



Información general de la instalación

Astra Control Center

NetApp

November 21, 2023

This PDF was generated from https://docs.netapp.com/es-es/astra-control-center-2208/get-started/acc_cluster_cr_options.html on November 21, 2023. Always check docs.netapp.com for the latest.

Tabla de contenidos

- Información general de la instalación. 1
 - Instale Astra Control Center mediante el proceso estándar. 1
 - Instale Astra Control Center utilizando OpenShift OperatorHub 27
 - Instale Astra Control Center con un back-end de almacenamiento de Cloud Volumes ONTAP 34

Información general de la instalación

Elija y complete uno de los siguientes procedimientos de instalación de Astra Control Center:

- ["Instale Astra Control Center mediante el proceso estándar"](#)
- ["\(Si utiliza Red Hat OpenShift\) instale Astra Control Center mediante OpenShift OperatorHub"](#)
- ["Instale Astra Control Center con un back-end de almacenamiento de Cloud Volumes ONTAP"](#)

Instale Astra Control Center mediante el proceso estándar

Para instalar Astra Control Center, descargue el paquete de instalación desde el sitio de soporte de NetApp y realice los siguientes pasos para instalar Astra Control Center Operator y Astra Control Center en su entorno. Puede utilizar este procedimiento para instalar Astra Control Center en entornos conectados a Internet o con conexión por aire.

Para entornos Red Hat OpenShift, puede utilizar un ["procedimiento alternativo"](#) Para instalar Astra Control Center con OpenShift OperatorHub.

Lo que necesitará

- ["Antes de comenzar la instalación, prepare su entorno para la implementación de Astra Control Center"](#).
- Si ha configurado o desea configurar directivas de seguridad de POD en su entorno, familiarícese con las directivas de seguridad de POD y cómo afectan a la instalación de Astra Control Center. Consulte ["Comprender las restricciones de directivas de seguridad de POD"](#).
- Asegurarse de que todos los operadores del clúster se encuentren en estado correcto y estén disponibles.

```
kubectl get clusteroperators
```

- Asegúrese de que todos los servicios de API se encuentren en buen estado y estén disponibles:

```
kubectl get apiservices
```

- Asegúrese de que el FQDN de Astra que tiene previsto utilizar se puede enrutar a este clúster. Esto significa que tiene una entrada DNS en el servidor DNS interno o que está utilizando una ruta URL principal que ya está registrada.
- Si ya existe un administrador de certificados en el clúster, tendrá que realizar algunos ["requisitos previos"](#) Por lo tanto, Astra Control Center no instala su propio cert-Manager.

Acerca de esta tarea

El proceso de instalación de Astra Control Center realiza lo siguiente:

- Instala los componentes de Astra en `netapp-acc` (o nombre personalizado).
- Crea una cuenta predeterminada.
- Establece una dirección de correo electrónico de usuario administrativo predeterminada y una contraseña única predeterminada. A este usuario se le asigna el rol de propietario del sistema que se necesita para iniciar sesión por primera vez en la interfaz de usuario.

- Le ayuda a determinar que se están ejecutando todas las pods de Astra Control Center.
- Instala la interfaz de usuario de Astra.



(Se aplica sólo a la versión Astra Data Store Early Access Program (EAP)) Si tiene intención de gestionar Astra Data Store mediante Astra Control Center y habilitar los flujos de trabajo de VMware, implemente Astra Control Center únicamente en `pcloud` espacio de nombres y no en `netapp-acc` espacio de nombres o un espacio de nombres personalizado que se describe en los pasos de este procedimiento.



No ejecute el siguiente comando durante todo el proceso de instalación para evitar eliminar todas las POD de Astra Control Center: `kubectl delete -f astra_control_center_operator_deploy.yaml`



Si utiliza Podman de Red Hat en lugar de Docker Engine, los comandos de Podman se pueden utilizar en lugar de los comandos de Docker.

Pasos

Para instalar Astra Control Center, lleve a cabo los siguientes pasos:

- [Descargue y desembale el paquete Astra Control Center](#)
- [Instale el complemento Astra kubectl de NetApp](#)
- [Agregue las imágenes al registro local](#)
- [Configurar espacio de nombres y secreto para registros con requisitos de autenticación](#)
- [Instale el operador de Astra Control Center](#)
- [Configurar Astra Control Center](#)
- [Complete la instalación del centro de control de Astra y del operador](#)
- [Comprobar el estado del sistema](#)
- [Configure la entrada para el equilibrio de carga](#)
- [Inicie sesión en la interfaz de usuario de Astra Control Center](#)

Descargue y desembale el paquete Astra Control Center

1. Descargue el paquete Astra Control Center (`astra-control-center-[version].tar.gz`) del ["Sitio de soporte de NetApp"](#).
2. Descargue el archivo zip de los certificados y claves de Astra Control Center de ["Sitio de soporte de NetApp"](#).
3. (Opcional) Use el siguiente comando para verificar la firma del paquete:

```
openssl dgst -sha256 -verify AstraControlCenter-public.pub -signature
astra-control-center-[version].tar.gz.sig astra-control-center-
[version].tar.gz
```

4. Extraiga las imágenes:

```
tar -vxzf astra-control-center-[version].tar.gz
```

Instale el complemento Astra kubectl de NetApp

La Astra de NetApp `kubectl` El complemento de línea de comandos ahorra tiempo al realizar tareas comunes asociadas con la implementación y actualización de Astra Control Center.

Lo que necesitará

NetApp proporciona binarios para el complemento para distintas arquitecturas de CPU y sistemas operativos. Debe saber qué CPU y sistema operativo tiene antes de realizar esta tarea. En los sistemas operativos Linux y Mac, puede utilizar `uname -a` comando para recopilar esta información.

Pasos

1. Enumere la Astra de NetApp disponible `kubectl` Haga un complemento para binarios y anote el nombre del archivo que necesita para su sistema operativo y arquitectura de CPU:

```
ls kubectl-astra/
```

2. Copie el archivo en la misma ubicación que el estándar `kubectl` utilidad. En este ejemplo, la `kubectl` la utilidad se encuentra en `/usr/local/bin` directorio. Sustituya `<binary-name>` con el nombre del archivo que necesita:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Agregue las imágenes al registro local

1. Complete la secuencia de pasos apropiada para el motor del contenedor:

Docker

1. Cambie al directorio Astra:

```
cd acc
```

2. Push las imágenes del paquete del directorio imagen de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el comando:

- Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, acc.manifest.yaml).
- Sustituya MY_REGISTRATION por la URL del repositorio de Docker.
- Sustituya MY_REGISTRATION_USER por el nombre de usuario.
- Sustituya MY_REGISTRATION_TOKEN por un token autorizado para el registro.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY  
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Inicie sesión en su registro:

```
podman login [your_registry_path]
```

2. Ejecute el siguiente script, haciendo la sustitución de <YOUR_REGISTRY> como se indica en los comentarios:

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
    # Load to local cache
    astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //'')

    # Remove path and keep imageName.
    astraImageNoPath=$(echo ${astraImage} | sed 's:.*/:::')

    # Tag with local image repo.
    podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

    # Push to the local repo.
    podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

Configurar espacio de nombres y secreto para registros con requisitos de autenticación

1. Exporte el KUBECONFIG para el clúster de host de Astra Control Center:

```
export KUBECONFIG=[file path]
```

2. Si utiliza un registro que requiere autenticación, debe hacer lo siguiente:

- a. Cree el netapp-acc-operator espacio de nombres:

```
kubectl create ns netapp-acc-operator
```

Respuesta:

```
namespace/netapp-acc-operator created
```

- b. Cree un secreto para netapp-acc-operator espacio de nombres. Añada información sobre Docker y ejecute el siguiente comando:



El marcador de posición `your_registry_path` debe coincidir con la ubicación de las imágenes que ha cargado anteriormente (por ejemplo, `[Registry_URL]/netapp/astra/astracc/22.08.1-26`).

```
kubectl create secret docker-registry astra-registry-cred -n netapp-acc-operator --docker-server=[your_registry_path] --docker-username=[username] --docker-password=[token]
```

Respuesta de ejemplo:

```
secret/astra-registry-cred created
```



Si elimina el espacio de nombres después de que se genere el secreto, deberá volver a generar el secreto para el espacio de nombres después de volver a crear el espacio de nombres.

- c. Cree el netapp-acc (o espacio de nombres personalizado).

```
kubectl create ns [netapp-acc or custom namespace]
```

Respuesta de ejemplo:

```
namespace/netapp-acc created
```

- d. Cree un secreto para netapp-acc (o espacio de nombres personalizado). Añada información sobre Docker y ejecute el siguiente comando:

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-acc or custom namespace] --docker-server=[your_registry_path] --docker-username=[username] --docker-password=[token]
```

Respuesta

```
secret/astra-registry-cred created
```


- a. `[[substep_kubeconfig_secret]]`(opcional) Si desea que el clúster sea gestionado automáticamente por Astra Control Center después de la instalación, asegúrese de proporcionar el kubeconfig como secreto dentro del espacio de nombres Astra Control Center que tiene intención de implementar utilizando este comando:

```
kubectl create secret generic [acc-kubeconfig-cred or custom secret name] --from-file=<path-to-your-kubeconfig> -n [netapp-acc or custom namespace]
```

Instale el operador de Astra Control Center

1. Cambie el directorio:

```
cd manifests
```

2. Edite la implementación del operador de Astra Control Center YAML (`astra_control_center_operator_deploy.yaml`) para referirse a su registro local y secreto.

```
vim astra_control_center_operator_deploy.yaml
```



Una muestra anotada de AYLMA sigue estos pasos.

- a. Si utiliza un registro que requiere autenticación, reemplace la línea predeterminada de `imagePullSecrets: []` con lo siguiente:

```
imagePullSecrets:
- name: <astra-registry-cred>
```

- b. Cambiar `[your_registry_path]` para la `kube-rbac-proxy` imagen a la ruta del registro en la que se insertó la imagen en un [paso anterior](#).
- c. Cambiar `[your_registry_path]` para la `acc-operator-controller-manager` imagen a la ruta del registro en la que se insertó la imagen en un [paso anterior](#).
- d. (Para instalaciones que utilizan la vista previa de Astra Data Store) Consulte este problema conocido con respecto a "[Los aprovisionadores de clases de almacenamiento y los cambios adicionales que deberá realizar en la YAML](#)".

```

apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
    name: acc-operator-controller-manager
    namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
        - args:
            - --secure-listen-address=0.0.0.0:8443
            - --upstream=http://127.0.0.1:8080/
            - --logtostderr=true
            - --v=10
          image: [your_registry_path]/kube-rbac-proxy:v4.8.0
          name: kube-rbac-proxy
          ports:
            - containerPort: 8443
              name: https
        - args:
            - --health-probe-bind-address=:8081
            - --metrics-bind-address=127.0.0.1:8080
            - --leader-elect
          command:
            - /manager
          env:
            - name: ACCOP_LOG_LEVEL
              value: "2"
          image: [your_registry_path]/acc-operator:[version x.y.z]
          imagePullPolicy: IfNotPresent
      imagePullSecrets: []

```

3. Instale el operador de Astra Control Center:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Respuesta de ejemplo:

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io created
role.rbac.authorization.k8s.io/acc-operator-leader-election-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role created
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
created
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role created
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding created
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding created
configmap/acc-operator-manager-config created
service/acc-operator-controller-manager-metrics-service created
deployment.apps/acc-operator-controller-manager created
```

4. Verifique que los pods se estén ejecutando:

```
kubectl get pods -n netapp-acc-operator
```

Configurar Astra Control Center

1. Edite el archivo de recursos personalizados (CR) del Centro de control de Astra (astra_control_center_min.yaml) Para realizar las configuraciones de cuenta, AutoSupport, Registro y otras necesarias:



astra_control_center_min.yaml Es la CR predeterminada y es adecuada para la mayoría de las instalaciones. Familiarícese con todos "[Opciones CR y sus valores potenciales](#)" Garantizar la puesta en marcha correcta de Astra Control Center en su entorno. Si se requieren personalizaciones adicionales para su entorno, puede utilizar astra_control_center.yaml Como CR alternativo.

```
vim astra_control_center_min.yaml
```



Si está utilizando un registro que no requiere autorización, debe eliminar secret línea dentro imageRegistry o se producirá un error en la instalación.

- a. Cambiar [your_registry_path] a la ruta de acceso del registro en la que ha insertado las imágenes en el paso anterior.

- b. Cambie el `accountName` cadena al nombre que desea asociar a la cuenta.
- c. Cambie el `astraAddress` Cadena al FQDN que desea utilizar en su navegador para acceder a Astra. No utilizar `http://` o `https://` en la dirección. Copie este FQDN para utilizarlo en un [paso posterior](#).
- d. Cambie el `email` cadena en la dirección inicial predeterminada del administrador. Copie esta dirección de correo electrónico para su uso en un [paso posterior](#).
- e. Cambiar `enrolled` Para AutoSupport a. `false` para sitios sin conexión a internet o retención `true` para sitios conectados.
- f. Si utiliza un administrador de certificados externo, añada las siguientes líneas a. `spec`:

```
spec:
  crds:
    externalCertManager: true
```

- g. (Opcional) Añada un nombre `firstName` y apellidos `lastName` del usuario asociado con la cuenta. Este paso se puede realizar ahora o una versión posterior dentro de la interfaz de usuario.
- h. (Opcional) cambie el `storageClass` Valor en otro recurso de la clase de almacenamiento de Trident, si es necesario para su instalación.
- i. (Opcional) Si desea que el clúster sea gestionado automáticamente por Astra Control Center después de la instalación y ya lo tiene [se ha creado el secreto que contiene el kubeconfig para este cluster](#), Proporcione el nombre del secreto agregando un nuevo campo a este archivo YLMA llamado `astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"`
- j. Realice uno de los siguientes pasos:

- **Otro controlador de entrada (`ingressType:Generic`):** Esta es la acción predeterminada con Astra Control Center. Después de implementar Astra Control Center, deberá configurar el controlador Ingress para exponer Astra Control Center con una dirección URL.

La instalación predeterminada de Astra Control Center configura su puerta de enlace (`service/traefik`) ser del tipo `ClusterIP`. Esta instalación predeterminada requiere que configure además un dispositivo de entrada/controlador de Kubernetes para enrutar el tráfico hacia él. Si desea utilizar una entrada, consulte ["Configure la entrada para el equilibrio de carga"](#).

- **Equilibrador de carga de servicio (`ingressType:AccTraefik`):** Si no desea instalar un controlador IngressController o crear un recurso de entrada, establezca `ingressType` para `AccTraefik`.

Esto despliega el Astra Control Center `traefik` Puerta de enlace como servicio de tipo Kubernetes LoadBalancer.

Astra Control Center utiliza un servicio del tipo "LoadBalancer" (`svc/traefik` En el espacio de nombres de Astra Control Center) y requiere que se le asigne una dirección IP externa accesible. Si se permiten equilibradores de carga en su entorno y no tiene uno configurado, puede utilizar MetalLB u otro equilibrador de carga de servicio externo para asignar una dirección IP externa al servicio. En la configuración interna del servidor DNS, debe apuntar el nombre DNS elegido para Astra Control Center a la dirección IP con equilibrio de carga.



Para obtener más información sobre el tipo de servicio de "LoadBalancer" y la entrada, consulte ["Requisitos"](#).

```

apiVersion: astra.netapp.io/v1
kind: AstraControlCenter
metadata:
  name: astra
spec:
  accountName: "Example"
  astraVersion: "ASTRA_VERSION"
  astraAddress: "astra.example.com"
  astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"
  ingressType: "Generic"
  autoSupport:
    enrolled: true
  email: "[admin@example.com]"
  firstName: "SRE"
  lastName: "Admin"
  imageRegistry:
    name: "[your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"

```

Complete la instalación del centro de control de Astra y del operador

1. Si todavía no lo ha hecho en un paso anterior, cree el `netapp-acc` espacio de nombres (o personalizado):

```
kubectl create ns [netapp-acc or custom namespace]
```

Respuesta de ejemplo:

```
namespace/netapp-acc created
```

2. Instale Astra Control Center en `netapp-acc` (o su espacio de nombres personalizado):

```
kubectl apply -f astra_control_center_min.yaml -n [netapp-acc or custom namespace]
```

Respuesta de ejemplo:

```
astracontrolcenter.astra.netapp.io/astra created
```

Comprobar el estado del sistema



Si prefiere utilizar OpenShift, puede utilizar comandos de OC comparables para realizar los pasos de verificación.

1. Compruebe que todos los componentes del sistema se han instalado correctamente.

```
kubectl get pods -n [netapp-acc or custom namespace]
```

Cada pod debe tener el estado de `Running`. Pueden tardar varios minutos en implementar los pods del sistema.

Ejemplo de respuesta

NAME	READY	STATUS	RESTARTS
AGE			
acc-helm-repo-6b44d68d94-d8m55 13m	1/1	Running	0
activity-78f99ddf8-hltct 10m	1/1	Running	0
api-token-authentication-457nl 9m28s	1/1	Running	0
api-token-authentication-dgwsz 9m28s	1/1	Running	0
api-token-authentication-hmqqc 9m28s	1/1	Running	0
asup-75fd554dc6-m6qzh 9m38s	1/1	Running	0
authentication-6779b4c85d-92gds 8m11s	1/1	Running	0
bucket-service-7cc767f8f8-lqwr8 9m31s	1/1	Running	0
certificates-549fd5d6cb-5kmd6 9m56s	1/1	Running	0
certificates-549fd5d6cb-bkjh9 9m56s	1/1	Running	0
cloud-extension-7bcb7948b-hn8h2 10m	1/1	Running	0
cloud-insights-service-56ccf86647-fgg69 9m46s	1/1	Running	0
composite-compute-677685b9bb-7vgsf 10m	1/1	Running	0
composite-volume-657d6c5585-dnq79 9m49s	1/1	Running	0
credentials-755fd867c8-vrlmt 11m	1/1	Running	0
entitlement-86495cdf5b-nwhh2 10m	1/1	Running	2
features-5684fb8b56-8d6s8 10m	1/1	Running	0
fluent-bit-ds-rhx7v 7m48s	1/1	Running	0
fluent-bit-ds-rjms4 7m48s	1/1	Running	0
fluent-bit-ds-zf5ph 7m48s	1/1	Running	0
graphql-server-66d895f544-w6hjd 3m29s	1/1	Running	0

identity-744df448d5-rlcmm	1/1	Running	0
10m			
influxdb2-0	1/1	Running	0
13m			
keycloak-operator-75c965cc54-z7csw	1/1	Running	0
8m16s			
krakend-798d6df96f-9z2sk	1/1	Running	0
3m26s			
license-5fb7d75765-f8mjg	1/1	Running	0
9m50s			
login-ui-7d5b7df85d-l2s7s	1/1	Running	0
3m20s			
loki-0	1/1	Running	0
13m			
metrics-facade-599b9d7fcc-gtmgl	1/1	Running	0
9m40s			
monitoring-operator-67cc74f844-cdplp	2/2	Running	0
8m11s			
nats-0	1/1	Running	0
13m			
nats-1	1/1	Running	0
13m			
nats-2	1/1	Running	0
12m			
nautilus-769f5b74cd-k5jxm	1/1	Running	0
9m42s			
nautilus-769f5b74cd-kd9gd	1/1	Running	0
8m59s			
openapi-84f6ccd8ff-76kvp	1/1	Running	0
9m34s			
packages-6f59fc67dc-4g2f5	1/1	Running	0
9m52s			
polaris-consul-consul-server-0	1/1	Running	0
13m			
polaris-consul-consul-server-1	1/1	Running	0
13m			
polaris-consul-consul-server-2	1/1	Running	0
13m			
polaris-keycloak-0	1/1	Running	0
8m7s			
polaris-keycloak-1	1/1	Running	0
5m49s			
polaris-keycloak-2	1/1	Running	0
5m15s			
polaris-keycloak-db-0	1/1	Running	0
8m6s			

polaris-keycloak-db-1	1/1	Running	0
5m49s			
polaris-keycloak-db-2	1/1	Running	0
4m57s			
polaris-mongodb-0	2/2	Running	0
13m			
polaris-mongodb-1	2/2	Running	0
12m			
polaris-mongodb-2	2/2	Running	0
12m			
polaris-ui-565f56bf7b-zwr8b	1/1	Running	0
3m19s			
polaris-vault-0	1/1	Running	0
13m			
polaris-vault-1	1/1	Running	0
13m			
polaris-vault-2	1/1	Running	0
13m			
public-metrics-6d86d66444-2wbz1	1/1	Running	0
9m30s			
storage-backend-metrics-77c5d98dcd-dbhg5	1/1	Running	0
9m44s			
storage-provider-78c885f57c-6zcv4	1/1	Running	0
9m36s			
telegraf-ds-212m9	1/1	Running	0
7m48s			
telegraf-ds-qfzgh	1/1	Running	0
7m48s			
telegraf-ds-shrms	1/1	Running	0
7m48s			
telegraf-rs-bjpkt	1/1	Running	0
7m48s			
telemetry-service-6684696c64-qzfdf	1/1	Running	0
10m			
tenancy-6596b6c54d-vmpsm	1/1	Running	0
10m			
traefik-7489dc59f9-6mnst	1/1	Running	0
3m19s			
traefik-7489dc59f9-xrkkg	1/1	Running	0
3m4s			
trident-svc-6c8dc458f5-jswcl	1/1	Running	0
10m			
vault-controller-6b954f9b76-gz9nm	1/1	Running	0
11m			

2. (Opcional) para asegurarse de que la instalación ha finalizado, puede ver el `acc-operator` registra utilizando el siguiente comando.

```
kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f
```



`accHost` el registro del clúster es una de las últimas operaciones y, si no se produce un error en la implementación, no provocará un error. En el caso de un error de registro del clúster que se indica en los registros, puede volver a intentar el registro a través del flujo de trabajo de add cluster ["En la interfaz de usuario de"](#) O API.

3. Cuando todos los pods estén en ejecución, verifique que la instalación se haya realizado correctamente (`READY` es `True`) Y obtenga la contraseña única que utilizará cuando inicie sesión en Astra Control Center:

```
kubectl get AstraControlCenter -n netapp-acc
```

Respuesta:

NAME	UUID	VERSION	ADDRESS
READY			
astra	ACC-9aa5fdde-4214-4cb7-9976-5d8b4c0ce27f	22.08.1-26	
10.111.111.111	True		



Copie el valor de UUID. La contraseña es `ACC-` Seguido del valor UUID (`ACC-[UUID]` o, en este ejemplo, `ACC-9aa5fdde-4214-4cb7-9976-5d8b4c0ce27f`).

Configure la entrada para el equilibrio de carga

Puede configurar una controladora de entrada de Kubernetes que gestione el acceso externo a los servicios, como el equilibrio de carga en un clúster.

Este procedimiento explica cómo configurar un controlador de entrada (`ingressType: Generic`). Esta es la acción predeterminada con Astra Control Center. Después de implementar Astra Control Center, deberá configurar el controlador Ingress para exponer Astra Control Center con una dirección URL.



Si no desea configurar un controlador de entrada, puede configurarlo `ingressType: AccTraefik`). Astra Control Center utiliza un servicio del tipo "LoadBalancer" (`svc/traefik` En el espacio de nombres de Astra Control Center) y requiere que se le asigne una dirección IP externa accesible. Si se permiten equilibradores de carga en su entorno y no tiene uno configurado, puede utilizar MetalLB u otro equilibrador de carga de servicio externo para asignar una dirección IP externa al servicio. En la configuración interna del servidor DNS, debe apuntar el nombre DNS elegido para Astra Control Center a la dirección IP con equilibrio de carga. Para obtener más información sobre el tipo de servicio de "LoadBalancer" y la entrada, consulte ["Requisitos"](#).

Los pasos varían en función del tipo de controlador de entrada que utilice:

- Entrada Istio
- Controlador de entrada nginx
- Controlador OpenShift Ingress

Lo que necesitará

- El requerido "controlador de entrada" ya debe ponerse en marcha.
- La "clase de entrada" ya se debe crear la correspondiente al controlador de entrada.
- Se utilizan versiones de Kubernetes entre e incluidas v1.19 y v1.22.

Pasos para la entrada de Istio

1. Configurar la entrada de Istio.



En este procedimiento se asume que Istio se implementa utilizando el perfil de configuración "predeterminado".

2. Recopile o cree el certificado y el archivo de claves privadas deseados para la puerta de enlace de entrada.

Es posible usar un certificado firmado por CA o autofirmado. El nombre común debe ser la dirección Astra (FQDN).

Comando de ejemplo:

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048  
-keyout tls.key -out tls.crt
```

3. Cree un secreto `tls secret` name de tipo `kubernetes.io/tls` Para una clave privada TLS y un certificado en `istio-system` namespace Tal como se describe en los secretos TLS.

Comando de ejemplo:

```
kubectl create secret tls [tls secret name]  
--key="tls.key"  
--cert="tls.crt" -n istio-system
```



El nombre del secreto debe coincidir con el `spec.tls.secretName` proporcionado en `istio-ingress.yaml` archivo.

4. Implemente un recurso de entrada en `netapp-acc` Espacio de nombres (o con nombre personalizado) mediante el uso del tipo de recurso `v1beta1` (obsoleto en la versión de Kubernetes menor que o 1.22) o `v1` para un esquema obsoleto o nuevo:

Salida:

```

apiVersion: networking.k8s.io/v1beta1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1beta1
kind: Ingress
metadata:
  name: ingress
  namespace: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          serviceName: traefik
          servicePort: 80

```

Para el nuevo esquema v1, siga este ejemplo:

```
kubectl apply -f istio-Ingress.yaml
```

Salida:

```

apiVersion: networking.k8s.io/v1
kind: IngressClass
metadata:
  name: istio
spec:
  controller: istio.io/ingress-controller
---
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: ingress
  namespace: istio-system
spec:
  ingressClassName: istio
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - path: /
        pathType: Prefix
        backend:
          service:
            name: traefik
            port:
              number: 80

```

5. Implementar Astra Control Center como es habitual.
6. Compruebe el estado de la entrada:

```
kubectl get ingress -n netapp-acc
```

Respuesta:

NAME	CLASS	HOSTS	ADDRESS	PORTS	AGE
ingress	istio	astra.example.com	172.16.103.248	80, 443	1h

Pasos para el controlador de entrada Nginx

1. Cree un secreto de tipo[kubernetes.io/tls] Para una clave privada TLS y un certificado en netapp-acc (o nombre personalizado) como se describe en ["Secretos TLS"](#).

2. Implemente un recurso de entrada en `netapp-acc` (o nombre personalizado) mediante el `v1beta1` (Obsoleto en la versión de Kubernetes inferior a o 1.22) o. `v1` tipo de recurso para un esquema obsoleto o nuevo:

a. Para un `v1beta1` esquema obsoleto, siga este ejemplo:

```
apiVersion: extensions/v1beta1
Kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: [class name for nginx controller]
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
          serviceName: traefik
          servicePort: 80
          pathType: ImplementationSpecific
```

b. Para la `v1` nuevo esquema, siga este ejemplo:

```

apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC address>
    http:
      paths:
      - path:
        backend:
          service:
            name: traefik
            port:
              number: 80
          pathType: ImplementationSpecific

```

Pasos para el controlador de entrada de OpenShift

1. Obtenga su certificado y consiga los archivos de clave, certificado y CA listos para su uso por la ruta OpenShift.
2. Cree la ruta OpenShift:

```

oc create route edge --service=traefik
--port=web -n [netapp-acc or custom namespace]
--insecure-policy=Redirect --hostname=<ACC address>
--cert=cert.pem --key=key.pem

```

Inicie sesión en la interfaz de usuario de Astra Control Center

Después de instalar Astra Control Center, cambiará la contraseña del administrador predeterminado e inicie sesión en el panel de interfaz de usuario de Astra Control Center.

Pasos

1. En un explorador, introduzca el FQDN que utilizó en `astraAddress` en la `astra_control_center_min.yaml` CR cuando [Ha instalado Astra Control Center](#).
2. Acepte los certificados autofirmados cuando se le solicite.



Se puede crear un certificado personalizado después de iniciar sesión.

3. En la página de inicio de sesión de Astra Control Center, introduzca el valor utilizado `email` en `astra_control_center_min.yaml` CR cuando [Ha instalado Astra Control Center](#), seguido de la contraseña única (`ACC-[UUID]`).



Si introduce una contraseña incorrecta tres veces, la cuenta de administrador se bloqueará durante 15 minutos.

4. Seleccione **Iniciar sesión**.
5. Cambie la contraseña cuando se le solicite.



Si este es su primer inicio de sesión y olvida la contraseña y aún no se han creado otras cuentas de usuario administrativas, comuníquese con el servicio de soporte de NetApp para obtener ayuda para la recuperación de contraseñas.

6. (Opcional) quite el certificado TLS autofirmado existente y sustitúyalo por un ["Certificado TLS personalizado firmado por una entidad de certificación \(CA\)"](#).

Solucione los problemas de instalación

Si alguno de los servicios está en `Error` puede inspeccionar los registros. Busque códigos de respuesta API en la gama 400 a 500. Esos indican el lugar donde ocurrió un fracaso.

Pasos

1. Para inspeccionar los registros del operador de Astra Control Center, introduzca lo siguiente:

```
kubectl logs --follow -n netapp-acc-operator $(kubectl get pods -n netapp-acc-operator -o name) -c manager
```

El futuro

Complete la implementación llevando a cabo ["tareas de configuración"](#).

=
:allow-uri-read:

Comprender las restricciones de directivas de seguridad de POD

Astra Control Center admite la limitación de privilegios mediante directivas de seguridad de POD (PSP). Las políticas de seguridad de POD permiten limitar los usuarios o grupos que pueden ejecutar contenedores y los privilegios que dichos contenedores pueden tener.

Algunas distribuciones de Kubernetes, como RKE2, tienen una política de seguridad de POD predeterminada que es demasiado restrictiva y provoca problemas al instalar Astra Control Center.

Puede utilizar la información y los ejemplos que se incluyen aquí para comprender las directivas de seguridad de POD que Astra Control Center crea y configurar las directivas de seguridad de POD que proporcionan la protección necesaria sin interferir con las funciones de Astra Control Center.

PSP instalado por Astra Control Center

Astra Control Center crea varias directivas de seguridad de POD durante la instalación. Algunas de ellas son permanentes y algunas se crean durante ciertas operaciones y se eliminan una vez que se completa la operación.

Se crean PSP durante la instalación

Durante la instalación de Astra Control Center, el operador Astra Control Center instala una directiva de seguridad de POD personalizada, un objeto Role y un objeto RoleBinding para admitir la implementación de los servicios Astra Control Center en el espacio de nombres Astra Control Center.

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp
```

NAME	FSGROUP	SUPGROUP	PRIV	READONLYROOTFS	CAPS	VOLUMES	SELINUX	RUNASUSER
avp-psp			false				RunAsAny	RunAsAny
RunAsAny	RunAsAny	false		*			RunAsAny	RunAsAny
netapp-astra-deployment-psp			false				RunAsAny	RunAsAny
RunAsAny	RunAsAny	false		*				

```
kubectl get role
```

NAME	CREATED AT
netapp-astra-deployment-role	2022-06-27T19:34:58Z

```
kubectl get rolebinding
```

NAME	AGE	ROLE
netapp-astra-deployment-rb	32m	Role/netapp-astra-deployment-role

Se crean PSP durante las operaciones de backup

Durante las operaciones de copia de seguridad, Astra Control Center crea una política de seguridad de POD dinámica, un objeto ClusterRole y un objeto RoleBinding. Estos permiten utilizar el proceso de backup, que se produce en un espacio de nombres aparte.

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp
```

NAME		PRIV	CAPS		
SELINUX	RUNASUSER	FSGROUP	SUPGROUP	READONLYROOTFS	
VOLUMES					
netapp-astra-backup		false	DAC_READ_SEARCH		
RunAsAny	RunAsAny	RunAsAny	RunAsAny	false	*

```
kubectl get role
```

NAME	CREATED AT
netapp-astra-backup	2022-07-21T00:00:00Z

```
kubectl get rolebinding
```

NAME	ROLE	AGE
netapp-astra-backup	Role/netapp-astra-backup	62s

Se crean PSP durante la gestión del clúster

Cuando gestiona un clúster, Astra Control Center instala el operador de supervisión de netapp en el clúster gestionado. Este operador crea una directiva de seguridad de POD, un objeto ClusterRole y un objeto RoleBinding para implementar servicios de telemetría en el espacio de nombres Astra Control Center.

La política y los objetos nuevos tienen los siguientes atributos:

```
kubectl get psp
```

NAME		PRIV	CAPS		
SELINUX	RUNASUSER	FSGROUP	SUPGROUP	READONLYROOTFS	
VOLUMES					
netapp-monitoring-bsp-nkmo		true	AUDIT_WRITE,NET_ADMIN,NET_RAW		
RunAsAny	RunAsAny	RunAsAny	RunAsAny	false	*

```
kubectl get role
```

NAME	CREATED AT
netapp-monitoring-role-privileged	2022-07-21T00:00:00Z

```
kubectl get rolebinding
```

NAME	ROLE	
AGE		
netapp-monitoring-role-binding-privileged	Role/netapp-monitoring-role-privileged	
2m5s		

Active la comunicación de red entre espacios de nombres

Algunos entornos utilizan construcciones de NetworkPolicy para restringir el tráfico entre espacios de nombres. El operador Astra Control Center, Astra Control Center y el complemento Astra para VMware vSphere están todos en espacios de nombres diferentes. Los servicios de estos distintos espacios de nombres deben poder comunicarse entre sí. Para activar esta comunicación, siga estos pasos.

Pasos

1. Elimine los recursos de NetworkPolicy que existan en el espacio de nombres de Astra Control Center:

```
kubectl get networkpolicy -n netapp-acc
```

2. Para cada objeto NetworkPolicy devuelto por el comando anterior, utilice el siguiente comando para eliminarlo. Sustituya <OBJECT_NAME> por el nombre del objeto devuelto:

```
kubectl delete networkpolicy <OBJECT_NAME> -n netapp-acc
```

3. Aplique el siguiente archivo de recursos para configurar el objeto de política de red ACC-avp con el fin de permitir que los servicios de Astra Plugin para VMware vSphere puedan realizar solicitudes a los servicios de Astra Control Center. Reemplace la información entre paréntesis <> por la información de su entorno:

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-avp-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: <PLUGIN_NAMESPACE_NAME> #
REPLACE THIS WITH THE ASTRA PLUGIN FOR VMWARE VSPHERE NAMESPACE NAME
```

4. Aplique el siguiente archivo de recursos para configurar el objeto de directiva de red-operador de ACC con el fin de permitir que el operador de Astra Control Center se comunice con los servicios de Astra Control Center. Reemplace la información entre paréntesis <> por la información de su entorno:

```

apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: acc-operator-network-policy
  namespace: <ACC_NAMESPACE_NAME> # REPLACE THIS WITH THE ASTRA CONTROL
CENTER NAMESPACE NAME
spec:
  podSelector: {}
  policyTypes:
    - Ingress
  ingress:
    - from:
      - namespaceSelector:
          matchLabels:
            kubernetes.io/metadata.name: <NETAPP-ACC-OPERATOR> #
REPLACE THIS WITH THE OPERATOR NAMESPACE NAME

```

Quite las limitaciones de recursos

Algunos entornos utilizan los objetos ResourceQuotas y LimitRanges para evitar que los recursos de un espacio de nombres consuman toda la CPU y memoria disponibles en el clúster. Astra Control Center no establece límites máximos, por lo que no se ajusta a esos recursos. Debe eliminarlos de los espacios de nombres en los que planea instalar Astra Control Center.

Puede utilizar los siguientes pasos para recuperar y eliminar estas cuotas y límites. En estos ejemplos, el resultado del comando se muestra inmediatamente después del comando.

Pasos

1. Obtenga las cuotas de recursos en el espacio de nombres ACC-netapp:

```
kubectl get quota -n netapp-acc
```

Respuesta:

NAME	AGE	REQUEST	LIMIT
pods-high	16s	requests.cpu: 0/20, requests.memory: 0/100Gi	
limits.cpu: 0/200, limits.memory: 0/1000Gi			
pods-low	15s	requests.cpu: 0/1, requests.memory: 0/1Gi	
limits.cpu: 0/2, limits.memory: 0/2Gi			
pods-medium	16s	requests.cpu: 0/10, requests.memory: 0/20Gi	
limits.cpu: 0/20, limits.memory: 0/200Gi			

2. Elimine todas las cuotas de recursos por nombre:

```
kubectl delete resourcequota pods-high -n netapp-acc
```

```
kubectl delete resourcequota pods-low -n netapp-acc
```

```
kubectl delete resourcequota pods-medium -n netapp-acc
```

3. Obtenga los rangos de límites en el espacio de nombres ACC-netapp:

```
kubectl get limits -n netapp-acc
```

Respuesta:

NAME	CREATED AT
cpu-limit-range	2022-06-27T19:01:23Z

4. Eliminar los rangos de límites por nombre:

```
kubectl delete limitrange cpu-limit-range -n netapp-acc
```

=

:allow-uri-read:

Instale Astra Control Center utilizando OpenShift OperatorHub

Si utiliza Red Hat OpenShift, puede instalar Astra Control Center mediante el operador certificado de Red Hat. Utilice este procedimiento para instalar Astra Control Center desde ["Catálogo de Red Hat Ecosystem"](#) O con Red Hat OpenShift Container Platform.

Después de completar este procedimiento, debe volver al procedimiento de instalación para completar el ["pasos restantes"](#) para verificar que la instalación se ha realizado correctamente e iniciar sesión.

Lo que necesitará

- ["Antes de comenzar la instalación, prepare su entorno para la implementación de Astra Control Center"](#).
- En el clúster OpenShift, asegúrese de que todos los operadores de clúster se encuentran en buen estado (available es true):

```
oc get clusteroperators
```

- Desde su clúster OpenShift, asegúrese de que todos los servicios API se encuentran en buen estado (`available es true`):

```
oc get apiservices
```

- Cree una dirección FQDN para Astra Control Center en su centro de datos.
- Obtenga los permisos necesarios y acceda a Red Hat OpenShift Container Platform para realizar los pasos de instalación descritos.
- Si ya existe un administrador de certificados en el clúster, tendrá que realizar algunos ["requisitos previos"](#). Por lo tanto, Astra Control Center no instala su propio cert-Manager.

Pasos

- [Descargue y desembale el paquete Astra Control Center](#)
- [Instale el complemento Astra kubectl de NetApp](#)
- [Agregue las imágenes al registro local](#)
- [Busque la página de instalación del operador](#)
- [Instale el operador](#)
- [Instalar Astra Control Center](#)

Descargue y desembale el paquete Astra Control Center

1. Descargue el paquete Astra Control Center (`astra-control-center-[version].tar.gz`) del ["Sitio de soporte de NetApp"](#).
2. Descargue el archivo zip de los certificados y claves de Astra Control Center de ["Sitio de soporte de NetApp"](#).
3. (Opcional) Use el siguiente comando para verificar la firma del paquete:

```
openssl dgst -sha256 -verify AstraControlCenter-public.pub -signature  
astra-control-center-[version].tar.gz.sig astra-control-center-  
[version].tar.gz
```

4. Extraiga las imágenes:

```
tar -vxzf astra-control-center-[version].tar.gz
```

Instale el complemento Astra kubectl de NetApp

La Astra de NetApp `kubectl` El complemento de línea de comandos ahorra tiempo al realizar tareas comunes asociadas con la implementación y actualización de Astra Control Center.

Lo que necesitará

NetApp proporciona binarios para el complemento para distintas arquitecturas de CPU y sistemas operativos. Debe saber qué CPU y sistema operativo tiene antes de realizar esta tarea. En los sistemas operativos Linux

y Mac, puede utilizar `uname -a` comando para recopilar esta información.

Pasos

1. Enumere la Astra de NetApp disponible `kubect1` Haga un complemento para binarios y anote el nombre del archivo que necesita para su sistema operativo y arquitectura de CPU:

```
ls kubect1-astra/
```

2. Copie el archivo en la misma ubicación que el estándar `kubect1` utilidad. En este ejemplo, la `kubect1` la utilidad se encuentra en `/usr/local/bin` directorio. Sustituya `<binary-name>` con el nombre del archivo que necesita:

```
cp kubect1-astra/<binary-name> /usr/local/bin/kubect1-astra
```

Agregue las imágenes al registro local

1. Complete la secuencia de pasos apropiada para el motor del contenedor:

Docker

1. Cambie al directorio Astra:

```
cd acc
```

2. Push las imágenes del paquete del directorio imagen de Astra Control Center en su registro local. Realice las siguientes sustituciones antes de ejecutar el comando:

- Sustituya BUNDLE_FILE por el nombre del archivo Astra Control Bundle (por ejemplo, acc.manifest.yaml).
- Sustituya MY_REGISTRATION por la URL del repositorio de Docker.
- Sustituya MY_REGISTRATION_USER por el nombre de usuario.
- Sustituya MY_REGISTRATION_TOKEN por un token autorizado para el registro.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY  
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Inicie sesión en su registro:

```
podman login [your_registry_path]
```

2. Ejecute el siguiente script, haciendo la sustitución de <YOUR_REGISTRY> como se indica en los comentarios:


```

# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
    # Load to local cache
    astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //'')

    # Remove path and keep imageName.
    astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

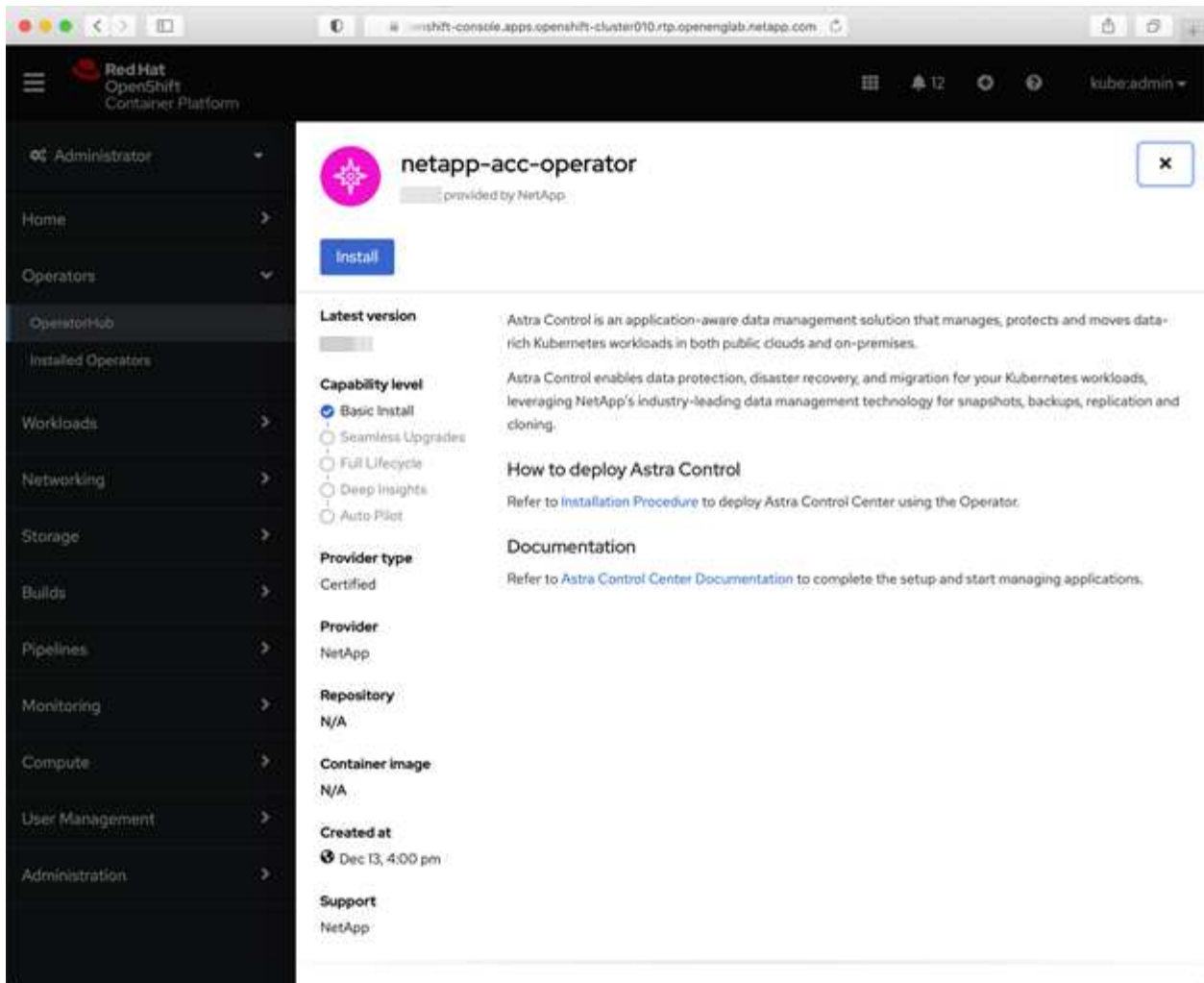
    # Tag with local image repo.
    podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

    # Push to the local repo.
    podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done

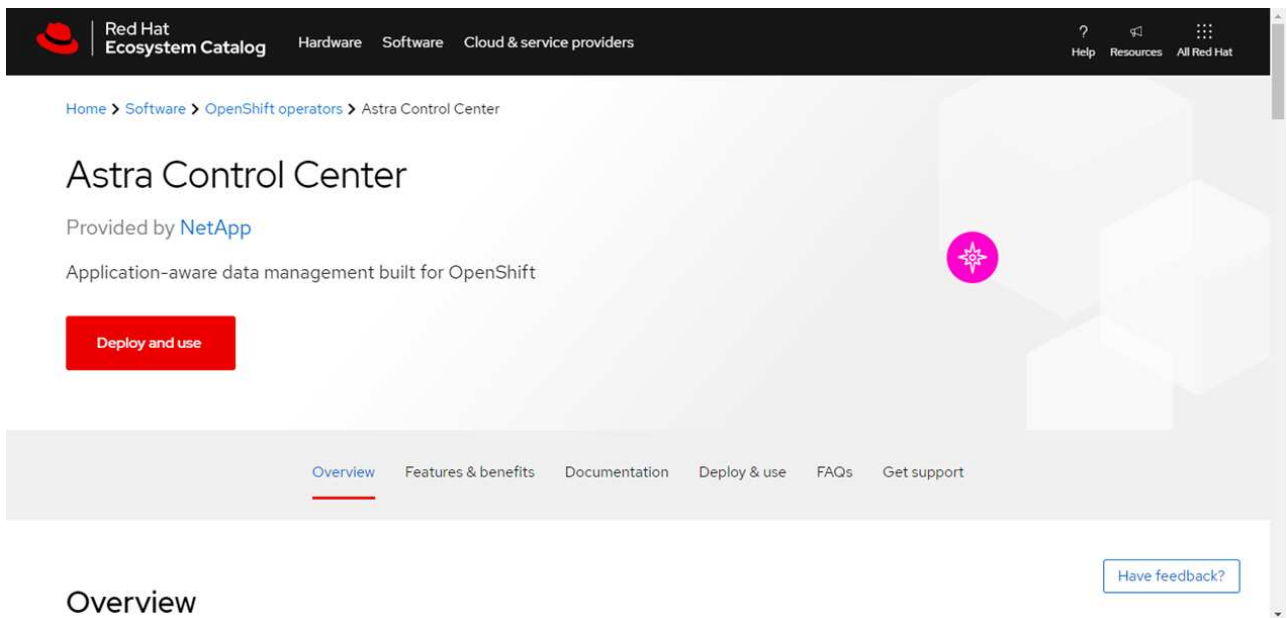
```

Busque la página de instalación del operador

1. Realice uno de los siguientes procedimientos para acceder a la página de instalación del operador:
 - Desde la consola web de Red Hat OpenShift:



- i. Inicie sesión en la IU de OpenShift Container Platform.
 - ii. En el menú lateral, seleccione **operadores > OperatorHub**.
 - iii. Seleccione el operador NetApp Astra Control Center.
 - iv. Seleccione **instalar**.
- En el catálogo de ecosistemas de Red Hat:



- Overview**
- Seleccione Astra Control Center de NetApp "operador".
 - Seleccione **desplegar y utilizar**.

Instale el operador

- Complete la página **Install Operator** e instale el operador:



El operador estará disponible en todos los espacios de nombres del clúster.

- Seleccione el espacio de nombres del operador o. `netapp-acc-operator` el espacio de nombres se creará automáticamente como parte de la instalación del operador.
- Seleccione una estrategia de aprobación manual o automática.



Se recomienda la aprobación manual. Solo debe tener una instancia de operador en ejecución por clúster.

- Seleccione **instalar**.



Si ha seleccionado una estrategia de aprobación manual, se le pedirá que apruebe el plan de instalación manual para este operador.

- Desde la consola, vaya al menú OperatorHub y confirme que el operador se ha instalado correctamente.

Instalar Astra Control Center

- En la consola de la vista de detalles del operador del Centro de control de Astra, seleccione `Create instance` En la sección proporcionada API.
- Complete el `Create AstraControlCenter` campo de formulario:
 - Mantenga o ajuste el nombre del Centro de control de Astra.
 - (Opcional) Habilitar o deshabilitar AutoSupport. Se recomienda conservar la funcionalidad de AutoSupport.

- c. Introduzca la dirección de Astra Control Center. No entre `http://` o `https://` en la dirección.
 - d. Introduzca la versión de Astra Control Center; por ejemplo, 21.12.60.
 - e. Introduzca un nombre de cuenta, una dirección de correo electrónico y un apellido de administrador.
 - f. Conserve la política de reclamaciones de volumen predeterminada.
 - g. En **Registro de imágenes**, introduzca la ruta de registro de la imagen del contenedor local. No entre `http://` o `https://` en la dirección.
 - h. Si utiliza un registro que requiere autenticación, introduzca el secreto.
 - i. Introduzca el nombre del administrador.
 - j. Configure el escalado de recursos.
 - k. Conserve la clase de almacenamiento predeterminada.
 - l. Defina las preferencias de manejo de CRD.
3. Seleccione `Create`.

El futuro

Compruebe que la instalación de Astra Control Center se ha realizado correctamente y complete el "[pasos restantes](#)" para iniciar sesión. Además, completará la implementación siguiendo este proceso "[tareas de configuración](#)".

Instale Astra Control Center con un back-end de almacenamiento de Cloud Volumes ONTAP

Con Astra Control Center, puede gestionar sus aplicaciones en un entorno de cloud híbrido con clústeres de Kubernetes e instancias de Cloud Volumes ONTAP autogestionados. Puede poner en marcha Astra Control Center en sus clústeres de Kubernetes en las instalaciones o en uno de los clústeres de Kubernetes autogestionados en el entorno de cloud.

Con una de estas puestas en marcha, puede realizar operaciones de gestión de datos de aplicaciones utilizando Cloud Volumes ONTAP como back-end de almacenamiento. También es posible configurar un bloque de S3 como destino de backup.

Para instalar Astra Control Center en Amazon Web Services (AWS), Google Cloud Platform (GCP) y Microsoft Azure con una back-end de almacenamiento de Cloud Volumes ONTAP, realice los siguientes pasos en función de su entorno de cloud.

- [Ponga en marcha Astra Control Center en Amazon Web Services](#)
- [Ponga en marcha Astra Control Center en Google Cloud Platform](#)
- [Ponga en marcha Astra Control Center en Microsoft Azure](#)

Puede gestionar sus aplicaciones en distribuciones con clústeres de Kubernetes autogestionados, como OpenShift Container Platform (OCP). Sólo se validan los clústeres OCP autogestionados para la implantación de Astra Control Center.

Ponga en marcha Astra Control Center en Amazon Web Services

Puede poner en marcha Astra Control Center en un clúster de Kubernetes autogestionado alojado en un cloud público de Amazon Web Services (AWS).

Lo que necesitará para AWS

Antes de poner en marcha Astra Control Center en AWS, necesitará los siguientes elementos:

- Licencia Astra Control Center. Consulte ["Requisitos de licencia de Astra Control Center"](#).
- ["Cumpla los requisitos de Astra Control Center"](#).
- Cuenta de Cloud Central de NetApp
- Si utiliza OCP, los permisos de Red Hat OpenShift Container Platform (OCP) (en el nivel de espacio de nombres para crear pods)
- Credenciales de AWS, Access ID y Secret Key con permisos que permiten crear cubos y conectores
- Acceso e inicio de sesión del Elastic Container Registry (ECR) de la cuenta de AWS
- Se requieren entradas de zona alojada de AWS y ruta 53 para acceder a la interfaz de usuario de Astra Control

Requisitos de los entornos operativos para AWS

Astra Control Center requiere los siguientes entornos operativos para AWS:


- OpenShift Container Platform de Red Hat 4.8



Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno.

Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno:

Componente	Requisito
Capacidad de almacenamiento Cloud Volumes ONTAP de back-end de NetApp	300 GB como mínimo disponible
Nodos de trabajo (requisitos de AWS EC2)	Al menos 3 nodos de trabajo en total, con 4 núcleos vCPU y 12 GB de RAM en cada uno
Equilibrador de carga	Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios en el clúster de entorno operativo
FQDN	Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada
Astra Trident (instalado como parte de la detección de clústeres de Kubernetes en NetApp Cloud Manager)	Astra Trident 21.04 o posterior instalado y configurado y NetApp ONTAP versión 9.5 o posterior como back-end de almacenamiento

Componente	Requisito
Registro de imágenes	<p>Debe tener un registro privado existente, como AWS Elastic Container Registry, al que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes.</p> <div>  <p>El clúster alojado de Astra Control Center y el clúster gestionado deben tener acceso al mismo registro de imágenes para poder realizar copias de seguridad y restaurar aplicaciones mediante la imagen basada en Restic.</p> </div>
Configuración de Astra Trident/ONTAP	<p>Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. Astra Control Center es compatible con las siguientes clases de almacenamiento ONTAP Kubernetes que se crean al importar su clúster Kubernetes a Cloud Manager de NetApp. Los proporciona Astra Trident:</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san</code> <code>csi.trident.netapp.io</code>



Estos requisitos suponen que Astra Control Center es la única aplicación que se ejecuta en el entorno operativo. Si el entorno ejecuta aplicaciones adicionales, ajuste estos requisitos mínimos según corresponda.



El token del registro de AWS caduca en 12 horas, después del cual deberá renovar el secreto del registro de imagen Docker.

Información general sobre la implementación para AWS

He aquí una descripción general del proceso de instalación de Astra Control Center para AWS con Cloud Volumes ONTAP como back-end de almacenamiento.

Cada uno de estos pasos se explica más detalladamente a continuación.

1. [Compruebe que dispone de suficientes permisos IAM.](#)
2. [Instale un clúster RedHat OpenShift en AWS.](#)
3. [Configure AWS.](#)
4. [Configure Cloud Manager de NetApp.](#)
5. [Instalar Astra Control Center.](#)

Compruebe que dispone de suficientes permisos IAM

Asegúrese de tener suficientes roles y permisos de IAM para poder instalar un clúster RedHat OpenShift y un conector Cloud Manager de NetApp.

Consulte "[Credenciales iniciales de AWS](#)".

Instale un clúster RedHat OpenShift en AWS

Instale un clúster RedHat OpenShift Container Platform en AWS.

Para obtener instrucciones de instalación, consulte "[Instalación de un clúster en AWS en OpenShift Container Platform](#)".

Configure AWS

A continuación, configure AWS para crear una red virtual, configurar instancias de computación EC2, crear un bloque de AWS S3, crear un Elastic Container Register (ECR) para alojar las imágenes de Astra Control Center y empujar las imágenes a este registro.

Siga la documentación de AWS para completar los pasos siguientes. Consulte "[Documentación de instalación de AWS](#)".

1. Cree una red virtual AWS.
2. Revise las instancias de computación EC2. Puede ser un servidor con configuración básica o máquinas virtuales en AWS.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestros y trabajadores, cambie el tipo de instancia en AWS para cumplir los requisitos de Astra. Consulte "[Requisitos del Centro de Control de Astra](#)".
4. Cree al menos un bloque de AWS S3 para almacenar los backups.
5. Cree un AWS Elastic Container Registry (ECR) para alojar todas las imágenes ACC.



Si no crea la ECR, Astra Control Center no puede acceder a los datos de supervisión de un clúster que contenga Cloud Volumes ONTAP con un back-end de AWS. El problema se produce cuando el clúster que intenta detectar y gestionar mediante Astra Control Center no tiene acceso a AWS ECR.

6. Inserte las imágenes ACC en el registro definido.



El token del registro de contenedor elástico de AWS (ECR) caduca al cabo de 12 horas y provoca errores en las operaciones de clonado de varios clústeres. Este problema ocurre cuando se gestiona un back-end de almacenamiento desde Cloud Volumes ONTAP configurado para AWS. Para corregir este problema, vuelva a autenticarse con la ECR y genere un nuevo secreto para que las operaciones de clonación se reanuden correctamente.

A continuación mostramos un ejemplo de una puesta en marcha de AWS:



Configure Cloud Manager de NetApp

Con Cloud Manager, cree un espacio de trabajo, añada un conector a AWS, cree un entorno de trabajo e importe el clúster.

Siga la documentación de Cloud Manager para completar los siguientes pasos. Consulte lo siguiente:

- ["Introducción a Cloud Volumes ONTAP en AWS"](#).
- ["Cree un conector en AWS mediante Cloud Manager"](#)

Pasos

1. Añada sus credenciales a Cloud Manager.
2. Crear un área de trabajo.
3. Agregue un conector para AWS. Elija AWS como proveedor.
4. Cree un entorno de trabajo para su entorno de cloud.
 - a. Ubicación: "Amazon Web Services (AWS)"
 - b. Tipo: "Cloud Volumes ONTAP ha"
5. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.
 - a. Consulte los detalles del clúster de NetApp seleccionando **K8s > Lista de clústeres > Detalles del clúster**.

- b. En la esquina superior derecha, tenga en cuenta la versión de Trident.
- c. Observe las clases de almacenamiento del clúster Cloud Volumes ONTAP que muestran NetApp como el aprovisionador.

Esto importa su clúster de Red Hat OpenShift y le asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento. Trident se instala automáticamente como parte del proceso de importación y detección.

6. Obsérvese todos los volúmenes y volúmenes persistentes en esta puesta en marcha de Cloud Volumes ONTAP.



Cloud Volumes ONTAP puede funcionar como un nodo único o en alta disponibilidad. Si está habilitada, anote el estado de alta disponibilidad y el estado de implementación del nodo que se ejecutan en AWS.

Instalar Astra Control Center

Siga la norma ["Instrucciones de instalación de Astra Control Center"](#).



AWS utiliza el tipo de bloque Generic S3.

Ponga en marcha Astra Control Center en Google Cloud Platform

Puede poner en marcha Astra Control Center en un clúster de Kubernetes autogestionado alojado en un cloud público de Google Cloud Platform (GCP).

Qué necesitará para GCP

Antes de implementar Astra Control Center en GCP, necesitará los siguientes elementos:

- Licencia Astra Control Center. Consulte ["Requisitos de licencia de Astra Control Center"](#).
- ["Cumpla los requisitos de Astra Control Center"](#).
- Cuenta de Cloud Central de NetApp
- Si se utiliza OCP, Red Hat OpenShift Container Platform (OCP) 4.10
- Si utiliza OCP, los permisos de Red Hat OpenShift Container Platform (OCP) (en el nivel de espacio de nombres para crear pods)
- Cuenta de servicio de GCP con permisos que le permiten crear cubos y conectores


Requisitos del entorno operativo para GCP



Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno.

Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno:

Componente	Requisito
Capacidad de almacenamiento Cloud Volumes ONTAP de back-end de NetApp	300 GB como mínimo disponible

Componente	Requisito
Nodos de trabajo (requisitos de computación de GCP)	Al menos 3 nodos de trabajo en total, con 4 núcleos vCPU y 12 GB de RAM en cada uno
Equilibrador de carga	Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios en el clúster de entorno operativo
FQDN (ZONA DNS DE GCP)	Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada
Astra Trident (instalado como parte de la detección de clústeres de Kubernetes en NetApp Cloud Manager)	Astra Trident 21.04 o posterior instalado y configurado y NetApp ONTAP versión 9.5 o posterior como back-end de almacenamiento
Registro de imágenes	<p>Debe tener un registro privado existente, como Google Container Registry, al que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes.</p> <div>  <p>Es necesario habilitar el acceso anónimo para extraer imágenes RTIC para realizar copias de seguridad.</p> </div>
Configuración de Astra Trident/ONTAP	<p>Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. Astra Control Center es compatible con las siguientes clases de almacenamiento ONTAP Kubernetes que se crean al importar su clúster Kubernetes a Cloud Manager de NetApp. Los proporciona Astra Trident:</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san</code> <code>csi.trident.netapp.io</code>



Estos requisitos suponen que Astra Control Center es la única aplicación que se ejecuta en el entorno operativo. Si el entorno ejecuta aplicaciones adicionales, ajuste estos requisitos mínimos según corresponda.

Información general de puesta en marcha para GCP

A continuación se ofrece una descripción general del proceso de instalación de Astra Control Center en un clúster OCP autogestionado en GCP con Cloud Volumes ONTAP como back-end de almacenamiento.

Cada uno de estos pasos se explica más detalladamente a continuación.

1. [Instale un clúster RedHat OpenShift en GCP.](#)
2. [Cree un proyecto de GCP y una nube privada virtual.](#)
3. [Compruebe que dispone de suficientes permisos IAM.](#)
4. [Configure GCP.](#)
5. [Configure Cloud Manager de NetApp.](#)
6. [Instalar y configurar Astra Control Center.](#)

Instale un clúster RedHat OpenShift en GCP

El primer paso es instalar un clúster RedHat OpenShift en GCP.

Para obtener instrucciones de instalación, consulte lo siguiente:

- ["Instalar un clúster OpenShift en GCP"](#)
- ["Creación de una cuenta de servicio de GCP"](#)

Cree un proyecto de GCP y una nube privada virtual

Cree al menos un proyecto de GCP y una nube privada virtual (VPC).



OpenShift podría crear sus propios grupos de recursos. Además de ellas, debe definir también un VPC de GCP. Consulte la documentación de OpenShift.

Es posible que desee crear un grupo de recursos de clúster de plataforma y un grupo de recursos de clúster de aplicación OpenShift de destino.

Compruebe que dispone de suficientes permisos IAM

Asegúrese de tener suficientes roles y permisos de IAM para poder instalar un clúster RedHat OpenShift y un conector Cloud Manager de NetApp.

Consulte ["Credenciales y permisos iniciales de GCP"](#).

Configure GCP

A continuación, configure GCP para crear un VPC, configure instancias de computación, cree un almacenamiento de objetos de Google Cloud, cree un Registro de contenedor de Google para alojar las imágenes de Astra Control Center y empuje las imágenes a este registro.

Siga la documentación de GCP para completar los siguientes pasos. Consulte [instalación del clúster OpenShift en GCP](#).

1. Cree un proyecto de GCP y VPC en el GCP que planea utilizar para el clúster de OCP con el back-end de CVO.
2. Revise las instancias de computación. Puede tratarse de un servidor de configuración básica o máquinas virtuales en GCP.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestro y trabajador, cambie el tipo de instancia de GCP para que cumpla los requisitos de Astra. Consulte ["Requisitos del Centro de Control de Astra"](#).
4. Cree al menos un bloque de almacenamiento en cloud de GCP para almacenar sus backups.

5. Crear un secreto, que es necesario para el acceso a bloques.
6. Cree un registro de Google Container para alojar todas las imágenes de Astra Control Center.
7. Configure el acceso al registro de contenedores de Google para inserción/extracción de Docker para todas las imágenes de Astra Control Center.

Ejemplo: Las imágenes ACC se pueden insertar en este registro introduciendo la siguiente secuencia de comandos:

```
gcloud auth activate-service-account <service account email address>
--key-file=<GCP Service Account JSON file>
```

Este script requiere un archivo de manifiesto de Astra Control Center y su ubicación del Registro de imágenes de Google.

Ejemplo:

```
manifestfile=astra-control-center-<version>.manifest
GCP_CR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $GCP_CR_REGISTRY/$image
    docker push $GCP_CR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

8. Configure zonas DNS.

Configure Cloud Manager de NetApp

Con Cloud Manager, cree un espacio de trabajo, añada un conector a GCP, cree un entorno de trabajo e importe el clúster.

Siga la documentación de Cloud Manager para completar los siguientes pasos. Consulte ["Introducción a Cloud Volumes ONTAP en GCP"](#).

Lo que necesitará

- Acceso a la cuenta de servicio de GCP con los permisos y roles de IAM necesarios

Pasos

1. Añada sus credenciales a Cloud Manager. Consulte ["Adición de cuentas de GCP"](#).
2. Agregue un conector para GCP.
 - a. Elija "GCP" como el proveedor.

- b. Introduzca las credenciales de GCP. Consulte ["Creación de un conector en GCP desde Cloud Manager"](#).
 - c. Asegúrese de que el conector está en marcha y cambie a dicho conector.
3. Cree un entorno de trabajo para su entorno de cloud.
 - a. Ubicación: "GCP"
 - b. Tipo: "Cloud Volumes ONTAP ha"
4. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.
 - a. Consulte los detalles del clúster de NetApp seleccionando **K8s > Lista de clústeres > Detalles del clúster**.
 - b. En la esquina superior derecha, tenga en cuenta la versión de Trident.
 - c. Tenga en cuenta las clases de almacenamiento del clúster de Cloud Volumes ONTAP que muestran "NetApp" como el proveedor.

Esto importa su clúster de Red Hat OpenShift y le asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento. Trident se instala automáticamente como parte del proceso de importación y detección.
5. Obsérvese todos los volúmenes y volúmenes persistentes en esta puesta en marcha de Cloud Volumes ONTAP.



Cloud Volumes ONTAP puede funcionar como un nodo único o en alta disponibilidad. Si está habilitada, anote el estado de alta disponibilidad y el estado de puesta en marcha del nodo que se ejecutan en GCP.

Instalar Astra Control Center

Siga la norma ["Instrucciones de instalación de Astra Control Center"](#).



GCP utiliza el tipo de bloque Generic S3.

1. Genere el secreto Docker para obtener imágenes de la instalación de Astra Control Center:

```
kubectl create secret docker-registry <secret name>
--docker-server=<Registry location>
--docker-username=_json_key
--docker-password="$(cat <GCP Service Account JSON file>)"
--namespace=pcloud
```

Ponga en marcha Astra Control Center en Microsoft Azure

Puede poner en marcha Astra Control Center en un clúster de Kubernetes autogestionado que se aloja en un cloud público de Microsoft Azure.

Lo que necesitará para Azure

Antes de poner en marcha Astra Control Center en Azure, necesitará los siguientes elementos:


- Licencia Astra Control Center. Consulte ["Requisitos de licencia de Astra Control Center"](#).
- ["Cumpla los requisitos de Astra Control Center"](#).
- Cuenta de Cloud Central de NetApp
- Si se utiliza OCP, Red Hat OpenShift Container Platform (OCP) 4.8
- Si utiliza OCP, los permisos de Red Hat OpenShift Container Platform (OCP) (en el nivel de espacio de nombres para crear pods)
- Credenciales de Azure con permisos que le permiten crear cubos y conectores

Requisitos del entorno operativo para Azure

Asegúrese de que el entorno operativo que elija para alojar Astra Control Center cumple los requisitos de recursos básicos que se describen en la documentación oficial del entorno.

Astra Control Center requiere los siguientes recursos además de los requisitos de recursos del entorno:

Consulte ["Requisitos del entorno operativo del Centro de control de Astra"](#).

Componente	Requisito
Capacidad de almacenamiento Cloud Volumes ONTAP de back-end de NetApp	300 GB como mínimo disponible
Nodos de trabajo (requisitos de computación de Azure)	Al menos 3 nodos de trabajo en total, con 4 núcleos vCPU y 12 GB de RAM en cada uno
Equilibrador de carga	Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios en el clúster de entorno operativo
FQDN (zona DNS de Azure)	Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada
Astra Trident (instalado como parte de la detección de clústeres de Kubernetes en NetApp Cloud Manager)	Como back-end de almacenamiento, se usará Astra Trident 21.04 o posterior instalado y configurado, y NetApp ONTAP versión 9.5 o posterior
Registro de imágenes	<p>Debe disponer de un registro privado existente, como Azure Container Registry (ACR), al que puede insertar imágenes de creación de Astra Control Center. Debe proporcionar la dirección URL del registro de imágenes donde cargará las imágenes.</p> <div>  <p>Es necesario habilitar el acceso anónimo para extraer imágenes RTIC para realizar copias de seguridad.</p> </div>

Componente	Requisito
Configuración de Astra Trident/ONTAP	<p>Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. Astra Control Center es compatible con las siguientes clases de almacenamiento ONTAP Kubernetes que se crean al importar su clúster Kubernetes a Cloud Manager de NetApp. Los proporciona Astra Trident:</p> <ul style="list-style-type: none"> • <code>vsaworkingenvironment-<>-ha-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-ha-san</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-nas</code> <code>csi.trident.netapp.io</code> • <code>vsaworkingenvironment-<>-single-san</code> <code>csi.trident.netapp.io</code>



Estos requisitos suponen que Astra Control Center es la única aplicación que se ejecuta en el entorno operativo. Si el entorno ejecuta aplicaciones adicionales, ajuste estos requisitos mínimos según corresponda.

Información general sobre la implementación para Azure

A continuación se ofrece una descripción general del proceso de instalación de Astra Control Center para Azure.

Cada uno de estos pasos se explica más detalladamente a continuación.

1. [Instale un clúster RedHat OpenShift en Azure.](#)
2. [Cree grupos de recursos de Azure.](#)
3. [Compruebe que dispone de suficientes permisos IAM.](#)
4. [Configure Azure.](#)
5. [Configure Cloud Manager de NetApp.](#)
6. [Instalar y configurar Astra Control Center.](#)

Instale un clúster RedHat OpenShift en Azure

El primer paso es instalar un clúster RedHat OpenShift en Azure.

Para obtener instrucciones de instalación, consulte la documentación de RedHat en ["Instalación del clúster OpenShift en Azure"](#) y.. ["Instalar una cuenta de Azure"](#).

Cree grupos de recursos de Azure

Cree al menos un grupo de recursos de Azure.



OpenShift podría crear sus propios grupos de recursos. Además de estos, también debe definir los grupos de recursos de Azure. Consulte la documentación de OpenShift.

Es posible que desee crear un grupo de recursos de clúster de plataforma y un grupo de recursos de clúster de aplicación OpenShift de destino.

Compruebe que dispone de suficientes permisos IAM

Asegúrese de tener suficientes roles y permisos de IAM para poder instalar un clúster RedHat OpenShift y un conector Cloud Manager de NetApp.

Consulte "[Credenciales y permisos de Azure](#)".

Configure Azure

A continuación, configure Azure para crear una red virtual, configurar instancias de computación, crear un contenedor de Azure Blob, crear un registro de contenedores de Azure (ACR) para alojar las imágenes de Astra Control Center y colocar las imágenes en este registro.

Siga la documentación de Azure para completar los siguientes pasos. Consulte "[Instalando el clúster de OpenShift en Azure](#)".

1. Cree una red virtual de Azure.
2. Revise las instancias de computación. Puede ser un servidor con configuración básica o máquinas virtuales en Azure.
3. Si el tipo de instancia no coincide con los requisitos mínimos de recursos de Astra para los nodos maestros y trabajadores, cambie el tipo de instancia en Azure para cumplir los requisitos de Astra. Consulte "[Requisitos del Centro de Control de Astra](#)".
4. Cree al menos un contenedor de Azure Blob para almacenar los backups.
5. Cree una cuenta de almacenamiento. Necesitará una cuenta de almacenamiento para crear un contenedor que se utilizará como bloque en Astra Control Center.
6. Crear un secreto, que es necesario para el acceso a bloques.
7. Cree un Azure Container Registry (ACR) para alojar todas las imágenes de Astra Control Center.
8. Configure el acceso ACR para pulsar/extraer todas las imágenes del Centro de control de Astra.
9. Inserte las imágenes ACC en este registro introduciendo el siguiente script:

```
az acr login -n <AZ ACR URL/Location>  
This script requires ACC manifest file and your Azure ACR location.
```

Ejemplo:


```
manifestfile=astra-control-center-<version>.manifest
AZ_ACR_REGISTRY=<target image repository>
ASTRA_REGISTRY=<source ACC image repository>

while IFS= read -r image; do
    echo "image: $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image"
    root_image=${image%:*}
    echo $root_image
    docker pull $ASTRA_REGISTRY/$image
    docker tag $ASTRA_REGISTRY/$image $AZ_ACR_REGISTRY/$image
    docker push $AZ_ACR_REGISTRY/$image
done < astra-control-center-22.04.41.manifest
```

10. Configure zonas DNS.

Configure Cloud Manager de NetApp

Con Cloud Manager, cree un espacio de trabajo, añada un conector a Azure, cree un entorno de trabajo e importe el clúster.

Siga la documentación de Cloud Manager para completar los siguientes pasos. Consulte ["Introducción a Cloud Manager en Azure"](#).

Lo que necesitará

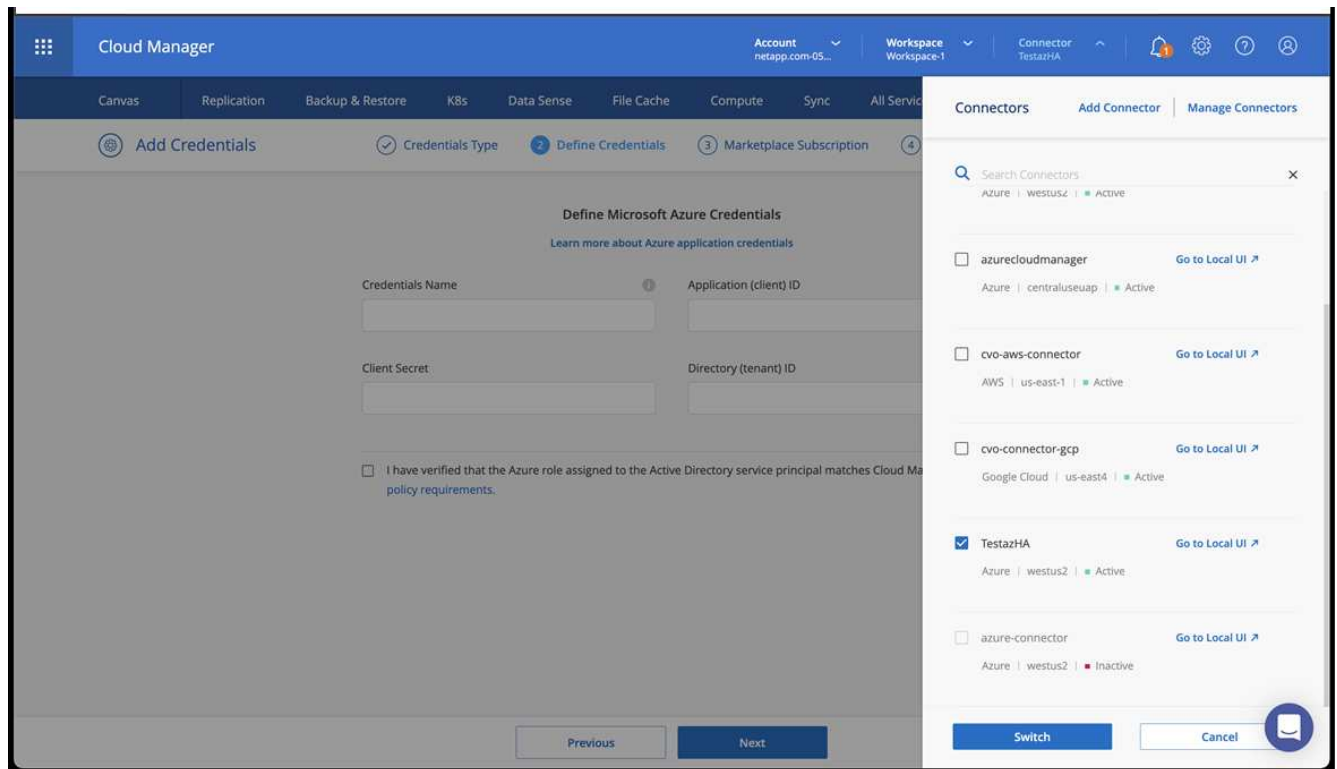
Acceso a la cuenta de Azure con los permisos y roles de IAM necesarios

Pasos

1. Añada sus credenciales a Cloud Manager.
2. Agregue un conector para Azure. Consulte ["Políticas de Cloud Manager"](#).
 - a. Elija **Azure** como proveedor.
 - b. Introduzca las credenciales de Azure, incluidos el ID de aplicación, el secreto de cliente y el ID del directorio (inquilino).

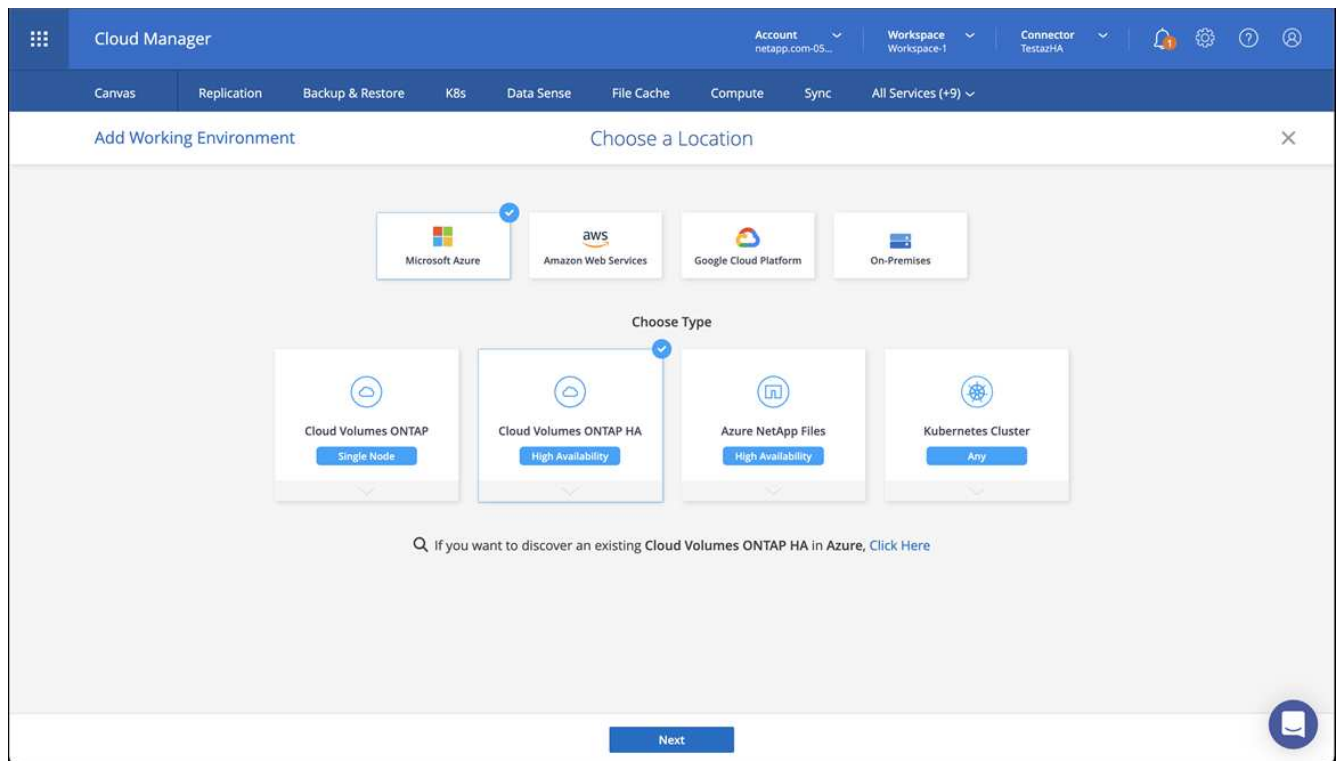
Consulte ["Crear un conector en Azure desde Cloud Manager"](#).

3. Asegúrese de que el conector está en marcha y cambie a dicho conector.



4. Cree un entorno de trabajo para su entorno de cloud.

- Ubicación: "Microsoft Azure".
- Tipo: "Cloud Volumes ONTAP ha".



5. Importe el clúster OpenShift. El clúster se conectará al entorno de trabajo que acaba de crear.

- Consulte los detalles del clúster de NetApp seleccionando **K8s > Lista de clústeres > Detalles del**

clúster.

The screenshot displays the Cloud Manager interface for a cluster named 'targetazacc'. The top navigation bar includes 'Account', 'Workspace', and 'Connector'. The main menu has tabs for 'Canvas', 'Replication', 'Backup & Restore', 'K8s', 'Data Sense', 'File Cache', 'Compute', 'Sync', and 'All Services (+9)'. The 'K8s' tab is active, showing the 'Cluster List' and 'Cluster Details' for 'targetazacc'. The cluster status is 'Running'. Key details include Cluster Version 'v1.21.6+bb8d50a', Added by 'Import', Volumes '3', VPC '-', Date Added 'April 14, 2022', Trident Version 'v21.04.1', and Provider 'Microsoft Azure'. Below this, there is a section for '1 Working Environments' with a table showing 'testHAenvaz' as the environment name, Microsoft Azure as the provider, westus2 as the region, and 10.0.0.0/16 as the subnet. The capacity is 0.00 used of 500 GB available. Further down, there is a section for '3 Storage Classes' with a table showing 'managed-premium' as the storage class ID, Microsoft Azure as the provisioner, and 0 volumes. Another storage class 'vsaworkingenvironment-xr1hs5pd-ha-nas' is listed with NetApp as the provisioner and 3 volumes. The interface also includes buttons for 'Update Kubeconfig' and 'Connect to Working Environment'.

b. En la esquina superior derecha, tenga en cuenta la versión de Trident.

c. Observe las clases de almacenamiento del clúster Cloud Volumes ONTAP que muestran NetApp como el aprovisionador.

Esto importa su clúster de Red Hat OpenShift y asigna una clase de almacenamiento predeterminada. Seleccione la clase de almacenamiento. Trident se instala automáticamente como parte del proceso de importación y detección.

6. Obsérvese todos los volúmenes y volúmenes persistentes en esta puesta en marcha de Cloud Volumes ONTAP.

7. Cloud Volumes ONTAP puede funcionar como un nodo único o en alta disponibilidad. Si ha está habilitada, anote el estado de alta disponibilidad y el estado de puesta en marcha del nodo que se ejecutan en Azure.

Instalar y configurar Astra Control Center

Instale Astra Control Center con el estándar ["instrucciones de instalación"](#).

Con Astra Control Center, añada un bucket de Azure. Consulte ["Configure Astra Control Center y añada cucharones"](#).

Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.