Descripción general de las integraciones de almacenamiento de NetApp

NetApp Solutions

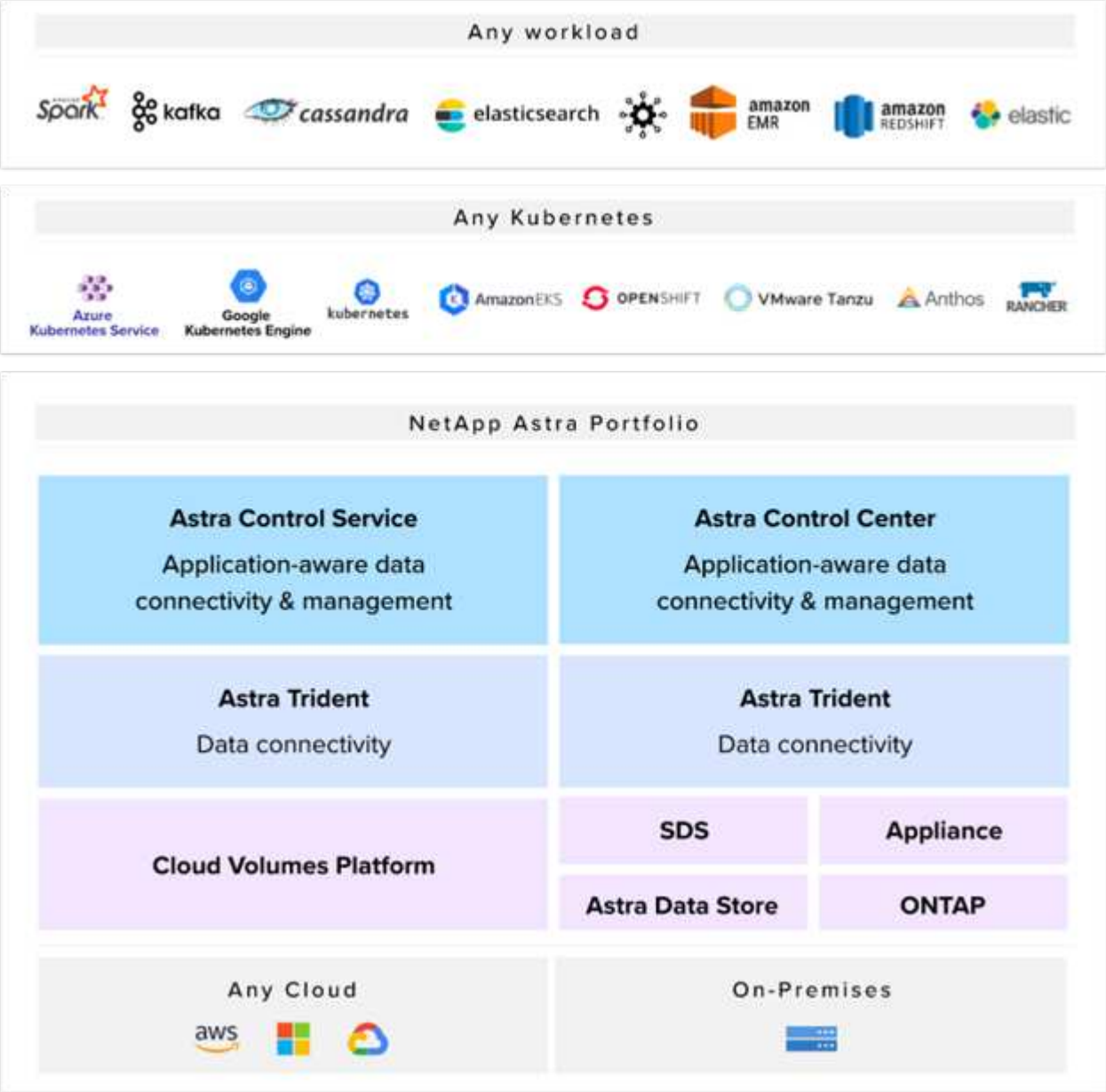
NetApp
April 26, 2024

Tabla de contenidos

Información general sobre la integración del almacenamiento de NetApp 1
Descripción general de Astra Control de NetApp 2
Descripción general de Astra Trident 20

Información general sobre la integración del almacenamiento de NetApp

NetApp proporciona una serie de productos para ayudarle a orquestar, gestionar, proteger y migrar aplicaciones con contenedores con estado y sus datos.



Astra Control de NetApp ofrece un amplio conjunto de servicios de gestión de datos para aplicaciones y almacenamiento para cargas de trabajo con estado de Kubernetes gracias a la tecnología de protección de datos de NetApp. El servicio Astra Control está disponible para admitir cargas de trabajo con estado en puestas en marcha de Kubernetes nativas para el cloud. Astra Control Center está disponible para admitir cargas de trabajo con estado en puestas en marcha en las instalaciones de plataformas Enterprise Kubernetes como Red Hat OpenShift, Rancher, VMware Tanzu etc. Si quiere más información, visite el sitio web de Astra Control de NetApp "aquí".

NetApp Astra Trident es un orquestador de almacenamiento de código abierto y totalmente compatible para contenedores y distribuciones de Kubernetes como Red Hat OpenShift, Rancher, VMware Tanzu etc. Si quiere

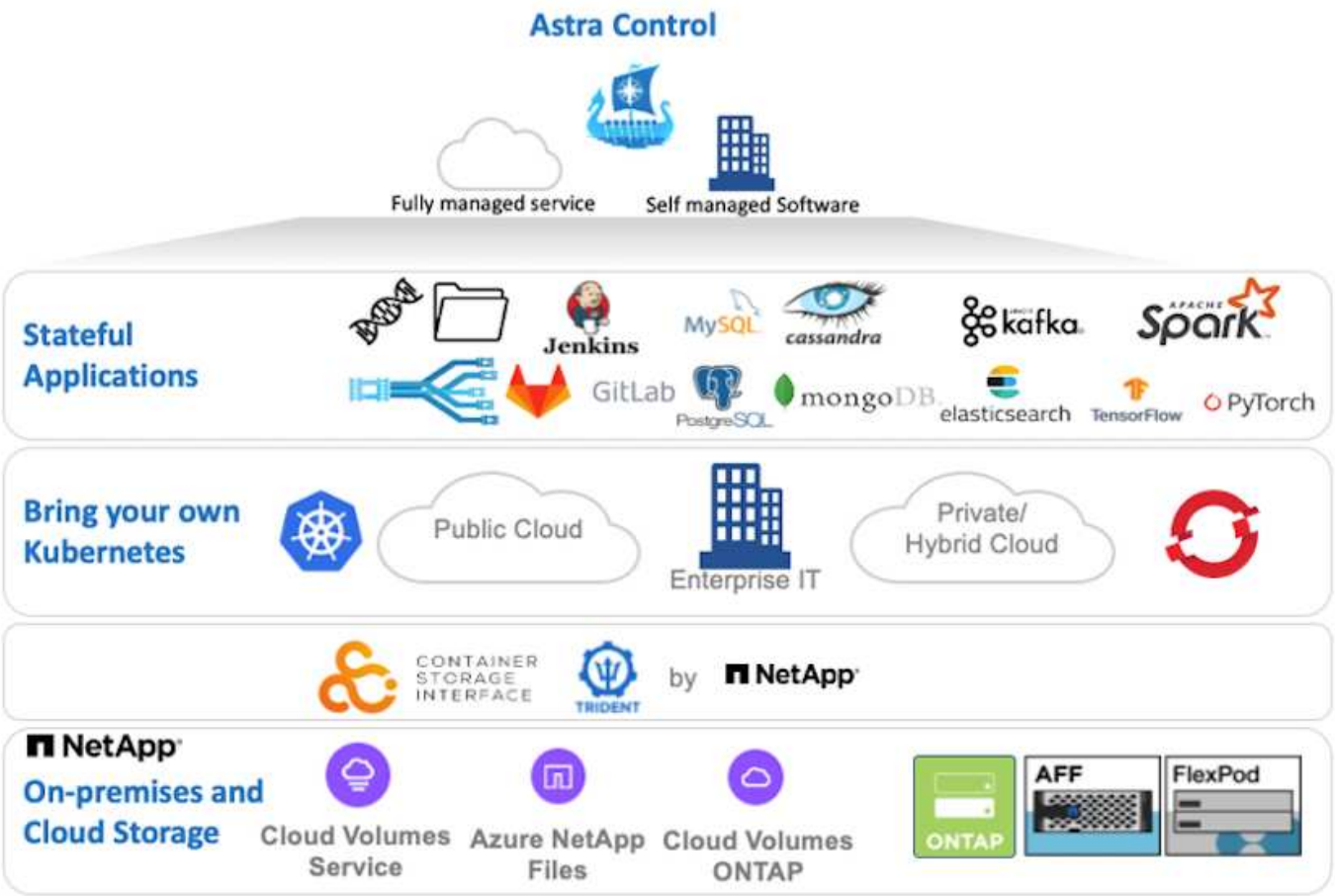
más información, visite el sitio web de Astra Trident "aquí".

En las siguientes páginas se ofrece información adicional sobre los productos de NetApp que se han validado para la administración del almacenamiento persistente y de aplicaciones en la solución VMware Tanzu with NetApp:

- "Centro de control de Astra de NetApp"
- "Astra Trident de NetApp"

Descripción general de Astra Control de NetApp

Astra Control Center de NetApp ofrece un amplio conjunto de servicios de gestión de datos para aplicaciones y almacenamiento para cargas de trabajo con estado de Kubernetes puestas en marcha en un entorno local con la tecnología de protección de datos de NetApp.



NetApp Astra Control Center se puede instalar en un clúster de VMware Tanzu que tenga el orquestador de almacenamiento Astra Trident puesto en marcha y configurado con clases de almacenamiento y back-ends en los sistemas de almacenamiento ONTAP de NetApp.

Si desea obtener más información sobre Astra Trident, consulte "este documento aquí".

En un entorno conectado a la nube, Astra Control Center utiliza Cloud Insights para proporcionar supervisión y telemetría avanzadas. Ante la ausencia de una conexión con Cloud Insights, la supervisión y la telemetría limitadas (en siete días de métricas) están disponibles y se exportan a herramientas de supervisión nativas de Kubernetes (Prometheus y Grafana) mediante extremos de métricas abiertos.

Astra Control Center está totalmente integrado en el ecosistema de AutoSupport y Active IQ de NetApp para proporcionar soporte a los usuarios y proporcionar asistencia para la solución de problemas y mostrar las estadísticas de uso.

Además de la versión pagada de Astra Control Center, también hay disponible una licencia de evaluación de 90 días. La versión de evaluación se admite a través del correo electrónico y el canal de Slack de la comunidad. Los clientes tienen acceso a estos recursos, a otros artículos de la base de conocimientos y a la documentación disponible en la consola de soporte del producto.

Para obtener más información sobre la cartera de Astra, visite "Sitio web de Astra".

Automatización de Astra Control Center

Astra Control Center tiene una API DE REST totalmente funcional para el acceso a la programación. Los usuarios pueden utilizar cualquier lenguaje de programación o utilidad para interactuar con los extremos de la API REST de Astra Control. Para obtener más información acerca de esta API, consulte la documentación de "aquí".

Si busca un kit de herramientas de desarrollo de software listo para usar con las API REST de Astra Control, NetApp le proporciona un kit de herramientas con Astra Control Python SDK que puede descargar "aquí".

Si la programación no es adecuada para su situación y le gustaría utilizar una herramienta de gestión de configuración, puede clonar y ejecutar los libros de estrategia de Ansible que publica NetApp "aquí".

Requisitos previos de instalación de Astra Control Center

La instalación de Astra Control Center requiere los siguientes requisitos previos:

- Uno o varios clústeres de Kubernetes de Tanzania, gestionados por un clúster de gestión o TKGS o TKGI. Se admiten clústeres de carga de trabajo TKG de 1.4+ y clústeres de usuario TKGI de 1.12.2+.
- Astra Trident ya debe estar instalado y configurado en cada uno de los clústeres de Kubernetes de Tanzania.
- Uno o más sistemas de almacenamiento ONTAP de NetApp que ejecutan ONTAP 9.5 o superior.

> Se trata de una mejor práctica para cada instalación de Kubernetes en Tanzania en un sitio que consiste en disponer de una SVM dedicada para el almacenamiento persistente. Las puestas en marcha de varios sitios requieren sistemas de almacenamiento adicionales.

- Se debe configurar un back-end de almacenamiento Trident en cada clúster de Kubernetes tanzu con una SVM respaldada por un clúster de ONTAP.
- Un StorageClass predeterminado configurado en cada clúster Kubernetes tanzu con Astra Trident como aprovisionador de almacenamiento.
- Debe instalarse y configurar un equilibrador de carga en cada clúster de Kubernetes de Tanzu para equilibrar la carga y exponer Astra Control Center si está utilizando ingressType `AccTraefik`.
- Debe instalar y configurar un controlador de entrada en cada clúster de Kubernetes de Tanzu para exponer Astra Control Center si utiliza ingressType `Generic`.
- Debe configurarse un registro de imagen privada para alojar las imágenes de Astra Control Center de NetApp.
- Debe tener acceso de administrador del clúster al clúster Tanzania Kubernetes donde se está instalando Astra Control Center.

- Debe tener acceso de administrador a los clústeres de ONTAP de NetApp.
- Una estación de trabajo de administración de RHEL o Ubuntu.

Instalar Astra Control Center

Esta solución describe un procedimiento automatizado para instalar Astra Control Center mediante los libros de estrategia de Ansible. Si está buscando un procedimiento manual para instalar Astra Control Center, siga la guía detallada de instalación y operaciones "aquí".

1. Para utilizar los libros de estrategia de Ansible que ponen en marcha Astra Control Center, debe tener una máquina Ubuntu/RHEL con Ansible instalada. Siga los procedimientos "aquí" Para Ubuntu y RHEL.
2. Clone el repositorio de GitHub que aloja el contenido de Ansible.

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

3. Inicie sesión en el sitio de soporte de NetApp y descargue la versión más reciente de Astra Control Center de NetApp. Para ello, es necesario disponer de una licencia adjunta a su cuenta de NetApp. Después de descargar el tarball, transfiéralo a la estación de trabajo.

> Para empezar con una licencia de prueba de Astra Control, visite "Sitio de registro de Astra".

4. Cree o obtenga el archivo kubeconfig con acceso de administrador al clúster de Kubernetes de tanzu de carga de trabajo o usuario en el que se va a instalar Astra Control Center.
5. Cambie el directorio a. `na_astra_control_suite`.

```
cd na_astra_control_suite
```

6. Edite el `vars/vars.yml` archive y rellene las variables con la información necesaria.

```
#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. Ejecute el libro de estrategia para implementar Astra Control Center. El libro de estrategia requiere privilegios raíz para determinadas configuraciones.

   Ejecute el siguiente comando para ejecutar el libro de estrategia si el usuario que ejecuta la tableta playbook es raíz o tiene un sudo configurado sin contraseñas.

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

   Si el usuario tiene configurado un acceso sudo basado en contraseña, ejecute el siguiente comando para ejecutar la libro de estrategia y, a continuación, introduzca la contraseña sudo.

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

Pasos posteriores a la instalación

1. La instalación puede tardar varios minutos en completarse. Verifique que todos los pods y servicios del `netapp-astra-cc` el espacio de nombres está activo y en funcionamiento.

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

2. Compruebe la `acc-operator-controller-manager` registros para garantizar que se completa la instalación.

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

   > El siguiente mensaje indica que la instalación de Astra Control Center se ha realizado correctamente.

   ```
   {"level":"info","ts":1624054318.029971,"logger":"controllers.AstraContro
   lCenter","msg":"Successfully Reconciled AstraControlCenter in
   [seconds]s","AstraControlCenter":"netapp-astra-
   cc/astra","ae.Version":"[22.04.0]"}
   ```

3. El nombre de usuario para iniciar sesión en Astra Control Center es la dirección de correo electrónico del

administrador que se proporciona en el archivo CRD y la contraseña es una cadena `ACC-` Se adjunta al UUID del Centro de control de Astra. Ejecute el siguiente comando:

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

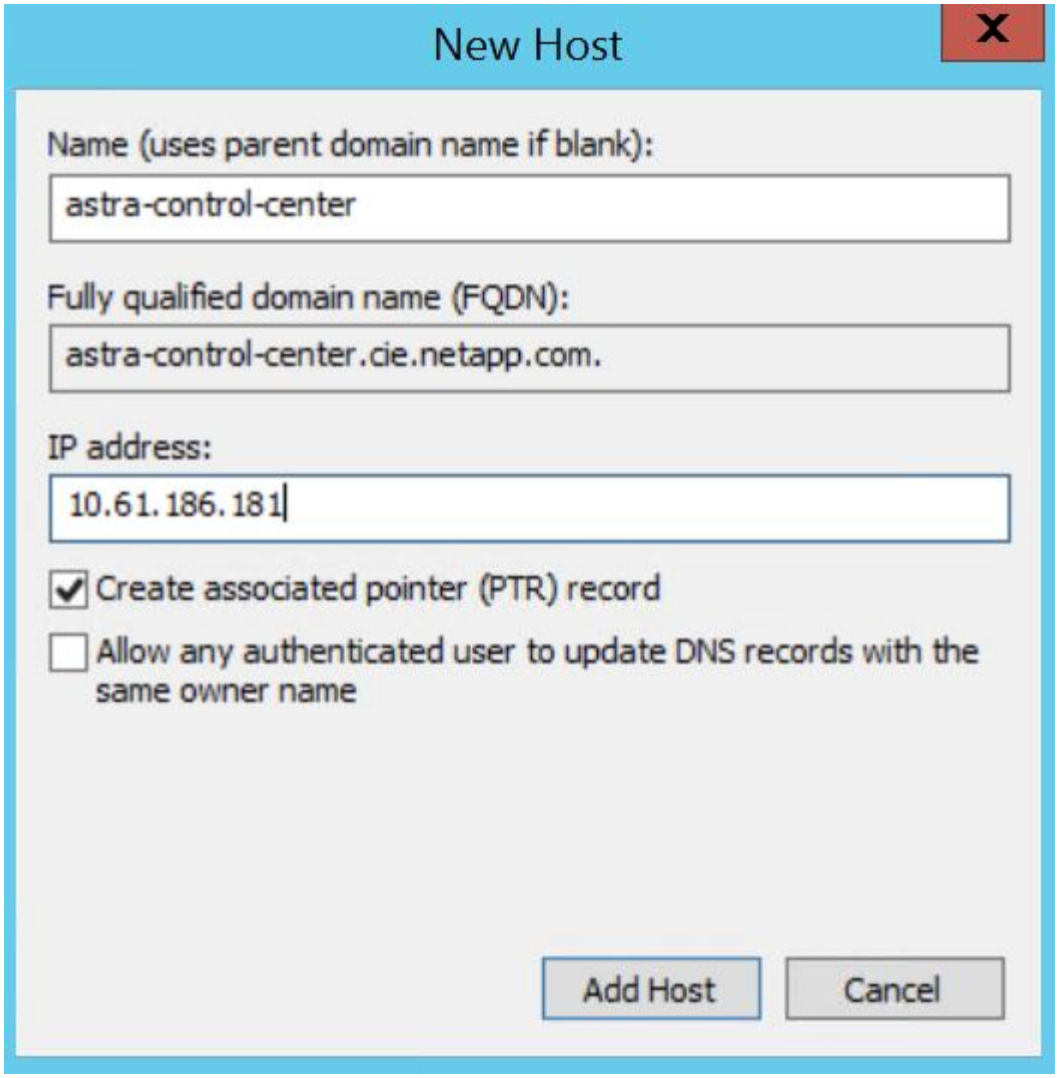
En este ejemplo, la contraseña es `ACC-345c55a5-bf2e-21f0-84b8-b6f2bce5e95f`.

4. Obtenga el IP del equilibrador de carga de servicio de Traefik si el ingressType es Accefik.

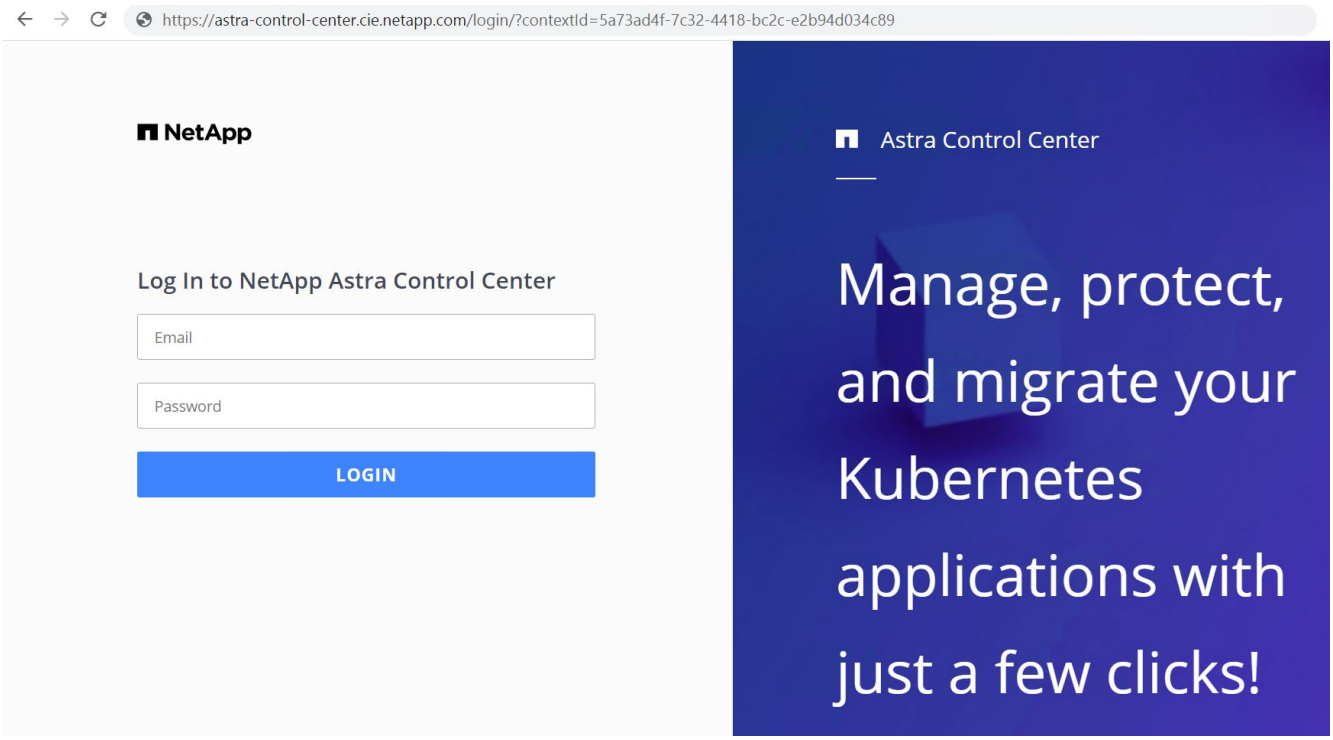
```
[netapp-user@rhel7 ~]$ oc get svc -n netapp-astra-cc | egrep
'EXTERNAL|traefik'

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
```

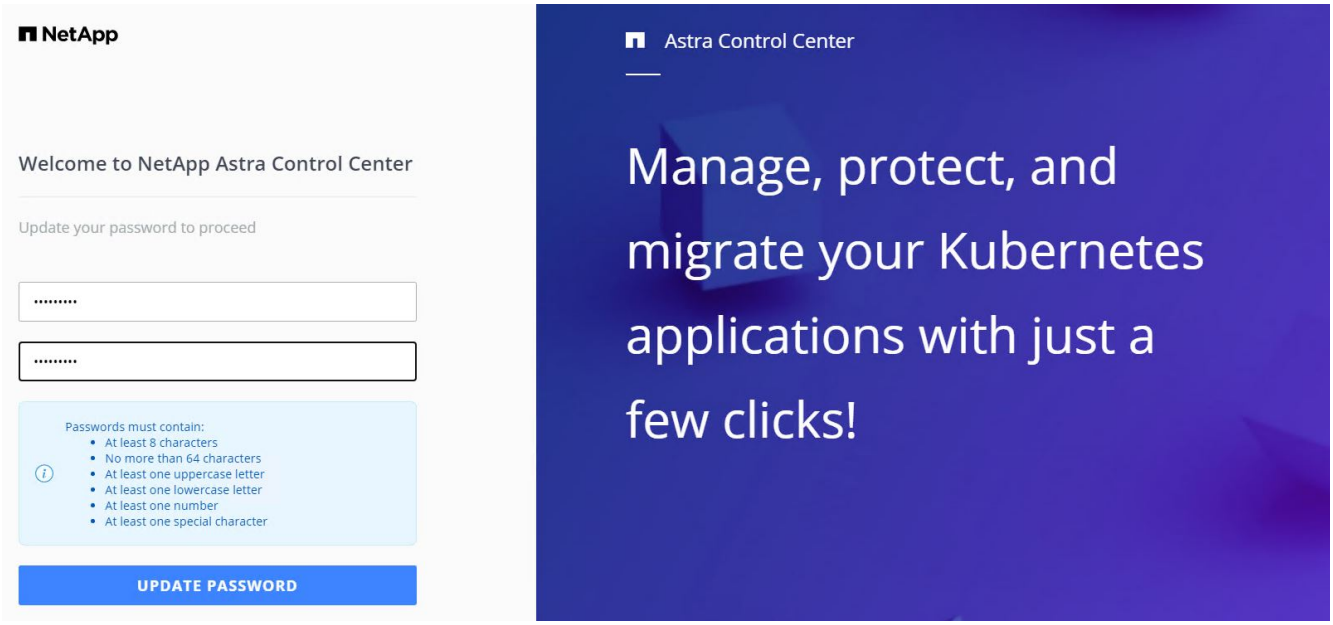
5. Agregue una entrada en el servidor DNS apuntando al FQDN que se proporciona en el archivo CRD de Astra Control Center al `EXTERNAL-IP` del servicio de trafik.



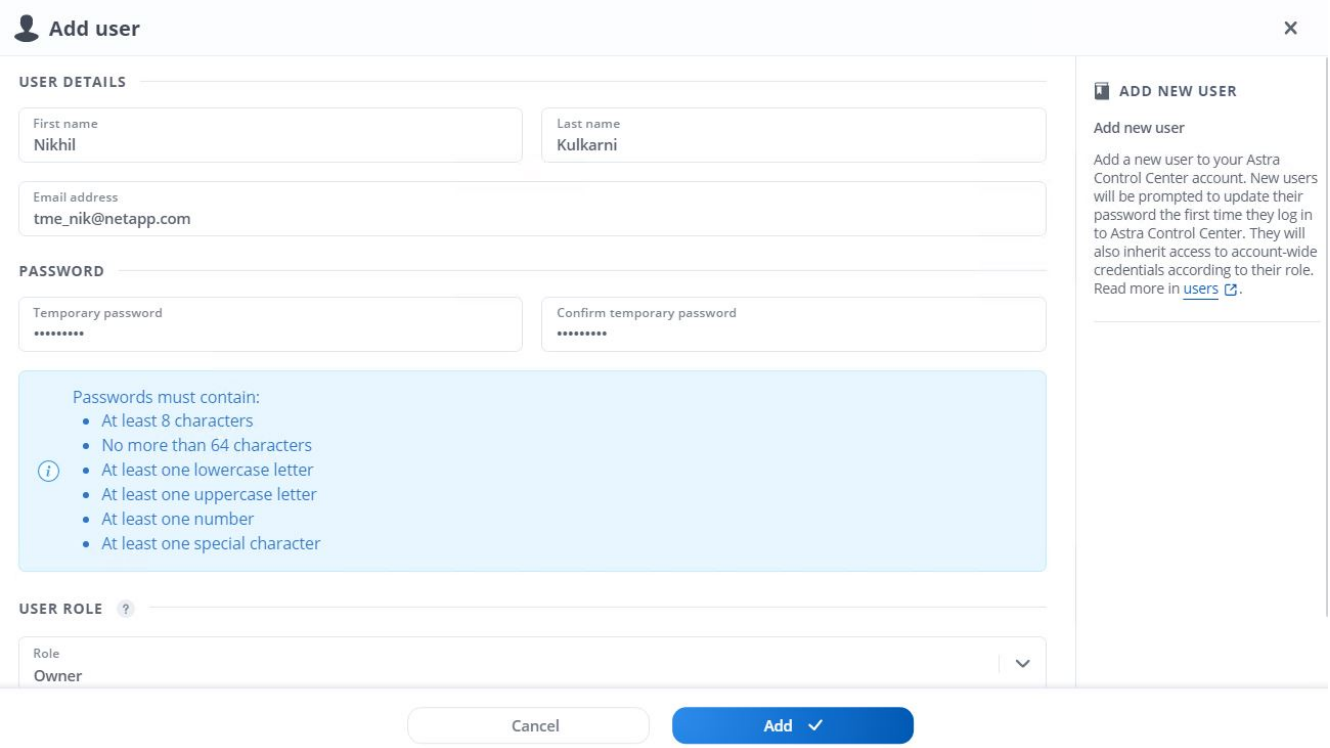
6. Inicie sesión en la GUI de Astra Control Center navegando por su FQDN.



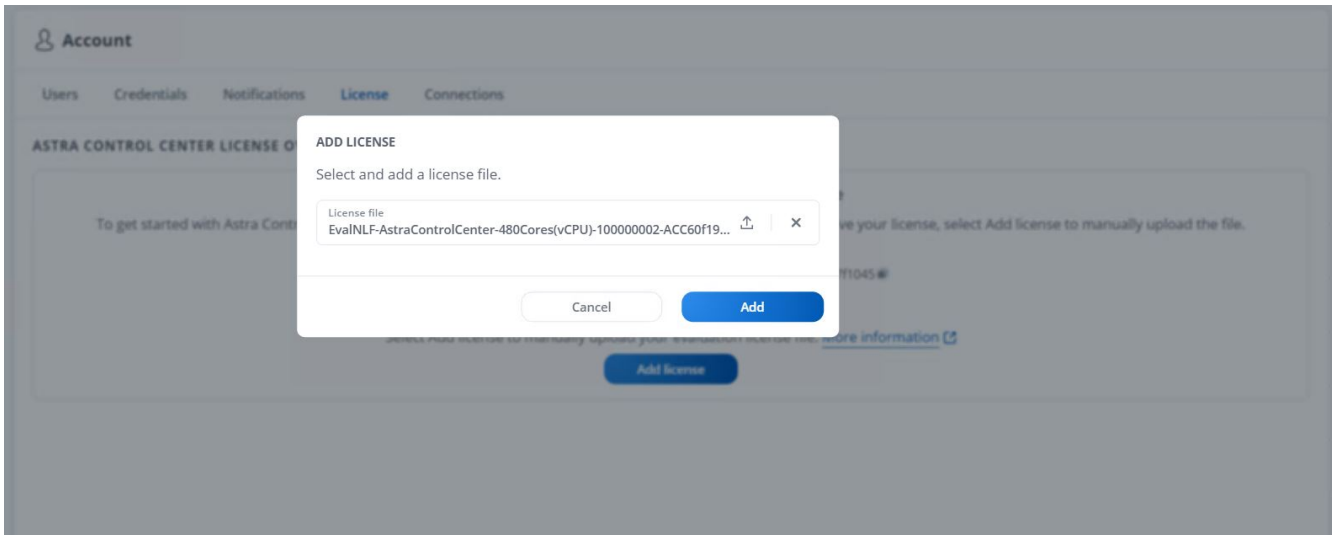
7. Cuando inicie sesión en la GUI de Astra Control Center por primera vez con la dirección de correo electrónico de administrador proporcionada en CRD, deberá cambiar la contraseña.



8. Si desea agregar un usuario a Astra Control Center, desplácese a cuenta > usuarios, haga clic en Agregar, introduzca los detalles del usuario y haga clic en Agregar.



9. Astra Control Center requiere una licencia para que funcionen todas sus funciones. Para añadir una licencia, vaya a cuenta > Licencia, haga clic en Añadir licencia y cargue el archivo de licencia.



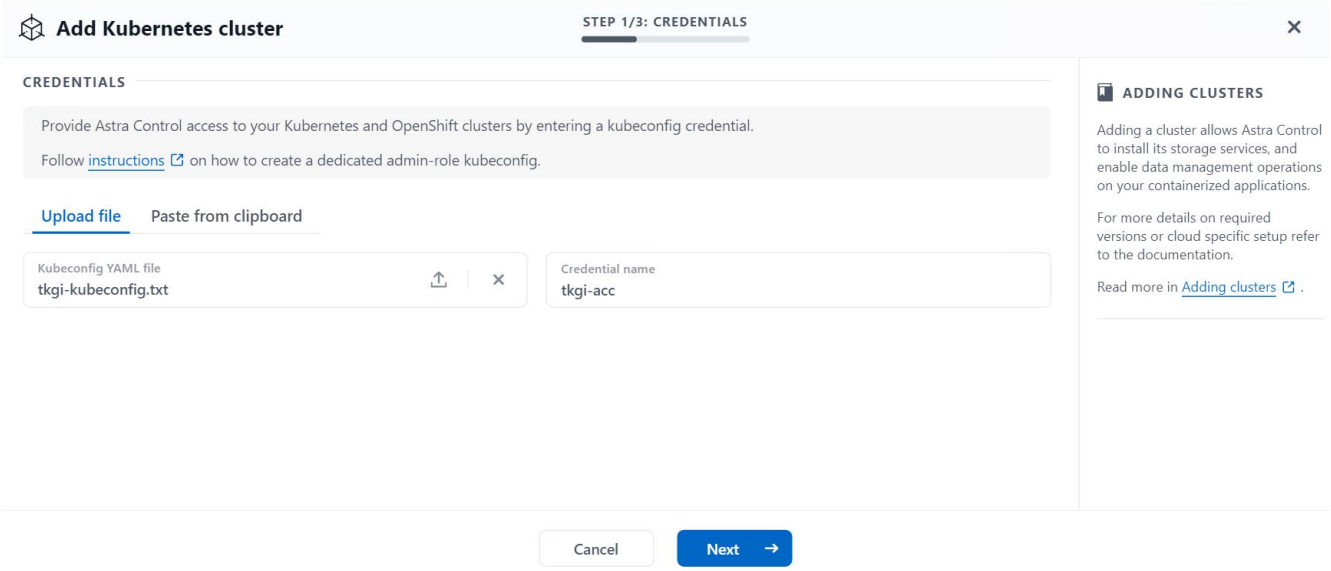
Si tiene problemas con la instalación o la configuración de NetApp Astra Control Center, está disponible la base de conocimientos sobre problemas conocidos "aquí".

Registre sus clústeres de Kubernetes de VMware Tanzu con Astra Control Center

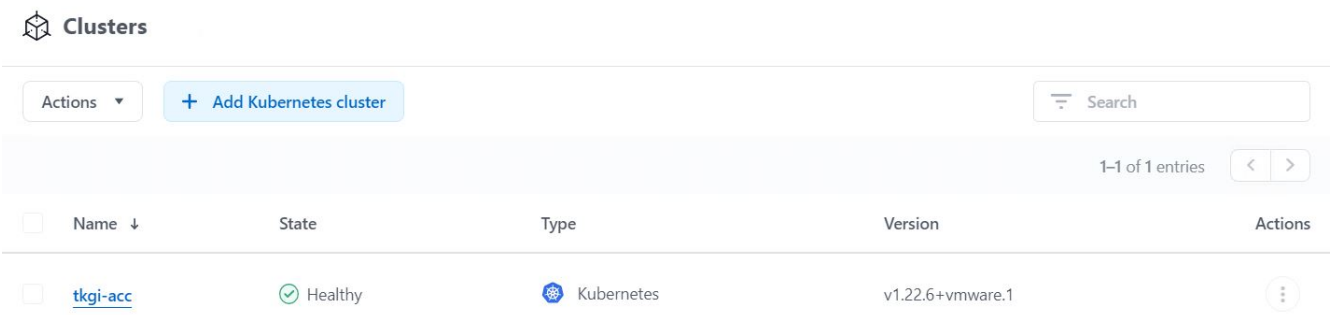
Para permitir que Astra Control Center gestione sus cargas de trabajo, primero debe registrar sus clústeres de Kubernetes tanzu.

Registre clústeres de Kubernetes de VMware Tanzania

1. El primer paso es añadir los clústeres de Tanzania Kubernetes al Astra Control Center y gestionarlos. Vaya a Clusters y haga clic en Add a Cluster, cargue el archivo kubeconfig para el clúster Tanzania Kubernetes y haga clic en Select Storage.



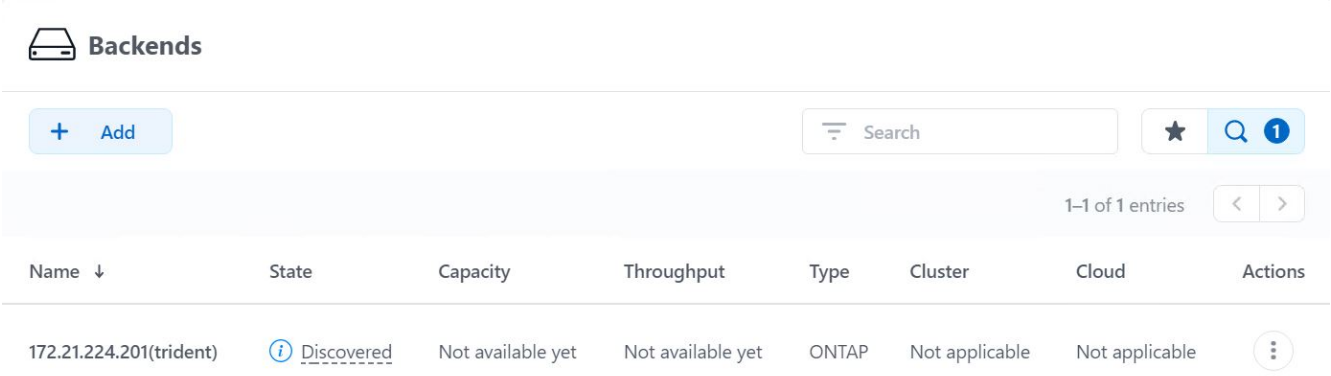
2. Astra Control Center detecta las clases de almacenamiento elegibles. Ahora seleccione la forma en que storagegrid aprovisiona volúmenes mediante Trident con backup de una SVM en ONTAP de NetApp y haga clic en Review. En el panel siguiente, compruebe los detalles y haga clic en Add Cluster.
3. Cuando se agrega el clúster, se mueve al estado de detección mientras Astra Control Center lo inspecciona e instala los agentes necesarios. El estado del clúster cambia de `Healthy` después de que se haya registrado correctamente.



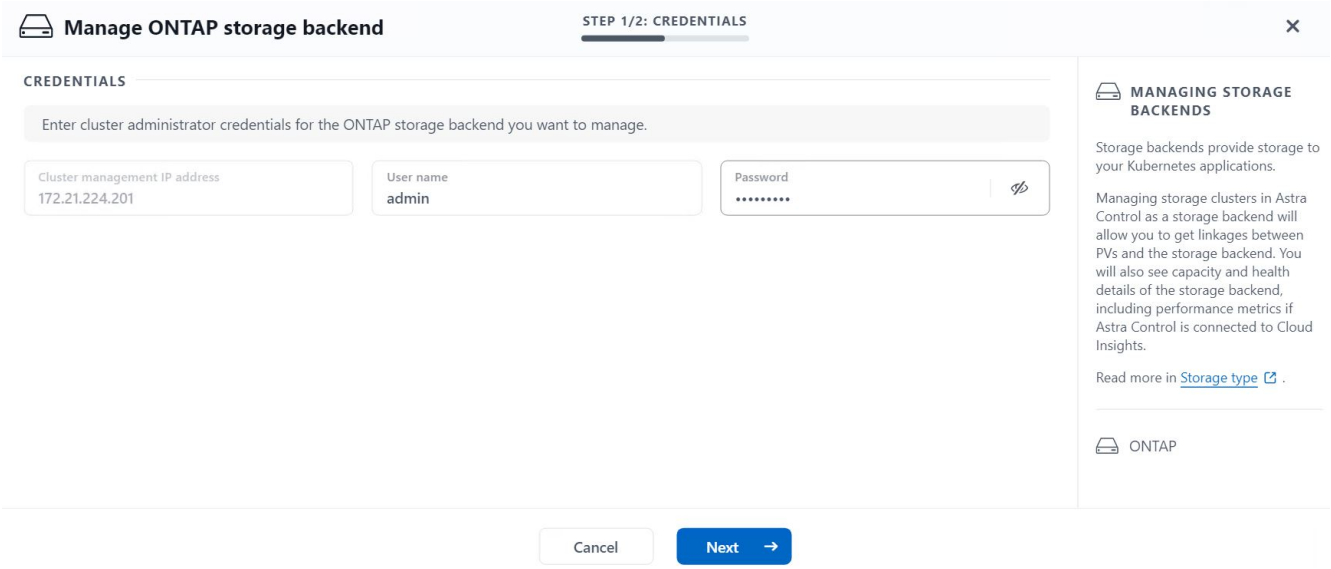
> Todos los clústeres de Kubernetes de Tanzania que gestiona Astra Control Center deben tener acceso al registro de imágenes que se utilizó para su instalación, ya que los agentes instalados en los clústeres gestionados extraen las imágenes de ese registro.

4. Importe clústeres de ONTAP como recursos de almacenamiento que Astra Control Center gestiona como back-ends. Cuando se añaden los clústeres de Kubernetes tanzu a Astra y se configura un storagegrid, detecta e inspecciona automáticamente el clúster de ONTAP para realizar la copia de seguridad de

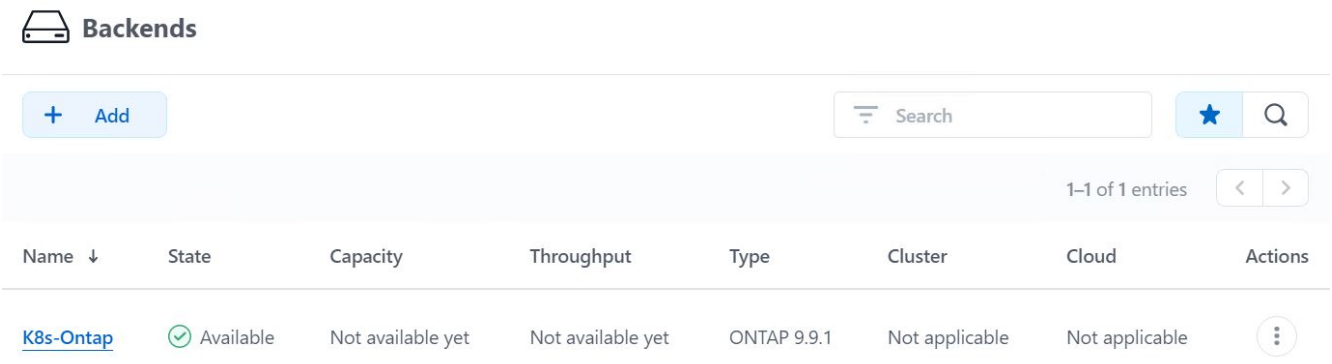
storageecleclass pero no la importa al Centro de control de Astra para su gestión.



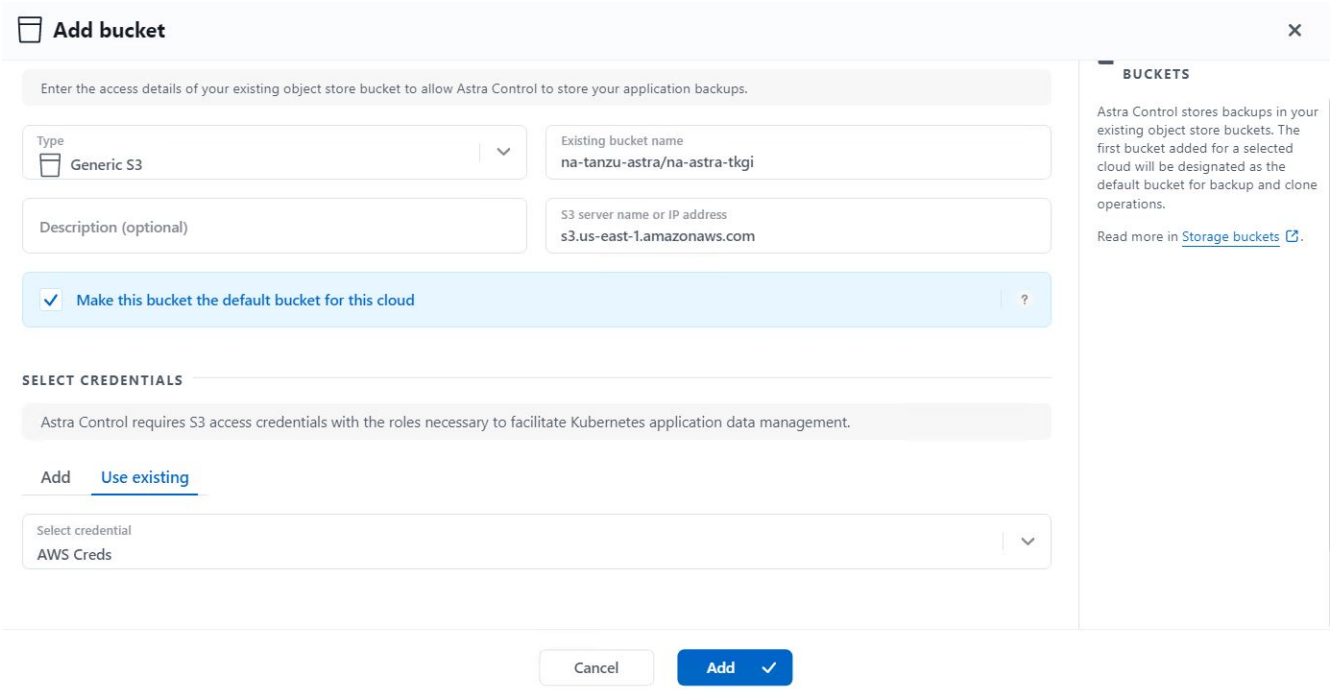
5. Para importar los clústeres de ONTAP, desplácese hasta Back-ends, haga clic en el menú desplegable y seleccione Manage junto al clúster de ONTAP que se va a gestionar. Introduzca las credenciales del clúster de ONTAP, haga clic en revisar información y, a continuación, haga clic en Importar back-end de almacenamiento.



6. Una vez añadidos los back-ends, el estado cambia a Available. Ahora, estos back-ends presentan la información sobre los volúmenes persistentes en el clúster de Kubernetes tanzu y los volúmenes correspondientes en el sistema ONTAP.



7. Para realizar operaciones de backup y restauración en todos los clústeres de Kubernetes de Tanzania mediante Astra Control Center, debe aprovisionar un bloque de almacenamiento de objetos que sea compatible con el protocolo S3. Las opciones admitidas actualmente son ONTAP S3, StorageGRID, AWS S3 y almacenamiento blob de Microsoft Azure. Para el objetivo de esta instalación, vamos a configurar un bloque de AWS S3. Vaya a Buckets, haga clic en Add bucket y seleccione Generic S3. Introduzca los detalles sobre el bloque de S3 y las credenciales para acceder a él, haga clic en la casilla de comprobación Mase this Bucket Default Bucket para el cloud y, a continuación, haga clic en Add.

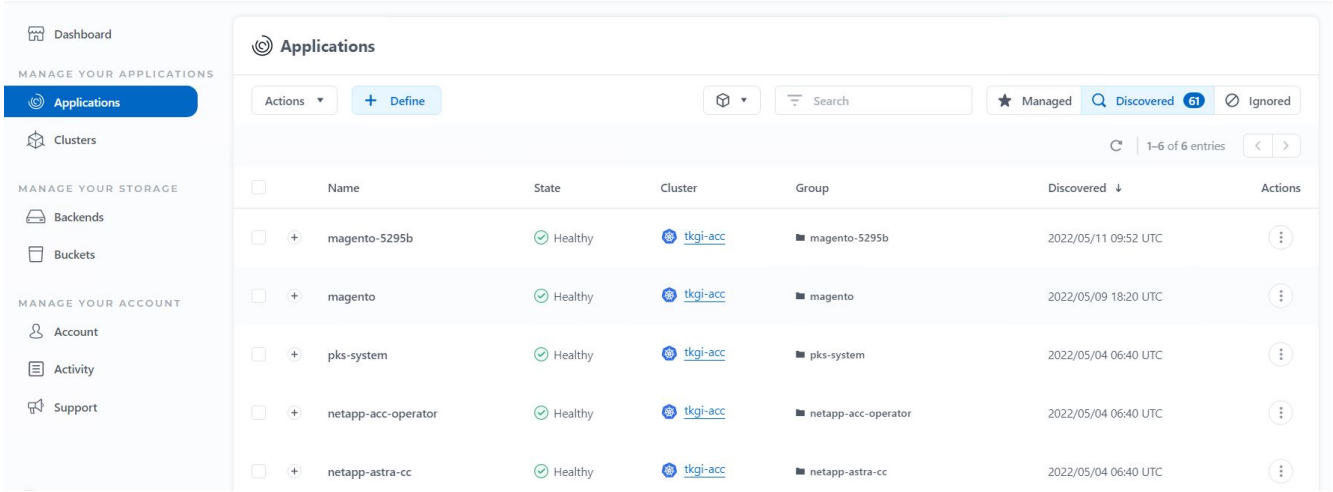


Elija las aplicaciones que desea proteger

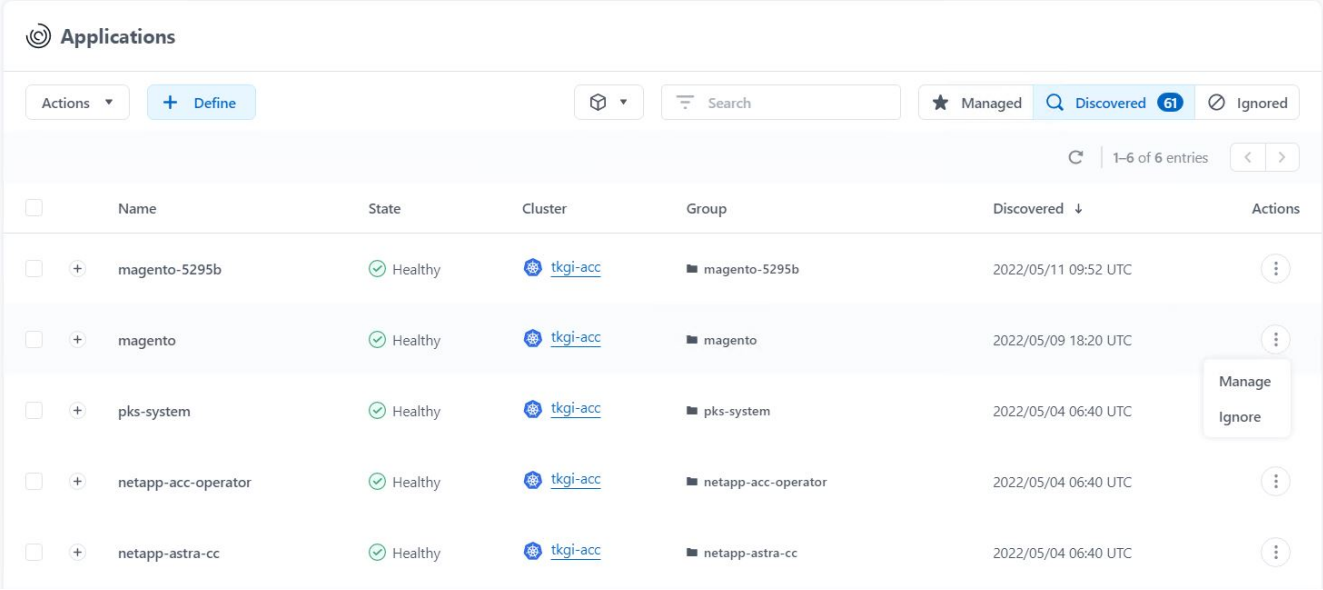
Después de registrar los clústeres de Tanzania Kubernetes, podrá descubrir las aplicaciones que se implementan y gestionan a través de Astra Control Center.

Gestione las aplicaciones

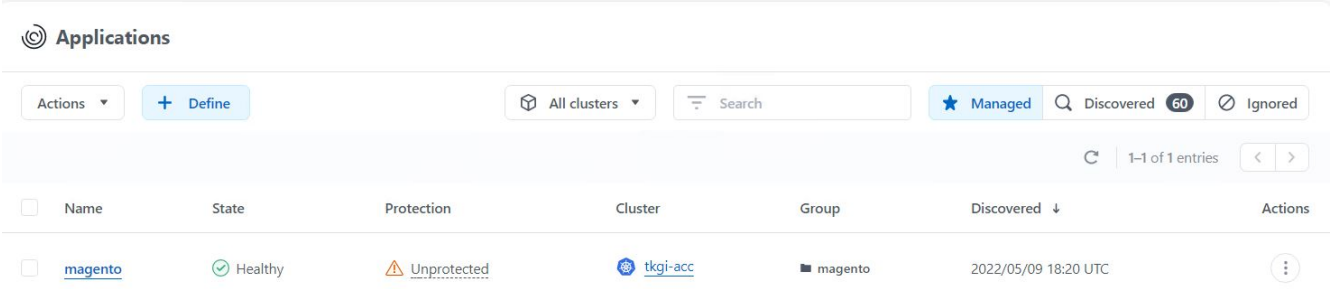
1. Una vez registrados los clústeres de Tanzu Kubernetes y los back-ends de ONTAP en el Centro de control de Astra, el centro de control inicia automáticamente el descubrimiento de las aplicaciones en todos los espacios de nombres que utilizan storageeclcaso configurado con el back-end de ONTAP especificado.



2. Desplácese a aplicaciones > descubiertas y haga clic en el menú desplegable situado junto a la aplicación que desea gestionar mediante Astra. A continuación, haga clic en gestionar.



3. La aplicación entra en el estado disponible y se puede ver en la ficha gestionado de la sección aplicaciones.



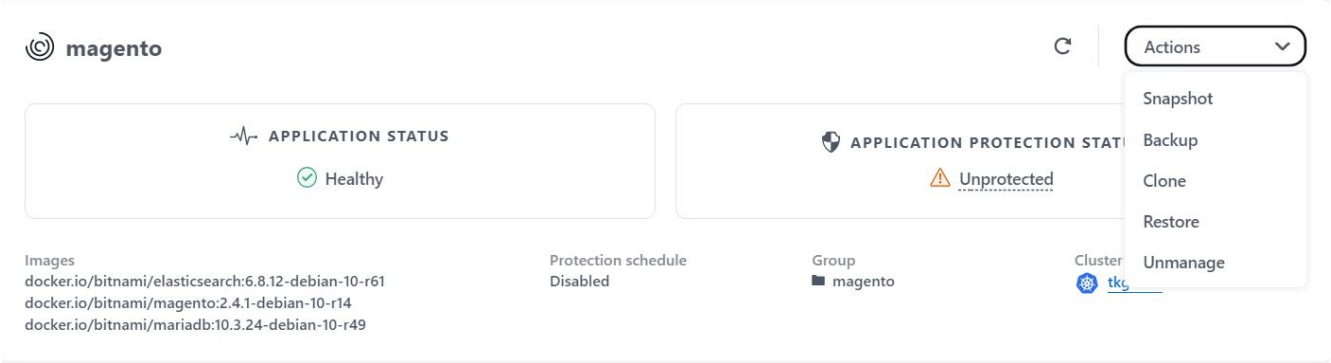
Proteja sus aplicaciones

Una vez que Astra Control Center gestiona las cargas de trabajo de las aplicaciones, puede configurar los ajustes de protección para esas cargas de trabajo.

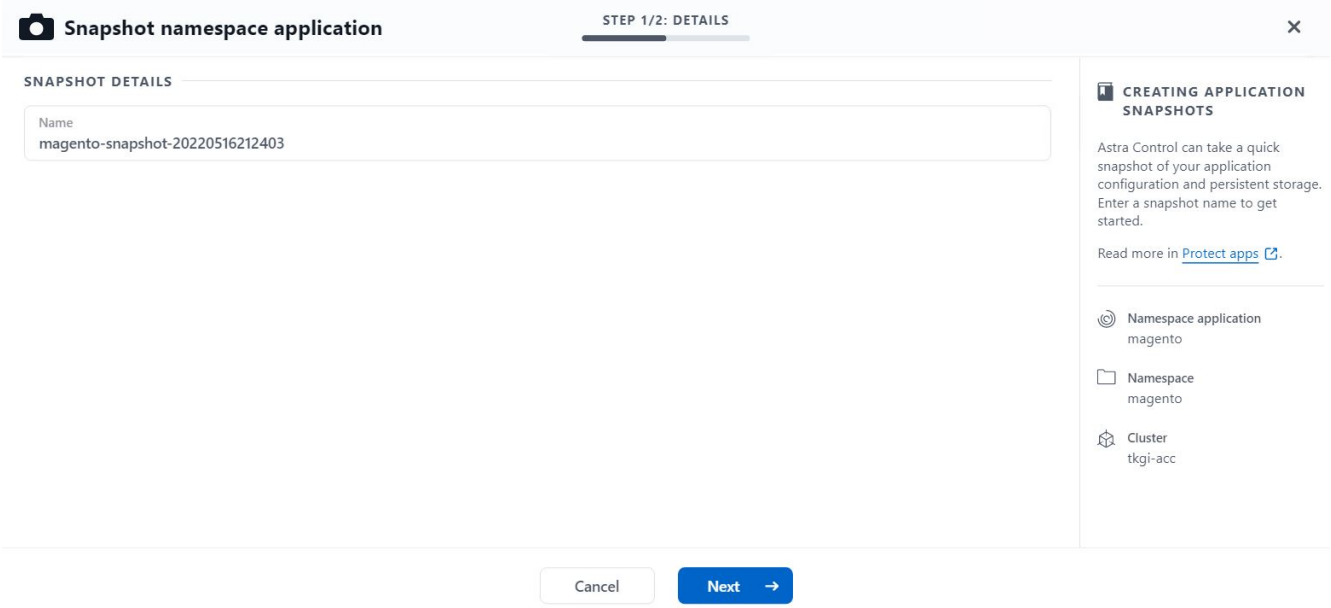
Crear una instantánea de aplicación

Una copia Snapshot de una aplicación crea una copia Snapshot de ONTAP y una copia de los metadatos de la aplicación que se pueden usar para restaurar o clonar la aplicación en un momento específico según esa copia Snapshot.

1. Para tomar una instantánea de la aplicación, desplácese a la ficha aplicaciones > gestionado y haga clic en la aplicación de la que desea realizar una copia snapshot. Haga clic en el menú desplegable junto al nombre de la aplicación y haga clic en Snapshot.



2. Introduzca los detalles de la snapshot, haga clic en Siguiente y luego en Snapshot. La creación de la snapshot tarda aproximadamente un minuto y el estado cambia a disponible después de que se cree correctamente la snapshot.



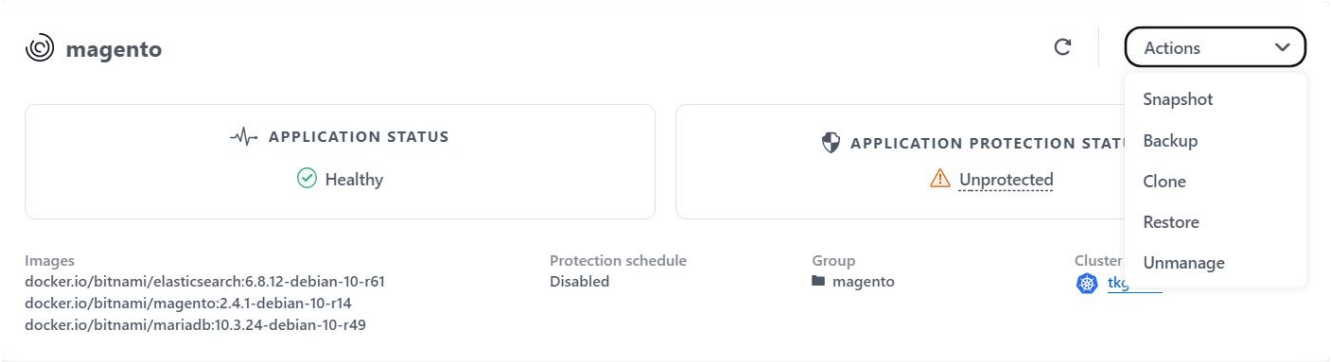
Crear un backup de aplicación

Un backup de una aplicación captura el estado activo de la aplicación y la configuración de sus recursos de TI, los coloca en archivos y los almacena en un bloque de almacenamiento de objetos remotos.

1. Para realizar la copia de seguridad y la restauración de las aplicaciones gestionadas en el Centro de control de Astra, debe configurar los ajustes de superusuario para los sistemas ONTAP de respaldo como requisito previo. Para ello, introduzca los comandos siguientes.

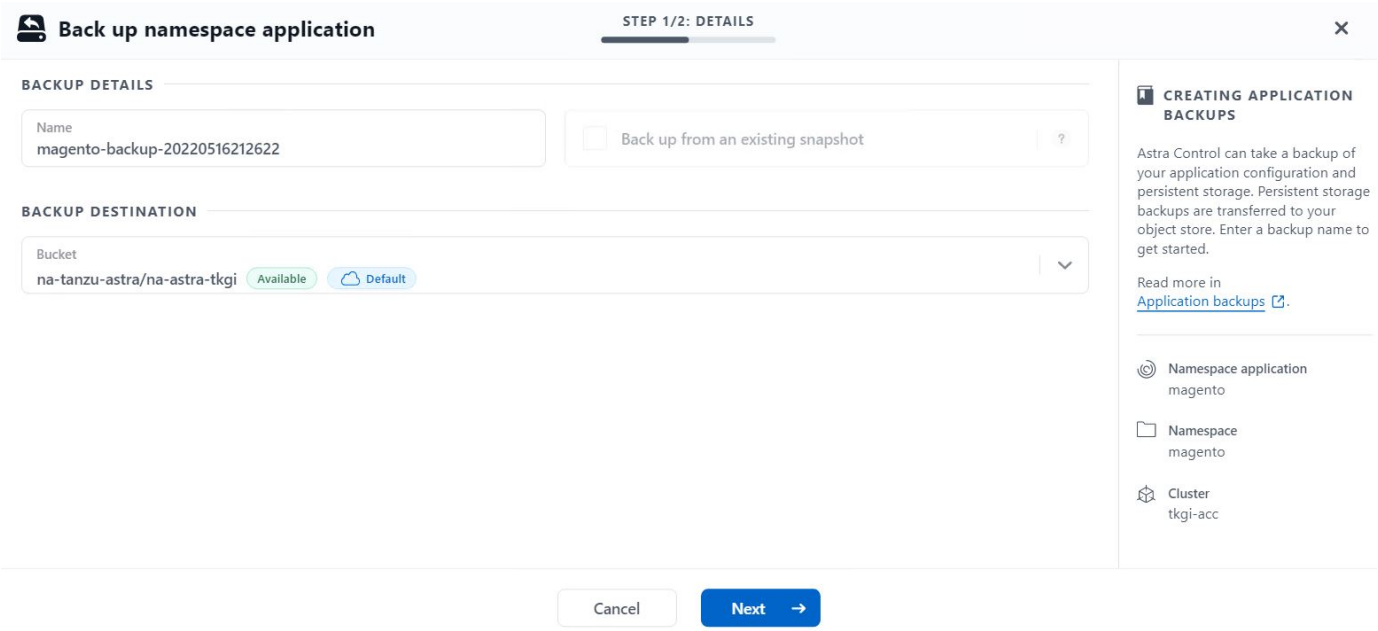
```
ONTAP::> export-policy rule modify -vserver ocp-trident -policyname
default -ruleindex 1 -superuser sys
ONTAP::> export-policy rule modify -policyname default -ruleindex 1
-anon 65534 -vserver ocp-trident
```

2. Para crear una copia de seguridad de la aplicación gestionada en Astra Control Center, desplácese a la ficha aplicaciones > administradas y haga clic en la aplicación de la que desea realizar una copia de seguridad. Haga clic en el menú desplegable junto al nombre de la aplicación y haga clic en copia de seguridad.



3. Introduzca los detalles de la copia de seguridad, seleccione el bloque de almacenamiento de objetos donde se retengan los archivos de copia de seguridad, haga clic en Siguiente y, tras revisar los detalles,

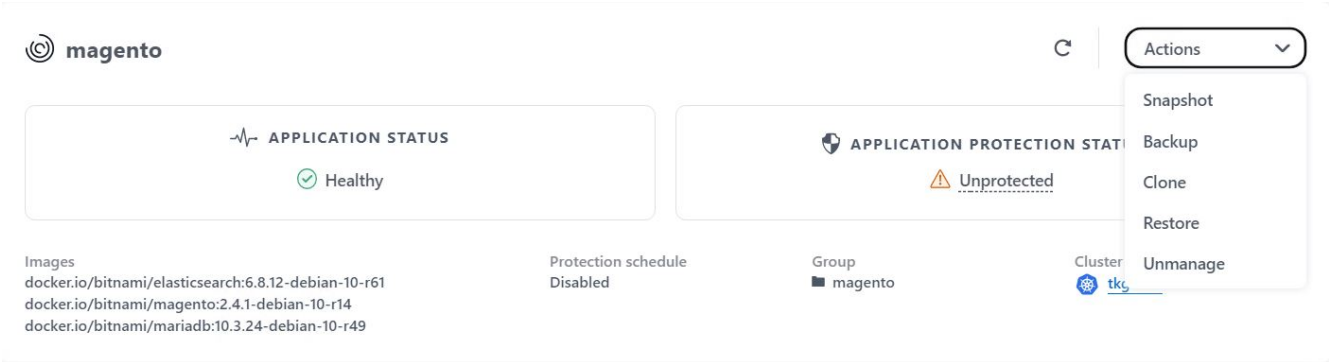
haga clic en Backup. Según el tamaño de la aplicación y los datos, el backup puede tardar varios minutos y el estado del backup pasa a estar disponible después de que el backup se haya completado correctamente.



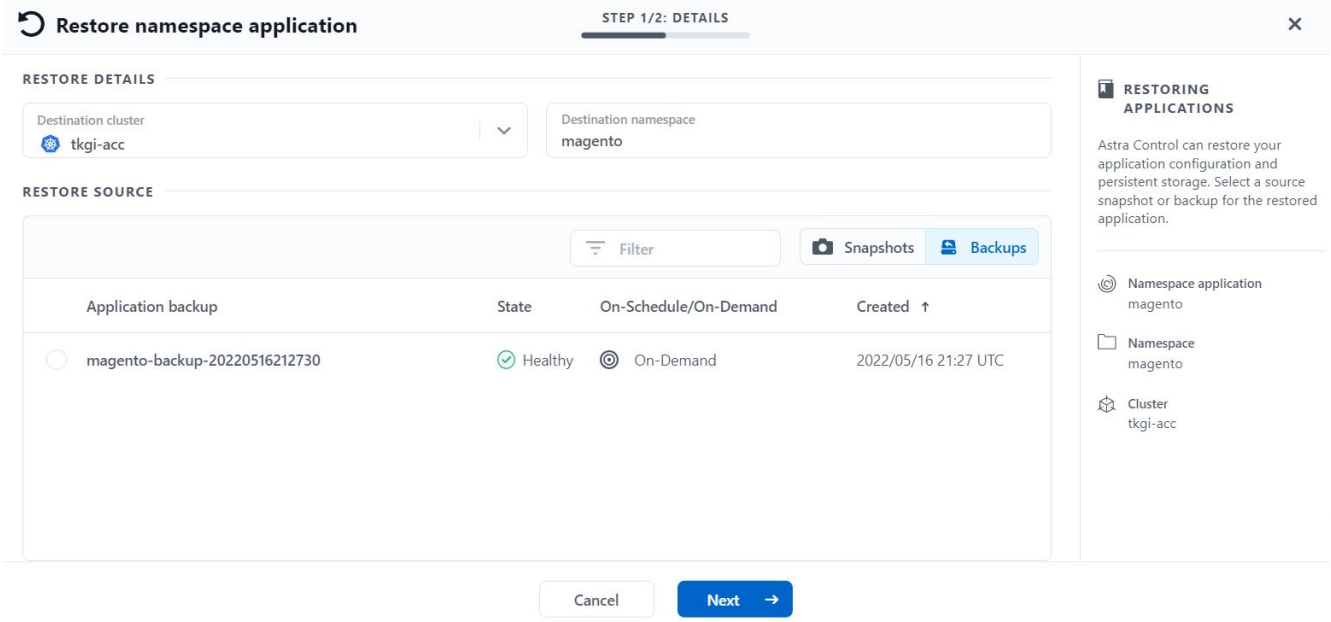
Restaurar una aplicación

Con solo pulsar un botón, puede restaurar una aplicación en el espacio de nombres de origen del mismo clúster o en un clúster remoto para realizar tareas de protección de aplicaciones y recuperación ante desastres.

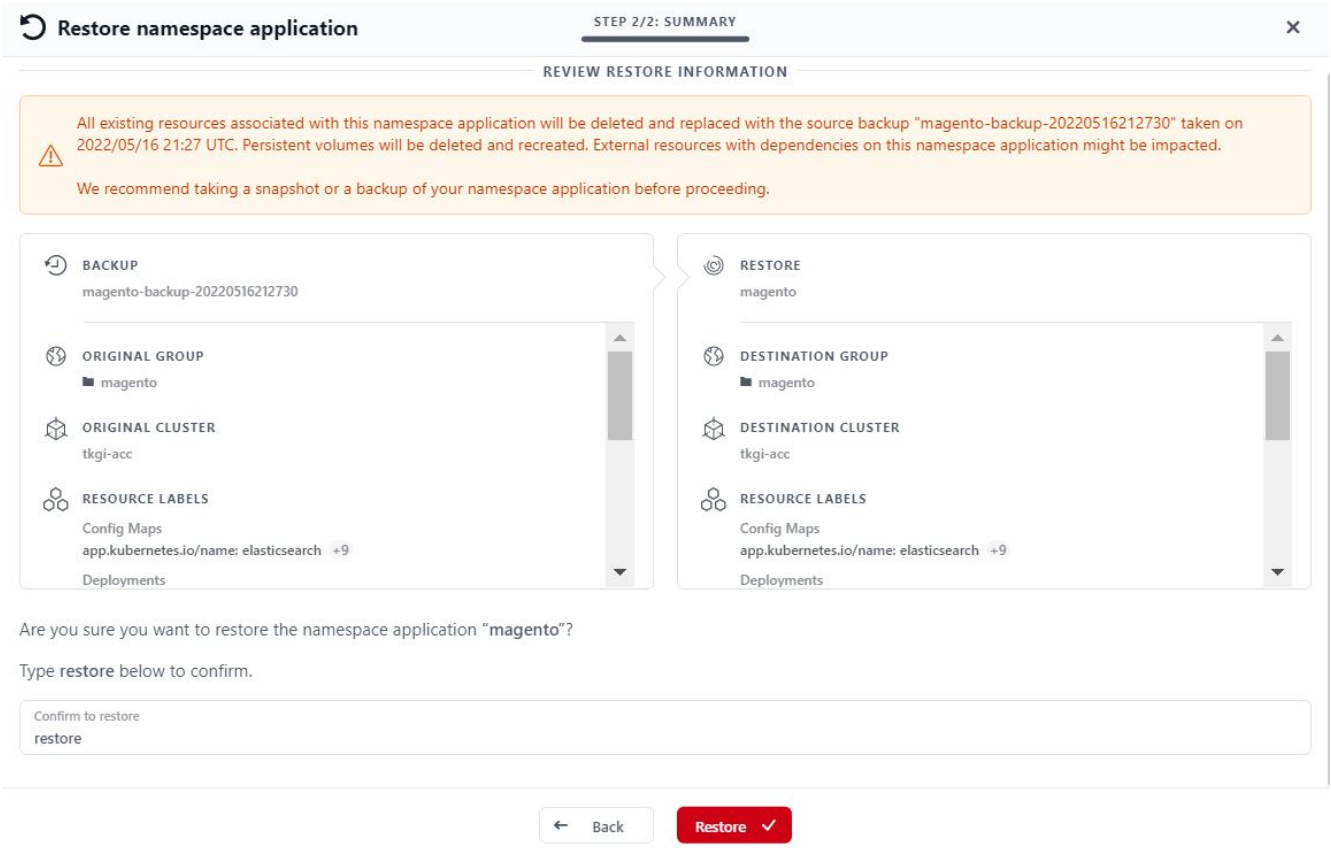
1. Para restaurar una aplicación, desplácese a la ficha aplicaciones > administradas y haga clic en la aplicación en cuestión. Haga clic en el menú desplegable junto al nombre de la aplicación y haga clic en Restaurar.



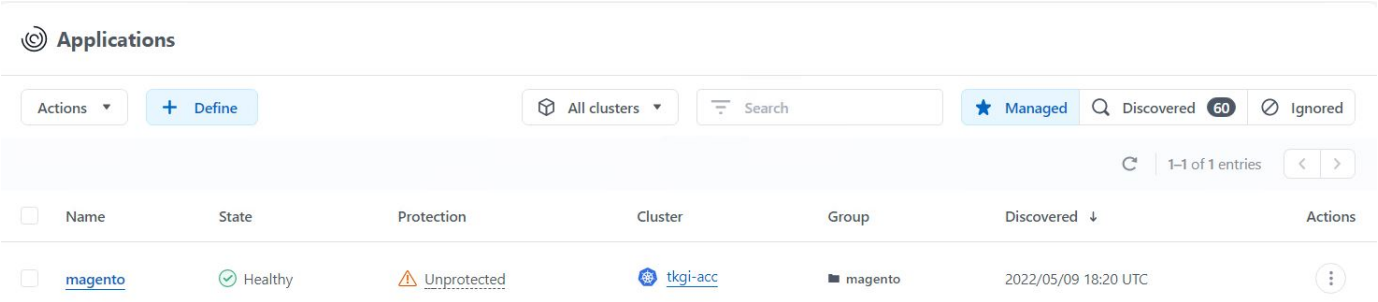
2. Introduzca el nombre del espacio de nombres de la restauración, seleccione el clúster donde desea restaurarlo y elija si desea restaurarlo desde la copia de Snapshot existente o desde el backup de la aplicación. Haga clic en Siguiente.



3. En el panel de revisión, introduzca `restore` Y haga clic en Restaurar después de haber revisado los detalles.



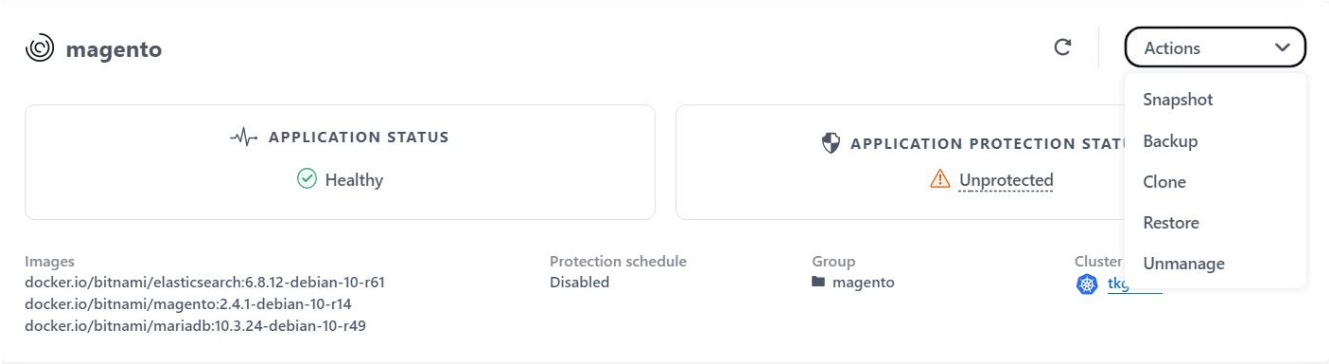
4. La nueva aplicación pasa al estado de restauración mientras Astra Control Center restaura la aplicación en el clúster seleccionado. Una vez que todos los recursos de la aplicación son instalados y detectados por Astra, la aplicación pasa al estado disponible.



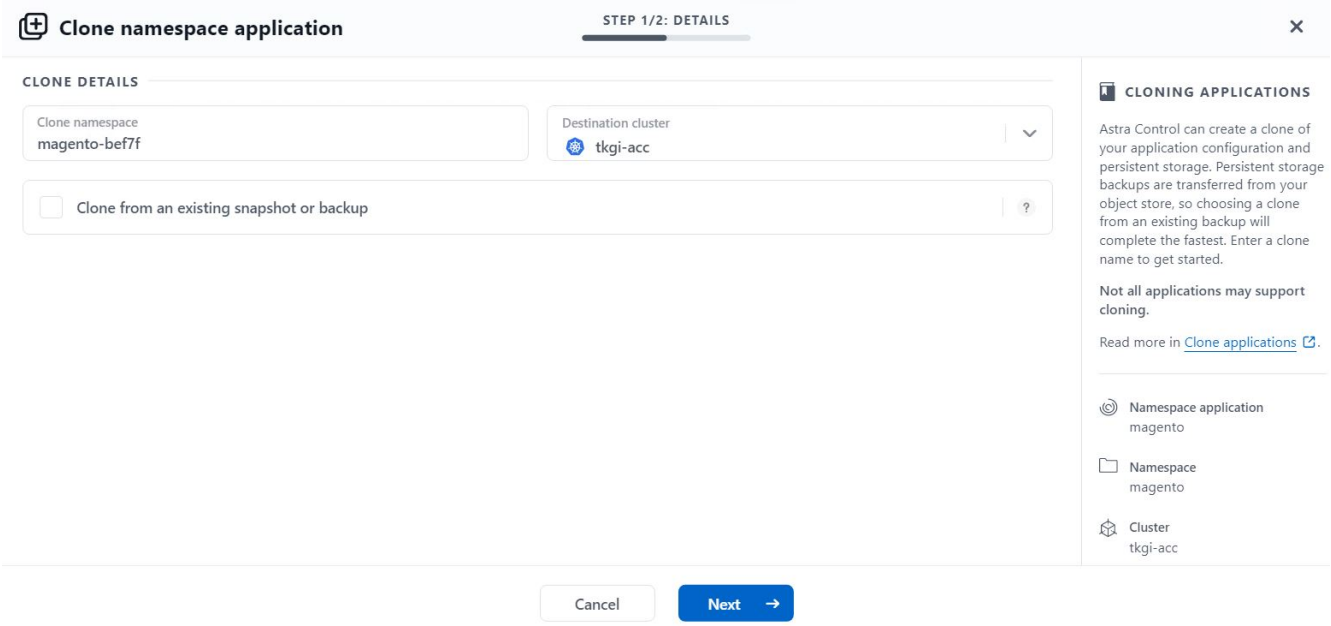
Clonar una aplicación

Es posible clonar una aplicación en el clúster de origen o en un clúster remoto para fines de desarrollo/pruebas o protección de aplicaciones y recuperación ante desastres. La clonado de una aplicación dentro del mismo clúster en el mismo back-end de almacenamiento utiliza la tecnología FlexClone de NetApp, que clona las RVP de forma instantánea y ahorra espacio de almacenamiento.

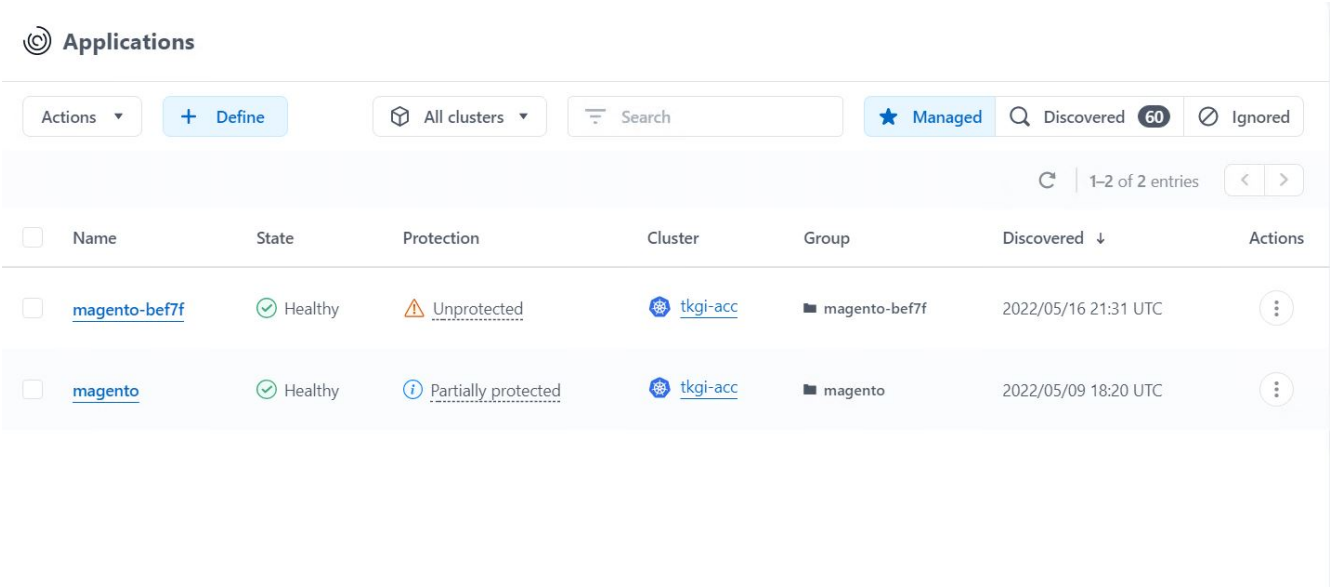
1. Para clonar una aplicación, vaya a la ficha aplicaciones > administradas y haga clic en la aplicación en cuestión. Haga clic en el menú desplegable junto al nombre de la aplicación y haga clic en Clonar.



2. Introduzca los detalles del nuevo espacio de nombres, seleccione el clúster al que desea clonarlo y elija si desea clonarlo desde una snapshot existente, desde un backup o desde el estado actual de la aplicación. Haga clic en Siguiente y, a continuación, en Clonar en el panel de revisión después de haber revisado los detalles.



3. La nueva aplicación pasa al estado de descubrimiento mientras Astra Control Center crea la aplicación en el clúster seleccionado. Una vez que todos los recursos de la aplicación son instalados y detectados por Astra, la aplicación pasa al estado disponible.

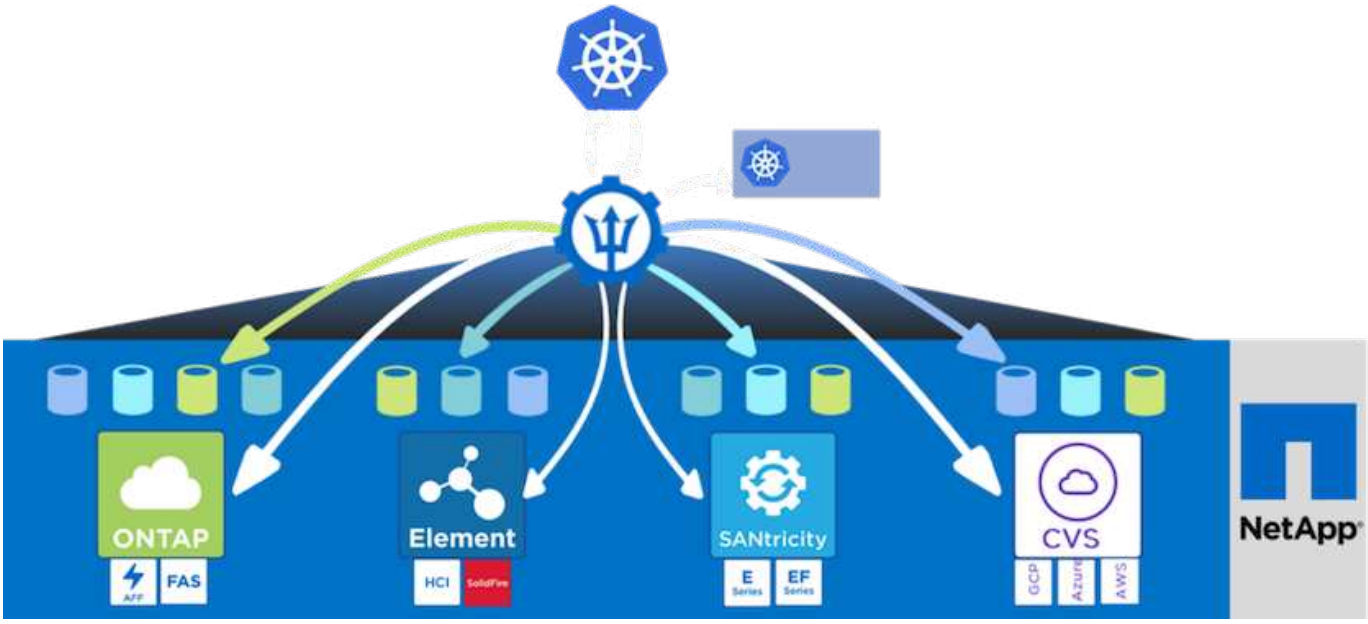


Descripción general de Astra Trident

Astra Trident es un orquestador de almacenamiento de código abierto y totalmente compatible para contenedores y distribuciones de Kubernetes como Red Hat OpenShift, VMware Tanzu, Anthos by Google Cloud, Rancher etc. Trident funciona con toda la cartera de almacenamiento de NetApp, incluidos los sistemas de almacenamiento ONTAP y Element de NetApp, y también admite conexiones NFS e iSCSI. Trident acelera el flujo de trabajo de DevOps al permitir que los usuarios finales aprovisionen y gestionen el almacenamiento desde sus sistemas de almacenamiento de NetApp sin necesidad de intervención del administrador de almacenamiento.

Un administrador puede configurar varios back-ends de almacenamiento a partir de necesidades de proyectos y modelos de sistema de almacenamiento que permiten funciones de almacenamiento avanzadas, como

compresión, tipos de disco específicos o niveles de calidad de servicio que garantizan un cierto nivel de rendimiento. Una vez definidas estos back-ends pueden ser utilizados por los desarrolladores en sus proyectos para crear reclamaciones de volumen persistente (RVP) y conectar almacenamiento persistente a sus contenedores bajo demanda.



Astra Trident tiene un rápido ciclo de desarrollo y, al igual que Kubernetes, se publica cuatro veces al año.

La última versión de Astra Trident se lanzó en abril de 2022 en 22.04. Existe una matriz de compatibilidad con la versión de Trident probada en la que se puede encontrar la distribución de Kubernetes "aquí".

A partir del lanzamiento de la versión 20.04, el operador de Trident realiza la configuración de Trident. El operador facilita las puestas en marcha a gran escala y ofrece soporte adicional, incluida la reparación automática de pods que se implementan como parte de la instalación de Trident.

Con la versión 21.01, se puso a disposición un gráfico Helm para facilitar la instalación del operador Trident.

Ponga en marcha al operador de Trident con Helm

1. En primer lugar, defina la ubicación del clúster de usuarios `kubeconfig` Archivo como variable de entorno para no tener que referirla, porque Trident no tiene opción para pasar este archivo.

```
<<<<<<< HEAD
[netapp-user@rhel7]$ export KUBECONFIG=~/tanzu-install/auth/kubeconfig
=======
[netapp-user@rhel7]$ export KUBECONFIG=~/Tanzu-install/auth/kubeconfig
>>>>>>> eba1007b77b1ef6011dadd158f1df991acc5299f
```

2. Añada el repositorio del timón de NetApp Astra Trident.

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

3. Actualizar los repositorios del timón.

```
[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. Cree un nuevo espacio de nombres para la instalación de Trident.

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

5. Cree un secreto con las credenciales de DockerHub para descargar las imágenes de 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. Para los clústeres de usuarios o cargas de trabajo gestionados por TKGS (vSphere con tanzu) o TKG con implementaciones de clústeres de gestión, complete el siguiente procedimiento para instalar Astra Trident:
   a. Asegúrese de que el usuario que ha iniciado sesión tiene los permisos para crear cuentas de servicio en el espacio de nombres de trident y de que las cuentas de servicio en el espacio de nombres de trident tienen los permisos para crear POD.
   b. Ejecute el comando siguiente timón para instalar el operador Trident en el espacio de nombres creado.

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

7. Para un usuario o clúster de cargas de trabajo gestionado por implementaciones TKGI, ejecute el siguiente comando helm para instalar el operador Trident en el espacio de nombres creado.

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

8. Compruebe que los pods de Trident estén activos y en ejecución.

```
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          |
+----------------+----------------+
```

Cree back-ends del sistema de almacenamiento

Una vez finalizada la instalación del operador de Astra Trident, debe configurar el back-end para la plataforma de almacenamiento específica de NetApp que esté usando. Siga los siguientes enlaces para continuar con la instalación y configuración de Astra Trident.

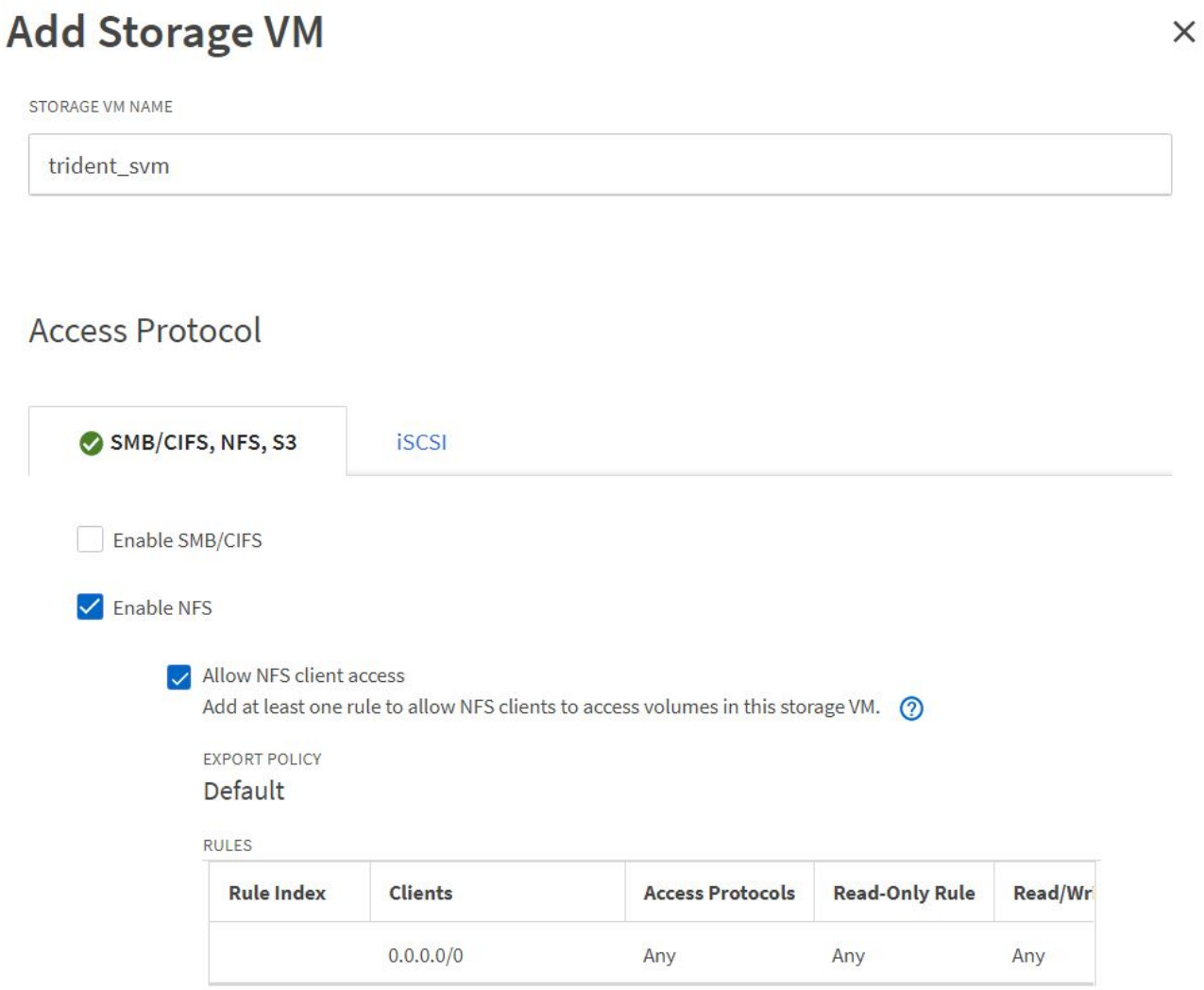
- "NFS de ONTAP de NetApp"
- "ISCSI de ONTAP de NetApp"

Configuración NFS de ONTAP de NetApp

Para habilitar la integración de Trident con el sistema de almacenamiento ONTAP de NetApp mediante NFS, debe crear un back-end que permita la comunicación con el sistema de almacenamiento. Configuramos un back-end básico en esta solución, pero si busca opciones más personalizadas, visite la documentación "aquí".

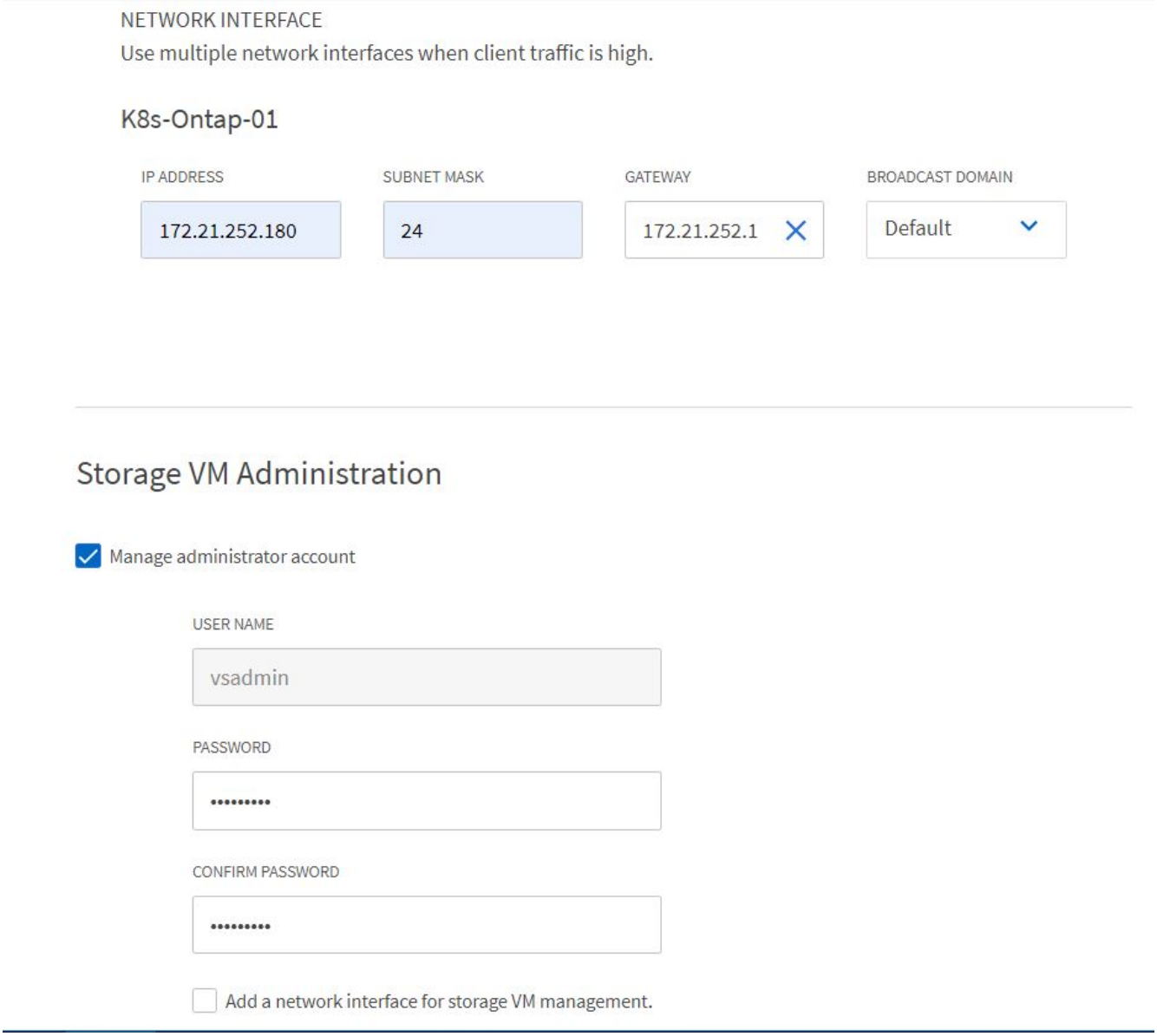
Cree una SVM en ONTAP

1. Inicie sesión en el Administrador del sistema de ONTAP, desplácese hasta almacenamiento > Storage VMs y haga clic en Add.
2. Introduzca un nombre para la SVM, habilite el protocolo NFS, active la casilla de comprobación allow NFS Client Access y añada las subredes en las reglas de política de exportación para permitir el montaje de los volúmenes como VP en los clústeres de carga de trabajo.

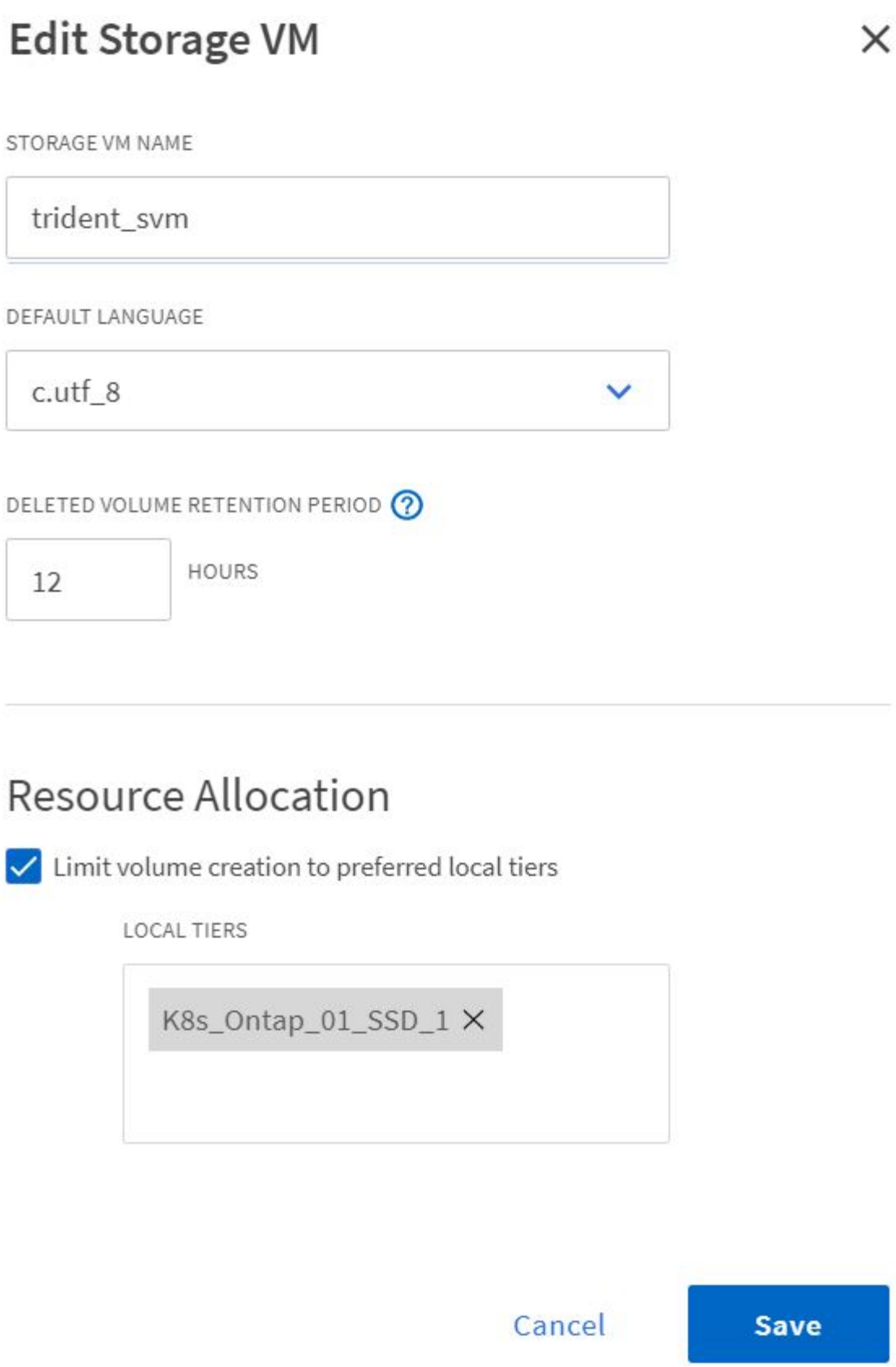


Si está utilizando NAT'ed despliegues de clústeres de usuarios o clústeres de cargas de trabajo con NSX-T, debe agregar la subred Egress (en el caso de TKGS0 o la subred Floating IP (en el caso de TKGI) a las reglas de la política de exportación.

3. Proporcione los detalles de las LIF de datos y los detalles de la cuenta de administración de SVM y, a continuación, haga clic en Save.



4. Asigne los agregados a una SVM. Desplácese hasta almacenamiento > Storage VMs, haga clic en los tres puntos junto a la SVM recién creada y, a continuación, haga clic en Edit. Active la casilla de comprobación Limit Volume Creation to Preferred local Tiers y adjunte los agregados necesarios.



5. En caso de implementaciones en NAT de clústeres de usuarios o cargas de trabajo en los que se instale Trident, la solicitud de montaje del almacenamiento puede llegar desde un puerto no estándar debido a SNAT. De forma predeterminada, ONTAP solo permite las solicitudes de montaje del volumen cuando se

origina desde el puerto raíz. Por lo tanto, inicie sesión en la CLI de ONTAP y modifique la configuración para permitir las solicitudes de montaje de puertos no estándares.

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

Cree back-ends y StorageClass

1. Para los sistemas ONTAP de NetApp que sirven NFS, cree un archivo de configuración de back-end en el host con backendName, managementLIF, dataLIF, svm, username, contraseña y otros detalles.

```
{
    "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"
}
```

> Se recomienda definir el valor de backendName personalizado como una combinación de storageDriverName y DataLIF que sirve NFS para una identificación sencilla.

2. Ejecute el siguiente comando para crear el back-end de Trident.

```
[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. Con el back-end creado, debe crear después una clase de almacenamiento. La siguiente definición de clase de almacenamiento de ejemplo resalta los campos necesarios y básicos. El parámetro `backendType` Debe reflejar el controlador de almacenamiento desde el back-end de Trident recién creado.

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

4. Cree la clase de almacenamiento con el comando kubectl.

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

5. Con la clase de almacenamiento creada, debe crear la primera reclamación de volumen persistente (RVP). A continuación se proporciona una definición de PVC de muestra. Compruebe que la `storageClassName` el campo coincide con el nombre de la clase de almacenamiento que se acaba de crear. La definición de PVC se puede personalizar aún más según sea necesario, en función de la carga de trabajo que se vaya a aprovisionar.

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

6. Cree la RVP emitiendo el comando kubectl. La creación puede tardar un poco de tiempo, según el tamaño del volumen de backup que se esté creando, para que pueda ver el proceso a medida que finalice.

```
[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
```

Configuración de iSCSI de ONTAP de NetApp

Para integrar el sistema de almacenamiento ONTAP de NetApp con clústeres Kubernetes de VMware Tanzania para volúmenes persistentes a través de iSCSI, el primer paso es preparar los nodos iniciando sesión en cada nodo y configurando las utilidades o paquetes iSCSI para montar volúmenes iSCSI. Para ello, siga el procedimiento establecido en este documento "enlace".

> NetApp no recomienda este procedimiento para las puestas en marcha NAT de clústeres VMware Tanzania Kubernetes.

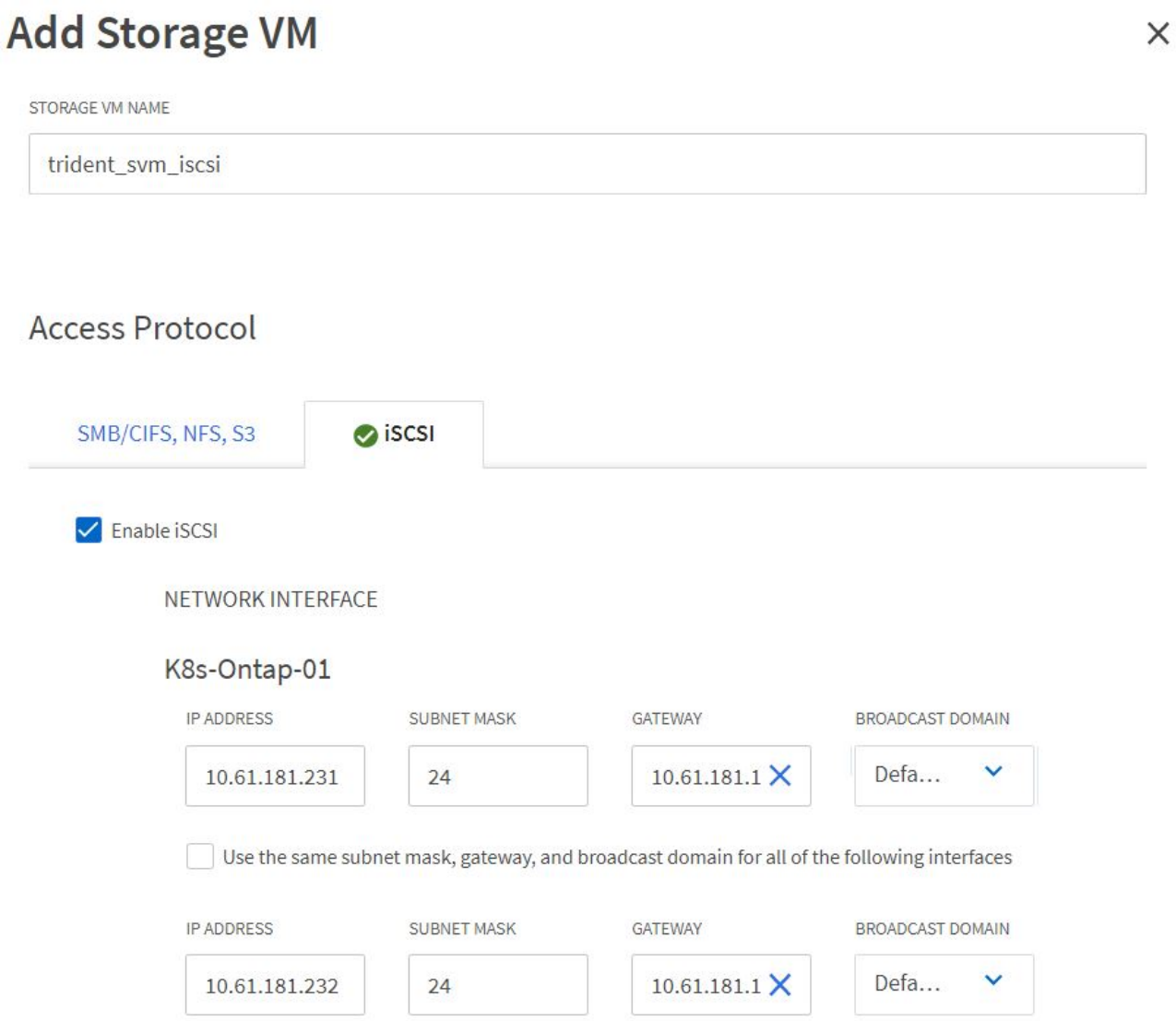
> TKGI utiliza máquinas virtuales bosh como nodos para clústeres de Kubernetes tanzu que ejecutan imágenes de configuración inmutables y cualquier cambio manual de paquetes iSCSI en equipos virtuales bosh no permanece constante entre reinicios. Por lo tanto, NetApp recomienda el uso de volúmenes NFS para el almacenamiento persistente de clústeres de Kubernetes tanzu puestos en marcha y operados por TKGI.

Una vez que los nodos del clúster se han preparado para los volúmenes iSCSI, debe crear un back-end que permita la comunicación con el sistema de almacenamiento. Hemos configurado un back-end básico en esta solución pero, si busca opciones más personalizadas, visite la documentación "aquí".

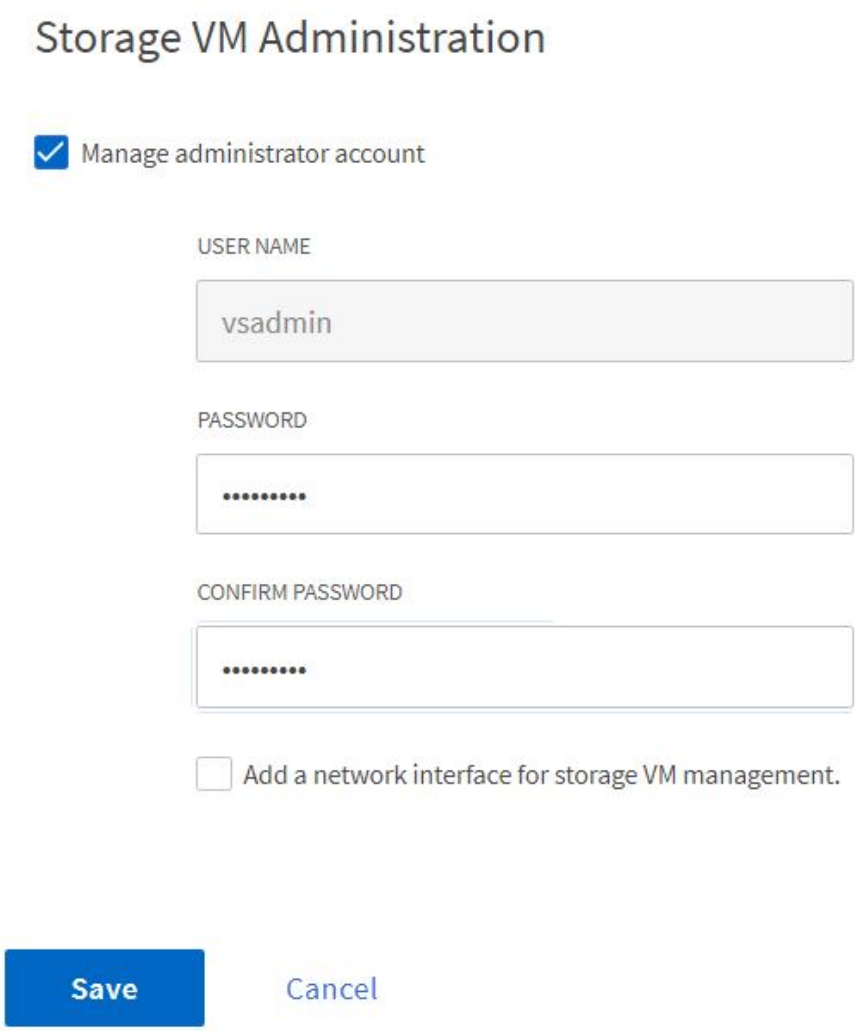
Cree una SVM en ONTAP

Para crear una SVM en ONTAP, complete los siguientes pasos:

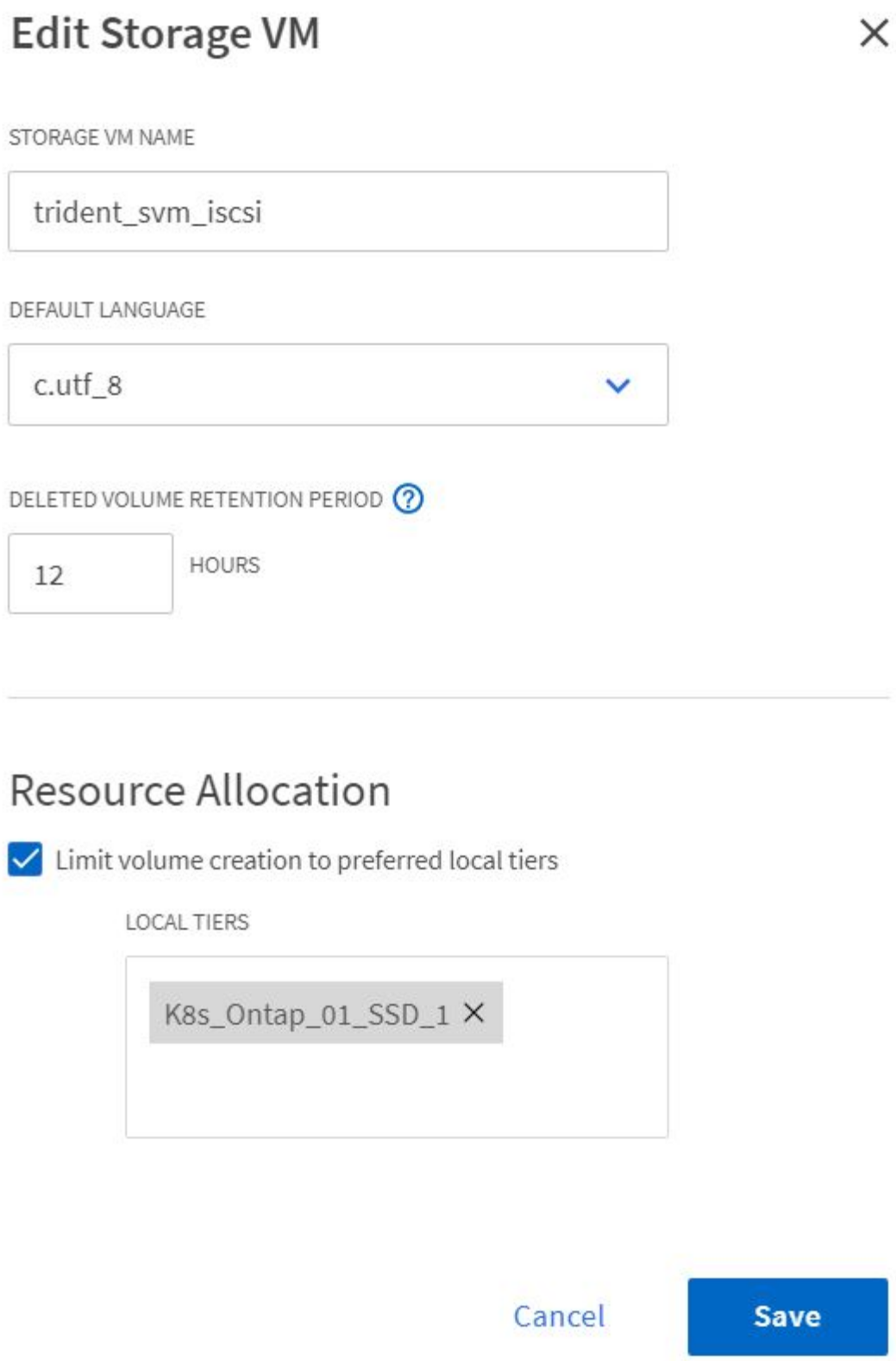
1. Inicie sesión en el Administrador del sistema de ONTAP, desplácese hasta almacenamiento > Storage VMs y haga clic en Add.
2. Escriba un nombre para la SVM, habilite el protocolo iSCSI y a continuación, proporcione detalles para las LIF de datos.



3. Introduzca los detalles de la cuenta de administración de la SVM y, a continuación, haga clic en Save.



4. Para asignar los agregados a la SVM, desplácese a almacenamiento > Storage VMs, haga clic en los tres puntos junto a la SVM recién creada y, a continuación, haga clic en Edit. Active la casilla de comprobación Limit Volume Creation to Preferred local Tiers y adjunte los agregados necesarios.



Cree back-ends y StorageClass

1. Para los sistemas ONTAP de NetApp que sirven NFS, cree un archivo de configuración de back-end en el host con backendName, managementLIF, dataLIF, svm, username, contraseña y otros detalles.

```
{
  "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. Ejecute el siguiente comando para crear el back-end de Trident.

```
[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. Tras crear un back-end, debe crear después una clase de almacenamiento. La siguiente definición de clase de almacenamiento de ejemplo resalta los campos necesarios y básicos. El parámetro `backendType` Debe reflejar el controlador de almacenamiento desde el back-end de Trident recién creado. Observe también el valor del campo de nombre, al que se debe hacer referencia en un paso posterior.

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

> Hay un campo opcional llamado `fsType` que se define en este archivo. En los back-ends iSCSI, este valor se puede establecer en un tipo de sistema de archivos Linux específico (XFS, ext4, etc.) o se puede eliminar para permitir a los clústeres de Kubernetes de Tanzania decidir qué sistema de archivos utilizar.

4. Cree la clase de almacenamiento con el comando kubectl.

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

5. Con la clase de almacenamiento creada, debe crear la primera reclamación de volumen persistente (RVP). A continuación se proporciona una definición de PVC de muestra. Compruebe que la `storageClassName` el campo coincide con el nombre de la clase de almacenamiento que se acaba de crear. La definición de PVC se puede personalizar aún más según sea necesario, en función de la carga de trabajo que se vaya a aprovisionar.

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

6. Cree la RVP emitiendo el comando kubectl. La creación puede tardar un poco de tiempo, según el tamaño del volumen de backup que se esté creando, para que pueda ver el proceso a medida que finalice.

```
[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
```