



## **Concetti**

### **Astra Control Center**

NetApp  
November 21, 2023

# Sommario

- Concetti ..... 1
  - Scopri di più su Astra Control ..... 1
  - Architettura e componenti ..... 4
  - Protezione dei dati ..... 5
  - Licensing ..... 8
  - Comprendere la gestione delle app ..... 9
  - Classi di storage e dimensioni del volume persistente ..... 10
  - Ruoli e spazi dei nomi degli utenti ..... 11

# Concetti

## Scopri di più su Astra Control

Astra Control è una soluzione per la gestione del ciclo di vita dei dati delle applicazioni Kubernetes che semplifica le operazioni per le applicazioni stateful. Proteggi, esegui il backup, replica 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
- Replica dell'applicazione su un sistema remoto utilizzando la tecnologia NetApp SnapMirror
- 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

### Modelli di implementazione

Astra Control è disponibile in due modelli di implementazione:

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

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

	Servizio di controllo Astra	Centro di controllo Astra
<b>Che cos'è il supporto back-end dello storage?</b>	Offerte di servizi cloud NetApp	<ul style="list-style-type: none"> <li>• Sistemi NetApp ONTAP AFF e FAS</li> <li>• Astra Data Store come back-end dello storage</li> <li>• Back-end dello storage Cloud Volumes ONTAP</li> </ul>

## Come funziona Astra Control Service

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

Ad alto livello, Astra Control Service funziona come segue:

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

In Azure, Astra Control Service crea anche un gruppo di risorse, un account di storage e chiavi per il container Blob.

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

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

## Come funziona Astra Control Center

Astra Control Center viene eseguito localmente nel tuo cloud privato.

Astra Control Center supporta i cluster Kubernetes con:

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

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

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

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

Per installare e utilizzare Astra Control Center, è necessario soddisfare determinati requisiti ["requisiti"](#).

Ad alto livello, Astra Control Center funziona come segue:

- Astra Control Center viene installato nel proprio ambiente locale. Scopri di più su come ["Installare Astra Control Center"](#).
- È possibile completare alcune attività di configurazione, come ad esempio:
  - Impostare la licenza.
  - Aggiungere il primo cluster.
  - Aggiungere il backend di storage rilevato quando si aggiunge il cluster.
  - Aggiungere 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:

- Rileva i dettagli del cluster, inclusi gli spazi dei nomi, e consente di definire e proteggere le applicazioni.
- Rileva la configurazione di Astra Trident o Astra Data Store sui cluster che si sceglie di gestire e consente di monitorare i backend dello storage.

È possibile aggiungere applicazioni al cluster. In alternativa, se nel cluster gestito sono già presenti alcune applicazioni, è possibile utilizzare Astra Control Center per gestirle. Quindi, utilizza Astra Control Center per creare snapshot, backup, cloni e relazioni di replica.

## Per ulteriori informazioni

- ["Documentazione del servizio Astra Control"](#)
- ["Documentazione di Astra Control Center"](#)
- ["Documentazione di Astra Data Store"](#)



storage per i cluster GKE

- ["Azure NetApp Files"](#) O Azure Managed Disks come backend di storage per i cluster AKS.
- ["Amazon Elastic Block Store \(EBS\)"](#) oppure ["Amazon FSX per NetApp ONTAP"](#) Come opzioni di storage back-end per i cluster EKS.

◦ Astra Control Center utilizza i seguenti 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 Volumes ONTAP

- **Cloud Insights:** Uno strumento di monitoraggio dell'infrastruttura cloud NetApp, Cloud Insights consente di monitorare le performance e l'utilizzo dei cluster Kubernetes gestiti dal centro di controllo Astra. Cloud Insights mette in relazione l'utilizzo dello storage con i carichi di lavoro. Quando si attiva la connessione Cloud Insights in Astra Control Center, le informazioni di telemetria vengono visualizzate nelle pagine dell'interfaccia utente di Astra Control Center.

## Interfacce di controllo Astra

È possibile completare le attività utilizzando diverse interfacce:

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

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

## Per ulteriori informazioni

- ["Documentazione del servizio Astra Control"](#)
- ["Documentazione di Astra Control Center"](#)
- ["Documentazione di Astra Trident"](#)
- ["Utilizzare l'API di controllo Astra"](#)
- ["Documentazione Cloud Insights"](#)
- ["Documentazione ONTAP"](#)

## Protezione dei dati

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

### Snapshot, backup e policy di protezione

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

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

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



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

## Cloni

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

## Replica su un cluster remoto

Grazie ad Astra Control, puoi creare business continuity per le tue applicazioni con un RPO (Recovery Point Objective) basso e un RTO basso (Recovery Time Objective) utilizzando le funzionalità di replica asincrona della tecnologia NetApp SnapMirror. Una volta configurata, questa opzione consente alle applicazioni di replicare le modifiche dei dati e delle applicazioni da un cluster all'altro.

Astra Control replica in modo asincrono le copie Snapshot dell'applicazione su un cluster remoto. Il processo di replica include i dati nei volumi persistenti replicati da SnapMirror e i metadati dell'applicazione protetti da Astra Control.

La replica dell'app è diversa dal backup e ripristino dell'app nei seguenti modi:

- **Replica dell'applicazione:** Astra Control richiede la disponibilità e la gestione dei cluster Kubernetes di origine e di destinazione con i rispettivi backend di storage ONTAP configurati per abilitare NetApp SnapMirror. Astra Control porta Snapshot, l'applicazione basata su policy, e la replica nel cluster remoto. La tecnologia NetApp SnapMirror viene utilizzata per replicare i dati del volume persistente. Per eseguire il failover, Astra Control può portare online l'applicazione replicata ricreando gli oggetti dell'applicazione sul cluster Kubernetes di destinazione con i volumi replicati sul cluster ONTAP di destinazione. Poiché i dati del volume persistente sono già presenti nel cluster ONTAP di destinazione, Astra Control può offrire tempi di ripristino rapidi per il failover.
- **Backup e ripristino dell'applicazione:** Durante il backup delle applicazioni, Astra Control crea un'istantanea dei dati dell'applicazione e li memorizza in un bucket di storage a oggetti. Quando è necessario un ripristino, i dati nel bucket devono essere copiati in un volume persistente sul cluster ONTAP. L'operazione di backup/ripristino non richiede la disponibilità e la gestione del cluster Kubernetes/ONTAP secondario, ma la copia dei dati aggiuntiva può comportare tempi di ripristino più lunghi.

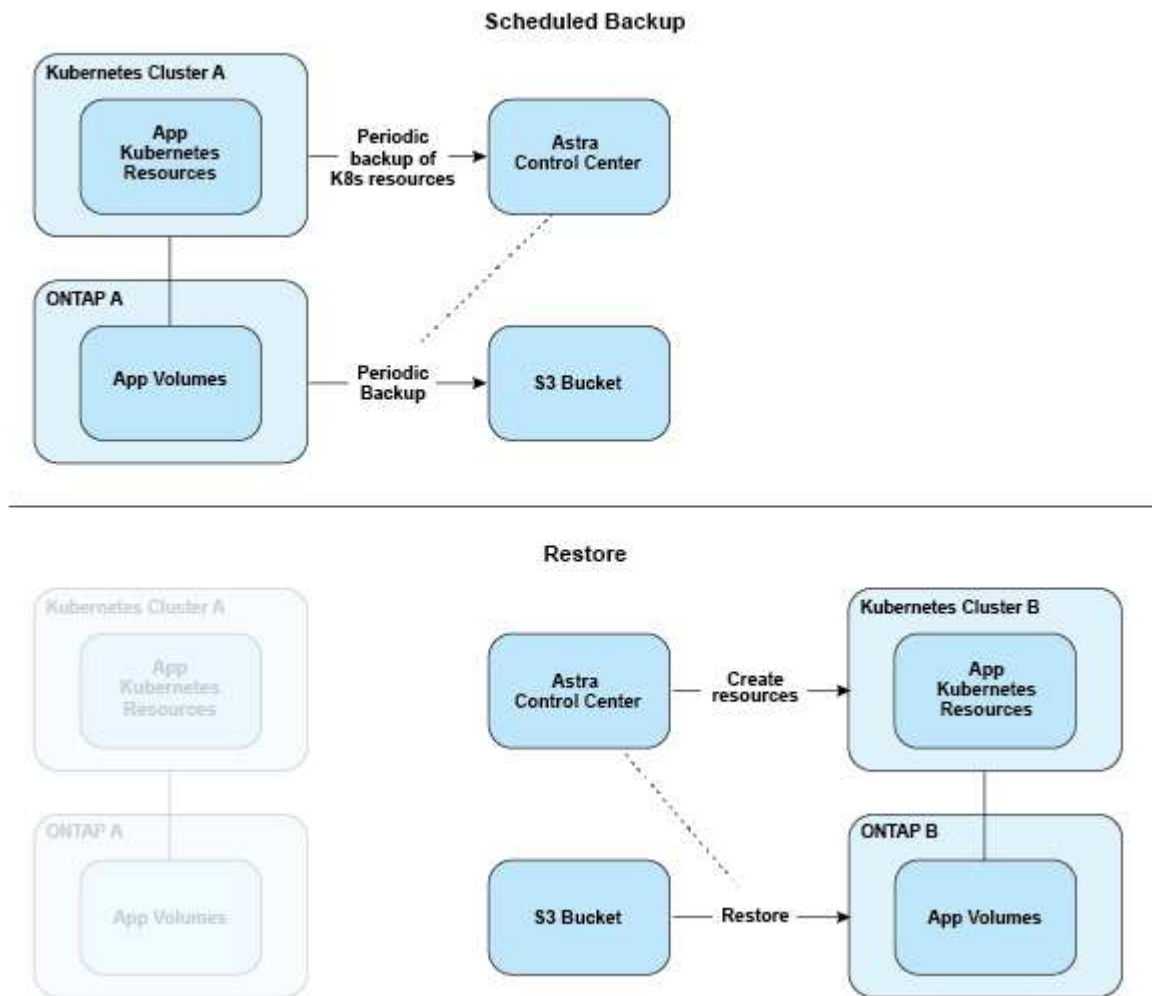
Per informazioni su come replicare le applicazioni, consulta ["Replica delle applicazioni su un sistema remoto"](#)



utilizzando la tecnologia SnapMirror".

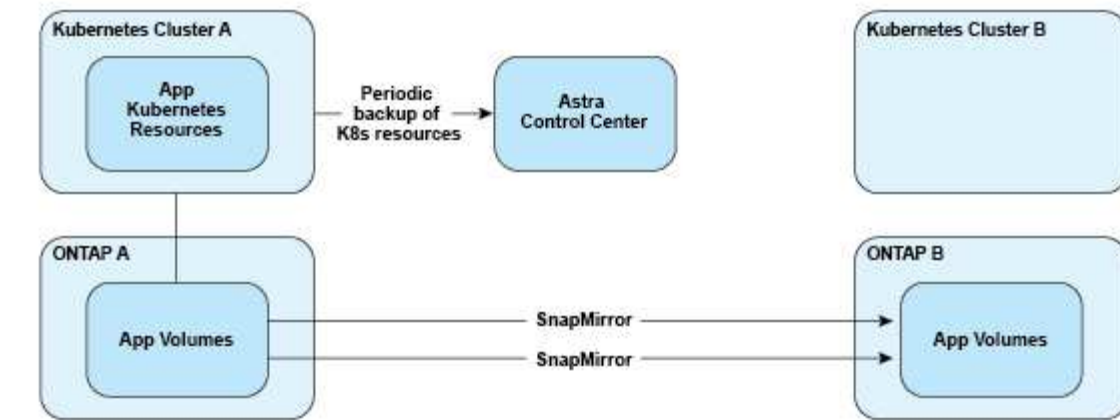
Le seguenti immagini mostrano il processo di backup e ripristino pianificato rispetto al processo di replica.

Il processo di backup copia i dati nei bucket S3 e li ripristina dai bucket S3:

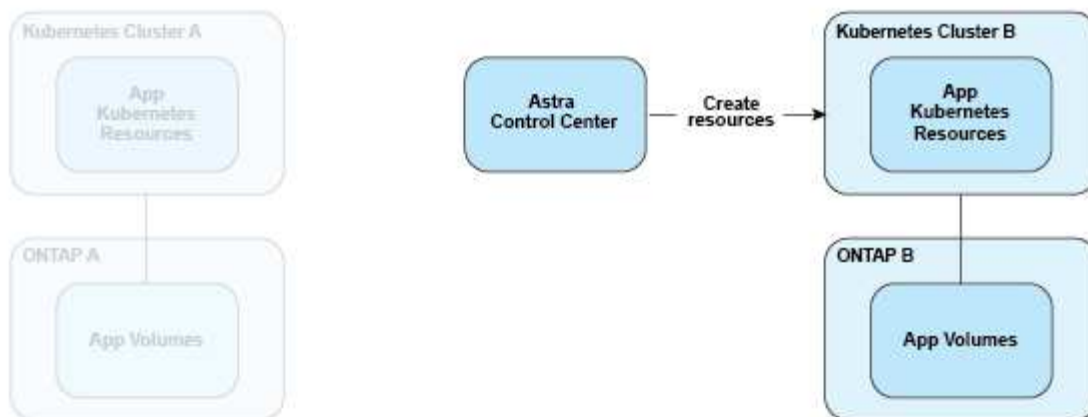


D'altro canto, la replica viene eseguita replicando in ONTAP e quindi un failover crea le risorse Kubernetes:

### Replication Relationship



### Fail over



## Licensing

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

Hai bisogno di una licenza per proteggere le tue applicazioni e i tuoi dati. Fare riferimento a Astra Control Center ["caratteristiche"](#) per ulteriori informazioni.

Una volta acquistato il prodotto, si riceveranno un numero di serie e una licenza. È possibile generare il file di licenza NetApp (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. Per ulteriori informazioni, fare riferimento a ["Requisiti"](#).

Per ulteriori informazioni sulle licenze necessarie per i backend di storage ONTAP, fare riferimento a ["backend di storage supportati"](#).



È possibile aggiungere un cluster, aggiungere un bucket e gestire un backend di storage senza una licenza.

## Come viene calcolato il consumo delle licenze

Quando si aggiunge un nuovo cluster ad Astra Control Center, non viene contato per ottenere licenze consumate fino a quando almeno un'applicazione in esecuzione sul cluster non viene gestita da Astra Control Center.

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

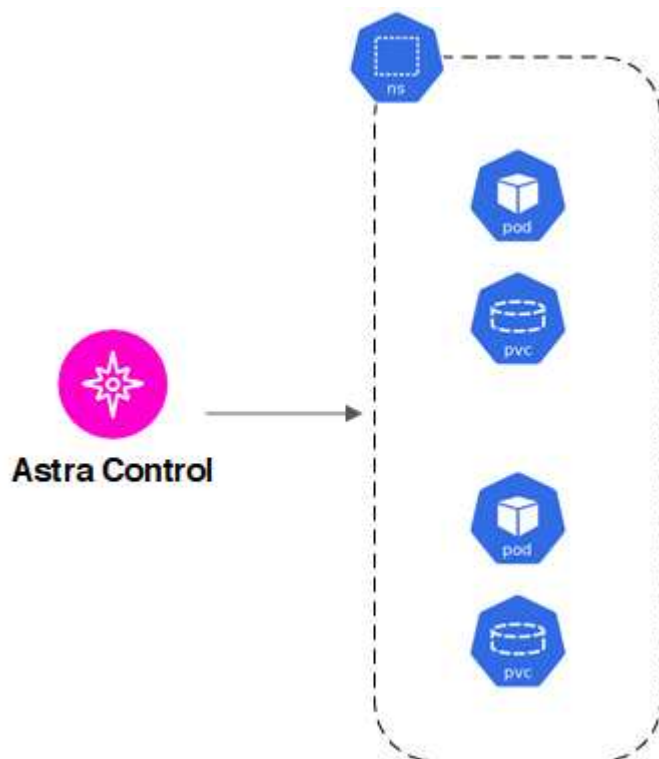
## Trova ulteriori informazioni

- ["Aggiornare una licenza esistente"](#)

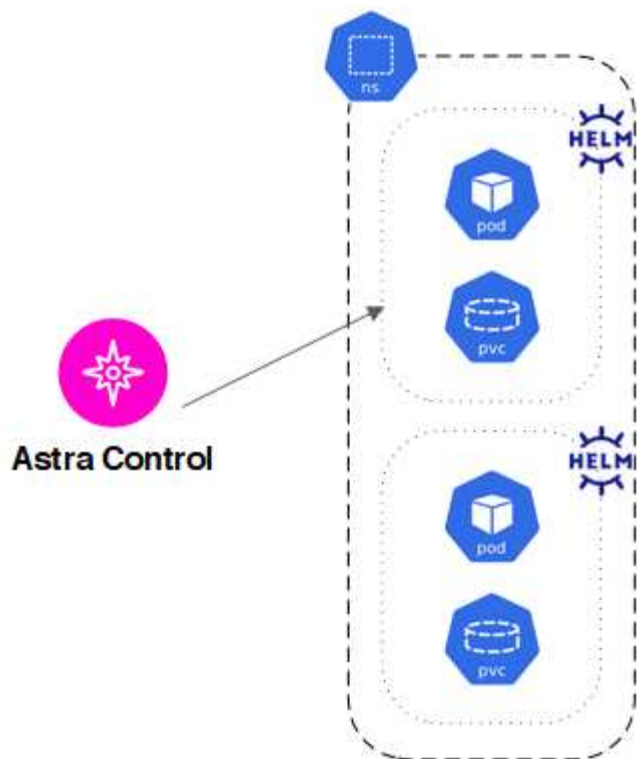
## Comprendere la gestione delle app

Quando Astra Control rileva i tuoi cluster, le applicazioni di questi ultimi non vengono gestite fino a quando non scegli come gestirli. Un'applicazione gestita in Astra Control può essere una delle seguenti:

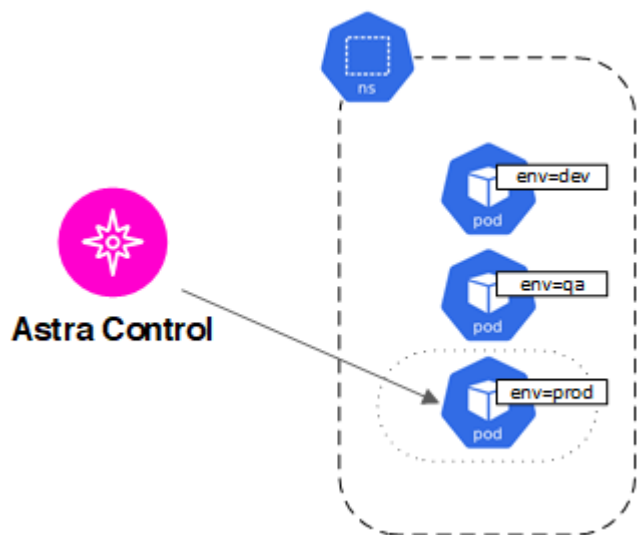
- Uno spazio dei nomi, che include tutte le risorse dello spazio dei nomi



- Una singola applicazione implementata all'interno di uno spazio dei nomi (in questo esempio viene utilizzato helm3)



- Gruppo di risorse identificate da un'etichetta Kubernetes all'interno di uno spazio dei nomi



## Classi di storage e dimensioni del volume persistente

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

### Panoramica

Astra Control Center supporta:

- **Classi di storage Trident supportate dallo storage Astra Data Store:** Se sono stati installati manualmente uno o più cluster Astra Data Store, Astra Control Center offre la possibilità di importare

questi cluster e recuperare la loro topologia (nodi, dischi) e vari stati.

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

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



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

## Classi di storage

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

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

## Per ulteriori informazioni

- ["Documentazione di Astra Trident"](#)

## Ruoli e spazi dei nomi degli utenti

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

### Ruoli utente

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

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

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

## Spazi dei nomi

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

## Trova ulteriori informazioni

["Gestire i ruoli"](#)

## Informazioni sul copyright

Copyright © 2023 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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