# Documentazione di Astra Control Center 22.04

## Astra Control Center

NetApp
November 21, 2023

# Sommario

# Documentazione di Astra Control Center 22.04

# Note di rilascio

Siamo lieti di annunciare la release 22.04.0 di Astra Control Center.

- "Cosa c'è in questa release di Astra Control Center"
- "Problemi noti"
- "Problemi noti con Astra Data Store e questa release di Astra Control Center"
- "Limitazioni note"

Seguici su Twitter @NetAppDoc. Invia un feedback sulla documentazione diventando un "Collaboratore di GitHub" oppure inviare un'e-mail all'indirizzo doccomments@netapp.com.

# Novità di questa release di Astra Control Center

Siamo lieti di annunciare l'ultima release 22.04.0 di Astra Control Center.

## 26 aprile 2022 (22.04.0)

### Nuove funzionalità e supporto

- "Implementazione di Astra Data Store da Astra Control Center"
- "RBAC (role-based access control) dello spazio dei nomi"
- "Supporto per Cloud Volumes ONTAP"
- "Abilitazione ingresso generico per Astra Control Center"
- "Rimozione della benna da Astra Control"
- "Supporto per il portfolio VMware Tanzu"

### Problemi noti e limitazioni

- "Problemi noti per questa release"
- "Problemi noti con Astra Data Store e questa release di Astra Control Center"
- "Limitazioni note per questa versione"

## 14 dicembre 2021 (21.12)

### Nuove funzionalità e supporto

- "Ripristino dell'applicazione"
- "Ganci di esecuzione"
- "Supporto per le applicazioni implementate con operatori con ambito namespace"
- "Supporto aggiuntivo per Kubernetes e Rancher upstream"
- "Astra Data Store visualizza in anteprima la gestione e il monitoraggio del back-end"
- "Aggiornamenti di Astra Control Center"
- "Opzione Red Hat OperatorHub per l'installazione"

### Problemi risolti

- "Problemi risolti per questa release"

**Problemi noti e limitazioni**

- "Problemi noti per questa release"
- "Problemi noti con l'anteprima di Astra Data Store e questa release di Astra Control Center"
- "Limitazioni note per questa versione"

## 5 agosto 2021 (21.08)

Release iniziale di Astra Control Center.

- "Che cos'è"
- "Comprendere l'architettura e i componenti"
- "Cosa serve per iniziare"
- "Installare" e. "setup (configurazione)"
- "Gestire" e. "proteggere" applicazioni
- "Gestire i bucket" e. "back-end dello storage"
- "Gestire gli account"
- "Automatizzare con API"

## Trova ulteriori informazioni

- "Problemi noti per questa release"
- "Limitazioni note per questa versione"
- "Documentazione di Astra Data Store"
- "Versioni precedenti della documentazione di Astra Control Center"

# Problemi noti

I problemi noti identificano i problemi che potrebbero impedire l'utilizzo corretto di questa versione del prodotto.

I seguenti problemi noti riguardano la versione corrente:

**Applicazioni**

- Il ripristino di un'applicazione comporta una dimensione PV superiore a quella del PV originale
- I cloni delle applicazioni non riescono a utilizzare una versione specifica di PostgreSQL
- I cloni delle applicazioni non funzionano quando si utilizzano i vincoli di contesto di protezione OCP a livello di account di servizio (SCC)
- I cloni delle applicazioni si guastano dopo l'implementazione di un'applicazione con una classe di storage set

**Cluster**

- La gestione di un cluster con Astra Control Center non riesce quando il file kubeconfig predefinito contiene più di un contesto

**Altri problemi**

- Le operazioni di gestione dei dati dell'app non riescono e si verificano errori di servizio interni (500) quando Astra Trident è offline

- Le snapshot potrebbero non funzionare con la versione 4.2.0 del controller di snapshot

## Il ripristino di un'applicazione comporta una dimensione PV superiore a quella del PV originale

Se si ridimensiona un volume persistente dopo la creazione di un backup e poi si ripristina da tale backup, le dimensioni del volume persistente corrispondono alle nuove dimensioni del PV invece di utilizzare le dimensioni del backup.

## I cloni delle applicazioni non riescono a utilizzare una versione specifica di PostgreSQL

I cloni delle applicazioni all'interno dello stesso cluster si guastano costantemente con il grafico BitNami PostgreSQL 11.5.0. Per clonare correttamente, utilizzare una versione precedente o successiva del grafico.

## I cloni delle applicazioni non funzionano quando si utilizzano i vincoli di contesto di protezione OCP a livello di account di servizio (SCC)

Un clone dell'applicazione potrebbe non riuscire se i vincoli del contesto di protezione originale sono configurati a livello di account di servizio all'interno dello spazio dei nomi nel cluster OpenShift Container Platform. Quando il clone dell'applicazione non funziona, viene visualizzato nell'area delle applicazioni gestite di Astra Control Center con lo stato `Removed`. Vedere "articolo della knowledge base" per ulteriori informazioni.

## I cloni delle applicazioni si guastano dopo l'implementazione di un'applicazione con una classe di storage set

Dopo che un'applicazione è stata distribuita con una classe di storage esplicitamente impostata (ad esempio, `helm install …-set global.storageClass=netapp-cvs-perf-extreme`), i successivi tentativi di clonare l'applicazione richiedono che il cluster di destinazione abbia la classe di storage specificata in origine. La clonazione di un'applicazione con una classe di storage esplicitamente impostata su un cluster che non ha la stessa classe di storage non avrà esito positivo. In questo scenario non sono disponibili procedure di ripristino.

## La gestione di un cluster con Astra Control Center non riesce quando il file kubeconfig predefinito contiene più di un contesto

Non è possibile utilizzare un kubeconfig con più di un cluster e un contesto. Vedere "articolo della knowledge base" per ulteriori informazioni.

## Le operazioni di gestione dei dati dell'app non riescono e si verificano errori di servizio interni (500) quando Astra Trident è offline

Se Astra Trident su un cluster di applicazioni diventa offline (e viene riportato online) e si verificano 500 errori di servizio interni durante il tentativo di gestione dei dati dell'applicazione, riavviare tutti i nodi Kubernetes nel cluster di applicazioni per ripristinare la funzionalità.

## Le snapshot potrebbero non funzionare con la versione 4.2.0 del controller di snapshot

Quando si utilizza Kubernetes snapshot-controller (noto anche come external-snapshotter) versione 4.2.0 con Kubernetes 1.20 o 1.21, le snapshot possono iniziare a fallire. Per evitare questo problema, utilizzare un altro "versione supportata" Di external-snapshotter, come la versione 4.2.1, con Kubernetes versioni 1.20 o 1.21.

1. Eseguire UNA CHIAMATA POST per aggiungere un file kubeconfig aggiornato a `/credentials` endpoint e recuperare l'assegnato `id` dal corpo di risposta.
2. Eseguire una chiamata PUT da `/clusters` Endpoint utilizzando l'ID cluster appropriato e impostare `credentialID` al `id` valore dal passo precedente.

Una volta completata questa procedura, la credenziale associata al cluster viene aggiornata e il cluster si riconnetterà e aggiornerà il proprio stato a. `available`.

### Trova ulteriori informazioni

- "Problemi noti con la prreview di Astra Data Store e questa release di Astra Control Center"
- "Limitazioni note"

### Problemi noti con Astra Data Store e questa release di Astra Control Center

I problemi noti identificano i problemi che potrebbero impedire l'utilizzo corretto di questa versione del prodotto.

"Vedere questi problemi noti" Ciò potrebbe influire sulla gestione di Astra Data Store con l'attuale release di Astra Control Center.

#### Trova ulteriori informazioni

- "Problemi noti"
- "Limitazioni note"

## Limitazioni note

Le limitazioni note identificano piattaforme, dispositivi o funzioni non supportate da questa versione del prodotto o che non interagiscono correttamente con esso. Esaminare attentamente queste limitazioni.

#### Limitazioni della gestione del cluster

- Lo stesso cluster non può essere gestito da due istanze di Astra Control Center
- Astra Control Center non è in grado di gestire due cluster con lo stesso nome

#### Limitazioni RBAC (Role-Based Access Control)

- Un utente con vincoli RBAC dello spazio dei nomi può aggiungere e annullare la gestione di un cluster
- Un membro con vincoli dello spazio dei nomi non può accedere alle applicazioni clonate o ripristinate fino a quando admin non aggiunge lo spazio dei nomi al vincolo

#### Limitazioni della gestione delle applicazioni

- I backup delle applicazioni in corso non possono essere interrotti
- I cloni delle applicazioni installate utilizzando operatori pass-by-reference possono fallire
- Le operazioni di ripristino in-place delle applicazioni che utilizzano un gestore dei certificati non sono supportate
- Le applicazioni implementate dall'operatore CON ambito cluster e abilitato OLM non sono supportate
- Le app implementate con Helm 2 non sono supportate

#### Limitazioni generali

- I bucket S3 in Astra Control Center non riportano la capacità disponibile
- Astra Control Center non convalida i dati immessi per il server proxy
- Le connessioni esistenti a un pod Postgres causano errori
- I backup e le snapshot potrebbero non essere conservati durante la rimozione di un'istanza di Astra Control Center

## Lo stesso cluster non può essere gestito da due istanze di Astra Control Center

Se si desidera gestire un cluster su un'altra istanza di Astra Control Center, è necessario innanzitutto "annullare la gestione del cluster" dall'istanza in cui viene gestito prima di gestirlo su un'altra istanza. Dopo aver rimosso il cluster dalla gestione, verificare che il cluster non sia gestito eseguendo questo comando:

```
oc get pods n -netapp-monitoring
```

Non devono essere presenti pod in esecuzione nello spazio dei nomi, altrimenti lo spazio dei nomi non dovrebbe esistere. Se uno di questi è vero, il cluster non viene gestito.

## Astra Control Center non è in grado di gestire due cluster con lo stesso nome

Se si tenta di aggiungere un cluster con lo stesso nome di un cluster già esistente, l'operazione non riesce. Questo problema si verifica più spesso in un ambiente Kubernetes standard se non è stato modificato il nome predefinito del cluster nei file di configurazione Kubernetes.

Per risolvere il problema, procedere come segue:

1. Modifica la configurazione di kubeadm-config:

   ```
   kubectl edit configmaps -n kube-system kubeadm-config
   ```

2. Modificare il `clusterName` valore campo da `kubernetes` (Il nome predefinito di Kubernetes) con un nome personalizzato univoco.
3. Modifica kubeconfig (`.kube/config`).
4. Aggiorna il nome del cluster da `kubernetes` su un nome personalizzato univoco (`xyz-cluster` viene utilizzato negli esempi seguenti). Eseguire l'aggiornamento in entrambi `clusters` e. `contexts` sezioni come mostrato in questo esempio:

```
apiVersion: v1
clusters:
- cluster:
    certificate-authority-data:
ExAmPLERb2tCcjZ5K3E2Njk4eQotLExAMpLEORCBDRVJUSUZJQ0FURS0txxxxXX==
    server: https://x.x.x.x:6443
  name: xyz-cluster
contexts:
- context:
    cluster: xyz-cluster
    namespace: default
    user: kubernetes-admin
  name: kubernetes-admin@kubernetes
current-context: kubernetes-admin@kubernetes
```

## Un utente con vincoli RBAC dello spazio dei nomi può aggiungere e annullare la gestione di un cluster

Un utente con vincoli RBAC dello spazio dei nomi non deve essere autorizzato ad aggiungere o annullare la gestione dei cluster. A causa di un limite corrente, Astra non impedisce a tali utenti di annullare la gestione dei cluster.

## Un membro con vincoli dello spazio dei nomi non può accedere alle applicazioni clonate o ripristinate fino a quando admin non aggiunge lo spazio dei nomi al vincolo

Qualsiasi `member` Gli utenti con vincoli RBAC in base al nome/ID dello spazio dei nomi o alle etichette dello spazio dei nomi possono clonare o ripristinare un'applicazione in un nuovo spazio dei nomi nello stesso cluster o in qualsiasi altro cluster dell'account dell'organizzazione. Tuttavia, lo stesso utente non può accedere all'applicazione clonata o ripristinata nel nuovo namespace. Una volta creato un nuovo spazio dei nomi mediante un'operazione di clonazione o ripristino, l'amministratore/proprietario dell'account può modificare `member` account utente e limitazioni del ruolo di aggiornamento per consentire all'utente interessato di concedere l'accesso al nuovo spazio dei nomi.

## I backup delle applicazioni in corso non possono essere interrotti

Non esiste alcun modo per interrompere un backup in esecuzione. Se è necessario eliminare il backup, attendere che sia stato completato, quindi seguire le istruzioni riportate in "Eliminare i backup". Per eliminare un backup non riuscito, utilizzare "API di controllo Astra".

## I cloni delle applicazioni installate utilizzando operatori pass-by-reference possono fallire

Astra Control supporta le applicazioni installate con operatori con ambito namespace. Questi operatori sono generalmente progettati con un'architettura "pass-by-value" piuttosto che "pass-by-reference". Di seguito sono riportate alcune applicazioni per operatori che seguono questi modelli:

- "Apache K8ssandra"

> Per K8ssandra, sono supportate le operazioni di ripristino in-place. Un'operazione di ripristino su un nuovo namespace o cluster richiede che l'istanza originale dell'applicazione venga tolto. In questo modo si garantisce che le informazioni del peer group trasportate non conducano a comunicazioni tra istanze. La clonazione dell'applicazione non è supportata.

- "Ci Jenkins"
- "Cluster XtraDB Percona"

Si noti che Astra Control potrebbe non essere in grado di clonare un operatore progettato con un'architettura "pass-by-reference" (ad esempio, l'operatore CockroachDB). Durante questi tipi di operazioni di cloning, l'operatore clonato tenta di fare riferimento ai segreti di Kubernetes dall'operatore di origine, nonostante abbia il proprio nuovo segreto come parte del processo di cloning. L'operazione di clonazione potrebbe non riuscire perché Astra Control non è a conoscenza dei segreti di Kubernetes nell'operatore di origine.

## Le operazioni di ripristino in-place delle applicazioni che utilizzano un gestore dei certificati non sono supportate

Questa versione di Astra Control Center non supporta il ripristino in-place delle applicazioni con i gestori dei certificati. Sono supportate le operazioni di ripristino su uno spazio dei nomi diverso e le operazioni di clonazione.

## Le applicazioni implementate dall'operatore CON ambito cluster e abilitato OLM non sono supportate

Astra Control Center non supporta le attività di gestione delle applicazioni con operatori con ambito cluster.

## Le app implementate con Helm 2 non sono supportate

Se utilizzi Helm per implementare le app, Astra Control Center richiede Helm versione 3. La gestione e la clonazione delle applicazioni implementate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. Per ulteriori informazioni, vedere "Requisiti di Astra Control Center".

## I bucket S3 in Astra Control Center non riportano la capacità disponibile

Prima di eseguire il backup o la clonazione delle applicazioni gestite da Astra Control Center, controllare le informazioni del bucket nel sistema di gestione ONTAP o StorageGRID.

## Astra Control Center non convalida i dati immessi per il server proxy

Assicurati di "inserire i valori corretti" quando si stabilisce una connessione.

## Le connessioni esistenti a un pod Postgres causano errori

Quando si eseguono operazioni su POD Postgres, non si dovrebbe connettersi direttamente all'interno del pod per utilizzare il comando psql. Astra Control richiede l'accesso a psql per bloccare e scongelare i database. Se è presente una connessione preesistente, lo snapshot, il backup o il clone non avranno esito positivo.

## I backup e le snapshot potrebbero non essere conservati durante la rimozione di un'istanza di Astra Control Center

Se si dispone di una licenza di valutazione, assicurarsi di memorizzare l'ID account per evitare la perdita di dati in caso di guasto di Astra Control Center se non si inviano ASUP.

## Trova ulteriori informazioni

- "Problemi noti"
- "Problemi noti con Astra Data Store e questa release di Astra Control Center"

# Concetti

## Scopri di più su Astra Control

Astra Control è una soluzione per la gestione del ciclo di vita dei dati delle applicazioni Kubernetes che semplifica le operazioni per le applicazioni stateful. Proteggi, esegui il backup e migra facilmente i carichi di lavoro Kubernetes e crea istantaneamente cloni applicativi funzionanti.

### Caratteristiche

Astra Control offre funzionalità critiche per la gestione del ciclo di vita dei dati delle applicazioni Kubernetes:

- Gestire automaticamente lo storage persistente
- Creazione di snapshot e backup on-demand basati sulle applicazioni
- Automatizzare le operazioni di backup e snapshot basate su policy
- Migrare applicazioni e dati da un cluster Kubernetes a un altro
- Clonare facilmente un'applicazione dalla produzione allo staging
- Visualizzare lo stato di salute e protezione dell'applicazione
- Utilizzare un'interfaccia utente o un'API per implementare i flussi di lavoro di backup e migrazione

Astra Control controlla continuamente il tuo calcolo per individuare eventuali modifiche dello stato, in modo che sia consapevole di eventuali nuove applicazioni aggiunte lungo il percorso.

### Modelli di implementazione

Astra Control è disponibile in due modelli di implementazione:

- **Astra Control Service**: Un servizio gestito da NetApp che fornisce la gestione dei dati application-aware dei cluster Kubernetes in Google Kubernetes Engine (GKE) e Azure Kubernetes Service (AKS).
- **Astra Control Center**: Software autogestito che fornisce la gestione dei dati applicativa dei cluster Kubernetes in esecuzione nel tuo ambiente on-premise.

| | **Servizio di controllo Astra** | **Centro di controllo Astra** |
|---|---|---|
| **Come viene offerto?** | Come servizio cloud completamente gestito da NetApp | Come software scaricato, installato e gestito |
| **Dove è ospitato?** | Su un cloud pubblico scelto da NetApp | Sul cluster Kubernetes fornito |
| **Come viene aggiornato?** | Gestito da NetApp | Gli aggiornamenti vengono gestiti |
| **Quali sono le funzionalità di gestione dei dati delle applicazioni?** | Stesse funzionalità su entrambe le piattaforme con eccezioni al backend dello storage o ai servizi esterni | Stesse funzionalità su entrambe le piattaforme con eccezioni al backend dello storage o ai servizi esterni |

| | Servizio di controllo Astra | Centro di controllo Astra |
|---|---|---|
| **Che cos'è il supporto back-end dello storage?** | Offerte di servizi cloud NetApp | • Sistemi NetApp ONTAP AFF e FAS<br>• Astra Data Store come back-end dello storage<br>• Back-end dello storage Cloud Volumes ONTAP |

## Applicazioni supportate

NetApp ha validato alcune applicazioni per garantire la sicurezza e la coerenza di snapshot e backup.

- "Scopri la differenza tra un'applicazione validata e un'applicazione standard in Astra Control".

Indipendentemente dal tipo di applicazione utilizzata con Astra Control, è sempre necessario testare autonomamente il flusso di lavoro di backup e ripristino per assicurarsi di poter soddisfare i requisiti di disaster recovery.

## Come funziona Astra Control Service

Astra Control Service è un servizio cloud gestito da NetApp sempre attivo e aggiornato con le funzionalità più recenti. Utilizza diversi componenti per consentire la gestione del ciclo di vita dei dati delle applicazioni.

Ad alto livello, Astra Control Service funziona come segue:

- Per iniziare a utilizzare Astra Control Service, devi configurare il tuo cloud provider e registrarti per un account Astra.
  - Per i cluster GKE, Astra Control Service utilizza "NetApp Cloud Volumes Service per Google Cloud" O Google Persistent Disks come back-end di storage per i volumi persistenti.
  - Per i cluster AKS, Astra Control Service utilizza "Azure NetApp Files" O Azure Disk Storage come back-end di storage per i volumi persistenti.
- Aggiungi il tuo primo calcolo Kubernetes ad Astra Control Service. Astra Control Service esegue le seguenti operazioni:
  - Crea un archivio di oggetti nel tuo account cloud provider, dove vengono memorizzate le copie di backup.

    In Azure, Astra Control Service crea anche un gruppo di risorse, un account di storage e chiavi per il container Blob.
  - Crea un nuovo ruolo di amministratore e un nuovo account del servizio Kubernetes sul cluster.
  - Utilizza il nuovo ruolo di amministratore per l'installazione "Astra Trident" sul cluster e per creare una o più classi di storage.
  - Se utilizzi Azure NetApp Files o NetApp Cloud Volumes Service per Google Cloud come back-end di storage, il servizio di controllo di Astra utilizza Astra Trident per eseguire il provisioning di volumi persistenti per le tue applicazioni.
- A questo punto, è possibile aggiungere applicazioni al cluster. Il provisioning dei volumi persistenti verrà eseguito sulla nuova classe di storage predefinita.
- Quindi, utilizza Astra Control Service per gestire queste applicazioni e iniziare a creare snapshot, backup e cloni.

Astra Control Service controlla continuamente il tuo calcolo per individuare eventuali modifiche dello stato, in modo che sia consapevole di eventuali nuove applicazioni aggiunte lungo il percorso.

Il piano gratuito di Astra Control ti consente di gestire fino a 10 applicazioni nel tuo account. Se desideri gestire più di 10 app, dovrai impostare la fatturazione eseguendo l'aggiornamento dal piano gratuito al piano Premium.

## Come funziona Astra Control Center

Astra Control Center viene eseguito localmente nel tuo cloud privato.

Astra Control Center supporta i cluster OpenShift Kubernetes con:

- Lo storage Trident si backend con ONTAP 9.5 e versioni successive
- Back-end storage Astra Data Store

In un ambiente connesso al cloud, Astra Control Center utilizza Cloud Insights per fornire monitoraggio e telemetria avanzati. In assenza di una connessione Cloud Insights, il monitoraggio e la telemetria sono disponibili in un centro di controllo Astra per un periodo di 7 giorni ed esportati anche in strumenti di monitoraggio nativi Kubernetes (come Prometheus e Grafana) attraverso endpoint di metriche aperte.

Il centro di controllo Astra è completamente integrato nell'ecosistema AutoSupport e Active IQ per fornire agli utenti e al supporto NetApp informazioni sulla risoluzione dei problemi e sull'utilizzo.

Puoi provare Astra Control Center utilizzando una licenza di valutazione di 90 giorni. La versione di valutazione è supportata tramite le opzioni e-mail e community (slack channel). Inoltre, puoi accedere agli articoli e alla documentazione della Knowledge base dalla dashboard di supporto all'interno del prodotto.

Per installare e utilizzare Astra Control Center, è necessario soddisfare determinati requisiti "requisiti".

Ad alto livello, Astra Control Center funziona come segue:

- Astra Control Center viene installato nel proprio ambiente locale. Scopri di più su come "Installare Astra Control Center".
- È possibile completare alcune attività di configurazione, come ad esempio:
  - Impostare la licenza.
  - Aggiungere il primo cluster.
  - Aggiungere il backend di storage rilevato quando si aggiunge il cluster.
  - Aggiungi un bucket di store di oggetti che memorizzerà i backup delle tue app.

Scopri di più su come "Configurare Astra Control Center".

Astra Control Center esegue questa operazione:

- Scopre i dettagli sui cluster Kubernetes gestiti.
- Rileva la configurazione di Astra Trident o Astra Data Store sui cluster che si sceglie di gestire e consente di monitorare i backend dello storage.
- Rileva le applicazioni su tali cluster e ti consente di gestirle e proteggerle.

È possibile aggiungere applicazioni al cluster. In alternativa, se nel cluster gestito sono già presenti alcune applicazioni, puoi utilizzare Astra Control Center per rilevarle e gestirle. Quindi, utilizza Astra Control Center

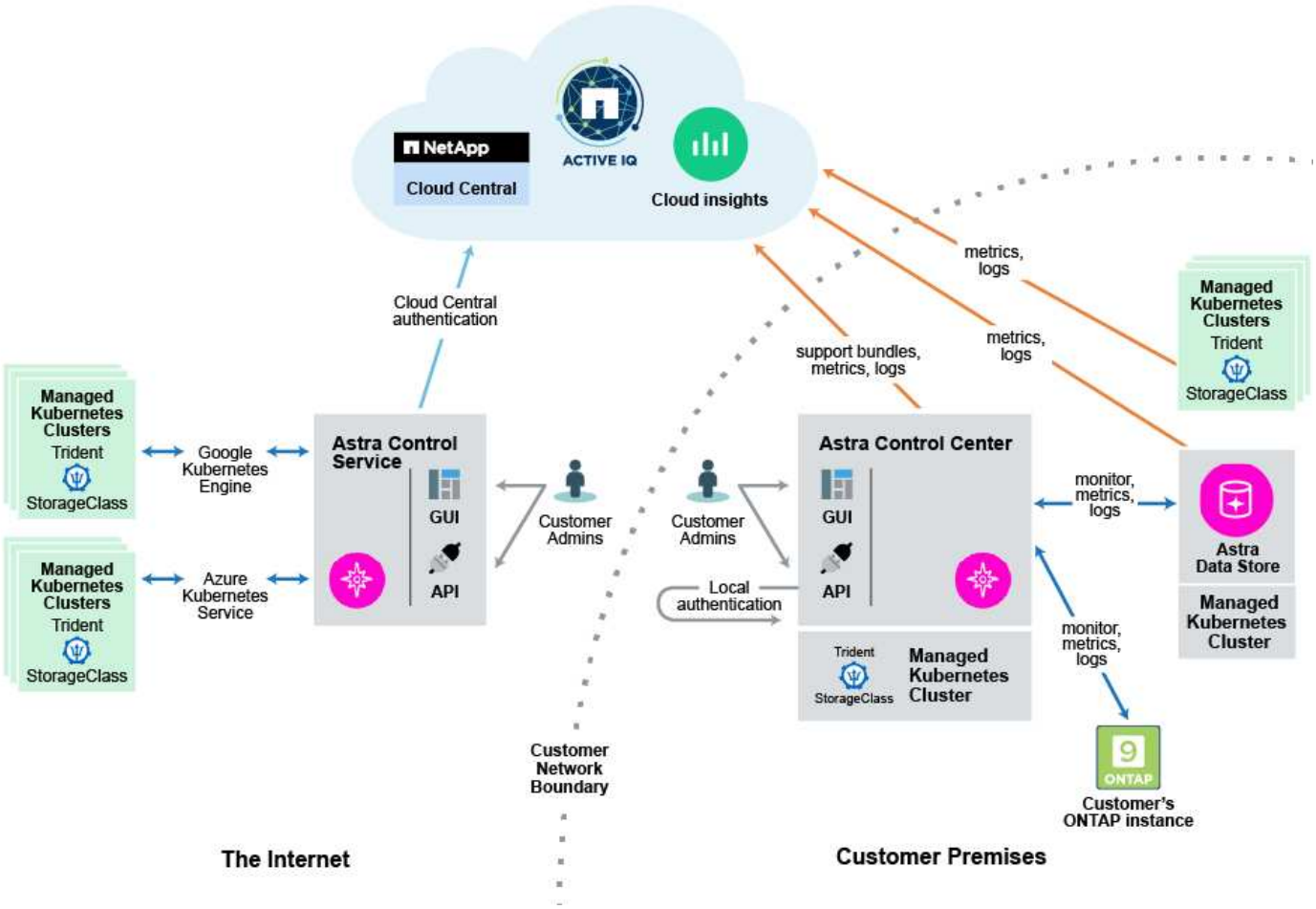
per creare snapshot, backup e cloni.

### Per ulteriori informazioni

- "Documentazione del servizio Astra Control"
- "Documentazione di Astra Control Center"
- "Documentazione di Astra Data Store"
- "Documentazione di Astra Trident"
- "Utilizzare l'API di controllo Astra"
- "Documentazione Cloud Insights"
- "Documentazione ONTAP"

## Architettura e componenti

Ecco una panoramica dei vari componenti dell'ambiente Astra Control.




### Componenti di controllo Astra

- **Kubernetes Clusters**: Kubernetes è una piattaforma open-source portatile, estensibile per la gestione di carichi di lavoro e servizi containerizzati, che facilita sia la configurazione dichiarativa che l'automazione. Astra fornisce servizi di gestione per le applicazioni ospitate in un cluster Kubernetes.

- * Astra Trident*: In qualità di provider di storage open source e orchestrator gestiti da NetApp, Trident consente di creare volumi di storage per applicazioni containerizzate gestite da Docker e Kubernetes. Se implementato con il centro di controllo Astra, Trident include un backend di storage ONTAP configurato e supporta anche l'archivio dati Astra come backend di storage.
- **Storage backend**:
  - Utilizzo di Astra Control Service "NetApp Cloud Volumes Service per Google Cloud" Come back-end di storage per i cluster GKE e. "Azure NetApp Files" Come back-end di storage per i cluster AKS.
  - Astra Control Service supporta anche Azure Managed Disks e Google Persistent Disk come opzioni di storage back-end.
  - Astra Control Center utilizza i seguenti backend di storage:
    - Back-end di storage Astra Data Store
    - Backend di storage ONTAP AFF e FAS. In qualità di piattaforma hardware e software per lo storage, ONTAP offre servizi di storage di base, supporto per più protocolli di accesso allo storage e funzionalità di gestione dello storage, come snapshot e mirroring.
    - Back-end dello storage Cloud Volumes ONTAP
- **Cloud Insights**: Uno strumento di monitoraggio dell'infrastruttura cloud NetApp, Cloud Insights consente di monitorare le performance e l'utilizzo dei cluster Kubernetes gestiti dal centro di controllo Astra. Cloud Insights mette in relazione l'utilizzo dello storage con i carichi di lavoro. Quando si attiva la connessione Cloud Insights in Astra Control Center, le informazioni di telemetria vengono visualizzate nelle pagine dell'interfaccia utente di Astra Control Center.

### Interfacce di controllo Astra

È possibile completare le attività utilizzando diverse interfacce:

- **Interfaccia utente Web (UI)**: Sia Astra Control Service che Astra Control Center utilizzano la stessa interfaccia utente basata sul Web, in cui è possibile gestire, migrare e proteggere le applicazioni. Utilizzare l'interfaccia utente anche per gestire gli account utente e le impostazioni di configurazione.
- **API**: Sia Astra Control Service che Astra Control Center utilizzano la stessa API Astra Control. Utilizzando l'API, è possibile eseguire le stesse attività dell'interfaccia utente.

Astra Control Center consente inoltre di gestire, migrare e proteggere i cluster Kubernetes in esecuzione negli ambienti delle macchine virtuali.

### Per ulteriori informazioni

- "Documentazione del servizio Astra Control"
- "Documentazione di Astra Control Center"
- "Documentazione di Astra Trident"
- "Utilizzare l'API di controllo Astra"
- "Documentazione Cloud Insights"
- "Documentazione ONTAP"

# Protezione dei dati

Scopri i tipi di protezione dei dati disponibili in Astra Control Center e come utilizzarli al meglio per proteggere le tue applicazioni.

### Snapshot, backup e policy di protezione

Una *snapshot* è una copia point-in-time di un'applicazione memorizzata sullo stesso volume fornito dell'applicazione. Di solito sono veloci. È possibile utilizzare snapshot locali per ripristinare l'applicazione a un punto precedente. Le snapshot sono utili per cloni veloci; le snapshot includono tutti gli oggetti Kubernetes per l'applicazione, inclusi i file di configurazione.

Un *backup* viene memorizzato nell'archivio di oggetti esterno e può essere più lento rispetto agli snapshot locali. È possibile ripristinare un backup dell'applicazione nello stesso cluster oppure migrare un'applicazione ripristinando il backup su un cluster diverso. È inoltre possibile scegliere un periodo di conservazione più lungo per i backup. Poiché sono memorizzati nell'archivio di oggetti esterno, i backup offrono in genere una protezione migliore rispetto alle snapshot in caso di guasto al server o perdita di dati.

Una *policy di protezione* è un metodo per proteggere un'applicazione creando automaticamente snapshot, backup o entrambi in base a un programma definito per tale applicazione. Una policy di protezione consente inoltre di scegliere il numero di snapshot e backup da conservare nella pianificazione. L'automazione di backup e snapshot con una policy di protezione è il modo migliore per garantire che ogni applicazione sia protetta in base alle esigenze della tua organizzazione.

> *Non è possibile essere completamente protetti fino a quando non si dispone di un backup recente*. Ciò è importante perché i backup vengono memorizzati in un archivio a oggetti lontano dai volumi persistenti. Se un guasto o un incidente cancella il cluster e lo storage persistente associato, è necessario un backup per il ripristino. Un'istantanea non consentirebbe il ripristino.

### Cloni

Un *clone* è un duplicato esatto di un'applicazione, della sua configurazione e del suo storage persistente. È possibile creare manualmente un clone sullo stesso cluster Kubernetes o su un altro cluster. La clonazione di un'applicazione può essere utile se è necessario spostare applicazioni e storage da un cluster Kubernetes a un altro.

## Licensing

Astra Control Center richiede l'installazione di una licenza per abilitare la funzionalità completa di gestione dei dati dell'applicazione. Quando si implementa Astra Control Center senza licenza, viene visualizzato un banner nell'interfaccia utente Web, che avvisa che le funzionalità del sistema sono limitate.

Le seguenti operazioni richiedono una licenza valida:

- Gestione di nuove applicazioni
- Creazione di snapshot o backup
- Configurazione di un criterio di protezione per la pianificazione di snapshot o backup
- Ripristino da uno snapshot o da un backup
- Clonazione da uno snapshot o da uno stato corrente

> È possibile aggiungere un cluster, aggiungere un bucket e gestire un backend di storage Astra Data Store senza licenza. Tuttavia, è necessaria una licenza Astra Control Center valida per gestire le applicazioni utilizzando Astra Data Store come back-end di storage.

### Come viene calcolato il consumo delle licenze

Quando si aggiunge un nuovo cluster ad Astra Control Center, non viene contato per ottenere licenze consumate fino a quando almeno un'applicazione in esecuzione sul cluster non viene gestita da Astra Control Center. È inoltre possibile aggiungere un backend di storage Astra Data Store ad Astra Control Center senza influire sul consumo delle licenze. Questo consente di gestire un back-end Astra Data Store da un sistema Astra Control Center senza licenza.

Quando si inizia a gestire un'applicazione su un cluster, le unità CPU del cluster vengono incluse nel calcolo del consumo di licenza di Astra Control Center.

### Trova ulteriori informazioni

- "Aggiornare una licenza esistente"

# Applicazioni validate e standard

Ci sono due tipi di applicazioni che puoi portare ad Astra Control: Validate e standard. Scopri la differenza tra queste due categorie e i potenziali impatti sui tuoi progetti e sulla tua strategia.

> È allettante pensare a queste due categorie come "supportate" e "non supportate". Tuttavia, come si vedrà, in Astra Control non esiste un'applicazione "non supportata". Puoi aggiungere qualsiasi applicazione ad Astra Control, anche se le app validate hanno più infrastruttura costruita intorno ai flussi di lavoro di Astra Control rispetto alle app standard.

### Applicazioni validate

Le applicazioni validate per Astra Control includono:

- MySQL 8.0.25
- MariaDB 10.5.9
- PostgreSQL 11.12
- Jenkins 2.277.4 LTS e 2.289.1 LTS

L'elenco delle applicazioni validate rappresenta le applicazioni riconosciute da Astra Control. Il team di Astra Control ha analizzato e confermato che queste applicazioni sono state completamente testate per il ripristino. Astra Control esegue flussi di lavoro personalizzati per garantire la coerenza a livello di applicazione di snapshot e backup.

Se un'applicazione viene convalidata, il team di Astra Control ha identificato e implementato i passaggi che possono essere intrapresi per interrompere l'applicazione prima di creare uno snapshot per ottenere uno snapshot coerente con l'applicazione. Ad esempio, quando Astra Control esegue un backup di un database PostgreSQL, prima di tutto il database viene posto in pausa. Una volta completato il backup, Astra Control ripristina il normale funzionamento del database.

Indipendentemente dal tipo di applicazione utilizzata con Astra Control, verificate sempre il flusso di lavoro di backup e ripristino per assicurarvi di soddisfare i vostri requisiti di disaster recovery.

### Applicazioni standard

Altre applicazioni, tra cui programmi personalizzati, sono considerate applicazioni standard. Puoi aggiungere e

gestire le applicazioni standard attraverso Astra Control. Puoi anche creare snapshot e backup di base coerenti con il crash di un'applicazione standard. Tuttavia, questi non sono stati completamente testati per ripristinare l'applicazione al suo stato originale.

> Astra Control non è un'applicazione standard, ma un'applicazione di sistema. Per impostazione predefinita, Astra Control non viene visualizzato per la gestione. Non si dovrebbe tentare di gestire Astra Control da solo.

# Classi di storage e dimensioni del volume persistente

Il centro di controllo Astra supporta ONTAP o l'archivio dati Astra come back-end dello storage.

## Panoramica

Astra Control Center supporta:

- **Classi di storage Trident supportate dallo storage Astra Data Store**: Se sono stati installati manualmente uno o più cluster Astra Data Store, Astra Control Center offre la possibilità di importare questi cluster e recuperare la loro topologia (nodi, dischi) e vari stati.

  Astra Control Center visualizza il cluster Kubernetes sottostante dalla configurazione di Astra Data Store, il cloud a cui appartiene il cluster Kubernetes, tutti i volumi persistenti forniti da Astra Data Store, il nome del volume interno corrispondente, l'applicazione che utilizza il volume persistente e il cluster che contiene l'applicazione.

- **Classi di storage Trident supportate dallo storage ONTAP**: Se si utilizza un backend ONTAP, Astra Control Center offre la possibilità di importare il backend ONTAP per la segnalazione di varie informazioni di monitoraggio.

> Le classi di storage Trident devono essere preconfigurate all'esterno di Astra Control Center.

## Classi di storage

Quando si aggiunge un cluster ad Astra Control Center, viene richiesto di selezionare una classe di storage precedentemente configurata su tale cluster come classe di storage predefinita. Questa classe di storage verrà utilizzata quando non viene specificata alcuna classe di storage in una dichiarazione di volume persistente (PVC). La classe di storage predefinita può essere modificata in qualsiasi momento all'interno di Astra Control Center e qualsiasi classe di storage può essere utilizzata in qualsiasi momento specificando il nome della classe di storage all'interno del grafico PVC o Helm. Assicurarsi di avere definito solo una singola classe di storage predefinita per il cluster Kubernetes.

Quando si utilizza Astra Control Center integrato con un backend di storage Astra Data Store, dopo l'installazione non vengono definite classi di storage. Sarà necessario creare la classe di storage predefinita Trident e applicarla al backend dello storage. Vedere "Guida introduttiva di Astra Data Store" Per creare una classe di storage Astra Data Store predefinita.

## Per ulteriori informazioni

- "Documentazione di Astra Trident"

# Ruoli e spazi dei nomi degli utenti

Scopri i ruoli e gli spazi dei nomi degli utenti in Astra Control e come utilizzarli per controllare l'accesso alle risorse della tua organizzazione.

## Ruoli utente

È possibile utilizzare i ruoli per controllare l'accesso degli utenti alle risorse o alle funzionalità di Astra Control. Di seguito sono riportati i ruoli utente in Astra Control:

- Un **Viewer** può visualizzare le risorse.
- Un **Member** dispone delle autorizzazioni per il ruolo Viewer e può gestire app e cluster, annullare la gestione delle app ed eliminare snapshot e backup.
- Un **Admin** dispone delle autorizzazioni di ruolo membro e può aggiungere e rimuovere qualsiasi altro utente ad eccezione del Proprietario.
- Un **Owner** dispone delle autorizzazioni di ruolo Admin e può aggiungere e rimuovere qualsiasi account utente.

È possibile aggiungere vincoli a un utente membro o Viewer per limitare l'utente a uno o più utenti Spazi dei nomi.

## Spazi dei nomi

Uno spazio dei nomi è un ambito che è possibile assegnare a risorse specifiche all'interno di un cluster gestito da Astra Control. Astra Control rileva gli spazi dei nomi di un cluster quando si aggiunge il cluster ad Astra Control. Una volta rilevati, gli spazi dei nomi sono disponibili per l'assegnazione come vincoli agli utenti. Solo i membri che hanno accesso a tale spazio dei nomi possono utilizzare tale risorsa. È possibile utilizzare gli spazi dei nomi per controllare l'accesso alle risorse utilizzando un paradigma adatto alla propria organizzazione, ad esempio per aree fisiche o divisioni all'interno di un'azienda. Quando si aggiungono vincoli a un utente, è possibile configurare tale utente in modo che abbia accesso a tutti gli spazi dei nomi o solo a un set specifico di spazi dei nomi. È inoltre possibile assegnare vincoli dello spazio dei nomi utilizzando le etichette dello spazio dei nomi.

## Trova ulteriori informazioni

"Gestire i ruoli"

# Inizia subito

## Requisiti di Astra Control Center

Inizia verificando la preparazione del tuo ambiente operativo, dei cluster di applicazioni, delle applicazioni, delle licenze e del browser Web.

### Requisiti dell'ambiente operativo

Astra Control Center richiede uno dei seguenti tipi di ambienti operativi:

- Kubernetes da 1.20 a 1.23
- Rancher 2.5.8, 2.5.9 o 2.6 con RKE1
- Red Hat OpenShift Container Platform 4.6.8, 4.7, 4.8 o 4.9
- VMware Tanzu Kubernetes Grid 1.4
- VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2

Assicurarsi che l'ambiente operativo scelto per ospitare Astra Control Center soddisfi i requisiti delle risorse di base descritti nella documentazione ufficiale dell'ambiente. Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse dell'ambiente:

| Componente | Requisito |
|---|---|
| Capacità di back-end dello storage | Almeno 500 GB disponibili |
| Nodi di lavoro | Almeno 3 nodi di lavoro in totale, con 4 core CPU e 12 GB di RAM ciascuno |
| Indirizzo FQDN | Un indirizzo FQDN per Astra Control Center |
| Astra Trident | • Astra Trident 21.04 o versione successiva installata e configurata<br>• Astra Trident 21.10.1 o versione successiva installata e configurata se Astra Data Store verrà utilizzato come backend di storage |

Questi requisiti presuppongono che Astra Control Center sia l'unica applicazione in esecuzione nell'ambiente operativo. Se nell'ambiente sono in esecuzione applicazioni aggiuntive, modificare di conseguenza questi requisiti minimi.

- **Registro immagini**: È necessario disporre di un registro di immagini Docker privato in cui è possibile trasferire le immagini di build di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui verranno caricate le immagini.
- **Astra Trident / ONTAP Configuration**: Astra Control Center richiede la creazione e l'impostazione di una classe di storage come classe di storage predefinita. Centro di controllo Astra supporta i seguenti driver ONTAP forniti da Astra Trident:
  - ontap-nas
  - ontap-san

- ontap-san-economy

> Durante la clonazione delle applicazioni in ambienti OpenShift, Astra Control Center deve consentire a OpenShift di montare volumi e modificare la proprietà dei file. Per questo motivo, è necessario configurare un criterio di esportazione dei volumi ONTAP per consentire queste operazioni. Puoi farlo con i seguenti comandi:
>
> 1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
> 2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

> Se si prevede di aggiungere un secondo ambiente operativo OpenShift come risorsa di calcolo gestita, è necessario assicurarsi che la funzione Astra Trident Volume Snapshot sia attivata. Per abilitare e testare le snapshot dei volumi con Astra Trident, "Consulta le istruzioni ufficiali di Astra Trident".

#### Requisiti del cluster Grid VMware Tanzu Kubernetes

Quando si ospita Astra Control Center su un cluster VMware Tanzu Kubernetes Grid (TKG) o Tanzu Kubernetes Grid Integrated Edition (TKGi), tenere presente quanto segue.

- Disattivare l'applicazione della classe di storage predefinita TKG o TKGi su qualsiasi cluster di applicazioni che deve essere gestito da Astra Control. Per eseguire questa operazione, modificare il `TanzuKubernetesCluster` risorsa sul cluster dello spazio dei nomi.
- È necessario creare una policy di sicurezza che consenta ad Astra Control Center di creare pod all'interno del cluster. È possibile eseguire questa operazione utilizzando i seguenti comandi:

```
kubectl config use-context <context-of-workload-cluster>
kubectl create clusterrolebinding default-tkg-admin-privileged-binding
--clusterrole=psp:vmware-system-privileged --group=system:authenticated
```

- Quando si implementa Astra Control Center in un ambiente TKG o TKGi, è necessario conoscere i requisiti specifici di Astra Trident. Per ulteriori informazioni, consultare "Documentazione di Astra Trident".

> Il token del file di configurazione predefinito di VMware TKG e TKGi scade dieci ore dopo l'implementazione. Se si utilizzano prodotti del portfolio Tanzu, è necessario generare un file di configurazione del cluster Tanzu Kubernetes con un token non in scadenza per evitare problemi di connessione tra Astra Control Center e cluster di applicazioni gestiti. Per istruzioni, visitare il sito "Documentazione del prodotto VMware NSX-T Data Center."

## Backend di storage supportati

Astra Control Center supporta i seguenti backend di storage.

- Archivio dati Astra
- NetApp ONTAP 9.5 o sistemi AFF e FAS più recenti
- NetApp Cloud Volumes ONTAP

## Requisiti del cluster di applicazioni

Astra Control Center ha i seguenti requisiti per i cluster che si intende gestire da Astra Control Center. Questi requisiti si applicano anche se il cluster che si intende gestire è il cluster dell'ambiente operativo che ospita Astra Control Center.

- La versione più recente di Kubernetes "componente snapshot-controller" è installato
- Un tridente Astra "oggetto volumesnapshotclass" è stato definito da un amministratore
- Nel cluster esiste una classe di storage Kubernetes predefinita
- Almeno una classe di storage è configurata per utilizzare Astra Trident

> Il cluster di applicazioni deve disporre di un `kubeconfig.yaml` file che definisce un solo elemento *context*. Visitare la documentazione Kubernetes per "informazioni sulla creazione di file kubeconfig".

> Quando si gestiscono i cluster di applicazioni in un ambiente Rancher, modificare il contesto predefinito del cluster di applicazioni in `kubeconfig` File fornito da Rancher per utilizzare un contesto del piano di controllo invece del contesto del server API Rancher. In questo modo si riduce il carico sul server API Rancher e si migliorano le performance.

## Requisiti di gestione delle applicazioni

Astra Control ha i seguenti requisiti di gestione delle applicazioni:

- **Licensing**: Per gestire le applicazioni utilizzando Astra Control Center, è necessaria una licenza Astra Control Center.
- **Namespaces**: Astra Control richiede che un'applicazione non si estende più di un singolo namespace, ma uno spazio dei nomi può contenere più di un'applicazione.
- **StorageClass**: Se si installa un'applicazione con un StorageClass esplicitamente impostato ed è necessario clonare l'applicazione, il cluster di destinazione per l'operazione di clone deve avere la StorageClass specificata in origine. Il cloning di un'applicazione con un StorageClass esplicitamente impostato su un cluster che non ha lo stesso StorageClass avrà esito negativo.
- **Kubernetes resources**: Le applicazioni che utilizzano risorse Kubernetes non raccolte da Astra Control potrebbero non disporre di funzionalità complete di gestione dei dati delle applicazioni. Astra Control raccoglie le seguenti risorse Kubernetes:

| | | |
|---|---|---|
| ClusterRole | ClusterRoleBinding | ConfigMap |
| Lavoro di cassa | CustomResourceDefinition | CustomResource |
| DemonSet | DeploymentConfig | HorizontalPodAutoscaler |
| Ingresso | MutatingWebhook | NetworkPolicy |
| PersistentVolumeClaim | Pod | PodDisruptionBudget |
| PodTemplate | ReplicaSet | Ruolo |
| RoleBinding | Percorso | Segreto |
| Servizio | ServiceAccount | StatefulSet |
| ValidatingWebhook | | |

#### Metodi di installazione delle applicazioni supportati

Astra Control supporta i seguenti metodi di installazione dell'applicazione:

- **Manifest file**: Astra Control supporta le applicazioni installate da un file manifest utilizzando kubectl. Ad esempio:

```
kubectl apply -f myapp.yaml
```

- **Helm 3**: Se utilizzi Helm per installare le app, Astra Control richiede Helm versione 3. La gestione e la clonazione delle applicazioni installate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. La gestione delle applicazioni installate con Helm 2 non è supportata.
- **Applicazioni distribuite dall'operatore**: Astra Control supporta le applicazioni installate con operatori con ambito namespace. Di seguito sono riportate alcune applicazioni che sono state validate per questo modello di installazione:
  - "Apache K8ssandra"
  - "Ci Jenkins"
  - "Cluster XtraDB Percona"

> Un operatore e l'applicazione che installa devono utilizzare lo stesso namespace; potrebbe essere necessario modificare il file .yaml di implementazione per l'operatore per assicurarsi che questo sia il caso.

## Accesso a Internet

È necessario determinare se si dispone di un accesso esterno a Internet. In caso contrario, alcune funzionalità potrebbero essere limitate, ad esempio la ricezione di dati di monitoraggio e metriche da NetApp Cloud Insights o l'invio di pacchetti di supporto a "Sito di supporto NetApp".

## Licenza

Astra Control Center richiede una licenza Astra Control Center per una funzionalità completa. Ottenere una licenza di valutazione o una licenza completa da NetApp. Senza una licenza, non sarà possibile:

- Definire applicazioni personalizzate
- Creare snapshot o cloni di applicazioni esistenti
- Configurare le policy di protezione dei dati

Se si desidera provare Astra Control Center, è possibile "utilizzare una licenza di valutazione di 90 giorni".

Per ulteriori informazioni sul funzionamento delle licenze, vedere "Licensing".

## Ingresso per cluster Kubernetes on-premise

È possibile scegliere il tipo di ingresso di rete utilizzato da Astra Control Center. Per impostazione predefinita, Astra Control Center implementa il gateway Astra Control Center (servizio/traefik) come risorsa a livello di cluster. Astra Control Center supporta anche l'utilizzo di un servizio di bilanciamento del carico, se consentito nel tuo ambiente. Se si preferisce utilizzare un servizio di bilanciamento del carico e non ne si dispone già di uno configurato, è possibile utilizzare il bilanciamento del carico MetalLB per assegnare automaticamente un

indirizzo IP esterno al servizio. Nella configurazione del server DNS interno, puntare il nome DNS scelto per Astra Control Center sull'indirizzo IP con bilanciamento del carico.

> Se si ospita Astra Control Center su un cluster Tanzu Kubernetes Grid, utilizzare `kubectl get nsxlbmonitors -A` per verificare se è già stato configurato un monitor dei servizi per accettare il traffico in entrata. Se ne esiste uno, non installare MetalLB, perché il monitor di servizio esistente sovrascriverà qualsiasi nuova configurazione del bilanciamento del carico.

Per ulteriori informazioni, vedere "Impostare l'ingresso per il bilanciamento del carico".

## Requisiti di rete

L'ambiente operativo che ospita Astra Control Center comunica utilizzando le seguenti porte TCP. Assicurarsi che queste porte siano consentite attraverso qualsiasi firewall e configurare i firewall in modo da consentire qualsiasi traffico HTTPS in uscita dalla rete Astra. Alcune porte richiedono la connettività tra l'ambiente che ospita Astra Control Center e ciascun cluster gestito (annotato dove applicabile).

> Puoi implementare Astra Control Center in un cluster Kubernetes dual-stack, mentre Astra Control Center può gestire le applicazioni e i back-end di storage configurati per il funzionamento dual-stack. Per ulteriori informazioni sui requisiti del cluster dual-stack, vedere "Documentazione Kubernetes".

| Origine | Destinazione | Porta | Protocollo | Scopo |
|---|---|---|---|---|
| PC client | Centro di controllo Astra | 443 | HTTPS | Accesso UI/API - assicurarsi che questa porta sia aperta in entrambi i modi tra il cluster che ospita Astra Control Center e ciascun cluster gestito |
| Metriche consumer | Nodo di lavoro Astra Control Center | 9090 | HTTPS | Comunicazione dei dati delle metriche - garantire che ciascun cluster gestito possa accedere a questa porta sul cluster che ospita Astra Control Center (è richiesta una comunicazione bidirezionale) |
| Centro di controllo Astra | Servizio Hosted Cloud Insights (https://cloudinsights.netapp.com) | 443 | HTTPS | Comunicazione Cloud Insights |

| Origine | Destinazione | Porta | Protocollo | Scopo |
|---|---|---|---|---|
| Centro di controllo Astra | Provider di bucket di storage Amazon S3 (https://my-bucket.s3.us-west-2.amazonaws.com/) | 443 | HTTPS | Comunicazione con lo storage Amazon S3 |
| Centro di controllo Astra | NetApp AutoSupport (https://support.netapp.com) | 443 | HTTPS | Comunicazioni NetApp AutoSupport |

### Browser Web supportati

Astra Control Center supporta versioni recenti di Firefox, Safari e Chrome con una risoluzione minima di 1280 x 720.

### Cosa succederà

Visualizzare il "avvio rapido" panoramica.

# Avvio rapido per Astra Control Center

Questa pagina fornisce una panoramica generale dei passaggi necessari per iniziare a utilizzare Astra Control Center. I collegamenti all'interno di ogni passaggio consentono di accedere a una pagina che fornisce ulteriori dettagli.

Provalo! Se si desidera provare Astra Control Center, è possibile utilizzare una licenza di valutazione di 90 giorni. Vedere "informazioni sulle licenze" per ulteriori informazioni.

1 **Esaminare i requisiti del cluster Kubernetes**

- Astra funziona con i cluster Kubernetes con un backend di storage ONTAP configurato con Trident o un backend di storage Astra Data Store.
- I cluster devono essere in esecuzione in condizioni di salute, con almeno tre nodi di lavoro online.
- Il cluster deve eseguire Kubernetes.

"Scopri di più sui requisiti di Astra Control Center".

2 **Scaricare e installare Astra Control Center**

- Scaricare Astra Control Center dal "Sito di supporto NetApp pagina Download di Astra Control Center".
- Installare Astra Control Center nell'ambiente locale.

  Se lo si desidera, installare Astra Control Center utilizzando Red Hat OperatorHub.

"Scopri di più sull'installazione di Astra Control Center".

3 **Completare alcune attività di configurazione iniziali**

- Aggiungere una licenza.
- Aggiungi un cluster Kubernetes e Astra Control Center scopre i dettagli.
- Aggiungere un ONTAP o. "Archivio dati Astra" back-end dello storage.
- Facoltativamente, Aggiungi un bucket di store di oggetti che memorizzerà i backup delle app.

"Scopri di più sul processo di configurazione iniziale".

**4 Utilizzare Astra Control Center**

Dopo aver completato la configurazione di Astra Control Center, ecco cosa fare:

- Gestire un'applicazione. "Scopri di più su come gestire le app".
- Se lo si desidera, connettersi a NetApp Cloud Insights per visualizzare le metriche sullo stato di salute del sistema, sulla capacità e sul throughput all'interno dell'interfaccia utente di Astra Control Center. "Scopri di più sulla connessione a Cloud Insights".

**5 Continuare da questa guida di avvio rapido**

"Installare Astra Control Center".

### Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"

# Panoramica dell'installazione

Scegliere e completare una delle seguenti procedure di installazione di Astra Control Center:

- "Installare Astra Control Center utilizzando il processo standard"
- "(Se utilizzi Red Hat OpenShift) Installa Astra Control Center usando OpenShift OperatorHub"
- "Installare il centro di controllo Astra con un backend di storage Cloud Volumes ONTAP"

## Installare Astra Control Center utilizzando il processo standard

Per installare Astra Control Center, scaricare il pacchetto di installazione dal NetApp Support Site ed eseguire la procedura seguente per installare Astra Control Center Operator e Astra Control Center nel proprio ambiente. È possibile utilizzare questa procedura per installare Astra Control Center in ambienti connessi a Internet o con connessione ad aria.

Per gli ambienti Red Hat OpenShift, è possibile utilizzare anche un "procedura alternativa" Per installare Astra Control Center utilizzando OpenShift OperatorHub.

#### Di cosa hai bisogno

- "Prima di iniziare l'installazione, preparare l'ambiente per l'implementazione di Astra Control Center".
- Assicurarsi che tutti gli operatori del cluster siano in buono stato e disponibili.

  Esempio di OpenShift:

```
oc get clusteroperators
```

- Assicurarsi che tutti i servizi API siano in buono stato e disponibili:

  Esempio di OpenShift:

```
oc get apiservices
```

- L'FQDN Astra che si intende utilizzare deve essere instradabile a questo cluster. Ciò significa che si dispone di una voce DNS nel server DNS interno o si sta utilizzando un percorso URL principale già registrato.

**A proposito di questa attività**

Il processo di installazione di Astra Control Center esegue le seguenti operazioni:

- Installa i componenti Astra in `netapp-acc` namespace (o personalizzato).
- Crea un account predefinito.
- Stabilisce un indirizzo e-mail predefinito per l'utente amministrativo e una password monouso predefinita di `ACC-<UUID_of_installation>` Per questo caso di Astra Control Center. A questo utente viene assegnato il ruolo Owner (Proprietario) nel sistema ed è necessario per il primo accesso all'interfaccia utente.
- Consente di determinare se tutti i pod Astra Control Center sono in esecuzione.
- Installa l'interfaccia utente Astra.

> (Valido solo per la release Astra Data Store Early Access Program (EAP)). Se si intende gestire Astra Data Store utilizzando Astra Control Center e abilitare i flussi di lavoro VMware, implementare Astra Control Center solo su `pcloud` namespace e non su `netapp-acc` namespace o uno spazio dei nomi personalizzato descritto nei passaggi di questa procedura.

> Non eseguire il seguente comando durante l'intero processo di installazione per evitare di eliminare tutti i pod di Astra Control Center: `kubectl delete -f astra_control_center_operator_deploy.yaml`

> Se si utilizza Podman di Red Hat invece di Docker Engine, è possibile utilizzare i comandi Podman al posto dei comandi Docker.

**Fasi**

Per installare Astra Control Center, procedere come segue:

- Scarica e disimballa il bundle Astra Control Center
- Installare il plug-in NetApp Astra kubectl
- Aggiungere le immagini al 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

### Scarica e disimballa il bundle Astra Control Center

1. Scarica il bundle Astra Control Center (`astra-control-center-[version].tar.gz`) da "Sito di supporto NetApp".
2. Scarica la zip dei certificati e delle chiavi di Astra Control Center dal "Sito di supporto NetApp".
3. (Facoltativo) utilizzare il seguente comando per verificare la firma del bundle:

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

4. Estrarre le immagini:

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

### Installare il plug-in NetApp Astra kubectl

NetApp Astra `kubectl` Il plug-in della riga di comando consente di risparmiare tempo durante l'esecuzione di attività comuni associate all'implementazione e all'aggiornamento di Astra Control Center.

#### Di cosa hai bisogno

NetApp fornisce binari per il 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. Sui sistemi operativi Linux e Mac, è possibile utilizzare `uname -a` per raccogliere queste informazioni.

#### Fasi

1. Elencare NetApp Astra disponibile `kubectl` Binari del plug-in e annotare il nome del file necessario per il sistema operativo e l'architettura della CPU:

```
ls kubectl-astra/
```

2. Copiare il file nella stessa posizione dello standard `kubectl` utility. In questo esempio, il `kubectl` l'utility si trova in `/usr/local/bin` directory. Sostituire `<binary-name>` con il nome del file desiderato:

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

### Aggiungere le immagini al registro locale

1. Passare alla directory Astra:

```
cd acc
```

2. Aggiungere i file nella directory dell'immagine di Astra Control Center al registro locale.

   Vedere gli script di esempio per il caricamento automatico delle immagini di seguito.

   a. Accedere al Registro di sistema:

      Docker:

```
docker login [your_registry_path]
```

      Podman:

```
podman login [your_registry_path]
```

   b. Utilizzare lo script appropriato per caricare le immagini, contrassegnare le immagini e inviare le immagini al registro locale:

      Docker:

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

      Podman:

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

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

1. 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
   ```

   Risposta:

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

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

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

   Esempio di risposta:

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

   c. Creare il `netapp-acc` namespace (o personalizzato).

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

   Esempio di risposta:

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

d. Creare un segreto per `netapp-acc` namespace (o personalizzato). Aggiungere informazioni su Docker ed eseguire il seguente comando:

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

Risposta

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

a. (opzionale) se si desidera che il cluster venga gestito automaticamente da Astra Control Center dopo l'installazione, assicurarsi di fornire il kubeconfig come segreto all'interno dello spazio dei nomi di Astra Control Center in cui si intende eseguire la distribuzione utilizzando questo comando:

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

**Installare l'operatore del centro di controllo Astra**

1. Modificare l'YAML di implementazione dell'operatore di Astra Control Center (`astra_control_center_operator_deploy.yaml`) per fare riferimento al registro locale e al segreto.

```
vim astra_control_center_operator_deploy.yaml
```

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

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

b. Cambiare `[your_registry_path]` per `kube-rbac-proxy` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

c. Cambiare `[your_registry_path]` per `acc-operator-controller-manager` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

d. (Per le installazioni che utilizzano l'anteprima di Astra Data Store) vedere questo problema noto relativo a. "Provisioning delle classi di storage e modifiche aggiuntive da apportare al programma YAML".

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

2. Installare l’operatore del centro di controllo Astra:

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

Esempio di risposta:

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

**Configurare Astra Control Center**

1. Modificare il file delle risorse personalizzate (CR) di Astra Control Center (`astra_control_center_min.yaml`) Per creare account, AutoSupport, Registro di sistema e altre configurazioni necessarie:

> Se sono necessarie personalizzazioni aggiuntive per il proprio ambiente, è possibile utilizzare `astra_control_center.yaml` Come CR alternativa. `astra_control_center_min.yaml` È il CR predefinito ed è adatto per la maggior parte delle installazioni.

```
vim astra_control_center_min.yaml
```

> Le proprietà configurate dal CR non possono essere modificate dopo l'implementazione iniziale di Astra Control Center.

> Se si utilizza un registro che non richiede autorizzazione, è necessario eliminare `secret` linea entro `imageRegistry` in caso negativo, l'installazione non riesce.

a. Cambiare `[your_registry_path]` al percorso del registro di sistema in cui sono state inviate le immagini nel passaggio precedente.

b. Modificare il `accountName` stringa al nome che si desidera associare all'account.

c. Modificare il `astraAddress` Stringa all'FQDN che si desidera utilizzare nel browser per accedere ad Astra. Non utilizzare `http://` oppure `https://` nell'indirizzo. Copiare questo FQDN per utilizzarlo in

un passo successivo.

d. Modificare il `email` stringa all'indirizzo iniziale predefinito dell'amministratore. Copiare questo indirizzo e-mail per utilizzarlo in passo successivo.

e. Cambiare `enrolled` Per AutoSupport a. `false` per i siti senza connettività internet o senza retain `true` per i siti connessi.

f. (Facoltativo) aggiungere un nome `firstName` e cognome `lastName` dell'utente associato all'account. È possibile eseguire questo passaggio ora o in un secondo momento all'interno dell'interfaccia utente.

g. (Facoltativo) modificare `storageClass` Valore per un'altra risorsa Trident storageClass, se richiesto dall'installazione.

h. (Facoltativo) se si desidera che il cluster venga gestito automaticamente da Astra Control Center dopo l'installazione e si è già provveduto creato il segreto contenente il kubeconfig per questo cluster, Fornire il nome del segreto aggiungendo un nuovo campo a questo file YAML chiamato `astraKubeConfigSecret: "acc-kubeconfig-cred or custom secret name"`

i. Completare una delle seguenti operazioni:

   - **Other ingress controller (ingressType:Generic)**: Questa è l'azione predefinita con Astra Control Center. Dopo l'implementazione di Astra Control Center, è necessario configurare il controller di ingresso per esporre Astra Control Center con un URL.

     L'installazione predefinita di Astra Control Center imposta il gateway (`service/traefik`) per essere del tipo `ClusterIP`. Questa installazione predefinita richiede l'impostazione di Kubernetes IngressController/Ingress per instradare il traffico verso di essa. Se si desidera utilizzare un ingresso, vedere "Impostare l'ingresso per il bilanciamento del carico".

   - **Service load balancer (ingressType:AccTraefik)**: Se non si desidera installare un IngressController o creare una risorsa Ingress, impostare `ingressType` a. `AccTraefik`.

     In questo modo viene implementato l'Astra Control Center `traefik` Gateway come servizio di tipo Kubernetes LoadBalancer.

     Astra Control Center utilizza un servizio del tipo "LoadBalancer" (`svc/traefik` Nello spazio dei nomi di Astra Control Center) e richiede l'assegnazione di un indirizzo IP esterno accessibile. Se nel proprio ambiente sono consentiti i bilanciatori di carico e non ne è già configurato uno, è possibile utilizzare MetalLB o un altro servizio di bilanciamento del carico esterno per assegnare un indirizzo IP esterno al servizio. Nella configurazione del server DNS interno, puntare il nome DNS scelto per Astra Control Center sull'indirizzo IP con bilanciamento del carico.

     > Per ulteriori informazioni sul tipo di servizio "LoadBalancer" e sull'ingresso, vedere "Requisiti".

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

#### 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]
   ```

   Esempio di risposta:

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

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

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

   Esempio di risposta:

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

### Verificare lo stato del sistema

Se preferisci utilizzare OpenShift, puoi utilizzare comandi oc paragonabili per le fasi di verifica.

1. 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.

Esempio di risposta:

```
NAME                                        READY   STATUS    RESTARTS
AGE
acc-helm-repo-5f75c5f564-bzqmt              1/1     Running   0
11m
activity-6b8f7cccb9-mlrn4                   1/1     Running   0
9m2s
api-token-authentication-6hznt              1/1     Running   0
8m50s
api-token-authentication-qpfgb              1/1     Running   0
8m50s
api-token-authentication-sqnb7              1/1     Running   0
8m50s
asup-5578bbdd57-dxkbp                       1/1     Running   0
9m3s
authentication-56bff4f95d-mspmq             1/1     Running   0
7m31s
bucketservice-6f7968b95d-9rrrl              1/1     Running   0
8m36s
cert-manager-5f6cf4bc4b-82khn               1/1     Running   0
6m19s
cert-manager-cainjector-76cf976458-sdrbc    1/1     Running   0
6m19s
cert-manager-webhook-5b7896bfd8-2n45j       1/1     Running   0
6m19s
cloud-extension-749d9f684c-8bdhq            1/1     Running   0
9m6s
cloud-insights-service-7d58687d9-h5tzw      1/1     Running   2
8m56s
composite-compute-968c79cb5-nv7l4           1/1     Running   0
9m11s
composite-volume-7687569985-jg9gg           1/1     Running   0
8m33s
credentials-5c9b75f4d6-nx9cz                1/1     Running   0
```

```
8m42s
entitlement-6c96fd8b78-zt7f8                1/1     Running   0
8m28s
features-5f7bfc9f68-gsjnl                   1/1     Running   0
8m57s
fluent-bit-ds-h88p7                         1/1     Running   0
7m22s
fluent-bit-ds-krhnj                         1/1     Running   0
7m23s
fluent-bit-ds-l5bjj                         1/1     Running   0
7m22s
fluent-bit-ds-lrclb                         1/1     Running   0
7m23s
fluent-bit-ds-s5t4n                         1/1     Running   0
7m23s
fluent-bit-ds-zpr6v                         1/1     Running   0
7m22s
graphql-server-5f5976f4bd-vbb4z             1/1     Running   0
7m13s
identity-56f78b8f9f-8h9p9                   1/1     Running   0
8m29s
influxdb2-0                                 1/1     Running   0
11m
krakend-6f8d995b4d-5khkl                    1/1     Running   0
7m7s
license-5b5db87c97-jmxzc                    1/1     Running   0
9m
login-ui-57b57c74b8-6xtv7                   1/1     Running   0
7m10s
loki-0                                      1/1     Running   0
11m
monitoring-operator-9dbc9c76d-8znck         2/2     Running   0
7m33s
nats-0                                      1/1     Running   0
11m
nats-1                                      1/1     Running   0
10m
nats-2                                      1/1     Running   0
10m
nautilus-6b9d88bc86-h8kfb                   1/1     Running   0
8m6s
nautilus-6b9d88bc86-vn68r                   1/1     Running   0
8m35s
openapi-b87d77dd8-5dz9h                     1/1     Running   0
9m7s
polaris-consul-consul-5ljfb                 1/1     Running   0
```

```
11m
polaris-consul-consul-s5d5z                1/1     Running   0
11m
polaris-consul-consul-server-0             1/1     Running   0
11m
polaris-consul-consul-server-1             1/1     Running   0
11m
polaris-consul-consul-server-2             1/1     Running   0
11m
polaris-consul-consul-twmpq                1/1     Running   0
11m
polaris-mongodb-0                          2/2     Running   0
11m
polaris-mongodb-1                          2/2     Running   0
10m
polaris-mongodb-2                          2/2     Running   0
10m
polaris-ui-84dc87847f-zrg8w                1/1     Running   0
7m12s
polaris-vault-0                            1/1     Running   0
11m
polaris-vault-1                            1/1     Running   0
11m
polaris-vault-2                            1/1     Running   0
11m
public-metrics-657698b66f-67pgt            1/1     Running   0
8m47s
storage-backend-metrics-6848b9fd87-w7x8r   1/1     Running   0
8m39s
storage-provider-5ff5868cd5-r9hj7          1/1     Running   0
8m45s
telegraf-ds-dw4hg                          1/1     Running   0
7m23s
telegraf-ds-k92gn                          1/1     Running   0
7m23s
telegraf-ds-mmxjl                          1/1     Running   0
7m23s
telegraf-ds-nhs8s                          1/1     Running   0
7m23s
telegraf-ds-rj7lw                          1/1     Running   0
7m23s
telegraf-ds-tqrkb                          1/1     Running   0
7m23s
telegraf-rs-9mwgj                          1/1     Running   0
7m23s
telemetry-service-56c49d689b-ffrzx         1/1     Running   0
```

```
8m42s
tenancy-767c77fb9d-g9ctv                    1/1     Running   0
8m52s
traefik-5857d87f85-7pmx8                    1/1     Running   0
6m49s
traefik-5857d87f85-cpxgv                    1/1     Running   0
5m34s
traefik-5857d87f85-lvmlb                    1/1     Running   0
4m33s
traefik-5857d87f85-t2xlk                    1/1     Running   0
4m33s
traefik-5857d87f85-v9wpf                    1/1     Running   0
7m3s
trident-svc-595f84dd78-zb8l6                1/1     Running   0
8m54s
vault-controller-86c94fbf4f-krttq           1/1     Running   0
9m24s
```

2. (Facoltativo) per assicurarsi che l'installazione sia completata, è possibile guardare `acc-operator` registra usando il seguente comando.

```
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 attraverso il flusso di lavoro add cluster "Nell'interfaccia utente" O API.

3. Una volta eseguiti tutti i pod, verificare che l'installazione sia riuscita recuperando `AstraControlCenter` Istanza installata dall'operatore di Astra Control Center.

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

4. Nell'YAML, selezionare `status.deploymentState` nella risposta per `Deployed` valore. Se l'implementazione non ha avuto esito positivo, viene visualizzato un messaggio di errore.
5. Per ottenere la password monouso da utilizzare quando si accede ad Astra Control Center, copiare il `status.uuid` valore. La password è `ACC-` Seguito dal valore UUID (`ACC-[UUID]` oppure, in questo esempio, `ACC-9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f`).

**Dettagli YAML di esempio**

```
name: astra
   namespace: netapp-acc
   resourceVersion: "104424560"
   selfLink: /apis/astra.netapp.io/v1/namespaces/netapp-
acc/astracontrolcenters/astra
   uid: 9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f
 spec:
   accountName: Example
   astraAddress: astra.example.com
   astraVersion: 21.12.60
   autoSupport:
     enrolled: true
     url: https://support.netapp.com/asupprod/post/1.0/postAsup
   crds: {}
   email: admin@example.com
   firstName: SRE
   imageRegistry:
     name: registry_name/astra
     secret: astra-registry-cred
   lastName: Admin
 status:
   accConditionHistory:
     items:
     - astraVersion: 21.12.60
       condition:
         lastTransitionTime: "2021-11-23T02:23:59Z"
         message: Deploying is currently in progress.
         reason: InProgress
         status: "False"
         type: Ready
       generation: 2
       observedSpec:
         accountName: Example
         astraAddress: astra.example.com
         astraVersion: 21.12.60
         autoSupport:
           enrolled: true
           url: https://support.netapp.com/asupprod/post/1.0/postAsup
         crds: {}
         email: admin@example.com
         firstName: SRE
         imageRegistry:
           name: registry_name/astra
           secret: astra-registry-cred
```

```
        lastName: Admin
      timestamp: "2021-11-23T02:23:59Z"
    - astraVersion: 21.12.60
      condition:
        lastTransitionTime: "2021-11-23T02:23:59Z"
        message: Deploying is currently in progress.
        reason: InProgress
        status: "True"
        type: Deploying
      generation: 2
      observedSpec:
        accountName: Example
        astraAddress: astra.example.com
        astraVersion: 21.12.60
        autoSupport:
          enrolled: true
          url: https://support.netapp.com/asupprod/post/1.0/postAsup
        crds: {}
        email: admin@example.com
        firstName: SRE
        imageRegistry:
          name: registry_name/astra
          secret: astra-registry-cred
        lastName: Admin
      timestamp: "2021-11-23T02:23:59Z"
    - astraVersion: 21.12.60
      condition:
        lastTransitionTime: "2021-11-23T02:29:41Z"
        message: Post Install was successful
        observedGeneration: 2
        reason: Complete
        status: "True"
        type: PostInstallComplete
      generation: 2
      observedSpec:
        accountName: Example
        astraAddress: astra.example.com
        astraVersion: 21.12.60
        autoSupport:
          enrolled: true
          url: https://support.netapp.com/asupprod/post/1.0/postAsup
        crds: {}
        email: admin@example.com
        firstName: SRE
        imageRegistry:
          name: registry_name/astra
```

```
          secret: astra-registry-cred
        lastName: Admin
      timestamp: "2021-11-23T02:29:41Z"
    - astraVersion: 21.12.60
      condition:
        lastTransitionTime: "2021-11-23T02:29:41Z"
        message: Deploying succeeded.
        reason: Complete
        status: "False"
        type: Deploying
      generation: 2
      observedGeneration: 2
      observedSpec:
        accountName: Example
        astraAddress: astra.example.com
        astraVersion: 21.12.60
        autoSupport:
          enrolled: true
          url: https://support.netapp.com/asupprod/post/1.0/postAsup
        crds: {}
        email: admin@example.com
        firstName: SRE
        imageRegistry:
          name: registry_name/astra
          secret: astra-registry-cred
        lastName: Admin
      observedVersion: 21.12.60
      timestamp: "2021-11-23T02:29:41Z"
    - astraVersion: 21.12.60
      condition:
        lastTransitionTime: "2021-11-23T02:29:41Z"
        message: Astra is deployed
        reason: Complete
        status: "True"
        type: Deployed
      generation: 2
      observedGeneration: 2
      observedSpec:
        accountName: Example
        astraAddress: astra.example.com
        astraVersion: 21.12.60
        autoSupport:
          enrolled: true
          url: https://support.netapp.com/asupprod/post/1.0/postAsup
        crds: {}
        email: admin@example.com
```

```
        firstName: SRE
        imageRegistry:
          name: registry_name/astra
          secret: astra-registry-cred
        lastName: Admin
      observedVersion: 21.12.60
      timestamp: "2021-11-23T02:29:41Z"
    - astraVersion: 21.12.60
      condition:
        lastTransitionTime: "2021-11-23T02:29:41Z"
        message: Astra is deployed
        reason: Complete
        status: "True"
        type: Ready
      generation: 2
      observedGeneration: 2
      observedSpec:
        accountName: Example
        astraAddress: astra.example.com
        astraVersion: 21.12.60
        autoSupport:
          enrolled: true
          url: https://support.netapp.com/asupprod/post/1.0/postAsup
        crds: {}
        email: admin@example.com
        firstName: SRE
        imageRegistry:
          name: registry_name/astra
          secret: astra-registry-cred
        lastName: Admin
      observedVersion: 21.12.60
      timestamp: "2021-11-23T02:29:41Z"
  certManager: deploy
  cluster:
    type: OCP
    vendorVersion: 4.7.5
    version: v1.20.0+bafe72f
  conditions:
  - lastTransitionTime: "2021-12-08T16:19:55Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Ready
  - lastTransitionTime: "2021-12-08T16:19:55Z"
    message: Deploying succeeded.
    reason: Complete
```

```
      status: "False"
      type: Deploying
    - lastTransitionTime: "2021-12-08T16:19:53Z"
      message: Post Install was successful
      observedGeneration: 2
      reason: Complete
      status: "True"
      type: PostInstallComplete
    - lastTransitionTime: "2021-12-08T16:19:55Z"
      message: Astra is deployed
      reason: Complete
      status: "True"
      type: Deployed
    deploymentState: Deployed
    observedGeneration: 2
    observedSpec:
      accountName: Example
      astraAddress: astra.example.com
      astraVersion: 21.12.60
      autoSupport:
        enrolled: true
        url: https://support.netapp.com/asupprod/post/1.0/postAsup
      crds: {}
      email: admin@example.com
      firstName: SRE
      imageRegistry:
        name: registry_name/astra
        secret: astra-registry-cred
      lastName: Admin
    observedVersion: 21.12.60
    postInstall: Complete
    uuid: 9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f
kind: List
metadata:
 resourceVersion: ""
 selfLink: ""
```

#### Impostare l’ingresso per il bilanciamento del carico

È possibile configurare un controller di ingresso Kubernetes che gestisce l’accesso esterno ai servizi, come il bilanciamento del carico in un cluster.

Questa procedura spiega come configurare un controller di ingresso (`ingressType:Generic`). Questa è l’azione predefinita con Astra Control Center. Dopo l’implementazione di Astra Control Center, è necessario configurare il controller di ingresso per esporre Astra Control Center con un URL.

> Se non si desidera configurare un controller di ingresso, è possibile impostarlo `ingressType:AccTraefik)`. Astra Control Center utilizza un servizio del tipo "LoadBalancer" (`svc/traefik` Nello spazio dei nomi di Astra Control Center) e richiede l'assegnazione di un indirizzo IP esterno accessibile. Se nel proprio ambiente sono consentiti i bilanciatori di carico e non ne è già configurato uno, è possibile utilizzare MetalLB o un altro servizio di bilanciamento del carico esterno per assegnare un indirizzo IP esterno al servizio. Nella configurazione del server DNS interno, puntare il nome DNS scelto per Astra Control Center sull'indirizzo IP con bilanciamento del carico. Per ulteriori informazioni sul tipo di servizio "LoadBalancer" e sull'ingresso, vedere "Requisiti".

I passaggi variano a seconda del tipo di controller di ingresso utilizzato:

- Controller di ingresso nginx
- Controller di ingresso OpenShift

**Di cosa hai bisogno**

- Il necessario "controller di ingresso" dovrebbe essere già implementato.
- Il "classe di ingresso" corrispondente al controller di ingresso dovrebbe già essere creato.
- Si stanno utilizzando versioni di Kubernetes comprese tra v1.19 e v1.22.

**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 income in `netapp-acc` (o con nome personalizzato) namespace utilizzando `v1beta1` (Obsoleto in Kubernetes versione inferiore a o 1.22) o. `v1` tipo di risorsa per uno schema obsoleto o nuovo:
   a. Per a. `v1beta1` schema obsoleto, seguire questo esempio:

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

b. Per `v1` nuovo schema, seguire 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 addess>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

**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, si modifica la password dell'amministratore predefinito e si accede alla dashboard dell'interfaccia utente di Astra Control Center.

**Fasi**

1. In un browser, immettere l'FQDN utilizzato in `astraAddress` in `astra_control_center_min.yaml` CR quando Astra Control Center è stato installato.
2. Accettare i certificati autofirmati quando 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_min.yaml` CR quando Astra Control Center è stato installato, seguito dalla password monouso (`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 ancora stati creati altri account utente amministrativi, contattare il 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.

#### Fasi

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

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

#### Cosa succederà

Completare l'implementazione eseguendo "attività di installazione".

## Installare Astra Control Center utilizzando OpenShift OperatorHub

Se utilizzi Red Hat OpenShift, puoi installare Astra Control Center usando l'operatore certificato Red Hat. Seguire questa procedura per installare Astra Control Center da "Catalogo Red Hat Ecosystem" Oppure utilizzando Red Hat OpenShift Container Platform.

Una volta completata questa procedura, tornare alla procedura di installazione per completare la "fasi rimanenti" per verificare che l'installazione sia riuscita e accedere.

#### Di cosa hai bisogno

- "Prima di iniziare l'installazione, preparare l'ambiente per l'implementazione di Astra Control Center".
- Dal tuo cluster OpenShift, assicurati che tutti gli operatori del cluster siano in buono stato (`available` è `true`):

```
oc get clusteroperators
```

- Dal cluster OpenShift, assicurati che tutti i servizi API siano in buono stato (`available` è `true`):

```
oc get apiservices
```

- Hai creato un indirizzo FQDN per Astra Control Center nel tuo data center.
- Hai i permessi necessari e l'accesso alla piattaforma container Red Hat OpenShift per eseguire le fasi di installazione descritte.

**Fasi**

- Scarica e disimballa il bundle Astra Control Center
- Installare il plug-in NetApp Astra kubectl
- Aggiungere le immagini al registro locale
- Individuare la pagina di installazione dell'operatore
- Installare l'operatore
- Installare Astra Control Center

### Scarica e disimballa il bundle Astra Control Center

1. Scarica il bundle Astra Control Center (`astra-control-center-[version].tar.gz`) da "Sito di supporto NetApp".
2. Scarica la zip dei certificati e delle chiavi di Astra Control Center dal "Sito di supporto NetApp".
3. (Facoltativo) utilizzare il seguente comando per verificare la firma del bundle:

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

4. Estrarre le immagini:

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

### Installare il plug-in NetApp Astra kubectl

NetApp Astra `kubectl` Il plug-in della riga di comando consente di risparmiare tempo durante l'esecuzione di attività comuni associate all'implementazione e all'aggiornamento di Astra Control Center.

**Di cosa hai bisogno**

NetApp fornisce binari per il 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. Sui sistemi operativi Linux e Mac, è possibile utilizzare `uname -a` per raccogliere queste informazioni.

**Fasi**

1. Elencare NetApp Astra disponibile `kubectl` Binari del plug-in e annotare il nome del file necessario per il sistema operativo e l'architettura della CPU:

```
ls kubectl-astra/
```

2. Copiare il file nella stessa posizione dello standard `kubectl` utility. In questo esempio, il `kubectl` l'utility si trova in `/usr/local/bin` directory. Sostituire `<binary-name>` con il nome del file desiderato:

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

**Aggiungere le immagini al registro locale**

1. Passare alla directory Astra:

```
cd acc
```

2. Aggiungere i file nella directory dell'immagine di Astra Control Center al registro locale.

   Vedere gli script di esempio per il caricamento automatico delle immagini di seguito.

   a. Accedere al Registro di sistema:

      Docker:

```
docker login [your_registry_path]
```

      Podman:

```
podman login [your_registry_path]
```

   b. Utilizzare lo script appropriato per caricare le immagini, contrassegnare le immagini e inviare le immagini al registro locale:

      Docker:

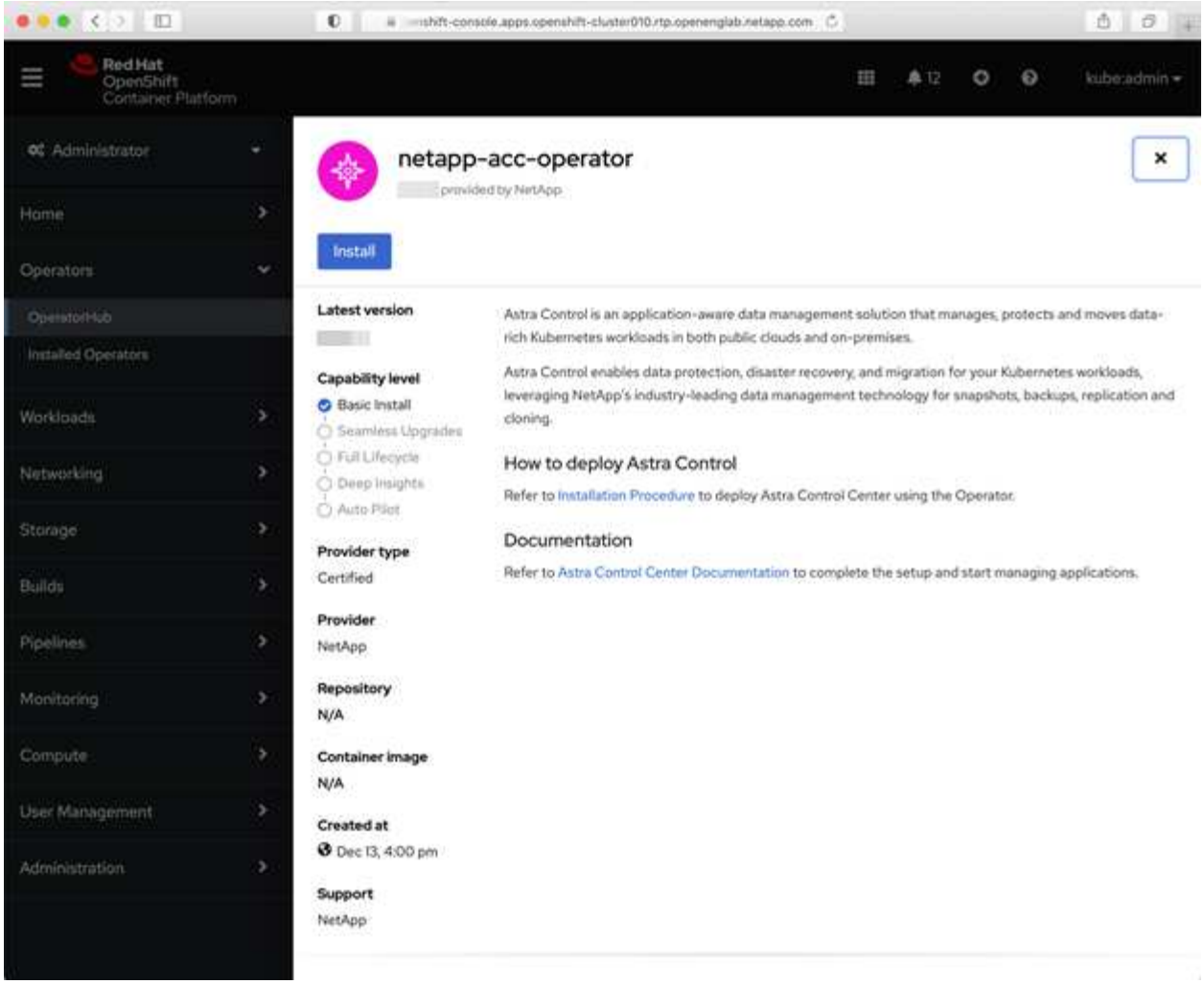
```
export REGISTRY=[Docker_registry_path]
for astraImageFile in $(ls images/*.tar) ; do
  # Load to local cache. And store the name of the loaded image
trimming the 'Loaded images: '
  astraImage=$(docker load --input ${astraImageFile} | sed 's/Loaded
image: //')
  astraImage=$(echo ${astraImage} |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

Podman:

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

**Individuare la pagina di installazione dell'operatore**

1. Completare una delle seguenti procedure per accedere alla pagina di installazione dell'operatore:
   - Dalla console Web Red Hat OpenShift:



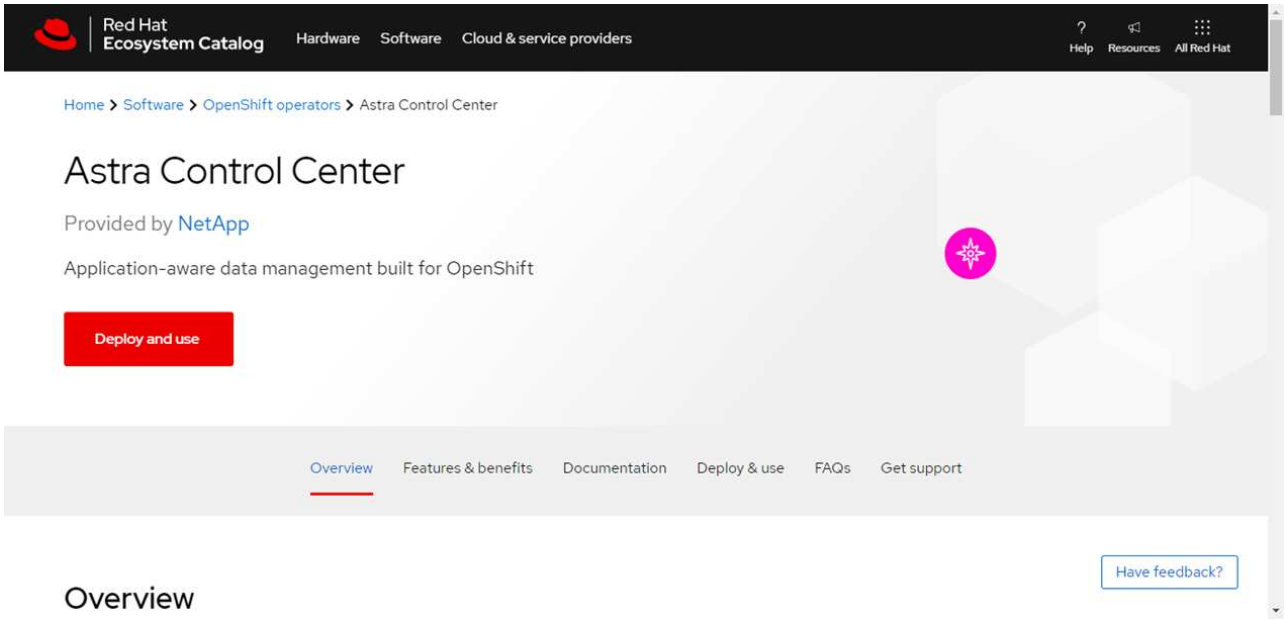

i. Accedere all'interfaccia utente di OpenShift Container Platform.

ii. Dal menu laterale, selezionare **Operator (operatori) > OperatorHub**.

iii. Selezionare l'operatore di NetApp Astra Control Center.

iv. Selezionare **Installa**.

- Dal Red Hat Ecosystem Catalog:




i. Selezionare NetApp Astra Control Center "operatore".

ii. Selezionare **Deploy and Use** (implementazione e utilizzo).

### Installare l'operatore

1. Completare la pagina **Install Operator** (Installazione operatore) e installare l'operatore:

> L'operatore sarà disponibile in tutti gli spazi dei nomi dei cluster.

   a. Selezionare lo spazio dei nomi dell'operatore o. `netapp-acc-operator` lo spazio dei nomi verrà creato automaticamente come parte dell'installazione dell'operatore.

   b. Selezionare una strategia di approvazione manuale o automatica.

> Si consiglia l'approvazione manuale. Per ogni cluster dovrebbe essere in esecuzione una sola istanza dell'operatore.

   c. Selezionare **Installa**.

> Se è stata selezionata una strategia di approvazione manuale, verrà richiesto di approvare il piano di installazione manuale per questo operatore.

2. Dalla console, accedere al menu OperatorHub e verificare che l'installazione dell'operatore sia stata eseguita correttamente.

### Installare Astra Control Center

1. Dalla console nella vista dettagli dell'operatore Astra Control Center, selezionare `Create instance` Nella sezione API fornite.

2. Completare il `Create AstraControlCenter` campo del modulo:

   a. Mantenere o regolare il nome di Astra Control Center.

   b. (Facoltativo) attivare o disattivare il supporto automatico. Si consiglia di mantenere la funzionalità di supporto automatico.

c. Inserire l'indirizzo di Astra Control Center. Non entrare `http://` oppure `https://` nell'indirizzo.
d. Inserire la versione di Astra Control Center, ad esempio 21.12.60.
e. Immettere un nome account, un indirizzo e-mail e un cognome amministratore.
f. Mantenere la policy di recupero del volume predefinita.
g. In **Image Registry**, immettere il percorso locale del Registro di sistema dell'immagine container. Non entrare `http://` oppure `https://` nell'indirizzo.
h. Se si utilizza un registro che richiede l'autenticazione, immettere il segreto.
i. Inserire il nome admin.
j. Configurare la scalabilità delle risorse.
k. Mantenere la classe di storage predefinita.
l. Definire le preferenze di gestione CRD.

3. Selezionare `Create`.

#### Cosa succederà

Verificare che Astra Control Center sia stato installato correttamente e completare il "fasi rimanenti" per accedere. Inoltre, completerai l'implementazione eseguendo anche questa operazione "attività di installazione".

## Installare il centro di controllo Astra con un backend di storage Cloud Volumes ONTAP

Con Astra Control Center, puoi gestire le tue app in un ambiente di cloud ibrido con cluster Kubernetes e istanze di Cloud Volumes ONTAP autogestiti. Puoi implementare Astra Control Center nei tuoi cluster Kubernetes on-premise o in uno dei cluster Kubernetes autogestiti nell'ambiente cloud.

Con una di queste implementazioni, è possibile eseguire operazioni di gestione dei dati delle applicazioni utilizzando Cloud Volumes ONTAP come back-end dello storage. È inoltre possibile configurare un bucket S3 come destinazione del backup.

Per installare Astra Control Center in Amazon Web Services (AWS) e Microsoft Azure con un backend di storage Cloud Volumes ONTAP, eseguire i seguenti passaggi a seconda dell'ambiente cloud in uso.

- Implementare Astra Control Center in Amazon Web Services
- Implementare Astra Control Center in Microsoft Azure

### Implementare Astra Control Center in Amazon Web Services

Puoi implementare Astra Control Center su un cluster Kubernetes autogestito ospitato su un cloud pubblico Amazon Web Services (AWS).

Solo i cluster OpenShift Container Platform (OCP) autogestiti sono supportati per l'implementazione di Astra Control Center.

#### Ciò di cui hai bisogno per AWS

Prima di implementare Astra Control Center in AWS, sono necessari i seguenti elementi:

- Licenza Astra Control Center. Vedere "Requisiti di licenza di Astra Control Center".

- "Soddisfare i requisiti di Astra Control Center".
- Account NetApp Cloud Central
- Autorizzazioni Red Hat OpenShift Container Platform (OCP) (a livello di spazio dei nomi per la creazione di pod)
- Credenziali AWS, Access ID e Secret Key con autorizzazioni che consentono di creare bucket e connettori
- Accesso e login al Registro dei container elastici (ECR) dell'account AWS
- Per accedere all'interfaccia utente di Astra Control, è necessario immettere AWS Hosted zone e Route 53

#### Requisiti dell'ambiente operativo per AWS

Astra Control Center richiede il seguente ambiente operativo per AWS:

- Red Hat OpenShift Container Platform 4.8

> Assicurarsi che l'ambiente operativo scelto per ospitare Astra Control Center soddisfi i requisiti di base delle risorse descritti nella documentazione ufficiale dell'ambiente.

Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse dell'ambiente:

| Componente | Requisito |
|---|---|
| **Capacità di storage NetApp Cloud Volumes ONTAP di back-end** | Almeno 300 GB disponibili |
| **Nodi di lavoro (requisito AWS EC2)** | Almeno 3 nodi di lavoro in totale, con 4 core vCPU e 12 GB di RAM ciascuno |
| **Bilanciamento del carico** | Tipo di servizio "LoadBalancer" disponibile per il traffico in ingresso da inviare ai servizi nel cluster dell'ambiente operativo |
| **FQDN** | Metodo per indirizzare l'FQDN di Astra Control Center all'indirizzo IP con bilanciamento del carico |
| **Astra Trident (installato come parte del rilevamento dei cluster Kubernetes in NetApp Cloud Manager)** | Astra Trident 21.04 o versione successiva installata e configurata e NetApp ONTAP versione 9.5 o successiva come backend di storage |
| **Registro delle immagini** | È necessario disporre di un registro privato esistente, ad esempio AWS Elastic Container Registry, in cui è possibile trasferire le immagini di build di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui verranno caricate le immagini.<br><br>Il cluster ospitato da Astra Control Center e il cluster gestito devono avere accesso alla stessa immagine di registro per poter eseguire il backup e il ripristino delle applicazioni utilizzando l'immagine basata su Restic. |

| Componente | Requisito |
| --- | --- |
| **Configurazione di Astra Trident/ONTAP** | Astra Control Center richiede la creazione e l'impostazione di una classe di storage come classe di storage predefinita. Il centro di controllo Astra supporta le seguenti classi di storage Kubernetes create quando si importa il cluster Kubernetes in ONTAP. Questi sono forniti da Astra Trident:<br>• `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io`<br>• `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io`<br>• `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io`<br>• `vsaworkingenvironment-<>-single-san csi.trident.netapp.io` |

Questi requisiti presuppongono che Astra Control Center sia l'unica applicazione in esecuzione nell'ambiente operativo. Se nell'ambiente sono in esecuzione applicazioni aggiuntive, modificare di conseguenza questi requisiti minimi.

Il token del Registro di sistema AWS scade tra 12 ore, dopodiché sarà necessario rinnovare il segreto del Registro di sistema dell'immagine Docker.

#### Panoramica dell'implementazione per AWS

Di seguito viene fornita una panoramica del processo di installazione di Astra Control Center per AWS con Cloud Volumes ONTAP come backend di storage.

Ciascuna di queste fasi viene illustrata più dettagliatamente di seguito.

1. Assicurarsi di disporre di autorizzazioni IAM sufficienti.
2. Installare un cluster RedHat OpenShift su AWS.
3. Configurare AWS.
4. Configurare NetApp Cloud Manager.
5. Installare Astra Control Center.

#### Assicurarsi di disporre di autorizzazioni IAM sufficienti

Assicurarsi di disporre di ruoli e autorizzazioni IAM sufficienti per installare un cluster RedHat OpenShift e un connettore NetApp Cloud Manager.

Vedere "Credenziali AWS iniziali".

#### Installare un cluster RedHat OpenShift su AWS

Installare un cluster RedHat OpenShift Container Platform su AWS.

Per istruzioni sull'installazione, vedere "Installazione di un cluster su AWS in OpenShift Container Platform".

#### Configurare AWS

Quindi, configurare AWS per creare una rete virtuale, configurare istanze di calcolo EC2, creare un bucket AWS S3, creare un Elastic Container Register (ECR) per ospitare le immagini di Astra Control Center e inviare le immagini a questo registro.

Seguire la documentazione di AWS per completare i seguenti passaggi. Vedere "Documentazione di installazione di AWS".

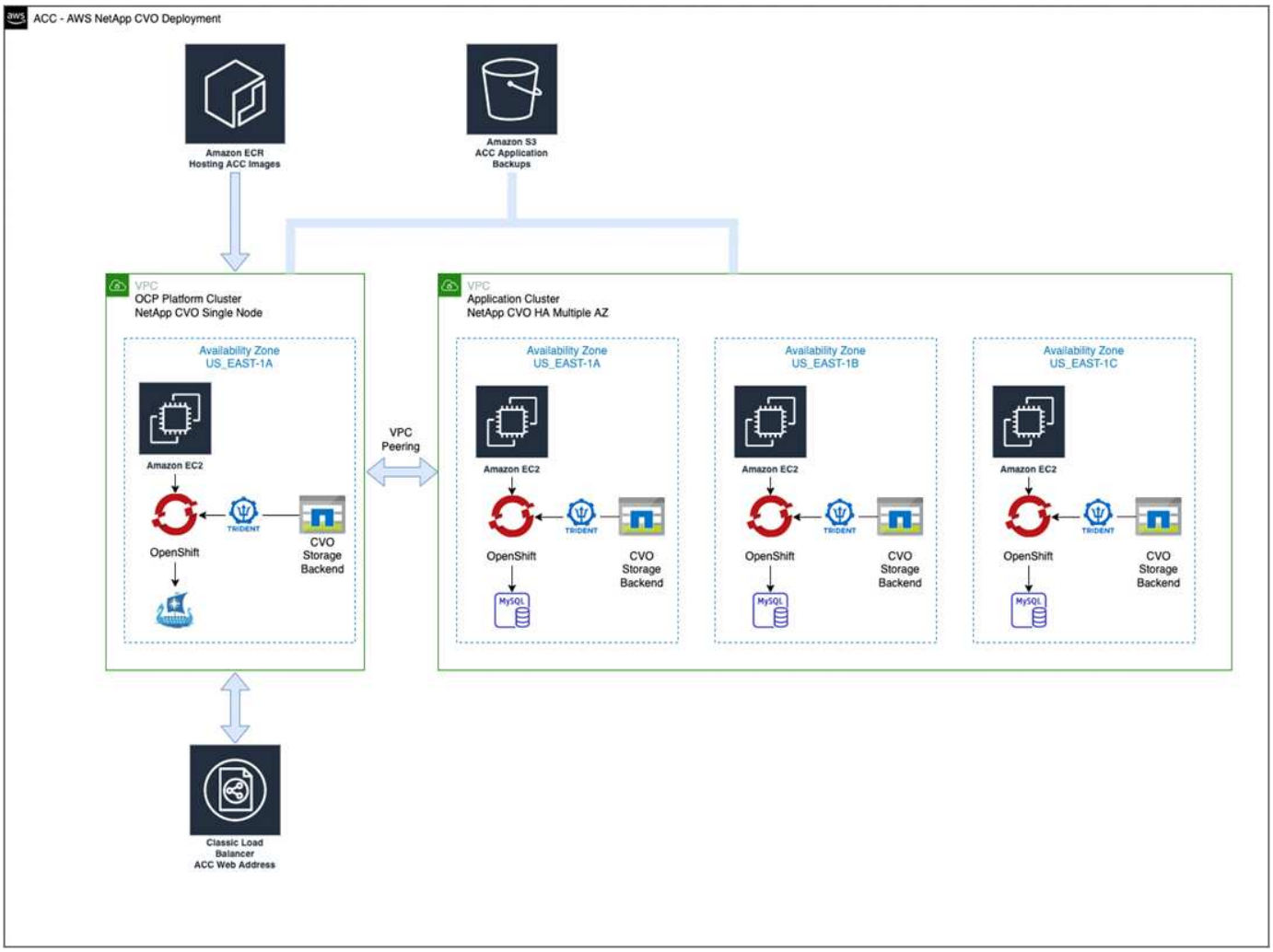
1. Creare una rete virtuale AWS.
2. Esaminare le istanze di calcolo EC2. Può trattarsi di un server bare metal o di macchine virtuali in AWS.
3. Se il tipo di istanza non corrisponde già ai requisiti minimi di risorsa Astra per i nodi master e worker, modificare il tipo di istanza in AWS per soddisfare i requisiti Astra. Vedere "Requisiti di Astra Control Center".
4. Creare almeno un bucket AWS S3 per memorizzare i backup.
5. Creare un AWS Elastic Container Registry (ECR) per ospitare tutte le immagini ACC.

> Se non si crea ECR, il centro di controllo Astra non può accedere ai dati di monitoraggio da un cluster contenente Cloud Volumes ONTAP con un backend AWS. Il problema si verifica quando il cluster che si tenta di rilevare e gestire utilizzando Astra Control Center non dispone dell'accesso ad AWS ECR.

6. Trasferire le immagini ACC nel registro definito.

> Il token AWS Elastic Container Registry (ECR) scade dopo 12 ore e causa il fallimento delle operazioni di cloni tra cluster. Questo problema si verifica quando si gestisce un backend di storage da Cloud Volumes ONTAP configurato per AWS. Per correggere questo problema, autenticare nuovamente con ECR e generare un nuovo segreto per la ripresa delle operazioni di clonazione.

Ecco un esempio di implementazione di AWS:




**Configurare NetApp Cloud Manager**

Utilizzando Cloud Manager, creare un'area di lavoro, aggiungere un connettore ad AWS, creare un ambiente di lavoro e importare il cluster.

Seguire la documentazione di Cloud Manager per completare i seguenti passaggi. Vedere quanto segue:

- "Introduzione a Cloud Volumes ONTAP in AWS".
- "Creare un connettore in AWS utilizzando Cloud Manager"

**Fasi**

1. Aggiungi le tue credenziali a Cloud Manager.
2. Creare un'area di lavoro.
3. Aggiungere un connettore per AWS. Scegliere AWS come provider.
4. Crea un ambiente di lavoro per il tuo ambiente cloud.
   a. Location: "Amazon Web Services (AWS)"
   b. Tipo: "Cloud Volumes ONTAP ha"
5. Importare il cluster OpenShift. Il cluster si connetterà all'ambiente di lavoro appena creato.
   a. Per visualizzare i dettagli del cluster NetApp, selezionare **K8s** > **elenco cluster** > **Dettagli cluster**.

b. Nell'angolo in alto a destra, prendere nota della versione di Trident.

c. Si noti che le classi di storage cluster Cloud Volumes ONTAP mostrano NetApp come provider.

   In questo modo, il cluster Red Hat OpenShift viene importato e viene assegnata una classe di storage predefinita. Selezionare la classe di storage. Trident viene installato automaticamente come parte del processo di importazione e rilevamento.

6. Tenere presenti tutti i volumi e i volumi persistenti in questa implementazione di Cloud Volumes ONTAP.

> Cloud Volumes ONTAP può funzionare come nodo singolo o in alta disponibilità. Se ha è attivato, annotare lo stato ha e lo stato di implementazione del nodo in esecuzione in AWS.

#### Installare Astra Control Center

Seguire lo standard "Istruzioni di installazione di Astra Control Center".

### Implementare Astra Control Center in Microsoft Azure

Puoi implementare Astra Control Center su un cluster Kubernetes autogestito ospitato su un cloud pubblico Microsoft Azure.

#### Ciò di cui hai bisogno per Azure

Prima di implementare Astra Control Center in Azure, sono necessari i seguenti elementi:

- Licenza Astra Control Center. Vedere "Requisiti di licenza di Astra Control Center".
- "Soddisfare i requisiti di Astra Control Center".
- Account NetApp Cloud Central
- Red Hat OpenShift Container Platform (OCP) 4.8
- Autorizzazioni Red Hat OpenShift Container Platform (OCP) (a livello di spazio dei nomi per la creazione di pod)
- Credenziali Azure con autorizzazioni che consentono di creare bucket e connettori

#### Requisiti dell'ambiente operativo per Azure

Assicurarsi che l'ambiente operativo scelto per ospitare Astra Control Center soddisfi i requisiti di base delle risorse descritti nella documentazione ufficiale dell'ambiente.

Astra Control Center richiede le seguenti risorse oltre ai requisiti delle risorse dell'ambiente:

Vedere "Requisiti dell'ambiente operativo di Astra Control Center".

| Componente | Requisito |
|---|---|
| **Capacità di storage NetApp Cloud Volumes ONTAP di back-end** | Almeno 300 GB disponibili |
| **Nodi di lavoro (requisito di calcolo di Azure)** | Almeno 3 nodi di lavoro in totale, con 4 core vCPU e 12 GB di RAM ciascuno |

| Componente | Requisito |
| --- | --- |
| **Bilanciamento del carico** | Tipo di servizio "LoadBalancer" disponibile per il traffico in ingresso da inviare ai servizi nel cluster dell'ambiente operativo |
| **FQDN (Azure DNS zone)** | Metodo per indirizzare l'FQDN di Astra Control Center all'indirizzo IP con bilanciamento del carico |
| **Astra Trident (installato come parte del rilevamento dei cluster Kubernetes in NetApp Cloud Manager)** | Astra Trident 21.04 o versione successiva installata e configurata e NetApp ONTAP versione 9.5 o successiva verrà utilizzato come backend di storage |
| **Registro delle immagini** | È necessario disporre di un registro privato esistente, ad esempio Azure Container Registry (ACR), in cui è possibile trasferire le immagini di build di Astra Control Center. È necessario fornire l'URL del registro delle immagini in cui verranno caricate le immagini.<br><br>È necessario abilitare l'accesso anonimo per estrarre le immagini Restic per i backup. |
| **Configurazione di Astra Trident/ONTAP** | Astra Control Center richiede la creazione e l'impostazione di una classe di storage come classe di storage predefinita. Il centro di controllo Astra supporta le seguenti classi di storage Kubernetes create quando si importa il cluster Kubernetes in ONTAP. Questi sono forniti da Astra Trident:<br><br>• `vsaworkingenvironment-<>-ha-nas csi.trident.netapp.io`<br>• `vsaworkingenvironment-<>-ha-san csi.trident.netapp.io`<br>• `vsaworkingenvironment-<>-single-nas csi.trident.netapp.io`<br>• `vsaworkingenvironment-<>-single-san csi.trident.netapp.io` |

Questi requisiti presuppongono che Astra Control Center sia l'unica applicazione in esecuzione nell'ambiente operativo. Se nell'ambiente sono in esecuzione applicazioni aggiuntive, modificare di conseguenza questi requisiti minimi.

#### Panoramica dell'implementazione di Azure

Ecco una panoramica del processo di installazione di Astra Control Center per Azure.

Ciascuna di queste fasi viene illustrata più dettagliatamente di seguito.

1. Installare un cluster RedHat OpenShift su Azure.
2. Creare gruppi di risorse Azure.

3. Assicurarsi di disporre di autorizzazioni IAM sufficienti.
4. Configurare Azure.
5. Configurare NetApp Cloud Manager.
6. Installare e configurare Astra Control Center.

#### Installare un cluster RedHat OpenShift su Azure

Il primo passo consiste nell'installare un cluster RedHat OpenShift su Azure.

Per istruzioni sull'installazione, consulta la documentazione di RedHat all'indirizzo "Installazione del cluster OpenShift su Azure" e. "Installazione di un account Azure".

#### Creare gruppi di risorse Azure

Creare almeno un gruppo di risorse Azure.

> OpenShift potrebbe creare i propri gruppi di risorse. Oltre a questi, è necessario definire anche i gruppi di risorse di Azure. Fare riferimento alla documentazione di OpenShift.

È possibile creare un gruppo di risorse del cluster di piattaforme e un gruppo di risorse del cluster OpenShift dell'applicazione di destinazione.

#### Assicurarsi di disporre di autorizzazioni IAM sufficienti

Assicurarsi di disporre di ruoli e autorizzazioni IAM sufficienti per installare un cluster RedHat OpenShift e un connettore NetApp Cloud Manager.

Vedere "Credenziali e permessi di Azure".

#### Configurare Azure

Quindi, configurare Azure per creare una rete virtuale, configurare istanze di calcolo, creare un container Azure Blob, creare un Azure Container Register (ACR) per ospitare le immagini di Astra Control Center e inviare le immagini a questo registro.

Seguire la documentazione di Azure per completare i seguenti passaggi. Vedere "Installazione del cluster OpenShift su Azure".

1. Creare una rete virtuale Azure.
2. Esaminare le istanze di calcolo. Si tratta di un server bare metal o di macchine virtuali in Azure.
3. Se il tipo di istanza non corrisponde già ai requisiti minimi di risorsa Astra per i nodi master e worker, modificare il tipo di istanza in Azure per soddisfare i requisiti Astra. Vedere "Requisiti di Astra Control Center".
4. Creare almeno un container Azure Blob per memorizzare i backup.
5. Creare un account storage. Per creare un container da utilizzare come bucket in Astra Control Center è necessario un account storage.
6. Creare un segreto, necessario per l'accesso al bucket.
7. Creare un Azure Container Registry (ACR) per ospitare tutte le immagini di Astra Control Center.
8. Impostare l'accesso ACR per il push/pull di tutte le immagini di Astra Control Center di Docker.

9. Inviare le immagini ACC a questo registro inserendo il seguente script:

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

**Esempio**:

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

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

10. Impostare le zone DNS.

#### Configurare NetApp Cloud Manager

Utilizzando Cloud Manager, creare un'area di lavoro, aggiungere un connettore ad Azure, creare un ambiente di lavoro e importare il cluster.

Seguire la documentazione di Cloud Manager per completare i seguenti passaggi. Vedere "Introduzione a Cloud Manager in Azure".

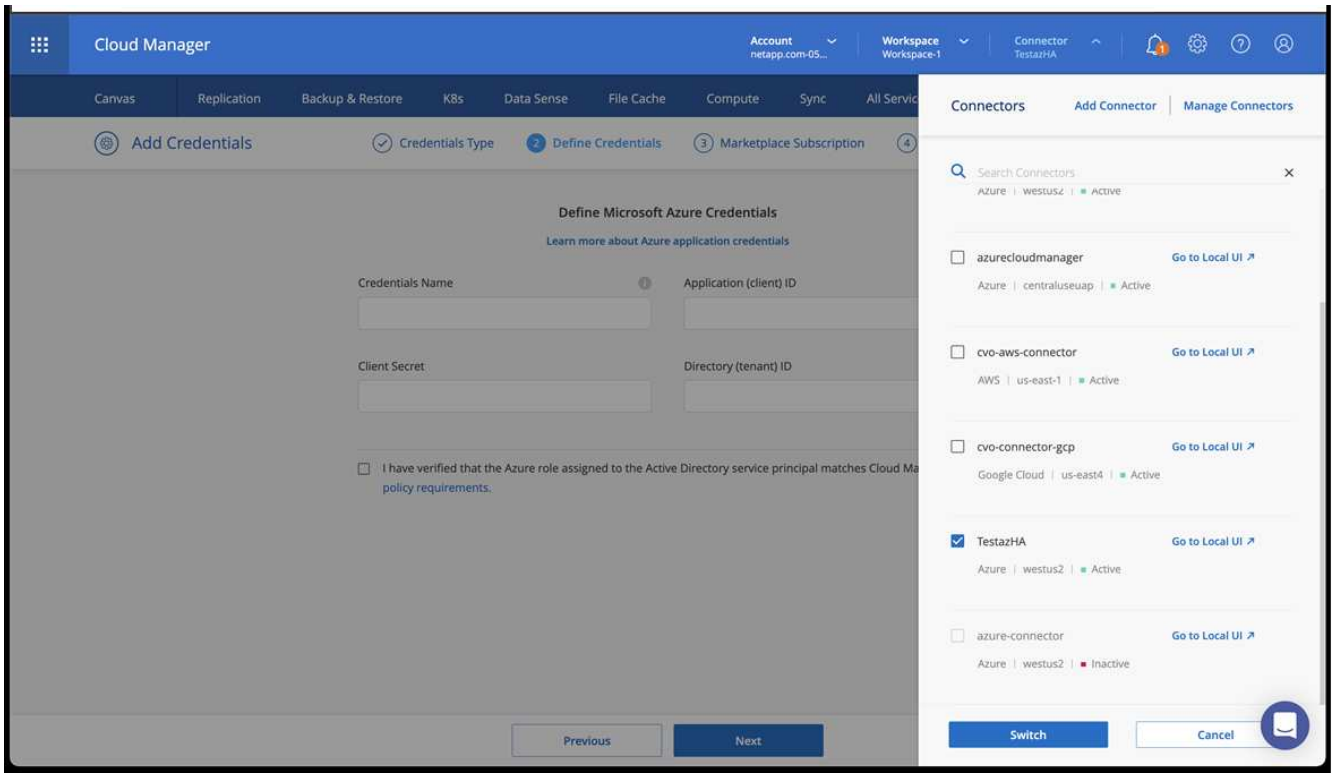
**Di cosa hai bisogno**

Accesso all'account Azure con le autorizzazioni e i ruoli IAM richiesti

**Fasi**

1. Aggiungi le tue credenziali a Cloud Manager.
2. Aggiungere un connettore per Azure. Vedere "Policy di Cloud Manager".
   a. Scegliere **Azure** come provider.
   b. Immettere le credenziali Azure, inclusi ID applicazione, segreto client e ID directory (tenant).

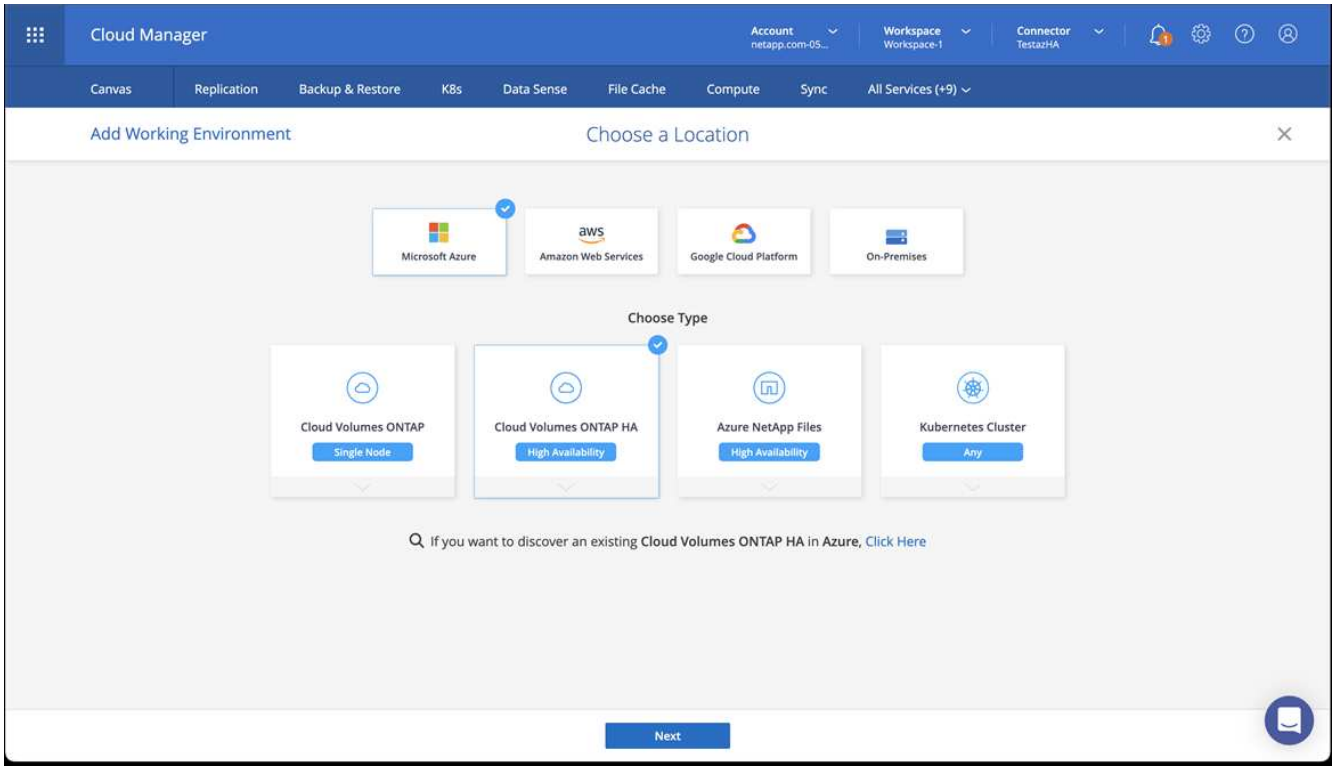
      Vedere "Creazione di un connettore in Azure da Cloud Manager".
3. Assicurarsi che il connettore sia in funzione e passare a tale connettore.




4. Crea un ambiente di lavoro per il tuo ambiente cloud.

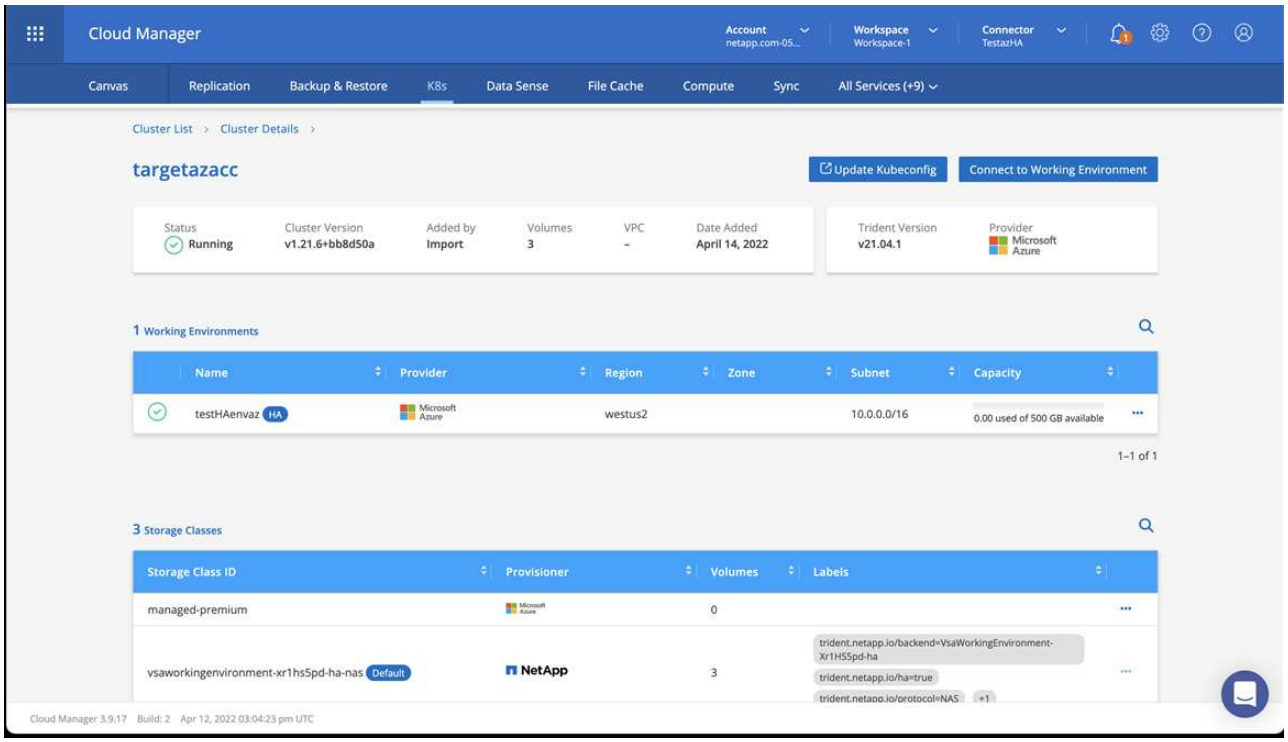
   a. Percorso: "Microsoft Azure".

   b. Tipo: "Cloud Volumes ONTAP ha".




5. Importare il cluster OpenShift. Il cluster si connetterà all'ambiente di lavoro appena creato.

   a. Per visualizzare i dettagli del cluster NetApp, selezionare **K8s** > **elenco cluster** > **Dettagli cluster**.




b. Nell'angolo in alto a destra, prendere nota della versione di Trident.

c. Si noti che le classi di storage cluster Cloud Volumes ONTAP mostrano NetApp come provider.

In questo modo viene importato il cluster Red Hat OpenShift e viene assegnata una classe di storage predefinita. Selezionare la classe di storage. Trident viene installato automaticamente come parte del processo di importazione e rilevamento.

6. Tenere presenti tutti i volumi e i volumi persistenti in questa implementazione di Cloud Volumes ONTAP.
7. Cloud Volumes ONTAP può funzionare come nodo singolo o in alta disponibilità. Se ha è attivato, annotare lo stato ha e lo stato di implementazione del nodo in esecuzione in Azure.

#### Installare e configurare Astra Control Center

Installare Astra Control Center con lo standard "istruzioni per l'installazione".

Utilizzando Astra Control Center, aggiungere un bucket Azure. Vedere "Configurare Astra Control Center e aggiungere i bucket".

## Configurare Astra Control Center

Il centro di controllo Astra supporta e monitora l'archivio dati ONTAP e Astra come back-end dello storage. Dopo aver installato Astra Control Center, aver effettuato l'accesso all'interfaccia utente e aver modificato la password, sarà necessario impostare una licenza, aggiungere cluster, gestire lo storage e aggiungere bucket.

#### Attività

- Aggiungere una licenza per Astra Control Center
- Aggiungere il cluster
- Aggiungere un backend di storage
- Aggiungi un bucket

## Aggiungere una licenza per Astra Control Center

È possibile aggiungere una nuova licenza utilizzando l'interfaccia utente o. "API" Per ottenere la funzionalità completa di Astra Control Center. Senza una licenza, l'utilizzo di Astra Control Center è limitato alla gestione degli utenti e all'aggiunta di nuovi cluster.

Per ulteriori informazioni sul calcolo delle licenze, vedere "Licensing".

> Per aggiornare una licenza di valutazione o una licenza completa, vedere "Aggiornare una licenza esistente".

Le licenze di Astra Control Center misurano le risorse della CPU utilizzando le unità CPU di Kubernetes. La licenza deve tenere conto delle risorse CPU assegnate ai nodi di lavoro di tutti i cluster Kubernetes gestiti. Prima di aggiungere una licenza, è necessario ottenere il file di licenza (NLF) da "Sito di supporto NetApp".

Puoi anche provare Astra Control Center con una licenza di valutazione, che ti consente di utilizzare Astra Control Center per 90 giorni dalla data di download della licenza. Puoi iscriverti per una prova gratuita registrandoti "qui".

> Se l'installazione supera il numero concesso in licenza di unità CPU, Astra Control Center impedisce la gestione di nuove applicazioni. Quando viene superata la capacità, viene visualizzato un avviso.

#### Di cosa hai bisogno

Quando si scarica Astra Control Center da "Sito di supporto NetApp", Inoltre, è stato scaricato il file di licenza NetApp (NLF). Assicurarsi di avere accesso a questo file di licenza.

#### Fasi

1. Accedere all'interfaccia utente di Astra Control Center.
2. Selezionare **account** > **licenza**.
3. Selezionare **Aggiungi licenza**.
4. Individuare il file di licenza (NLF) scaricato.
5. Selezionare **Aggiungi licenza**.

La pagina **account** > **licenza** visualizza le informazioni sulla licenza, la data di scadenza, il numero di serie della licenza, l'ID account e le unità CPU utilizzate.

> Se si dispone di una licenza di valutazione, assicurarsi di memorizzare l'ID account per evitare la perdita di dati in caso di guasto di Astra Control Center se non si inviano ASUP.

## Aggiungere il cluster

Per iniziare a gestire le tue applicazioni, Aggiungi un cluster Kubernetes e gestilo come risorsa di calcolo. Devi aggiungere un cluster per Astra Control Center per scoprire le tue applicazioni Kubernetes. Per Astra Data Store, si desidera aggiungere il cluster di applicazioni Kubernetes che contiene applicazioni che utilizzano volumi forniti da Astra Data Store.

Si consiglia ad Astra Control Center di gestire il cluster su cui viene implementato prima di aggiungere altri cluster ad Astra Control Center da gestire. La gestione del cluster iniziale è necessaria per inviare i dati Kublemetrics e i dati associati al cluster per metriche e troubleshooting. È possibile utilizzare la funzione **Add Cluster** per gestire un cluster con Astra Control Center.

Quando Astra Control gestisce un cluster, tiene traccia della classe di storage predefinita del cluster. Se si modifica la classe di storage utilizzando `kubectl` Comandi, Astra Control ripristina la modifica. Per modificare la classe di storage predefinita in un cluster gestito da Astra Control, utilizzare uno dei seguenti metodi:

- Utilizzare l'API di controllo Astra `PUT /managedClusters` e assegnare una classe di storage predefinita diversa con `DefaultStorageClass` parametro.
- Utilizzare l'interfaccia utente Web di Astra Control per assegnare una classe di storage predefinita diversa. Vedere Modificare la classe di storage predefinita.

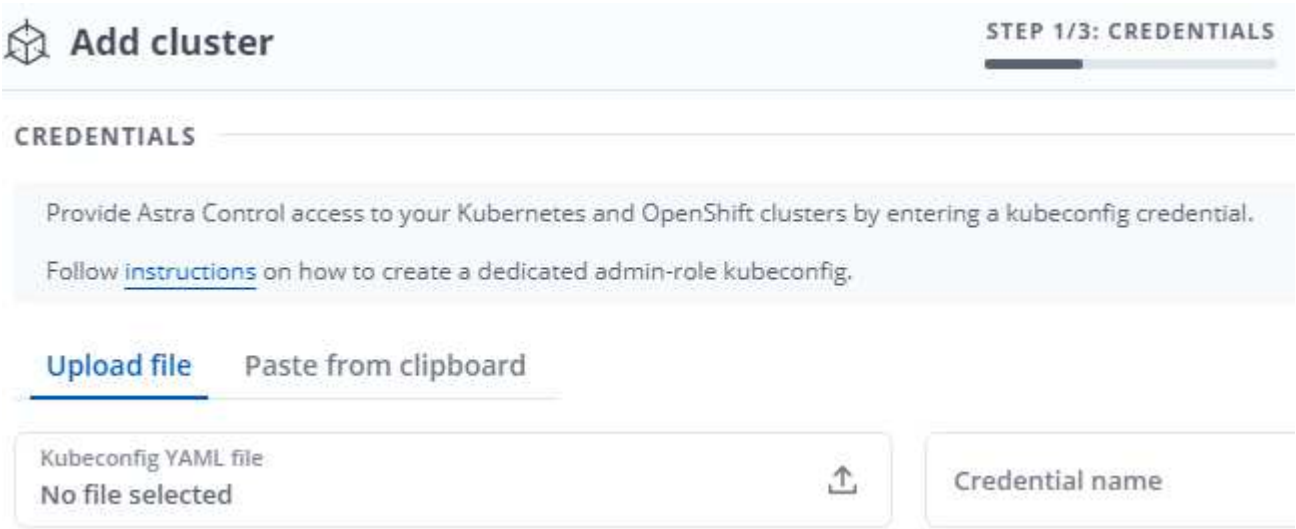
**Di cosa hai bisogno**

- Prima di aggiungere un cluster, esaminare ed eseguire le operazioni necessarie "attività prerequisite".

**Fasi**

1. Dal pannello **Dashboard** dell'interfaccia utente di Astra Control Center, selezionare **Add** (Aggiungi) nella sezione Clusters (Clusters).
2. Nella finestra **Add Cluster** che si apre, caricare un `kubeconfig.yaml` archiviare o incollare il contenuto di a. `kubeconfig.yaml` file.

   Il `kubeconfig.yaml` il file deve includere **solo le credenziali del cluster per un cluster**.

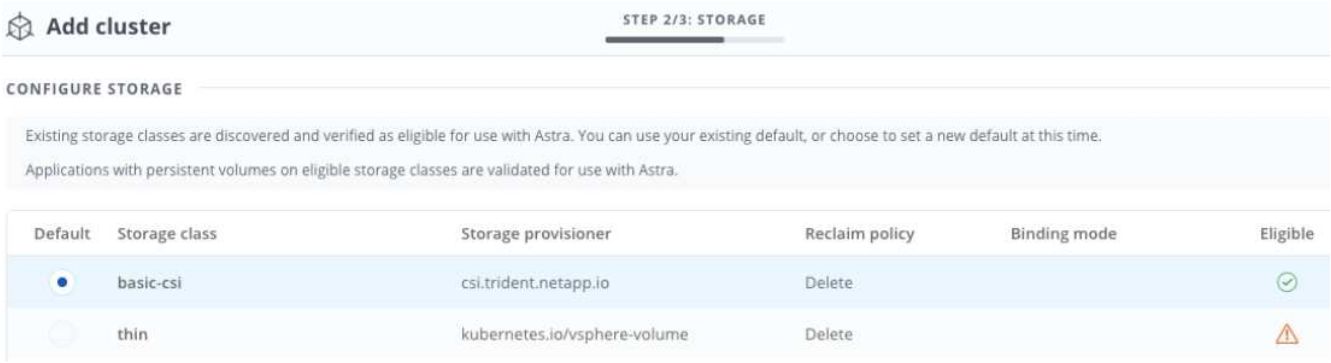



   Se crei il tuo `kubeconfig` file, è necessario definire solo **un** elemento di contesto al suo interno. Vedere "Documentazione Kubernetes" per informazioni sulla creazione `kubeconfig` file.

3. Fornire un nome di credenziale. Per impostazione predefinita, il nome della credenziale viene compilato automaticamente come nome del cluster.

4. Selezionare **Configura storage**.
5. Selezionare la classe di storage da utilizzare per questo cluster Kubernetes e selezionare **Review**.

> È necessario selezionare una classe di storage Trident supportata dallo storage ONTAP o dall'archivio dati Astra.




6. Esaminare le informazioni e, se l'aspetto è soddisfacente, selezionare **Aggiungi cluster**.

**Risultato**

Il cluster passa allo stato **rilevamento**, quindi passa a **in esecuzione**. Hai aggiunto un cluster Kubernetes e lo stai gestendo in Astra Control Center.

> Dopo aver aggiunto un cluster da gestire in Astra Control Center, l'implementazione dell'operatore di monitoraggio potrebbe richiedere alcuni minuti. Fino a quel momento, l'icona di notifica diventa rossa e registra un evento **Monitoring Agent Status Check Failed** (controllo stato agente non riuscito). È possibile ignorarlo, perché il problema si risolve quando Astra Control Center ottiene lo stato corretto. Se il problema non si risolve in pochi minuti, accedere al cluster ed eseguire `oc get pods -n netapp-monitoring` come punto di partenza. Per eseguire il debug del problema, consultare i log dell'operatore di monitoraggio.

## Aggiungere un backend di storage

È possibile aggiungere un backend di storage in modo che Astra Control possa gestire le proprie risorse. È possibile implementare un backend di storage su un cluster gestito o utilizzare un backend di storage esistente.

La gestione dei cluster di storage in Astra Control come back-end dello storage consente di ottenere collegamenti tra volumi persistenti (PVS) e il back-end dello storage, oltre a metriche di storage aggiuntive.

**Ciò di cui hai bisogno per le implementazioni di Astra Data Store esistenti**

- Hai aggiunto il cluster di applicazioni Kubernetes e il cluster di calcolo sottostante.

> Dopo aver aggiunto il cluster di applicazioni Kubernetes per Astra Data Store ed essere gestito da Astra Control, il cluster viene visualizzato come `unmanaged` nell'elenco dei backend rilevati. È quindi necessario aggiungere il cluster di calcolo che contiene Astra Data Store e che si trova sotto il cluster di applicazioni Kubernetes. È possibile eseguire questa operazione da **Backend** nell'interfaccia utente. Selezionare il menu Actions (azioni) per il cluster, quindi scegliere `Manage`, e. "aggiungere il cluster". Dopo lo stato del cluster di `unmanaged` Modifiche al nome del cluster Kubernetes, è possibile procedere con l'aggiunta di un backend.

**Ciò di cui hai bisogno per le nuove implementazioni di Astra Data Store**

- Lo hai fatto "ha caricato la versione del bundle di installazione che si intende implementare" In una posizione accessibile da Astra Control.
- È stato aggiunto il cluster Kubernetes che si intende utilizzare per la distribuzione.
- Hai caricato Licenza Astra Data Store Per l'implementazione in una posizione accessibile ad Astra Control.

**Opzioni**

- Implementare le risorse di storage
- Utilizzare un backend di storage esistente

### Implementare le risorse di storage

È possibile implementare un nuovo archivio dati Astra e gestire il backend dello storage associato.

**Fasi**

1. Spostarsi dal menu Dashboard o Backend:
   - Da **Dashboard**: Dal riepilogo delle risorse, selezionare un collegamento dal riquadro Storage Backends e selezionare **Add** dalla sezione Backend.
   - Da **backend**:
     i. Nell'area di navigazione a sinistra, selezionare **Backend**.
     ii. Selezionare **Aggiungi**.
2. Selezionare l'opzione di implementazione **Astra Data Store** nella scheda **Deploy**.
3. Selezionare il pacchetto Astra Data Store da implementare:
   a. Immettere un nome per l'applicazione Astra Data Store.
   b. Scegli la versione di Astra Data Store che desideri implementare.

   > Se non è stata ancora caricata la versione che si intende distribuire, è possibile utilizzare l'opzione **Add package** (Aggiungi pacchetto) o uscire dalla procedura guidata e utilizzarla "gestione dei pacchetti" per caricare il bundle di installazione.

4. Selezionare una licenza Astra Data Store precedentemente caricata oppure utilizzare l'opzione **Add License** (Aggiungi licenza) per caricare una licenza da utilizzare con l'applicazione.

   > Le licenze di Astra Data Store con autorizzazioni complete sono associate al cluster Kubernetes e i cluster associati dovrebbero essere visualizzati automaticamente. Se non è presente alcun cluster gestito, è possibile selezionare l'opzione **Aggiungi un cluster** per aggiungerne uno alla gestione di Astra Control. Per le licenze Astra Data Store, se non è stata effettuata alcuna associazione tra la licenza e il cluster, è possibile definire questa associazione nella pagina successiva della procedura guidata.

5. Se non hai aggiunto un cluster Kubernetes alla gestione di Astra Control, devi farlo dalla pagina **Kubernetes cluster**. Selezionare un cluster esistente dall'elenco o selezionare **add the underlying cluster** (Aggiungi cluster sottostante) per aggiungere un cluster alla gestione di Astra Control.
6. Selezionare la dimensione del modello di implementazione per il cluster Kubernetes che fornirà le risorse per Astra Data Store.

> Quando si sceglie un modello, selezionare nodi più grandi con più memoria e core per carichi di lavoro più grandi o un numero maggiore di nodi per carichi di lavoro più piccoli. Selezionare un modello in base a quanto consentito dalla licenza. Ogni opzione di modello suggerisce il numero di nodi idonei che soddisfano lo schema di modello per memoria, core e capacità per ciascun nodo.

7. Configurare i nodi:
   a. Aggiungere un'etichetta di nodo per identificare il pool di nodi di lavoro che supporta questo cluster Astra Data Store.

      > L'etichetta deve essere aggiunta a ogni singolo nodo del cluster che verrà utilizzato per l'implementazione di Astra Data Store prima dell'inizio dell'implementazione, altrimenti l'implementazione non avrà esito positivo.

   b. Configurare manualmente la capacità (GiB) per nodo o selezionare la capacità massima consentita per nodo.
   c. Configurare un numero massimo di nodi consentiti nel cluster o consentire il numero massimo di nodi nel cluster.
8. (Solo per le licenze complete di Astra Data Store) inserire la chiave dell'etichetta che si desidera utilizzare per i domini di protezione.

   > Creare almeno tre etichette univoche per la chiave per ciascun nodo. Ad esempio, se la chiave è `astra.datastore.protection.domain`, è possibile creare le seguenti etichette: `astra.datastore.protection.domain=domain1` ,`astra.datastore.protection.domain=domain2`, e. `astra.datastore.protection.domain=domain3`.

9. Configurare la rete di gestione:
   a. Inserire un indirizzo IP di gestione per la gestione interna di Astra Data Store che si trova sulla stessa sottorete degli indirizzi IP del nodo di lavoro.
   b. Scegliere di utilizzare la stessa scheda NIC per reti di gestione e dati o configurarle separatamente.
   c. Inserire il pool di indirizzi IP della rete dati, la subnet mask e il gateway per l'accesso allo storage.
10. Esaminare la configurazione e selezionare **Deploy** per iniziare l'installazione.

**Risultato**

Una volta completata l'installazione, il backend viene visualizzato in `available` indicare nell'elenco backend insieme alle informazioni sulle performance attive.

> Potrebbe essere necessario aggiornare la pagina per visualizzare il backend.

### Utilizzare un backend di storage esistente

Puoi portare un backend di storage ONTAP o Astra Data Store scoperto nella gestione del centro di controllo Astra.

**Fasi**

1. Spostarsi dal menu Dashboard o Backend:
   - Da **Dashboard**: Dal riepilogo delle risorse, selezionare un collegamento dal riquadro Storage

Backends e selezionare **Add** dalla sezione Backend.

- Da **backend**:
  i. Nell'area di navigazione a sinistra, selezionare **Backend**.
  ii. Selezionare **Gestisci** su un backend rilevato dal cluster gestito oppure selezionare **Aggiungi** per gestire un backend esistente aggiuntivo.

2. Selezionare la scheda **Usa esistente**.
3. Eseguire una delle seguenti operazioni in base al tipo di backend:
   - **Archivio dati Astra**:
     i. Selezionare **Astra Data Store**.
     ii. Selezionare il cluster di calcolo gestito e selezionare **Avanti**.
     iii. Confermare i dettagli del back-end e selezionare **Add storage backend**.
   - **ONTAP**:
     i. Selezionare **ONTAP**.
     ii. Immettere le credenziali di amministratore di ONTAP e selezionare **Rivedi**.
     iii. Confermare i dettagli del back-end e selezionare **Add storage backend**.

**Risultato**

Il backend viene visualizzato in `available` indicare nell'elenco le informazioni di riepilogo.

> Potrebbe essere necessario aggiornare la pagina per visualizzare il backend.

## Aggiungi un bucket

L'aggiunta di provider di bucket di archivi di oggetti è essenziale se si desidera eseguire il backup delle applicazioni e dello storage persistente o se si desidera clonare le applicazioni tra cluster. Astra Control memorizza i backup o i cloni nei bucket dell'archivio di oggetti definiti dall'utente.

Quando si aggiunge un bucket, Astra Control contrassegna un bucket come indicatore di bucket predefinito. Il primo bucket creato diventa quello predefinito.

Non è necessario un bucket se si clonano la configurazione dell'applicazione e lo storage persistente sullo stesso cluster.

Utilizzare uno dei seguenti tipi di bucket:

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Generico S3

> Sebbene Astra Control Center supporti Amazon S3 come provider di bucket S3 generico, Astra Control Center potrebbe non supportare tutti i vendor di archivi di oggetti che sostengono il supporto S3 di Amazon.

Per istruzioni su come aggiungere bucket utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

**Fasi**

1. Nell'area di navigazione a sinistra, selezionare **Bucket**.
   a. Selezionare **Aggiungi**.
   b. Selezionare il tipo di bucket.

   > Quando si aggiunge un bucket, selezionare il bucket provider corretto e fornire le credenziali corrette per tale provider. Ad esempio, l'interfaccia utente accetta come tipo NetApp ONTAP S3 e accetta le credenziali StorageGRID; tuttavia, questo causerà l'errore di tutti i backup e ripristini futuri dell'applicazione che utilizzano questo bucket.

   c. Creare un nuovo nome di bucket o inserire un nome di bucket esistente e una descrizione opzionale.

   > Il nome e la descrizione del bucket vengono visualizzati come percorso di backup che è possibile scegliere in seguito quando si crea un backup. Il nome viene visualizzato anche durante la configurazione del criterio di protezione.

   d. Inserire il nome o l'indirizzo IP dell'endpoint S3.
   e. Se si desidera che questo bucket sia il bucket predefinito per tutti i backup, selezionare `Make this bucket the default bucket for this private cloud` opzione.

   > Questa opzione non viene visualizzata per il primo bucket creato.

   f. Continuare aggiungendo informazioni sulle credenziali.

**Aggiungere le credenziali di accesso S3**

Aggiungi credenziali di accesso S3 in qualsiasi momento.

**Fasi**

1. Dalla finestra di dialogo bucket, selezionare la scheda **Add** (Aggiungi) o **Use existing** (Usa esistente).
   a. Immettere un nome per la credenziale che la distingue dalle altre credenziali in Astra Control.
   b. Inserire l'ID di accesso e la chiave segreta incollando il contenuto dagli Appunti.

## Modificare la classe di storage predefinita

È possibile modificare la classe di storage predefinita per un cluster.

**Fasi**

1. Nell'interfaccia utente Web di Astra Control Center, selezionare **Clusters**.
2. Nella pagina **Clusters**, selezionare il cluster che si desidera modificare.
3. Selezionare la scheda **Storage**.
4. Selezionare la categoria **classi di storage**.
5. Selezionare il menu **azioni** per la classe di storage che si desidera impostare come predefinita.
6. Selezionare **Imposta come predefinito**.

## Quali sono le prossime novità?

Ora che hai effettuato l'accesso e aggiunto i cluster ad Astra Control Center, sei pronto per iniziare a utilizzare le funzionalità di gestione dei dati delle applicazioni di Astra Control Center.

- "Gestire gli utenti"
- "Inizia a gestire le app"
- "Proteggi le app"
- "Clonare le applicazioni"
- "Gestire le notifiche"
- "Connettersi a Cloud Insights"
- "Aggiungere un certificato TLS personalizzato"

## Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"
- "Problemi noti"

## Prerequisiti per l'aggiunta di un cluster

Prima di aggiungere un cluster, assicurarsi che le condizioni preliminari siano soddisfatte. È inoltre necessario eseguire i controlli di idoneità per assicurarsi che il cluster sia pronto per essere aggiunto ad Astra Control Center.

### Cosa serve prima di aggiungere un cluster

- Uno dei seguenti tipi di cluster:
  - Cluster che eseguono OpenShift 4.6.8, 4.7, 4.8 o 4.9
  - Cluster che eseguono Rancher 2.5.8, 2.5.9 o 2.6 con RKE1
  - Cluster che eseguono Kubernetes da 1.20 a 1.23
  - Cluster che eseguono VMware Tanzu Kubernetes Grid 1.4
  - Cluster che eseguono VMware Tanzu Kubernetes Grid Integrated Edition 1.12.2

    Assicurarsi che i cluster dispongano di uno o più nodi di lavoro con almeno 1 GB di RAM disponibile per l'esecuzione dei servizi di telemetria.

> Se si intende aggiungere un secondo cluster OpenShift 4.6, 4.7 o 4.8 come risorsa di calcolo gestita, assicurarsi che la funzione Astra Trident Volume Snapshot sia attivata. Vedi l'Astra Trident ufficiale "istruzioni" Per attivare e testare le istantanee dei volumi con Astra Trident.

- Astra Trident StorageClasses configurato con un "back-end di storage supportato" (richiesto per qualsiasi tipo di cluster)
- Il superuser e l'ID utente impostati sul sistema ONTAP di backup per eseguire il backup e il ripristino delle applicazioni con Centro di controllo Astra. Eseguire il seguente comando nella riga di comando di ONTAP: `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sysm --anon 65534`

- Un tridente Astra `volumesnapshotclass` oggetto definito da un amministratore. Vedi Astra Trident "istruzioni" Per attivare e testare le istantanee dei volumi con Astra Trident.
- Assicurarsi di avere definito solo una singola classe di storage predefinita per il cluster Kubernetes.

### Eseguire i controlli di idoneità

Eseguire i seguenti controlli di idoneità per assicurarsi che il cluster sia pronto per essere aggiunto ad Astra Control Center.

#### Fasi

1. Controllare la versione di Trident.

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

Se Trident esiste, l'output è simile a quanto segue:

```
NAME      VERSION
trident   21.04.0
```

Se Trident non esiste, viene visualizzato un output simile a quanto segue:

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

> Se Trident non è installato o se la versione installata non è la più recente, è necessario installare la versione più recente di Trident prima di procedere. Vedere "Documentazione di Trident" per istruzioni.

2. Controllare se le classi di storage utilizzano i driver Trident supportati. Il nome del provider deve essere `csi.trident.netapp.io`. Vedere il seguente esempio:

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

### Creare un kubeconfig con ruolo di amministratore

Prima di eseguire la procedura, assicurarsi di disporre dei seguenti elementi sul computer:

- `kubectl` v1.19 o versione successiva installata

- Un kubeconfig attivo con diritti di amministratore del cluster per il contesto attivo

**Fasi**

1. Creare un account di servizio come segue:

   a. Creare un file di account del servizio denominato `astracontrol-service-account.yaml`.

      Regolare il nome e lo spazio dei nomi in base alle esigenze. Se le modifiche vengono apportate qui, è necessario applicare le stesse modifiche nei passaggi seguenti.

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

+

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

   a. Applicare l'account del servizio:

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

2. (Facoltativo) se il cluster utilizza una policy di sicurezza del pod restrittiva che non consente la creazione di pod privilegiati o consente l'esecuzione di processi all'interno dei container del pod come utente root, creare una policy di sicurezza del pod personalizzata per il cluster che consenta ad Astra Control di creare e gestire i pod. Per istruzioni, vedere "Creare una policy di sicurezza pod personalizzata".

3. Concedere le autorizzazioni di amministratore del cluster come segue:

   a. Creare un `ClusterRoleBinding` file chiamato `astracontrol-clusterrolebinding.yaml`.

      Modificare i nomi e gli spazi dei nomi modificati quando si crea l'account del servizio, in base alle necessità.

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

+

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

a. Applicare l'associazione del ruolo del cluster:

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

4. Elencare i segreti dell'account di servizio, sostituendo `<context>` con il contesto corretto per l'installazione:

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

La fine dell'output dovrebbe essere simile a quanto segue:

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

Gli indici di ciascun elemento in `secrets` l'array inizia con 0. Nell'esempio precedente, l'indice per `astracontrol-service-account-dockercfg-vhz87` sarebbe 0 e l'indice per `astracontrol-service-account-token-r59kr` sarebbe 1. Nell'output, annotare l'indice del nome dell'account del servizio che contiene la parola "token".

5. Generare il kubeconfig come segue:

a. Creare un `create-kubeconfig.sh` file. Sostituire `TOKEN_INDEX` all'inizio del seguente script con il valore corretto.

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

```
```

```
# Update these to match your environment.
# Replace TOKEN_INDEX with the correct value
# from the output in the previous step. If you
# didn't change anything else above, don't change
# anything else here.

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

CONTEXT=$(kubectl config current-context)

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

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

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

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

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

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

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

# Set context to use token user
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
```

```
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

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

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

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

b. Eseguire la sorgente dei comandi per applicarli al cluster Kubernetes.

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

6. (**opzionale**) rinominare il kubeconfig con un nome significativo per il cluster. Proteggi la tua credenziale del cluster.

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

#### Quali sono le prossime novità?

Ora che hai verificato che i prerequisiti sono stati soddisfatti, sei pronto "aggiungere un cluster".

#### Trova ulteriori informazioni

- "Documentazione di Trident"
- "Utilizzare l'API di controllo Astra"

## Aggiungere un certificato TLS personalizzato

È possibile rimuovere il certificato TLS autofirmato esistente e sostituirlo con un certificato TLS firmato da un'autorità di certificazione (CA).

#### Di cosa hai bisogno

- Kubernetes cluster con Astra Control Center installato
- Accesso amministrativo a una shell dei comandi sul cluster da eseguire `kubectl` comandi
- Chiave privata e file di certificato dalla CA

#### Rimuovere il certificato autofirmato

Rimuovere il certificato TLS autofirmato esistente.

1. Utilizzando SSH, accedere al cluster Kubernetes che ospita Astra Control Center come utente amministrativo.
2. Individuare il segreto TLS associato al certificato corrente utilizzando il seguente comando, sostituendo `<ACC-deployment-namespace>` Con lo spazio dei nomi di implementazione di Astra Control Center:

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

3. Eliminare il certificato e il segreto attualmente installati utilizzando i seguenti comandi:

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

#### Aggiungere un nuovo certificato

Aggiungere un nuovo certificato TLS firmato da una CA.

1. Utilizzare il seguente comando per creare il nuovo segreto TLS con la chiave privata e i file di certificato della CA, sostituendo gli argomenti tra parentesi <> con le informazioni appropriate:

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

2. Utilizzare il seguente comando e l'esempio per modificare il file CRD (Custom Resource Definition) del cluster e modificare `spec.selfSigned` valore a. `spec.ca.secretName` Per fare riferimento al segreto TLS creato in precedenza:

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

#spec:
#  selfSigned: {}

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

3. Utilizzare il seguente comando e l'output di esempio per confermare che le modifiche sono corrette e che il cluster è pronto per validare i certificati, sostituendo `<ACC-deployment-namespace>` Con lo spazio dei nomi di implementazione di Astra Control Center:

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

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

4. Creare il `certificate.yaml` file utilizzando il seguente esempio, sostituendo i valori segnaposto tra parentesi <> con le informazioni appropriate:

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

5. Creare il certificato utilizzando il seguente comando:

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

6. Utilizzando il seguente comando e l'output di esempio, verificare che il certificato sia stato creato correttamente e con gli argomenti specificati durante la creazione (ad esempio nome, durata, scadenza di rinnovo e nomi DNS).

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

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

7. Modificare l’opzione TLS CRD di ingresso per indicare il nuovo segreto del certificato utilizzando il seguente comando ed esempio, sostituendo i valori segnaposto tra parentesi <> con le informazioni appropriate:

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

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

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

8. Utilizzando un browser Web, accedere all'indirizzo IP di implementazione di Astra Control Center.
9. Verificare che i dettagli del certificato corrispondano ai dettagli del certificato installato.
10. Esportare il certificato e importare il risultato nel gestore dei certificati nel browser Web.

## Creare una policy di sicurezza pod personalizzata

Astra Control deve creare e gestire i pod Kubernetes sui cluster gestiti. Se il cluster utilizza una policy di sicurezza del pod restrittiva che non consente la creazione di pod con privilegi o l'esecuzione di processi all'interno dei container del pod come utente root, è necessario creare una policy di sicurezza del pod meno restrittiva per consentire ad Astra Control di creare e gestire questi pod.

**Fasi**

1. Creare un criterio di protezione pod per il cluster meno restrittivo di quello predefinito e salvarlo in un file. Ad esempio:

```yaml
apiVersion: policy/v1beta1
kind: PodSecurityPolicy
metadata:
  name: astracontrol
  annotations:
    seccomp.security.alpha.kubernetes.io/allowedProfileNames: '*'
spec:
  privileged: true
  allowPrivilegeEscalation: true
  allowedCapabilities:
  - '*'
  volumes:
  - '*'
  hostNetwork: true
  hostPorts:
  - min: 0
    max: 65535
  hostIPC: true
  hostPID: true
  runAsUser:
    rule: 'RunAsAny'
  seLinux:
    rule: 'RunAsAny'
  supplementalGroups:
    rule: 'RunAsAny'
  fsGroup:
    rule: 'RunAsAny'
```

2. Creare un nuovo ruolo per la policy di sicurezza del pod.

```bash
kubectl-admin create role psp:astracontrol \
    --verb=use \
    --resource=podsecuritypolicy \
    --resource-name=astracontrol
```

3. Associare il nuovo ruolo all'account del servizio.

```bash
kubectl-admin create rolebinding default:psp:astracontrol \
    --role=psp:astracontrol \
    --serviceaccount=astracontrol-service-account:default
```

# Domande frequenti per Astra Control Center

Queste FAQ possono essere utili se stai cercando una risposta rapida a una domanda.

## Panoramica

Le sezioni seguenti forniscono risposte ad alcune domande aggiuntive che potrebbero essere presentate durante l'utilizzo di Astra Control Center. Per ulteriori chiarimenti, contatta il sito astra.feedback@netapp.com

## Accesso al centro di controllo Astra

### Cos'è l'URL di Astra Control?

Astra Control Center utilizza l'autenticazione locale e un URL specifico per ciascun ambiente.

Per l'URL, in un browser, immettere il nome di dominio completo (FQDN) impostato nel campo spec.astraAddress nel file Astra_Control_Center_min.yaml custom resource Definition (CRD) al momento dell'installazione di Astra Control Center. Il messaggio di posta elettronica è il valore impostato nel campo spec.email nel CRD Astra_Control_Center_min.yaml.

### Utilizzo la licenza di valutazione. Come si passa alla licenza completa?

È possibile passare facilmente a una licenza completa ottenendo il file di licenza NetApp (NLF).

#### Fasi

- Dalla barra di navigazione a sinistra, selezionare **account** > **licenza**.
- Selezionare **Aggiungi licenza**.
- Individuare il file di licenza scaricato e selezionare **Aggiungi**.

### Utilizzo la licenza di valutazione. Posso comunque gestire le applicazioni?

Sì, puoi testare la funzionalità di gestione delle app con la licenza Evaluation.

## Registrazione dei cluster Kubernetes

### Devo aggiungere nodi di lavoro al cluster Kubernetes dopo l'aggiunta ad Astra Control. Cosa devo fare?

È possibile aggiungere nuovi nodi di lavoro ai pool esistenti. Questi verranno rilevati automaticamente da Astra Control. Se i nuovi nodi non sono visibili in Astra Control, controllare se i nuovi nodi di lavoro eseguono il tipo di immagine supportato. È inoltre possibile verificare lo stato dei nuovi nodi di lavoro utilizzando `kubectl get nodes` comando.

### Come si annulla la gestione corretta di un cluster?

1. "Annulla la gestione delle applicazioni da Astra Control".
2. "Annullare la gestione del cluster da Astra Control".

### Cosa succede alle mie applicazioni e ai miei dati dopo aver rimosso il cluster Kubernetes da Astra Control?

La rimozione di un cluster da Astra Control non apporta alcuna modifica alla configurazione del cluster

(applicazioni e storage persistente). Eventuali snapshot di Astra Control o backup delle applicazioni su quel cluster non saranno disponibili per il ripristino. I backup persistenti dello storage creati da Astra Control rimangono all'interno di Astra Control, ma non sono disponibili per il ripristino.

> Rimuovere sempre un cluster da Astra Control prima di eliminarlo con altri metodi. L'eliminazione di un cluster utilizzando un altro tool mentre viene ancora gestito da Astra Control può causare problemi all'account Astra Control.

**NetApp Trident viene disinstallato automaticamente da un cluster quando viene disgestito?** quando si disgestisce un cluster da Astra Control Center, Trident non viene disinstallato automaticamente dal cluster. Per disinstallare Trident, è necessario "Seguire questa procedura nella documentazione di Trident".

## Gestione delle applicazioni

**Astra Control può implementare un'applicazione?**

Astra Control non implementa le applicazioni. Le applicazioni devono essere implementate all'esterno di Astra Control.

**Cosa succede alle applicazioni dopo che non li gestisco da Astra Control?**

Eventuali backup o snapshot esistenti verranno eliminati. Le applicazioni e i dati rimangono disponibili. Le operazioni di gestione dei dati non saranno disponibili per le applicazioni non gestite o per eventuali backup o snapshot ad esse appartenenti.

- Astra Control può gestire un'applicazione su storage non NetApp?*

No Mentre Astra Control è in grado di rilevare applicazioni che utilizzano storage non NetApp, non può gestire un'applicazione che utilizza storage non NetApp.

**Dovrei gestire Astra Control da solo?** No, non dovresti gestire Astra Control perché è un'applicazione di sistema.

**I pod malsani influiscono sulla gestione delle applicazioni?** se un'applicazione gestita ha i pod in uno stato non integro, Astra Control non può creare nuovi backup e cloni.

## Operazioni di gestione dei dati

**Nel mio account sono presenti snapshot che non ho creato. Da dove sono venuti?**

In alcune situazioni, Astra Control crea automaticamente uno snapshot come parte di un processo di backup, clonazione o ripristino.

**La mia applicazione utilizza diversi PVS. Astra Control eseguirà snapshot e backup di tutti questi PVC?**

Sì. Un'operazione snapshot su un'applicazione di Astra Control include l'istantanea di tutti i PVS associati ai PVC dell'applicazione.

**È possibile gestire le snapshot acquisite da Astra Control direttamente attraverso un'interfaccia o un'archiviazione a oggetti diversa?**

No Le snapshot e i backup eseguiti da Astra Control possono essere gestiti solo con Astra Control.

# Utilizzare Astra

## Gestire le applicazioni

### Inizia a gestire le app

Dopo di lei "Aggiungere un cluster alla gestione di Astra Control", È possibile installare le applicazioni sul cluster (al di fuori di Astra Control), quindi andare alla pagina Apps (applicazioni) in Astra Control per iniziare a gestire le applicazioni e le relative risorse.

Per ulteriori informazioni, vedere "Requisiti di gestione delle applicazioni".

#### Metodi di installazione delle applicazioni supportati

Astra Control supporta i seguenti metodi di installazione dell'applicazione:

- **Manifest file**: Astra Control supporta le applicazioni installate da un file manifest utilizzando kubectl. Ad esempio:

  ```
  kubectl apply -f myapp.yaml
  ```

- **Helm 3**: Se utilizzi Helm per installare le app, Astra Control richiede Helm versione 3. La gestione e la clonazione delle applicazioni installate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. La gestione delle applicazioni installate con Helm 2 non è supportata.
- **Applicazioni distribuite dall'operatore**: Astra Control supporta le applicazioni installate con operatori con ambito namespace. Questi operatori sono generalmente progettati con un'architettura "pass-by-value" piuttosto che "pass-by-reference". Di seguito sono riportate alcune applicazioni per operatori che seguono questi modelli:
  - "Apache K8ssandra"
  - "Ci Jenkins"
  - "Cluster XtraDB Percona"

Si noti che Astra Control potrebbe non essere in grado di clonare un operatore progettato con un'architettura "pass-by-reference" (ad esempio, l'operatore CockroachDB). Durante questi tipi di operazioni di cloning, l'operatore clonato tenta di fare riferimento ai segreti di Kubernetes dall'operatore di origine, nonostante abbia il proprio nuovo segreto come parte del processo di cloning. L'operazione di clonazione potrebbe non riuscire perché Astra Control non è a conoscenza dei segreti di Kubernetes nell'operatore di origine.

> Un operatore e l'applicazione che installa devono utilizzare lo stesso namespace; potrebbe essere necessario modificare il file .yaml di implementazione per l'operatore per assicurarsi che questo sia il caso.

#### Installa le app sul tuo cluster

Una volta aggiunto il cluster ad Astra Control, è possibile installare le applicazioni o gestire quelle esistenti sul cluster. È possibile gestire qualsiasi applicazione con ambito per uno spazio dei nomi. Una volta che i pod sono online, puoi gestire l'applicazione con Astra Control.

Per assistenza nell'implementazione delle applicazioni validate dai grafici Helm, fare riferimento a quanto

segue:

- "Implementare MariaDB da un grafico Helm"
- "Implementa MySQL da un grafico Helm"
- "Implementare Postgres da un grafico Helm"
- "Implementare Jenkins da un grafico Helm"

### Gestire le applicazioni

Astra Control consente di gestire le applicazioni a livello di spazio dei nomi o in base all'etichetta Kubernetes.

> Le applicazioni installate con Helm 2 non sono supportate.

Per gestire le applicazioni, è possibile eseguire le seguenti attività:

- Gestire le applicazioni
  - Gestire le applicazioni in base allo spazio dei nomi
  - Gestisci le app in base all'etichetta Kubernetes
- Ignorare le applicazioni
- Annulla gestione delle applicazioni

> Astra Control non è un'applicazione standard, ma un'applicazione di sistema. Non si dovrebbe tentare di gestire Astra Control da solo. Per impostazione predefinita, Astra Control non viene visualizzato per la gestione. Per visualizzare le applicazioni di sistema, utilizza il filtro "Mostra app di sistema".

Per istruzioni su come gestire le applicazioni utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

> Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

#### Gestire le applicazioni in base allo spazio dei nomi

La sezione **scoperta** della pagina App mostra gli spazi dei nomi e le applicazioni installate da Helm o personalizzate in tali spazi dei nomi. Puoi scegliere di gestire ogni applicazione singolarmente o a livello di spazio dei nomi. Tutto questo si riduce al livello di granularità necessario per le operazioni di protezione dei dati.

Ad esempio, è possibile impostare una policy di backup per "maria" con cadenza settimanale, ma potrebbe essere necessario eseguire il backup di "mariadb" (che si trova nello stesso namespace) con maggiore frequenza. In base a tali esigenze, sarebbe necessario gestire le applicazioni separatamente e non in un singolo namespace.

Mentre Astra Control consente di gestire separatamente entrambi i livelli della gerarchia (lo spazio dei nomi e le applicazioni in tale spazio dei nomi), la procedura migliore è scegliere uno o l'altro. Le azioni eseguite in

Astra Control possono non riuscire se vengono eseguite contemporaneamente sia a livello di spazio dei nomi che di applicazione.

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **applicazioni**.
2. Selezionare il filtro **rilevato**.


3. Visualizzare l'elenco degli spazi dei nomi rilevati. Espandere lo spazio dei nomi per visualizzare le applicazioni e le risorse associate.

   Astra Control mostra le applicazioni Helm e le applicazioni con etichetta personalizzata nello spazio dei nomi. Se le etichette Helm sono disponibili, sono contrassegnate da un'icona di tag.

4. Esaminare la colonna **Gruppo** per visualizzare lo spazio dei nomi in cui viene eseguita l'applicazione (indicato con l'icona della cartella).
5. Decidere se si desidera gestire ciascuna applicazione singolarmente o a livello di spazio dei nomi.
6. Individuare l'applicazione desiderata al livello desiderato nella gerarchia e selezionare **Manage** (Gestisci) dal menu Options (Opzioni) nella colonna **Actions** (azioni).
7. Se non si desidera gestire un'applicazione, selezionare **Ignora** dal menu Opzioni nella colonna **azioni**.

   Ad esempio, se si desidera gestire tutte le applicazioni nello spazio dei nomi "maria" insieme in modo che abbiano le stesse policy di backup e snapshot, è necessario gestire lo spazio dei nomi e ignorare le applicazioni nello spazio dei nomi.

8. Per visualizzare l'elenco delle applicazioni gestite, selezionare **Managed** come filtro di visualizzazione.


> L'applicazione appena aggiunta potrebbe presentare un'icona di avviso sotto la colonna Protected, che indica che il backup non è stato ancora eseguito e non è stato pianificato per i backup.

9. Per visualizzare i dettagli di una particolare applicazione, selezionare il nome dell'applicazione.

**Risultato**

Le applicazioni che hai scelto di gestire sono ora disponibili nella scheda **Managed**. Tutte le applicazioni ignorate verranno spostate nella scheda **ignored**. Idealmente, la scheda scoperta non mostra alcuna applicazione, in modo che, una volta installate, siano più facili da trovare e gestire.

#### Gestisci le app in base all'etichetta Kubernetes

Astra Control include un'azione nella parte superiore della pagina Apps denominata **define custom app**. Puoi utilizzare questa azione per gestire le app identificate con un'etichetta Kubernetes. "Scopri di più sulla definizione di applicazioni personalizzate con l'etichetta Kubernetes".

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **applicazioni**.

2. Selezionare **Definisci**.
3. Nella finestra di dialogo **Definisci applicazione personalizzata**, fornire le informazioni necessarie per gestire l'applicazione:
   a. **Nuova applicazione**: Immettere il nome visualizzato dell'applicazione.
   b. **Cluster**: Selezionare il cluster in cui risiede l'applicazione.
   c. **Namespace:** selezionare lo spazio dei nomi dell'applicazione.
   d. **Label:** inserire un'etichetta o selezionare un'etichetta dalle risorse sottostanti.
   e. **Risorse selezionate**: Consente di visualizzare e gestire le risorse Kubernetes selezionate che si desidera proteggere (pod, segreti, volumi persistenti e altro ancora).
      - Visualizzare le etichette disponibili espandendo una risorsa e selezionando il numero di etichette.
      - Selezionare una delle etichette.

        Dopo aver scelto un'etichetta, questa viene visualizzata nel campo **etichetta**. Astra Control aggiorna anche la sezione **risorse non selezionate** per mostrare le risorse che non corrispondono all'etichetta selezionata.
   f. **Risorse non selezionate**: Verifica le risorse dell'app che non desideri proteggere.
4. Selezionare **Definisci applicazione personalizzata**.

**Risultato**

Astra Control consente la gestione dell'applicazione. A questo punto, è possibile trovarlo nella scheda **Managed**.

### Ignorare le applicazioni

Se un'applicazione è stata rilevata, viene visualizzata nell'elenco rilevato. In questo caso, è possibile pulire l'elenco scoperto in modo che le nuove applicazioni appena installate siano più facili da trovare. Oppure, potresti avere applicazioni che gestisci e decidere in seguito di non doverle più gestire. Se non si desidera gestire queste applicazioni, è possibile indicare che devono essere ignorate.

Inoltre, è possibile gestire le applicazioni in un unico namespace insieme (gestito dallo spazio dei nomi). È possibile ignorare le applicazioni che si desidera escludere dallo spazio dei nomi.

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **applicazioni**.
2. Selezionare **rilevato** come filtro.
3. Selezionare l'applicazione.
4. Dal menu Opzioni nella colonna **azioni**, selezionare **Ignora**.
5. Per non ignorare, selezionare **Unignore**.

### Annulla gestione delle applicazioni

Quando non si desidera più eseguire il backup, lo snapshot o la clonazione di un'applicazione, è possibile interromperne la gestione.

> Se si annulla la gestione di un'applicazione, i backup o le snapshot creati in precedenza andranno persi.

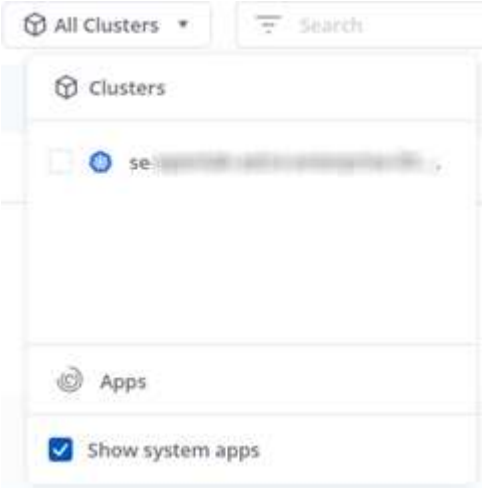
**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **applicazioni**.
2. Selezionare **Managed** come filtro.
3. Selezionare l'applicazione.
4. Dal menu Opzioni nella colonna **azioni**, selezionare **Annulla gestione**.
5. Esaminare le informazioni.
6. Digitare "unManage" per confermare.
7. Selezionare **Sì, Annulla gestione applicazione**.

**E le applicazioni di sistema?**

Astra Control rileva anche le applicazioni di sistema in esecuzione su un cluster Kubernetes. Per impostazione predefinita, queste applicazioni di sistema non vengono visualizzate perché è raro che sia necessario eseguirne il backup.

È possibile visualizzare le applicazioni di sistema dalla pagina applicazioni selezionando la casella di controllo **Mostra applicazioni di sistema** sotto il filtro Clusters nella barra degli strumenti.




Astra Control non è un'applicazione standard, ma un'applicazione di sistema. Non si dovrebbe tentare di gestire Astra Control da solo. Per impostazione predefinita, Astra Control non viene visualizzato per la gestione.

**Trova ulteriori informazioni**

- "Utilizzare l'API di controllo Astra"

## Definire un esempio di applicazione personalizzata

La creazione di un'applicazione personalizzata consente di raggruppare gli elementi del cluster Kubernetes in una singola applicazione. Questa raccolta di risorse Kubernetes si basa su uno spazio dei nomi e un'etichetta.

Un'applicazione personalizzata ti offre un controllo più granulare su ciò che devi includere in un'operazione Astra Control, tra cui:

- Clonare
- Snapshot
- Backup
- Policy di protezione

Nella maggior parte dei casi, è consigliabile utilizzare le funzionalità di Astra Control sull'intera applicazione. Tuttavia, è anche possibile creare un'applicazione personalizzata per utilizzare queste funzionalità tramite le etichette assegnate agli oggetti Kubernetes in uno spazio dei nomi.

> Le applicazioni personalizzate possono essere create solo all'interno di uno spazio dei nomi specificato in un singolo cluster. Astra Control non supporta la capacità di un'applicazione personalizzata di includere più spazi dei nomi o cluster.

Un'etichetta è una coppia chiave/valore che è possibile assegnare agli oggetti Kubernetes per l'identificazione. Le etichette semplificano l'ordinamento, l'organizzazione e la ricerca degli oggetti Kubernetes. Per ulteriori informazioni sulle etichette Kubernetes, "Consulta la documentazione ufficiale di Kubernetes".

> La sovrapposizione di policy per la stessa risorsa con nomi diversi può causare conflitti di dati. Se crei un'applicazione personalizzata per una risorsa, assicurati che non venga clonata o sottoposta a backup in base ad altre policy.

**Di cosa hai bisogno**

- Un cluster aggiunto ad Astra Control

**Fasi**

1. Dalla pagina App, selezionare **+ Definisci**.

   La finestra Custom App mostra le risorse che verranno incluse o escluse dall'applicazione personalizzata. Questo ti aiuta a scegliere i criteri corretti per la definizione della tua applicazione personalizzata.

2. Nella finestra a comparsa, inserisci il nome dell'applicazione, scegli il cluster nell'elenco a discesa **Cluster** e scegli lo spazio dei nomi dell'applicazione dall'elenco a discesa **namespace**.
3. Dall'elenco a discesa **Label** (etichetta), selezionare un'etichetta per le applicazioni e lo spazio dei nomi.
4. Dopo aver definito l'applicazione personalizzata per un'implementazione, ripetere il processo per altre implementazioni, se necessario.

Al termine della creazione delle due applicazioni personalizzate, è possibile considerare queste risorse come qualsiasi altra applicazione Astra Control. Possono clonarli, creare backup e snapshot e creare una policy di protezione personalizzata per ciascun gruppo di risorse in base alle etichette Kubernetes.

**Esempio: Policy di protezione separata per release diverse**

In questo esempio, il team devops sta gestendo un'implementazione di release canary. Il cluster dispone di tre pod che eseguono nginx. Due dei pod sono dedicati al rilascio stabile. Il terzo pod è per la release canary.

L'amministratore Kubernetes del team devops aggiunge l'etichetta `deployment=stable` ai pod a rilascio stabile. Il team aggiunge l'etichetta `deployment=canary` al pod di rilascio canary.

La release stabile del team include un requisito per snapshot orarie e backup giornalieri. La release canary è più effimera, quindi vogliono creare una politica di protezione meno aggressiva e a breve termine per qualsiasi cosa etichettata `deployment=canary`.

Per evitare possibili conflitti di dati, l'amministratore creerà due applicazioni personalizzate: Una per la release "canary" e una per la release "stable". In questo modo i backup, gli snapshot e le operazioni di clonazione vengono separati per i due gruppi di oggetti Kubernetes.

# Proteggi le app

## Panoramica della protezione

Con Astra Control Center puoi creare backup, cloni, snapshot e policy di protezione per le tue applicazioni. Il backup delle tue applicazioni aiuta i tuoi servizi e i dati associati a essere il più possibile disponibili; durante uno scenario di disastro, il ripristino dal backup può garantire il ripristino completo di un'applicazione e dei dati associati con interruzioni minime. Backup, cloni e snapshot possono contribuire a proteggere da minacce comuni come ransomware, perdita accidentale di dati e disastri ambientali. "Scopri i tipi di protezione dei dati disponibili in Astra Control Center e quando utilizzarli".

### Workflow di protezione delle app

Puoi utilizzare il seguente flusso di lavoro di esempio per iniziare a proteggere le tue applicazioni.

#### [Uno] Eseguire il backup di tutte le applicazioni

Per garantire la protezione immediata delle applicazioni, "creare un backup manuale di tutte le applicazioni".

#### [Due] Configurare una policy di protezione per ogni applicazione

Per automatizzare backup e snapshot futuri, "configurare una policy di protezione per ogni applicazione". Ad esempio, è possibile iniziare con backup settimanali e snapshot giornalieri, con un mese di conservazione per entrambi. Si consiglia vivamente di automatizzare backup e snapshot con una policy di protezione rispetto a backup e snapshot manuali.

#### [Tre] Facoltativo: Regolare i criteri di protezione

Man mano che le applicazioni e i loro modelli di utilizzo cambiano, regola le policy di protezione in base alle necessità per fornire la migliore protezione.

#### [Quattro] In caso di disastro, ripristinate le vostre applicazioni

In caso di perdita di dati, è possibile eseguire il ripristino "ripristino del backup più recente" primo per ogni applicazione. È quindi possibile ripristinare l'ultimo snapshot (se disponibile).

## Proteggi le app con snapshot e backup

Proteggi le tue applicazioni eseguendo snapshot e backup utilizzando una policy di protezione automatica o ad-hoc. È possibile utilizzare l'interfaccia utente Astra o. "L'API Astra Control" per proteggere le applicazioni.

> Se utilizzi Helm per implementare le app, Astra Control Center richiede Helm versione 3. La gestione e la clonazione delle applicazioni implementate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. Le app implementate con Helm 2 non sono supportate.

Quando crei un progetto per ospitare un'applicazione su un cluster OpenShift, al progetto (o namespace Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

### Configurare un criterio di protezione

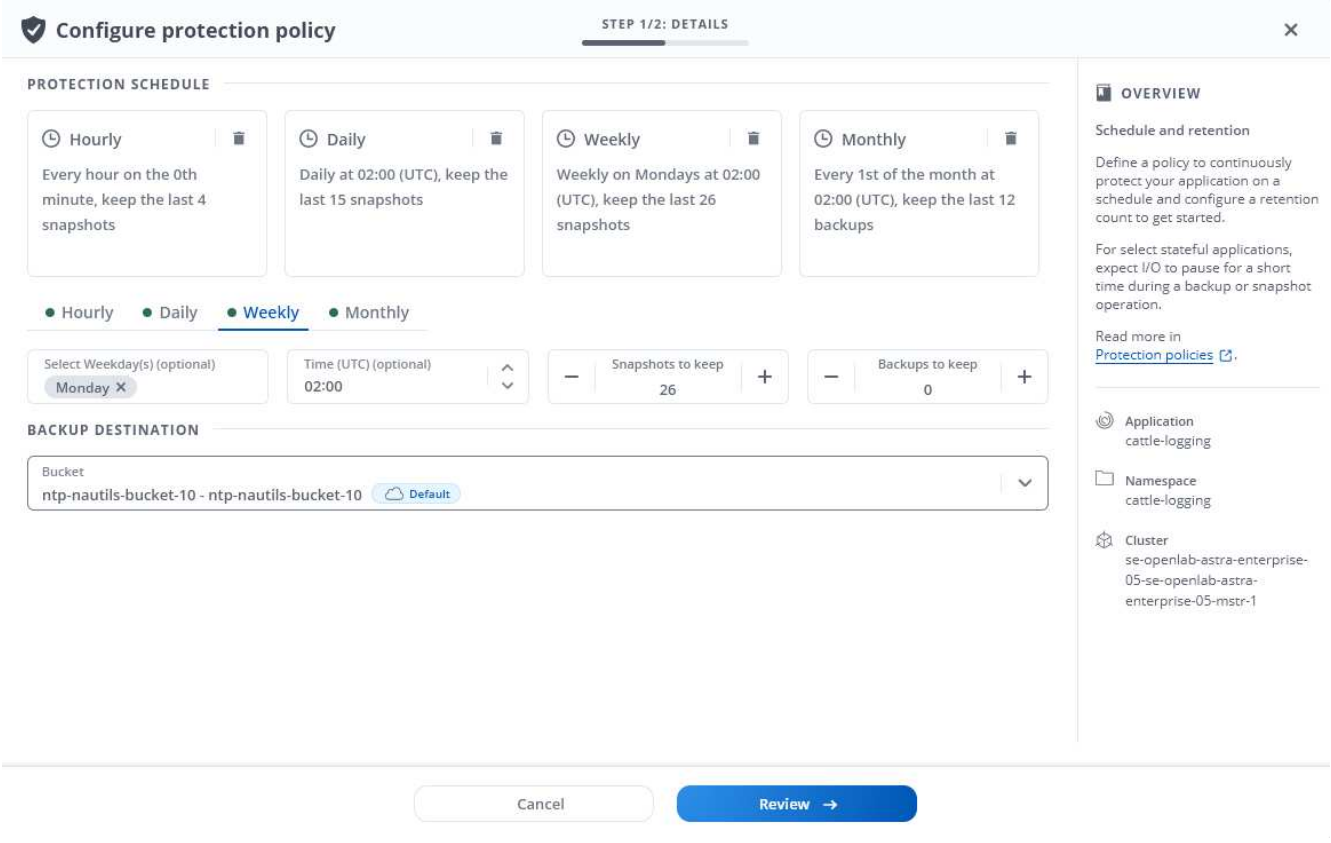
Una policy di protezione protegge un'applicazione creando snapshot, backup o entrambi in base a una pianificazione definita. È possibile scegliere di creare snapshot e backup ogni ora, ogni giorno, ogni settimana e ogni mese, nonché specificare il numero di copie da conservare. Ad esempio, una policy di protezione potrebbe creare backup settimanali e snapshot giornalieri e conservare backup e snapshot per un mese. La frequenza con cui vengono creati snapshot e backup e la durata della conservazione dipendono dalle esigenze dell'organizzazione.

#### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Configura policy di protezione**.
4. Definire un programma di protezione scegliendo il numero di snapshot e backup da conservare ogni ora, ogni giorno, ogni settimana e ogni mese.

   È possibile definire le pianificazioni orarie, giornaliere, settimanali e mensili contemporaneamente. Un programma non diventa attivo fino a quando non viene impostato un livello di conservazione.

   Nell'esempio seguente vengono impostati quattro programmi di protezione: ogni ora, ogni giorno, ogni settimana e ogni mese per snapshot e backup.




5. Selezionare **Revisione**.
6. Selezionare **Imposta policy di protezione.**

### Risultato

Astra Control Center implementa la policy di protezione dei dati creando e conservando snapshot e backup utilizzando i criteri di pianificazione e conservazione definiti dall'utente.

## Creare un'istantanea

Puoi creare uno snapshot on-demand in qualsiasi momento.

### Fasi

1. Selezionare **applicazioni**.
2. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) dell'applicazione desiderata, selezionare **Snapshot**.
3. Personalizzare il nome dell'istantanea, quindi selezionare **Review** (Rivedi).
4. Esaminare il riepilogo dell'istantanea e selezionare **Snapshot**.

### Risultato

Viene avviato il processo di snapshot. Un'istantanea viene eseguita correttamente quando lo stato è **Available** nella colonna **Actions** nella pagina **Data Protection** > **Snapshots**.

## Creare un backup

Puoi anche eseguire il backup di un'applicazione in qualsiasi momento.

> I bucket S3 in Astra Control Center non riportano la capacità disponibile. Prima di eseguire il backup o la clonazione delle applicazioni gestite da Astra Control Center, controllare le informazioni del bucket nel sistema di gestione ONTAP o StorageGRID.

**Fasi**

1. Selezionare **applicazioni**.
2. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) dell'applicazione desiderata, selezionare **Backup**.
3. Personalizzare il nome del backup.
4. Scegliere se eseguire il backup dell'applicazione da uno snapshot esistente. Se si seleziona questa opzione, è possibile scegliere da un elenco di snapshot esistenti.
5. Scegliere una destinazione per il backup selezionandola dall'elenco dei bucket di storage.
6. Selezionare **Revisione**.
7. Esaminare il riepilogo del backup e selezionare **Backup**.

**Risultato**

Astra Control Center crea un backup dell'applicazione.

> Se la rete presenta un'interruzione o è eccessivamente lenta, potrebbe verificarsi un timeout dell'operazione di backup. In questo modo, il backup non viene eseguito correttamente.

> Non esiste alcun modo per interrompere un backup in esecuzione. Se è necessario eliminare il backup, attendere che sia stato completato, quindi seguire le istruzioni riportate in Eliminare i backup. Per eliminare un backup non riuscito, "Utilizzare l'API di controllo Astra".

> Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

### Visualizzare snapshot e backup

È possibile visualizzare le istantanee e i backup di un'applicazione dalla scheda Data Protection (protezione dati).

**Fasi**

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).

   Le istantanee vengono visualizzate per impostazione predefinita.

3. Selezionare **Backup** per visualizzare l'elenco dei backup.

### Eliminare le istantanee

Eliminare le snapshot pianificate o on-demand non più necessarie.

#### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per lo snapshot desiderato, selezionare **Delete snapshot** (Elimina snapshot).
4. Digitare la parola "DELETE" per confermare l'eliminazione, quindi selezionare **Yes, Delete snapshot**.

#### Risultato

Astra Control Center elimina lo snapshot.

### Eliminare i backup

Eliminare i backup pianificati o on-demand non più necessari.

> Non esiste alcun modo per interrompere un backup in esecuzione. Se è necessario eliminare il backup, attendere che sia stato completato, quindi seguire queste istruzioni. Per eliminare un backup non riuscito, "Utilizzare l'API di controllo Astra".

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Backup**.
4. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per il backup desiderato, selezionare **Delete backup** (Elimina backup).
5. Digitare la parola "DELETE" per confermare l'eliminazione, quindi selezionare **Yes, Delete backup**.

#### Risultato

Astra Control Center elimina il backup.

## Ripristinare le applicazioni

Astra Control può ripristinare l'applicazione da uno snapshot o da un backup. Il ripristino da uno snapshot esistente sarà più rapido quando si ripristina l'applicazione nello stesso cluster. È possibile utilizzare l'interfaccia utente di Astra Control o. "L'API Astra Control" per ripristinare le applicazioni.

#### A proposito di questa attività

- Si consiglia vivamente di eseguire un'istantanea o un backup dell'applicazione prima di ripristinarla. In questo modo, è possibile clonare lo snapshot o il backup nel caso in cui il ripristino non abbia esito positivo.
- Se utilizzi Helm per implementare le app, Astra Control Center richiede Helm versione 3. La gestione e la clonazione delle applicazioni implementate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. Le app implementate con Helm 2 non sono supportate.
- Se si esegue il ripristino in un cluster diverso, assicurarsi che il cluster utilizzi la stessa modalità di accesso al volume persistente (ad esempio ReadWriteMany). L'operazione di ripristino non riesce se la modalità di accesso al volume persistente di destinazione è diversa.
- Qualsiasi utente membro con vincoli di spazio dei nomi in base al nome/ID dello spazio dei nomi o alle etichette dello spazio dei nomi può clonare o ripristinare un'applicazione in un nuovo spazio dei nomi nello

stesso cluster o in qualsiasi altro cluster dell'account dell'organizzazione. Tuttavia, lo stesso utente non può accedere all'applicazione clonata o ripristinata nel nuovo namespace. Dopo la creazione di un nuovo spazio dei nomi mediante un'operazione di clone o ripristino, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo per consentire all'utente interessato di accedere al nuovo spazio dei nomi.

- Quando crei un progetto per ospitare un'applicazione su un cluster OpenShift, al progetto (o namespace Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

**Fasi**

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection**.
3. Se si desidera eseguire il ripristino da uno snapshot, tenere selezionata l'icona **Snapshot**. In caso contrario, selezionare l'icona **Backup** per eseguire il ripristino da un backup.
4. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per lo snapshot o il backup da cui si desidera eseguire il ripristino, selezionare **Restore application** (Ripristina applicazione).
5. **Restore details** (Dettagli ripristino): Specificare i dettagli dell'applicazione ripristinata. Per impostazione predefinita, vengono visualizzati il cluster e lo spazio dei nomi correnti. Lasciare intatti questi valori per ripristinare un'applicazione in-place, che ripristina l'applicazione a una versione precedente di se stessa. Modificare questi valori se si desidera ripristinare un cluster o uno spazio dei nomi diverso.
   - Immettere un nome e uno spazio dei nomi per l'applicazione.
   - Scegliere il cluster di destinazione per l'applicazione.
   - Selezionare **Revisione**.

   > Se si ripristina uno spazio dei nomi precedentemente cancellato, viene creato un nuovo spazio dei nomi con lo stesso nome come parte del processo di ripristino. Tutti gli utenti che disponevano dei diritti per gestire le applicazioni nello spazio dei nomi precedentemente cancellato devono ripristinare manualmente i diritti nello spazio dei nomi appena ricreato.

6. **Restore Summary** (Riepilogo ripristino): Esaminare i dettagli relativi all'azione di ripristino, digitare "restore" e selezionare **Restore**.

**Risultato**

Astra Control Center ripristina l'applicazione in base alle informazioni fornite. Se hai ripristinato l'applicazione in-place, il contenuto di eventuali volumi persistenti esistenti viene sostituito con il contenuto dei volumi persistenti dell'applicazione ripristinata.

Dopo un'operazione di protezione dei dati (cloning, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo fino a venti minuti prima che la nuova dimensione del volume venga visualizzata nell'interfaccia utente Web. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

## Clonare e migrare le applicazioni

Clonare un'applicazione esistente per creare un'applicazione duplicata sullo stesso cluster Kubernetes o su un altro cluster. Quando Astra Control Center clona un'applicazione, crea un clone della configurazione dell'applicazione e dello storage persistente.

La clonazione può essere di aiuto nel caso in cui sia necessario spostare applicazioni e storage da un cluster Kubernetes a un altro. Ad esempio, è possibile spostare i carichi di lavoro attraverso una pipeline ci/CD e attraverso gli spazi dei nomi Kubernetes. È possibile utilizzare l'interfaccia utente Astra o. "L'API Astra Control" per clonare e migrare le applicazioni.

### Di cosa hai bisogno

Per clonare le applicazioni in un cluster diverso, è necessario un bucket predefinito. Quando si aggiunge il primo bucket, questo diventa quello predefinito.

### A proposito di questa attività

- Se si implementa un'applicazione con un StorageClass esplicitamente impostato e si deve clonare l'applicazione, il cluster di destinazione deve avere la StorageClass specificata in origine. Il cloning di un'applicazione con un StorageClass esplicitamente impostato su un cluster che non ha lo stesso StorageClass avrà esito negativo.
- Se si clonano istanze distribuite dall'operatore di Jenkins ci, è necessario ripristinare manualmente i dati persistenti. Si tratta di un limite del modello di implementazione dell'applicazione.
- I bucket S3 in Astra Control Center non riportano la capacità disponibile. Prima di eseguire il backup o la clonazione delle applicazioni gestite da Astra Control Center, controllare le informazioni del bucket nel sistema di gestione ONTAP o StorageGRID.
- Durante il backup di un'applicazione o il ripristino di un'applicazione, è possibile specificare un ID bucket. Un'operazione di cloni dell'applicazione, tuttavia, utilizza sempre il bucket predefinito definito. Non esiste alcuna opzione per modificare i bucket per un clone. Se si desidera controllare quale bucket viene utilizzato, è possibile farlo "modificare l'impostazione predefinita del bucket" oppure fare una "backup" seguito da un "ripristinare" separatamente.
- Qualsiasi utente membro con vincoli di spazio dei nomi in base al nome/ID dello spazio dei nomi o alle etichette dello spazio dei nomi può clonare o ripristinare un'applicazione in un nuovo spazio dei nomi nello stesso cluster o in qualsiasi altro cluster dell'account dell'organizzazione. Tuttavia, lo stesso utente non può accedere all'applicazione clonata o ripristinata nel nuovo namespace. Dopo la creazione di un nuovo spazio dei nomi mediante un'operazione di clone o ripristino, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo per consentire all'utente interessato di accedere al nuovo spazio dei nomi.

### Considerazioni su OpenShift

- Se clonate un'applicazione tra cluster, i cluster di origine e di destinazione devono essere della stessa distribuzione di OpenShift. Ad esempio, se clonate un'applicazione da un cluster OpenShift 4.7, utilizzate un cluster di destinazione che è anche OpenShift 4.7.

- Quando crei un progetto per ospitare un'applicazione su un cluster OpenShift, al progetto (o namespace Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

**Fasi**

1. Selezionare **applicazioni**.
2. Effettuare una delle seguenti operazioni:
   - Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per l'applicazione desiderata.
   - Selezionare il nome dell'applicazione desiderata e l'elenco a discesa Status (Stato) in alto a destra nella pagina.
3. Selezionare **Clone**.
4. **Clone Details**: Specificare i dettagli per il clone:
   - Immettere un nome.
   - Immettere uno spazio dei nomi per il clone.
   - Scegliere un cluster di destinazione per il clone.
   - Scegliere se si desidera creare il clone da uno snapshot o da un backup esistente. Se non si seleziona questa opzione, Astra Control Center crea il clone dallo stato corrente dell'applicazione.
5. **Origine**: Se si sceglie di clonare da uno snapshot o da un backup esistente, scegliere lo snapshot o il backup che si desidera utilizzare.
6. Selezionare **Revisione**.
7. **Clone Summary**: Leggi i dettagli sul clone e seleziona **Clone**.

**Risultato**

Astra Control Center clona l'applicazione in base alle informazioni fornite. L'operazione di clonazione viene eseguita correttamente quando il nuovo clone dell'applicazione si trova in `Available` nella pagina **applicazioni**.

> Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

## Gestire gli hook di esecuzione delle applicazioni

Un gancio di esecuzione è uno script personalizzato che è possibile eseguire prima o dopo uno snapshot di un'applicazione gestita. Ad esempio, se si dispone di un'applicazione di database, è possibile utilizzare i ganci di esecuzione per sospendere tutte le transazioni del database prima di uno snapshot e riprendere le transazioni dopo il

completamento dello snapshot. Ciò garantisce snapshot coerenti con l'applicazione.

### Hook di esecuzione predefiniti ed espressioni regolari

Per alcune applicazioni, Astra Control viene fornito con gli hook di esecuzione predefiniti, forniti da NetApp, che gestiscono le operazioni di blocco e scongelamento prima e dopo le snapshot. Astra Control utilizza espressioni regolari per associare l'immagine container di un'applicazione a queste applicazioni:

- MariaDB
  - Espressione regolare corrispondente
- MySQL
  - Espressione regolare corrispondente
- PostgreSQL
  - Espressione regolare corrispondente

In caso di corrispondenza, gli hook di esecuzione predefiniti forniti da NetApp per l'applicazione vengono visualizzati nell'elenco degli hook di esecuzione attivi dell'applicazione, che vengono eseguiti automaticamente quando vengono eseguite le istantanee dell'applicazione. Se una delle applicazioni personalizzate ha un nome immagine simile che corrisponde a una delle espressioni regolari (e non si desidera utilizzare gli hook di esecuzione predefiniti), è possibile modificare il nome dell'immagine, oppure disattiva il gancio di esecuzione predefinito per l'applicazione e utilizza un gancio personalizzato.

Non è possibile eliminare o modificare gli hook di esecuzione predefiniti.

### Note importanti sugli hook di esecuzione personalizzati

Quando si pianificano gli hook di esecuzione per le applicazioni, considerare quanto segue.

- Astra Control richiede che gli hook di esecuzione siano scritti nel formato degli script di shell eseguibili.
- La dimensione dello script è limitata a 128 KB.
- Astra Control utilizza le impostazioni di esecuzione degli hook e qualsiasi criterio di corrispondenza per determinare quali hook sono applicabili a uno snapshot.
- Tutti i guasti degli uncini di esecuzione sono guasti di tipo soft; altri hook e snapshot vengono ancora tentati anche se un hook non funziona. Tuttavia, quando un gancio non funziona, viene registrato un evento di avviso nel registro eventi della pagina **attività**.
- Per creare, modificare o eliminare gli hook di esecuzione, è necessario essere un utente con autorizzazioni Owner, Admin o Member.
- Se l'esecuzione di un gancio di esecuzione richiede più di 25 minuti, l'hook non riesce, creando una voce del registro eventi con un codice di ritorno "N/A". Qualsiasi snapshot interessata verrà contrassegnata come non riuscita e una voce del registro eventi risultante annoterà il timeout.

> Poiché gli hook di esecuzione spesso riducono o disattivano completamente le funzionalità dell'applicazione con cui vengono eseguiti, è consigliabile ridurre al minimo il tempo necessario per l'esecuzione degli hook di esecuzione personalizzati.

Quando viene eseguita una snapshot, gli eventi di esecuzione hook hanno luogo nel seguente ordine:

1. Tutti gli hook di esecuzione pre-snapshot predefiniti forniti da NetApp applicabili vengono eseguiti sui container appropriati.

2. Tutti gli hook di esecuzione pre-snapshot personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook pre-snapshot personalizzati necessari, ma l'ordine di esecuzione di questi hook prima dell'istantanea non è garantito né configurabile.
3. Viene eseguita l'istantanea.
4. Tutti gli hook di esecuzione post-snapshot personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook post-snapshot personalizzati necessari, ma l'ordine di esecuzione di questi hook dopo l'istantanea non è garantito né configurabile.
5. Tutti gli hook di esecuzione post-snapshot predefiniti forniti da NetApp applicabili vengono eseguiti sui container appropriati.

> Prima di abilitarli in un ambiente di produzione, è necessario verificare sempre gli script hook di esecuzione. È possibile utilizzare il comando 'kubectl exec' per testare comodamente gli script. Dopo aver attivato gli hook di esecuzione in un ambiente di produzione, testare le snapshot risultanti per assicurarsi che siano coerenti. Per eseguire questa operazione, clonare l'applicazione in uno spazio dei nomi temporaneo, ripristinare lo snapshot e quindi testare l'applicazione.

### Visualizzare gli hook di esecuzione esistenti

È possibile visualizzare gli hook di esecuzione predefiniti personalizzati o forniti da NetApp per un'applicazione.

#### Fasi

1. Accedere a **applicazioni** e selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.

   È possibile visualizzare tutti gli hook di esecuzione attivati o disattivati nell'elenco risultante. È possibile visualizzare lo stato, l'origine e il momento dell'esecuzione di un gancio (pre o post-snapshot). Per visualizzare i registri degli eventi che circondano gli hook di esecuzione, accedere alla pagina **Activity** nell'area di navigazione a sinistra.

### Creare un gancio di esecuzione personalizzato

È possibile creare un gancio di esecuzione personalizzato per un'applicazione. Vedere "Esempi di gancio di esecuzione" per esempi di gancio. Per creare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner (Proprietario), Admin (Amministratore) o Member (membro).

> Quando si crea uno script shell personalizzato da utilizzare come uncino di esecuzione, ricordarsi di specificare la shell appropriata all'inizio del file, a meno che non si stiano eseguendo comandi linux o fornendo il percorso completo di un eseguibile.

#### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare **Aggiungi un nuovo gancio**.
4. Nell'area **Dettagli gancio**, a seconda dell'esecuzione del gancio, scegliere **Pre-Snapshot** o **Post-Snapshot**.
5. Immettere un nome univoco per l'hook.

6. (Facoltativo) inserire gli argomenti da passare al gancio durante l'esecuzione, premendo il tasto Invio dopo ogni argomento inserito per registrarne ciascuno.
7. Nell'area **Container Images** (immagini container), se il gancio deve essere eseguito su tutte le immagini container contenute nell'applicazione, attivare la casella di controllo **Apply to all container images** (Applica a tutte le immagini container). Se invece il gancio dovrebbe agire solo su una o più immagini container specificate, inserire i nomi delle immagini container nel campo **nomi delle immagini container da abbinare**.
8. Nell'area **script**, eseguire una delle seguenti operazioni:
   - Caricare uno script personalizzato.
     i. Selezionare l'opzione **carica file**.
     ii. Selezionare un file e caricarlo.
     iii. Assegnare allo script un nome univoco.
     iv. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
   - Incollare uno script personalizzato dagli Appunti.
     i. Selezionare l'opzione **Incolla dagli Appunti**.
     ii. Selezionare il campo di testo e incollare il testo dello script nel campo.
     iii. Assegnare allo script un nome univoco.
     iv. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
9. Selezionare **Aggiungi gancio**.

### Disattiva un gancio di esecuzione

È possibile disattivare un gancio di esecuzione se si desidera impedirne temporaneamente l'esecuzione prima o dopo un'istantanea di un'applicazione. Per disattivare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner, Admin o Member.

#### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per un gancio che si desidera disattivare.
4. Selezionare **Disable** (Disattiva).

### Eliminare un gancio di esecuzione

È possibile rimuovere completamente un gancio di esecuzione se non è più necessario. Per eliminare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner, Admin o Member.

#### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per il gancio che si desidera eliminare.
4. Selezionare **Delete** (Elimina).

#### Esempi di gancio di esecuzione

USA i seguenti esempi per avere un'idea di come strutturare i tuoi hook di esecuzione. È possibile utilizzare questi ganci come modelli o come script di test.

##### Semplice esempio di successo

Questo è un esempio di un semplice hook che riesce e scrive un messaggio in output standard e in errore standard.

```
#!/bin/sh

# success_sample.sh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}
```

```
#
# main
#

# log something to stdout
info "running success_sample.sh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

#### Semplice esempio di successo (versione bash)

Questo è un esempio di un semplice hook che riesce e scrive un messaggio in output standard e standard error, scritto per bash.

```
#!/bin/bash

# success_sample.bash
#
# A simple noop success hook script for testing purposes.
#
# args: None


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}
```

```
#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample.bash"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

#### Semplice esempio di successo (versione zsh)

Questo è un esempio di un semplice hook che riesce e scrive un messaggio in output standard e errore standard, scritto per la shell Z.

```
#!/bin/zsh

# success_sample.zsh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}
```

```
#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.zsh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

#### Esempio di successo con argomenti

Nell’esempio riportato di seguito viene illustrato come utilizzare gli ARG in un gancio.

```
#!/bin/sh

# success_sample_args.sh
#
# A simple success hook script with args for testing purposes.
#
# args: Up to two optional args that are echoed to stdout

#
# Writes the given message to standard output
#
# $* - The message to write
#
```

```
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample_args.sh"


# collect args
arg1=$1
arg2=$2

# output args and arg count to stdout
info "number of args: $#"
info "arg1 ${arg1}"
info "arg2 ${arg2}"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

#### Esempio di gancio pre-snapshot/post-snapshot

Nell'esempio seguente viene illustrato come utilizzare lo stesso script sia per un hook pre-snapshot che per un hook post-snapshot.

```
#!/bin/sh

# success_sample_pre_post.sh
#
# A simple success hook script example with an arg for testing purposes
# to demonstrate how the same script can be used for both a prehook and
posthook
#
# args: [pre|post]

# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))
epost=$((ebase+4))


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
```

```
error() {
    msg "ERROR: $*" 1>&2
}


#
# Would run prehook steps here
#
prehook() {
    info "Running noop prehook"
    return 0
}

#
# Would run posthook steps here
#
posthook() {
    info "Running noop posthook"
    return 0
}


#
# main
#

# check arg
stage=$1
if [ -z "${stage}" ]; then
    echo "Usage: $0 <pre|post>"
    exit ${eusage}
fi

if [ "${stage}" != "pre" ] && [ "${stage}" != "post" ]; then
    echo "Invalid arg: ${stage}"
    exit ${ebadstage}
fi

# log something to stdout
info "running success_sample_pre_post.sh"

if [ "${stage}" = "pre" ]; then
    prehook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during prehook"
```

```
    fi
fi

if [ "${stage}" = "post" ]; then
    posthook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during posthook"
    fi
fi

exit ${rc}
```

#### Esempio di guasto

Nell’esempio riportato di seguito viene illustrato come gestire gli errori in un hook.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}
```

```
#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

#### Esempio di errore dettagliato

Nell'esempio riportato di seguito viene illustrato come gestire gli errori in modo semplice, con una registrazione più dettagliata.

```
#!/bin/sh

# failure_sample_verbose.sh
#
# A simple failure hook script with args for testing purposes.
#
# args: [The number of lines to output to stdout]


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
```

```
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_verbose.sh"


# output arg value to stdout
linecount=$1
info "line count ${linecount}"

# write out a line to stdout based on line count arg
i=1
while [ "$i" -le ${linecount} ]; do
    info "This is line ${i} from failure_sample_verbose.sh"
    i=$(( i + 1 ))
done

error "exiting with error code 8"
exit 8
```

#### Errore con un esempio di codice di uscita

Nell'esempio riportato di seguito viene illustrato un errore di hook con un codice di uscita.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#
```

```
# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

#### Esempio di successo dopo il guasto

Nell'esempio riportato di seguito viene illustrato un errore di hook alla prima esecuzione, ma dopo la seconda esecuzione.

```
#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for
testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}
```

```
#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_success sample.sh"


if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist.  Removing /tmp/hook-test.junk"
    rm /tmp/hook-test.junk
    info "Second run so returning exit code 0"
    exit 0
else
    info "File does not exist.  Creating /tmp/hook-test.junk"
    echo "test" > /tmp/hook-test.junk
    error "Failed first run, returning exit code 5"
    exit 5
fi
```

# Visualizzare lo stato delle applicazioni e del cluster

## Visualizza un riepilogo dello stato delle applicazioni e dei cluster

Seleziona la * dashboard* per visualizzare una vista di alto livello delle tue app, cluster, backend di storage e della loro salute.

Questi non sono solo numeri statici o stati, ma puoi eseguire il drill-down da ciascuno di essi. Ad esempio, se le applicazioni non sono completamente protette, puoi passare il mouse sull'icona per identificare le applicazioni non completamente protette, il che include un motivo.

#### Sezione applicazioni

La sezione **applicazioni** consente di identificare quanto segue:

- Quante app stai attualmente gestendo con Astra.

- Se queste applicazioni gestite sono in buona salute.
- Se le applicazioni sono completamente protette (sono protette se sono disponibili backup recenti).
- Il numero di applicazioni rilevate, ma non ancora gestite.

  Idealmente, questo numero sarebbe pari a zero perché, una volta scoperte, gestireste o ignorereste le applicazioni. Quindi, è necessario monitorare il numero di applicazioni rilevate nella dashboard per identificare quando gli sviluppatori aggiungono nuove applicazioni a un cluster.

#### Riquadro dei cluster

Il riquadro **Clusters** fornisce dettagli simili sullo stato dei cluster gestiti tramite Astra Control Center e consente di analizzare più dettagli come con un'applicazione.

#### Riquadro backend storage

Il riquadro **Storage backend** fornisce informazioni utili per identificare lo stato dei back-end dello storage, tra cui:

- Quanti backend di storage vengono gestiti
- Se questi backend gestiti sono in buono stato
- Se i backend sono completamente protetti
- Il numero di backend rilevati, ma non ancora gestiti.

## Visualizza lo stato di salute e i dettagli dei cluster

Dopo aver aggiunto i cluster da gestire da Astra Control Center, è possibile visualizzare i dettagli del cluster, ad esempio la sua posizione, i nodi di lavoro, i volumi persistenti e le classi di storage.

#### Fasi

1. Nell'interfaccia utente di Astra Control Center, selezionare **Clusters**.
2. Nella pagina **Clusters**, selezionare il cluster di cui si desidera visualizzare i dettagli.

   > Se un cluster si trova in `removed` state Yet la connettività di rete e del cluster sembra sana (i tentativi esterni di accesso al cluster utilizzando le API di Kubernetes sono riusciti), il kubeconfig che hai fornito ad Astra Control potrebbe non essere più valido. Ciò può essere dovuto alla rotazione o alla scadenza del certificato sul cluster. Per risolvere questo problema, aggiornare le credenziali associate al cluster in Astra Control utilizzando "API di controllo Astra".

3. Visualizzare le informazioni nelle schede **Overview**, **Storage** e **Activity** per trovare le informazioni desiderate.
   - **Panoramica**: Dettagli sui nodi di lavoro, incluso il loro stato.
   - **Storage**: I volumi persistenti associati al calcolo, inclusi la classe e lo stato dello storage.
   - **Attività**: Mostra le attività correlate al cluster.

È inoltre possibile visualizzare le informazioni sul cluster partendo da Astra Control Center **Dashboard**. Nella scheda **Clusters** sotto **Riepilogo risorse**, è possibile selezionare i cluster gestiti, che consentono di accedere alla pagina **Clusters**. Una volta visualizzata la pagina **Clusters**, seguire la procedura descritta in precedenza.

## Visualizza lo stato di salute e i dettagli di un'applicazione

Dopo aver iniziato a gestire un'applicazione, Astra fornisce informazioni dettagliate sull'applicazione che consentono di identificarne lo stato (se è integro), lo stato di protezione (se è completamente protetto in caso di guasto), i pod, lo storage persistente e molto altro ancora.

**Fasi**

1. Nell'interfaccia utente di Astra Control Center, selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Trova le informazioni che cerchi:

   **Stato dell'app**

   Fornisce uno stato che riflette lo stato dell'applicazione in Kubernetes. Ad esempio, i pod e i volumi persistenti sono online? Se un'applicazione non è in buone condizioni, è necessario risolvere il problema sul cluster osservando i log di Kubernetes. Astra non fornisce informazioni utili per la risoluzione di un'applicazione guasta.

   **Stato di protezione dell'app**

   Fornisce uno stato di protezione dell'applicazione:

   - **Completamente protetto**: L'applicazione dispone di una pianificazione di backup attiva e di un backup riuscito che risale a meno di una settimana fa
   - **Protezione parziale**: L'applicazione dispone di una pianificazione di backup attiva, di una pianificazione di snapshot attiva o di un backup o snapshot riuscito
   - **Non protetto**: Applicazioni non completamente protette o parzialmente protette.

     *Non è possibile essere completamente protetti fino a quando non si dispone di un backup recente*. Ciò è importante perché i backup vengono memorizzati in un archivio a oggetti lontano dai volumi persistenti. Se un guasto o un incidente cancella il cluster e lo storage persistente, è necessario un backup per il ripristino. Un'istantanea non ti consentirebbe di ripristinarla.

   **Panoramica**

   Informazioni sullo stato dei pod associati all'applicazione.

   **Protezione dei dati**

   Consente di configurare una policy di protezione dei dati e di visualizzare le snapshot e i backup esistenti.

   **Storage**

   Mostra i volumi persistenti a livello di applicazione. Lo stato di un volume persistente è dal punto di vista del cluster Kubernetes.

**Risorse**

Consente di verificare quali risorse vengono sottoposte a backup e gestite.

**Attività**

Mostra le attività correlate all'applicazione.

> È inoltre possibile visualizzare le informazioni dell'applicazione partendo da Astra Control Center **Dashboard**. Nella scheda **applicazioni** sotto **Riepilogo risorse**, è possibile selezionare le applicazioni gestite, che consentono di accedere alla pagina **applicazioni**. Una volta visualizzata la pagina **applicazioni**, seguire la procedura descritta in precedenza.

# Gestisci il tuo account

## Gestire gli utenti

È possibile invitare, aggiungere, rimuovere e modificare gli utenti dell'installazione di Astra Control Center utilizzando l'interfaccia utente di Astra Control. È possibile utilizzare l'interfaccia utente di Astra Control o. "L'API Astra Control" per gestire gli utenti.

### Invitare utenti

I proprietari e gli amministratori degli account possono invitare nuovi utenti ad Astra Control Center.

**Fasi**

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Selezionare **invita utente**.
4. Immettere il nome e l'indirizzo e-mail dell'utente.
5. Selezionare un ruolo utente con le autorizzazioni di sistema appropriate.

   Ciascun ruolo fornisce le seguenti autorizzazioni:

   - Un **Viewer** può visualizzare le risorse.
   - Un **Member** dispone delle autorizzazioni per il ruolo Viewer e può gestire app e cluster, annullare la gestione delle app ed eliminare snapshot e backup.
   - Un **Admin** dispone delle autorizzazioni di ruolo membro e può aggiungere e rimuovere qualsiasi altro utente ad eccezione del Proprietario.
   - Un **Owner** dispone delle autorizzazioni di ruolo Admin e può aggiungere e rimuovere qualsiasi account utente.
6. Per aggiungere vincoli a un utente con ruolo membro o visualizzatore, attivare la casella di controllo **limita ruolo ai vincoli**.

   Per ulteriori informazioni sull'aggiunta di vincoli, vedere "Gestire i ruoli".

7. Selezionare **invita utenti**.

   L'utente riceve un'e-mail per informarlo che è stato invitato ad Astra Control Center. L'e-mail include la password temporanea, che dovrà essere modificata al primo accesso.

### Aggiungere utenti

Gli account Owner e gli amministratori possono aggiungere altri utenti all'installazione di Astra Control Center.

#### Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Selezionare **Aggiungi utente**.
4. Immettere il nome dell'utente, l'indirizzo e-mail e una password temporanea.

   L'utente dovrà modificare la password al primo accesso.

5. Selezionare un ruolo utente con le autorizzazioni di sistema appropriate.

   Ciascun ruolo fornisce le seguenti autorizzazioni:

   - Un **Viewer** può visualizzare le risorse.
   - Un **Member** dispone delle autorizzazioni per il ruolo Viewer e può gestire app e cluster, annullare la gestione delle app ed eliminare snapshot e backup.
   - Un **Admin** dispone delle autorizzazioni di ruolo membro e può aggiungere e rimuovere qualsiasi altro utente ad eccezione del Proprietario.
   - Un **Owner** dispone delle autorizzazioni di ruolo Admin e può aggiungere e rimuovere qualsiasi account utente.

6. Per aggiungere vincoli a un utente con ruolo membro o visualizzatore, attivare la casella di controllo **limita ruolo ai vincoli**.

   Per ulteriori informazioni sull'aggiunta di vincoli, vedere "Gestire i ruoli".

7. Selezionare **Aggiungi**.

### Gestire le password

Puoi gestire le password per gli account utente in Astra Control Center.

#### Modificare la password

È possibile modificare la password dell'account utente in qualsiasi momento.

#### Fasi

1. Selezionare l'icona User (utente) nella parte superiore destra della schermata.
2. Selezionare **Profilo**.
3. Dal menu Opzioni nella colonna **azioni** e selezionare **Modifica password**.
4. Immettere una password conforme ai requisiti.
5. Immettere nuovamente la password per confermare.
6. Selezionare **Cambia password**.

#### Reimpostare la password di un altro utente

Se l'account dispone delle autorizzazioni di ruolo Amministratore o Proprietario, è possibile reimpostare le

password per altri account utente e per i propri. Quando si reimposta una password, si assegna una password temporanea che l'utente dovrà modificare al momento dell'accesso.

**Fasi**

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare l'elenco a discesa **azioni**.
3. Selezionare **Reset Password** (Ripristina password).
4. Immettere una password temporanea conforme ai requisiti della password.
5. Immettere nuovamente la password per confermare.

   Al successivo accesso, all'utente verrà richiesto di modificare la password.

6. Selezionare **Ripristina password**.

### Modificare il ruolo di un utente

Gli utenti con il ruolo Owner possono modificare il ruolo di tutti gli utenti, mentre gli utenti con il ruolo Admin possono modificare il ruolo degli utenti con il ruolo Admin, Member o Viewer.

**Fasi**

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare l'elenco a discesa **azioni**.
3. Selezionare **Modifica ruolo**.
4. Selezionare un nuovo ruolo.
5. Per applicare i vincoli al ruolo, attivare la casella di controllo **limita ruolo ai vincoli** e selezionare un vincolo dall'elenco.

   Se non ci sono vincoli, è possibile aggiungere un vincolo. Per ulteriori informazioni, vedere "Gestire i ruoli".

6. Selezionare **Conferma**.

**Risultato**

Astra Control Center aggiorna le autorizzazioni dell'utente in base al nuovo ruolo selezionato.

### Rimuovere gli utenti

Gli utenti con il ruolo Owner (Proprietario) o Admin (Amministratore) possono rimuovere altri utenti dall'account in qualsiasi momento.

**Fasi**

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Nella scheda **utenti**, selezionare la casella di controllo nella riga di ciascun utente che si desidera rimuovere.
3. Dal menu Options (Opzioni) nella colonna **Actions** (azioni), selezionare **Remove user/s** (Rimuovi utenti).
4. Quando richiesto, confermare l'eliminazione digitando la parola "remove", quindi selezionare **Yes, Remove User** (Sì, Rimuovi utente).

**Risultato**

Astra Control Center rimuove l'utente dall'account.

## Gestire i ruoli

È possibile gestire i ruoli aggiungendo vincoli dello spazio dei nomi e limitando i ruoli utente a tali vincoli. In questo modo è possibile controllare l'accesso alle risorse all'interno dell'organizzazione. È possibile utilizzare l'interfaccia utente di Astra Control o. "L'API Astra Control" per gestire i ruoli.

### Aggiungere un vincolo dello spazio dei nomi a un ruolo

Un utente Admin o Owner può aggiungere vincoli dello spazio dei nomi.

#### Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore.
4. Selezionare **Modifica ruolo**.
5. Attivare la casella di controllo **limita ruolo ai vincoli**.

   La casella di controllo è disponibile solo per i ruoli Member o Viewer. È possibile selezionare un ruolo diverso dall'elenco a discesa **ruolo**.

6. Selezionare **Aggiungi vincolo**.

   È possibile visualizzare l'elenco dei vincoli disponibili in base allo spazio dei nomi o all'etichetta dello spazio dei nomi.

7. Nell'elenco a discesa **tipo di vincolo**, selezionare **spazio dei nomi Kubernetes** o **etichetta dello spazio dei nomi Kubernetes** a seconda della configurazione degli spazi dei nomi.
8. Selezionare uno o più spazi dei nomi o etichette dall'elenco per comporre un vincolo che limiti i ruoli a tali spazi dei nomi.
9. Selezionare **Conferma**.

   La pagina **Modifica ruolo** visualizza l'elenco dei vincoli scelti per questo ruolo.

10. Selezionare **Conferma**.

    Nella pagina **account**, è possibile visualizzare i vincoli per qualsiasi ruolo membro o visualizzatore nella colonna **ruolo**.

> Se si abilitano i vincoli per un ruolo e si seleziona **Conferma** senza aggiungere alcun vincolo, il ruolo viene considerato con restrizioni complete (al ruolo viene negato l'accesso a tutte le risorse assegnate agli spazi dei nomi).

### Rimuovere un vincolo dello spazio dei nomi da un ruolo

Un utente Admin o Owner può rimuovere un vincolo dello spazio dei nomi da un ruolo.

#### Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.

2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore con vincoli attivi.
4. Selezionare **Modifica ruolo**.

   La finestra di dialogo **Modifica ruolo** visualizza i vincoli attivi per il ruolo.

5. Selezionare la **X** a destra del vincolo da rimuovere.
6. Selezionare **Conferma**.

#### Per ulteriori informazioni

- "Ruoli e spazi dei nomi degli utenti"

## Visualizzare e gestire le notifiche

Astra informa l'utente quando le azioni sono state completate o non sono riuscite. Ad esempio, se il backup di un'applicazione è stato completato correttamente, viene visualizzata una notifica.

È possibile gestire queste notifiche dall'alto a destra dell'interfaccia:

#### Fasi

1. Selezionare il numero di notifiche non lette in alto a destra.
2. Esaminare le notifiche, quindi selezionare **Contrassegna come letto** o **Mostra tutte le notifiche**.

   Se si seleziona **Mostra tutte le notifiche**, viene caricata la pagina Notifiche.

3. Nella pagina **Notifiche**, visualizzare le notifiche, selezionare quelle che si desidera contrassegnare come lette, selezionare **azione** e selezionare **Contrassegna come letta**.

## Aggiungere e rimuovere le credenziali

Aggiungi e rimuovi le credenziali per i provider di cloud privato locali, come ONTAP S3, i cluster Kubernetes gestiti con OpenShift o i cluster Kubernetes non gestiti dal tuo account in qualsiasi momento. Astra Control Center utilizza queste credenziali per scoprire i cluster Kubernetes e le applicazioni sui cluster e per eseguire il provisioning delle risorse per conto dell'utente.

Tutti gli utenti di Astra Control Center condividono gli stessi set di credenziali.

#### Aggiungere credenziali

È possibile aggiungere credenziali ad Astra Control Center quando si gestiscono i cluster. Per aggiungere credenziali aggiungendo un nuovo cluster, vedere "Aggiungere un cluster Kubernetes".

> Se crei il tuo `kubeconfig` file, è necessario definire solo **un** elemento di contesto al suo interno. Vedere "Documentazione Kubernetes" per informazioni sulla creazione `kubeconfig` file.

#### Rimuovere le credenziali

Rimuovere le credenziali da un account in qualsiasi momento. Rimuovere le credenziali solo dopo "annullamento della gestione di tutti i cluster associati".

> Il primo set di credenziali aggiunto ad Astra Control Center è sempre in uso perché Astra Control Center utilizza le credenziali per l'autenticazione nel bucket di backup. Si consiglia di non rimuovere queste credenziali.

#### Fasi

1. Selezionare **account**.
2. Selezionare la scheda **credenziali**.
3. Selezionare il menu Opzioni nella colonna **Stato** per le credenziali che si desidera rimuovere.
4. Selezionare **Rimuovi**.
5. Digitare la parola "remove" per confermare l'eliminazione, quindi selezionare **Sì, Rimuovi credenziale**.

#### Risultato

Astra Control Center rimuove le credenziali dall'account.

## Monitorare l'attività dell'account

Puoi visualizzare i dettagli delle attività nel tuo account Astra Control. Ad esempio, quando sono stati invitati nuovi utenti, quando è stato aggiunto un cluster o quando è stata acquisita una snapshot. È inoltre possibile esportare l'attività dell'account in un file CSV.

#### Visualizza tutte le attività dell'account in Astra Control

1. Selezionare **Activity** (attività).
2. Utilizza i filtri per restringere l'elenco delle attività o utilizza la casella di ricerca per trovare esattamente ciò che stai cercando.
3. Selezionare **Export to CSV** (Esporta in CSV) per scaricare l'attività dell'account in un file CSV.

#### Visualizzare l'attività dell'account per un'applicazione specifica

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Activity** (attività).

#### Visualizzare l'attività dell'account per i cluster

1. Selezionare **Clusters**, quindi il nome del cluster.
2. Selezionare **Activity** (attività).

#### Intraprendere azioni per risolvere gli eventi che richiedono attenzione

1. Selezionare **Activity** (attività).

2. Selezionare un evento che richiede attenzione.
3. Selezionare l'opzione a discesa **take action**.

   Da questo elenco è possibile visualizzare le possibili azioni correttive da intraprendere, visualizzare la documentazione relativa al problema e ottenere supporto per risolvere il problema.

## Aggiornare una licenza esistente

È possibile convertire una licenza di valutazione in una licenza completa oppure aggiornare una licenza di valutazione o una licenza completa esistente con una nuova licenza. Se non si dispone di una licenza completa, rivolgersi al contatto commerciale NetApp per ottenere una licenza completa e un numero di serie. È possibile utilizzare l'interfaccia utente Astra o. "L'API Astra Control" per aggiornare una licenza esistente.

### Fasi

1. Accedere a. "Sito di supporto NetApp".
2. Accedere alla pagina di download di Astra Control Center, inserire il numero di serie e scaricare il file di licenza NetApp completo (NLF).
3. Accedere all'interfaccia utente di Astra Control Center.
4. Dalla barra di navigazione a sinistra, selezionare **account** > **licenza**.
5. Nella pagina **account** > **licenza**, selezionare il menu a discesa dello stato della licenza esistente e selezionare **Sostituisci**.
6. Individuare il file di licenza scaricato.
7. Selezionare **Aggiungi**.

La pagina **account** > **licenze** visualizza le informazioni sulla licenza, la data di scadenza, il numero di serie della licenza, l'ID account e le unità CPU utilizzate.

### Per ulteriori informazioni

- "Licenza Astra Control Center"

## Gestire le connessioni al repository

È possibile collegare i repository ad Astra Control per utilizzarli come riferimento per immagini e artefatti di installazione dei pacchetti software. Quando si importano pacchetti software, Astra Control fa riferimento alle immagini di installazione nel repository di immagini, ai binari e ad altri artefatti nel repository di artefatti.

### Di cosa hai bisogno

- Kubernetes cluster con Astra Control Center installato
- Un repository Docker in esecuzione a cui è possibile accedere
- Un repository di artefatti in esecuzione (ad esempio Artifactory) a cui è possibile accedere

### Collegare un repository di immagini Docker

È possibile collegare un repository di immagini Docker per contenere le immagini di installazione dei pacchetti, come quelle di Astra Data Store. Quando si installano i pacchetti, Astra Control importa i file di immagine del pacchetto dal repository di immagini.

### Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **connessioni**.
3. Nella sezione **Docker Image Repository**, selezionare il menu in alto a destra.
4. Selezionare **Connect**.
5. Aggiungere l'URL e la porta per il repository.
6. Immettere le credenziali per il repository.
7. Selezionare **Connect**.

**Risultato**

Il repository è connesso. Nella sezione **Docker Image Repository**, il repository dovrebbe mostrare uno stato di connessione.

### Scollegare un repository di immagini Docker

È possibile rimuovere la connessione a un repository di immagini Docker se non è più necessaria.

**Fasi**

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **connessioni**.
3. Nella sezione **Docker Image Repository**, selezionare il menu in alto a destra.
4. Selezionare **Disconnect**.
5. Selezionare **Sì, disconnettere il repository di immagini Docker**.

**Risultato**

Il repository viene scollegato. Nella sezione **Docker Image Repository**, il repository dovrebbe mostrare uno stato disconnesso.

### Collegare un repository di artefatti

È possibile collegare un repository di artefatti all'host di artefatti come i binari dei pacchetti software. Quando si installano i pacchetti, Astra Control importa gli artefatti per i pacchetti software dal repository di immagini.

**Fasi**

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **connessioni**.
3. Nella sezione **Archivio artefatti**, selezionare il menu in alto a destra.
4. Selezionare **Connect**.
5. Aggiungere l'URL e la porta per il repository.
6. Se è richiesta l'autenticazione, attivare la casella di controllo **Usa autenticazione** e immettere le credenziali per il repository.
7. Selezionare **Connect**.

**Risultato**

Il repository è connesso. Nella sezione **Archivio artefatti**, il repository dovrebbe mostrare uno stato di connessione.

### Scollegare un repository di artefatti

È possibile rimuovere la connessione a un repository di artefatti se non è più necessaria.

#### Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **connessioni**.
3. Nella sezione **Archivio artefatti**, selezionare il menu in alto a destra.
4. Selezionare **Disconnect**.
5. Selezionare **Sì, disconnettere il repository degli artefatti**.

#### Risultato

Il repository viene scollegato. Nella sezione **Archivio artefatti**, il repository dovrebbe mostrare uno stato di connessione.

### Trova ulteriori informazioni

- "Gestire i pacchetti software"

## Gestire i pacchetti software

NetApp offre funzionalità aggiuntive per Astra Control Center con pacchetti software che è possibile scaricare dal NetApp Support Site. Dopo aver collegato i repository Docker e degli artefatti, è possibile caricare e importare pacchetti per aggiungere questa funzionalità ad Astra Control Center. È possibile utilizzare l'interfaccia utente Web di CLI o Astra Control Center per gestire i pacchetti software.

#### Di cosa hai bisogno

- Kubernetes cluster con Astra Control Center installato
- Un repository di immagini Docker connesso per contenere le immagini dei pacchetti software. Per ulteriori informazioni, vedere "Gestire le connessioni al repository".
- Un repository di artefatti collegato per contenere file binari e artefatti dei pacchetti software. Per ulteriori informazioni, vedere "Gestire le connessioni al repository".
- Un pacchetto software dal NetApp Support Site

### Caricare le immagini dei pacchetti software nei repository

Astra Control Center fa riferimento alle immagini dei pacchetti e agli artefatti nei repository collegati. È possibile caricare immagini e artefatti nei repository utilizzando la CLI.

#### Fasi

1. Scaricare il pacchetto software dal sito di supporto NetApp e salvarlo su un computer dotato di `kubectl` utility installata.
2. Estrarre il file di pacchetto compresso e modificare la directory nella posizione del file di bundle di Astra Control (ad esempio, `acc.manifest.bundle.yaml`).
3. Trasferire le immagini del pacchetto nel repository Docker. Effettuare le seguenti sostituzioni:
    - Sostituire BUNDLE_FILE con il nome del file bundle Astra Control.
    - Sostituire MY_REGISTRY con l'URL del repository Docker.
    - Sostituire MY_REGISTRY_USER e MY_REGISTRY_PASSWORD con le credenziali per il repository.

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

4. Se il pacchetto contiene artefatti, copiarli nel repository degli artefatti. Sostituire BUNDLE_FILE con il nome del file bundle Astra Control e NETWORK_LOCATION con il percorso di rete in cui copiare i file degli artefatti:

```
kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
```

## Aggiungere un pacchetto software

È possibile importare pacchetti software utilizzando un file bundle di Astra Control Center. Questa operazione consente di installare il pacchetto e di rendere disponibile il software per Astra Control Center.

### Aggiungere un pacchetto software utilizzando l'interfaccia utente Web Astra Control

È possibile utilizzare l'interfaccia utente Web di Astra Control Center per aggiungere un pacchetto software che è stato caricato nei repository collegati.

**Fasi**

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **pacchetti**.
3. Selezionare il pulsante **Aggiungi**.
4. Nella finestra di dialogo di selezione del file, selezionare l'icona di caricamento.
5. Scegliere un file bundle Astra Control, in `.yaml` da caricare.
6. Selezionare **Aggiungi**.

**Risultato**

Se il file bundle è valido e le immagini e gli artefatti del pacchetto si trovano nei repository collegati, il pacchetto viene aggiunto ad Astra Control Center. Quando lo stato nella colonna **Status** diventa **Available**, è possibile utilizzare il pacchetto. Per ottenere ulteriori informazioni, passare il mouse sullo stato di un pacchetto.

> Se una o più immagini o artefatti per un pacchetto non vengono trovati nel repository, viene visualizzato un messaggio di errore per quel pacchetto.

### Aggiungere un pacchetto software utilizzando l'interfaccia CLI

È possibile utilizzare l'interfaccia CLI per importare un pacchetto software caricato nei repository collegati. Per farlo, devi prima registrare il tuo ID account Astra Control Center e un token API.

**Fasi**

1. Utilizzando un browser Web, accedere all'interfaccia utente Web di Astra Control Center.
2. Dalla dashboard, selezionare l'icona utente in alto a destra.
3. Selezionare **API access**.
4. Annotare l'ID account nella parte superiore della schermata.

5. Selezionare **generate API token**.
6. Nella finestra di dialogo visualizzata, selezionare **generate API token**.
7. Prendere nota del token risultante e selezionare **Chiudi**. Nella CLI, modificare le directory in base alla posizione di `.yaml` file bundle nel contenuto del pacchetto estratto.
8. Importare il pacchetto utilizzando il file bundle, effettuando le seguenti sostituzioni:
   - Sostituire BUNDLE_FILE con il nome del file bundle Astra Control.
   - Sostituire IL SERVER con il nome DNS dell'istanza di Astra Control.
   - Sostituire ACCOUNT_ID e TOKEN con l'ID account e il token API registrati in precedenza.

```
kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
-k TOKEN
```

#### Risultato

Se il file bundle è valido e le immagini e gli artefatti del pacchetto si trovano nei repository collegati, il pacchetto viene aggiunto ad Astra Control Center.

> Se una o più immagini o artefatti per un pacchetto non vengono trovati nel repository, viene visualizzato un messaggio di errore per quel pacchetto.

### Rimuovere un pacchetto software

È possibile utilizzare l'interfaccia utente Web di Astra Control Center per rimuovere un pacchetto software precedentemente importato in Astra Control Center.

#### Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **pacchetti**.

   In questa pagina è possibile visualizzare l'elenco dei pacchetti installati e i relativi stati.

3. Nella colonna **azioni** del pacchetto, aprire il menu delle azioni.
4. Selezionare **Delete** (Elimina).

#### Risultato

Il pacchetto viene cancellato da Astra Control Center, ma le immagini e gli artefatti del pacchetto rimangono nei repository.

### Trova ulteriori informazioni

- "Gestire le connessioni al repository"

# Gestire i bucket

Un provider di bucket dell'archivio di oggetti è essenziale se si desidera eseguire il backup delle applicazioni e dello storage persistente o se si desidera clonare le applicazioni tra cluster. Utilizzando Astra Control Center, Aggiungi un provider di archivi di oggetti come destinazione di backup off-cluster per le tue applicazioni.

Non è necessario un bucket se si clonano la configurazione dell'applicazione e lo storage persistente sullo stesso cluster.

Utilizza uno dei seguenti provider di bucket Amazon Simple Storage Service (S3):

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Generico S3
- Microsoft Azure

> Sebbene Astra Control Center supporti Amazon S3 come provider di bucket S3 generico, Astra Control Center potrebbe non supportare tutti i vendor di archivi di oggetti che sostengono il supporto S3 di Amazon.

Un bucket può trovarsi in uno dei seguenti stati:

- In sospeso: Il bucket è pianificato per il rilevamento.
- Disponibile: La benna è disponibile per l'uso.
- Rimosso: Il bucket non è attualmente accessibile.

Per istruzioni su come gestire i bucket utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

È possibile eseguire queste attività relative alla gestione dei bucket:

- "Aggiungi un bucket"
- Modificare un bucket
- Ruotare o rimuovere le credenziali bucket
- Rimuovere una benna

> I bucket S3 in Astra Control Center non riportano la capacità disponibile. Prima di eseguire il backup o la clonazione delle applicazioni gestite da Astra Control Center, controllare le informazioni del bucket nel sistema di gestione ONTAP o StorageGRID.

## Modificare un bucket

È possibile modificare le informazioni delle credenziali di accesso per un bucket e modificare se un bucket selezionato è il bucket predefinito.

> Quando si aggiunge un bucket, selezionare il bucket provider corretto e fornire le credenziali corrette per tale provider. Ad esempio, l'interfaccia utente accetta come tipo NetApp ONTAP S3 e accetta le credenziali StorageGRID; tuttavia, questo causerà l'errore di tutti i backup e ripristini futuri dell'applicazione che utilizzano questo bucket. Vedere "Note di rilascio".

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
2. Dal menu Opzioni nella colonna **azioni**, selezionare **Modifica**.
3. Modificare qualsiasi informazione diversa dal tipo di bucket.

Impossibile modificare il tipo di bucket.

4. Selezionare **Aggiorna**.

## Ruotare o rimuovere le credenziali bucket

Astra Control utilizza le credenziali bucket per ottenere l'accesso e fornire chiavi segrete per un bucket S3 in modo che Astra Control Center possa comunicare con il bucket.

### Ruotare le credenziali del bucket

Se si ruotano le credenziali, ruotarle durante una finestra di manutenzione quando non sono in corso backup (pianificati o on-demand).

#### Procedura per modificare e ruotare le credenziali

1. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
2. Dal menu Opzioni nella colonna **azioni**, selezionare **Modifica**.
3. Creare la nuova credenziale.
4. Selezionare **Aggiorna**.

### Rimuovere le credenziali bucket

È necessario rimuovere le credenziali bucket solo se sono state applicate nuove credenziali a un bucket o se il bucket non è più utilizzato attivamente.

Il primo set di credenziali aggiunto ad Astra Control è sempre in uso perché Astra Control utilizza le credenziali per autenticare il bucket di backup. Non rimuovere queste credenziali se il bucket è in uso, in quanto ciò potrebbe causare errori di backup e indisponibilità del backup.

Se si rimuovono le credenziali bucket attive, vedere "risoluzione dei problemi relativi alla rimozione delle credenziali bucket".

Per istruzioni su come rimuovere le credenziali S3 utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

## Rimuovere una benna

È possibile rimuovere un bucket che non è più in uso o che non è integro. Questa operazione può essere utile per mantenere la configurazione dell'archivio di oggetti semplice e aggiornata.

Non è possibile rimuovere un bucket predefinito. Se si desidera rimuovere tale bucket, selezionare prima un altro bucket come predefinito.

#### Di cosa hai bisogno

- Prima di iniziare, verificare che non vi siano backup in esecuzione o completati per questo bucket.
- È necessario verificare che il bucket non venga utilizzato in alcuna policy di protezione attiva.

In tal caso, non sarà possibile continuare.

#### Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
2. Dal menu **azioni**, selezionare **Rimuovi**.

> Astra Control garantisce innanzitutto che non vi siano policy di pianificazione che utilizzano il bucket per i backup e che non vi siano backup attivi nel bucket che si sta per rimuovere.

3. Digitare "remove" per confermare l'azione.
4. Selezionare **Sì, Rimuovi bucket**.

### Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"

# Gestire il back-end dello storage

La gestione dei cluster di storage in Astra Control come back-end dello storage consente di ottenere collegamenti tra volumi persistenti (PVS) e il back-end dello storage, oltre a metriche di storage aggiuntive. È possibile monitorare la capacità dello storage e i dettagli relativi allo stato di salute, incluse le prestazioni, se il centro di controllo Astra è connesso a Cloud Insights.

Per istruzioni su come gestire i back-end dello storage utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

È possibile completare le seguenti attività relative alla gestione di un backend di storage:

- "Aggiungere un backend di storage"
- Visualizza i dettagli del back-end dello storage
- Annullare la gestione di un backend di storage
- Aggiornare una licenza di back-end per lo storage
- Aggiunta di nodi a un cluster di storage back-end
- Rimuovere un backend di storage

## Visualizza i dettagli del back-end dello storage

È possibile visualizzare le informazioni di back-end dello storage dalla dashboard o dall'opzione Backend.

Nella pagina Storage backend Details (Dettagli back-end storage), per Astra Data Store, sono disponibili le seguenti informazioni:

- Cluster Astra Data Store
  - Throughput, IOPS e latenza
  - Capacità utilizzata rispetto alla capacità totale
- Per ogni volume cluster Astra Data Store
  - Capacità utilizzata rispetto alla capacità totale
  - Throughput

### Visualizza i dettagli del back-end dello storage dalla dashboard

#### Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Dashboard**.
2. Esaminare la sezione Storage backend che mostra lo stato:
    - **Non integro**: Lo storage non è in uno stato ottimale. Ciò potrebbe essere dovuto a un problema di latenza o a un'applicazione degradata, ad esempio, a causa di un problema di container.
    - **Tutto sano**: Lo storage è stato gestito ed è in uno stato ottimale.
    - **Scoperto**: Lo storage è stato scoperto, ma non gestito da Astra Control.

### Visualizza i dettagli del back-end dello storage dall'opzione Backend

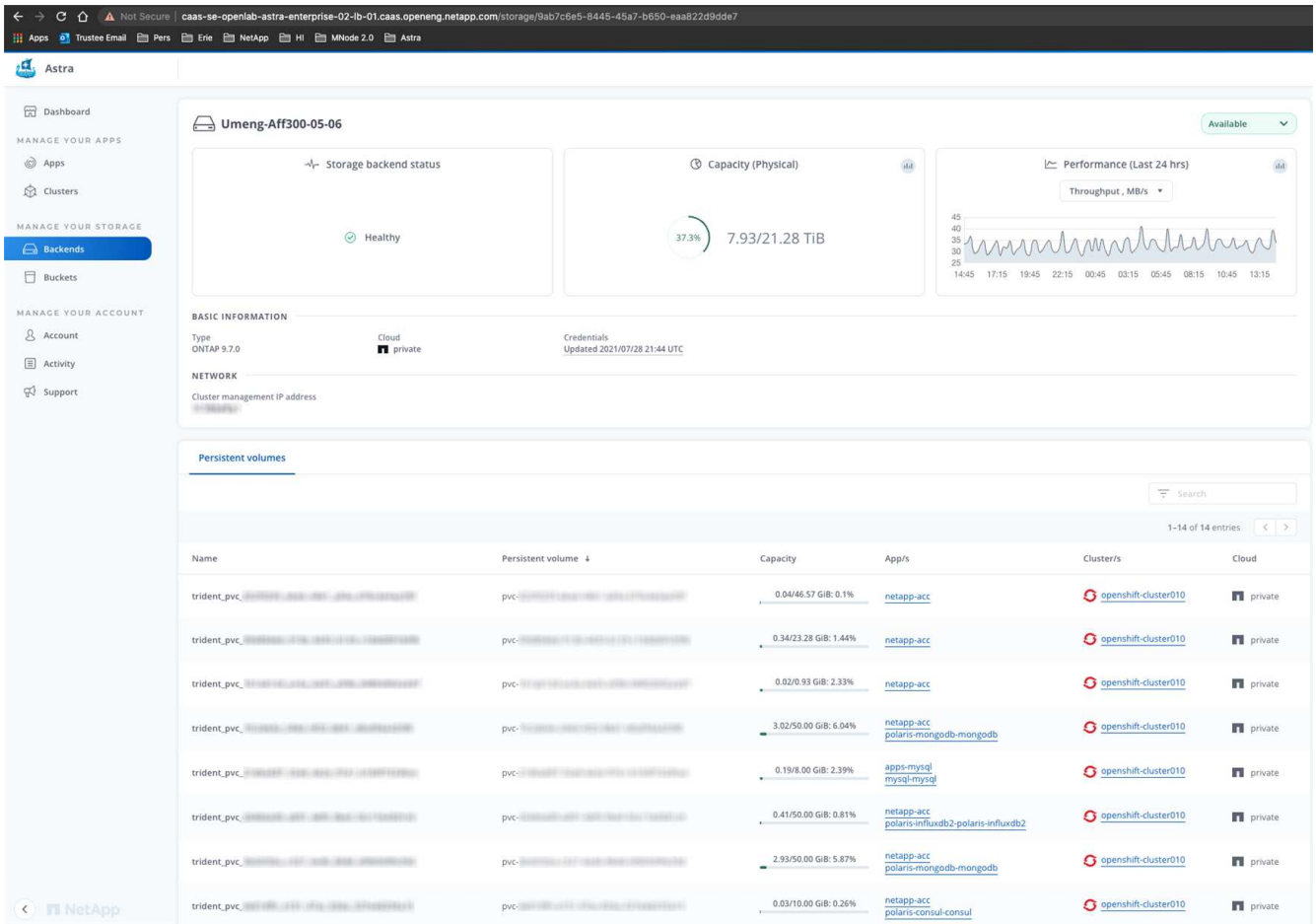
Visualizza informazioni sullo stato, la capacità e le performance del back-end (throughput IOPS e/o latenza).

Con una connessione a Cloud Insights, è possibile visualizzare i volumi utilizzati dalle applicazioni Kubernetes, che vengono memorizzati in un backend di storage selezionato.

#### Fasi

1. Nell'area di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il backend dello storage.

> Se si è connessi a NetApp Cloud Insights, gli estratti di dati da Cloud Insights vengono visualizzati nella pagina backend.



3. Per accedere direttamente a Cloud Insights, selezionare l'icona **Cloud Insights** accanto all'immagine delle metriche.

## Annullare la gestione di un backend di storage

È possibile annullare la gestione del backend.

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il backend dello storage.
3. Dal menu Opzioni nella colonna **azioni**, selezionare **Annulla gestione**.
4. Digitare "unManage" per confermare l'azione.
5. Selezionare **Sì, Annulla gestione del backend di storage**.

## Rimuovere un backend di storage

È possibile rimuovere un backend di storage non più in uso. Questa operazione può essere utile per mantenere la configurazione semplice e aggiornata.

Se si rimuove un backend Astra Data Store, questo non deve essere stato creato da vCenter.

**Di cosa hai bisogno**

- Assicurarsi che il backend dello storage non sia gestito.
- Assicurarsi che il backend dello storage non abbia volumi associati al cluster Astra Data Store.

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Se il backend viene gestito, annullarne la gestione.
   a. Selezionare **Managed**.
   b. Selezionare il backend dello storage.
   c. Dall'opzione **azioni**, selezionare **Annulla gestione**.
   d. Digitare "unManage" per confermare l'azione.
   e. Selezionare **Sì, Annulla gestione del backend di storage**.
3. Selezionare **rilevato**.
   a. Selezionare il backend dello storage.
   b. Dall'opzione **azioni**, selezionare **Rimuovi**.
   c. Digitare "remove" per confermare l'azione.
   d. Selezionare **Sì, rimuovere il backend di storage**.

## Aggiornare una licenza di back-end per lo storage

È possibile aggiornare la licenza per un backend di storage Astra Data Store per supportare un'implementazione più ampia o funzionalità avanzate.

**Di cosa hai bisogno**

- Un back-end storage Astra Data Store implementato e gestito
- Un file di licenza Astra Data Store (contatta il tuo commerciale NetApp per acquistare una licenza Astra Data Store)

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il nome di un backend di storage.
3. In **Basic Information** (informazioni di base), viene visualizzato il tipo di licenza installata.

   Se si passa il mouse sopra le informazioni sulla licenza, viene visualizzata una finestra a comparsa con ulteriori informazioni, come ad esempio la scadenza e le informazioni sui diritti.

4. In **licenza**, selezionare l'icona di modifica accanto al nome della licenza.
5. Nella pagina **Aggiorna licenza**, eseguire una delle seguenti operazioni:

| Stato della licenza | Azione |
|---|---|
| Almeno una licenza è stata aggiunta ad Astra Data Store. | Selezionare una licenza dall'elenco. |
| Nessuna licenza aggiunta ad Astra Data Store. | a. Selezionare il pulsante **Aggiungi**.<br>b. Selezionare un file di licenza da caricare.<br>c. Selezionare **Aggiungi** per caricare il file di licenza. |

6. Selezionare **Aggiorna**.

## Aggiunta di nodi a un cluster di storage back-end

È possibile aggiungere nodi a un cluster Astra Data Store, fino al numero di nodi supportati dal tipo di licenza installata per Astra Data Store.

**Di cosa hai bisogno**

- Un back-end di storage Astra Data Store distribuito e concesso in licenza
- È stato aggiunto il pacchetto software Astra Data Store in Astra Control Center
- Uno o più nuovi nodi da aggiungere al cluster

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il nome di un backend di storage.
3. In Basic Information (informazioni di base), è possibile visualizzare il numero di nodi in questo cluster di back-end dello storage.
4. In **nodi**, selezionare l'icona di modifica accanto al numero di nodi.
5. Nella pagina **Add Nodes** (Aggiungi nodi), immettere le informazioni relative al nuovo nodo o ai nuovi nodi:
   a. Assegnare un'etichetta di nodo per ciascun nodo.
   b. Effettuare una delle seguenti operazioni:

    - Se si desidera che Astra Data Store utilizzi sempre il numero massimo di nodi disponibili in base alla licenza, attivare la casella di controllo **Usa sempre fino al numero massimo di nodi consentiti**.
    - Se non si desidera che Astra Data Store utilizzi sempre il numero massimo di nodi disponibili, selezionare il numero desiderato di nodi totali da utilizzare.

  c. Se è stato implementato Astra Data Store con i domini di protezione attivati, assegnare il nuovo nodo o i nuovi nodi ai domini di protezione.

6. Selezionare **Avanti**.
7. Inserire l'indirizzo IP e le informazioni di rete per ogni nuovo nodo. Inserire un singolo indirizzo IP per un singolo nodo o un pool di indirizzi IP per più nuovi nodi.

   Se Astra Data Store è in grado di utilizzare gli indirizzi IP configurati durante l'implementazione, non è necessario inserire alcuna informazione sull'indirizzo IP.

8. Selezionare **Avanti**.
9. Esaminare la configurazione del nuovo nodo o dei nuovi nodi.
10. Selezionare **Aggiungi nodi**.

### Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"

# Monitorare e proteggere l'infrastruttura

È possibile configurare diverse impostazioni opzionali per migliorare l'esperienza di Astra Control Center. Se la rete in cui si utilizza Astra Control Center richiede un proxy per la connessione a Internet (per caricare pacchetti di supporto sul sito di supporto NetApp o stabilire una connessione a Cloud Insights), è necessario configurare un server proxy in Astra Control Center. Per monitorare e ottenere informazioni sulla tua infrastruttura completa, crea una connessione con NetApp Cloud Insights. Per raccogliere gli eventi Kubernetes dai sistemi monitorati da Astra Control Center, aggiungere una connessione Fluentd.

## Aggiungere un server proxy

Se la rete in cui si utilizza Astra Control Center richiede un proxy per la connessione a Internet (per caricare pacchetti di supporto sul sito di supporto NetApp o stabilire una connessione a Cloud Insights), è necessario configurare un server proxy in Astra Control Center.

> Astra Control Center non convalida i dati immessi per il server proxy. Assicurarsi di immettere i valori corretti.

**Fasi**

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Connect** dall'elenco a discesa per aggiungere un server proxy.


4. Immettere il nome del server proxy o l'indirizzo IP e il numero della porta proxy.
5. Se il server proxy richiede l'autenticazione, selezionare la casella di controllo e immettere il nome utente e la password.
6. Selezionare **Connect**.

**Risultato**

Se le informazioni sul proxy inserite sono state salvate, la sezione **Proxy HTTP** della pagina **account** > **connessioni** indica che è connesso e visualizza il nome del server.


### Modificare le impostazioni del server proxy

È possibile modificare le impostazioni del server proxy.

**Fasi**

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Edit** (Modifica) dall'elenco a discesa per modificare la connessione.
4. Modificare i dettagli del server e le informazioni di autenticazione.
5. Selezionare **Salva**.

### Disattiva la connessione al server proxy

È possibile disattivare la connessione al server proxy. Prima di disattivare l'opzione, viene visualizzato un avviso che potrebbe causare interruzioni ad altre connessioni.

**Fasi**

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Disconnect** dall'elenco a discesa per disattivare la connessione.
4. Nella finestra di dialogo visualizzata, confermare l'operazione.

## Connettersi a Cloud Insights

Per monitorare e ottenere informazioni sulla tua infrastruttura completa, collega NetApp Cloud Insights con la tua istanza del centro di controllo Astra. Cloud Insights è incluso nella licenza di Astra Control Center.

Cloud Insights deve essere accessibile dalla rete utilizzata dal centro di controllo Astra o indirettamente tramite un server proxy.

Quando il centro di controllo Astra è collegato a Cloud Insights, viene creato un pod unità di acquisizione. Questo pod raccoglie i dati dai back-end di storage gestiti dal centro di controllo Astra e li invia a Cloud Insights. Questo pod richiede 8 GB di RAM e 2 core CPU.

> Dopo aver attivato la connessione Cloud Insights, è possibile visualizzare le informazioni sul throughput nella pagina **backend** e connettersi a Cloud Insights da qui dopo aver selezionato un backend di storage. Le informazioni sono disponibili anche nella sezione cluster del pannello **Dashboard** e da qui è possibile connettersi a Cloud Insights.

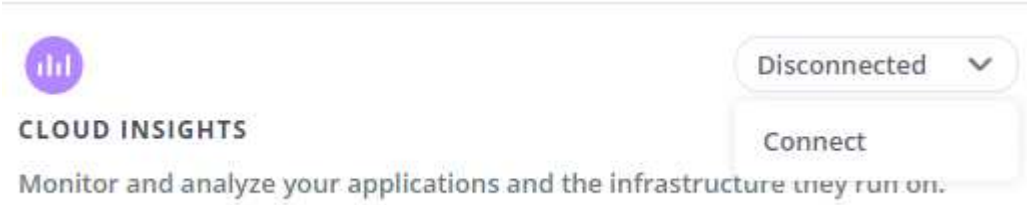
**Di cosa hai bisogno**

- Un account Astra Control Center con privilegi **admin**/**owner**.
- Una licenza Astra Control Center valida.
- Un server proxy se la rete in cui si utilizza Astra Control Center richiede un proxy per la connessione a Internet.

> Se sei un nuovo utente di Cloud Insights, familiarizza con le caratteristiche e le funzionalità. Vedere "Documentazione Cloud Insights".

**Fasi**

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Connect** dove nell'elenco a discesa viene visualizzato **disconnected** per aggiungere la connessione.



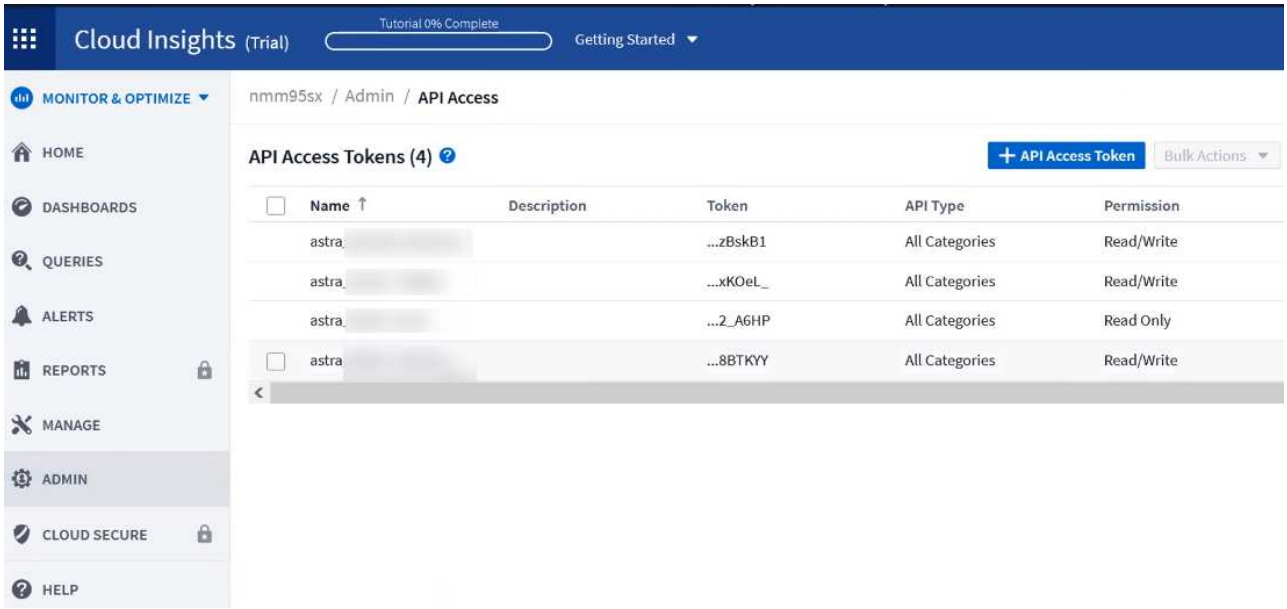

4. Inserire i token API Cloud Insights e l'URL del tenant. L'URL del tenant ha il seguente formato, ad esempio:

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

   Quando si ottiene la licenza Cloud Insights, si ottiene l'URL del tenant. Se non si dispone dell'URL del tenant, consultare "Documentazione Cloud Insights".

   a. Per ottenere il "Token API", Accedere all'URL del tenant Cloud Insights.
   b. In Cloud Insights, generare un token di accesso API **lettura/scrittura** e **sola lettura** facendo clic su

**Amministratore** > **accesso API**.




c. Copiare la chiave **sola lettura**. Per attivare la connessione Cloud Insights, è necessario incollarla nella finestra di Astra Control Center. Per le autorizzazioni della chiave Read API Access Token, selezionare: Assets (risorse), Alerts (Avvisi), Acquisition Unit (unità di acquisizione) e Data Collection (raccolta dati).

d. Copiare la chiave **Read/Write**. È necessario incollarlo nella finestra di dialogo di Astra Control Center **Connect Cloud Insights**. Per le autorizzazioni della chiave del token di accesso API di lettura/scrittura, selezionare: Asset, acquisizione dati, acquisizione log, unità di acquisizione, E raccolta dati.

> Si consiglia di generare una chiave **Read Only** e una chiave **Read/Write** e di non utilizzare la stessa chiave per entrambi gli scopi. Per impostazione predefinita, il periodo di scadenza del token è impostato su un anno. Si consiglia di mantenere la selezione predefinita per assegnare al token la durata massima prima della scadenza. Se il token scade, la telemetria si interrompe.

e. Incollare le chiavi copiate da Cloud Insights in Astra Control Center.

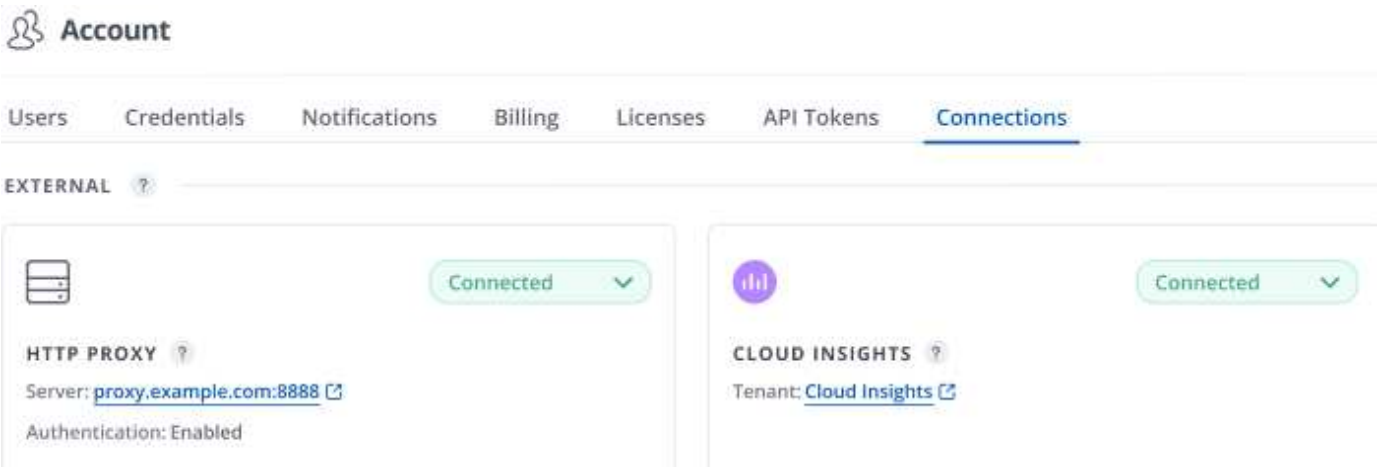
5. Selezionare **Connect**.

> Dopo aver selezionato **Connetti,** lo stato della connessione diventa **in sospeso** nella sezione **Cloud Insights** della pagina **account** > **connessioni**. L'attivazione della connessione e il passaggio allo stato **connesso** possono richiedere alcuni minuti.

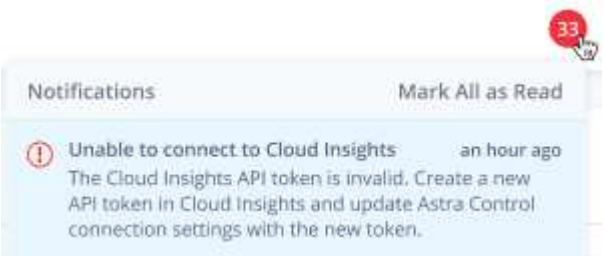
> Per passare facilmente da un'unità di controllo Astra a un'interfaccia utente Cloud Insights e viceversa, assicurarsi di aver effettuato l'accesso a entrambe.

### Visualizzare i dati in Cloud Insights

Se la connessione ha avuto esito positivo, la sezione **Cloud Insights** della pagina **account** > **connessioni** indica che la connessione è stata stabilita e visualizza l'URL del tenant. È possibile visitare Cloud Insights per visualizzare e ricevere correttamente i dati.

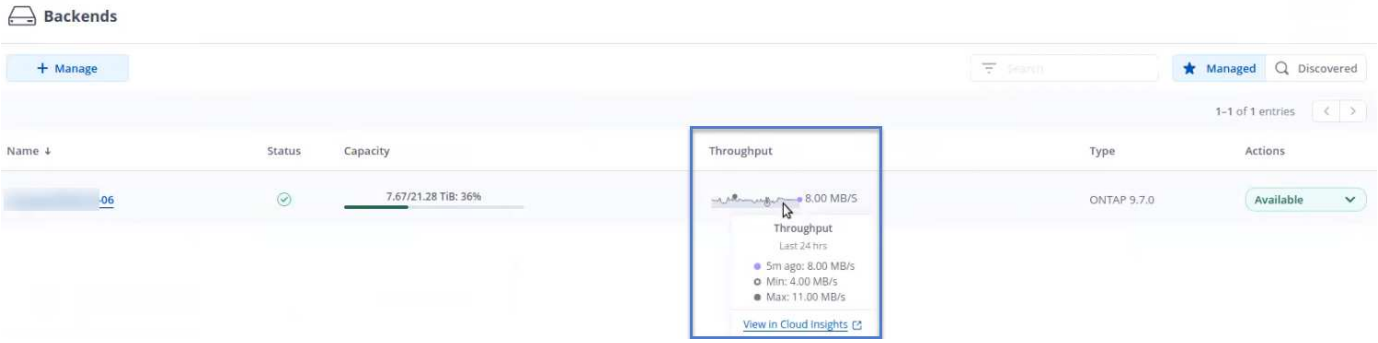



Se la connessione non è riuscita per qualche motivo, lo stato visualizza **Failed** (non riuscito). Il motivo del guasto è disponibile in **Notifiche** nella parte superiore destra dell'interfaccia utente.



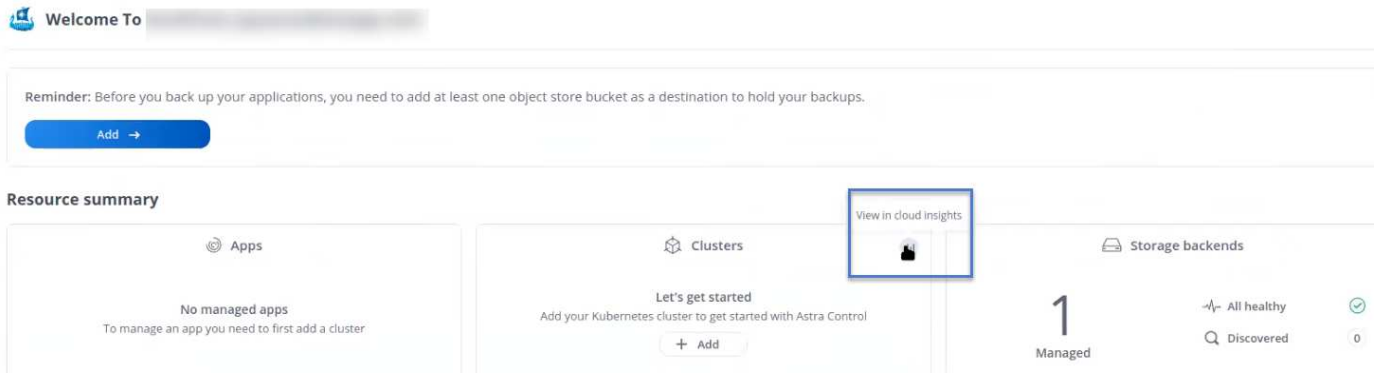

Le stesse informazioni sono disponibili anche in **account** > **Notifiche**.

Da Astra Control Center, è possibile visualizzare le informazioni sul throughput nella pagina **backend** e connettersi a Cloud Insights da qui dopo aver selezionato un backend di storage.




Per accedere direttamente a Cloud Insights, selezionare l'icona **Cloud Insights** accanto all'immagine delle metriche.

Le informazioni sono disponibili anche nella * Dashboard*.




Dopo aver attivato la connessione Cloud Insights, se si rimuovono i backend aggiunti in Centro di controllo Astra, i backend smettono di inviare i report a Cloud Insights.

### Modificare la connessione Cloud Insights

È possibile modificare la connessione Cloud Insights.

È possibile modificare solo le chiavi API. Per modificare l'URL del tenant Cloud Insights, si consiglia di scollegare la connessione Cloud Insights e di connettersi al nuovo URL.

#### Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Edit** (Modifica) dall'elenco a discesa per modificare la connessione.
4. Modificare le impostazioni di connessione Cloud Insights.
5. Selezionare **Salva**.

### Disattiva la connessione Cloud Insights

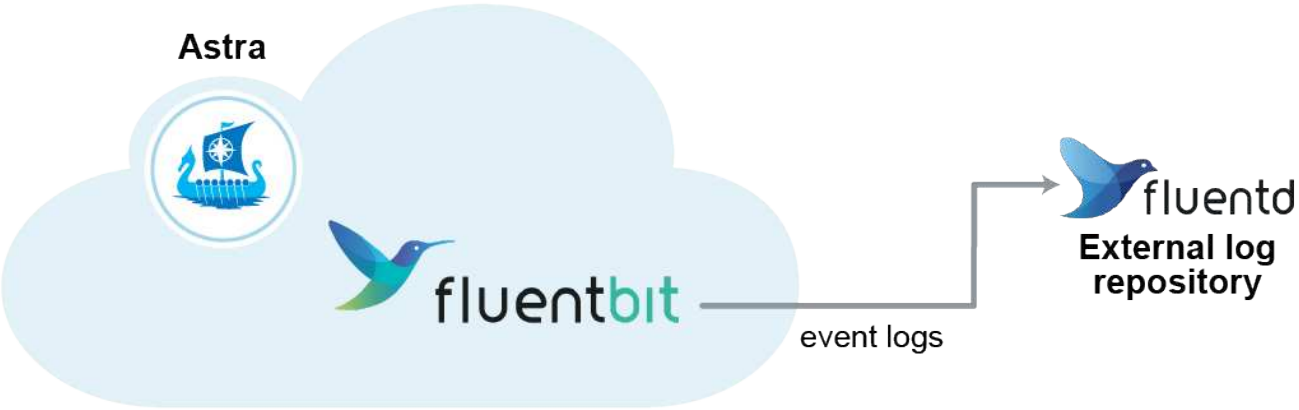
È possibile disattivare la connessione Cloud Insights per un cluster Kubernetes gestito da Astra Control Center. La disattivazione della connessione Cloud Insights non elimina i dati di telemetria già caricati su Cloud Insights.

#### Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Disconnect** dall'elenco a discesa per disattivare la connessione.
4. Nella finestra di dialogo visualizzata, confermare l'operazione. Dopo aver confermato l'operazione, nella pagina **account** > **connessioni**, lo stato Cloud Insights diventa **in sospeso**. Il passaggio allo stato **disconnesso** richiede alcuni minuti.

## Connettersi a Fluentd

È possibile inviare registri (eventi Kubernetes) da Astra Control Center all'endpoint Fluentd. La connessione Fluentd è disattivata per impostazione predefinita.




A Fluentd vengono inoltrati solo i log degli eventi dei cluster gestiti.

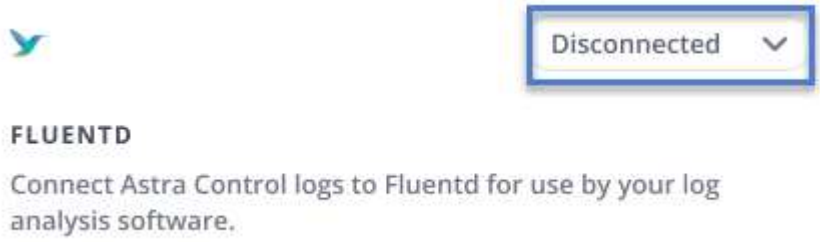
**Di cosa hai bisogno**

- Un account Astra Control Center con privilegi **admin**/**owner**.
- Astra Control Center installato e in esecuzione su un cluster Kubernetes.

Astra Control Center non convalida i dati immessi per il server Fluentd. Assicurarsi di immettere i valori corretti.

**Fasi**

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Connect** dall'elenco a discesa in cui viene visualizzato **disconnected** per aggiungere la connessione.




4. Inserire l'indirizzo IP dell'host, il numero di porta e la chiave condivisa per il server Fluentd.
5. Selezionare **Connect**.

**Risultato**

Se i dati immessi per il server Fluentd sono stati salvati, la sezione **Fluentd** della pagina **account** > **connessioni** indica che è connesso. A questo punto, è possibile visitare il server Fluentd collegato e visualizzare i registri degli eventi.

Se la connessione non è riuscita per qualche motivo, lo stato visualizza **Failed** (non riuscito). Il motivo del guasto è disponibile in **Notifiche** nella parte superiore destra dell'interfaccia utente.

Le stesse informazioni sono disponibili anche in **account** > **Notifiche**.

In caso di problemi con la raccolta dei log, è necessario accedere al nodo di lavoro e assicurarsi che i log siano disponibili in `/var/log/containers/`.

#### Modificare la connessione Fluentd

È possibile modificare la connessione di Fluentd all'istanza di Astra Control Center.

**Fasi**

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Edit** (Modifica) dall'elenco a discesa per modificare la connessione.
4. Modificare le impostazioni dell'endpoint Fluentd.
5. Selezionare **Salva**.

#### Disattiva la connessione Fluentd

È possibile disattivare la connessione di Fluentd all'istanza di Astra Control Center.

**Fasi**

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Disconnect** dall'elenco a discesa per disattivare la connessione.
4. Nella finestra di dialogo visualizzata, confermare l'operazione.

# Annulla la gestione di app e cluster

Rimuovi le app o i cluster che non vuoi più gestire da Astra Control Center.

## Annullare la gestione di un'applicazione

Smetta di gestire le app che non vuoi più eseguire il backup, lo snapshot o la clonazione da Astra Control Center.

- Eventuali backup e snapshot esistenti verranno eliminati.
- Le applicazioni e i dati rimangono disponibili.

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **applicazioni**.
2. Selezionare la casella di controllo per le applicazioni che non si desidera più gestire.
3. Dal menu **azione**, selezionare **Annulla gestione**.
4. Digitare "unManage" per confermare.
5. Confermare che si desidera annullare la gestione delle applicazioni, quindi selezionare **Sì, Annulla gestione applicazione**.

**Risultato**

Astra Control Center interrompe la gestione dell'applicazione.

## Annullare la gestione di un cluster

Annulla la gestione del cluster che non si desidera più gestire da Astra Control Center.

- Questa azione impedisce la gestione del cluster da parte di Astra Control Center. Non apporta modifiche alla configurazione del cluster e non elimina il cluster.
- Trident non verrà disinstallato dal cluster. "Scopri come disinstallare Trident".

> Prima di annullare la gestione del cluster, è necessario annullare la gestione delle applicazioni associate al cluster.

**Fasi**

1. Dalla barra di navigazione a sinistra, selezionare **Clusters**.
2. Selezionare la casella di controllo del cluster che non si desidera più gestire in Astra Control Center.
3. Dal menu Opzioni nella colonna **azioni**, selezionare **Annulla gestione**.
4. Confermare che si desidera annullare la gestione del cluster, quindi selezionare **Sì, Annulla gestione cluster**.

**Risultato**

Lo stato del cluster cambia in **Removing** (Rimozione), quindi il cluster viene rimosso dalla pagina **Clusters** e non viene più gestito da Astra Control Center.

> **Se il centro di controllo Astra e Cloud Insights non sono connessi**, la disinstallazione del cluster rimuove tutte le risorse installate per l'invio dei dati di telemetria. **Se il centro di controllo Astra e Cloud Insights sono connessi**, la mancata gestione del cluster elimina solo il `fluentbit` e. `event-exporter` pod.

# Aggiornare Astra Control Center

Per aggiornare Astra Control Center, scaricare il pacchetto di installazione dal NetApp Support Site e completare queste istruzioni per aggiornare i componenti di Astra Control Center nel proprio ambiente. È possibile utilizzare questa procedura per aggiornare Astra Control Center in ambienti connessi a Internet o con connessione ad aria.

**Di cosa hai bisogno**

- "Prima di iniziare l'aggiornamento, assicurarsi che l'ambiente soddisfi ancora i requisiti minimi per l'implementazione di Astra Control Center".
- Assicurarsi che tutti gli operatori del cluster siano in buono stato e disponibili.

  Esempio di OpenShift:

  ```
  oc get clusteroperators
  ```

- Assicurarsi che tutti i servizi API siano in buono stato e disponibili.

  Esempio di OpenShift:

```
oc get apiservices
```

- Disconnettersi da Astra Control Center.

**A proposito di questa attività**

Il processo di aggiornamento di Astra Control Center ti guida attraverso le seguenti fasi di alto livello:

- Scarica il bundle Astra Control Center
- Disimballare il bundle e modificare la directory
- Aggiungere le immagini al registro locale
- Installare l'operatore Astra Control Center aggiornato
- Aggiornare Astra Control Center
- Upgrade dei servizi di terze parti (opzionale)
- Verificare lo stato del sistema
- Impostare l'ingresso per il bilanciamento del carico

Non eseguire il seguente comando durante l'intero processo di aggiornamento per evitare di eliminare tutti i pod di Astra Control Center: `kubectl delete -f astra_control_center_operator_deploy.yaml`

Eseguire gli aggiornamenti in una finestra di manutenzione quando pianificazioni, backup e snapshot non sono in esecuzione.

I comandi Podman possono essere utilizzati al posto dei comandi Docker se si utilizza il Podman di Red Hat invece di Docker Engine.

## Scarica il bundle Astra Control Center

1. Scarica il bundle di aggiornamento di Astra Control Center (`astra-control-center-[version].tar.gz`) da "Sito di supporto NetApp".
2. (Facoltativo) utilizzare il seguente comando per verificare la firma del bundle:

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

## Disimballare il bundle e modificare la directory

1. Estrarre le immagini:

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

2. Passare alla directory Astra.

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

## Aggiungere le immagini al registro locale

1. Aggiungere i file nella directory dell'immagine di Astra Control Center al registro locale.

> Di seguito viene riportato uno script di esempio per il caricamento automatico delle immagini.

   a. Accedere al registro di sistema di Docker:

```
docker login [your_registry_path]
```

   b. Caricare le immagini in Docker.
   c. Contrassegnare le immagini.
   d. Trasmetti le immagini nel registro locale.

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

## Installare l'operatore Astra Control Center aggiornato

1. Modificare l'yaml di implementazione dell'operatore di Astra Control Center (`astra_control_center_operator_deploy.yaml`) per fare riferimento al registro locale e al segreto.

```
vim astra_control_center_operator_deploy.yaml
```

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

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

b. Cambiare `[your_registry_path]` per `kube-rbac-proxy` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

c. Cambiare `[your_registry_path]` per `acc-operator-controller-manager` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

d. Aggiungere i seguenti valori a `env` sezione:

```
- name: ACCOP_HELM_UPGRADETIMEOUT
  value: 300m
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: [your_registry_path]/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

2. Installare l’operatore Astra Control Center aggiornato:

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

Esempio di risposta:

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

## Aggiornare Astra Control Center

1. Modificare la risorsa personalizzata di Astra Control Center (CR) (`astra_control_center_min.yaml`) E modificare la versione di Astra (`astraVersion` all'interno di `Spec`) al numero più recente:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

> Il percorso del Registro di sistema deve corrispondere al percorso del Registro di sistema in cui sono state inviate le immagini in a. passaggio precedente.

2. Aggiungere le seguenti righe all'interno di `additionalValues` all'interno di `Spec` In Astra Control Center CR:

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
```

3. Effettuare una delle seguenti operazioni:
   a. Se non si dispone di IngressController o ingresso personale e si utilizza Astra Control Center con il gateway Traefik come servizio di tipo LoadBalancer e si desidera continuare con l'installazione, specificare un altro campo `ingressType` (se non è già presente) e impostarlo su `AccTraefik`.

      ```
      ingressType: AccTraefik
      ```

   b. Se si desidera passare all'implementazione di ingresso generica di Astra Control Center predefinita, fornire la propria configurazione IngressController/Ingress (con terminazione TLS, ecc.), aprire un percorso per Astra Control Center e impostare `ingressType` a. `Generic`.

      ```
      ingressType: Generic
      ```

      Se si omette il campo, il processo diventa l'implementazione generica. Se non si desidera un'implementazione generica, assicurarsi di aggiungere il campo.

4. (Facoltativo) verificare che i pod terminino e diventino nuovamente disponibili:

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

5. Attendere che le condizioni di stato di Astra indichino che l'aggiornamento è completo e pronto:

   ```
   kubectl get -o yaml -n [netapp-acc or custom namespace]
   astracontrolcenters.astra.netapp.io astra
   ```

   Risposta:

   ```
   conditions:
     - lastTransitionTime: "2021-10-25T18:49:26Z"
       message: Astra is deployed
       reason: Complete
       status: "True"
       type: Ready
     - lastTransitionTime: "2021-10-25T18:49:26Z"
       message: Upgrading succeeded.
       reason: Complete
       status: "False"
       type: Upgrading
   ```

6. Effettua nuovamente l'accesso e verifica che tutti i cluster e le applicazioni gestiti siano ancora presenti e protetti.
7. Se l'operatore non ha aggiornato il Cert-manager, aggiornare i servizi di terze parti, quindi.

## Upgrade dei servizi di terze parti (opzionale)

I servizi di terze parti Traefik e Cert-manager non vengono aggiornati durante le fasi di aggiornamento precedenti. Se necessario, è possibile aggiornarli utilizzando la procedura descritta qui o conservare le versioni dei servizi esistenti.

- **Traefik**: Per impostazione predefinita, Astra Control Center gestisce il ciclo di vita dell'implementazione di Traefik. Impostazione `externalTraefik` a. `false` (Impostazione predefinita) indica che non esiste alcun Traefik esterno nel sistema e che Traefik viene installato e gestito da Astra Control Center. In questo caso, `externalTraefik` è impostato su `false`.

  D'altra parte, se si dispone di una propria implementazione Traefik, impostare `externalTraefik` a. `true`. In questo caso, si mantiene l'implementazione e Astra Control Center non aggiornerà i CRD, a meno che non sia `shouldUpgrade` è impostato su `true`.

- **Cert-manager**: Per impostazione predefinita, Astra Control Center installa il cert-manager (e i CRD), a meno che non sia stato impostato `externalCertManager` a. `true`. Impostare `shouldUpgrade` a. `true` Per fare in modo che Astra Control Center aggiorni i CRD.

Traefik viene aggiornato se viene soddisfatta una delle seguenti condizioni:

- ExternalTraefik: Falso O.
- ExternalTraefik: True E shouldUpgrade: True.

**Fasi**

1. Modificare il `acc` CR:

   ```
   kubectl edit acc -n [netapp-acc or custom namespace]
   ```

2. Modificare il `externalTraefik` e il `shouldUpgrade` su entrambi i campi `true` oppure `false` in base alle necessità.

   ```
   crds:
       externalTraefik: false
       externalCertManager: false
       shouldUpgrade: false
   ```

## Verificare lo stato del sistema

1. Accedere ad Astra Control Center.
2. Verificare che tutti i cluster e le applicazioni gestiti siano ancora presenti e protetti.

## Impostare l'ingresso per il bilanciamento del carico

È possibile impostare un oggetto Kubernetes Ingress che gestisca l'accesso esterno ai servizi, ad esempio il bilanciamento del carico in un cluster.

- L'aggiornamento predefinito utilizza l'implementazione di ingresso generica. In questo caso, sarà

necessario anche configurare un controller di ingresso o una risorsa di ingresso.

- Se non si desidera un controller di ingresso e si desidera conservare ciò che si dispone già, impostare `ingressType` a. `AccTraefik`.

> Per ulteriori informazioni sul tipo di servizio "LoadBalancer" e sull'ingresso, vedere "Requisiti".

I passaggi variano a seconda del tipo di controller di ingresso utilizzato:

- Controller di ingresso nginx
- Controller di ingresso OpenShift

**Di cosa hai bisogno**

- Nella specifica CR,
  - Se `crd.externalTraefik` è presente, deve essere impostato su `false` OPPURE
  - Se `crd.externalTraefik` è `true`, `crd.shouldUpgrade` dovrebbe anche essere `true`.
- Il necessario "controller di ingresso" dovrebbe essere già implementato.
- Il "classe di ingresso" corrispondente al controller di ingresso dovrebbe già essere creato.
- Si stanno utilizzando versioni di Kubernetes comprese tra v1.19 e v1.21.

**Procedura per il controller di ingresso Nginx**

1. Utilizzare il segreto esistente `secure-testing-cert` oppure 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 income in `netapp-acc` namespace (o personalizzato) per uno schema obsoleto o nuovo:
   a. Per uno schema obsoleto, seguire questo esempio:

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

b. Per un nuovo schema, seguire 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
```

**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
```

### Verificare la configurazione dell'ingresso

È possibile verificare la configurazione dell'ingresso prima di continuare.

1. Assicurarsi che Traefik sia cambiato in `clusterIP` Da LoadBalancer:

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

2. Verificare i percorsi in Traefik:

```
Kubectl get ingressroute ingressroutetls -n [netapp-acc or custom
namespace]
-o yaml | grep "Host("
```

Il risultato deve essere vuoto.

# Disinstallare Astra Control Center

Potrebbe essere necessario rimuovere i componenti di Astra Control Center se si esegue l'aggiornamento da una versione di prova a una versione completa del prodotto. Per rimuovere Astra Control Center e Astra Control Center Operator, eseguire i comandi descritti in questa procedura in sequenza.

In caso di problemi con la disinstallazione, vedere Risoluzione dei problemi di disinstallazione.

**Di cosa hai bisogno**

- Utilizzare l'interfaccia utente di Astra Control Center per annullare la gestione di tutto "cluster".

**Fasi**

1. Eliminare Astra Control Center. Il seguente comando di esempio si basa su un'installazione predefinita. Modificare il comando se sono state create configurazioni personalizzate.

   ```
   kubectl delete -f astra_control_center_min.yaml -n netapp-acc
   ```

   Risultato:

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. Utilizzare il seguente comando per eliminare `netapp-acc` spazio dei nomi:

   ```
   kubectl delete ns netapp-acc
   ```

   Risultato:

   ```
   namespace "netapp-acc" deleted
   ```

3. Utilizzare il seguente comando per eliminare i componenti del sistema dell'operatore di Astra Control Center:

   ```
   kubectl delete -f astra_control_center_operator_deploy.yaml
   ```

   Risultato:

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

## Risoluzione dei problemi di disinstallazione

Utilizzare le seguenti soluzioni alternative per risolvere eventuali problemi riscontrati durante la disinstallazione di Astra Control Center.

#### La disinstallazione di Astra Control Center non riesce a pulire il pod operatore di monitoraggio sul cluster gestito

Se i cluster non sono stati disgestiti prima della disinstallazione di Astra Control Center, è possibile eliminare manualmente i pod nello spazio dei nomi di monitoraggio netapp e nello spazio dei nomi con i seguenti comandi:

**Fasi**

1. Eliminare `acc-monitoring` agente:

   ```
   kubectl delete agents acc-monitoring -n netapp-monitoring
   ```

   Risultato:

   ```
   agent.monitoring.netapp.com "acc-monitoring" deleted
   ```

2. Eliminare lo spazio dei nomi:

```
kubectl delete ns netapp-monitoring
```

Risultato:

```
namespace "netapp-monitoring" deleted
```

3. Conferma la rimozione delle risorse:

```
kubectl get pods -n netapp-monitoring
```

Risultato:

```
No resources found in netapp-monitoring namespace.
```

4. Conferma rimozione dell'agente di monitoraggio:

```
kubectl get crd|grep agent
```

Risultato del campione:

```
agents.monitoring.netapp.com                    2021-07-21T06:08:13Z
```

5. Eliminare le informazioni CRD (Custom Resource Definition):

```
kubectl delete crds agents.monitoring.netapp.com
```

Risultato:

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

#### La disinstallazione di Astra Control Center non consente di eliminare i CRD Traefik

È possibile eliminare manualmente i CRD Traefik. Le CRDS sono risorse globali e l'eliminazione di queste risorse potrebbe avere un impatto sulle altre applicazioni del cluster.

**Fasi**

1. Elencare i CRD Traefik installati sul cluster:

```
kubectl get crds |grep -E 'traefik'
```

Risposta

```
ingressroutes.traefik.containo.us             2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us          2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us          2021-06-23T23:29:12Z
middlewares.traefik.containo.us               2021-06-23T23:29:12Z
middlewaretcps.traefik.containo.us            2021-06-23T23:29:12Z
serverstransports.traefik.containo.us         2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us                2021-06-23T23:29:13Z
tlsstores.traefik.containo.us                 2021-06-23T23:29:14Z
traefikservices.traefik.containo.us           2021-06-23T23:29:15Z
```

2. Eliminare i CRD:

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewaretcps.traefik.containo.us
```

## Trova ulteriori informazioni

- "Problemi noti per la disinstallazione"

# Automatizza con REST API

## Automazione mediante l’API REST di Astra Control

Astra Control dispone di un’API REST che consente di accedere direttamente alla funzionalità Astra Control utilizzando un linguaggio di programmazione o un’utility come Curl. Puoi anche gestire le implementazioni di Astra Control utilizzando Ansible e altre tecnologie di automazione.

Per configurare e gestire le applicazioni Kubernetes, è possibile utilizzare l’interfaccia utente Astra o l’API Astra Control.

Per ulteriori informazioni, visitare il sito "Documentazione di automazione Astra".

# Implementa le app

## Implementare Jenkins da un grafico Helm

Scopri come implementare Jenkins da "Grafico di BitNami Helm". Dopo aver implementato Jenkins nel cluster, è possibile registrare l'applicazione con Astra Control.

Jenkins è un'applicazione validata per Astra Control.

- "Scopri la differenza tra un'applicazione validata e un'applicazione standard in Astra Control".

Queste istruzioni sono valide sia per Astra Control Service che per Astra Control Center.

> Le applicazioni implementate da Google Marketplace non sono state validate. Alcuni utenti segnalano problemi di rilevamento e/o backup con le implementazioni Google Marketplace di Postgres, MariaDB e MySQL.

### Requisiti

- Cluster aggiunto ad Astra Control.

  > Per Astra Control Center, è possibile aggiungere prima il cluster ad Astra Control Center o aggiungere prima l'applicazione.

- Versioni aggiornate di Helm (versione 3.2+) e Kubectl installate su una macchina locale con il kubeconfig appropriato per il cluster

Astra Control non supporta attualmente "Kubernetes plugin per Jenkins". È possibile eseguire Jenkins in un cluster Kubernetes senza il plug-in. Il plug-in offre scalabilità al cluster Jenkins.

### Installare Jenkins

Due note importanti su questo processo:

- È necessario implementare l'applicazione dopo che il cluster è stato aggiunto ad Astra Control Service, non prima. Astra Control Center accetta le applicazioni prima o dopo l'aggiunta del cluster ad Astra Control Center.
- È necessario implementare il grafico Helm in uno spazio dei nomi diverso da quello predefinito.

#### Fasi

1. Aggiungere il repo grafico BitNami:

   ```
   helm repo add bitnami https://charts.bitnami.com/bitnami
   ```

2. Creare il `jenkins` Namespace e implementazione di Jenkins all'interno dell'IT con il comando:

```
helm install <name> bitnami/jenkins --namespace <namespace> --create
-namespace
--set global.storageClass=<storage_class_name>
```

> Se le dimensioni del volume vengono modificate, utilizzare le unità Kibibyte (Ki), Mebibyte (mi) o Gibibibyte (Gi).

È necessario definire la classe di storage solo nelle seguenti situazioni:

- Si sta utilizzando Astra Control Service e non si desidera utilizzare la classe di storage predefinita.
- Stai utilizzando Astra Control Center e non hai ancora importato il cluster in Astra Control Center. In alternativa, è stato importato il cluster, ma non si desidera utilizzare la classe di storage predefinita.

**Risultato**

Ciò consente di:

- Crea uno spazio dei nomi.
- Imposta la classe di storage corretta.

Una volta che i pod sono online, puoi gestire l'applicazione con Astra Control. Astra Control consente di gestire un'applicazione a livello di spazio dei nomi o utilizzando un'etichetta Helm.

# Implementare MariaDB da un grafico Helm

Scopri come implementare MariaDB da "Grafico di BitNami Helm". Dopo aver implementato MariaDB sul cluster, è possibile gestire l'applicazione con Astra Control.

MariaDB è un'applicazione validata per Astra.

- "Scopri la differenza tra un'applicazione validata e un'applicazione standard in Astra Control".

Queste istruzioni sono valide sia per Astra Control Service che per Astra Control Center.

> Le applicazioni implementate da Google Marketplace non sono state validate. Alcuni utenti segnalano problemi di rilevamento e/o backup con le implementazioni Google Marketplace di Postgres, MariaDB e MySQL.

## Requisiti

- Cluster aggiunto ad Astra Control.

  > Per Astra Control Center, è possibile aggiungere prima il cluster ad Astra Control Center o aggiungere prima l'applicazione.

- Versioni aggiornate di Helm (versione 3.2+) e Kubectl installate su una macchina locale con il kubeconfig appropriato per il cluster

### Installare MariaDB

Due note importanti su questo processo:

- È necessario implementare l'applicazione dopo che il cluster è stato aggiunto ad Astra Control Service, non prima. Astra Control Center accetta le applicazioni prima o dopo l'aggiunta del cluster ad Astra Control Center.
- È necessario implementare il grafico Helm in uno spazio dei nomi diverso da quello predefinito.

**Fasi**

1. Aggiungere il repo grafico BitNami:

```
helm repo add bitnami https://charts.bitnami.com/bitnami
```

2. Implementare MariaDB con il comando:

```
helm install <name> bitnami/MariaDB --namespace <namespace> --create
-namespace
--set global.storageClass=<storage_class_name>
```

> Se le dimensioni del volume vengono modificate, utilizzare le unità Kibibyte (Ki), Mebibyte (mi) o Gibibibyte (Gi).

È necessario definire la classe di storage solo nelle seguenti situazioni:

- Si sta utilizzando Astra Control Service e non si desidera utilizzare la classe di storage predefinita.
- Stai utilizzando Astra Control Center e non hai ancora importato il cluster in Astra Control Center. In alternativa, è stato importato il cluster, ma non si desidera utilizzare la classe di storage predefinita.

**Risultato**

Ciò consente di:

- Crea uno spazio dei nomi.
- Implementa MariaDB nello spazio dei nomi.
- Crea un database.

> Questo metodo di impostazione della password durante l'implementazione non è sicuro. Non è consigliabile per un ambiente di produzione.

Una volta che i pod sono online, puoi gestire l'applicazione con Astra Control. Astra Control consente di gestire un'applicazione a livello di spazio dei nomi o utilizzando un'etichetta Helm.

# Implementa MySQL da un grafico Helm

Scopri come implementare MySQL da "Grafico di BitNami Helm". Dopo aver implementato MySQL sul cluster Kubernetes, è possibile gestire l'applicazione con Astra Control.

MySQL è un'applicazione validata per Astra Control.

- "Scopri la differenza tra un'applicazione validata e un'applicazione standard in Astra Control".

Queste istruzioni sono valide sia per Astra Control Service che per Astra Control Center.

> Le applicazioni implementate da Google Marketplace non sono state validate. Alcuni utenti segnalano problemi di rilevamento e/o backup con le implementazioni Google Marketplace di Postgres, MariaDB e MySQL.

## Requisiti

- Cluster aggiunto ad Astra Control.

  > Per Astra Control Center, è possibile aggiungere prima il cluster ad Astra Control Center o aggiungere prima l'applicazione.

- Versioni aggiornate di Helm (versione 3.2+) e Kubectl installate su una macchina locale con il kubeconfig appropriato per il cluster

## Installare MySQL

Due note importanti su questo processo:

- È necessario implementare l'applicazione dopo che il cluster è stato aggiunto ad Astra Control Service, non prima. Astra Control Center accetta le applicazioni prima o dopo l'aggiunta del cluster ad Astra Control Center.
- Si consiglia di implementare il grafico Helm in uno spazio dei nomi diverso da quello predefinito.

**Fasi**

1. Aggiungere il repo grafico BitNami:

   ```
   helm repo add bitnami https://charts.bitnami.com/bitnami
   ```

2. Implementare MySQL con il comando:

   ```
   helm install <name> bitnami/mysql --namespace <namespace> --create
   -namespace
   --set global.storageClass=<storage_class_name>
   ```

   > Se le dimensioni del volume vengono modificate, utilizzare le unità Kibibyte (Ki), Mebibyte (mi) o Gibibibyte (Gi).

   È necessario definire la classe di storage solo nelle seguenti situazioni:

   - Si sta utilizzando Astra Control Service e non si desidera utilizzare la classe di storage predefinita.
   - Stai utilizzando Astra Control Center e non hai ancora importato il cluster in Astra Control Center. In alternativa, è stato importato il cluster, ma non si desidera utilizzare la classe di storage predefinita.

**Risultato**

Ciò consente di:

- Crea uno spazio dei nomi.
- Implementa MySQL sullo spazio dei nomi.

Una volta che i pod sono online, puoi gestire l'applicazione con Astra Control. Astra Control consente di gestire un'applicazione con il suo nome, a livello di spazio dei nomi o utilizzando un'etichetta Helm.

# Implementare Postgres da un grafico Helm

Scopri come implementare Postgres da "Grafico di BitNami Helm". Dopo aver implementato Postgres sul cluster, è possibile registrare l'applicazione con Astra Control.

Postgres è un'applicazione validata per Astra.

- "Scopri la differenza tra un'applicazione validata e un'applicazione standard in Astra Control".

Queste istruzioni sono valide sia per Astra Control Service che per Astra Control Center.

> Le applicazioni implementate da Google Marketplace non sono state validate. Alcuni utenti segnalano problemi di rilevamento e/o backup con le implementazioni Google Marketplace di Postgres, MariaDB e MySQL.

## Requisiti

- Cluster aggiunto ad Astra Control.

  > Per Astra Control Center, è possibile aggiungere prima il cluster ad Astra Control Center o aggiungere prima l'applicazione.

- Versioni aggiornate di Helm (versione 3.2+) e Kubectl installate su una macchina locale con il kubeconfig appropriato per il cluster

## Installare Postgres

Due note importanti su questo processo:

- È necessario implementare l'applicazione dopo che il cluster è stato aggiunto ad Astra Control Service, non prima. Astra Control Center accetta le applicazioni prima o dopo l'aggiunta del cluster ad Astra Control Center.
- È necessario implementare il grafico Helm in uno spazio dei nomi diverso da quello predefinito.

**Fasi**

1. Aggiungere il repo grafico BitNami:

   ```
   helm repo add bitnami https://charts.bitnami.com/bitnami
   ```

2. Implementare Postgres con il comando:

```
helm install <name> bitnami/postgresql --namespace <namespace> --create
-namespace
--set global.storageClass=<storage_class_name>
```

> Se le dimensioni del volume vengono modificate, utilizzare le unità Kibibyte (Ki), Mebibyte (mi) o Gibibibyte (Gi).

È necessario definire la classe di storage solo nelle seguenti situazioni:

- Si sta utilizzando Astra Control Service e non si desidera utilizzare la classe di storage predefinita.
- Stai utilizzando Astra Control Center e non hai ancora importato il cluster in Astra Control Center. In alternativa, è stato importato il cluster, ma non si desidera utilizzare la classe di storage predefinita.

**Risultato**

Ciò consente di:

- Crea uno spazio dei nomi.
- Implementa Postgres nello spazio dei nomi.

Una volta che i pod sono online, puoi gestire l'applicazione con Astra Control. Astra Control consente di gestire un'applicazione a livello di spazio dei nomi o utilizzando un'etichetta Helm.

# Conoscenza e supporto

## Risoluzione dei problemi

Scopri come risolvere alcuni problemi comuni che potresti incontrare.

https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Astra

### Trova ulteriori informazioni

- "Come caricare un file su NetApp (accesso richiesto)"
- "Come caricare manualmente un file su NetApp (accesso richiesto)"

## Richiedi assistenza

NetApp fornisce supporto per Astra Control in diversi modi. Sono disponibili opzioni complete di supporto autonomo gratuito 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un canale slack. Il tuo account Astra Control include il supporto tecnico remoto via web ticketing.

> Se si dispone di una licenza di valutazione per Astra Control Center, è possibile ottenere supporto tecnico. Tuttavia, la creazione del caso tramite il NetApp Support Site (NSS) non è disponibile. Puoi contattare il supporto tramite l'opzione di feedback o utilizzare il canale Slack per il self-service.

Devi prima "Attivare il supporto per il numero di serie NetApp" per utilizzare queste opzioni di supporto non self-service. È necessario un account SSO NetApp Support Site (NSS) per la chat e il web ticketing insieme alla gestione del caso.

### Opzioni di supporto automatico

È possibile accedere alle opzioni di supporto dall'interfaccia utente di Astra Control Center selezionando la scheda **Support** (supporto) dal menu principale.

Queste opzioni sono disponibili gratuitamente, 24 ore su 24, 7 giorni su 7:

- "**Knowledge base** (accesso richiesto)": Cerca articoli, FAQ o informazioni di riparazione in caso di interruzione relative ad Astra Control.
- **Centro di documentazione**: Questo è il sito di documentazione che stai visualizzando.
- "**Richiedi assistenza tramite Slack**": Vai al canale Containers nello spazio di lavoro Pub per entrare in contatto con colleghi ed esperti.
- **Creare un caso di supporto**: Generare pacchetti di supporto da fornire al supporto NetApp per la risoluzione dei problemi.
- **Invia un feedback su Astra Control**: Invia un'e-mail a astra.feedback@netapp.com per farci conoscere le tue opinioni, le tue idee o i tuoi dubbi.

## Abilita il caricamento giornaliero del bundle di supporto pianificato sul supporto NetApp

Durante l'installazione di Astra Control Center, se specificato `enrolled: true` per `autoSupport` Nel file CRD (Custom Resource Definition) di Astra Control Center (`astra_control_center_min.yaml`), i pacchetti di supporto giornalieri vengono caricati automaticamente su "Sito di supporto NetApp".

## Generare bundle di supporto da fornire al supporto NetApp

Astra Control Center consente all'utente amministratore di generare bundle, che includono informazioni utili al supporto NetApp, inclusi registri, eventi per tutti i componenti dell'implementazione Astra, metriche e informazioni sulla topologia dei cluster e delle applicazioni in gestione. Se si è connessi a Internet, è possibile caricare pacchetti di supporto sul NetApp Support Site (NSS) direttamente dall'interfaccia utente di Astra Control Center.

> Il tempo impiegato da Astra Control Center per generare il bundle dipende dalle dimensioni dell'installazione di Astra Control Center e dai parametri del bundle di supporto richiesto. La durata specificata per la richiesta di un bundle di supporto determina il tempo necessario per la generazione del bundle (ad esempio, un periodo di tempo più breve comporta una generazione più rapida del bundle).

#### Prima di iniziare

Determinare se sarà richiesta una connessione proxy per caricare bundle su NSS. Se è necessaria una connessione proxy, verificare che Astra Control Center sia stato configurato per l'utilizzo di un server proxy.

1. Selezionare **account** > **connessioni**.
2. Controllare le impostazioni del proxy in **Impostazioni di connessione**.

#### Fasi

1. Creare un caso sul portale NSS utilizzando il numero di serie della licenza elencato nella pagina **Support** dell'interfaccia utente di Astra Control Center.
2. Per generare il bundle di supporto, attenersi alla seguente procedura utilizzando l'interfaccia utente di Astra Control Center:

   a. Nella sezione Support bundle della pagina **Support**, selezionare **generate**.

   b. Nella finestra **generate a Support Bundle** (genera un pacchetto di supporto), selezionare il periodo di tempo.

      È possibile scegliere tra tempi rapidi o personalizzati.

      > È possibile scegliere un intervallo di date personalizzato e specificare un periodo di tempo personalizzato durante l'intervallo di date.

   c. Una volta effettuate le selezioni, selezionare **Confirm** (Conferma).

   d. Selezionare la casella di controllo **caricare il bundle nel sito di supporto NetApp quando generato**.

   e. Selezionare **generate Bundle** (genera bundle).

      Quando il bundle di supporto è pronto, viene visualizzata una notifica nella pagina **account** > **notifica** nell'area Avvisi, nella pagina **attività** e nell'elenco delle notifiche (accessibile selezionando l'icona nella parte superiore destra dell'interfaccia utente).

Se la generazione non riesce, viene visualizzata un'icona nella pagina generate Bundle (genera bundle). Selezionare l'icona per visualizzare il messaggio.

> L'icona delle notifiche nella parte superiore destra dell'interfaccia utente fornisce informazioni sugli eventi correlati al bundle di supporto, ad esempio quando il bundle viene creato correttamente, quando la creazione del bundle non riesce, quando il bundle non può essere caricato, quando il bundle non può essere scaricato e così via.

**Se si dispone di un'installazione con aria compressa**

Se si dispone di un'installazione con aria compressa, attenersi alla seguente procedura dopo la generazione del pacchetto di supporto. Quando il bundle è disponibile per il download, l'icona Download viene visualizzata accanto a **generate** nella sezione **Support Bundle** della pagina **Support**.

**Fasi**

1. Selezionare l'icona Download per scaricare il pacchetto localmente.
2. Caricare manualmente il bundle su NSS.

   A tale scopo, è possibile utilizzare uno dei seguenti metodi:

   - Utilizzare "NetApp Authenticated file Upload (accesso richiesto)".
   - Collegare il bundle alla custodia direttamente su NSS.
   - Utilizza NetApp Active IQ.

## Trova ulteriori informazioni

- "Come caricare un file su NetApp (accesso richiesto)"
- "Come caricare manualmente un file su NetApp (accesso richiesto)"

# Versioni precedenti della documentazione di Astra Control Center

È disponibile la documentazione per le release precedenti.

- "Documentazione di Astra Control Center 21.12"
- "Documentazione di Astra Control Center 21.08"

# Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

## Copyright

"https://www.netapp.com/company/legal/copyright/"

## Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

## Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

## Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

## Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per Astra Control Center"
- "Avviso per Astra Data Store"

## Licenza API Astra Control

https://docs.netapp.com/us-en/astra-automation-2204/media/astra-api-license.pdf