Panoramica di NetApp Astra Control Center

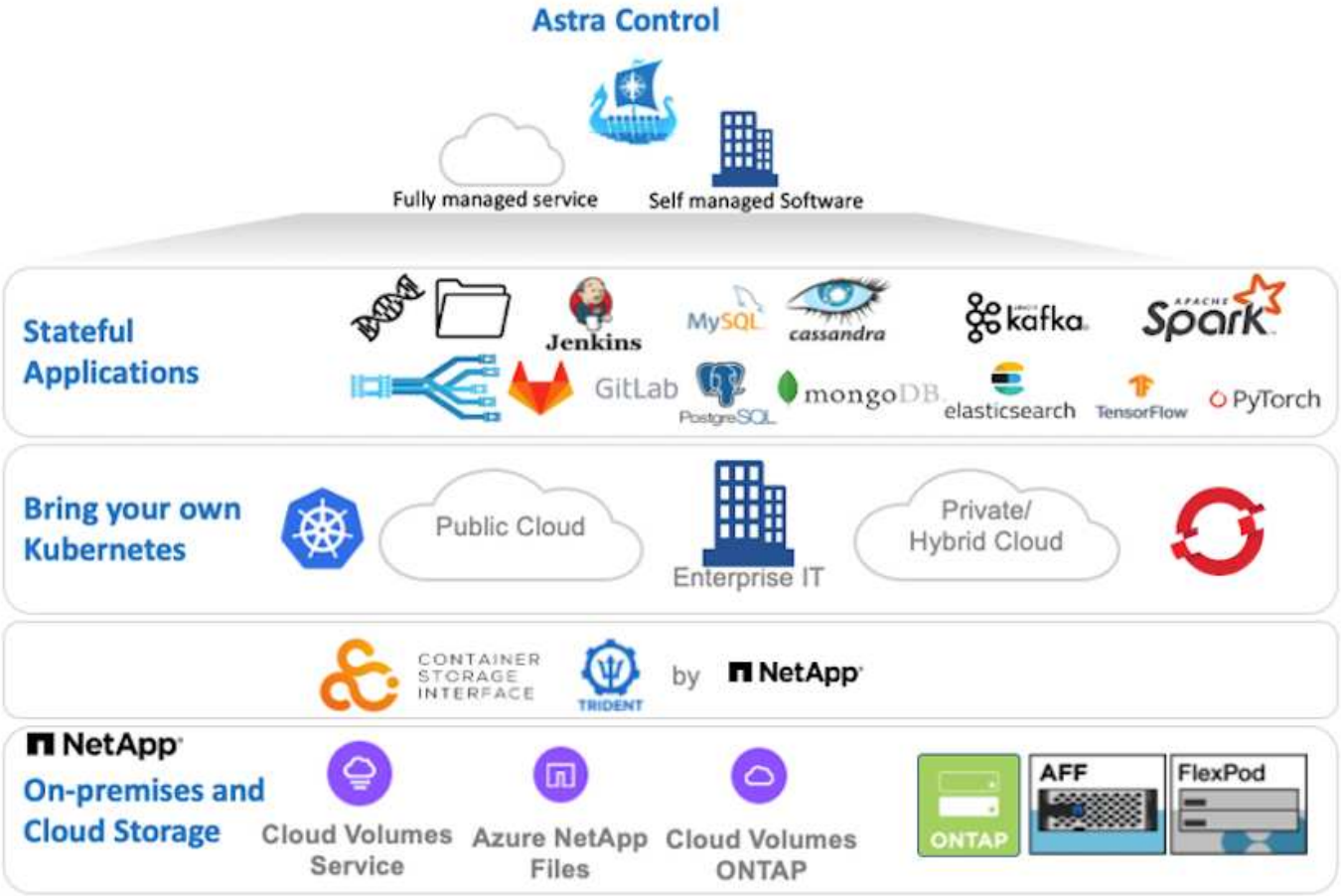
NetApp Solutions

NetApp
April 26, 2024

Sommario

Panoramica di NetApp Astra Control Center

NetApp Astra Control Center offre un'ampia gamma di servizi di gestione dei dati basati su applicazioni e storage per carichi di lavoro Kubernetes stateful implementati in un ambiente on-premise e basati sulla tecnologia di protezione dei dati di NetApp.



È possibile installare NetApp Astra Control Center su un cluster Red Hat OpenShift che dispone di Astra Trident Storage orchestrator implementato e configurato con classi di storage e backend di storage per i sistemi storage NetApp ONTAP.

Per l'installazione e la configurazione di Astra Trident per il supporto di Astra Control Center, vedere "questo documento qui".

In un ambiente connesso al cloud, il centro di controllo Astra utilizza Cloud Insights per fornire monitoraggio avanzato e telemetria. In assenza di una connessione Cloud Insights, sono disponibili funzioni limitate di monitoraggio e telemetria (7 giorni di metriche) ed esportate negli strumenti di monitoraggio nativi di Kubernetes (Prometheus e Grafana) attraverso endpoint di metriche aperte.

Il centro di controllo Astra è completamente integrato nell'ecosistema NetApp AutoSupport e Active IQ per fornire supporto agli utenti, fornire assistenza per la risoluzione dei problemi e visualizzare le statistiche di utilizzo.

Oltre alla versione a pagamento di Astra Control Center, è disponibile una licenza di valutazione di 90 giorni. La versione di valutazione è supportata tramite e-mail e community (canale slack). I clienti hanno accesso a questi e ad altri articoli della Knowledge base e alla documentazione disponibile nella dashboard di supporto dei prodotti.

Per iniziare a utilizzare NetApp Astra Control Center, visita il "Sito web Astra".

Prerequisiti per l'installazione di Astra Control Center

1. Uno o più cluster Red Hat OpenShift. Le versioni 4.6 EUS e 4.7 sono attualmente supportate.
2. Astra Trident deve essere già installato e configurato su ogni cluster Red Hat OpenShift.
3. Uno o più sistemi storage NetApp ONTAP con ONTAP 9.5 o superiore.

   Per ogni installazione di OpenShift in un sito è consigliabile disporre di una SVM dedicata per lo storage persistente. Le implementazioni multi-sito richiedono sistemi storage aggiuntivi.

4. È necessario configurare un backend di storage Trident su ciascun cluster OpenShift con una SVM supportata da un cluster ONTAP.
5. StorageClass predefinita configurata su ciascun cluster OpenShift con Astra Trident come storage provisioning.
6. È necessario installare e configurare un bilanciamento del carico su ciascun cluster OpenShift per il bilanciamento del carico e l'esposizione dei servizi OpenShift.

   Vedere il link "qui" per informazioni sui bilanciatori di carico validati per questo scopo.

7. È necessario configurare un registro di immagini privato per ospitare le immagini di NetApp Astra Control Center.

   Vedere il link "qui" Per installare e configurare un registro privato OpenShift a tale scopo.

8. È necessario disporre dell'accesso Cluster Admin al cluster Red Hat OpenShift.
9. È necessario disporre dell'accesso come amministratore ai cluster NetApp ONTAP.
10. Una workstation di amministrazione con i tool docker o podman, tridentctl e oc o kubectl installati e aggiunti al percorso dei dollari.

    Le installazioni di Docker devono avere una versione di Docker superiore alla 20.10 e le installazioni di Podman devono avere una versione di podman superiore alla 3.0.

Installare Astra Control Center

Utilizzo di OperatorHub

1. Accedere al NetApp Support Site e scaricare l'ultima versione di NetApp Astra Control Center. Per farlo, è necessaria una licenza allegata al tuo account NetApp. Dopo aver scaricato il tarball, trasferirlo sulla workstation di amministrazione.

   > Per iniziare a utilizzare una licenza di prova per Astra Control, visitare il sito "Sito di registrazione Astra".

2. Disimballare il tar ball e modificare la directory di lavoro nella cartella risultante.

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

3. Prima di iniziare l'installazione, trasferire le immagini di Astra Control Center in un registro di immagini. Puoi scegliere di farlo con Docker o Podman; in questo passaggio vengono fornite le istruzioni per entrambi.

Podman

a. Esportare ‘reFQDN del Registro di sistema con il nome dell’organizzazione/namespace/progetto come variabile di ambiente 'gistry'.

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

b. Accedere al Registro di sistema.

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

> Se si utilizza `kubeadmin` utente per accedere al registro privato, quindi utilizzare il token invece della password - `podman login -u ocp-user -p token --tls-verify=false astra-registry.apps.ocp-vmw.cie.netapp.com`.

> In alternativa, è possibile creare un account di servizio, assegnare un ruolo di editor del Registro di sistema e/o di visualizzatore del Registro di sistema (a seconda che si richieda l’accesso push/pull) e accedere al Registro di sistema utilizzando il token dell’account di servizio.

c. Creare un file script della shell e incollarne il contenuto seguente.

```
[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
```

> Se si utilizzano certificati non attendibili per il Registro di sistema, modificare lo script della shell e utilizzare `--tls-verify=false` per il comando podman push `podman push $REGISTRY/$(echo $astraImage | sed 's/[\/]\+\///') --tls-verify=false`.

d. Rendere il file eseguibile.

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

e. Eseguire lo script della shell.

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

Docker

a. Esportare ‘reFQDN del Registro di sistema con il nome dell’organizzazione/namespace/progetto come variabile di ambiente 'gistry'.

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

b. Accedere al Registro di sistema.

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

> Se si utilizza `kubeadmin` utente per accedere al registro privato, quindi utilizzare il token invece della password - `docker login -u ocp-user -p token astra-registry.apps.ocp-vmw.cie.netapp.com`.

> In alternativa, è possibile creare un account di servizio, assegnare un ruolo di editor del Registro di sistema e/o di visualizzatore del Registro di sistema (a seconda che si richieda l’accesso push/pull) e accedere al Registro di sistema utilizzando il token dell’account di servizio.

c. Creare un file script della shell e incollarne il contenuto seguente.

```
[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. Rendere il file eseguibile.

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

e. Eseguire lo script della shell.

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

4. Quando si utilizzano registri di immagini private non pubblicamente attendibili, caricare i certificati TLS del registro di immagini nei nodi OpenShift. A tale scopo, creare una configurazione nello spazio dei nomi openshift-config utilizzando i certificati TLS e applicarla alla configurazione dell'immagine del cluster per rendere attendibile il certificato.

```
[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
```

> Se si utilizza un registro interno di OpenShift con certificati TLS predefiniti dall'operatore di ingresso con un percorso, è comunque necessario seguire la procedura precedente per applicare la patch ai certificati con il nome host del percorso. Per estrarre i certificati dall'operatore di ingresso, è possibile utilizzare il comando `oc extract secret/router-ca --keys=tls.crt -n openshift-ingress-operator`.

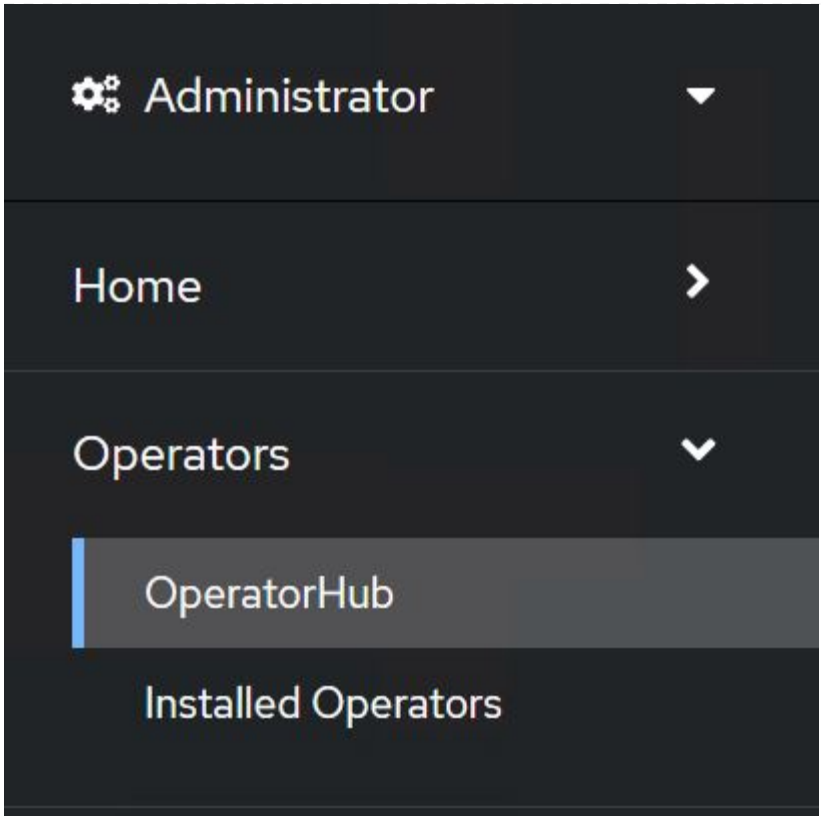
5. Creare uno spazio dei nomi `netapp-acc-operator` Per Astra Control Center.

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

namespace/netapp-acc-operator created
```

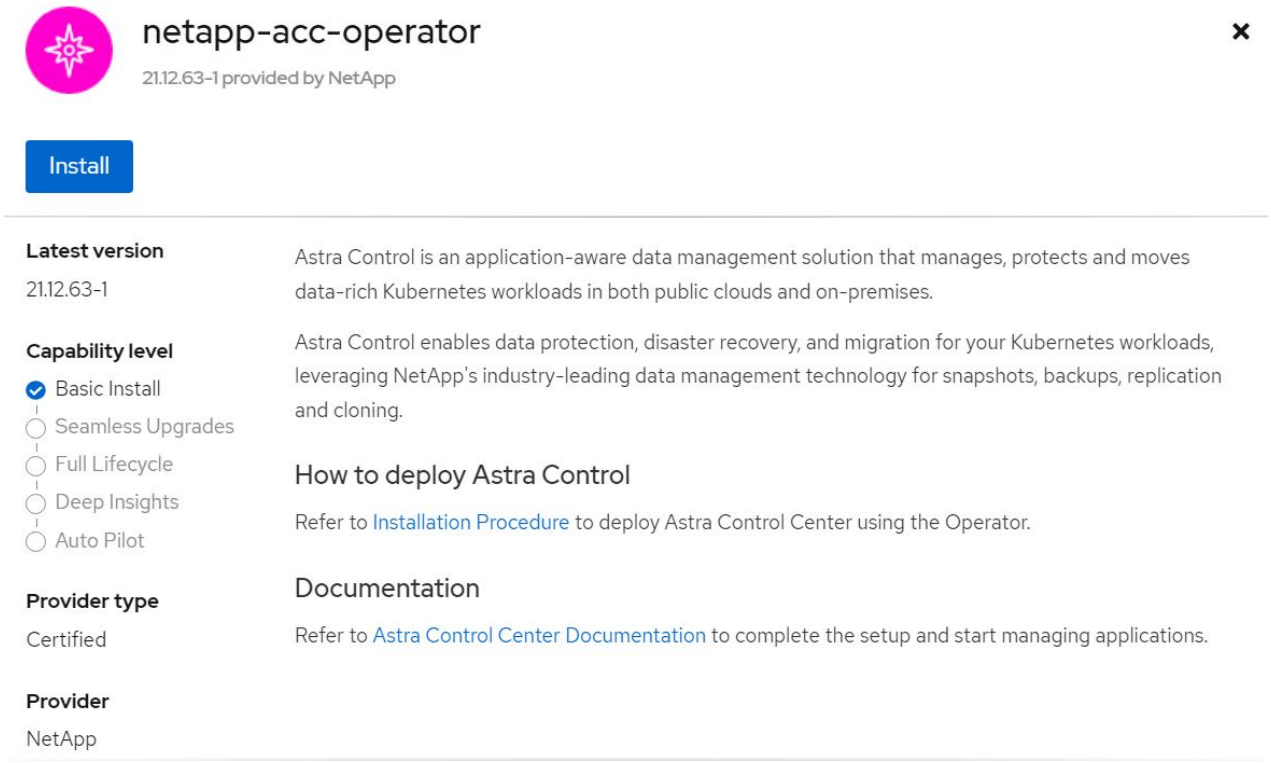
6. Creare un segreto con le credenziali per accedere al registro delle immagini in `netapp-acc-operator` namespace.

```
[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
```

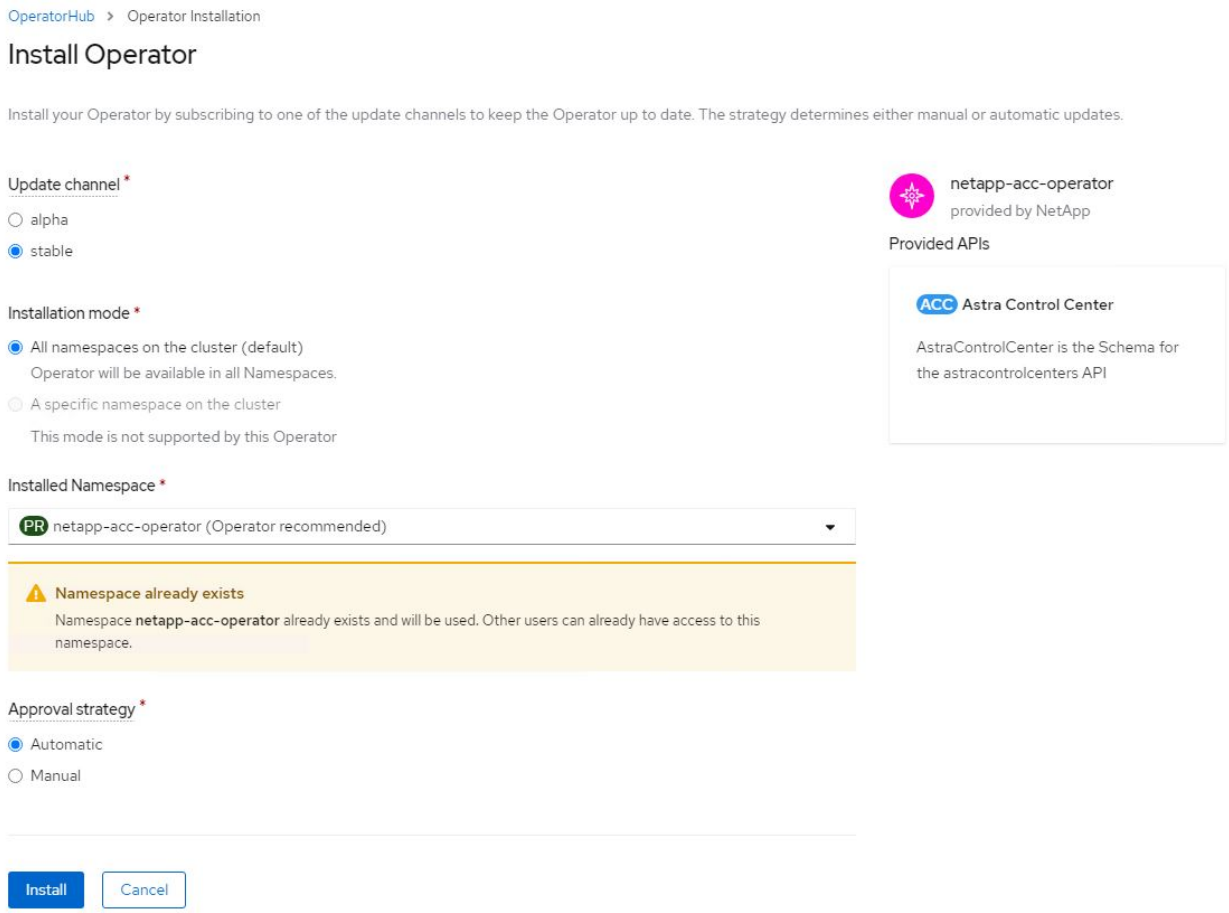
7. Accedi alla console GUI di Red Hat OpenShift con accesso cluster-admin.
8. Selezionare Administrator (Amministratore) dal menu a discesa Perspective (prospettiva).
9. Accedere a Operator > OperatorHub e cercare Astra.



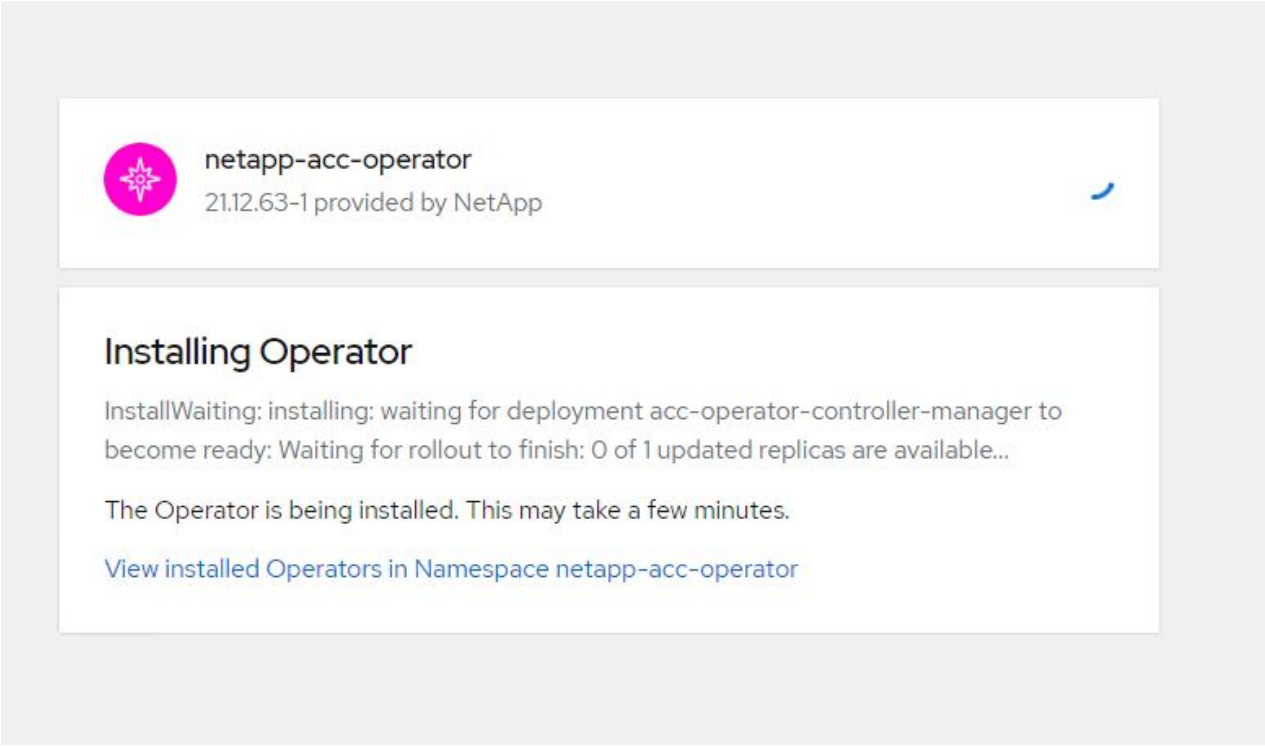
10. Selezionare `netapp-acc-operator` affiancare e fare clic su `Install`.



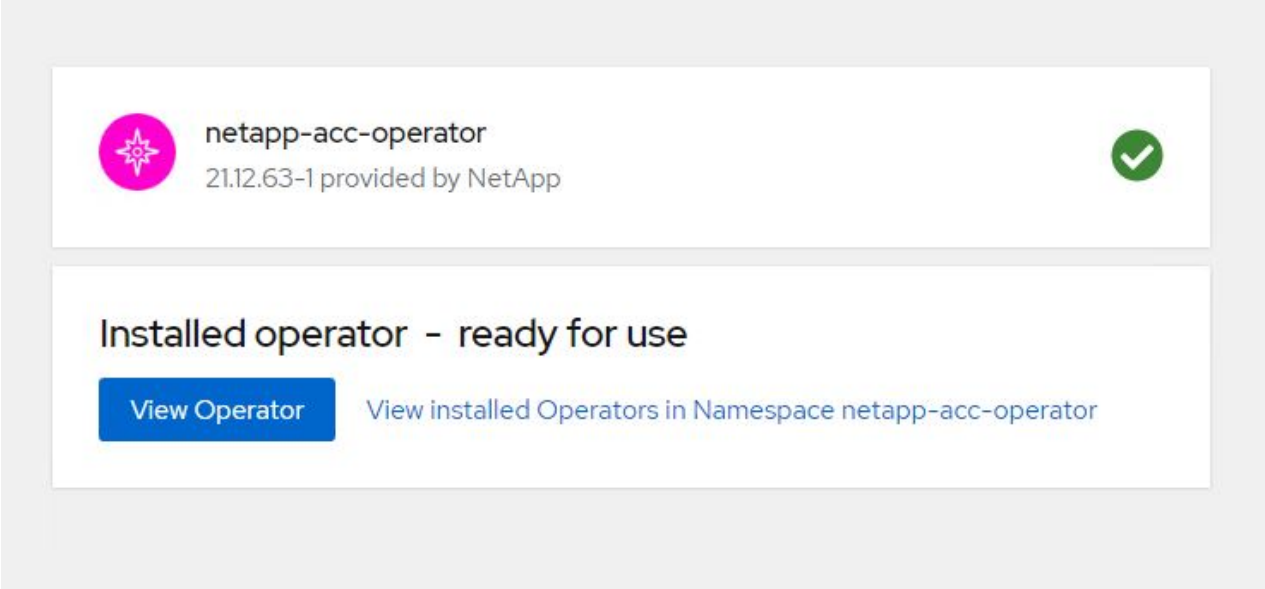
11. Nella schermata Install Operator (Installa operatore), accettare tutti i parametri predefiniti e fare clic su `Install`.



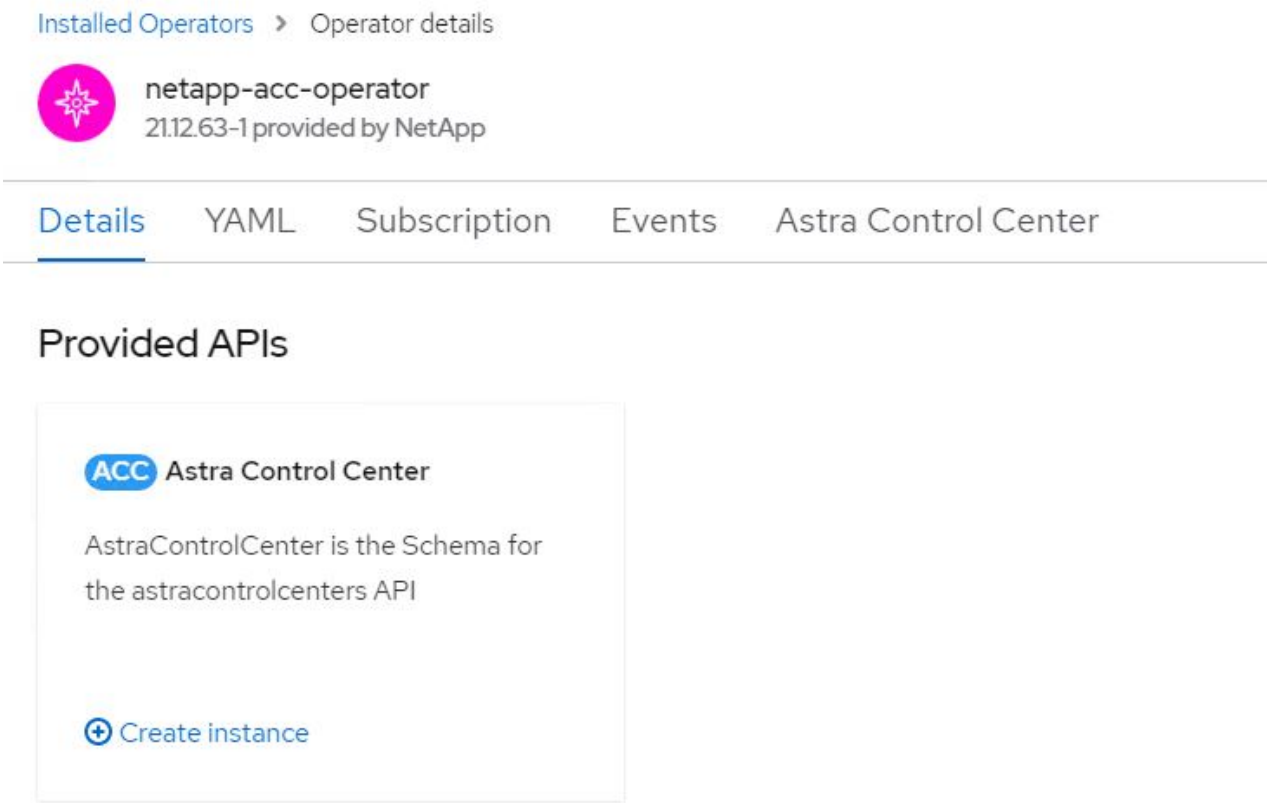
12. Attendere il completamento dell'installazione da parte dell'operatore.



13. Una volta completata l'installazione dell'operatore, selezionare per fare clic su `View Operator`.



14. Quindi fare clic su `Create Instance` Nel riquadro Astra Control Center dell'operatore.



15. Riempire `Create AstraControlCenter` campi del modulo e fare clic su `Create`.

    a. Se si desidera, modificare il nome dell'istanza di Astra Control Center.
    b. Se si desidera, attivare o disattivare il supporto automatico. Si consiglia di mantenere la funzionalità di supporto automatico.
    c. Inserire il nome FQDN per Astra Control Center.
    d. Inserire la versione di Astra Control Center; per impostazione predefinita viene visualizzata la

versione più recente.

e. Inserisci un nome account per Astra Control Center e i dettagli dell'amministratore come nome, cognome e indirizzo e-mail.

f. Inserire il criterio di recupero del volume, l'impostazione predefinita è Mantieni.

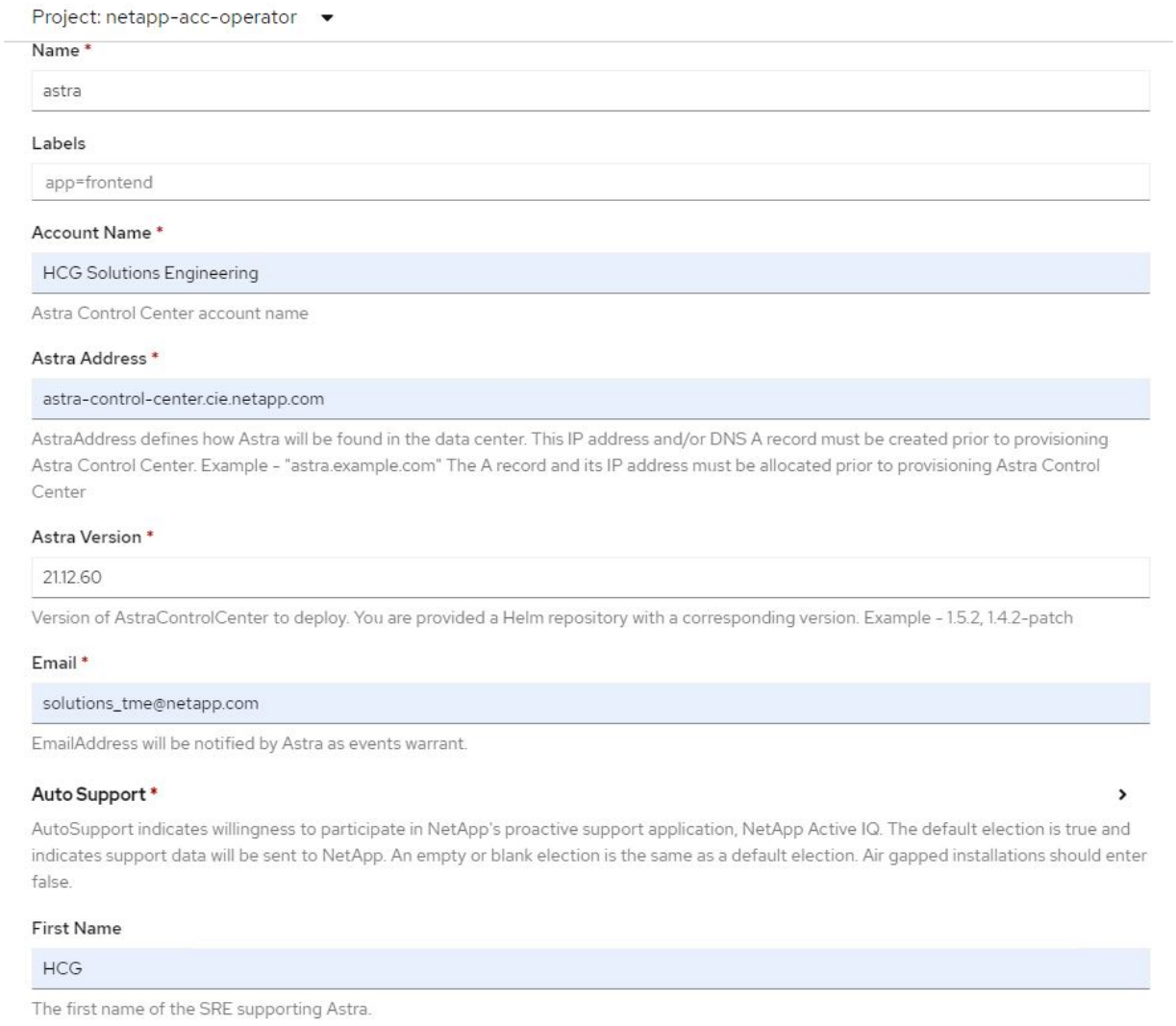
g. In Image Registry (Registro immagini), immettere l'FQDN del registro insieme al nome dell'organizzazione assegnato durante l'invio delle immagini al registro (in questo esempio, `astra-registry.apps.ocp-vmw.cie.netapp.com/netapp-astra`)

h. Se si utilizza un registro che richiede l'autenticazione, inserire il nome segreto nella sezione Registro immagini.

i. Configurare le opzioni di scalabilità per i limiti delle risorse di Astra Control Center.

j. Inserire il nome della classe di storage se si desidera inserire PVC in una classe di storage non predefinita.

k. Definire le preferenze di gestione 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

Automatizzato [Ansible]

1. Per utilizzare i playbook Ansible per implementare Astra Control Center, è necessaria una macchina Ubuntu/RHEL con Ansible installato. Seguire le procedure "qui" Per Ubuntu e RHEL.
2. Clonare il repository GitHub che ospita il contenuto Ansible.

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

3. Accedi al sito NetApp Support e scarica l'ultima versione di NetApp Astra Control Center. Per farlo, è necessaria una licenza allegata al tuo account NetApp. Dopo aver scaricato il tarball, trasferirlo sulla workstation.

> Per iniziare a utilizzare una licenza di prova per Astra Control, visitare il sito "Sito di registrazione Astra".

4. Creare o ottenere il file kubeconfig con accesso amministratore al cluster OpenShift su cui deve essere installato Astra Control Center.

5. Modificare la directory in na_astra_control_suite.

```
cd na_astra_control_suite
```

6. Modificare il `vars/vars.yml` e inserire le variabili con le informazioni richieste.

```
#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. Esegui il manuale per implementare Astra Control Center. Il playbook richiede privilegi root per alcune configurazioni.

   Se l'utente che esegue il playbook è root o ha configurato sudo senza password, eseguire il seguente comando per eseguire il playbook.

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

   Se l'utente ha configurato l'accesso sudo basato su password, eseguire il seguente comando per eseguire il manuale, quindi inserire la password sudo.

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

Fasi successive all'installazione

1. Il completamento dell'installazione potrebbe richiedere alcuni minuti. Verificare che tutti i pod e i servizi in `netapp-astra-cc` namespace in esecuzione.

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

2. Controllare `acc-operator-controller-manager` registri per garantire che l'installazione sia completata.

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

Il seguente messaggio indica la corretta installazione di Astra Control Center.

```
{"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. Il nome utente per l'accesso ad Astra Control Center è l'indirizzo e-mail dell'amministratore fornito nel file CRD e la password è una stringa `ACC-` Aggiunto all'UUID di Astra Control Center. Eseguire il seguente comando:

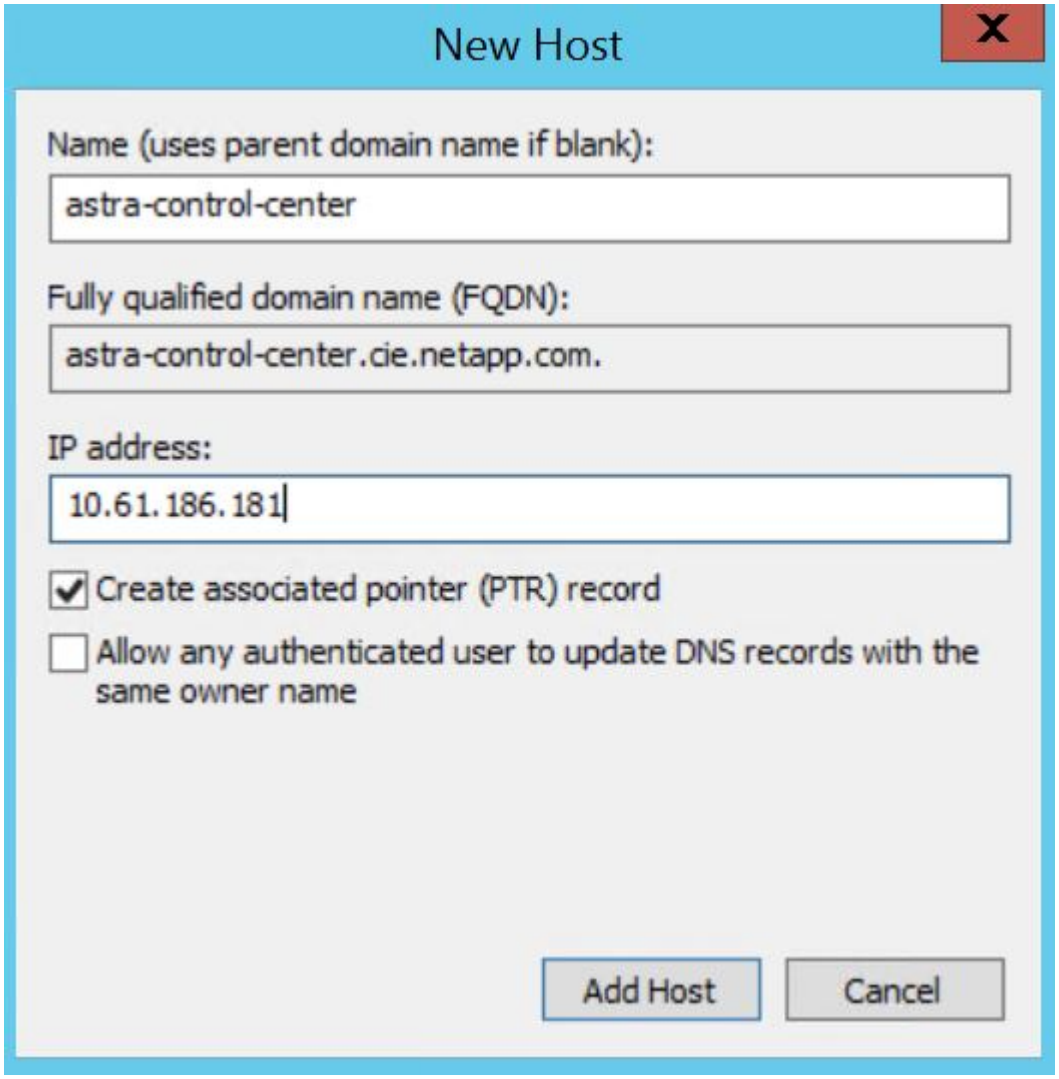
```
[netapp-user@rhel7 ~]$ oc get astracontrolcenters -n netapp-astra-cc
NAME    UUID
astra   345c55a5-bf2e-21f0-84b8-b6f2bce5e95f
```

In questo esempio, la password è `ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f`.

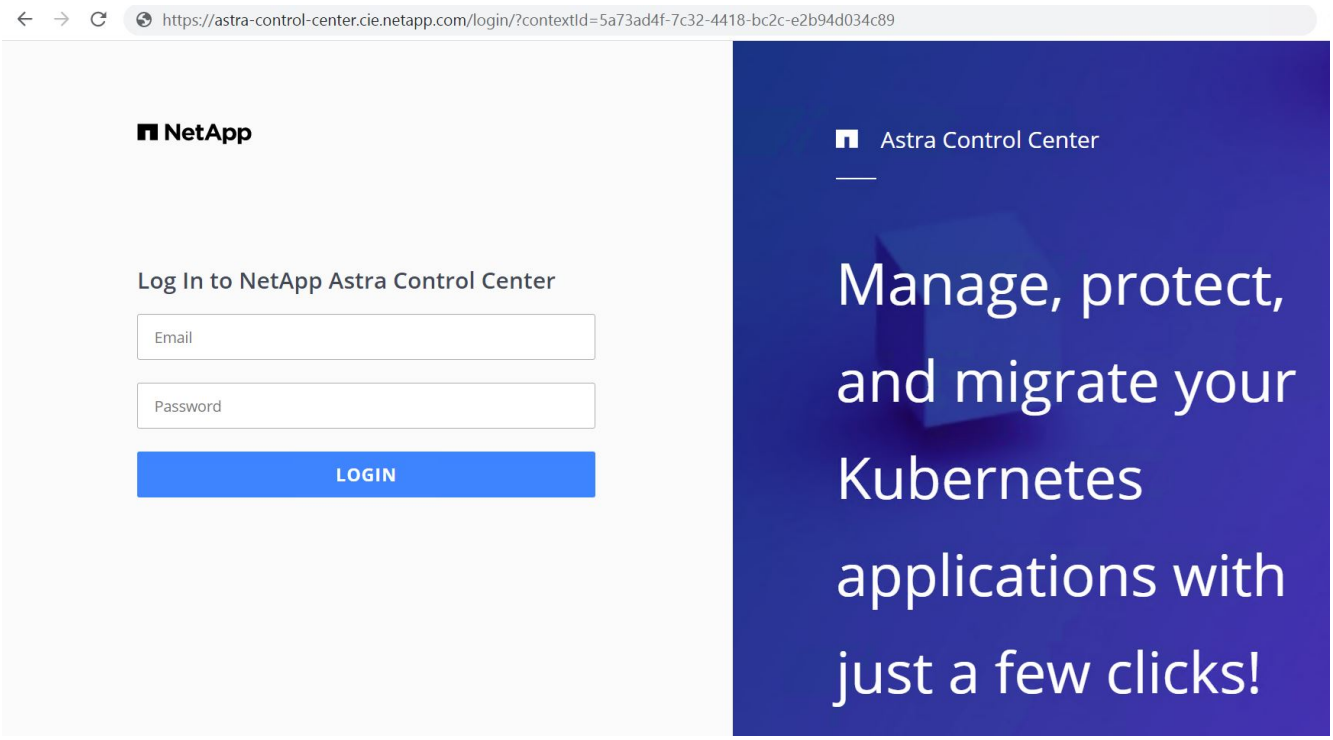
4. Ottieni l'IP del bilanciamento del carico del servizio traefik.

```
[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
```

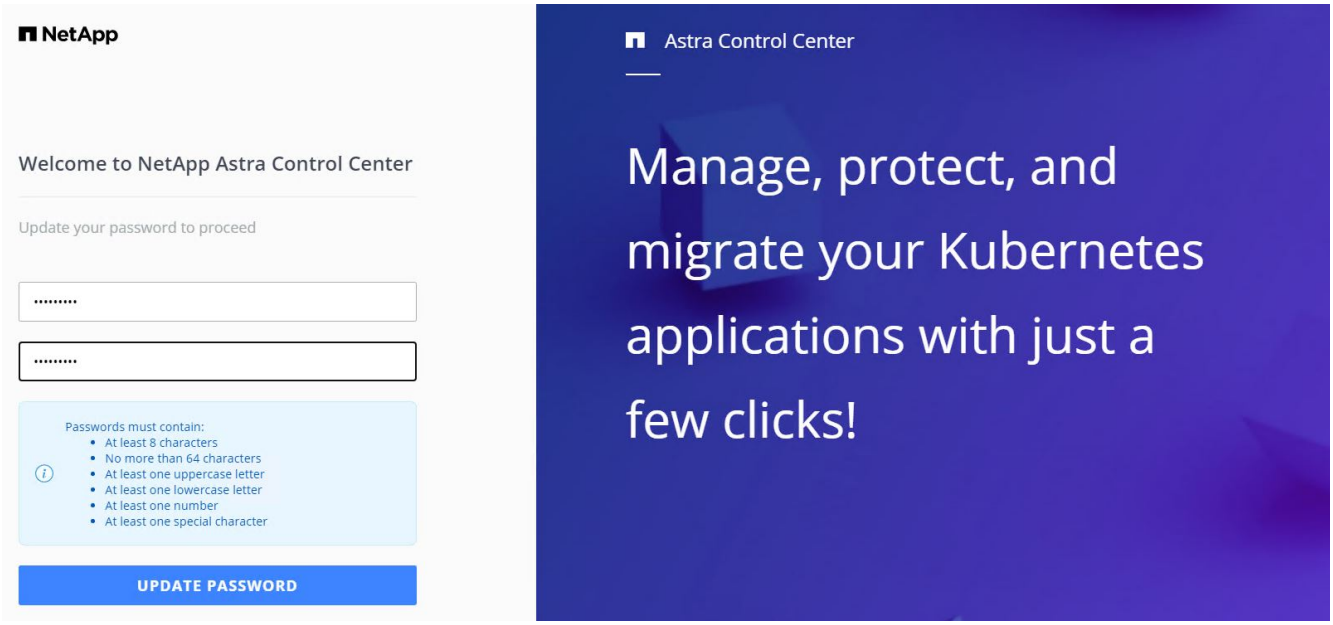
5. Aggiungere una voce nel server DNS che punta all'FQDN fornito nel file CRD di Astra Control Center `EXTERNAL-IP` del servizio traefik.



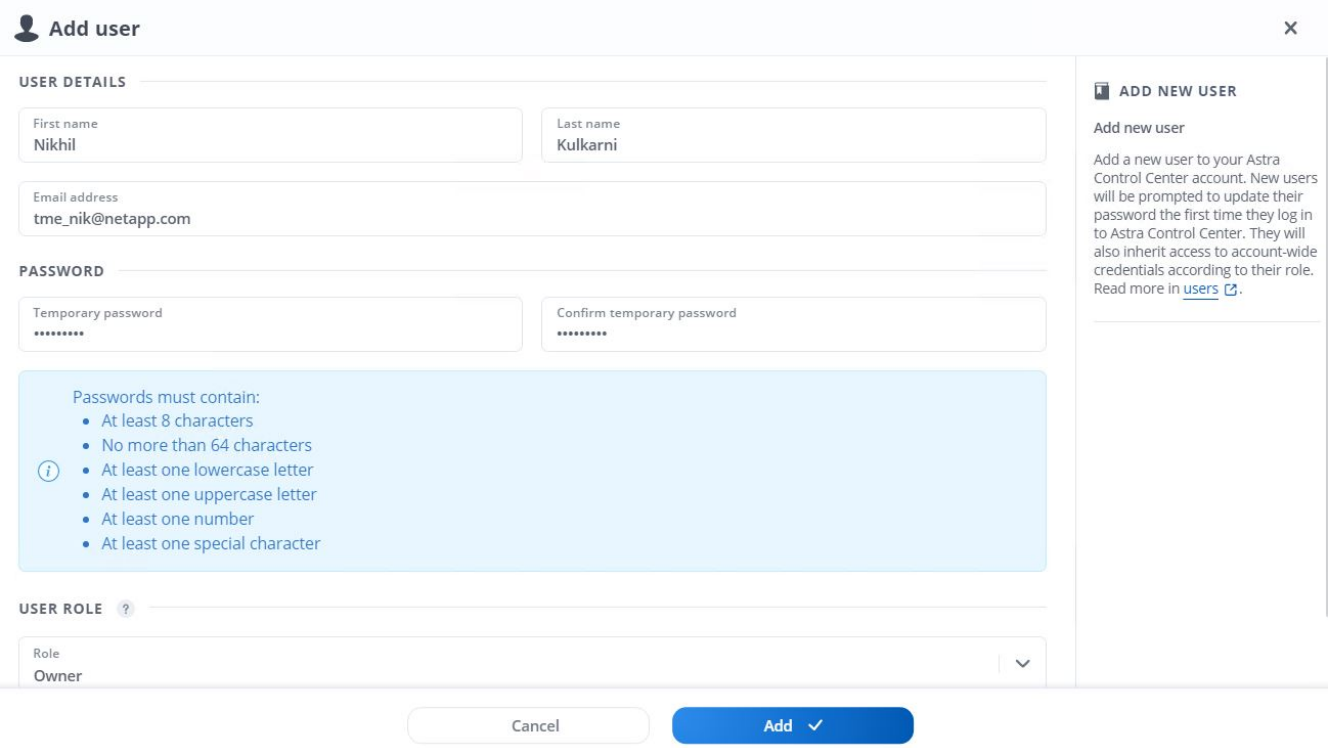
6. Accedere alla GUI di Astra Control Center esplorando il relativo FQDN.



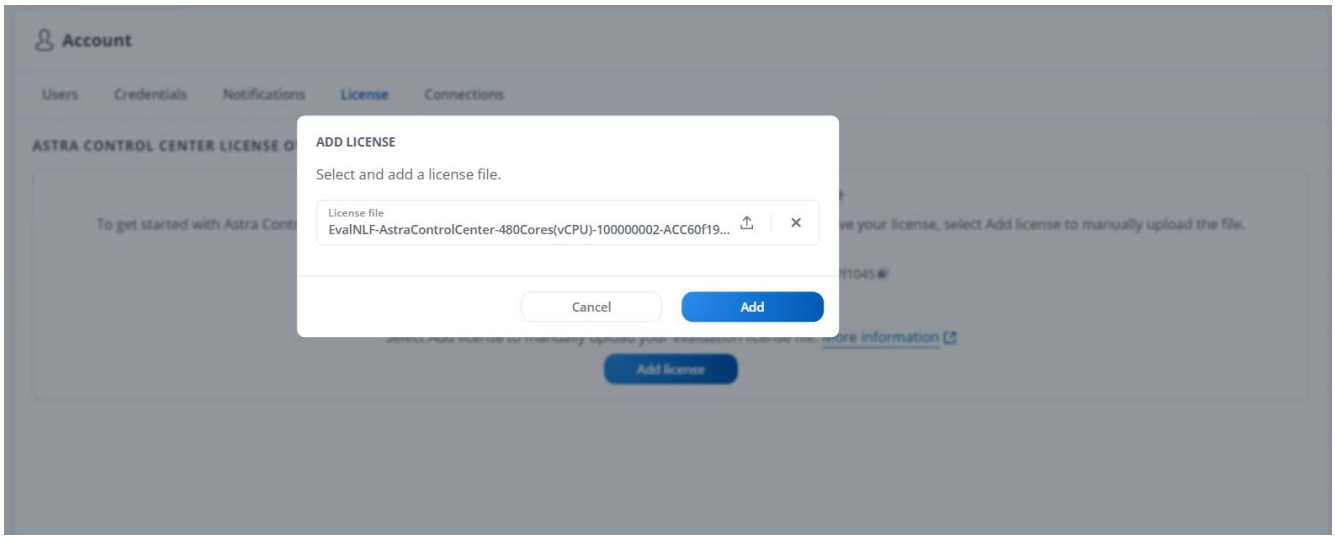
7. Quando si accede all'interfaccia grafica di Astra Control Center per la prima volta utilizzando l'indirizzo email admin fornito in CRD, è necessario modificare la password.



8. Se si desidera aggiungere un utente ad Astra Control Center, accedere a account > Users (account > utenti), fare clic su Add (Aggiungi), inserire i dettagli dell'utente e fare clic su Add (Aggiungi).



9. Astra Control Center richiede una licenza per il funzionamento di tutte le funzionalità IT. Per aggiungere una licenza, accedere a account > License (account > licenza), fare clic su Add License (Aggiungi licenza) e caricare il file di licenza.



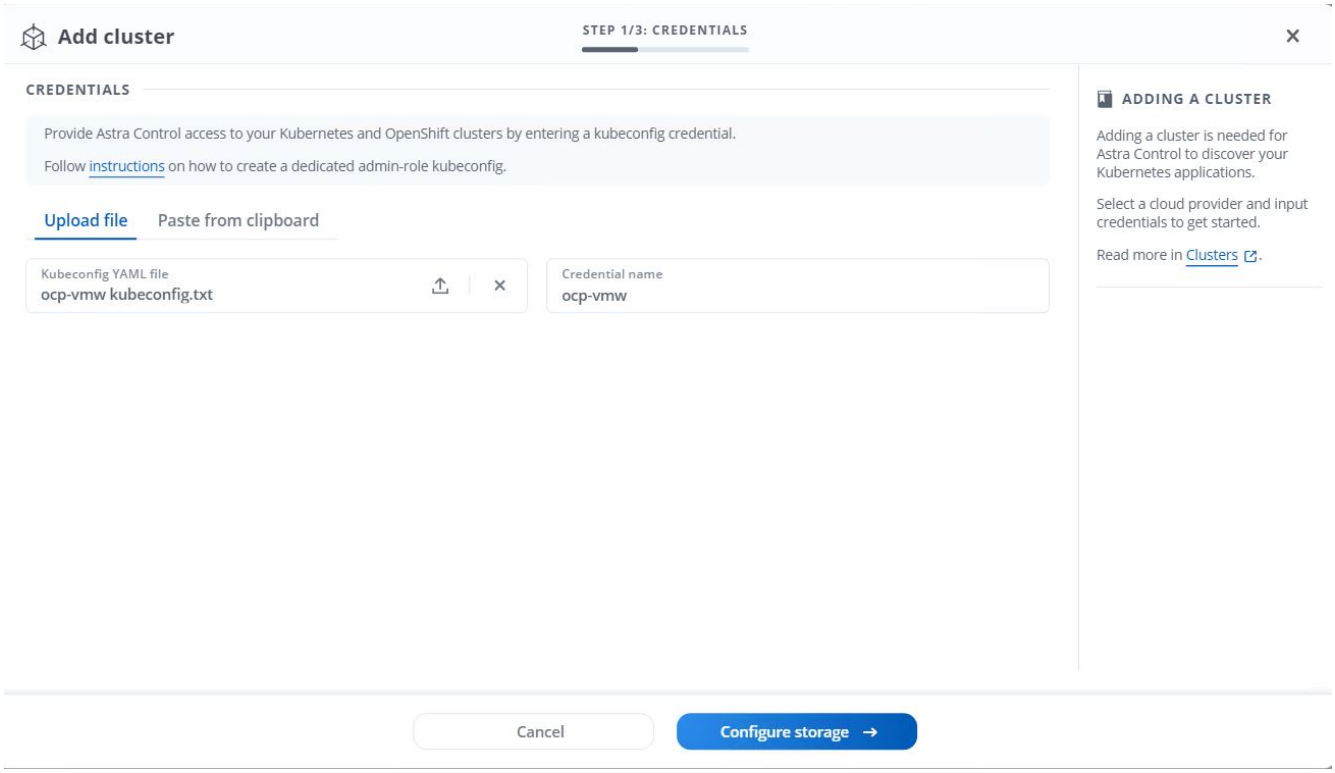
In caso di problemi con l'installazione o la configurazione di NetApp Astra Control Center, è disponibile la knowledge base dei problemi noti "qui".

Registra i tuoi Red Hat OpenShift Clusters con Astra Control Center

Per consentire ad Astra Control Center di gestire i carichi di lavoro, devi prima registrare il cluster Red Hat OpenShift.

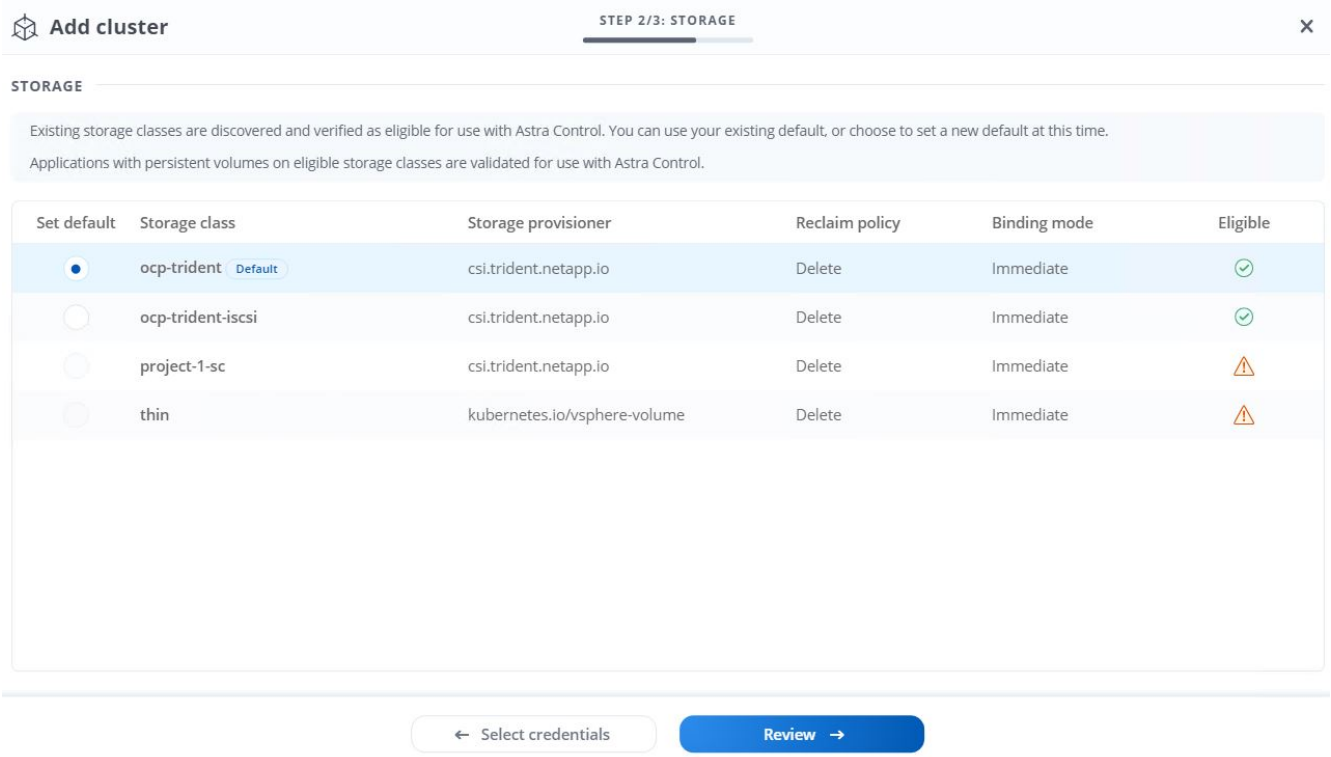
Registra i cluster Red Hat OpenShift

1. Il primo passo consiste nell'aggiungere i cluster OpenShift all'Astra Control Center e gestirli. Accedere a Clusters e fare clic su Add a Cluster (Aggiungi cluster), caricare il file kubeconfig per il cluster OpenShift e fare clic su Select Storage (Seleziona storage).

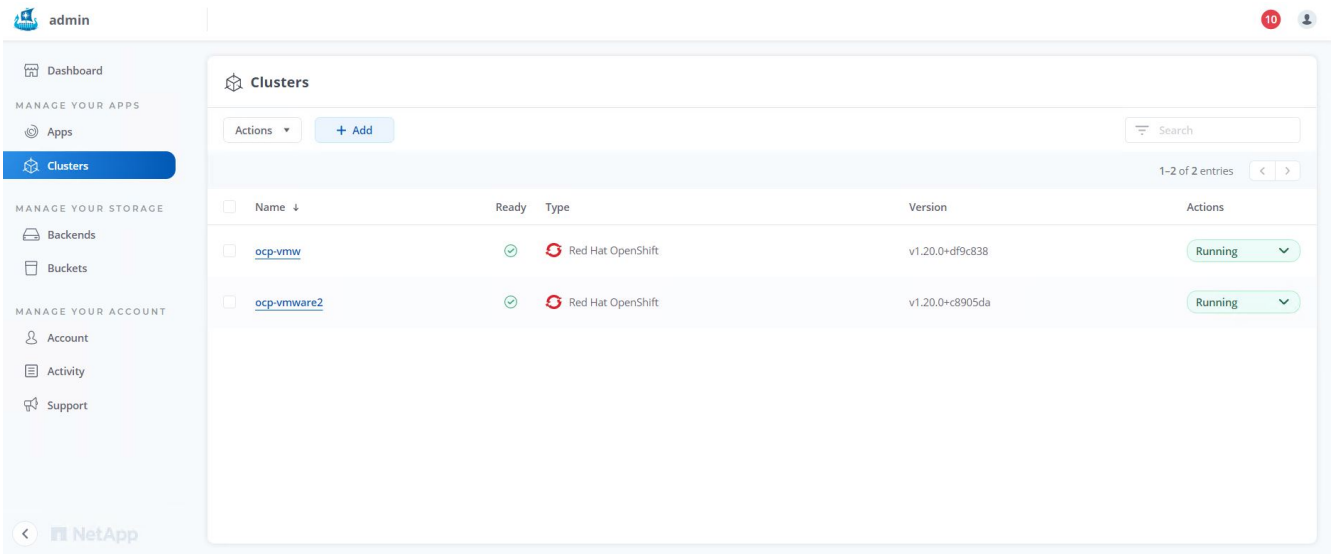


> Il file kubeconfig può essere generato per l'autenticazione con un nome utente e una password o un token. I token scadono dopo un periodo di tempo limitato e potrebbero non essere raggiungibili dal cluster registrato. NetApp consiglia di utilizzare un file kubeconfig con nome utente e password per registrare i cluster OpenShift su Astra Control Center.

2. Astra Control Center rileva le classi di storage idonee. Selezionare ora il modo in cui lo storageclass effettua il provisioning dei volumi utilizzando Trident supportato da una SVM su NetApp ONTAP e fare clic su Review (esamina). Nel riquadro successivo, verificare i dettagli e fare clic su Add Cluster (Aggiungi cluster).

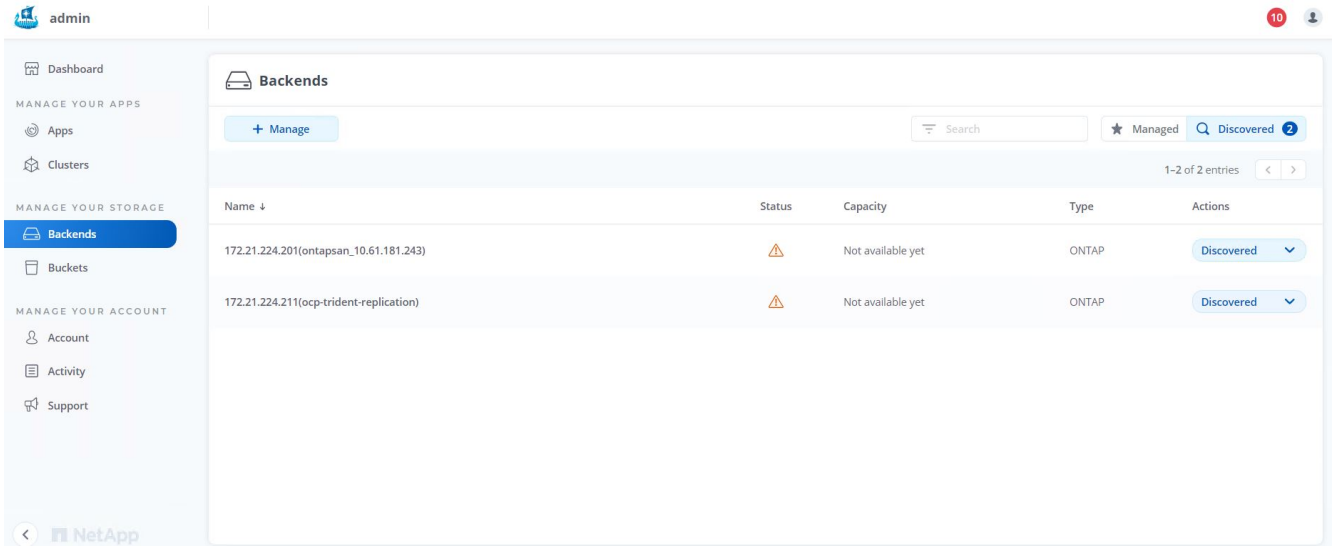


3. Registrare entrambi i cluster OpenShift come descritto al punto 1. Una volta aggiunti, i cluster passano allo stato di rilevamento mentre Astra Control Center li ispeziona e installa gli agenti necessari. Lo stato del cluster diventa in esecuzione dopo che sono stati registrati correttamente.

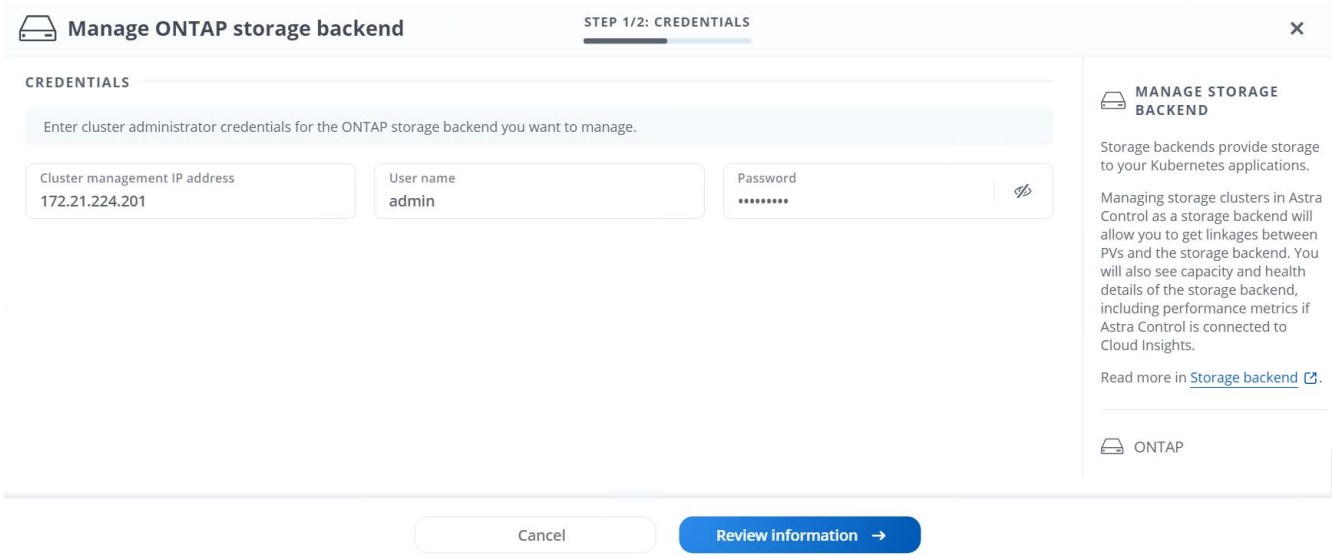


> Tutti i cluster Red Hat OpenShift che devono essere gestiti da Astra Control Center devono avere accesso al registro delle immagini utilizzato per l'installazione, poiché gli agenti installati sui cluster gestiti estraggono le immagini da tale registro.

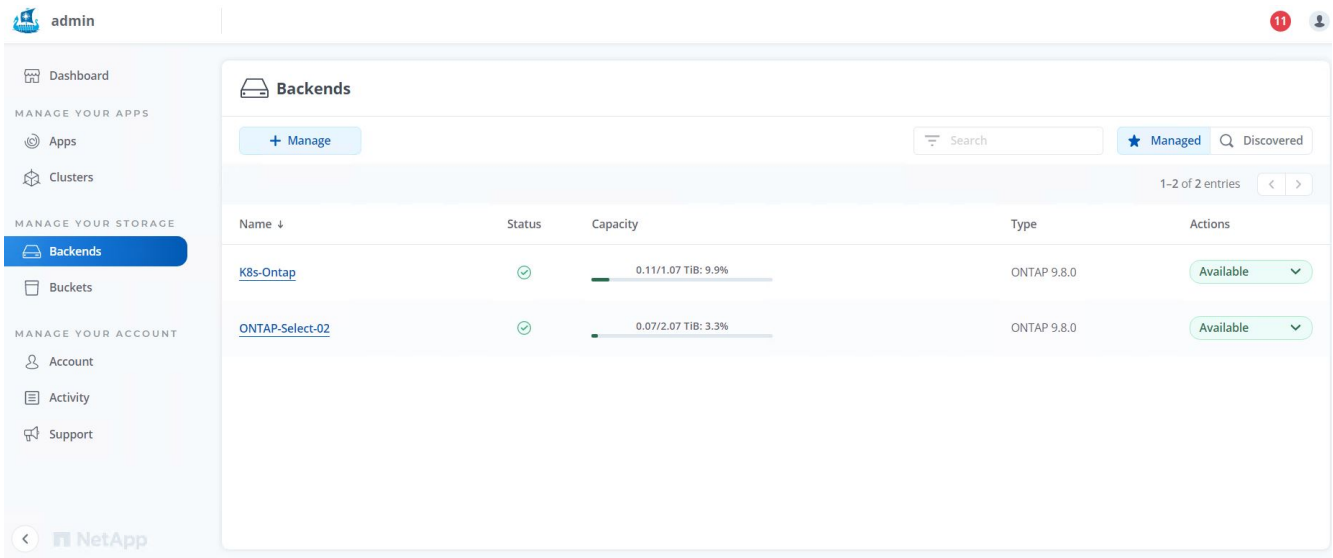
4. Importa i cluster ONTAP come risorse storage da gestire come back-end dal centro di controllo Astra. Quando i cluster OpenShift vengono aggiunti ad Astra e viene configurato uno storageclass, il cluster ONTAP viene automaticamente ispezionato e ispezionato per il backup dello storageclass, ma non viene importato nel centro di controllo Astra da gestire.



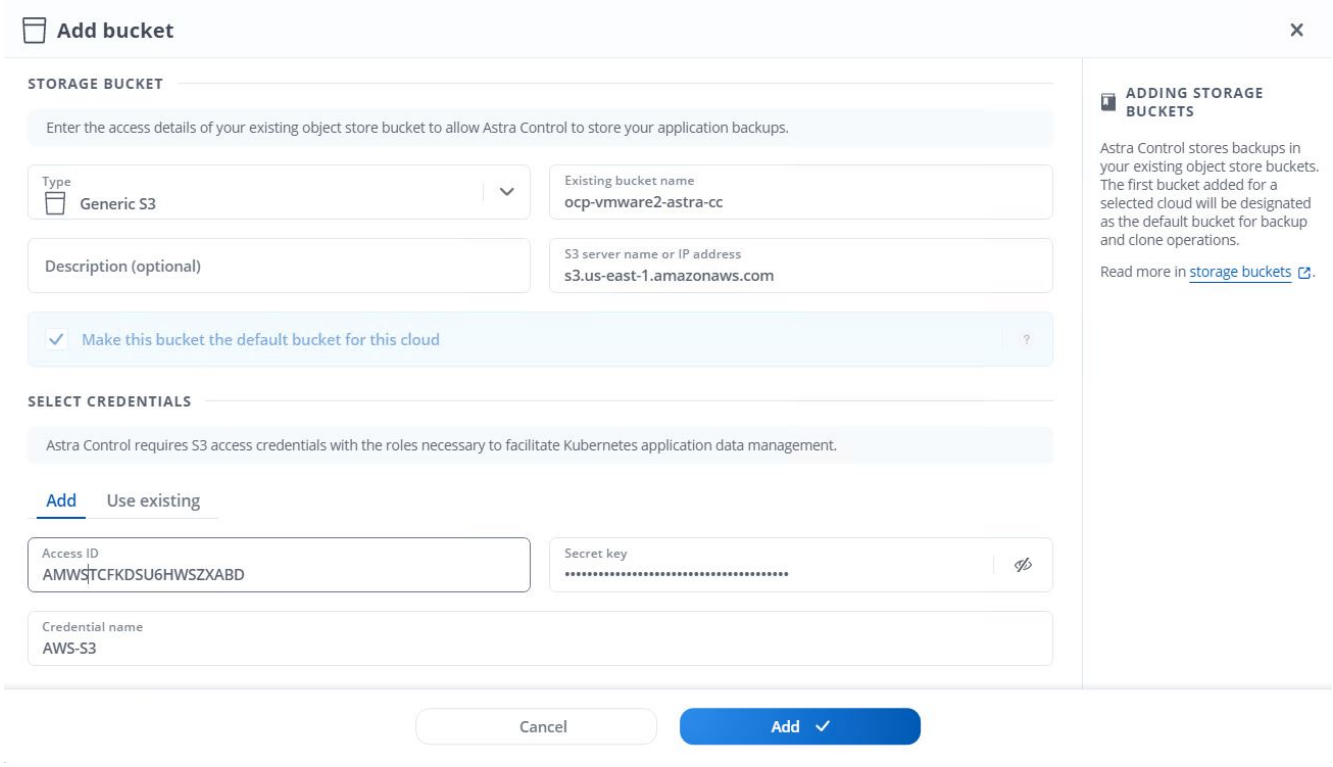
5. Per importare i cluster ONTAP, accedere a Backend, fare clic sul menu a discesa e selezionare Manage (Gestisci) accanto al cluster ONTAP da gestire. Immettere le credenziali del cluster ONTAP, fare clic su informazioni di revisione, quindi fare clic su Importa backend storage.



6. Una volta aggiunti i backend, lo stato diventa disponibile. Questi backend ora dispongono delle informazioni sui volumi persistenti nel cluster OpenShift e sui volumi corrispondenti nel sistema ONTAP.



7. Per il backup e il ripristino tra cluster OpenShift utilizzando Astra Control Center, è necessario eseguire il provisioning di un bucket di storage a oggetti che supporti il protocollo S3. Le opzioni attualmente supportate sono ONTAP S3, StorageGRID e AWS S3. Ai fini di questa installazione, configureremo un bucket AWS S3. Accedere a Bucket, fare clic su Add bucket (Aggiungi bucket) e selezionare Generic S3. Inserisci i dettagli sul bucket S3 e le credenziali per accedervi, fai clic sulla casella di controllo "Rendi questo bucket il bucket predefinito per il cloud", quindi fai clic su Aggiungi.

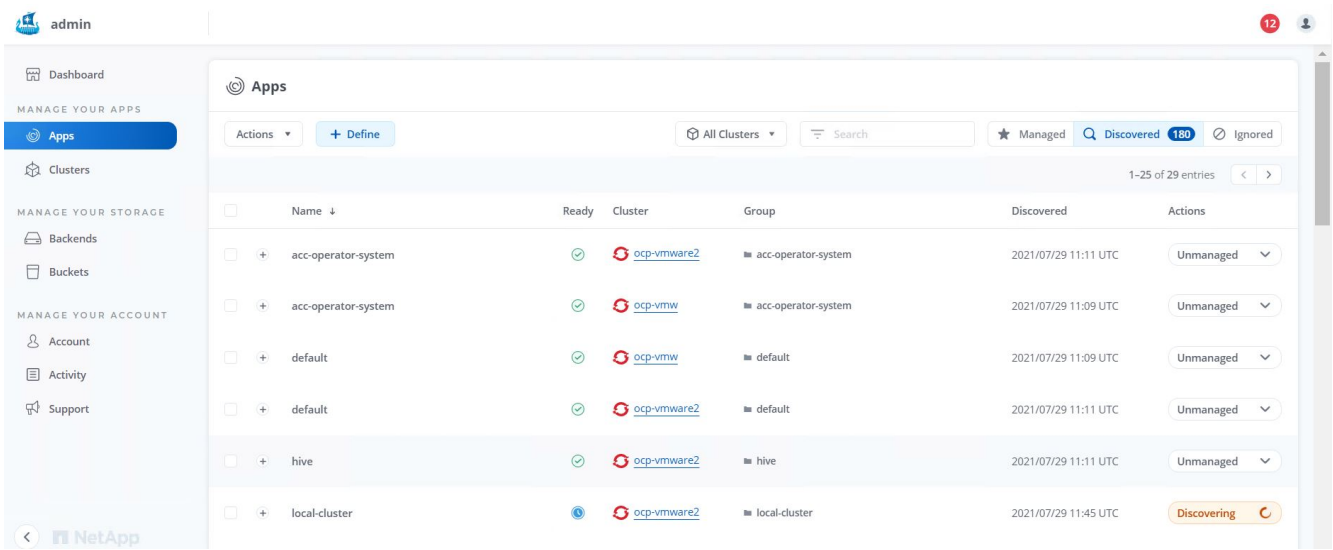


Scegliere le applicazioni da proteggere

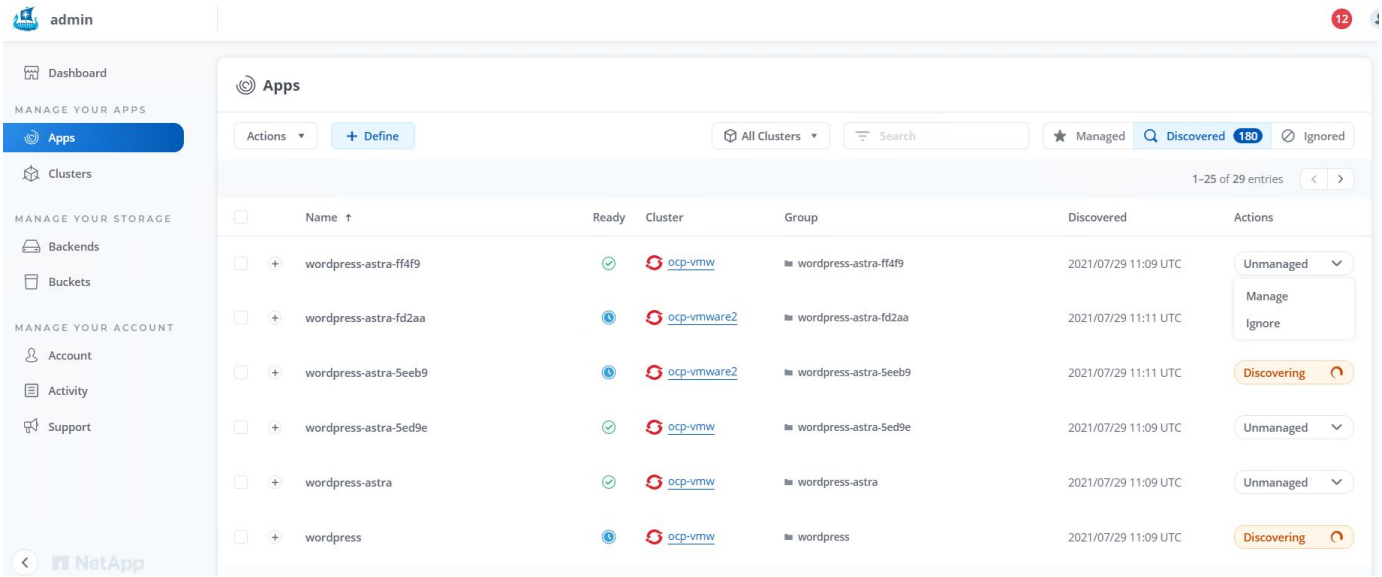
Dopo aver registrato i cluster Red Hat OpenShift, è possibile individuare le applicazioni implementate e gestirle tramite Astra Control Center.

Gestire le applicazioni

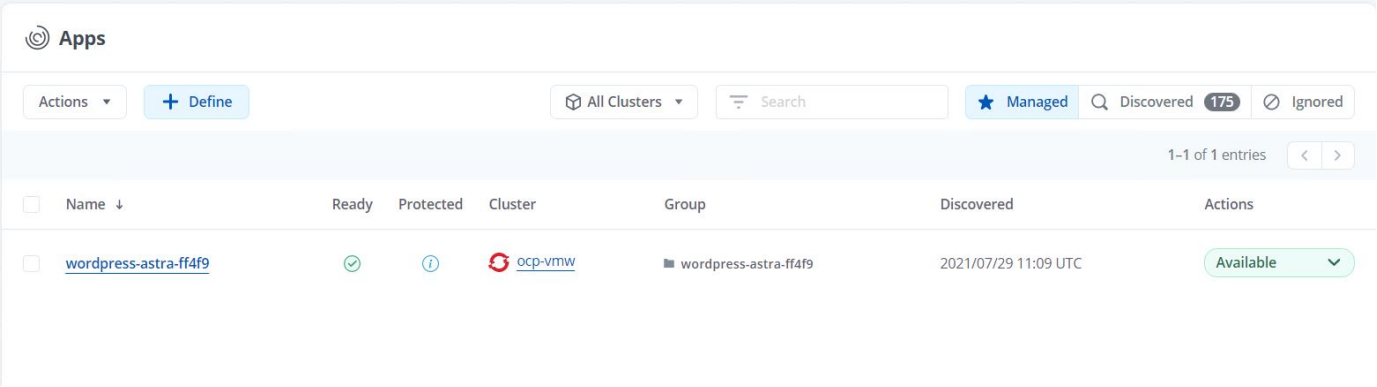
1. Una volta registrati i cluster OpenShift e i backend ONTAP con il centro di controllo Astra, il centro di controllo inizia automaticamente a rilevare le applicazioni in tutti gli spazi dei nomi che utilizzano lo storageclass configurato con il backend ONTAP specificato.



2. Accedere a Apps > Dovered (applicazioni > rilevate) e fare clic sul menu a discesa accanto all'applicazione che si desidera gestire utilizzando Astra. Quindi fare clic su Manage (Gestisci)



1. L'applicazione entra nello stato Available (disponibile) e può essere visualizzata nella scheda Managed (gestito) nella sezione Apps (applicazioni).



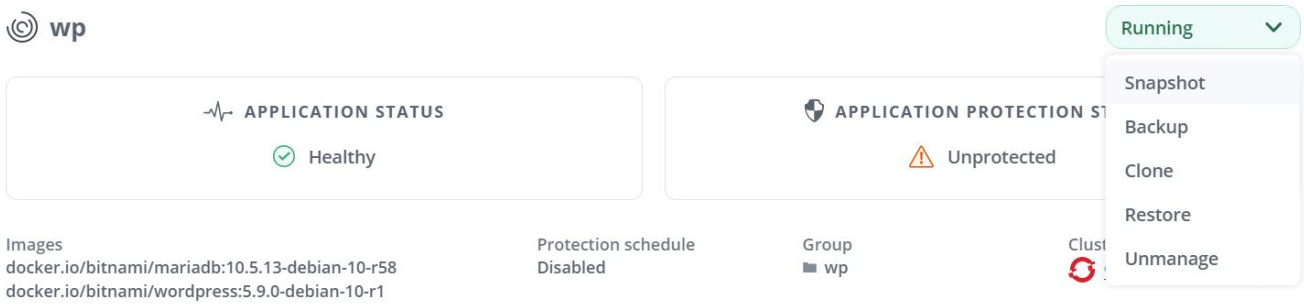
Proteggi le tue applicazioni

Una volta gestiti i carichi di lavoro delle applicazioni da Astra Control Center, è possibile configurare le impostazioni di protezione per tali carichi di lavoro.

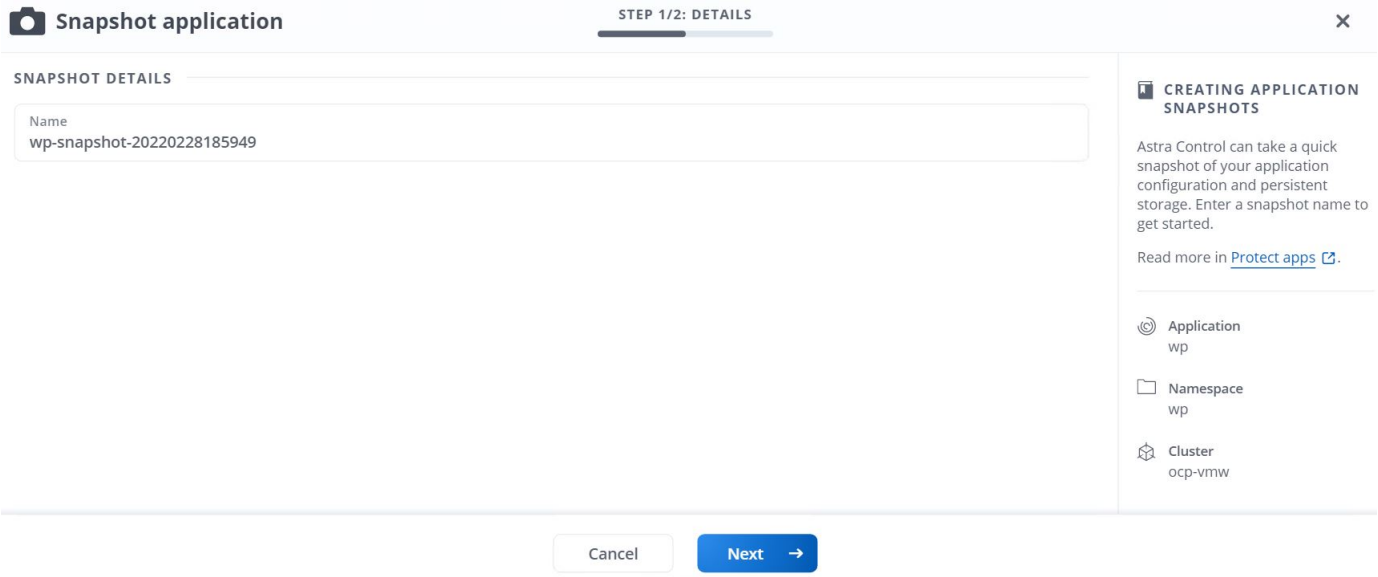
Creazione di un'istantanea dell'applicazione

Un'istantanea di un'applicazione crea una copia Snapshot di ONTAP che può essere utilizzata per ripristinare o clonare l'applicazione in un momento specifico in base a tale copia Snapshot.

1. Per creare un'istantanea dell'applicazione, accedere alla scheda applicazioni > gestite e fare clic sull'applicazione di cui si desidera creare una copia Snapshot. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Snapshot.



2. Inserire i dettagli dell'istantanea, fare clic su Next (Avanti), quindi su Snapshot (istantanea). La creazione dello snapshot richiede circa un minuto e lo stato diventa disponibile dopo la creazione dello snapshot.



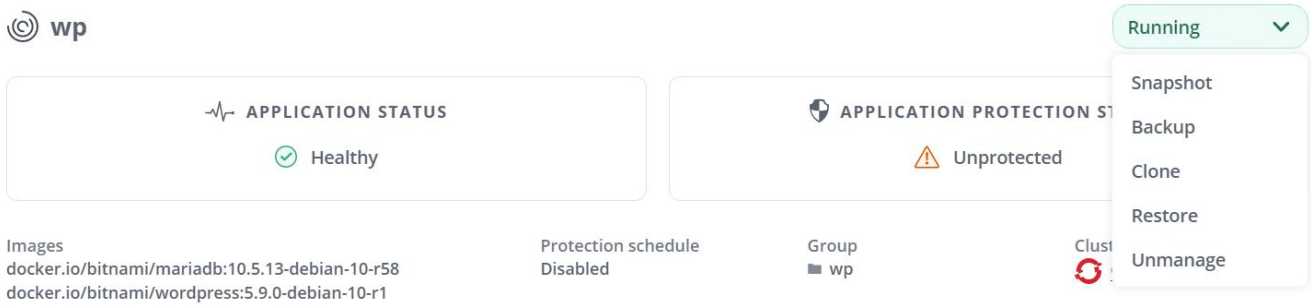
Creazione di un backup dell'applicazione

Un backup di un'applicazione acquisisce lo stato attivo dell'applicazione e la configurazione delle risorse IT, le taglia in file e le memorizza in un bucket di storage a oggetti remoto.

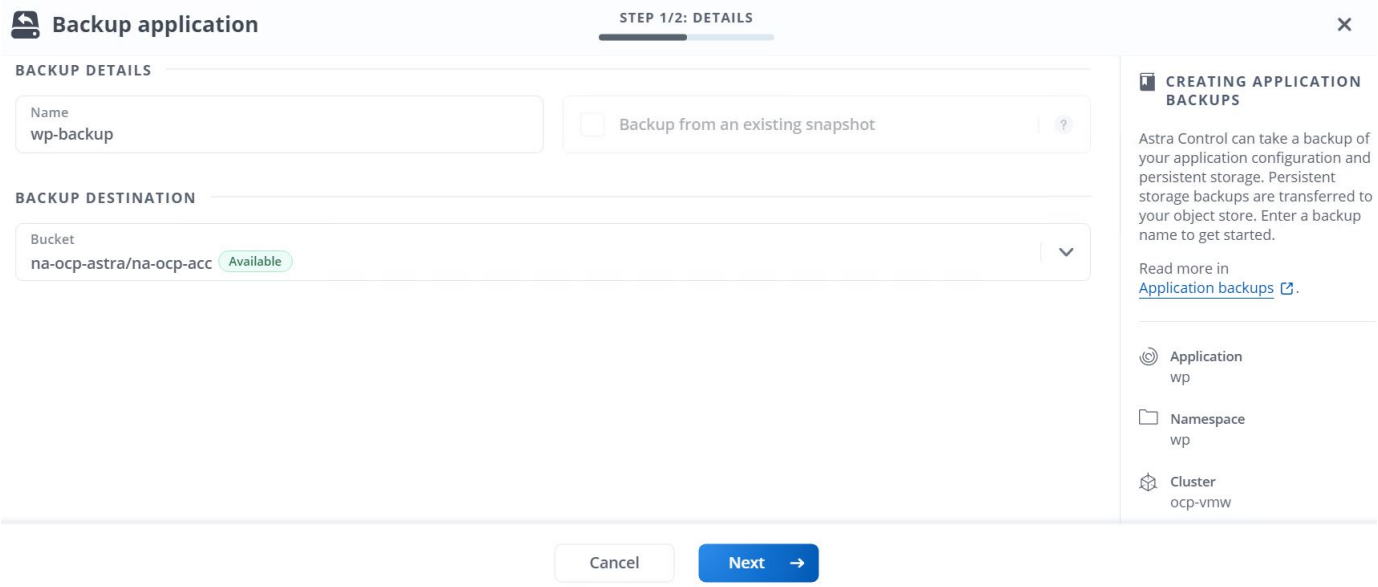
Per il backup e il ripristino delle applicazioni gestite nel centro di controllo Astra, è necessario configurare le impostazioni del superutente per i sistemi ONTAP di backup come prerequisito. A tale scopo, immettere i seguenti comandi.

```
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. Per creare un backup dell'applicazione gestita in Astra Control Center, accedere alla scheda Apps (applicazioni) > Managed (gestite) e fare clic sull'applicazione di cui si desidera eseguire il backup. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Backup.



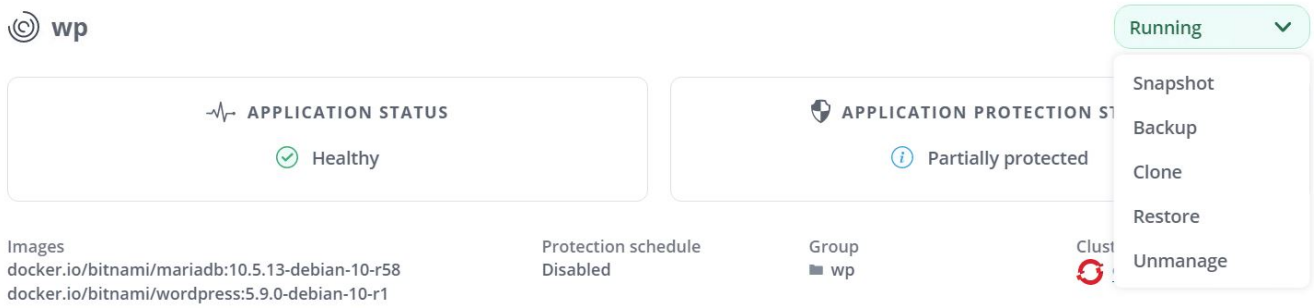
2. Inserire i dettagli del backup, selezionare il bucket di storage a oggetti in cui memorizzare i file di backup, fare clic su Next (Avanti) e, dopo aver esaminato i dettagli, fare clic su Backup (Backup). A seconda delle dimensioni dell'applicazione e dei dati, il backup può richiedere alcuni minuti e lo stato del backup diventa disponibile una volta completato correttamente il backup.



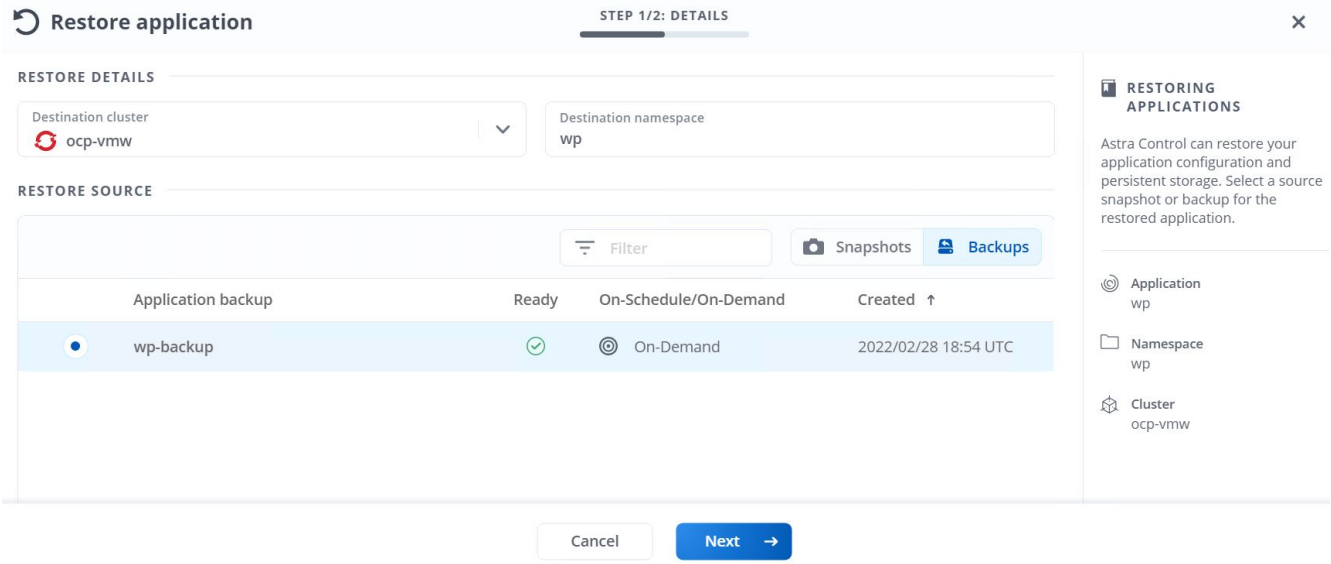
Ripristino di un’applicazione

Con la semplice pressione di un pulsante, è possibile ripristinare un’applicazione nello spazio dei nomi di origine nello stesso cluster o in un cluster remoto per la protezione delle applicazioni e il disaster recovery.

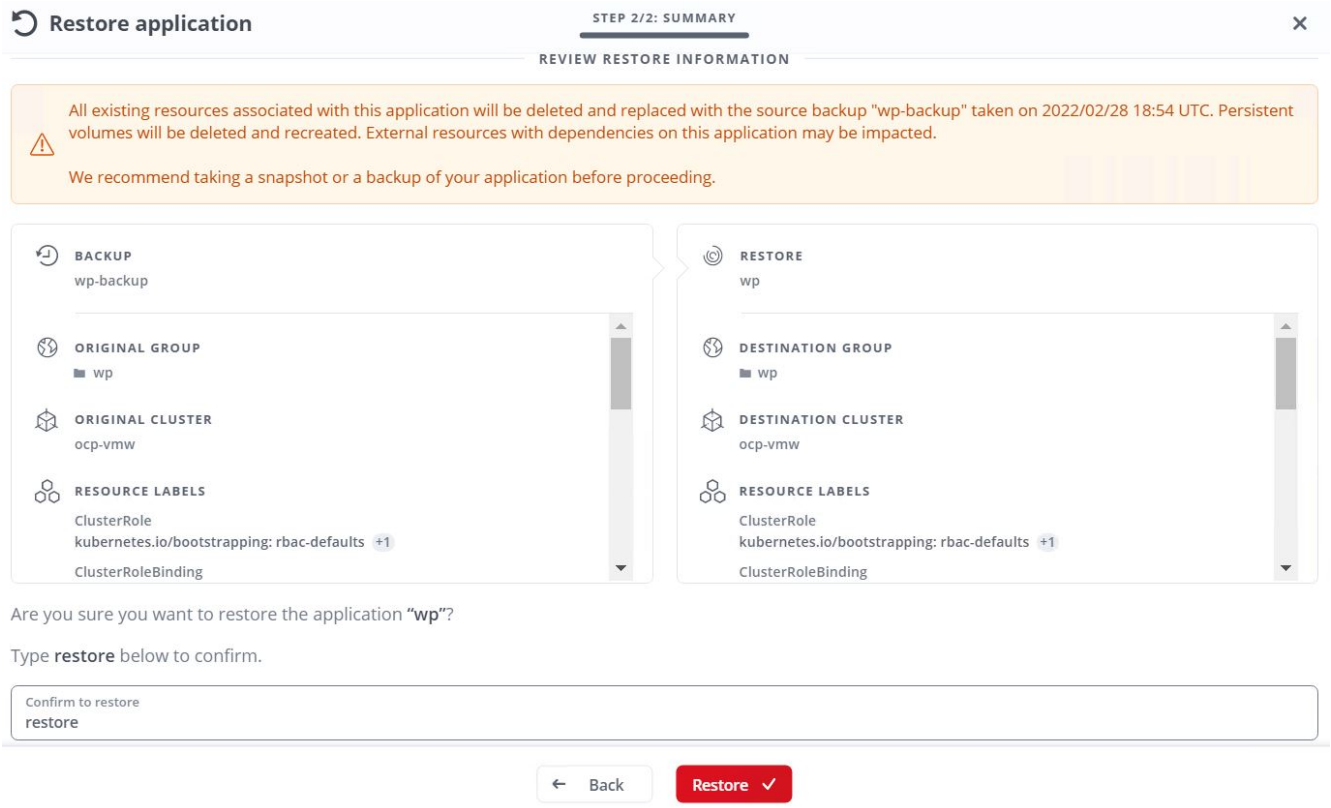
1. Per ripristinare un’applicazione, selezionare Apps (applicazioni) > Managed Tab (scheda gestita) e fare clic sull’applicazione in questione. Fare clic sul menu a discesa accanto al nome dell’applicazione e fare clic su `Restore`.



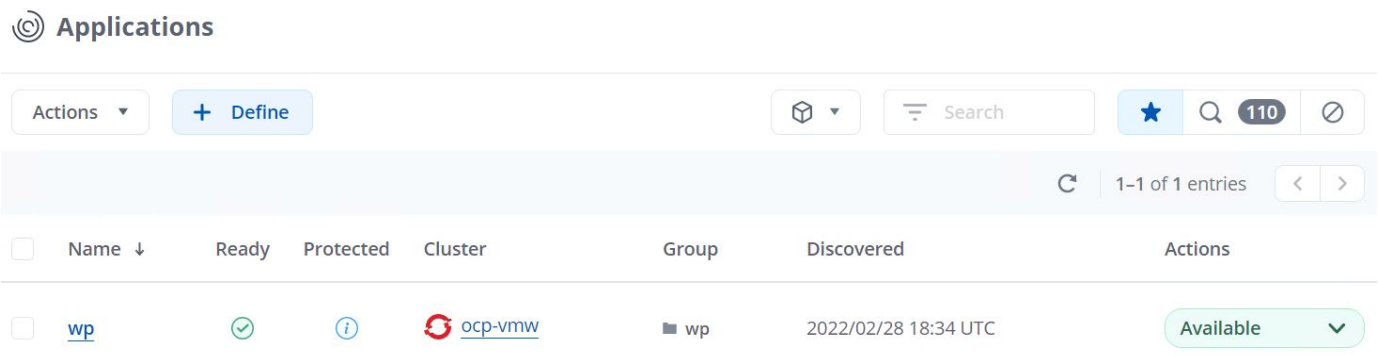
2. Immettere il nome dello spazio dei nomi di ripristino, selezionare il cluster in cui si desidera ripristinarlo e scegliere se si desidera ripristinarlo da uno snapshot esistente o da un backup dell’applicazione. Fare clic su Avanti.



3. Nel riquadro di revisione, immettere `restore` E fare clic su Restore (Ripristina) dopo aver esaminato i dettagli.



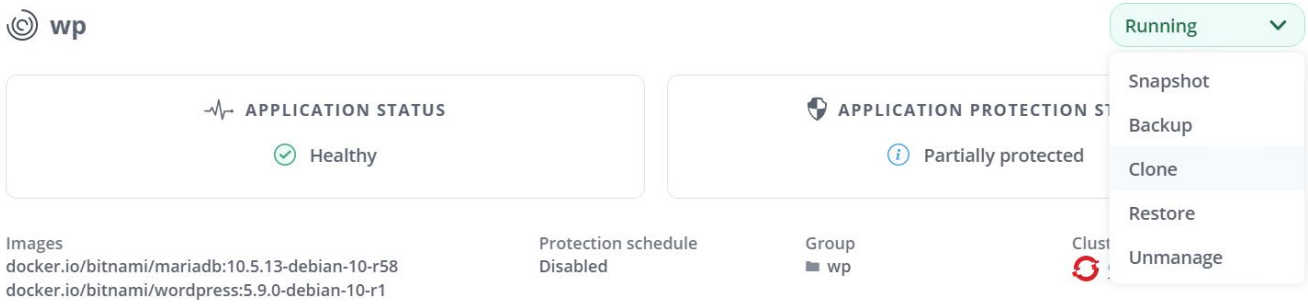
4. La nuova applicazione passa allo stato di ripristino mentre Astra Control Center ripristina l'applicazione sul cluster selezionato. Una volta installate e rilevate tutte le risorse dell'applicazione da Astra, l'applicazione passa allo stato Available (disponibile).



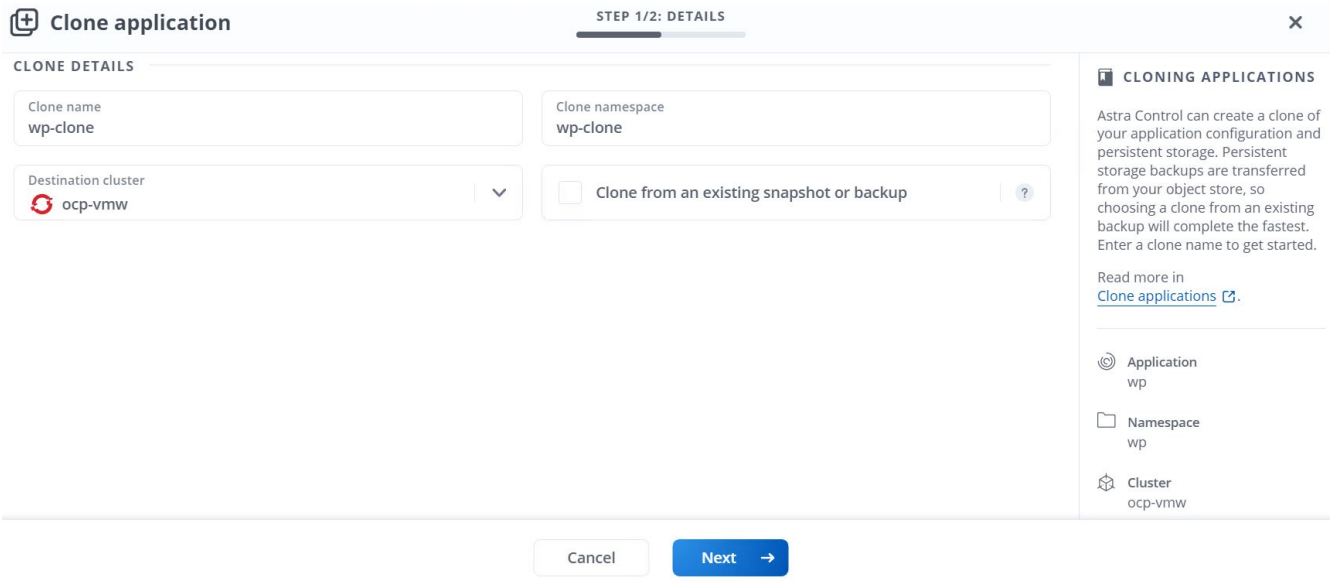
Clonare un'applicazione

È possibile clonare un'applicazione nel cluster di origine o in un cluster remoto per scopi di sviluppo/test o protezione dell'applicazione e disaster recovery. La clonazione di un'applicazione all'interno dello stesso cluster sullo stesso backend di storage utilizza la tecnologia NetApp FlexClone, che clona i PVC all'istante e consente di risparmiare spazio di storage.

1. Per clonare un'applicazione, accedere alla scheda applicazioni > gestite e fare clic sull'applicazione in questione. Fare clic sul menu a discesa accanto al nome dell'applicazione e fare clic su Clone (Clona).



2. Immettere i dettagli del nuovo spazio dei nomi, selezionare il cluster in cui si desidera clonarlo e scegliere se clonarlo da uno snapshot esistente o da un backup o dallo stato corrente dell'applicazione. Quindi, fare clic su Next (Avanti) e su Clone on review pane (Clona sul pannello di revisione) dopo aver esaminato i dettagli.



3. La nuova applicazione passa allo stato di rilevamento mentre Astra Control Center crea l'applicazione sul cluster selezionato. Una volta installate e rilevate tutte le risorse dell'applicazione da Astra, l'applicazione passa allo stato Available (disponibile).