Manos a la obra

Astra Control Center

NetApp
October 23, 2024

Tabla de contenidos

Manos a la obra

Requisitos del Centro de Control de Astra

Para comenzar, verifique la compatibilidad de los clústeres de Kubernetes, sus aplicaciones, las licencias y el explorador web.

Requisitos generales del clúster de Kubernetes

Un clúster de Kubernetes debe cumplir los siguientes requisitos generales para poder detectarlo y gestionarlo desde Astra Control Center.

- **Registro de imágenes**: Debe tener un registro de imágenes Docker privado existente en el que puede insertar imágenes de creación de Astra Control Center. Debe tener la dirección URL del registro de imágenes donde cargará las imágenes y debe haber etiquetado las imágenes para el registro del contenedor privado.
- **Configuración del almacenamiento de Trident/ONTAP**: Astra Control Center requiere que Trident versión 21.01 o 21.04 ya esté instalado y configurado para que funcione con NetApp ONTAP versión 9.5 o posterior como back-end de almacenamiento. Astra Control Center requiere que se cree una clase de almacenamiento y se establezca como la clase de almacenamiento predeterminada. El Centro de control de Astra admite los siguientes controladores de ONTAP proporcionados por Trident:
  - ontap-nas
  - ontap-nas-flexgroup
  - san ontap
  - ontap-san-economía

Si tiene pensado gestionar el clúster Kubernetes desde Astra Control Center y usar el clúster para alojar la instalación de Astra Control Center, el clúster tiene los siguientes requisitos adicionales:

- La versión más reciente de Kubernetes "componente de controladora snapshot" está instalado
- Un Trident "volumesnapshotclass object" ha sido definido por un administrador
- Existe una clase de almacenamiento de Kubernetes predeterminada en el clúster
- Se configura al menos una clase de almacenamiento para usar Trident
- Método para señalar el FQDN de Astra Control Center a la dirección IP externa del servicio Astra Control Center

Clusters OpenShift

Astra Control Center requiere un clúster de la plataforma de contenedores Red Hat OpenShift 4.6.8 o 4.7 con clases de almacenamiento de Trident respaldadas por ONTAP 9.5 o una versión más reciente, con los siguientes atributos:

- Al menos 300 GB de capacidad de almacenamiento disponible de ONTAP
- 3 nodos de controladoras con 4 núcleos CPU, 16 GB de RAM y 120 GB de almacenamiento disponibles cada uno
- 3 nodos de trabajo con al menos 12 núcleos de CPU, 32 GB de RAM y 50 GB de almacenamiento disponible cada uno

- Kubernetes, versión 1.19 o 1.20
- Tipo de servicio "LoadBalancer" disponible para que el tráfico de entrada se envíe a los servicios del clúster de OpenShift
- Método para señalar el FQDN de Astra Control Center a la dirección IP de carga equilibrada

> Estos requisitos mínimos suponen que Astra Control Center es la única aplicación que se ejecuta en el clúster OpenShift. Si el clúster ejecuta aplicaciones adicionales, debe ajustar estos requisitos mínimos según corresponda.

Asegúrese de que su clúster cumple los requisitos mínimos y de que sigue las prácticas recomendadas de Kubernetes para que Astra Control Center esté altamente disponible en su clúster de Kubernetes.

> OpenShift 4.8 no es compatible.

> Durante la clonación de aplicaciones, Astra Control Center debe permitir a OpenShift montar volúmenes y cambiar la propiedad de los archivos. Por este motivo, es necesario configurar el ONTAP para que las operaciones de volumen se completen correctamente mediante los siguientes comandos:
>
> 1. `export-policy rule modify -vserver svm0 -policyname default -ruleindex 1 -superuser sys`
> 2. `export-policy rule modify -policyname default -ruleindex 1 -anon 65534`

> Si tiene pensado añadir un segundo clúster OpenShift 4.6 o 4.7 como un recurso de computación gestionado, debe asegurarse de que la función Trident Volume Snapshot está habilitada. Consulte la información oficial de Trident "instrucciones" Para habilitar y probar Snapshots de volumen con Trident.

Requisitos de gestión de aplicaciones

Astra Control Center tiene los siguientes requisitos de gestión de aplicaciones:

- **Licencia**: Necesita una licencia de Astra Control Center para gestionar aplicaciones mediante Astra Control Center.
- **Helm 3**: Si utiliza Helm para desplegar aplicaciones, Astra Control Center requiere Helm versión 3. Se admite por completo la gestión y clonación de las aplicaciones implementadas con Helm 3 (o actualizadas de Helm 2 a Helm 3). Las aplicaciones implementadas con Helm 2 no son compatibles.
- **Gestión del operador**: Astra Control Center no admite aplicaciones que se implementan con operadores habilitados para Operator Lifecycle Manager (OLM) o operadores con ámbito de clúster.

Acceso a Internet

Debe determinar si tiene acceso externo a Internet. Si no lo hace, es posible que algunas funcionalidades sean limitadas, como recibir datos de supervisión y métricas de Cloud Insights de NetApp, o enviar paquetes de soporte al sitio de soporte de NetApp.

Licencia

Astra Control Center requiere una licencia de Astra Control Center para obtener todas las funciones. Obtenga una licencia de evaluación o una licencia completa de NetApp. Sin una licencia, no podrá:

- Defina aplicaciones personalizadas
- Cree instantáneas o clones de las aplicaciones existentes
- Configure las políticas de protección de datos

Si desea probar Astra Control Center, puede "utilice una licencia de evaluación de 90 días".

Tipo de servicio "LoadBalancer" para clústeres de Kubernetes en las instalaciones

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. Para clústeres OpenShift en las instalaciones, puede utilizar "MetalLB" Para asignar automáticamente 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.

Requisitos de red

El clúster que aloja a Astra Control Center se comunica mediante los siguientes puertos TCP. Debe asegurarse de que estos puertos estén permitidos a través de cualquier firewall y configurar firewalls para permitir que cualquier tráfico de salida HTTPS que se origine en la red Astra. Algunos puertos requieren conectividad de ambas formas entre el clúster que aloja Astra Control Center y cada clúster gestionado (se indica si procede).

Producto	Puerto	Protocolo	Dirección	Específico
Astra Control Center	443	HTTPS	Entrada	Acceso de interfaz de usuario/API: Asegúrese de que este puerto está abierto de ambas formas entre el clúster que aloja a Astra Control Center y cada clúster gestionado
Astra Control Center	9090	HTTPS	• Entrada (al cluster que aloja Astra Control Center) • Salida (puerto aleatorio de la dirección IP del nodo de cada nodo de trabajo de cada clúster gestionado)	Datos de métricas al consumidor de mediciones: Asegúrese de que cada clúster gestionado pueda acceder a este puerto en el clúster que aloja a Astra Control Center

Producto	Puerto	Protocolo	Dirección	Específico
Trident	34571	HTTPS	Entrada	Comunicación en Pod de nodo
Trident	9220	HTTP	Entrada	Extremo de métricas

Exploradores web compatibles

Astra Control Center es compatible con las versiones recientes de Firefox, Safari y Chrome con una resolución mínima de 1280 x 720.

El futuro

Vea la "inicio rápido" descripción general.

Inicio rápido para Astra Control Center

Esta página ofrece una descripción general de alto nivel de los pasos necesarios para empezar con Astra Control Center. Los vínculos de cada paso le llevan a una página que proporciona más detalles.

¡Pruébela! Si desea probar Astra Control Center, puede utilizar una licencia de evaluación de 90 días. Consulte "información sobre licencias" para obtener más detalles.

1 **Revise los requisitos del clúster de Kubernetes**

- Astra funciona con clústeres de Kubernetes con un back-end de almacenamiento de ONTAP configurado con Trident.
- Los clústeres deben ejecutarse en buen estado, con al menos tres nodos de trabajo en línea.
- El clúster debe ejecutar Kubernetes.

"Más información sobre los requisitos de Astra Control Center".

2 **Descargue e instale Astra Control Center**

- Descargue Astra Control Center desde el sitio de soporte de NetApp.
- Instale Astra Control Center en su entorno local.
- Descubra su configuración de Trident respaldada por el back-end de almacenamiento de ONTAP.

  Para nuestra primera versión, instalará las imágenes en un registro de OpenShift o utilizará su registro local.

"Más información sobre la instalación de Astra Control Center".

3 **Complete algunas tareas de configuración inicial**

- Añadir una licencia.
- Añada un clúster de Kubernetes y Astra Control Center descubre los detalles.

- Añada un back-end de almacenamiento de ONTAP.
- Opcionalmente, agregue un bucket de almacén de objetos que almacenará las copias de seguridad de la aplicación.

"Obtenga más información acerca del proceso de configuración inicial".

4 Utilice Astra Control Center

Cuando termine de configurar Astra Control Center, a continuación puede hacer lo siguiente:

- Gestionar una aplicación. "Más información sobre cómo gestionar aplicaciones".
- De manera opcional, conéctese a Cloud Insights de NetApp para mostrar métricas sobre el estado del sistema, la capacidad y el rendimiento dentro de la IU del centro de control de Astra. "Obtenga más información sobre cómo conectarse a Cloud Insights".

5 Continuar desde este Inicio rápido

"Instalar Astra Control Center".

Obtenga más información

- "Utilice la API Astra"

Instalar Astra Control Center

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

- Instalar Astra Control Center
- Inicie sesión en la interfaz de usuario de Astra Control Center

Instalar Astra Control Center

Para instalar Astra Control Center, descargue el paquete de instalación desde el sitio de soporte de NetApp y realice una serie de comandos 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.

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
```

Acerca de esta tarea

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

- Instala los componentes de Astra en `netapp-acc` (o espacio de nombres personalizado).
- Crea una cuenta predeterminada.
- Establece una dirección de correo electrónico de usuario administrativo predeterminada y una contraseña única predeterminada de `ACC-<UUID_of_installation>` Por este ejemplo de Astra Control Center. A este usuario se le asigna el rol de propietario del sistema y es necesario 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.

> Los comandos de Podman se pueden utilizar en lugar de los comandos de Docker si está utilizando el repositorio de Podman de Red Hat.

Pasos

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 desde "Sitio de soporte de NetApp".
3. (Opcional) Use el siguiente comando para verificar la firma del paquete:

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

4. Extraiga las imágenes:

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

5. Cambie al directorio Astra.

```
cd astra-control-center-[version]
```

6. Agregue los archivos del directorio imagen de Astra Control Center al registro local.

> Consulte una secuencia de comandos de ejemplo para la carga automática de imágenes a continuación.

   a. Inicie sesión en su registro de Docker:

```
docker login [Docker_registry_path]
```

b. Cargue las imágenes en Docker.

c. Etiquete las imágenes.

d. Inserte las imágenes en el registro local.

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

7. (Sólo para registros con requisitos de autenticación) 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:

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

Respuesta de ejemplo:

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

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

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

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] --docker-server=[Docker_registry_path] --docker
-username=[username] --docker-password=[token]
```

Respuesta

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

8. 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
```

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

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

b. Cambiar `[Docker_registry_path]` para la `kube-rbac-prox` imagen a la ruta del registro en la que ha insertado las imágenes en un paso anterior.

c. Cambiar `[Docker_registry_path]` para la `acc-operator-controller-manager` imagen a la ruta del registro en la que ha insertado las imágenes en un paso anterior.

```
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: [Docker_registry_path]/kube-rbac-proxy:v0.5.0
        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: [Docker_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

9. Edite el archivo de recursos personalizados (CR) del Centro de control de Astra (`astra_control_center_min.yaml`):

```
vim astra_control_center_min.yaml
```

> Si se requieren personalizaciones adicionales para su entorno, puede utilizar `astra_control_center.yaml` Como CR alternativo. `astra_control_center_min.yaml` Es la CR predeterminada y es adecuada para la mayoría de las instalaciones.

> Las propiedades configuradas por la CR no se pueden cambiar tras la implementación inicial de Astra Control Center.

a. Cambiar `[Docker_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. (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.

g. (Opcional) cambie el `storageClass` Valor en otro recurso de la clase de almacenamiento de Trident, si es necesario para su instalación.

h. Si no está utilizando un registro que requiere autorización, elimine el `secret` línea.

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

10. 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
```

11. 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]
```

Respuesta de ejemplo:

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

12. Ejecute el siguiente parche para corregir "vinculación de roles del clúster".
13. 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]
```

Respuesta de ejemplo:

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

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

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

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

Respuesta de ejemplo:

```
NAME                                          READY   STATUS    RESTARTS
AGE
acc-helm-repo-5fdfff786f-gkv6z                1/1     Running   0
4m58s
activity-649f869bf7-jn5gs                     1/1     Running   0
3m14s
asup-79846b5fdc-s9s97                         1/1     Running   0
3m10s
authentication-84c78f5cf4-qhx9t               1/1     Running   0
118s
billing-9b8496787-v8rzv                       1/1     Running   0
2m54s
bucketservice-5fb876d9d5-wkfvz                1/1     Running   0
3m26s
cloud-extension-f9f4f59c6-dz6s6               1/1     Running   0
3m
cloud-insights-service-5676b8c6d4-6q7lv       1/1     Running   0
2m52s
composite-compute-7dcc9c6d6c-lxdr6            1/1     Running   0
2m50s
composite-volume-74dbfd7577-cd42b             1/1     Running   0
3m2s
credentials-75dbf46f9d-5qm2b                  1/1     Running   0
3m32s
entitlement-6cf875cb48-gkvhp                  1/1     Running   0
3m12s
features-74fd97bb46-vss2n                     1/1     Running   0
3m6s
fluent-bit-ds-2g9jb                           1/1     Running   0
113s
fluent-bit-ds-5tg5h                           1/1     Running   0
113s
fluent-bit-ds-qfxb8                           1/1     Running   0
```

```
113s
graphql-server-7769f98b86-p4qrv              1/1     Running   0
90s
identity-566c566cd5-ntfj6                    1/1     Running   0
3m16s
influxdb2-0                                  1/1     Running   0
4m43s
krakend-5cb8d56978-44q66                     1/1     Running   0
93s
license-66cbbc6f48-27kgf                     1/1     Running   0
3m4s
login-ui-584f7fd84b-dmdrp                    1/1     Running   0
87s
loki-0                                       1/1     Running   0
4m44s
metrics-ingestion-service-6dcfddf45f-mhnvh   1/1     Running   0
3m8s
monitoring-operator-78d67b4d4-nxs6v          2/2     Running   0
116s
nats-0                                       1/1     Running   0
4m40s
nats-1                                       1/1     Running   0
4m26s
nats-2                                       1/1     Running   0
4m15s
nautilus-9b664bc55-rn9t8                     1/1     Running   0
2m56s
openapi-dc5ddfb7d-6q8vh                      1/1     Running   0
3m20s
polaris-consul-consul-5tjs7                  1/1     Running   0
4m43s
polaris-consul-consul-5wbnx                  1/1     Running   0
4m43s
polaris-consul-consul-bfvl7                  1/1     Running   0
4m43s
polaris-consul-consul-server-0               1/1     Running   0
4m43s
polaris-consul-consul-server-1               1/1     Running   0
4m43s
polaris-consul-consul-server-2               1/1     Running   0
4m43s
polaris-mongodb-0                            2/2     Running   0
4m49s
polaris-mongodb-1                            2/2     Running   0
4m22s
polaris-mongodb-arbiter-0                    1/1     Running   0
```

```
4m49s
polaris-ui-6648875998-75d98                   1/1     Running   0
92s
polaris-vault-0                               1/1     Running   0
4m41s
polaris-vault-1                               1/1     Running   0
4m41s
polaris-vault-2                               1/1     Running   0
4m41s
storage-backend-metrics-69546f4fc8-m7lfj      1/1     Running   0
3m22s
storage-provider-5d46f755b-qfv89              1/1     Running   0
3m30s
support-5dc579865c-z4pwq                      1/1     Running   0
3m18s
telegraf-ds-4452f                             1/1     Running   0
113s
telegraf-ds-gnqxl                             1/1     Running   0
113s
telegraf-ds-jhw74                             1/1     Running   0
113s
telegraf-rs-gg6m4                             1/1     Running   0
113s
telemetry-service-6dcc875f98-zft26            1/1     Running   0
3m24s
tenancy-7f7f77f699-q7l6w                      1/1     Running   0
3m28s
traefik-769d846f9b-c9crt                      1/1     Running   0
83s
traefik-769d846f9b-l9n4k                      1/1     Running   0
67s
trident-svc-8649c8bfc5-pdj79                  1/1     Running   0
2m57s
vault-controller-745879f98b-49c5v             1/1     Running   0
4m51s
```

15. (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
```

16. Cuando se estén ejecutando todos los POD, verifique el éxito de la instalación mediante la recuperación de la instancia de AstraControlCenter instalada por el operador ACC.

```
kubectl get acc -o yaml -n netapp-acc
```

17. Compruebe la `status.deploymentState` en la respuesta para `Deployed` valor. Si la implementación no se realizó correctamente, aparece en su lugar un mensaje de error.

> Utilizará la `uuid` en el siguiente paso.

```
apiVersion: v1
items:
- apiVersion: astra.netapp.io/v1
  kind: AstraControlCenter
  metadata:
    creationTimestamp: "2021-07-28T21:36:49Z"
    finalizers:
    - astracontrolcenter.netapp.io/finalizer
   generation: 1
    name: astra
    namespace: netapp-acc
    resourceVersion: "27797604"
    selfLink: /apis/astra.netapp.io/v1/namespaces/netapp-
acc/astracontrolcenters/astra
    uid: 61cd8b65-047b-431a-ba35-510afcb845f1
  spec:
    accountName: Example
    astraAddress: astra.example.com
    astraResourcesScaler: "Off"
    astraVersion: 21.08.52
    autoSupport:
      enrolled: false
    email: admin@example.com
    firstName: SRE
    lastName: Admin
    imageRegistry:
      name: registry_name/astra
  status:
    certManager: deploy
    deploymentState: Deployed
    observedGeneration: 1
    observedVersion: 21.08.52
    postInstall: Complete
    uuid: c49008a5-4ef1-4c5d-a53e-830daf994116
kind: List
metadata:
  resourceVersion: ""
  selfLink: ""
```

18. Para obtener la contraseña única que utilizará cuando inicie sesión en Astra Control Center, copie la `status.uuid` valor de la respuesta en el paso anterior. La contraseña es `ACC-` Seguido del valor UUID (`ACC-[UUID]` o, en este ejemplo, `ACC-c49008a5-4ef1-4c5d-a53e-830daf994116`).

Inicie sesión en la interfaz de usuario de Astra Control Center

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

Pasos

1. En un explorador, introduzca el FQDN que utilizó en `astraAddress` en la `astra_control_center_min.yaml` CR cuando Ha instalado ACC.
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` pulg `astra_control_center_min.yaml` CR cuando Ha instalado ACC, 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".

Configure Astra Control Center

Después de instalar Astra Control Center, inicie sesión en la interfaz de usuario y cambie la contraseña, le interesa configurar una licencia, añadir clústeres, gestionar el almacenamiento y añadir bloques.

Tareas

- Agregue una licencia de Astra Control Center
- Añada el clúster
- Añada un back-end de almacenamiento
- Añadir un bucket

Agregue una licencia de Astra Control Center

Puede añadir una licencia nueva con la interfaz de usuario o. "API" Para obtener todas las funciones de Astra Control Center. Sin una licencia, el uso de Astra Control Center se limita a gestionar usuarios y agregar nuevos clústeres.

Lo que necesitará

Al descargar Astra Control Center desde "Sitio de soporte de NetApp"También puede descargar el archivo de licencia de NetApp (NLF). Asegúrese de tener acceso a este archivo de licencia.

> Para actualizar una evaluación existente o una licencia completa, consulte "Actualizar una licencia existente".

Añada una licencia completa o de evaluación

Las licencias de Astra Control Center miden los recursos de CPU mediante unidades de CPU de Kubernetes. La licencia debe tener en cuenta los recursos de CPU asignados a los nodos de trabajo de todos los clústeres de Kubernetes gestionados. Antes de agregar una licencia, debe obtener el archivo de licencia (NLF) de "Sitio de soporte de NetApp".

También puede probar Astra Control Center con una licencia de evaluación, que le permite utilizar Astra Control Center durante 90 días a partir de la fecha de descarga de la licencia. Puede inscribirse para obtener una prueba gratuita registrándose "aquí".

> Si su instalación crece para superar el número de unidades CPU con licencia, Astra Control Center le impide gestionar nuevas aplicaciones. Se muestra una alerta cuando se supera la capacidad.

Pasos

1. Inicie sesión en la interfaz de usuario de Astra Control Center.
2. Seleccione **cuenta** > **Licencia**.
3. Seleccione **Agregar licencia**.
4. Busque el archivo de licencia (NLF) que descargó.
5. Seleccione **Agregar licencia**.

La página **cuenta** > **Licencia** muestra la información de la licencia, la fecha de caducidad, el número de serie de la licencia, el ID de cuenta y las unidades de CPU utilizadas.

> Si dispone de una licencia de evaluación, asegúrese de almacenar su ID de cuenta para evitar la pérdida de datos en caso de que se produzca un error en Astra Control Center si no envía los ASUP.

Añada el clúster

Para comenzar a gestionar las aplicaciones, añada un clúster de Kubernetes y gestiónelo como un recurso de computación. Es necesario añadir un clúster para Astra Control Center para descubrir sus aplicaciones Kubernetes.

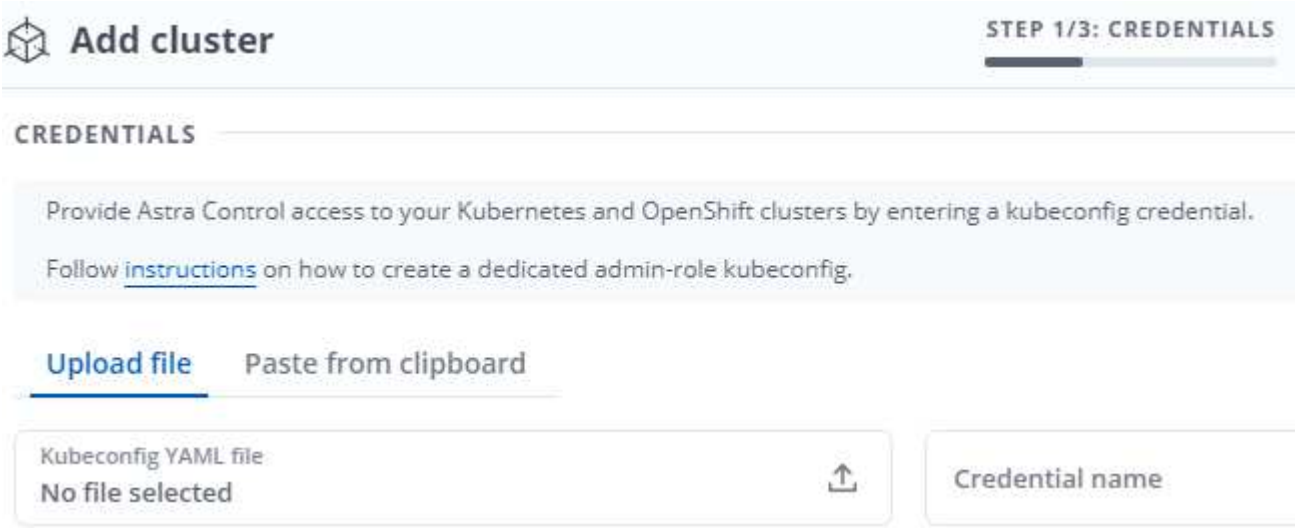
> Le recomendamos que Astra Control Center gestione el clúster en el que se implementa primero antes de añadir otros clústeres a Astra Control Center para su gestión. Disponer del cluster inicial en administración es necesario para enviar datos Kubemetrics y datos asociados al cluster para mediciones y resolución de problemas. Puede utilizar la función **Agregar clúster** para administrar un clúster con Astra Control Center.

> **Lo que necesite.#8217;lo necesitará**
>
> Antes de añadir un clúster, revise y realice la operación necesaria "requisitos previos".

Pasos

1. En **Dashboard** de la interfaz de usuario de Astra Control Center, seleccione **Agregar** en la sección Clusters.
2. En la ventana **Agregar clúster** que se abre, cargue un `kubeconfig.yaml` archivar o pegar el contenido de un `kubeconfig.yaml` archivo.

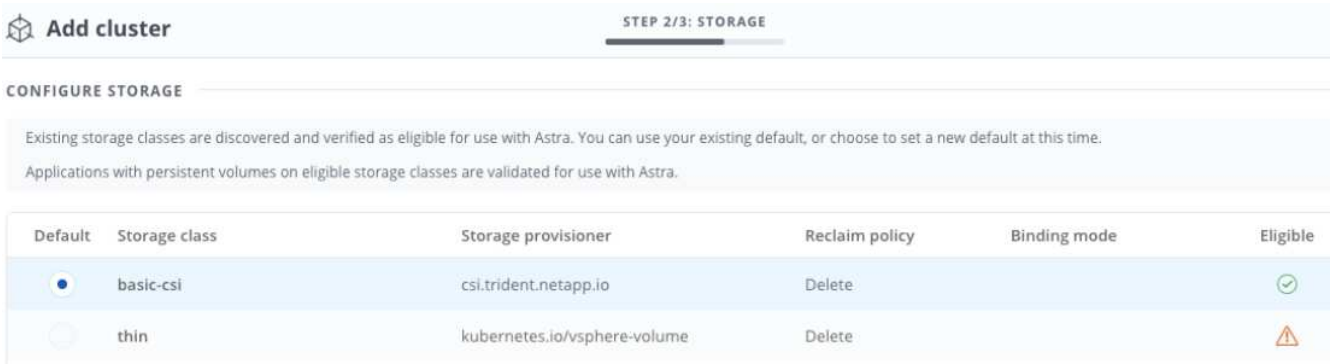
   > La `kubeconfig.yaml` el archivo debe incluir **sólo la credencial de cluster para un cluster**.



   > Si crea el suyo propio `kubeconfig` file, debe definir sólo un elemento de contexto **uno** en él. Consulte "Documentación de Kubernetes" para obtener información acerca de cómo crear `kubeconfig` archivos.

3. Introduzca un nombre de credencial. De forma predeterminada, el nombre de las credenciales se completa automáticamente como nombre del clúster.
4. Seleccione **Configurar almacenamiento**.
5. Seleccione la clase de almacenamiento que se va a utilizar para este clúster de Kubernetes y seleccione **Review**.

> Debe seleccionar una clase de almacenamiento de Trident respaldada por un almacenamiento de ONTAP.



6. Revise la información y si todo parece bien, seleccione **Agregar clúster**.

Resultado

El clúster entra en el estado **detectando** y luego cambia a **ejecutando**. Ha añadido correctamente un clúster de Kubernetes y ahora lo gestiona en Astra Control Center.

> Después de agregar un clúster para administrarlo en Astra Control Center, puede que el operador de supervisión tarde unos minutos en implementar. Hasta entonces, el icono de notificación se vuelve rojo y registra un evento **Comprobación de estado del agente de supervisión fallida**. Puede ignorar esto porque el problema se resuelve cuando Astra Control Center obtiene el estado correcto. Si el problema no se resuelve en unos minutos, vaya al clúster y ejecute `oc get pods -n netapp-monitoring` como punto de partida. Deberá consultar los registros del operador de supervisión para depurar el problema.

Añada un back-end de almacenamiento

Puede añadir un back-end de almacenamiento para que Astra Control pueda gestionar sus recursos. Gestionar los clústeres de almacenamiento en Astra Control como back-end de almacenamiento le permite obtener vínculos entre los volúmenes persistentes (VP) y el back-end de almacenamiento, así como mediciones de almacenamiento adicionales.

Puede añadir un back-end de almacenamiento de las siguientes formas:

- Configure el almacenamiento cuando añada un clúster. Consulte "Añada el clúster".
- Añada un back-end de almacenamiento detectado mediante la opción Dashboard o Backends.

Puede añadir un back-end de almacenamiento ya detectado mediante las siguientes opciones:

- Agregue el back-end de almacenamiento mediante Dashboard
- Agregue el backends de almacenamiento mediante la opción Backends

Agregue el back-end de almacenamiento mediante Dashboard

1. Desde la consola, realice una de las siguientes acciones:
   a. En la sección backend de almacenamiento del panel, seleccione **gestionar**.
   b. En la sección Resumen de recursos del panel > Gestión de fondo de almacenamiento, seleccione **Agregar**.

2. Introduzca las credenciales de administración de ONTAP y seleccione **Revisión**.
3. Confirme los detalles del backend y seleccione **Administrar**.

   El backend aparece en la lista con información de resumen.

Agregue el backends de almacenamiento mediante la opción Backends

1. En el área de navegación de la izquierda, seleccione **Backends**.
2. Seleccione **gestionar**.
3. Introduzca las credenciales de administración de ONTAP y seleccione **Revisión**.
4. Confirme los detalles del backend y seleccione **Administrar**.

   El backend aparece en la lista con información de resumen.

5. Para ver los detalles del almacenamiento del entorno de administración, selecciónelo.

> También se muestran los volúmenes persistentes que utilizan las aplicaciones del clúster de computación gestionado.

Añadir un bucket

Añadir proveedores de bloques de almacenamiento de objetos es esencial si desea realizar backups de sus aplicaciones y del almacenamiento persistente o si desea clonar aplicaciones entre clústeres. Astra Control almacena estas copias de seguridad o clones en los bloques de almacenamiento de objetos que defina.

Cuando se agrega un bloque, Astra Control Marca un bloque como el indicador de segmento predeterminado. El primer bloque que crea se convierte en el bloque predeterminado.

No necesita un bucket si va a clonar la configuración de sus aplicaciones y el almacenamiento persistente en el mismo clúster.

Utilice cualquiera de los siguientes tipos de bloques:

- ONTAP S3 de NetApp
- StorageGRID S3 de NetApp
- Genérico S3

> Aunque Astra Control Center es compatible con Amazon S3 como proveedor de cubos de S3 genérico, Astra Control Center podría no admitir todos los proveedores de almacenes de objetos que afirman que Amazon es compatible con S3.

Para obtener instrucciones sobre cómo añadir cubos con la API Astra, consulte "Información sobre API y automatización de Astra".

Pasos

1. En el área de navegación de la izquierda, seleccione **Cuchos**.
   a. Seleccione **Agregar**.
   b. Seleccione el tipo de bloque.

> Cuando agregue un cubo, seleccione el tipo de proveedor de cucharón correcto con las credenciales que sean correctas para ese proveedor. Por ejemplo, la interfaz de usuario acepta ONTAP S3 de NetApp como el tipo con credenciales de StorageGRID; sin embargo, esto hará que se produzcan errores en todos los backups y las restauraciones futuras de aplicaciones que utilizan este bloque.

c. Cree un nuevo nombre de bloque o introduzca un nombre de bloque existente y una descripción opcional.

> El nombre del bloque y la descripción aparecen como una ubicación de copia de seguridad que puede elegir más tarde al crear una copia de seguridad. El nombre también aparece durante la configuración de la política de protección.

d. Introduzca el nombre o la dirección IP del servidor S3.

e. Si desea que este bloque sea el bloque predeterminado para todos los backups, compruebe la `Make this bucket the default bucket for this private cloud` opción.

> Esta opción no aparece para el primer bloque que cree.

f. Continúe añadiendo información sobre credenciales.

Añada credenciales de acceso de S3

Añada credenciales de acceso de S3 en cualquier momento.

Pasos

1. En el cuadro de diálogo Cuchos, seleccione la ficha **Agregar** o **utilizar existente**.
   a. Introduzca un nombre para la credencial que la distingue de otras credenciales en Astra Control.
   b. Escriba el identificador de acceso y la clave secreta pegando el contenido del portapapeles.

El futuro

Ahora que ha iniciado sesión y agregado clústeres a Astra Control Center, está listo para empezar a utilizar las funciones de gestión de datos de aplicaciones de Astra Control Center.

- "Gestionar usuarios"
- "Inicie la gestión de aplicaciones"
- "Proteja sus aplicaciones"
- "Clone aplicaciones"
- "Gestionar notificaciones"
- "Conéctese a Cloud Insights"
- "Agregue un certificado TLS personalizado"

Obtenga más información

- "Utilice la API Astra"
- "Problemas conocidos"

Requisitos previos para añadir un clúster

Debe asegurarse de que se cumplan las condiciones previas antes de añadir un clúster. También debe ejecutar las comprobaciones de elegibilidad para asegurarse de que su clúster esté listo para ser agregado a Astra Control Center.

Qué necesitará antes de añadir un clúster

- Un clúster que ejecuta OpenShift 4.6 o 4.7, y que cuenta con clases de almacenamiento de Trident respaldadas por ONTAP 9.5 o una versión posterior.
  - Uno o varios nodos de trabajo con al menos 1 GB de RAM disponibles para ejecutar servicios de telemetría.

> Si tiene pensado añadir un segundo clúster OpenShift 4.6 o 4.7 como un recurso de computación gestionado, debe asegurarse de que la función Snapshot de volumen de Trident esté habilitada. Consulte la información oficial de Trident "instrucciones" Para habilitar y probar Snapshots de volumen con Trident.

- El superusuario y el ID de usuario establecidos en el sistema ONTAP de respaldo para realizar copias de seguridad y restaurar aplicaciones con Astra Control Center (ACC). Ejecute los siguientes comandos en la línea de comandos de la ONTAP:
  `export policy rule modify -vserver svm0 -policyname default -ruleindex 1 -superuser sys`
  `export-policy rule modify -policyname default -ruleindex 1 -anon 65534` (este es el valor predeterminado)

Ejecutar las comprobaciones de elegibilidad

Ejecute las siguientes comprobaciones de elegibilidad para asegurarse de que su clúster esté listo para ser agregado a Astra Control Center.

Pasos

1. Compruebe la versión de Trident.

```
kubectl get tridentversions -n trident
```

Si Trident existe, se muestra una salida similar a la siguiente:

```
NAME      VERSION
trident   21.04.0
```

Si Trident no existe, se muestra un resultado similar al siguiente:

```
error: the server doesn't have a resource type "tridentversions"
```

Si Trident no está instalado o la versión instalada no es la más reciente, debe instalar la versión más reciente de Trident antes de continuar. Consulte "Documentación de Trident" si desea obtener instrucciones.

2. Compruebe si las clases de almacenamiento están usando los controladores de Trident compatibles. El nombre del aprovisionador debe ser `csi.trident.netapp.io`. Consulte el siguiente ejemplo:

```
kubectl get storageClass -A
NAME                    PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)    csi.trident.netapp.io          Delete
Immediate           true                   5d23h
thin                    kubernetes.io/vsphere-volume   Delete
Immediate           false                  6d
```

Cree una imagen de rol administrativo

Asegúrese de que dispone de lo siguiente en su máquina antes de realizar los pasos siguientes:

- `kubectl` v1.19 o posterior instalado
- Una imagen marcada activa con los derechos de administrador del clúster para el contexto activo

Pasos

1. Cree una cuenta de servicio del siguiente modo:

   a. Cree un archivo de cuenta de servicio llamado `astracontrol-service-account.yaml`.

      Ajuste el nombre y el espacio de nombres según sea necesario. Si se realizan cambios aquí, debe aplicar los mismos cambios en los pasos siguientes.

```
<strong>astracontrol-service-account.yaml</strong>
```

+

```
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astracontrol-service-account
  namespace: default
```

   a. Aplicar la cuenta de servicio:

```
kubectl apply -f astracontrol-service-account.yaml
```

2. Conceda permisos de administrador del clúster de la siguiente manera:

   a. Cree un `ClusterRoleBinding` archivo llamado `astracontrol-clusterrolebinding.yaml`.

      Ajuste los nombres y espacios de nombres modificados al crear la cuenta de servicio según sea necesario.

```
<strong>astracontrol-clusterrolebinding.yaml</strong>
```

+

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astracontrol-admin
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astracontrol-service-account
  namespace: default
```

   a. Aplique el enlace de roles del clúster:

```
kubectl apply -f astracontrol-clusterrolebinding.yaml
```

3. Enumere los secretos de la cuenta de servicio, reemplazando `<context>` con el contexto correcto para su instalación:

```
kubectl get serviceaccount astracontrol-service-account --context
<context> --namespace default -o json
```

El final de la salida debe ser similar a lo siguiente:

```
"secrets": [
{ "name": "astracontrol-service-account-dockercfg-vhz87"},
{ "name": "astracontrol-service-account-token-r59kr"}
]
```

Los índices de cada elemento de la `secrets` la matriz comienza con 0. En el ejemplo anterior, el índice para `astracontrol-service-account-dockercfg-vhz87` sería 0 y el índice para `astracontrol-`

`service-account-token-r59kr` sería 1. En la salida, anote el índice del nombre de la cuenta de servicio que contiene la palabra "token".

4. Genere la kubeconfig de la siguiente manera:

   a. Cree un `create-kubeconfig.sh` archivo. Si el índice de token que anotó en el paso anterior no era 0, reemplace el valor para `TOKEN_INDEX` al principio de la secuencia de comandos siguiente con el valor correcto.

```
<strong>create-kubeconfig.sh</strong>
```

```
# Update these to match your environment. Replace the value for
TOKEN_INDEX from
# the output in the previous step if it was not 0. If you didn't
change anything
# else above, don't change anything else here.

SERVICE_ACCOUNT_NAME=astracontrol-service-account
NAMESPACE=default
NEW_CONTEXT=astracontrol
KUBECONFIG_FILE='kubeconfig-sa'
TOKEN_INDEX=0

CONTEXT=$(kubectl config current-context)

SECRET_NAME=$(kubectl get serviceaccount ${SERVICE_ACCOUNT_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.secrets[TOKEN_INDEX].name}')
TOKEN_DATA=$(kubectl get secret ${SECRET_NAME} \
  --context ${CONTEXT} \
  --namespace ${NAMESPACE} \
  -o jsonpath='{.data.token}')

TOKEN=$(echo ${TOKEN_DATA} | base64 -d)

# Create dedicated kubeconfig
# Create a full copy
kubectl config view --raw > ${KUBECONFIG_FILE}.full.tmp

# Switch working context to correct context
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp config use-context
${CONTEXT}

# Minify
kubectl --kubeconfig ${KUBECONFIG_FILE}.full.tmp \
```

```
  config view --flatten --minify > ${KUBECONFIG_FILE}.tmp

# Rename context
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  rename-context ${CONTEXT} ${NEW_CONTEXT}

# Create token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-credentials ${CONTEXT}-${NAMESPACE}-token-user \
  --token ${TOKEN}

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token-
user

# Set context to correct namespace
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --namespace ${NAMESPACE}

# Flatten/minify kubeconfig
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  view --flatten --minify > ${KUBECONFIG_FILE}

# Remove tmp
rm ${KUBECONFIG_FILE}.full.tmp
rm ${KUBECONFIG_FILE}.tmp
```

b. Origen de los comandos para aplicarlos al clúster de Kubernetes.

```
source create-kubeconfig.sh
```

5. (**opcional**) cambie el nombre de la kubeconfig por un nombre significativo para el clúster. Proteja las credenciales del clúster.

```
chmod 700 create-kubeconfig.sh
mv kubeconfig-sa.txt YOUR_CLUSTER_NAME_kubeconfig
```

El futuro

Ahora que ha comprobado que se cumplen los requisitos previos, está listo "añadir un clúster".

Obtenga más información

- "Documentación de Trident"

- "Utilice la API Astra"

Agregue un certificado TLS personalizado

Puede quitar el certificado TLS autofirmado existente y reemplazarlo con un certificado TLS firmado por una entidad de certificación (CA).

Lo que necesitará

- Clúster Kubernetes con Astra Control Center instalado
- Acceso administrativo a un shell de comandos en el clúster para ejecutar `kubectl` comandos
- Archivos de claves privadas y certificados de la CA

Quite el certificado autofirmado

1. Con SSH, inicie sesión en el clúster Kubernetes que aloja Astra Control Center como usuario administrativo.
2. Busque el secreto TLS asociado con el certificado actual mediante el comando siguiente, reemplazo `<ACC-deployment-namespace>` Con el espacio de nombres de puesta en marcha de Astra Control Center:

```
kubectl get certificate -n <ACC-deployment-namespace>
```

3. Elimine el secreto y certificado instalados actualmente con los comandos siguientes:

```
kubectl delete cert cert-manager-certificates -n <ACC-deployment-
namespace>
kubectl delete secret secure-testing-cert -n <ACC-deployment-namespace>
```

Añadir un nuevo certificado

1. Utilice el siguiente comando para crear el nuevo secreto TLS con la clave privada y los archivos de certificado de la CA, reemplazando los argumentos entre paréntesis <> con la información adecuada:

```
kubectl create secret tls <secret-name> --key <private-key-filename>
--cert <certificate-filename> -n <ACC-deployment-namespace>
```

2. Utilice el siguiente comando y el ejemplo para editar el archivo de definición de recursos personalizados (CRD) del clúster y cambiar el `spec.selfSigned` valor a. `spec.ca.secretName` Para hacer referencia al secreto TLS que ha creado anteriormente:

```
kubectl edit clusterissuers.cert-manager.io/cert-manager-certificates -n
<ACC-deployment-namespace>
....

#spec:
#  selfSigned: {}

spec:
  ca:
    secretName: <secret-name>
```

3. Utilice el siguiente comando y el resultado de ejemplo para validar que los cambios son correctos y que el clúster está listo para validar certificados, sustituir `<ACC-deployment-namespace>` Con el espacio de nombres de puesta en marcha de Astra Control Center:

```
kubectl describe clusterissuers.cert-manager.io/cert-manager-
certificates -n <ACC-deployment-namespace>
....

Status:
  Conditions:
    Last Transition Time:  2021-07-01T23:50:27Z
    Message:               Signing CA verified
    Reason:                KeyPairVerified
    Status:                True
    Type:                  Ready
Events:                    <none>
```

4. Cree el `certificate.yaml` archivo utilizando el ejemplo siguiente, reemplazando los valores de marcador de posición entre corchetes <> con la información apropiada:

```
apiVersion: cert-manager.io/v1
kind: Certificate
metadata:
  name: <certificate-name>
  namespace: <ACC-deployment-namespace>
spec:
  secretName: <certificate-secret-name>
  duration: 2160h # 90d
  renewBefore: 360h # 15d
  dnsNames:
  - <astra.dnsname.example.com> #Replace with the correct Astra Control
Center DNS address
  issuerRef:
    kind: ClusterIssuer
    name: cert-manager-certificates
```

5. Cree el certificado con el comando siguiente:

```
kubectl apply -f certificate.yaml
```

6. Con el siguiente comando y el resultado de ejemplo, valide que el certificado se ha creado correctamente y con los argumentos especificados durante la creación (como nombre, duración, plazo de renovación y nombres DNS).

```
kubectl describe certificate -n <ACC-deployment-namespace>
....

Spec:
  Dns Names:
    astra.example.com
  Duration:  125h0m0s
  Issuer Ref:
    Kind:        ClusterIssuer
    Name:        cert-manager-certificates
  Renew Before:  61h0m0s
  Secret Name:   <certificate-secret-name>
Status:
  Conditions:
    Last Transition Time:  2021-07-02T00:45:41Z
    Message:               Certificate is up to date and has not expired
    Reason:                Ready
    Status:                True
    Type:                  Ready
  Not After:               2021-07-07T05:45:41Z
  Not Before:              2021-07-02T00:45:41Z
  Renewal Time:            2021-07-04T16:45:41Z
  Revision:                1
Events:                    <none>
```

7. Edite la opción Ingress CRD TLS para que apunte al nuevo secreto de certificado utilizando el siguiente comando y ejemplo, reemplazando los valores de marcador de posición entre paréntesis <> con la información adecuada:

```
kubectl edit ingressroutes.traefik.containo.us -n <ACC-deployment-
namespace>
....

# tls:
#    options:
#      name: default
#    secretName: secure-testing-cert
#    store:
#      name: default

 tls:
    options:
      name: default
    secretName: <certificate-secret-name>
    store:
      name: default
```

8. Con un explorador web, vaya a la dirección IP de implementación de Astra Control Center.
9. Compruebe que los detalles del certificado coinciden con los detalles del certificado que ha instalado.
10. Exporte el certificado e importe el resultado en el administrador de certificados en su navegador web.

Preguntas frecuentes para Astra Control Center

Estas preguntas frecuentes pueden ser de ayuda si solo está buscando una respuesta rápida a una pregunta.

Descripción general

En las siguientes secciones se ofrecen respuestas a algunas preguntas adicionales que puede encontrar a medida que utiliza Astra Control Center. Para obtener más aclaraciones, por favor, diríjase a astra.feedback@netapp.com

Acceso a Astra Control Center

- ¿Cuál es la URL de Astra Control?*

Astra Control Center utiliza autenticación local y una dirección URL específica para cada entorno.

Para la dirección URL, en un explorador, introduzca el nombre de dominio completo (FQDN) establecido en el campo spec.astraAddress del archivo astra_control_Center_min.yaml custom resource definition (CRD) cuando instaló Astra Control Center. El mensaje de correo electrónico es el valor que se ha establecido en el campo SPEC.Email del astra_control_Center_min.ylma CRD.

Estoy utilizando la licencia de Evaluación. ¿Cómo puedo cambiar a la licencia completa?

Si desea cambiar fácilmente a una licencia completa, obtenga el archivo de licencia de NetApp (NLF).

- Pasos*

- En la navegación de la izquierda, seleccione **cuenta** > **Licencia**.
- Seleccione **Agregar licencia**.
- Busque el archivo de licencia que ha descargado y seleccione **Agregar**.

Estoy utilizando la licencia de Evaluación. ¿Puedo seguir gestionando aplicaciones?

Sí, puede comprobar la funcionalidad de administración de aplicaciones con la licencia de evaluación.

Registrar clústeres de Kubernetes

Necesito añadir nodos de trabajo a mi clúster Kubernetes después de añadir a Astra Control. ¿Qué debo hacer?

Los nodos de trabajo nuevos se pueden agregar a los pools existentes. Estos serán descubiertos automáticamente por Astra Control. Si los nuevos nodos no están visibles en Astra Control, compruebe si los nuevos nodos de trabajo están ejecutando el tipo de imagen admitido. También puede verificar el estado de los nuevos nodos de trabajo mediante el `kubectl get nodes` comando.

¿Cómo descontrolo correctamente un clúster?

1. "Desgestione las aplicaciones desde Astra Control".
2. "Desgestione el clúster desde Astra Control".

¿Qué ocurre con mis aplicaciones y datos después de eliminar el clúster Kubernetes de Astra Control?

La eliminación de un clúster de Astra Control no realizará ningún cambio en la configuración del clúster (aplicaciones y almacenamiento persistente). Las instantáneas de Astra Control o las copias de seguridad tomadas de las aplicaciones en ese clúster no estarán disponibles para restaurar. Los backups de almacenamiento persistentes creados por Astra Control permanecen en Astra Control, pero no están disponibles para la restauración.

> Quite siempre un clúster de Astra Control antes de eliminarlo mediante cualquier otro método. La eliminación de un clúster con otra herramienta mientras Astra Control sigue gestionando puede causar problemas para su cuenta Astra Control.

¿Se desinstala NetApp Trident cuando extrizo un clúster de Kubernetes de Astra Control?

Trident no se desinstala de un clúster cuando lo elimina de Astra Control.

Gestionar aplicaciones

- ¿Puede Astra Control implementar una aplicación?*

Astra Control no implementa aplicaciones. Las aplicaciones deben implementarse fuera de Astra Control.

¿Qué sucede con las aplicaciones después de dejar de administrarlas desde Astra Control?

Se eliminarán todos los backups o las snapshots existentes. Las aplicaciones y los datos siguen estando disponibles. Las operaciones de administración de datos no estarán disponibles para aplicaciones no administradas o para cualquier copia de seguridad o copia Snapshot que pertenezcan a él.

¿Puede Astra Control gestionar una aplicación que utiliza un almacenamiento que no sea de NetApp?

No Aunque Astra Control puede detectar aplicaciones que utilizan almacenamiento de terceros, no puede gestionar una aplicación que utilice almacenamiento de terceros.

¿Debo administrar Astra Control mismo? no, no debería gestionar Astra Control por sí mismo porque es una "app del sistema".

Operaciones de gestión de datos

- hay instantáneas en mi cuenta que no creé. ¿de dónde vienen?*

En algunas situaciones, Astra Control creará automáticamente una instantánea como parte de un proceso de backup, clonado o restauración.

Mi aplicación utiliza varios VP. ¿Tomará Astra Control instantáneas y copias de seguridad de todas estas EVs?

Sí. Una operación de instantánea en una aplicación de Astra Control incluye una instantánea de todos los VP vinculados a las RVP de la aplicación.

¿Puedo gestionar las instantáneas tomadas por Astra Control directamente a través de una interfaz o almacenamiento de objetos diferente?

No Las copias Snapshot y las copias de seguridad realizadas por Astra Control solo se pueden gestionar con Astra Control.