Documentazione del servizio Astra Control

Astra Control Service

NetApp
April 24, 2024

Sommario

Documentazione del servizio Astra Control

Note di rilascio

Novità di Astra Control Service

NetApp aggiorna periodicamente Astra Control Service per offrire nuove funzionalità, miglioramenti e correzioni di bug.

14 marzo 2024

(Anteprima tecnica) flussi di lavoro Kubernetes dichiarativi

Questa release di Astra Control Center contiene una funzionalità dichiarativa di Kubernetes che consente di eseguire la gestione dei dati da una risorsa personalizzata (CR) di Kubernetes nativa.

Questa funzionalità è disponibile solo nell'istanza del programma EAP (Early Adopter Program) del servizio Astra Control. Per informazioni sulla partecipazione al programma EAP, contattare il rappresentante commerciale NetApp di zona.

Dopo l'installazione di "Connettore Astra" Nel cluster che si desidera gestire, è possibile eseguire le seguenti operazioni cluster basate su CR nell'interfaccia utente o da una CR:

- "Definire un'applicazione utilizzando una risorsa personalizzata"
- "Definire il bucket"
- "Protezione di un intero cluster"
- "Eseguire il backup dell'applicazione"
- "Creare un'istantanea"
- "Creare pianificazioni per snapshot o backup"
- "Ripristinare un'applicazione da uno snapshot o da un backup"

7 novembre 2023

Nuove funzionalità e supporto

- **Funzionalità di backup e ripristino per applicazioni con backend di storage ontap-nas-Economy con driver-backend**: Abilita le operazioni di backup e ripristino per `ontap-nas-economy` con alcuni "semplici passaggi".
- **Supporto di Astra Control Service per i cluster Red Hat OpenShift Container Platform on-premise**

  "Aggiungere un cluster"

- **Backup immutabili**: Astra Control ora supporta "backup di sola lettura inalterabili" come livello di sicurezza aggiuntivo contro malware e altre minacce.
- **Presentazione di Astra Control Provisioner**

  Con la release 23,10, Astra Control introduce un nuovo componente software chiamato Astra Control Provisioner, che sarà disponibile per tutti gli utenti di Astra Control con licenza. Astra Control Provivisioner offre l'accesso a un superset di funzionalità avanzate di gestione e provisioning dello storage oltre a quelle offerte da Astra Trident. Queste funzionalità sono disponibili per tutti i clienti Astra Control senza costi aggiuntivi.

- **Inizia con Astra Control Provisioner**
  È possibile "Abilita Astra Control Provisioner" Se hai installato e configurato il tuo ambiente per l'utilizzo di Astra Trident 23,10.
- **Funzionalità di Astra Control Provisioner**

  Le seguenti funzionalità sono disponibili con la release Astra Control Provisioner 23,10:

  - **Protezione backend dello storage avanzata con crittografia Kerberos 5**: È possibile migliorare la protezione dello storage "attivazione della crittografia" per il traffico tra il cluster gestito e il back-end dello storage. Astra Control Provisioner supporta la crittografia Kerberos 5 su connessioni NFSv4,1 da cluster Red Hat OpenShift a Azure NetApp Files e volumi ONTAP on-premise.
  - **Recupera i dati utilizzando uno snapshot**: Astra Control Provivisioner fornisce un rapido ripristino dei volumi in-place da uno snapshot utilizzando `TridentActionSnapshotRestore` (TASR) CR.
  - **Funzionalità di backup e ripristino per le applicazioni con `ontap-nas-economy` Backend di archiviazione con driver**: Come descritto sopra.

- **Supporto di Astra Control Service per Red Hat OpenShift Service su cluster AWS (ROSA)**

  "Aggiungere un cluster"

- **Supporto per la gestione delle applicazioni che utilizzano lo storage NVMe/TCP**
  Astra Control è ora in grado di gestire le applicazioni supportate da volumi persistenti connessi tramite NVMe/TCP.
- **I ganci di esecuzione sono disattivati per impostazione predefinita**: A partire da questa release, la funzionalità dei ganci di esecuzione può essere "attivato" o è disattivato per maggiore protezione (è disattivato per impostazione predefinita). Se non sono ancora stati creati ganci di esecuzione da utilizzare con Astra Control, è necessario "attivare la funzione ganci di esecuzione" per iniziare a creare ganci. Se sono stati creati dei ganci di esecuzione prima di questa release, la funzionalità dei ganci di esecuzione rimane attivata ed è possibile utilizzare i ganci normalmente.

2 ottobre 2023

Nuove funzionalità e supporto

Si tratta di una versione di correzione dei bug di minore entità.

27 luglio 2023

Nuove funzionalità e supporto

- Le operazioni di cloni ora supportano solo cloni attivi (stato corrente dell'applicazione gestita). Per clonare da uno snapshot o da un backup, utilizzare il flusso di lavoro di ripristino.

  "Ripristinare le applicazioni"

26 giugno 2023

Nuove funzionalità e supporto

- Gli abbonamenti a Azure Marketplace vengono fatturati ora anziché al minuto

  "Impostare la fatturazione"

30 maggio 2023

Nuove funzionalità e supporto

- Supporto per cluster Amazon EKS privati

  "Gestire i cluster privati da Astra Control Service"

- Supporto per la selezione della classe di storage di destinazione durante le operazioni di ripristino o clonazione

  "Ripristinare le applicazioni"

15 maggio 2023

Nuove funzionalità e supporto

Si tratta di una versione di correzione dei bug di minore entità.

25 aprile 2023

Nuove funzionalità e supporto

- Supporto per cluster Red Hat OpenShift privati

  "Gestire i cluster privati da Astra Control Service"

- Supporto per l'inclusione o l'esclusione delle risorse applicative durante le operazioni di ripristino

  "Ripristinare le applicazioni"

- Supporto per la gestione delle applicazioni solo dati

  "Inizia a gestire le app"

17 gennaio 2023

Nuove funzionalità e supporto

- Funzionalità migliorata di esecuzione hook con opzioni di filtraggio aggiuntive

  "Gestire gli hook di esecuzione delle applicazioni"

- Supporto per NetApp Cloud Volumes ONTAP come back-end per lo storage

  "Scopri di più su Astra Control"

22 novembre 2022

Nuove funzionalità e supporto

- Supporto per applicazioni che si estendono su più spazi dei nomi

  "Definire le applicazioni"

- Supporto per l'inclusione delle risorse cluster in una definizione applicativa

"Definire le applicazioni"

- Report avanzati sui progressi delle operazioni di backup, ripristino e clonazione

  "Monitorare le attività in esecuzione"

- Supporto per la gestione di cluster che hanno già una versione compatibile di Astra Trident installata

  "Inizia a gestire i cluster Kubernetes da Astra Control Service"

- Supporto per la gestione di più abbonamenti a provider cloud in un singolo account Astra Control Service

  "Gestire le istanze cloud"

- Supporto per l'aggiunta di cluster Kubernetes autogestiti ospitati in ambienti di cloud pubblico ad Astra Control Service

  "Inizia a gestire i cluster Kubernetes da Astra Control Service"

- La fatturazione per Astra Control Service viene ora misurata per namespace invece che per applicazione

  "Impostare la fatturazione"

- Supporto per l'iscrizione alle offerte basate sui termini di Astra Control Service tramite AWS Marketplace

  "Impostare la fatturazione"

Problemi noti e limitazioni

- "Problemi noti per questa release"
- "Limitazioni note per questa versione"

7 settembre 2022

Questa release include miglioramenti di stabilità e resilienza per l'infrastruttura Astra Control Service.

10 agosto 2022

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Workflow di gestione delle applicazioni migliorato i flussi di lavoro di gestione delle applicazioni migliorati offrono una maggiore flessibilità nella definizione delle applicazioni gestite da Astra Control.

  "Gestire le applicazioni"

- Supporto per i cluster Amazon Web Services Astra Control Service ora può gestire le applicazioni in esecuzione sui cluster ospitati in Amazon Elastic Kubernetes Service. È possibile configurare i cluster in modo che utilizzino Amazon Elastic Block Store o Amazon FSX per NetApp ONTAP come back-end dello storage.

  "Configurare Amazon Web Services"

- Hook di esecuzione migliorati oltre agli hook di esecuzione pre e post-snapshot, è ora possibile configurare i seguenti tipi di hook di esecuzione:

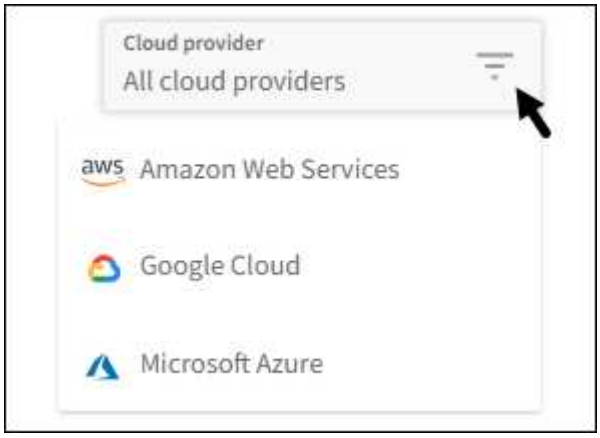
- Pre-backup
- Post-backup
- Post-ripristino

  Tra gli altri miglioramenti, Astra Control supporta ora l'utilizzo dello stesso script per più hook di esecuzione.

> In questa release sono stati rimossi gli hook di esecuzione predefiniti pre e post-snapshot forniti da NetApp per applicazioni specifiche. Se non fornisci i tuoi hook di esecuzione per le snapshot, Astra Control Service effettuerà snapshot coerenti con il crash solo a partire dal 4 agosto 2022. Visitare il "Repository NetApp Verda GitHub" per gli script hook di esecuzione di esempio che è possibile modificare per adattarsi al proprio ambiente.

"Gestire gli hook di esecuzione delle applicazioni"

- Supporto di Azure Marketplace ora puoi iscriverti a Astra Control Service tramite Azure Marketplace.
- Selezione del provider di cloud leggendo la documentazione di Astra Control Service, è ora possibile selezionare il provider di cloud in alto a destra nella pagina. Verrà visualizzata la documentazione relativa solo al cloud provider selezionato.



26 aprile 2022

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Namespace RBAC (Role-Based Access Control) Astra Control Service supporta ora l'assegnazione di vincoli di spazio dei nomi agli utenti Member o Viewer.

  "RBAC (role-based access control) dello spazio dei nomi"

- Supporto di Azure Active Directory Astra Control Service supporta i cluster AKS che utilizzano Azure Active Directory per l'autenticazione e la gestione delle identità.

  "Inizia a gestire i cluster Kubernetes da Astra Control Service"

- Supporto per cluster AKS privati è ora possibile gestire cluster AKS che utilizzano indirizzi IP privati.

  "Inizia a gestire i cluster Kubernetes da Astra Control Service"

- Rimozione del bucket da Astra Control è ora possibile rimuovere un bucket da Astra Control Service.

  "Rimuovere una benna"

14 dicembre 2021

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Nuove opzioni di back-end per lo storage
- Ripristino delle applicazioni in-place è ora possibile ripristinare uno snapshot, un clone o un backup di un'applicazione in uso ripristinando sullo stesso cluster e namespace.

  "Ripristinare le applicazioni"

- Eventi di script con hook di esecuzione Astra Control supporta script personalizzati che possono essere eseguiti prima o dopo l'esecuzione di un'istantanea di un'applicazione. Ciò consente di eseguire attività come la sospensione delle transazioni del database in modo che l'istantanea dell'applicazione di database sia coerente.

  "Gestire gli hook di esecuzione delle applicazioni"

- Applicazioni implementate dall'operatore Astra Control supporta alcune applicazioni quando vengono implementate con gli operatori.

  "Inizia a gestire le app"

- Entità del servizio con ambito del gruppo di risorse Astra Control Service supporta ora le entità del servizio che utilizzano un ambito del gruppo di risorse.

  "Creare un'entità del servizio Azure"

5 agosto 2021

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Centro di controllo Astra
  Astra Control è ora disponibile in un nuovo modello di implementazione. *Astra Control Center* è un software a gestione autonoma che puoi installare e utilizzare nel tuo data center, in modo da poter gestire il Lifecycle management delle applicazioni Kubernetes per i cluster Kubernetes on-premise.

  Per saperne di più, "Consultare la documentazione di Astra Control Center".

- Porta il tuo bucket personale ora puoi gestire i bucket che Astra utilizza per backup e cloni aggiungendo bucket aggiuntivi e modificando il bucket predefinito per i cluster Kubernetes nel tuo cloud provider.

  "Gestire i bucket"

2 giugno 2021

Questa versione include correzioni di bug e i seguenti miglioramenti al supporto di Google Cloud.

- Supporto per VPC condivisi è ora possibile gestire i cluster GKE nei progetti GCP con una configurazione di rete VPC condivisa.

- La dimensione del volume persistente per il tipo di servizio CVS Astra Control Service crea ora volumi persistenti con una dimensione minima di 300 GiB quando si utilizza il tipo di servizio CVS.

  "Scopri come Astra Control Service utilizza Cloud Volumes Service per Google Cloud come back-end dello storage per i volumi persistenti".

- Il supporto per sistemi operativi ottimizzati per container è ora supportato con i nodi di lavoro GKE. Oltre al supporto per Ubuntu.

  "Scopri di più sui requisiti del cluster GKE".

15 aprile 2021

Questa versione include le seguenti nuove funzioni e miglioramenti.

- Supporto per i cluster AKS Astra Control Service è ora in grado di gestire le applicazioni in esecuzione su un cluster Kubernetes gestito in Azure Kubernetes Service (AKS).

  "Scopri come iniziare".

- REST API l'API REST di Astra Control è ora disponibile per l'uso. L'API si basa sulle tecnologie moderne e sulle Best practice attuali.

  "Scopri come automatizzare la gestione del ciclo di vita dei dati delle applicazioni utilizzando l'API REST".

- L'abbonamento annuale Astra Control Service offre ora un *abbonamento Premium*.

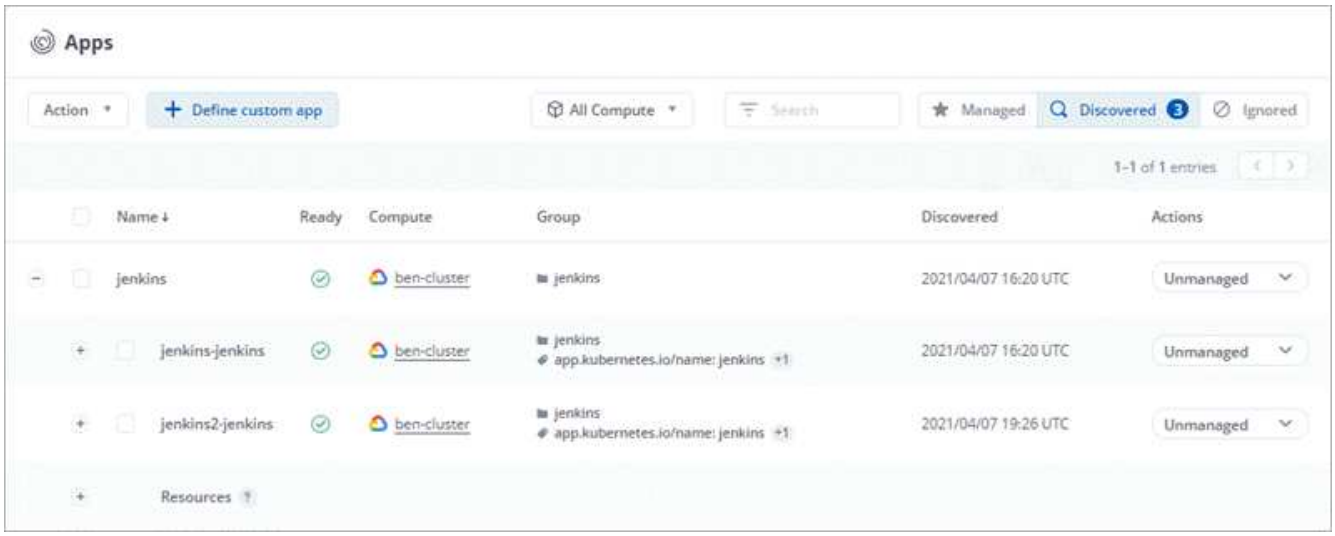
  Effettua il pre-pagamento a una tariffa scontata con un abbonamento annuale che ti consente di gestire fino a 10 app per *pacchetto applicativo*. Contatta il reparto vendite NetApp per acquistare tutti i pacchetti necessari per la tua organizzazione, ad esempio acquistando 3 pacchetti per gestire 30 applicazioni da Astra Control Service.

  Se gestisci un numero di applicazioni superiore a quello consentito dal tuo abbonamento annuale, ti verrà addebitato un importo di 0.005 dollari al minuto per applicazione (lo stesso di Premium PayGo).

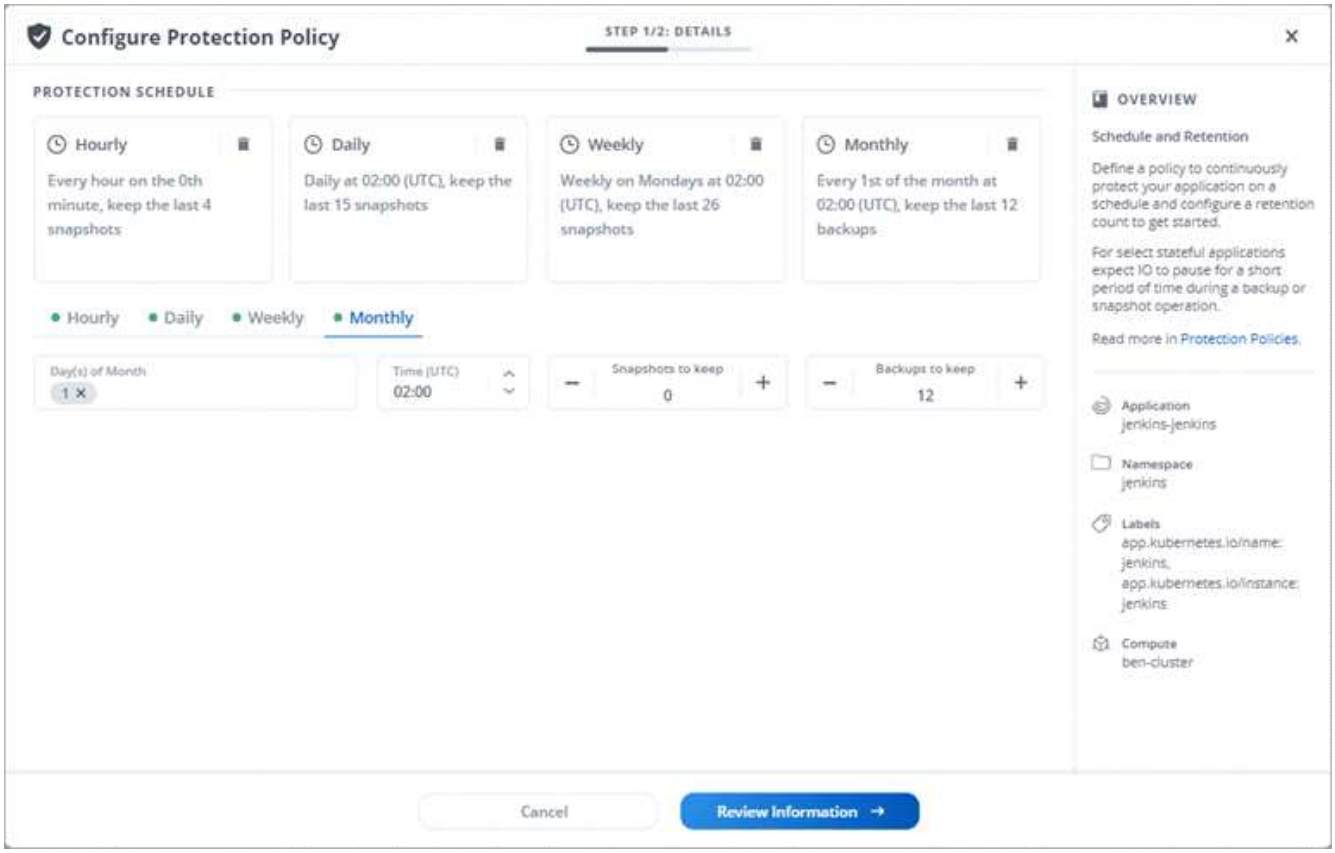
  "Scopri di più sui prezzi di Astra Control Service".

- Spazio dei nomi e visualizzazione delle applicazioni abbiamo migliorato la pagina delle applicazioni scoperte per mostrare meglio la gerarchia tra spazi dei nomi e applicazioni. È sufficiente espandere uno spazio dei nomi per visualizzare le applicazioni contenute in tale spazio dei nomi.

  "Scopri di più sulla gestione delle app".



- Miglioramenti dell'interfaccia utente le procedure guidate per la protezione dei dati sono state migliorate per una maggiore facilità di utilizzo. Ad esempio, abbiamo perfezionato la procedura guidata dei criteri di protezione per visualizzare più facilmente il programma di protezione definito dall'utente.



- Miglioramenti delle attività abbiamo semplificato la visualizzazione dei dettagli delle attività nel tuo account Astra Control.
  - Filtrare l'elenco delle attività in base all'applicazione gestita, al livello di severità, all'utente e all'intervallo di tempo.
  - Scarica l'attività dell'account Astra Control in un file CSV.
  - Visualizzare le attività direttamente dalla pagina Clusters o dalla pagina Apps dopo aver selezionato un cluster o un'applicazione.

"Scopri di più sulla visualizzazione dell'attività del tuo account".

1 marzo 2021

Astra Control Service ora supporta "*CVS* tipo di servizio" Con Cloud Volumes Service per Google Cloud. Oltre a supportare già il tipo di servizio *CVS-Performance*. Come promemoria, il servizio di controllo Astra utilizza Cloud Volumes Service per Google Cloud come back-end di storage per i volumi persistenti.

Questo miglioramento significa che Astra Control Service è ora in grado di gestire i dati delle applicazioni per i cluster Kubernetes in esecuzione in *any* "Area di Google Cloud in cui è supportato Cloud Volumes Service".

Se hai la flessibilità di scegliere tra le aree di Google Cloud, puoi scegliere CVS o CVS-Performance, a seconda dei tuoi requisiti di performance. "Scopri di più sulla scelta di un tipo di servizio".

25 gennaio 2021

Siamo lieti di annunciare che Astra Control Service è ora generalmente disponibile. Abbiamo incluso molti dei feedback ricevuti dalla versione Beta e abbiamo apportato alcuni miglioramenti significativi.

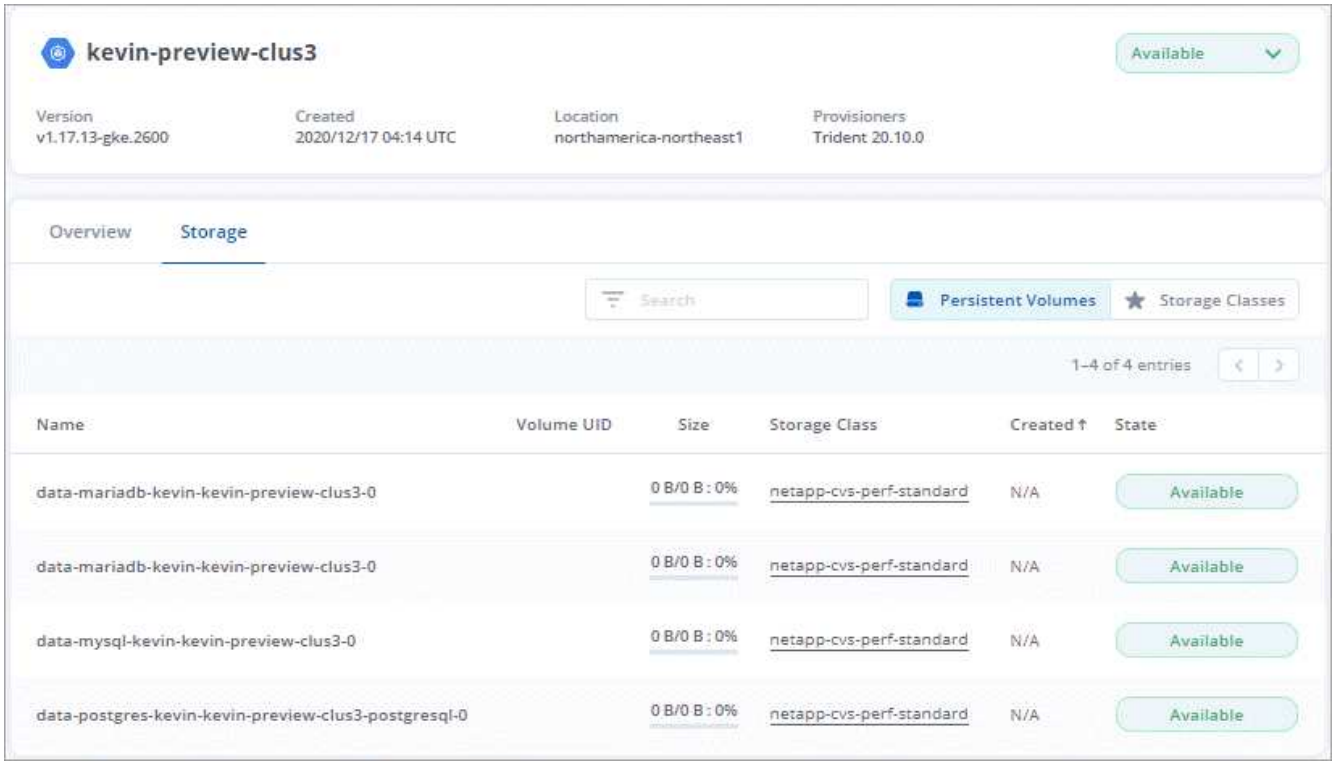
- È ora disponibile la fatturazione, che consente di passare dal piano gratuito al piano Premium. "Scopri di più sulla fatturazione".
- Astra Control Service ora crea volumi persistenti con una dimensione minima di 100 GiB quando si utilizza il tipo di servizio CVS-Performance.
- Astra Control Service è ora in grado di rilevare le applicazioni più rapidamente.
- È ora possibile creare ed eliminare account da soli.
- Abbiamo migliorato le notifiche quando Astra Control Service non può più accedere a un cluster Kubernetes.

  Queste notifiche sono importanti perché Astra Control Service non è in grado di gestire le applicazioni per i cluster disconnessi.

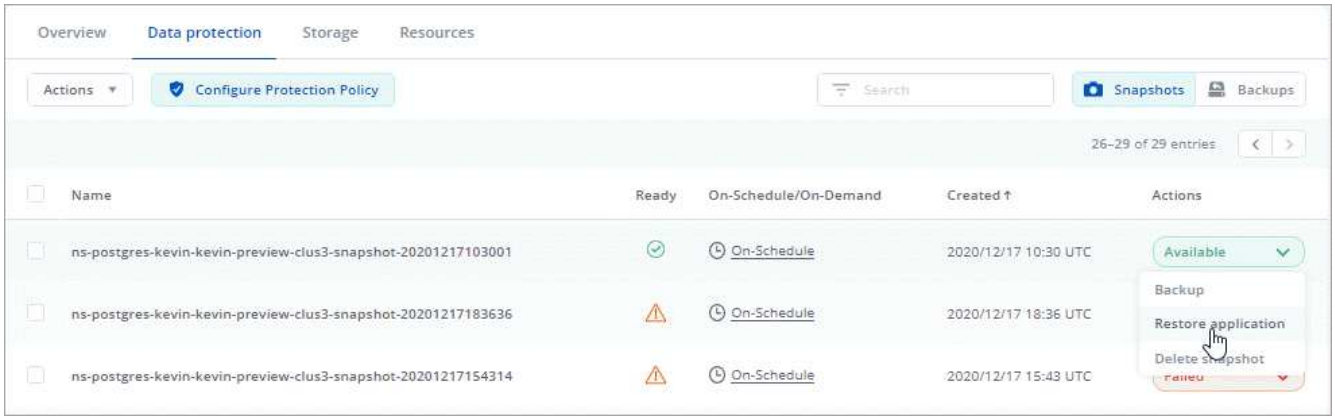
17 dicembre 2020 (aggiornamento Beta)

Ci siamo concentrati principalmente sulle correzioni dei bug per migliorare la tua esperienza, ma abbiamo apportato alcuni miglioramenti notevoli:

- Quando si aggiunge il primo calcolo di Kubernetes ad Astra Control Service, l'archivio di oggetti viene ora creato nella regione in cui risiede il cluster.
- I dettagli sui volumi persistenti sono ora disponibili quando si visualizzano i dettagli dello storage a livello di calcolo.



- È stata aggiunta un'opzione per ripristinare un'applicazione da uno snapshot o da un backup esistente.



- Se si elimina un cluster Kubernetes gestito da Astra Control Service, il cluster viene visualizzato in uno stato **removed**. È quindi possibile rimuovere il cluster da Astra Control Service.
- I proprietari degli account possono ora modificare i ruoli assegnati ad altri utenti.
- Abbiamo aggiunto una sezione per la fatturazione, che verrà attivata quando Astra Control Service viene rilasciato per la disponibilità generale (GA).

Problemi noti

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

I seguenti problemi noti riguardano la versione corrente:

Applicazioni

- Impossibile definire un’applicazione su uno spazio dei nomi che è stato cancellato e ricreato

Backup, ripristino e clonazione

- I cloni delle applicazioni non riescono a utilizzare una versione specifica di PostgreSQL
- I backup e le snapshot delle applicazioni non vengono eseguiti se la classe volumesnapshotclass viene aggiunta dopo la gestione di un cluster
- Le operazioni di ripristino in-place alle classi di storage economiche ontap-nas falliscono
- Il ripristino da un backup quando si utilizza la crittografia in-flight Kerberos può non riuscire
- I dati di backup rimangono nel bucket dopo l’eliminazione per bucket con criteri di conservazione scaduti

Altri problemi

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

Impossibile definire un’applicazione su uno spazio dei nomi che è stato cancellato e ricreato

Se si definisce un’applicazione con uno spazio dei nomi, si elimina lo spazio dei nomi e si reinstalla l’applicazione nello stesso spazio dei nomi, l’operazione non riesce e viene visualizzato un codice di errore 409. Per definire l’applicazione utilizzando lo spazio dei nomi ricreato, eliminare prima la vecchia istanza dell’applicazione.

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 backup e le snapshot delle applicazioni non vengono eseguiti se la classe volumesnapshotclass viene aggiunta dopo la gestione di un cluster

In questo scenario, i backup e le snapshot non vengono eseguiti correttamente e viene visualizzato un errore UI 500. Come soluzione, aggiornare l’elenco delle applicazioni.

Le operazioni di ripristino in-place alle classi di storage economiche ontap-nas falliscono

Se si esegue un ripristino sul posto di un’applicazione (ripristinando l’applicazione nello spazio dei nomi originale) e la classe di archiviazione dell’applicazione utilizza `ontap-nas-economy` driver, l’operazione di ripristino può non riuscire se la directory dello snapshot non è nascosta. Prima di eseguire il ripristino sul posto, seguire le istruzioni riportate in "Abilita backup e ripristino per le operazioni economiche a ontap-nas" per nascondere la directory dell’istantanea.

Il ripristino da un backup quando si utilizza la crittografia in-flight Kerberos può non riuscire

Quando si ripristina un’applicazione da un backup a un backend di storage che utilizza la crittografia in-flight Kerberos, l’operazione di ripristino potrebbe non riuscire. Questo problema non influisce sul ripristino da uno snapshot o sulla replica dei dati dell’applicazione tramite SnapMirror di NetApp.

> Quando si utilizza la crittografia in-flight Kerberos con volumi NFSv4, assicurarsi che i volumi NFSv4 stiano utilizzando le impostazioni corrette. Consultare la sezione Configurazione di dominio NetApp NFSv4 (pagina 13) della "Guida ai miglioramenti e alle Best practice di NetApp NFSv4".

I dati di backup rimangono nel bucket dopo l'eliminazione per bucket con criteri di conservazione scaduti

Se elimini il backup immutabile di un'app dopo che il criterio di conservazione del bucket è scaduto, il backup viene eliminato da Astra Control ma non dal bucket. Questo problema verrà risolto in una prossima release.

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

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

Limitazioni note

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

Limitazioni generali

Le seguenti limitazioni influiscono sulla gestione dei cluster Kubernetes da parte di Astra Control Service in qualsiasi implementazione di Kubernetes supportata.

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 Service 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.

La pagina Activity (attività) visualizza fino a 100,000 eventi

La pagina Astra Control Activity (attività di controllo Astra) può visualizzare fino a 100,000 eventi. Per visualizzare tutti gli eventi registrati, recuperare gli eventi utilizzando "API REST di Astra Control".

Limitazioni per la gestione dei cluster GKE

Le seguenti limitazioni si applicano alla gestione dei cluster Kubernetes in Google Kubernetes Engine (GKE).

Limitazioni della gestione delle applicazioni

Le seguenti limitazioni influiscono sulla gestione delle applicazioni da parte di Astra Control Service.

Non è possibile ripristinare collettivamente più applicazioni che utilizzano lo stesso namespace in un namespace diverso

Se si gestiscono più applicazioni che utilizzano lo stesso namespace (creando più definizioni di applicazioni in Astra Control), non è possibile ripristinare tutte le applicazioni in un singolo namespace diverso. È necessario ripristinare ogni applicazione nel proprio spazio dei nomi separato.

Astra Control non assegna automaticamente i bucket predefiniti per le istanze cloud

Astra Control non assegna automaticamente un bucket predefinito per nessuna istanza di cloud. È necessario impostare manualmente un bucket predefinito per un'istanza di cloud. Se non viene impostato un bucket predefinito, non sarà possibile eseguire operazioni di cloni tra due cluster.

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

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

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

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

I cloni delle applicazioni installate utilizzando gli operatori di riferimento pass-by possono fallire

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

- "Apache K8ssandra"

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

- "Ci Jenkins"
- "Cluster XtraDB Percona"

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

Durante le operazioni di cloni, le applicazioni che necessitano di una risorsa IngressClass o di webhook per funzionare correttamente non devono disporre di tali risorse già definite nel cluster di destinazione.

Limitazioni RBAC (Role-Based Access Control)

Le seguenti limitazioni si applicano al modo in cui Astra Control limita l'accesso degli utenti alle risorse o alle funzionalità.

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

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

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

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

Gli snapshot potrebbero non funzionare per i cluster Kubernetes 1.25 o versioni successive con determinate versioni di snapshot controller

Le snapshot per i cluster Kubernetes che eseguono la versione 1.25 o successiva possono non riuscire se sul cluster è installata la versione v1beta1 delle API del controller di snapshot.

Per risolvere il problema, eseguire le seguenti operazioni quando si aggiornano le installazioni esistenti di Kubernetes 1.25 o versioni successive:

1. Rimuovere tutti gli Snapshot CRD esistenti e tutti gli snapshot controller esistenti.
2. "Disinstallare Astra Trident".
3. "Installare gli snapshot CRD e lo snapshot controller".
4. "Installare la versione più recente di Astra Trident".
5. "Creare una classe VolumeSnapshotClass".

Inizia subito

Scopri di più su Astra Control

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

Caratteristiche

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

- Gestire automaticamente lo storage persistente
- Creazione di snapshot e backup on-demand basati sulle applicazioni
- Automatizzare le operazioni di backup e snapshot basate su policy
- Migrare applicazioni e dati da un cluster Kubernetes a un altro
- Replica delle applicazioni su un sistema remoto utilizzando la tecnologia NetApp SnapMirror (Astra Control Center)
- Clonare le applicazioni dallo staging alla produzione
- Visualizzare lo stato di salute e protezione dell'applicazione
- Utilizzare un'interfaccia utente Web 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 offre la gestione dei dati application-aware dei cluster Kubernetes in ambienti di cloud provider multipli, oltre ai cluster Kubernetes autogestiti.
- **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.

	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

	Servizio di controllo Astra	Centro di controllo Astra

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"

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 Managed Disks 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 questo nuovo ruolo di amministratore per installare link../concepts/architecture#astra-control-components[Astra Control Protivioner] nel cluster e per creare una o più classi di storage.
- Se utilizzi un'offerta di cloud storage NetApp come back-end dello storage, Astra Control Service utilizza Astra Control Provivisioner per il provisioning dei volumi persistenti per le tue app. Se si utilizzano dischi gestiti Amazon EBS o Azure come back-end dello storage, è necessario installare un driver CSI specifico del provider. Le istruzioni di installazione sono fornite in "Configurare Amazon Web Services" e. "Configurare Microsoft Azure con dischi gestiti Azure".
  - A questo punto, è possibile definire le applicazioni dal cluster. Il provisioning dei volumi persistenti sul back-end dello storage viene eseguito attraverso la 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 spazi dei nomi nel tuo account. Se si desidera gestire più di 10 spazi dei nomi, è necessario 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 una classe di storage configurata da Astra Control Provisioner con un backend di storage ONTAP.

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 e-mail e opzioni della community. Inoltre, puoi accedere agli articoli e alla documentazione della Knowledge base dalla dashboard di supporto all'interno del prodotto.

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

Ad alto livello, Astra Control Center funziona come segue:

- Astra Control Center viene installato nel proprio ambiente locale. Scopri di più su come "Installare Astra

Control Center".

- È possibile completare alcune attività di configurazione, come ad esempio:
  - Impostare la licenza.
  - Aggiungere il primo cluster.
  - Aggiungere il backend di storage rilevato quando si aggiunge il cluster.
  - Aggiungi un bucket di store di oggetti che memorizzerà i backup delle tue app.

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

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 della famiglia di prodotti NetApp Astra"
- "Documentazione di Astra Control Center"
- "Documentazione sull'API Astra Control"
- "Documentazione di Astra Trident"
- "Documentazione ONTAP"

Implementazioni Kubernetes supportate

Astra Control Service può gestire le applicazioni in esecuzione su un cluster Kubernetes gestito in Amazon Elastic Kubernetes Service (EKS) e i cluster gestiti da soli.

Astra Control Service è in grado di gestire le applicazioni in esecuzione su un cluster Kubernetes gestito in Google Kubernetes Engine (GKE) e i cluster gestiti autonomamente.

Astra Control Service può gestire le applicazioni in esecuzione su un cluster Kubernetes gestito in Azure Kubernetes Service (AKS) e i cluster gestiti da soli.

- "Scopri come configurare Amazon Web Services per Astra Control Service".
- "Scopri come configurare Google Cloud per Astra Control Service".
- "Scopri come configurare Microsoft Azure con Azure NetApp Files per il servizio di controllo Astra".
- "Scopri come configurare Microsoft Azure con dischi gestiti Azure per Astra Control Service".
- "Scopri come preparare i cluster autogestiti prima di aggiungerli ad Astra Control Service".

Avvio rapido per Astra Control Service

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

[Uno] Configura il tuo cloud provider

1. Google Cloud:
    - Esaminare i requisiti del cluster di Google Kubernetes Engine.
    - Acquista Cloud Volumes Service per Google Cloud da Google Cloud Marketplace.
    - Abilitare le API richieste.
    - Creare un account di servizio e una chiave dell'account di servizio.
    - Imposta il peering di rete dal tuo VPC a Cloud Volumes Service per Google Cloud.

      "Scopri di più sui requisiti di Google Cloud".

2. Servizi Web Amazon:
    - Esaminare i requisiti del cluster di Amazon Web Services.
    - Crea un account Amazon.
    - Installare la CLI di Amazon Web Services.
    - Creare un utente IAM.
    - Creare e allegare un criterio di autorizzazioni.
    - Salvare le credenziali per l'utente IAM.

      "Scopri di più sui requisiti di Amazon Web Services".

3. Microsoft Azure:
    - Esaminate i requisiti del cluster di Azure Kubernetes Service per il backend di storage che intendete utilizzare.

      "Scopri di più sui requisiti di Microsoft Azure e Azure NetApp Files".

   "Scopri di più sui requisiti dei dischi gestiti di Microsoft Azure e Azure".

Se stai gestendo il tuo cluster e non è ospitato da un cloud provider, esamina i requisiti per i cluster autogestiti. "Scopri di più sui requisiti del cluster a gestione automatica".

[Due] Completare la registrazione di Astra Control

1. Creare un "NetApp BlueXP" account.
2. Specifica il tuo ID email NetApp BlueXP durante la creazione dell'account Astra Control "Dalla pagina del prodotto Astra Control".

"Scopri di più sul processo di registrazione".

[Tre] Aggiungere cluster ad Astra Control

Dopo aver effettuato l'accesso, selezionare **Add cluster** (Aggiungi cluster) per iniziare a gestire il cluster con Astra Control.

"Scopri di più sull'aggiunta di cluster".

Configura il tuo cloud provider

Configurare Amazon Web Services

Sono necessari alcuni passaggi per preparare il tuo progetto Amazon Web Services prima di poter gestire i cluster Amazon Elastic Kubernetes Service (EKS) con Astra Control Service.

Avvio rapido per la configurazione di Amazon Web Services

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

[Uno] Consulta i requisiti del servizio Astra Control per Amazon Web Services

Assicurarsi che i cluster siano integri e che eseguano una versione supportata di Kubernetes, che i nodi di lavoro siano online e che eseguano Linux o Windows e altro ancora. Scopri di più su questo passaggio.

[Due] Crea un account Amazon

Se non disponi già di un account Amazon, devi crearne uno per poter utilizzare EKS. Scopri di più su questo passaggio.

[Tre] Installare la CLI di Amazon Web Services

Installare la CLI AWS in modo da poter gestire AWS dalla riga di comando. Seguire le istruzioni dettagliate.

[Quattro] Facoltativo: Creare un utente IAM

Creare un utente Amazon Identity and Access Management (IAM). Puoi anche saltare questo passaggio e utilizzare un utente IAM esistente con Astra Control Service.

Leggi le istruzioni dettagliate.

[Cinque] Creare e allegare un criterio di autorizzazioni

Creare una policy con le autorizzazioni richieste per Astra Control Service per interagire con l'account AWS.

Leggi le istruzioni dettagliate.

[Sei] Salvare le credenziali per l'utente IAM

Salvare le credenziali per l'utente IAM in modo da poter importare le credenziali in Astra Control Service.

Leggi le istruzioni dettagliate.

Requisiti del cluster EKS

Un cluster Kubernetes deve soddisfare i seguenti requisiti per consentirne il rilevamento e la gestione da Astra Control Service.

Versione di Kubernetes

Un cluster deve eseguire una versione di Kubernetes compresa tra 1,25 e 1,28.

Tipo di immagine

Il tipo di immagine per ciascun nodo di lavoro deve essere Linux.

Stato del cluster

I cluster devono essere in esecuzione in uno stato integro e avere almeno un nodo di lavoro online senza nodi di lavoro in uno stato di errore.

Astra Control provisioner

Astra Control Provivisioner e un controller delle snapshot esterno sono necessari per le operazioni con backend di storage. Per attivare queste operazioni, procedere come segue:

1. "Installare gli snapshot CRD e lo snapshot controller".
2. "Abilita Astra Control Provisioner".
3. "Creare una classe VolumeSnapshotClass".

Driver CSI per Amazon Elastic Block Store (EBS)

Se si utilizza il backend dello storage Amazon EBS, è necessario installare il driver CSI (Container Storage Interface) per EBS (non viene installato automaticamente).

Per istruzioni sull'installazione del driver CSI, fare riferimento alla procedura.

Installare uno snap-shot esterno

Se non l'hai già fatto, "Installare gli snapshot CRD e lo snapshot controller".

Installare il driver CSI come add-on Amazon EKS

1. Creare il ruolo IAM del driver CSI Amazon EBS per gli account del servizio. Seguire le istruzioni "Nella documentazione Amazon", Utilizzando i comandi CLI di AWS nelle istruzioni.
2. Aggiungere il componente aggiuntivo Amazon EBS CSI utilizzando il seguente comando AWS CLI, sostituendo le informazioni tra parentesi <> con valori specifici per il proprio ambiente. Sostituire <DRIVER_ROLE> con il nome del ruolo del driver EBS CSI creato nel passaggio precedente:

```
aws eks create-addon \
  --cluster-name <CLUSTER_NAME> \
  --addon-name aws-ebs-csi-driver \
  --service-account-role-arn
arn:aws:iam::<ACCOUNT_ID>:role/<DRIVER_ROLE>
```

Configurare la classe di storage EBS

1. Clonare il repository GitHub del driver CSI di Amazon EBS nel sistema.

```
git clone https://github.com/kubernetes-sigs/aws-ebs-csi-
driver.git
```

2. Accedere alla directory di esempio del provisioning dinamico.

```
cd aws-ebs-csi-driver/examples/kubernetes/dynamic-provisioning/
```

3. Implementare la classe di storage ebs-sc e l'attestazione di volume persistente ebs-claim dalla directory manifests.

```
kubectl apply -f manifests/storageclass.yaml
kubectl apply -f manifests/claim.yaml
```

4. Descrivere la classe di storage ebs-sc.

```
kubectl describe storageclass ebs-sc
```

Viene visualizzato un output che descrive gli attributi della classe di storage.

Crea un account Amazon

Se non disponi già di un account Amazon, devi crearne uno per attivare la fatturazione per Amazon EKS.

Fasi

1. Accedere alla "Pagina principale Amazon" , Selezionare **Accedi** in alto a destra e selezionare **inizia qui**.
2. Seguire le istruzioni per creare un account.

Installare la CLI di Amazon Web Services

Installare la CLI AWS in modo da poter gestire le risorse AWS dalla riga di comando.

Fase

1. Passare a. "Introduzione a AWS CLI" E seguire le istruzioni per installare l'interfaccia CLI.

Facoltativo: Creare un utente IAM

Creare un utente IAM in modo da poter utilizzare e gestire i servizi e le risorse AWS con maggiore sicurezza. È inoltre possibile saltare questo passaggio e utilizzare un utente IAM esistente con Astra Control Service.

Fase

1. Passare a. "Creazione di utenti IAM" E seguire le istruzioni per creare un utente IAM.

Creare e allegare un criterio di autorizzazioni

Creare una policy con le autorizzazioni richieste per Astra Control Service per interagire con l'account AWS.

Fasi

1. Creare un nuovo file chiamato `policy.json`.
2. Copiare il seguente contenuto JSON nel file:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricData",
                "fsx:DescribeVolumes",
                "ec2:DescribeRegions",
                "s3:CreateBucket",
                "s3:ListBucket",
                "s3:PutObject",
                "s3:GetObject",
                "iam:SimulatePrincipalPolicy",
                "s3:ListAllMyBuckets",
                "eks:DescribeCluster",
                "eks:ListNodegroups",
                "eks:DescribeNodegroup",
                "eks:ListClusters",
                "iam:GetUser",
                "s3:DeleteObject",
                "s3:DeleteBucket",
                "autoscaling:DescribeAutoScalingGroups"
            ],
            "Resource": "*"
        }
    ]
}
```

3. Creare la policy:

```
POLICY_ARN=$(aws iam create-policy  --policy-name <policy-name> --policy
-document file://policy.json  --query='Policy.Arn' --output=text)
```

4. Allegare il criterio all'utente IAM. Sostituire `<IAM-USER-NAME>` Con il nome utente dell'utente IAM creato o con un utente IAM esistente:

```
aws iam attach-user-policy --user-name <IAM-USER-NAME> --policy-arn
=$POLICY_ARN
```

Salvare le credenziali per l'utente IAM

Salvare le credenziali per l'utente IAM in modo da rendere Astra Control Service consapevole dell'utente.

Fasi

1. Scarica le credenziali. Sostituire `<IAM-USER-NAME>` Con il nome utente dell'utente IAM che si desidera utilizzare:

```
aws iam create-access-key --user-name <IAM-USER-NAME> --output json >
credential.json
```

Risultato

Il `credential.json` Il file viene creato ed è possibile importare le credenziali in Astra Control Service.

Configurare Google Cloud

Sono necessari alcuni passaggi per preparare il tuo progetto Google Cloud prima di poter gestire i cluster di Google Kubernetes Engine con Astra Control Service.

> Se non si inizia a utilizzare Google Cloud Volumes Service per Google Cloud come back-end di storage ma si prevede di utilizzarlo in un secondo momento, è necessario completare i passaggi necessari per configurare Google Cloud Volumes Service per Google Cloud ora. La creazione di un account di servizio in un secondo momento implica la perdita di accesso ai bucket di storage esistenti.

Avvio rapido per la configurazione di Google Cloud

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

[Uno] Consulta i requisiti del servizio Astra Control per Google Kubernetes Engine

Assicurarsi che i cluster siano integri e che eseguano una versione di Kubernetes supportata, che i nodi di lavoro siano online e che eseguano un tipo di immagine supportato e altro ancora. Scopri di più su questo passaggio.

[Due] (Facoltativo): Acquista Cloud Volumes Service per Google Cloud

Se si intende utilizzare Cloud Volumes Service per Google Cloud come back-end di storage, accedere alla pagina NetApp Cloud Volumes Service nel Google Cloud Marketplace e selezionare Acquista. Scopri di più su questo passaggio.

[Tre] Abilita le API nel tuo progetto Google Cloud

Abilitare le seguenti API di Google Cloud:

- Motore di Google Kubernetes
- Cloud Storage
- API JSON per lo storage cloud

- Utilizzo del servizio
- API Cloud Resource Manager
- NetApp Cloud Volumes Service
  - Richiesto per Cloud Volumes Service per Google Cloud
  - Opzionale (ma consigliato) per Google Persistent Disk
- API Service Consumer Management
- API di Service Networking
- API di gestione dei servizi

Seguire le istruzioni dettagliate.

[Quattro] Creare un account di servizio con le autorizzazioni richieste

Creare un account di servizio Google Cloud con le seguenti autorizzazioni:

- Amministratore del motore di Kubernetes
- NetApp Cloud Volumes Admin
  - Richiesto per Cloud Volumes Service per Google Cloud
  - Opzionale (ma consigliato) per Google Persistent Disk
- Amministratore dello storage
- Visualizzatore utilizzo servizio
- Visualizzatore di Compute Network

Leggi le istruzioni dettagliate.

[Cinque] Creare una chiave dell'account del servizio

Creare una chiave per l'account del servizio e salvare il file delle chiavi in una posizione sicura. Seguire le istruzioni dettagliate.

[Sei] (Facoltativo): Impostare il peering di rete per il VPC

Se intendi utilizzare Cloud Volumes Service per Google Cloud come back-end di storage, imposta il peering di rete dal tuo VPC a Cloud Volumes Service per Google Cloud. Seguire le istruzioni dettagliate.

Requisiti del cluster GKE

Un cluster Kubernetes deve soddisfare i seguenti requisiti per consentirne il rilevamento e la gestione da Astra Control Service. Alcuni di questi requisiti si applicano solo se si prevede di utilizzare Cloud Volumes Service per Google Cloud come back-end di storage.

Versione di Kubernetes

Un cluster deve eseguire una versione di Kubernetes compresa tra 1,26 e 1,28.

Tipo di immagine

Il tipo di immagine per ciascun nodo di lavoro deve essere `COS_CONTAINERD`.

Stato del cluster

I cluster devono essere in esecuzione in uno stato integro e avere almeno un nodo di lavoro online senza nodi di lavoro in uno stato di errore.

Regione di Google Cloud

Se si prevede di utilizzare Cloud Volumes Service per Google Cloud come backend di storage, i cluster devono essere eseguiti in un "Area di Google Cloud in cui è supportato Cloud Volumes Service per Google Cloud." Si noti che Astra Control Service supporta entrambi i tipi di servizio: CVS e CVS-Performance. Come Best practice, devi scegliere una regione che supporti Cloud Volumes Service per Google Cloud, anche se non la utilizzi come back-end di storage. In questo modo sarà più semplice utilizzare Cloud Volumes Service per Google Cloud come back-end di storage in futuro, se i requisiti di performance cambiano.

Networking

Se si intende utilizzare Cloud Volumes Service per Google Cloud come backend di storage, il cluster deve risiedere in un VPC con Cloud Volumes Service per Google Cloud. Questo passaggio è descritto di seguito.

Cluster privati

Se il cluster è privato, il "reti autorizzate" Deve consentire l'indirizzo IP di Astra Control Service:

52.188.218.166/32

Modalità operativa per un cluster GKE

Si consiglia di utilizzare la modalità operativa standard. La modalità Autopilot non è stata testata al momento. "Scopri di più sulle modalità operative".

Pool di storage

Se si utilizza NetApp Cloud Volumes Service come backend di storage con il tipo di servizio CVS, è necessario configurare i pool di storage prima di poter eseguire il provisioning dei volumi. Fare riferimento a. "Tipo di servizio, classi di storage e dimensione PV per cluster GKE" per ulteriori informazioni.

Opzionale: Acquista Cloud Volumes Service per Google Cloud

Il servizio di controllo Astra può utilizzare Cloud Volumes Service per Google Cloud come back-end di storage per i volumi persistenti. Se intendi utilizzare questo servizio, devi acquistare Cloud Volumes Service per Google Cloud da Google Cloud Marketplace per abilitare la fatturazione per volumi persistenti.

Fase

1. Accedere alla "Pagina Cloud Volumes Service di NetApp" In Google Cloud Marketplace, selezionare **Purchase** (Acquista) e seguire le istruzioni.

   "Seguire le istruzioni dettagliate nella documentazione di Google Cloud per acquistare e attivare il servizio".

Abilitare le API nel progetto

Il progetto richiede autorizzazioni per accedere a specifiche API di Google Cloud. Le API vengono utilizzate per interagire con le risorse cloud di Google, come i cluster GKE e lo storage NetApp Cloud Volumes Service.

Fase

1. "Utilizzare la console Google Cloud o la CLI gcloud per abilitare le seguenti API":
   - Motore di Google Kubernetes

- Cloud Storage
- API JSON per lo storage cloud
- Utilizzo del servizio
- API Cloud Resource Manager
- NetApp Cloud Volumes Service (richiesto per Cloud Volumes Service per Google Cloud)
- API Service Consumer Management
- API di Service Networking
- API di gestione dei servizi

Il video seguente mostra come abilitare le API dalla console Google Cloud.

► https://docs.netapp.com/it-it/astra-control-service/media/get-started/video-enable-gcp-apis.mp4 *(video)*

Creare un account di servizio

Astra Control Service utilizza un account di servizio Google Cloud per facilitare la gestione dei dati dell'applicazione Kubernetes per conto dell'utente.

Fasi

1. Accedere a Google Cloud e. "creare un account di servizio utilizzando la console, il comando gcloud o un altro metodo preferito".
2. Assegnare all'account del servizio i seguenti ruoli:
   - **Kubernetes Engine Admin** - utilizzato per elencare i cluster e creare l'accesso amministratore per gestire le applicazioni.
   - **NetApp Cloud Volumes Admin** - utilizzato per gestire lo storage persistente per le applicazioni.
   - **Storage Admin** - utilizzato per gestire bucket e oggetti per il backup delle applicazioni.
   - **Visualizzatore utilizzo servizio** - consente di verificare se le API Cloud Volumes Service per Google Cloud richieste sono attivate.
   - **Visualizzatore di rete di calcolo** - utilizzato per verificare se il VPC Kubernetes è autorizzato a raggiungere Cloud Volumes Service per Google Cloud.

Se si desidera utilizzare gcloud, è possibile seguire i passaggi dall'interfaccia Astra Control. Selezionare **account > credenziali > Aggiungi credenziali**, quindi selezionare **istruzioni**.

Se si desidera utilizzare la console Google Cloud, il video seguente mostra come creare l'account del servizio dalla console.

► https://docs.netapp.com/it-it/astra-control-service/media/get-started/video-create-gcp-service-account.mp4

(video)

Configurare l’account di servizio per un VPC condiviso

Per gestire i cluster GKE che risiedono in un progetto, ma utilizzano un VPC di un progetto diverso (un VPC condiviso), è necessario specificare l’account del servizio Astra come membro del progetto host con il ruolo **Compute Network Viewer**.

Fasi

1. Dalla console di Google Cloud, accedere a **IAM & Admin** e selezionare **Service Accounts**.
2. Individuare l’account di servizio Astra "le autorizzazioni richieste" quindi copiare l’indirizzo e-mail.
3. Accedere al progetto host e selezionare **IAM & Admin** > **IAM**.
4. Selezionare **Aggiungi** e aggiungere una voce per l’account del servizio.
   a. **Nuovi membri**: Inserire l’indirizzo e-mail dell’account del servizio.
   b. **Ruolo**: Selezionare **Compute Network Viewer**.
   c. Selezionare **Salva**.

Risultato

L’aggiunta di un cluster GKE utilizzando un VPC condiviso funziona perfettamente con Astra.

Creare una chiave dell’account del servizio

Invece di fornire un nome utente e una password ad Astra Control Service, fornirai una chiave account del servizio quando Aggiungi il tuo primo cluster. Astra Control Service utilizza la chiave dell’account del servizio per stabilire l’identità dell’account del servizio appena configurato.

La chiave dell’account del servizio è in formato non crittografato e memorizzata nel formato JSON (JavaScript Object Notation). Contiene informazioni sulle risorse GCP a cui si dispone dei diritti di accesso.

È possibile visualizzare o scaricare il file JSON solo quando si crea la chiave. Tuttavia, è possibile creare una nuova chiave in qualsiasi momento.

Fasi

1. Accedere a Google Cloud e. "creare una chiave dell’account di servizio utilizzando la console, il comando gcloud o un altro metodo preferito".
2. Quando richiesto, salvare il file delle chiavi dell’account di servizio in una posizione sicura.

Il video seguente mostra come creare la chiave dell’account di servizio dalla console Google Cloud.

► https://docs.netapp.com/it-it/astra-control-service/media/get-started/video-create-gcp-service-account-

key.mp4 *(video)*

Opzionale: Configurare il peering di rete per il VPC

Se intendi utilizzare Cloud Volumes Service per Google Cloud come servizio di back-end per lo storage, il passaggio finale è configurare il peering di rete dal tuo VPC a Cloud Volumes Service per Google Cloud.

Il modo più semplice per configurare il peering di rete è ottenere i comandi gcloud direttamente da Cloud Volumes Service. I comandi sono disponibili da Cloud Volumes Service quando si crea un nuovo file system.

Fasi

1. "Vai alle mappe delle regioni globali BlueXP di NetApp" E identificare il tipo di servizio che si utilizza nell'area di Google Cloud in cui risiede il cluster.

   Cloud Volumes Service offre due tipi di servizio: CVS e CVS-Performance. "Scopri di più su questi tipi di servizi".

2. "Vai a Cloud Volumes in Google Cloud Platform".
3. Nella pagina **volumi**, selezionare **Crea**.
4. In **tipo di servizio**, selezionare **CVS** o **CVS-Performance**.

   Devi scegliere il tipo di servizio corretto per la tua area geografica Google Cloud. Questo è il tipo di servizio identificato al punto 1. Dopo aver selezionato un tipo di servizio, l'elenco delle regioni nella pagina viene aggiornato con le regioni in cui tale tipo di servizio è supportato.

   Dopo questa fase, è sufficiente inserire le informazioni di rete per ottenere i comandi.

5. In **Regione**, selezionare la propria regione e zona.
6. In **Dettagli rete**, selezionare il VPC.

   Se non hai configurato il peering di rete, verrà visualizzata la seguente notifica:

7. Selezionare il pulsante per visualizzare i comandi di configurazione del peering di rete.
8. Copiare i comandi ed eseguirli in Cloud Shell.

   Per ulteriori informazioni sull'utilizzo di questi comandi, fare riferimento a. "Guida rapida per Cloud Volumes Service per GCP".

"Scopri di più sulla configurazione dell'accesso ai servizi privati e sulla configurazione del peering di rete".

9. Al termine, selezionare Annulla nella pagina **Crea file system**.

   Abbiamo iniziato a creare questo volume solo per ottenere i comandi per il peering di rete.

Configurare Microsoft Azure con Azure NetApp Files

Sono necessari alcuni passaggi per preparare l'abbonamento a Microsoft Azure prima di poter gestire i cluster di servizi Azure Kubernetes con Astra Control Service. Seguire queste istruzioni se si intende utilizzare Azure NetApp Files come backend di storage.

Avvio rapido per la configurazione di Azure

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

[Uno] Esaminare i requisiti del servizio di controllo Astra per Azure Kubernetes Service

Assicurarsi che i cluster siano integri e che eseguano una versione supportata di Kubernetes, che i pool di nodi siano online e che eseguano Linux e altro ancora. Scopri di più su questo passaggio.

[Due] Iscriviti a Microsoft Azure

Creare un account Microsoft Azure. Scopri di più su questo passaggio.

[Tre] Registrati a Azure NetApp Files

Registrare il NetApp Resource Provider. Scopri di più su questo passaggio.

[Quattro] Creare un account NetApp

Accedere a Azure NetApp Files nel portale Azure e creare un account NetApp. Scopri di più su questo passaggio.

[Cinque] Configurare i pool di capacità

Configurare uno o più pool di capacità per i volumi persistenti. Scopri di più su questo passaggio.

[Sei] Delegare una subnet a Azure NetApp Files

Delegare una subnet a Azure NetApp Files in modo che il servizio di controllo Astra possa creare volumi persistenti in tale subnet. Scopri di più su questo passaggio.

[Sette] Creare un'entità del servizio Azure

Creare un'entità del servizio Azure con il ruolo di collaboratore. Scopri di più su questo passaggio.

[Otto] Opzionale: Configurare la ridondanza per i bucket di backup di Azure

Per impostazione predefinita, i bucket Astra Control Service utilizzati per memorizzare i backup di Azure Kubernetes Service utilizzano l'opzione di ridondanza LRS (Redundant Storage) locale. Come passaggio opzionale, è possibile configurare un livello di ridondanza più duraturo per i bucket Azure. Scopri di più su questo passaggio.

Azure Kubernetes Service Cluster Requirements

Un cluster Kubernetes deve soddisfare i seguenti requisiti per consentirne il rilevamento e la gestione da Astra Control Service.

Versione di Kubernetes

I cluster devono eseguire Kubernetes versione 1,26 - 1,28.

Tipo di immagine

Il tipo di immagine per tutti i pool di nodi deve essere Linux.

Stato del cluster

I cluster devono essere in esecuzione in uno stato integro e avere almeno un nodo di lavoro online senza nodi di lavoro in uno stato di errore.

Regione di Azure

I cluster devono risiedere in una regione in cui è disponibile Azure NetApp Files. "Visualizza i prodotti Azure per regione".

Iscrizione

I cluster devono risiedere in un abbonamento in cui Azure NetApp Files è attivato. Scegli un abbonamento quando lo desideri Registrati a Azure NetApp Files.

VNET

Considerare i seguenti requisiti VNET:

- I cluster devono risiedere in una rete virtuale con accesso diretto a una subnet delegata da Azure NetApp Files. Scopri come configurare una subnet delegata.
- Se i cluster Kubernetes si trovano in un VNET collegato alla subnet delegata Azure NetApp Files di un altro VNET, entrambi i lati della connessione di peering devono essere in linea.
- Tenere presente che il limite predefinito per il numero di IP utilizzati in una rete virtuale (inclusi i VNet con peering immediato) con Azure NetApp Files è 1,000. "Visualizza i limiti delle risorse Azure NetApp Files".

  Se sei vicino al limite, hai due opzioni:

  - È possibile "inviare una richiesta di aumento del limite". Per assistenza, contatta il tuo rappresentante NetApp.
  - Quando si crea un nuovo cluster Amazon Kubernetes Service (AKS), specificare una nuova rete per il cluster. Una volta creata la nuova rete, eseguire il provisioning di una nuova subnet e delegare la subnet a Azure NetApp Files.

Iscriviti a Microsoft Azure

Se non disponi di un account Microsoft Azure, inizia iscrivendoti a Microsoft Azure.

Fasi

1. Accedere alla "Pagina di iscrizione Azure" Per iscriversi al servizio Azure.
2. Selezionare un piano e seguire le istruzioni per completare l'abbonamento.

Registrati a Azure NetApp Files

Ottieni l'accesso a Azure NetApp Files registrando il provider di risorse NetApp.

Fasi

1. Accedere al portale Azure.
2. "Seguire la documentazione di Azure NetApp Files per registrare il provider di risorse NetApp".

Creare un account NetApp

Creare un account NetApp in Azure NetApp Files.

Fase

1. "Seguire la documentazione di Azure NetApp Files per creare un account NetApp dal portale Azure".

Impostare un pool di capacità

Sono necessari uno o più pool di capacità per consentire ad Astra Control Service di eseguire il provisioning di volumi persistenti in un pool di capacità. Astra Control Service non crea pool di capacità per te.

Durante la configurazione dei pool di capacità per le applicazioni Kubernetes, prendere in considerazione quanto segue:

- I pool di capacità devono essere creati nella stessa regione di Azure in cui i cluster AKS saranno gestiti con Astra Control Service.
- Un pool di capacità può avere un livello di servizio Ultra, Premium o Standard. Ciascuno di questi livelli di servizio è progettato per soddisfare diverse esigenze di performance. Astra Control Service supporta tutti e tre.

  È necessario impostare un pool di capacità per ciascun livello di servizio che si desidera utilizzare con i cluster Kubernetes.

  "Scopri di più sui livelli di servizio per Azure NetApp Files".

- Prima di creare un pool di capacità per le applicazioni che si intende proteggere con Astra Control Service, scegliere le prestazioni e la capacità richieste per tali applicazioni.

  Il provisioning della giusta quantità di capacità garantisce agli utenti la possibilità di creare volumi persistenti in base alle esigenze. Se la capacità non è disponibile, non è possibile eseguire il provisioning dei volumi persistenti.

- Un pool di capacità Azure NetApp Files può utilizzare il tipo di QoS manuale o automatico. Astra Control Service supporta i pool di capacità QoS automatici. I pool di capacità QoS manuali non sono supportati.

Fase

1. "Seguire la documentazione di Azure NetApp Files per impostare un pool di capacità QoS automatico".

Delegare una subnet a Azure NetApp Files

È necessario delegare una subnet a Azure NetApp Files in modo che il servizio di controllo Astra possa creare volumi persistenti in tale subnet. Tenere presente che Azure NetApp Files consente di avere una sola subnet delegata in una rete virtuale.

Se si utilizzano reti virtuali peering, entrambi i lati della connessione di peering devono essere online: La rete

virtuale in cui risiedono i cluster Kubernetes e la rete virtuale con la subnet delegata Azure NetApp Files.

Fase

1. "Seguire la documentazione di Azure NetApp Files per delegare una subnet a Azure NetApp Files".

Al termine

Attendere circa 10 minuti prima di rilevare il cluster in esecuzione nella subnet delegata.

Creare un'entità del servizio Azure

Astra Control Service richiede un'entità del servizio Azure a cui viene assegnato il ruolo di collaboratore. Astra Control Service utilizza questo principio del servizio per facilitare la gestione dei dati delle applicazioni Kubernetes per conto dell'utente.

Un service principal è un'identità creata appositamente per l'utilizzo con applicazioni, servizi e strumenti. L'assegnazione di un ruolo all'entità del servizio limita l'accesso a risorse Azure specifiche.

Seguire la procedura riportata di seguito per creare un'entità servizio utilizzando la CLI di Azure. Sarà necessario salvare l'output in un file JSON e fornirlo successivamente ad Astra Control Service. "Fare riferimento alla documentazione di Azure per ulteriori dettagli sull'utilizzo della CLI".

I seguenti passaggi presuppongono che si disponga dell'autorizzazione per creare un'entità servizio e che Microsoft Azure SDK (comando az) sia installato sul computer.

Requisiti

- L'entità del servizio deve utilizzare l'autenticazione regolare. I certificati non sono supportati.
- All'entità del servizio deve essere concesso l'accesso al tuo abbonamento Azure da parte di Contributor o Owner.
- L'abbonamento o il gruppo di risorse scelto per l'ambito deve contenere i cluster AKS e l'account Azure NetApp Files.

Fasi

1. Identificare l'abbonamento e l'ID tenant in cui risiedono i cluster AKS (si tratta dei cluster che si desidera gestire in Astra Control Service).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Eseguire una delle seguenti operazioni, a seconda che si utilizzi un'intera sottoscrizione o un gruppo di risorse:
   - Creare l'entità del servizio, assegnare il ruolo di collaboratore e specificare l'ambito dell'intera sottoscrizione in cui risiedono i cluster.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-ID
     ```

   - Creare l'entità del servizio, assegnare il ruolo di collaboratore e specificare il gruppo di risorse in cui risiedono i cluster.

```
az ad sp create-for-rbac --name service-principal-name --role
contributor --scopes /subscriptions/SUBSCRIPTION-
ID/resourceGroups/RESOURCE-GROUP-ID
```

3. Memorizzare l'output della CLI Azure risultante come file JSON.

   Dovrai fornire questo file in modo che Astra Control Service possa rilevare i tuoi cluster AKS e gestire le operazioni di gestione dei dati Kubernetes. "Scopri di più sulla gestione delle credenziali in Astra Control Service".

4. Facoltativo: Aggiungere l'ID di abbonamento al file JSON in modo che Astra Control Service compili automaticamente l'ID quando si seleziona il file.

   In caso contrario, dovrai inserire l'ID dell'abbonamento in Astra Control Service quando richiesto.

   Esempio

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Facoltativo: Verificare l'entità del servizio. Scegliere tra i seguenti comandi di esempio a seconda dell'ambito utilizzato dall'entità del servizio.

   Scopo dell'abbonamento

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az group list --subscription SUBSCRIPTION-ID
az aks list --subscription SUBSCRIPTION-ID
az storage container list --account-name STORAGE-ACCOUNT-NAME
```

   Ambito del gruppo di risorse

```
az login --service-principal --username APP-ID-SERVICEPRINCIPAL
--password PASSWORD --tenant TENANT-ID
az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
GROUP-ID
```

Opzionale: Configurare la ridondanza per i bucket di backup di Azure

È possibile configurare un livello di ridondanza più duraturo per i bucket di backup di Azure. Per impostazione predefinita, i bucket Astra Control Service utilizzati per memorizzare i backup di Azure Kubernetes Service utilizzano l'opzione di ridondanza LRS (Redundant Storage) locale. Per utilizzare un'opzione di ridondanza più durevole per i bucket Azure, è necessario eseguire le seguenti operazioni:

Fasi

1. Creare un account di storage Azure che utilizzi il livello di ridondanza necessario "queste istruzioni".
2. Creare un container Azure nel nuovo account storage utilizzando "queste istruzioni".
3. Aggiungere il container come bucket ad Astra Control Service. Fare riferimento a. "Aggiungere un bucket aggiuntivo".
4. (Facoltativo) per utilizzare il bucket appena creato come bucket predefinito per i backup di Azure, impostarlo come bucket predefinito per Azure. Fare riferimento a. "Modificare il bucket predefinito".

Configurare Microsoft Azure con dischi gestiti Azure

Sono necessari alcuni passaggi per preparare l'abbonamento a Microsoft Azure prima di poter gestire i cluster di servizi Azure Kubernetes con Astra Control Service. Seguire queste istruzioni se si intende utilizzare i dischi gestiti da Azure come backend di storage.

Avvio rapido per la configurazione di Azure

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

[Uno] Esaminare i requisiti del servizio di controllo Astra per Azure Kubernetes Service

Assicurarsi che i cluster siano integri e che eseguano una versione supportata di Kubernetes, che i pool di nodi siano online e che eseguano Linux e altro ancora. Scopri di più su questo passaggio.

[Due] Iscriviti a Microsoft Azure

Creare un account Microsoft Azure. Scopri di più su questo passaggio.

[Tre] Creare un'entità del servizio Azure

Creare un'entità del servizio Azure con il ruolo di collaboratore. Scopri di più su questo passaggio.

[Quattro] Configurare i dettagli del driver CSI (Container Storage Interface)

È necessario configurare l'abbonamento Azure e il cluster per il funzionamento con i driver CSI. Scopri di più su questo passaggio.

[Cinque] Opzionale: Configurare la ridondanza per i bucket di backup di Azure

Per impostazione predefinita, i bucket Astra Control Service utilizzati per memorizzare i backup di Azure Kubernetes Service utilizzano l'opzione di ridondanza LRS (Redundant Storage) locale. Come passaggio opzionale, è possibile configurare un livello di ridondanza più duraturo per i bucket Azure. Scopri di più su questo passaggio.

Azure Kubernetes Service Cluster Requirements

Un cluster Kubernetes deve soddisfare i seguenti requisiti per consentirne il rilevamento e la gestione da Astra Control Service.

Versione di Kubernetes

I cluster devono eseguire Kubernetes versione 1,26 - 1,28.

Tipo di immagine

Il tipo di immagine per tutti i pool di nodi deve essere Linux.

Stato del cluster

I cluster devono essere in esecuzione in uno stato integro e avere almeno un nodo di lavoro online senza nodi di lavoro in uno stato di errore.

Regione di Azure

Come Best practice, è necessario scegliere una regione che supporti Azure NetApp Files, anche se non viene utilizzata come back-end di storage. In questo modo sarà più semplice utilizzare Azure NetApp Files come back-end di storage in futuro se i requisiti di performance cambiano. "Visualizza i prodotti Azure per regione".

Driver CSI

I cluster devono avere installati i driver CSI appropriati.

Iscriviti a Microsoft Azure

Se non disponi di un account Microsoft Azure, inizia iscrivendoti a Microsoft Azure.

Fasi

1. Accedere alla "Pagina di iscrizione Azure" Per iscriversi al servizio Azure.
2. Selezionare un piano e seguire le istruzioni per completare l'abbonamento.

Creare un'entità del servizio Azure

Astra Control Service richiede un'entità del servizio Azure a cui viene assegnato il ruolo di collaboratore. Astra Control Service utilizza questo principio del servizio per facilitare la gestione dei dati delle applicazioni Kubernetes per conto dell'utente.

Un service principal è un'identità creata appositamente per l'utilizzo con applicazioni, servizi e strumenti. L'assegnazione di un ruolo all'entità del servizio limita l'accesso a risorse Azure specifiche.

Seguire la procedura riportata di seguito per creare un'entità servizio utilizzando la CLI di Azure. Sarà necessario salvare l'output in un file JSON e fornirlo successivamente ad Astra Control Service. "Fare riferimento alla documentazione di Azure per ulteriori dettagli sull'utilizzo della CLI".

I seguenti passaggi presuppongono che si disponga dell'autorizzazione per creare un'entità servizio e che Microsoft Azure SDK (comando az) sia installato sul computer.

Requisiti

- L'entità del servizio deve utilizzare l'autenticazione regolare. I certificati non sono supportati.
- All'entità del servizio deve essere concesso l'accesso al tuo abbonamento Azure da parte di Contributor o Owner.

- L'abbonamento o il gruppo di risorse scelto per l'ambito deve contenere i cluster AKS e l'account Azure NetApp Files.

Fasi

1. Identificare l'abbonamento e l'ID tenant in cui risiedono i cluster AKS (si tratta dei cluster che si desidera gestire in Astra Control Service).

   ```
   az configure --list-defaults
   az account list --output table
   ```

2. Eseguire una delle seguenti operazioni, a seconda che si utilizzi un'intera sottoscrizione o un gruppo di risorse:
   - Creare l'entità del servizio, assegnare il ruolo di collaboratore e specificare l'ambito dell'intera sottoscrizione in cui risiedono i cluster.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-ID
     ```

   - Creare l'entità del servizio, assegnare il ruolo di collaboratore e specificare il gruppo di risorse in cui risiedono i cluster.

     ```
     az ad sp create-for-rbac --name service-principal-name --role
     contributor --scopes /subscriptions/SUBSCRIPTION-
     ID/resourceGroups/RESOURCE-GROUP-ID
     ```

3. Memorizzare l'output della CLI Azure risultante come file JSON.

   Dovrai fornire questo file in modo che Astra Control Service possa rilevare i tuoi cluster AKS e gestire le operazioni di gestione dei dati Kubernetes. "Scopri di più sulla gestione delle credenziali in Astra Control Service".

4. Facoltativo: Aggiungere l'ID di abbonamento al file JSON in modo che Astra Control Service compili automaticamente l'ID quando si seleziona il file.

   In caso contrario, dovrai inserire l'ID dell'abbonamento in Astra Control Service quando richiesto.

   Esempio

```
{
  "appId": "0db3929a-bfb0-4c93-baee-aaf8",
  "displayName": "sp-example-dev-sandbox",
  "name": "http://sp-example-dev-sandbox",
  "password": "mypassword",
  "tenant": "011cdf6c-7512-4805-aaf8-7721afd8ca37",
  "subscriptionId": "99ce999a-8c99-99d9-a9d9-99cce99f99ad"
}
```

5. Facoltativo: Verificare l'entità del servizio. Scegliere tra i seguenti comandi di esempio a seconda dell'ambito utilizzato dall'entità del servizio.

   Scopo dell'abbonamento

   ```
   az login --service-principal --username APP-ID-SERVICEPRINCIPAL
   --password PASSWORD --tenant TENANT-ID
   az group list --subscription SUBSCRIPTION-ID
   az aks list --subscription SUBSCRIPTION-ID
   az storage container list --account-name STORAGE-ACCOUNT-NAME
   ```

   Ambito del gruppo di risorse

   ```
   az login --service-principal --username APP-ID-SERVICEPRINCIPAL
   --password PASSWORD --tenant TENANT-ID
   az aks list --subscription SUBSCRIPTION-ID --resource-group RESOURCE-
   GROUP-ID
   ```

Configurare i dettagli del driver CSI (Container Storage Interface)

Per utilizzare i dischi gestiti Azure con Astra Control Service, è necessario installare i driver CSI richiesti.

Attivare la funzione del driver CSI nell'abbonamento Azure

Prima di installare i driver CSI, è necessario attivare la funzionalità del driver CSI nell'abbonamento Azure.

Fasi

1. Aprire l'interfaccia della riga di comando di Azure.
2. Eseguire il seguente comando per registrare il driver:

   ```
   az feature register --namespace "Microsoft.ContainerService" --name
   "EnableAzureDiskFileCSIDriver"
   ```

3. Eseguire il seguente comando per assicurarsi che la modifica venga propagata:

```
az provider register -n Microsoft.ContainerService
```

L'output dovrebbe essere simile a quanto segue:

```
{
"id": "/subscriptions/b200155f-001a-43be-87be-
3edde83acef4/providers/Microsoft.Features/providers/Microsoft.ContainerSer
vice/features/EnableAzureDiskFileCSIDriver",
"name": "Microsoft.ContainerService/EnableAzureDiskFileCSIDriver",
"properties": {
   "state": "Registering"
},
"type": "Microsoft.Features/providers/features"
}
```

Installare i driver CSI del disco gestito Azure nel cluster Azure Kubernetes Service

È possibile installare i driver di Azure CSI per completare la preparazione.

Fase

1. Passare a. "La documentazione del driver Microsoft CSI".
2. Seguire le istruzioni per installare i driver CSI richiesti.

Opzionale: Configurare la ridondanza per i bucket di backup di Azure

È possibile configurare un livello di ridondanza più duraturo per i bucket di backup di Azure. Per impostazione predefinita, i bucket Astra Control Service utilizzati per memorizzare i backup di Azure Kubernetes Service utilizzano l'opzione di ridondanza LRS (Redundant Storage) locale. Per utilizzare un'opzione di ridondanza più durevole per i bucket Azure, è necessario eseguire le seguenti operazioni:

Fasi

1. Creare un account di storage Azure che utilizzi il livello di ridondanza necessario "queste istruzioni".
2. Creare un container Azure nel nuovo account storage utilizzando "queste istruzioni".
3. Aggiungere il container come bucket ad Astra Control Service. Fare riferimento a. "Aggiungere un bucket aggiuntivo".
4. (Facoltativo) per utilizzare il bucket appena creato come bucket predefinito per i backup di Azure, impostarlo come bucket predefinito per Azure. Fare riferimento a. "Modificare il bucket predefinito".

Registrati per un account Astra Control Service

Per utilizzare il servizio Astra Control, devi disporre di un account Astra Control Service associato al tuo account NetApp BlueXP. Completa il processo di registrazione ad Astra Control Service e, se non disponi già di un account BlueXP, registrati a BlueXP per accedere ad Astra Control Service.

Registrati per un account Astra Control

Prima di accedere ad Astra Control Service, è necessario completare un processo di registrazione per ottenere un account Astra Control Service.

Quando utilizzi Astra Control Service, gestirai le tue applicazioni dall'interno di un account. Un account include gli utenti che possono visualizzare e gestire le applicazioni all'interno dell'account, oltre ai dati di fatturazione.

Fasi

1. "Visita la pagina Astra Control su BlueXP".
2. Selezionare **Iscriviti al piano gratuito**.
3. Fornire le informazioni richieste nel modulo.

   Durante la compilazione del modulo, è necessario prendere nota di alcuni elementi importanti:

   - Il nome e l'indirizzo della tua azienda devono essere precisi perché li verificheremo per soddisfare i requisiti della Global Trade Compliance.
   - Il nome dell'account * Astra è il nome dell'account Astra Control Service della tua azienda. Questo nome viene visualizzato nell'interfaccia utente di Astra Control Service. Nota: Se necessario, è possibile creare altri account (fino a 5).
   - Nel campo **Indirizzo e-mail aziendale**, se si dispone di un account NetApp BlueXP, immettere qui l'e-mail che si utilizza per tale account. Se non disponi ancora di un account NetApp BlueXP, utilizza l'indirizzo email che inserisci qui quando effettui l'iscrizione ad BlueXP.
4. Selezionare **Crea account**.

Iscriviti a BlueXP

Il servizio di controllo Astra è integrato nel servizio di autenticazione di NetApp BlueXP. Puoi accedere a NetApp BlueXP usando le tue credenziali del sito di supporto BlueXP o NetApp. Se non disponi già di un account NetApp BlueXP o del sito di supporto NetApp, iscriviti a BlueXP per poter accedere al servizio Astra Control e agli altri servizi cloud di NetApp. Se disponi già di un account BlueXP o sul sito di supporto NetApp e hai completato la registrazione, puoi accedere "Servizio di controllo Astra" Utilizzando direttamente le credenziali del sito di supporto BlueXP o NetApp.

> Puoi anche utilizzare il single sign-on per accedere a BlueXP utilizzando le credenziali della directory aziendale (identità federata). Per ulteriori informazioni, visitare il sito "Centro assistenza" Quindi selezionare **Cloud Central sign-in options** (Opzioni di accesso Cloud Central).

Fasi

1. Passare a. "NetApp BlueXP".
2. In alto a destra, seleziona **inizia**.
3. Selezionare **Registrati**.
4. Compila il modulo.

   Assicurati che il numero di telefono e l'indirizzo e-mail inseriti in questo campo siano gli stessi utilizzati nel modulo di registrazione Astra Control precedente.

5. Selezionare **Registrati**.

L'indirizzo email inserito in questi moduli corrisponde al tuo ID utente NetApp BlueXP. Utilizza questo ID utente BlueXP quando effettui l'iscrizione a un nuovo account Astra Control o quando un amministratore Astra Control ti invita a un account Astra Control esistente.

6. Attende un'e-mail da NetApp BlueXP. L'e-mail proviene dall'indirizzo saas.support@netapp.com e potrebbe richiedere alcuni minuti per arrivare. Controllare la cartella spam.
7. All'arrivo del messaggio, selezionare il collegamento nell'e-mail per verificare l'indirizzo e-mail.

Risultato

Hai ora un accesso utente BlueXP attivo.

Ora che sei registrato, puoi accedere direttamente a Astra Control usando le tue credenziali BlueXP di https://astra.netapp.io.

Aggiungere un cluster a Astra Control Service

Dopo aver configurato l'ambiente, è possibile creare un cluster Kubernetes e aggiungerlo ad Astra Control Service. Questo consente di utilizzare Astra Control Service per proteggere le applicazioni sul cluster.

A seconda del tipo di cluster da aggiungere ad Astra Control Service, è necessario utilizzare diversi passaggi per aggiungere il cluster.

- "Aggiungere un cluster gestito da un provider pubblico ad Astra Control Service": Utilizzare questa procedura per aggiungere un cluster con un indirizzo IP pubblico e gestito da un provider cloud. È necessario disporre dell'account Service Principal, dell'account del servizio o dell'account utente per il provider cloud.
- "Aggiungere un cluster gestito da provider privato ad Astra Control Service": Utilizzare questa procedura per aggiungere un cluster che dispone di un indirizzo IP privato ed è gestito da un provider cloud. È necessario disporre dell'account Service Principal, dell'account del servizio o dell'account utente per il provider cloud.
- "Aggiungere un cluster pubblico autogestato ad Astra Control Service": Utilizzare questa procedura per aggiungere un cluster con un indirizzo IP pubblico e gestito dall'organizzazione. Sarà necessario creare un file kubeconfig per il cluster che si desidera aggiungere.
- "Aggiungere un cluster privato autogestato ad Astra Control Service": Utilizzare questa procedura per aggiungere un cluster con un indirizzo IP privato e gestito dall'organizzazione. Sarà necessario creare un file kubeconfig per il cluster che si desidera aggiungere.

Installa Astra Connector per gestire i cluster

Astra Connector è un software che risiede nei cluster gestiti e facilita la comunicazione tra il cluster gestito e Astra Control. Per i cluster gestiti mediante Astra Control Service, sono disponibili due versioni di Astra Connector:

- **Versione precedente del connettore Astra**: "Installare la versione precedente del connettore Astra" Sul tuo cluster, se intendi gestire il cluster con flussi di lavoro non nativi di Kubernetes.
- [Tech preview] * connettore dichiarativo di Kubernetes Astra*: "Installa Astra Connector per i cluster gestiti con flussi di lavoro Kubernetes dichiarativi" Sul cluster, se si intende gestire il cluster utilizzando flussi di

lavoro Kubernetes dichiarativi. Dopo aver installato Astra Connector sul cluster, il cluster viene aggiunto automaticamente ad Astra Control.

> Il connettore dichiarativo Kubernetes Astra è disponibile solo come parte del programma Astra Control Early Adopter Program (EAP). Per informazioni sulla partecipazione al programma EAP, contattare il rappresentante commerciale NetApp di zona.

Installare la versione precedente del connettore Astra

Astra Control Service utilizza la versione precedente di Astra Connector per consentire la comunicazione tra Astra Control Service e i cluster privati gestiti con flussi di lavoro non nativi per Kubernetes. Devi installare Astra Connector su cluster privati che vuoi gestire con flussi di lavoro non nativi di Kubernetes.

La versione precedente di Astra Connector supporta i seguenti tipi di cluster privati gestiti con flussi di lavoro non nativi di Kubernetes:

- Amazon Elastic Kubernetes Service (EKS)
- Servizio Azure Kubernetes (AKS)
- Google Kubernetes Engine (GKE)
- Red Hat OpenShift Service su AWS (ROSA)
- ROSA con AWS PrivateLink
- Piattaforma Red Hat OpenShift Container all'interno dell'hotel

A proposito di questa attività

- Per eseguire questi passaggi, esegui questi comandi sul cluster privato che desideri gestire con Astra Control Service.
- Se si utilizza un host Bastion, eseguire questi comandi dalla riga di comando dell'host Bastion.

Prima di iniziare

- Devi accedere al cluster privato da gestire con Astra Control Service.
- Sono necessarie autorizzazioni di amministratore di Kubernetes per installare l'operatore Astra Connector sul cluster.

Fasi

1. Installa l'operatore Astra Connector precedente sul cluster privato che desideri gestire con flussi di lavoro non nativi di Kubernetes. Quando si esegue questo comando, lo spazio dei nomi `astra-connector-operator` viene creato e la configurazione viene applicata allo spazio dei nomi:

   ```
   kubectl apply -f https://github.com/NetApp/astra-connector-
   operator/releases/download/23.07.0-
   202310251519/astraconnector_operator.yaml
   ```

2. Verificare che l'operatore sia installato e pronto:

```
kubectl get all -n astra-connector-operator
```

3. Ottieni un token API da Astra Control. Fare riferimento a. "Documentazione di Astra Automation" per istruzioni.
4. Creare lo spazio dei nomi astra-Connector:

```
kubectl create ns astra-connector
```

5. Creare il file Astra Connector CR e assegnargli un nome `astra-connector-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - **<ASTRA_CONTROL_SERVICE_URL>**: L'URL dell'interfaccia utente web del servizio di controllo Astra. Ad esempio:

     ```
     https://astra.netapp.io
     ```

   - **<ASTRA_CONTROL_SERVICE_API_TOKEN>**: Il token dell'API di controllo Astra ottenuto nel passaggio precedente.
   - **<PRIVATE_AKS_CLUSTER_NAME>**: (Solo cluster AKS) - il nome del cluster del cluster privato Azure Kubernetes Service. Annullare il commento e popolare questa riga solo se si aggiunge un cluster AKS privato.
   - **<ASTRA_CONTROL_ACCOUNT_ID>**: Ottenuto dall'interfaccia utente web Astra Control. Selezionare l'icona a forma di figura in alto a destra nella pagina e selezionare **accesso API**.

     ```
     apiVersion: netapp.astraconnector.com/v1
     kind: AstraConnector
     metadata:
       name: astra-connector
       namespace: astra-connector
     spec:
       natssync-client:
         cloud-bridge-url: <ASTRA_CONTROL_SERVICE_URL>
       imageRegistry:
         name: theotw
         secret: ""
       astra:
         token: <ASTRA_CONTROL_SERVICE_API_TOKEN>
         #clusterName: <PRIVATE_AKS_CLUSTER_NAME>
         accountId: <ASTRA_CONTROL_ACCOUNT_ID>
         acceptEULA: yes
     ```

6. Dopo aver popolato il `astra-connector-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-connector-cr.yaml
```

7. Verificare che il connettore Astra sia completamente distribuito:

```
kubectl get all -n astra-connector
```

8. Verifica che il cluster sia registrato con Astra Control:

```
kubectl get astraconnector -n astra-connector
```

L'output dovrebbe essere simile a quanto segue:

```
NAME              REGISTERED   ASTRACONNECTORID
STATUS
astra-connector   true         be475ae5-1511-4eaa-9b9e-712f09b0d065
Registered with Astra
```

Prendere nota di ASTRACONNECTORID; sarà necessario quando si aggiunge il cluster ad Astra Control.

Quali sono le prossime novità?

Una volta installato Astra Connector, puoi aggiungere il cluster privato ad Astra Control Service.

- "Aggiungere un cluster gestito da provider privato ad Astra Control Service": Utilizzare questa procedura per aggiungere un cluster che dispone di un indirizzo IP privato ed è gestito da un provider cloud. È necessario disporre dell'account Service Principal, dell'account del servizio o dell'account utente per il provider cloud.
- "Aggiungere un cluster privato autogestato ad Astra Control Service": Utilizzare questa procedura per aggiungere un cluster con un indirizzo IP privato e gestito dall'organizzazione. Sarà necessario creare un file kubeconfig per il cluster che si desidera aggiungere.

Per ulteriori informazioni

- "Aggiungere un cluster"

(Anteprima tecnica) Installa il connettore dichiarativo di Kubernetes Astra

I cluster gestiti utilizzando flussi di lavoro Kubernetes dichiarativi utilizzano Astra Connector per consentire la comunicazione tra il cluster gestito e Astra Control. Devi installare Astra Connector su tutti i cluster che verranno gestiti con flussi di lavoro Kubernetes dichiarativi.

Viene installato il connettore Astra dichiarativo di Kubernetes utilizzando i comandi di Kubernetes e i file Custom Resource (CR).

A proposito di questa attività

- Quando esegui questi passaggi, esegui questi comandi sul cluster che desideri gestire con Astra Control.
- Se si utilizza un host Bastion, eseguire questi comandi dalla riga di comando dell'host Bastion.

Prima di iniziare

- Devi accedere al cluster da gestire con Astra Control.
- Sono necessarie autorizzazioni di amministratore di Kubernetes per installare l'operatore Astra Connector sul cluster.

> Se il cluster è configurato con l'imposizione dell'ammissione di sicurezza pod, che è l'impostazione predefinita per i cluster Kubernetes 1,25 e versioni successive, è necessario abilitare le restrizioni PSA sugli spazi dei nomi appropriati. Fare riferimento a. "Prepara il tuo ambiente per la gestione dei cluster utilizzando Astra Control" per istruzioni.

Fasi

1. Installare l'operatore Astra Connector sul cluster che si desidera gestire con flussi di lavoro Kubernetes dichiarativi. Quando si esegue questo comando, lo spazio dei nomi `astra-connector-operator` viene creato e la configurazione viene applicata allo spazio dei nomi:

```
kubectl apply -f https://github.com/NetApp/astra-connector-
operator/releases/download/24.02.0-
202403151353/astraconnector_operator.yaml
```

2. Verificare che l'operatore sia installato e pronto:

```
kubectl get all -n astra-connector-operator
```

3. Ottieni un token API da Astra Control. Fare riferimento a. "Documentazione di Astra Automation" per istruzioni.
4. Creare un segreto utilizzando il token. Sostituisci <API_TOKEN> con il token ricevuto da Astra Control:

```
kubectl create secret generic astra-token \
--from-literal=apiToken=<API_TOKEN> \
-n astra-connector
```

5. Crea un Docker Secret da usare per estrarre l'immagine di Astra Connector. Sostituire i valori tra parentesi <> con le informazioni dell'ambiente:

> Puoi trovare il <ASTRA_CONTROL_ACCOUNT_ID> nell'interfaccia utente web di Astra Control. Nell'interfaccia utente Web, selezionare l'icona della figura in alto a destra nella pagina e selezionare **accesso API**.

```
kubectl create secret docker-registry regcred \
--docker-username=<ASTRA_CONTROL_ACCOUNT_ID> \
--docker-password=<API_TOKEN> \
-n astra-connector \
--docker-server=cr.astra.netapp.io
```

6. Creare il file Astra Connector CR e assegnargli un nome `astra-connector-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - <ASTRA_CONTROL_ACCOUNT_ID>: Ottenuto dall'interfaccia utente web Astra Control durante la fase precedente.
   - <CLUSTER_NAME>: Il nome che il cluster deve essere assegnato in Astra Control.
   - <ASTRA_CONTROL_URL>: L'URL dell'interfaccia utente web di Astra Control. Ad esempio:

```
https://astra.control.url
```

```yaml
apiVersion: astra.netapp.io/v1
kind: AstraConnector
metadata:
  name: astra-connector
  namespace: astra-connector
spec:
  astra:
    accountId: <ASTRA_CONTROL_ACCOUNT_ID>
    clusterName: <CLUSTER_NAME>
    #Only set `skipTLSValidation` to `true` when using the default
self-signed
    #certificate in a proof-of-concept environment.
    skipTLSValidation: false #Should be set to false in production
environments
    tokenRef: astra-token
  natsSyncClient:
    cloudBridgeURL: <ASTRA_CONTROL_HOST_URL>
  imageRegistry:
    name: cr.astra.netapp.io
    secret: regcred
```

7. Dopo aver popolato il `astra-connector-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -n astra-connector -f astra-connector-cr.yaml
```

8. Verificare che il connettore Astra sia completamente distribuito:

```
kubectl get all -n astra-connector
```

9. Verifica che il cluster sia registrato con Astra Control:

```
kubectl get astraconnectors.astra.netapp.io -A
```

L'output dovrebbe essere simile a quanto segue:

```
NAMESPACE         NAME              REGISTERED   ASTRACONNECTORID
STATUS
astra-connector   astra-connector   true         00ac8-2cef-41ac-8777-
ed0583e   Registered with Astra
```

10. Verificare che il cluster compaia nell'elenco dei cluster gestiti nella pagina **cluster** dell'interfaccia utente Web Astra Control.

Aggiungere un cluster gestito dal provider

Aggiungere un cluster gestito da un provider pubblico ad Astra Control Service

Dopo aver configurato l'ambiente cloud, sei pronto per creare un cluster Kubernetes e aggiungerlo ad Astra Control Service.

- Creare un cluster Kubernetes
- Aggiungere il cluster ad Astra Control Service
- Modificare la classe di storage predefinita

Creare un cluster Kubernetes

Se non si dispone ancora di un cluster, è possibile crearne uno che soddisfi le esigenze "Requisiti del servizio Astra Control per Amazon Elastic Kubernetes Service (EKS)". Se non si dispone ancora di un cluster, è possibile crearne uno che soddisfi le esigenze "Requisiti del servizio Astra Control per Google Kubernetes Engine (GKE)". Se non si dispone ancora di un cluster, è possibile crearne uno che soddisfi le esigenze "Requisiti del servizio di controllo Astra per il servizio Azure Kubernetes (AKS) con Azure NetApp Files" oppure "Requisiti del servizio di controllo Astra per Azure Kubernetes Service (AKS) con dischi gestiti Azure".

> Astra Control Service supporta i cluster AKS che utilizzano Azure Active Directory (Azure ad) per l'autenticazione e la gestione delle identità. Quando si crea il cluster, seguire le istruzioni in "documentazione ufficiale" Per configurare il cluster per l'utilizzo di Azure ad. È necessario assicurarsi che i cluster soddisfino i requisiti per l'integrazione di Azure ad gestita da AKS.

Aggiungere il cluster ad Astra Control Service

Dopo aver effettuato l'accesso ad Astra Control Service, il primo passo è iniziare a gestire i cluster. Prima di aggiungere un cluster ad Astra Control Service, è necessario eseguire attività specifiche e assicurarsi che il cluster soddisfi determinati requisiti.

Quando gestisci i cluster Azure Kubernetes Service e Google Kubernetes Engine, tieni presente che hai due opzioni per l'installazione di Astra Control Provivisioner e la gestione del ciclo di vita:

- Puoi utilizzare Astra Control Service per gestire automaticamente il ciclo di vita di Astra Control Provisioner. Per fare questo, assicurati che Astra Trident non sia installato e Astra Control provisioner non sia abilitato nel cluster che vuoi gestire con Astra Control Service. In questo caso, Astra Control Service abilita automaticamente Astra Control Provisioner quando inizi a gestire il cluster e gli aggiornamenti di Astra Control Provisioner vengono gestiti automaticamente.
- Puoi gestire tu stesso il ciclo di vita di Astra Control Provisioner. A tale scopo, abilita Astra Control Provisioner sul cluster prima di gestire il cluster con Astra Control Service. In questo caso, Astra Control Service rileva che Astra Control Provisioner è già abilitato e non lo reinstalla né gestisce gli aggiornamenti di Astra Control Provisioner. Fare riferimento a. "Abilita Astra Control Provisioner" Per i passaggi, abilita Astra Control provisioner.

Se gestisci i cluster di Amazon Web Services con Astra Control Service, se hai bisogno di backend di storage che possono essere utilizzati solo con Astra Control Provivisioner, devi abilitare Astra Control Provivisioner manualmente sul cluster prima di gestirlo con Astra Control Service. Fare riferimento a. "Abilita Astra Control Provisioner" Per informazioni su come attivare Astra Control Provivioner.

Prima di iniziare

Amazon Web Services

- Il file JSON contiene le credenziali dell'utente IAM che ha creato il cluster. "Scopri come creare un utente IAM".
- Per Amazon FSX per NetApp ONTAP è necessario Astra Control Provisioner. Se intendi usare Amazon FSX per NetApp ONTAP come back-end dello storage per il tuo cluster EKS, fai riferimento alle informazioni Astra Control Provivisioner nel "Requisiti del cluster EKS".
- (Facoltativo) se è necessario fornire `kubectl` Accesso ai comandi per un cluster ad altri utenti IAM che non sono i creatori del cluster, fare riferimento alle istruzioni in "Come posso fornire l'accesso ad altri utenti e ruoli IAM dopo la creazione del cluster in Amazon EKS?".
- Se intendi utilizzare NetApp Cloud Volumes ONTAP come backend di storage, devi configurare Cloud Volumes ONTAP per l'utilizzo con Amazon Web Services. Fare riferimento alla Cloud Volumes ONTAP "documentazione di installazione".

Microsoft Azure

- Il file JSON che contiene l'output della CLI di Azure deve essere presente al momento della creazione dell'entità del servizio. "Scopri come configurare un service principal".

  Avrai inoltre bisogno del tuo ID di abbonamento Azure, se non lo hai aggiunto al file JSON.

- Se si intende utilizzare NetApp Cloud Volumes ONTAP come back-end per lo storage, è necessario configurare Cloud Volumes ONTAP per l'utilizzo con Microsoft Azure. Fare riferimento alla Cloud Volumes ONTAP "documentazione di installazione".

Google Cloud

- È necessario disporre del file della chiave dell'account di servizio per un account di servizio che dispone delle autorizzazioni necessarie. "Scopri come configurare un account di servizio".
- Se si intende utilizzare NetApp Cloud Volumes ONTAP come back-end per lo storage, è necessario configurare Cloud Volumes ONTAP per l'utilizzo con Google Cloud. Fare riferimento alla Cloud Volumes ONTAP "documentazione di installazione".

Fasi

1. (Facoltativo) se stai aggiungendo un cluster Amazon EKS o vuoi gestire da solo l'installazione e gli aggiornamenti di Astra Control Provivisioner, abilita Astra Control Provivisioner sul cluster. Fare riferimento a. "Abilita Astra Control Provisioner" per i passaggi di abilitazione.
2. Aprire l'interfaccia utente Web di Astra Control Service in un browser.
3. Nella dashboard, selezionare **Manage Kubernetes cluster** (Gestisci cluster Kubernetes).

   Seguire le istruzioni per aggiungere il cluster.

4. **Provider**: Seleziona il tuo cloud provider e fornisci le credenziali necessarie per creare una nuova istanza di cloud oppure seleziona un'istanza di cloud esistente da utilizzare.
5. **Amazon Web Services**: Fornisci i dettagli del tuo account utente IAM Amazon Web Services caricando un file JSON o incollando il contenuto del file JSON dagli Appunti.

   Il file JSON deve contenere le credenziali dell'utente IAM che ha creato il cluster.

6. **Microsoft Azure**: Fornisci dettagli sull'entità del servizio Azure caricando un file JSON o incollando il contenuto di tale file JSON dagli Appunti.

   Il file JSON deve contenere l'output dell'interfaccia CLI di Azure al momento della creazione dell'entità del servizio. Può anche includere il tuo ID di abbonamento per aggiungerlo automaticamente ad Astra. In caso contrario, è necessario inserire manualmente l'ID dopo aver fornito il codice JSON.

7. **Google Cloud Platform**: Fornire il file delle chiavi dell'account di servizio caricando il file o incollando il contenuto dagli Appunti.

   Astra Control Service utilizza l'account del servizio per rilevare i cluster in esecuzione in Google Kubernetes Engine.

8. **Altro**: Questa scheda è destinata solo ai cluster a gestione automatica.
   a. **Nome istanza cloud**: Fornire un nome per la nuova istanza cloud che verrà creata quando si aggiunge questo cluster. Scopri di più "istanze cloud".
   b. Selezionare **Avanti**.

      Astra Control Service visualizza un elenco di cluster tra i quali è possibile scegliere.

   c. **Cluster**: Selezionare un cluster dall'elenco da aggiungere ad Astra Control Service.

      > Durante la selezione dall'elenco dei cluster, prestare attenzione alla colonna **Eligiblity**. Se un cluster è "non idoneo" o "parzialmente idoneo", passare il mouse sullo stato per determinare se si è verificato un problema con il cluster. Ad esempio, potrebbe identificare che il cluster non dispone di un nodo di lavoro.

   d. Selezionare **Avanti**.
   e. (Facoltativo) **Storage**: Facoltativamente, selezionare la classe di storage che si desidera utilizzare per impostazione predefinita per le applicazioni Kubernetes distribuite in questo cluster.
9. Per selezionare una nuova classe di storage predefinita per il cluster, attivare la casella di controllo **Assegna una nuova classe di storage predefinita**.
10. Selezionare una nuova classe di storage predefinita dall'elenco.

Ogni servizio di storage del cloud provider visualizza le seguenti informazioni su prezzo, performance e resilienza:

- Cloud Volumes Service per Google Cloud: Informazioni su prezzi, performance e resilienza
- Google Persistent Disk: Non sono disponibili informazioni su prezzi, performance o resilienza
- Azure NetApp Files: Informazioni su performance e resilienza
- Dischi gestiti Azure: Non sono disponibili informazioni su prezzi, performance o resilienza
- Amazon Elastic Block Store: Nessuna informazione su prezzi, performance o resilienza disponibile
- Amazon FSX per NetApp ONTAP: Nessuna informazione su prezzi, performance o resilienza disponibile
- NetApp Cloud Volumes ONTAP: Non sono disponibili informazioni su prezzi, performance o resilienza

Ogni classe di storage può utilizzare uno dei seguenti servizi:

- "Cloud Volumes Service per Google Cloud"
- "Disco persistente di Google"
  - "Azure NetApp Files"
  - "Dischi gestiti da Azure"
  - "Amazon Elastic Block Store"
  - "Amazon FSX per NetApp ONTAP"
  - "NetApp Cloud Volumes ONTAP"

  Scopri di più "Classi di storage per cluster Amazon Web Services". Scopri di più "Classi di storage per cluster AKS". Scopri di più "Classi di storage per cluster GKE".

  a. Selezionare **Avanti**.
  b. **Review & Approve** (Rivedi e approva): Verifica dei dettagli della configurazione.
  c. Selezionare **Add** per aggiungere il cluster ad Astra Control Service.

Risultato

Se si tratta del primo cluster aggiunto per questo provider cloud, Astra Control Service crea un archivio di oggetti per il provider cloud per i backup delle applicazioni in esecuzione sui cluster idonei. (Quando si aggiungono cluster successivi per questo provider cloud, non vengono creati ulteriori archivi di oggetti). Se è stata specificata una classe di storage predefinita, Astra Control Service imposta la classe di storage predefinita specificata. Per i cluster gestiti in Amazon Web Services o Google Cloud Platform, Astra Control Service crea anche un account admin sul cluster. Queste operazioni possono richiedere alcuni minuti.

Modificare la classe di storage predefinita

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

Modificare la classe di storage predefinita utilizzando Astra Control

È possibile modificare la classe di storage predefinita per un cluster da Astra Control. Se il cluster utilizza un servizio backend di storage precedentemente installato, potrebbe non essere possibile utilizzare questo metodo per modificare la classe di storage predefinita (l'azione **Set as default** non è selezionabile). In questo caso, è possibile Modificare la classe di storage predefinita utilizzando la riga di comando.

Fasi

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

Modificare la classe di storage predefinita utilizzando la riga di comando

È possibile modificare la classe di storage predefinita per un cluster utilizzando i comandi Kubernetes. Questo metodo funziona indipendentemente dalla configurazione del cluster.

Fasi

1. Accedere al cluster Kubernetes.
2. Elencare le classi di storage nel cluster:

```
kubectl get storageclass
```

3. Rimuovere la designazione predefinita dalla classe di storage predefinita. Sostituire <SC_NAME> con il nome della classe di storage:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Contrassegna una classe di storage diversa come predefinita. Sostituire <SC_NAME> con il nome della classe di storage:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confermare la nuova classe di storage predefinita:

```
kubectl get storageclass
```

Aggiungere un cluster gestito da provider privato ad Astra Control Service

Puoi utilizzare Astra Control Service per gestire cluster privati di Google Kubernetes Engine (GKE). Queste istruzioni presuppongono che sia già stato creato un cluster AKS o OpenShift privato e che sia stato preparato un metodo sicuro per accedervi in remoto; per ulteriori informazioni sulla creazione e l'accesso a cluster AKS o OpenShift privati, fare riferimento alla seguente documentazione:

- "Documentazione di Azure per cluster AKS privati"
- "Documentazione di Azure per cluster OpenShift privati"

Puoi utilizzare Astra Control Service per gestire cluster privati Azure Kubernetes Service (AKS) e cluster privati Red Hat OpenShift in AKS. Queste istruzioni presuppongono che sia già stato creato un cluster AKS o OpenShift privato e che sia stato preparato un metodo sicuro per accedervi in remoto; per ulteriori informazioni sulla creazione e l'accesso a cluster AKS o OpenShift privati, fare riferimento alla seguente documentazione:

- "Documentazione di Azure per cluster AKS privati"
- "Documentazione di Azure per cluster OpenShift privati"

Puoi utilizzare Astra Control Service per gestire cluster privati Amazon Elastic Kubernetes Service (EKS). Queste istruzioni presuppongono che sia già stato creato un cluster EKS privato e che sia stato preparato un metodo sicuro per accedervi in remoto; per ulteriori informazioni sulla creazione e l'accesso a cluster EKS privati, fare riferimento a. "Documentazione Amazon EKS".

Per aggiungere il cluster privato ad Astra Control Service, è necessario eseguire le seguenti operazioni:

1. Installare il connettore Astra
2. Configurare lo storage persistente
3. Aggiungere il cluster gestito dal provider privato ad Astra Control Service

Installare il connettore Astra

Prima di aggiungere un cluster privato, devi installare Astra Connector sul cluster in modo che Astra Control possa comunicare con esso. Fare riferimento a. "Installa la versione precedente di Astra Connector per cluster privati gestiti con flussi di lavoro non nativi di Kubernetes" per istruzioni.

Configurare lo storage persistente

Configurare lo storage persistente per il cluster. Fare riferimento alla documentazione introduttiva per ulteriori informazioni sulla configurazione dello storage persistente:

- "Configurare Microsoft Azure con Azure NetApp Files"
- "Configurare Microsoft Azure con dischi gestiti Azure"
- "Configurare Amazon Web Services"
- "Configurare Google Cloud"

Aggiungere il cluster gestito dal provider privato ad Astra Control Service

È ora possibile aggiungere il cluster privato ad Astra Control Service.

Quando gestisci i cluster Azure Kubernetes Service e Google Kubernetes Engine, tieni presente che hai due

opzioni per l'installazione di Astra Control Provivisioner e la gestione del ciclo di vita:

- Puoi utilizzare Astra Control Service per gestire automaticamente il ciclo di vita di Astra Control Provisioner. Per fare questo, assicurati che Astra Trident non sia installato e Astra Control provisioner non sia abilitato nel cluster che vuoi gestire con Astra Control Service. In questo caso, Astra Control Service abilita automaticamente Astra Control Provisioner quando inizi a gestire il cluster e gli aggiornamenti di Astra Control Provisioner vengono gestiti automaticamente.
- Puoi gestire tu stesso il ciclo di vita di Astra Control Provisioner. A tale scopo, abilita Astra Control Provisioner sul cluster prima di gestire il cluster con Astra Control Service. In questo caso, Astra Control Service rileva che Astra Control Provisioner è già abilitato e non lo reinstalla né gestisce gli aggiornamenti di Astra Control Provisioner. Fare riferimento a. "Abilita Astra Control Provisioner" Per i passaggi, abilita Astra Control provisioner.

Se gestisci i cluster di Amazon Web Services con Astra Control Service, se hai bisogno di backend di storage che possono essere utilizzati solo con Astra Control Provivisioner, devi abilitare Astra Control Provivisioner manualmente sul cluster prima di gestirlo con Astra Control Service. Fare riferimento a. "Abilita Astra Control Provisioner" Per informazioni su come attivare Astra Control Provivioner.

Prima di iniziare

Amazon Web Services

- Il file JSON contiene le credenziali dell'utente IAM che ha creato il cluster. "Scopri come creare un utente IAM".
- Per Amazon FSX per NetApp ONTAP è necessario Astra Control Provisioner. Se intendi usare Amazon FSX per NetApp ONTAP come back-end dello storage per il tuo cluster EKS, fai riferimento alle informazioni Astra Control Provivisioner nel "Requisiti del cluster EKS".
- (Facoltativo) se è necessario fornire `kubectl` Accesso ai comandi per un cluster ad altri utenti IAM che non sono i creatori del cluster, fare riferimento alle istruzioni in "Come posso fornire l'accesso ad altri utenti e ruoli IAM dopo la creazione del cluster in Amazon EKS?".
- Se intendi utilizzare NetApp Cloud Volumes ONTAP come backend di storage, devi configurare Cloud Volumes ONTAP per l'utilizzo con Amazon Web Services. Fare riferimento alla Cloud Volumes ONTAP "documentazione di installazione".

Microsoft Azure

- Il file JSON che contiene l'output della CLI di Azure deve essere presente al momento della creazione dell'entità del servizio. "Scopri come configurare un service principal".

  Avrai inoltre bisogno del tuo ID di abbonamento Azure, se non lo hai aggiunto al file JSON.

- Se si intende utilizzare NetApp Cloud Volumes ONTAP come back-end per lo storage, è necessario configurare Cloud Volumes ONTAP per l'utilizzo con Microsoft Azure. Fare riferimento alla Cloud Volumes ONTAP "documentazione di installazione".

Google Cloud

- È necessario disporre del file della chiave dell'account di servizio per un account di servizio che dispone delle autorizzazioni necessarie. "Scopri come configurare un account di servizio".
- Se il cluster è privato, il "reti autorizzate" Deve consentire l'indirizzo IP di Astra Control Service:

  52.188.218.166/32

- Se si intende utilizzare NetApp Cloud Volumes ONTAP come back-end per lo storage, è necessario configurare Cloud Volumes ONTAP per l'utilizzo con Google Cloud. Fare riferimento alla Cloud Volumes ONTAP "documentazione di installazione".

Fasi

1. (Facoltativo) se stai aggiungendo un cluster Amazon EKS o vuoi gestire da solo l'installazione e gli aggiornamenti di Astra Control Provivisioner, abilita Astra Control Provivisioner sul cluster. Fare riferimento a. "Abilita Astra Control Provisioner" per i passaggi di abilitazione.
2. Aprire l'interfaccia utente Web di Astra Control Service in un browser.
3. Nella dashboard, selezionare **Manage Kubernetes cluster** (Gestisci cluster Kubernetes).

   Seguire le istruzioni per aggiungere il cluster.

4. **Provider**: Seleziona il tuo cloud provider e fornisci le credenziali necessarie per creare una nuova istanza di cloud oppure seleziona un'istanza di cloud esistente da utilizzare.
5. **Amazon Web Services**: Fornisci i dettagli del tuo account utente IAM Amazon Web Services caricando un file JSON o incollando il contenuto del file JSON dagli Appunti.

Il file JSON deve contenere le credenziali dell'utente IAM che ha creato il cluster.

6. **Microsoft Azure**: Fornisci dettagli sull'entità del servizio Azure caricando un file JSON o incollando il contenuto di tale file JSON dagli Appunti.

   Il file JSON deve contenere l'output dell'interfaccia CLI di Azure al momento della creazione dell'entità del servizio. Può anche includere il tuo ID di abbonamento per aggiungerlo automaticamente ad Astra. In caso contrario, è necessario inserire manualmente l'ID dopo aver fornito il codice JSON.

7. **Google Cloud Platform**: Fornire il file delle chiavi dell'account di servizio caricando il file o incollando il contenuto dagli Appunti.

   Astra Control Service utilizza l'account del servizio per rilevare i cluster in esecuzione in Google Kubernetes Engine.

8. **Altro**: Questa scheda è destinata solo ai cluster a gestione automatica.
   a. **Nome istanza cloud**: Fornire un nome per la nuova istanza cloud che verrà creata quando si aggiunge questo cluster. Scopri di più "istanze cloud".
   b. Selezionare **Avanti**.

      Astra Control Service visualizza un elenco di cluster tra i quali è possibile scegliere.

   c. **Cluster**: Selezionare un cluster dall'elenco da aggiungere ad Astra Control Service.

      Durante la selezione dall'elenco dei cluster, prestare attenzione alla colonna **Eligiblity**. Se un cluster è "non idoneo" o "parzialmente idoneo", passare il mouse sullo stato per determinare se si è verificato un problema con il cluster. Ad esempio, potrebbe identificare che il cluster non dispone di un nodo di lavoro.

9. Selezionare **Avanti**.
10. (Facoltativo) **Storage**: Facoltativamente, selezionare la classe di storage che si desidera utilizzare per impostazione predefinita per le applicazioni Kubernetes distribuite in questo cluster.
    a. Per selezionare una nuova classe di storage predefinita per il cluster, attivare la casella di controllo **Assegna una nuova classe di storage predefinita**.
    b. Selezionare una nuova classe di storage predefinita dall'elenco.

Ogni servizio di storage del cloud provider visualizza le seguenti informazioni su prezzo, performance e resilienza:

- Cloud Volumes Service per Google Cloud: Informazioni su prezzi, performance e resilienza
- Google Persistent Disk: Non sono disponibili informazioni su prezzi, performance o resilienza
- Azure NetApp Files: Informazioni su performance e resilienza
- Dischi gestiti Azure: Non sono disponibili informazioni su prezzi, performance o resilienza
- Amazon Elastic Block Store: Nessuna informazione su prezzi, performance o resilienza disponibile
- Amazon FSX per NetApp ONTAP: Nessuna informazione su prezzi, performance o resilienza disponibile
- NetApp Cloud Volumes ONTAP: Non sono disponibili informazioni su prezzi, performance o resilienza

Ogni classe di storage può utilizzare uno dei seguenti servizi:

- "Cloud Volumes Service per Google Cloud"
- "Disco persistente di Google"
- "Azure NetApp Files"
- "Dischi gestiti da Azure"
- "Amazon Elastic Block Store"
- "Amazon FSX per NetApp ONTAP"
- "NetApp Cloud Volumes ONTAP"

Scopri di più "Classi di storage per cluster Amazon Web Services". Scopri di più "Classi di storage per cluster AKS". Scopri di più "Classi di storage per cluster GKE".

c. Selezionare **Avanti**.

d. **Review & Approve** (Rivedi e approva): Verifica dei dettagli della configurazione.

e. Selezionare **Add** per aggiungere il cluster ad Astra Control Service.

Risultato

Se si tratta del primo cluster aggiunto per questo provider cloud, Astra Control Service crea un archivio di oggetti per il provider cloud per i backup delle applicazioni in esecuzione sui cluster idonei. (Quando si aggiungono cluster successivi per questo provider cloud, non vengono creati ulteriori archivi di oggetti). Se è stata specificata una classe di storage predefinita, Astra Control Service imposta la classe di storage predefinita specificata. Per i cluster gestiti in Amazon Web Services o Google Cloud Platform, Astra Control Service crea anche un account admin sul cluster. Queste operazioni possono richiedere alcuni minuti.

Modificare la classe di storage predefinita

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

Modificare la classe di storage predefinita utilizzando Astra Control

È possibile modificare la classe di storage predefinita per un cluster da Astra Control. Se il cluster utilizza un servizio backend di storage precedentemente installato, potrebbe non essere possibile utilizzare questo metodo per modificare la classe di storage predefinita (l'azione **Set as default** non è selezionabile). In questo caso, è possibile Modificare la classe di storage predefinita utilizzando la riga di comando.

Fasi

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

Modificare la classe di storage predefinita utilizzando la riga di comando

È possibile modificare la classe di storage predefinita per un cluster utilizzando i comandi Kubernetes. Questo metodo funziona indipendentemente dalla configurazione del cluster.

Fasi

1. Accedere al cluster Kubernetes.
2. Elencare le classi di storage nel cluster:

```
kubectl get storageclass
```

3. Rimuovere la designazione predefinita dalla classe di storage predefinita. Sostituire <SC_NAME> con il nome della classe di storage:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Contrassegna una classe di storage diversa come predefinita. Sostituire <SC_NAME> con il nome della classe di storage:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confermare la nuova classe di storage predefinita:

```
kubectl get storageclass
```

Aggiungere un cluster a gestione automatica

Aggiungere un cluster pubblico autogestato ad Astra Control Service

Dopo aver configurato l'ambiente, è possibile creare un cluster Kubernetes e aggiungerlo ad Astra Control Service.

Un cluster a gestione automatica è un cluster che viene direttamente provisioning e gestione. Astra Control Service supporta cluster autogestiti eseguiti in un ambiente di cloud pubblico. È possibile aggiungere un cluster a gestione automatica ad Astra Control Service caricando un `kubeconfig.yaml` file. È necessario assicurarsi che il cluster soddisfi i requisiti descritti di seguito.

Distribuzioni Kubernetes supportate

È possibile utilizzare Astra Control Service per gestire i seguenti tipi di cluster pubblici e autogestati:

Distribuzione Kubernetes	Versioni supportate
Kubernetes (upstream)	da 1,27 a 1,29
Rancher Kubernetes Engine (RKE)	RKE 1: Versioni 1.24.17, 1.25.13, 1.26.8 con Rancher Manager 2.7.9 RKE 2: Versioni 1.23.16 e 1.24.13 con Rancher Manager 2.6.13 RKE 2: Versioni 1.24.17, 1.25.14, 1.26.9 con Rancher Manager 2.7.9
Red Hat OpenShift Container Platform	da 4,12 a 4,14

Queste istruzioni presuppongono che sia già stato creato un cluster a gestione automatica.

- Aggiungere il cluster ad Astra Control Service
- Modificare la classe di storage predefinita

Aggiungere il cluster ad Astra Control Service

Dopo aver effettuato l'accesso ad Astra Control Service, il primo passo è iniziare a gestire i cluster. Prima di aggiungere un cluster ad Astra Control Service, è necessario eseguire attività specifiche e assicurarsi che il cluster soddisfi determinati requisiti.

Prima di iniziare

Un cluster a gestione automatica è un cluster che viene direttamente provisioning e gestione. Astra Control Service supporta cluster autogestiti eseguiti in un ambiente di cloud pubblico. I tuoi cluster a gestione autonoma possono utilizzare Astra Control Provivisioner per interfacciarsi con i servizi storage NetApp, oppure possono utilizzare driver Container Storage Interface (CSI) per interfacciarsi con Amazon Elastic Block Store (EBS), Azure Managed Disks e Google Persistent Disk.

Astra Control Service supporta cluster autogestiti che utilizzano le seguenti distribuzioni Kubernetes:

- Red Hat OpenShift Container Platform
- Motore di rancher Kubernetes
- Kubernetes upstream

Il cluster a gestione automatica deve soddisfare i seguenti requisiti:

- Il cluster deve essere accessibile via Internet.
- Se si utilizza o si prevede di utilizzare lo storage abilitato con i driver CSI, i driver CSI appropriati devono essere installati sul cluster. Per ulteriori informazioni sull'utilizzo dei driver CSI per integrare lo storage, consultare la documentazione del servizio di storage.
- Si ha accesso al file cluster kubeconfig che include un solo elemento di contesto. Segui "queste istruzioni" per generare un file kubeconfig.
- Se si aggiunge il cluster utilizzando un file kubeconfig che fa riferimento a un'autorità di certificazione privata, aggiungere la riga seguente al `cluster` sezione del file kubeconfig. In questo modo si permette ad Astra Control di aggiungere il cluster:

  ```
  insecure-skip-tls-verify: true
  ```

- **Solo Rancher**: Quando si gestiscono i cluster di applicazioni in un ambiente Rancher, modificare il contesto predefinito del cluster di applicazioni nel file kubeconfig fornito da Rancher per utilizzare un contesto del piano di controllo invece del contesto del server API Rancher. In questo modo si riduce il carico sul server API Rancher e si migliorano le performance.
- **Requisiti di Astra Control Provisioner**: Dovresti avere un Astra Control Provisioner configurato correttamente, inclusi i suoi componenti Astra Trident, per gestire i cluster.
  - **Rivedi i requisiti dell'ambiente Astra Trident**: Prima di installare o aggiornare Astra Control provisioner, consulta "frontend, backend e configurazioni host supportati".
  - **Abilitare la funzionalità Astra Control Provisioner**: Si consiglia vivamente di installare Astra Trident 23,10 o versione successiva e di abilitare "Astra Control Provivisioner funzionalità di storage avanzate". Nelle prossime release, Astra Control non supporterà Astra Trident se anche Astra Control Provisioner non è abilitato.
  - **Configurare un backend di archiviazione**: Deve essere presente almeno un backend di archiviazione "Configurato in Astra Trident" sul cluster.
  - **Configurare una classe di archiviazione**: Deve essere presente almeno una classe di archiviazione "Configurato in Astra Trident" sul cluster. Se è configurata una classe di archiviazione predefinita, assicurarsi che sia la classe di archiviazione **only** con l'annotazione predefinita.
  - **Configurare un controller snapshot volume e installare una classe snapshot volume**: "Installare un controller per lo snapshot del volume" In modo che le snapshot possano essere

create in Astra Control. "Creare" almeno uno `VolumeSnapshotClass` Utilizzando Astra Trident.

Fasi

1. Nella dashboard, selezionare **Manage Kubernetes cluster** (Gestisci cluster Kubernetes).

   Seguire le istruzioni per aggiungere il cluster.

2. **Provider**: Selezionare la scheda **Other** per aggiungere dettagli sul cluster a gestione automatica.
   a. **Altro**: Fornisci dettagli sul tuo cluster autogestito caricando un `kubeconfig.yaml` o incollando il contenuto di `kubeconfig.yaml` file dagli appunti.

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

3. **Nome credenziale**: Fornire un nome per la credenziale del cluster a gestione automatica che si sta caricando su Astra Control. Per impostazione predefinita, il nome della credenziale viene compilato automaticamente come nome del cluster.
4. **Private route identifier**: Questo campo può essere utilizzato solo con cluster privati.
5. Selezionare **Avanti**.
6. (Facoltativo) **Storage**: Facoltativamente, selezionare la classe di storage che si desidera utilizzare per impostazione predefinita per le applicazioni Kubernetes distribuite in questo cluster.
   a. Per selezionare una nuova classe di storage predefinita per il cluster, attivare la casella di controllo **Assegna una nuova classe di storage predefinita**.
   b. Selezionare una nuova classe di storage predefinita dall'elenco.

   > Ogni servizio di storage del cloud provider visualizza le seguenti informazioni su prezzo, performance e resilienza:
   >
   > - Cloud Volumes Service per Google Cloud: Informazioni su prezzi, performance e resilienza
   > - Google Persistent Disk: Non sono disponibili informazioni su prezzi, performance o resilienza
   > - Azure NetApp Files: Informazioni su performance e resilienza
   > - Dischi gestiti Azure: Non sono disponibili informazioni su prezzi, performance o resilienza
   > - Amazon Elastic Block Store: Nessuna informazione su prezzi, performance o resilienza disponibile
   > - Amazon FSX per NetApp ONTAP: Nessuna informazione su prezzi, performance o resilienza disponibile
   > - NetApp Cloud Volumes ONTAP: Non sono disponibili informazioni su prezzi, performance o resilienza

   Ogni classe di storage può utilizzare uno dei seguenti servizi:

   - "Cloud Volumes Service per Google Cloud"

- "Disco persistente di Google"
  - "Azure NetApp Files"
  - "Dischi gestiti da Azure"
  - "Amazon Elastic Block Store"
  - "Amazon FSX per NetApp ONTAP"
  - "NetApp Cloud Volumes ONTAP"

    Scopri di più "Classi di storage per cluster Amazon Web Services". Scopri di più "Classi di storage per cluster AKS". Scopri di più "Classi di storage per cluster GKE".

c. Selezionare **Avanti**.

d. **Review & Approve** (Rivedi e approva): Verifica dei dettagli della configurazione.

e. Selezionare **Add** per aggiungere il cluster ad Astra Control Service.

Modificare la classe di storage predefinita

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

Modificare la classe di storage predefinita utilizzando Astra Control

È possibile modificare la classe di storage predefinita per un cluster da Astra Control. Se il cluster utilizza un servizio backend di storage precedentemente installato, potrebbe non essere possibile utilizzare questo metodo per modificare la classe di storage predefinita (l'azione **Set as default** non è selezionabile). In questo caso, è possibile Modificare la classe di storage predefinita utilizzando la riga di comando.

Fasi

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

Modificare la classe di storage predefinita utilizzando la riga di comando

È possibile modificare la classe di storage predefinita per un cluster utilizzando i comandi Kubernetes. Questo metodo funziona indipendentemente dalla configurazione del cluster.

Fasi

1. Accedere al cluster Kubernetes.
2. Elencare le classi di storage nel cluster:

```
kubectl get storageclass
```

3. Rimuovere la designazione predefinita dalla classe di storage predefinita. Sostituire <SC_NAME> con il nome della classe di storage:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Contrassegna una classe di storage diversa come predefinita. Sostituire <SC_NAME> con il nome della classe di storage:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confermare la nuova classe di storage predefinita:

```
kubectl get storageclass
```

Aggiungere un cluster privato autogestato ad Astra Control Service

Dopo aver configurato l'ambiente, è possibile creare un cluster Kubernetes e aggiungerlo ad Astra Control Service.

Un cluster a gestione automatica è un cluster che viene direttamente provisioning e gestione. Astra Control Service supporta cluster autogestiti eseguiti in un ambiente di cloud pubblico. È possibile aggiungere un cluster a gestione automatica ad Astra Control Service caricando un `kubeconfig.yaml` file. È necessario assicurarsi che il cluster soddisfi i requisiti descritti di seguito.

Distribuzioni Kubernetes supportate

È possibile utilizzare Astra Control Service per gestire i seguenti tipi di cluster privati a gestione automatica:

Distribuzione Kubernetes	Versioni supportate
Kubernetes (upstream)	da 1,27 a 1,29
Rancher Kubernetes Engine (RKE)	RKE 1: Versioni 1.24.17, 1.25.13, 1.26.8 con Rancher Manager 2.7.9 RKE 2: Versioni 1.23.16 e 1.24.13 con Rancher Manager 2.6.13 RKE 2: Versioni 1.24.17, 1.25.14, 1.26.9 con Rancher Manager 2.7.9
Red Hat OpenShift Container Platform	da 4,12 a 4,14

Queste istruzioni presuppongono che sia già stato creato un cluster privato e che sia stato preparato un metodo sicuro per accedervi in remoto.

Per aggiungere il cluster privato ad Astra Control Service, è necessario eseguire le seguenti operazioni:

1. Installare il connettore Astra
2. Configurare lo storage persistente

3. Aggiungere il cluster privato autogestato ad Astra Control Service

Installare il connettore Astra

Prima di aggiungere un cluster privato, devi installare Astra Connector sul cluster in modo che Astra Control possa comunicare con esso. Fare riferimento a. "Installa la versione precedente di Astra Connector per cluster privati gestiti con flussi di lavoro non nativi di Kubernetes" per istruzioni.

Configurare lo storage persistente

Configurare lo storage persistente per il cluster. Fare riferimento alla documentazione introduttiva per ulteriori informazioni sulla configurazione dello storage persistente:

- "Configurare Microsoft Azure con Azure NetApp Files"
- "Configurare Microsoft Azure con dischi gestiti Azure"
- "Configurare Amazon Web Services"
- "Configurare Google Cloud"

Aggiungere il cluster privato autogestato ad Astra Control Service

È ora possibile aggiungere il cluster privato ad Astra Control Service.

Prima di iniziare

Un cluster a gestione automatica è un cluster che viene direttamente provisioning e gestione. Astra Control Service supporta cluster autogestiti eseguiti in un ambiente di cloud pubblico. I tuoi cluster a gestione autonoma possono utilizzare Astra Control Provivisioner per interfacciarsi con i servizi storage NetApp, oppure possono utilizzare driver Container Storage Interface (CSI) per interfacciarsi con Amazon Elastic Block Store (EBS), Azure Managed Disks e Google Persistent Disk.

Astra Control Service supporta cluster autogestiti che utilizzano le seguenti distribuzioni Kubernetes:

- Red Hat OpenShift Container Platform
- Motore di rancher Kubernetes
- Kubernetes upstream

Il cluster a gestione automatica deve soddisfare i seguenti requisiti:

- Il cluster deve essere accessibile via Internet.
- Se si utilizza o si prevede di utilizzare lo storage abilitato con i driver CSI, i driver CSI appropriati devono essere installati sul cluster. Per ulteriori informazioni sull'utilizzo dei driver CSI per integrare lo storage, consultare la documentazione del servizio di storage.
- Si ha accesso al file cluster kubeconfig che include un solo elemento di contesto. Segui "queste istruzioni" per generare un file kubeconfig.
- Se si aggiunge il cluster utilizzando un file kubeconfig che fa riferimento a un'autorità di certificazione privata, aggiungere la riga seguente al `cluster` sezione del file kubeconfig. In questo modo si permette ad Astra Control di aggiungere il cluster:

  ```
  insecure-skip-tls-verify: true
  ```

- **Solo Rancher**: Quando si gestiscono i cluster di applicazioni in un ambiente Rancher, modificare il contesto predefinito del cluster di applicazioni nel file kubeconfig fornito da Rancher per utilizzare un contesto del piano di controllo invece del contesto del server API Rancher. In questo modo si riduce il carico sul server API Rancher e si migliorano le performance.
- **Requisiti di Astra Control Provisioner**: Dovresti avere un Astra Control Provisioner configurato correttamente, inclusi i suoi componenti Astra Trident, per gestire i cluster.
  - **Rivedi i requisiti dell'ambiente Astra Trident**: Prima di installare o aggiornare Astra Control provisioner, consulta "frontend, backend e configurazioni host supportati".
  - **Abilitare la funzionalità Astra Control Provisioner**: Si consiglia vivamente di installare Astra Trident 23,10 o versione successiva e di abilitare "Astra Control Provivisioner funzionalità di storage avanzate". Nelle prossime release, Astra Control non supporterà Astra Trident se anche Astra Control Provisioner non è abilitato.
  - **Configurare un backend di archiviazione**: Deve essere presente almeno un backend di archiviazione "Configurato in Astra Trident" sul cluster.
  - **Configurare una classe di archiviazione**: Deve essere presente almeno una classe di archiviazione "Configurato in Astra Trident" sul cluster. Se è configurata una classe di archiviazione predefinita, assicurarsi che sia la classe di archiviazione **only** con l'annotazione predefinita.
  - **Configurare un controller snapshot volume e installare una classe snapshot volume**: "Installare un controller per lo snapshot del volume" In modo che le snapshot possano essere

create in Astra Control. "Creare" almeno uno `VolumeSnapshotClass` Utilizzando Astra Trident.

Fasi

1. Nella dashboard, selezionare **Manage Kubernetes cluster** (Gestisci cluster Kubernetes).

   Seguire le istruzioni per aggiungere il cluster.

2. **Provider**: Selezionare la scheda **Other** per aggiungere dettagli sul cluster a gestione automatica.
3. **Altro**: Fornisci dettagli sul tuo cluster autogestito caricando un `kubeconfig.yaml` o incollando il contenuto di `kubeconfig.yaml` file dagli appunti.

   > Se crei il tuo `kubeconfig` file, è necessario definire solo **un** elemento di contesto al suo interno. Fare riferimento a. "queste istruzioni" per informazioni sulla creazione `kubeconfig` file.

4. **Nome credenziale**: Fornire un nome per la credenziale del cluster a gestione automatica che si sta caricando su Astra Control. Per impostazione predefinita, il nome della credenziale viene compilato automaticamente come nome del cluster.
5. **Private route identifier**: Immettere l'identificativo di percorso privato, che è possibile ottenere da Astra Connector. Se si esegue una query su Astra Connector tramite `kubectl get astraconnector -n astra-connector` l'identificatore di route privato viene definito `ASTRACONNECTORID`.

   > L'identificatore di route privato è il nome associato al connettore Astra che consente la gestione di un cluster Kubernetes privato da parte di Astra. In questo contesto, un cluster privato è un cluster Kubernetes che non espone il proprio server API a Internet.

6. Selezionare **Avanti**.
7. (Facoltativo) **Storage**: Facoltativamente, selezionare la classe di storage che si desidera utilizzare per impostazione predefinita per le applicazioni Kubernetes distribuite in questo cluster.
   a. Per selezionare una nuova classe di storage predefinita per il cluster, attivare la casella di controllo **Assegna una nuova classe di storage predefinita**.
   b. Selezionare una nuova classe di storage predefinita dall'elenco.

Ogni servizio di storage del cloud provider visualizza le seguenti informazioni su prezzo, performance e resilienza:

- Cloud Volumes Service per Google Cloud: Informazioni su prezzi, performance e resilienza
- Google Persistent Disk: Non sono disponibili informazioni su prezzi, performance o resilienza
- Azure NetApp Files: Informazioni su performance e resilienza
- Dischi gestiti Azure: Non sono disponibili informazioni su prezzi, performance o resilienza
- Amazon Elastic Block Store: Nessuna informazione su prezzi, performance o resilienza disponibile
- Amazon FSX per NetApp ONTAP: Nessuna informazione su prezzi, performance o resilienza disponibile
- NetApp Cloud Volumes ONTAP: Non sono disponibili informazioni su prezzi, performance o resilienza

Ogni classe di storage può utilizzare uno dei seguenti servizi:

- "Cloud Volumes Service per Google Cloud"
- "Disco persistente di Google"
- "Azure NetApp Files"
- "Dischi gestiti da Azure"
- "Amazon Elastic Block Store"
- "Amazon FSX per NetApp ONTAP"
- "NetApp Cloud Volumes ONTAP"

Scopri di più "Classi di storage per cluster Amazon Web Services". Scopri di più "Classi di storage per cluster AKS". Scopri di più "Classi di storage per cluster GKE".

c. Selezionare **Avanti**.
d. **Review & Approve** (Rivedi e approva): Verifica dei dettagli della configurazione.
e. Selezionare **Add** per aggiungere il cluster ad Astra Control Service.

Modificare la classe di storage predefinita

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

Modificare la classe di storage predefinita utilizzando Astra Control

È possibile modificare la classe di storage predefinita per un cluster da Astra Control. Se il cluster utilizza un servizio backend di storage precedentemente installato, potrebbe non essere possibile utilizzare questo metodo per modificare la classe di storage predefinita (l'azione **Set as default** non è selezionabile). In questo caso, è possibile Modificare la classe di storage predefinita utilizzando la riga di comando.

Fasi

1. Nell'interfaccia utente di Astra Control Service, selezionare **Clusters**.

2. Nella pagina **Clusters**, selezionare il cluster che si desidera modificare.
3. Selezionare la scheda **Storage**.
4. Selezionare la categoria **classi di storage**.
5. Selezionare il menu **azioni** per la classe di storage che si desidera impostare come predefinita.
6. Selezionare **Imposta come predefinito**.

Modificare la classe di storage predefinita utilizzando la riga di comando

È possibile modificare la classe di storage predefinita per un cluster utilizzando i comandi Kubernetes. Questo metodo funziona indipendentemente dalla configurazione del cluster.

Fasi

1. Accedere al cluster Kubernetes.
2. Elencare le classi di storage nel cluster:

```
kubectl get storageclass
```

3. Rimuovere la designazione predefinita dalla classe di storage predefinita. Sostituire <SC_NAME> con il nome della classe di storage:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-
class":"false"}}}'
```

4. Contrassegna una classe di storage diversa come predefinita. Sostituire <SC_NAME> con il nome della classe di storage:

```
kubectl patch storageclass <SC_NAME> -p '{"metadata":
{"annotations":{"storageclass.kubernetes.io/is-default-class":"true"}}}'
```

5. Confermare la nuova classe di storage predefinita:

```
kubectl get storageclass
```

Controllare la versione di Astra Trident

Per aggiungere un cluster a gestione autonoma che utilizzi Astra Control Provivisioner o Astra Trident per i servizi di storage, assicurati che la versione installata di Astra Trident sia la 23,10 o più recente.

Fasi

1. Determina la versione di Astra Trident che stai utilizzando:

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

Se Astra Trident è installato, viene visualizzato un output simile a quanto segue:

```
NAME      VERSION
trident   24.02.0
```

Se Astra Trident non è installato, viene visualizzato un output simile a quanto segue:

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

2. Effettuare una delle seguenti operazioni:
   - Se utilizzi Astra Trident 23,01 o versione precedente, utilizza questi elementi "istruzioni" Per effettuare l'aggiornamento a una versione più recente di Astra Trident prima di effettuare l'aggiornamento a Astra Control Provivisioner. È possibile "eseguire un aggiornamento diretto" A Astra Control Provivisioner 24,02 se il tuo Astra Trident si trova all'interno di una finestra a quattro release della versione 24,02. Ad esempio, puoi eseguire l'upgrade direttamente da Astra Trident 23,04 a Astra Control Provisioner 24,02.
   - Se stai eseguendo Astra Trident 23,10 o versione successiva, verifica che Astra Control provisioner sia stato "attivato". Astra Control Provisioner non funzionerà con le versioni di Astra Control Center precedenti alla 23,10. "Aggiorna Astra Control provisioner" In modo che abbia la stessa versione di Astra Control Center che stai effettuando l'aggiornamento per accedere alle funzionalità più recenti.
3. Assicurarsi che i pod siano in funzione:

```
kubectl get pods -n trident
```

4. Controllare se le classi di storage utilizzano i driver Astra Trident supportati. Il nome del provider deve essere `csi.trident.netapp.io`. Fare riferimento al seguente esempio:

```
kubectl get sc
```

Esempio di risposta:

```
NAME                    PROVISIONER                    RECLAIMPOLICY
VOLUMEBINDINGMODE   ALLOWVOLUMEEXPANSION   AGE
ontap-gold (default)    csi.trident.netapp.io          Delete
Immediate           true                   5d23h
```

Creare un file kubeconfig

È possibile aggiungere un cluster ad Astra Control Service utilizzando un file kubeconfig.

A seconda del tipo di cluster che si desidera aggiungere, potrebbe essere necessario creare manualmente un file kubeconfig per il cluster utilizzando passaggi specifici.

- Creare un file kubeconfig per i cluster Amazon EKS
- Creare un file kubeconfig per Red Hat OpenShift Service su cluster AWS (ROSA)
- Creare un file kubeconfig per altri tipi di cluster

Creare un file kubeconfig per i cluster Amazon EKS

Segui queste istruzioni per creare un file kubeconfig e un token secret permanente per i cluster Amazon EKS. Per i cluster ospitati in EKS è necessario un token secret permanente.

Fasi

1. Seguire le istruzioni nella documentazione di Amazon per generare un file kubeconfig:

   "Creazione o aggiornamento di un file kubeconfig per un cluster Amazon EKS"

2. Creare un account di servizio come segue:

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

      Modificare il nome dell'account di servizio in base alle necessità. Lo spazio dei nomi `kube-system` è necessario per questi passaggi. Se si modifica il nome dell'account di servizio, è necessario apportare le stesse modifiche nei seguenti passaggi.

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

+

```yaml
apiVersion: v1
kind: ServiceAccount
metadata:
  name: astra-admin-account
  namespace: kube-system
```

3. Applicare l'account del servizio:

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

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

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

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: astra-admin-binding
roleRef:
  apiGroup: rbac.authorization.k8s.io
  kind: ClusterRole
  name: cluster-admin
subjects:
- kind: ServiceAccount
  name: astra-admin-account
  namespace: kube-system
```

5. Applicare l'associazione del ruolo del cluster:

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

6. Creare un file token secret dell'account di servizio chiamato `astracontrol-secret.yaml`.

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

```yaml
apiVersion: v1
kind: Secret
metadata:
  annotations:
    kubernetes.io/service-account.name: astra-admin-account
  name: astra-admin-account
  namespace: kube-system
type: kubernetes.io/service-account-token
```

7. Applicare il token secret:

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

8. Recuperare il token secret:

```
kubectl get secret astra-admin-account -n kube-system -o
jsonpath='{.data.token}' | base64 -d
```

9. Sostituire `user` Sezione del file kubeconfig AWS EKS con il token, come mostrato nell'esempio seguente:

```
user:
    token: k8s-aws-
v1.aHR0cHM6Ly9zdHMudXMtd2VzdC0yLmFtYXpvbmF3cy5jb20vP0FjdGlvbj1HZXRDYWxsZ
XJJZGVudGl0eSZWZXJzaW9uPTIwMTEtMDYtMTUmWC1BbXotQWxnb3JpdGhtPUFXUzQtSE1BQ
y1TSEEyNTYmWC1BbXotQ3JlZGVudGlhbD1BS0lBM1JEWDdKU0haWU9LSEQ2SyUyRjIwMjMwN
DAzJTJGdXMtd2VzdC0yJTJGc3RzJTJGYXdzNF9yZXF1ZXN0JlgtQW16LURhdGU9MjAyMzA0M
DNUMjA0MzQwWiZYLUFtei1FeHBpcmVzPTYwJlgtQW16LVNpZ25lZEhlYWRlcnM9aG9zdCUzQ
ngtazhzLWF3cy1pZCZYLUFtei1TaWduYXR1cmU9YjU4ZWM0NzdiM2NkZGYxNGRhNzU4MGI2Z
WQ2zY2NzI2YWIwM2UyNThjMjRhNTJjNmVhNjc4MTRlNjJkOTg2Mg
```

Creare un file kubeconfig per Red Hat OpenShift Service su cluster AWS (ROSA)

Segui queste istruzioni per creare un file kubeconfig per Red Hat OpenShift Service su cluster AWS (ROSA).

Fasi

1. Accedere al cluster ROSA.
2. Creare un account di servizio:

```
oc create sa astracontrol-service-account
```

3. Aggiungere un ruolo cluster:

```
oc adm policy add-cluster-role-to-user cluster-admin -z astracontrol-
service-account
```

4. Utilizzando l'esempio seguente, creare un file di configurazione segreto dell'account di servizio:

```
<strong>secret-astra-sa.yaml</strong>
```

```
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-account"
type: kubernetes.io/service-account-token
```

5. Creare il segreto:

```
oc create -f secret-astra-sa.yaml
```

6. Modificare l'account di servizio creato e aggiungere il nome segreto dell'account del servizio Astra Control
   a. `secrets` sezione:

```
oc edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-dvfcd
kind: ServiceAccount
metadata:
  creationTimestamp: "2023-08-04T04:18:30Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "169770"
  uid: 965fa151-923f-4fbd-9289-30cad15998ac
secrets:
- name: astracontrol-service-account-dockercfg-dvfcd
- name: secret-astracontrol-service-account ####ADD THIS ONLY####
```

7. 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-dvfcd"},
{ "name": "secret-astracontrol-service-account"}
]
```

Gli indici di ciascun elemento in `secrets` l'array inizia con 0. Nell'esempio precedente, l'indice per `astracontrol-service-account-dockercfg-dvfcd` sarebbe 0 e l'indice per `secret-astracontrol-service-account` sarebbe 1. Nell'output, annotare il numero dell'indice per il segreto dell'account del servizio. Questo numero di indice sarà necessario nella fase successiva.

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

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

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

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

CONTEXT=$(kubectl config current-context)

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

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

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

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

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

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

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

# Set context to use token user
```

```
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token
-user

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

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

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

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

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

9. (Facoltativo) rinominare il kubeconfig con un nome significativo per il cluster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Creare un file kubeconfig per altri tipi di cluster

Segui queste istruzioni per creare un file kubeconfig con ruolo limitato o esteso per i cluster Rancher, Upstream Kubernetes e Red Hat OpenShift.

Per i cluster gestiti utilizzando kubeconfig, è possibile creare un'autorizzazione limitata o un ruolo di amministratore di autorizzazioni esteso per Astra Control Service.

Questa procedura consente di creare una configurazione separata se uno dei seguenti scenari si applica al proprio ambiente:

- Si desidera limitare le autorizzazioni di Astra Control sui cluster gestiti
- Si utilizzano più contesti e non è possibile utilizzare il kubeconfig di Astra Control predefinito configurato durante l'installazione oppure un ruolo limitato con un singolo contesto non funziona nell'ambiente

Prima di iniziare

Prima di completare la procedura, assicurarsi di disporre dei seguenti elementi per il cluster che si desidera gestire:

- R "versione supportata" di kubectl è installato.
- Kubectl accesso al cluster che si intende aggiungere e gestire con Astra Control Service

> Per questa procedura, non è necessario l'accesso kubectl al cluster che esegue Astra Control Service.

- Un kubeconfig attivo per il cluster che si intende gestire con i diritti di amministratore del cluster per il contesto attivo

Fasi

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

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

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

   b. Applicare l'account del servizio:

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

2. Creare uno dei seguenti ruoli del cluster con autorizzazioni sufficienti per la gestione di un cluster da parte di Astra Control:

Ruolo cluster limitato

Questo ruolo contiene le autorizzazioni minime necessarie per gestire un cluster da Astra Control:

a. Creare un `ClusterRole` file chiamato, ad esempio, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:

# Get, List, Create, and Update all resources
# Necessary to backup and restore all resources in an app
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - get
  - list
  - create
  - patch

# Delete Resources
# Necessary for in-place restore and AppMirror failover
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - crd.projectcalico.org
  - extensions
  - networking.k8s.io
  - policy
  - rbac.authorization.k8s.io
  - snapshot.storage.k8s.io
  - trident.netapp.io
  resources:
  - configmaps
  - cronjobs
  - daemonsets
  - deployments
```

```
    - horizontalpodautoscalers
    - ingresses
    - jobs
    - namespaces
    - networkpolicies
    - persistentvolumeclaims
    - poddisruptionbudgets
    - pods
    - podtemplates
    - replicasets
    - replicationcontrollers
    - replicationcontrollers/scale
    - rolebindings
    - roles
    - secrets
    - serviceaccounts
    - services
    - statefulsets
    - tridentmirrorrelationships
    - tridentsnapshotinfos
    - volumesnapshots
    - volumesnapshotcontents
    verbs:
    - delete

  # Watch resources
  # Necessary to monitor progress
  - apiGroups:
    - ""
    resources:
    - pods
    - replicationcontrollers
    - replicationcontrollers/scale
    verbs:
    - watch

  # Update resources
  - apiGroups:
    - ""
    - build.openshift.io
    - image.openshift.io
    resources:
    - builds/details
    - replicationcontrollers
    - replicationcontrollers/scale
    - imagestreams/layers
```

```
  - imagestreamtags
  - imagetags
  verbs:
  - update
```

b. (Solo per i cluster OpenShift) aggiungere quanto segue alla fine di `astra-admin-account.yaml` file:

```
# OpenShift security
- apiGroups:
  - security.openshift.io
  resources:
  - securitycontextconstraints
  verbs:
  - use
  - update
```

c. Applicare il ruolo del cluster:

```
kubectl apply -f astra-admin-account.yaml
```

Ruolo cluster esteso

Questo ruolo contiene autorizzazioni estese per un cluster da gestire con Astra Control. È possibile utilizzare questo ruolo se si utilizzano più contesti e non è possibile utilizzare il kubeconfig di Astra Control predefinito configurato durante l'installazione oppure se un ruolo limitato con un singolo contesto non funziona nell'ambiente:

> Quanto segue `ClusterRole` I passaggi sono un esempio generale di Kubernetes. Consultare la documentazione della distribuzione Kubernetes per istruzioni specifiche sull'ambiente in uso.

a. Creare un `ClusterRole` file chiamato, ad esempio, `astra-admin-account.yaml`.

```
<strong>astra-admin-account.yaml</strong>
```

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: astra-admin-account
rules:
- apiGroups:
  - '*'
  resources:
  - '*'
  verbs:
  - '*'
- nonResourceURLs:
  - '*'
  verbs:
  - '*'
```

b. Applicare il ruolo del cluster:

```
kubectl apply -f astra-admin-account.yaml
```

3. Creare l'associazione del ruolo del cluster all'account del servizio per il ruolo del cluster:

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

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

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

b. Applicare l'associazione del ruolo del cluster:

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

4. Creare e applicare il token secret:
   a. Creare un file token secret chiamato `secret-astracontrol-service-account.yaml`.

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

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: secret-astracontrol-service-account
  namespace: default
  annotations:
    kubernetes.io/service-account.name: "astracontrol-service-
account"
type: kubernetes.io/service-account-token
```

   b. Applicare il token secret:

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

5. Aggiungere il token secret all'account del servizio aggiungendo il nome a `secrets` array (l'ultima riga dell'esempio seguente):

```
kubectl edit sa astracontrol-service-account
```

```
apiVersion: v1
imagePullSecrets:
- name: astracontrol-service-account-dockercfg-48xhx
kind: ServiceAccount
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |

{"apiVersion":"v1","kind":"ServiceAccount","metadata":{"annotations":{},
"name":"astracontrol-service-account","namespace":"default"}}
  creationTimestamp: "2023-06-14T15:25:45Z"
  name: astracontrol-service-account
  namespace: default
  resourceVersion: "2767069"
  uid: 2ce068c4-810e-4a96-ada3-49cbf9ec3f89
secrets:
- name: astracontrol-service-account-dockercfg-48xhx
<strong>- name: secret-astracontrol-service-account</strong>
```

6. 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-48xhx"},
{ "name": "secret-astracontrol-service-account"}
]
```

Gli indici di ciascun elemento in `secrets` l'array inizia con 0. Nell'esempio precedente, l'indice per `astracontrol-service-account-dockercfg-48xhx` sarebbe 0 e l'indice per `secret-astracontrol-service-account` sarebbe 1. Nell'output, annotare il numero dell'indice per il segreto dell'account del servizio. Questo numero di indice è necessario nel passaggio successivo.

7. Generare il kubeconfig come segue:
   a. Creare un `create-kubeconfig.sh` file.
   b. Sostituire `TOKEN_INDEX` all'inizio del seguente script con il valore corretto.

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

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

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

CONTEXT=$(kubectl config current-context)

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

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

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

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

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

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

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

# Set context to use token user
```

```
kubectl config --kubeconfig ${KUBECONFIG_FILE}.tmp \
  set-context ${NEW_CONTEXT} --user ${CONTEXT}-${NAMESPACE}-token-
user

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

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

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

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

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

8. (Facoltativo) rinominare il kubeconfig con un nome significativo per il cluster.

```
mv kubeconfig-sa YOUR_CLUSTER_NAME_kubeconfig
```

Quali sono le prossime novità?

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

- "Inizia a gestire le app"
- "Proteggi le app"
- "Clonare le applicazioni"
- "Impostare la fatturazione"
- "Invitare e gestire gli utenti"
- "Gestire le credenziali del cloud provider"
- "Gestire le notifiche"
- "Implementa un'istanza autogestita di Astra Control"

Video di Astra Control Service

Scopri NetApp TV per i contenuti video più recenti con Astra Control Service. NetApp TV include video che mostrano alcune funzionalità di Astra Control Service o mostrano come

completare determinate attività comuni.

"Video di Astra Control Service"

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

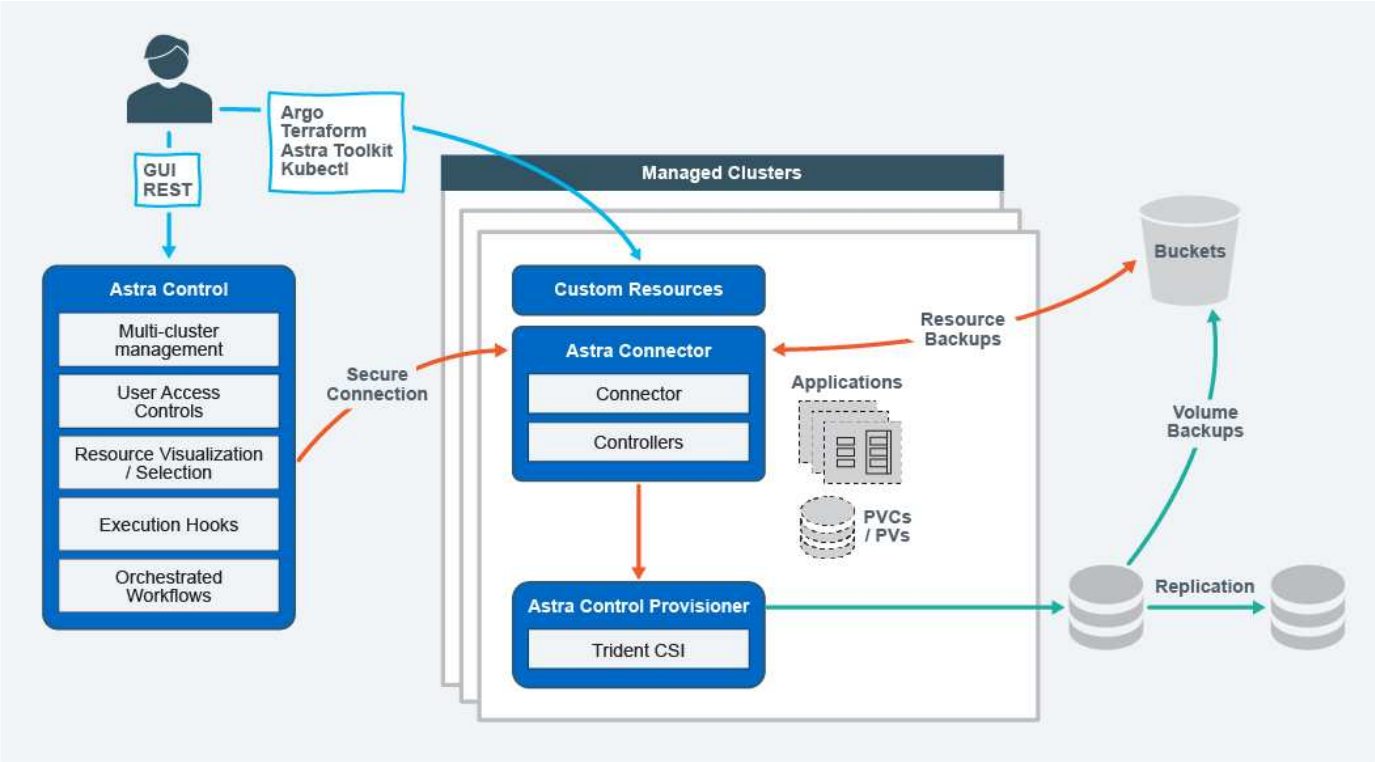
Sposta:

- 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.



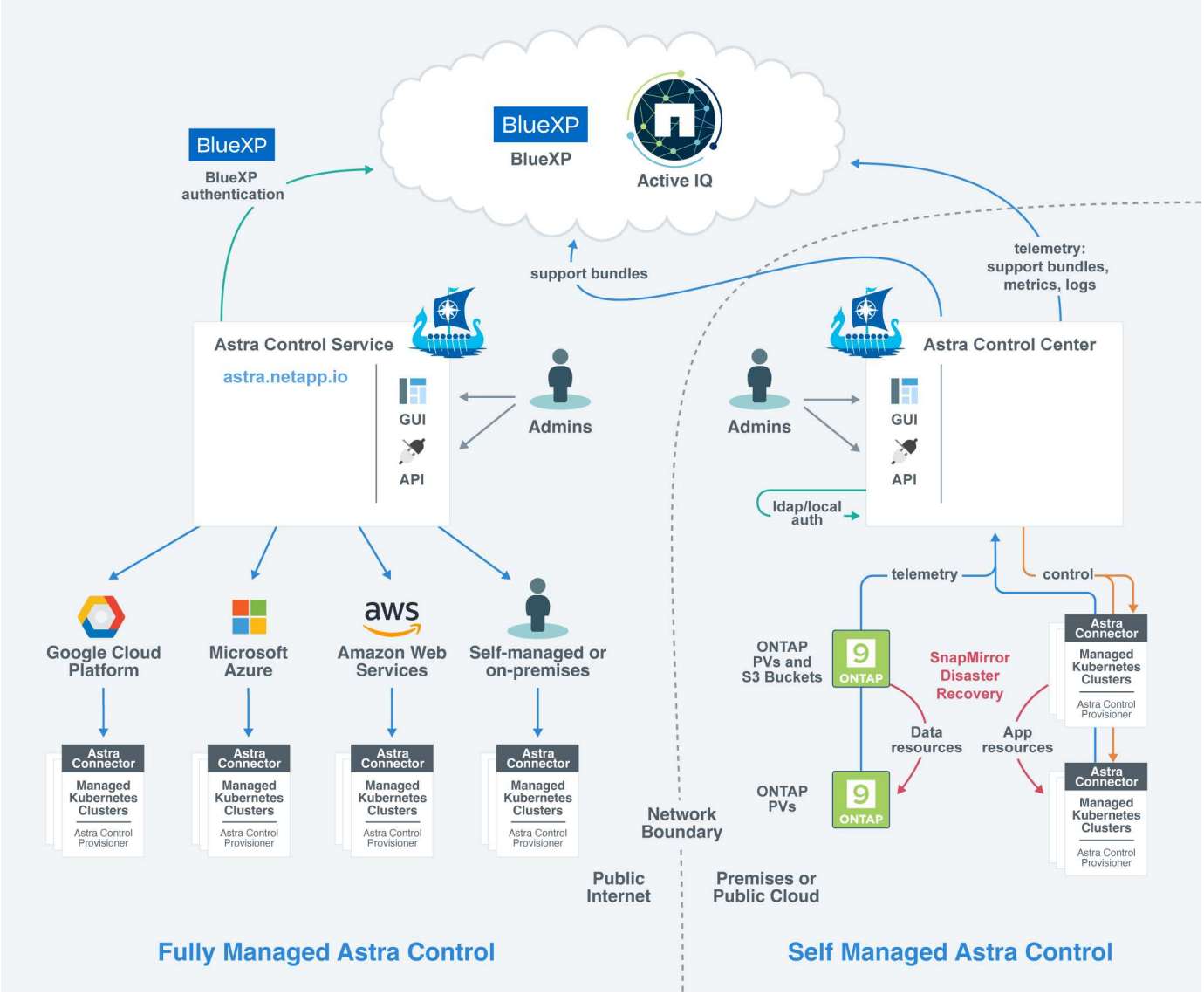
Astra Control è costruito su quattro componenti complementari:

- **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".

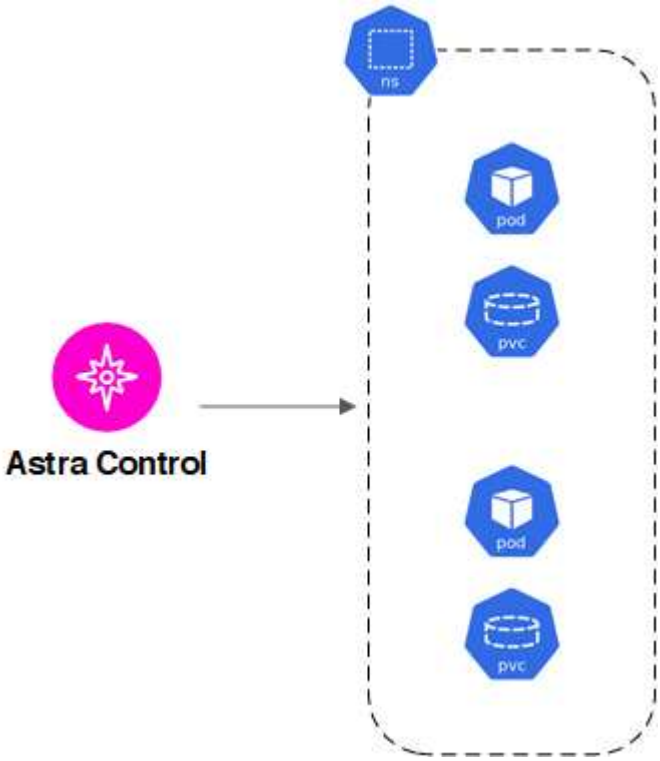
NetApp Cloud Volumes ONTAP

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

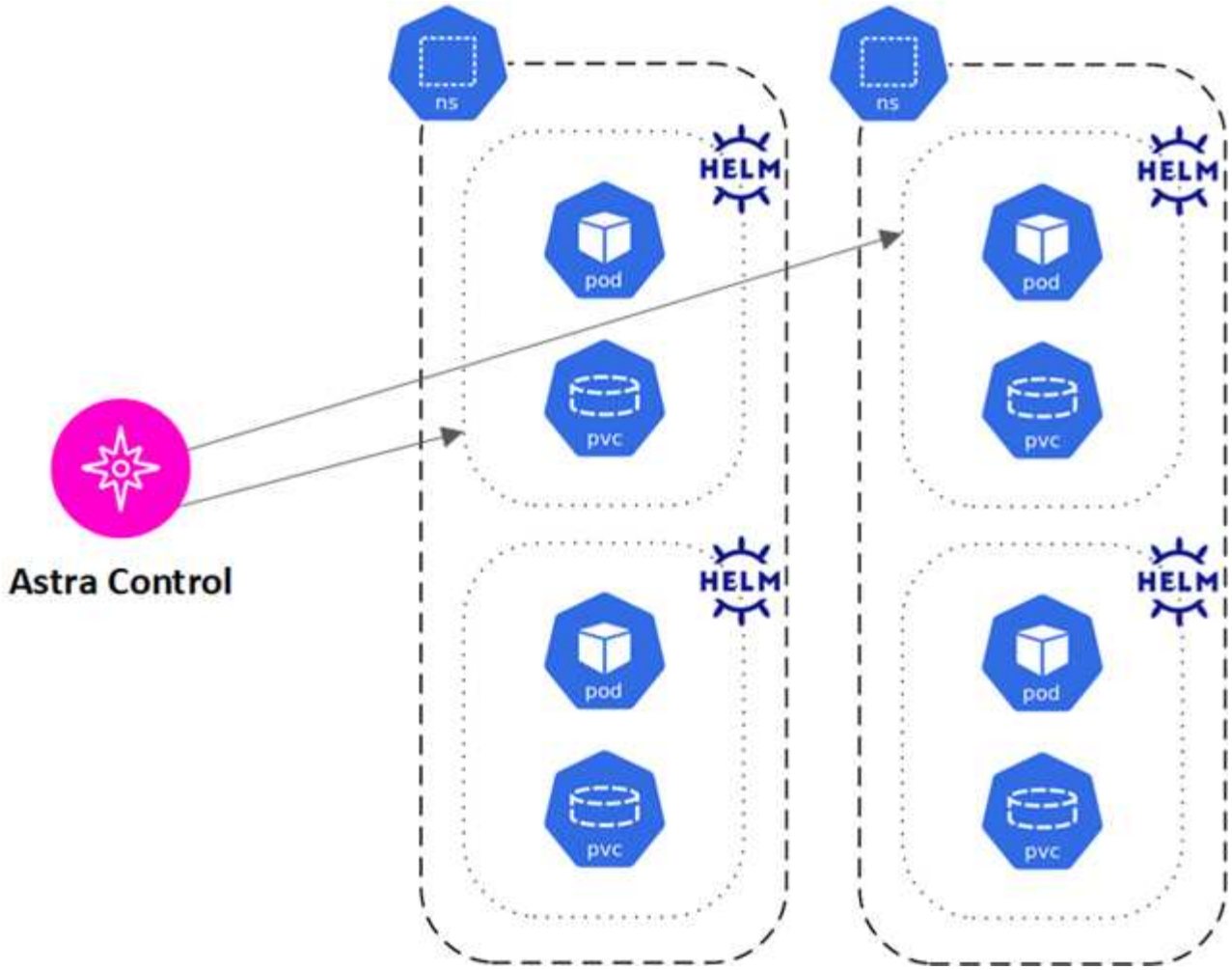
Gestione delle applicazioni

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:

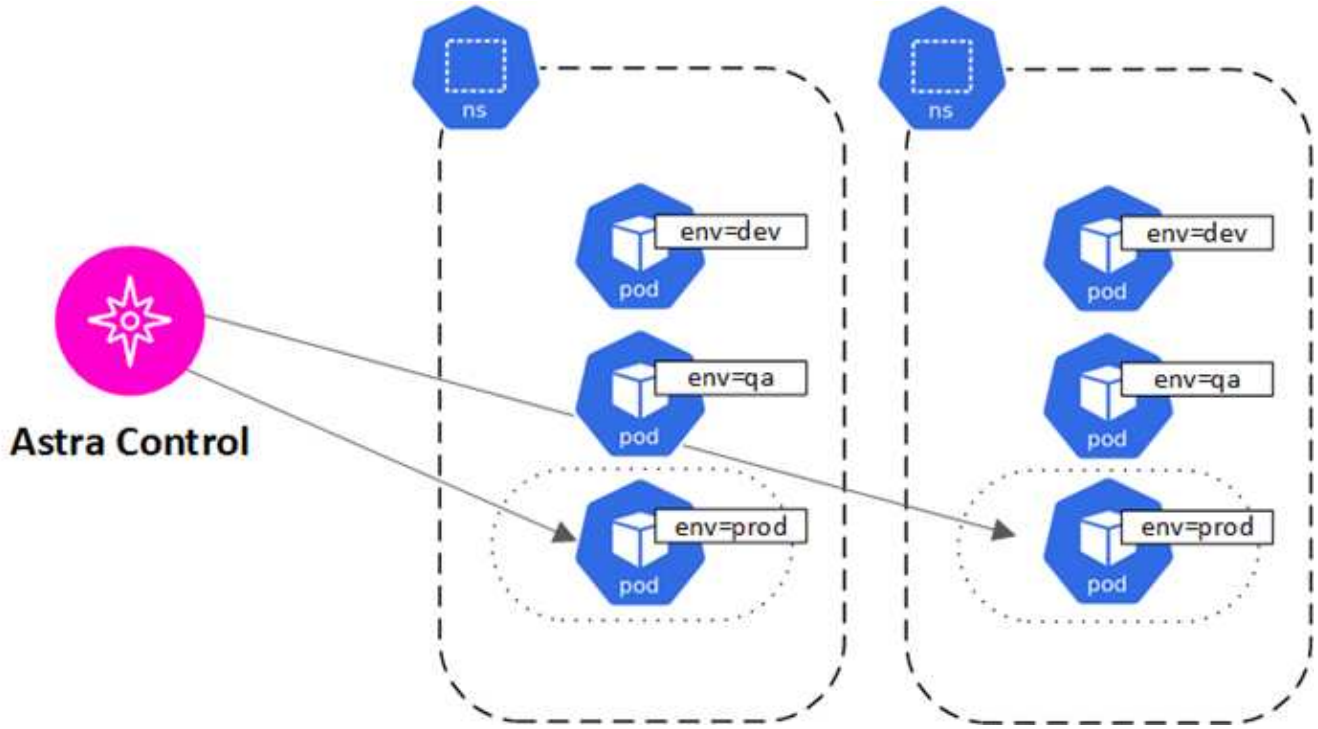
- Uno spazio dei nomi, che include tutte le risorse dello spazio dei nomi



- 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"

Utilizzare Astra Control Service

Accedere a Astra Control Service

Astra Control Service è accessibile tramite un'interfaccia utente basata su SaaS visitando il sito https://astra.netapp.io.

> È possibile utilizzare il Single Sign-on per accedere utilizzando le credenziali della directory aziendale (identità federata). Per ulteriori informazioni, visitare il sito "Centro assistenza" Quindi selezionare **Cloud Central sign-in options** (Opzioni di accesso Cloud Central).

Prima di iniziare

- "Un ID utente BlueXP".
- "Un nuovo account Astra Control" oppure "invito a un account esistente".
- Un browser Web supportato.

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

Fasi

1. Aprire un browser Web e visitare il sito Web all'indirizzo https://astra.netapp.io.
2. Accedi usando le tue credenziali NetApp BlueXP.

Gestire e proteggere le applicazioni

Inizia a gestire le app

Dopo di lei "Aggiungere un cluster Kubernetes ad Astra Control", È possibile installare le applicazioni sul cluster (al di fuori di Astra Control), quindi andare alla pagina delle applicazioni in Astra Control per definire le applicazioni.

Puoi definire e gestire le app che includono risorse storage con pod in esecuzione o app che includono risorse storage senza pod in esecuzione. Le app che non hanno pod in esecuzione sono note come applicazioni solo dati.

Requisiti di gestione delle applicazioni

Astra Control ha i seguenti requisiti di gestione delle applicazioni:

- **Licensing**: Per gestire più di 10 spazi dei nomi, è necessario un abbonamento Astra Control.
- **Namespace**: Le applicazioni possono essere definite all'interno di uno o più namespace specificati su un singolo cluster utilizzando Astra Control. Un'applicazione può contenere risorse che spaziano da più spazi dei nomi all'interno dello stesso cluster. Astra Control non supporta la possibilità di definire le applicazioni in più cluster.
- **Storage class**: Se si installa un'applicazione con una classe di storage impostata in modo esplicito e si deve clonare l'applicazione, il cluster di destinazione per l'operazione di clone deve avere la classe di storage specificata in origine. La clonazione di un'applicazione con una classe di storage esplicitamente

impostata su un cluster che non ha la stessa classe di storage non avrà esito positivo.

- **Kubernetes resources**: Le applicazioni che utilizzano Kubernetes Resources non raccolte da Astra Control potrebbero non disporre di funzionalità complete di gestione dei dati delle applicazioni. Astra Control raccoglie le seguenti risorse Kubernetes:

`ClusterRole`	`ClusterRoleBinding`	`ConfigMap`
`CronJob`	`CustomResourceDefinition`	`CustomResource`
`DaemonSet`	`DeploymentConfig`	`HorizontalPodAutoscaler`
`Ingress`	`MutatingWebhook`	`NetworkPolicy`
`PersistentVolumeClaim`	`Pod`	`PodDisruptionBudget`
`PodTemplate`	`ReplicaSet`	`Role`
`RoleBinding`	`Route`	`Secret`
`Service`	`ServiceAccount`	`StatefulSet`
`ValidatingWebhook`		

Metodi di installazione delle applicazioni supportati

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

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

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

- **Helm 3**: Se utilizzi Helm per installare le app, Astra Control richiede Helm versione 3. La gestione e la clonazione delle applicazioni installate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. La gestione delle applicazioni installate con Helm 2 non è supportata.
- **Applicazioni distribuite dall'operatore**: Astra Control supporta le applicazioni installate con operatori con ambito namespace, in generale progettati con un'architettura "pass-by-value" piuttosto che "pass-by-reference". Un operatore e l'applicazione che installa devono utilizzare lo stesso namespace; potrebbe essere necessario modificare il file .yaml di implementazione per l'operatore per assicurarsi che questo sia il caso.

  Di seguito sono riportate alcune applicazioni per operatori che seguono questi modelli:

  - "Apache K8ssandra"

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

  - "Ci Jenkins"
  - "Cluster XtraDB Percona"

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

Installa le app sul tuo cluster

Dopo di che "aggiunto il cluster" In Astra Control, puoi installare le app o gestire quelle esistenti sul cluster. È possibile gestire qualsiasi applicazione con un ambito per uno o più spazi dei nomi.

Astra Control gestirà le applicazioni stateful solo se lo storage si trova su una classe di storage supportata da Astra Control. Astra Control Service supporta qualsiasi classe di storage supportata da Astra Control Provivioner o da un driver CSI generico.

- "Scopri le classi di storage per i cluster GKE"
- "Scopri le classi di storage per i cluster AKS"
- "Scopri le classi di storage per i cluster AWS"

Definire le applicazioni

Una volta che Astra Control rileva gli spazi dei nomi sui cluster, è possibile definire le applicazioni che si desidera gestire. È possibile scegliere gestisci un'applicazione che spazia uno o più spazi dei nomi oppure gestire un intero namespace come singola applicazione. Tutto questo si riduce al livello di granularità necessario per le operazioni di protezione dei dati.

Sebbene Astra Control ti consenta di gestire separatamente entrambi i livelli della gerarchia (lo spazio dei nomi e le applicazioni nello spazio dei nomi o negli spazi dei nomi), la Best practice 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.

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 come un'applicazione con un singolo spazio dei nomi.

Prima di iniziare

- Un cluster Kubernetes aggiunto ad Astra Control.
- Una o più applicazioni installate sul cluster. Scopri di più sui metodi di installazione delle app supportati.
- Spazi dei nomi esistenti nel cluster Kubernetes aggiunto ad Astra Control.
- (Facoltativo) un'etichetta Kubernetes su qualsiasi "Risorse Kubernetes supportate".

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, "Consultare la documentazione ufficiale di Kubernetes".

A proposito di questa attività

- Prima di iniziare, dovresti anche capire "gestione degli spazi dei nomi standard e di sistema".

- Se si prevede di utilizzare più spazi dei nomi con le applicazioni in Astra Control, prendere in considerazione "modifica dei ruoli utente con vincoli dello spazio dei nomi" prima di definire le applicazioni.
- Per istruzioni su come gestire le applicazioni utilizzando l'API Astra Control, fare riferimento a. "Astra Automation e informazioni API".

Opzioni di gestione delle applicazioni

- Definire le risorse da gestire come applicazione
- Definire uno spazio dei nomi da gestire come applicazione

Definire le risorse da gestire come applicazione

È possibile specificare "Kubernetes risorse che compongono un'applicazione" Che si desidera gestire con Astra Control. La definizione di un'applicazione consente di raggruppare gli elementi del cluster Kubernetes in una singola applicazione. Questa raccolta di risorse Kubernetes è organizzata in base allo spazio dei nomi e ai criteri di selezione delle etichette.

La definizione di un'applicazione offre un controllo più granulare su ciò che deve essere incluso in un'operazione Astra Control, inclusi cloni, snapshot e backup.

> Quando definisci le app, assicurati di non includere una risorsa Kubernetes in più app con policy di protezione. La sovrapposizione di policy di protezione su risorse Kubernetes può causare conflitti di dati.

Scopri di più sull'aggiunta di risorse con ambito cluster agli spazi dei nomi delle app.

È possibile importare risorse del cluster associate alle risorse dello spazio dei nomi oltre a quelle incluse automaticamente in Astra Control. È possibile aggiungere una regola che includerà le risorse di un gruppo specifico, un tipo, una versione e, facoltativamente, un'etichetta. Questa operazione potrebbe essere utile se ci sono risorse che Astra Control non include automaticamente.

Non è possibile escludere nessuna delle risorse con ambito del cluster incluse automaticamente da Astra Control.

È possibile aggiungere quanto segue `apiVersions` (Che sono i gruppi combinati con la versione API):

Tipo di risorsa	ApiVersions (gruppo + versione)
`ClusterRole`	rbac.authorization.k8s.io/v1
`ClusterRoleBinding`	rbac.authorization.k8s.io/v1
`CustomResource`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`CustomResourceDefinition`	apiextensions.k8s.io/v1, apiextensions.k8s.io/v1beta1
`MutatingWebhookConfiguration`	admissionregistration.k8s.io/v1
`ValidatingWebhookConfiguration`	admissionregistration.k8s.io/v1

Fasi

1. Dalla pagina applicazioni, selezionare **Definisci**.

2. Nella finestra **define application** (Definisci applicazione), inserire il nome dell'applicazione.
3. Scegliere il cluster in cui viene eseguita l'applicazione nell'elenco a discesa **Cluster**.
4. Scegliere uno spazio dei nomi per l'applicazione dall'elenco a discesa **namespace**.

> Le applicazioni possono essere definite all'interno di uno o più spazi dei nomi specifici su un singolo cluster utilizzando Astra Control. Un'applicazione può contenere risorse che spaziano da più spazi dei nomi all'interno dello stesso cluster. Astra Control non supporta la possibilità di definire le applicazioni in più cluster.

5. (Facoltativo) inserire un'etichetta per le risorse Kubernetes in ogni namespace. È possibile specificare un'etichetta singola o criteri di selezione delle etichette (query).

> Per ulteriori informazioni sulle etichette Kubernetes, "Consultare la documentazione ufficiale di Kubernetes".

6. (Facoltativo) aggiungere spazi dei nomi aggiuntivi per l'applicazione selezionando **Aggiungi spazio dei nomi** e scegliendo lo spazio dei nomi dall'elenco a discesa.
7. (Facoltativo) inserire i criteri di selezione di un'etichetta o di un'etichetta singola per gli spazi dei nomi aggiuntivi aggiunti.
8. (Facoltativo) per includere risorse con ambito cluster oltre a quelle incluse automaticamente da Astra Control, selezionare **Includi risorse aggiuntive con ambito cluster** e completare quanto segue:
   a. Selezionare **Aggiungi regola di inclusione**.
   b. **Gruppo**: Selezionare il gruppo di risorse API dall'elenco a discesa.
   c. **Kind**: Dall'elenco a discesa, selezionare il nome dello schema dell'oggetto.
   d. **Version**: Inserire la versione dell'API.
   e. **Selettore etichetta**: Facoltativamente, includere un'etichetta da aggiungere alla regola. Questa etichetta viene utilizzata per recuperare solo le risorse corrispondenti a questa etichetta. Se non si fornisce un'etichetta, Astra Control raccoglie tutte le istanze del tipo di risorsa specificato per quel cluster.
   f. Esaminare la regola creata in base alle voci immesse.
   g. Selezionare **Aggiungi**.

   > È possibile creare tutte le regole di risorse con ambito cluster desiderate. Le regole vengono visualizzate nel riepilogo dell'applicazione Definisci.

9. Selezionare **Definisci**.
10. Dopo aver selezionato **define**, ripetere la procedura per altre applicazioni, in base alle necessità.

Al termine della definizione di un'applicazione, l'applicazione viene visualizzata in `Healthy` indicare nell'elenco delle applicazioni nella pagina applicazioni. Ora è possibile clonarlo e creare backup e snapshot.

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

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

Per visualizzare le risorse aggiunte a questa applicazione, selezionare la scheda **risorse**. Selezionare il numero dopo il nome della risorsa nella colonna Resource (risorsa) o inserire il nome della risorsa in Search (Cerca) per visualizzare le risorse aggiuntive incluse nell'ambito del cluster.

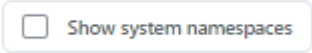
Definire uno spazio dei nomi da gestire come applicazione

È possibile aggiungere tutte le risorse Kubernetes in uno spazio dei nomi alla gestione di Astra Control definendo le risorse dello spazio dei nomi come applicazione. Questo metodo è preferibile alla definizione individuale delle applicazioni, se necessario "intende gestire e proteggere tutte le risorse in uno spazio dei nomi specifico" in modo simile e ad intervalli comuni.

Fasi

1. Dalla pagina Clusters, selezionare un cluster.
2. Selezionare la scheda **spazi dei nomi**.
3. Selezionare il menu Actions (azioni) per lo spazio dei nomi che contiene le risorse dell'applicazione che si desidera gestire e selezionare **define as application** (Definisci come applicazione).

> Se si desidera definire più applicazioni, selezionare dall'elenco namespace e selezionare il pulsante **azioni** nell'angolo in alto a sinistra, quindi selezionare **Definisci come applicazione**. In questo modo verranno definite più applicazioni singole nei rispettivi spazi dei nomi. Per le applicazioni multi-spazio dei nomi, fare riferimento a. Definire le risorse da gestire come applicazione.

> Selezionare la casella di controllo **Show system namespace** (Mostra spazi dei nomi di sistema) per visualizzare gli spazi dei nomi di sistema solitamente non utilizzati nella gestione delle applicazioni per impostazione predefinita. 

"Scopri di più".

Al termine del processo, le applicazioni associate allo spazio dei nomi vengono visualizzate in `Associated applications` colonna.

[Anteprima tecnica] Definisci un'applicazione usando una risorsa personalizzata di Kubernetes

Puoi specificare le risorse Kubernetes da gestire con Astra Control definendole come un'applicazione tramite una risorsa personalizzata (CR). Puoi aggiungere risorse destinate al cluster se desideri gestire tali risorse singolarmente o tutte le risorse Kubernetes in un namespace, se, ad esempio, intendi gestire e proteggere tutte le risorse in un namespace specifico in modo simile e a intervalli comuni.

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome (ad esempio, `astra_mysql_app.yaml`).
2. Assegnare un nome all'applicazione in `metadata.name`.
3. Definire le risorse dell'applicazione da gestire:

spec.includedClusterScopedResources

Inserisci i tipi di risorse riferiti all'ambito del cluster e quelli indicati automaticamente da Astra Control:

- **spec.includedClusterScopedResources**: *(opzionale)* elenco dei tipi di risorse con ambito cluster da includere.
  - **GroupVersionKind**: *(opzionale)* identifica in modo inequivocabile un tipo.
    - **Gruppo**: *(obbligatorio se viene utilizzato groupVersionKind)* gruppo API della risorsa da includere.
    - **Version**: *(obbligatorio se si utilizza groupVersionKind)* versione API della risorsa da includere.
    - **Tipo**: *(richiesto se viene utilizzato groupVersionKind)* tipo di risorsa da includere.
  - **LabelSelector**: *(Optional)* Una query di etichetta per un insieme di risorse. Viene utilizzato per recuperare solo le risorse corrispondenti all'etichetta. Se non si fornisce un'etichetta, Astra Control raccoglie tutte le istanze del tipo di risorsa specificato per quel cluster. Il risultato di MatchLabels e MatchExpressions è ANDed.
    - **MatchLabels**: *(Optional)* Una mappa di {key,value} coppie. Un singolo {key,value} nella mappa matchLabels è equivalente a un elemento di matchExpressions che ha un campo chiave di "key", operatore di "in" e matrice di valori contenente solo "value". I requisiti sono ANDed.
    - **MatchExpressions**: *(Optional)* elenco dei requisiti del selettore di etichette. I requisiti sono ANDed.
      - **Tasto**: *(obbligatorio se si utilizza matchExpressions)* il tasto etichetta associato al selettore etichetta.
      - **Operatore**: *(obbligatorio se si utilizza matchExpressions)* rappresenta la relazione di una chiave con un insieme di valori. Gli operatori validi sono `In`, `NotIn`, `Exists` e. `DoesNotExist`.
      - **Values**: *(obbligatorio se viene utilizzato matchExpressions)_una matrice di valori di stringa. Se l'operatore è `In` oppure `NotIn`, la matrice dei valori deve _non* essere vuota. Se l'operatore è `Exists` oppure `DoesNotExist`, la matrice dei valori deve essere vuota.

spec.includedNamespaces

Includere spazi dei nomi e risorse all'interno di tali risorse nell'applicazione:

- **spec.includedNamespaces**: _(required)_definisce lo spazio dei nomi e i filtri opzionali per la selezione delle risorse.
  - **Namespace**: *(obbligatorio)* lo spazio dei nomi che contiene le risorse dell'applicazione che si desidera gestire con Astra Control.
  - **LabelSelector**: *(Optional)* Una query di etichetta per un insieme di risorse. Viene utilizzato per recuperare solo le risorse corrispondenti all'etichetta. Se non si fornisce un'etichetta, Astra Control raccoglie tutte le istanze del tipo di risorsa specificato per quel cluster. Il risultato di MatchLabels e MatchExpressions è ANDed.
    - **MatchLabels**: *(Optional)* Una mappa di {key,value} coppie. Un singolo {key,value} nella mappa matchLabels è equivalente a un elemento di matchExpressions che ha un campo chiave di "key", operatore di "in" e matrice di valori contenente solo "value". I requisiti sono ANDed.

- **MatchExpressions**: *(Optional)* elenco dei requisiti del selettore di etichette. `key` e. `operator` sono obbligatori. I requisiti sono ANDed.
  - **Tasto**: *(obbligatorio se si utilizza matchExpressions)* il tasto etichetta associato al selettore etichetta.
  - **Operatore**: *(obbligatorio se si utilizza matchExpressions)* rappresenta la relazione di una chiave con un insieme di valori. Gli operatori validi sono `In`, `NotIn`, `Exists` e. `DoesNotExist`.
  - **Values**: *(obbligatorio se si utilizza matchExpressions)* una matrice di valori di stringa. Se l'operatore è `In` oppure `NotIn`, la matrice dei valori deve *non* essere vuota. Se l'operatore è `Exists` oppure `DoesNotExist`, la matrice dei valori deve essere vuota.

Esempio YAML:

```yaml
apiVersion: astra.netapp.io/v1
kind: Application
metadata:
  name: astra_mysql_app
spec:
  includedNamespaces:
    - namespace: astra_mysql_app
      labelSelector:
        matchLabels:
          app: nginx
          env: production
        matchExpressions:
          - key: tier
            operator: In
            values:
              - frontend
              - backend
```

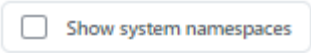
4. Dopo aver popolato il `astra_mysql_app.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra_mysql_app.yaml -n astra-connector
```

E gli spazi dei nomi di sistema?

Astra Control rileva anche gli spazi dei nomi di sistema su un cluster Kubernetes. Per impostazione predefinita, questi spazi dei nomi di sistema non vengono visualizzati perché è raro che sia necessario eseguire il backup delle risorse delle applicazioni di sistema.

È possibile visualizzare gli spazi dei nomi di sistema dalla scheda spazi dei nomi di un cluster selezionato selezionando la casella di controllo **Mostra spazi dei nomi di sistema**.



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.

Proteggi le app con snapshot e backup

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

Scopri di più "Protezione dei dati in Astra Control".

È possibile eseguire le seguenti attività relative alla protezione dei dati dell'applicazione:

- Configurare un criterio di protezione
- Creare un'istantanea
- Creare un backup
- Abilita backup e ripristino per le operazioni economiche a ontap-nas
- Creare un backup immutabile
- Visualizzare snapshot e backup
- Eliminare le istantanee
- Annullare i backup
- Eliminare i backup

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. È possibile definire un criterio di protezione utilizzando l'interfaccia utente Web Astra Control o un file di risorse personalizzato (CR).

Se hai bisogno di backup o snapshot per eseguire più frequentemente di una volta all'ora, è possibile "Utilizza l'API REST di Astra Control per creare snapshot e backup".

Se si sta definendo un criterio di protezione che crea backup immutabili per bucket WORM (Write Once Read Many), assicurarsi che il tempo di conservazione per i backup non sia inferiore al periodo di conservazione configurato per il bucket.

Eseguire l'offset delle pianificazioni di backup e replica per evitare sovrapposizioni di pianificazione. Ad esempio, eseguire backup all'inizio dell'ora ogni ora e pianificare la replica per iniziare con un offset di 5 minuti e un intervallo di 10 minuti.

Configurare un criterio di protezione utilizzando l'interfaccia utente Web

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Configura policy di protezione**.
4. Definire una pianificazione di protezione scegliendo il numero di snapshot e backup da conservare per le pianificazioni orarie, giornaliere, settimanali e mensili.

   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.

   Quando si imposta un livello di conservazione per i backup, è possibile scegliere il bucket in cui si desidera memorizzare i backup.

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

   [Schermata di una policy di configurazione di esempio in cui è possibile scegliere di eseguire snapshot e backup su base oraria, giornaliera, settimanale o mensile.]

5. [**Tech preview**] Scegliete un bucket di destinazione per i backup o le istantanee dall'elenco dei bucket di storage.
6. Selezionare **Revisione**.
7. Selezionare **Imposta policy di protezione.**

[Anteprima tecnica] configurare un criterio di protezione utilizzando una CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-schedule-cr.yaml`. Aggiorna i valori tra parentesi <> per soddisfare le tue esigenze di ambiente Astra Control, configurazione del cluster e protezione dei dati:
   - <CR_NAME>: Il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per l'ambiente.
   - <APPLICATION_NAME>: Il nome Kubernetes dell'applicazione di cui eseguire il backup.
   - <APPVAULT_NAME>: Il nome dell'AppVault in cui devono essere memorizzati i contenuti di backup.
   - <BACKUPS_RETAINED>: Il numero di backup da conservare. Zero indica che non è necessario creare backup.
   - <SNAPSHOTS_RETAINED>: Il numero di snapshot da conservare. Zero indica che non è necessario creare snapshot.
   - <GRANULARITY> (frequenza): La frequenza di esecuzione della pianificazione. Valori possibili, insieme ai campi associati obbligatori:
     - `hourly` (richiede di specificare `spec.minute`)
     - `daily` (richiede di specificare `spec.minute` e. `spec.hour`)
     - `weekly` (richiede di specificare `spec.minute`, `spec.hour`, e. `spec.dayOfWeek`)
     - `monthly` (richiede di specificare `spec.minute`, `spec.hour`, e. `spec.dayOfMonth`)

- <DAY_OF_MONTH>: *(facoltativo)* il giorno del mese (1 - 31) in cui deve essere eseguito il programma. Questo campo è obbligatorio se la granularità è impostata su `monthly`.
- <DAY_OF_WEEK>: *(opzionale)* il giorno della settimana (0 - 7) in cui dovrebbe essere eseguito il programma. I valori di 0 o 7 indicano la domenica. Questo campo è obbligatorio se la granularità è impostata su `weekly`.
- <HOUR_OF_DAY>: *(opzionale)* l'ora del giorno (0 - 23) in cui deve essere eseguito il programma. Questo campo è obbligatorio se la granularità è impostata su `daily`, `weekly`, o. `monthly`.
- <MINUTE_OF_HOUR>: *(opzionale)* il minuto dell'ora (0 - 59) che la programmazione dovrebbe essere eseguita. Questo campo è obbligatorio se la granularità è impostata su `hourly`, `daily`, `weekly`, o. `monthly`.

```
apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"
```

2. Dopo aver popolato il `astra-control-schedule-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-schedule-cr.yaml
```

Risultato

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

Creare un'istantanea

Puoi creare uno snapshot on-demand in qualsiasi momento.

A proposito di questa attività

Astra Control supporta la creazione di snapshot utilizzando classi di storage supportate dai seguenti driver:

- `ontap-nas`

- `ontap-san`
- `ontap-san-economy`

> Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, impossibile creare snapshot. Utilizzare una classe di storage alternativa per gli snapshot.

Creare un'istantanea utilizzando l'interfaccia utente Web

Fasi

1. Selezionare **applicazioni**.
2. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) dell'applicazione desiderata, selezionare **Snapshot**.
3. Personalizzare il nome dell'istantanea, quindi selezionare **Avanti**.
4. [**Tech preview**] Scegli un bucket di destinazione per l'istantanea dall'elenco dei bucket di storage.
5. Esaminare il riepilogo dell'istantanea e selezionare **Snapshot**.

[Anteprima tecnica] Crea un'istantanea utilizzando una CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-snapshot-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - <CR_NAME>: Il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per l'ambiente.
   - <APPLICATION_NAME>: Il nome Kubernetes dell'applicazione da snapshot.
   - <APPVAULT_NAME>: Il nome dell'AppVault in cui devono essere memorizzati i contenuti dello snapshot.
   - <RECLAIM_POLICY>: *(opzionale)* definisce cosa accade a uno snapshot quando lo snapshot CR viene eliminato. Opzioni valide:
     - `Retain`
     - `Delete` (impostazione predefinita)

```
apiVersion: astra.netapp.io/v1
kind: Snapshot
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  reclaimPolicy: <RECLAIM_POLICY>
```

2. Dopo aver popolato il `astra-control-snapshot-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-snapshot-cr.yaml
```

Risultato

Viene avviato il processo di snapshot. Un'istantanea ha successo quando lo stato è **integro** nella colonna

Stato della pagina **Data Protection** > **Snapshot**.

Creare un backup

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

> Tenere presente come viene gestito lo spazio di storage quando si esegue il backup di un'applicazione ospitata sullo storage Azure NetApp Files. Fare riferimento a. "Backup delle applicazioni" per ulteriori informazioni.

> Astra Control supporta la creazione di backup utilizzando classi di storage supportate dai seguenti driver:
>
> - `ontap-nas`
> - `ontap-nas-economy`
> - `ontap-san`
> - `ontap-san-economy`

A proposito di questa attività

I bucket in Astra Control non riportano la capacità disponibile. Prima di eseguire il backup o il cloning delle applicazioni gestite da Astra Control, controllare le informazioni del bucket nel sistema di gestione dello storage appropriato.

Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, è necessario attivare il backup e il ripristino funzionalità. Accertarsi di aver definito un `backendType` nel "Oggetto storage Kubernetes" con un valore di `ontap-nas-economy` prima di eseguire qualsiasi operazione di protezione.

Creare un backup utilizzando l'interfaccia utente Web

Fasi

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

[Anteprima tecnica] creare un backup utilizzando una CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-backup-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - <CR_NAME>: Il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per l'ambiente.
   - <APPLICATION_NAME>: Il nome Kubernetes dell'applicazione di cui eseguire il backup.
   - <APPVAULT_NAME>: Il nome dell'AppVault in cui devono essere memorizzati i contenuti di backup.

   ```
   apiVersion: astra.netapp.io/v1
   kind: Backup
   metadata:
     namespace: astra-connector
     name: <CR_NAME>
   spec:
     applicationRef: <APPLICATION_NAME>
     appVaultRef: <APPVAULT_NAME>
   ```

2. Dopo aver popolato il `astra-control-backup-cr.yaml` File con i valori corretti, applicare il CR:

   ```
   kubectl apply -f astra-control-backup-cr.yaml
   ```

Risultato

Astra Control 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.
- Per annullare un backup in esecuzione, seguire le istruzioni riportate in Annullare i backup. Per eliminare il backup, attendere il completamento, quindi seguire le istruzioni riportate in Eliminare i backup.
- 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.

Abilita backup e ripristino per le operazioni economiche a ontap-nas

Astra Control Provivisioner fornisce funzionalità di backup e ripristino che possono essere abilitate per i backend di storage che stanno utilizzando `ontap-nas-economy` classe di storage.

Prima di iniziare

- Hai abilitato Astra Control provisioner o Astra Trident.
- Hai definito un'applicazione in Astra Control. Questa applicazione dispone di funzionalità di protezione limitate fino al completamento di questa procedura.
- Lo hai fatto `ontap-nas-economy` selezionata come classe di archiviazione predefinita per il backend di archiviazione.

Espandere per la procedura di configurazione

1. Sul back-end dello storage ONTAP:

   a. Trova la SVM che ospita `ontap-nas-economy`volumi basati su -dell'applicazione.

   b. Accedere a un terminale connesso a ONTAP in cui vengono creati i volumi.

   c. Nascondi la directory snapshot per la SVM:

   > Questo cambiamento influisce sull'intera SVM. La directory nascosta continuerà ad essere accessibile.

```
nfs modify -vserver <svm name> -v3-hide-snapshot enabled
```

+

> Verificare che la directory snapshot sul backend di archiviazione ONTAP sia nascosta. La mancata visualizzazione di questa directory potrebbe causare la perdita di accesso all'applicazione, in particolare se si utilizza NFSv3.

2. Esegui le seguenti operazioni in Astra Control Provisioner o Astra Trident:

   a. Abilitare la directory Snapshot per ogni PV in base a ontap-nas-Economy e associata all'applicazione:

```
tridentctl update volume <pv name> --snapshot-dir=true --pool
-level=true -n trident
```

   b. Confermare che la directory snapshot è stata abilitata per ogni PV associato:

```
tridentctl get volume <pv name> -n trident -o yaml | grep
snapshotDir
```

   Risposta:

```
snapshotDirectory: "true"
```

3. In Astra Control, aggiorna l'applicazione dopo aver abilitato tutte le directory di snapshot associate, in modo che Astra Control riconosca il valore modificato.

Risultato

L'applicazione è pronta per il backup e il ripristino utilizzando Astra Control. Ciascun PVC è inoltre disponibile per essere utilizzato da altre applicazioni per backup e ripristini.

Creare un backup immutabile

Un backup immutabile non può essere modificato, eliminato o sovrascritto se la politica di conservazione nel bucket che archivia il backup lo vieta. Puoi creare backup immutabili eseguendo il backup delle applicazioni in bucket che hanno configurato un criterio di conservazione. Fare riferimento a. "Protezione dei dati" per informazioni importanti sull'utilizzo dei backup immutabili.

Prima di iniziare

È necessario configurare il bucket di destinazione con un criterio di conservazione. La scelta varia in base al provider di storage utilizzato. Per ulteriori informazioni, consultare la documentazione del provider di storage:

- **Amazon Web Services**: "Abilitare il blocco degli oggetti S3 durante la creazione del bucket e impostare una modalità di conservazione predefinita di "governance" con un periodo di conservazione predefinito".
- **Google Cloud**: "Configurare un bucket con un criterio di conservazione e specificare un periodo di conservazione".
- **Microsoft Azure**: "Configurare un bucket storage BLOB con una politica di conservazione basata sul tempo sull'ambito a livello di container".
- **NetApp StorageGRID**: "Abilitare blocco oggetto S3 durante la creazione del bucket e impostare una modalità di conservazione predefinita di "conformità" con un periodo di conservazione predefinito".

> I bucket in Astra Control non riportano la capacità disponibile. Prima di eseguire il backup o il cloning delle applicazioni gestite da Astra Control, controllare le informazioni del bucket nel sistema di gestione dello storage appropriato.

> Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, assicurarsi di aver definito un `backendType` nel "Oggetto storage Kubernetes" con un valore di `ontap-nas-economy` prima di eseguire qualsiasi operazione di protezione.

Fasi

1. Selezionare **applicazioni**.
2. Dal menu Opzioni nella colonna **azioni** dell'applicazione desiderata, selezionare **Backup**.
3. Personalizzare il nome del backup.
4. Scegliere se eseguire il backup dell'applicazione da uno snapshot esistente. Se si seleziona questa opzione, è possibile scegliere da un elenco di snapshot esistenti.
5. Scegliere un bucket di destinazione per il backup dall'elenco dei bucket di storage. Un bucket WORM (Write Once Read Many) viene indicato con lo stato "bloccato" accanto al nome del bucket.

   > Se la benna è di tipo non supportato, ciò viene indicato quando si passa il mouse o si seleziona la benna.

6. Selezionare **Avanti**.
7. Esaminare il riepilogo del backup e selezionare **Backup**.

Risultato

Astra Control crea un backup immutabile dell'app.

- 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.
- Se provi a creare due backup immutabili della stessa app nello stesso bucket contemporaneamente, Astra Control impedisce l'avvio del secondo backup. Attendere il completamento del primo backup prima di avviarne un altro.
- Non è possibile annullare un backup immutabile in esecuzione.
- 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).

Un backup immutabile viene indicato con lo stato "bloccato" accanto al bucket in uso.

Fasi

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

   Le istantanee vengono visualizzate per impostazione predefinita.

3. Selezionare **Backup** per fare riferimento all'elenco dei backup.

Eliminare le istantanee

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

Fasi

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

Risultato

Astra Control elimina lo snapshot.

Annullare i backup

È possibile annullare un backup in corso.

Per annullare un backup, il backup deve essere in `Running` stato. Non è possibile annullare un backup in `Pending` stato.

Non è possibile annullare un backup immutabile in esecuzione.

Fasi

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

Eliminare i backup

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

Per annullare un backup in esecuzione, seguire le istruzioni riportate in Annullare i backup. Per eliminare il backup, attendere che sia stato completato, quindi seguire queste istruzioni.

Non è possibile eliminare un backup immutabile prima della scadenza del periodo di conservazione.

Fasi

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

Risultato

Astra Control elimina il backup.

[Anteprima tecnica] proteggi un intero cluster

È possibile creare un backup pianificato e automatico di uno o di tutti gli spazi dei nomi non gestiti su un cluster. Questi workflow sono forniti da NetApp as a Kubernetes Service account, binding di ruolo e un job cron, orchestrato con uno script Python.

Come funziona

Quando si configura e installa il flusso di lavoro del backup completo del cluster, un processo cron viene eseguito periodicamente e protegge qualsiasi namespace non ancora gestito, creando automaticamente criteri di protezione in base alle pianificazioni scelte durante l'installazione.

Se non si desidera proteggere ogni spazio dei nomi non gestito sul cluster con l'intero flusso di lavoro di backup del cluster, è possibile utilizzare invece il flusso di lavoro di backup basato su etichette. Il flusso di lavoro di backup basato su etichetta utilizza anche un task cron, ma invece di proteggere tutti i namespace non

gestiti, identifica i namespace in base alle etichette fornite per proteggere facoltativamente i namespace in base a policy di backup Bronze, Silver o Gold.

Quando viene creato un nuovo namespace che rientra nell'ambito del flusso di lavoro scelto, viene automaticamente protetto, senza alcun intervento dell'amministratore. Questi flussi di lavoro vengono implementati per ogni cluster in modo che cluster diversi possano utilizzare entrambi i flussi di lavoro con livelli di protezione unici, a seconda dell'importanza del cluster.

Esempio: Protezione completa del cluster

Ad esempio, quando configuri e installi l'intero workflow di backup del cluster, tutte le applicazioni in qualsiasi namespace vengono periodicamente gestite e protette senza ulteriori interventi da parte dell'amministratore. Lo spazio dei nomi non deve esistere al momento dell'installazione del flusso di lavoro; se in futuro viene aggiunto uno spazio dei nomi, verrà protetto.

Esempio: Protezione basata sull'etichetta

Per una maggiore granularità, è possibile utilizzare il flusso di lavoro basato su etichette. Ad esempio, è possibile installare questo flusso di lavoro e dire agli utenti di applicare una delle diverse etichette a qualsiasi namespace che desiderano proteggere, a seconda del livello di protezione necessario. In questo modo, gli utenti possono creare lo spazio dei nomi con una di queste etichette e non devono inviare notifiche a un amministratore. Il nuovo namespace e tutte le applicazioni all'interno dell'IT sono protetti automaticamente.

Creare un backup pianificato di tutti gli spazi dei nomi

È possibile creare un backup pianificato di tutti i namespace in un cluster utilizzando il flusso di lavoro di backup completo del cluster.

Fasi

1. Scaricare i seguenti file su un computer con accesso di rete al cluster:
   - "File CRD Components.yaml"
   - "protectCluster.py script Python"
2. Per configurare e installare il toolkit, "seguire le istruzioni incluse".

Creare un backup pianificato di spazi dei nomi specifici

È possibile creare un backup pianificato di spazi dei nomi specifici mediante le relative etichette utilizzando il flusso di lavoro di backup basato su etichette.

Fasi

1. Scaricare i seguenti file su un computer con accesso di rete al cluster:
   - "File CRD Components.yaml"
   - "protectCluster.py script Python"
2. Per configurare e installare il toolkit, "seguire le istruzioni incluse".

Ripristinare le applicazioni

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

> Se si aggiunge un filtro dello spazio dei nomi a un gancio di esecuzione che viene eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o del clone si trovano in spazi dei nomi diversi, il filtro dello spazio dei nomi viene applicato solo allo spazio dei nomi di destinazione.

Prima di iniziare

- **Proteggi prima le tue applicazioni**: Ti consigliamo vivamente di creare un'istantanea o un backup dell'applicazione prima di ripristinarla. Ciò consente di clonare dallo snapshot o dal backup se il ripristino non ha avuto esito positivo.
- **Check destination Volumes** (Controlla volumi di destinazione): Se si esegue il ripristino in una classe di storage diversa, assicurarsi che la classe di storage 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. Ad esempio, se il volume persistente di origine utilizza la modalità di accesso RWX, selezionare una classe di storage di destinazione che non è in grado di fornire RWX, come Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, causa l'errore dell'operazione di ripristino. Per ulteriori informazioni sulle modalità di accesso al volume persistente, fare riferimento a. "Kubernetes" documentazione.
- **Pianificare le esigenze di spazio**: Quando si esegue un ripristino in-place di un'applicazione che utilizza lo storage NetApp ONTAP, lo spazio utilizzato dall'applicazione ripristinata può raddoppiare. Dopo aver eseguito un ripristino in-place, rimuovere eventuali snapshot indesiderati dall'applicazione ripristinata per liberare spazio di storage.
- **Driver di classe di archiviazione supportati**: Astra Control supporta il ripristino dei backup utilizzando classi di archiviazione supportate dai seguenti driver:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- * (Solo driver ontap-nas-Economy) esegue backup e ripristini*: Prima di eseguire il backup o il ripristino di un'app che utilizza una classe di storage supportata da `ontap-nas-economy` driver, verificare che "La directory snapshot sul backend dello storage ONTAP è nascosta". La mancata visualizzazione di questa directory potrebbe causare la perdita di accesso all'applicazione, in particolare se si utilizza NFSv3.

> L'esecuzione di un'operazione di ripristino in-place su un'applicazione che condivida le risorse con un'altra applicazione può avere risultati non intenzionale. Tutte le risorse condivise tra le applicazioni vengono sostituite quando viene eseguito un ripristino in-place su una delle applicazioni.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Dal menu Opzioni nella colonna azioni, selezionare **Ripristina**.
3. Scegliere il tipo di ripristino:
   - **Ripristina gli spazi dei nomi originali**: Utilizzare questa procedura per ripristinare l'applicazione sul posto nel cluster originale.
     i. Seleziona lo snapshot o il backup da utilizzare per ripristinare l'applicazione in-place, che ripristina l'applicazione a una versione precedente di se stessa.
     ii. Selezionare **Avanti**.

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

- **Ripristina nuovi spazi dei nomi**: Utilizzare questa procedura per ripristinare l'applicazione in un altro cluster o con spazi dei nomi diversi dall'origine. È inoltre possibile utilizzare questa procedura per migrare un'applicazione a una classe di storage diversa.
  i. Specificare il nome dell'applicazione ripristinata.
  ii. Scegliere il cluster di destinazione per l'applicazione che si desidera ripristinare.
  iii. Immettere uno spazio dei nomi di destinazione per ogni spazio dei nomi di origine associato all'applicazione.

  > Astra Control crea nuovi spazi dei nomi di destinazione come parte di questa opzione di ripristino. Gli spazi dei nomi di destinazione specificati non devono essere già presenti nel cluster di destinazione.

  iv. Selezionare **Avanti**.
  v. Selezionare lo snapshot o il backup da utilizzare per ripristinare l'applicazione.
  vi. Selezionare **Avanti**.
  vii. Scegliere una delle seguenti opzioni:
    - **Ripristina utilizzando le classi di storage originali**: L'applicazione utilizza la classe di storage originariamente associata, a meno che non esista nel cluster di destinazione. In questo caso, viene utilizzata la classe di storage predefinita per il cluster.
    - **Ripristinare utilizzando una classe di storage diversa**: Selezionare una classe di storage esistente nel cluster di destinazione. Tutti i volumi delle applicazioni, indipendentemente dalle classi di storage originariamente associate, verranno migrati in questa diversa classe di storage come parte del ripristino.

  viii. Selezionare **Avanti**.

4. Scegli le risorse da filtrare:
   - **Restore all resources** (Ripristina tutte le risorse): Ripristina tutte le risorse associate all'applicazione originale.
   - **Filter resources**: Specificare le regole per ripristinare un sottoinsieme delle risorse applicative originali:
     i. Scegliere di includere o escludere risorse dall'applicazione ripristinata.
     ii. Selezionare **Aggiungi regola di inclusione** o **Aggiungi regola di esclusione** e configurare la regola per filtrare le risorse corrette durante il ripristino dell'applicazione. È possibile modificare una regola o rimuoverla e crearne di nuovo fino a quando la configurazione non è corretta.

     > Per ulteriori informazioni sulla configurazione delle regole di inclusione ed esclusione, vedere Filtrare le risorse durante il ripristino di un'applicazione.

5. Selezionare **Avanti**.
6. Esaminare attentamente i dettagli relativi all'azione di ripristino, digitare "restore" (se richiesto) e selezionare **Restore**.

[Tech preview] Ripristino da backup utilizzando una risorsa personalizzata (CR)

È possibile ripristinare i dati da un backup utilizzando un file di risorse personalizzato (CR) in uno spazio dei nomi diverso o nello spazio dei nomi di origine originale.

Ripristino da backup utilizzando una CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-backup-restore-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - <CR_NAME>: Il nome di questa operazione CR; scegliere un nome sensibile per il proprio ambiente.
   - <APPVAULT_NAME>: Il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
   - <BACKUP_PATH>: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Ad esempio:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: Lo spazio dei nomi di origine dell'operazione di ripristino.
   - <DESTINATION_NAMESPACE>: Lo spazio dei nomi di destinazione dell'operazione di ripristino.

     ```
     apiVersion: astra.netapp.io/v1
     kind: BackupRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appVaultRef: <APPVAULT_NAME>
       appArchivePath: <BACKUP_PATH>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Direttiva non risolta in <stdin> - include:./_include/selective-restore-cr.adoc[]

1. Dopo aver popolato il `astra-control-backup-restore-cr.yaml` File con i valori corretti, applicare il CR:

   ```
   kubectl apply -f astra-control-backup-restore-cr.yaml
   ```

Eseguire il ripristino dal backup allo spazio dei nomi originale utilizzando una CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-backup-ipr-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - <CR_NAME>: Il nome di questa operazione CR; scegliere un nome sensibile per il proprio ambiente.

- <APPVAULT_NAME>: Il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
- <BACKUP_PATH>: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Ad esempio:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```yaml
apiVersion: astra.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
```

Direttiva non risolta in <stdin> - include:./_include/selective-restore-cr.adoc[]

1. Dopo aver popolato il `astra-control-backup-ipr-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

[Anteprima tecnica] Ripristino da snapshot utilizzando una risorsa personalizzata (CR)

È possibile ripristinare i dati da uno snapshot utilizzando un file di risorse personalizzato (CR) in uno spazio dei nomi diverso o nello spazio dei nomi di origine originale.

Eseguire il ripristino da uno snapshot utilizzando una CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-snapshot-restore-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - <CR_NAME>: Il nome di questa operazione CR; scegliere un nome sensibile per il proprio ambiente.
   - <APPVAULT_NAME>: Il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
   - <BACKUP_PATH>: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Ad esempio:

     ```
     ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
     20231213023800_94347756-9d9b-401d-a0c3
     ```

   - <SOURCE_NAMESPACE>: Lo spazio dei nomi di origine dell'operazione di ripristino.
   - <DESTINATION_NAMESPACE>: Lo spazio dei nomi di destinazione dell'operazione di ripristino.

     ```
     apiVersion: astra.netapp.io/v1
     kind: SnapshotRestore
     metadata:
       name: <CR_NAME>
       namespace: astra-connector
     spec:
       appArchivePath: <BACKUP_PATH>
       appVaultRef: <APPVAULT_NAME>
       namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
     "destination": "<DESTINATION_NAMESPACE>"}]
     ```

Direttiva non risolta in <stdin> - include:./_include/selective-restore-cr.adoc[]

1. Dopo aver popolato il `astra-control-snapshot-restore-cr.yaml` File con i valori corretti, applicare il CR:

   ```
   kubectl apply -f astra-control-snapshot-restore-cr.yaml
   ```

Eseguire il ripristino dallo snapshot allo spazio dei nomi originale utilizzando una CR

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-snapshot-ipr-cr.yaml`. Aggiorna i valori tra parentesi <> per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
   - <CR_NAME>: Il nome di questa operazione CR; scegliere un nome sensibile per il proprio ambiente.

- <APPVAULT_NAME>: Il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
- <BACKUP_PATH>: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Ad esempio:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```yaml
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

Direttiva non risolta in <stdin> - include:./_include/selective-restore-cr.adoc[]

1. Dopo aver popolato il `astra-control-snapshot-ipr-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

Risultato

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

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

> Qualsiasi utente membro con vincoli di spazio dei nomi in base al nome/ID dello spazio dei nomi o alle etichette dello spazio dei nomi può clonare o ripristinare un'applicazione in un nuovo spazio dei nomi nello stesso cluster o in qualsiasi altro cluster dell'account dell'organizzazione. Tuttavia, lo stesso utente non può accedere all'applicazione clonata o ripristinata nel nuovo namespace. Dopo che un'operazione di clonazione o ripristino crea un nuovo spazio dei nomi, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo affinché l'utente interessato conceda l'accesso al nuovo spazio dei nomi.

Filtrare le risorse durante il ripristino di un'applicazione

È possibile aggiungere una regola di filtro a un "ripristinare" operazione che specifica le risorse applicative esistenti da includere o escludere dall'applicazione ripristinata. È possibile includere o escludere risorse in base a uno spazio dei nomi, un'etichetta o un GVK (GroupVersionKind) specificati.

Scopri di più sugli scenari di inclusione ed esclusione

- **Si seleziona una regola di inclusione con spazi dei nomi originali (ripristino in-place)**: Le risorse applicative esistenti definite nella regola verranno eliminate e sostituite da quelle dello snapshot o del backup selezionato che si sta utilizzando per il ripristino. Tutte le risorse non specificate nella regola di inclusione resteranno invariate.
- **Selezionare una regola di inclusione con nuovi spazi dei nomi**: Utilizzare la regola per selezionare le risorse specifiche che si desidera utilizzare nell'applicazione ripristinata. Le risorse non specificate nella regola di inclusione non verranno incluse nell'applicazione ripristinata.
- **Si seleziona una regola di esclusione con spazi dei nomi originali (ripristino in-place)**: Le risorse specificate per l'esclusione non verranno ripristinate e rimarranno invariate. Le risorse non specificate da escludere verranno ripristinate dallo snapshot o dal backup. Tutti i dati sui volumi persistenti verranno cancellati e ricreati se il corrispondente StatefulSet fa parte delle risorse filtrate.
- **Selezionare una regola di esclusione con nuovi spazi dei nomi**: Utilizzare la regola per selezionare le risorse specifiche che si desidera rimuovere dall'applicazione ripristinata. Le risorse non specificate da escludere verranno ripristinate dallo snapshot o dal backup.

Le regole possono includere o escludere tipi. Non sono disponibili regole che combinano inclusione ed esclusione delle risorse.

Fasi

1. Dopo aver scelto di filtrare le risorse e aver selezionato un'opzione di inclusione o esclusione nella procedura guidata Restore App, selezionare **Aggiungi regola di inclusione** o **Aggiungi regola di esclusione**.

   Non è possibile escludere risorse con ambito cluster che vengono automaticamente incluse da Astra Control.

2. Configurare la regola di filtro:

   È necessario specificare almeno uno spazio dei nomi, un'etichetta o un GVK. Assicurarsi che tutte le risorse conservate dopo l'applicazione delle regole di filtro siano sufficienti per mantenere l'applicazione ripristinata in uno stato di integrità.

   a. Selezionare uno spazio dei nomi specifico per la regola. Se non si effettua una selezione, nel filtro verranno utilizzati tutti gli spazi dei nomi.

      Se l'applicazione conteneva originariamente più spazi dei nomi e la ripristinerai in nuovi spazi dei nomi, tutti gli spazi dei nomi verranno creati anche se non contengono risorse.

   b. (Facoltativo) inserire un nome di risorsa.

   c. (Facoltativo) **selettore di etichette**: Includere un "selettore di etichette" da aggiungere alla regola. Il selettore di etichette viene utilizzato per filtrare solo le risorse corrispondenti all'etichetta selezionata.

d. (Facoltativo) selezionare **Use GVK (GroupVersionKind) set to filter resources** for additional filtering options.

> Se si utilizza un filtro GVK, è necessario specificare versione e tipo.

i. (Facoltativo) **Group**: Dall'elenco a discesa, selezionare il gruppo Kubernetes API.

ii. **Kind**: Dall'elenco a discesa, selezionare lo schema dell'oggetto per il tipo di risorsa Kubernetes da utilizzare nel filtro.

iii. **Version** (versione): Selezionare la versione dell'API Kubernetes.

3. Esaminare la regola creata in base alle voci immesse.
4. Selezionare **Aggiungi**.

> È possibile creare tutte le regole di inclusione ed esclusione delle risorse desiderate. Le regole vengono visualizzate nel riepilogo dell'applicazione di ripristino prima di avviare l'operazione.

Clonare e migrare le applicazioni

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

La clonazione può essere di aiuto nel caso in cui sia necessario spostare applicazioni e storage da un cluster Kubernetes a un altro. Ad esempio, è possibile spostare i carichi di lavoro attraverso una pipeline ci/CD e attraverso gli spazi dei nomi Kubernetes.

> Se si aggiunge un filtro dello spazio dei nomi a un gancio di esecuzione che viene eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o del clone si trovano in spazi dei nomi diversi, il filtro dello spazio dei nomi viene applicato solo allo spazio dei nomi di destinazione.

Prima di iniziare

- **Check destination Volumes** (Controlla volumi di destinazione): Se si esegue la clonazione in una classe di storage diversa, assicurarsi che la classe di storage utilizzi la stessa modalità di accesso al volume persistente (ad esempio ReadWriteMany). L'operazione di clonazione non riesce se la modalità di accesso al volume persistente di destinazione è diversa. Ad esempio, se il volume persistente di origine utilizza la modalità di accesso RWX, selezionare una classe di storage di destinazione che non è in grado di fornire RWX, come Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, causerà l'errore dell'operazione di clonazione. Per ulteriori informazioni sulle modalità di accesso al volume persistente, fare riferimento a. "Kubernetes" documentazione.
- Per clonare le applicazioni in un cluster diverso, è necessario assicurarsi di aver assegnato un bucket predefinito per l'istanza cloud contenente il cluster di origine. Se l'istanza del cloud di origine non ha un bucket predefinito impostato, l'operazione di cloni tra cluster avrà esito negativo.
- Durante le operazioni di cloni, le applicazioni che necessitano di una risorsa IngressClass o di webhook per funzionare correttamente non devono disporre di tali risorse già definite nel cluster di destinazione.

Limitazioni dei cloni

- **Classi di storage esplicite**: Se si implementa un'applicazione con una classe di storage esplicitamente impostata e si deve clonare l'applicazione, il cluster di destinazione deve avere la classe di storage specificata in origine. La clonazione di un'applicazione con una classe di storage esplicitamente impostata su un cluster che non ha la stessa classe di storage non avrà esito positivo.
- **Applicazioni supportate da ontap-nas a economia**: Non è possibile utilizzare le operazioni di clonazione se la classe di storage dell'applicazione è supportata da `ontap-nas-economy` driver. Tuttavia, è possibile "abilita backup e ripristino per le operazioni economiche a ontap-nas".
- **Cloni e vincoli dell'utente**: Qualsiasi utente membro con vincoli dello spazio dei nomi in base al nome/ID dello spazio dei nomi o alle etichette dello spazio dei nomi può clonare o ripristinare un'applicazione in un nuovo spazio dei nomi sullo stesso cluster o in qualsiasi altro cluster dell'account dell'organizzazione. Tuttavia, lo stesso utente non può accedere all'applicazione clonata o ripristinata nel nuovo namespace. Dopo che un'operazione di clonazione o ripristino crea un nuovo spazio dei nomi, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo affinché l'utente interessato conceda l'accesso al nuovo spazio dei nomi.
- **I cloni utilizzano bucket predefiniti**:
  - Durante il backup o il ripristino di un'applicazione, è possibile specificare un bucket da utilizzare. È necessario specificare un bucket predefinito quando si clonano tra cluster, ma specificare un bucket è facoltativo quando si esegue la clonazione all'interno dello stesso cluster.
  - Quando si clonano tra cluster, l'istanza cloud contenente il cluster di origine dell'operazione di clone deve avere un bucket predefinito.
  - 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.
- **Con Jenkins ci**: Se si clonano istanze distribuite dall'operatore di Jenkins ci, è necessario ripristinare manualmente i dati persistenti. Si tratta di un limite del modello di implementazione dell'applicazione.

Fasi

1. Selezionare **applicazioni**.
2. Effettuare una delle seguenti operazioni:
   - Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per l'applicazione desiderata.
   - Selezionare il nome dell'applicazione desiderata e l'elenco a discesa Status (Stato) in alto a destra nella pagina.
3. Selezionare **Clone**.
4. Specificare i dettagli per il clone:
   - Immettere un nome.
   - Scegliere un cluster di destinazione per il clone.
   - Immettere gli spazi dei nomi di destinazione per il clone. Ogni namespace di origine associato all'applicazione viene mappato a uno spazio dei nomi di destinazione.

     > Astra Control crea nuovi spazi dei nomi di destinazione come parte dell'operazione di clone. Gli spazi dei nomi di destinazione specificati non devono essere già presenti nel cluster di destinazione.

   - Selezionare **Avanti**.
   - Scegliere di mantenere la classe di storage originale associata all'applicazione o di selezionare una classe di storage diversa.

> Puoi migrare la classe di storage di un'app a una classe di storage di un cloud provider nativo o a un'altra classe di storage supportata, migrare un'app da una classe di storage supportata da `ontap-nas-economy` a una classe di storage supportata da `ontap-nas` sullo stesso cluster oppure copiare l'applicazione in un altro cluster con una classe di storage supportata da `ontap-nas-economy` driver.

> Se si seleziona una classe di storage diversa e questa classe di storage non esiste al momento del ripristino, viene restituito un errore.

5. Selezionare **Avanti**.
6. Esaminare le informazioni relative al clone e selezionare **Clone**.

Risultato

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

Dopo che un'operazione di clonazione o ripristino crea un nuovo spazio dei nomi, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo affinché l'utente interessato conceda l'accesso al nuovo spazio dei nomi.

Gestire gli hook di esecuzione delle applicazioni

Un gancio di esecuzione è un'azione personalizzata che è possibile configurare per l'esecuzione in combinazione con un'operazione di protezione dei dati di un'applicazione gestita. Ad esempio, se si dispone di un'applicazione di database, è possibile utilizzare un gancio di esecuzione per mettere in pausa tutte le transazioni del database prima di uno snapshot e riprendere le transazioni al termine dello snapshot. Ciò garantisce snapshot coerenti con l'applicazione.

Tipi di hook di esecuzione

Astra Control Service supporta i seguenti tipi di hook di esecuzione, in base a quando possono essere eseguiti:

- Pre-snapshot
- Post-snapshot
- Pre-backup
- Post-backup
- Post-ripristino

Esecuzione dei filtri hook

Quando si aggiunge o si modifica un gancio di esecuzione a un'applicazione, è possibile aggiungere filtri a un gancio di esecuzione per gestire i contenitori corrispondenti. I filtri sono utili per le applicazioni che utilizzano la stessa immagine container su tutti i container, ma possono utilizzare ogni immagine per uno scopo diverso (ad esempio Elasticsearch). I filtri consentono di creare scenari in cui gli hook di esecuzione vengono eseguiti su alcuni container identici, ma non necessariamente su tutti. Se si creano più filtri per un singolo gancio di esecuzione, questi vengono combinati con un operatore AND logico. È possibile avere fino a 10 filtri attivi per gancio di esecuzione.

Ogni filtro aggiunto a un gancio di esecuzione utilizza un'espressione regolare per far corrispondere i contenitori nel cluster. Quando un gancio corrisponde a un container, il gancio esegue lo script associato su quel container. Le espressioni regolari per i filtri utilizzano la sintassi RE2 (espressione regolare), che non supporta la creazione di un filtro che esclude i contenitori dall'elenco di corrispondenze. Per informazioni sulla sintassi supportata da Astra Control per le espressioni regolari nei filtri hook di esecuzione, vedere "Supporto della sintassi RE2 (Regular Expression 2)".

> Se si aggiunge un filtro dello spazio dei nomi a un gancio di esecuzione che viene eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o del clone si trovano in spazi dei nomi diversi, il filtro dello spazio dei nomi viene applicato solo allo spazio dei nomi di destinazione.

Note importanti sugli hook di esecuzione personalizzati

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

> Poiché gli hook di esecuzione spesso riducono o disattivano completamente le funzionalità dell'applicazione con cui vengono eseguiti, si consiglia di ridurre al minimo il tempo necessario per l'esecuzione degli hook di esecuzione personalizzati.
> Se si avvia un'operazione di backup o snapshot con gli hook di esecuzione associati, ma poi si annulla, gli hook possono ancora essere eseguiti se l'operazione di backup o snapshot è già iniziata. Ciò significa che la logica utilizzata in un gancio di esecuzione post-backup non può presumere che il backup sia stato completato.

- La funzionalità hook di esecuzione è disabilitata per impostazione predefinita per le nuove implementazioni di Astra Control.
  - È necessario attivare la funzione di hook di esecuzione prima di poter utilizzare i hook di esecuzione.
  - Gli utenti proprietari o amministratori possono attivare o disattivare la funzionalità di hook di esecuzione per tutti gli utenti definiti nell'account Astra Control corrente. Fare riferimento a. Attivare la funzione ganci di esecuzione e. Disattivare la funzione ganci di esecuzione per istruzioni.
  - Lo stato di abilitazione delle funzioni viene mantenuto durante gli aggiornamenti di Astra Control.
- Un gancio di esecuzione deve utilizzare uno script per eseguire le azioni. Molti hook di esecuzione possono fare riferimento allo stesso script.
- Astra Control richiede che gli script utilizzati dagli hook di esecuzione siano scritti nel formato degli script shell eseguibili.
- La dimensione dello script è limitata a 96 KB.
- Astra Control utilizza le impostazioni degli uncino di esecuzione e qualsiasi criterio corrispondente per determinare quali hook sono applicabili a un'operazione di snapshot, backup o ripristino.
- Tutti i guasti degli uncini di esecuzione sono guasti di tipo soft; altri hook e l'operazione di protezione dei dati vengono ancora tentati anche in caso di interruzione di un hook. Tuttavia, quando un gancio non funziona, viene registrato un evento di avviso nel registro eventi della pagina **attività**.
- Per creare, modificare o eliminare gli hook di esecuzione, è necessario essere un utente con autorizzazioni Owner, Admin o Member.
- Se l'esecuzione di un gancio di esecuzione richiede più di 25 minuti, l'hook non riesce, creando una voce del registro eventi con un codice di ritorno "N/A". Qualsiasi snapshot interessata verrà contrassegnata come non riuscita e una voce del registro eventi risultante annoterà il timeout.
- Per le operazioni di protezione dei dati ad hoc, tutti gli eventi hook vengono generati e salvati nel registro eventi della pagina **Activity**. Tuttavia, per le operazioni di protezione dei dati pianificate, nel registro eventi

vengono registrati solo gli eventi di errore hook (gli eventi generati dalle operazioni di protezione dei dati pianificate vengono ancora registrati).

Ordine di esecuzione

Quando viene eseguita un'operazione di protezione dei dati, gli eventi hook di esecuzione hanno luogo nel seguente ordine:

1. Gli eventuali hook di esecuzione pre-operation personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook pre-operation personalizzati necessari, ma l'ordine di esecuzione di questi hook prima dell'operazione non è garantito né configurabile.
2. Viene eseguita l'operazione di protezione dei dati.
3. Gli eventuali hook di esecuzione post-operation personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook post-operation personalizzati necessari, ma l'ordine di esecuzione di questi hook dopo l'operazione non è garantito né configurabile.

Se si creano più hook di esecuzione dello stesso tipo (ad esempio, pre-snapshot), l'ordine di esecuzione di tali hook non è garantito. Tuttavia, è garantito l'ordine di esecuzione di ganci di tipi diversi. Ad esempio, l'ordine di esecuzione di una configurazione con tutti i diversi tipi di hook è simile al seguente:

1. Hook pre-backup eseguiti
2. Hook pre-snapshot eseguiti
3. Esecuzione di hook post-snapshot
4. Hook post-backup eseguiti
5. Esecuzione degli hook di post-ripristino

È possibile vedere un esempio di questa configurazione nello scenario numero 2 dalla tabella nella Determinare se verrà eseguito un gancio.

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

Determinare se verrà eseguito un gancio

Utilizza la seguente tabella per determinare se verrà eseguito un gancio di esecuzione personalizzato per l'applicazione.

Si noti che tutte le operazioni di alto livello delle applicazioni consistono nell'eseguire una delle operazioni di base di snapshot, backup o ripristino. A seconda dello scenario, un'operazione di cloni può consistere in varie combinazioni di queste operazioni, quindi gli hook di esecuzione eseguiti da un'operazione di cloni variano.

Le operazioni di ripristino in-place richiedono un'istantanea o un backup esistente, in modo che queste operazioni non eseguano snapshot o hook di backup.

Se si avvia e poi si annulla un backup che include uno snapshot e sono associati degli hook di esecuzione, alcuni hook potrebbero essere eseguiti e altri no. Ciò significa che un gancio di esecuzione post-backup non può presumere che il backup sia stato completato. Tenere presente i seguenti punti per i backup annullati con gli hook di esecuzione associati:

- Gli hook pre-backup e post-backup sono sempre in esecuzione.
- Se il backup include un nuovo snapshot e lo snapshot è stato avviato, vengono eseguiti gli hook pre-snapshot e post-snapshot.
- Se il backup viene annullato prima dell'avvio dello snapshot, gli hook pre-snapshot e post-snapshot non vengono eseguiti.

Scenario	Operazione	Snapshot esistente	Backup esistente	Namespace	Cluster	Esecuzione di Snapshot Hooks	Esecuzione dei ganci di backup	Esecuzione degli hook di ripristino
1	Clonare	N	N	Novità	Stesso	Y	N	Y
2	Clonare	N	N	Novità	Diverso	Y	Y	Y
3	Clonare o ripristinare	Y	N	Novità	Stesso	N	N	Y
4	Clonare o ripristinare	N	Y	Novità	Stesso	N	N	Y
5	Clonare o ripristinare	Y	N	Novità	Diverso	N	N	Y
6	Clonare o ripristinare	N	Y	Novità	Diverso	N	N	Y
7	Ripristinare	Y	N	Esistente	Stesso	N	N	Y
8	Ripristinare	N	Y	Esistente	Stesso	N	N	Y
9	Snapshot	N/A.	N/A.	N/A.	N/A.	Y	N/A.	N/A.
10	Backup	N	N/A.	N/A.	N/A.	Y	Y	N/A.
11	Backup	Y	N/A.	N/A.	N/A.	N	N	N/A.

Esempi di gancio di esecuzione

Visitare il "Progetto NetApp Verda GitHub" Per scaricare gli hook di esecuzione per le applicazioni più diffuse come Apache Cassandra ed Elasticsearch. Puoi anche vedere esempi e trovare idee per strutturare i tuoi hook di esecuzione personalizzati.

Attivare la funzione ganci di esecuzione

Se si è un utente Proprietario o Amministratore, è possibile attivare la funzione ganci di esecuzione. Quando si attiva la funzionalità, tutti gli utenti definiti in questo account Astra Control possono utilizzare i ganci di esecuzione e visualizzare i ganci di esecuzione e gli script hook esistenti.

Fasi

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

   Viene visualizzata la scheda **account** > **Impostazioni funzioni**.

4. Nel riquadro **ganci di esecuzione**, selezionare il menu delle impostazioni.
5. Selezionare **Abilita**.
6. Prendere nota dell'avviso di protezione visualizzato.
7. Selezionare **Sì, abilita i ganci di esecuzione**.

Disattivare la funzione ganci di esecuzione

Se si è un utente Proprietario o Amministratore, è possibile disattivare la funzionalità Hook di esecuzione per tutti gli utenti definiti in questo account Astra Control. È necessario eliminare tutti i ganci di esecuzione esistenti prima di disattivare la funzione ganci di esecuzione. Fare riferimento a. Eliminare un gancio di esecuzione per istruzioni sull'eliminazione di un gancio di esecuzione esistente.

Fasi

1. Andare su **account**, quindi selezionare la scheda **Impostazioni funzione**.
2. Selezionare la scheda **Execution Hooks**.
3. Nel riquadro **ganci di esecuzione**, selezionare il menu delle impostazioni.
4. Selezionare **Disable** (Disattiva).
5. Prendere nota dell'avviso visualizzato.
6. Tipo `disable` per confermare che si desidera disattivare la funzione per tutti gli utenti.
7. Selezionare **Sì, disabilita**.

Visualizzare gli hook di esecuzione esistenti

È possibile visualizzare gli hook di esecuzione personalizzati esistenti per un'applicazione.

Fasi

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

   È possibile visualizzare tutti gli hook di esecuzione attivati o disattivati nell'elenco risultante. È possibile visualizzare lo stato di un gancio, il numero di contenitori corrispondenti, il tempo di creazione e il momento in cui viene eseguito (pre- o post-operazione). È possibile selezionare + accanto al nome dell'hook per espandere l'elenco dei container su cui verrà eseguito. Per visualizzare i registri degli eventi relativi agli hook di esecuzione per questa applicazione, accedere alla scheda **attività**.

Visualizzare gli script esistenti

È possibile visualizzare gli script caricati. In questa pagina puoi anche vedere quali script sono in uso e quali hook li stanno utilizzando.

Fasi

1. Vai a **account**.
2. Selezionare la scheda **script**.

   In questa pagina è possibile visualizzare un elenco degli script caricati. La colonna **Used by** mostra gli hook di esecuzione che utilizzano ogni script.

Aggiungere uno script

Ogni gancio di esecuzione deve utilizzare uno script per eseguire le azioni. È possibile aggiungere uno o più script a cui possono fare riferimento gli hook di esecuzione. Molti hook di esecuzione possono fare riferimento allo stesso script; ciò consente di aggiornare molti hook di esecuzione modificando solo uno script.

Fasi

1. Verificare che la funzione ganci di esecuzione sia attivato.
2. Vai a **account**.
3. Selezionare la scheda **script**.
4. Selezionare **Aggiungi**.
5. Effettuare una delle seguenti operazioni:
   - Caricare uno script personalizzato.
     i. Selezionare l'opzione **carica file**.
     ii. Selezionare un file e caricarlo.
     iii. Assegnare allo script un nome univoco.
     iv. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
     v. Selezionare **Salva script**.
   - Incollare uno script personalizzato dagli Appunti.
     i. Selezionare l'opzione **Incolla o tipo**.
     ii. Selezionare il campo di testo e incollare il testo dello script nel campo.
     iii. Assegnare allo script un nome univoco.
     iv. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
6. Selezionare **Salva script**.

Risultato

Il nuovo script viene visualizzato nell'elenco della scheda **script**.

Eliminare uno script

È possibile rimuovere uno script dal sistema se non è più necessario e non viene utilizzato da alcun hook di esecuzione.

Fasi

1. Vai a **account**.
2. Selezionare la scheda **script**.
3. Scegliere uno script da rimuovere e selezionare il menu nella colonna **azioni**.
4. Selezionare **Delete** (Elimina).

> Se lo script è associato a uno o più hook di esecuzione, l'azione **Delete** non è disponibile. Per eliminare lo script, modificare prima gli hook di esecuzione associati e associarli a uno script diverso.

Creare un gancio di esecuzione personalizzato

È possibile creare un gancio di esecuzione personalizzato per un'applicazione e aggiungerlo ad Astra Control. Fare riferimento a. Esempi di gancio di esecuzione per esempi di gancio. Per creare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner (Proprietario), Admin (Amministratore) o Member (membro).

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

Fasi

1. Verificare che la funzione ganci di esecuzione sia attivato.
2. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
3. Selezionare la scheda **Execution Hooks**.
4. Selezionare **Aggiungi**.
5. Nell'area **Dettagli gancio**:
   a. Determinare quando il gancio deve funzionare selezionando un tipo di operazione dal menu a discesa **operazione**.
   b. Immettere un nome univoco per l'hook.
   c. (Facoltativo) inserire gli argomenti da passare al gancio durante l'esecuzione, premendo il tasto Invio dopo ogni argomento inserito per registrarne ciascuno.
6. (Facoltativo) nell'area **Dettagli filtro gancio**, è possibile aggiungere filtri per controllare i contenitori su cui viene eseguito l'gancio di esecuzione:
   a. Selezionare **Aggiungi filtro**.
   b. Nella colonna **tipo filtro gancio**, scegliere un attributo sul quale filtrare dal menu a discesa.
   c. Nella colonna **Regex**, immettere un'espressione regolare da utilizzare come filtro. Astra Control utilizza "Sintassi regex espressione regolare 2 (RE2)".

      > Se si filtra sul nome esatto di un attributo (ad esempio il nome di un pod) senza altro testo nel campo di espressione regolare, viene eseguita una corrispondenza di sottostringa. Per associare un nome esatto e solo il nome, utilizzare la sintassi di corrispondenza stringa esatta (ad esempio, `^exact_podname$`).

   d. Per aggiungere altri filtri, selezionare **Aggiungi filtro**.

      > I filtri multipli per un gancio di esecuzione sono combinati con un operatore and logico. È possibile avere fino a 10 filtri attivi per gancio di esecuzione.
7. Al termine, selezionare **Avanti**.
8. Nell'area **script**, eseguire una delle seguenti operazioni:
   - Aggiungere un nuovo script.

i. Selezionare **Aggiungi**.

ii. Effettuare una delle seguenti operazioni:

- Caricare uno script personalizzato.

  I. Selezionare l'opzione **carica file**.

  II. Selezionare un file e caricarlo.

  III. Assegnare allo script un nome univoco.

  IV. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.

  V. Selezionare **Salva script**.

- Incollare uno script personalizzato dagli Appunti.

  I. Selezionare l'opzione **Incolla o tipo**.

  II. Selezionare il campo di testo e incollare il testo dello script nel campo.

  III. Assegnare allo script un nome univoco.

  IV. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.

- Selezionare uno script esistente dall'elenco.

  In questo modo, il gancio di esecuzione deve utilizzare questo script.

9. Selezionare **Avanti**.
10. Esaminare la configurazione degli uncino di esecuzione.
11. Selezionare **Aggiungi**.

Controllare lo stato di un gancio di esecuzione

Al termine dell'esecuzione di un'operazione di snapshot, backup o ripristino, è possibile controllare lo stato degli hook di esecuzione eseguiti come parte dell'operazione. È possibile utilizzare queste informazioni di stato per determinare se si desidera mantenere l'esecuzione agganciata, modificarla o eliminarla.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Data Protection**.
3. Selezionare **Snapshot** per visualizzare le snapshot in esecuzione o **Backup** per visualizzare i backup in esecuzione.

   Lo stato **Hook** mostra lo stato dell'esecuzione dell'hook al termine dell'operazione. Per ulteriori informazioni, passare il mouse sullo stato. Ad esempio, se si verificano errori di uncino di esecuzione durante uno snapshot, passando il mouse sullo stato di uncino per tale snapshot si ottiene un elenco di uncini di esecuzione non riusciti. Per visualizzare i motivi di ciascun guasto, consultare la pagina **Activity** (attività) nell'area di navigazione a sinistra.

Visualizzare l'utilizzo dello script

È possibile vedere quali hook di esecuzione utilizzano uno script specifico nell'interfaccia utente Web di Astra Control.

Fasi

1. Selezionare **account**.
2. Selezionare la scheda **script**.

   La colonna **Used by** nell'elenco degli script contiene i dettagli su quali hook utilizzano ciascuno script dell'elenco.

3. Selezionare le informazioni nella colonna **utilizzato da** per lo script desiderato.

   Viene visualizzato un elenco più dettagliato con i nomi degli hook che utilizzano lo script e il tipo di operazione con cui sono configurati per l'esecuzione.

Modificare un gancio di esecuzione

È possibile modificare un gancio di esecuzione se si desidera modificarne gli attributi, i filtri o lo script utilizzato. Per modificare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner, Admin o Member.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per un gancio che si desidera modificare.
4. Selezionare **Modifica**.
5. Apportare le modifiche necessarie, selezionando **Avanti** dopo aver completato ciascuna sezione.
6. Selezionare **Salva**.

Disattiva un gancio di esecuzione

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

Fasi

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

Eliminare un gancio di esecuzione

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

Fasi

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

eliminare.

4. Selezionare **Delete** (Elimina).
5. Nella finestra di dialogo visualizzata, digitare "DELETE" per confermare.
6. Selezionare **Sì, elimina gancio di esecuzione**.

Per ulteriori informazioni

- "Progetto NetApp Verda GitHub"

Visualizza lo stato di salute delle applicazioni e del calcolo

Visualizza un riepilogo dello stato delle applicazioni e dei cluster

Fai clic su **Dashboard** per visualizzare una vista di alto livello delle tue applicazioni, dei cluster e della loro salute.

Il riquadro Apps (applicazioni) consente di identificare i seguenti elementi:

- Quante applicazioni stai attualmente gestendo.
- Se queste applicazioni gestite sono in buona salute.
- Se le applicazioni sono completamente protette (sono protette se sono disponibili backup recenti).

Si noti che questi non sono solo numeri 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.

Il riquadro Clusters fornisce dettagli simili sullo stato del cluster ed è possibile eseguire il drill-down per ottenere ulteriori dettagli come si può fare con un'applicazione.

Visualizza lo stato di salute e i dettagli dei cluster

Dopo aver aggiunto i cluster Kubernetes ad Astra Control, 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 Service, selezionare **Clusters**.
2. Nella pagina **Clusters**, selezionare il cluster di cui si desidera visualizzare i dettagli.

> Se un cluster si trova in `removed` state Yet la connettività di rete e del cluster sembra sana (i tentativi esterni di accesso al cluster utilizzando le API di Kubernetes sono riusciti), il kubeconfig che hai fornito ad Astra Control potrebbe non essere più valido. Ciò può essere dovuto alla rotazione o alla scadenza del certificato sul cluster. Per risolvere questo problema, aggiornare le credenziali associate al cluster in Astra Control utilizzando "API di controllo Astra".

3. Visualizzare le informazioni nelle schede **Overview**, **Storage** e **Activity** per trovare le informazioni desiderate.

- **Panoramica**: Dettagli sui nodi di lavoro, incluso il loro stato.
- **Storage**: I volumi persistenti associati al calcolo, inclusi la classe e lo stato dello storage.
- **Attività**: Le attività correlate al cluster.

> È inoltre possibile visualizzare le informazioni sul cluster partendo da Astra Control Service **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'app, Astra Control fornisce dettagli sull'app che ti permette di identificarne lo stato di comunicazione (se Astra Control è in grado di comunicare con l'app), il suo stato di protezione (se è completamente protetto in caso di guasto), i pod, lo storage persistente e altro ancora.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Trova le informazioni che cerchi:

Stato dell'app

Fornisce uno stato che riflette se Astra Control può comunicare con l'applicazione.

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

Le attività di Astra Control correlate all'applicazione.

Gestire i bucket

È possibile gestire i bucket utilizzati da Astra per backup e cloni. È possibile aggiungere bucket aggiuntivi, rimuovere bucket esistenti e modificare il bucket predefinito per i cluster Kubernetes in un'istanza cloud.

Solo i proprietari e gli amministratori possono gestire i bucket.

Come Astra Control utilizza i bucket

Quando inizi a gestire il tuo primo cluster Kubernetes per un'istanza cloud, Astra Control Service crea il bucket iniziale per questo "istanza di cloud".

È possibile designare manualmente un bucket come bucket predefinito per un'istanza di cloud. In tal caso, Astra Control Service utilizza questo bucket per impostazione predefinita per i backup e i cloni creati su qualsiasi cluster gestito in tale istanza del cloud (è possibile selezionare un bucket diverso per i backup). Se si esegue un clone live di un'applicazione da uno qualsiasi dei cluster gestiti in un'istanza cloud a un altro cluster, Astra Control Service utilizza il bucket predefinito per l'istanza del cloud di origine per eseguire l'operazione di clone.

È possibile impostare lo stesso bucket del bucket predefinito per più istanze cloud.

È possibile selezionare da qualsiasi bucket quando si crea una policy di protezione o si avvia un backup ad-hoc.

> Astra Control Service verifica se un bucket di destinazione è accessibile prima di avviare un backup o un clone.

Visualizzare i bucket esistenti

Visualizza l'elenco dei bucket disponibili per Astra Control Service per determinarne lo stato e identificare il bucket predefinito (se definito) per la tua istanza di cloud.

Un bucket può avere uno dei seguenti stati:

In sospeso

Dopo aver aggiunto un bucket, questo inizia nello stato in sospeso mentre Astra Control lo rileva.

Disponibile

Il bucket è disponibile per l'utilizzo da parte di Astra Control.

Rimosso

Al momento il bucket non è operativo. Passare il mouse sull'icona di stato per identificare il problema.

Se un bucket si trova nello stato rimosso, è comunque possibile impostarlo come bucket predefinito e

assegnarlo a un programma di protezione. Tuttavia, se il bucket non si trova nello stato disponibile entro il momento in cui viene avviata un'operazione di protezione dei dati, l'operazione non riuscirà.

Fase

1. Accedere a **Bucket**.

   Viene visualizzato l'elenco dei bucket disponibili per Astra Control Service.

Aggiungere un bucket aggiuntivo

È possibile aggiungere altri bucket in qualsiasi momento. Ciò consente di scegliere tra bucket durante la creazione di una policy di protezione o l'avvio di un backup ad-hoc e consente di modificare il bucket predefinito utilizzato da un'istanza del cloud.

È possibile aggiungere i seguenti tipi di bucket:

- Amazon Web Services
- Generico S3
- Piattaforma Google Cloud
- Microsoft Azure
- NetApp ONTAP S3
- NetApp StorageGRID S3

Prima di iniziare

- Assicurarsi di conoscere il nome di un bucket esistente.
- Assicurarsi di disporre di credenziali per il bucket che forniscono ad Astra Control le autorizzazioni necessarie per gestire il bucket.
- Se il bucket è in Microsoft Azure:
  - Il bucket deve appartenere al gruppo di risorse denominato *astra-backup-rg*.
  - Se l'impostazione delle prestazioni dell'istanza dell'account di storage Azure è impostata su "Premium", l'impostazione "Premium account type" deve essere impostata su "Block blob".

Fasi

1. Accedere a **Bucket**.
2. Selezionare **Add** (Aggiungi) e seguire le istruzioni per aggiungere il bucket.
   - **Type**: Scegli il tuo cloud provider.
   - **Nome bucket esistente**: Immettere il nome del bucket.
   - **Description**: Se si desidera, inserire una descrizione del bucket.
     - **Storage account** (solo Azure): Immettere il nome dell'account di storage Azure. Questo bucket deve appartenere al gruppo di risorse denominato *astra-backup-rg*.
     - **Nome server S3 o indirizzo IP** (solo per i tipi di bucket AWS e S3): Immettere il nome di dominio completo dell'endpoint S3 che corrisponde alla propria regione, senza `https://`. Fare riferimento a. "La documentazione Amazon" per ulteriori informazioni.
     - **Select credentials** (Seleziona credenziali): Immettere le credenziali che forniscono ad Astra Control Service le autorizzazioni necessarie per gestire il bucket. Le informazioni da fornire variano a seconda del tipo di bucket.

a. Selezionare **Aggiungi** per aggiungere il bucket.

Risultato

Astra Control Service aggiunge il bucket. È ora possibile scegliere questo bucket quando si crea una policy di protezione o si esegue un backup ad-hoc. È anche possibile impostare questo bucket come bucket predefinito per un'istanza di cloud.

Modificare il bucket predefinito

È possibile modificare il bucket predefinito per un'istanza cloud. Astra Control Service utilizzerà questo bucket per impostazione predefinita per backup e cloni. Ogni istanza di cloud ha un proprio bucket predefinito.

> Astra Control non assegna automaticamente un bucket predefinito per nessuna istanza di cloud. È necessario impostare manualmente un bucket predefinito per un'istanza cloud prima di eseguire operazioni di cloni delle applicazioni tra due cluster.

Fasi

1. Accedere a **istanze cloud**.
2. Selezionare il menu di configurazione nella colonna **azioni** dell'istanza di cloud che si desidera modificare.
3. Selezionare **Modifica**.
4. Nell'elenco dei bucket, selezionare il bucket che si desidera impostare come predefinito per questa istanza di cloud.
5. Selezionare **Aggiorna**.

Rimuovere una benna

È possibile rimuovere un bucket che non è più in uso o che non è integro. Questa operazione può essere utile per mantenere la configurazione dell'archivio di oggetti semplice e aggiornata.

> - Non è possibile rimuovere un bucket predefinito. Se si desidera rimuovere tale bucket, selezionare prima un altro bucket come predefinito.
> - Non è possibile rimuovere un bucket WORM (Write Once Read Many) prima che il periodo di conservazione del cloud provider del bucket sia scaduto. Le benne A VITE SENZA FINE sono contrassegnate con "bloccate" accanto al nome della benna.

Prima di iniziare

- Prima di iniziare, verificare che non vi siano backup in esecuzione o completati per questo bucket.
- È necessario verificare che il bucket non venga utilizzato per i backup pianificati.

In tal caso, non sarà possibile continuare.

Fasi

1. Accedere a **Bucket**.
2. Dal menu **azioni**, selezionare **Rimuovi**.

> Astra Control garantisce innanzitutto che non vi siano policy di pianificazione che utilizzano il bucket per i backup e che non vi siano backup attivi nel bucket che si sta per rimuovere.

3. Digitare "remove" per confermare l'azione.
4. Selezionare **Sì, Rimuovi bucket**.

[Anteprima tecnica] Gestione di un bucket utilizzando una risorsa personalizzata

È possibile aggiungere un bucket utilizzando una risorsa personalizzata (CR) Astra Control sul cluster di applicazioni. 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. Se si utilizza il metodo di risorsa personalizzato, la funzionalità snapshot applicazione richiede un bucket.

Non è necessario un bucket in Astra Control se si esegue il cloning della configurazione dell'applicazione e dello storage persistente sullo stesso cluster.

La risorsa personalizzata bucket per Astra Control è nota come AppVault. Questo CR contiene le configurazioni necessarie per l'uso di una benna nelle operazioni di protezione.

Prima di iniziare

- Assicurati di avere un bucket raggiungibile dai cluster gestiti da Astra Control Center.
- Assicurarsi di disporre delle credenziali per il bucket.
- Assicurarsi che la benna sia di uno dei seguenti tipi:
  - NetApp ONTAP S3
  - NetApp StorageGRID S3
  - Microsoft Azure
  - Generico S3

> Amazon Web Services (AWS) e Google Cloud Platform (GCP) utilizzano il tipo di bucket S3 generico.

> 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 rivendicano il supporto S3 di Amazon.

Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome (ad esempio, `astra-appvault.yaml`).
2. Configurare i seguenti attributi:
   - **metadata.name**: *(obbligatorio)* il nome della risorsa personalizzata AppVault.
   - **Spec.prefix**: *(Optional)* percorso preceduto dai nomi di tutte le entità memorizzate in AppVault.
   - **spec.providerConfig**: *(obbligatorio)* Memorizza la configurazione necessaria per accedere ad AppVault utilizzando il provider specificato.
   - **spec.providerCredentials**: *(obbligatorio)* archivia i riferimenti a qualsiasi credenziale richiesta per accedere ad AppVault utilizzando il provider specificato.
     - **spec.providerCredentials.valueFromSecret**: *(opzionale)* indica che il valore della credenziale deve provenire da un segreto.

    - **Key**: *(obbligatorio se viene utilizzato il valore FromSecret)* la chiave valida del segreto da selezionare.
    - **Nome**: *(obbligatorio se viene utilizzato il valore FromSecret)* Nome del segreto che contiene il valore per questo campo. Deve trovarsi nello stesso spazio dei nomi.
  - **spec.providerType**: *(obbligatorio)* determina cosa fornisce il backup; ad esempio, NetApp ONTAP S3 o Microsoft Azure.

  Esempio YAML:

```yaml
apiVersion: astra.netapp.io/v1
kind: AppVault
metadata:
  name: astra-appvault
spec:
  providerType: generic-s3
  providerConfig:
    path: testpath
    endpoint: 192.168.1.100:80
    bucketName: bucket1
    secure: "false"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        name: s3-creds
        key: accessKeyID
    secretAccessKey:
      valueFromSecret:
        name: s3-creds
        key: secretAccessKey
```

3. Dopo aver popolato il `astra-appvault.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-appvault.yaml -n astra-connector
```

> Quando si aggiunge un bucket, Astra Control contrassegna un bucket con l'indicatore bucket predefinito. Il primo bucket creato diventa quello predefinito. Con l'aggiunta di bucket, è possibile decidere in un secondo momento "impostare un altro bucket predefinito".

Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"

Monitorare le attività in esecuzione

In Astra Control è possibile visualizzare i dettagli relativi alle attività in esecuzione e alle attività che sono state completate, non riuscite o annullate nelle ultime 24 ore. Ad esempio, è possibile visualizzare lo stato di un'operazione di backup, ripristino o clonazione in esecuzione e visualizzare dettagli come percentuale completata e tempo rimanente stimato. È possibile visualizzare lo stato di un'operazione pianificata eseguita o avviata manualmente.

Durante la visualizzazione di un'attività in esecuzione o completata, è possibile espandere i dettagli dell'attività per visualizzare lo stato di ciascuna delle attività secondarie. La barra di avanzamento dell'attività è verde per le attività in corso o completate, blu per le attività annullate e rossa per le attività non riuscite a causa di un errore.

> Per le operazioni di cloni, le sottoattività dell'attività consistono in un'operazione di snapshot e un'operazione di ripristino dello snapshot.

Per ulteriori informazioni sulle attività non riuscite, fare riferimento a. "Monitorare l'attività dell'account".

Fasi

1. Mentre un'attività è in esecuzione, passare a **applicazioni**.
2. Selezionare il nome di un'applicazione dall'elenco.
3. Nei dettagli dell'applicazione, selezionare la scheda **Tasks**.

   È possibile visualizzare i dettagli delle attività correnti o passate e filtrare in base allo stato dell'attività.

> Le attività vengono conservate nell'elenco **Tasks** per un massimo di 24 ore. È possibile configurare questo limite e altre impostazioni di monitoraggio attività utilizzando "API di controllo Astra".

Gestisci il tuo account

Impostare la fatturazione

Puoi utilizzare più metodi per gestire la fatturazione del tuo account Astra Control Service. Se utilizzi Azure o Amazon AWS, puoi sottoscrivere un piano Astra Control Service tramite Microsoft Azure Marketplace o AWS Marketplace. In questo modo, è possibile gestire i dettagli di fatturazione tramite Marketplace. In alternativa, puoi iscriverti direttamente a NetApp. Se ti iscrivi direttamente a NetApp, puoi gestire i tuoi dati di fatturazione tramite Astra Control Service. Se utilizzi Astra Control Service senza un abbonamento, sei automaticamente iscritto al Free Plan.

Il piano gratuito di Astra Control Service ti consente di gestire fino a 10 spazi dei nomi nel tuo account. Se si desidera gestire più di 10 spazi dei nomi, è necessario impostare la fatturazione eseguendo l'aggiornamento dal piano gratuito al piano Premium o iscrivendosi a Azure Marketplace o AWS Marketplace.

Panoramica sulla fatturazione

Ci sono due tipi di costi associati all'utilizzo di Astra Control Service: Costi da parte di NetApp per l'Astra Control Service e costi da parte del cloud provider per volumi persistenti e storage a oggetti.

Fatturazione Astra Control Service

Astra Control Service offre tre piani:

Piano gratuito
: Gestisci fino a 10 spazi dei nomi gratuitamente.

Premium PayGo
: Gestisci una quantità illimitata di spazi dei nomi a una velocità specifica, per spazio dei nomi.

Abbonamento Premium
: Paga in anticipo a una tariffa scontata con un abbonamento annuale che ti consente di gestire fino a 20 spazi dei nomi per *namespace pack*. Contatta il reparto vendite NetApp per acquistare tutti i pacchetti necessari per la tua organizzazione. Ad esempio, acquistare 3 pacchetti per gestire 60 namespace da Astra Control Service. Se gestisci più spazi dei nomi di quelli consentiti dal tuo abbonamento annuale, ti verrà addebitato il costo del tasso di overage dipendente dall'abbonamento per spazio dei nomi aggiuntivo. Se non disponi ancora di un account Astra Control, l'acquisto dell'abbonamento Premium crea automaticamente un account Astra Control. Se disponi di un piano gratuito, sarai automaticamente convertito in un abbonamento Premium.

Quando crei un account Astra Control, sei automaticamente iscritto al Free Plan. La dashboard di Astra Control mostra quanti spazi dei nomi stai attualmente gestendo dai 10 spazi dei nomi liberi consentiti. La fatturazione inizia per uno spazio dei nomi quando viene gestita la prima applicazione contenente lo spazio dei nomi e si interrompe per tale spazio dei nomi quando l'ultima applicazione contenente lo spazio dei nomi non viene gestita.

Se cerchi di gestire un 11esimo spazio dei nomi, Astra Control ti avvisa che hai raggiunto il limite del Free Plan. Viene quindi richiesto di eseguire l'aggiornamento dal piano gratuito a un piano Premium. Ti verrà addebitata la tariffa di overage dipendente dall'abbonamento per spazio dei nomi extra.

Puoi passare a un Premium Plan in qualsiasi momento. Dopo l'aggiornamento, Astra Control inizia a addebitare i nomi dell'account. I primi 10 spazi dei nomi non rimangono nel piano libero.

Fatturazione Google Cloud

I volumi persistenti sono supportati da NetApp Cloud Volumes Service e i backup delle applicazioni vengono memorizzati in un bucket di storage cloud di Google.

- "Visualizza i dettagli dei prezzi per Cloud Volumes Service".

  Si noti che Astra Control Service supporta tutti i tipi di servizio e i livelli di servizio. Il tipo di servizio utilizzato dipende dal "Regione di Google Cloud".

- "Visualizza i dettagli dei prezzi per i bucket di storage Google Cloud".

Fatturazione a Microsoft Azure

I volumi persistenti sono supportati da Azure NetApp Files e i backup delle applicazioni vengono memorizzati in un container Azure Blob.

- "Visualizza i dettagli dei prezzi per Azure NetApp Files".
- "Visualizza i dettagli sui prezzi per lo storage Microsoft Azure Blob".
- "Visualizza i piani e i prezzi dei servizi Astra Control in Azure Marketplace"

> La tariffa di fatturazione di Azure per Astra Control Service è all'ora e una nuova ora di fatturazione inizia dopo 29 minuti dell'ora di utilizzo.

Fatturazione Amazon Web Services

I volumi persistenti sono supportati da EBS o FSX per NetApp ONTAP e i backup delle tue applicazioni sono memorizzati in un bucket AWS.

- "Visualizza i dettagli dei prezzi per Amazon Web Services".

Iscriviti a Astra Control Service in Azure Marketplace

Puoi iscriverti ad Astra Control Service utilizzando Azure Marketplace. Il tuo account e i dati di fatturazione vengono gestiti tramite Marketplace.

> Per visualizzare una panoramica video della procedura di abbonamento a Azure Marketplace, visitare il sito Web all'indirizzo "TV NetApp".

Fasi

1. Accedere alla "Azure Marketplace".
2. Selezionare **Get IT Now** (Ottieni ora).
3. Seguire le istruzioni per iscriversi a un piano.

Iscriviti a Astra Control Service in AWS Marketplace

Puoi iscriverti ad Astra Control Service utilizzando AWS Marketplace. Il tuo account e i dati di fatturazione vengono gestiti tramite Marketplace.

Fasi

1. Accedere alla "Mercato AWS".
2. Selezionare **Visualizza opzioni di acquisto**.
3. Se richiesto, accedere all'account AWS o creare un nuovo account.
4. Seguire le istruzioni per iscriversi a un piano.

Iscriviti ad Astra Control Service direttamente con NetApp

Puoi iscriverti ad Astra Control Service dall'interfaccia utente di Astra Control Service o contattando NetApp Sales.

Passa dal piano gratuito al piano Premium PayGo

Aggiorna il tuo piano di fatturazione in qualsiasi momento per iniziare a gestire più di 10 spazi dei nomi da Astra Control pagando a consumo. Tutto ciò di cui hai bisogno è una carta di credito valida.

Fasi

1. Selezionare **account**, quindi **Billing**.
2. In **piani**, accedere a **Premium PayGo** e selezionare **Aggiorna ora**.
3. Fornisci i dettagli di pagamento per una carta di credito valida e seleziona **Upgrade to Premium Plan**.

> Astra Control ti invia un'e-mail se la carta di credito sta per scadere.

Risultato

Ora puoi gestire più di 10 spazi dei nomi. Astra Control inizia a addebitare *tutti* gli spazi dei nomi che stai attualmente gestendo.

Passa dal piano gratuito all'abbonamento Premium

Contatta il reparto vendite NetApp per effettuare il prepagamento a un prezzo scontato con un abbonamento annuale.

Fasi

1. Selezionare **account**, quindi **Billing**.
2. In **piani**, accedere a **abbonamento Premium** e selezionare **contatto vendite**.
3. Fornire i dettagli al team di vendita per avviare il processo.

Risultato

Un rappresentante commerciale NetApp ti contatterà per elaborare l'ordine di acquisto. Una volta completato l'ordine, Astra Control rifletterà il piano corrente nella scheda **Billing**.

Visualizza i costi correnti e la cronologia di fatturazione

Astra Control mostra i costi mensili correnti, oltre a una cronologia di fatturazione dettagliata per spazio dei nomi. Se si è sottoscritto un piano tramite un Marketplace, la cronologia di fatturazione non è visibile (ma è possibile visualizzarla accedendo al Marketplace).

Fasi

1. Selezionare **account**, quindi **Billing**.

   I costi correnti vengono visualizzati sotto la panoramica di fatturazione.

2. Per visualizzare la cronologia di fatturazione in base allo spazio dei nomi, selezionare **Cronologia fatturazione**.

   Astra Control mostra i minuti di utilizzo e i costi per ogni namespace. Un minuto di utilizzo è il numero di minuti in cui Astra Control ha gestito lo spazio dei nomi durante un periodo di fatturazione.

3. Selezionare l'elenco a discesa per selezionare un mese precedente.

Cambiare la carta di credito per Premium PayGo

Se necessario, puoi cambiare la carta di credito che Astra Control ha in archivio per la fatturazione.

Fasi

1. Seleziona **account > fatturazione > metodo di pagamento**.
2. Selezionare l'icona di configurazione.

3. Modificare la carta di credito.

Note importanti

- Il tuo piano di fatturazione è per account Astra Control.

  Se si dispone di più account, ciascuno dispone di un proprio piano di fatturazione.

- La fattura di Astra Control include i costi per la gestione degli spazi dei nomi. Il tuo cloud provider addebita separatamente il back-end dello storage per i volumi persistenti.

  "Scopri di più sui prezzi di Astra Control".

- Ogni periodo di fatturazione termina l'ultimo giorno del mese.
- Non è possibile eseguire il downgrade da un piano Premium a un piano gratuito.

Invitare e rimuovere utenti

Invita gli utenti a unirsi al tuo account Astra Control e rimuovi gli utenti che non dovrebbero più avere accesso all'account.

Invitare utenti

I proprietari e gli amministratori dell'account possono invitare altri utenti a iscriversi all'account Astra Control.

Fasi

1. Assicurarsi che l'utente disponga di un "Accedi BlueXP".
2. Selezionare **account**.
3. Nella scheda **utenti**, selezionare **invita**.
4. Inserire il nome, l'indirizzo e-mail e il ruolo dell'utente.

   Tenere presente quanto segue:

   - L'indirizzo e-mail deve corrispondere all'indirizzo e-mail utilizzato dall'utente per l'iscrizione a BlueXP.
   - Ciascun ruolo fornisce le seguenti autorizzazioni:
     - 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.
5. Per aggiungere vincoli a un utente con ruolo membro o visualizzatore, attivare la casella di controllo **limita ruolo ai vincoli**.

   Per ulteriori informazioni sull'aggiunta di vincoli, fare riferimento a. "Gestire i ruoli".

6. Per invitare un altro utente, selezionare **Aggiungi un altro utente** e immettere le informazioni relative al nuovo utente.

   È possibile invitare fino a 10 utenti alla volta. È possibile spostarsi tra gli utenti che si stanno invitando nella parte sinistra della finestra di dialogo **invita utenti**.

7. Selezionare **invita utenti**.

Risultato

L'utente o gli utenti riceveranno un'e-mail che li invita a unirsi al tuo account.

Modificare il ruolo di un utente

Un account Owner può modificare il ruolo di tutti gli utenti, mentre un account Admin può modificare il ruolo degli utenti che hanno il ruolo di Amministratore, membro o visualizzatore.

Fasi

1. Selezionare **account**.
2. Nella scheda **utenti**, selezionare il menu nella colonna **azioni** dell'utente.
3. Selezionare **Modifica ruolo**.
4. Selezionare un nuovo ruolo.
5. Per aggiungere vincoli a un utente con ruolo membro o visualizzatore, attivare la casella di controllo **limita ruolo ai vincoli**.

   Per ulteriori informazioni sull'aggiunta di vincoli, fare riferimento a. "Gestire i ruoli".

6. Selezionare **Conferma**.

Risultato

Astra Control aggiorna le autorizzazioni dell'utente in base al nuovo ruolo selezionato.

Rimuovere gli utenti

Un utente con il ruolo Owner può rimuovere altri utenti dall'account in qualsiasi momento.

Fasi

1. Selezionare **account**.
2. Nella scheda **utenti**, selezionare gli utenti che si desidera rimuovere.
3. Selezionare il menu nella colonna **azioni** e selezionare **Rimuovi utente**.
4. Quando richiesto, confermare l'eliminazione digitando "Remove" (Rimuovi), quindi selezionare **Yes (Sì), Remove User (Rimuovi utente)**.

Risultato

Astra Control rimuove l'utente dall'account.

Gestire i ruoli

È possibile gestire i ruoli aggiungendo vincoli dello spazio dei nomi e limitando i ruoli utente a tali vincoli. In questo modo è possibile controllare l'accesso alle risorse all'interno dell'organizzazione. È possibile utilizzare l'interfaccia utente di Astra Control o. "L'API Astra Control" per gestire i ruoli.

Aggiungere un vincolo dello spazio dei nomi a un ruolo

Un utente Admin o Owner può aggiungere vincoli dello spazio dei nomi.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore.
4. Selezionare **Modifica ruolo**.
5. Attivare la casella di controllo **limita ruolo ai vincoli**.

   La casella di controllo è disponibile solo per i ruoli Member o Viewer. È possibile selezionare un ruolo diverso dall'elenco a discesa **ruolo**.

6. Selezionare **Aggiungi vincolo**.

   È possibile visualizzare l'elenco dei vincoli disponibili in base allo spazio dei nomi o all'etichetta dello spazio dei nomi.

7. Nell'elenco a discesa **tipo di vincolo**, selezionare **spazio dei nomi Kubernetes** o **etichetta dello spazio dei nomi Kubernetes** a seconda della configurazione degli spazi dei nomi.
8. Selezionare uno o più spazi dei nomi o etichette dall'elenco per comporre un vincolo che limiti i ruoli a tali spazi dei nomi.
9. Selezionare **Conferma**.

   La pagina **Modifica ruolo** visualizza l'elenco dei vincoli scelti per questo ruolo.

10. Selezionare **Conferma**.

    Nella pagina **account**, è possibile visualizzare i vincoli per qualsiasi ruolo membro o visualizzatore nella colonna **ruolo**.

> Se si abilitano i vincoli per un ruolo e si seleziona **Conferma** senza aggiungere alcun vincolo, il ruolo viene considerato con restrizioni complete (al ruolo viene negato l'accesso a tutte le risorse assegnate agli spazi dei nomi).

Rimuovere un vincolo dello spazio dei nomi da un ruolo

Un utente Admin o Owner può rimuovere un vincolo dello spazio dei nomi da un ruolo.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore con vincoli attivi.
4. Selezionare **Modifica ruolo**.

   La finestra di dialogo **Modifica ruolo** visualizza i vincoli attivi per il ruolo.

5. Selezionare la **X** a destra del vincolo da rimuovere.
6. Selezionare **Conferma**.

Per ulteriori informazioni

- "Ruoli e spazi dei nomi degli utenti"

Aggiungere e rimuovere le credenziali

Aggiungi e rimuovi le credenziali del cloud provider dal tuo account in qualsiasi momento. Astra Control utilizza queste credenziali per rilevare un cluster Kubernetes, le applicazioni sul cluster e per eseguire il provisioning delle risorse per conto dell'utente.

Tutti gli utenti di Astra Control condividono gli stessi set di credenziali.

Aggiungere credenziali

Il metodo più comune per aggiungere credenziali ad Astra Control consiste nella gestione dei cluster, ma è anche possibile aggiungere credenziali dalla pagina account. Le credenziali saranno quindi disponibili per la gestione di cluster Kubernetes aggiuntivi.

Prima di iniziare

- Per Amazon Web Services, è necessario disporre dell'output JSON delle credenziali dell'account IAM utilizzato per creare il cluster. "Scopri come configurare un utente IAM".
- Per GKE, è necessario disporre del file della chiave dell'account di servizio per un account di servizio che dispone delle autorizzazioni necessarie. "Scopri come configurare un account di servizio".
- Per AKS, è necessario disporre del file JSON che contiene l'output dell'interfaccia CLI di Azure al momento della creazione dell'entità del servizio. "Scopri come configurare un service principal".

  Avrai inoltre bisogno del tuo ID di abbonamento Azure, se non lo hai aggiunto al file JSON.

Fasi

1. Selezionare **account > credenziali**.
2. Selezionare **Aggiungi credenziali**.
3. Selezionare **Microsoft Azure**.
4. Selezionare **Google Cloud Platform**.
5. Selezionare **Amazon Web Services**.
6. Immettere un nome per le credenziali che le distinguano dalle altre in Astra Control.
7. Fornire le credenziali richieste.
8. **Microsoft Azure**: Fornisci ad Astra Control i dettagli sull'entità del servizio Azure caricando un file JSON o incollando il contenuto del file JSON dagli Appunti.

   Il file JSON deve contenere l'output dell'interfaccia CLI di Azure al momento della creazione dell'entità del servizio. Può anche includere il tuo ID di abbonamento in modo che venga aggiunto automaticamente ad Astra Control. In caso contrario, è necessario inserire manualmente l'ID dopo aver fornito il codice JSON.

9. **Google Cloud Platform**: Fornire il file delle chiavi dell'account del servizio Google Cloud caricando il file o incollando il contenuto dagli Appunti.
10. **Amazon Web Services**: Fornisci le credenziali utente IAM di Amazon Web Services caricando il file o incollando il contenuto dagli Appunti.
11. Selezionare **Aggiungi credenziali**.

Risultato

Le credenziali sono ora disponibili per la selezione quando si aggiunge un cluster ad Astra Control.

Rimuovere le credenziali

Rimuovere le credenziali da un account in qualsiasi momento. Rimuovere le credenziali solo dopo "annullamento della gestione di tutti i cluster", a meno che non si stiano ruotando le credenziali (fare riferimento a. Ruotare le credenziali).

> Il primo set di credenziali aggiunto ad Astra Control è sempre in uso perché Astra Control utilizza le credenziali per l'autenticazione nel bucket di backup. Si consiglia di non rimuovere queste credenziali.

Fasi

1. Selezionare **account > credenziali**.
2. Selezionare l'elenco a discesa nella colonna **Stato** per le credenziali che si desidera rimuovere.
3. Selezionare **Rimuovi**.
4. Digitare il nome delle credenziali per confermare l'eliminazione, quindi selezionare **Sì, Rimuovi credenziali**.

Risultato

Astra Control rimuove le credenziali dall'account.

Ruotare le credenziali

È possibile ruotare le credenziali nell'account. Se si ruotano le credenziali, ruotarle durante una finestra di manutenzione quando non sono in corso backup (pianificati o on-demand).

Fasi

1. Rimuovere le credenziali esistenti seguendo la procedura descritta in Rimuovere le credenziali.
2. Aggiungere le nuove credenziali seguendo la procedura descritta in Aggiungere credenziali.
3. Aggiorna tutti i bucket per utilizzare le nuove credenziali:
   a. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
   b. Selezionare l'elenco a discesa nella colonna **azioni** per il bucket che si desidera modificare.
   c. Selezionare **Modifica**.
   d. Nella sezione **Select credentials** (Seleziona credenziali), scegliere le nuove credenziali aggiunte ad Astra Control.
   e. Selezionare **Aggiorna**.
   f. Ripetere i passaggi da **b** a **e** per tutti i bucket rimanenti sul sistema.

Risultato

Astra Control inizia a utilizzare le nuove credenziali del cloud provider.

Monitorare l'attività dell'account

Puoi visualizzare i dettagli delle attività nel tuo account Astra Control. Ad esempio, quando sono stati invitati nuovi utenti, quando è stato aggiunto un cluster o quando è

stata acquisita una snapshot. È inoltre possibile esportare l'attività dell'account in un file CSV.

Visualizza tutte le attività dell'account in Astra Control

1. Selezionare **Activity** (attività).
2. Utilizza i filtri per restringere l'elenco delle attività o utilizza la casella di ricerca per trovare esattamente ciò che stai cercando.
3. Selezionare **Export to CSV** (Esporta in CSV) per scaricare l'attività dell'account in un file CSV.

Visualizzare l'attività dell'account per un'applicazione specifica

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Activity** (attività).

Visualizzare l'attività dell'account per i cluster

1. Selezionare **Clusters**, quindi il nome del cluster.
2. Selezionare **Activity** (attività).

Visualizzare e gestire le notifiche

Astra Control avvisa 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. Selezionare il numero di notifiche non lette in alto a destra.
2. Esaminare le notifiche, quindi selezionare **Contrassegna come letto** o **Mostra tutte le notifiche**.

   Se si seleziona **Mostra tutte le notifiche**, viene caricata la pagina Notifiche.

3. Nella pagina **Notifiche**, visualizzare le notifiche, selezionare quelle che si desidera contrassegnare come lette, selezionare **azione** e selezionare **Contrassegna come letta**.

Chiudere l'account

Se non hai più bisogno del tuo account Astra Control, puoi chiuderlo in qualsiasi momento.

> I bucket creati automaticamente da Astra Control verranno eliminati automaticamente alla chiusura dell'account.

Fasi

1. "Annulla la gestione di tutte le applicazioni e i cluster".
2. "Rimuovere le credenziali da Astra Control".

3. Seleziona **account > fatturazione > metodo di pagamento**.
4. Selezionare **Chiudi account**.
5. Inserire il nome dell'account e confermare per chiudere l'account.

Gestire le istanze cloud

Un'istanza di cloud è un dominio unico all'interno di un cloud provider. È possibile creare più istanze cloud per ciascun provider cloud e ogni istanza cloud ha il proprio nome, le proprie credenziali e i cluster associati.

Si crea un'istanza cloud quando si aggiunge un nuovo cluster ad Astra Control. È possibile modificare un'istanza cloud per modificarne il nome o il bucket predefinito utilizzando l'interfaccia utente di Astra Control ed eseguire altre azioni con l'istanza cloud utilizzando l'API di Astra Control.

Aggiungere un'istanza cloud

È possibile aggiungere una nuova istanza di cloud quando si aggiunge un nuovo cluster ad Astra Control. Fare riferimento a. "Inizia a gestire i cluster Kubernetes da Astra Control Service" per ulteriori informazioni.

Modificare un'istanza di cloud

È possibile modificare un'istanza di cloud esistente per un provider di cloud.

Fasi

1. Accedere a **istanze cloud**.
2. Nell'elenco delle istanze cloud, selezionare il menu **azioni** dell'istanza cloud che si desidera modificare.
3. Selezionare **Modifica**.

   In questa pagina, è possibile aggiornare il nome e il bucket predefinito per l'istanza del cloud.

   Ogni istanza di cloud in Astra Control deve avere un nome univoco.

Ruotare le credenziali per un'istanza cloud

È possibile utilizzare l'API di controllo Astra per ruotare le credenziali per un'istanza cloud. Per saperne di più, "Consultare i documenti di automazione Astra".

Rimuovere un'istanza cloud

È possibile utilizzare l'API Astra Control per rimuovere un'istanza cloud da un provider cloud. Per saperne di più, "Consultare i documenti di automazione Astra".

Abilita Astra Control Provisioner

Astra Trident le versioni 23,10 e successive includono la possibilità di utilizzare Astra Control Provivisioner, che consente agli utenti dotati di licenza Astra Control di accedere a funzionalità avanzate di provisioning dello storage. Astra Control Provisioner fornisce questa funzionalità estesa oltre alle funzionalità standard basate su CSI Astra Trident. È

possibile utilizzare questa procedura per abilitare e installare Astra Control Provisioner.

L'abbonamento a Astra Control Service include automaticamente la licenza per l'utilizzo di Astra Control Provisioner.

In arrivo gli update di Astra Control, Astra Control Provivisioner sostituirà Astra Trident come provisioner di storage e orchestrator e sarà obbligatorio per l'utilizzo di Astra Control. Per questo motivo, si consiglia vivamente agli utenti di Astra Control di attivare Astra Control Provisioner. Astra Trident continuerà a rimanere open source e ad essere rilasciato, mantenuto, supportato e aggiornato con le nuove CSI e altre funzionalità di NetApp.

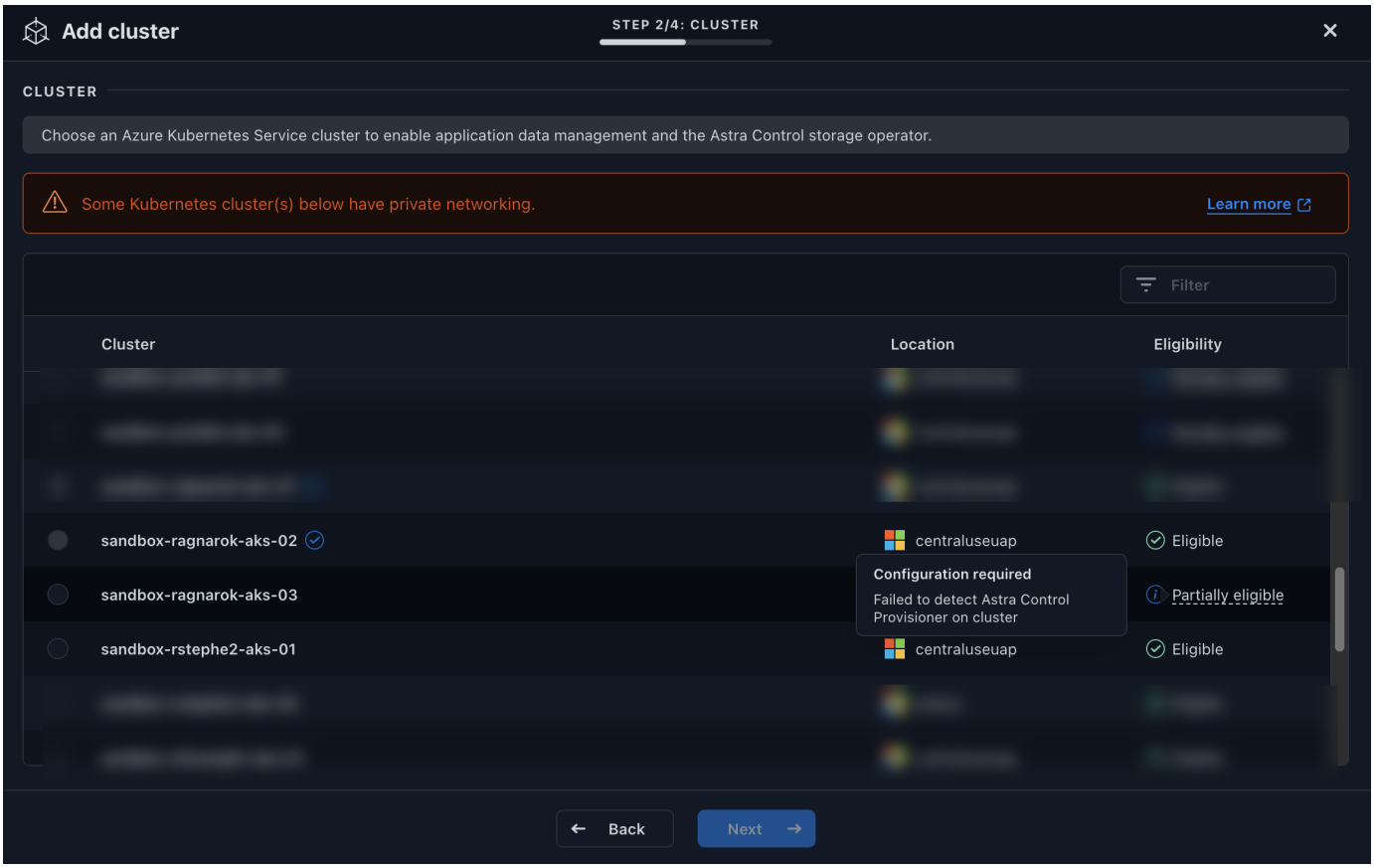
Come faccio a sapere se devo abilitare Astra Control Provivisioner?

Se Aggiungi un cluster a Astra Control Service che non ha Astra Trident precedentemente installato, il cluster verrà contrassegnato come `Eligible`. Dopo di lei "Aggiungi il cluster a Astra Control", Astra Control provisioner verrà abilitato automaticamente.

Se il cluster non è contrassegnato `Eligible`, verrà contrassegnato `Partially eligible` per uno dei seguenti motivi:

- Sta utilizzando una versione meno recente di Astra Trident
- Sta utilizzando un Astra Trident 23,10 che non ha ancora attivato l'opzione di provisioning
- Si tratta di un tipo di cluster che non consente l'abilitazione automatica

Per `Partially eligible` Casi, usa queste istruzioni per abilitare manualmente Astra Control Provisioner per il tuo cluster.



Prima di attivare Astra Control Provisioner

Se hai già un Astra Trident senza Astra Control Provivisioner e vuoi abilitare Astra Control Provivisioner, esegui prima quanto segue:

- **Se Astra Trident è installato, conferma che la sua versione si trovi all'interno di una finestra a quattro release**: Puoi eseguire un aggiornamento diretto a Astra Trident 24,02 con Astra Control Provisioner se il tuo Astra Trident si trova all'interno di una finestra a quattro release della versione 24,02. Ad esempio, puoi eseguire l'upgrade direttamente da Astra Trident 23,04 a 24,02.
- **Confirmi che il tuo cluster ha un'architettura di sistema AMD64**: L'immagine Astra Control Provivisioner è fornita in entrambe le architetture CPU AMD64 e ARM64, ma solo AMD64 è supportato da Astra Control.

Fasi

1. Accedere al Registro di sistema dell'immagine di controllo Astra di NetApp:
   a. Effettua l'accesso all'interfaccia utente di Astra Control Service e registra l'ID account Astra Control.
      i. Selezionare l'icona della figura in alto a destra nella pagina.
      ii. Selezionare **API access**.
      iii. Annotare l'ID account.
   b. Nella stessa pagina, selezionare **generate API token**, copiare la stringa del token API negli Appunti e salvarla nell'editor.
   c. Accedere al registro Astra Control utilizzando il metodo preferito:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. (Solo registri personalizzati) attenersi alla seguente procedura per spostare l'immagine nel registro personalizzato. Se non si utilizza un registro, seguire i passaggi dell'operatore Trident nel sezione successiva.

> Per i seguenti comandi, puoi utilizzare Podman al posto di Docker. Se si utilizza un ambiente Windows, si consiglia di utilizzare PowerShell.

Docker

a. Estrarre l'immagine di Astra Control provisioner dal Registro di sistema:

> L'immagine estratta non supporta più piattaforme e supporta solo la stessa piattaforma dell'host che ha estratto l'immagine, ad esempio Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform <cluster platform>
```

Esempio:

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform linux/amd64
```

b. Contrassegnare l'immagine:

```
docker tag cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

c. Inviare l'immagine al registro personalizzato:

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

Gru

a. Copiare il manifesto di Astra Control Provisioner nel registro personalizzato:

```
crane copy cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

3. Determinare se il metodo di installazione originale di Astra Trident ha utilizzato un.
4. Abilita Astra Control Provisioner in Astra Trident utilizzando il metodo di installazione utilizzato originariamente:

Operatore Astra Trident

a. "Scaricare il programma di installazione di Astra Trident ed estrarlo".

b. Completa questi passaggi se non hai ancora installato Astra Trident o se hai rimosso l'operatore dall'implementazione originale di Astra Trident:

   i. Creare il CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.1
6.yaml
```

   ii. Creare lo spazio dei nomi tridente (`kubectl create namespace trident`) o confermare che lo spazio dei nomi tridente esiste ancora (`kubectl get all -n trident`). Se lo spazio dei nomi è stato rimosso, crearlo di nuovo.

c. Aggiorna Astra Trident alla versione 24.02.0:

> Per i cluster che eseguono Kubernetes 1.24 o versioni precedenti, utilizzare `bundle_pre_1_25.yaml`. Per i cluster che eseguono Kubernetes 1.25 o versioni successive, utilizzare `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer/deploy/<bundle-
name.yaml>
```

d. Verificare che Astra Trident sia in esecuzione:

```
kubectl get torc -n trident
```

Risposta:

```
NAME      AGE
trident   21m
```

e. se si dispone di un registro che utilizza segreti, creare un segreto da utilizzare per estrarre l'immagine di Astra Control Provisioner:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

f. Modificare il TridentOrchestrator CR e apportare le seguenti modifiche:

```
kubectl edit torc trident -n trident
```

i. Impostare una posizione del Registro di sistema personalizzata per l'immagine Astra Trident o estrarla dal Registro di sistema Astra Control (`tridentImage: <my_custom_registry>/trident:24.02.0` oppure `tridentImage: netapp/trident:24.02.0`).

ii. Abilita Astra Control Provisioner (`enableACP: true`).

iii. Impostare la posizione del Registro di sistema personalizzata per l'immagine Astra Control Provivioner o estrarla dal Registro di sistema Astra Control (`acpImage: <my_custom_registry>/trident-acp:24.02.0` oppure `acpImage: cr.astra.netapp.io/astra/trident-acp:24.02.0`).

iv. Se stabilito segreti di estrazione delle immagini in precedenza, è possibile impostarle qui (`imagePullSecrets: - <secret_name>`). Usare lo stesso nome segreto che hai stabilito nei passaggi precedenti.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:24.02.0
  enableACP: true
  acpImage: <registry>/trident-acp:24.02.0
  imagePullSecrets:
  - <secret_name>
```

g. Salvare e uscire dal file. Il processo di distribuzione si avvia automaticamente.

h. Verificare che l'operatore, la distribuzione e i replicaset siano stati creati.

```
kubectl get all -n trident
```

> In un cluster Kubernetes dovrebbe esserci solo **un'istanza** dell'operatore. Non creare implementazioni multiple dell'operatore Astra Trident.

i. Verificare `trident-acp` il container è in esecuzione e così `acpVersion` è `24.02.0` con stato di `Installed`:

```
kubectl get torc -o yaml
```

Risposta:

```
status:
  acpVersion: 24.02.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:24.02.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

a. "Scaricare il programma di installazione di Astra Trident ed estrarlo".

b. "Se disponi già di un Astra Trident, disinstallarlo dal cluster che lo ospita".

c. Installa Astra Trident con Astra Control Provisioner abilitato (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:24.02
```

d. Confermare che Astra Control Provisioner è stato abilitato:

```
./tridentctl -n trident version
```

Risposta:

```
+----------------+----------------+-------------+ | SERVER
VERSION | CLIENT VERSION | ACP VERSION | +----------------
+----------------+-------------+ | 24.02.0 | 24.02.0 | 24.02.0. |
+----------------+----------------+-------------+
```

Timone

a. Se hai installato Astra Trident 23.07.1 o una versione precedente, "disinstallazione" l'operatore e gli altri componenti.

b. Se il cluster Kubernetes esegue la versione 1,24 o precedente, elimina psp:

```
kubectl delete psp tridentoperatorpod
```

c. Aggiungere il repository Astra Trident Helm:

```
helm repo add netapp-trident https://netapp.github.io/trident-
helm-chart
```

d. Aggiornare il grafico Helm:

```
helm repo update netapp-trident
```

Risposta:

```
Hang tight while we grab the latest from your chart
repositories...
...Successfully got an update from the "netapp-trident" chart
repository
Update Complete. □Happy Helming!□
```

e. Elencare le immagini:

```
./tridentctl images -n trident
```

Risposta:

```
| v1.28.0            | netapp/trident:24.02.0|
|                    | docker.io/netapp/trident-
autosupport:24.02|
|                    | registry.k8s.io/sig-storage/csi-
provisioner:v4.0.0|
|                    | registry.k8s.io/sig-storage/csi-
attacher:v4.5.0|
|                    | registry.k8s.io/sig-storage/csi-
resizer:v1.9.3|
|                    | registry.k8s.io/sig-storage/csi-
snapshotter:v6.3.3|
|                    | registry.k8s.io/sig-storage/csi-node-
driver-registrar:v2.10.0 |
|                    | netapp/trident-operator:24.02.0 (optional)
```

f. Assicurarsi che l’operatore di tridente 24.02.0 sia disponibile:

```
helm search repo netapp-trident/trident-operator --versions
```

Risposta:

```
NAME                            CHART VERSION   APP VERSION
DESCRIPTION
netapp-trident/trident-operator 100.2402.0      24.02.0         A
```

g. Utilizzare `helm install` ed eseguire una delle seguenti opzioni che includono queste impostazioni:
   - Un nome per la posizione di distribuzione
   - La versione di Astra Trident
   - Il nome dell'immagine di Astra Control provisioner
   - Il flag per abilitare il provisioner
   - (Facoltativo) percorso del Registro di sistema locale. Se si utilizza un registro locale, il "Immagini Trident" Può trovarsi in un registro o in registri diversi, ma tutte le immagini CSI devono trovarsi nello stesso registro.
   - Il namespace Trident

Opzioni

- Immagini senza registro

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=cr.astra.netapp.io/astra/trident-
acp:24.02.0 --set enableACP=true --set operatorImage=netapp/trident-
operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

- Immagini in uno o più registri

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=<your-registry>:<acp image> --set
enableACP=true --set imageRegistry=<your-registry>/sig-storage --set
operatorImage=netapp/trident-operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

È possibile utilizzare `helm list` per rivedere i dettagli dell'installazione, ad esempio nome, spazio dei nomi, grafico, stato, versione dell'applicazione, e numero di revisione.

Se hai problemi nell'implementazione di Trident utilizzando Helm, esegui questo comando per disinstallare completamente Astra Trident:

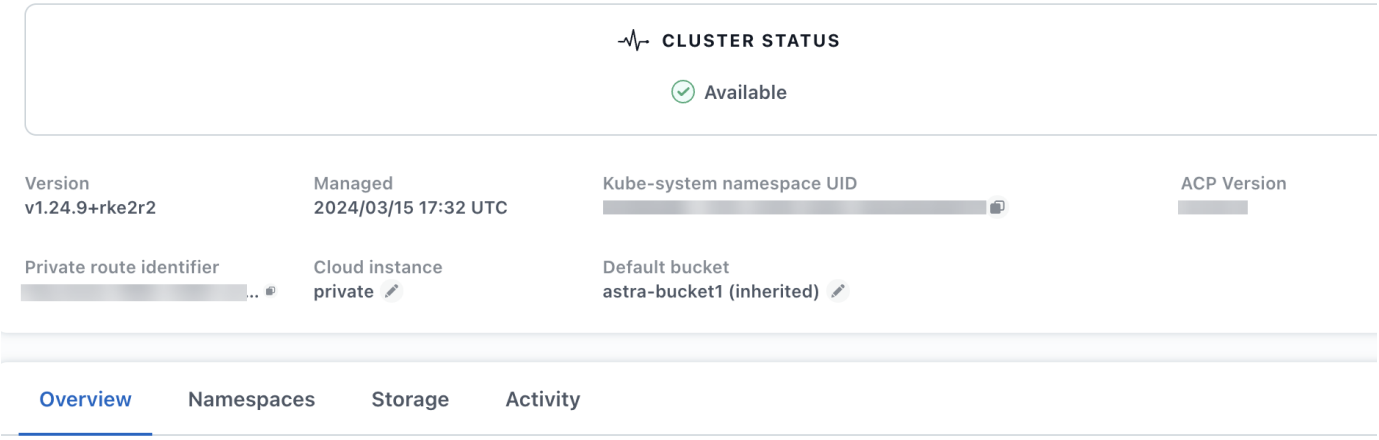
```
./tridentctl uninstall -n trident
```

Non fare "Rimuovere completamente i CRD Astra Trident" Come parte della disinstallazione prima di tentare di attivare nuovamente Astra Control Provivisioner.

Risultato

La funzionalità Astra Control Provisioner è abilitata ed è possibile utilizzare qualsiasi funzionalità disponibile per la versione in esecuzione.

Dopo l'installazione di Astra Control provisioner, il cluster che ospita il provisioner nell'interfaccia utente Astra Control mostrerà un `ACP version` piuttosto che `Trident version` campo e numero della versione installata corrente.



Per ulteriori informazioni

- "Documentazione sugli aggiornamenti di Astra Trident"

Annulla la gestione di app e cluster

Rimuovi le app o i cluster che non vuoi più gestire da Astra Control.

Interrompere 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.

Quando si annulla la gestione di un'applicazione:

- Eventuali backup e snapshot esistenti verranno eliminati.
- Le applicazioni e i dati rimangono disponibili.

Fasi

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

Risultato

Astra Control interrompe la gestione dell'applicazione.

Interrompere la gestione di un cluster

Interrompere la gestione del cluster che non si desidera più gestire da Astra Control.

> Prima di annullare la gestione del cluster, è necessario annullare la gestione delle applicazioni associate al cluster.

Come Best practice, si consiglia di rimuovere il cluster da Astra Control prima di eliminarlo tramite GCP.

Quando si annulla la gestione di un cluster:

- Questa azione impedisce la gestione del cluster da parte di Astra Control. Non apporta modifiche alla configurazione del cluster e non elimina il cluster.
- Astra Control Provivisioner o Astra Trident non verranno disinstallati dal cluster. "Scopri come disinstallare Astra Trident".

Fasi

1. Selezionare **Clusters**.
2. Selezionare la casella di controllo del cluster che non si desidera più gestire.
3. Dal menu delle opzioni nella colonna **azioni**, selezionare **Annulla gestione**.
4. Confermare che si desidera annullare la gestione del cluster, quindi selezionare **Sì, Annulla gestione**.

Risultato

Lo stato del cluster cambia in **Removing** (Rimozione). In seguito, il cluster verrà rimosso dalla pagina **Clusters** e non sarà più gestito da Astra Control.

Eliminazione di cluster dal provider cloud

Prima di eliminare un cluster Kubernetes con volumi persistenti (PV) che risiedono nelle classi di storage NetApp, è necessario prima eliminare le dichiarazioni di volumi persistenti (PVC) seguendo uno dei metodi riportati di seguito. Eliminando PVC e PV prima di eliminare il cluster, non riceverai fatture inattese dal tuo cloud provider.

- Metodo n. 1*: Eliminare gli spazi dei nomi dei carichi di lavoro dell'applicazione dal cluster. Non eliminare lo spazio dei nomi Trident.
- Metodo 2*: Eliminare i PVC e i pod o l'implementazione in cui sono montati i PVS.

Quando gestisci un cluster Kubernetes da Astra Control, le applicazioni su quel cluster utilizzano il tuo cloud provider come back-end dello storage per i volumi persistenti. Se elimini il cluster dal tuo cloud provider senza prima rimuovere il PVS, i volumi di back-end vengono *non* cancellati insieme al cluster.

Utilizzando uno dei metodi descritti in precedenza, il PVS corrispondente viene eliminato dal cluster. Assicurarsi che non vi siano PVS che risiedono nelle classi di storage NetApp sul cluster prima di eliminarlo.

Se i volumi persistenti non sono stati eliminati prima dell'eliminazione del cluster, sarà necessario eliminare manualmente i volumi di back-end dal provider cloud.

Implementa un’istanza autogestita di Astra Control

Se desideri un’istanza autogestita di Astra Control all’interno della rete, puoi implementare Astra Control Center direttamente da Astra Control Service.

Fasi

1. Nell’area Getting Started del Dashboard, selezionare **distribuire un’istanza autogestita di Astra Control**.
2. Effettuare una delle seguenti operazioni:
   - Generare un nuovo token API selezionando **generate**.
   - Incolla in un token dell’API REST Astra Control esistente. Fare riferimento a. "Documentazione di Astra Automation" Per istruzioni sulla generazione di un token API.
3. Seguire le istruzioni nella finestra **Deploy Astra Control Center**.

Utilizza Astra Control Provisioner

Configurare la crittografia backend dello storage

Con Astra Control Provivisioner, puoi migliorare la sicurezza dell'accesso ai dati abilitando la crittografia per il traffico tra il cluster gestito e il backend dello storage.

Astra Control Provivisioner supporta la crittografia Kerberos per due tipi di backend di storage:

- **On-premise ONTAP** - Astra Control Provisioner supporta la crittografia Kerberos su connessioni NFSv3 e NFSv4 da Red Hat OpenShift e dai cluster Kubernetes upstream ai volumi ONTAP on-premise.
- **Azure NetApp Files** - Astra Control Provisioner supporta la crittografia Kerberos su connessioni NFSv4,1 da cluster Kubernetes upstream a volumi Azure NetApp Files.

Puoi creare, eliminare, ridimensionare, creare snapshot, clonare clone di sola lettura e importare i volumi che utilizzano la crittografia NFS.

Configura la crittografia Kerberos in-flight con i volumi ONTAP on-premise

Puoi attivare la crittografia Kerberos sul traffico storage tra il cluster gestito e un backend dello storage ONTAP on-premise.

> La crittografia Kerberos per il traffico NFS con backend di storage ONTAP on-premise è supportata solo utilizzando `ontap-nas` driver di storage.

Prima di iniziare

- Assicurarsi di avere "Abilitato Astra Control Provisioner" nel cluster gestito.
- Assicurarsi di avere accesso a. `tridentctl` utility.
- Assicurarsi di disporre dell'accesso come amministratore al back-end dello storage ONTAP.
- Conoscere il nome del volume o dei volumi che si desidera condividere dal back-end dello storage ONTAP.
- Verificare di aver preparato la VM di storage ONTAP per supportare la crittografia Kerberos per i volumi NFS. Fare riferimento a. "Attivare Kerberos su una LIF dati" per istruzioni.
- Verificare che tutti i volumi NFSv4 utilizzati con la crittografia Kerberos siano configurati correttamente. Consultare la sezione Configurazione di dominio NetApp NFSv4 (pagina 13) della "Guida ai miglioramenti e alle Best practice di NetApp NFSv4".

Aggiungere o modificare criteri di esportazione ONTAP

Devi aggiungere regole alle policy di esportazione ONTAP esistenti o creare nuove policy di esportazione che supportino la crittografia Kerberos per il volume root delle macchine virtuali di storage ONTAP, oltre a qualsiasi volume ONTAP condiviso con il cluster Kubernetes upstream. Le regole dei criteri di esportazione aggiunte o i nuovi criteri di esportazione creati devono supportare i seguenti protocolli di accesso e autorizzazioni di accesso:

Protocolli di accesso

Configura la policy di esportazione con i protocolli di accesso NFS, NFSv3 e NFSv4.

Dettagli di accesso

È possibile configurare una delle tre diverse versioni della crittografia Kerberos, a seconda delle esigenze del volume:

- **Kerberos 5** - (autenticazione e crittografia)
- **Kerberos 5i** - (autenticazione e crittografia con protezione dell'identità)
- **Kerberos 5p** - (autenticazione e crittografia con protezione di identità e privacy)

Configurare la regola dei criteri di esportazione ONTAP con le autorizzazioni di accesso appropriate. Ad esempio, se i cluster montano i volumi NFS con una combinazione di crittografia Kerberos 5i e Kerberos 5p, utilizza le seguenti impostazioni di accesso:

Tipo	Accesso in sola lettura	Accesso in lettura/scrittura	Accesso superutente
UNIX	Attivato	Attivato	Attivato
Kerberos 5i	Attivato	Attivato	Attivato
Kerberos 5p	Attivato	Attivato	Attivato

Per informazioni su come creare policy di esportazione e regole delle policy di esportazione di ONTAP, consulta la seguente documentazione:

- "Creare una policy di esportazione"
- "Aggiungere una regola a un criterio di esportazione"

Creazione di un backend dello storage

Puoi creare una configurazione backend dello storage Astra Control Provivisioner che include funzionalità di crittografia Kerberos.

A proposito di questa attività

Quando si crea un file di configurazione backend di archiviazione che configura la crittografia Kerberos, è possibile specificare una delle tre versioni diverse della crittografia Kerberos utilizzando `spec.nfsMountOptions` parametro:

- `spec.nfsMountOptions: sec=krb5` (autenticazione e crittografia)
- `spec.nfsMountOptions: sec=krb5i` (autenticazione e crittografia con protezione dell'identità)
- `spec.nfsMountOptions: sec=krb5p` (autenticazione e crittografia con protezione di identità e privacy)

Specificare un solo livello Kerberos. Se si specificano più livelli di crittografia Kerberos nell'elenco dei parametri, viene utilizzata solo la prima opzione.

Fasi

1. Nel cluster gestito, creare un file di configurazione backend dello storage utilizzando l'esempio seguente. Sostituire i valori tra parentesi <> con le informazioni dell'ambiente:

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-ontap-nas-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-ontap-nas
spec:
  version: 1
  storageDriverName: "ontap-nas"
  managementLIF: <STORAGE_VM_MGMT_LIF_IP_ADDRESS>
  dataLIF: <PROTOCOL_LIF_FQDN_OR_IP_ADDRESS>
  svm: <STORAGE_VM_NAME>
  username: <STORAGE_VM_USERNAME_CREDENTIAL>
  password: <STORAGE_VM_PASSWORD_CREDENTIAL>
  nasType: nfs
  nfsMountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
  qtreesPerFlexvol:
  credentials:
    name: backend-ontap-nas-secret
```

2. Utilizzare il file di configurazione creato nel passaggio precedente per creare il backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Se la creazione del backend non riesce, si è verificato un errore nella configurazione del backend. È possibile visualizzare i log per determinare la causa eseguendo il seguente comando:

```
tridentctl logs
```

Dopo aver identificato e corretto il problema con il file di configurazione, è possibile eseguire nuovamente il comando create.

Creare una classe di storage

È possibile creare una classe di archiviazione per il provisioning dei volumi con la crittografia Kerberos.

A proposito di questa attività

Quando si crea un oggetto classe di archiviazione, è possibile specificare una delle tre versioni diverse della crittografia Kerberos utilizzando `mountOptions` parametro:

- `mountOptions: sec=krb5` (autenticazione e crittografia)
- `mountOptions: sec=krb5i` (autenticazione e crittografia con protezione dell'identità)
- `mountOptions: sec=krb5p` (autenticazione e crittografia con protezione di identità e privacy)

Specificare un solo livello Kerberos. Se si specificano più livelli di crittografia Kerberos nell'elenco dei parametri, viene utilizzata solo la prima opzione. Se il livello di crittografia specificato nella configurazione backend di archiviazione è diverso dal livello specificato nell'oggetto della classe di archiviazione, l'oggetto della classe di archiviazione ha la precedenza.

Fasi

1. Creare un oggetto Kubernetes StorageClass, usando il seguente esempio:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: ontap-nas-sc
provisioner: csi.trident.netapp.io
mountOptions: ["sec=krb5i"] #can be krb5, krb5i, or krb5p
parameters:
  backendType: "ontap-nas"
  storagePools: "ontapnas_pool"
  trident.netapp.io/nasType: "nfs"
allowVolumeExpansion: True
```

2. Creare la classe di storage:

```
kubectl create -f sample-input/storage-class-ontap-nas-sc.yaml
```

3. Assicurarsi che la classe di archiviazione sia stata creata:

```
kubectl get sc ontap-nas-sc
```

L'output dovrebbe essere simile a quanto segue:

```
NAME            PROVISIONER             AGE
ontap-nas-sc    csi.trident.netapp.io   15h
```

Provisioning dei volumi

Dopo aver creato un backend di storage e una classe di storage, è ora possibile eseguire il provisioning di un

volume. Fare riferimento a queste istruzioni per "provisioning di un volume".

Configurare la crittografia Kerberos in-flight con i volumi Azure NetApp Files

È possibile attivare la crittografia Kerberos sul traffico di storage tra il cluster gestito e un singolo backend di storage Azure NetApp Files o un pool virtuale di backend di storage Azure NetApp Files.

Prima di iniziare

- Assicurati di aver abilitato Astra Control Provivisioner sul cluster Red Hat OpenShift gestito. Fare riferimento a. "Abilita Astra Control Provisioner" per istruzioni.
- Assicurarsi di avere accesso a. `tridentctl` utility.
- Assicurarsi di aver preparato il backend dello storage Azure NetApp Files per la crittografia Kerberos annotando i requisiti e seguendo le istruzioni in "Documentazione Azure NetApp Files".
- Verificare che tutti i volumi NFSv4 utilizzati con la crittografia Kerberos siano configurati correttamente. Consultare la sezione Configurazione di dominio NetApp NFSv4 (pagina 13) della "Guida ai miglioramenti e alle Best practice di NetApp NFSv4".

Creazione di un backend dello storage

È possibile creare una configurazione backend dello storage Azure NetApp Files che include la funzionalità di crittografia Kerberos.

A proposito di questa attività

Quando si crea un file di configurazione backend dello storage che configura la crittografia Kerberos, è possibile definirlo in modo che venga applicato a uno dei due livelli possibili:

- Il **livello backend di archiviazione** utilizzando `spec.kerberos` campo
- Il livello **pool virtuale** utilizzando `spec.storage.kerberos` campo

Quando si definisce la configurazione a livello del pool virtuale, il pool viene selezionato utilizzando l'etichetta nella classe di archiviazione.

In entrambi i livelli, è possibile specificare una delle tre diverse versioni della crittografia Kerberos:

- `kerberos: sec=krb5` (autenticazione e crittografia)
- `kerberos: sec=krb5i` (autenticazione e crittografia con protezione dell'identità)
- `kerberos: sec=krb5p` (autenticazione e crittografia con protezione di identità e privacy)

Fasi

1. Nel cluster gestito, creare un file di configurazione backend dello storage utilizzando uno dei seguenti esempi, a seconda del punto in cui occorre definire il backend dello storage (livello di backend dello storage o livello del pool virtuale). Sostituire i valori tra parentesi <> con le informazioni dell'ambiente:

Esempio di livello di backend di archiviazione

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

Esempio di livello del pool virtuale

```yaml
apiVersion: v1
kind: Secret
metadata:
  name: backend-tbc-anf-secret
type: Opaque
stringData:
  clientID: <CLIENT_ID>
  clientSecret: <CLIENT_SECRET>
---
apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-anf
spec:
  version: 1
  storageDriverName: azure-netapp-files
  subscriptionID: <SUBSCRIPTION_ID>
  tenantID: <TENANT_ID>
  location: <AZURE_REGION_LOCATION>
  serviceLevel: Standard
  networkFeatures: Standard
  capacityPools: <CAPACITY_POOL>
  resourceGroups: <RESOURCE_GROUP>
  netappAccounts: <NETAPP_ACCOUNT>
  virtualNetwork: <VIRTUAL_NETWORK>
  subnet: <SUBNET>
  nasType: nfs
  storage:
    - labels:
        type: encryption
      kerberos: sec=krb5i #can be krb5, krb5i, or krb5p
  credentials:
    name: backend-tbc-anf-secret
```

2. Utilizzare il file di configurazione creato nel passaggio precedente per creare il backend:

```
tridentctl create backend -f <backend-configuration-file>
```

Se la creazione del backend non riesce, si è verificato un errore nella configurazione del backend. È possibile visualizzare i log per determinare la causa eseguendo il seguente comando:

```
tridentctl logs
```

Dopo aver identificato e corretto il problema con il file di configurazione, è possibile eseguire nuovamente il comando create.

Creare una classe di storage

È possibile creare una classe di archiviazione per il provisioning dei volumi con la crittografia Kerberos.

Fasi

1. Creare un oggetto Kubernetes StorageClass, usando il seguente esempio:

```
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
  name: anf-sc-nfs
provisioner: csi.trident.netapp.io
parameters:
  backendType: "azure-netapp-files"
  trident.netapp.io/nasType: "nfs"
  selector: "type=encryption"
```

2. Creare la classe di storage:

```
kubectl create -f sample-input/storage-class-anf-sc-nfs.yaml
```

3. Assicurarsi che la classe di archiviazione sia stata creata:

```
kubectl get sc anf-sc-nfs
```

L'output dovrebbe essere simile a quanto segue:

```
NAME          PROVISIONER              AGE
anf-sc-nfs     csi.trident.netapp.io   15h
```

Provisioning dei volumi

Dopo aver creato un backend di storage e una classe di storage, è ora possibile eseguire il provisioning di un volume. Fare riferimento a queste istruzioni per "provisioning di un volume".

Ripristina i dati dei volumi utilizzando uno snapshot

Astra Control Provivisioner esegue un ripristino rapido e in-place dei volumi da uno snapshot utilizzando `TridentActionSnapshotRestore` (TASR) CR. Questo CR funziona come un'azione imperativa di Kubernetes e non persiste al termine

dell'operazione.

Astra Control provisioner supporta il ripristino delle snapshot su `ontap-san`, `ontap-san-economy`, `ontap-nas`, `ontap-nas-flexgroup`, `azure-netapp-files`, `gcp-cvs`, e. `solidfire-san` driver.

Prima di iniziare

È necessario disporre di un PVC associato e di uno snapshot del volume disponibile.

- Verificare che lo stato del PVC sia limitato.

```
kubectl get pvc
```

- Verificare che lo snapshot del volume sia pronto per l'uso.

```
kubectl get vs
```

Fasi

1. Creare TASR CR. In questo esempio viene creato un CR per PVC `pvc1` e snapshot del volume `pvc1-snapshot`.

```
cat tasr-pvc1-snapshot.yaml

apiVersion: v1
kind: TridentActionSnapshotRestore
metadata:
  name: this-doesnt-matter
  namespace: trident
spec:
  pvcName: pvc1
  volumeSnapshotName: pvc1-snapshot
```

2. Applicare la CR per eseguire il ripristino dall'istantanea. In questo esempio vengono ripristinati gli snapshot `pvc1`.

```
kubectl create -f tasr-pvc1-snapshot.yaml

tridentactionsnapshotrestore.trident.netapp.io/this-doesnt-matter
created
```

Risultati

Astra Control Provivisioner ripristina i dati dalla snapshot. È possibile verificare lo stato di ripristino dello snapshot.

```
kubectl get tasr -o yaml

apiVersion: v1
items:
- apiVersion: trident.netapp.io/v1
  kind: TridentActionSnapshotRestore
  metadata:
    creationTimestamp: "2023-04-14T00:20:33Z"
    generation: 3
    name: this-doesnt-matter
    namespace: trident
    resourceVersion: "3453847"
    uid: <uid>
  spec:
    pvcName: pvc1
    volumeSnapshotName: pvc1-snapshot
  status:
    startTime: "2023-04-14T00:20:34Z"
    completionTime: "2023-04-14T00:20:37Z"
    state: Succeeded
kind: List
metadata:
  resourceVersion: ""
```

- Nella maggior parte dei casi, Astra Control provisioner non ritenta automaticamente l'operazione in caso di guasto. Sarà necessario eseguire nuovamente l'operazione.
- Gli utenti Kubernetes senza accesso amministrativo potrebbero dover essere autorizzati dall'amministratore a creare una TASR CR nel namespace delle applicazioni.

Replica dei volumi con SnapMirror

Con Astra Control Provivisioner, puoi creare relazioni di mirroring tra un volume di origine su un cluster e il volume di destinazione sul cluster in peering per replicare i dati per il disaster recovery. È possibile utilizzare una definizione di risorsa personalizzata (CRD) con nome per eseguire le seguenti operazioni:

- Creare relazioni di mirroring tra volumi (PVC)
- Rimuovere le relazioni di mirroring tra volumi
- Interrompere le relazioni di mirroring
- Promozione del volume secondario in condizioni di disastro (failover)
- Eseguire la transizione senza perdita di dati delle applicazioni da cluster a cluster (durante failover o migrazioni pianificati)

Prerequisiti per la replica

Prima di iniziare, verificare che siano soddisfatti i seguenti prerequisiti:

Cluster ONTAP

- **Astra Control Provisioner**: Astra Control Provisioner versione 23,10 o successiva deve esistere sia sui cluster Kubernetes di origine che di destinazione che utilizzano ONTAP come backend.
- **Licenze**: Le licenze asincrone di ONTAP SnapMirror che utilizzano il bundle di protezione dati devono essere attivate sia sul cluster ONTAP di origine che su quello di destinazione. Fare riferimento a. "Panoramica sulle licenze SnapMirror in ONTAP" per ulteriori informazioni.

Peering

- **Cluster e SVM**: I backend dello storage ONTAP devono essere peering. Fare riferimento a. "Panoramica del peering di cluster e SVM" per ulteriori informazioni.

  > Assicurati che i nomi delle SVM utilizzati nella relazione di replica tra due cluster ONTAP siano univoci.

- **Astra Control Provisioner e SVM**: Le SVM remote in cui è stato eseguito il peering devono essere disponibili per Astra Control Provisioner nel cluster di destinazione.

Driver supportati

- La replica di un volume è supportata per i driver ontap-nas e ontap-san.

Creare un PVC specchiato

Seguire questi passaggi e utilizzare gli esempi CRD per creare una relazione di mirroring tra volumi primari e secondari.

Fasi

1. Eseguire i seguenti passaggi sul cluster Kubernetes primario:
   a. Creare un oggetto StorageClass con `trident.netapp.io/replication: true` parametro.

      Esempio

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        backendType: "ontap-nas"
        fsType: "nfs"
        trident.netapp.io/replication: "true"
      ```

   b. Crea un PVC con StorageClass creato in precedenza.

Esempio

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
spec:
  accessModes:
  - ReadWriteMany
  resources:
    requests:
      storage: 1Gi
  storageClassName: csi-nas
```

c. Creare una CR MirrorRelationship con informazioni locali.

Esempio

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
```

Astra Control Provivisioner recupera le informazioni interne del volume e dello stato attuale di data Protection (DP) del volume, quindi popola il campo di stato di MirrorRelationship.

d. Procurarsi il TridentMirrorRelationship CR per ottenere il nome interno e la SVM del PVC.

```
kubectl get tmr csi-nas
```

```
kind: TridentMirrorRelationship
apiVersion: trident.netapp.io/v1
metadata:
  name: csi-nas
  generation: 1
spec:
  state: promoted
  volumeMappings:
  - localPVCName: csi-nas
status:
  conditions:
  - state: promoted
    localVolumeHandle:
"datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
    localPVCName: csi-nas
    observedGeneration: 1
```

2. Eseguire i seguenti passaggi sul cluster Kubernetes secondario:
   a. Creare una classe StorageClass con il parametro trident.netapp.io/replication: true.

      Esempio

      ```
      apiVersion: storage.k8s.io/v1
      kind: StorageClass
      metadata:
        name: csi-nas
      provisioner: csi.trident.netapp.io
      parameters:
        trident.netapp.io/replication: true
      ```

   b. Creare una CR MirrorRelationship con informazioni sulla destinazione e sulla sorgente.

      Esempio

      ```
      kind: TridentMirrorRelationship
      apiVersion: trident.netapp.io/v1
      metadata:
        name: csi-nas
      spec:
        state: established
        volumeMappings:
        - localPVCName: csi-nas
          remoteVolumeHandle:
      "datavserver:trident_pvc_3bedd23c_46a8_4384_b12b_3c38b313c1e1"
      ```

Astra Control Provisioner creerà una relazione SnapMirror con il nome della policy di relazione configurata (o default per ONTAP) e la inizializzerà.

c. Crea un PVC con StorageClass creato in precedenza per agire come secondario (destinazione SnapMirror).

Esempio

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: csi-nas
  annotations:
    trident.netapp.io/mirrorRelationship: csi-nas
spec:
  accessModes:
  - ReadWriteMany
resources:
  requests:
    storage: 1Gi
storageClassName: csi-nas
```

Astra Control Provisioner controllerà la CRD TridentMirrorRelationship e non creerà il volume se la relazione non esiste. Se esiste una relazione, Astra Control Provisioner garantirà che il nuovo volume FlexVol venga inserito in una SVM a cui viene inviata la SVM remota definita in MirrorRelationship.

Stati di replica dei volumi

Una relazione mirror Trident (TMR) è un CRD che rappresenta un'estremità di una relazione di replica tra PVC. Il TMR di destinazione ha uno stato, che indica ad Astra Control Provisioner lo stato desiderato. Il TMR di destinazione ha i seguenti stati:

- **Stabilito**: Il PVC locale è il volume di destinazione di una relazione speculare, e questa è una nuova relazione.
- **Promosso**: Il PVC locale è ReadWrite e montabile, senza alcuna relazione speculare attualmente in vigore.
- **Ristabilito**: Il PVC locale è il volume di destinazione di una relazione speculare ed era anche precedentemente in quella relazione speculare.
  - Lo stato ristabilito deve essere utilizzato se il volume di destinazione era in una relazione con il volume di origine perché sovrascrive il contenuto del volume di destinazione.
  - Se il volume non era precedentemente in relazione con l'origine, lo stato ristabilito non riuscirà.

Promozione del PVC secondario durante un failover non pianificato

Eseguire il seguente passaggio sul cluster Kubernetes secondario:

- Aggiornare il campo *spec.state* di TridentMirrorRelationship su `promoted`.

Promozione del PVC secondario durante un failover pianificato

Durante un failover pianificato (migrazione), eseguire le seguenti operazioni per promuovere il PVC secondario:

Fasi

1. Sul cluster Kubernetes primario, creare una snapshot del PVC e attendere la creazione dello snapshot.
2. Sul cluster Kubernetes primario, creare SnapshotInfo CR per ottenere dettagli interni.

   Esempio

   ```
   kind: SnapshotInfo
   apiVersion: trident.netapp.io/v1
   metadata:
     name: csi-nas
   spec:
     snapshot-name: csi-nas-snapshot
   ```

3. Nel cluster Kubernetes secondario, aggiornare il campo *spec.state* del *TridentMirrorRelationship* CR a *Promoted* e *spec.promotedSnapshotHandle* come nome interno dello snapshot.
4. Sul cluster Kubernetes secondario, confermare lo stato (campo status.state) di TridentMirrorRelationship a promosso.

Ripristinare una relazione di mirroring dopo un failover

Prima di ripristinare una relazione di specchiatura, scegliere il lato che si desidera creare come nuovo primario.

Fasi

1. Nel cluster Kubernetes secondario, verificare che i valori per il campo *spec.remoteVolumeHandle* in TridentMirrorRelationship siano aggiornati.
2. Sul cluster Kubernetes secondario, aggiornare il campo *spec.mirror* di TridentMirrorRelationship a. `reestablished`.

Operazioni supplementari

Astra Control Provivisioner supporta le seguenti operazioni sui volumi primario e secondario:

Replicare il PVC primario in un nuovo PVC secondario

Assicurarsi di disporre già di un PVC primario e di un PVC secondario.

Fasi

1. Eliminare i CRD PersistentVolumeClaim e TridentMirrorRelationship dal cluster (destinazione) secondario stabilito.
2. Eliminare il CRD TridentMirrorRelationship dal cluster primario (origine).
3. Creare un nuovo CRD TridentMirrorRelationship nel cluster primario (di origine) per il nuovo PVC secondario (di destinazione) che si desidera stabilire.

Ridimensionare un PVC specchiato, primario o secondario

Il PVC può essere ridimensionato normalmente, ONTAP espanderà automaticamente qualsiasi flevxols di destinazione se la quantità di dati supera le dimensioni correnti.

Rimuovere la replica da un PVC

Per rimuovere la replica, eseguire una delle seguenti operazioni sul volume secondario corrente:

- Eliminare MirrorRelationship sul PVC secondario. Questo interrompe la relazione di replica.
- In alternativa, aggiornare il campo spec.state a *Promoted*.

Eliminazione di un PVC (precedentemente specchiato)

Astra Control Provivisioner verifica la presenza di PVC replicati e rilascia la relazione di replica prima di tentare di eliminare il volume.

Eliminare una TMR

L'eliminazione di una TMR su un lato di una relazione specchiata fa sì che la TMR rimanente passi allo stato *promosso* prima che Astra Control Provivisioner completi l'eliminazione. Se il TMR selezionato per l'eliminazione è già nello stato *promosso*, non esiste alcuna relazione di mirror esistente e il TMR verrà rimosso e Astra Control Provisioner promuoverà il PVC locale in *ReadWrite*. Questa eliminazione rilascia i metadati SnapMirror per il volume locale in ONTAP. Se in futuro questo volume viene utilizzato in una relazione di mirroring, deve utilizzare un nuovo TMR con uno stato di replica del volume *stabilito* quando si crea la nuova relazione di mirroring.

Aggiorna relazioni mirror quando ONTAP è online

Le relazioni speculari possono essere aggiornate in qualsiasi momento dopo che sono state stabilite. È possibile utilizzare `state: promoted` oppure `state: reestablished` per aggiornare le relazioni. Quando si trasferisce un volume di destinazione a un volume ReadWrite regolare, è possibile utilizzare *PromotedSnapshotHandle* per specificare uno snapshot specifico su cui ripristinare il volume corrente.

Aggiorna relazioni di mirroring quando ONTAP non è in linea

Puoi utilizzare un CRD per eseguire un update di SnapMirror senza che Astra Control disponga di connettività diretta al cluster ONTAP. Fare riferimento al seguente formato di esempio di TridentActionMirrorUpdate:

Esempio

```
apiVersion: trident.netapp.io/v1
kind: TridentActionMirrorUpdate
metadata:
  name: update-mirror-b
spec:
  snapshotHandle: "pvc-1234/snapshot-1234"
  tridentMirrorRelationshipName: mirror-b
```

`status.state` Riflette lo stato del CRD TridentActionMirrorUpdate. Può assumere un valore da *riuscito*, *in corso* o *non riuscito*.

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 saperne di più, "Consultare i documenti di automazione Astra".

Conoscenza e supporto

Registrati per ricevere assistenza

Astra Control tenta di registrare automaticamente il tuo account per il supporto quando configuri il tuo account. In caso contrario, puoi registrarti manualmente per ricevere assistenza. Per ottenere assistenza dal supporto tecnico NetApp, è necessaria la registrazione del supporto.

Verificare la registrazione del supporto

Astra Control include un campo Support Status (Stato supporto) che consente di confermare la registrazione al supporto.

Fasi

1. Selezionare **supporto**.
2. Date un'occhiata al campo Support Status (Stato supporto).

   Il Support Status (Stato supporto) inizia come "Not Registered" (non registrato), ma passa a "in corso" e infine a "Registered" (registrato) una volta completato il processo.

   Questo stato di registrazione del supporto viene interrogato ogni 15 minuti. I nuovi clienti NetApp potrebbero richiedere fino al giorno di lavoro successivo per completare l'onboarding e la registrazione del supporto. Se il numero di serie non viene visualizzato come "registrato" entro 48 ore, puoi contattare NetApp utilizzando astra.feedback@netapp.com o registrarti manualmente all'indirizzo https://register.netapp.com.

Ottenere il numero di serie

Quando ti registri a un account, Astra Control utilizza le informazioni fornite sulla tua azienda per generare un numero di serie NetApp a 20 cifre che inizia con "941".

Il numero di serie di NetApp rappresenta l'account Astra Control. Quando si apre un ticket Web, è necessario utilizzare questo numero di serie.

Il numero di serie è disponibile nell'interfaccia Astra Control della pagina **Support**.

Attivare i diritti di supporto

Se Astra Control non è riuscito a registrare automaticamente il tuo account per il supporto, devi registrare il numero di serie NetApp associato ad Astra Control per attivare il supporto. Offriamo 2 opzioni per la registrazione del supporto:

1. Attuale cliente NetApp con account SSO NetApp Support Site (NSS) esistente
2. Nuovo cliente NetApp senza account SSO NetApp Support Site (NSS) esistente

Opzione 1: Cliente NetApp attuale con un account NetApp Support Site (NSS) esistente

Fasi

1. Passare a. "Registrazione del supporto Cloud Data Services" pagina.

2. Selezionare **sono già registrato come cliente NetApp**.
3. Immettere le credenziali del NetApp Support Site per accedere.

   Viene visualizzata la pagina registrazione cliente esistente.

4. Completare le informazioni richieste nel modulo:
   a. Immettere il nome, la società e l'indirizzo e-mail.
   b. Selezionare **Astra Control Service** come linea di prodotti.
   c. Selezionare un provider di fatturazione.
   d. Inserire il numero di serie.
   e. Selezionare **Invia**.

Risultato

Dovresti essere reindirizzato a una pagina "Registration Submitted Successfully" (registrazione inviata correttamente). L'indirizzo e-mail associato alla registrazione riceverà un'e-mail entro un paio di minuti in cui viene indicato che il prodotto è ora idoneo per il supporto.

Si tratta di una registrazione del supporto una tantum per il numero di serie applicabile.

Opzione 2: Nuovo cliente NetApp senza account NetApp Support Site (NSS) esistente

Fasi

1. Passare a. "Registrazione del supporto Cloud Data Services" pagina.
2. Selezionare **non sono un cliente NetApp registrato**.

   Viene visualizzata la pagina New Customer Registration (registrazione nuovo cliente).

3. Completare le informazioni richieste nel modulo:

   a. Immettere il proprio nome, le informazioni sulla società e i dettagli di contatto.
   b. Selezionare **Astra Control Service** come linea di prodotti.
   c. Selezionare un provider di fatturazione.
   d. Inserire il numero di serie.
   e. Immettere il valore captcha.
   f. Selezionare la casella di controllo per confermare di aver letto l'informativa sulla privacy di NetApp.
   g. Selezionare **Invia**.

      Riceverai un'e-mail di conferma dalla registrazione inviata. Se non si verificano errori, verrà visualizzata nuovamente la pagina "registrazione inviata correttamente". Riceverai anche un'e-mail entro un'ora in cui viene indicato che "il tuo prodotto è ora idoneo per il supporto".

   Si tratta di una registrazione del supporto una tantum per il numero di serie applicabile.

4. In qualità di nuovo cliente NetApp, devi anche creare un account utente del NetApp Support Site (NSS) per attivazioni future del supporto e per accedere al portale di supporto per la chat del supporto tecnico e il web ticketing.

   Accedere alla "Sito NetApp Support Registration" per eseguire questa attività. Per accelerare il processo, è possibile fornire il numero di serie di Astra Control appena registrato.

Risoluzione dei problemi

Scopri come risolvere alcuni problemi comuni che potresti incontrare.

https://kb.netapp.com/Cloud/Astra/Control

Per ulteriori informazioni

- "Risoluzione dei problemi"

Richiedi assistenza

NetApp fornisce supporto per Astra Control in diversi modi. Sono disponibili numerose opzioni di supporto self-service gratuite 24 ore su 24, 7 giorni su 7, come articoli della knowledge base (KB) e un canale di discording. Il tuo account Astra Control include il supporto tecnico remoto via web ticketing.

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 selezionando la scheda **Support** (supporto) dal menu principale.

Supporto autonomo

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

- "Knowledge base"

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

- Documentazione

  Questo è il sito doc attualmente visualizzato.

- "Ricevi assistenza tramite discordia"

  Vai ad Astra nella categoria Pub per entrare in contatto con colleghi ed esperti.

- 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.

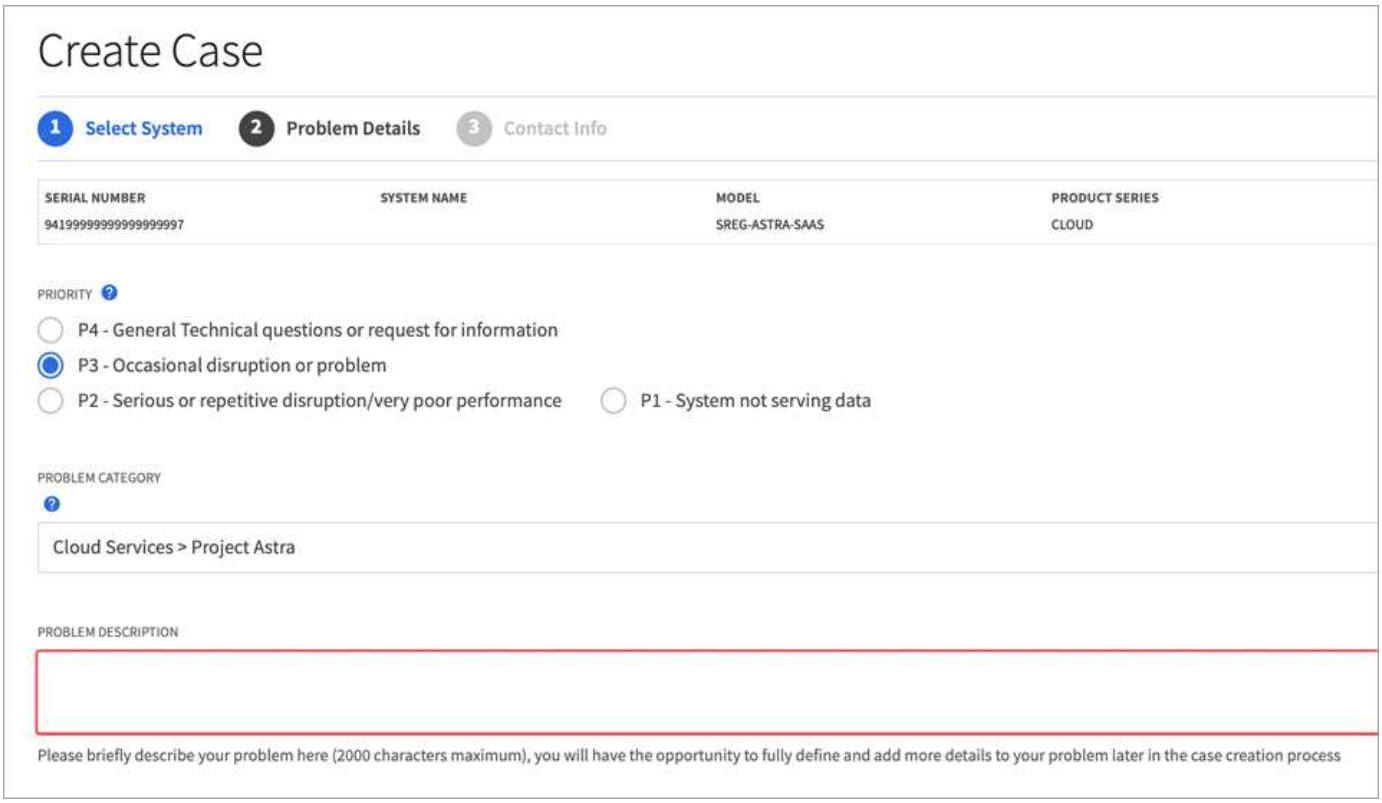
Supporto in abbonamento

Oltre alle opzioni di supporto autonomo sopra descritte, puoi collaborare con un Support Engineer di NetApp per risolvere eventuali problemi successivi "Attivare il supporto per il numero di serie NetApp".

Una volta attivato il numero di serie di Astra Control, è possibile accedere alle risorse di supporto tecnico di NetApp creando un "Ticket di supporto".

Selezionare **Cloud Data Services > Astra**.

Utilizzare il numero di serie "941" per aprire il ticket Web. "Scopri di più sul numero di serie".



Domande frequenti

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

Panoramica

Astra Control punta a semplificare le operazioni di Lifecycle management dei dati delle applicazioni per le applicazioni native di Kubernetes. Astra Control Service supporta i cluster Kubernetes in esecuzione su più ambienti cloud provider.

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

Accesso ad Astra Control

Perché devo fornire tanti dettagli quando mi registri ad Astra Control?

Astra Control richiede informazioni accurate sui clienti al momento della registrazione. Queste informazioni sono necessarie per eseguire un controllo GTC (Global Trade Compliance).

Perché viene visualizzato un errore di registrazione non riuscita quando si esegue la registrazione a Astra Control?

Astra Control richiede di fornire informazioni accurate sui clienti nella sezione di assunzione. Se sono state fornite informazioni non corrette, viene visualizzato il messaggio di errore "Registration Failed" (registrazione non riuscita). Anche gli altri account di cui sei membro vengono bloccati.

Che cos'è l'URL di Astra Control Service?

È possibile accedere a Astra Control Service all'indirizzo https://astra.netapp.io.

Ho inviato un invito tramite e-mail a un collega, ma non l'ho ricevuto. Cosa devo fare?

Chiedi loro di controllare la cartella spam per un'e-mail da do-not-reply@netapp.com o di cercare nella loro casella di posta "invito". È inoltre possibile rimuovere l'utente e tentare di aggiungerlo nuovamente.

Ho effettuato l'upgrade al Premium PayGo Plan dal Free Plan. Mi verrà addebitato il costo dei primi 10 spazi dei nomi?

Sì. Dopo l'aggiornamento al Premium Plan, Astra Control inizia a addebitare tutti gli spazi dei nomi gestiti nel tuo account.

Ho effettuato l'upgrade al Premium PayGo Plan a metà mese. Mi verrà addebitato l'intero mese?

No La fatturazione inizia dal momento dell'aggiornamento al piano Premium.

Sto utilizzando il piano gratuito, mi verrà addebitato il costo delle richieste di rimborso persistenti?

Sì, otterrai dei costi per i volumi persistenti utilizzati dai cluster dal tuo cloud provider.

Registrazione dei cluster Kubernetes

Devo installare i driver CSI sul mio cluster prima di aggiungerlo a Astra Control Service?

No Quando il cluster viene aggiunto a Astra Control, il servizio installa automaticamente il driver Astra Trident Container Storage Interface (CSI) sul cluster Kubernetes. Questo driver CSI viene utilizzato per eseguire il provisioning di volumi persistenti per i cluster supportati dal provider cloud.

Devo aggiungere nodi di lavoro al mio cluster in seguito all'aggiunta di Astra Control Service. Cosa devo fare?

È possibile aggiungere nuovi nodi di lavoro ai pool esistenti oppure creare nuovi pool fintanto che sono `COS_CONTAINERD` tipo di immagine. 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.

Registrazione dei cluster EKS (Elastic Kubernetes Service)

Posso aggiungere un cluster EKS privato ad Astra Control Service?

Sì, puoi aggiungere cluster EKS privati ad Astra Control Service. Per aggiungere un cluster EKS privato, fare riferimento a. "Inizia a gestire i cluster Kubernetes da Astra Control Service".

Registrazione dei cluster Azure Kubernetes Service (AKS)

Posso aggiungere un cluster AKS privato ad Astra Control Service?

Sì, puoi aggiungere cluster AKS privati ad Astra Control Service. Per aggiungere un cluster AKS privato, fare riferimento a. "Inizia a gestire i cluster Kubernetes da Astra Control Service".

Posso utilizzare Active Directory per gestire l'autenticazione per i miei cluster AKS?

Sì, è possibile configurare i cluster AKS in modo che utilizzino Azure Active Directory (Azure ad) per l'autenticazione e la gestione delle identità. Quando si crea il cluster, seguire le istruzioni in "documentazione ufficiale" Per configurare il cluster per l'utilizzo di Azure ad. È necessario assicurarsi che i cluster soddisfino i requisiti per l'integrazione di Azure ad gestita da AKS.

Registrazione dei cluster Google Kubernetes Engine (GKE)

Posso aggiungere un cluster GKE privato ad Astra Control Service?

Sì, è possibile aggiungere cluster GKE privati a Astra Control Service. Per aggiungere un cluster GKE privato, fare riferimento a. "Inizia a gestire i cluster Kubernetes da Astra Control Service".

I cluster GKE privati devono disporre di "reti autorizzate" Impostare per consentire l'indirizzo IP di Astra Control:

52.188.218.166/32

Il mio cluster GKE può risiedere su un VPC condiviso?

Sì. Astra Control è in grado di gestire i cluster che risiedono in un VPC condiviso. "Scopri come configurare l'account di servizio Astra per una configurazione VPC condivisa".

Dove posso trovare le mie credenziali dell'account di servizio su GCP?

Dopo aver effettuato l'accesso a "Console Google Cloud", I dettagli dell'account di servizio si trovano nella sezione **IAM e Admin**. Per ulteriori informazioni, fare riferimento a. "Come configurare Google Cloud per Astra Control".

Vorrei aggiungere cluster GKE diversi da diversi progetti GCP. È supportato in Astra Control?

No, questa non è una configurazione supportata. È supportato solo un singolo progetto GCP.

Rimozione dei cluster

Come posso annullare la registrazione, arrestare un cluster ed eliminare i volumi associati in maniera corretta?

1. "Annulla la gestione delle applicazioni da Astra Control".
2. "Annullare la registrazione del cluster da Astra Control".
3. "Eliminare le richieste di rimborso del volume persistente".
4. Eliminare il cluster.

Cosa accade alle applicazioni e ai dati dopo aver rimosso il cluster 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 dati di snapshot del volume memorizzati nel backend dello storage non verranno rimossi. I backup persistenti dello storage creati da Astra Control resteranno nell'archivio di oggetti del provider di cloud, ma non saranno disponibili per il ripristino.

> Rimuovere sempre un cluster da Astra Control prima di eliminarlo tramite GCP. L'eliminazione di un cluster da GCP mentre è ancora gestito da Astra Control può causare problemi all'account Astra Control.

Astra Control Provivisioner viene disinstallato automaticamente da un cluster quando lo disgestisco?

Quando annulli la gestione di un cluster da Astra Control Center, Astra Control Provivisioner o Astra Trident non viene disinstallato automaticamente dal cluster. Per disinstallare Astra Control provisioner e i suoi componenti o Astra Trident, devi farlo "Segui questa procedura per disinstallare l'istanza di Astra Trident che contiene il servizio Astra Control provisioner".

Gestione delle applicazioni

Astra Control è in grado di implementare un'applicazione?

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

Non vedo alcun PVC della mia applicazione legato a CVS GCP. Cosa c'è di sbagliato?

L'operatore Astra Trident imposta la classe di storage predefinita su `netapp-cvs-perf-premium` Una volta aggiunto correttamente ad Astra Control. Quando i PVC di un'applicazione non sono vincolati a Cloud Volumes Service per Google Cloud, è possibile eseguire alcuni passaggi:

- Eseguire `kubectl get sc` e selezionare la classe di storage predefinita.
- Controllare il file yaml o il grafico Helm utilizzato per implementare l'applicazione e verificare se è stata definita una classe di storage diversa.
- GKE versione 1.24 e successive non supporta le immagini di nodi basate su Docker. Verificare che il tipo di immagine del nodo di lavoro in GKE sia `COS_CONTAINERD` E che il montaggio NFS è riuscito.

Cosa accade alle applicazioni dopo che ho smesso di gestirle 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.

Operazioni di gestione dei dati

Dove viene creato il bucket degli archivi di oggetti con Astra Control?

La geografia del primo cluster gestito determina la posizione dell'archivio di oggetti. Ad esempio, se il primo cluster aggiunto si trova in una zona europea, il bucket viene creato nella stessa area geografica. Se necessario, è possibile "aggiungere bucket aggiuntivi".

Ci sono istantanee nel mio account che non ho creato. Da dove sono venuti?

In alcune situazioni, Astra Control crea automaticamente uno snapshot come parte dell'esecuzione di un altro processo. Se queste istantanee sono più vecchie di pochi minuti, è possibile eliminarle in modo sicuro.

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

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

Posso gestire le snapshot scattate da Astra Control direttamente attraverso il mio cloud provider?

No Snapshot e backup creati da Astra Control possono essere gestiti solo con Astra Control.

Astra Control provisioner

In che modo le funzionalità di provisioning dello storage di Astra Control Provivisioner sono diverse da quelle di Astra Trident?

Astra Control Provivisioner, in qualità di parte di Astra Control, supporta un superset di funzionalità di provisioning dello storage che non sono disponibili in Astra Trident, open-source. Queste funzionalità si aggiungono a tutte le funzionalità disponibili per Trident open-source.

Astra Control Provivisioner sostituisce Astra Trident?

Astra Control Provisioner ha sostituito Astra Trident come provisioner di storage e orchestrator nell'architettura Astra Control. Gli utenti di Astra Control devono farlo "Abilita Astra Control Provisioner" Per utilizzare Astra Control. Astra Trident continuerà a essere supportato in questa release, ma non sarà supportato nelle release future. Astra Trident rimarrà open source e verrà rilasciato, mantenuto, supportato e aggiornato con nuove CSI e altre funzionalità di NetApp. Tuttavia, solo Astra Control Provisioner, che contiene la funzionalità Astra Trident CSI e le capacità estese di gestione dello storage, possono essere utilizzati nelle prossime release di Astra Control.

Devo pagare per Astra Trident?

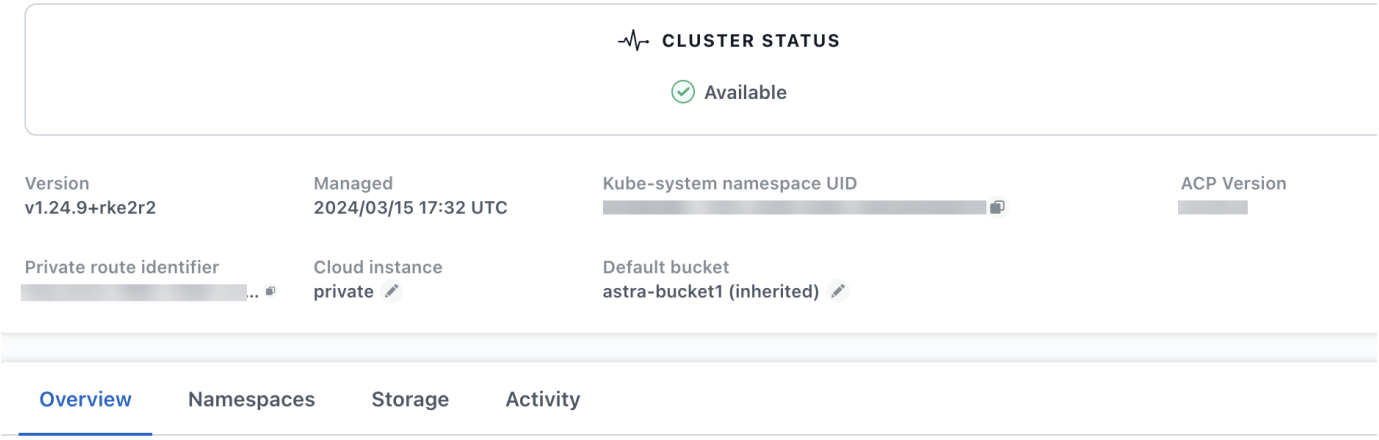
No Astra Trident continuerà a essere open source e scaricabile gratuitamente. L'utilizzo della funzionalità di Astra Control provisioner richiede ora una licenza Astra Control.

Posso utilizzare le funzionalità di gestione e provisioning dello storage di Astra Control senza installare e utilizzare tutto Astra Control?

Sì, puoi eseguire l'aggiornamento a Astra Control Provisioner e utilizzarne le funzionalità anche se non vuoi utilizzare il set completo di funzionalità di gestione dei dati di Astra Control.

Come faccio a sapere se Astra Control Provivisioner ha sostituito Astra Trident nel mio cluster?

Dopo l'installazione di Astra Control Provisioner, il cluster host nell'interfaccia utente di Astra Control mostrerà un `ACP version` piuttosto che `Trident version` campo e numero della versione installata corrente.



Se non si dispone dell’accesso all’interfaccia utente, è possibile confermare la corretta installazione utilizzando i seguenti metodi:

Operatore Astra Trident

Verificare `trident-acp` il container è in esecuzione e così `acpVersion` è `23.10.0` o versione successiva con stato di `Installed`:

```
kubectl get torc -o yaml
```

Risposta:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <my_custom_registry>/trident-acp:v23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

Confermare che Astra Control Provisioner è stato abilitato:

```
./tridentctl -n trident version
```

Risposta:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

"Avviso per Astra"

Licenza API Astra Control

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