



# **Installare Astra Control Center**

## **Astra Control Center**

NetApp  
April 25, 2024

# Sommario

- Installare Astra Control Center utilizzando il processo standard . . . . . 1
  - Scarica ed estrai Astra Control Center. . . . . 3
  - Completare ulteriori passaggi se si utilizza un registro locale . . . . . 4
  - Impostare namespace e secret per i registri con requisiti di autenticazione . . . . . 8
  - Installare l'operatore del centro di controllo Astra . . . . . 9
  - Configurare Astra Control Center. . . . . 12
  - Completare l'installazione dell'Astra Control Center e dell'operatore . . . . . 26
  - Verificare lo stato del sistema . . . . . 27
  - Impostare l'ingresso per il bilanciamento del carico. . . . . 34
  - Accedere all'interfaccia utente di Astra Control Center . . . . . 37
  - Risolvere i problemi di installazione . . . . . 38
  - Procedure di installazione alternative . . . . . 38
  - Cosa succederà . . . . . 38
  - Configurare un gestore esterno dei certificati . . . . . 38

# Installare Astra Control Center utilizzando il processo standard

Per installare Astra Control Center, scaricare le immagini di installazione ed eseguire i seguenti passaggi. È possibile utilizzare questa procedura per installare Astra Control Center in ambienti connessi a Internet o con connessione ad aria.

Per una dimostrazione del processo di installazione di Astra Control Center, vedere ["questo video"](#).

## Prima di iniziare

- **Soddisfare i requisiti ambientali:** ["Prima di iniziare l'installazione, preparare l'ambiente per l'implementazione di Astra Control Center"](#).



Implementare Astra Control Center in un terzo dominio di errore o in un sito secondario. Questa opzione è consigliata per la replica delle applicazioni e il disaster recovery perfetto.

- **Garantire servizi integri:** Controllare che tutti i servizi API siano in buono stato e disponibili:

```
kubectl get apiservices
```

- **Assicurarsi che un FQDN instradabile:** Il FQDN Astra che si intende utilizzare può essere instradato al cluster. Ciò significa che si dispone di una voce DNS nel server DNS interno o si sta utilizzando un percorso URL principale già registrato.
- **Configure cert manager:** Se nel cluster esiste già un cert manager, è necessario eseguirne alcuni ["fasi preliminari"](#) In modo che Astra Control Center non tenti di installare il proprio cert manager. Per impostazione predefinita, Astra Control Center installa il proprio cert manager durante l'installazione.
- \* (Solo driver SAN ONTAP) Abilita multipath\*: Se stai utilizzando un driver SAN ONTAP, assicurati che multipath sia abilitato su tutti i tuoi cluster Kubernetes.

È inoltre necessario considerare quanto segue:

- **Ottenere l'accesso al Registro di sistema dell'immagine di controllo Astra di NetApp:**

È possibile ottenere le immagini di installazione e i miglioramenti delle funzionalità per Astra Control, come Astra Control provisioner, dal registro delle immagini di NetApp.

- a. Registrare l'ID dell'account Astra Control necessario per accedere al Registro di sistema.

Puoi visualizzare l'ID dell'account nell'interfaccia utente Web di Astra Control Service. Selezionare l'icona a forma di figura in alto a destra nella pagina, selezionare **accesso API** e annotare l'ID account.

- b. Nella stessa pagina, selezionare **generate API token**, copiare la stringa del token API negli Appunti e salvarla nell'editor.
- c. Accedere al registro Astra Control:

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

- **Installare una mesh di servizio per comunicazioni sicure:** Si consiglia vivamente di proteggere i canali di comunicazione del cluster host Astra Control utilizzando un ["mesh di servizio supportata"](#).



L'integrazione di Astra Control Center con una mesh di servizio può essere eseguita solo durante Astra Control Center ["installazione"](#) e non indipendente da questo processo. Il passaggio da un ambiente con mesh a un ambiente senza mesh non è supportato.

Per l'uso della mesh del servizio Istio, è necessario effettuare le seguenti operazioni:

- Aggiungere un `istio-injection:enabled` [etichetta](#) Al namespace Astra prima di implementare Astra Control Center.
- Utilizzare Generic [impostazione ingresso](#) e fornire un ingresso alternativo per [bilanciamento del carico esterno](#).
- Per i cluster Red Hat OpenShift, è necessario definire `NetworkAttachmentDefinition` Su tutti i namespace Astra Control Center associati (`netapp-acc-operator`, `netapp-acc`, `netapp-monitoring` per i cluster di applicazioni o qualsiasi namespace personalizzato che sia stato sostituito).

```
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
```

## Fasi

Per installare Astra Control Center, procedere come segue:

- [Scarica ed estrai Astra Control Center](#)
- [Completare ulteriori passaggi se si utilizza un registro locale](#)
- [Impostare namespace e secret per i registri con requisiti di autenticazione](#)

- [Installare l'operatore del centro di controllo Astra](#)
- [Configurare Astra Control Center](#)
- [Completare l'installazione dell'Astra Control Center e dell'operatore](#)
- [Verificare lo stato del sistema](#)
- [Impostare l'ingresso per il bilanciamento del carico](#)
- [Accedere all'interfaccia utente di Astra Control Center](#)



Non eliminare l'operatore di Astra Control Center (ad esempio, `kubectl delete -f astra_control_center_operator_deploy.yaml`) in qualsiasi momento durante l'installazione o il funzionamento di Astra Control Center per evitare di eliminare i pod.

## Scarica ed estrai Astra Control Center

Scarica le immagini di Astra Control Center da una delle seguenti posizioni:

- **Registro di sistema dell'immagine del servizio di controllo Astra:** Utilizzare questa opzione se non si utilizza un registro locale con le immagini del centro di controllo Astra o se si preferisce questo metodo per il download del pacchetto dal sito di supporto NetApp.
- **Sito di supporto NetApp:** Utilizzare questa opzione se si utilizza un registro locale con le immagini del Centro di controllo Astra.

### Registro delle immagini di Astra Control

1. Effettua l'accesso ad Astra Control Service.
2. Nella Dashboard, selezionare **distribuire un'istanza autogestita di Astra Control**.
3. Seguire le istruzioni per accedere al registro delle immagini di Astra Control, estrarre l'immagine di installazione di Astra Control Center ed estrarre l'immagine.

### Sito di supporto NetApp

1. Scarica il bundle contenente Astra Control Center (`astra-control-center-[version].tar.gz`) da "[Pagina di download di Astra Control Center](#)".
2. (Consigliato ma opzionale) Scarica il bundle di certificati e firme per Astra Control Center (`astra-control-center-certs-[version].tar.gz`) per verificare la firma del bundle.

```
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
```

Viene visualizzato l'output `Verified OK` una volta completata la verifica.

3. Estrarre le immagini dal bundle Astra Control Center:

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

## Completare ulteriori passaggi se si utilizza un registro locale

Se si intende inviare il pacchetto Astra Control Center al registro locale, è necessario utilizzare il plugin della riga di comando di NetApp Astra kubectl.

### Installare il plug-in NetApp Astra kubectl

Completare questi passaggi per installare il più recente plugin della riga di comando di NetApp Astra kubectl.

#### Prima di iniziare

NetApp fornisce binari per plug-in per diverse architetture CPU e sistemi operativi. Prima di eseguire questa attività, è necessario conoscere la CPU e il sistema operativo in uso.

Se il plug-in è già stato installato da un'installazione precedente, "[assicurarsi di disporre della versione più recente](#)" prima di completare questa procedura.

#### Fasi

1. Elencare i binari disponibili per il plugin NetApp Astra kubectl:



La libreria di plugin kubectl fa parte del bundle tar e viene estratta nella cartella `kubectl-astra`.

```
ls kubectl-astra/
```

2. Spostare il file necessario per il sistema operativo e l'architettura della CPU nel percorso corrente e rinominarlo `kubectl-astra`:

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

## Aggiungere le immagini al registro

1. Se si prevede di inviare il pacchetto Astra Control Center al registro locale, completare la sequenza di passaggi appropriata per il motore del contenitore:

## Docker

- a. Passare alla directory root del tarball. Viene visualizzata la `acc.manifest.bundle.yaml` file e queste directory:

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

- b. Trasferire le immagini del pacchetto nella directory delle immagini di Astra Control Center nel registro locale. Eseguire le seguenti sostituzioni prima di eseguire `push-images` comando:

- Sostituire `<BUNDLE_FILE>` con il nome del file bundle di controllo Astra (`acc.manifest.bundle.yaml`).
- Sostituire `<MY_FULL_REGISTRY_PATH>` con l'URL del repository Docker; ad esempio, `"<a href='\"https://<my_full_registry_path>\"' class='\"bare\">https://<my_full_registry_path>\"</a>`.
- Sostituire `<MY_REGISTRY_USER>` con il nome utente.
- Sostituire `<MY_REGISTRY_TOKEN>` con un token autorizzato per il registro.

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

## Podman

- a. Passare alla directory root del tarball. Vengono visualizzati il file e la directory seguenti:

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

- b. Accedere al Registro di sistema:

```
podman login <YOUR_REGISTRY>
```

- c. Preparare ed eseguire uno dei seguenti script personalizzato per la versione di Podman utilizzata. Sostituire `<MY_FULL_REGISTRY_PATH>` con l'URL del repository che include le sottodirectory.

```
<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

```



Il percorso dell'immagine creato dallo script deve essere simile al seguente, a seconda della configurazione del Registro di sistema:

```

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

```

## 2. Modificare la directory:

```

cd manifests

```

# Impostare namespace e secret per i registri con requisiti di autenticazione

1. Esportare il file kubeconfig per il cluster host Astra Control Center:

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



Prima di completare l'installazione, assicurarsi che kubeconfig punti al cluster in cui si desidera installare Astra Control Center.

2. Se si utilizza un registro che richiede l'autenticazione, è necessario effettuare le seguenti operazioni:

- a. Creare il netapp-acc-operator spazio dei nomi:

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

- b. Creare un segreto per netapp-acc-operator namespace. Aggiungere informazioni su Docker ed eseguire il seguente comando:



Il segnaposto `your_registry_path` deve corrispondere alla posizione delle immagini caricate in precedenza (ad esempio, `[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]
```

+



Se si elimina lo spazio dei nomi dopo la generazione del segreto, ricreare lo spazio dei nomi e rigenerare il segreto per lo spazio dei nomi.

- a. Creare il netapp-acc namespace (o personalizzato).

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

- b. Creare un segreto per `netapp-acc` namespace (o personalizzato). Aggiungere informazioni su Docker ed eseguire uno dei comandi appropriati in base alle preferenze del Registro di sistema:

```
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]
```

## Installare l'operatore del centro di controllo Astra

1. (Solo registri locali) se si utilizza un registro locale, completare i seguenti passaggi:

- a. Aprire il programma YAML di distribuzione dell'operatore Astra Control Center:

```
vim astra_control_center_operator_deploy.yaml
```



Un YAML di esempio annotato segue questi passaggi.

- b. Se si utilizza un registro che richiede l'autenticazione, sostituire la riga predefinita di `imagePullSecrets: []` con i seguenti elementi:

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

- c. Cambiare `ASTRA_IMAGE_REGISTRY` per `kube-rbac-proxy` al percorso del registro in cui sono state inviate le immagini in a. [passaggio precedente](#).
- d. Cambiare `ASTRA_IMAGE_REGISTRY` per `acc-operator-controller-manager` al percorso del registro in cui sono state inviate le immagini in a. [passaggio precedente](#).

```
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. Installare l'operatore del centro di controllo Astra:

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

### Espandi per la risposta di esempio:

```

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. Verificare che i pod siano in esecuzione:

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

# Configurare Astra Control Center

1. Modificare il file delle risorse personalizzate (CR) di Astra Control Center (`astra_control_center.yaml`) per creare account, supporto, registro e altre configurazioni necessarie:

```
vim astra_control_center.yaml
```



Un YAML di esempio annotato segue questi passaggi.

2. Modificare o confermare le seguenti impostazioni:

## Nome account

Impostazione	Guida	Tipo	Esempio
<code>accountName</code>	Modificare il <code>accountName</code> Stringa al nome che si desidera associare all'account Astra Control Center. Può essere presente un solo nome account.	stringa	Example

## AstraVersion

Impostazione	Guida	Tipo	Esempio
<code>astraVersion</code>	La versione di Astra Control Center da implementare. Non è necessaria alcuna azione per questa impostazione, in quanto il valore verrà pre-compilato.	stringa	24.02.0-69

## AstraAddress

Impostazione	Guida	Tipo	Esempio
astraAddress	<p>Modificare il <code>astraAddress</code></p> <p>Inserire l'FQDN (consigliato) o l'indirizzo IP che si desidera utilizzare nel browser per accedere ad Astra Control Center. Questo indirizzo definisce il modo in cui Astra Control Center verrà trovato nel data center e corrisponde allo stesso FQDN o indirizzo IP fornito dal bilanciamento del carico al termine dell'operazione <a href="#">"Requisiti di Astra Control Center"</a>.</p> <p>NOTA: Non utilizzare <code>http://</code> oppure <code>https://</code> nell'indirizzo. Copiare questo FQDN per utilizzarlo in un <a href="#">passo successivo</a>.</p>	stringa	<code>astra.example.com</code>

## AutoSupport

Le selezioni effettuate in questa sezione determinano se parteciperai all'applicazione di supporto proattivo di NetApp, NetApp Active IQ, e dove vengono inviati i dati. È necessaria una connessione a Internet (porta 442) e tutti i dati di supporto sono resi anonimi.

Impostazione	Utilizzare	Guida	Tipo	Esempio
<code>autoSupport.enrolled</code>	Entrambi <code>enrolled</code> oppure <code>url</code> i campi devono essere selezionati	Cambiare <code>enrolled</code> Per AutoSupport a. <code>false</code> per i siti senza connettività internet o senza <code>retain true</code> per i siti connessi. Un'impostazione di <code>true</code> Consente l'invio di dati anonimi a NetApp a scopo di supporto. L'elezione predefinita è <code>false</code> E indica che non verranno inviati dati di supporto a NetApp.	Booleano	<code>false</code> (valore predefinito)
<code>autoSupport.url</code>	Entrambi <code>enrolled</code> oppure <code>url</code> i campi devono essere selezionati	Questo URL determina dove verranno inviati i dati anonimi.	stringa	<a href="https://support.netapp.com/asupprod/post/1.0/postAsup">https://support.netapp.com/asupprod/post/1.0/postAsup</a>



## e-mail

Impostazione	Guida	Tipo	Esempio
email	Modificare il email stringa all'indirizzo iniziale predefinito dell'amministratore. Copiare questo indirizzo e-mail per utilizzarlo in <a href="#">passo successivo</a> . Questo indirizzo e-mail verrà utilizzato come nome utente per l'account iniziale per accedere all'interfaccia utente e verrà notificato degli eventi in Astra Control.	stringa	admin@example.com

## Nome

Impostazione	Guida	Tipo	Esempio
firstName	Il nome dell'amministratore iniziale predefinito associato all'account Astra. Il nome utilizzato qui sarà visibile in un'intestazione dell'interfaccia utente dopo il primo accesso.	stringa	SRE

## Cognome

Impostazione	Guida	Tipo	Esempio
lastName	Il cognome dell'amministratore iniziale predefinito associato all'account Astra. Il nome utilizzato qui sarà visibile in un'intestazione dell'interfaccia utente dopo il primo accesso.	stringa	Admin

## ImageRegistry

Le selezioni effettuate in questa sezione definiscono il registro delle immagini container che ospita le immagini dell'applicazione Astra, Astra Control Center Operator e il repository Astra Control Center Helm.

Impostazione	Utilizzare	Guida	Tipo	Esempio
imageRegistry.name	Obbligatorio	Nome del registro delle immagini di Astra Control che ospita tutte le immagini richieste per distribuire Astra Control Center. Il valore viene precompilato e non è richiesta alcuna azione, a meno che non sia stato configurato un registro locale. Per un registro locale, sostituire questo valore esistente con il nome del registro delle immagini in cui sono state inserite le immagini in <a href="#">passaggio precedente</a> . Non utilizzare <code>http://</code> oppure <code>https://</code> nel nome del registro di sistema.	stringa	<code>cr.astra.netapp.io</code> (impostazione predefinita) <code>example.registry.com/astra</code> (esempio di registro locale)

Impostazione	Utilizzare	Guida	Tipo	Esempio
imageRegistry. secret	Opzionale	<p>Il nome del segreto Kubernetes utilizzato per l'autenticazione con il registro delle immagini. Il valore viene precompilato e non è richiesta alcuna azione, a meno che non sia stato configurato un registro locale e la stringa immessa per tale registro imageRegistry.name richiede un segreto.</p> <p><b>IMPORTANTE:</b> Se si utilizza un registro locale che non richiede l'autorizzazione, è necessario eliminarlo <code>secret</code> linea entro <code>imageRegistry</code> in caso negativo, l'installazione non riesce.</p>	stringa	astra-registry-cred

## StorageClass

Impostazione	Guida	Tipo	Esempio
storageClass	<p>Modificare il storageClass valore da ontap-gold A un'altra risorsa storageClass come richiesto dall'installazione. Eseguire il comando <code>kubectl get sc</code> per determinare le classi di storage configurate esistenti. Una delle classi di storage configurate per Astra Control provisioner deve essere inserita nel file manifest (astra-control-center-&lt;version&gt;.manifest) E verranno utilizzati per Astra PVS. Se non è impostata, viene utilizzata la classe di storage predefinita.</p> <p>NOTA: Se è configurata una classe di storage predefinita, assicurarsi che sia l'unica classe di storage con l'annotazione predefinita.</p>	stringa	ontap-gold

## VolumeReclaimPolicy

Impostazione	Guida	Tipo	Opzioni
volumeReclaimPolicy	In questo modo viene impostata la policy di recupero per il PVS di Astra. Impostare questo criterio su <code>Retain</code> Conserva i volumi persistenti dopo l'eliminazione di Astra. Impostare questo criterio su <code>Delete</code> elimina i volumi persistenti dopo l'eliminazione di astra. Se questo valore non viene impostato, il PVS viene mantenuto.	stringa	<ul style="list-style-type: none"><li>• <code>Retain</code> (Valore predefinito)</li><li>• <code>Delete</code></li></ul>





Impostazione	Guida	Tipo	Opzioni
ingressType	<p>Utilizzare uno dei seguenti tipi di ingresso:</p> <p><b>Generic</b> (ingressType: "Generic") (Impostazione predefinita) Utilizzare questa opzione quando si utilizza un altro controller di ingresso o si preferisce utilizzare un controller di ingresso personalizzato. Dopo aver implementato Astra Control Center, è necessario configurare <a href="#">"controller di ingresso"</a> Per esporre Astra Control Center con un URL.</p> <p>IMPORTANTE: Se si intende utilizzare una mesh di servizio con Astra Control Center, è necessario selezionare Generic come tipo di ingresso e configurare il proprio <a href="#">"controller di ingresso"</a>.</p> <p><b>AccTraefik</b> (ingressType: "AccTraefik") Utilizzare questa opzione quando si preferisce non configurare un controller di ingresso. In questo modo viene implementato l'Astra Control Center traefik Gateway come servizio di tipo Kubernetes LoadBalancer.</p> <p>Astra Control Center utilizza un servizio del tipo "LoadBalancer" (svc/traefik Nello</p>	stringa	<ul style="list-style-type: none"> <li>• Generic (valore predefinito)</li> <li>• AccTraefik</li> </ul>



## Dimensione scala

Impostazione	Guida	Tipo	Opzioni
scaleSize	<p>Per impostazione predefinita, Astra utilizza High Availability (ha) scaleSize di Medium, Che implementa la maggior parte dei servizi in ha e implementa più repliche per la ridondanza. Con scaleSize come Small, Astra ridurrà il numero di repliche per tutti i servizi ad eccezione dei servizi essenziali per ridurre il consumo.</p> <p><b>SUGGERIMENTO:</b> Medium le implementazioni sono costituite da circa 100 pod (non inclusi i carichi di lavoro transitori. 100 pod si basa su una configurazione a tre nodi master e tre nodi worker). Tenere a conoscenza dei limiti di rete per pod che potrebbero rappresentare un problema nell'ambiente, in particolare quando si prendono in considerazione scenari di disaster recovery.</p>	stringa	<ul style="list-style-type: none"><li>• Small</li><li>• Medium (Valore predefinito)</li></ul>

## AstraResourcesScaler

Impostazione	Guida	Tipo	Opzioni
<code>astraResourcesScaler</code>	Opzioni di scalabilità per i limiti delle risorse di AstraControlCenter. Per impostazione predefinita, Astra Control Center implementa le richieste di risorse impostate per la maggior parte dei componenti all'interno di Astra. Questa configurazione consente allo stack software Astra Control Center di migliorare le prestazioni in ambienti con maggiore carico e scalabilità delle applicazioni. Tuttavia, negli scenari che utilizzano cluster di sviluppo o test più piccoli, il campo CR <code>astraResourcesScaler</code> può essere impostato su <code>Off</code> . In questo modo vengono disattivate le richieste di risorse e viene eseguita l'implementazione su cluster più piccoli.	stringa	<ul style="list-style-type: none"><li>• Default (Valore predefinito)</li><li>• Off</li></ul>

### AdditionalValues



Aggiungere i seguenti valori aggiuntivi ad Astra Control Center CR per evitare un problema noto durante l'installazione:

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

## crds

Le selezioni effettuate in questa sezione determinano il modo in cui Astra Control Center deve gestire i CRD.

Impostazione	Guida	Tipo	Esempio
<code>crds.externalCertManager</code>	Se si utilizza un gestore esterno dei certificati, cambiare <code>externalCertManager</code> a <code>true</code> . L'impostazione predefinita <code>false</code> Fa in modo che Astra Control Center installi i propri CRD di gestione dei certificati durante l'installazione. I CRDS sono oggetti a livello di cluster e l'installazione potrebbe avere un impatto su altre parti del cluster. È possibile utilizzare questo indicatore per segnalare ad Astra Control Center che questi CRD verranno installati e gestiti dall'amministratore del cluster al di fuori di Astra Control Center.	Booleano	<code>False</code> (valore predefinito)
<code>crds.externalTraefik</code>	Per impostazione predefinita, Astra Control Center installerà i CRD Traefik richiesti. I CRDS sono oggetti a livello di cluster e l'installazione potrebbe avere un impatto su altre parti del cluster. È possibile utilizzare questo indicatore per segnalare ad Astra Control Center che questi CRD verranno installati e gestiti dall'amministratore del cluster al di fuori di Astra Control Center.	Booleano	<code>False</code> (valore predefinito)



Assicurarsi di aver selezionato la classe di storage e il tipo di ingresso corretti per la configurazione prima di completare l'installazione.

#### esempio 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
```

## Completare l'installazione dell'Astra Control Center e dell'operatore

1. Se non lo si è già fatto in un passaggio precedente, creare il netapp-acc namespace (o personalizzato):

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

2. Se si utilizza una mesh di servizio con Astra Control Center, aggiungere la seguente etichetta al netapp-

acc o namespace personalizzato:



Il tipo di ingresso (ingressType) deve essere impostato su Generic In Astra Control Center CR prima di procedere con questo comando.

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

### 3. (Consigliato) "Attivare Strict MTLS" Per la mesh di servizio Istio:

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

### 4. Installare Astra Control Center in netapp-acc spazio dei nomi (o personalizzato):

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



L'operatore di Astra Control Center esegue un controllo automatico dei requisiti ambientali. Mancante "requisiti" Può causare problemi di installazione o il funzionamento non corretto di Astra Control Center. Vedere [sezione successiva](#) per verificare la presenza di messaggi di avvertenza relativi al controllo automatico del sistema.

## Verificare lo stato del sistema

È possibile verificare lo stato del sistema utilizzando i comandi kubectl. Se preferisci utilizzare OpenShift, puoi utilizzare comandi oc paragonabili per le fasi di verifica.

### Fasi

1. Verificare che il processo di installazione non abbia prodotto messaggi di avviso relativi ai controlli di convalida:

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



Ulteriori messaggi di avviso sono riportati anche nei registri dell'operatore di Astra Control Center.

2. Correggere eventuali problemi dell'ambiente segnalati dai controlli automatici dei requisiti.



È possibile correggere i problemi assicurandosi che l'ambiente soddisfi i requisiti ["requisiti"](#) Per Astra Control Center.

3. Verificare che tutti i componenti del sistema siano installati correttamente.

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

Ogni pod deve avere uno stato di `Running`. L'implementazione dei pod di sistema potrebbe richiedere alcuni minuti.

## Espandere per la risposta del campione

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
bucketervice-84d47487d-n9xgp 1h	1/1	Running	0
bucketervice-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-f69cdbd77-4p2kn 1h	1/1	Running	0
entitlement-f69cdbd77-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. (Facoltativo) guardare acc-operator registri per monitorare l'avanzamento:

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



accHost la registrazione del cluster è una delle ultime operazioni e, in caso di errore, la distribuzione non avrà esito negativo. In caso di errore di registrazione del cluster indicato nei registri, è possibile tentare di nuovo la registrazione tramite ["Aggiungere il flusso di lavoro del cluster nell'interfaccia utente"](#) O API.

5. Una volta eseguiti tutti i pod, verificare che l'installazione sia stata eseguita correttamente (READY è True) E ottieni la password di configurazione iniziale che userai quando accedi ad Astra Control Center:

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

Risposta:

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



Copiare il valore UUID. La password è ACC- Seguito dal valore UUID (ACC-[UUID] oppure, in questo esempio, ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f).

## Impostare l'ingresso per il bilanciamento del carico

È possibile configurare un controller di ingresso Kubernetes che gestisce l'accesso esterno ai servizi. Queste procedure forniscono esempi di configurazione per un controller di ingresso se si utilizza il valore predefinito di `ingressType: "Generic"` Nella risorsa personalizzata di Astra Control Center (`astra_control_center.yaml`). Non è necessario utilizzare questa procedura, se specificato `ingressType: "AccTraefik"` Nella risorsa personalizzata di Astra Control Center (`astra_control_center.yaml`).

Dopo l'implementazione di Astra Control Center, è necessario configurare il controller di ingresso per esporre Astra Control Center con un URL.

Le fasi di installazione variano a seconda del tipo di controller di ingresso utilizzato. Astra Control Center supporta molti tipi di controller di ingresso. Queste procedure di configurazione forniscono alcuni esempi di passaggi per alcuni tipi di controller di ingresso comuni.

### Prima di iniziare

- Il necessario "[controller di ingresso](#)" dovrebbe essere già implementato.
- Il "[classe di ingresso](#)" corrispondente al controller di ingresso dovrebbe già essere creato.

## Passaggi per l'ingresso di Istio

1. Configurare l'ingresso Istio.



Questa procedura presuppone che Istio venga distribuito utilizzando il profilo di configurazione "predefinito".

2. Raccogliere o creare il certificato e il file della chiave privata desiderati per Ingress Gateway.

È possibile utilizzare un certificato CA o autofirmato. Il nome comune deve essere l'indirizzo Astra (FQDN).

Esempio di comando:

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

3. Crea un segreto `tls secret name` di tipo `kubernetes.io/tls` Per una chiave privata TLS e un

certificato in `istio-system` namespace Come descritto in TLS secrets (segreti TLS).

Esempio di comando:

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



Il nome del segreto deve corrispondere a `spec.tls.secretName` fornito in `istio-ingress.yaml` file.

4. Implementare una risorsa di ingresso in `netapp-acc` namespace (o personalizzato) che utilizza il tipo di risorsa `v1` per uno schema (`istio-Ingress.yaml` in questo esempio):

```
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. Applicare le modifiche:

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

## 6. Controllare lo stato dell'ingresso:

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

Risposta:

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

## 7. Completare l'installazione di Astra Control Center.

### Procedura per il controller di ingresso Nginx

1. Creare un segreto di tipo `kubernetes.io/tls` Per una chiave privata TLS e un certificato in `netapp-acc` (o con nome personalizzato) come descritto in "[Segreti TLS](#)".
2. Implementare una risorsa `ingress` in `netapp-acc` namespace (o personalizzato) che utilizza il tipo di risorsa `v1` per uno schema (`nginx-Ingress.yaml` in questo esempio):

```
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. Applicare le modifiche:

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



NetApp consiglia di installare il controller nginx come implementazione piuttosto che come daemonSet.

## Procedura per il controller di ingresso OpenShift

1. Procurarsi il certificato e ottenere la chiave, il certificato e i file CA pronti per l'uso con il percorso OpenShift.
2. Creare il percorso OpenShift:

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

## Accedere all'interfaccia utente di Astra Control Center

Dopo aver installato Astra Control Center, modificherai la password per l'amministratore predefinito ed effettuerai l'accesso alla dashboard dell'interfaccia utente di Astra Control Center.

### Fasi

1. In un browser, immettere l'FQDN (compreso il `https://` prefisso) utilizzato in `astraAddress` in `astra_control_center.yaml` CR quando [Astra Control Center è stato installato](#).
2. Accettare i certificati autofirmati, se richiesto.



È possibile creare un certificato personalizzato dopo l'accesso.

3. Nella pagina di accesso di Astra Control Center, inserire il valore utilizzato per `email` poll `astra_control_center.yaml` CR quando [Astra Control Center è stato installato](#), seguito dalla password di configurazione iniziale (`ACC-[UUID]`).



Se si immette una password errata per tre volte, l'account admin viene bloccato per 15 minuti.

4. Selezionare **Login**.
5. Modificare la password quando richiesto.



Se si tratta del primo accesso e si dimentica la password e non sono stati ancora creati altri account utente amministrativi, contattare ["Supporto NetApp"](#) per assistenza per il recupero della password.

6. (Facoltativo) rimuovere il certificato TLS autofirmato esistente e sostituirlo con un ["Certificato TLS"](#)

personalizzato firmato da un'autorità di certificazione (CA)".

## Risolvere i problemi di installazione

Se uno dei servizi è in `Error` stato, è possibile esaminare i registri. Cercare i codici di risposta API nell'intervallo da 400 a 500. Questi indicano il luogo in cui si è verificato un guasto.

### Opzioni

- Per esaminare i registri dell'operatore di Astra Control Center, immettere quanto segue:

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

- Per controllare l'output di Astra Control Center CR:

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

## Procedure di installazione alternative

- **Installa con Red Hat OpenShift OperatorHub:** USA questo ["procedura alternativa"](#) Per installare Astra Control Center su OpenShift utilizzando OperatorHub.
- **Installare nel cloud pubblico con backend Cloud Volumes ONTAP:** Utilizzare ["queste procedure"](#) Per installare Astra Control Center in Amazon Web Services (AWS), Google Cloud Platform (GCP) o Microsoft Azure con un backend di storage Cloud Volumes ONTAP.

## Cosa succederà

- (Opzionale) a seconda dell'ambiente, completare la post-installazione ["fasi di configurazione"](#).
- ["Dopo aver installato Astra Control Center, effettuato l'accesso all'interfaccia utente e modificato la password, è necessario impostare una licenza, aggiungere cluster, abilitare l'autenticazione, gestire lo storage e aggiungere bucket"](#).

## Configurare un gestore esterno dei certificati

Se nel cluster Kubernetes esiste già un cert manager, è necessario eseguire alcuni passaggi preliminari in modo che Astra Control Center non installi il proprio cert manager.

### Fasi

1. Verificare che sia installato un gestore dei certificati:

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

Esempio di risposta:



```

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. Creare una coppia certificato/chiave per astraAddress FQDN:

```

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

```

Esempio di risposta:

```

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

```

## 3. Creare un segreto con i file generati in precedenza:

```

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

```

Esempio di risposta:

```

secret/selfsigned-tls created

```

## 4. Creare un ClusterIssuer file che è **esattamente** il seguente, ma include la posizione dello spazio dei nomi in cui si trova il cert-manager i pod sono installati:

```

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
```

Esempio di risposta:

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

5. Verificare che il ClusterIssuer è venuto in su correttamente. Ready deve essere True prima di procedere:

```
kubectl get ClusterIssuer
```

Esempio di risposta:

NAME	READY	AGE
astra-ca-clusterissuer	True	9s

6. Completare il ["Processo di installazione di Astra Control Center"](#). Esiste un ["Fase di configurazione richiesta per il cluster Astra Control Center YAML"](#) In cui si modifica il valore CRD per indicare che il gestore dei certificati è installato esternamente. È necessario completare questa fase durante l'installazione in modo che Astra Control Center riconosca il cert manager esterno.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.