



Installieren Sie Astra Control Center

Astra Control Center

NetApp
May 20, 2024

Inhalt

Installieren Sie das Astra Control Center mithilfe des Standardprozesses	1
Laden Sie das Astra Control Center herunter und extrahieren Sie es	3
Führen Sie zusätzliche Schritte durch, wenn Sie eine lokale Registrierung verwenden	4
Einrichten von Namespace und Geheimdienstraum für Registrys mit auth Anforderungen	8
Installieren Sie den Operator Astra Control Center	9
Konfigurieren Sie Astra Control Center	12
Komplette Astra Control Center und Bedienerinstallation	26
Überprüfen Sie den Systemstatus	27
Eindringen für den Lastenausgleich einrichten	34
Melden Sie sich in der UI des Astra Control Center an	38
Beheben Sie die Fehlerbehebung für die Installation	38
Alternative Installationsverfahren	39
Wie es weiter geht	39
Konfigurieren Sie einen externen Zertifikaten-Manager	39

Installieren Sie das Astra Control Center mithilfe des Standardprozesses

Um Astra Control Center zu installieren, laden Sie die Installationsabbilder herunter und führen Sie die folgenden Schritte aus. Mit diesem Verfahren können Sie Astra Control Center in Internet-angeschlossenen oder luftgekapselten Umgebungen installieren.

Eine Demonstration des Installationsvorgangs für Astra Control Center finden Sie unter "[Dieses Video](#)".

Bevor Sie beginnen

- **Umweltvoraussetzungen erfüllen:** "[Bevor Sie mit der Installation beginnen, bereiten Sie Ihre Umgebung auf die Implementierung des Astra Control Center vor](#)".



Astra Control Center kann in einer dritten Fehlerdomäne oder an einem sekundären Standort implementiert werden. Dies wird für Applikationsreplizierung und nahtlose Disaster Recovery empfohlen.

- **Gesunde Dienste sicherstellen:** Überprüfen Sie, ob alle API-Dienste in einem gesunden Zustand sind und verfügbar sind:

```
kubectl get apiservices
```

- **Stellen Sie einen routingfähigen FQDN sicher:** Der Astra FQDN, den Sie verwenden möchten, kann zum Cluster weitergeleitet werden. Das bedeutet, dass Sie entweder einen DNS-Eintrag in Ihrem internen DNS-Server haben oder eine bereits registrierte Core URL-Route verwenden.
- **Configure cert Manager:** Wenn ein cert Manager bereits im Cluster existiert, müssen Sie einige durchführen "[Erforderliche Schritte](#)" Damit Astra Control Center nicht versucht, seinen eigenen Cert Manager zu installieren. Standardmäßig installiert Astra Control Center während der Installation einen eigenen Cert-Manager.
- **(nur ONTAP-SAN-Treiber) Aktivieren Sie Multipath:** Wenn Sie einen ONTAP-SAN-Treiber verwenden, stellen Sie sicher, dass Multipath auf allen Kubernetes-Clustern aktiviert ist.

Sie sollten auch Folgendes berücksichtigen:

- **Zugriff auf die NetApp Astra Control Image Registry:**

Sie haben die Möglichkeit, Installations-Images und Funktionserweiterungen für Astra Control, wie z. B. Astra Control Provisioner, aus der NetApp-Image-Registrierung zu beziehen.

- a. Notieren Sie Ihre Astra Control Account-ID, die Sie zur Anmeldung in der Registrierung benötigen.

Ihre Konto-ID wird in der Web-UI des Astra Control Service angezeigt. Wählen Sie das Symbol oben rechts auf der Seite aus, wählen Sie **API Access** aus und notieren Sie sich Ihre Konto-ID.

- b. Wählen Sie auf derselben Seite **API-Token generieren** aus und kopieren Sie die API-Token-Zeichenfolge in die Zwischenablage und speichern Sie sie in Ihrem Editor.

- c. Melden Sie sich in der Astra Control Registry an:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

- **Installieren Sie ein Service-Mesh für sichere Kommunikation:** Es wird dringend empfohlen, die Kommunikationskanäle des Host-Clusters Astra Control mit einem zu sichern "[Unterstütztes Service-Mesh](#)".



Die Integration von Astra Control Center mit einem Service-Mesh ist nur während des Astra Control Center möglich "[Installation](#)" Und nicht unabhängig von diesem Prozess. Ein Wechsel von einer vernetzten in eine nicht vernetzte Umgebung wird nicht unterstützt.

Für die Nutzung von Istio Service Mesh müssen Sie Folgendes tun:

- Fügen Sie ein hinzu `istio-injection:enabled` [Etikett](#) In den Astra Namespace vor der Implementierung von Astra Control Center.
- Verwenden Sie die `Generic` [Einstellung für Eindringen](#) Und bieten eine alternative Ingress für [Externe Lastverteilung](#).
- Für Red hat OpenShift-Cluster müssen Sie definieren `NetworkAttachmentDefinition` In allen zugehörigen Astra Control Center-Namespace (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` Für Anwendungscluster oder alle benutzerdefinierten Namespaces, die ersetzt wurden).

```
cat <<EOF | oc -n netapp-acc-operator create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

```
cat <<EOF | oc -n netapp-acc create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

```
cat <<EOF | oc -n netapp-monitoring create -f -
apiVersion: "k8s.cni.cncf.io/v1"
kind: NetworkAttachmentDefinition
metadata:
  name: istio-cni
EOF
```

Schritte

Gehen Sie wie folgt vor, um Astra Control Center zu installieren:

- [Laden Sie das Astra Control Center herunter und extrahieren Sie es](#)

- wenn Sie eine lokale Registrierung verwenden
- Einrichten von Namespace und Geheimdienstraum für Registrys mit auth Anforderungen
- Installieren Sie den Operator Astra Control Center
- Konfigurieren Sie Astra Control Center
- Komplette Astra Control Center und Bedienerinstallation
- Überprüfen Sie den Systemstatus
- Eindringen für den Lastenausgleich einrichten
- Melden Sie sich in der UI des Astra Control Center an



Löschen Sie den Operator Astra Control Center nicht (z. B. `kubectl delete -f astra_control_center_operator_deploy.yaml`) Zu jeder Zeit während der Astra Control Center Installation oder Betrieb, um das Löschen von Pods zu vermeiden.

Laden Sie das Astra Control Center herunter und extrahieren Sie es

Laden Sie die Bilder des Astra Control Center von einem der folgenden Standorte herunter:

- **Astra Control Service Image Registry:** Verwenden Sie diese Option, wenn Sie keine lokale Registrierung mit den Astra Control Center Images verwenden oder wenn Sie diese Methode dem Bundle-Download von der NetApp Support-Website vorziehen.
- **NetApp Support-Seite:** Verwenden Sie diese Option, wenn Sie eine lokale Registrierung mit den Astra Control Center-Images verwenden.

Astra Control-Image-Registrierung

1. Melden Sie sich beim Astra Control Service an.
2. Wählen Sie im Dashboard **Deploy a self-Managed Instance of Astra Control** aus.
3. Folgen Sie den Anweisungen, um sich bei der Astra Control-Image-Registrierung anzumelden, das Astra Control Center-Installationsabbild zu ziehen und das Image zu extrahieren.

NetApp Support Website

1. Laden Sie das Bundle mit Astra Control Center herunter (`astra-control-center-[version].tar.gz`) Vom "[Download-Seite für Astra Control Center](#)".
2. (Empfohlen, aber optional) Laden Sie das Zertifikaten- und Unterschriftenpaket für Astra Control Center herunter (`astra-control-center-certs-[version].tar.gz`) Um die Signatur des Bündels zu überprüfen.

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

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

Die Ausgabe wird angezeigt `Verified OK` Nach erfolgreicher Überprüfung.

3. Extrahieren Sie die Bilder aus dem Astra Control Center Bundle:

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

Führen Sie zusätzliche Schritte durch, wenn Sie eine lokale Registrierung verwenden

Wenn Sie planen, das Astra Control Center Bundle in Ihre lokale Registry zu schieben, müssen Sie das NetApp Astra `kubectrl` Kommandozeilen-Plugin verwenden.

Installieren Sie das NetApp Astra `kubectrl` Plug-in

Führen Sie diese Schritte aus, um das neueste NetApp Astra `kubectrl` Kommandozeilen-Plugin zu installieren.

Bevor Sie beginnen

NetApp bietet Plug-ins-Binärdateien für verschiedene CPU-Architekturen und Betriebssysteme. Sie müssen wissen, welche CPU und welches Betriebssystem Sie haben, bevor Sie diese Aufgabe ausführen.

Wenn Sie das Plugin bereits von einer früheren Installation installiert haben, "[Stellen Sie sicher, dass Sie über die neueste Version verfügen](#)" Bevor Sie diese Schritte ausführen.

Schritte

1. Listen Sie die verfügbaren NetApp Astra kubectl Plugin-Binärdateien auf:



Die kubectl Plugin-Bibliothek ist Teil des tar-Bündels und wird in den Ordner extrahiert `kubectl-astra`.

```
ls kubectl-astra/
```

2. Verschieben Sie die für Ihr Betriebssystem und die CPU-Architektur benötigte Datei in den aktuellen Pfad und benennen Sie sie in um `kubectl-astra`:

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

Fügen Sie die Bilder zu Ihrer Registrierung hinzu

1. Wenn Sie planen, das Astra Control Center-Paket in Ihre lokale Registrierung zu übertragen, führen Sie die entsprechende Schrittfolge für Ihre Container-Engine aus:

Docker

- a. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten den sehen `acc.manifest.bundle.yaml` Datei und diese Verzeichnisse:

```
acc/  
kubect1-astra/  
acc.manifest.bundle.yaml
```

- b. Übertragen Sie die Paketbilder im Astra Control Center-Bildverzeichnis in Ihre lokale Registrierung. Führen Sie die folgenden Ersetzungen durch, bevor Sie den ausführen `push-images` Befehl:

- Ersetzen Sie `<BUNDLE_FILE>` durch den Namen der Astra Control Bundle-Datei (`acc.manifest.bundle.yaml`).
- Ersetzen Sie `<MY_FULL_REGISTRY_PATH>` durch die URL des Docker Repositorys ersetzen, beispielsweise "`<a href="https://<docker-registry>"; class="bare">https://<docker-registry>;`".
- Ersetzen Sie `<MY_REGISTRY_USER>` durch den Benutzernamen.
- Ersetzen Sie `<MY_REGISTRY_TOKEN>` durch ein autorisiertes Token für die Registrierung.

```
kubect1 astra packages push-images -m <BUNDLE_FILE> -r  
<MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p  
<MY_REGISTRY_TOKEN>
```

Podman

- a. Wechseln Sie in das Stammverzeichnis des Tarballs. Sie sollten diese Datei und das Verzeichnis sehen:

```
acc/  
kubect1-astra/  
acc.manifest.bundle.yaml
```

- b. Melden Sie sich bei Ihrer Registrierung an:

```
podman login <YOUR_REGISTRY>
```

- c. Vorbereiten und Ausführen eines der folgenden Skripts, das für die von Ihnen verwendete Podman-Version angepasst ist. Ersetzen Sie `<MY_FULL_REGISTRY_PATH>` durch die URL Ihres Repositorys, die alle Unterverzeichnisse enthält.

```
<strong>Podman 4</strong>
```



```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::~')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done

```

Podman 3

```

export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=24.02.0-69
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed
's/Loaded image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::~')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done

```



Der Bildpfad, den das Skript erstellt, sollte abhängig von Ihrer Registrierungskonfiguration wie folgt aussehen:

```

https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/24.02.0-69/image:version

```

2. Telefonbuch ändern:

```

cd manifests

```

Einrichten von Namespace und Geheimdienstraum für Registrys mit auth Anforderungen

1. Exportieren Sie den kubeconfig für den Host-Cluster Astra Control Center:

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



Bevor Sie die Installation abschließen, vergewissern Sie sich, dass Ihr kubeconfig auf den Cluster zeigt, in dem Sie Astra Control Center installieren möchten.

2. Wenn Sie eine Registrierung verwenden, für die eine Authentifizierung erforderlich ist, müssen Sie Folgendes tun:

- a. Erstellen Sie die `netapp-acc-operator` Namespace:

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

- b. Erstellen Sie ein Geheimnis für das `netapp-acc-operator` Namespace. Fügen Sie Docker-Informationen hinzu und führen Sie den folgenden Befehl aus:



Platzhalter `your_registry_path` Sollte die Position der Bilder, die Sie früher hochgeladen haben, entsprechen (z. B. `[Registry_URL]/netapp/astra/astracc/24.02.0-69`).

```
kubectl create secret docker-registry astra-registry-cred -n netapp-acc-operator --docker-server=cr.astra.netapp.io --docker-username=[astra_account_id] --docker-password=[astra_api_token]
```

+

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

+



Wenn Sie den Namespace löschen, nachdem das Geheimnis generiert wurde, erstellen Sie den Namespace neu und generieren Sie dann das Geheimnis für den Namespace neu.

- a. Erstellen Sie die `netapp-acc` (Oder Name des benutzerdefinierten Namespace).

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

- b. Erstellen Sie ein Geheimnis für das `netapp-acc` (Oder Name des benutzerdefinierten Namespace). Fügen Sie Docker-Informationen hinzu, und führen Sie je nach Registrierungseinstellung einen der entsprechenden Befehle aus:

```
kubectl create secret docker-registry astra-registry-cred -n [netapp-acc or custom namespace] --docker-server=cr.astra.netapp.io --docker-username=[astra_account_id] --docker-password=[astra_api_token]
```

```
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]
```

Installieren Sie den Operator Astra Control Center

1. (Nur lokale Registrierungsstellen) Wenn Sie eine lokale Registrierung verwenden, führen Sie die folgenden Schritte aus:

- a. Astra Control Center Operator Deployment YAML öffnen:

```
vim astra_control_center_operator_deploy.yaml
```



Ein YAML-Beispiel mit Anmerkungen folgt diesen Schritten.

- b. Wenn Sie eine Registrierung verwenden, für die eine Authentifizierung erforderlich ist, ersetzen Sie die Standardzeile von `imagePullSecrets: []` Mit folgenden Optionen:

```
imagePullSecrets: [{name: astra-registry-cred}]
```

- c. Ändern `ASTRA_IMAGE_REGISTRY` Für das `kube-rbac-proxy` Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben [Vorheriger Schritt](#).
- d. Ändern `ASTRA_IMAGE_REGISTRY` Für das `acc-operator-controller-manager` Bild zum Registrierungspfad, in dem Sie die Bilder in ein geschoben haben [Vorheriger Schritt](#).

```
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
strategy:
  type: Recreate
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: ASTRA_IMAGE_REGISTRY/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
        env:
          - name: ACCOP_LOG_LEVEL
            value: "2"
          - name: ACCOP_HELM_INSTALLTIMEOUT
            value: 5m
          image: ASTRA_IMAGE_REGISTRY/acc-operator:24.02.68
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
            port: 8081
            initialDelaySeconds: 15
            periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
            initialDelaySeconds: 5
            periodSeconds: 10
        resources:

```

```
    limits:
      cpu: 300m
      memory: 750Mi
    requests:
      cpu: 100m
      memory: 75Mi
    securityContext:
      allowPrivilegeEscalation: false
  imagePullSecrets: []
  securityContext:
    runAsUser: 65532
  terminationGracePeriodSeconds: 10
```

2. Installieren Sie den Astra Control Center-Operator:

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

Erweitern für Probenantwort:

```
namespace/netapp-acc-operator created
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.as
tra.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
```

3. Überprüfen Sie, ob Pods ausgeführt werden:

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

Konfigurieren Sie Astra Control Center

1. Bearbeiten Sie die Datei Astra Control Center Custom Resource (CR) (`astra_control_center.yaml`) Zur Berücksichtigung, Unterstützung, Registrierung und anderen notwendigen Konfigurationen:

```
vim astra_control_center.yaml
```



Ein YAML-Beispiel mit Anmerkungen folgt diesen Schritten.

2. Ändern oder bestätigen Sie die folgenden Einstellungen:

AccountName

Einstellung	Anleitung	Typ	Beispiel
<code>accountName</code>	Ändern Sie das <code>accountName</code> Zeichenfolge an den Namen, den Sie dem Astra Control Center-Konto zuordnen möchten. Es kann nur ein <code>AccountName</code> geben.	Zeichenfolge	<code>Example</code>

AstraVersion

Einstellung	Anleitung	Typ	Beispiel
<code>astraVersion</code>	Die zu implementierende Version des Astra Control Center: Für diese Einstellung ist keine Aktion erforderlich, da der Wert bereits ausgefüllt wird.	Zeichenfolge	<code>24.02.0-69</code>

AstraAddress

Einstellung	Anleitung	Typ	Beispiel
astraAddress	<p>Ändern Sie das <code>astraAddress</code> Zeichenfolge an den FQDN (empfohlen) oder die IP-Adresse, die Sie in Ihrem Browser verwenden möchten, um auf Astra Control Center zuzugreifen. Diese Adresse legt fest, wie Astra Control Center in Ihrem Rechenzentrum zu finden ist und ist die gleiche FQDN- oder IP-Adresse, die Sie von Ihrem Load Balancer bereitgestellt haben, wenn Sie fertig sind "Anforderungen des Astra Control Centers".</p> <p>HINWEIS: Nicht verwenden <code>http://</code> Oder <code>https://</code> In der Adresse. Kopieren Sie diesen FQDN zur Verwendung in einem Später Schritt.</p>	Zeichenfolge	<code>astra.example.com</code>

AutoSupport

Durch Ihre Auswahl in diesem Abschnitt wird bestimmt, ob Sie an der proaktiven Support-Applikation von NetApp, NetApp Active IQ, teilnehmen und an welchen Orten Daten gesendet werden. Eine Internetverbindung ist erforderlich (Port 442), und alle Supportdaten werden anonymisiert.

Einstellung	Nutzung	Anleitung	Typ	Beispiel
<code>autoSupport.enrolled</code>	Entweder <code>enrolled</code> Oder <code>url</code> Felder müssen ausgewählt werden	Ändern <code>enrolled</code> Für AutoSupport bis <code>false</code> Für Websites ohne Internetverbindung oder Aufbewahrung <code>true</code> Für verbundene Standorte. Eine Einstellung von <code>true</code> Anonyme Daten können zu Supportzwecken an NetApp gesendet werden. Die Standardwahl ist <code>false</code> Und zeigt an, dass keine Support-Daten an NetApp gesendet werden.	Boolesch	<code>false</code> (Dieser Wert ist der Standardwert)
<code>autoSupport.url</code>	Entweder <code>enrolled</code> Oder <code>url</code> Felder müssen ausgewählt werden	Diese URL legt fest, wo die anonymen Daten gesendet werden.	Zeichenfolge	https://support.netapp.com/asupprod/post/1.0/postAsup

E-Mail

Einstellung	Anleitung	Typ	Beispiel
email	Ändern Sie das email Zeichenfolge zur standardmäßigen ursprünglichen Administratoradresse. Kopieren Sie diese E-Mail-Adresse zur Verwendung in A Später Schritt . Diese E-Mail-Adresse wird als Benutzername für das erste Konto verwendet, um sich bei der UI anzumelden und wird über Ereignisse in Astra Control informiert.	Zeichenfolge	admin@example.com

Vorname

Einstellung	Anleitung	Typ	Beispiel
firstName	Der erste Name des mit dem Astra-Konto verknüpften Standardadministrators. Der hier verwendete Name wird nach der ersten Anmeldung in einer Überschrift in der UI angezeigt.	Zeichenfolge	SRE

Nachname

Einstellung	Anleitung	Typ	Beispiel
lastName	Der Nachname des mit dem Astra-Konto verknüpften Standard-Initialadministrators. Der hier verwendete Name wird nach der ersten Anmeldung in einer Überschrift in der UI angezeigt.	Zeichenfolge	Admin

ImageRegistry

Ihre Auswahl in diesem Abschnitt definiert die Container-Image-Registry, die die Astra-Anwendungsabbilder, den Astra Control Center Operator und das Astra Control Center Helm Repository hostet.

Einstellung	Nutzung	Anleitung	Typ	Beispiel
imageRegistry.name	Erforderlich	Der Name der Astra Control-Image-Registrierung, die alle Images hostet, die für die Bereitstellung von Astra Control Center erforderlich sind. Der Wert wird vorausgefüllt, und es ist keine Aktion erforderlich, es sei denn, Sie haben eine lokale Registrierung konfiguriert. Ersetzen Sie bei einer lokalen Registrierung diesen vorhandenen Wert durch den Namen der Bildregistrierung, in die Sie die Bilder in der verschoben haben Vorheriger Schritt . Verwenden Sie es nicht <code>http://</code> Oder <code>https://</code> Im Registrierungsnamen.	Zeichenfolge	<code>cr.astra.netapp.io</code> (Standard) <code>example.registry.com/astra</code> (Beispiel für eine lokale Registrierung)

Einstellung	Nutzung	Anleitung	Typ	Beispiel
<pre>imageRegistry. secret</pre>	Optional	<p>Der Name des Kubernetes Secret, das zur Authentifizierung mit der Bildregistrierung verwendet wird. Der Wert wird vorausgefüllt, und es ist keine Aktion erforderlich, es sei denn, Sie haben eine lokale Registrierung und den String konfiguriert, den Sie für diese Registrierung in eingegeben haben <code>imageRegistry.name</code> Erfordert ein Geheimnis.</p> <p>WICHTIG: Wenn Sie eine lokale Registrierung verwenden, die keine Autorisierung erfordert, müssen Sie diese löschen <code>secret</code> Zeile in <code>imageRegistry</code> Oder die Installation schlägt fehl.</p>	Zeichenfolge	<pre>astra- registry-cred</pre>

Storage Class

Einstellung	Anleitung	Typ	Beispiel
storageClass	<p>Ändern Sie das storageClass Wert von ontap-gold Auf eine andere Ressource von storageClass, wie von Ihrer Installation gefordert. Führen Sie den Befehl aus</p> <pre>kubectl get sc</pre> <p>So ermitteln Sie Ihre vorhandenen konfigurierten Speicherklassen. In die Manifestdatei muss eine für die Astra Control Provisioner konfigurierte Storage-Klasse eingegeben werden (astra-control-center-<version>.manifest) Und wird für Astra PVS verwendet. Wenn er nicht festgelegt ist, wird die Standard-Speicherklasse verwendet.</p> <p>HINWEIS: Wenn eine Standard-Storage-Klasse konfiguriert ist, stellen Sie sicher, dass diese die einzige Storage-Klasse mit der Standardbeschriftung ist.</p>	Zeichenfolge	ontap-gold

VolumeReclaimPolicy

Einstellung	Anleitung	Typ	Optionen
volumeReclaimPolicy	Damit wird die Rückgewinnungsrichtlinie für die PVS von Astra festgelegt. Festlegen dieser Richtlinie auf <code>Retain</code> Behält persistente Volumes nach dem Löschen von Astra bei. Festlegen dieser Richtlinie auf <code>Delete</code> Löscht persistente Volumes nach dem Löschen von astra. Wenn dieser Wert nicht festgelegt ist, werden die PVS beibehalten.	Zeichenfolge	<ul style="list-style-type: none">• <code>Retain</code> (Dies ist der Standardwert)• <code>Delete</code>

Typ

A large, empty rectangular box with a thin, dashed border, occupying most of the page. It is intended for a drawing or diagram.



Einstellung	Anleitung	Typ	Optionen
ingressType	<p>Verwenden Sie einen der folgenden Eingangstypen:</p> <p>Allgemein (ingressType: "Generic") (Standard) Verwenden Sie diese Option, wenn Sie einen anderen Ingress-Controller verwenden oder Ihren eigenen Ingress-Controller verwenden möchten. Nachdem Astra Control Center bereitgestellt ist, müssen Sie das konfigurieren "Eingangs-Controller" Um Astra Control Center mit einer URL zu zeigen.</p> <p>WICHTIG: Wenn Sie ein Service-Mesh mit Astra Control Center verwenden möchten, müssen Sie auswählen <code>Generic</code> Als Eindringen Typ und richten Sie Ihre eigenen "Eingangs-Controller".</p> <p>AccTraefik (ingressType: "AccTraefik") Verwenden Sie diese Option, wenn Sie keinen Ingress-Controller konfigurieren möchten. Dies implementiert das Astra Control Center <code>traefik</code> Gateway als Service des Typs <code>Kubernetes Load Balancer</code>:</p> <p>Astra Control Center nutzt einen Service vom Typ „loadbalancer“ (svc/traefik Im Astra Control Center</p>	Zeichenfolge	<ul style="list-style-type: none"> • <code>Generic</code> (Dies ist der Standardwert) • <code>AccTraefik</code>

Skalengröße

Einstellung	Anleitung	Typ	Optionen
scaleSize	<p>Astra verwendet standardmäßig High Availability (HA). scaleSize Von Medium, Die die meisten Dienste in HA bereitstellt und mehrere Replikate für Redundanz bereitstellt. Mit scaleSize Als Small, Astra wird die Anzahl der Replikate für alle Dienste reduzieren, außer für wesentliche Dienste, um den Verbrauch zu reduzieren. TIPP: Medium Implementierungen bestehen aus etwa 100 Pods (einschließlich transienter Workloads). 100 Pods basieren auf drei Master Nodes und einer Konfiguration mit drei Worker Nodes). Beachten Sie die Einschränkungen bei der Netzwerkgrenze pro Pod, die in Ihrer Umgebung möglicherweise ein Problem darstellen, insbesondere bei der Betrachtung von Disaster-Recovery-Szenarien.</p>	Zeichenfolge	<ul style="list-style-type: none">• Small• Medium (Dies ist der Standardwert)

AstraResourcesScaler

Einstellung	Anleitung	Typ	Optionen
<code>astraResourcesScaler</code>	<p>Skalierungsoptionen für die Ressourcengrenzen von AstraControlCenter. Astra Control Center implementiert standardmäßig mit Ressourcenanfragen, die für die meisten Komponenten in Astra bereitgestellt werden. Mit dieser Konfiguration verbessert sich die Leistung des Astra Control Center Software-Stacks auch bei erhöhter Applikationslast und -Skalierung. In Szenarien mit kleineren Entwicklungs- oder Testclustern jedoch das CR-Feld <code>astraResourcesScaler</code> Kann auf festgelegt werden <code>Off</code>. Dadurch werden Ressourcenanforderungen deaktiviert und die Bereitstellung auf kleineren Clustern ist möglich.</p>	Zeichenfolge	<ul style="list-style-type: none">• Default (Dies ist der Standardwert)• Off

Zusätzliche Werte



Fügen Sie dem Astra Control Center CR die folgenden zusätzlichen Werte hinzu, um ein bekanntes Problem bei der Installation zu vermeiden:

```
additionalValues:  
  keycloak-operator:  
    livenessProbe:  
      initialDelaySeconds: 180  
    readinessProbe:  
      initialDelaySeconds: 180
```

crds

Ihre Auswahl in diesem Abschnitt legt fest, wie Astra Control Center mit CRDs umgehen soll.

Einstellung	Anleitung	Typ	Beispiel
<code>crds.externalCertManager</code>	Wenn Sie einen externen Zertifikaten-Manager verwenden, ändern Sie <code>externalCertManager</code> Bis <code>true</code> . Der Standardwert <code>false</code> Führt dazu, dass Astra Control Center während der Installation seine eigenen CRT-Manager-CRDs installiert. CRDs sind Cluster-weite Objekte, die sich auf andere Teile des Clusters auswirken können. Mit diesem Flag können Sie dem Astra Control Center signalisieren, dass diese CRDs vom Clusteradministrator außerhalb des Astra Control Center installiert und verwaltet werden.	Boolesch	<code>False</code> (Dieser Wert ist der Standardwert)
<code>crds.externalTraffic</code>	Astra Control Center installiert standardmäßig die erforderlichen Trafik-CRDs. CRDs sind Cluster-weite Objekte, die sich auf andere Teile des Clusters auswirken können. Mit diesem Flag können Sie dem Astra Control Center signalisieren, dass diese CRDs vom Clusteradministrator außerhalb des Astra Control Center installiert und verwaltet werden.	Boolesch	<code>False</code> (Dieser Wert ist der Standardwert)



Stellen Sie sicher, dass Sie die richtige Storage-Klasse und den richtigen Ingress-Typ für Ihre Konfiguration ausgewählt haben, bevor Sie die Installation abschließen.

Beispiel für `astra_control_center.yaml`

```
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: "[cr.astra.netapp.io or your_registry_path]"
    secret: "astra-registry-cred"
  storageClass: "ontap-gold"
  volumeReclaimPolicy: "Retain"
  ingressType: "Generic"
  scaleSize: "Medium"
  astraResourcesScaler: "Default"
  additionalValues:
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
  crds:
    externalTraefik: false
    externalCertManager: false
```

Komplette Astra Control Center und Bedienerinstallation

1. Wenn Sie dies in einem vorherigen Schritt nicht bereits getan haben, erstellen Sie das `netapp-acc` (Oder benutzerdefinierter) Namespace:

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

2. Wenn Sie ein Service-Mesh mit Astra Control Center verwenden, fügen Sie dem die folgende Beschriftung hinzu `netapp-acc` Oder benutzerdefinierter Namespace:



Ihre Art des Eingangs (`ingressType`) Muss auf `generic` gesetzt werden Im Astra Control Center CR, bevor Sie mit diesem Befehl fortfahren.

```
kubectl label ns [netapp-acc or custom namespace] istio-  
injection:enabled
```

3. (Empfohlen) "Aktivieren Sie strenge MTLs" Für Istio Service Mesh:

```
kubectl apply -n istio-system -f - <<EOF  
apiVersion: security.istio.io/v1beta1  
kind: PeerAuthentication  
metadata:  
  name: default  
spec:  
  mtls:  
    mode: STRICT  
EOF
```

4. Installieren Sie das Astra Control Center im netapp-acc (Oder Ihr individueller) Namespace:

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



Der Fahrer des Astra Control Center überprüft automatisch die Umgebungsanforderungen. Fehlt "Anforderungen" Kann dazu führen, dass Ihre Installation fehlschlägt oder Astra Control Center nicht ordnungsgemäß funktioniert. Siehe [Nächster Abschnitt](#) So prüfen Sie, ob Warnmeldungen zur automatischen Systemprüfung vorliegen.

Überprüfen Sie den Systemstatus

Sie können den Systemstatus mithilfe von kubectl-Befehlen überprüfen. Wenn Sie OpenShift verwenden möchten, können Sie vergleichbare oc-Befehle für Verifizierungsschritte verwenden.

Schritte

1. Vergewissern Sie sich, dass beim Installationsprozess keine Warnmeldungen zu den Validierungsprüfungen ausgegeben wurden:

```
kubectl get acc [astra or custom Astra Control Center CR name] -n  
[netapp-acc or custom namespace] -o yaml
```



Zusätzliche Warnmeldungen werden auch in den Bedienerprotokollen des Astra Control Centers gemeldet.

2. Beheben Sie alle Probleme mit Ihrer Umgebung, die durch automatisierte Anforderungsprüfungen gemeldet wurden.



Sie können Probleme beheben, indem Sie sicherstellen, dass Ihre Umgebung den erfüllt ["Anforderungen"](#) Für Astra Control Center.

3. Vergewissern Sie sich, dass alle Systemkomponenten erfolgreich installiert wurden.

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

Jeder Pod sollte einen Status von `Running` haben. Es kann mehrere Minuten dauern, bis die System-Pods implementiert sind.

Erweitern, um die Probenantwort zu erhalten

acc-helm-repo-5bd77c9ddd-8wxm2 1h	1/1	Running	0
activity-5bb474dc67-819ss 1h	1/1	Running	0
activity-5bb474dc67-qbrtq 1h	1/1	Running	0
api-token-authentication-6wbj2 1h	1/1	Running	0
api-token-authentication-9pgw6 1h	1/1	Running	0
api-token-authentication-tqf6d 1h	1/1	Running	0
asup-5495f44dbd-z4kft 1h	1/1	Running	0
authentication-6fdd899858-5x45s 1h	1/1	Running	0
bucket-service-84d47487d-n9xgp 1h	1/1	Running	0
bucket-service-84d47487d-t5jhm 1h	1/1	Running	0
cert-manager-5dcb7648c4-hbldc 1h	1/1	Running	0
cert-manager-5dcb7648c4-nr9qf 1h	1/1	Running	0
cert-manager-cainjector-59b666fb75-bk2tf 1h	1/1	Running	0
cert-manager-cainjector-59b666fb75-pfnck 1h	1/1	Running	0
cert-manager-webhook-c6f9b6796-ngz2x 1h	1/1	Running	0
cert-manager-webhook-c6f9b6796-rwtbn 1h	1/1	Running	0
certificates-5f5b7b4dd-52tnj 1h	1/1	Running	0
certificates-5f5b7b4dd-gtjbx 1h	1/1	Running	0
certificates-expiry-check-28477260-dz5vw 1h	0/1	Completed	0
cloud-extension-6f58cc579c-lzfmv 1h	1/1	Running	0
cloud-extension-6f58cc579c-zw2km 1h	1/1	Running	0
cluster-orchestrator-79dd5c8d95-qjg92 1h	1/1	Running	0

composite-compute-85dc84579c-nz82f 1h	1/1	Running	0
composite-compute-85dc84579c-wx2z2 1h	1/1	Running	0
composite-volume-bff6f4f76-789nj 1h	1/1	Running	0
composite-volume-bff6f4f76-kwnd4 1h	1/1	Running	0
credentials-79fd64f788-m7m8f 1h	1/1	Running	0
credentials-79fd64f788-qnc6c 1h	1/1	Running	0
entitlement-f69cdbc77-4p2kn 1h	1/1	Running	0
entitlement-f69cdbc77-hswm6 1h	1/1	Running	0
features-7b9585444c-7xd7m 1h	1/1	Running	0
features-7b9585444c-dcqwc 1h	1/1	Running	0
fluent-bit-ds-crq8m 1h	1/1	Running	0
fluent-bit-ds-gmgq8 1h	1/1	Running	0
fluent-bit-ds-gzr4f 1h	1/1	Running	0
fluent-bit-ds-j6sf6 1h	1/1	Running	0
fluent-bit-ds-v4t9f 1h	1/1	Running	0
fluent-bit-ds-x7j59 1h	1/1	Running	0
graphql-server-6cc684fb46-2x8lr 1h	1/1	Running	0
graphql-server-6cc684fb46-bshbd 1h	1/1	Running	0
hybridauth-84599f79fd-fjc7k 1h	1/1	Running	0
hybridauth-84599f79fd-s9pmn 1h	1/1	Running	0
identity-95df98cb5-dvlmz 1h	1/1	Running	0
identity-95df98cb5-krf59 1h	1/1	Running	0
influxdb2-0 1h	1/1	Running	0

keycloak-operator-6d4d688697-cfq8b	1/1	Running	0
1h			
krakend-5d5c8f4668-7bq8g	1/1	Running	0
1h			
krakend-5d5c8f4668-t8hbn	1/1	Running	0
1h			
license-689cdd4595-2gsc8	1/1	Running	0
1h			
license-689cdd4595-g6vwk	1/1	Running	0
1h			
login-ui-57bb599956-4fwgz	1/1	Running	0
1h			
login-ui-57bb599956-rhztb	1/1	Running	0
1h			
loki-0	1/1	Running	0
1h			
metrics-facade-846999bdd4-f7jdm	1/1	Running	0
1h			
metrics-facade-846999bdd4-lnsxl	1/1	Running	0
1h			
monitoring-operator-6c9d6c4b8c-ggkrl	2/2	Running	0
1h			
nats-0	1/1	Running	0
1h			
nats-1	1/1	Running	0
1h			
nats-2	1/1	Running	0
1h			
natssync-server-6df7d6cc68-9v2gd	1/1	Running	0
1h			
nautilus-64b7fbdd98-bsgwb	1/1	Running	0
1h			
nautilus-64b7fbdd98-djlhw	1/1	Running	0
1h			
openapi-864584bccc-75nlv	1/1	Running	0
1h			
openapi-864584bccc-zh6bx	1/1	Running	0
1h			
polaris-consul-consul-server-0	1/1	Running	0
1h			
polaris-consul-consul-server-1	1/1	Running	0
1h			
polaris-consul-consul-server-2	1/1	Running	0
1h			
polaris-keycloak-0	1/1	Running	2 (1h
ago) 1h			

polaris-keycloak-1 1h	1/1	Running	0
polaris-keycloak-db-0 1h	1/1	Running	0
polaris-keycloak-db-1 1h	1/1	Running	0
polaris-keycloak-db-2 1h	1/1	Running	0
polaris-mongodb-0 1h	1/1	Running	0
polaris-mongodb-1 1h	1/1	Running	0
polaris-mongodb-2 1h	1/1	Running	0
polaris-ui-66476dcf87-f6s8j 1h	1/1	Running	0
polaris-ui-66476dcf87-ztjk7 1h	1/1	Running	0
polaris-vault-0 1h	1/1	Running	0
polaris-vault-1 1h	1/1	Running	0
polaris-vault-2 1h	1/1	Running	0
public-metrics-bfc4fc964-x4m79 1h	1/1	Running	0
storage-backend-metrics-7dbb88d4bc-g78cj 1h	1/1	Running	0
storage-provider-5969b5df5-hjvcm 1h	1/1	Running	0
storage-provider-5969b5df5-r79ld 1h	1/1	Running	0
task-service-5fc9dc8d99-4q4f4 1h	1/1	Running	0
task-service-5fc9dc8d99-8l5zl 1h	1/1	Running	0
task-service-task-purge-28485735-fdzkd 12m	1/1	Running	0
telegraf-ds-2rgm4 1h	1/1	Running	0
telegraf-ds-4qp6r 1h	1/1	Running	0
telegraf-ds-77frs 1h	1/1	Running	0
telegraf-ds-bc725 1h	1/1	Running	0

telegraf-ds-cvmxf 1h	1/1	Running	0
telegraf-ds-tqzgj 1h	1/1	Running	0
telegraf-rs-5wtd8 1h	1/1	Running	0
telemetry-service-6747866474-5djnc 1h	1/1	Running	0
telemetry-service-6747866474-thb7r ago) 1h	1/1	Running	1 (1h)
tenancy-5669854fb6-gzdzf 1h	1/1	Running	0
tenancy-5669854fb6-xvsm2 1h	1/1	Running	0
traefik-8f55f7d5d-4lgfw 1h	1/1	Running	0
traefik-8f55f7d5d-j4wt6 1h	1/1	Running	0
traefik-8f55f7d5d-p6gcq 1h	1/1	Running	0
trident-svc-7cb5bb4685-54cnq 1h	1/1	Running	0
trident-svc-7cb5bb4685-b28xh 1h	1/1	Running	0
vault-controller-777b9bbf88-b5bqt 1h	1/1	Running	0
vault-controller-777b9bbf88-fdfd8 1h	1/1	Running	0

4. (Optional) Sehen Sie sich den an `acc-operator` Protokolle zur Überwachung des Fortschritts:

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



`accHost` Die Cluster-Registrierung ist einer der letzten Vorgänge, und bei Ausfall wird die Implementierung nicht fehlschlagen. Sollten in den Protokollen ein Fehler bei der Cluster-Registrierung angegeben sein, können Sie die Registrierung erneut über das versuchen ["Fügen Sie in der UI einen Cluster-Workflow hinzu"](#) Oder API.

5. Wenn alle Pods ausgeführt werden, überprüfen Sie, ob die Installation erfolgreich war (`READY` ist `True`) Und erhalten Sie das erste Setup-Passwort, das Sie verwenden, wenn Sie sich bei Astra Control Center anmelden:

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

Antwort:

NAME	UUID	VERSION	ADDRESS
READY			
astra	9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f	24.02.0-69	
10.111.111.111	True		



Den UUID-Wert kopieren. Das Passwort lautet ACC- Anschließend der UUID-Wert (ACC-[UUID] Oder in diesem Beispiel ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f).

Eindringen für den Lastenausgleich einrichten

Sie können einen Kubernetes Ingress-Controller einrichten, der den externen Zugriff auf Services managt. Diese Verfahren enthalten Setup-Beispiele für einen Ingress-Controller, wenn Sie die Standardeinstellung von verwenden `ingressType: "Generic"` In der Astra Control Center Custom Resource (`astra_control_center.yaml`). Sie müssen diesen Vorgang nicht verwenden, wenn Sie angegeben haben `ingressType: "AccTraefik"` In der Astra Control Center Custom Resource (`astra_control_center.yaml`).

Nachdem Astra Control Center implementiert ist, müssen Sie den Ingress-Controller so konfigurieren, dass für das Astra Control Center eine URL verfügbar gemacht wird.

Die Einstellungsschritte unterscheiden sich je nach Typ des Ingress-Controllers. Astra Control Center unterstützt viele Ingress-Controller-Typen. Diese Einrichtungsverfahren bieten Beispielschritte für einige gängige Typen von Ingress-Controllern.

Bevor Sie beginnen

- Erforderlich "[Eingangs-Controller](#)" Sollte bereits eingesetzt werden.
- Der "[Eingangsklasse](#)" Entsprechend der Eingangs-Steuerung sollte bereits erstellt werden.

Schritte für Istio Ingress

1. Konfigurieren Sie Istio Ingress.



Bei diesem Verfahren wird davon ausgegangen, dass Istio mithilfe des Konfigurationsprofils „Standard“ bereitgestellt wird.

2. Sammeln oder erstellen Sie die gewünschte Zertifikatdatei und die private Schlüsseldatei für das Ingress Gateway.

Sie können ein CA-signiertes oder selbstsigniertes Zertifikat verwenden. Der allgemeine Name muss die Astra-Adresse (FQDN) sein.

Beispielbefehl:

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

- Erstellen Sie ein Geheimnis `tls secret name` vom Typ `kubernetes.io/tls` für einen privaten TLS-Schlüssel und ein Zertifikat im `istio-system namespace` wie in TLS Secrets beschrieben.

Beispielbefehl:

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



Der Name des Geheimnisses sollte mit dem übereinstimmen `spec.tls.secretName` verfügbar in `istio-ingress.yaml` Datei:

- Bereitstellung einer Ingress-Ressource im `netapp-acc (Oder Custom-Name) Namespace` unter Verwendung des `v1-Ressourcentyps` für ein Schema (`istio-Ingress.yaml` wird in diesem Beispiel verwendet):

```

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: [netapp-acc or custom namespace]
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. Übernehmen Sie die Änderungen:

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

6. Überprüfen Sie den Status des Eingangs:

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

Antwort:

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

7. Astra Control Center-Installation abschließen.

Schritte für Nginx Ingress Controller

1. Erstellen Sie ein Geheimnis des Typs `kubernetes.io/tls` Für einen privaten TLS-Schlüssel und ein Zertifikat in `netapp-acc` (Oder Custom-Name) Namespace wie in beschrieben "[TLS-Geheimnisse](#)".
2. Bereitstellung einer Ingress-Ressource in `netapp-acc` (Oder Custom-Name) Namespace unter Verwendung des `v1`-Ressourcentyps für ein Schema (`nginx-Ingress.yaml` Wird in diesem Beispiel verwendet):

```
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
```

3. Übernehmen Sie die Änderungen:

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



NetApp empfiehlt die Installation des nginx Controllers als Bereitstellung statt als a daemonSet.

Schritte für OpenShift-Eingangs-Controller

1. Beschaffen Sie Ihr Zertifikat, und holen Sie sich die Schlüssel-, Zertifikat- und CA-Dateien für die OpenShift-Route bereit.
2. Erstellen Sie die OpenShift-Route:

```
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
```

Melden Sie sich in der UI des Astra Control Center an

Nach der Installation von Astra Control Center ändern Sie das Passwort für den Standardadministrator und melden sich beim Astra Control Center UI Dashboard an.

Schritte

1. Geben Sie in einem Browser den FQDN ein (einschließlich `https://` Präfix), die Sie in verwendet haben `astraAddress` in `astra_control_center.yaml` CR, wenn [Sie haben das Astra Control Center installiert](#).
2. Akzeptieren Sie die selbstsignierten Zertifikate, wenn Sie dazu aufgefordert werden.



Sie können nach der Anmeldung ein benutzerdefiniertes Zertifikat erstellen.

3. Geben Sie auf der Anmeldeseite des Astra Control Center den Wert ein, den Sie für verwendet haben `email` in `astra_control_center.yaml` CR, wenn [Sie haben das Astra Control Center installiert](#), Gefolgt von dem anfänglichen Setup-Passwort (`ACC-[UUID]`).



Wenn Sie dreimal ein falsches Passwort eingeben, wird das Administratorkonto 15 Minuten lang gesperrt.

4. Wählen Sie **Login**.
5. Ändern Sie das Passwort, wenn Sie dazu aufgefordert werden.



Wenn dies Ihre erste Anmeldung ist und Sie das Passwort vergessen haben und noch keine anderen administrativen Benutzerkonten erstellt wurden, kontaktieren Sie ["NetApp Support"](#) Für Unterstützung bei der Kennwortwiederherstellung.

6. (Optional) Entfernen Sie das vorhandene selbst signierte TLS-Zertifikat und ersetzen Sie es durch ein ["Benutzerdefiniertes TLS-Zertifikat, signiert von einer Zertifizierungsstelle \(CA\)"](#).

Beheben Sie die Fehlerbehebung für die Installation

Wenn einer der Dienstleistungen in ist `ERROR` Status, können Sie die Protokolle überprüfen. Suchen Sie nach API-Antwortcodes im Bereich von 400 bis 500. Diese geben den Ort an, an dem ein Fehler aufgetreten ist.

Optionen

- Um die Bedienerprotokolle des Astra Control Center zu überprüfen, geben Sie Folgendes ein:

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


- So überprüfen Sie die Ausgabe des Astra Control Center CR:

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

Alternative Installationsverfahren

- **Installation mit Red hat OpenShift OperatorHub:** Verwenden Sie diese ["Alternativverfahren"](#) So installieren Sie Astra Control Center unter Verwendung von OperatorHub auf OpenShift.
- **In der öffentlichen Cloud mit Cloud Volumes ONTAP-Backend installieren:** Verwenden ["Derartige Verfahren"](#) Zur Installation von Astra Control Center in Amazon Web Services (AWS), Google Cloud Platform (GCP) oder Microsoft Azure mit einem Cloud Volumes ONTAP Storage-Back-End

Wie es weiter geht

- (Optional) Verarbeiten Sie abhängig von Ihrer Umgebung nach der Installation vollständig ["Konfigurationsschritte"](#).
- ["Nachdem Sie Astra Control Center installiert haben, sich bei der UI einloggen und Ihr Passwort ändern, sollten Sie eine Lizenz einrichten, Cluster hinzufügen, die Authentifizierung aktivieren, den Storage managen und Buckets hinzufügen"](#).

Konfigurieren Sie einen externen Zertifikaten-Manager

Wenn bereits ein Cert Manager in Ihrem Kubernetes Cluster vorhanden ist, müssen Sie einige erforderliche Schritte durchführen, damit Astra Control Center keinen eigenen Cert Manager installiert.

Schritte

1. Vergewissern Sie sich, dass ein Zertifikaten-Manager installiert ist:

```
kubectl get pods -A | grep 'cert-manager'
```

Beispielantwort:

```
cert-manager   essential-cert-manager-84446f49d5-sf2zd   1/1
Running       0     6d5h
cert-manager   essential-cert-manager-cainjector-66dc99cc56-9ldmt   1/1
Running       0     6d5h
cert-manager   essential-cert-manager-webhook-56b76db9cc-fjqrq     1/1
Running       0     6d5h
```

2. Erstellen Sie ein Zertifikat-/Schlüsselpaar für das `astraAddress` FQDN:

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

Beispielantwort:

```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'tls.key'
```

3. Erstellen eines Geheimnisses mit zuvor generierten Dateien:

```
kubectl create secret tls selfsigned-tls --key tls.key --cert tls.crt -n
<cert-manager-namespace>
```

Beispielantwort:

```
secret/selfsigned-tls created
```

4. Erstellen Sie ein ClusterIssuer Datei, die **genau** die folgenden ist, aber den Namespace-Speicherort enthält, wo Ihr cert-manager Pods sind installiert:

```
apiVersion: cert-manager.io/v1
kind: ClusterIssuer
metadata:
  name: astra-ca-clusterissuer
  namespace: <cert-manager-namespace>
spec:
  ca:
    secretName: selfsigned-tls
```

```
kubectl apply -f ClusterIssuer.yaml
```

Beispielantwort:

```
clusterissuer.cert-manager.io/astra-ca-clusterissuer created
```

5. Überprüfen Sie das ClusterIssuer Ist richtig aufgekommen. Ready Muss sein True Bevor Sie fortfahren können:

```
kubectl get ClusterIssuer
```

Beispielantwort:

NAME	READY	AGE
astra-ca-clusterissuer	True	9s

6. Füllen Sie die aus "[Astra Control Center-Installationsprozess](#)". Es gibt ein "[Erforderlicher Konfigurationsschritt für den Astra Control Center-Cluster YAML](#)" In dem Sie den CRD-Wert ändern, um anzuzeigen, dass der Zertifikaten-Manager extern installiert ist. Sie müssen diesen Schritt während der Installation abschließen, damit das Astra Control Center den externen Zertifikaten-Manager erkennt.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.