Documentazione di Astra Control Center 21.08

Astra Control Center

NetApp
November 20, 2023

Sommario

Documentazione di Astra Control Center 21.08

Note di rilascio

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

- "Cosa c'è in questa release di Astra Control Center"
- "Problemi noti"
- "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.

Cosa c'è in questa release di Astra Control Center

Siamo lieti di annunciare il rilascio di Astra Control Center.

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"

Problemi noti relativi a questa versione

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:

- ClusterRoleBinding non corretto creato da Astra Control Center CRD durante l'installazione
- L'applicazione con etichetta definita dall'utente passa allo stato "removed" (rimosso)
- Impossibile interrompere l'esecuzione del backup dell'applicazione
- Il backup o il clone non riesce per le applicazioni che utilizzano PVC con unità decimali in Astra Control Center
- ad esempio le modifiche persistenti del volume

- Trident crea un PV più grande del PV originale
- Clonare le performance influenzate da grandi volumi persistenti
- 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 bucket S3 in Astra Control Center non riportano la capacità disponibile
- Il riutilizzo dei bucket tra istanze di Astra Control Center causa errori
- La selezione di un tipo di provider bucket con credenziali per un altro tipo causa errori di protezione dei dati
- I backup e le snapshot potrebbero non essere conservati durante la rimozione di un'istanza di Astra Control Center
- I backup aggiuntivi vengono conservati come parte del backup pianificato
- "L'operazione di cloning non può utilizzare altri bucket oltre a quelli predefiniti"
- La gestione di un cluster con Astra Control Center non riesce quando il file kubeconfig predefinito contiene più di un contesto
- "Impossibile determinare lo stato del bundle tar ASUP in un ambiente scalato"
- La disinstallazione di Astra Control Center non riesce a pulire il pod operatore di monitoraggio sul cluster gestito
- La disinstallazione di Astra Control Center non consente di eliminare i CRD Traefik
- Raccolta ASUP bloccata in uno stato di generazione o caricamento

ClusterRoleBinding non corretto creato da Astra Control Center CRD durante l'installazione

Applicare la seguente patch a tutti i cluster Kubernetes in cui è stata implementata la versione 21.08.65 dell'operatore acc. Deve essere applicato anche se l'operatore acc viene riattivato.

Per risolvere questo problema:

1. Sostituire `ACC_NAMESPACE` nello script riportato di seguito con lo spazio dei nomi utilizzato "Implementare Astra Control Center".

```
cat <<EOF | kubectl apply -f -
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: acc-operator-manager-rolebinding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: acc-operator-manager-role
subjects:
- kind: ServiceAccount
  name: default
  namespace: netapp-acc-operator
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts:ACC_NAMESPACE
EOF
```

2. Eseguire lo script.

Il cerotto rimuove i seguenti due soggetti `ClusterRoleBinding: "acc-operator-manager-rolebinding"`

```
- apiGroup: rbac.authorization.k8s.io
  kind: Group
  name: system:serviceaccounts
- apiGroup: ""
  kind: Group
  name: system:serviceaccounts
```

L'applicazione con etichetta definita dall'utente passa allo stato "removed" (rimosso)

Se definisci un'applicazione con un'etichetta k8s inesistente, Astra Control Center creerà, gestirà e rimuoverà immediatamente l'applicazione. Per evitare questo problema, Aggiungi l'etichetta k8s ai pod e alle risorse dopo che l'applicazione è stata gestita da Astra Control Center.

Impossibile interrompere l'esecuzione del backup dell'applicazione

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 Astra".

Il backup o il clone non riesce per le applicazioni che utilizzano PVC con unità decimali in Astra Control Center

I volumi creati con unità decimali non riescono utilizzando il processo di backup o clone di Astra Control Center. Vedere "articolo della knowledge base" per ulteriori informazioni.

L'interfaccia utente di Astra Control Center mostra lentamente le modifiche apportate alle risorse dell'applicazione, ad esempio le modifiche persistenti del volume

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. Questo ritardo nell'interfaccia utente può verificarsi anche quando vengono aggiunte o modificate le risorse dell'applicazione. In questo caso, un'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.

Durante il ripristino dell'applicazione dal backup, Trident crea un PV più grande 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.

Clonare le performance influenzate da grandi volumi persistenti

I cloni di volumi persistenti molto grandi e consumati potrebbero essere lenti a intermittenza, a seconda dell'accesso del cluster all'archivio di oggetti. Se il clone viene bloccato e non sono stati copiati dati per più di 30 minuti, Astra Control termina l'azione del clone.

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 OCP. 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 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.

Il riutilizzo dei bucket tra istanze di Astra Control Center causa errori

Se si tenta di riutilizzare un bucket utilizzato da un'altra o da un'altra installazione di Astra Control Center, il

backup e il ripristino non avranno esito positivo. È necessario utilizzare una benna diversa o pulire completamente la benna utilizzata in precedenza. Non è possibile condividere i bucket tra istanze di Astra Control Center.

La selezione di un tipo di provider bucket con credenziali per un altro tipo causa errori di protezione dei dati

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

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.

I backup aggiuntivi vengono conservati come parte del backup pianificato

A volte uno o più backup in Astra Control Center vengono conservati oltre il numero specificato per essere conservati nella pianificazione del backup. Questi backup aggiuntivi devono essere cancellati come parte di un backup pianificato, ma non vengono cancellati e bloccati in un `pending` stato. Per risolvere il problema, "forza eliminazione" i backup aggiuntivi.

L'operazione di cloning non può utilizzare altri bucket oltre a quelli predefiniti

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.

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.

Impossibile determinare lo stato del bundle tar ASUP in un ambiente scalato

Durante la raccolta ASUP, lo stato del bundle nell'interfaccia utente viene riportato come uno dei due `collecting` oppure `done`. La raccolta può richiedere fino a un'ora per ambienti di grandi dimensioni. Durante il download di ASUP, la velocità di trasferimento dei file di rete per il bundle potrebbe essere insufficiente e il download potrebbe scadere dopo 15 minuti senza alcuna indicazione nell'interfaccia utente. I problemi di download dipendono dalle dimensioni dell'ASUP, dalle dimensioni del cluster scalate e se il tempo di raccolta supera il limite di sette giorni.

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:

   ```
   oc delete agents acc-monitoring -n netapp-monitoring
   ```

   Risultato:

   ```
   agent.monitoring.netapp.com "acc-monitoring" deleted
   ```

2. Eliminare lo spazio dei nomi:

   ```
   oc delete ns netapp-monitoring
   ```

   Risultato:

   ```
   namespace "netapp-monitoring" deleted
   ```

3. Conferma la rimozione delle risorse:

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

   Risultato:

   ```
   No resources found in netapp-monitoring namespace.
   ```

4. Conferma rimozione dell'agente di monitoraggio:

   ```
   oc get crd|grep agent
   ```

   Risultato del campione:

   ```
   agents.monitoring.netapp.com                    2021-07-21T06:08:13Z
   ```

5. Eliminare le informazioni CRD (Custom Resource Definition):

   ```
   oc 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:

Fasi

1. Verificare quali CRD non sono stati eliminati dal processo di disinstallazione:

```
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
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
```

Raccolta ASUP bloccata in uno stato di generazione o caricamento

Se un pod ASUP viene ucciso o riavviato, una raccolta ASUP potrebbe bloccarsi in uno stato di generazione o caricamento. Effettuare le seguenti operazioni "API REST di Astra Control" chiamata per avviare nuovamente la raccolta manuale:

Metodo HTTP	Percorso
POST	/Accounts/{AccountID}/core/v1/asups

Questa soluzione alternativa API funziona solo se eseguita più di 10 minuti dopo l'avvio di ASUP.

Trova ulteriori informazioni

- "Limitazioni note per questa versione"

Limitazioni note di questa versione

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.

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.

Il cluster è in `removed` stato anche se il cluster e la rete funzionano in modo diverso come previsto

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":

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`.

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

Astra Control Center non supporta le applicazioni implementate con operatori abilitati per Operator Lifecycle Manager (OLM) o con gli operatori con ambito cluster.

La clonazione delle applicazioni può essere eseguita solo con la stessa distribuzione K8s

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

OpenShift 4.8 non è supportato

OpenShift 4.8 non è supportato per la release di luglio di Astra Control Center. Per ulteriori informazioni, vedere "Requisiti di Astra Control Center".

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".

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

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

Data Protection per Astra Control Center come applicazione non ancora disponibile

Questa release non supporta la possibilità di gestire Astra come applicazione utilizzando opzioni di snapshot, backup o ripristino.

I pod non integri influiscono sulla gestione delle applicazioni

Se un'applicazione gestita ha dei pod in uno stato non integro, Astra Control non può creare nuovi backup e cloni.

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.

Trident non viene disinstallato da un cluster

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".

Trova ulteriori informazioni

- "Problemi noti per questa release"

Concetti

Introduzione a 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 allo storage back-end o ai servizi esterni	Stesse funzionalità su entrambe le piattaforme con eccezioni allo storage back-end o ai servizi esterni
Qual è il supporto dello storage back-end?	Offerte di servizi cloud NetApp	Sistemi NetApp ONTAP AFF e FAS

Applicazioni supportate

Astra Control Center non supporta le applicazioni implementate con operatori abilitati per Operator Lifecycle Manager (OLM) o con gli operatori con ambito cluster.

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 Center".

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" come storage back-end per i volumi persistenti.
  - Per i cluster AKS, Astra Control Service utilizza "Azure NetApp Files" come storage back-end 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.
  - 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.

Per la prima release, Astra Control Center supporterà cluster OpenShift Kubernetes e backend di storage Trident con ONTAP 9.5 e versioni successive.

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 lo storage back-end 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 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.

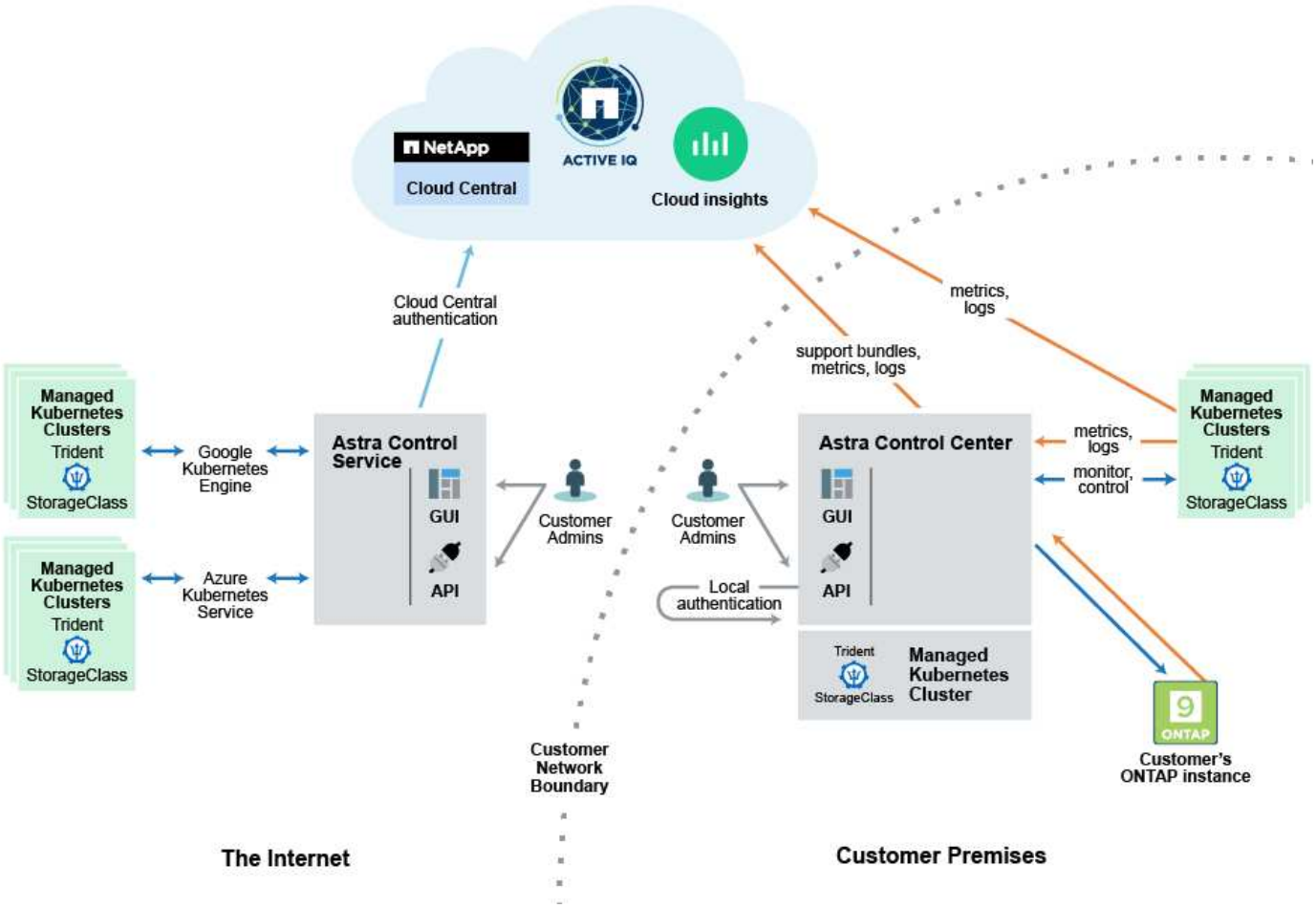
Per ulteriori informazioni

- "Documentazione del servizio Astra Control"
- "Documentazione di Astra Control Center"
- "Documentazione di Astra Trident"
- "Utilizzare l'API 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.
- **Storage backend**: Utilizzo di Astra Control Service "NetApp Cloud Volumes Service per Google Cloud" Come storage back-end per i cluster GKE e. "Azure NetApp Files" Come storage back-end per i cluster AKS.

  Il centro di controllo Astra utilizza un 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.

- **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 Control"
- "Documentazione di Astra Trident"
- "Utilizzare l'API Astra"
- "Documentazione Cloud Insights"
- "Documentazione ONTAP"

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

Centro di controllo Astra supporta ONTAP come storage back-end. Devi comprendere come la classe di storage e le dimensioni dei volumi persistenti (PV) possono aiutarti a raggiungere i tuoi obiettivi di performance.

Panoramica

Al momento, il Centro di controllo Astra supporta solo classi di storage Trident supportate dallo storage ONTAP. Centro di controllo Astra rileva e utilizza le risorse già implementate, tra cui ONTAP, Trident e le classi di storage associate.

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

Classi di storage

Quando si aggiungono cluster ad Astra Control Center, viene richiesto di scegliere una delle classi di storage rilevate in precedenza per i volumi persistenti. I livelli di servizio nelle classi di storage sono progettati per esigenze di capacità e larghezza di banda diverse. Queste classi di storage scoperte sono idonee per l'utilizzo all'interno di Astra Control Center.

Dimensioni e performance del volume persistenti

Consulta le informazioni di Trident che forniscono confronti dei costi ed esempi che possono aiutarti a comprendere meglio come abbinare un livello di servizio alle dimensioni del volume per soddisfare i tuoi obiettivi di performance.

Trova ulteriori informazioni

- "Documentazione di Trident sulla configurazione dello storage"

Inizia subito

Requisiti di Astra Control Center

Inizia verificando il supporto per cluster, applicazioni, licenze e browser web Kubernetes.

Requisiti generali del cluster Kubernetes

Un cluster Kubernetes deve soddisfare i seguenti requisiti generali in modo da poterlo individuare e gestire da Astra Control Center.

- **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 disporre dell'URL del registro delle immagini in cui caricare le immagini e contrassegnare le immagini per il registro dei container privati.
- **Configurazione dello storage Trident / ONTAP**: Il centro di controllo Astra richiede che Trident versione 21.01 o 21.04 sia già installato e configurato per funzionare con NetApp ONTAP versione 9.5 o successiva come backend dello storage. 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 Trident:
  - ontap-nas
  - ontap-nas-flexgroup
  - ontap-san
  - ontap-san-economy

Se si intende gestire il cluster Kubernetes da Astra Control Center e utilizzare il cluster per ospitare l'installazione di Astra Control Center, il cluster presenta i seguenti requisiti aggiuntivi:

- La versione più recente di Kubernetes "componente snapshot-controller" è installato
- Un Trident "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 Trident
- Metodo per indirizzare l'FQDN di Astra Control Center all'indirizzo IP esterno del servizio Astra Control Center

Cluster OpenShift

Centro di controllo Astra richiede un cluster Red Hat OpenShift Container Platform 4.6.8 o 4.7 con classi di storage Trident supportate da ONTAP 9.5 o versione successiva, con i seguenti attributi:

- Almeno 300 GB di capacità di storage ONTAP disponibile
- 3 nodi controller con 4 core CPU, 16 GB di RAM e 120 GB di storage disponibili ciascuno
- 3 nodi di lavoro con almeno 12 core CPU, 32 GB di RAM e 50 GB di storage disponibili ciascuno
- Kubernetes versione 1.19 o 1.20
- Tipo di servizio "LoadBalancer" disponibile per il traffico in ingresso da inviare ai servizi nel cluster OpenShift
- Metodo per indirizzare l'FQDN di Astra Control Center all'indirizzo IP con bilanciamento del carico

Questi requisiti minimi presuppongono che Astra Control Center sia l'unica applicazione in esecuzione sul cluster OpenShift. Se il cluster esegue applicazioni aggiuntive, è necessario modificare di conseguenza questi requisiti minimi.

Assicurarsi che il cluster soddisfi i requisiti minimi e seguire le Best practice di Kubernetes in modo che Astra Control Center sia altamente disponibile nel cluster Kubernetes.

OpenShift 4.8 non è supportato.

Durante la clonazione dell'applicazione, Astra Control Center deve consentire a OpenShift di montare volumi e modificare la proprietà dei file. Per questo motivo, ONTAP deve essere configurato in modo da consentire il completamento corretto delle operazioni del volume utilizzando i seguenti comandi:

1. `export-policy rule modify -vserver svm0 -policyname default -ruleindex 1 -superuser sys`
2. `export-policy rule modify -policyname default -ruleindex 1 -anon 65534`

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

Requisiti di gestione delle applicazioni

Astra Control Center ha i seguenti requisiti di gestione delle applicazioni:

- **Licensing**: È necessaria una licenza Astra Control Center per gestire le applicazioni utilizzando Astra Control Center.
- **Helm 3**: 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.
- **Gestione degli operatori**: Astra Control Center non supporta le applicazioni implementate con operatori abilitati per Operator Lifecycle Manager (OLM) o con gli operatori con ambito cluster.

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 al 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".

Tipo di servizio "LoadBalancer" per cluster Kubernetes on-premise

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. Per i cluster OpenShift on-premise, è possibile utilizzare "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.

Requisiti di rete

Il cluster 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 il cluster che ospita Astra Control Center e ciascun cluster gestito (annotato dove applicabile).

Prodotto	Porta	Protocollo	Direzione	Scopo
Centro di controllo Astra	443	HTTPS	Ingresso	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
Centro di controllo Astra	9090	HTTPS	• Ingresso (al cluster che ospita Astra Control Center) • Egress (porta casuale dall'indirizzo IP del nodo di ciascun nodo di lavoro di ciascun cluster gestito)	Dati delle metriche per il cliente: Assicurarsi che ogni cluster gestito possa accedere a questa porta sul cluster che ospita Astra Control Center
Trident	34571	HTTPS	Ingresso	Comunicazione del nodo pod
Trident	9220	HTTP	Ingresso	Endpoint delle metriche

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 da Trident.
- 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

- Scarica Astra Control Center dal NetApp Support Site.
- Installare Astra Control Center nell'ambiente locale.
- Scopri la tua configurazione Trident supportata dal backend dello storage ONTAP.

  Per la prima release, installerai le immagini su un registro OpenShift o utilizzerai il registro locale.

"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 backend di storage ONTAP.
- 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 Astra"

Installare Astra Control Center

Per installare Astra Control Center, procedere come segue:

- Installare Astra Control Center
- Accedere all'interfaccia utente di Astra Control Center

Installare Astra Control Center

Per installare Astra Control Center, scarica il pacchetto di installazione dal NetApp Support Site ed esegui una serie di comandi per installare Astra Control Center Operator e Astra Control Center nel tuo ambiente. È possibile utilizzare questa procedura per installare Astra Control Center in ambienti connessi a Internet o con connessione ad aria.

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
```

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.

> I comandi Podman possono essere utilizzati al posto dei comandi Docker se si utilizza il repository Podman di Red Hat.

Fasi

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 da "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
```

5. Passare alla directory Astra.

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

6. 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 [Docker_registry_path]
```

   b. Caricare le immagini in Docker.
   c. Contrassegnare le immagini.
   d. Trasferire le immagini nel registro locale.

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

7. (Solo per i registri con requisiti di autenticazione) 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=[Docker_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]
   ```

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

Risposta

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

8. 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: astra-registry-cred
```

b. Cambiare `[Docker_registry_path]` per `kube-rbac-prox` immagine al percorso del registro in cui sono state inviate le immagini in un passaggio precedente.

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

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: [Docker_registry_path]/kube-rbac-proxy:v0.5.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        image: [Docker_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

9. Modificare il file delle risorse personalizzate (CR) di Astra Control Center (`astra_control_center_min.yaml`):

```
vim astra_control_center_min.yaml
```

> 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.

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

a. Cambiare `[Docker_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. Se non si utilizza un registro che richiede l'autorizzazione, eliminare `secret` linea.

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

10. 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
```

11. 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]
```

Esempio di risposta:

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

12. Eseguire la seguente patch per correggere "associazione dei ruoli del cluster".
13. 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]
```

Esempio di risposta:

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

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

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

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-5fdfff786f-gkv6z              1/1     Running   0
4m58s
activity-649f869bf7-jn5gs                   1/1     Running   0
3m14s
asup-79846b5fdc-s9s97                       1/1     Running   0
3m10s
authentication-84c78f5cf4-qhx9t             1/1     Running   0
118s
billing-9b8496787-v8rzv                     1/1     Running   0
2m54s
bucketservice-5fb876d9d5-wkfvz              1/1     Running   0
3m26s
cloud-extension-f9f4f59c6-dz6s6             1/1     Running   0
3m
cloud-insights-service-5676b8c6d4-6q7lv     1/1     Running   0
2m52s
composite-compute-7dcc9c6d6c-lxdr6          1/1     Running   0
2m50s
composite-volume-74dbfd7577-cd42b           1/1     Running   0
3m2s
credentials-75dbf46f9d-5qm2b                1/1     Running   0
3m32s
entitlement-6cf875cb48-gkvhp                1/1     Running   0
3m12s
features-74fd97bb46-vss2n                   1/1     Running   0
3m6s
fluent-bit-ds-2g9jb                         1/1     Running   0
113s
fluent-bit-ds-5tg5h                         1/1     Running   0
113s
fluent-bit-ds-qfxb8                         1/1     Running   0
113s
graphql-server-7769f98b86-p4qrv             1/1     Running   0
90s
```

```
identity-566c566cd5-ntfj6                    1/1     Running   0
3m16s
influxdb2-0                                  1/1     Running   0
4m43s
krakend-5cb8d56978-44q66                     1/1     Running   0
93s
license-66cbbc6f48-27kgf                     1/1     Running   0
3m4s
login-ui-584f7fd84b-dmdrp                    1/1     Running   0
87s
loki-0                                       1/1     Running   0
4m44s
metrics-ingestion-service-6dcfddf45f-mhnvh   1/1     Running   0
3m8s
monitoring-operator-78d67b4d4-nxs6v          2/2     Running   0
116s
nats-0                                       1/1     Running   0
4m40s
nats-1                                       1/1     Running   0
4m26s
nats-2                                       1/1     Running   0
4m15s
nautilus-9b664bc55-rn9t8                     1/1     Running   0
2m56s
openapi-dc5ddfb7d-6q8vh                      1/1     Running   0
3m20s
polaris-consul-consul-5tjs7                  1/1     Running   0
4m43s
polaris-consul-consul-5wbnx                  1/1     Running   0
4m43s
polaris-consul-consul-bfvl7                  1/1     Running   0
4m43s
polaris-consul-consul-server-0               1/1     Running   0
4m43s
polaris-consul-consul-server-1               1/1     Running   0
4m43s
polaris-consul-consul-server-2               1/1     Running   0
4m43s
polaris-mongodb-0                            2/2     Running   0
4m49s
polaris-mongodb-1                            2/2     Running   0
4m22s
polaris-mongodb-arbiter-0                    1/1     Running   0
4m49s
polaris-ui-6648875998-75d98                  1/1     Running   0
92s
```

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

15. (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
```

16. Una volta eseguiti tutti i pod, verificare che l'installazione sia riuscita recuperando l'istanza di AstraControlCenter installata dall'operatore ACC.

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

17. Controllare `status.deploymentState` nella risposta per `Deployed` valore. Se l'implementazione non ha avuto esito positivo, viene visualizzato un messaggio di errore.

> Verrà utilizzato il `uuid` nella fase successiva.

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

18. Per ottenere la password monouso da utilizzare quando si accede ad Astra Control Center, copiare il

`status.uuid` valore della risposta nella fase precedente. La password è `ACC-` Seguito dal valore UUID (`ACC-[UUID]` oppure, in questo esempio, `ACC-c49008a5-4ef1-4c5d-a53e-830daf994116`).

Accedere all'interfaccia utente di Astra Control Center

Dopo aver installato ACC, si modifica la password dell'amministratore predefinito e si accede alla dashboard dell'interfaccia utente ACC.

Fasi

1. In un browser, immettere l'FQDN utilizzato in `astraAddress` in `astra_control_center_min.yaml` CR quando ACC 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 ACC 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".

Configurare Astra Control Center

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.

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.

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

Aggiungere una licenza completa o di valutazione

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.

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.

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.

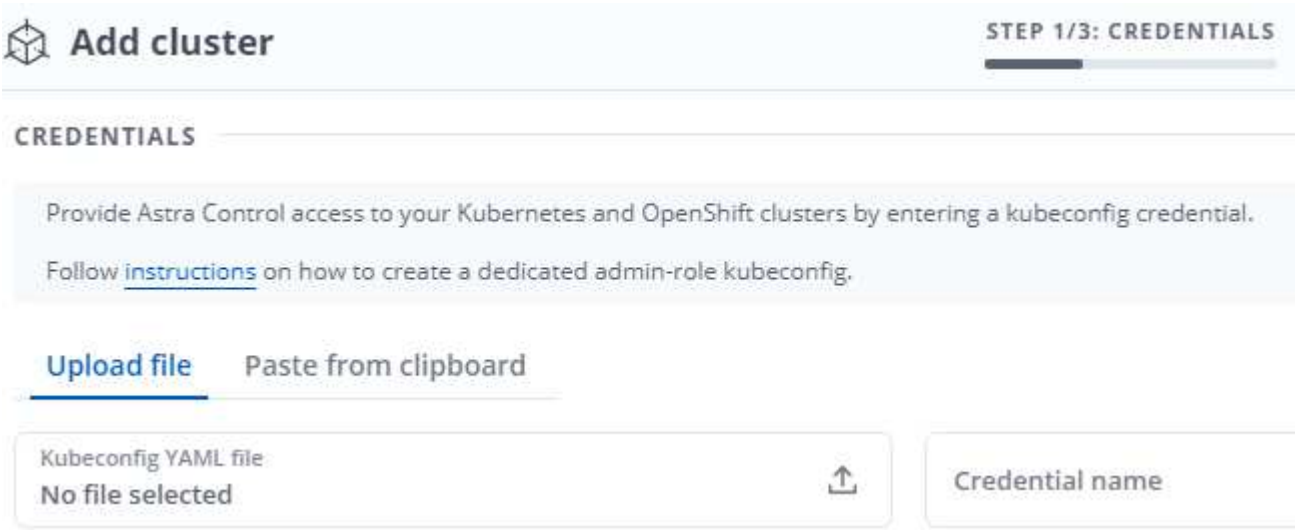
Cosa ti serve? 8217

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**.

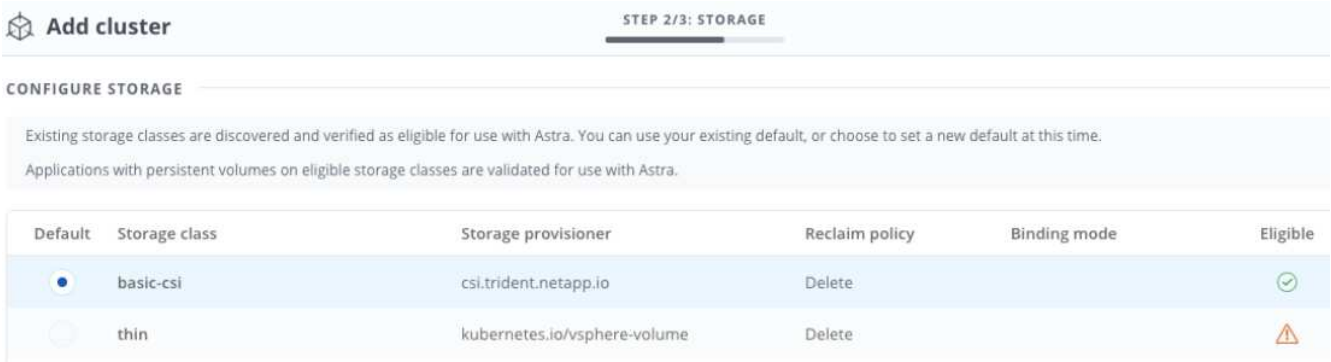


   Se crei il tuo `kubeconfig` file, è necessario definire solo **un** elemento di contesto al suo interno. Vedere "Documentazione Kubernetes" per informazioni sulla creazione `kubeconfig` file.

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**.

> Selezionare una classe di storage Trident supportata dallo storage ONTAP.



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. 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 aggiungere un backend di storage nei seguenti modi:

- Configurare lo storage quando si aggiunge un cluster. Vedere "Aggiungere il cluster".
- Aggiungere un backend di storage rilevato utilizzando la dashboard o l'opzione Backend.

È possibile aggiungere un backend di storage già rilevato utilizzando le seguenti opzioni:

- Aggiungere il back-end di storage utilizzando Dashboard
- Aggiungere il backend di storage utilizzando l'opzione Backend

Aggiungere il back-end di storage utilizzando Dashboard

1. Dalla dashboard eseguire una delle seguenti operazioni:
   a. Dalla sezione backend Dashboard Storage, selezionare **Manage** (Gestisci).
   b. Dalla sezione Dashboard Resource Summary > Storage Backend, selezionare **Add** (Aggiungi).

2. Immettere le credenziali di amministratore di ONTAP e selezionare **Rivedi**.
3. Confermare i dettagli del back-end e selezionare **Manage** (Gestisci).

   Il backend viene visualizzato nell'elenco con le informazioni di riepilogo.

Aggiungere il backend di storage utilizzando l'opzione Backend

1. Nell'area di navigazione a sinistra, selezionare **Backend**.
2. Selezionare **Gestisci**.
3. Immettere le credenziali di amministratore di ONTAP e selezionare **Rivedi**.
4. Confermare i dettagli del back-end e selezionare **Manage** (Gestisci).

   Il backend viene visualizzato nell'elenco con le informazioni di riepilogo.

5. Per visualizzare i dettagli dello storage back-end, selezionarlo.

   Vengono visualizzati anche i volumi persistenti utilizzati dalle applicazioni nel cluster di calcolo gestito.

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, 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 tipo di provider bucket corretto con le credenziali corrette per tale provider. Ad esempio, l'interfaccia utente accetta NetApp ONTAP S3 come tipo con 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. Immettere il nome o l'indirizzo IP del server 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.

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 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

- Un cluster che esegue OpenShift 4.6 o 4.7, con Trident StorageClasses supportato da ONTAP 9.5 o versione successiva.
  - Uno o più nodi di lavoro con almeno 1 GB di RAM disponibile per l'esecuzione dei servizi di telemetria.

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

- Il superuser e l'ID utente impostati sul sistema ONTAP di backup per eseguire il backup e il ripristino delle applicazioni con il centro di controllo Astra (ACC). Eseguire i seguenti comandi nella riga di comando di ONTAP:
  `export policy rule modify -vserver svm0 -policyname default -ruleindex 1 -superuser sys`
  `export-policy rule modify -policyname default -ruleindex 1 -anon 65534` (valore predefinito)

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

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>
```

+

```
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. 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
```

3. 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".

4. Generare il kubeconfig come segue:

a. Creare un `create-kubeconfig.sh` file. Se l'indice del token annotato nel passaggio precedente non era 0, sostituire il valore per `TOKEN_INDEX` all'inizio del seguente script con il valore corretto.

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

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

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

CONTEXT=$(kubectl config current-context)

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

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

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

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

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

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

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

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

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

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

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

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

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

5. (**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 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

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

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.

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 verrà disinstallato quando rimuoverò un cluster Kubernetes da Astra Control?

Trident non verrà disinstallato da un cluster quando viene rimosso da Astra Control.

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.

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.

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 app implementate 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, 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

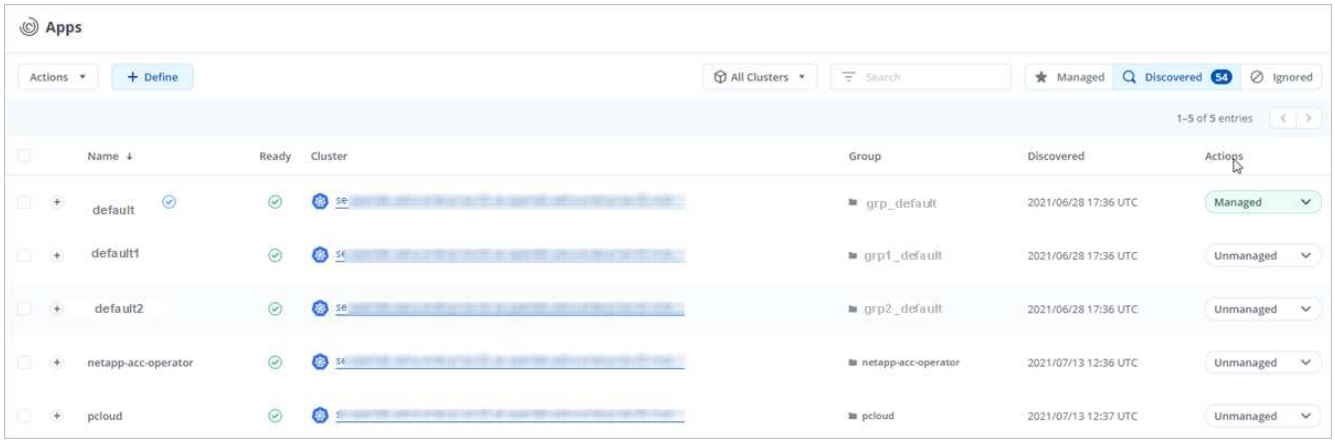
La sezione **scoperta** della pagina App mostra gli spazi dei nomi e le applicazioni installate da Helm o personalizzate in tali spazi dei nomi. Puoi scegliere di gestire ogni applicazione singolarmente o a livello di spazio dei nomi. Tutto questo si riduce al livello di granularità necessario per le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



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

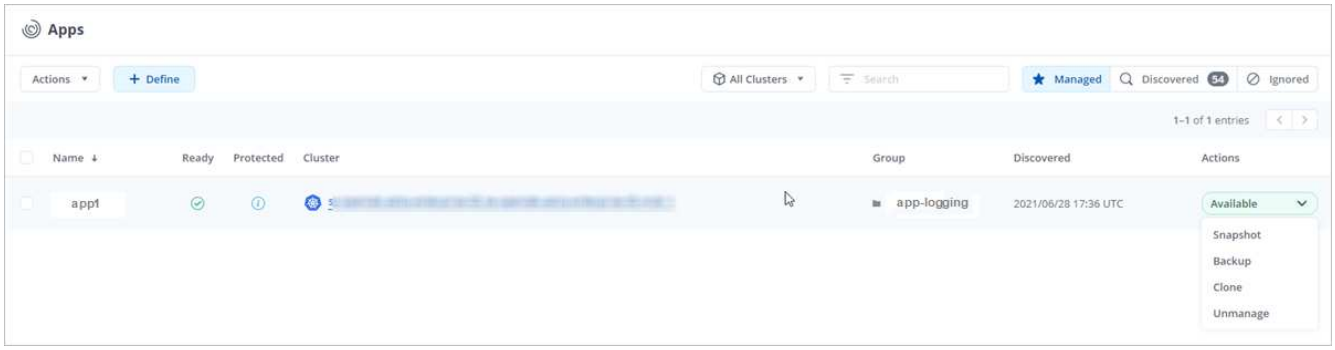
   Astra Control mostra le applicazioni Helm e le applicazioni con etichetta personalizzata nello spazio dei nomi. Se le etichette Helm sono disponibili, sono contrassegnate da un'icona di tag.

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 dal menu Actions (azioni), selezionare **Manage** (Gestisci).

7. Se non si desidera gestire un'applicazione, dal menu Actions (azioni) accanto all'applicazione, selezionare **Ignore** (Ignora).

   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.



   Notare che l'applicazione appena aggiunta presenta 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

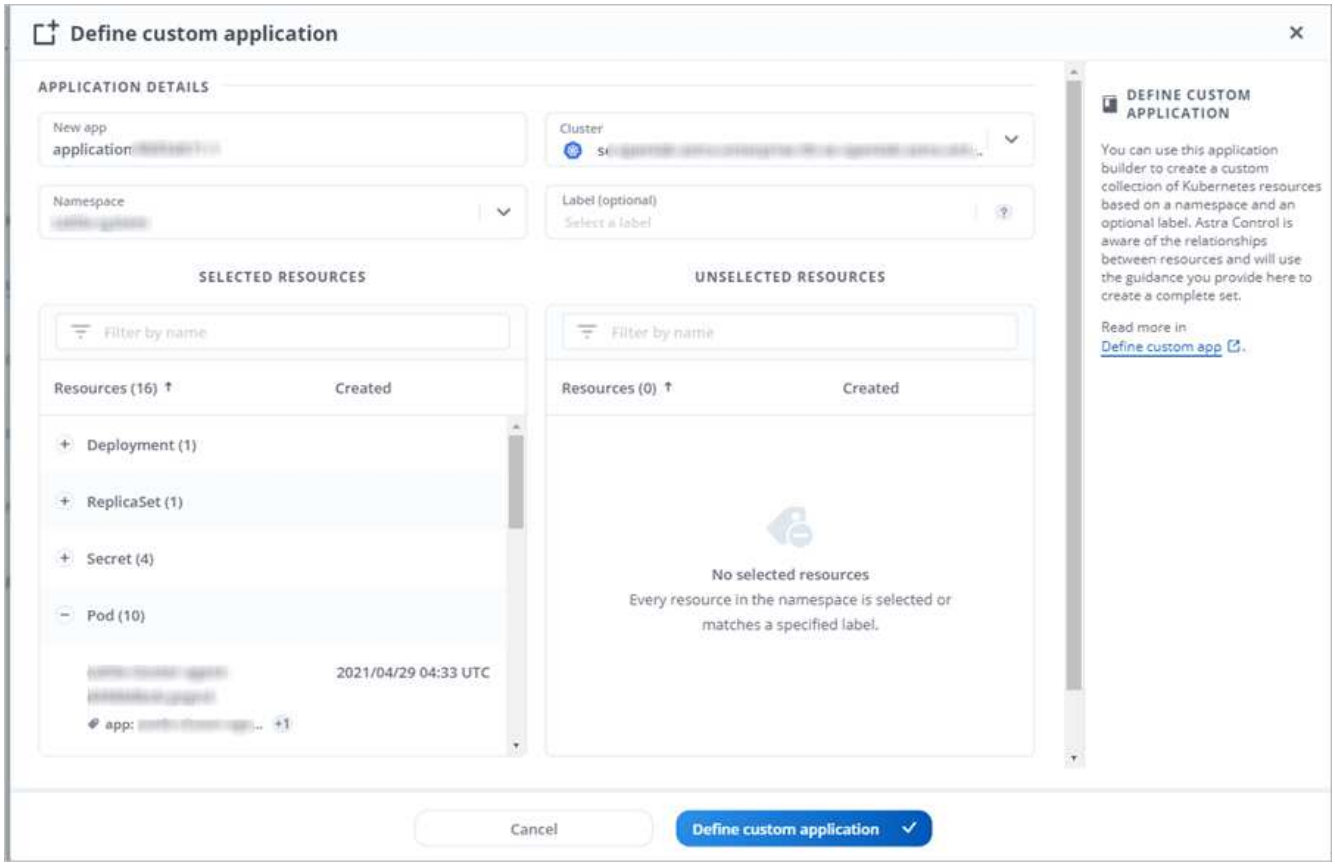
Le applicazioni che hai scelto di gestire sono ora disponibili nella scheda **Managed**. Tutte le applicazioni ignorate verranno spostate nella scheda **ignored**. Idealmente, la scheda scoperta non mostra alcuna applicazione, in modo che, una volta installate, siano più facili da trovare e gestire.

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 **Apps** (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 facendo clic sul 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. Fare clic su **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 **Apps** (applicazioni).
2. Selezionare **rilevato** come filtro.
3. Selezionare l'applicazione.
4. Dal menu Actions (azioni), selezionare **Ignore** (Ignora).
5. Per non ignorare, dal menu azioni, 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.

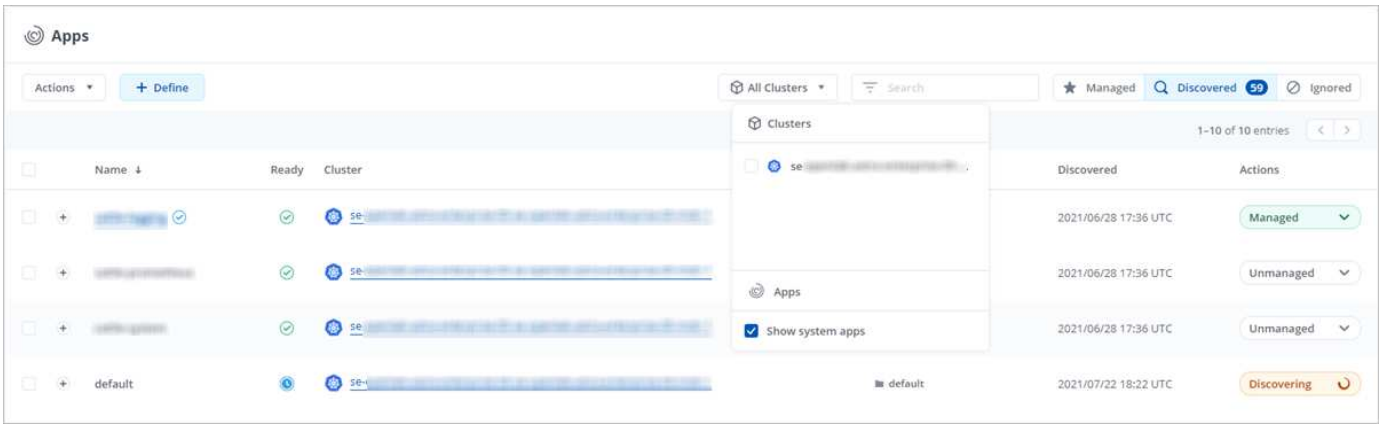
> Se si annulla la gestione di un'applicazione, i backup o le snapshot creati in precedenza andranno persi.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Apps** (applicazioni).
2. Selezionare **Managed** come filtro.
3. Selezionare l'applicazione.
4. Dal menu Actions (azioni), selezionare **UnManage** (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. È possibile visualizzare le applicazioni di sistema selezionando la casella di controllo **Mostra applicazioni di sistema** sotto il filtro cluster nella barra degli strumenti.



Per impostazione predefinita, queste applicazioni di sistema non vengono visualizzate perché è raro che sia necessario eseguirne il backup.

> 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".

Trova ulteriori informazioni

- "Utilizzare l'API 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.

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.

Per creare un'applicazione personalizzata, accedere alla pagina App e fare clic su **+ Definisci**.

Durante le selezioni, 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.

> 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.

Esempio: Policy di protezione separata per la release canary

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.

Fasi

1. Dopo che il team ha aggiunto il cluster ad Astra Control, il passaggio successivo consiste nella definizione di un'applicazione personalizzata. A tale scopo, il team fa clic sul pulsante **+ Definisci** nella pagina App.
2. Nella finestra a comparsa che viene visualizzata, il raggruppamento viene impostato `devops-canary-deployment` come nome dell'applicazione. Il team sceglie il cluster nell'elenco a discesa **Cluster**, quindi lo spazio dei nomi dell'applicazione dall'elenco a discesa **namespace**.
3. Il team può digitare entrambi i tipi `deployment=canary` Nel campo **etichette**, oppure selezionare l'etichetta dalle risorse elencate di seguito.
4. Dopo aver definito l'applicazione personalizzata per l'implementazione canary, il team ripete il processo per l'implementazione stabile.

Una volta terminata la creazione delle due applicazioni personalizzate, il team può trattare 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.

Proteggi le app

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" 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
```

Snapshot e backup

Una *snapshot* è una copia point-in-time di un'applicazione memorizzata sullo stesso volume fornito dell'applicazione. Di solito sono veloci. Gli snapshot locali vengono utilizzati 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. Un backup può essere più lento rispetto agli snapshot locali. È possibile migrare un'applicazione ripristinando il backup su un cluster diverso. È inoltre possibile scegliere un periodo di conservazione più lungo per i backup.

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.

Configurare un criterio di protezione

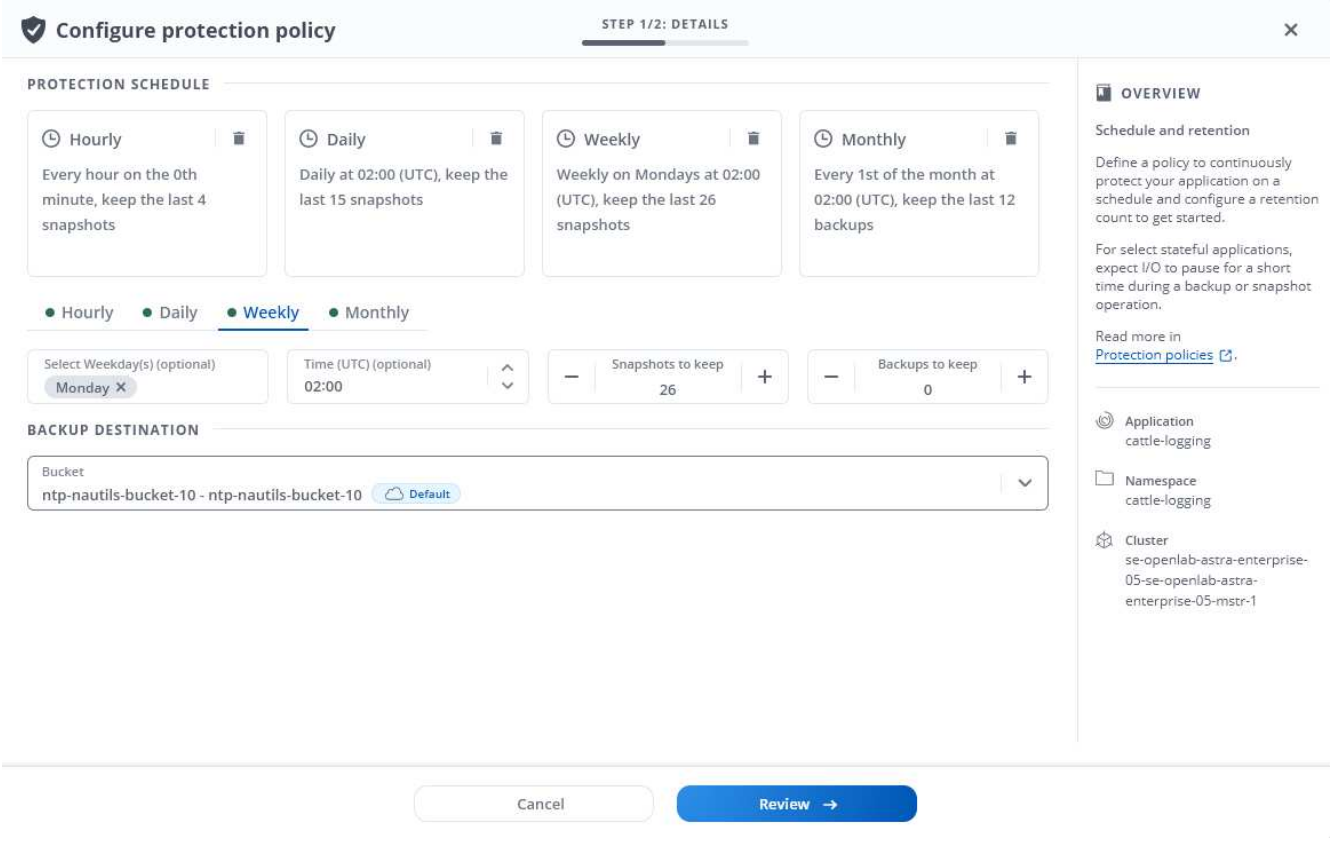
Una policy di protezione protegge un'applicazione creando snapshot, backup o entrambi in base a una pianificazione definita. È possibile scegliere di creare snapshot e backup ogni ora, ogni giorno, ogni settimana e ogni mese, nonché specificare il numero di copie da conservare.

Fasi

1. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection** (protezione dati).
3. Fare clic su **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. Fare clic su **Review** (Rivedi).
6. Fare clic su **Set Protection Policy (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. Fare clic su **Apps** (applicazioni).
2. Fare clic sull'elenco a discesa nella colonna **azioni** dell'applicazione desiderata.
3. Fare clic su **Snapshot**.
4. Personalizzare il nome dell'istantanea, quindi fare clic su **Review** (Rivedi).
5. Esaminare il riepilogo dell'istantanea e fare clic su **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. Fare clic su **Apps** (applicazioni).
2. Fare clic sull'elenco a discesa nella colonna **azioni** dell'applicazione desiderata.
3. Fare clic su **Backup**.
4. Personalizzare il nome del backup.
5. 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.
6. Scegliere una destinazione per il backup selezionandola dall'elenco dei bucket di storage.
7. Fare clic su **Review** (Rivedi).
8. Esaminare il riepilogo del backup e fare clic su **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 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. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection** (protezione dati).

   Le istantanee vengono visualizzate per impostazione predefinita.

3. Fare clic su **Backup** per visualizzare l'elenco dei backup.

Eliminare le istantanee

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

Fasi

1. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection** (protezione dati).
3. Fare clic sull'elenco a discesa nella colonna **Actions** per l'istantanea desiderata.
4. Fare clic su **Delete snapshot** (Elimina snapshot).
5. Digitare la parola "DELETE" per confermare l'eliminazione, quindi fare clic su **Yes, Delete snapshot** (Sì, Elimina 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 Astra".

1. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection** (protezione dati).
3. Fare clic su **Backup**.
4. Fare clic sull'elenco a discesa nella colonna **Actions** per il backup desiderato.
5. Fare clic su **Delete backup** (Elimina backup).
6. Digitare la parola "DELETE" per confermare l'eliminazione, quindi fare clic su **Yes, Delete backup**.

Risultato

Astra Control Center elimina il backup.

Ripristinare le applicazioni

Astra Control Center può ripristinare l'applicazione da uno snapshot o da un backup. I backup e le snapshot persistenti dello storage vengono trasferiti dall'archivio a oggetti, pertanto il ripristino da uno snapshot esistente allo stesso cluster sarà più rapido rispetto ad altri metodi. È possibile utilizzare l'interfaccia utente Astra o. "L'API Astra" per ripristinare 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.

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.

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. Fare clic su **Apps** (applicazioni), quindi sul nome di un'applicazione.
2. Fare clic su **Data Protection**.
3. Se si desidera eseguire il ripristino da uno snapshot, tenere selezionata l'icona **Snapshot**. In caso contrario, fare clic sull'icona **Backup** per eseguire il ripristino da un backup.
4. Fare clic sull'elenco a discesa nella colonna **azioni** per lo snapshot o il backup da cui si desidera eseguire il ripristino.
5. Fare clic su **Ripristina applicazione**.
6. **Dettagli ripristino**: Specificare i dettagli per il ripristino:
   - Immettere un nome e uno spazio dei nomi per l'applicazione.

     Se stai ripristinando un'applicazione che è stata eliminata, scegli un nome e uno spazio dei nomi diversi per l'applicazione rispetto al nome originale. Se il nome dell'applicazione ripristinata è uguale a quello dell'applicazione eliminata, l'operazione di ripristino non riesce.

   - Scegliere il cluster di destinazione per l'applicazione.
   - Fare clic su **Review** (Rivedi).
7. **Restore Summary** (Riepilogo ripristino): Esaminare i dettagli relativi all'azione di ripristino e fare clic su **Restore** (Ripristina).

Risultato

Astra Control Center ripristina l'applicazione in base alle informazioni fornite.

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.

Clonare e migrare le applicazioni

Clonare un'applicazione esistente per creare un'applicazione duplicata sullo stesso cluster Kubernetes o su un altro cluster. 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" per clonare e migrare le applicazioni.

> 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 Astra Control Center clona un'applicazione, crea un clone della configurazione dell'applicazione e dello storage persistente.

> 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.

> 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
> ```

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.

Fasi

1. Fare clic su **Apps** (applicazioni).
2. Effettuare una delle seguenti operazioni:
   - Fare clic sull'elenco a discesa nella colonna **azioni** dell'applicazione desiderata.
   - Fare clic sul nome dell'applicazione desiderata e selezionare l'elenco a discesa Status (Stato) nella parte superiore destra della pagina.
3. Fare clic su **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. Fare clic su **Review** (Rivedi).
7. **Clone Summary**: Leggi i dettagli sul clone e fai clic su **Clone**.

Risultato

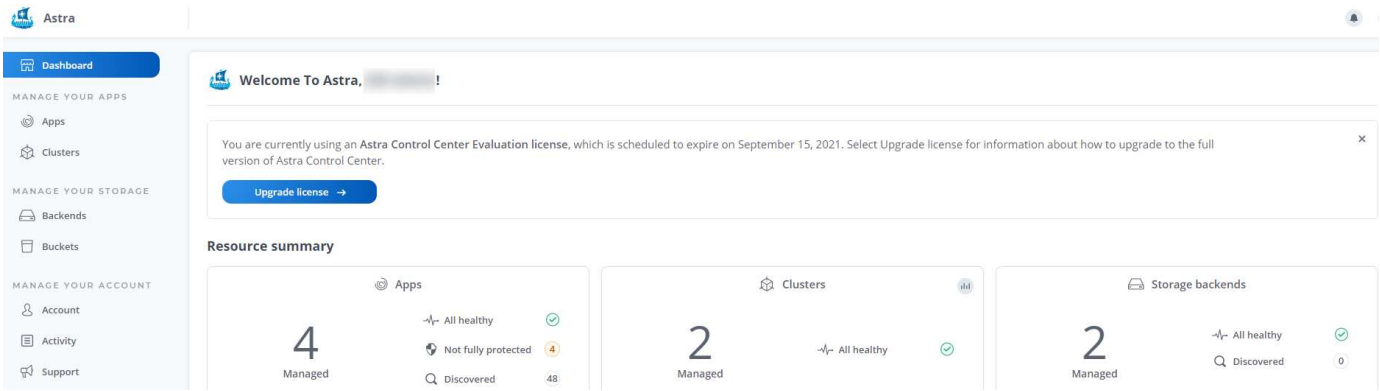
Astra Control Center clona l'applicazione in base alle informazioni fornite. L'operazione di clonazione viene eseguita correttamente quando il nuovo clone dell'applicazione si trova in `Available` nella pagina **Apps**.

> 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 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 è possibile eseguire il drill-down da ciascuno di questi. 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.

Riquadro Apps (applicazioni)

Il riquadro **Apps** 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.
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 **Apps**, quindi selezionare il nome di un'applicazione.
2. Fai clic per trovare 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 **Apps** sotto **Resource summary**, è possibile selezionare le applicazioni gestite, che consentono di accedere alla pagina **Apps**. Una volta visualizzata la pagina **Apps**, seguire i passaggi descritti in precedenza.

Gestisci il tuo account

Gestire gli utenti

È possibile aggiungere, rimuovere e modificare gli utenti dell'installazione di Astra Control Center utilizzando l'interfaccia utente di Astra Control Center. È possibile utilizzare l'interfaccia utente Astra o. "L'API Astra" per gestire gli utenti.

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**, fare clic su **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 di ruolo Viewer e può gestire app e cluster, ma non può annullare la gestione di app o cluster o eliminare snapshot o 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. Fare clic su **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. Fare clic sull'icona User (utente) nella parte superiore destra della schermata.
2. Selezionare **Profilo**.
3. Fare clic sull'elenco a discesa **azioni** e selezionare **Modifica password**.
4. Immettere una password conforme ai requisiti.
5. Immettere nuovamente la password per confermare.
6. Fare clic su **Change password** (Modifica 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**, fare clic su **account**.
2. Nella scheda **utenti**, selezionare l'elenco a discesa nella colonna **Stato** dell'utente.
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. Fare clic su **Reset password** (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**, fare clic su **account**.
2. Nella scheda **utenti**, selezionare l'elenco a discesa nella colonna **ruolo** dell'utente.
3. Selezionare un nuovo ruolo, quindi fare clic su **Cambia ruolo** quando richiesto.

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**, fare clic su **account**.
2. Nella scheda **utenti**, selezionare la casella di controllo nella riga di ciascun utente che si desidera rimuovere.
3. Fare clic su **azioni** e selezionare **Rimuovi utenti**.
4. Quando richiesto, confermare l'eliminazione digitando la parola "remove" (Rimuovi), quindi fare clic su **Yes, Remove User** (Sì, Rimuovi utente).

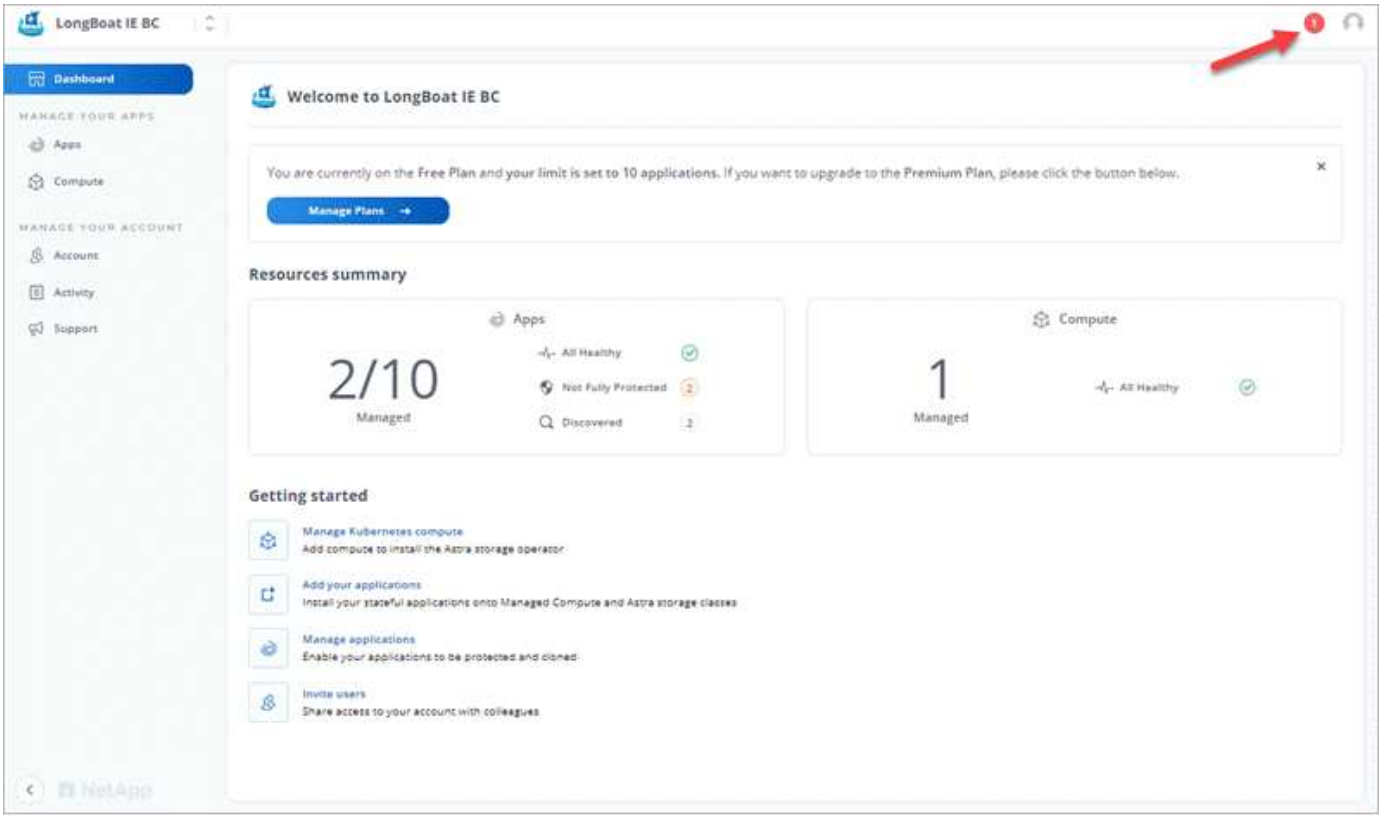
Risultato

Astra Control Center rimuove l'utente dall'account.

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.

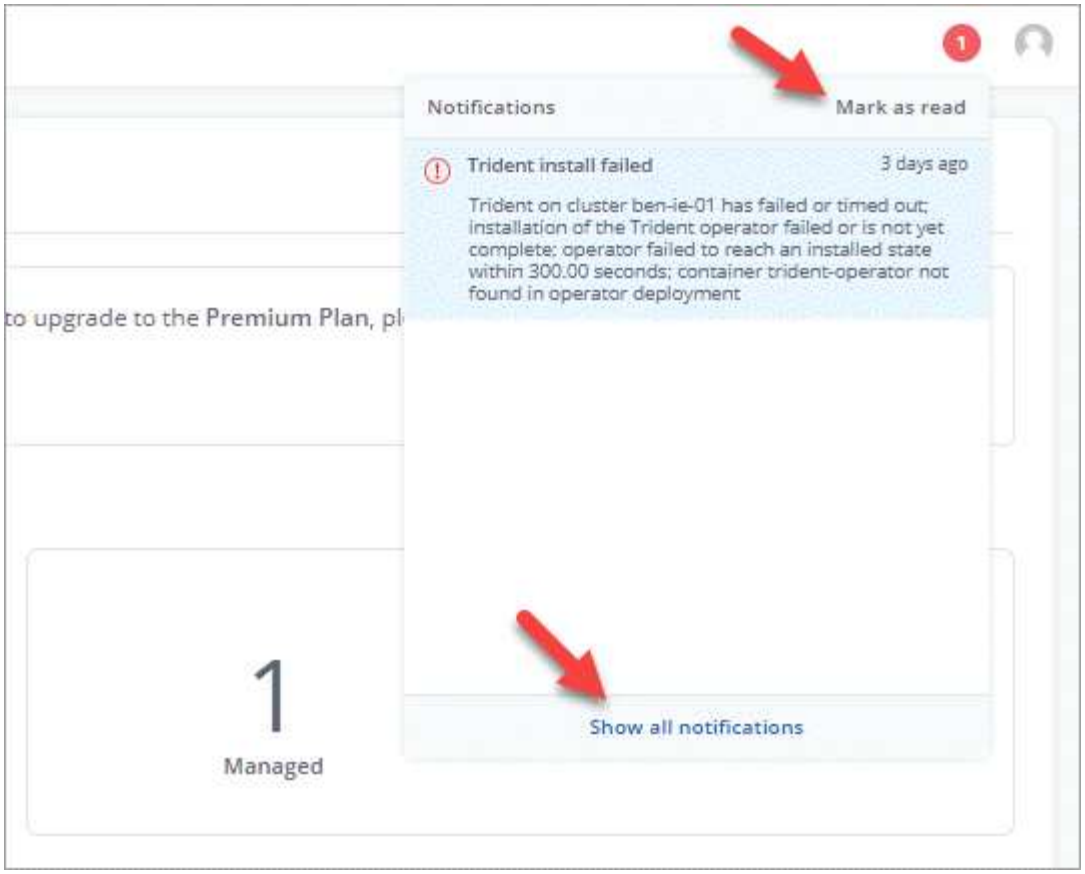
Il numero di notifiche non lette è disponibile nella parte superiore destra dell'interfaccia:



Puoi visualizzare queste notifiche e contrassegnarle come lette (questa operazione può risultare utile se desideri cancellare le notifiche non lette come noi).

Fasi

1. Fare clic sul numero di notifiche non lette in alto a destra.



2. Esaminare le notifiche, quindi fare clic su **Contrassegna come letto** o su **Mostra tutte le notifiche**.

   Se si fa clic su **Mostra tutte le notifiche**, viene caricata la pagina Notifiche.

3. Nella pagina **Notifiche**, visualizzare le notifiche, selezionare quelle che si desidera contrassegnare come lette, fare clic su **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.

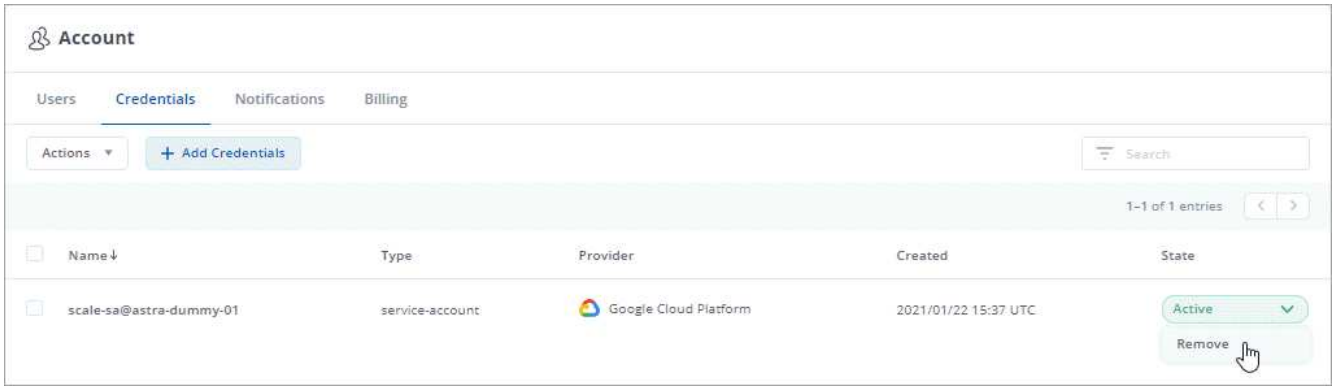
Rimuovere le credenziali

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. Fare clic su **account > Credentials**.
2. Fare clic sull'elenco a discesa nella colonna **Stato** per le credenziali che si desidera rimuovere.
3. Fare clic su **Rimuovi**.



4. Digitare la parola "remove" per confermare l'eliminazione, quindi fare clic su **Yes, Remove Credential** (Sì, Rimuovi credenziale).

Risultato

Astra Control Center rimuove le credenziali dall'account.

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" per aggiornare una licenza esistente.

Fasi

1. Accedere al 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**, fare clic sul 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.

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.

Utilizzare uno dei seguenti provider 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.

Non è possibile eliminare un bucket, tuttavia è possibile modificarlo.

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, vedere "Astra Automation e informazioni API".

È possibile eseguire queste attività relative alla gestione dei bucket:

- "Aggiungi un bucket"
- Modificare un bucket

> 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.

Rimuovere le credenziali

Rimuovere le credenziali S3 da un account in qualsiasi momento utilizzando l'API Astra Control.

Per ulteriori informazioni, vedere "Utilizzare l'API di controllo Astra".

> 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. Si consiglia di non rimuovere queste credenziali.

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 tipo di provider bucket corretto con le credenziali corrette per tale provider. Ad esempio, l'interfaccia utente accetta NetApp ONTAP S3 come tipo con 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 Actions (azioni), selezionare **Edit** (Modifica).
3. Modificare qualsiasi informazione diversa dal tipo di bucket.

   > Impossibile modificare il tipo di bucket.

4. Selezionare **Aggiorna**.

Trova ulteriori informazioni

- "Utilizzare l'API 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, 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

Visualizza i dettagli del back-end dello storage

È possibile visualizzare le informazioni di back-end dello storage dalla dashboard o dall'opzione Backend.

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

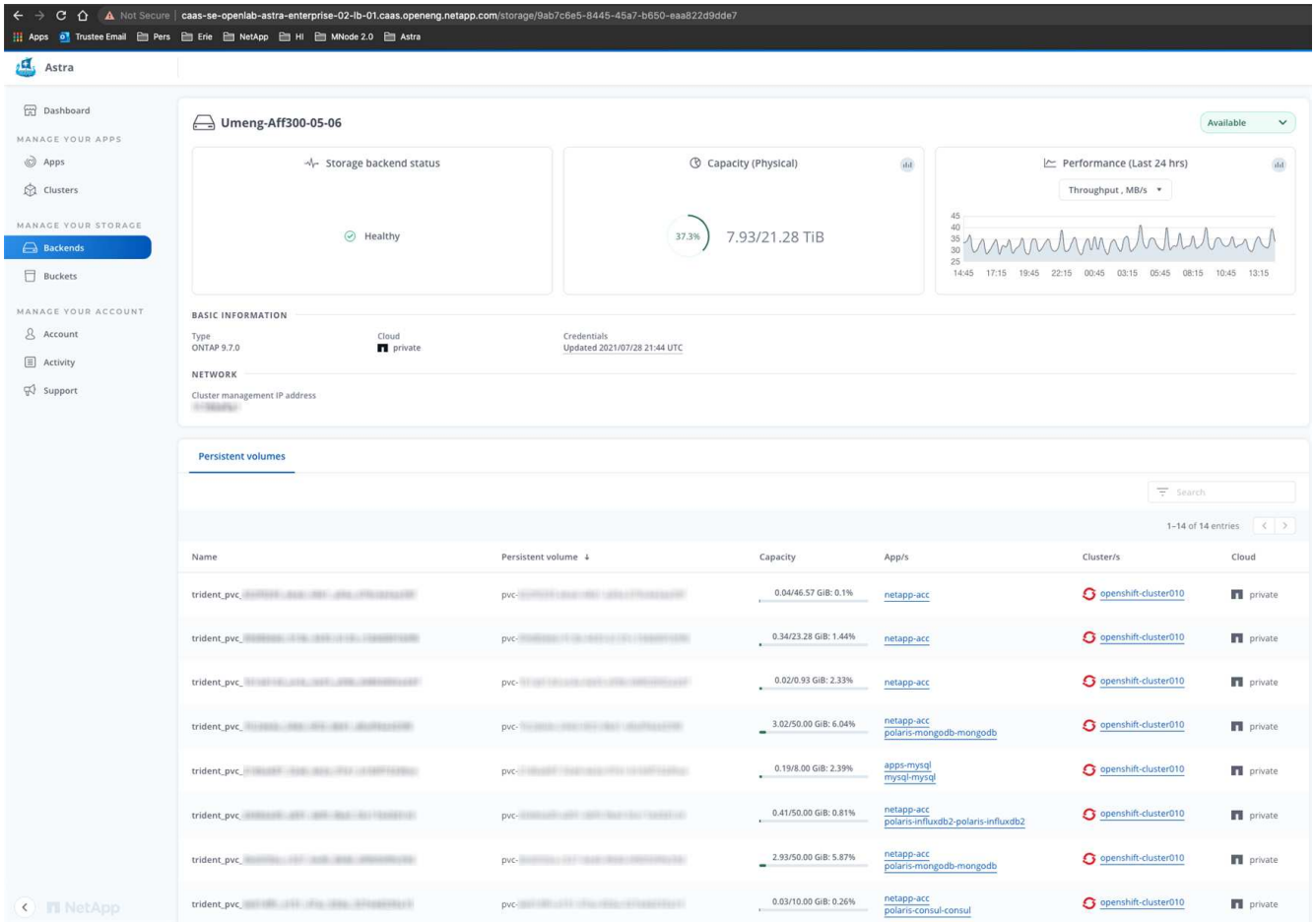
Visualizza informazioni sullo stato, la capacità e le performance del back-end (throughput IOPS e/o latenza).

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, fare clic sull'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 lo storage back-end.
3. Dal menu Actions (azioni), selezionare **UnManage** (Annulla gestione).
4. Digitare "unManage" per confermare la rimozione.
5. Selezionare **Sì, rimuovere il backend di storage**.

Trova ulteriori informazioni

- "Utilizzare l'API 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.

> 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 puoi collegarti a Cloud Insights da qui.

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.

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 "qui".

Fasi

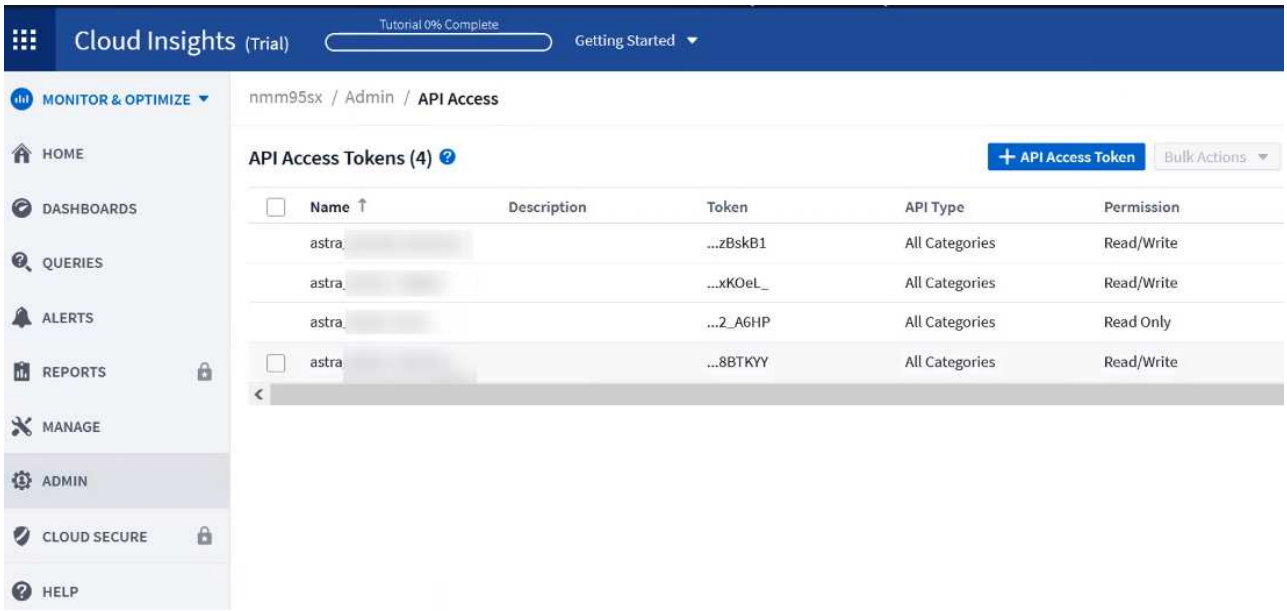
1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Connect** dove nell'elenco a discesa viene visualizzato **disconnected** per aggiungere la connessione.

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 API di tipo **sola lettura**.



c. Copiare la chiave **sola lettura**. Per attivare la connessione Cloud Insights, è necessario incollarla nella finestra di Astra Control Center.

d. In Cloud Insights, generare un token API di tipo **lettura/scrittura**.

e. Copiare la chiave **Read/Write**. È necessario incollarlo nella finestra di dialogo di Astra Control Center **Connect Cloud Insights**.

> 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.

f. Incollare le chiavi copiate da Cloud Insights in Astra Control Center.

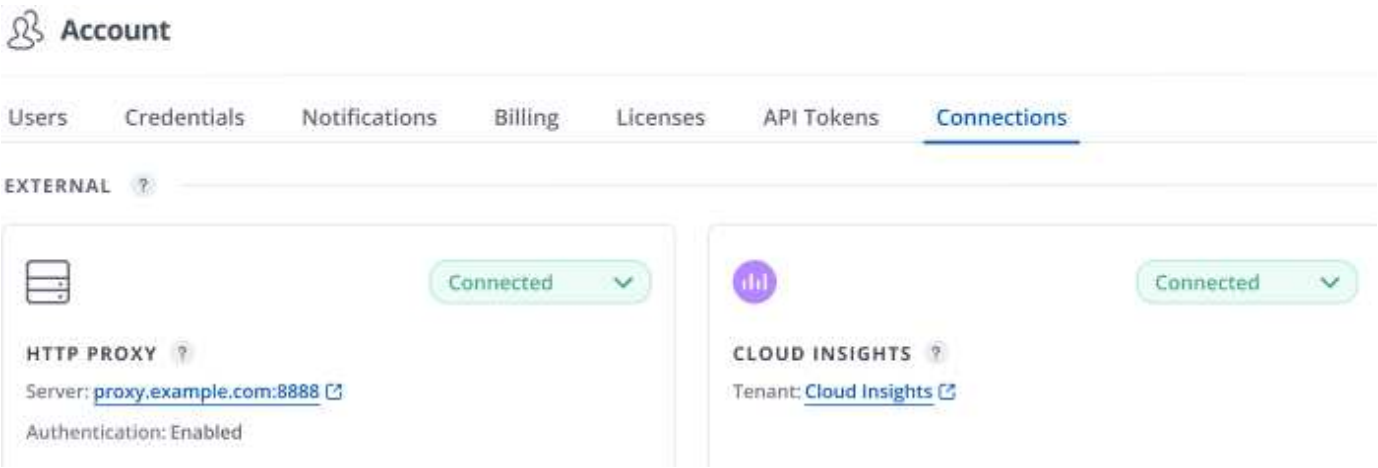
5. Selezionare **Connect**.

> 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.

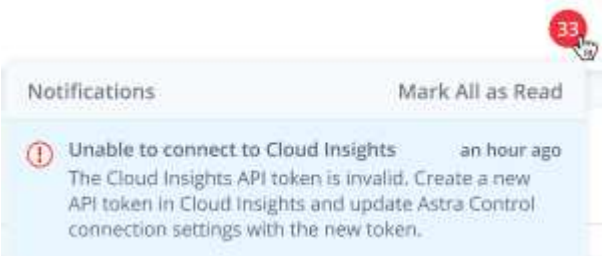
> Per passare facilmente da un'unità di controllo Astra a un'interfaccia utente Cloud Insights e viceversa, assicurarsi di aver effettuato l'accesso a entrambe.

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.

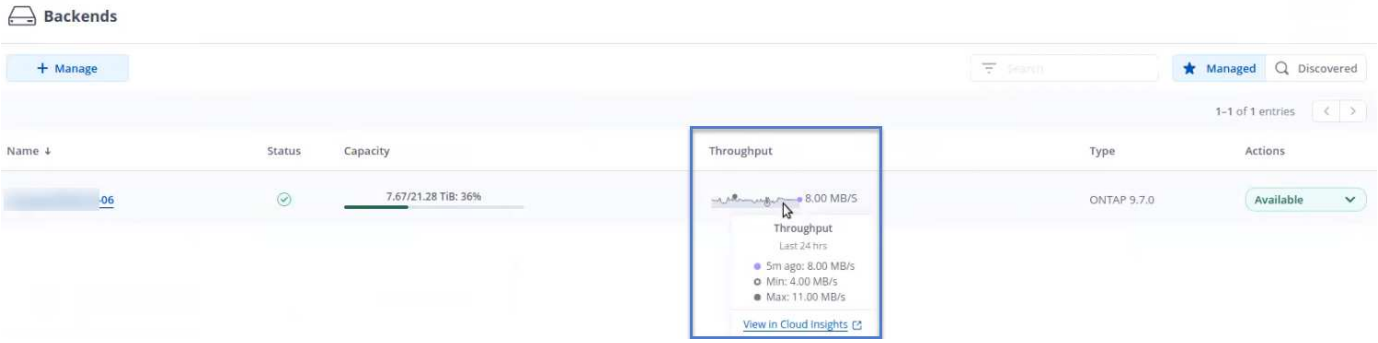


Se la connessione non è riuscita per qualche motivo, lo stato visualizza **Failed** (non riuscito). Il motivo del guasto è disponibile in **Notifiche** nella parte superiore destra dell'interfaccia utente.



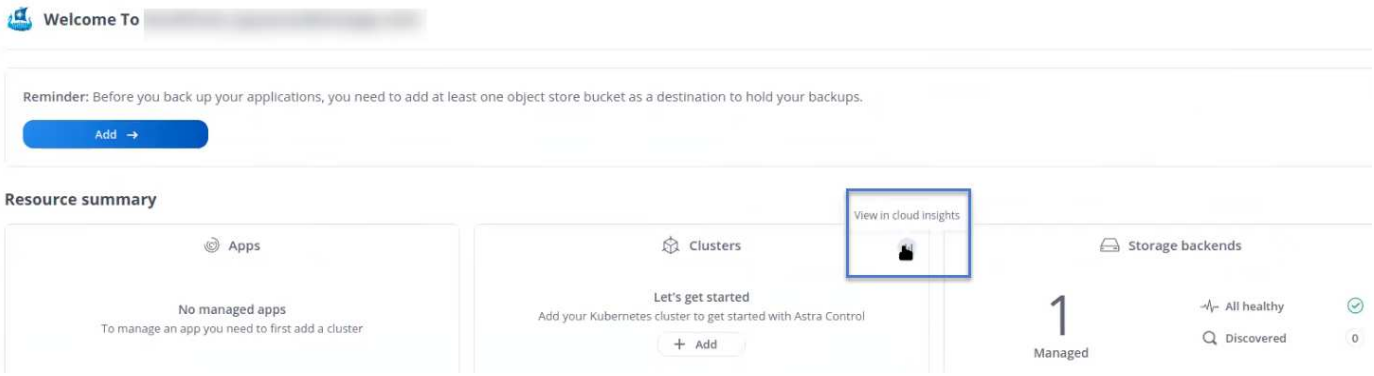
Le stesse informazioni sono disponibili anche in **account** > **Notifiche**.

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

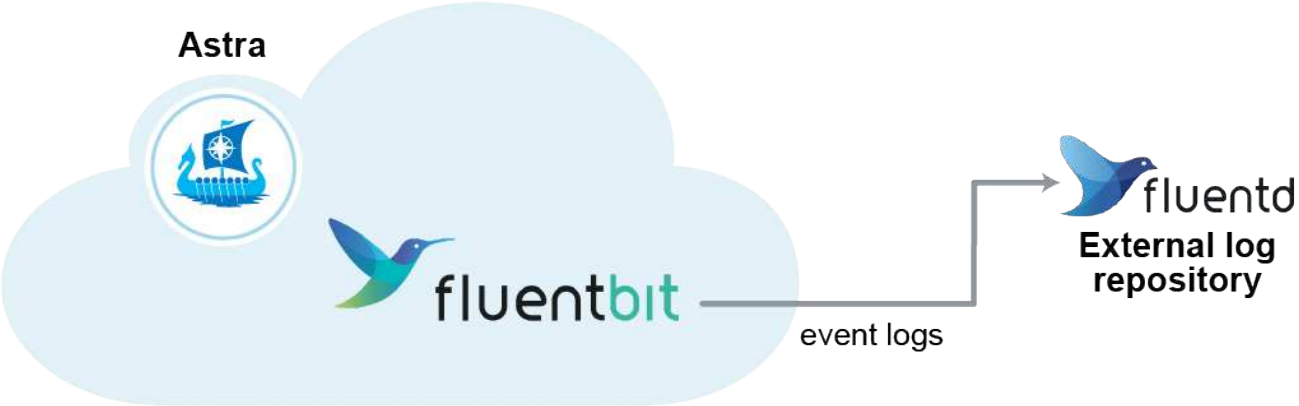
È possibile disattivare la connessione Cloud Insights per un cluster Kubernetes gestito da Astra Control Center. La disattivazione della connessione Cloud Insights non elimina i dati di telemetria già caricati su Cloud Insights.

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.

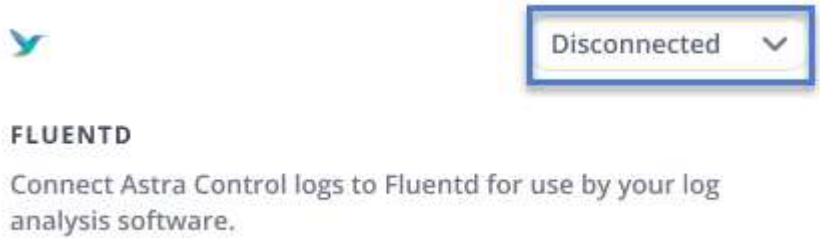
Di cosa hai bisogno

- 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.

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" per aggiornare una licenza esistente.

Fasi

1. Accedere al 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**, fare clic sul 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.

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 **Apps** (applicazioni).
2. Seleziona la casella di controllo delle applicazioni che non vuoi 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 **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.

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.

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
```

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 Center".

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> --namespace <namespace> --create-namespace --set
persistence.storageClass=<storage_class>
```

> 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 Center".

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> --namespace <namespace> --create-namespace --set
persistence.storageClass=<storage_class>
```

> 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 Center".

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> --namespace <namespace> --create-namespace --set
   persistence.storageClass=<storage_class>
   ```

   > 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 Center".

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> --namespace <namespace> --create-namespace --set
   persistence.storageClass=<storage_class>
   ```

> 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

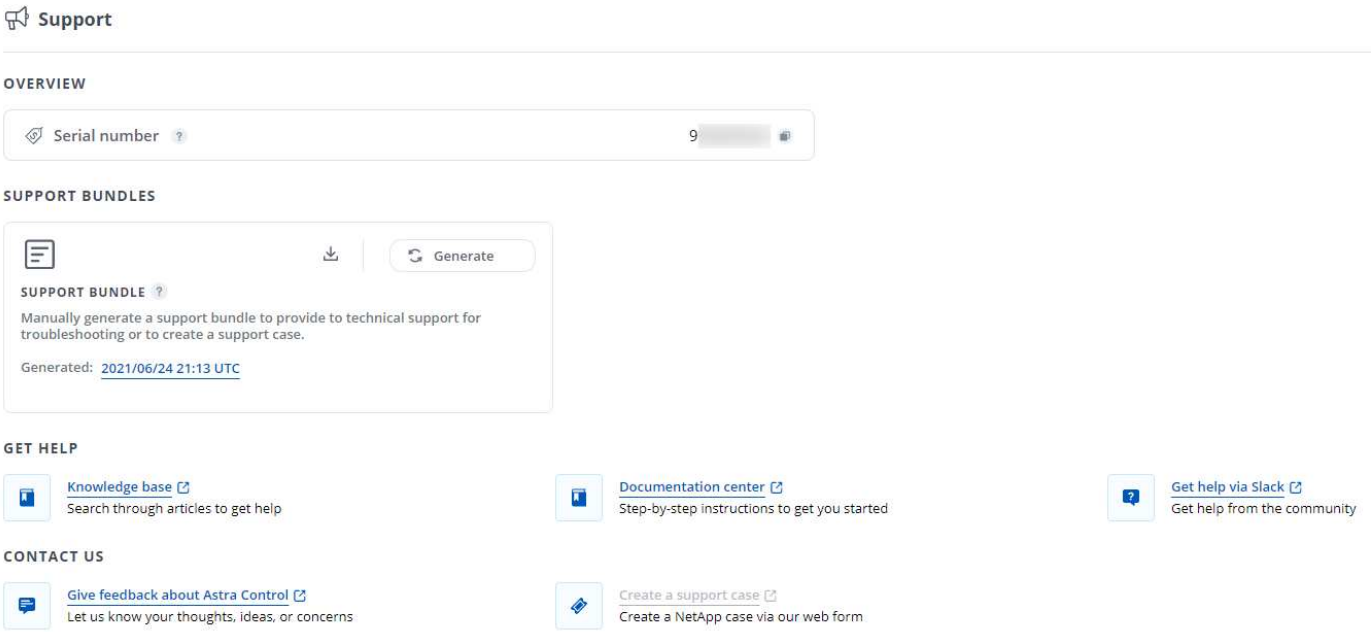
Richiedi assistenza

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.

È possibile accedere alle opzioni di supporto dall'interfaccia utente di Astra Control Center selezionando la scheda **Support** (supporto) dal menu principale.



Opzioni di supporto automatico

Queste opzioni sono disponibili gratuitamente 24 ore su 24, 7 giorni su 7:

- "Knowledge base (accesso richiesto)"

  Cerca articoli, FAQ o informazioni sulla riparazione in caso di interruzione relative ad Astra Control.

- Documentazione

  Questo è il sito doc attualmente visualizzato.

- "Lasco"

  Accedi al canale Containers nello spazio di lavoro Pub per entrare in contatto con colleghi ed esperti.

- Generare pacchetti di supporto da fornire al supporto NetApp per la risoluzione dei problemi
- Email di feedback

  Invia un'e-mail all'indirizzo 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 sul 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 necessaria una connessione proxy per caricare i 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**.

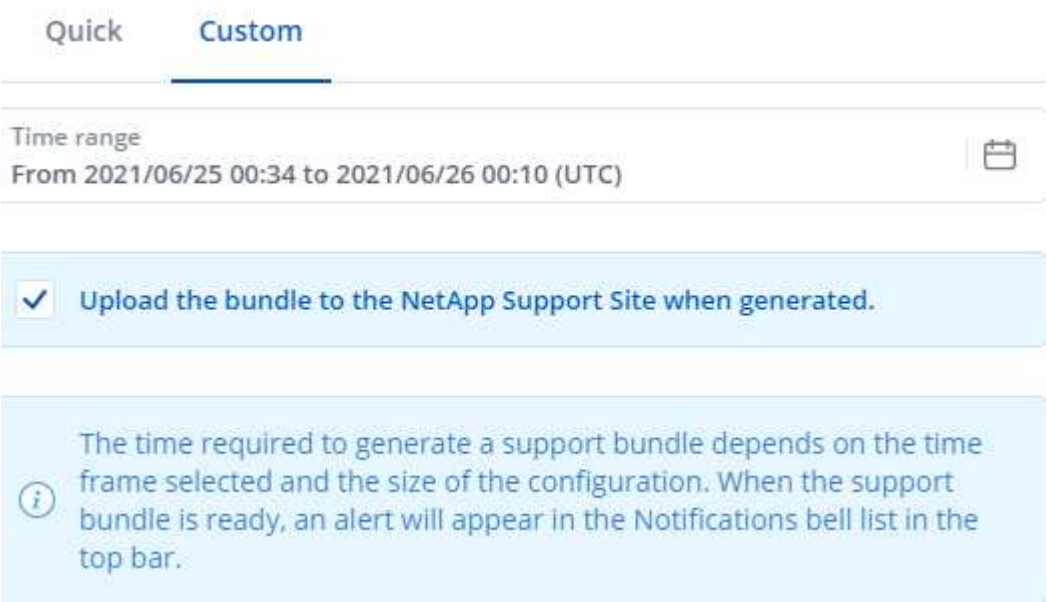
   b. Nella finestra **generate a Support Bundle** (genera un pacchetto di supporto), selezionare il periodo di tempo.

      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. Controllare la sezione **caricare il bundle sul sito di supporto NetApp quando viene generato**.



e. Selezionare **generate Bundle** (genera bundle).

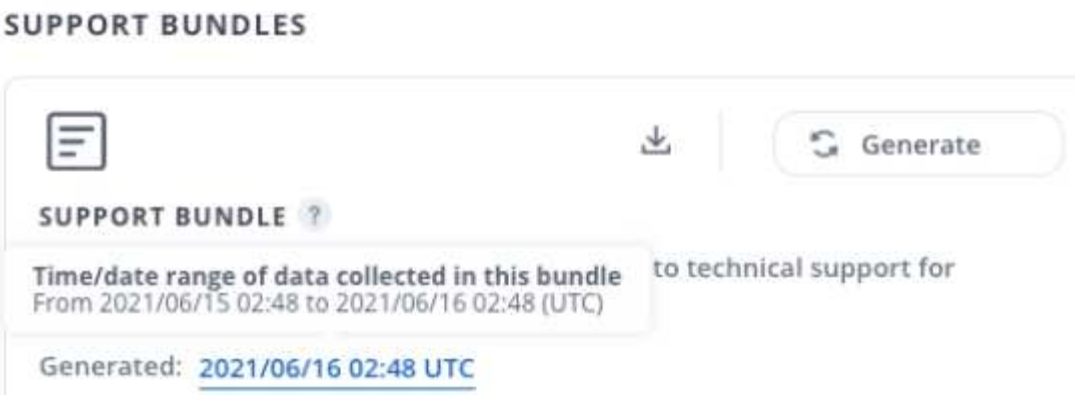
   Quando il bundle di supporto è pronto, viene visualizzata una notifica nella pagina **account** > **notifica** nell'area Avvisi, nella pagina **attività** e nell'elenco delle notifiche (accessibile selezionando l'icona nella parte superiore destra dell'interfaccia utente).

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, viene visualizzato accanto a **generated** nella sezione **Support Bundle** della pagina **Support**, come mostrato:



1. Selezionare l'icona **Download** per scaricare il bundle 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.
   - Utilizzare NetApp AIQ.

Trova ulteriori informazioni

- "Come caricare un file su NetApp (accesso richiesto)"
- "Come caricare manualmente un file su NetApp (accesso richiesto)"

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 la release Astra Control Center 21.08"

Licenza API Astra Control

https://docs.netapp.com/us-en/astra-automation-2108/media/astra-api-license.pdf