Panoramica delle integrazioni di storage NetApp

NetApp Solutions

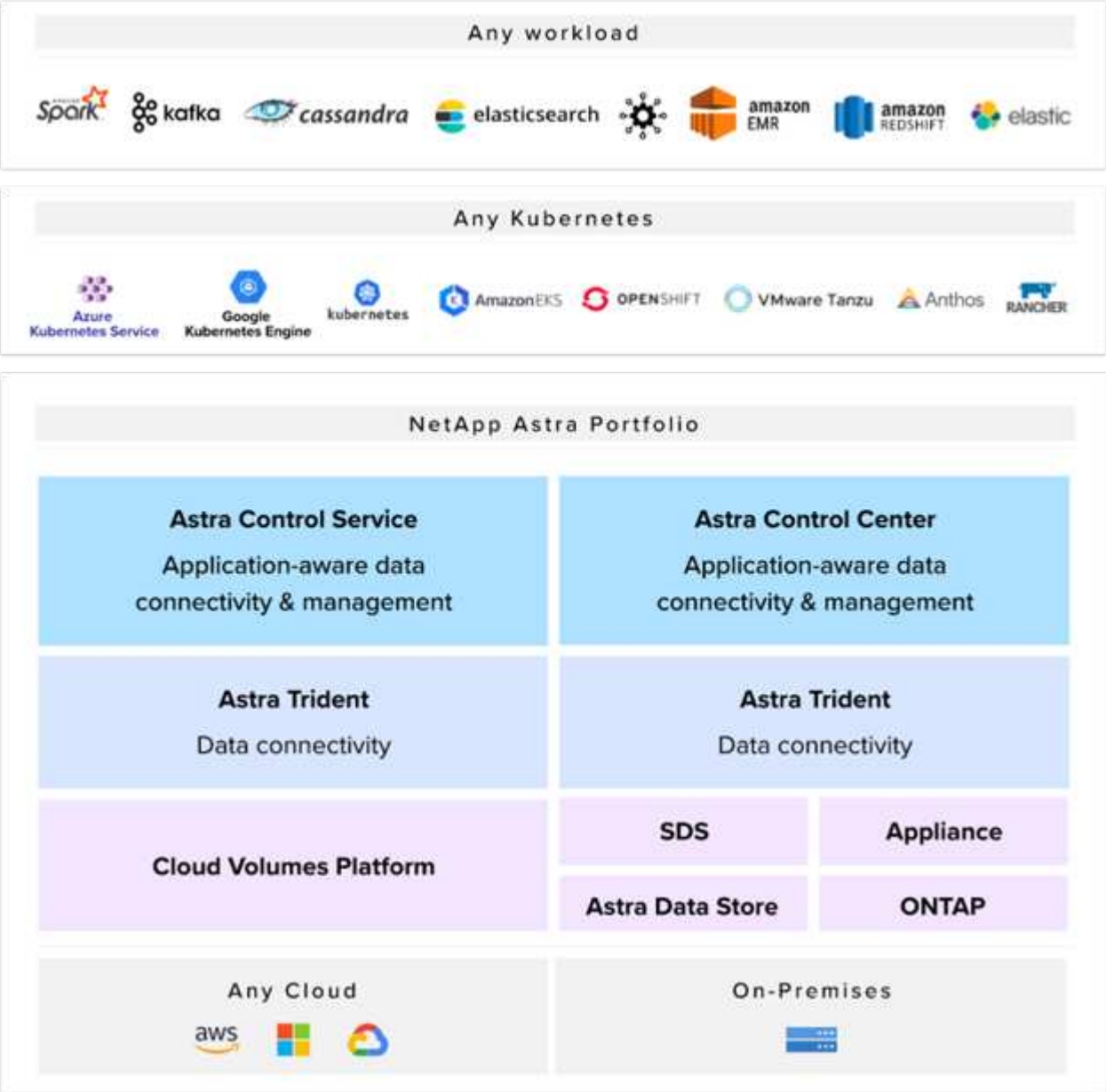
NetApp
September 10, 2024

Sommario

Panoramica sull’integrazione dello storage NetApp

```
NetApp provides a number of products which assist our customers with
orchestrating and managing persistent data in container based
environments.
```

NetApp offre una serie di prodotti che consentono di orchestrare, gestire, proteggere e migrare le applicazioni stateful containerizzate e i relativi dati.



NetApp Astra Control offre un set completo di servizi di gestione dei dati application-aware e storage per carichi di lavoro Kubernetes stateful basati sulla tecnologia di protezione dei dati di NetApp. Astra Control Service è disponibile per supportare carichi di lavoro stateful nelle implementazioni Kubernetes native nel cloud. Astra Control Center è disponibile per supportare carichi di lavoro stateful in implementazioni on-

premise di piattaforme Enterprise Kubernetes come Red Hat OpenShift, Rancher, VMware Tanzu etc. Per ulteriori informazioni, visita il sito Web di NetApp Astra Control "qui".

NetApp Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes come Red Hat OpenShift, Rancher, VMware Tanzu etc. Per ulteriori informazioni, visita il sito web di Astra Trident "qui".

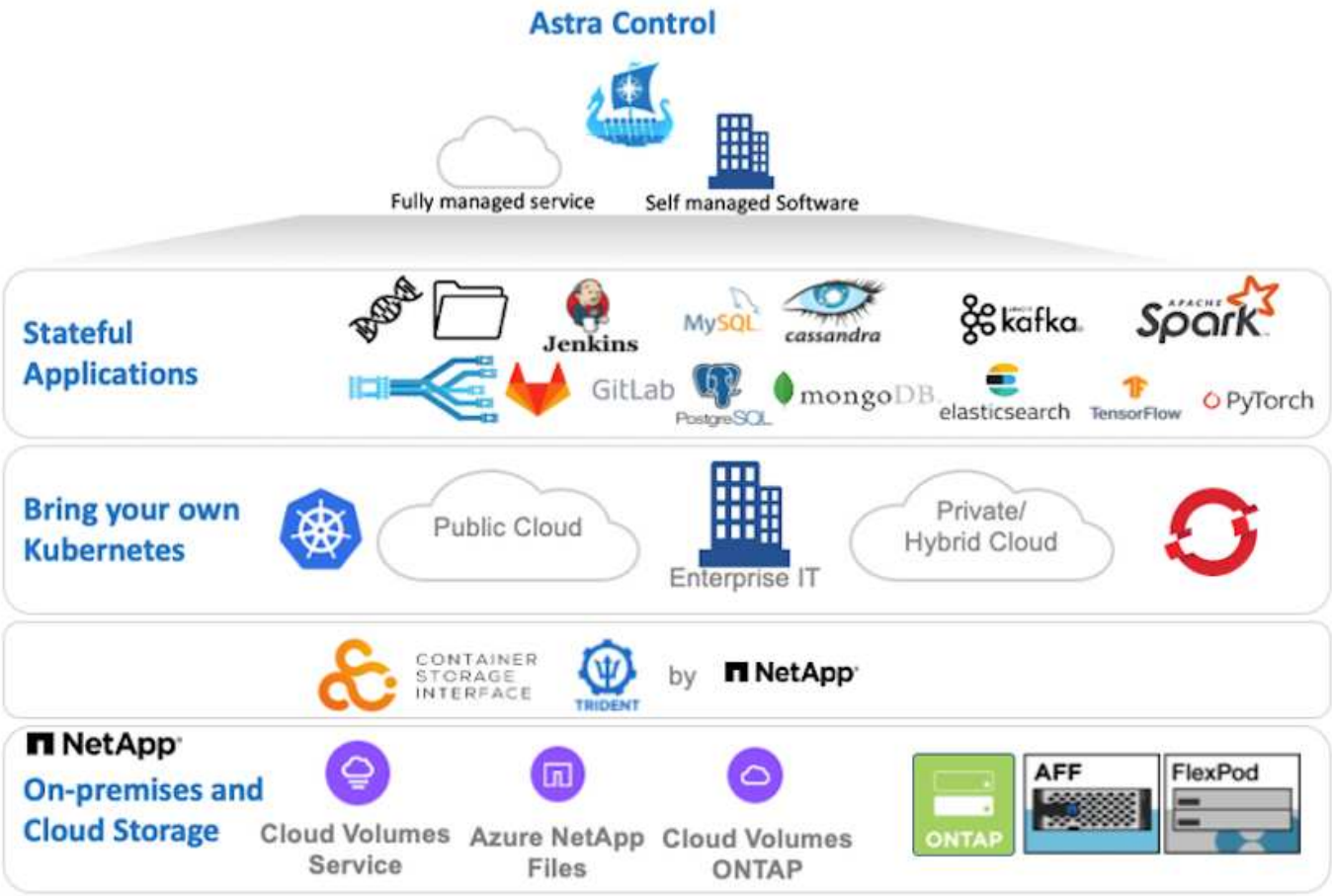
Le pagine seguenti contengono informazioni aggiuntive sui prodotti NetApp validati per la gestione delle applicazioni e dello storage persistente nella soluzione VMware Tanzu with NetApp:

- "NetApp Astra Control Center"
- "NetApp Astra Trident"

Panoramica di NetApp Astra Control

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

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.



NetApp Astra Control Center può essere installato su un cluster VMware Tanzu che ha installato e configurato Astra Trident Storage orchestrator con classi di storage e backend di storage per i sistemi storage NetApp

ONTAP.

Per ulteriori informazioni su Astra Trident, 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 (per un valore di sette giorni di metriche) ed esportate negli strumenti di monitoraggio nativi di Kubernetes (Prometheus e Grafana) attraverso endpoint di metriche aperte.

Astra Control Center è completamente integrato nell'ecosistema di consulente digitale di NetApp AutoSupport e Active IQ (detto anche Digital Advisor) per fornire supporto agli utenti, fornire assistenza nella risoluzione dei problemi e visualizzare statistiche di utilizzo.

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

Per ulteriori informazioni sul portfolio Astra, visitare il "Sito web Astra".

Automazione di Astra Control Center

Astra Control Center dispone di un'API REST completamente funzionale per l'accesso programmatico. Gli utenti possono utilizzare qualsiasi linguaggio di programmazione o utility per interagire con gli endpoint API REST di Astra Control. Per ulteriori informazioni su questa API, consultare la documentazione "qui".

Se stai cercando un toolkit di sviluppo software pronto per interagire con le API REST di Astra Control, NetApp fornisce un toolkit con l'SDK di Astra Control Python che puoi scaricare "qui".

Se la programmazione non è adatta alla situazione e si desidera utilizzare uno strumento di gestione della configurazione, è possibile clonare ed eseguire i playbook Ansible pubblicati da NetApp "qui".

Prerequisiti per l'installazione di Astra Control Center

L'installazione di Astra Control Center richiede i seguenti prerequisiti:

- Uno o più cluster Tanzu Kubernetes, gestiti da un cluster di gestione o da TKGS o TKGI. Sono supportati i cluster di workload TKG 1.4+ e i cluster di utenti TKGI 1.12.2+.
- Astra Trident deve essere già installato e configurato su ciascuno dei cluster Tanzu Kubernetes.
- Uno o più sistemi storage NetApp ONTAP con ONTAP 9.5 o superiore.

> È consigliabile che ogni Tanzu Kubernetes installato in un sito disponga di una SVM dedicata per lo storage persistente. Le implementazioni multi-sito richiedono sistemi storage aggiuntivi.

- È necessario configurare un backend di storage Trident su ogni cluster Tanzu Kubernetes con una SVM supportata da un cluster ONTAP.
- Un StorageClass predefinito configurato su ciascun cluster Tanzu Kubernetes con Astra Trident come provisioning dello storage.
- È necessario installare e configurare un bilanciamento del carico su ciascun cluster Tanzu Kubernetes per il bilanciamento del carico e l'esposizione di Astra Control Center se si utilizza ingressType `AccTraefik`.

- È necessario installare e configurare un controller di ingresso su ciascun cluster Tanzu Kubernetes per esporre Astra Control Center se si utilizza ingressType `Generic`.
- È necessario configurare un registro di immagini privato per ospitare le immagini di NetApp Astra Control Center.
- È necessario disporre dell'accesso Cluster Admin al cluster Tanzu Kubernetes in cui viene installato Astra Control Center.
- È necessario disporre dell'accesso come amministratore ai cluster NetApp ONTAP.
- Una workstation di amministrazione RHEL o Ubuntu.

Installare Astra Control Center

Questa soluzione descrive una procedura automatica per l'installazione di Astra Control Center utilizzando i playbook Ansible. Se si sta cercando una procedura manuale per installare Astra Control Center, seguire la guida dettagliata all'installazione e alle operazioni "qui".

1. Per utilizzare i playbook Ansible che implementano Astra Control Center, è necessario disporre di 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. 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.

> 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 all'utente o al cluster del carico di lavoro Tanzu Kubernetes 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` archiviare e compilare 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.

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

   ```
   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 e 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 ~]$ kubectl get all -n netapp-astra-cc
   ```

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

   ```
   [netapp-user@rhel7 ~]$ kubectl 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.AstraControl
lCenter","msg":"Successfully Reconciled AstraControlCenter in
[seconds]s","AstraControlCenter":"netapp-astra-
cc/astra","ae.Version":"[22.04.0]"}
```

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
```

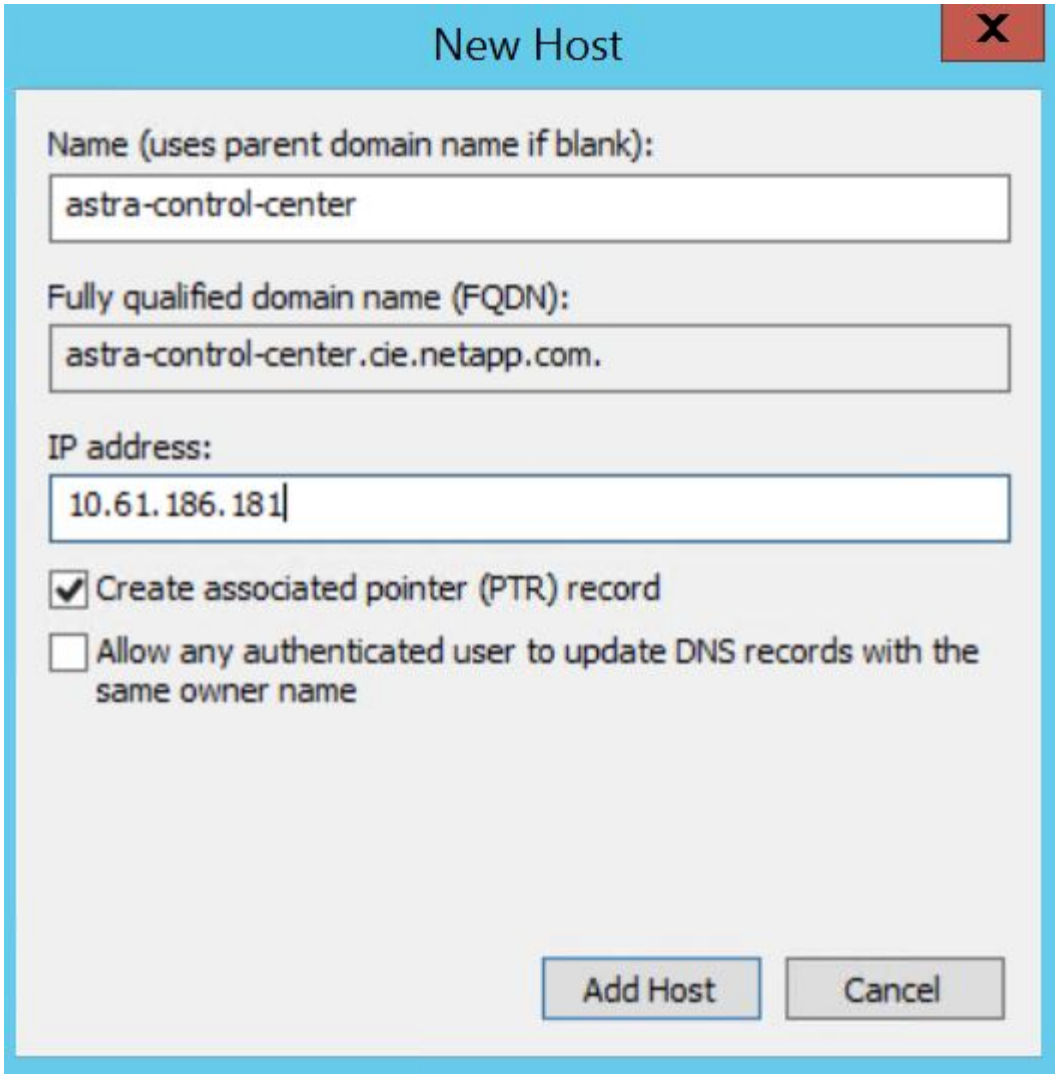
In questo esempio, la password è `ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f`.

4. Ottenere l'IP del bilanciamento del carico del servizio traefik se il tipo di entressType è AccTraefik.

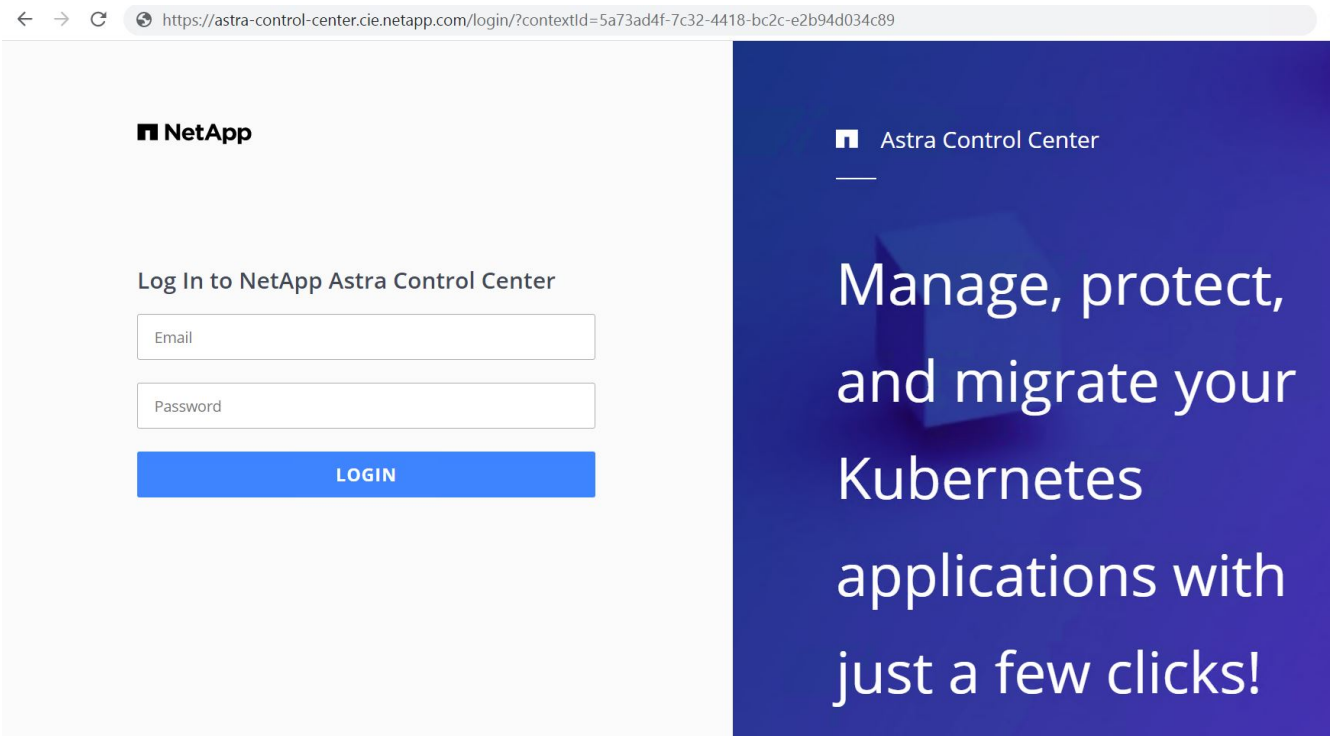
```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep
'EXTERNAL|traefik'

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
```

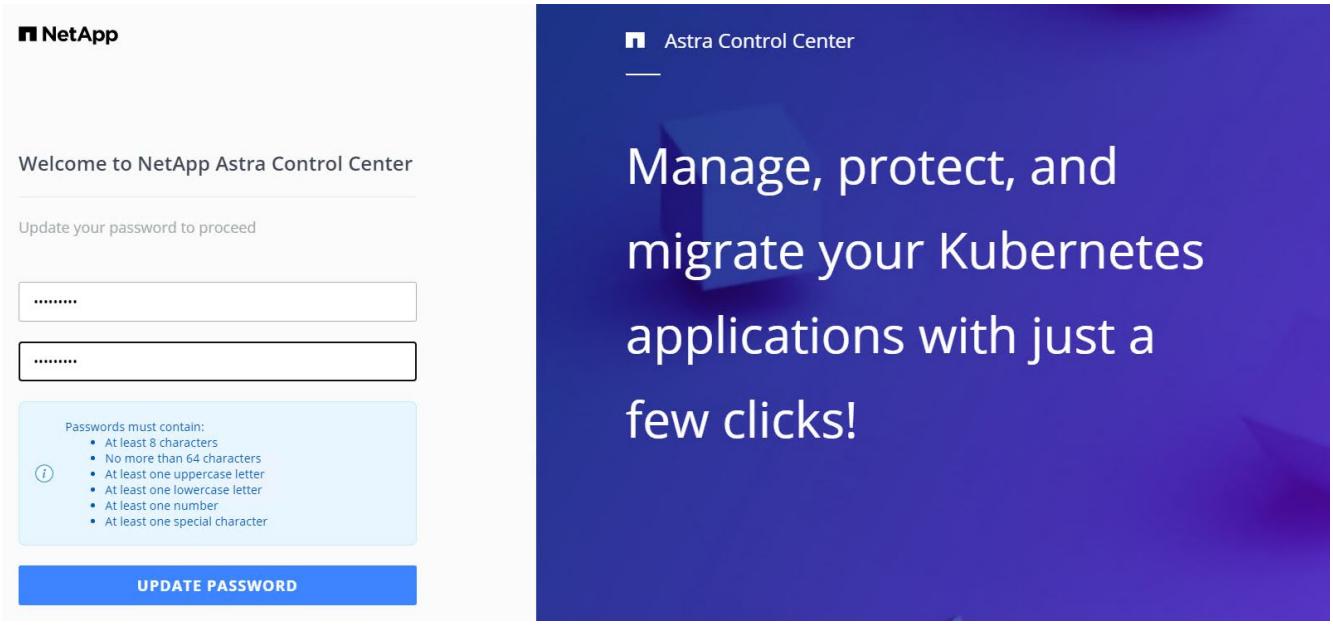
5. Aggiungere una voce nel server DNS che punta all'FQDN fornito nel file CRD di Astra Control Center `EXTERNAL-IP` del servizio traefik.



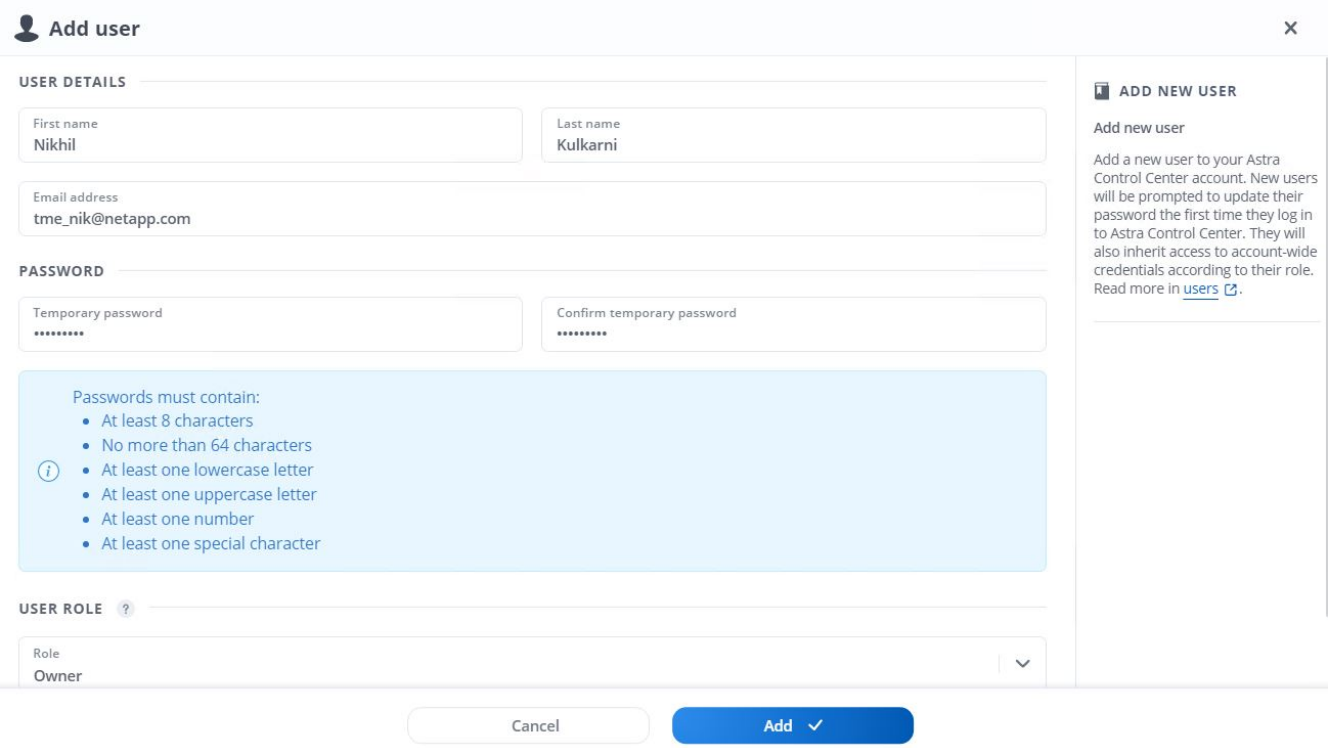
6. Accedere alla GUI di Astra Control Center esplorando il relativo FQDN.



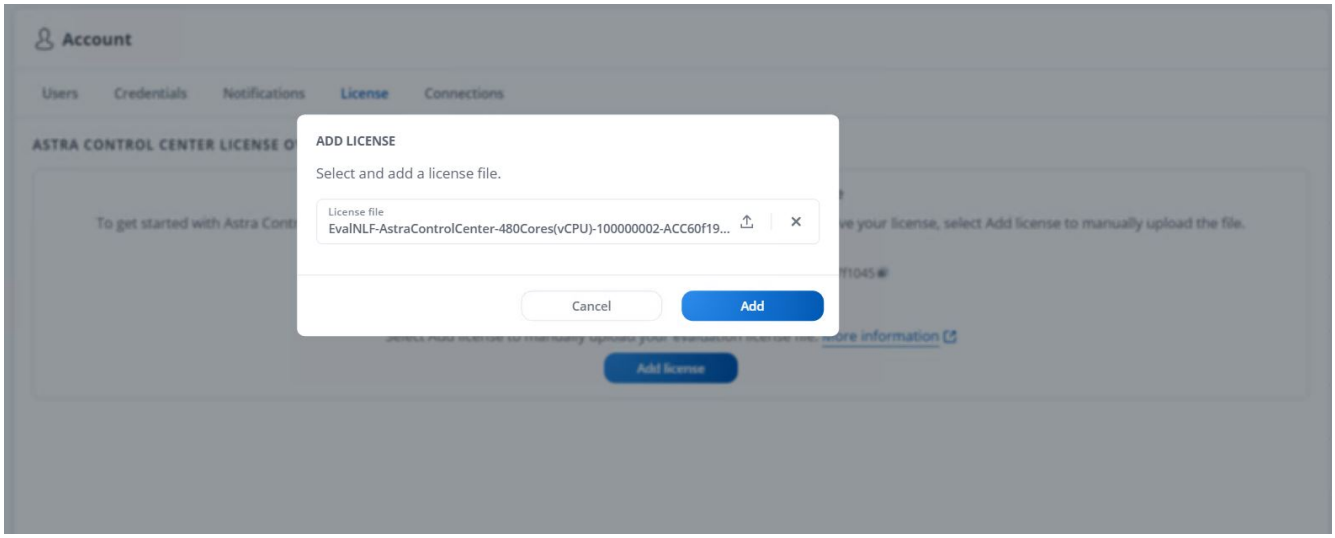
7. Quando si accede all'interfaccia grafica di Astra Control Center per la prima volta utilizzando l'indirizzo email admin fornito in CRD, è necessario modificare la password.



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 sue funzionalità. Per aggiungere una licenza, accedere a account > License (account > licenza), fare clic su Add License (Aggiungi licenza) e caricare il file di licenza.



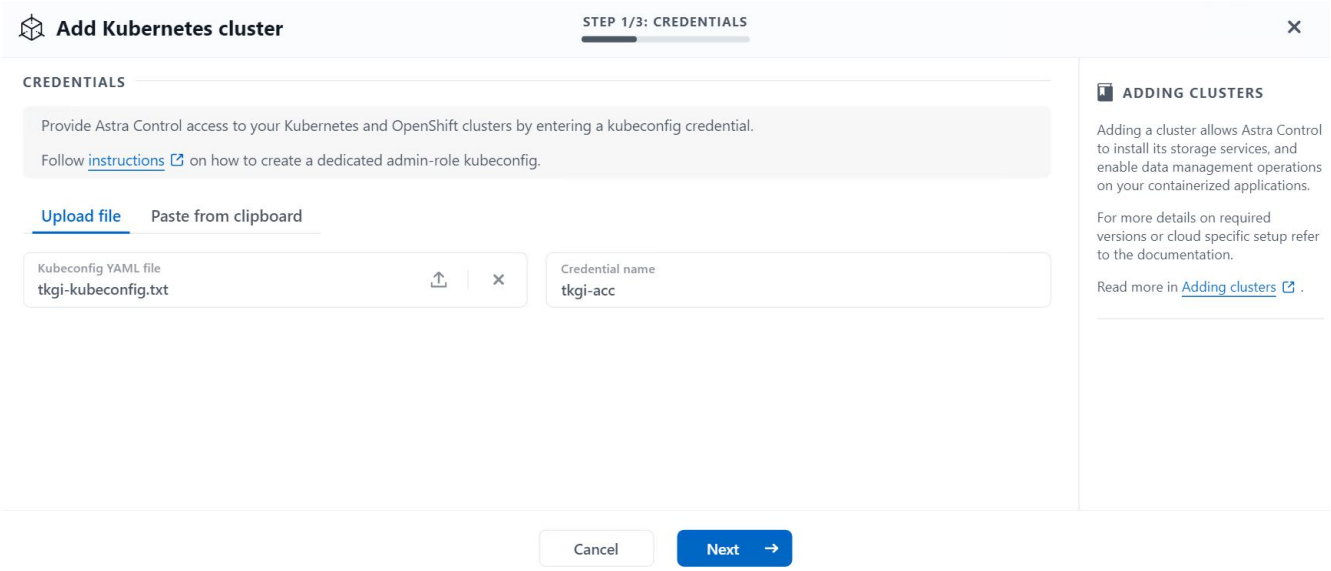
In caso di problemi con l'installazione o la configurazione di NetApp Astra Control Center, è disponibile la knowledge base dei problemi noti "qui".

Registra i tuoi cluster VMware Tanzu Kubernetes con Astra Control Center

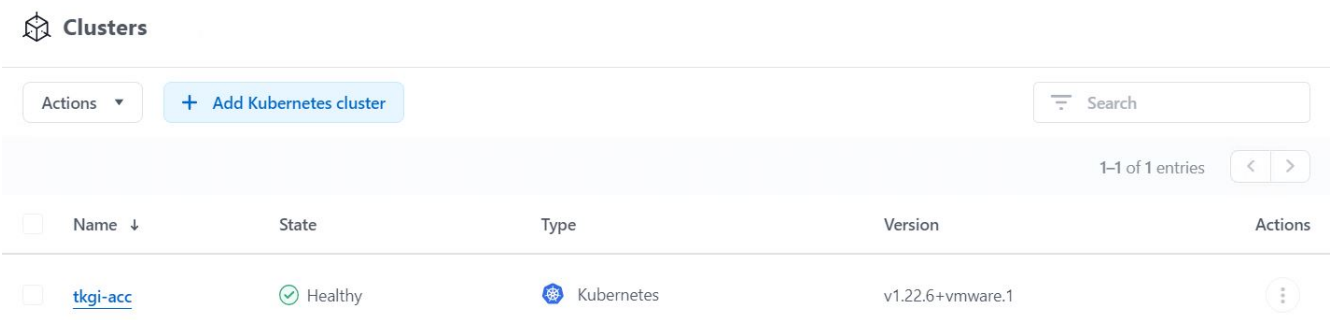
Per consentire ad Astra Control Center di gestire i carichi di lavoro, devi prima registrare i cluster Tanzu Kubernetes.

Registrare i cluster VMware Tanzu Kubernetes

1. Il primo passo consiste nell'aggiungere i cluster Tanzu Kubernetes 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 Tanzu Kubernetes e fare clic su Select Storage (Seleziona storage).



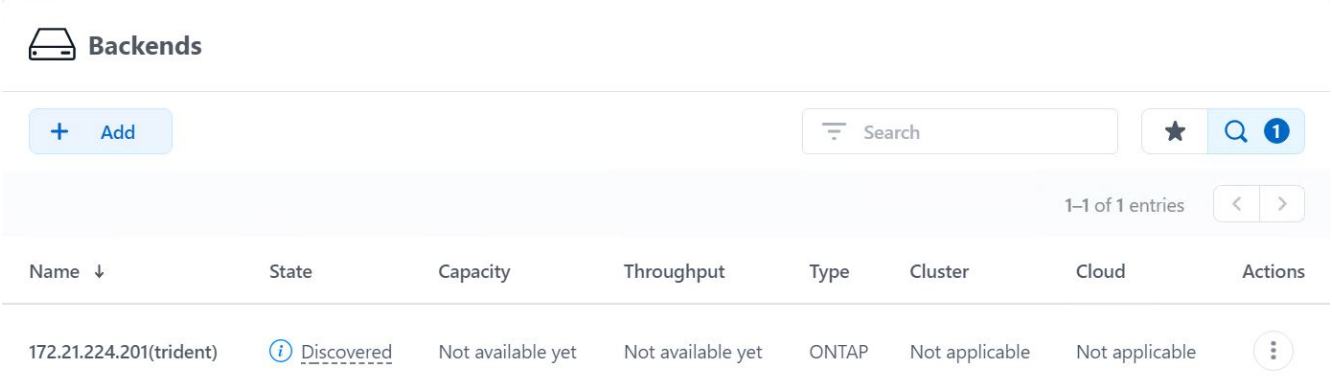
2. Astra Control Center rileva le classi di storage idonee. Selezionare ora il modo in cui lo storageclass effettua il provisioning dei volumi utilizzando Trident supportato da una SVM su NetApp ONTAP e fare clic su Review (esamina). Nel riquadro successivo, verificare i dettagli e fare clic su Add Cluster (Aggiungi cluster).
3. Una volta aggiunto, il cluster passa allo stato di rilevamento mentre Astra Control Center lo ispeziona e installa gli agenti necessari. Lo stato del cluster diventa `Healthy` una volta completata la registrazione.



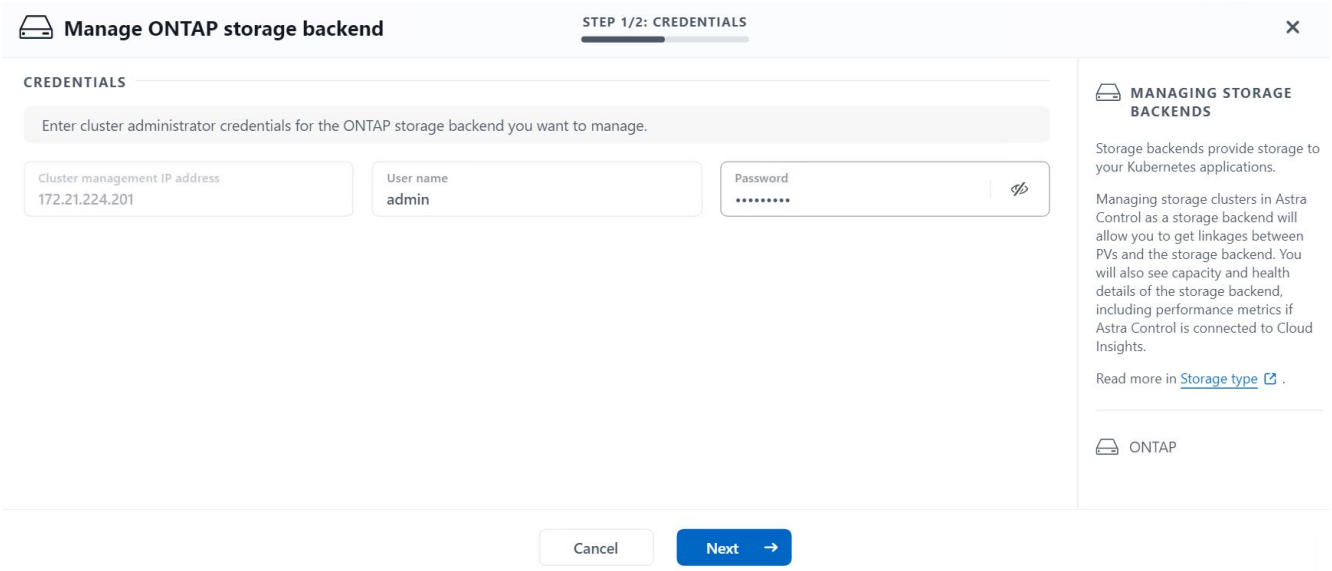
> Tutti i cluster di Tanzu Kubernetes gestiti da Astra Control Center devono avere accesso al registro delle immagini utilizzato per l'installazione, poiché gli agenti installati sui cluster gestiti estraggono le immagini da tale registro.

4. Importa i cluster ONTAP come risorse storage da gestire come back-end dal centro di controllo Astra. Quando i cluster Tanzu Kubernetes vengono aggiunti ad Astra e viene configurato uno storageclass, il cluster ONTAP viene automaticamente scoprito e ispezionato a supporto dello storageclass, ma non viene

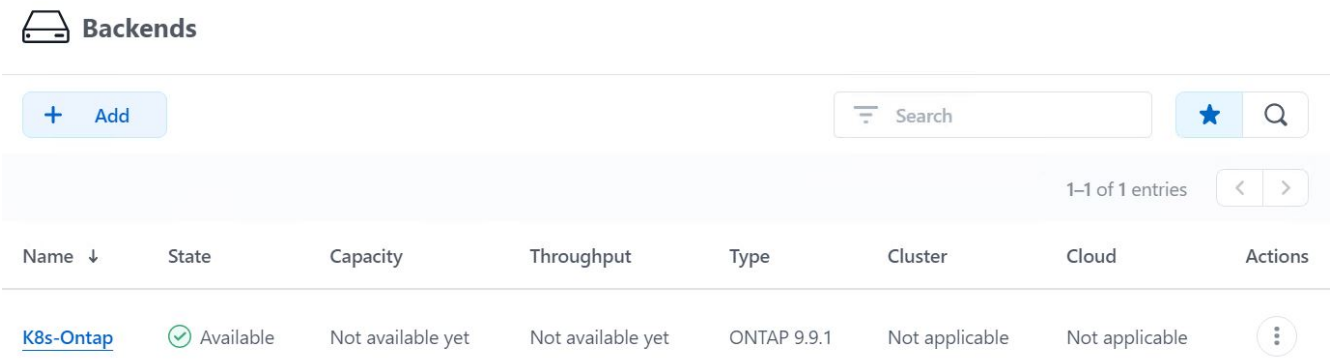
importato nel centro di controllo Astra da gestire.



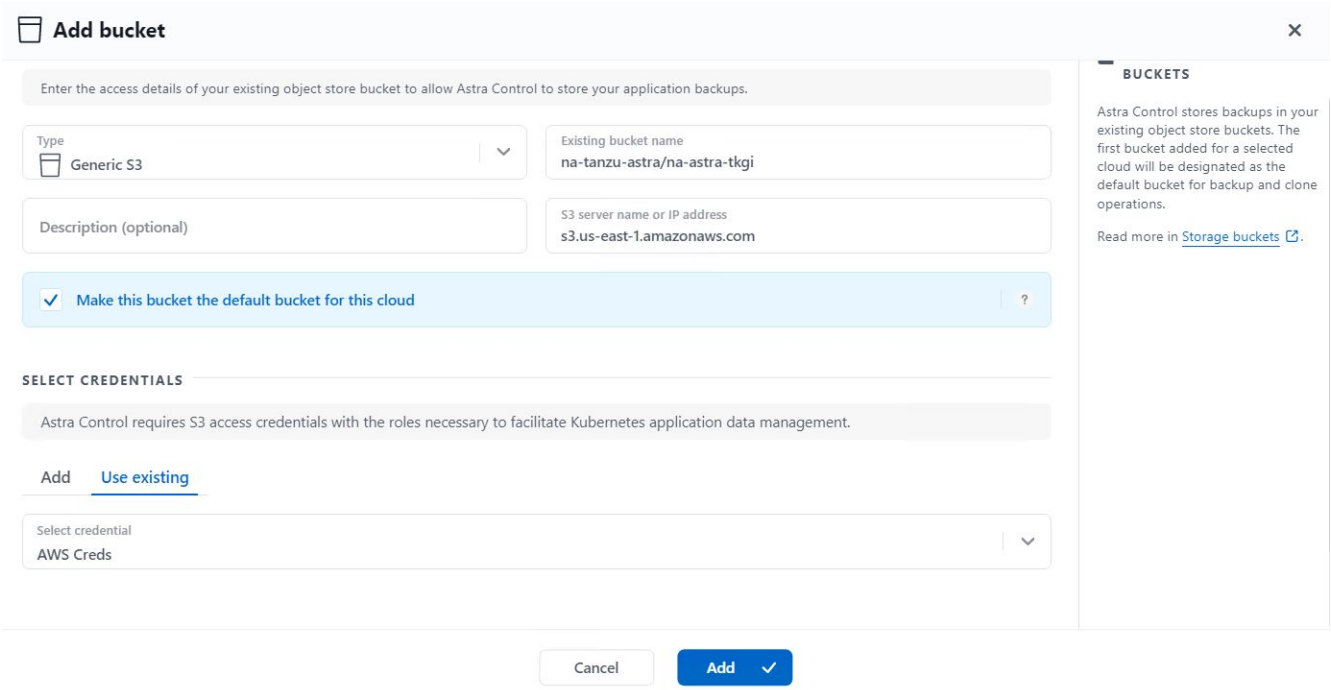
5. Per importare i cluster ONTAP, accedere a backend, fare clic sul menu a discesa e selezionare Manage (Gestisci) accanto al cluster ONTAP da gestire. Immettere le credenziali del cluster ONTAP, fare clic su informazioni di revisione, quindi fare clic su Importa backend storage.



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



7. Per il backup e il ripristino nei cluster Tanzu Kubernetes 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, AWS S3 e lo storage Microsoft Azure Blob. 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.

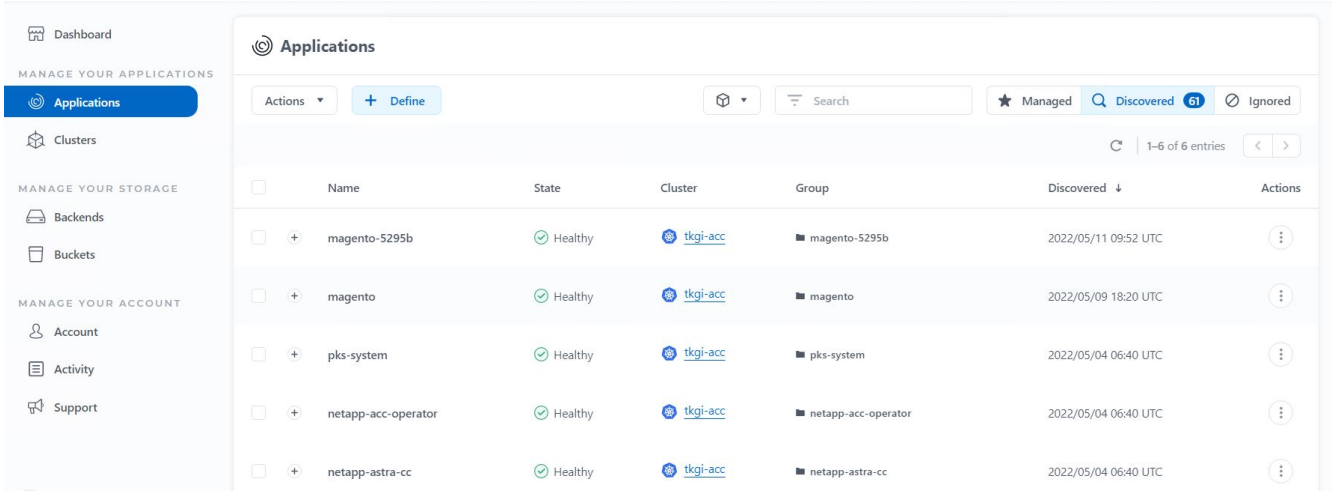


Scegliere le applicazioni da proteggere

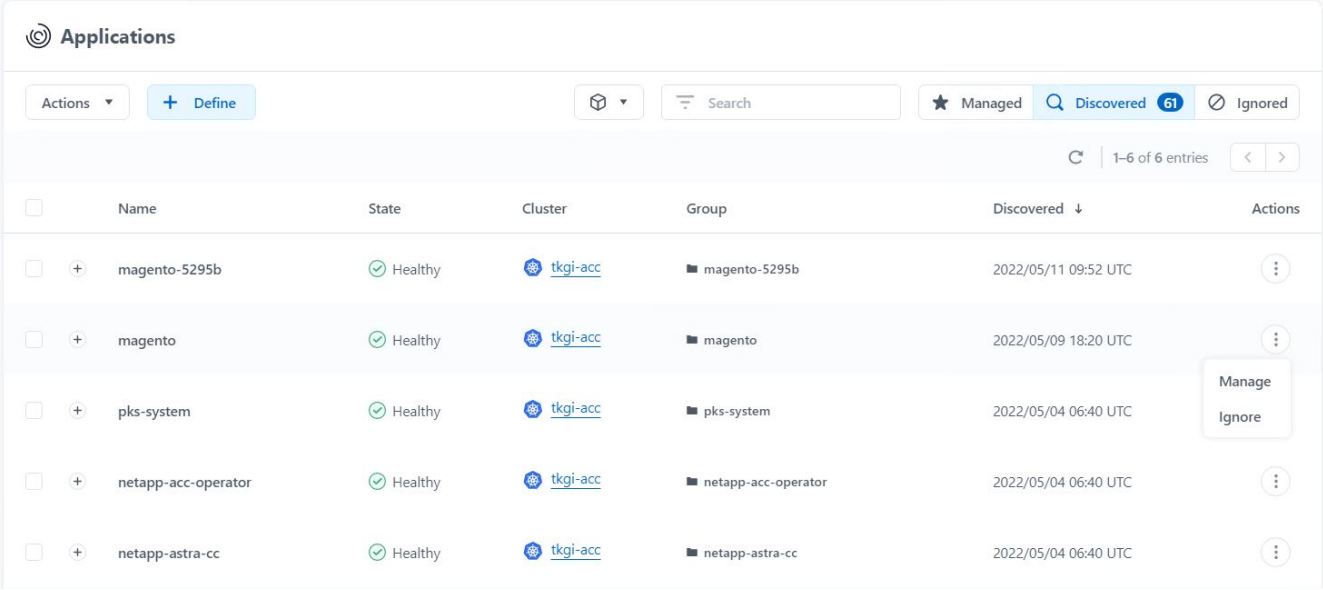
Dopo aver registrato i cluster Tanzu Kubernetes, è possibile individuare le applicazioni implementate e gestirle tramite Astra Control Center.

Gestire le applicazioni

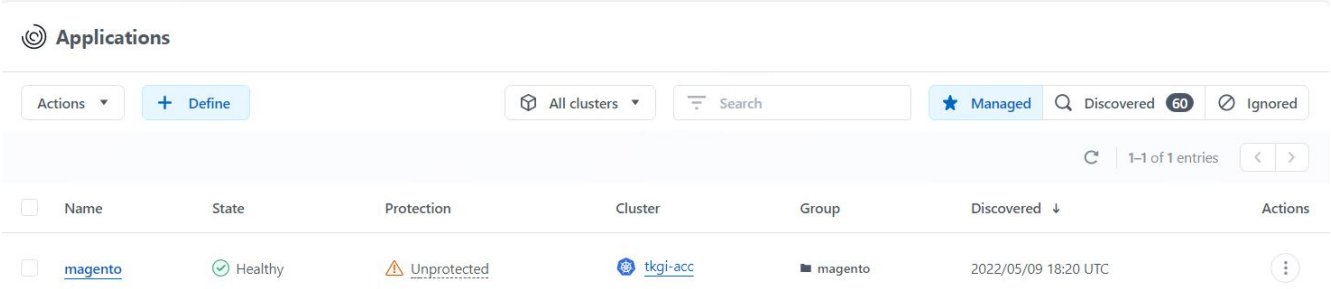
1. Una volta registrati i cluster e i backend ONTAP di Tanzu Kubernetes con il centro di controllo Astra, il centro di controllo inizia automaticamente a rilevare le applicazioni in tutti gli spazi dei nomi che utilizzano lo storageclass configurato con il backend ONTAP specificato.



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)



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



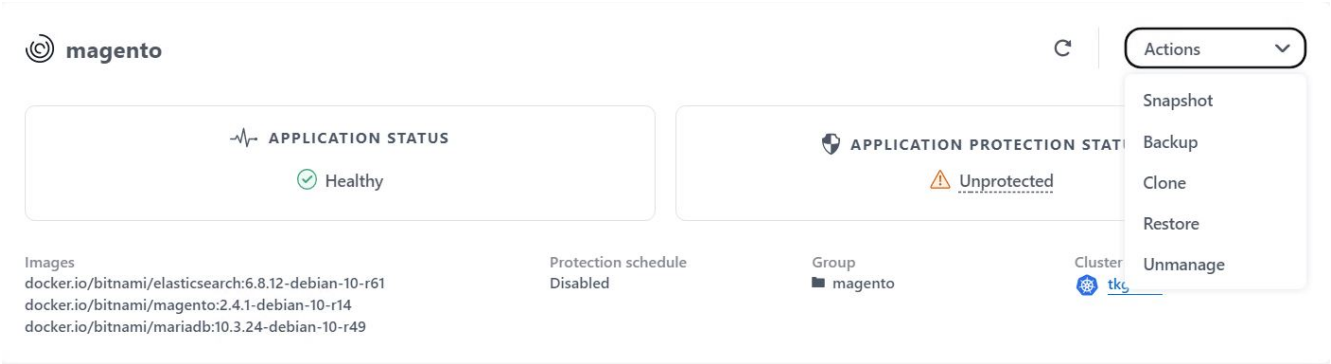
Proteggi le tue applicazioni

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.

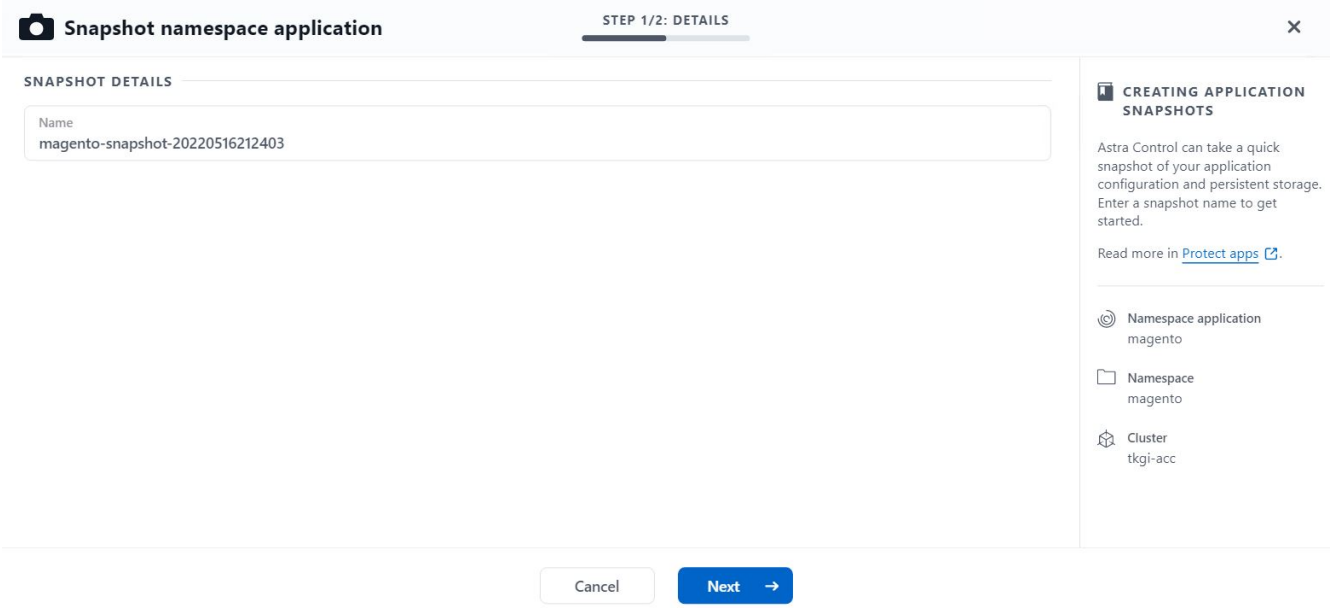
Creare un'istantanea dell'applicazione

Un'istantanea di un'applicazione crea una copia Snapshot di ONTAP e una copia dei metadati dell'applicazione che possono essere utilizzati 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.



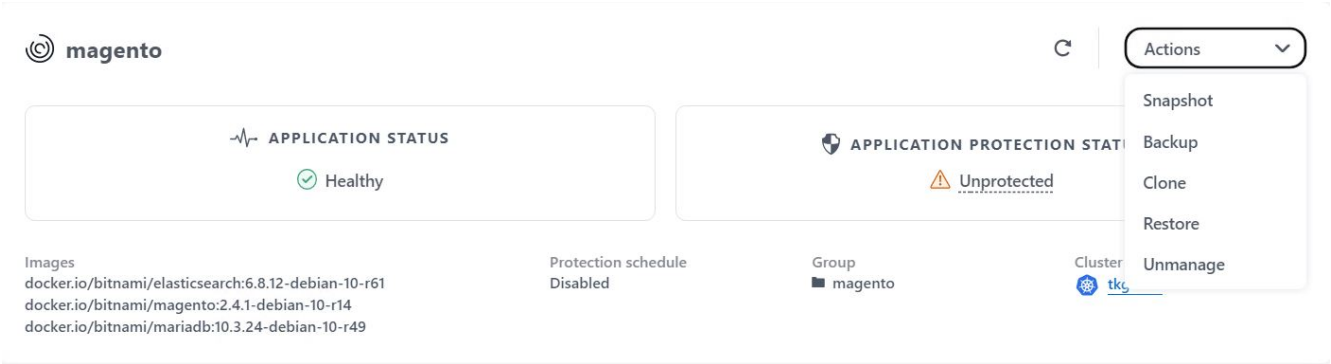
Creare un backup dell'applicazione

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.

1. 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.

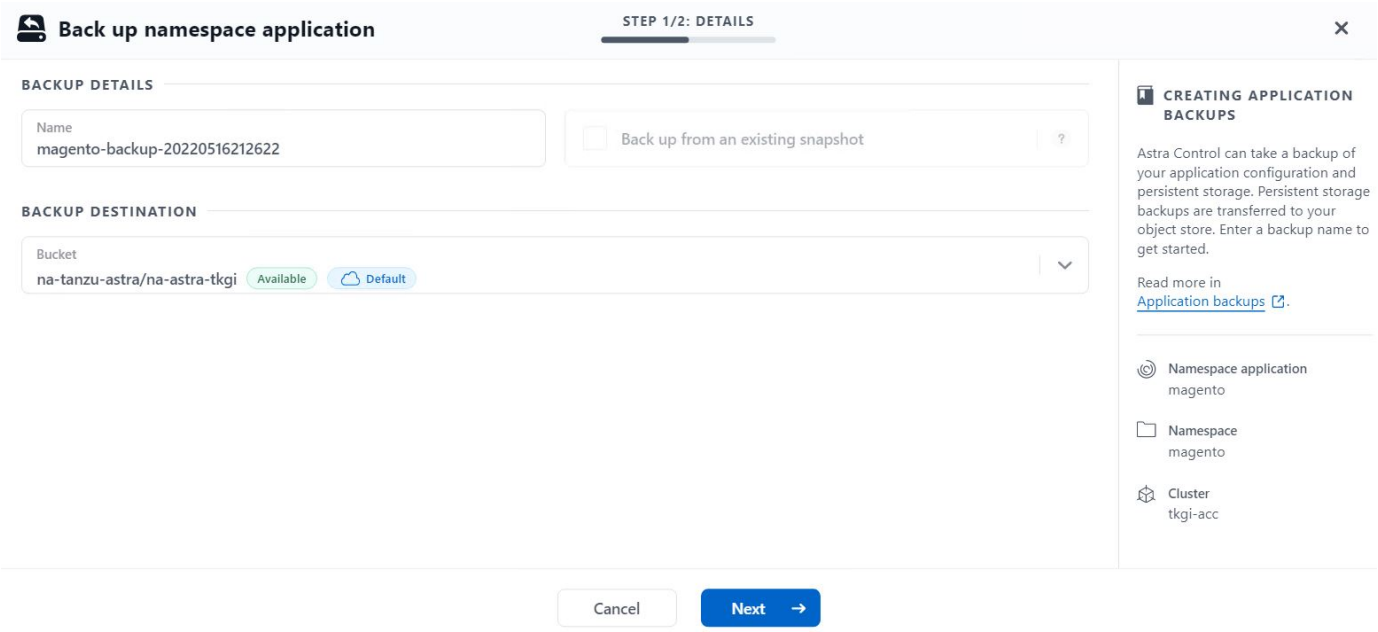
```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1
-anon 65534 -vserver ocp-trident
```

2. 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.



3. 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

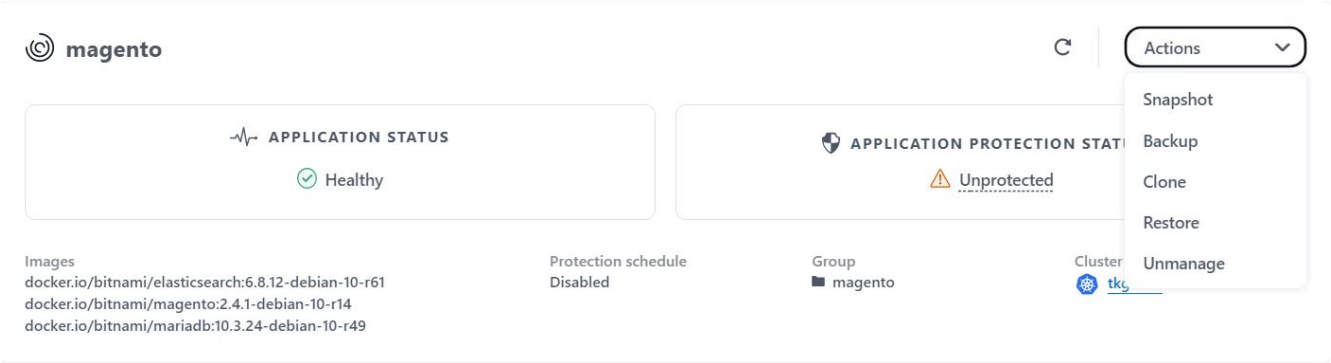
disponibile una volta completato correttamente il backup.



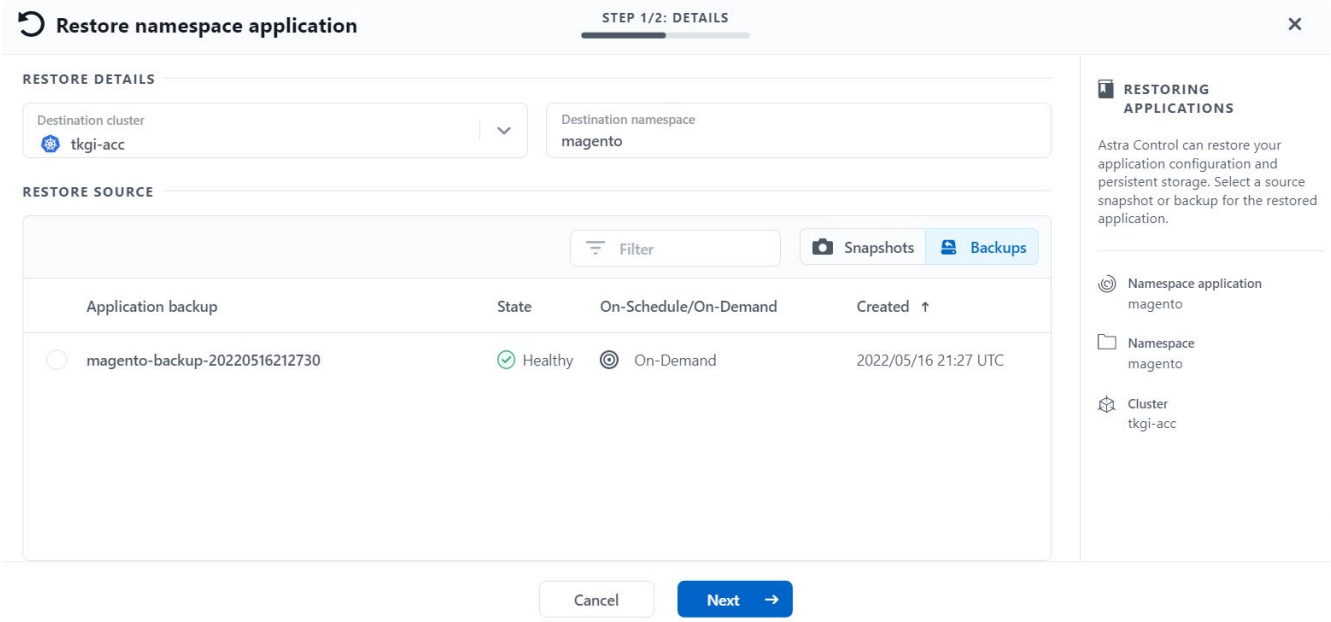
Ripristino di un’applicazione

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.

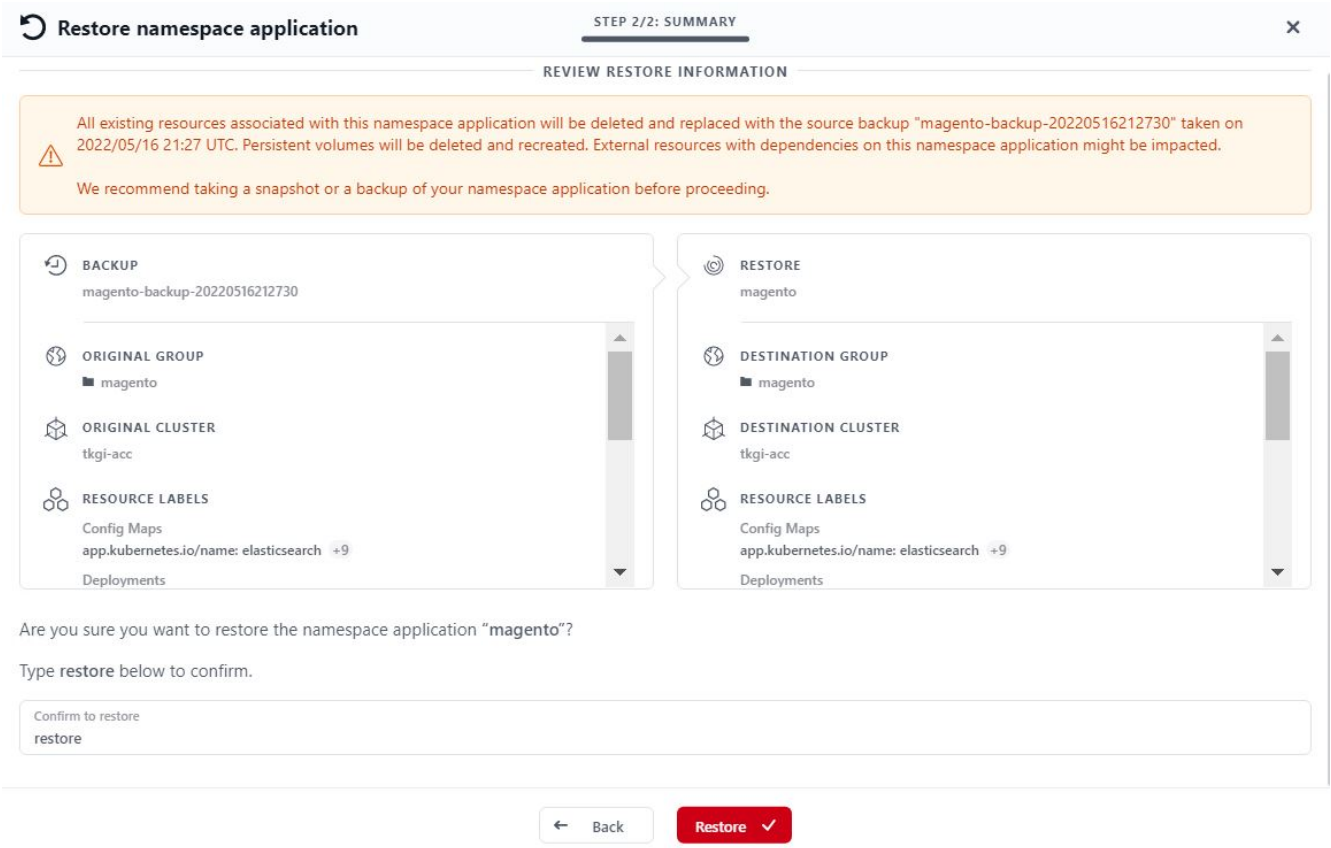
1. Per ripristinare un’applicazione, accedere alla scheda applicazioni > gestite e fare clic sull’applicazione in questione. Fare clic sul menu a discesa accanto al nome dell’applicazione e fare clic su Restore (Ripristina).



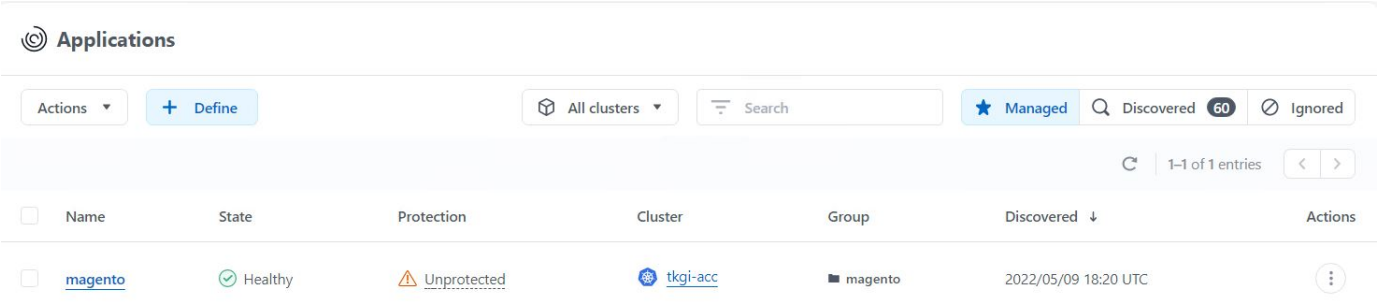
2. Immettere il nome dello spazio dei nomi di ripristino, selezionare il cluster in cui si desidera ripristinarlo e scegliere se si desidera ripristinarlo da uno snapshot esistente o da un backup dell’applicazione. Fare clic su Avanti.



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



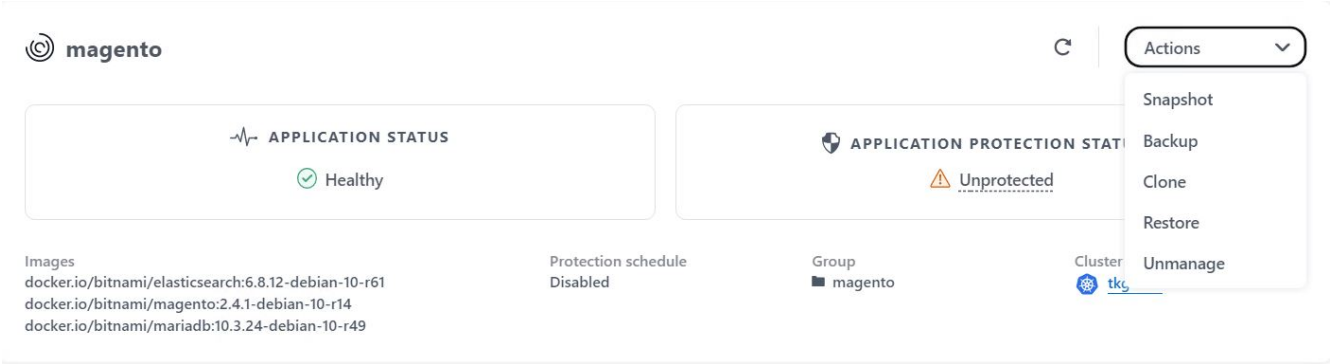
4. La nuova applicazione passa allo stato di ripristino mentre Astra Control Center ripristina l'applicazione sul cluster selezionato. Una volta installate e rilevate tutte le risorse dell'applicazione da Astra, l'applicazione passa allo stato Available (disponibile).



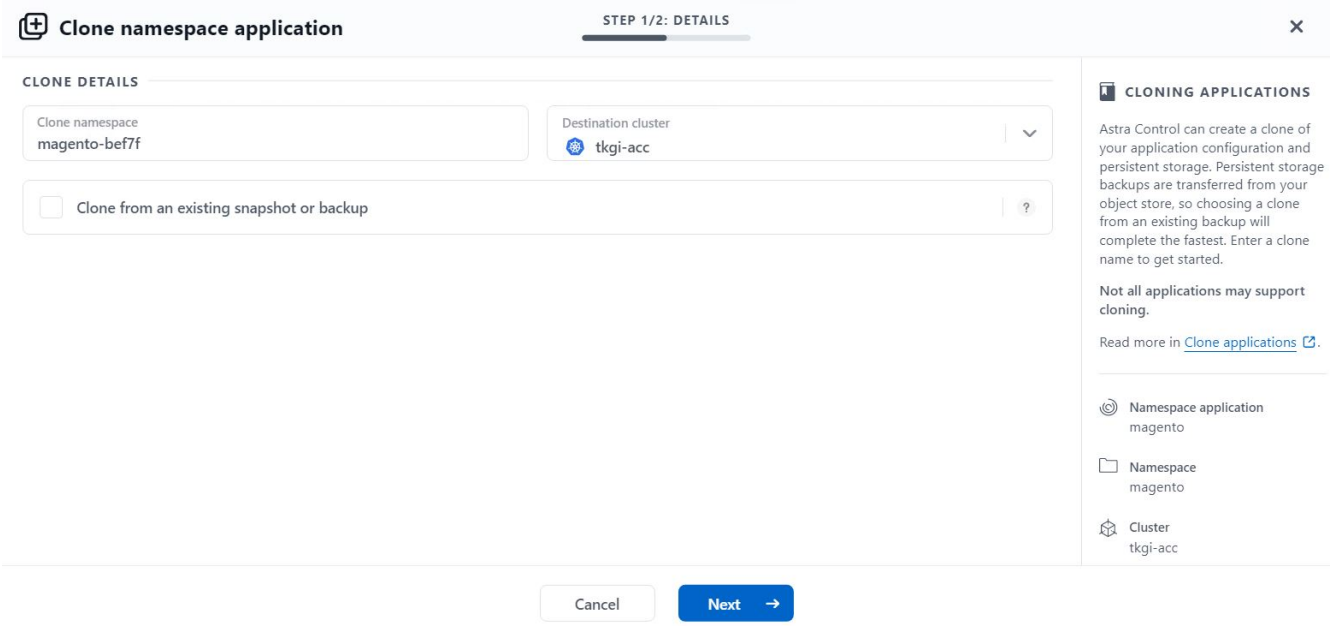
Clonare un’applicazione

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.

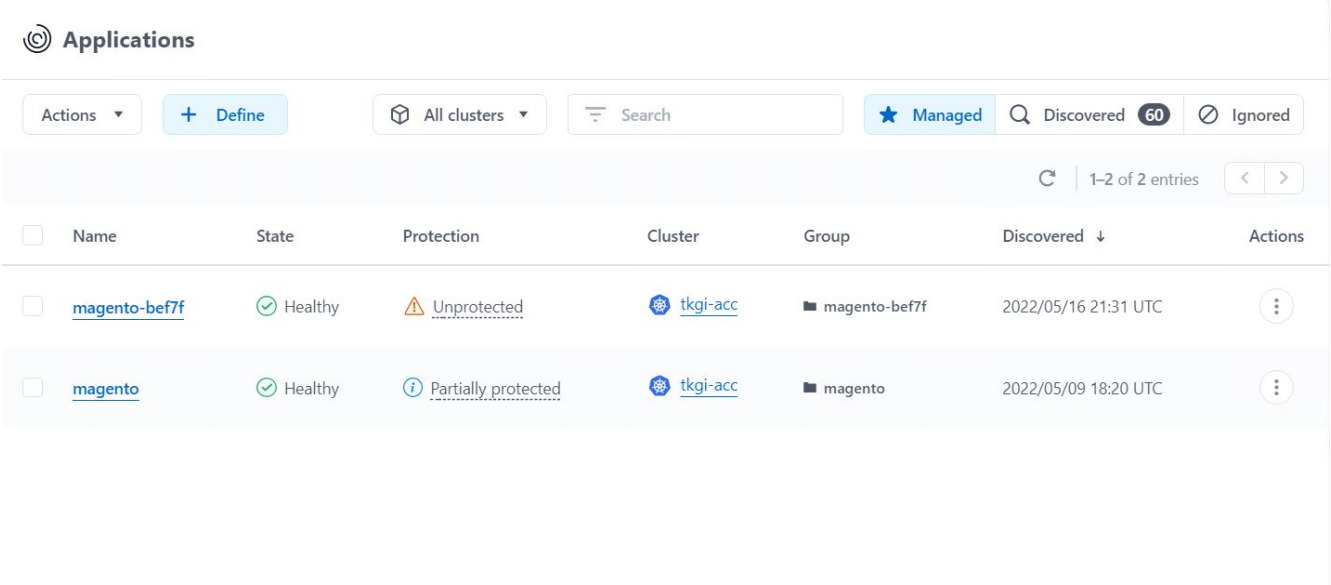
1. Per clonare un’applicazione, accedere alla scheda applicazioni > gestite e fare clic sull’applicazione in questione. Fare clic sul menu a discesa accanto al nome dell’applicazione e fare clic su Clone (Clona).



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, da un backup o dallo stato corrente dell’applicazione. Fare clic su Next (Avanti), quindi su Clone (Clona) nel riquadro 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).

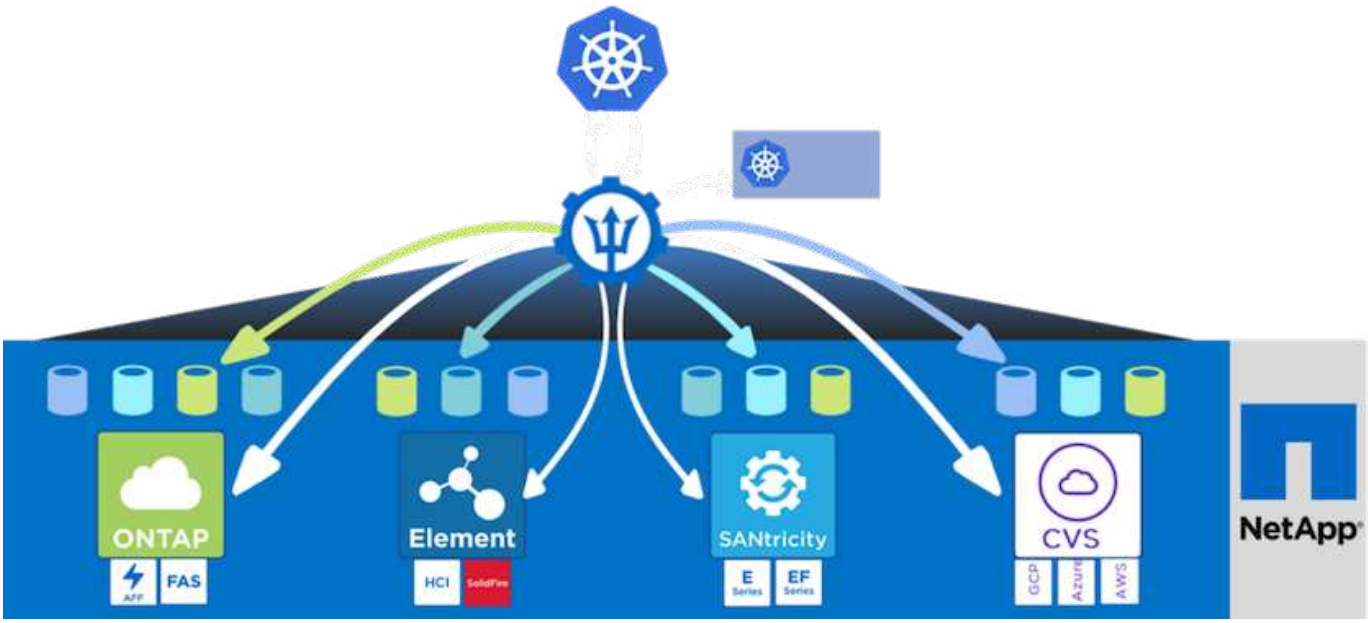


Panoramica di Astra Trident

Astra Trident è un orchestrator di storage open-source e completamente supportato per container e distribuzioni Kubernetes, tra cui VMware Tanzu.

Astra Trident è uno storage orchestrator open-source completamente supportato per container e distribuzioni Kubernetes come Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud, Rancher etc. Trident lavora con l'intero portfolio di storage NetApp, inclusi i sistemi storage NetApp ONTAP ed Element, e supporta anche connessioni NFS e iSCSI. Trident accelera il workflow DevOps consentendo agli utenti finali di eseguire il provisioning e gestire lo storage dai sistemi storage NetApp senza richiedere l'intervento di un amministratore dello storage.

Un amministratore può configurare una serie di backend di storage in base alle esigenze di progetto e ai modelli di sistemi di storage che consentono funzionalità di storage avanzate, tra cui compressione, tipi di dischi specifici o livelli di QoS che garantiscono un certo livello di performance. Una volta definiti, questi backend possono essere utilizzati dagli sviluppatori nei loro progetti per creare dichiarazioni di volume persistenti (PVC) e per collegare storage persistente ai propri container on-demand.



Astra Trident ha un rapido ciclo di sviluppo e, come Kubernetes, viene rilasciato quattro volte all'anno.

L'ultima versione di Astra Trident è la 22.04 rilasciata ad aprile 2022. Matrice di supporto per quale versione di Trident è stata testata con la quale è possibile trovare la distribuzione Kubernetes "qui".

A partire dalla versione 20.04, l'impostazione di Trident viene eseguita dall'operatore Trident. L'operatore semplifica le implementazioni su larga scala e fornisce supporto aggiuntivo, inclusa la riparazione automatica dei pod implementati nell'installazione di Trident.

Con la versione 21.01, è stato reso disponibile un grafico Helm per facilitare l'installazione dell'operatore Trident.

Implementare l'operatore Trident utilizzando Helm

1. Innanzitutto, impostare la posizione del cluster utente `kubeconfig` File come variabile di ambiente in modo da non doverla fare riferimento, perché Trident non ha alcuna opzione per passare questo file.

```
[netapp-user@rhel7]$ export KUBECONFIG=~/tanzu-install/auth/kubeconfig
```

2. Aggiungi il repository NetApp Astra Trident Helm.

```
[netapp-user@rhel7]$ helm repo add netapp-trident
https://netapp.github.io/trident-helm-chart
"netapp-trident" has been added to your repositories
```

3. Aggiornare i repository Helm.

```
[netapp-user@rhel7]$ helm repo update
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "netapp-trident" chart repository
...Successfully got an update from the "bitnami" chart repository
Update Complete. ⎈Happy Helming!⎈
```

4. Creare un nuovo namespace per l'installazione di Trident.

```
[netapp-user@rhel7]$ kubetcl create ns trident
```

5. Crea un segreto con le credenziali DockerHub per scaricare le immagini di Astra Trident.

```
[netapp-user@rhel7]$ kubectl create secret docker-registry docker-
registry-cred --docker-server=docker.io --docker-username=netapp
-solutions-tme --docker-password=xxxxxx -n trident
```

6. Per i cluster di utenti o carichi di lavoro gestiti da TKGS (vSphere con Tanzu) o TKG con implementazioni di cluster di gestione, completare la seguente procedura per installare Astra Trident:
   a. Assicurarsi che l'utente che ha effettuato l'accesso disponga delle autorizzazioni necessarie per creare account di servizio nello spazio dei nomi Trident e che gli account di servizio nello spazio dei nomi Trident dispongano delle autorizzazioni necessarie per creare pod.
   b. Eseguire il seguente comando helm per installare l'operatore Trident nello spazio dei nomi creato.

```
[netapp-user@rhel7]$ helm install trident netapp-trident/trident-
operator -n trident --set imagePullSecrets[0]=docker-registry-cred
```

7. Per un cluster di utenti o workload gestito dalle implementazioni TKGI, eseguire il seguente comando helm per installare l'operatore Trident nello spazio dei nomi creato.

```
[netapp-user@rhel7]$ helm install trident netapp-trident/trident-
operator -n trident --set imagePullSecrets[0]=docker-registry-
cred,kubeletDir="/var/vcap/data/kubelet"
```

8. Verificare che i pod Trident siano in funzione.

```
NAME                                READY   STATUS    RESTARTS
AGE
trident-csi-6vv62                   2/2     Running   0
14m
trident-csi-cfd844bcc-sqhcg         6/6     Running   0
12m
trident-csi-dfcmz                   2/2     Running   0
14m
trident-csi-pb2n7                   2/2     Running   0
14m
trident-csi-qsw6z                   2/2     Running   0
14m
trident-operator-67c94c4768-xw978   1/1     Running   0
14m

[netapp-user@rhel7]$ ./tridentctl -n trident version
+----------------+----------------+
| SERVER VERSION | CLIENT VERSION |
+----------------+----------------+
| 22.04.0          | 22.04.0          |
+----------------+----------------+
```

Creazione di backend per il sistema storage

Dopo aver completato l'installazione di Astra Trident Operator, è necessario configurare il backend per la piattaforma di storage NetApp specifica in uso. Seguire i collegamenti riportati di seguito per continuare l'installazione e la configurazione di Astra Trident.

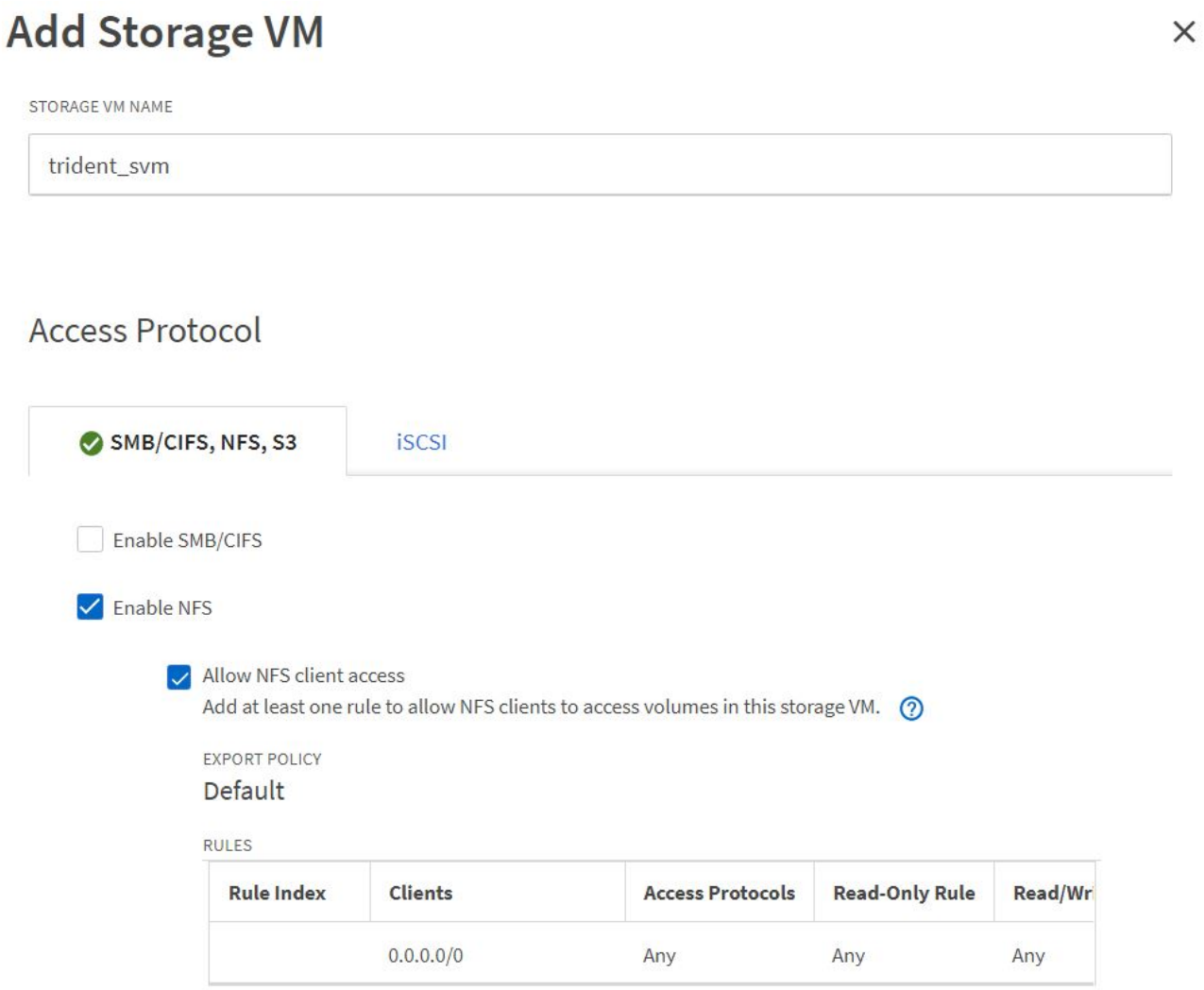
- "NetApp ONTAP NFS"
- "ISCSI NetApp ONTAP"

Configurazione NFS di NetApp ONTAP

Per consentire l'integrazione di Trident con il sistema storage NetApp ONTAP tramite NFS, è necessario creare un backend che consenta la comunicazione con il sistema storage. In questa soluzione viene configurato un backend di base, ma se si cercano opzioni più personalizzate, consultare la documentazione "qui".

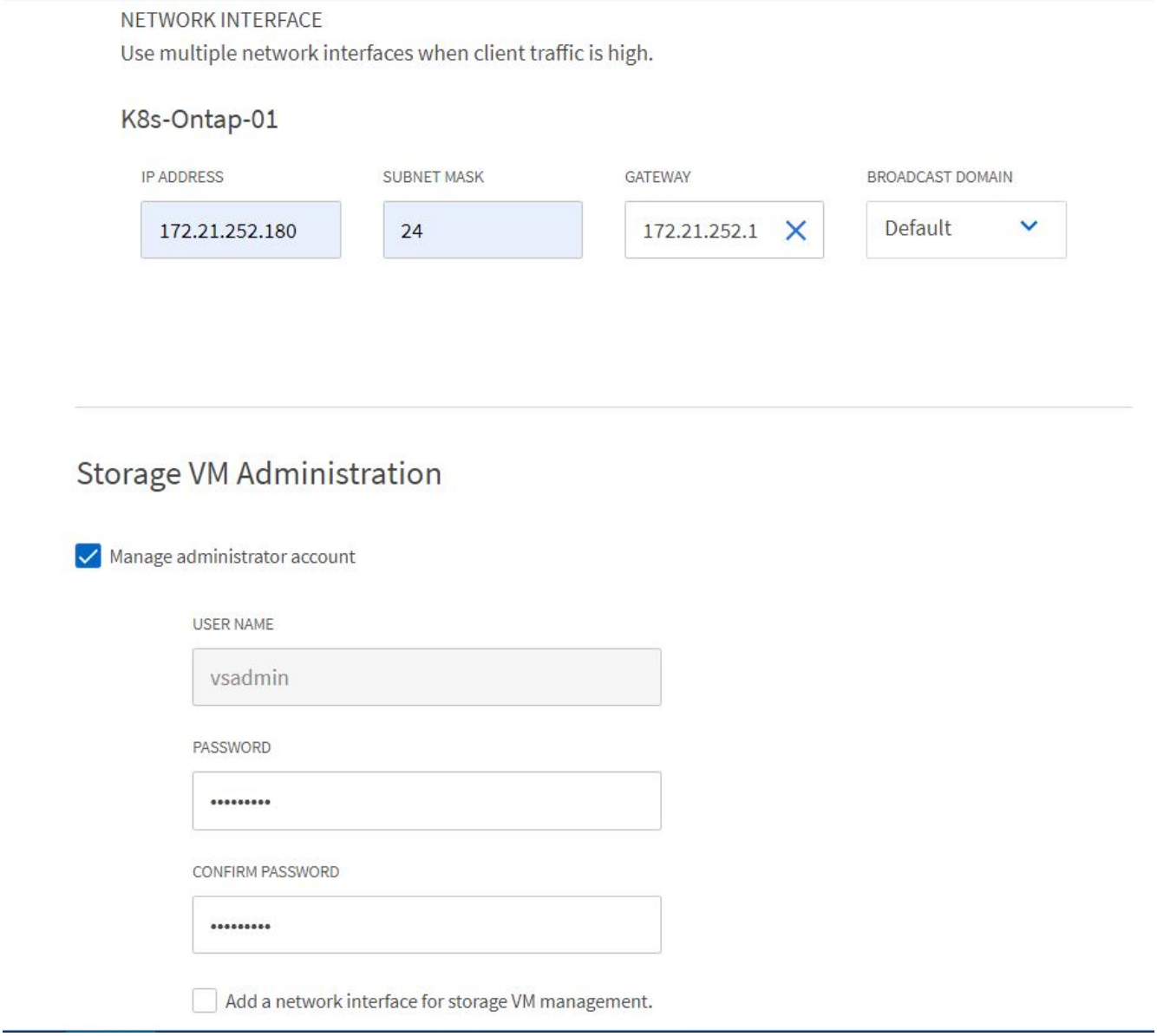
Creare una SVM in ONTAP

1. Accedere a Gestore di sistema di ONTAP, selezionare Storage > Storage VM e fare clic su Aggiungi.
2. Immettere un nome per SVM, attivare il protocollo NFS, selezionare la casella di controllo Allow NFS Client Access (Consenti accesso client NFS) e aggiungere le subnet su cui si trovano i nodi di lavoro nelle regole dei criteri di esportazione per consentire il montaggio dei volumi come PVS nei cluster di workload.

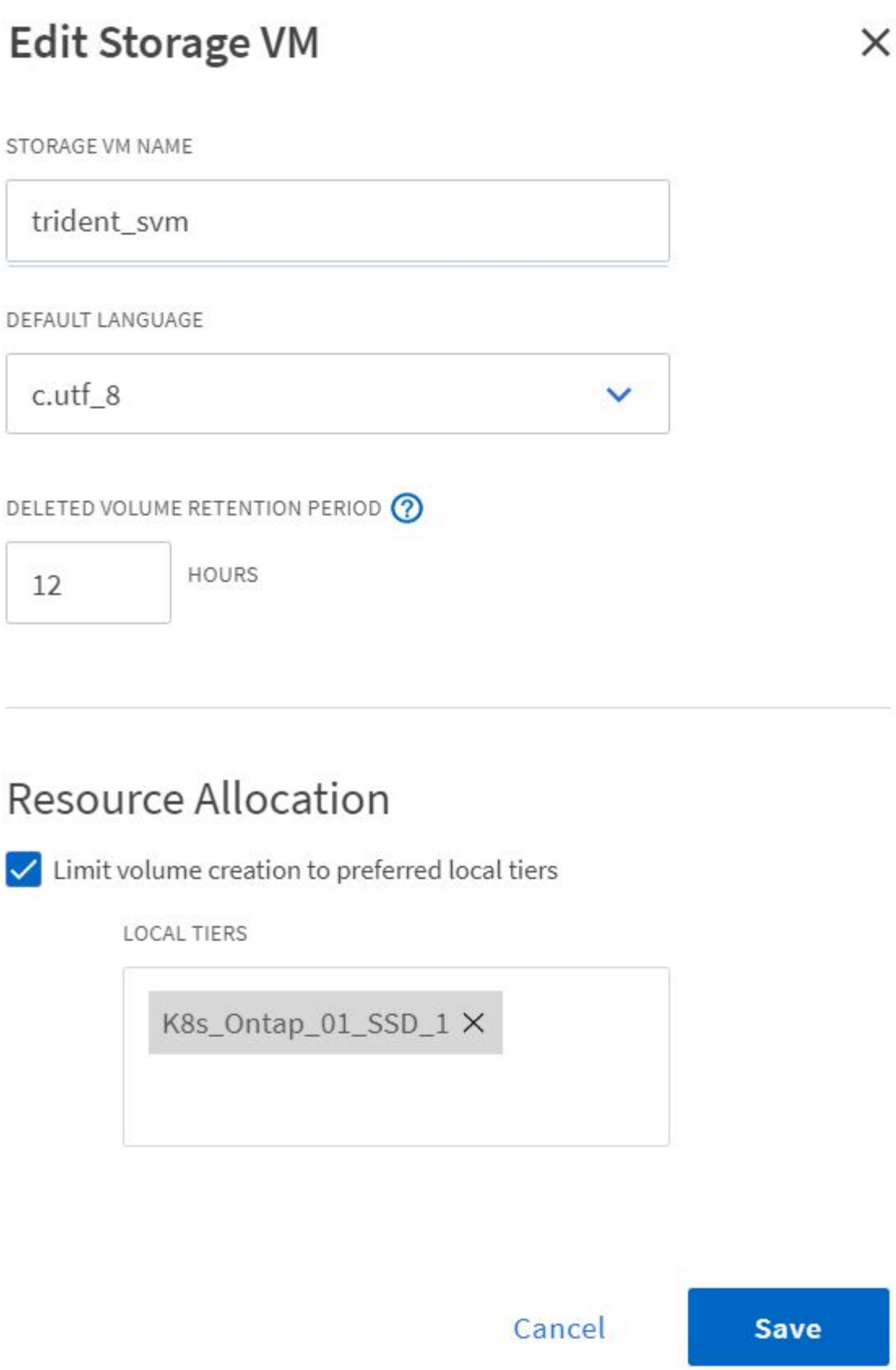


Se si utilizza l'implementazione NAT dei cluster di utenti o dei cluster di workload con NSX-T, è necessario aggiungere la subnet Egress (nel caso di TKGS0 o la subnet IP mobile (nel caso di TKGI) alle regole dei criteri di esportazione.

3. Fornire i dettagli relativi ai file LIF dei dati e all'account di amministrazione SVM, quindi fare clic su Save (Salva).



4. Assegnare gli aggregati a una SVM. Accedere a Storage > Storage VM (Storage VM), fare clic sui puntini di sospensione accanto alla SVM appena creata, quindi fare clic su Edit (Modifica). Selezionare la casella di controllo Limit Volume Creation to Preferred Local Tier (limita creazione volume a livelli locali preferiti) e allegarvi gli aggregati richiesti.



5. In caso di implementazioni NAT di cluster di utenti o workload su cui deve essere installato Trident, la richiesta di montaggio dello storage potrebbe provenire da una porta non standard a causa di SNAT. Per impostazione predefinita, ONTAP consente le richieste di montaggio del volume solo quando originate

dalla porta root. Quindi, accedere all'interfaccia utente di ONTAP e modificare l'impostazione per consentire le richieste di montaggio da porte non standard.

```
ontap-01> vserver nfs modify -vserver tanzu_svm -mount-rootonly disabled
```

Creare backend e StorageClasses

1. Per i sistemi NetApp ONTAP che utilizzano NFS, creare un file di configurazione back-end sul jumphost con backendName, managementLIF, dataLIF, svm, nome utente, password e altri dettagli.

```
{
    "version": 1,
    "storageDriverName": "ontap-nas",
    "backendName": "ontap-nas+10.61.181.221",
    "managementLIF": "172.21.224.201",
    "dataLIF": "10.61.181.221",
    "svm": "trident_svm",
    "username": "admin",
    "password": "password"
}
```

> È consigliabile definire il valore backendName personalizzato come combinazione di storageDriverName e dataLIF che fornisce NFS per una facile identificazione.

2. Creare il backend Trident eseguendo il seguente comando.

```
[netapp-user@rhel7]$ ./tridentctl -n trident create backend -f backend-
ontap-nas.json
+------------------------+----------------
+--------------------------------------+--------+---------+
|          NAME          | STORAGE DRIVER |                  UUID
| STATE  | VOLUMES |
+------------------------+----------------
+--------------------------------------+--------+---------+
| ontap-nas+10.61.181.221 | ontap-nas      | be7a619d-c81d-445c-b80c-
5c87a73c5b1e | online |       0 |
+------------------------+----------------
+--------------------------------------+--------+---------+
```

3. Una volta creato il backend, è necessario creare una classe di storage. La seguente definizione di classe di storage di esempio evidenzia i campi obbligatori e di base. Il parametro `backendType` Dovrebbe riflettere il driver di storage del backend Trident appena creato.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-nas"
```

4. Creare la classe di storage eseguendo il comando kubectl.

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f storage-class-
nfs.yaml
storageclass.storage.k8s.io/ontap-nfs created
```

5. Una volta creata la classe di storage, è necessario creare la prima dichiarazione di volume persistente (PVC). Di seguito viene fornita una definizione di PVC di esempio. Assicurarsi che il `storageClassName` il campo corrisponde al nome della classe di storage appena creata. La definizione del PVC può essere ulteriormente personalizzata in base alle esigenze, a seconda del carico di lavoro da fornire.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-nfs
```

6. Creare il PVC emettendo il comando kubectl. La creazione può richiedere del tempo a seconda delle dimensioni del volume di backup da creare, in modo da poter guardare il processo mentre viene completato.

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ kubectl get pvc
NAME    STATUS   VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS   AGE
basic   Bound    pvc-b4370d37-0fa4-4c17-bd86-94f96c94b42d   1Gi
RWO            ontap-nfs      7s
```

Configurazione iSCSI di NetApp ONTAP

Per integrare il sistema di storage NetApp ONTAP con i cluster VMware Tanzu Kubernetes per volumi persistenti tramite iSCSI, il primo passo è preparare i nodi accedendo a ciascun nodo e configurando le utility o i pacchetti iSCSI per il montaggio dei volumi iSCSI. A tale scopo, seguire la procedura descritta in questo documento "collegamento".

> NetApp sconsiglia questa procedura per le implementazioni NAT dei cluster VMware Tanzu Kubernetes.

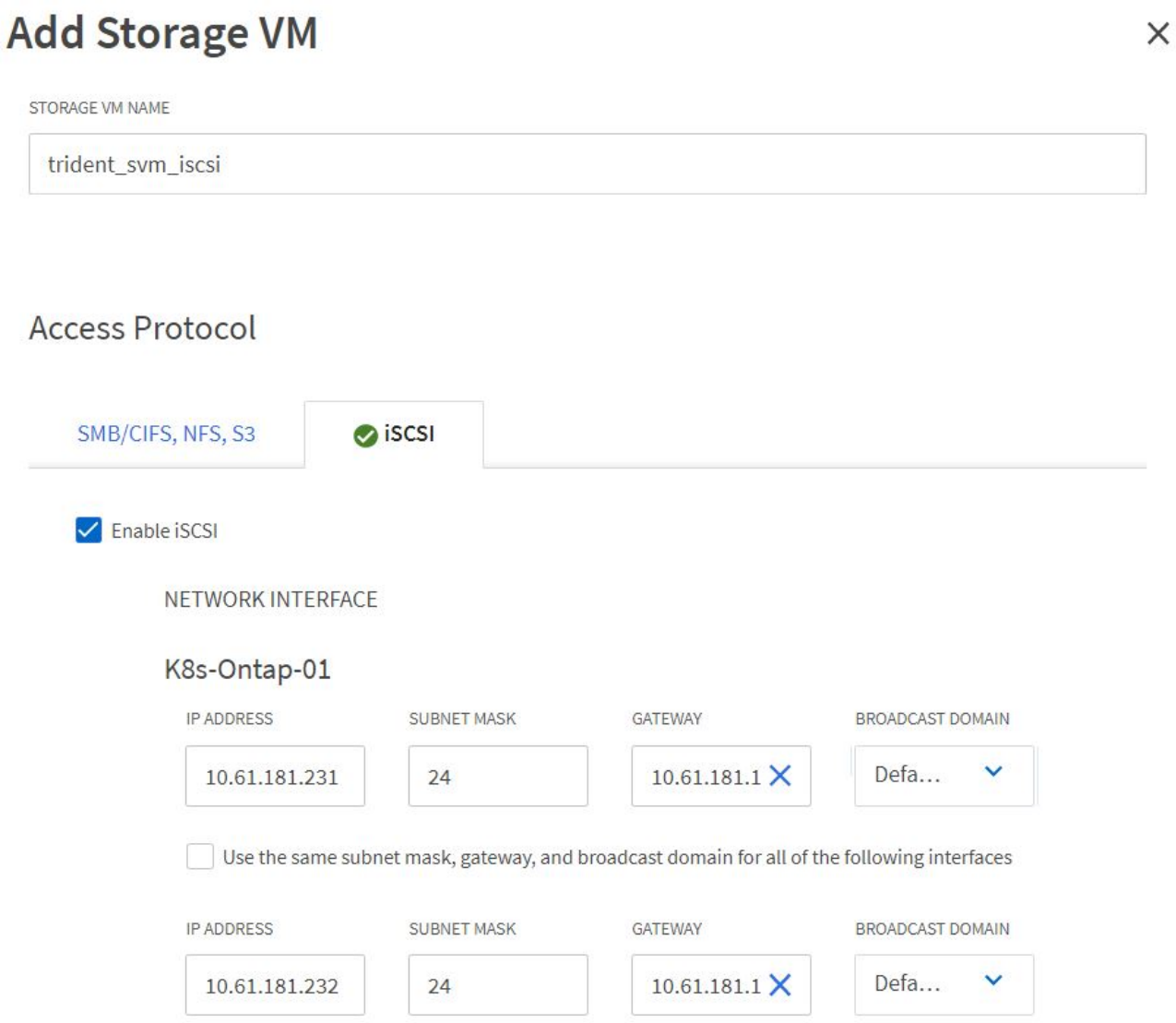
> TKGI utilizza le macchine virtuali Bosh come nodi per i cluster Tanzu Kubernetes che eseguono immagini di configurazione immutabili e qualsiasi modifica manuale dei pacchetti iSCSI sulle macchine virtuali Bosh non rimane persistente durante i riavvii. Pertanto, NetApp consiglia di utilizzare volumi NFS per lo storage persistente per i cluster Tanzu Kubernetes implementati e gestiti da TKGI.

Una volta preparati i nodi del cluster per i volumi iSCSI, è necessario creare un backend che consenta la comunicazione con il sistema storage. In questa soluzione è stato configurato un backend di base, ma per ulteriori opzioni personalizzate, consultare la documentazione "qui".

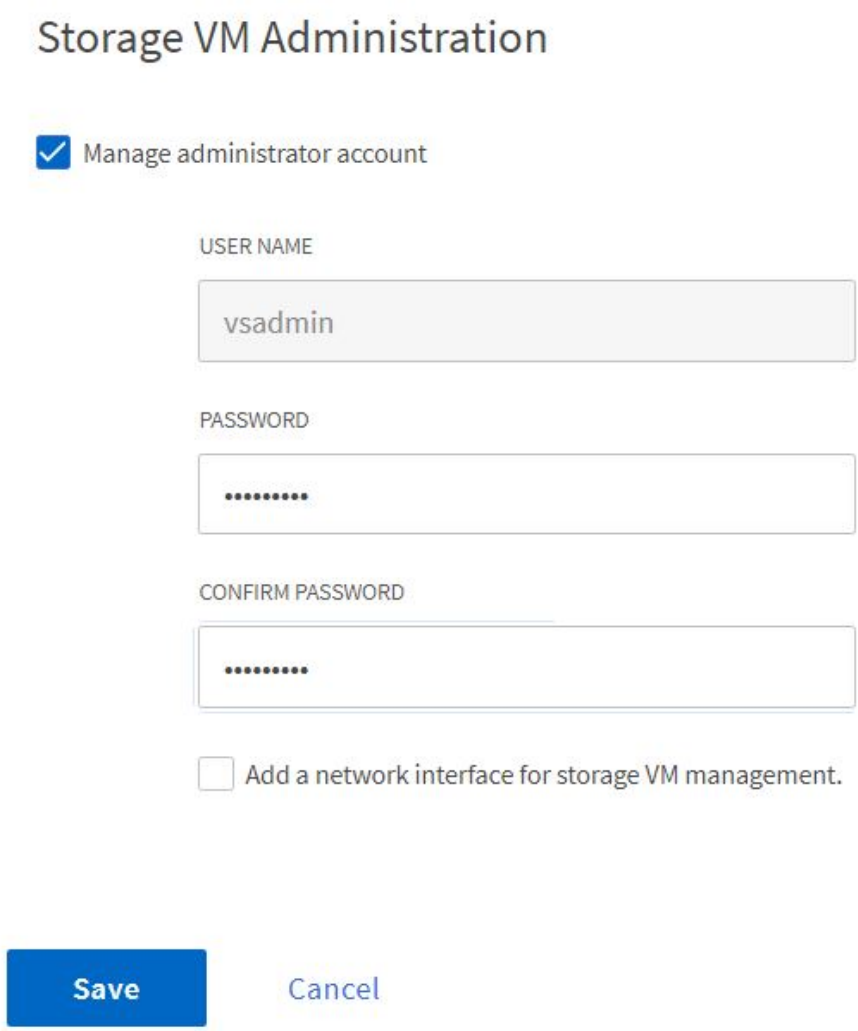
Creare una SVM in ONTAP

Per creare una SVM in ONTAP, attenersi alla seguente procedura:

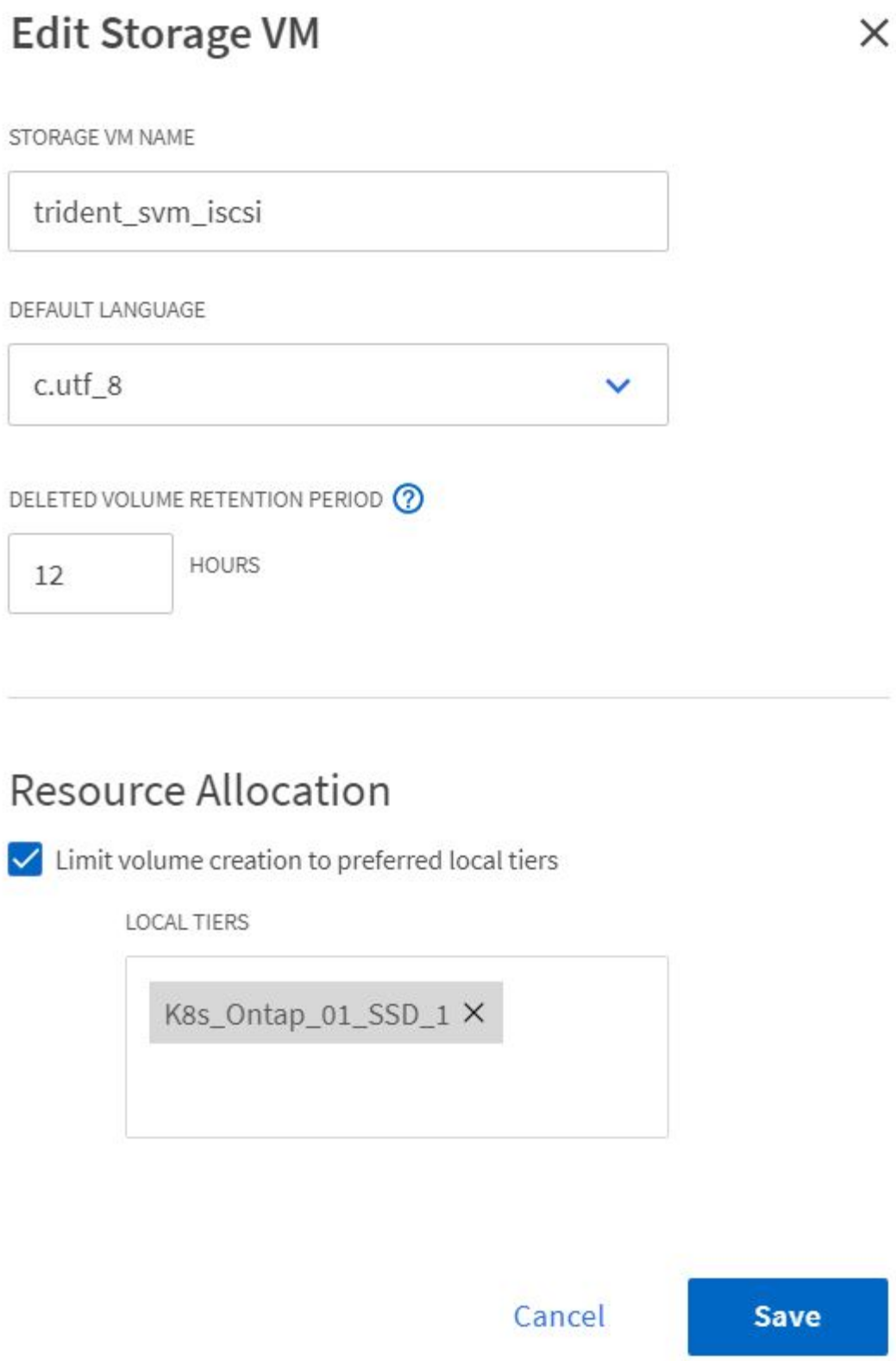
1. Accedere a Gestore di sistema di ONTAP, selezionare Storage > Storage VM e fare clic su Aggiungi.
2. Inserire un nome per la SVM, attivare il protocollo iSCSI, quindi fornire i dettagli per la LIF dei dati.



3. Inserire i dettagli dell’account di amministrazione SVM, quindi fare clic su Save (Salva).



4. Per assegnare gli aggregati alla SVM, selezionare Storage > Storage VM (Storage > Storage VM), fare clic sui puntini di sospensione accanto alla SVM appena creata, quindi fare clic su Edit (Modifica). Selezionare la casella di controllo Limit Volume Creation to Preferred Local Tier (limita creazione volume a livelli locali preferiti) e allegarvi gli aggregati richiesti.



Creare backend e StorageClasses

1. Per i sistemi NetApp ONTAP che utilizzano NFS, creare un file di configurazione back-end sul jumphost con backendName, managementLIF, dataLIF, svm, nome utente, password e altri dettagli.

```
{
  "version": 1,
  "storageDriverName": "ontap-san",
  "backendName": "ontap-san+10.61.181.231",
  "managementLIF": "172.21.224.201",
  "dataLIF": "10.61.181.231",
  "svm": "trident_svm_iscsi",
  "username": "admin",
  "password": "password"
}
```

2. Creare il backend Trident eseguendo il seguente comando.

```
[netapp-user@rhel7 trident-installer]$ ./tridentctl -n trident create
backend -f backend-ontap-san.json
+------------------------+----------------
+--------------------------------------+--------+---------+
|          NAME          | STORAGE DRIVER |                  UUID
| STATE  | VOLUMES |
+------------------------+----------------
+--------------------------------------+--------+---------+
| ontap-san+10.61.181.231 | ontap-san      | 6788533c-7fea-4a35-b797-
fb9bb3322b91 | online |       0 |
+------------------------+----------------
+--------------------------------------+--------+---------+
```

3. Dopo aver creato un backend, è necessario creare una classe di storage. La seguente definizione di classe di storage di esempio evidenzia i campi obbligatori e di base. Il parametro `backendType` Dovrebbe riflettere il driver di storage del backend Trident appena creato. Annotare anche il valore del campo nome, a cui si deve fare riferimento in un passaggio successivo.

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-iscsi
provisioner: csi.trident.netapp.io
parameters:
  backendType: "ontap-san"
```

> Esiste un campo opzionale chiamato `fsType` definito in questo file. Nei backend iSCSI, questo valore può essere impostato su un tipo di file system Linux specifico (XFS, ext4 e così via) o può essere cancellato per consentire ai cluster Tanzu Kubernetes di decidere quale filesystem utilizzare.

4. Creare la classe di storage eseguendo il comando kubectl.

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f storage-class-
iscsi.yaml
storageclass.storage.k8s.io/ontap-iscsi created
```

5. Una volta creata la classe di storage, è necessario creare la prima dichiarazione di volume persistente (PVC). Di seguito viene fornita una definizione di PVC di esempio. Assicurarsi che il `storageClassName` il campo corrisponde al nome della classe di storage appena creata. La definizione del PVC può essere ulteriormente personalizzata in base alle esigenze, a seconda del carico di lavoro da fornire.

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: basic
spec:
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
  storageClassName: ontap-iscsi
```

6. Creare il PVC emettendo il comando kubectl. La creazione può richiedere del tempo a seconda delle dimensioni del volume di backup da creare, in modo da poter guardare il processo mentre viene completato.

```
[netapp-user@rhel7 trident-installer]$ kubectl create -f pvc-basic.yaml
persistentvolumeclaim/basic created

[netapp-user@rhel7 trident-installer]$ kubectl get pvc
NAME    STATUS   VOLUME                                     CAPACITY
ACCESS MODES   STORAGECLASS   AGE
basic   Bound    pvc-7ceac1ba-0189-43c7-8f98-094719f7956c   1Gi
RWO            ontap-iscsi      3s
```