Concetti

Astra Control Center

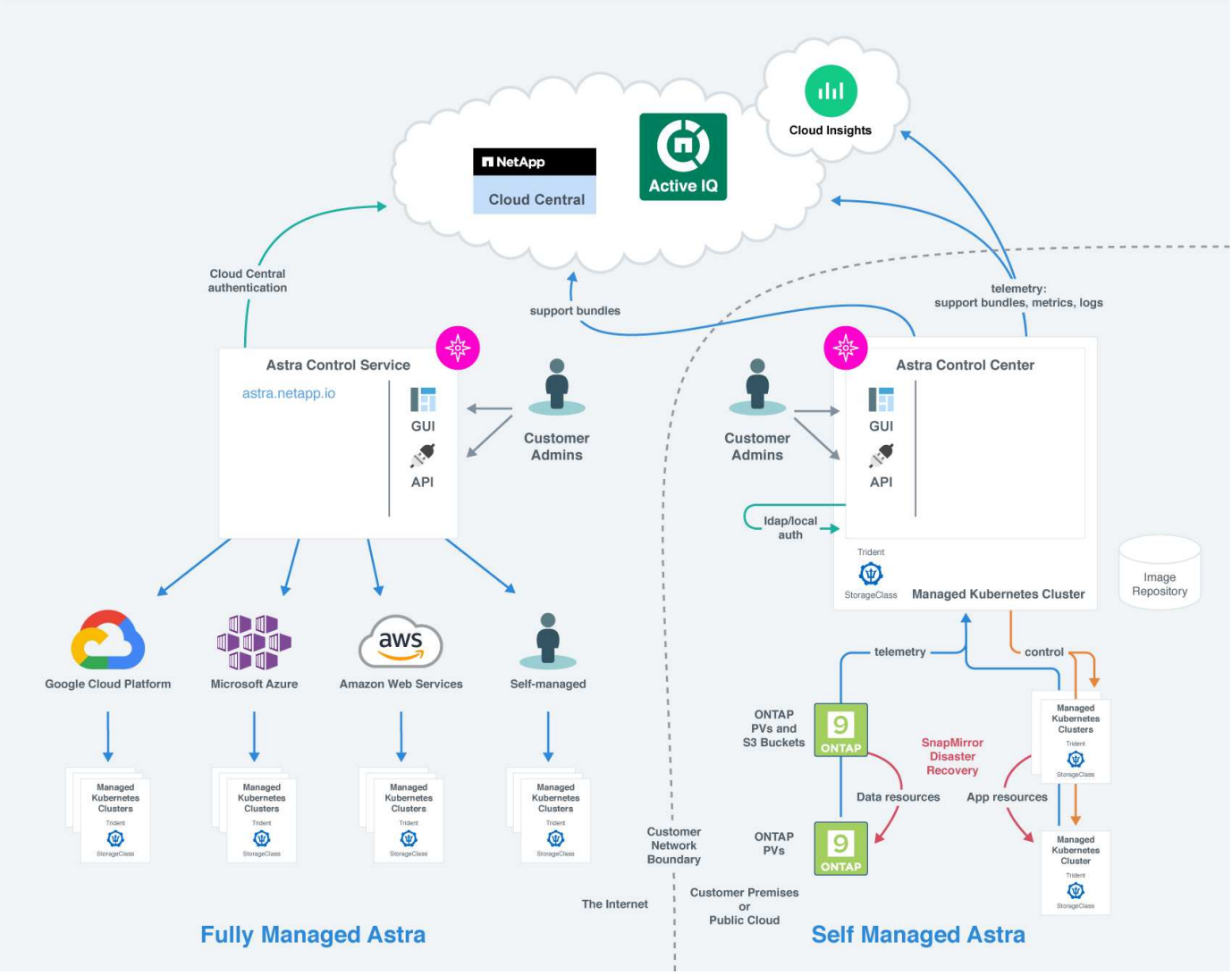
NetApp
November 21, 2023

Sommario

Concetti

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, Astra Trident consente di creare volumi di storage per applicazioni containerizzate gestite da Docker e Kubernetes. Se implementato con il centro di controllo Astra, Astra Trident include un backend di storage ONTAP configurato.
- **Storage backend**:
  - Astra Control Service utilizza i seguenti backend di storage:
    - "NetApp Cloud Volumes Service per Google Cloud" O Google Persistent Disk come backend di

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, FAS e ASA. 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 di 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

Sia le snapshot che i backup proteggono i seguenti tipi di dati:

- L'applicazione stessa

- Tutti i volumi di dati persistenti associati all'applicazione
- Qualsiasi elemento di risorsa appartenente all'applicazione

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. Le snapshot sono utili per clonare o ripristinare un'applicazione all'interno dello stesso cluster.

Un *backup* si basa su uno snapshot. Viene memorizzato nell'archivio di oggetti esterno e, per questo motivo, 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 e di impostare diversi livelli di granularità della 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 e ai requisiti SLA (Service Level Agreement).

> *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 dei suoi volumi di dati persistenti. 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 che i cluster Kubernetes di origine e di destinazione siano disponibili e gestiti 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 SnapMirror di NetApp viene utilizzata per replicare i dati dei volumi persistenti. Per eseguire il failover, Astra Control può portare online l'applicazione replicata ricreando gli oggetti dell'applicazione sul

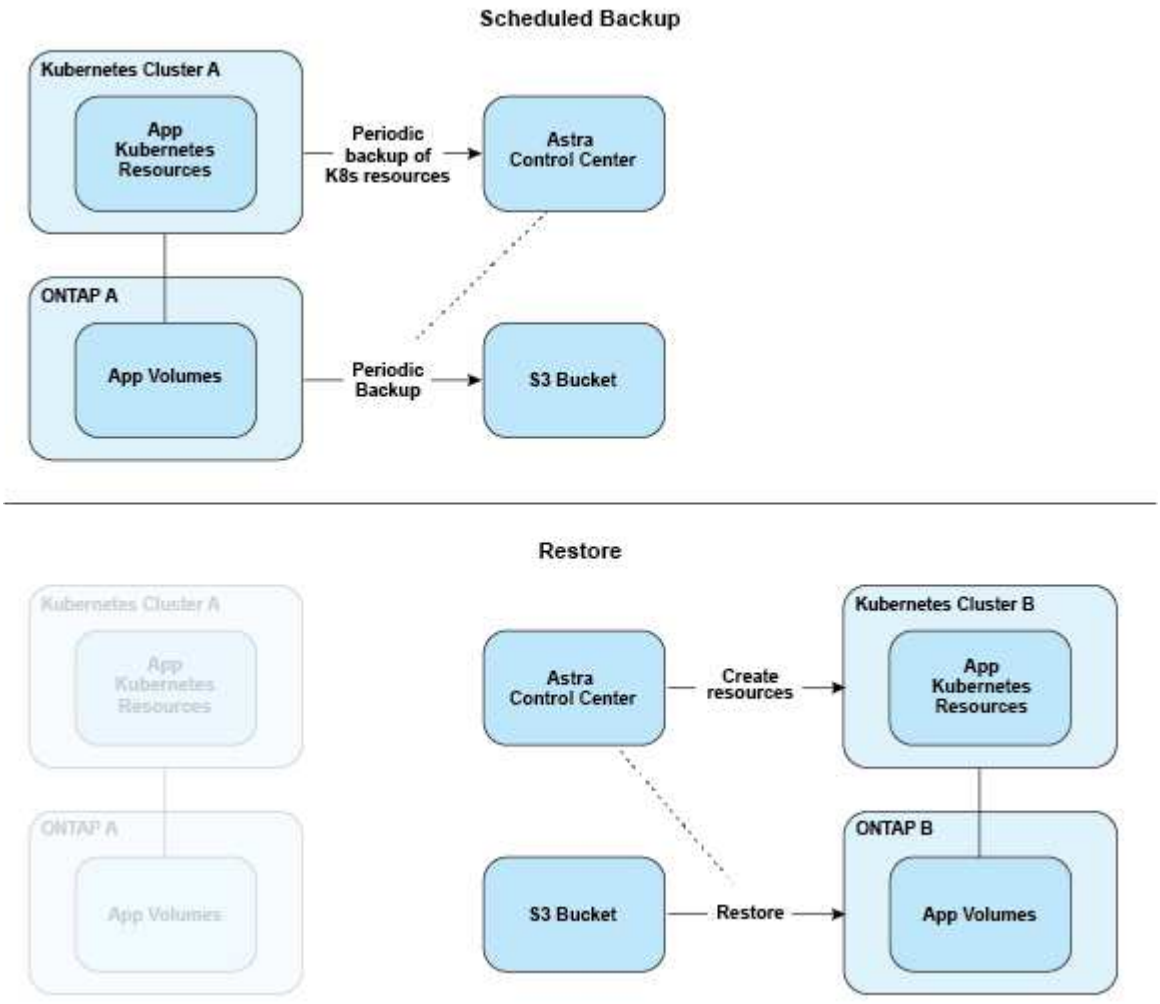
cluster Kubernetes di destinazione con i volumi replicati sul cluster ONTAP di destinazione. Poiché i dati del volume persistente sono già presenti nel cluster ONTAP di destinazione, Astra Control può offrire tempi di ripristino rapidi per il failover.

- **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.

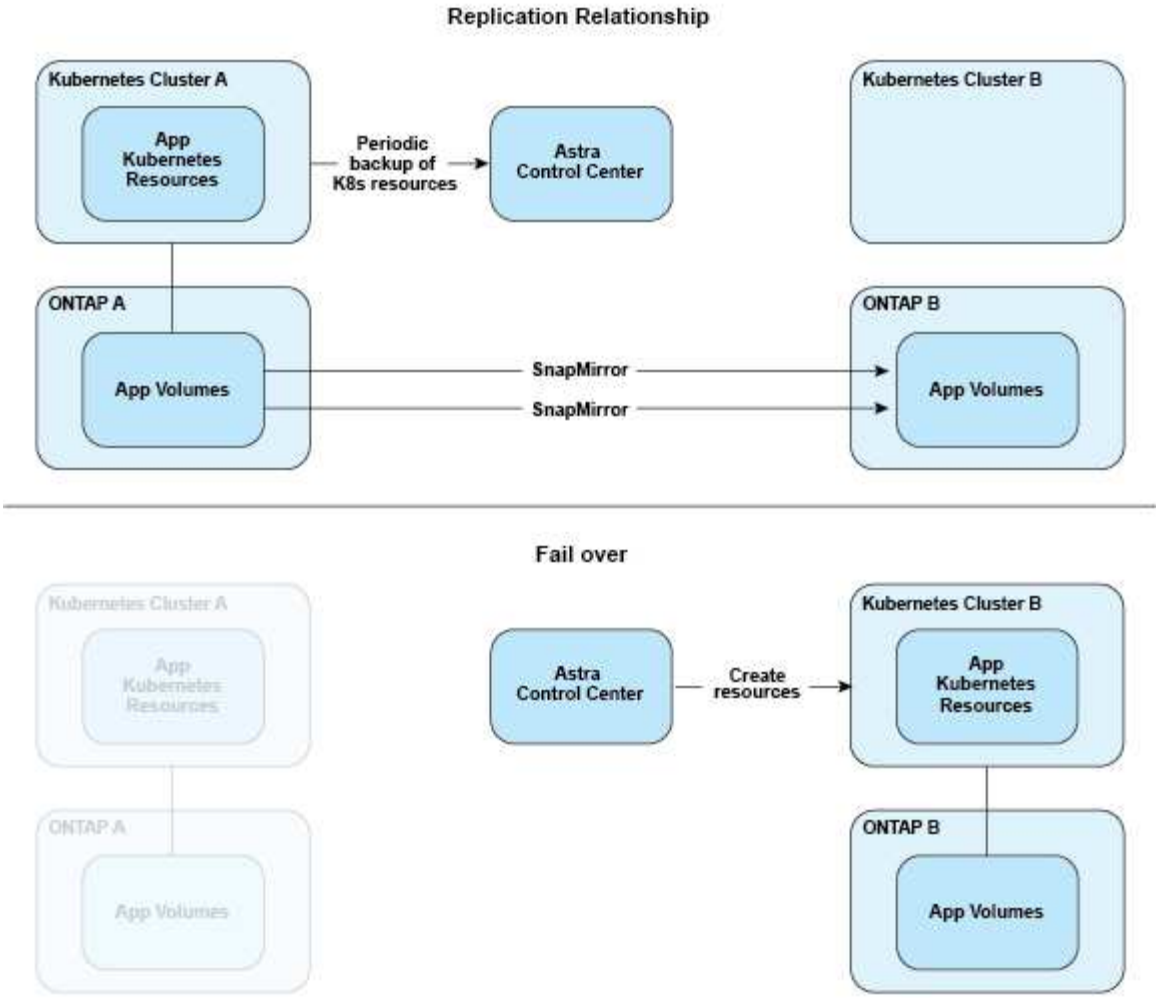
Per informazioni su come replicare le applicazioni, fare riferimento a. "Replica delle applicazioni su un sistema remoto utilizzando la tecnologia SnapMirror".

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:



Backup, snapshot e cloni con una licenza scaduta

Se la licenza scade, è possibile aggiungere una nuova applicazione o eseguire operazioni di protezione dell'applicazione (come snapshot, backup, cloni e operazioni di ripristino) solo se l'applicazione che si sta aggiungendo o proteggendo è un'altra istanza di Astra Control Center.

Licensing

Quando si implementa Astra Control Center, viene installato con una licenza di valutazione integrata di 90 giorni per 4,800 unità CPU. Se hai bisogno di maggiore capacità o di un periodo di valutazione più lungo, o se desideri passare a una licenza completa, puoi ottenere una licenza di valutazione o una licenza completa diversa da NetApp.

Si ottiene una licenza in uno dei seguenti modi:

- Se stai valutando Astra Control Center e hai bisogno di termini di valutazione diversi da quelli inclusi nella licenza di valutazione integrata, contatta NetApp per richiedere un file di licenza di valutazione diverso.
- "Se hai già acquistato Astra Control Center, genera il file di licenza NetApp (NLF)" Accedendo al NetApp Support Site e accedendo alle licenze software nel menu Systems.

Per ulteriori informazioni sulle licenze necessarie per i backend di storage ONTAP, fare riferimento a. "backend di storage supportati".

> Assicurarsi che la licenza consenta di utilizzare almeno tutte le unità CPU necessarie. Se il numero di unità CPU attualmente gestite da Astra Control Center supera le unità CPU disponibili nella nuova licenza applicata, non sarà possibile applicare la nuova licenza.

Licenze di valutazione e licenze complete

Una licenza di valutazione integrata viene fornita con una nuova installazione di Astra Control Center. Una licenza di valutazione offre le stesse funzionalità e funzionalità di una licenza completa per un periodo limitato (90 giorni). Dopo il periodo di valutazione, è necessaria una licenza completa per continuare con le funzionalità complete.

Scadenza della licenza

Se la licenza di Astra Control Center attiva scade, le funzionalità UI e API per le seguenti funzioni non sono disponibili:

- Snapshot e backup locali manuali
- Snapshot e backup locali pianificati
- Ripristino da uno snapshot o da un backup
- Clonazione da uno snapshot o da uno stato corrente
- Gestione di nuove applicazioni
- Configurazione dei criteri di replica

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 sono incluse nel consumo di licenza di Astra Control Center, ad eccezione delle unità CPU del nodo del cluster Red Hat OpenShift segnalate da un utilizzando l'etichetta `node-role.kubernetes.io/infra: ""`.

> I nodi dell'infrastruttura Red Hat OpenShift non consumano licenze in Astra Control Center. Per contrassegnare un nodo come nodo dell'infrastruttura, applicare l'etichetta `node-role.kubernetes.io/infra: ""` al nodo.

Trova ulteriori informazioni

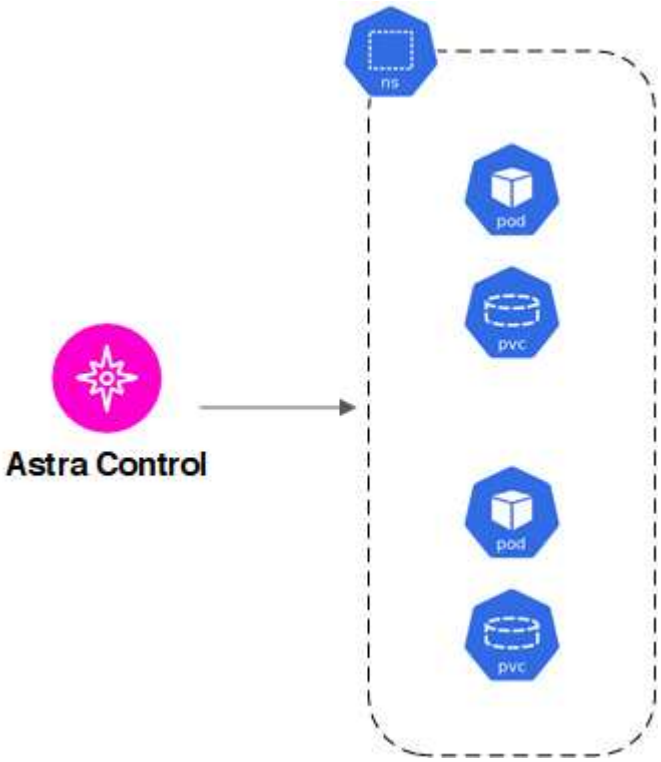
- "Aggiungere una licenza quando si imposta Astra Control Center per la prima volta"
- "Aggiornare una licenza esistente"

Gestione delle applicazioni

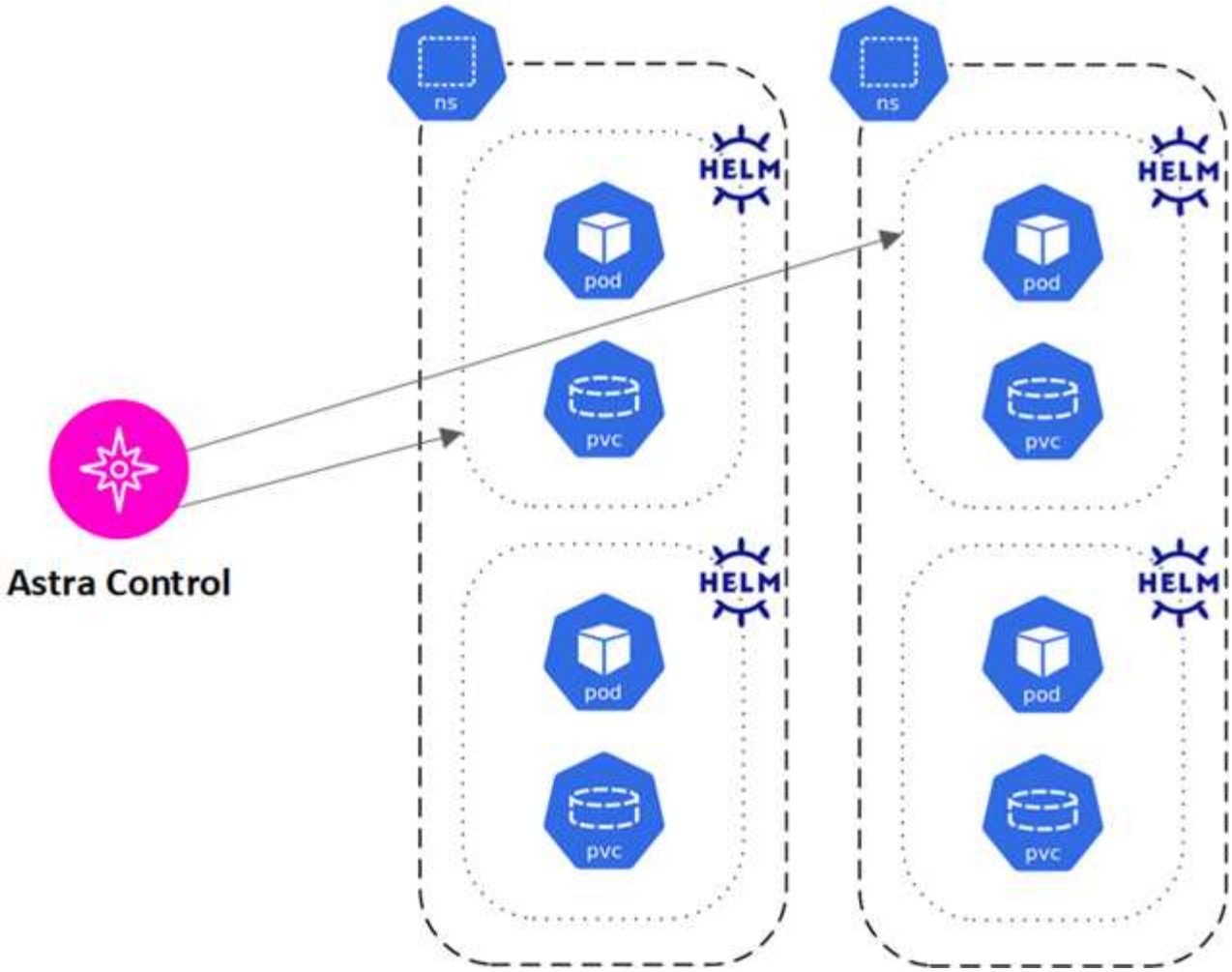
Quando Astra Control rileva i tuoi cluster, le applicazioni di questi ultimi non vengono gestite fino a quando non scegli come gestirli. Un'applicazione gestita in Astra Control

può essere una delle seguenti:

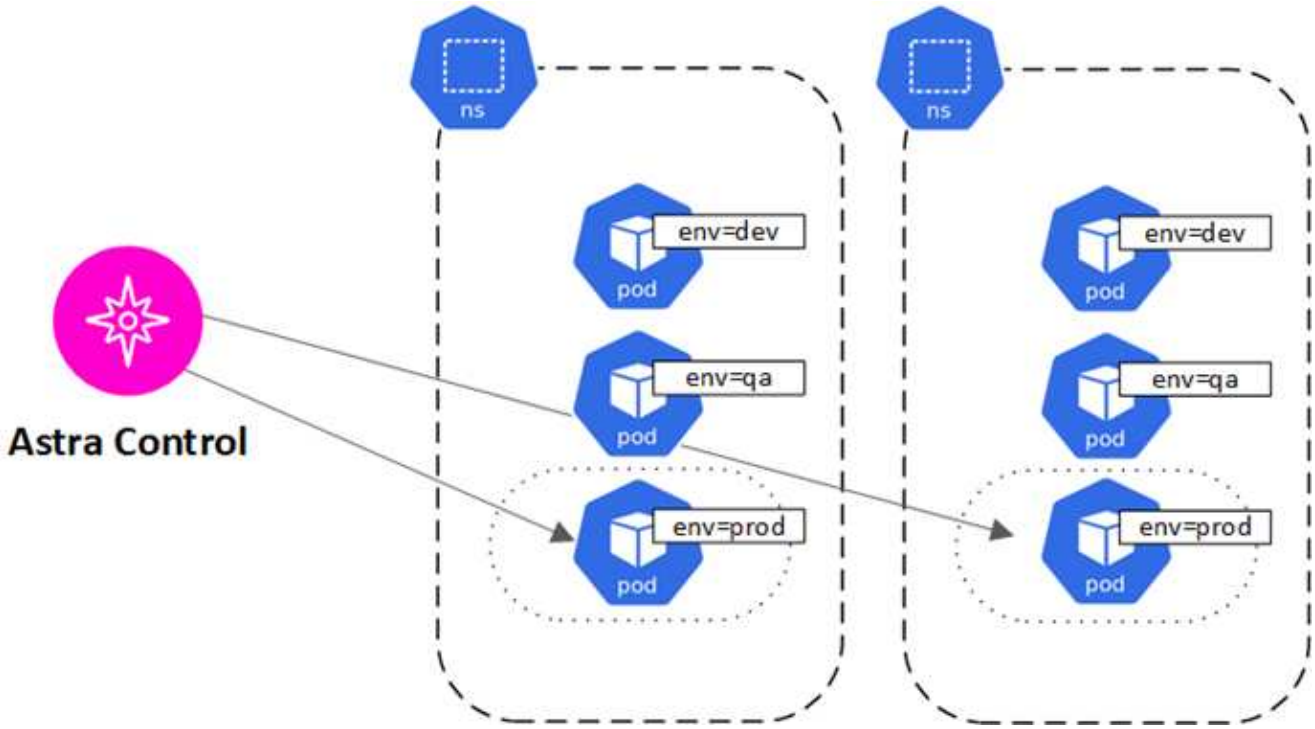
- Uno spazio dei nomi, che include tutte le risorse dello spazio dei nomi



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



- Un gruppo di risorse identificate da un'etichetta Kubernetes all'interno di uno o più spazi dei nomi



Classi di storage e dimensioni del volume persistente

Il centro di controllo Astra supporta ONTAP come backend dello storage.

Panoramica

Astra Control Center supporta:

- **Astra Trident storage classes backend supportato 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 Astra 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.

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 utenti e ruoli locali"

Sicurezza del pod

Astra Control Center supporta la limitazione dei privilegi attraverso PSP (Pod Security policy) e PSA (pod Security ammission). Questi framework consentono di limitare gli utenti o i gruppi in grado di eseguire i container e i privilegi che possono avere.

Alcune distribuzioni di Kubernetes potrebbero avere una configurazione di sicurezza pod predefinita troppo restrittiva e causare problemi durante l'installazione di Astra Control Center.

È possibile utilizzare le informazioni e gli esempi inclusi qui per comprendere le modifiche alla sicurezza dei pod apportate da Astra Control Center e utilizzare un approccio alla sicurezza dei pod che fornisca la protezione necessaria senza interferire con le funzioni di Astra Control Center.

PSA applicati da Astra Control Center

Durante l'installazione, Astra Control Center consente l'applicazione di un'ammissione di sicurezza Pod aggiungendo la seguente etichetta a `netapp-acc` o uno spazio dei nomi personalizzato:

```
pod-security.kubernetes.io/enforce: privileged
```

PSP installati da Astra Control Center

Quando si installa Astra Control Center su Kubernetes 1.23 o 1.24, durante l'installazione vengono create diverse policy di sicurezza del pod. Alcune di queste sono permanenti, alcune vengono create durante determinate operazioni e vengono rimosse una volta completata l'operazione. Astra Control Center non tenta di installare i PSP quando il cluster host esegue Kubernetes 1.25 o versioni successive, in quanto non sono supportati su queste versioni.

PSP creati durante l'installazione

Durante l'installazione di Astra Control Center, l'operatore di Astra Control Center installa una policy di sicurezza pod personalizzata, a. `Role` e a. `RoleBinding` Oggetto per supportare l'implementazione dei servizi Astra Control Center nello spazio dei nomi Astra Control Center.

I nuovi criteri e oggetti hanno i seguenti attributi:

```
kubectl get psp

NAME                              PRIV    CAPS          SELINUX    RUNASUSER
FSGROUP     SUPGROUP    READONLYROOTFS   VOLUMES
netapp-astra-deployment-psp    false                 RunAsAny   RunAsAny
RunAsAny    RunAsAny    false            *

kubectl get role -n <namespace_name>

NAME                                      CREATED AT
netapp-astra-deployment-role              2022-06-27T19:34:58Z

kubectl get rolebinding -n <namespace_name>

NAME                                      ROLE
AGE
netapp-astra-deployment-rb                Role/netapp-astra-deployment-role
32m
```

PSP creati durante le operazioni di backup

Durante le operazioni di backup, Astra Control Center crea una policy di sicurezza Pod dinamica, un `ClusterRole` e a. `RoleBinding` oggetto. Questi supportano il processo di backup, che avviene in uno spazio dei nomi separato.

I nuovi criteri e oggetti hanno i seguenti attributi:

```
kubectl get psp

NAME                              PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-astra-backup            false   DAC_READ_SEARCH
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false           *

kubectl get role -n <namespace_name>

NAME                  CREATED AT
netapp-astra-backup   2022-07-21T00:00:00Z

kubectl get rolebinding -n <namespace_name>

NAME                  ROLE                        AGE
netapp-astra-backup   Role/netapp-astra-backup   62s
```

PSP creati durante la gestione del cluster

Quando gestisci un cluster, Astra Control Center installa l'operatore di monitoraggio netapp nel cluster gestito. Questo operatore crea una policy di sicurezza pod, a. `ClusterRole` e a. `RoleBinding` Oggetto per implementare servizi di telemetria nello spazio dei nomi Astra Control Center.

I nuovi criteri e oggetti hanno i seguenti attributi:

```
kubectl get psp

NAME                            PRIV    CAPS
SELINUX    RUNASUSER          FSGROUP     SUPGROUP    READONLYROOTFS
VOLUMES
netapp-monitoring-psp-nkmo     true    AUDIT_WRITE,NET_ADMIN,NET_RAW
RunAsAny   RunAsAny           RunAsAny    RunAsAny    false            *

kubectl get role -n <namespace_name>

NAME                                          CREATED AT
netapp-monitoring-role-privileged             2022-07-21T00:00:00Z

kubectl get rolebinding -n <namespace_name>

NAME                                                  ROLE
AGE
netapp-monitoring-role-binding-privileged             Role/netapp-
monitoring-role-privileged              2m5s
```

Informazioni sul copyright

Informazioni sul marchio commerciale