Concetti

Astra Control Service

NetApp
June 04, 2024

Sommario

Concetti

Architettura e componenti

Astra Control è una soluzione di gestione del ciclo di vita dei dati delle applicazioni Kubernetes che semplifica le operazioni per le applicazioni stateful e ti aiuta a memorizzare, proteggere e spostare i carichi di lavoro Kubernetes negli ambienti ibridi e multi-cloud.

Funzionalità

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

Negozio:

- Provisioning dello storage dinamico per i carichi di lavoro in container
- Crittografia in-flight dei dati da container a volumi persistenti
- Replica tra aree e aree

Protezione:

- Rilevamento automatizzato e protezione integrata con l'applicazione di un'intera applicazione e dei relativi dati
- Ripristino istantaneo di un'applicazione da qualsiasi versione snapshot in base alle esigenze dell'organizzazione
- Failover rapido tra zone, aree e cloud provider

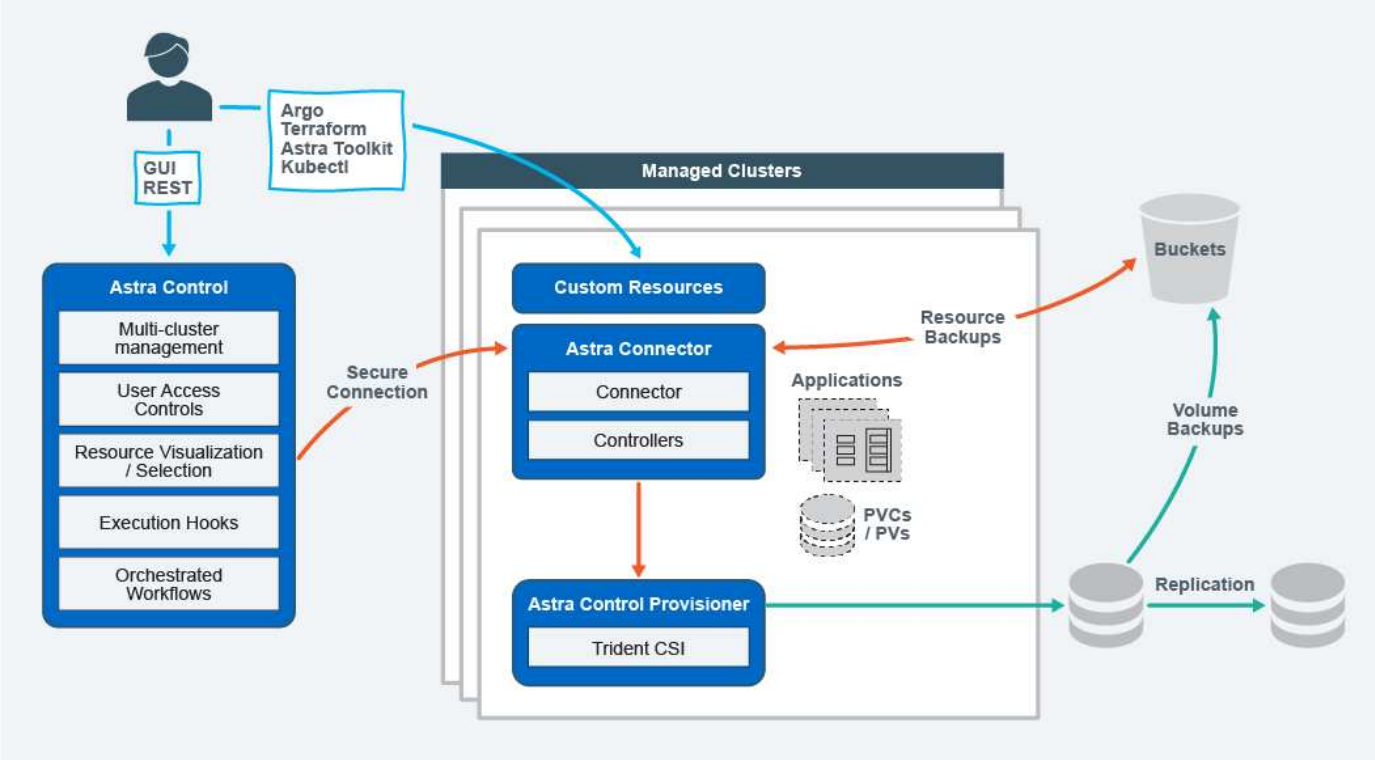
Sposta:

- Mobilità completa di applicazioni e dati all'interno e tra cluster Kubernetes e cloud
- Cloni istantanei di intere applicazioni e dati
- Migrazione delle applicazioni con un solo clic tramite API e UI web coerenti

Architettura

L'architettura di Astra Control consente all'IT di fornire funzionalità avanzate di gestione dei dati che migliorano sia la funzionalità che la disponibilità delle applicazioni Kubernetes, semplificano la gestione, la protezione e lo spostamento dei carichi di lavoro in container nei cloud pubblici e negli ambienti on-premise. inoltre, offre funzionalità di automazione tramite API REST e SDK, consentendo l'accesso programmatico per un'integrazione perfetta con i flussi di lavoro esistenti.

Astra Control è nativo di Kubernetes e consente workflow di data Protection che utilizzano risorse personalizzate pur rimanendo compatibile con le versioni precedenti dell'API e dell'SDK esistenti. La data Protection nativa di Kubernetes offre vantaggi significativi: Con l'integrazione perfetta con le risorse e le API Kubernetes, la data Protection può diventare una parte integrante del ciclo di vita delle applicazioni attraverso gli strumenti ci/CD e/o GitOps esistenti dell'organizzazione.



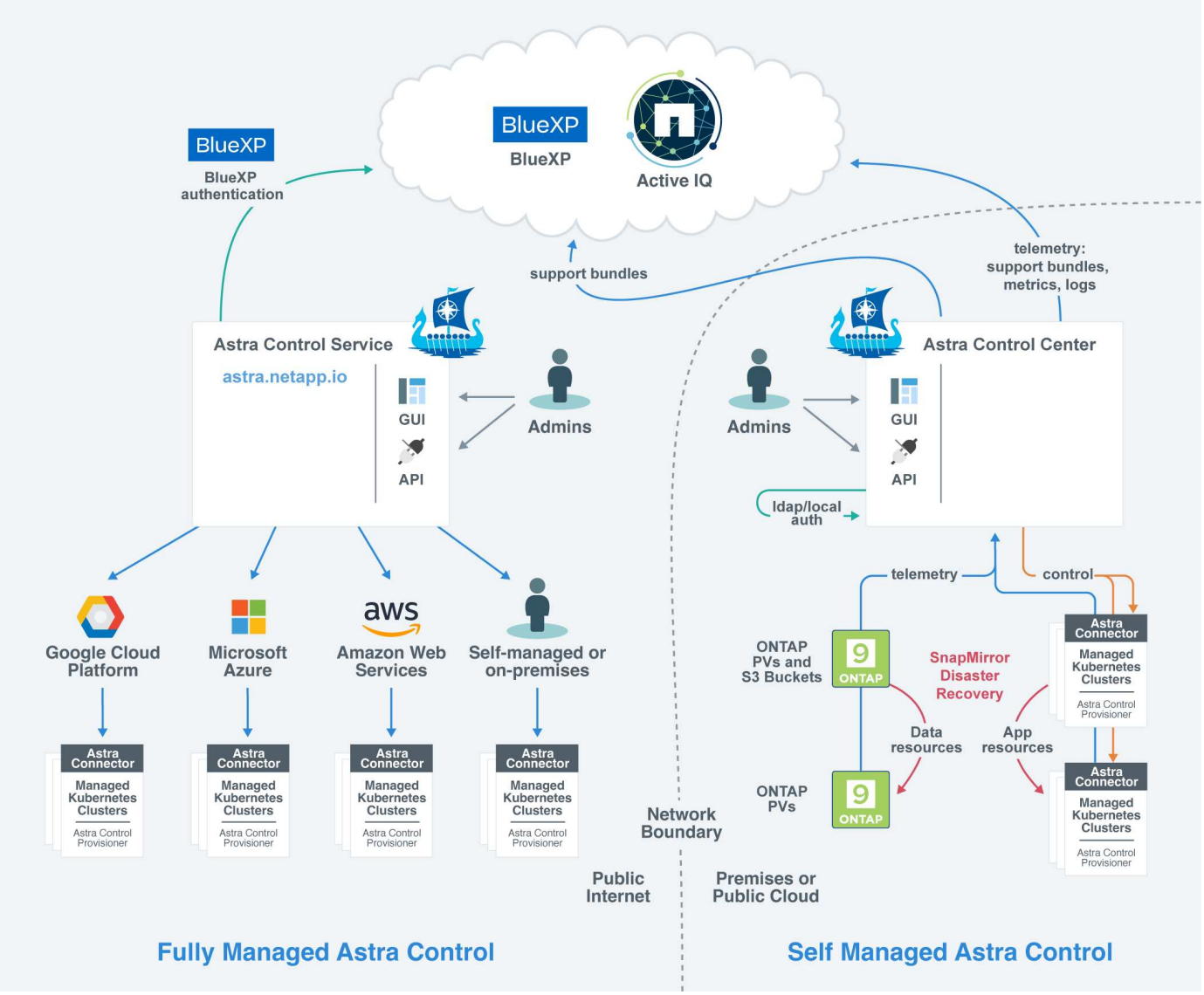
Astra Control è costruito su quattro componenti complementari:

- **Astra Control**: Astra Control è un servizio di gestione centralizzato per tutti i cluster gestiti, che fornisce workload orchestrati per la protezione e la mobilità delle applicazioni nel cloud e on-premise, nonché le seguenti funzionalità:
  - Vista combinata di cluster e cloud multipli
  - Protezione dei flussi di lavoro orchestrati
  - Visualizzazione e selezione granulare delle risorse
- **Astra Connector**: Astra Connector raggruppa Astra Control per fornire una connessione sicura a ciascun cluster gestito, offrendo l'esecuzione locale delle operazioni pianificate indipendentemente dallo stato della connessione e le seguenti funzionalità:
  - Esecuzione locale delle operazioni pianificate indipendentemente dallo stato della connessione
  - Operazioni locali che distribuiscono e ottimizzano l'utilizzo delle risorse di sistema di Astra tra i cluster
  - Installazione locale che consente l'accesso con privilegi minimi al cluster per una maggiore sicurezza
- **Astra Control Provisioner**: Astra Control Provisioner offre funzionalità di provisioning CSI core e capacità di gestione dello storage avanzate per una maggiore sicurezza e configurazione di disaster recovery, nonché le seguenti capacità:
  - Provisioning dello storage dinamico per i carichi di lavoro in container
  - Gestione avanzata dello storage:
    - Crittografia in-flight dei dati da container a PV
    - Funzionalità SnapMirror Cloud con replica tra aree e zone
- **Astra Custom Resources**: Le risorse personalizzate utilizzate su ogni cluster forniscono un approccio nativo per Kubernetes per l'esecuzione delle operazioni in locale, semplificando l'integrazione con altri tool e automazione compatibili con Kubernetes e fornendo le seguenti funzionalità:
  - Flussi di lavoro diretti di automazione e integrazione degli strumenti dell'ecosistema

- Primitive di livello inferiore che abilitano flussi di lavoro personalizzati

Modelli di implementazione

Astra Control è disponibile in due modelli di implementazione.



- **Astra Control Service**: Un servizio gestito da NetApp che offre la gestione dei dati application-aware dei cluster Kubernetes in ambienti di cloud provider multipli e cluster Kubernetes autogestiti.

  "Documentazione del servizio Astra Control"

- **Astra Control Center**: Software autogestito che fornisce la gestione dei dati applicativa dei cluster Kubernetes in esecuzione nel tuo ambiente on-premise. Il centro di controllo Astra può essere installato anche in ambienti di cloud provider multipli con un backend di storage NetApp Cloud Volumes ONTAP.

  "Documentazione di Astra Control Center"

	Servizio di controllo Astra	Centro di controllo Astra
Come viene offerto?	Come servizio cloud completamente gestito da NetApp	Come software che puoi scaricare, installare e gestire
Dove è ospitato?	Su un cloud pubblico scelto da NetApp	Sul tuo cluster Kubernetes
Come viene aggiornato?	Gestito da NetApp	Gli aggiornamenti vengono gestiti
Quali sono le distribuzioni Kubernetes supportate?	• **Cloud provider** ◦ Amazon Web Services ▪ Amazon Elastic Kubernetes Service (EKS) ◦ Google Cloud ▪ Google Kubernetes Engine (GKE) ◦ Microsoft Azure ▪ Servizio Azure Kubernetes (AKS) • **Cluster autogestiti** ◦ Kubernetes (upstream) ◦ Rancher Kubernetes Engine (RKE) ◦ Red Hat OpenShift Container Platform • **Cluster on-premise** ◦ Red Hat OpenShift Container Platform all'interno dell'hotel	• Azure Kubernetes Service su Azure Stack HCI • Google anthos • Kubernetes (upstream) • Rancher Kubernetes Engine (RKE) • Red Hat OpenShift Container Platform

	Servizio di controllo Astra	Centro di controllo Astra
Quali sono i backend di storage supportati?	• **Cloud provider** ◦ Amazon Web Services ▪ Amazon EBS ▪ Amazon FSX per NetApp ONTAP ▪ "Cloud Volumes ONTAP" ◦ Google Cloud ▪ Disco persistente di Google ▪ NetApp Cloud Volumes Service ▪ "Cloud Volumes ONTAP" ◦ Microsoft Azure ▪ Dischi gestiti Azure ▪ Azure NetApp Files ▪ "Cloud Volumes ONTAP" • **Cluster autogestiti** ◦ Amazon EBS ◦ Dischi gestiti Azure ◦ Disco persistente di Google ◦ "Cloud Volumes ONTAP" ◦ NetApp MetroCluster ◦ "Longhorn" • **Cluster on-premise** ◦ NetApp MetroCluster ◦ Sistemi NetApp ONTAP AFF e FAS ◦ NetApp ONTAP Select ◦ "Cloud Volumes ONTAP" ◦ "Longhorn"	• Sistemi NetApp ONTAP AFF e FAS • NetApp ONTAP Select • "Cloud Volumes ONTAP" • "Longhorn"

Per ulteriori informazioni

- "Documentazione del servizio Astra Control"
- "Documentazione di Astra Control Center"
- "Documentazione di Astra Trident"
- "API di controllo Astra"
- "Documentazione Cloud Insights"

- "Documentazione ONTAP"

Protezione dei dati

Scopri i tipi di protezione dei dati disponibili in Astra Control Service 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.

Se si esegue uno snapshot o un backup, ma l'operazione non riesce e viene visualizzato l'errore "la risorsa non è stata creata a causa di un problema interno al server", verificare che il backend di storage in uso abbia installato i driver corretti. Alcuni backend di storage richiedono driver CSI (Container Storage Interface), mentre altri necessitano di un controller di snapshot esterno.

Backup immutabili

Un backup immutabile è un backup che non può essere modificato o eliminato durante un periodo specificato. Quando crei un backup immutabile, Astra Control controlla che il bucket che stai utilizzando sia un bucket WORM (Write Once Read Many) e, in caso affermativo, garantisce che il backup sia immutabile dall'interno di Astra Control.

Astra Control Service supporta la creazione di backup immutabili con le seguenti piattaforme e tipi di bucket:

- Amazon Web Services che utilizza un bucket Amazon S3 con blocco oggetti S3 configurato
- Microsoft Azure mediante un bucket Azure con una policy di conservazione configurata
- Google Kubernetes Engine (GKE) utilizzando un bucket Google Cloud Storage con una policy di conservazione configurata
- NetApp StorageGRID che utilizza un bucket S3 con blocco oggetto S3 configurato

Tenere presente quanto segue quando si utilizzano i backup immutabili:

- Se si esegue il backup in un bucket WORM in una piattaforma non supportata o in un tipo di bucket non supportato, si potrebbero ottenere risultati imprevedibili, come il mancato completamento dell'eliminazione del backup anche se è trascorso il tempo di conservazione.
- Astra Control non supporta le policy di data Lifecycle management o l'eliminazione manuale di oggetti nei bucket utilizzati con backup immutabili. Verifica che il back-end dello storage non sia configurato per gestire il ciclo di vita delle snapshot di Astra Control o dei dati di cui è stato eseguito il backup.

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.

Classi di storage e performance per cluster AWS

Il servizio di controllo Astra può utilizzare Amazon Elastic Block Store (EBS), Amazon FSX per NetApp ONTAP o NetApp Cloud Volumes ONTAP come backend di storage per i cluster Amazon Elastic Kubernetes Service (EKS).

Amazon Elastic Block Store (EBS)

I cluster possono utilizzare i driver CSI (Container Storage Interface) per l'interfaccia con EBS. Quando si utilizza EBS come backend di storage per i cluster EKS, è possibile configurare alcuni parametri della classe di storage. Per ulteriori informazioni sul significato dei parametri e su come configurarli, fare riferimento a. "La documentazione di Kubernetes".

EBS consente di utilizzare diversi tipi di volumi:

- Unità a stato solido (SSD)
- Dischi rigidi (HDD)
- Generazione precedente

Per ulteriori informazioni su ciascun tipo di volume e sulle relative prestazioni, fare riferimento a. "La documentazione di Amazon EBS". Per informazioni sui prezzi, fare riferimento a. "Prezzo Amazon EBS".

Amazon FSX per NetApp ONTAP

Quando si utilizza FSX per NetApp ONTAP come backend di storage per i cluster AWS, le performance di i/o dipendono dalla configurazione del file system e dalle caratteristiche dei carichi di lavoro. Per informazioni

specifiche sulle performance di FSX per NetApp ONTAP, fare riferimento a. "Performance di Amazon FSX per NetApp ONTAP". Per informazioni sui prezzi, fare riferimento a. "Amazon FSX per NetApp ONTAP Pricing".

NetApp Cloud Volumes ONTAP

Per informazioni specifiche sulla configurazione di NetApp Cloud Volumes ONTAP, inclusi i consigli sulle performance, visitare il "Documentazione di NetApp Cloud Volumes ONTAP".

Classi di storage e dimensioni PV per cluster AKS

Il servizio di controllo Astra supporta Azure NetApp Files, i dischi gestiti Azure o NetApp Cloud Volumes ONTAP come backend di storage per i cluster AKS (Azure Kubernetes Service).

Azure NetApp Files

Il servizio di controllo Astra supporta Azure NetApp Files come backend di storage per i cluster AKS (Azure Kubernetes Service). Devi capire come scegliere una classe di storage e una dimensione del volume persistente possono aiutarti a raggiungere i tuoi obiettivi di performance.

Livelli di servizio e classi di storage

Azure NetApp Files supporta tre livelli di servizio: Storage ultra, storage premium e storage standard. Ciascuno di questi livelli di servizio è progettato per soddisfare diverse esigenze di performance:

Storage ultra
: Fornisce fino a 128 MIB/s di throughput per 1 TIB.

Storage premium
: Fornisce fino a 64 MIB/s di throughput per 1 TIB.

Storage standard
: Fornisce fino a 16 MIB/s di throughput per 1 TIB.

Questi livelli di servizio sono un attributo di un pool di capacità. È necessario impostare un pool di capacità per ciascun livello di servizio che si desidera utilizzare con i cluster Kubernetes. "Scopri come configurare i pool di capacità".

Astra Control Service utilizza questi livelli di servizio come classi di storage per i volumi persistenti. Quando si aggiungono cluster Kubernetes ad Astra Control Service, viene richiesto di scegliere Ultra, Premium o Standard come classe di storage predefinita. I nomi delle classi di storage sono *netapp-anf-perf-ultra*, *netapp-anf-perf-premium* e *netapp-anf-perf-standard*.

"Scopri di più su questi livelli di servizio nei documenti Azure NetApp Files".

Dimensioni e performance del volume persistenti

Come descritto in precedenza, il throughput per ciascun livello di servizio corrisponde a 1 TIB della capacità fornita. Ciò significa che volumi più grandi offrono performance migliori. Pertanto, è necessario tenere in considerazione le esigenze di capacità e performance durante il provisioning dei volumi.

Dimensione minima del volume

Astra Control Service fornisce volumi persistenti utilizzando una dimensione minima del volume di 100 GiB, anche se il PVC richiede una dimensione minore del volume. Ad esempio, se il PVC in un grafico Helm richiede 6 GiB, Astra Control Service effettua automaticamente il provisioning di un volume da 100 GiB.

Backup delle applicazioni

Se si esegue il backup di un'applicazione che risiede nello storage Azure NetApp Files, il servizio di controllo Astra espande automaticamente temporaneamente il pool di capacità. Una volta completato il backup, Astra Control Service riduce il pool di capacità alle dimensioni precedenti. In base al tuo abbonamento Azure, in questo caso potrebbero essere applicati costi di storage. È possibile visualizzare una cronologia degli eventi di ridimensionamento del pool di capacità nel registro eventi della pagina **attività**.

Se il pool di capacità supera le dimensioni massime consentite dall'abbonamento Azure durante l'operazione di ridimensionamento, l'operazione di backup non riesce e viene generato un avviso dall'API Azure.

Dischi gestiti da Azure

Astra Control Service può utilizzare i driver CSI (Container Storage Interface) per interfacciarsi con Azure Managed Disks come backend di storage. Questo servizio fornisce storage a livello di blocco gestito da Azure.

"Scopri di più sui dischi gestiti da Azure".

NetApp Cloud Volumes ONTAP

Per informazioni specifiche sulla configurazione di NetApp Cloud Volumes ONTAP, inclusi i consigli sulle performance, visitare il "Documentazione di NetApp Cloud Volumes ONTAP".

Tipo di servizio, classi di storage e dimensione PV per cluster GKE

Il servizio di controllo Astra supporta NetApp Cloud Volumes Service per Google Cloud, Google Persistent Disk o NetApp Cloud Volumes ONTAP come opzioni di back-end dello storage per i volumi persistenti.

Cloud Volumes Service per Google Cloud

Il servizio di controllo Astra può utilizzare Cloud Volumes Service per Google Cloud come back-end dello storage per i volumi persistenti. Devi capire come scegliere un tipo di servizio, una classe di storage e una dimensione del volume persistente possono aiutarti a raggiungere i tuoi obiettivi di performance.

Panoramica

Cloud Volumes Service per Google Cloud offre due tipi di servizi: *CVS* e *CVS-Performance*. Questi tipi di servizio sono supportati in aree specifiche di Google Cloud. "Vai alle mappe delle regioni globali BlueXP di NetApp" Per identificare il tipo di servizio supportato nell'area di Google Cloud in cui risiedono i cluster.

Se i cluster Kubernetes devono risiedere in una regione specifica, verrà utilizzato il tipo di servizio supportato in tale regione.

Tuttavia, se hai la flessibilità di scegliere tra le aree di Google Cloud, ti consigliamo di seguire i seguenti

suggerimenti in base ai tuoi requisiti di performance:

- Per le applicazioni K8s che hanno esigenze di storage dalle performance medio-elevate, scegli un'area di Google Cloud che supporti CVS-Performance e utilizzi la classe di storage Premium o Extreme. Tali carichi di lavoro includono pipeline ai/ML, pipeline ci/CD, elaborazione di supporti e database, tra cui relazionali, NoSQL, serie temporali, ecc.
- Per le applicazioni K8s che hanno esigenze di performance di storage da bassa a media (applicazioni web, storage di file General purpose, ecc.), scegli un'area Google Cloud che supporti CVS o CVS-Performance, con la classe di storage Standard.

> Se utilizzi il tipo di servizio CVS con Astra Control Provisioner, devi configurare i pool di storage prima di poter eseguire il provisioning dei volumi. Se esegui il provisioning di volumi senza pool di storage configurati, il provisioning del volume avrà esito negativo. Fare riferimento a. "Documentazione Cloud Volumes Service" per ulteriori informazioni sulla creazione di volumi.

La seguente tabella fornisce un rapido confronto delle informazioni descritte in questa pagina.

Tipo di servizio	Caso d'utilizzo	Regioni supportate	Classi di storage	Dimensione minima del volume
Performance CVS	Applicazioni con esigenze di performance dello storage medio-elevate	"Visualizza le aree di Google Cloud supportate"	• netapp-cvs-perf-standard • netapp-cvs-perf-premium • netapp-cvs-perf-extreme	100 GiB
CVS	Applicazioni con esigenze di performance dello storage medio-basse	"Visualizza le aree di Google Cloud supportate"	netapp-cvs-standard	300 GiB

Tipo di servizio CVS-Performance

Scopri di più sul tipo di servizio CVS-Performance prima di scegliere una classe di storage e creare volumi persistenti.

Classi di storage

Il tipo di servizio CVS-Performance supporta tre livelli di servizio: Standard, Premium ed Extreme. Quando si aggiunge un cluster ad Astra Control Service, viene richiesto di scegliere Standard, Premium o Extreme come classe di storage predefinita per i volumi persistenti. Ciascuno di questi livelli di servizio è progettato per soddisfare le diverse esigenze di capacità e larghezza di banda.

I nomi delle classi di storage sono *netapp-cvs-perf-standard*, *netapp-cvs-perf-premium* e *netapp-cvs-perf-Extreme*.

"Scopri di più su questi livelli di servizio nella documentazione di Cloud Volumes Service per Google Cloud".

Dimensioni e performance del volume persistenti

"Come spiega Google Cloud", La larghezza di banda consentita per ciascun livello di servizio è per GiB della capacità fornita. Ciò significa che volumi più grandi forniranno performance migliori.

Assicurati di leggere la pagina Google Cloud a cui si è collegati. Include 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.

Dimensione minima del volume

Astra Control Service effettua il provisioning dei volumi persistenti utilizzando una dimensione minima del volume di 100 GiB con il tipo di servizio CVS-Performance, anche se il PVC richiede una dimensione minore del volume. Ad esempio, se il PVC in un grafico Helm richiede 6 GiB, Astra Control Service effettua automaticamente il provisioning di un volume da 100 GiB.

Tipo di servizio CVS

Scopri di più sul tipo di servizio CVS prima di scegliere una classe di storage e creare volumi persistenti.

Classe di storage

Un livello di servizio è supportato con il tipo di servizio CVS: Standard. Quando si gestiscono i cluster in regioni in cui è supportato il tipo di servizio CVS, Astra Control Service utilizza il livello di servizio Standard come classe di storage predefinita per i volumi persistenti. La classe di storage è denominata *netapp-cvs-standard*.

"Scopri di più sul livello di servizio standard nei documenti Cloud Volumes Service per Google Cloud".

Dimensioni e performance del volume persistenti

La larghezza di banda consentita per il tipo di servizio CVS è per GiB della capacità fornita. Ciò significa che volumi più grandi forniranno performance migliori.

Dimensione minima del volume

Astra Control Service fornisce volumi persistenti utilizzando una dimensione minima del volume di 300 GiB con il tipo di servizio CVS, anche se il PVC richiede una dimensione del volume inferiore. Ad esempio, se viene richiesto 20 GiB, Astra Control Service effettua automaticamente il provisioning di un volume da 300 GiB.

A causa di una limitazione, se un PVC richiede un volume compreso tra 700-999 GiB, Astra Control Service fornisce automaticamente una dimensione del volume di 1000 GiB.

Disco persistente di Google

Astra Control Service può utilizzare i driver CSI (Container Storage Interface) per interfacciarsi con Google Persistent Disk come backend di storage. Questo servizio fornisce storage a livello di blocco gestito da Google.

"Scopri di più su Google Persistent Disk".

"Scopri di più sui diversi livelli di performance di Google Persistent Disk".

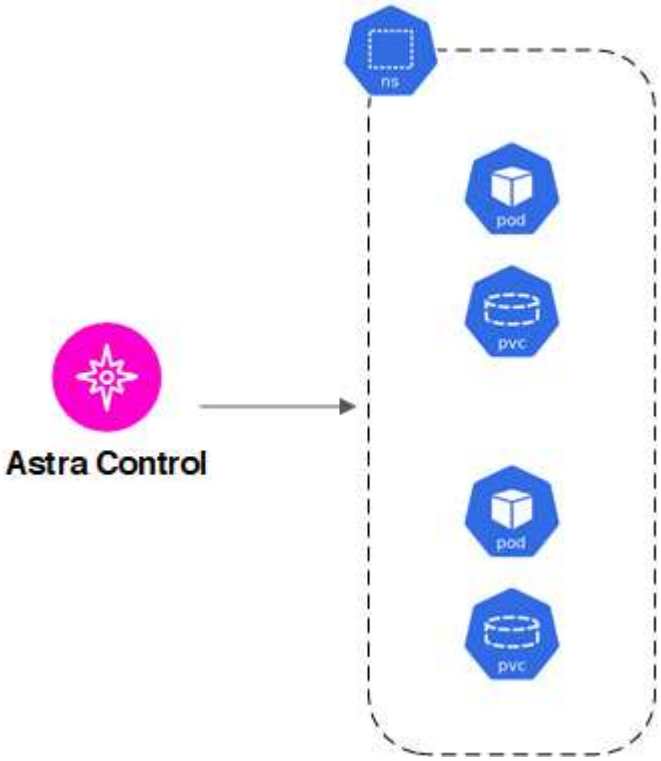
NetApp Cloud Volumes ONTAP

Per informazioni specifiche sulla configurazione di NetApp Cloud Volumes ONTAP, inclusi i consigli sulle performance, visitare il "Documentazione di NetApp Cloud Volumes ONTAP".

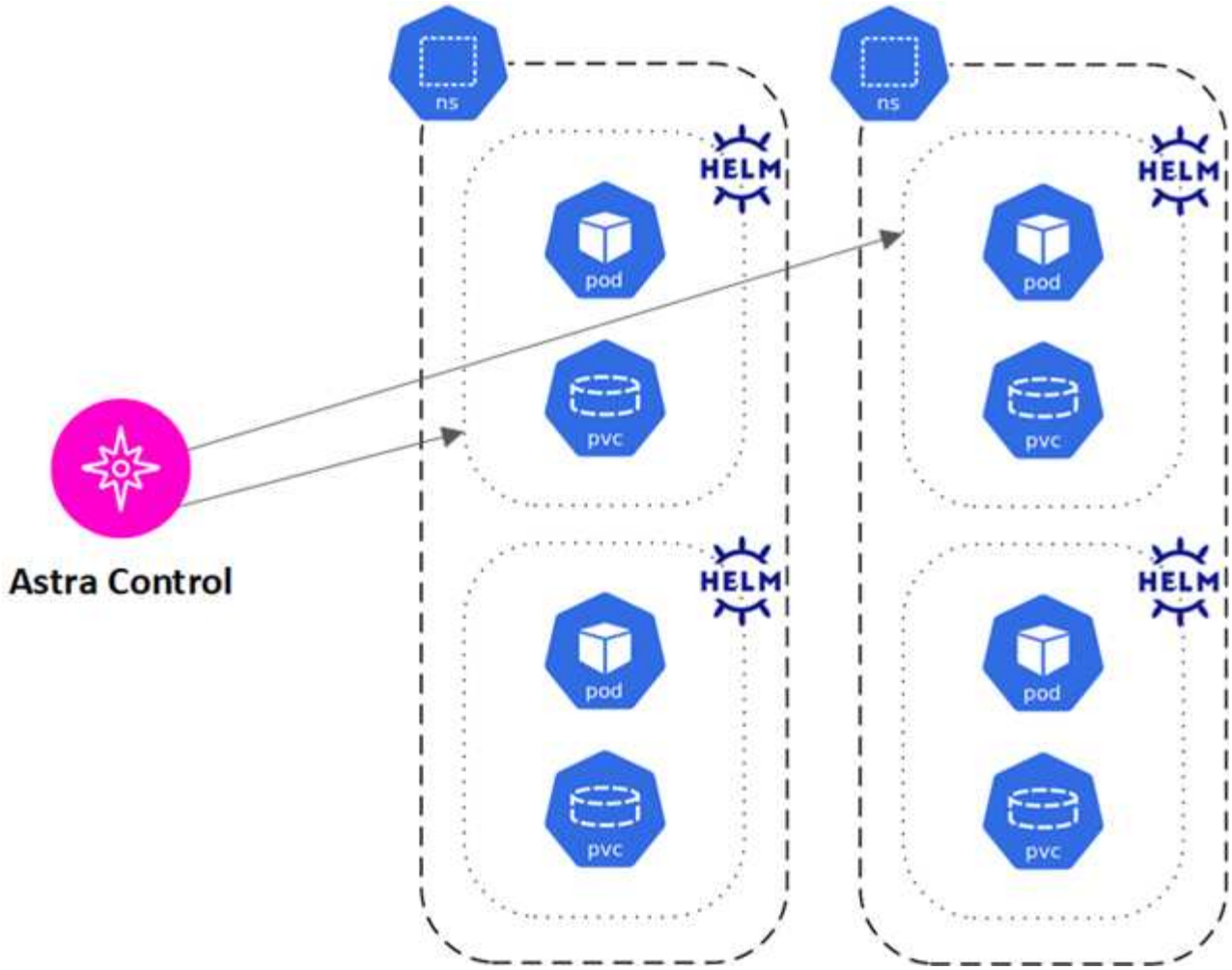
Gestione delle applicazioni

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:

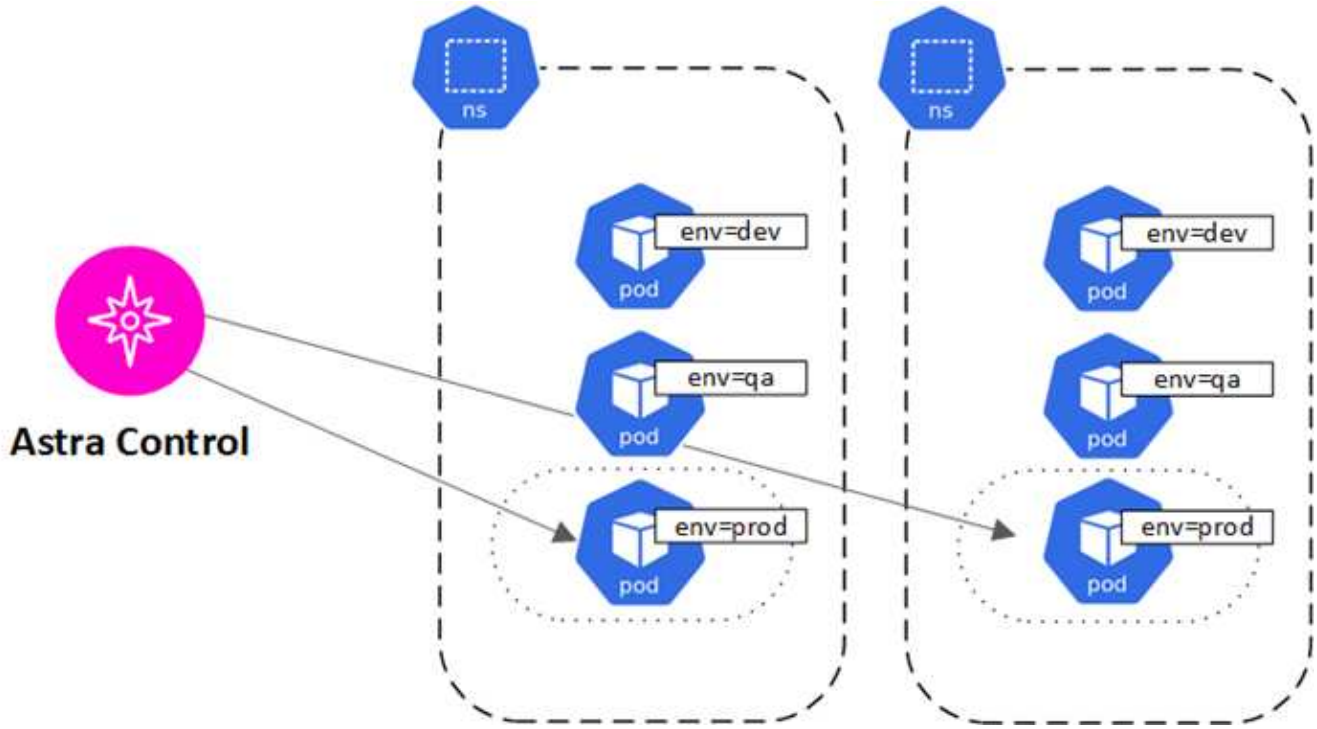
- Uno spazio dei nomi, che include tutte le risorse dello spazio dei nomi



- Una singola applicazione implementata all'interno di uno o più spazi dei nomi (in questo esempio viene utilizzato Helm 3)



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



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 **Owner** dispone delle autorizzazioni di amministratore e può eliminare gli account.
- Un **Admin** dispone delle autorizzazioni Member e può invitare altri utenti.
- Un **Member** può gestire completamente app e cluster.
- Un **Viewer** può visualizzare le risorse.

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

Informazioni sul marchio commerciale