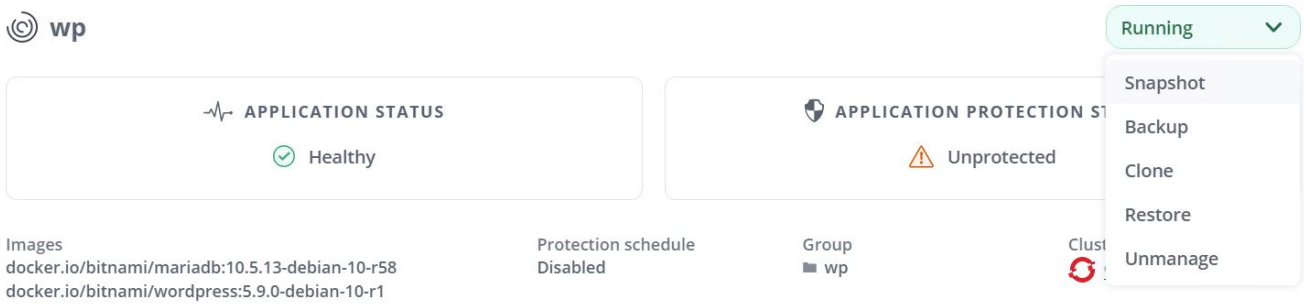
Protégez vos applications

Une fois les charges de travail applicatives gérées par Astra Control Center, vous pouvez configurer les paramètres de protection pour ces charges de travail.

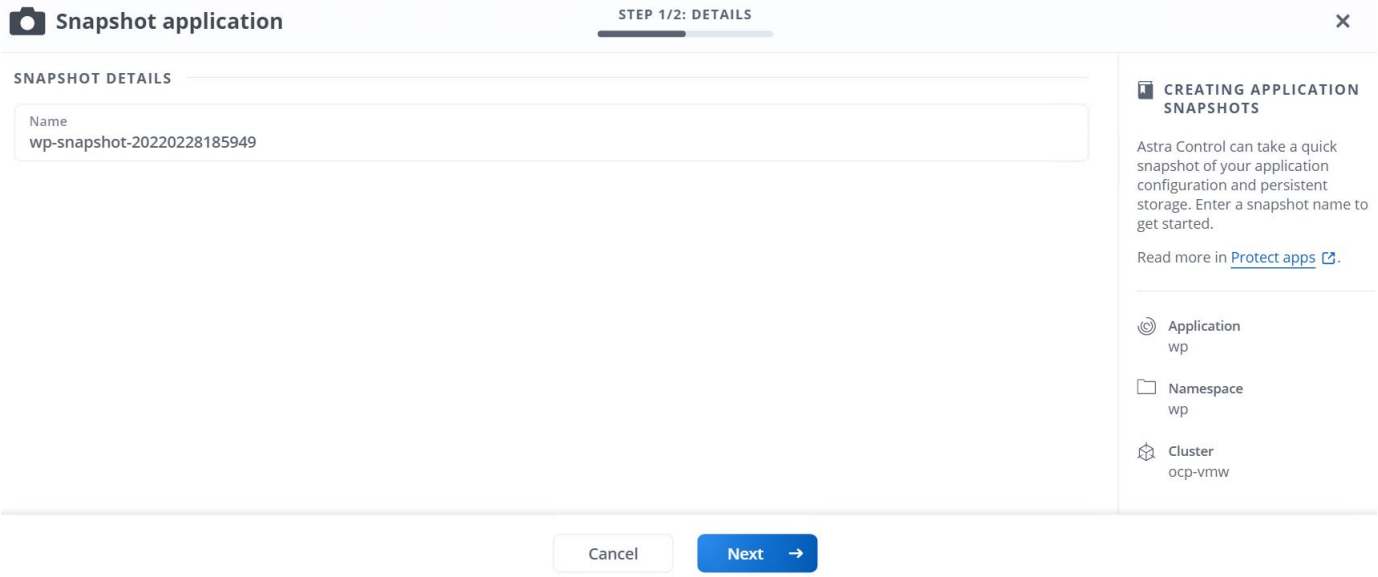
Création d'un instantané d'application

Un snapshot d'une application crée une copie Snapshot ONTAP qui peut être utilisée pour restaurer ou cloner l'application à un point dans le temps spécifique en fonction de cette copie Snapshot.

1. Pour prendre un instantané de l'application, accédez à l'onglet applications > gestion, puis cliquez sur l'application dont vous souhaitez effectuer une copie Snapshot. Cliquez sur le menu déroulant en regard du nom de l'application et cliquez sur instantané.



2. Entrez les détails du snapshot, cliquez sur Suivant, puis sur instantané. La création du Snapshot prend environ une minute et son état est disponible une fois celui-ci créé.



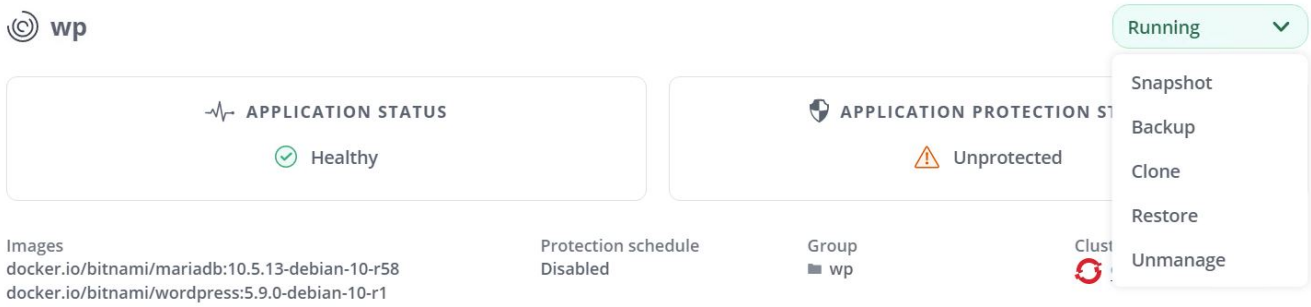
Création d'une sauvegarde d'application

Une sauvegarde d'une application capture l'état actif de l'application et la configuration des ressources informatiques, les analyse en fichiers et les stocke dans un compartiment de stockage objet distant.

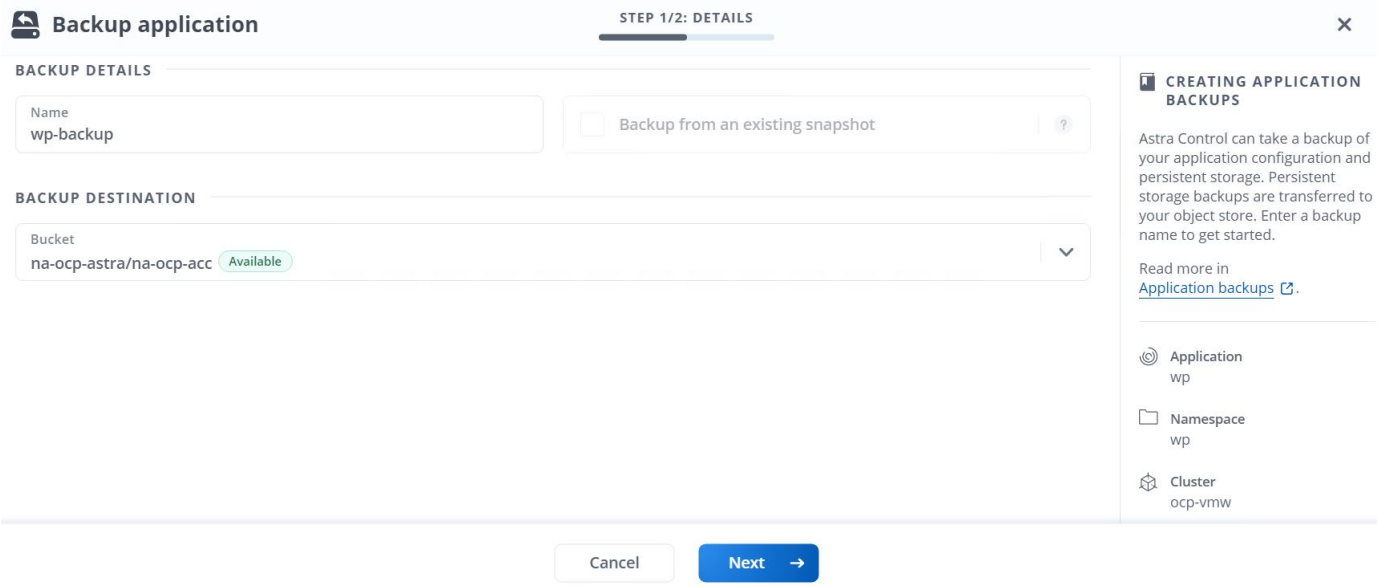
Pour la sauvegarde et la restauration des applications gérées dans le Centre de contrôle Astra, vous devez configurer les paramètres de superutilisateur des systèmes ONTAP de secours au préalable. Pour ce faire, entrez les commandes suivantes.

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

1. Pour créer une sauvegarde de l'application gérée dans Astra Control Center, accédez à l'onglet applications > géré et cliquez sur l'application dont vous souhaitez effectuer une sauvegarde. Cliquez sur le menu déroulant en regard du nom de l'application et cliquez sur Sauvegarder.



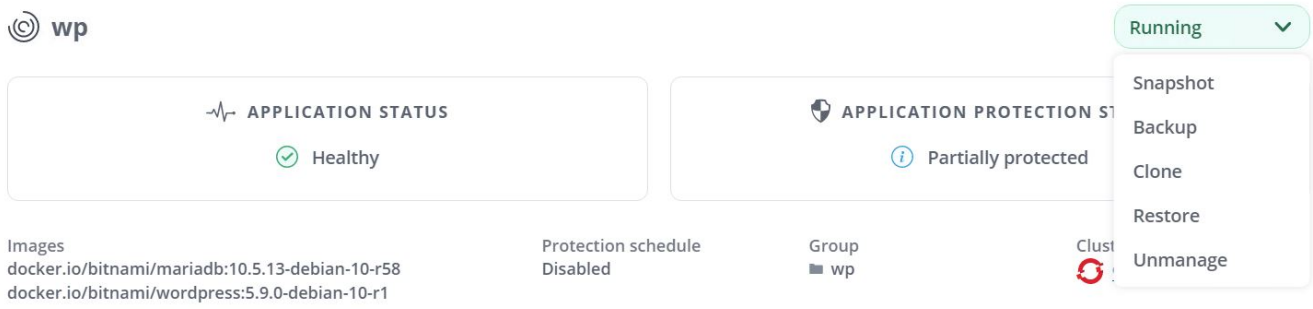
2. Entrez les détails de la sauvegarde, sélectionnez le compartiment de stockage objet pour contenir les fichiers de sauvegarde, cliquez sur Next (Suivant) et, après avoir vérifié les détails, cliquez sur Backup (Sauvegarder). Selon la taille de l'application et des données, la sauvegarde peut prendre plusieurs minutes, et l'état de la sauvegarde est disponible une fois la sauvegarde terminée.



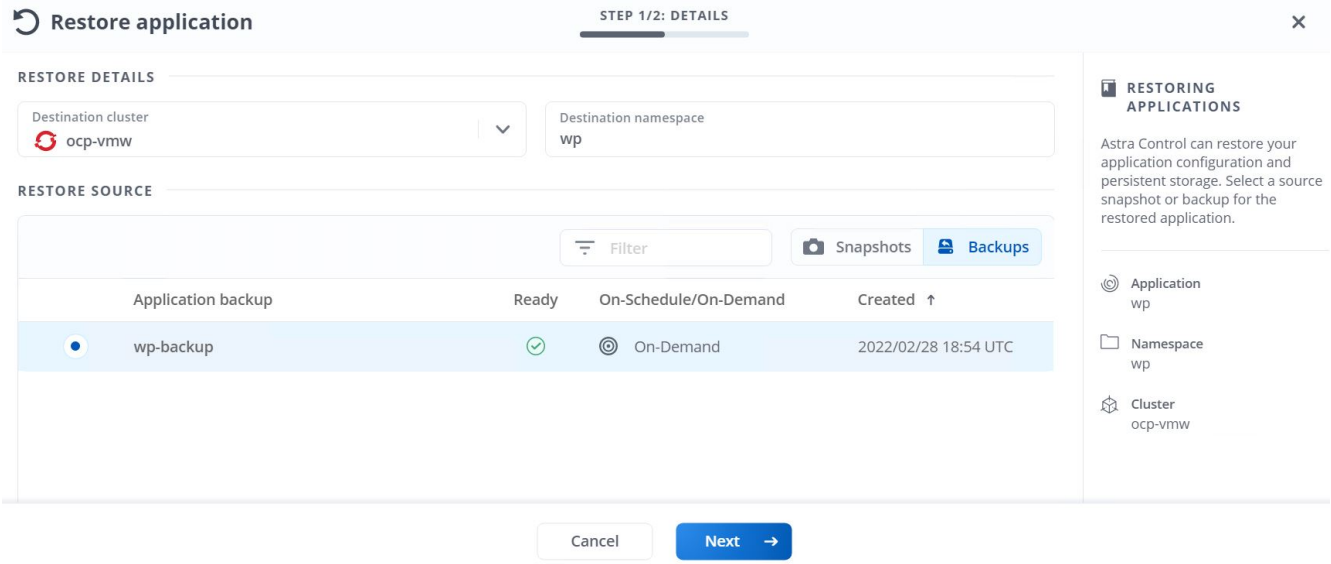
Restauration d’une application

En appuyant sur un bouton, vous pouvez restaurer une application sur l’espace de noms d’origine dans le même cluster ou sur un cluster distant afin d’assurer la protection des applications et la reprise sur incident.

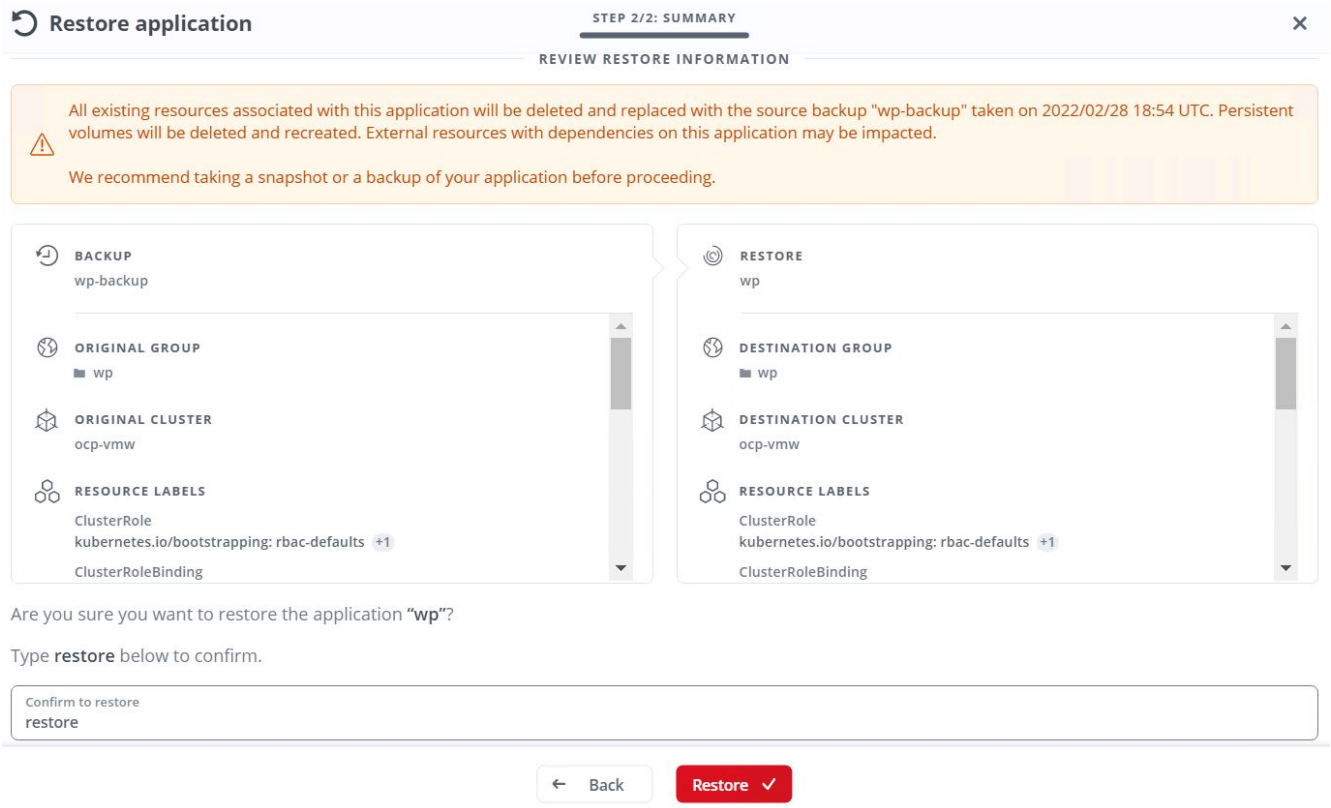
1. Pour restaurer une application, accédez à applications > onglet géré et cliquez sur l’application en question. Cliquez sur le menu déroulant en regard du nom de l’application et cliquez sur `Restore`.



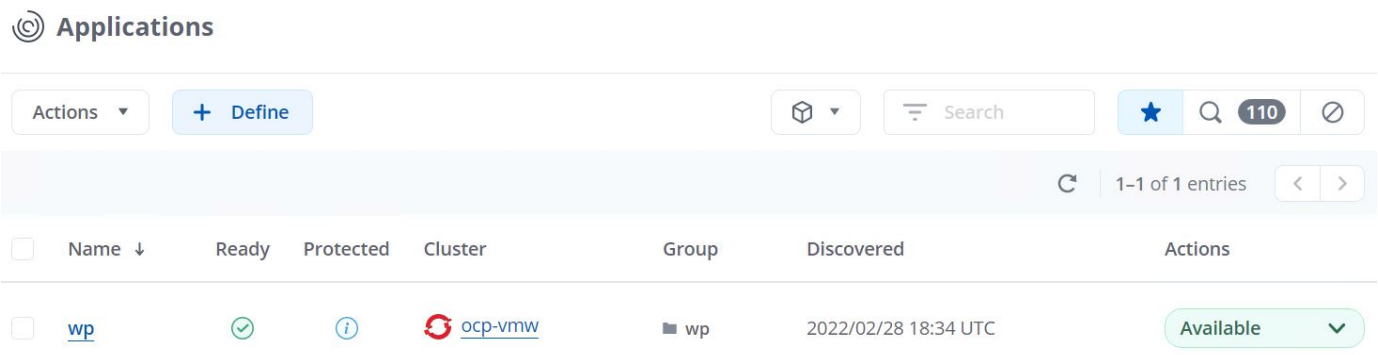
2. Entrez le nom de l’espace de noms de restauration, sélectionnez le cluster vers lequel vous souhaitez le restaurer et choisissez si vous souhaitez le restaurer à partir d’un snapshot existant ou à partir d’une sauvegarde de l’application. Cliquez sur Suivant.



3. Dans le volet de révision, entrez `restore` Puis cliquez sur Restaurer une fois que vous avez examiné les détails.



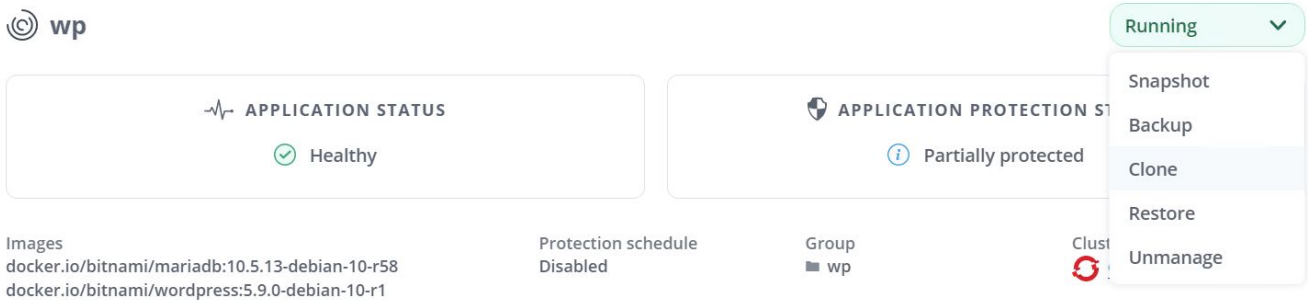
4. La nouvelle application passe à l'état de restauration tandis qu'Astra Control Center restaure l'application sur le cluster sélectionné. Une fois que toutes les ressources de l'application sont installées et détectées par Astra, l'application passe à l'état disponible.



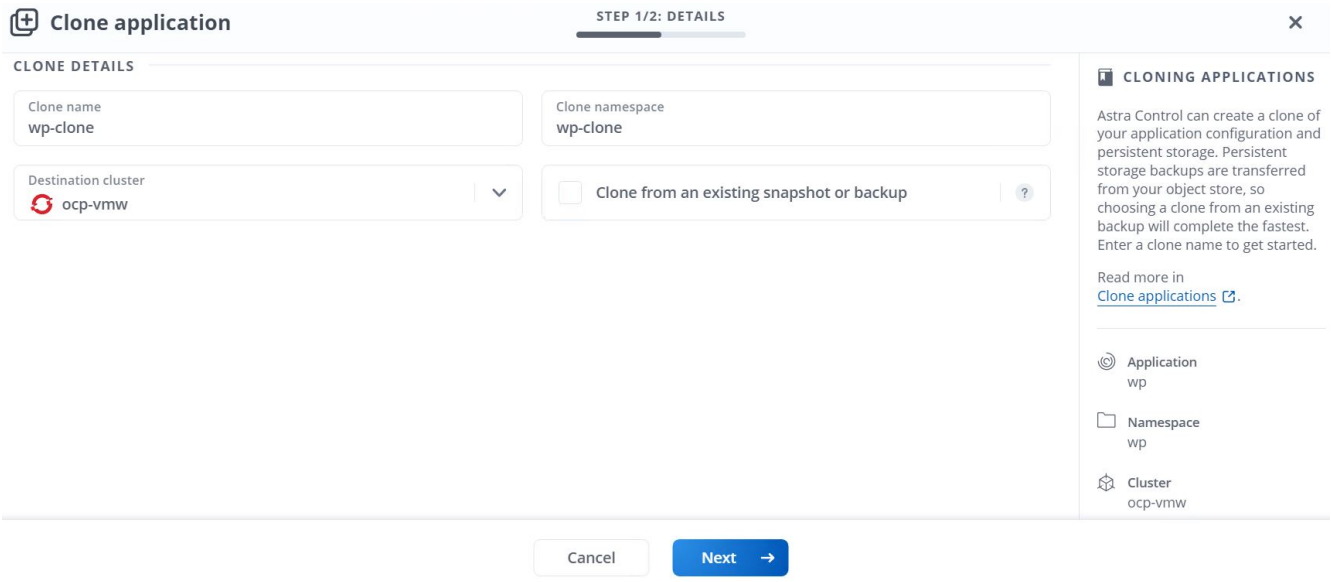
Clonage d’une application

Vous pouvez cloner une application sur le cluster d’origine ou sur un cluster distant à des fins de développement/test ou de protection des applications et de reprise sur incident. Le clonage d’une application au sein d’un même cluster sur le même système back-end utilise la technologie NetApp FlexClone, qui clonez instantanément les demandes de volume persistant et économise de l’espace de stockage.

1. Pour cloner une application, accédez à l’onglet applications > gestion et cliquez sur l’application en question. Cliquez sur le menu déroulant en regard du nom de l’application, puis cliquez sur Cloner.



2. Entrez les détails du nouveau namespace, sélectionnez le cluster vers lequel vous souhaitez le cloner à partir d’un snapshot existant ou d’une sauvegarde ou de l’état actuel de l’application. Cliquez ensuite sur Suivant et sur Cloner dans le volet d’évaluation une fois que vous avez passé en revue les détails.



3. La nouvelle application passe à l'état découverte tandis que Astra Control Center crée l'application sur le cluster sélectionné. Une fois que toutes les ressources de l'application sont installées et détectées par Astra, l'application passe à l'état disponible.