Utilizzare Astra

Astra Control Center

NetApp
November 21, 2023

Sommario

Utilizzare Astra

Inizia a gestire le app

Dopo di lei "Aggiungere un cluster alla gestione di Astra Control", È possibile installare le applicazioni sul cluster (al di fuori di Astra Control) e quindi andare alla pagina delle applicazioni in Astra Control per iniziare a gestire le applicazioni e le relative risorse.

Per ulteriori informazioni, vedere "Requisiti di gestione delle applicazioni".

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 ambito per un singolo namespace.

Gestire 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 "gestire un intero namespace come singola applicazione o gestire una o più applicazioni nello spazio dei nomi singolarmente". 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), la procedura migliore è scegliere uno o l'altro. Le azioni eseguite in Astra Control possono non riuscire se vengono eseguite contemporaneamente sia a livello di spazio dei nomi che di applicazione.

> 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.

Di cosa hai bisogno

- Un cluster Kubernetes aggiunto ad Astra Control.
- Una o più applicazioni installate sul cluster. Scopri di più sui metodi di installazione delle app supportati.
- Uno o più pod attivi.
- Gli spazi dei nomi specificati nel cluster Kubernetes aggiunto ad Astra Control.
- (Facoltativo) 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, "Consulta la documentazione ufficiale di Kubernetes".

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

Per istruzioni su come gestire le applicazioni utilizzando l'API Astra Control, vedere "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

Ulteriori opzioni di gestione delle applicazioni

- Annulla gestione delle applicazioni

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 sulle Best practice.

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 lo spazio dei nomi dell'applicazione dall'elenco a discesa **namespace**.

   > Le applicazioni possono essere definite solo all'interno di uno spazio dei nomi specifico su un singolo cluster. Astra Control non supporta la possibilità per le applicazioni di estendere più spazi dei nomi o cluster.

5. Immettere un'etichetta per l'applicazione e lo spazio dei nomi. È possibile specificare un'etichetta singola o criteri di selezione delle etichette (query).

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

6. Dopo aver selezionato **define**, ripetere la procedura per altre applicazioni, in base alle necessità.

Al termine della definizione di un'applicazione, questa viene visualizzata 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.

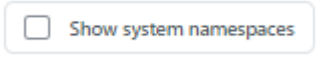
Definire uno spazio dei nomi da gestire come applicazione

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 si intende gestire e proteggere tutte le risorse in un determinato namespace in modo simile e a 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 gestire più spazi dei nomi, selezionare gli spazi dei nomi, quindi fare clic sul pulsante **azioni** nell'angolo in alto a sinistra e selezionare **Gestisci**.

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.

Annulla gestione delle applicazioni

Quando non si desidera più eseguire il backup, lo snapshot o la clonazione di un'applicazione, è possibile interromperne la gestione.

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

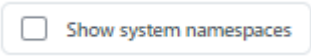
Fasi

1. Dalla barra di navigazione a sinistra, selezionare **applicazioni**.
2. Selezionare l'applicazione.
3. Dal menu nella colonna **azioni**, selezionare **Annulla gestione**.
4. Esaminare le informazioni.
5. Digitare "unManage" per confermare.
6. Selezionare **Sì, Annulla gestione applicazione**.

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.

Esempio: Policy di protezione separata per release diverse

In questo esempio, il team devops sta gestendo un'implementazione di release "canary". Il cluster del team dispone di tre pod che eseguono nginx. Due dei pod sono dedicati al rilascio stabile. Il terzo pod è per la release canary.

L'amministratore Kubernetes del team devops aggiunge l'etichetta `deployment=stable` ai pod a rilascio stabile. Il team aggiunge l'etichetta `deployment=canary` al pod di rilascio canary.

La release stabile del team include un requisito per snapshot orarie e backup giornalieri. La release canary è più effimera, quindi vogliono creare una politica di protezione meno aggressiva e a breve termine per qualsiasi cosa etichettata `deployment=canary`.

Per evitare possibili conflitti di dati, l'amministratore creerà due applicazioni: Una per la release "canary" e una per la release "stable". In questo modo i backup, gli snapshot e le operazioni di clonazione vengono separati per i due gruppi di oggetti Kubernetes.

Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"

Proteggi le app

Panoramica della protezione

Con Astra Control Center puoi creare backup, cloni, snapshot e policy di protezione per le tue applicazioni. Il backup delle tue applicazioni aiuta i tuoi servizi e i dati associati a essere il più possibile disponibili; durante uno scenario di disastro, il ripristino dal backup può garantire il ripristino completo di un'applicazione e dei dati associati con interruzioni minime. Backup, cloni e snapshot possono contribuire a proteggere da minacce comuni come ransomware, perdita accidentale di dati e disastri ambientali. "Scopri i tipi di protezione dei dati disponibili in Astra Control Center e quando utilizzarli".

Inoltre, è possibile replicare le applicazioni in un cluster remoto in preparazione del disaster recovery.

Workflow di protezione delle app

Puoi utilizzare il seguente flusso di lavoro di esempio per iniziare a proteggere le tue applicazioni.

[Uno] Proteggi tutte le app

Per garantire la protezione immediata delle applicazioni, "creare un backup manuale di tutte le applicazioni".

[Due] Configurare una policy di protezione per ogni applicazione

Per automatizzare backup e snapshot futuri, "configurare una policy di protezione per ogni applicazione". Ad esempio, è possibile iniziare con backup settimanali e snapshot giornalieri, con un mese di conservazione per entrambi. Si consiglia vivamente di automatizzare backup e snapshot con una policy di protezione rispetto a backup e snapshot manuali.

[Tre] Modificare i criteri di protezione

Man mano che le applicazioni e i loro modelli di utilizzo cambiano, regola le policy di protezione in base alle necessità per fornire la migliore protezione.

[Quattro] Replica delle applicazioni su un cluster remoto

"Replicare le applicazioni" A un cluster remoto utilizzando la tecnologia NetApp SnapMirror. Astra Control replica le snapshot su un cluster remoto, offrendo funzionalità di disaster recovery asincrone.

[Cinque] In caso di disastro, ripristinate le applicazioni con il backup o la replica più recente sul sistema remoto

In caso di perdita di dati, è possibile eseguire il ripristino "ripristino del backup più recente" primo per ogni applicazione. È quindi possibile ripristinare l'ultimo snapshot (se disponibile). In alternativa, è possibile utilizzare la replica su un sistema remoto.

Proteggi le app con snapshot e backup

Proteggi tutte le app 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.

Se utilizzi Helm per implementare le app, Astra Control Center richiede Helm versione 3. La gestione e la clonazione delle applicazioni implementate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. Le app implementate con Helm 2 non sono supportate.

Quando crei un progetto per ospitare un'applicazione su un cluster OpenShift, al progetto (o namespace Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

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

- Configurare un criterio di protezione
- Creare un'istantanea
- Creare un backup
- Visualizzare snapshot e backup
- Eliminare le istantanee
- Annullare i backup
- Eliminare i backup

Configurare un criterio di protezione

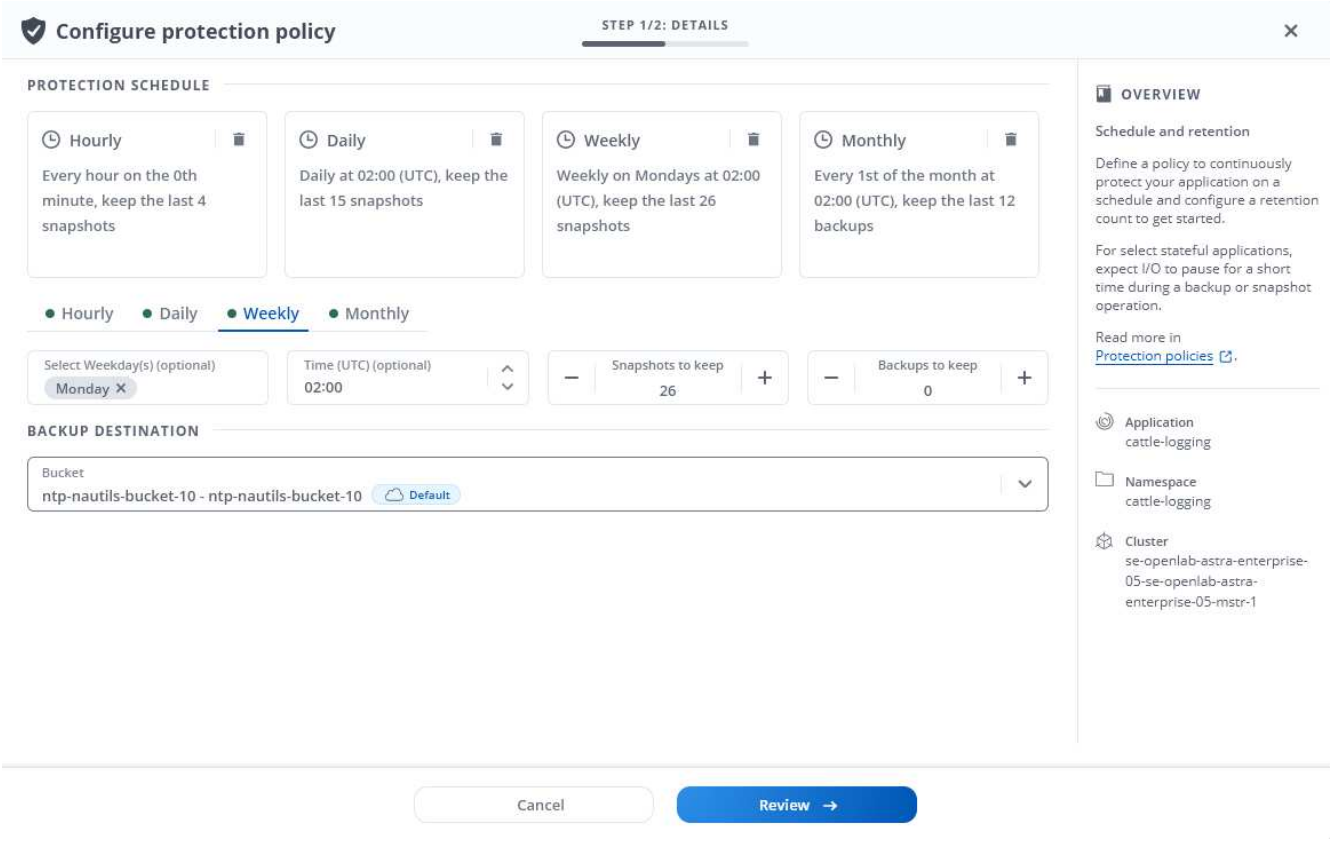
Una policy di protezione protegge un'applicazione creando snapshot, backup o entrambi in base a una pianificazione definita. È possibile scegliere di creare snapshot e backup ogni ora, ogni giorno, ogni settimana e ogni mese, nonché specificare il numero di copie da conservare. Ad esempio, una policy di protezione potrebbe creare backup settimanali e snapshot giornalieri e conservare backup e snapshot per un mese. La frequenza con cui vengono creati snapshot e backup e la durata della conservazione dipendono dalle esigenze dell'organizzazione.

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 un programma di protezione scegliendo il numero di snapshot e backup da conservare ogni ora, ogni giorno, ogni settimana e ogni mese.

È possibile definire le pianificazioni orarie, giornaliere, settimanali e mensili contemporaneamente. Un programma non diventa attivo fino a quando non viene impostato un livello di conservazione.

Nell'esempio seguente vengono impostati quattro programmi di protezione: ogni ora, ogni giorno, ogni settimana e ogni mese per snapshot e backup.



5. Selezionare **Revisione**.
6. Selezionare **Imposta policy di protezione.**

Risultato

Astra Control Center implementa la policy di protezione dei dati creando e conservando snapshot e backup utilizzando i criteri di pianificazione e conservazione definiti dall'utente.

Creare un'istantanea

Puoi creare uno snapshot on-demand in qualsiasi momento.

Fasi

1. Selezionare **applicazioni**.
2. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) dell'applicazione desiderata, selezionare **Snapshot**.
3. Personalizzare il nome dell'istantanea, quindi selezionare **Review** (Rivedi).
4. Esaminare il riepilogo dell'istantanea e selezionare **Snapshot**.

Risultato

Viene avviato il processo di snapshot. Un'istantanea viene eseguita correttamente quando lo stato è **Available** nella colonna **Actions** nella pagina **Data Protection** > **Snapshots**.

Creare un backup

Puoi anche eseguire il backup di un'applicazione in qualsiasi momento.

> I bucket S3 in Astra Control Center non riportano la capacità disponibile. Prima di eseguire il backup o la clonazione delle applicazioni gestite da Astra Control Center, controllare le informazioni del bucket nel sistema di gestione ONTAP o StorageGRID.

Fasi

1. Selezionare **applicazioni**.
2. Dal menu Options (Opzioni) nella colonna **Actions** (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 una destinazione per il backup selezionandola dall'elenco dei bucket di storage.
6. Selezionare **Revisione**.
7. Esaminare il riepilogo del backup e selezionare **Backup**.

Risultato

Astra Control Center crea un backup dell'applicazione.

> Se la rete presenta un'interruzione o è eccessivamente lenta, potrebbe verificarsi un timeout dell'operazione di backup. In questo modo, il backup non viene eseguito correttamente.

> Non esiste alcun modo per interrompere un backup in esecuzione. Se è necessario eliminare il backup, attendere che sia stato completato, quindi seguire le istruzioni riportate in Eliminare i backup. Per eliminare un backup non riuscito, "Utilizzare l'API di controllo Astra".

> Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

Visualizzare snapshot e backup

È possibile visualizzare le istantanee e i backup di un'applicazione dalla scheda Data Protection (protezione dati).

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).

   Le istantanee vengono visualizzate per impostazione predefinita.

3. Selezionare **Backup** per visualizzare l'elenco dei backup.

Eliminare le istantanee

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

> Non è possibile eliminare una copia Snapshot attualmente in corso di replica.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
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 Center elimina lo snapshot.

Annullare i backup

È possibile annullare un backup in corso.

> Per annullare un backup, il backup deve essere in esecuzione. Non è possibile annullare un backup che si trova in uno stato Pending (in sospeso).

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 "Annulla" per confermare l'eliminazione, quindi selezionare **Sì, Annulla backup**.

Eliminare i backup

Eliminare i backup pianificati o on-demand non più necessari.

> Non esiste alcun modo per interrompere un backup in esecuzione. Se è necessario eliminare il backup, attendere che sia stato completato, quindi seguire queste istruzioni. Per eliminare un backup non riuscito, "Utilizzare l'API di controllo Astra".

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 Center elimina il backup.

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.

A proposito di questa attività

- Si consiglia vivamente di eseguire un'istantanea o un backup dell'applicazione prima di ripristinarla. In questo modo, è possibile clonare lo snapshot o il backup nel caso in cui il ripristino non abbia esito positivo.
- Se utilizzi Helm per implementare le app, Astra Control Center richiede Helm versione 3. La gestione e la clonazione delle applicazioni implementate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. Le app implementate con Helm 2 non sono supportate.
- Se si esegue il ripristino in un cluster diverso, assicurarsi che il cluster utilizzi la stessa modalità di accesso al volume persistente (ad esempio ReadWriteMany). L'operazione di ripristino non riesce se la modalità di accesso al volume persistente di destinazione è diversa.
- 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 la creazione di un nuovo spazio dei nomi mediante un'operazione di clone o ripristino, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo per consentire all'utente interessato di accedere al nuovo spazio dei nomi.
- Quando crei un progetto per ospitare un'applicazione su un cluster OpenShift, al progetto (o namespace Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

  ```
  oc new-project wordpress
  oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
  oc adm policy add-scc-to-user privileged -z default -n wordpress
  ```

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection**.
3. Se si desidera eseguire il ripristino da uno snapshot, tenere selezionata l'icona **Snapshot**. In caso contrario, selezionare l'icona **Backup** per eseguire il ripristino da un backup.
4. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per lo snapshot o il backup da cui si desidera eseguire il ripristino, selezionare **Restore application** (Ripristina applicazione).
5. **Restore details** (Dettagli ripristino): Specificare i dettagli dell'applicazione ripristinata. Per impostazione predefinita, vengono visualizzati il cluster e lo spazio dei nomi correnti. Lasciare intatti questi valori per ripristinare un'applicazione in-place, che ripristina l'applicazione a una versione precedente di se stessa. Modificare questi valori se si desidera ripristinare un cluster o uno spazio dei nomi diverso.

- Immettere un nome e uno spazio dei nomi per l'applicazione.
- Scegliere il cluster di destinazione per l'applicazione.
- Selezionare **Revisione**.

> 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.

6. **Restore Summary** (Riepilogo ripristino): Esaminare i dettagli relativi all'azione di ripristino, digitare "restore" e selezionare **Restore**.

Risultato

Astra Control Center ripristina l'applicazione in base alle informazioni fornite. Se hai ripristinato l'applicazione in-place, il contenuto di eventuali volumi persistenti esistenti viene sostituito con il contenuto dei volumi persistenti dell'applicazione ripristinata.

> Dopo un'operazione di protezione dei dati (cloning, backup, 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.

Replica delle applicazioni su un sistema remoto utilizzando la tecnologia SnapMirror

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

Per un confronto tra backup/ripristini e replica, vedere "Concetti relativi alla protezione dei dati".

Puoi replicare le app in diversi scenari, come ad esempio i seguenti scenari on-premise, ibridi e multi-cloud:

- Dal sito a on-premise al sito B on-premise
- On-premise per il cloud con Cloud Volumes ONTAP
- Cloud con Cloud Volumes ONTAP in on-premise
- Cloud con Cloud Volumes ONTAP al cloud (tra diverse regioni dello stesso cloud provider o a diversi cloud provider)

Astra Control è in grado di replicare le applicazioni tra cluster on-premise, on-premise nel cloud (utilizzando Cloud Volumes ONTAP) o tra cloud (da Cloud Volumes ONTAP a Cloud Volumes ONTAP).

> È possibile replicare contemporaneamente un'altra applicazione (in esecuzione sull'altro cluster o sito) nella direzione opposta. Ad esempio, è possibile replicare le applicazioni A, B, C dal Datacenter 1 al Datacenter 2 e le applicazioni X, Y, Z dal Datacenter 2 al Datacenter 1.

Utilizzando Astra Control, è possibile eseguire le seguenti attività relative alla replica delle applicazioni:

- Impostare una relazione di replica
- Portare online un'applicazione replicata sul cluster di destinazione (failover)
- Risincronizzare una replica con esito negativo
- Replica inversa delle applicazioni
- Eseguire il failback delle applicazioni nel cluster di origine originale
- Eliminare una relazione di replica dell'applicazione

Prerequisiti per la replica

Vedere "prerequisiti per la replica" prima di iniziare.

Impostare una relazione di replica

L'impostazione di una relazione di replica implica quanto segue che costituisce il criterio di replica;

- Scelta della frequenza con cui Astra Control deve acquisire un'applicazione Snapshot (che include le risorse Kubernetes dell'applicazione e le snapshot dei volumi per ciascun volume dell'applicazione)
- Scelta della pianificazione della replica (incluse le risorse Kubernetes e i dati dei volumi persistenti)
- Impostazione del tempo di esecuzione dell'istantanea

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Nella pagina Application (applicazione), selezionare la scheda **Data Protection** > **Replication** (protezione dati).
3. Nella scheda Data Protection > Replication (protezione dati > replica), selezionare **Configure Replication policy** (Configura policy di replica). In alternativa, dalla casella protezione applicazione, selezionare l'opzione azioni e selezionare **Configura policy di replica**.
4. Inserire o selezionare le seguenti informazioni:
   - Cluster di destinazione
   - **Destination storage class** (Classe di storage di destinazione): Selezionare o immettere la classe di storage che utilizza la SVM associata sul cluster ONTAP di destinazione.
   - **Tipo di replica**: "Asincrono" è attualmente l'unico tipo di replica disponibile.
   - **Destination namespace**: Immettere uno spazio dei nomi di destinazione nuovo o esistente per il cluster di destinazione.

     > Eventuali risorse in conflitto nello spazio dei nomi selezionato verranno sovrascritte.

   - **Replication frequency** (frequenza di replica): Consente di impostare la frequenza con cui Astra Control deve acquisire un'istantanea e replicarla nella destinazione.
   - **Offset**: Consente di impostare il numero di minuti dall'inizio dell'ora in cui si desidera che Astra Control

prenda un'istantanea. È possibile utilizzare un offset in modo che non coincidano con altre operazioni pianificate. Ad esempio, se si desidera acquisire l'istantanea ogni 5 minuti a partire dalle 10:02, immettere "02" come minuti di offset. Il risultato sarebbe 10:02, 10:07, 10:12, ecc.

5. Selezionare **Avanti**, rivedere il riepilogo e selezionare **Salva**.

   > All'inizio, lo stato visualizza "app-mirror" prima che si verifichi la prima pianificazione.

   Astra Control crea un'applicazione Snapshot utilizzata per la replica.

6. Per visualizzare lo stato dell'applicazione Snapshot, selezionare la scheda **applicazioni** > **Snapshot**.

   Il nome Snapshot utilizza il formato "Replication-schedule-<string>". Astra Control conserva l'ultimo snapshot utilizzato per la replica. Le snapshot di replica precedenti vengono eliminate dopo il completamento della replica.

Risultato

In questo modo si crea la relazione di replica.

Astra Control completa le seguenti azioni in seguito alla definizione della relazione:

- Crea uno spazio dei nomi sulla destinazione (se non esiste)
- Crea un PVC sullo spazio dei nomi di destinazione corrispondente ai PVC dell'applicazione di origine.
- Utilizza un'istantanea iniziale coerente con l'applicazione.
- Stabilisce la relazione di SnapMirror per i volumi persistenti utilizzando l'istantanea iniziale.

La pagina protezione dati mostra lo stato e lo stato della relazione di replica: <Health status> | <Relationship life cycle state>

Ad esempio: Normale | stabilito

Scopri di seguito gli stati e lo stato della replica.

Portare online un'applicazione replicata sul cluster di destinazione (failover)

Utilizzando Astra Control, è possibile eseguire il failover delle applicazioni replicate in un cluster di destinazione. Questa procedura interrompe la relazione di replica e porta l'applicazione online sul cluster di destinazione. Questa procedura non interrompe l'applicazione sul cluster di origine se era operativa.

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Nella pagina Application (applicazione), selezionare la scheda **Data Protection** > **Replication** (protezione dati).
3. Nella scheda Data Protection > Replication (protezione dati > Replica), dal menu Actions (azioni), selezionare **failover**.
4. Nella pagina failover, esaminare le informazioni e selezionare **failover**.

Risultato

La procedura di failover consente di eseguire le seguenti operazioni:

- Sul cluster di destinazione, l'applicazione viene avviata in base all'ultima snapshot replicata.

- Il cluster e l'applicazione di origine (se operativi) non vengono arrestati e continueranno a funzionare.
- Lo stato di replica cambia in "failover", quindi in "failover" una volta completato.
- La policy di protezione dell'applicazione di origine viene copiata nell'applicazione di destinazione in base alle pianificazioni presenti nell'applicazione di origine al momento del failover.
- Astra Control mostra l'applicazione sia sul cluster di origine che di destinazione, nonché il relativo stato di salute.

Risincronizzare una replica con esito negativo

L'operazione di risincronizzazione ristabilisce la relazione di replica. È possibile scegliere l'origine della relazione per conservare i dati nel cluster di origine o di destinazione. Questa operazione ristabilisce le relazioni di SnapMirror per avviare la replica del volume nella direzione desiderata.

Il processo arresta l'applicazione sul nuovo cluster di destinazione prima di ristabilire la replica.

> Durante il processo di risincronizzazione, lo stato del ciclo di vita viene visualizzato come "stabiling" (in corso).

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Nella pagina Application (applicazione), selezionare la scheda **Data Protection** > **Replication** (protezione dati).
3. Nella scheda Data Protection > Replication (protezione dati > Replica), dal menu Actions (azioni), selezionare **Resync**.
4. Nella pagina Resync, selezionare l'istanza dell'applicazione di origine o di destinazione contenente i dati che si desidera conservare.

   > Scegliere con attenzione l'origine di risincronizzazione, in quanto i dati sulla destinazione verranno sovrascritti.

5. Selezionare **Resync** per continuare.
6. Digitare "resync" per confermare.
7. Selezionare **Sì, risincronizzare** per terminare.

Risultato

- La pagina Replication (Replica) mostra "stabiling" (in corso) come stato della replica.
- Astra Control arresta l'applicazione sul nuovo cluster di destinazione.
- Astra Control ristabilisce la replica del volume persistente nella direzione selezionata utilizzando la risincronizzazione di SnapMirror.
- La pagina Replication mostra la relazione aggiornata.

Replica inversa delle applicazioni

Si tratta dell'operazione pianificata per spostare l'applicazione nel cluster di destinazione continuando a replicare nel cluster di origine. Astra Control arresta l'applicazione nel cluster di origine e replica i dati nella destinazione prima di eseguire il failover dell'applicazione nel cluster di destinazione.

In questa situazione, si sta sostituendo l'origine e la destinazione. Il cluster di origine originale diventa il nuovo

cluster di destinazione e il cluster di destinazione originale diventa il nuovo cluster di origine.

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Nella pagina Application (applicazione), selezionare la scheda **Data Protection** > **Replication** (protezione dati).
3. Nella scheda Data Protection > Replication (protezione dati > Replica), dal menu Actions (azioni), selezionare **Reverse Replication** (replica inversa).
4. Nella pagina Replica inversa, esaminare le informazioni e selezionare **Replica inversa** per continuare.

Risultato

Le seguenti azioni si verificano in seguito alla replica inversa:

- Viene acquisita un'istantanea delle risorse Kubernetes dell'applicazione di origine.
- I pod dell'applicazione di origine vengono interrotti correttamente eliminando le risorse Kubernetes dell'applicazione (lasciando PVC e PVS in posizione).
- Una volta spenti i pod, le istantanee dei volumi dell'applicazione vengono acquisite e replicate.
- Le relazioni di SnapMirror vengono interrotte, rendendo i volumi di destinazione pronti per la lettura/scrittura.
- Le risorse Kubernetes dell'applicazione vengono ripristinate da Snapshot pre-shutdown, utilizzando i dati del volume replicati dopo l'arresto dell'applicazione di origine.
- La replica viene ristabilita in senso inverso.

Eseguire il failback delle applicazioni nel cluster di origine originale

Utilizzando Astra Control, è possibile ottenere il "failback" dopo un'operazione di "failover" utilizzando la seguente sequenza di operazioni. In questo flusso di lavoro per ripristinare la direzione di replica originale, Astra Control replica (risincronizza) le modifiche dell'applicazione nel cluster di origine prima di invertire la direzione di replica.

Questo processo inizia da una relazione che ha completato un failover a una destinazione e prevede i seguenti passaggi:

- Iniziare con uno stato di failover.
- Risincronizzare la relazione.
- Invertire la replica.

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Nella pagina Application (applicazione), selezionare la scheda **Data Protection** > **Replication** (protezione dati).
3. Nella scheda Data Protection > Replication (protezione dati > Replica), dal menu Actions (azioni), selezionare **Resync**.
4. Per un'operazione di fail back, scegliere l'applicazione failed over come origine dell'operazione di risync (preservando eventuali dati scritti post fail over).
5. Digitare "resync" per confermare.
6. Selezionare **Sì, risincronizzare** per terminare.

7. Al termine della risincronizzazione, nel menu azioni della scheda protezione dati > Replica, selezionare **Replica inversa**.
8. Nella pagina Replica inversa, esaminare le informazioni e selezionare **Replica inversa**.

Risultato

Questo combina i risultati delle operazioni di "risincronizzazione" e "reverse relationship" per portare l'applicazione online sul cluster di origine con la replica ripresa nel cluster di destinazione originale.

Eliminare una relazione di replica dell'applicazione

L'eliminazione della relazione comporta due applicazioni separate senza alcuna relazione tra di esse.

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Nella pagina Application (applicazione), selezionare la scheda **Data Protection** > **Replication** (protezione dati).
3. Nella scheda Data Protection > Replication (protezione dati > replica), dalla casella Application Protection (protezione applicazione) o nel diagramma delle relazioni, selezionare **Delete Replication Relationship (Elimina relazione di replica)**.

Risultato

Le seguenti azioni si verificano in seguito all'eliminazione di una relazione di replica:

- Se la relazione viene stabilita ma l'applicazione non è ancora stata messa in linea sul cluster di destinazione (failover), Astra Control conserva i PVC creati durante l'inizializzazione, lascia un'applicazione gestita "vuota" sul cluster di destinazione e conserva l'applicazione di destinazione per conservare eventuali backup creati.
- Se l'applicazione è stata portata online sul cluster di destinazione (failover), Astra Control conserva PVC e applicazioni di destinazione. Le applicazioni di origine e di destinazione sono ora considerate come applicazioni indipendenti. Le pianificazioni di backup rimangono su entrambe le applicazioni ma non sono associate l'una all'altra.

stato di salute della relazione di replica e stati del ciclo di vita della relazione

Astra Control visualizza lo stato della relazione e gli stati del ciclo di vita della relazione di replica.

Stati di integrità delle relazioni di replica

I seguenti stati indicano lo stato della relazione di replica:

- **Normale**: La relazione sta stabilendo o è stata stabilita e l'istantanea più recente è stata trasferita correttamente.
- **Attenzione**: La relazione sta fallendo o ha avuto un failover (e quindi non protegge più l'applicazione di origine).
- **Critico**
  - La relazione sta stabilendo o fallendo e l'ultimo tentativo di riconciliazione non è riuscito.
  - La relazione viene stabilita e l'ultimo tentativo di riconciliare l'aggiunta di un nuovo PVC sta fallendo.
  - La relazione viene stabilita (in modo da replicare un'istantanea di successo ed è possibile eseguire il failover), ma l'istantanea più recente non è riuscita o non è riuscita a replicarsi.

stati del ciclo di vita della replica

I seguenti stati riflettono le diverse fasi del ciclo di vita della replica:

- **Definizione**: È in corso la creazione di una nuova relazione di replica. Astra Control crea uno spazio dei nomi, se necessario, crea dichiarazioni di volumi persistenti (PVC) su nuovi volumi nel cluster di destinazione e crea relazioni SnapMirror. Questo stato può anche indicare che la replica sta eseguendo una risyncing o un'inversione della replica.
- **Stabilito**: Esiste una relazione di replica. Astra Control verifica periodicamente la disponibilità dei PVC, verifica la relazione di replica, crea periodicamente istantanee dell'applicazione e identifica eventuali nuovi PVC di origine nell'applicazione. In tal caso, Astra Control crea le risorse per includerle nella replica.
- **Failover**: Astra Control interrompe le relazioni SnapMirror e ripristina le risorse Kubernetes dell'applicazione dall'ultima snapshot dell'applicazione replicata con successo.
- **Failed over**: Astra Control interrompe la replica dal cluster di origine, utilizza l'applicazione Snapshot replicata più recente (riuscita) sulla destinazione e ripristina le risorse Kubernetes.
- **Risyncing**: Astra Control risincronizza i nuovi dati sull'origine resync alla destinazione resync utilizzando la risync di SnapMirror. Questa operazione potrebbe sovrascrivere alcuni dati sulla destinazione in base alla direzione della sincronizzazione. Astra Control interrompe l'esecuzione dell'applicazione sullo spazio dei nomi di destinazione e rimuove l'applicazione Kubernetes. Durante il processo di risyncing, lo stato viene visualizzato come "stabiling" (in corso).
- **Inversione**: È l'operazione pianificata per spostare l'applicazione nel cluster di destinazione continuando a replicare nel cluster di origine. Astra Control arresta l'applicazione sul cluster di origine, replica i dati nella destinazione prima di eseguire il failover dell'applicazione nel cluster di destinazione. Durante la replica inversa, lo stato viene visualizzato come "stabiling" (in corso).
- **Eliminazione**:
  - Se la relazione di replica è stata stabilita ma non è stato ancora eseguito il failover, Astra Control rimuove i PVC creati durante la replica ed elimina l'applicazione gestita di destinazione.
  - Se la replica ha già avuto esito negativo, Astra Control conserva i PVC e l'applicazione di destinazione.

Clonare e migrare le applicazioni

Clonare un'applicazione esistente per creare un'applicazione duplicata sullo stesso cluster Kubernetes o su un altro cluster. Quando Astra Control Center 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. È possibile utilizzare l'interfaccia utente Astra o. "L'API Astra Control" per clonare e migrare le applicazioni.

Di cosa hai bisogno

Per clonare le applicazioni in un cluster diverso, è necessario un bucket predefinito. Quando si aggiunge il primo bucket, questo diventa quello predefinito.

A proposito di questa attività

- Se si implementa un'applicazione con un StorageClass esplicitamente impostato e si deve clonare l'applicazione, il cluster di destinazione deve avere la StorageClass specificata in origine. Il cloning di un'applicazione con un StorageClass esplicitamente impostato su un cluster che non ha lo stesso StorageClass avrà esito negativo.

- 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.
- I bucket S3 in Astra Control Center non riportano la capacità disponibile. Prima di eseguire il backup o la clonazione delle applicazioni gestite da Astra Control Center, controllare le informazioni del bucket nel sistema di gestione ONTAP o StorageGRID.
- Durante il backup di un'applicazione o il ripristino di un'applicazione, è possibile specificare un ID bucket. Un'operazione di cloni dell'applicazione, tuttavia, utilizza sempre il bucket predefinito definito. Non esiste alcuna opzione per modificare i bucket per un clone. Se si desidera controllare quale bucket viene utilizzato, è possibile farlo "modificare l'impostazione predefinita del bucket" oppure fare una "backup" seguito da un "ripristinare" separatamente.
- 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 la creazione di un nuovo spazio dei nomi mediante un'operazione di clone o ripristino, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo per consentire all'utente interessato di accedere al nuovo spazio dei nomi.

Considerazioni su OpenShift

- Se clonate un'applicazione tra cluster, i cluster di origine e di destinazione devono essere della stessa distribuzione di OpenShift. Ad esempio, se clonate un'applicazione da un cluster OpenShift 4.7, utilizzate un cluster di destinazione che è anche OpenShift 4.7.
- Quando crei un progetto per ospitare un'applicazione su un cluster OpenShift, al progetto (o namespace Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

```
oc new-project wordpress
oc adm policy add-scc-to-group anyuid system:serviceaccounts:wordpress
oc adm policy add-scc-to-user privileged -z default -n wordpress
```

Fasi

1. 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. **Clone Details**: Specificare i dettagli per il clone:
   - Immettere un nome.
   - Immettere uno spazio dei nomi per il clone.
   - Scegliere un cluster di destinazione per il clone.
   - Scegliere se si desidera creare il clone da uno snapshot o da un backup esistente. Se non si seleziona questa opzione, Astra Control Center crea il clone dallo stato corrente dell'applicazione.
5. **Origine**: Se si sceglie di clonare da uno snapshot o da un backup esistente, scegliere lo snapshot o il backup che si desidera utilizzare.

6. Selezionare **Revisione**.
7. **Clone Summary**: Leggi i dettagli sul clone e seleziona **Clone**.

Risultato

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

> Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

Gestire 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 i ganci di esecuzione per sospendere tutte le transazioni del database prima di uno snapshot e riprendere le transazioni dopo il completamento dello snapshot. Ciò garantisce snapshot coerenti con l'applicazione.

Tipi di hook di esecuzione

Astra Control supporta i seguenti tipi di hook di esecuzione, in base al momento in cui possono essere eseguiti:

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

Note importanti sugli hook di esecuzione personalizzati

Quando si pianificano gli hook di esecuzione per le applicazioni, considerare quanto segue.

- 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).

> Poiché gli hook di esecuzione spesso riducono o disattivano completamente le funzionalità dell'applicazione con cui vengono eseguiti, è consigliabile 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 un gancio di esecuzione post-backup non può presumere che il backup sia stato completato.

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 e cinque 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	Y	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	Y	N/A.

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, l'origine e il momento dell'esecuzione di un gancio (pre o post-operazione). Per visualizzare i registri degli eventi che circondano gli hook di esecuzione, accedere alla pagina **Activity** nell'area di navigazione a sinistra.

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

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. Vai a **account**.
2. Selezionare la scheda **script**.
3. Selezionare **Aggiungi**.
4. 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.

5. 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. Vedere "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. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare **Aggiungi**.
4. Nell'area **Dettagli gancio**, determinare quando eseguire il gancio selezionando un tipo di operazione dal menu a discesa **operazione**.
5. Immettere un nome univoco per l'hook.
6. (Facoltativo) inserire gli argomenti da passare al gancio durante l'esecuzione, premendo il tasto Invio dopo ogni argomento inserito per registrarne ciascuno.
7. Nell'area **Container Images** (immagini container), se il gancio deve essere eseguito su tutte le immagini container contenute nell'applicazione, attivare la casella di controllo **Apply to all container images** (Applica a tutte le immagini container). Se invece il gancio dovrebbe agire solo su una o più immagini container specificate, inserire i nomi delle immagini container nel campo **nomi delle immagini container da abbinare**.
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 **Aggiungi gancio**.

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.

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).

Esempi di gancio di esecuzione

USA i seguenti esempi per avere un'idea di come strutturare i tuoi hook di esecuzione. È possibile utilizzare questi ganci come modelli o come script di test.

Semplice esempio di successo

Questo è un esempio di un semplice hook che riesce e scrive un messaggio in output standard e in errore standard.

```
#!/bin/sh

# success_sample.sh
#
```

```
# A simple noop success hook script for testing purposes.
#
# args: None
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}



#
# main
#

# log something to stdout
info "running success_sample.sh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Semplice esempio di successo (versione bash)

Questo è un esempio di un semplice hook che riesce e scrive un messaggio in output standard e standard error, scritto per bash.

```
#!/bin/bash

# success_sample.bash
#
# A simple noop success hook script for testing purposes.
#
# args: None


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#
```

```
# log something to stdout
info "running success_sample.bash"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Semplice esempio di successo (versione zsh)

Questo è un esempio di un semplice hook che riesce e scrive un messaggio in output standard e errore standard, scritto per la shell Z.

```
#!/bin/zsh

# success_sample.zsh
#
# A simple noop success hook script for testing purposes.
#
# args: None
#



#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}



#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
```

```
error() {
    msg "ERROR: $*" 1>&2
}

#
# main
#

# log something to stdout
info "running success_sample.zsh"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Esempio di successo con argomenti

Nell'esempio riportato di seguito viene illustrato come utilizzare gli ARG in un gancio.

```
#!/bin/sh

# success_sample_args.sh
#
# A simple success hook script with args for testing purposes.
#
# args: Up to two optional args that are echoed to stdout

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}
```

```
#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running success_sample_args.sh"


# collect args
arg1=$1
arg2=$2

# output args and arg count to stdout
info "number of args: $#"
info "arg1 ${arg1}"
info "arg2 ${arg2}"

# exit with 0 to indicate success
info "exit 0"
exit 0
```

Esempio di gancio pre-snapshot/post-snapshot

Nell'esempio seguente viene illustrato come utilizzare lo stesso script sia per un hook pre-snapshot che per un hook post-snapshot.

```
#!/bin/sh

# success_sample_pre_post.sh
#
# A simple success hook script example with an arg for testing purposes
# to demonstrate how the same script can be used for both a prehook and
posthook
#
# args: [pre|post]
```

```
# unique error codes for every error case
ebase=100
eusage=$((ebase+1))
ebadstage=$((ebase+2))
epre=$((ebase+3))
epost=$((ebase+4))


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# Would run prehook steps here
#
prehook() {
    info "Running noop prehook"
    return 0
}

#
```

```
# Would run posthook steps here
#
posthook() {
    info "Running noop posthook"
    return 0
}


#
# main
#

# check arg
stage=$1
if [ -z "${stage}" ]; then
    echo "Usage: $0 <pre|post>"
    exit ${eusage}
fi

if [ "${stage}" != "pre" ] && [ "${stage}" != "post" ]; then
    echo "Invalid arg: ${stage}"
    exit ${ebadstage}
fi

# log something to stdout
info "running success_sample_pre_post.sh"

if [ "${stage}" = "pre" ]; then
    prehook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during prehook"
    fi
fi

if [ "${stage}" = "post" ]; then
    posthook
    rc=$?
    if [ ${rc} -ne 0 ]; then
        error "Error during posthook"
    fi
fi

exit ${rc}
```

Esempio di guasto

Nell’esempio riportato di seguito viene illustrato come gestire gli errori in un hook.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#
```

```
# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Esempio di errore dettagliato

Nell'esempio riportato di seguito viene illustrato come gestire gli errori in modo semplice, con una registrazione più dettagliata.

```
#!/bin/sh

# failure_sample_verbose.sh
#
# A simple failure hook script with args for testing purposes.
#
# args: [The number of lines to output to stdout]


#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
```

```
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_verbose.sh"


# output arg value to stdout
linecount=$1
info "line count ${linecount}"

# write out a line to stdout based on line count arg
i=1
while [ "$i" -le ${linecount} ]; do
    info "This is line ${i} from failure_sample_verbose.sh"
    i=$(( i + 1 ))
done

error "exiting with error code 8"
exit 8
```

Errore con un esempio di codice di uscita

Nell'esempio riportato di seguito viene illustrato un errore di hook con un codice di uscita.

```
#!/bin/sh

# failure_sample_arg_exit_code.sh
#
# A simple failure hook script for testing purposes.
#
# args: [the exit code to return]
#


#
# Writes the given message to standard output
```

```
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
info "running failure_sample_arg_exit_code.sh"

argexitcode=$1

# log to stderr
error "script failed, returning exit code ${argexitcode}"

# exit with specified exit code
exit ${argexitcode}
```

Esempio di successo dopo il guasto

Nell’esempio riportato di seguito viene illustrato un errore di hook alla prima esecuzione, ma dopo la seconda esecuzione.

```
#!/bin/sh

# failure_then_success_sample.sh
#
# A hook script that fails on initial run but succeeds on second run for
testing purposes.
#
# Helpful for testing retry logic for post hooks.
#
# args: None
#

#
# Writes the given message to standard output
#
# $* - The message to write
#
msg() {
    echo "$*"
}


#
# Writes the given information message to standard output
#
# $* - The message to write
#
info() {
    msg "INFO: $*"
}

#
# Writes the given error message to standard error
#
# $* - The message to write
#
error() {
    msg "ERROR: $*" 1>&2
}


#
# main
#

# log something to stdout
```

```
info "running failure_success sample.sh"


if [ -e /tmp/hook-test.junk ] ; then
    info "File does exist.  Removing /tmp/hook-test.junk"
    rm /tmp/hook-test.junk
    info "Second run so returning exit code 0"
    exit 0
else
    info "File does not exist.  Creating /tmp/hook-test.junk"
    echo "test" > /tmp/hook-test.junk
    error "Failed first run, returning exit code 5"
    exit 5
fi
```

Monitorare lo stato delle applicazioni e del cluster

Visualizza un riepilogo dello stato delle applicazioni e dei cluster

Seleziona la * dashboard* per visualizzare una vista di alto livello delle tue app, cluster, backend di storage e della loro salute.

Questi non sono solo numeri statici o stati, ma puoi eseguire il drill-down da ciascuno di essi. 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.

Sezione applicazioni

La sezione **applicazioni** consente di identificare quanto segue:

- Quante app stai attualmente gestendo con Astra.
- Se queste applicazioni gestite sono in buona salute.
- Se le applicazioni sono completamente protette (sono protette se sono disponibili backup recenti).
- Il numero di applicazioni rilevate, ma non ancora gestite.

  Idealmente, questo numero sarebbe pari a zero perché, una volta scoperte, gestireste o ignorereste le applicazioni. Quindi, è necessario monitorare il numero di applicazioni rilevate nella dashboard per identificare quando gli sviluppatori aggiungono nuove applicazioni a un cluster.

Riquadro dei cluster

Il riquadro **Clusters** fornisce dettagli simili sullo stato dei cluster gestiti tramite Astra Control Center e consente di analizzare più dettagli come con un'applicazione.

Riquadro backend storage

Il riquadro **Storage backend** fornisce informazioni utili per identificare lo stato dei back-end dello storage, tra cui:

- Quanti backend di storage vengono gestiti
- Se questi backend gestiti sono in buono stato
- Se i backend sono completamente protetti
- Il numero di backend rilevati, ma non ancora gestiti.

Visualizza lo stato di salute e i dettagli dei cluster

Dopo aver aggiunto i cluster da gestire da Astra Control Center, è possibile visualizzare i dettagli del cluster, ad esempio la sua posizione, i nodi di lavoro, i volumi persistenti e le classi di storage.

Fasi

1. Nell'interfaccia utente di Astra Control Center, selezionare **Clusters**.
2. Nella pagina **Clusters**, selezionare il cluster di cui si desidera visualizzare i dettagli.

> 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**: Mostra le attività correlate al cluster.

> È inoltre possibile visualizzare le informazioni sul cluster partendo da Astra Control Center **Dashboard**. Nella scheda **Clusters** sotto **Riepilogo risorse**, è possibile selezionare i cluster gestiti, che consentono di accedere alla pagina **Clusters**. Una volta visualizzata la pagina **Clusters**, seguire la procedura descritta in precedenza.

Visualizza lo stato di salute e i dettagli di un'applicazione

Dopo aver iniziato a gestire un'applicazione, Astra fornisce informazioni dettagliate sull'applicazione che consentono di identificarne lo stato (se è integro), lo stato di protezione (se è completamente protetto in caso di guasto), i pod, lo storage persistente e molto altro ancora.

Fasi

1. Nell'interfaccia utente di Astra Control Center, selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Trova le informazioni che cerchi:

Stato dell'app

Fornisce uno stato che riflette lo stato dell'applicazione in Kubernetes. Ad esempio, i pod e i volumi persistenti sono online? Se un'applicazione non è in buone condizioni, è necessario risolvere il problema sul cluster osservando i log di Kubernetes. Astra non fornisce informazioni utili per la risoluzione di un'applicazione guasta.

Stato di protezione dell'app

Fornisce uno stato di protezione dell'applicazione:

- **Completamente protetto**: L'applicazione dispone di una pianificazione di backup attiva e di un backup riuscito che risale a meno di una settimana fa
- **Protezione parziale**: L'applicazione dispone di una pianificazione di backup attiva, di una pianificazione di snapshot attiva o di un backup o snapshot riuscito
- **Non protetto**: Applicazioni non completamente protette o parzialmente protette.

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

Panoramica

Informazioni sullo stato dei pod associati all'applicazione.

Protezione dei dati

Consente di configurare una policy di protezione dei dati e di visualizzare le snapshot e i backup esistenti.

Storage

Mostra i volumi persistenti a livello di applicazione. Lo stato di un volume persistente è dal punto di vista del cluster Kubernetes.

Risorse

Consente di verificare quali risorse vengono sottoposte a backup e gestite.

Attività

Mostra le attività correlate all'applicazione.

> È inoltre possibile visualizzare le informazioni dell'applicazione partendo da Astra Control Center **Dashboard**. Nella scheda **applicazioni** sotto **Riepilogo risorse**, è possibile selezionare le applicazioni gestite, che consentono di accedere alla pagina **applicazioni**. Una volta visualizzata la pagina **applicazioni**, seguire la procedura descritta in precedenza.

Gestisci il tuo account

Gestire gli utenti

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

È inoltre possibile utilizzare LDAP per eseguire l'autenticazione per gli utenti selezionati.

Utilizzare LDAP

LDAP è un protocollo standard di settore per l'accesso alle informazioni di directory distribuite e una scelta popolare per l'autenticazione aziendale. È possibile collegare Astra Control Center a un server LDAP per eseguire l'autenticazione per gli utenti Astra selezionati. Ad alto livello, la configurazione prevede l'integrazione di Astra con LDAP e la definizione degli utenti e dei gruppi Astra corrispondenti alle definizioni LDAP. Vedere "Autenticazione LDAP" per ulteriori informazioni.

Invitare utenti

I proprietari e gli amministratori degli account possono invitare nuovi utenti ad Astra Control Center.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Selezionare **invita utente**.
4. Immettere il nome e l'indirizzo e-mail dell'utente.
5. Selezionare un ruolo utente con le autorizzazioni di sistema appropriate.

   Ciascun ruolo fornisce le seguenti autorizzazioni:

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

7. Selezionare **invita utenti**.

   L'utente riceve un'e-mail per informarlo che è stato invitato ad Astra Control Center. L'e-mail include la password temporanea, che dovrà essere modificata al primo accesso.

Aggiungere utenti

Gli account Owner e gli amministratori possono aggiungere altri utenti all'installazione di Astra Control Center.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Selezionare **Aggiungi utente**.
4. Immettere il nome dell'utente, l'indirizzo e-mail e una password temporanea.

L'utente dovrà modificare la password al primo accesso.

5. Selezionare un ruolo utente con le autorizzazioni di sistema appropriate.

   Ciascun ruolo fornisce le seguenti autorizzazioni:

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

6. 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, vedere "Gestire i ruoli".

7. Selezionare **Aggiungi**.

Gestire le password

Puoi gestire le password per gli account utente in Astra Control Center.

Modificare la password

È possibile modificare la password dell'account utente in qualsiasi momento.

Fasi

1. Selezionare l'icona User (utente) nella parte superiore destra della schermata.
2. Selezionare **Profilo**.
3. Dal menu Opzioni nella colonna **azioni** e selezionare **Modifica password**.
4. Immettere una password conforme ai requisiti.
5. Immettere nuovamente la password per confermare.
6. Selezionare **Cambia password**.

Reimpostare la password di un altro utente

Se l'account dispone delle autorizzazioni di ruolo Amministratore o Proprietario, è possibile reimpostare le password per altri account utente e per i propri. Quando si reimposta una password, si assegna una password temporanea che l'utente dovrà modificare al momento dell'accesso.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare l'elenco a discesa **azioni**.
3. Selezionare **Reset Password** (Ripristina password).
4. Immettere una password temporanea conforme ai requisiti della password.
5. Immettere nuovamente la password per confermare.

Al successivo accesso, all'utente verrà richiesto di modificare la password.

6. Selezionare **Ripristina password**.

Modificare il ruolo di un utente

Gli utenti con il ruolo Owner possono modificare il ruolo di tutti gli utenti, mentre gli utenti con il ruolo Admin possono modificare il ruolo degli utenti con il ruolo Admin, Member o Viewer.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare l'elenco a discesa **azioni**.
3. Selezionare **Modifica ruolo**.
4. Selezionare un nuovo ruolo.
5. Per applicare i vincoli al ruolo, attivare la casella di controllo **limita ruolo ai vincoli** e selezionare un vincolo dall'elenco.

   Se non ci sono vincoli, è possibile aggiungere un vincolo. Per ulteriori informazioni, vedere "Gestire i ruoli".

6. Selezionare **Conferma**.

Risultato

Astra Control Center aggiorna le autorizzazioni dell'utente in base al nuovo ruolo selezionato.

Rimuovere gli utenti

Gli utenti con il ruolo Owner (Proprietario) o Admin (Amministratore) possono rimuovere altri utenti dall'account in qualsiasi momento.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Nella scheda **utenti**, selezionare la casella di controllo nella riga di ciascun utente che si desidera rimuovere.
3. Dal menu Options (Opzioni) nella colonna **Actions** (azioni), selezionare **Remove user/s** (Rimuovi utenti).
4. Quando richiesto, confermare l'eliminazione digitando la parola "remove", quindi selezionare **Yes, Remove User** (Sì, Rimuovi utente).

Risultato

Astra Control Center 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"

Visualizzare e gestire le notifiche

Astra informa l'utente quando le azioni sono state completate o non sono riuscite. Ad esempio, se il backup di un'applicazione è stato completato correttamente, viene visualizzata una notifica.

È possibile gestire queste notifiche dall'alto a destra dell'interfaccia:

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**.

Aggiungere e rimuovere le credenziali

Aggiungi e rimuovi le credenziali per i provider di cloud privato locali, come ONTAP S3, i cluster Kubernetes gestiti con OpenShift o i cluster Kubernetes non gestiti dal tuo account in qualsiasi momento. Astra Control Center utilizza queste credenziali per scoprire i cluster Kubernetes e le applicazioni sui cluster e per eseguire il provisioning delle risorse per conto dell'utente.

Tutti gli utenti di Astra Control Center condividono gli stessi set di credenziali.

Aggiungere credenziali

È possibile aggiungere credenziali ad Astra Control Center quando si gestiscono i cluster. Per aggiungere credenziali aggiungendo un nuovo cluster, vedere "Aggiungere un cluster Kubernetes".

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

Rimuovere le credenziali

Rimuovere le credenziali da un account in qualsiasi momento. Rimuovere le credenziali solo dopo "annullamento della gestione di tutti i cluster associati".

> Il primo set di credenziali aggiunto ad Astra Control Center è sempre in uso perché Astra Control Center utilizza le credenziali per l'autenticazione nel bucket di backup. Si consiglia di non rimuovere queste credenziali.

Fasi

1. Selezionare **account**.
2. Selezionare la scheda **credenziali**.
3. Selezionare il menu Opzioni nella colonna **Stato** per le credenziali che si desidera rimuovere.
4. Selezionare **Rimuovi**.
5. Digitare la parola "remove" per confermare l'eliminazione, quindi selezionare **Sì, Rimuovi credenziale**.

Risultato

Astra Control Center rimuove le credenziali dall'account.

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.

> Se gestisci i cluster Kubernetes da Astra Control e Astra Control è connesso a Cloud Insights, Astra Control invia i registri degli eventi a Cloud Insights. Le informazioni di log, incluse le informazioni sull'implementazione del pod e sugli allegati PVC, vengono visualizzate nel registro delle attività di controllo Astra. Utilizza queste informazioni per identificare eventuali problemi sui cluster Kubernetes che stai gestendo.

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).

Intraprendere azioni per risolvere gli eventi che richiedono attenzione

1. Selezionare **Activity** (attività).
2. Selezionare un evento che richiede attenzione.
3. Selezionare l'opzione a discesa **take action**.

   Da questo elenco è possibile visualizzare le possibili azioni correttive da intraprendere, visualizzare la documentazione relativa al problema e ottenere supporto per risolvere il problema.

Aggiornare una licenza esistente

È possibile convertire una licenza di valutazione in una licenza completa oppure aggiornare una licenza di valutazione o una licenza completa esistente con una nuova licenza. Se non si dispone di una licenza completa, rivolgersi al contatto commerciale NetApp per ottenere una licenza completa e un numero di serie. È possibile utilizzare l'interfaccia utente Astra o. "L'API Astra Control" per aggiornare una licenza esistente.

Fasi

1. Accedere a. "Sito di supporto NetApp".
2. Accedere alla pagina di download di Astra Control Center, inserire il numero di serie e scaricare il file di licenza NetApp completo (NLF).
3. Accedere all'interfaccia utente di Astra Control Center.
4. Dalla barra di navigazione a sinistra, selezionare **account** > **licenza**.
5. Nella pagina **account** > **licenza**, selezionare il menu a discesa dello stato della licenza esistente e selezionare **Sostituisci**.
6. Individuare il file di licenza scaricato.
7. Selezionare **Aggiungi**.

La pagina **account** > **licenze** visualizza le informazioni sulla licenza, la data di scadenza, il numero di serie della licenza, l'ID account e le unità CPU utilizzate.

Per ulteriori informazioni

- "Licenza Astra Control Center"

Gestire le connessioni al repository

È possibile collegare i repository ad Astra Control per utilizzarli come riferimento per immagini e artefatti di installazione dei pacchetti software. Quando si importano pacchetti software, Astra Control fa riferimento alle immagini di installazione nel repository di immagini, ai binari e ad altri artefatti nel repository di artefatti.

Di cosa hai bisogno

- Kubernetes cluster con Astra Control Center installato
- Un repository Docker in esecuzione a cui è possibile accedere
- Un repository di artefatti in esecuzione (ad esempio Artifactory) a cui è possibile accedere

Collegare un repository di immagini Docker

È possibile collegare un repository di immagini Docker per contenere le immagini di installazione dei pacchetti, come quelle di Astra Data Store. Quando si installano i pacchetti, Astra Control importa i file di immagine del pacchetto dal repository di immagini.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **connessioni**.
3. Nella sezione **Docker Image Repository**, selezionare il menu in alto a destra.
4. Selezionare **Connect**.
5. Aggiungere l'URL e la porta per il repository.

6. Immettere le credenziali per il repository.
7. Selezionare **Connect**.

Risultato

Il repository è connesso. Nella sezione **Docker Image Repository**, il repository dovrebbe mostrare uno stato di connessione.

Scollegare un repository di immagini Docker

È possibile rimuovere la connessione a un repository di immagini Docker se non è più necessaria.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **connessioni**.
3. Nella sezione **Docker Image Repository**, selezionare il menu in alto a destra.
4. Selezionare **Disconnect**.
5. Selezionare **Sì, disconnettere il repository di immagini Docker**.

Risultato

Il repository viene scollegato. Nella sezione **Docker Image Repository**, il repository dovrebbe mostrare uno stato disconnesso.

Collegare un repository di artefatti

È possibile collegare un repository di artefatti all'host di artefatti come i binari dei pacchetti software. Quando si installano i pacchetti, Astra Control importa gli artefatti per i pacchetti software dal repository di immagini.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **connessioni**.
3. Nella sezione **Archivio artefatti**, selezionare il menu in alto a destra.
4. Selezionare **Connect**.
5. Aggiungere l'URL e la porta per il repository.
6. Se è richiesta l'autenticazione, attivare la casella di controllo **Usa autenticazione** e immettere le credenziali per il repository.
7. Selezionare **Connect**.

Risultato

Il repository è connesso. Nella sezione **Archivio artefatti**, il repository dovrebbe mostrare uno stato di connessione.

Scollegare un repository di artefatti

È possibile rimuovere la connessione a un repository di artefatti se non è più necessaria.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.

2. Selezionare la scheda **connessioni**.
3. Nella sezione **Archivio artefatti**, selezionare il menu in alto a destra.
4. Selezionare **Disconnect**.
5. Selezionare **Sì, disconnettere il repository degli artefatti**.

Risultato

Il repository viene scollegato. Nella sezione **Archivio artefatti**, il repository dovrebbe mostrare uno stato di connessione.

Trova ulteriori informazioni

- "Gestire i pacchetti software"

Gestire i pacchetti software

NetApp offre funzionalità aggiuntive per Astra Control Center con pacchetti software che è possibile scaricare dal NetApp Support Site. Dopo aver collegato i repository Docker e degli artefatti, è possibile caricare e importare pacchetti per aggiungere questa funzionalità ad Astra Control Center. È possibile utilizzare l'interfaccia utente Web di CLI o Astra Control Center per gestire i pacchetti software.

Di cosa hai bisogno

- Kubernetes cluster con Astra Control Center installato
- Un repository di immagini Docker connesso per contenere le immagini dei pacchetti software. Per ulteriori informazioni, vedere "Gestire le connessioni al repository".
- Un repository di artefatti collegato per contenere file binari e artefatti dei pacchetti software. Per ulteriori informazioni, vedere "Gestire le connessioni al repository".
- Un pacchetto software dal NetApp Support Site

Caricare le immagini dei pacchetti software nei repository

Astra Control Center fa riferimento alle immagini dei pacchetti e agli artefatti nei repository collegati. È possibile caricare immagini e artefatti nei repository utilizzando la CLI.

Fasi

1. Scaricare il pacchetto software dal sito di supporto NetApp e salvarlo su un computer dotato di `kubectl` utility installata.
2. Estrarre il file di pacchetto compresso e modificare la directory nella posizione del file di bundle di Astra Control (ad esempio, `acc.manifest.yaml`).
3. Trasferire le immagini del pacchetto nel repository Docker. Effettuare le seguenti sostituzioni:
    - Sostituire BUNDLE_FILE con il nome del file bundle Astra Control (ad esempio, `acc.manifest.yaml`).
    - Sostituire MY_REGISTRY con l'URL del repository Docker.
    - Sostituire MY_REGISTRY_USER con il nome utente.
    - Sostituire MY_REGISTRY_TOKEN con un token autorizzato per il Registro di sistema.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY -u
MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

4. Se il pacchetto contiene artefatti, copiarli nel repository degli artefatti. Sostituire BUNDLE_FILE con il nome del file bundle Astra Control e NETWORK_LOCATION con il percorso di rete in cui copiare i file degli artefatti:

```
kubectl astra packages copy-artifacts -m BUNDLE_FILE -n NETWORK_LOCATION
```

Aggiungere un pacchetto software

È possibile importare pacchetti software utilizzando un file bundle di Astra Control Center. Questa operazione consente di installare il pacchetto e di rendere disponibile il software per Astra Control Center.

Aggiungere un pacchetto software utilizzando l'interfaccia utente Web Astra Control

È possibile utilizzare l'interfaccia utente Web di Astra Control Center per aggiungere un pacchetto software che è stato caricato nei repository collegati.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **pacchetti**.
3. Selezionare il pulsante **Aggiungi**.
4. Nella finestra di dialogo di selezione del file, selezionare l'icona di caricamento.
5. Scegliere un file bundle Astra Control, in `.yaml` da caricare.
6. Selezionare **Aggiungi**.

Risultato

Se il file bundle è valido e le immagini e gli artefatti del pacchetto si trovano nei repository collegati, il pacchetto viene aggiunto ad Astra Control Center. Quando lo stato nella colonna **Status** diventa **Available**, è possibile utilizzare il pacchetto. Per ottenere ulteriori informazioni, passare il mouse sullo stato di un pacchetto.

> Se una o più immagini o artefatti per un pacchetto non vengono trovati nel repository, viene visualizzato un messaggio di errore per quel pacchetto.

Aggiungere un pacchetto software utilizzando l'interfaccia CLI

È possibile utilizzare l'interfaccia CLI per importare un pacchetto software caricato nei repository collegati. Per farlo, devi prima registrare il tuo ID account Astra Control Center e un token API.

Fasi

1. Utilizzando un browser Web, accedere all'interfaccia utente Web di Astra Control Center.
2. Dalla dashboard, selezionare l'icona utente in alto a destra.
3. Selezionare **API access**.
4. Annotare l'ID account nella parte superiore della schermata.

5. Selezionare **generate API token**.
6. Nella finestra di dialogo visualizzata, selezionare **generate API token**.
7. Prendere nota del token risultante e selezionare **Chiudi**. Nella CLI, modificare le directory in base alla posizione di `.yaml` file bundle nel contenuto del pacchetto estratto.
8. Importare il pacchetto utilizzando il file bundle, effettuando le seguenti sostituzioni:
   - Sostituire BUNDLE_FILE con il nome del file bundle Astra Control.
   - Sostituire IL SERVER con il nome DNS dell'istanza di Astra Control.
   - Sostituire ACCOUNT_ID e TOKEN con l'ID account e il token API registrati in precedenza.

```
kubectl astra packages import -m BUNDLE_FILE -u SERVER -a ACCOUNT_ID
-k TOKEN
```

Risultato

Se il file bundle è valido e le immagini e gli artefatti del pacchetto si trovano nei repository collegati, il pacchetto viene aggiunto ad Astra Control Center.

> Se una o più immagini o artefatti per un pacchetto non vengono trovati nel repository, viene visualizzato un messaggio di errore per quel pacchetto.

Rimuovere un pacchetto software

È possibile utilizzare l'interfaccia utente Web di Astra Control Center per rimuovere un pacchetto software precedentemente importato in Astra Control Center.

Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **pacchetti**.

   In questa pagina è possibile visualizzare l'elenco dei pacchetti installati e i relativi stati.

3. Nella colonna **azioni** del pacchetto, aprire il menu delle azioni.
4. Selezionare **Delete** (Elimina).

Risultato

Il pacchetto viene cancellato da Astra Control Center, ma le immagini e gli artefatti del pacchetto rimangono nei repository.

Trova ulteriori informazioni

- "Gestire le connessioni al repository"

Gestire i bucket

Un provider di bucket dell'archivio di oggetti è essenziale se si desidera eseguire il backup delle applicazioni e dello storage persistente o se si desidera clonare le applicazioni tra cluster. Utilizzando Astra Control Center, Aggiungi un provider di archivi di oggetti come destinazione di backup off-cluster per le tue applicazioni.

Non è necessario un bucket se si clonano la configurazione dell'applicazione e lo storage persistente sullo stesso cluster.

Utilizza uno dei seguenti provider di bucket Amazon Simple Storage Service (S3):

- 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 sostengono il supporto S3 di Amazon.

Un bucket può trovarsi in uno dei seguenti stati:

- In sospeso: Il bucket è pianificato per il rilevamento.
- Disponibile: La benna è disponibile per l'uso.
- Rimosso: Il bucket non è attualmente accessibile.

Per istruzioni su come gestire i bucket utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

È possibile eseguire queste attività relative alla gestione dei bucket:

- "Aggiungi un bucket"
- Modificare un bucket
- Ruotare o rimuovere le credenziali bucket
- Rimuovere una benna

> I bucket S3 in Astra Control Center non riportano la capacità disponibile. Prima di eseguire il backup o la clonazione delle applicazioni gestite da Astra Control Center, controllare le informazioni del bucket nel sistema di gestione ONTAP o StorageGRID.

Modificare un bucket

È possibile modificare le informazioni delle credenziali di accesso per un bucket e modificare se un bucket selezionato è il bucket predefinito.

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

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
2. Dal menu Opzioni nella colonna **azioni**, selezionare **Modifica**.
3. Modificare qualsiasi informazione diversa dal tipo di bucket.

   Impossibile modificare il tipo di bucket.

4. Selezionare **Aggiorna**.

Ruotare o rimuovere le credenziali bucket

Astra Control utilizza le credenziali bucket per ottenere l'accesso e fornire chiavi segrete per un bucket S3 in modo che Astra Control Center possa comunicare con il bucket.

Ruotare le credenziali del bucket

Se si ruotano le credenziali, ruotarle durante una finestra di manutenzione quando non sono in corso backup (pianificati o on-demand).

Procedura per modificare e ruotare le credenziali

1. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
2. Dal menu Opzioni nella colonna **azioni**, selezionare **Modifica**.
3. Creare la nuova credenziale.
4. Selezionare **Aggiorna**.

Rimuovere le credenziali bucket

È necessario rimuovere le credenziali bucket solo se sono state applicate nuove credenziali a un bucket o se il bucket non è più utilizzato attivamente.

Il primo set di credenziali aggiunto ad Astra Control è sempre in uso perché Astra Control utilizza le credenziali per autenticare il bucket di backup. Non rimuovere queste credenziali se il bucket è in uso, in quanto ciò potrebbe causare errori di backup e indisponibilità del backup.

Se si rimuovono le credenziali bucket attive, vedere "risoluzione dei problemi relativi alla rimozione delle credenziali bucket".

Per istruzioni su come rimuovere le credenziali S3 utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

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.

Di cosa hai bisogno

- 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 in alcuna policy di protezione attiva.

In tal caso, non sarà possibile continuare.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **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**.

Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"

Gestire il back-end dello storage

La gestione dei cluster di storage in Astra Control come back-end dello storage consente di ottenere collegamenti tra volumi persistenti (PVS) e il back-end dello storage, oltre a metriche di storage aggiuntive. È possibile monitorare la capacità dello storage e i dettagli relativi allo stato di salute, incluse le prestazioni, se il centro di controllo Astra è connesso a Cloud Insights.

Per istruzioni su come gestire i back-end dello storage utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

È possibile completare le seguenti attività relative alla gestione di un backend di storage:

- "Aggiungere un backend di storage"
- Visualizza i dettagli del back-end dello storage
- Annullare la gestione di un backend di storage
- Aggiornare una licenza back-end per lo storage Astra Data Store
- Aggiorna un back-end di storage Astra Data Store
- Rimuovere un backend di storage
- Aggiunta di nodi a un cluster di storage back-end
- Rimuovere i nodi da un cluster di back-end dello storage

Visualizza i dettagli del back-end dello storage

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

Nella pagina Storage backend Details (Dettagli back-end storage), per Astra Data Store, sono disponibili le seguenti informazioni:

- Cluster Astra Data Store
  - Throughput, IOPS e latenza

    - Capacità utilizzata rispetto alla capacità totale
- Per ogni volume cluster Astra Data Store
    - Capacità utilizzata rispetto alla capacità totale
    - Throughput

Visualizza i dettagli del back-end dello storage dalla dashboard

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Dashboard**.
2. Esaminare la sezione Storage backend che mostra lo stato:
    - **Non integro**: Lo storage non è in uno stato ottimale. Ciò potrebbe essere dovuto a un problema di latenza o a un'applicazione degradata, ad esempio, a causa di un problema di container.
    - **Tutto sano**: Lo storage è stato gestito ed è in uno stato ottimale.
    - **Scoperto**: Lo storage è stato scoperto, ma non gestito da Astra Control.

Visualizza i dettagli del back-end dello storage dall'opzione Backend

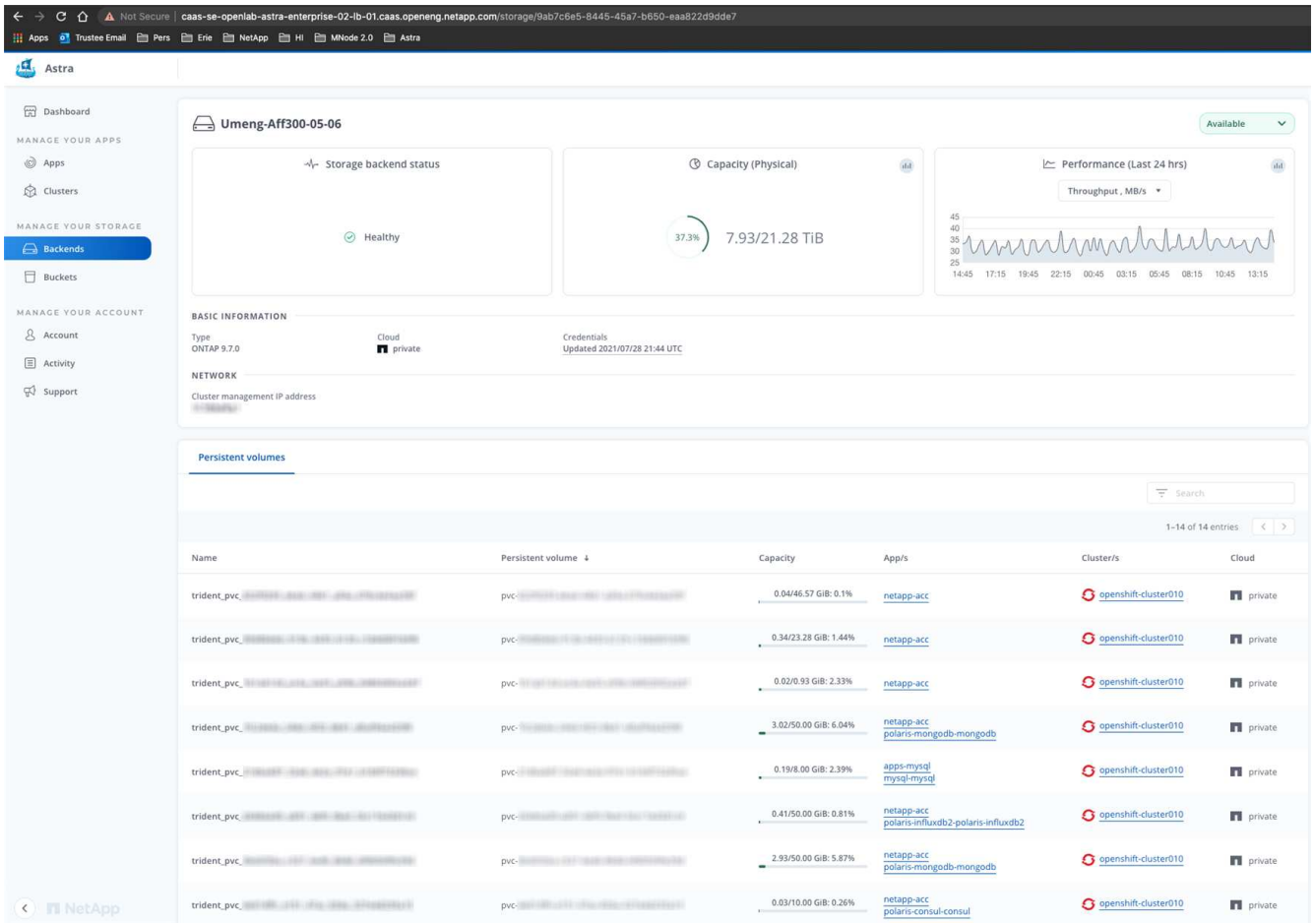
Visualizza informazioni sullo stato, la capacità e le performance del back-end (throughput IOPS e/o latenza).

È possibile visualizzare i volumi utilizzati dalle applicazioni Kubernetes, che vengono memorizzati in un backend di storage selezionato. Con Cloud Insights, è possibile visualizzare ulteriori informazioni. Vedere "Documentazione Cloud Insights".

Fasi

1. Nell'area di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il backend dello storage.

> Se si è connessi a NetApp Cloud Insights, gli estratti di dati da Cloud Insights vengono visualizzati nella pagina backend.



3. Per accedere direttamente a Cloud Insights, selezionare l'icona **Cloud Insights** accanto all'immagine delle metriche.

Annullare la gestione di un backend di storage

È possibile annullare la gestione del backend.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il backend dello storage.
3. Dal menu Opzioni nella colonna **azioni**, selezionare **Annulla gestione**.
4. Digitare "unManage" per confermare l'azione.
5. Selezionare **Sì, Annulla gestione del backend di storage**.

Rimuovere un backend di storage

È possibile rimuovere un backend di storage non più in uso. Questa operazione può essere utile per mantenere la configurazione semplice e aggiornata.

> Se si rimuove un backend Astra Data Store, questo non deve essere stato creato da vCenter.

Di cosa hai bisogno

- Assicurarsi che il backend dello storage non sia gestito.

- Assicurarsi che il backend dello storage non abbia volumi associati al cluster Astra Data Store.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Se il backend viene gestito, annullarne la gestione.
   a. Selezionare **Managed**.
   b. Selezionare il backend dello storage.
   c. Dall'opzione **azioni**, selezionare **Annulla gestione**.
   d. Digitare "unManage" per confermare l'azione.
   e. Selezionare **Sì, Annulla gestione del backend di storage**.
3. Selezionare **rilevato**.
   a. Selezionare il backend dello storage.
   b. Dall'opzione **azioni**, selezionare **Rimuovi**.
   c. Digitare "remove" per confermare l'azione.
   d. Selezionare **Sì, rimuovere il backend di storage**.

Aggiornare una licenza back-end per lo storage Astra Data Store

È possibile aggiornare la licenza per un backend di storage Astra Data Store per supportare un'implementazione più ampia o funzionalità avanzate.

Di cosa hai bisogno

- Un back-end storage Astra Data Store implementato e gestito
- Un file di licenza Astra Data Store (contatta il tuo commerciale NetApp per acquistare una licenza Astra Data Store)

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il nome di un backend di storage.
3. In **Basic Information** (informazioni di base), viene visualizzato il tipo di licenza installata.

   Se si passa il mouse sopra le informazioni sulla licenza, viene visualizzata una finestra a comparsa con ulteriori informazioni, come ad esempio la scadenza e le informazioni sui diritti.

4. In **licenza**, selezionare l'icona di modifica accanto al nome della licenza.
5. Nella pagina **Aggiorna licenza**, eseguire una delle seguenti operazioni:

Stato della licenza	Azione
Almeno una licenza è stata aggiunta ad Astra Data Store.	Selezionare una licenza dall'elenco.

Stato della licenza	Azione
Nessuna licenza aggiunta ad Astra Data Store.	a. Selezionare il pulsante **Aggiungi**. b. Selezionare un file di licenza da caricare. c. Selezionare **Aggiungi** per caricare il file di licenza.

6. Selezionare **Aggiorna**.

Aggiorna un back-end di storage Astra Data Store

Puoi aggiornare il tuo back-end Astra Data Store da Astra Control Center. A tale scopo, devi prima caricare un pacchetto di aggiornamento; Astra Control Center utilizzerà questo pacchetto di aggiornamento per aggiornare Astra Data Store.

Di cosa hai bisogno

- Un back-end di storage gestito da Astra Data Store
- Un pacchetto di aggiornamento di Astra Data Store caricato (vedere "Gestire i pacchetti software")

Fasi

1. Selezionare **Backend**.
2. Scegliere un backend di storage Astra Data Store dall'elenco e selezionare il menu corrispondente nella colonna **azioni**.
3. Selezionare **Upgrade**.
4. Selezionare una versione dell'aggiornamento dall'elenco.

   Se nel repository sono presenti diversi pacchetti di aggiornamento di versioni diverse, è possibile aprire l'elenco a discesa per selezionare la versione desiderata.

5. Selezionare **Avanti**.
6. Selezionare **Avvia aggiornamento**.

Risultato

La pagina **Backends** visualizza lo stato **Upgrading** (aggiornamento) nella colonna **Status** (Stato) fino al completamento dell'aggiornamento.

Aggiunta di nodi a un cluster di storage back-end

È possibile aggiungere nodi a un cluster Astra Data Store, fino al numero di nodi supportati dal tipo di licenza installata per Astra Data Store.

Di cosa hai bisogno

- Un back-end di storage Astra Data Store distribuito e concesso in licenza
- È stato aggiunto il pacchetto software Astra Data Store in Astra Control Center
- Uno o più nuovi nodi da aggiungere al cluster

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.

2. Selezionare il nome di un backend di storage.
3. In Basic Information (informazioni di base), è possibile visualizzare il numero di nodi in questo cluster di back-end dello storage.
4. In **nodi**, selezionare l'icona di modifica accanto al numero di nodi.
5. Nella pagina **Add Nodes** (Aggiungi nodi), immettere le informazioni relative al nuovo nodo o ai nuovi nodi:
   a. Assegnare un'etichetta di nodo per ciascun nodo.
   b. Effettuare una delle seguenti operazioni:
      - Se si desidera che Astra Data Store utilizzi sempre il numero massimo di nodi disponibili in base alla licenza, attivare la casella di controllo **Usa sempre fino al numero massimo di nodi consentiti**.
      - Se non si desidera che Astra Data Store utilizzi sempre il numero massimo di nodi disponibili, selezionare il numero desiderato di nodi totali da utilizzare.
   c. Se è stato implementato Astra Data Store con i domini di protezione attivati, assegnare il nuovo nodo o i nuovi nodi ai domini di protezione.
6. Selezionare **Avanti**.
7. Inserire l'indirizzo IP e le informazioni di rete per ogni nuovo nodo. Inserire un singolo indirizzo IP per un singolo nodo o un pool di indirizzi IP per più nuovi nodi.

   Se Astra Data Store è in grado di utilizzare gli indirizzi IP configurati durante l'implementazione, non è necessario inserire alcuna informazione sull'indirizzo IP.

8. Selezionare **Avanti**.
9. Esaminare la configurazione del nuovo nodo o dei nuovi nodi.
10. Selezionare **Aggiungi nodi**.

Rimuovere i nodi da un cluster di back-end dello storage

È possibile rimuovere i nodi da un cluster Astra Data Store. Questi nodi possono essere integri o guasti.

La rimozione di un nodo da un cluster Astra Data Store sposta i dati in altri nodi del cluster e rimuove il nodo da Astra Data Store.

Il processo richiede le seguenti condizioni:

- Gli altri nodi devono disporre di spazio libero sufficiente per ricevere i dati.
- Nel cluster devono essere presenti 4 o più nodi.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il nome di un backend di storage.
3. Selezionare la scheda **nodi**.
4. Dal menu Actions (azioni), selezionare **Remove** (Rimuovi).
5. Confermare l'eliminazione immettendo "remove".
6. Selezionare **Sì, Rimuovi nodo**.

Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"

Monitorare l'infrastruttura con connessioni Cloud Insights e Fluentd

È possibile configurare diverse impostazioni opzionali per migliorare l'esperienza di Astra Control Center. Per monitorare e ottenere informazioni sulla tua infrastruttura completa, crea una connessione con NetApp Cloud Insights. Per raccogliere gli eventi Kubernetes dai sistemi monitorati da Astra Control Center, aggiungere una connessione Fluentd.

Se la rete in cui si utilizza Astra Control Center richiede un proxy per la connessione a Internet (per caricare pacchetti di supporto sul sito di supporto NetApp o stabilire una connessione a Cloud Insights), è necessario configurare un server proxy in Astra Control Center.

È inoltre possibile monitorare il throughput back-end, gli IOPS e la capacità dello storage Astra Data Store dalla pagina Storage Backend di Astra Control Center. Vedere "Gestire i back-end dello storage".

Aggiungere un server proxy per le connessioni a Cloud Insight o al NetApp Support Site

Se la rete in cui si utilizza Astra Control Center richiede un proxy per la connessione a Internet (per caricare pacchetti di supporto sul sito di supporto NetApp o stabilire una connessione a Cloud Insights), è necessario configurare un server proxy in Astra Control Center.

> Astra Control Center non convalida i dati immessi per il server proxy. Assicurarsi di immettere i valori corretti.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Connect** dall'elenco a discesa per aggiungere un server proxy.

4. Immettere il nome del server proxy o l'indirizzo IP e il numero della porta proxy.
5. Se il server proxy richiede l'autenticazione, selezionare la casella di controllo e immettere il nome utente e la password.
6. Selezionare **Connect**.

Risultato

Se le informazioni sul proxy inserite sono state salvate, la sezione **Proxy HTTP** della pagina **account** > **connessioni** indica che è connesso e visualizza il nome del server.

Modificare le impostazioni del server proxy

È possibile modificare le impostazioni del server proxy.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Edit** (Modifica) dall'elenco a discesa per modificare la connessione.
4. Modificare i dettagli del server e le informazioni di autenticazione.
5. Selezionare **Salva**.

Disattiva la connessione al server proxy

È possibile disattivare la connessione al server proxy. Prima di disattivare l'opzione, viene visualizzato un avviso che potrebbe causare interruzioni ad altre connessioni.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Disconnect** dall'elenco a discesa per disattivare la connessione.
4. Nella finestra di dialogo visualizzata, confermare l'operazione.

Connettersi a Cloud Insights

Per monitorare e ottenere informazioni sulla tua infrastruttura completa, collega NetApp Cloud Insights con la tua istanza del centro di controllo Astra. Cloud Insights è incluso nella licenza di Astra Control Center.

Cloud Insights deve essere accessibile dalla rete utilizzata dal centro di controllo Astra o indirettamente tramite un server proxy.

Quando il centro di controllo Astra è collegato a Cloud Insights, viene creato un pod unità di acquisizione. Questo pod raccoglie i dati dai back-end di storage gestiti dal centro di controllo Astra e li invia a Cloud Insights. Questo pod richiede 8 GB di RAM e 2 core CPU.

Inoltre, se gestisci i cluster di archiviazione dati Astra su Astra Control (connesso a Cloud Insights), viene creato un pod unità di acquisizione su Astra Data Store per ciascun cluster di archiviazione dati Astra e le metriche vengono inviate da Astra Data Store al sistema Cloud Insights associato. Ogni pod richiede 8 GB di RAM e 2 core della CPU.

Dopo aver attivato la connessione Cloud Insights, è possibile visualizzare le informazioni sul throughput nella pagina **backend** e connettersi a Cloud Insights da qui dopo aver selezionato un backend di storage. Le informazioni sono disponibili anche nella sezione cluster del pannello **Dashboard** e da qui è possibile connettersi a Cloud Insights.

Di cosa hai bisogno

- Un account Astra Control Center con privilegi **admin**/**owner**.
- Una licenza Astra Control Center valida.
- Un server proxy se la rete in cui si utilizza Astra Control Center richiede un proxy per la connessione a Internet.

Se sei un nuovo utente di Cloud Insights, familiarizza con le caratteristiche e le funzionalità. Vedere "Documentazione Cloud Insights".

Fasi

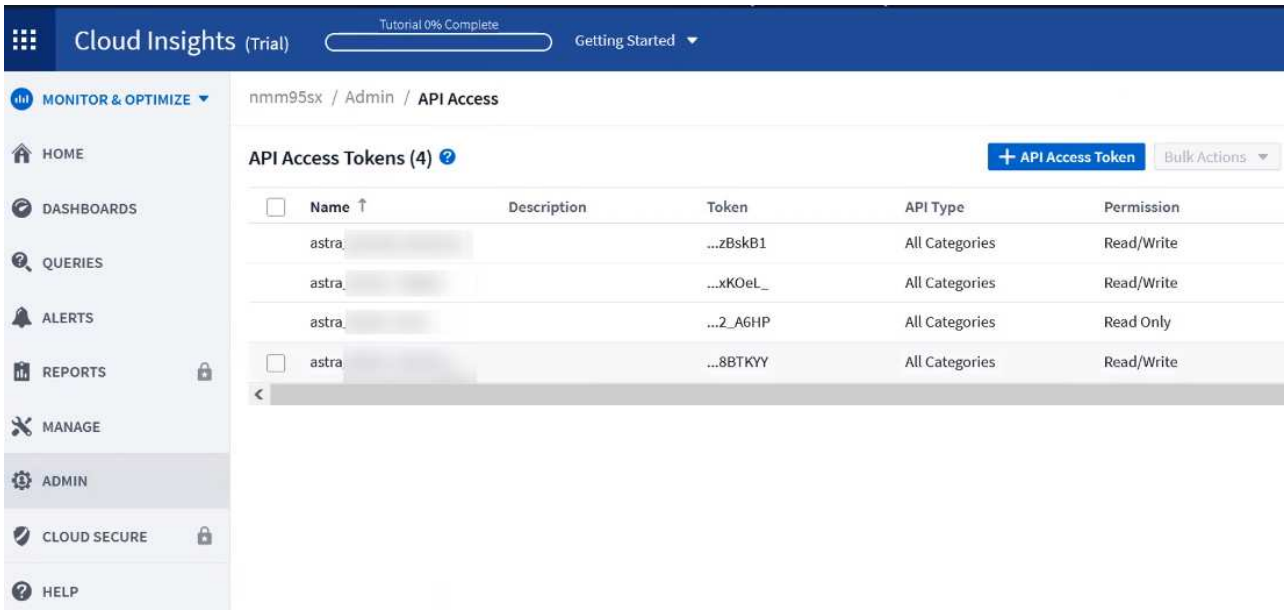
1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Connect** dove nell'elenco a discesa viene visualizzato **disconnected** per aggiungere la connessione.

4. Inserire i token API Cloud Insights e l'URL del tenant. L'URL del tenant ha il seguente formato, ad esempio:

```
https://<environment-name>.c01.cloudinsights.netapp.com/
```

Quando si ottiene la licenza Cloud Insights, si ottiene l'URL del tenant. Se non si dispone dell'URL del tenant, consultare "Documentazione Cloud Insights".

a. Per ottenere il "Token API", Accedere all'URL del tenant Cloud Insights.
b. In Cloud Insights, generare un token di accesso API **lettura/scrittura** e **sola lettura** facendo clic su **Amministratore** > **accesso API**.



c. Copiare la chiave **sola lettura**. Per attivare la connessione Cloud Insights, è necessario incollarla nella finestra di Astra Control Center. Per le autorizzazioni della chiave Read API Access Token, selezionare: Assets (risorse), Alerts (Avvisi), Acquisition Unit (unità di acquisizione) e Data Collection (raccolta dati).

d. Copiare la chiave **Read/Write**. È necessario incollarlo nella finestra di dialogo di Astra Control Center **Connect Cloud Insights**. Per le autorizzazioni della chiave del token di accesso API di lettura/scrittura, selezionare: Asset, acquisizione dati, acquisizione log, unità di acquisizione, E raccolta dati.

> Si consiglia di generare una chiave **Read Only** e una chiave **Read/Write** e di non utilizzare la stessa chiave per entrambi gli scopi. Per impostazione predefinita, il periodo di scadenza del token è impostato su un anno. Si consiglia di mantenere la selezione predefinita per assegnare al token la durata massima prima della scadenza. Se il token scade, la telemetria si interrompe.

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

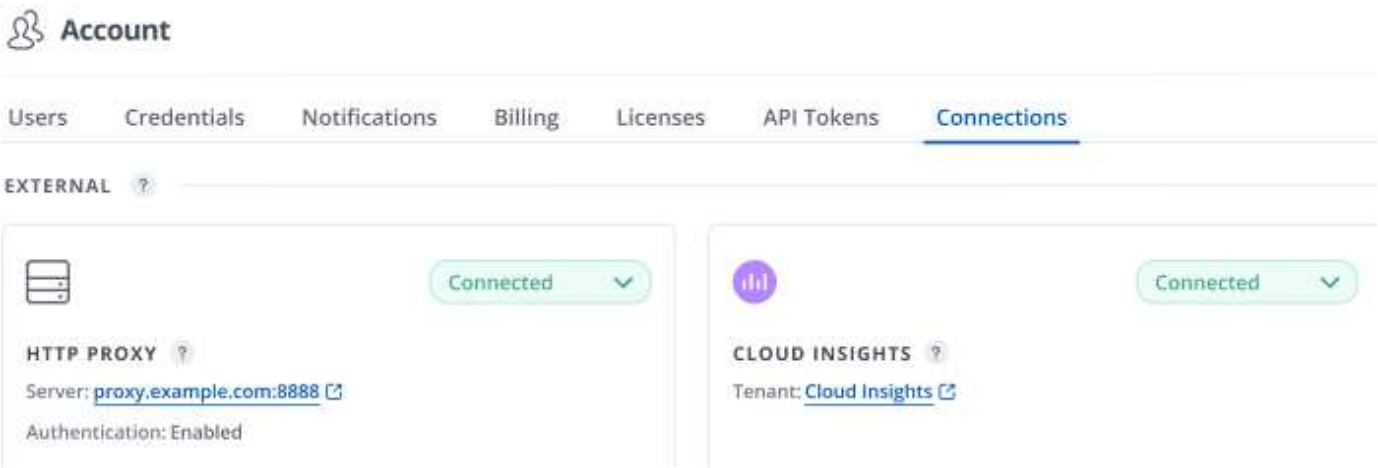
5. Selezionare **Connect**.

> Dopo aver selezionato **Connetti,** lo stato della connessione diventa **in sospeso** nella sezione **Cloud Insights** della pagina **account** > **connessioni**. L'attivazione della connessione e il passaggio allo stato **connesso** possono richiedere alcuni minuti.

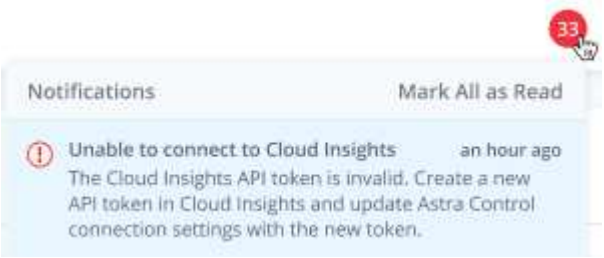
> Per passare facilmente da un'unità di controllo Astra a un'interfaccia utente Cloud Insights e viceversa, assicurarsi di aver effettuato l'accesso a entrambe.

Visualizzare i dati in Cloud Insights

Se la connessione ha avuto esito positivo, la sezione **Cloud Insights** della pagina **account** > **connessioni** indica che la connessione è stata stabilita e visualizza l'URL del tenant. È possibile visitare Cloud Insights per visualizzare e ricevere correttamente i dati.

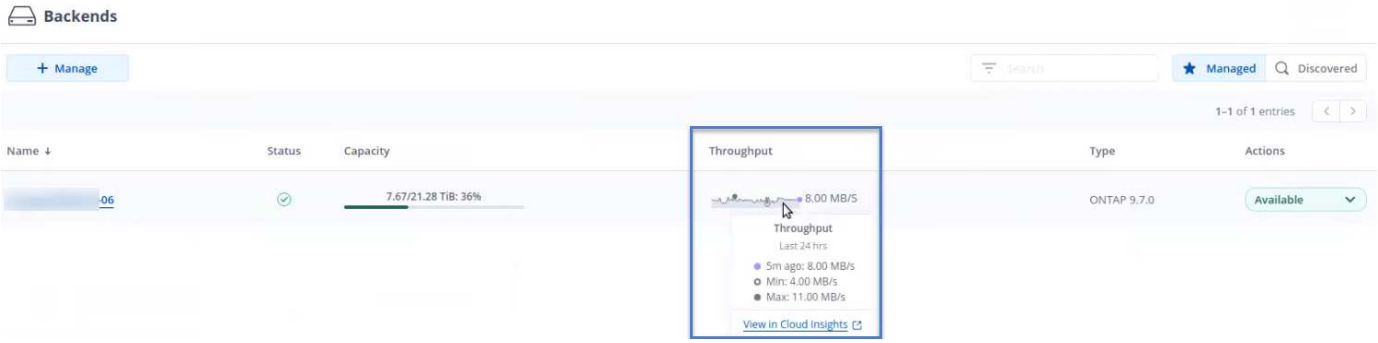


Se la connessione non è riuscita per qualche motivo, lo stato visualizza **Failed** (non riuscito). Il motivo del guasto è disponibile in **Notifiche** nella parte superiore destra dell'interfaccia utente.



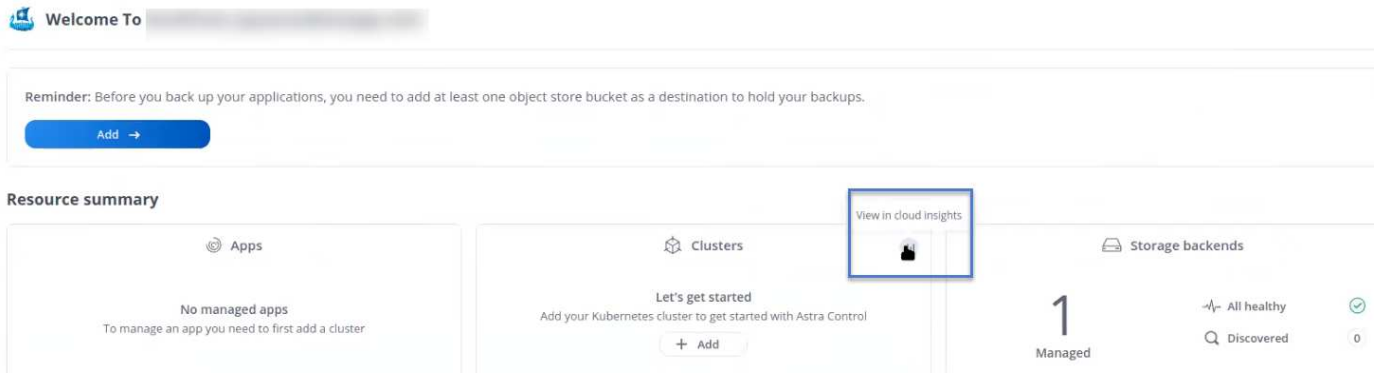
Le stesse informazioni sono disponibili anche in **account** > **Notifiche**.

Da Astra Control Center, è possibile visualizzare le informazioni sul throughput nella pagina **backend** e connettersi a Cloud Insights da qui dopo aver selezionato un backend di storage.



Per accedere direttamente a Cloud Insights, selezionare l'icona **Cloud Insights** accanto all'immagine delle metriche.

Le informazioni sono disponibili anche nella * Dashboard*.



Dopo aver attivato la connessione Cloud Insights, se si rimuovono i backend aggiunti in Centro di controllo Astra, i backend smettono di inviare i report a Cloud Insights.

Modificare la connessione Cloud Insights

È possibile modificare la connessione Cloud Insights.

È possibile modificare solo le chiavi API. Per modificare l'URL del tenant Cloud Insights, si consiglia di scollegare la connessione Cloud Insights e di connettersi al nuovo URL.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Edit** (Modifica) dall'elenco a discesa per modificare la connessione.
4. Modificare le impostazioni di connessione Cloud Insights.
5. Selezionare **Salva**.

Disattiva la connessione Cloud Insights

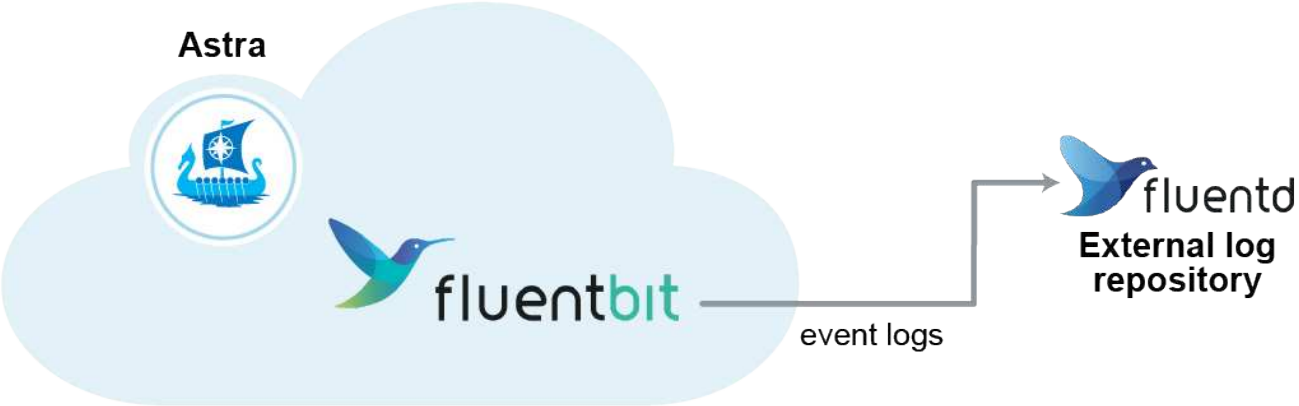
È possibile disattivare la connessione Cloud Insights per un cluster Kubernetes gestito da Astra Control Center. La disattivazione della connessione Cloud Insights non elimina i dati di telemetria già caricati su Cloud Insights.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Disconnect** dall'elenco a discesa per disattivare la connessione.
4. Nella finestra di dialogo visualizzata, confermare l'operazione. Dopo aver confermato l'operazione, nella pagina **account** > **connessioni**, lo stato Cloud Insights diventa **in sospeso**. Il passaggio allo stato **disconnesso** richiede alcuni minuti.

Connettersi a Fluentd

È possibile inviare registri (eventi Kubernetes) da Astra Control Center all'endpoint Fluentd. La connessione Fluentd è disattivata per impostazione predefinita.



A Fluentd vengono inoltrati solo i log degli eventi dei cluster gestiti.

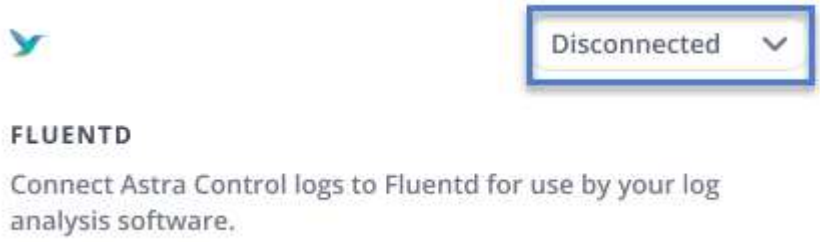
Di cosa hai bisogno

- Un account Astra Control Center con privilegi **admin**/**owner**.
- Astra Control Center installato e in esecuzione su un cluster Kubernetes.

Astra Control Center non convalida i dati immessi per il server Fluentd. Assicurarsi di immettere i valori corretti.

Fasi

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



4. Inserire l'indirizzo IP dell'host, il numero di porta e la chiave condivisa per il server Fluentd.
5. Selezionare **Connect**.

Risultato

Se i dati immessi per il server Fluentd sono stati salvati, la sezione **Fluentd** della pagina **account** > **connessioni** indica che è connesso. A questo punto, è possibile visitare il server Fluentd collegato e visualizzare i registri degli eventi.

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

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

In caso di problemi con la raccolta dei log, è necessario accedere al nodo di lavoro e assicurarsi che i log siano disponibili in `/var/log/containers/`.

Modificare la connessione Fluentd

È possibile modificare la connessione di Fluentd all'istanza di Astra Control Center.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Edit** (Modifica) dall'elenco a discesa per modificare la connessione.
4. Modificare le impostazioni dell'endpoint Fluentd.
5. Selezionare **Salva**.

Disattiva la connessione Fluentd

È possibile disattivare la connessione di Fluentd all'istanza di Astra Control Center.

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.
3. Selezionare **Disconnect** dall'elenco a discesa per disattivare la connessione.
4. Nella finestra di dialogo visualizzata, confermare l'operazione.

Annulla la gestione di app e cluster

Rimuovi le app o i cluster che non vuoi più gestire da Astra Control Center.

Annullare la gestione di un'applicazione

Smetta di gestire le app che non vuoi più eseguire il backup, lo snapshot o la clonazione da Astra Control Center.

- Eventuali backup e snapshot esistenti verranno eliminati.
- Le applicazioni e i dati rimangono disponibili.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **applicazioni**.
2. Selezionare la casella di controllo per le applicazioni che non si desidera più gestire.
3. Dal menu **azione**, selezionare **Annulla gestione**.
4. Digitare "unManage" per confermare.
5. Confermare che si desidera annullare la gestione delle applicazioni, quindi selezionare **Sì, Annulla gestione applicazione**.

Risultato

Astra Control Center interrompe la gestione dell'applicazione.

Annullare la gestione di un cluster

Annulla la gestione del cluster che non si desidera più gestire da Astra Control Center.

- Questa azione impedisce la gestione del cluster da parte di Astra Control Center. Non apporta modifiche alla configurazione del cluster e non elimina il cluster.
- Trident non verrà disinstallato dal cluster. "Scopri come disinstallare Trident".

> Prima di annullare la gestione del cluster, è necessario annullare la gestione delle applicazioni associate al cluster.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Clusters**.
2. Selezionare la casella di controllo del cluster che non si desidera più gestire in Astra Control Center.
3. Dal menu Opzioni nella colonna **azioni**, selezionare **Annulla gestione**.
4. Confermare che si desidera annullare la gestione del cluster, quindi selezionare **Sì, Annulla gestione cluster**.

Risultato

Lo stato del cluster cambia in **Removing** (Rimozione), quindi il cluster viene rimosso dalla pagina **Clusters** e non viene più gestito da Astra Control Center.

> **Se il centro di controllo Astra e Cloud Insights non sono connessi**, la disinstallazione del cluster rimuove tutte le risorse installate per l'invio dei dati di telemetria. **Se il centro di controllo Astra e Cloud Insights sono connessi**, la mancata gestione del cluster elimina solo il `fluentbit` e. `event-exporter` pod.

Aggiornare Astra Control Center

Per aggiornare Astra Control Center, scaricare il pacchetto di installazione dal NetApp Support Site e completare queste istruzioni per aggiornare i componenti di Astra Control Center nel proprio ambiente. È possibile utilizzare questa procedura per aggiornare Astra Control Center in ambienti connessi a Internet o con connessione ad aria.

Di cosa hai bisogno

- "Prima di iniziare l'aggiornamento, assicurarsi che l'ambiente soddisfi ancora i requisiti minimi per l'implementazione di Astra Control Center".
- Assicurarsi che tutti gli operatori del cluster siano in buono stato e disponibili.

```
kubectl get clusteroperators
```

- Assicurarsi che tutti i servizi API siano in buono stato e disponibili.

```
kubectl get apiservices
```

- Disconnettersi da Astra Control Center.

A proposito di questa attività

Il processo di aggiornamento di Astra Control Center ti guida attraverso le seguenti fasi di alto livello:

- Scarica il bundle Astra Control Center
- Disimballare il bundle e modificare la directory
- Aggiungere le immagini al registro locale
- Installare l'operatore Astra Control Center aggiornato
- Aggiornare Astra Control Center
- Upgrade dei servizi di terze parti (opzionale)
- Verificare lo stato del sistema
- Impostare l'ingresso per il bilanciamento del carico

Non eseguire il seguente comando durante l'intero processo di aggiornamento per evitare di eliminare tutti i pod di Astra Control Center: `kubectl delete -f astra_control_center_operator_deploy.yaml`

Eseguire gli aggiornamenti in una finestra di manutenzione quando pianificazioni, backup e snapshot non sono in esecuzione.

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

Scarica il bundle Astra Control Center

1. Scarica il bundle di aggiornamento di Astra Control Center (`astra-control-center-[version].tar.gz`) Dal sito di supporto https:mysupport.netapp.com/site/products/all/details/astra-control-center/downloads-tab[NetApp^].
2. (Facoltativo) utilizzare il seguente comando per verificare la firma del bundle:

```
openssl dgst -sha256 -verify AstraControlCenter-public.pub -signature
astra-control-center-[version].tar.gz.sig astra-control-center-
[version].tar.gz
```

Disimballare il bundle e modificare la directory

1. Estrarre le immagini:

```
tar -vxzf astra-control-center-[version].tar.gz
```

Aggiungere le immagini al registro locale

1. Completare la sequenza di passaggi appropriata per il motore dei container:

Docker

1. Passare alla directory Astra:

```
cd acc
```

2. inserire le immagini del pacchetto nella directory delle immagini di Astra Control Center nel registro locale. Eseguire le seguenti sostituzioni prima di eseguire il comando:
   - Sostituire BUNDLE_FILE con il nome del file bundle Astra Control (ad esempio, `acc.manifest.yaml`).
   - Sostituire MY_REGISTRY con l'URL del repository Docker.
   - Sostituire MY_REGISTRY_USER con il nome utente.
   - Sostituire MY_REGISTRY_TOKEN con un token autorizzato per il Registro di sistema.

```
kubectl astra packages push-images -m BUNDLE_FILE -r MY_REGISTRY
-u MY_REGISTRY_USER -p MY_REGISTRY_TOKEN
```

Podman

1. Accedere al Registro di sistema:

```
podman login [your_registry_path]
```

2. Eseguire il seguente script, eseguendo la sostituzione <YOUR_REGISTRY> come indicato nei commenti:

```
# You need to be at the root of the tarball.
# You should see these files to confirm correct location:
#   acc.manifest.yaml
#   acc/

# Replace <YOUR_REGISTRY> with your own registry (e.g
registry.customer.com or registry.customer.com/testing, etc..)
export REGISTRY=<YOUR_REGISTRY>
export PACKAGENAME=acc
export PACKAGEVERSION=22.08.1-26
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
  # Load to local cache
  astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image(s): //')

  # Remove path and keep imageName.
  astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')

  # Tag with local image repo.
  podman tag ${astraImage} ${REGISTRY}/netapp/astra/${PACKAGENAME}
/${PACKAGEVERSION}/${astraImageNoPath}

  # Push to the local repo.
  podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/
${PACKAGEVERSION}/${astraImageNoPath}
done
```

Installare l'operatore Astra Control Center aggiornato

1. Modificare la directory:

```
cd manifests
```

2. Modificare l'yaml di implementazione dell'operatore di Astra Control Center (`astra_control_center_operator_deploy.yaml`) per fare riferimento al registro locale e al segreto.

```
vim astra_control_center_operator_deploy.yaml
```

   a. Se si utilizza un registro che richiede l'autenticazione, sostituire la riga predefinita di `imagePullSecrets: []` con i seguenti elementi:

```
imagePullSecrets:
- name: <name_of_secret_with_creds_to_local_registry>
```

b. Cambiare `[your_registry_path]` per `kube-rbac-proxy` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

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

d. Aggiungere i seguenti valori a `env` sezione:

```
- name: ACCOP_HELM_UPGRADETIMEOUT
  value: 300m
```

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: [your_registry_path]/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        command:
        - /manager
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: [your_registry_path]/acc-operator:[version x.y.z]
        imagePullPolicy: IfNotPresent
      imagePullSecrets: []
```

3. Installare l’operatore Astra Control Center aggiornato:

```
kubectl apply -f astra_control_center_operator_deploy.yaml
```

Esempio di risposta:

```
namespace/netapp-acc-operator unchanged
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io configured
role.rbac.authorization.k8s.io/acc-operator-leader-election-role
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role
configured
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
unchanged
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role unchanged
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding unchanged
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding configured
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding unchanged
configmap/acc-operator-manager-config unchanged
service/acc-operator-controller-manager-metrics-service unchanged
deployment.apps/acc-operator-controller-manager configured
```

4. Verificare che i pod siano in esecuzione:

```
kubectl get pods -n netapp-acc-operator
```

Aggiornare Astra Control Center

1. Modificare la risorsa personalizzata di Astra Control Center (CR) (`astra_control_center_min.yaml`) E modificare la versione di Astra (`astraVersion` all'interno di `Spec`) al numero più recente:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

> Il percorso del Registro di sistema deve corrispondere al percorso del Registro di sistema in cui sono state inviate le immagini in a. passaggio precedente.

2. Aggiungere le seguenti righe all'interno di `additionalValues` all'interno di `Spec` In Astra Control Center CR:

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
```

3. Effettuare una delle seguenti operazioni:
   a. Se non si dispone di IngressController o ingresso personale e si utilizza Astra Control Center con il gateway Traefik come servizio di tipo LoadBalancer e si desidera continuare con l'installazione, specificare un altro campo `ingressType` (se non è già presente) e impostarlo su `AccTraefik`.

      ```
      ingressType: AccTraefik
      ```

   b. Se si desidera passare all'implementazione di ingresso generica di Astra Control Center predefinita, fornire la propria configurazione IngressController/Ingress (con terminazione TLS, ecc.), aprire un percorso per Astra Control Center e impostare `ingressType` a. `Generic`.

      ```
      ingressType: Generic
      ```

      Se si omette il campo, il processo diventa l'implementazione generica. Se non si desidera un'implementazione generica, assicurarsi di aggiungere il campo.

4. (Facoltativo) verificare che i pod terminino e diventino nuovamente disponibili:

   ```
   watch kubectl get po -n [netapp-acc or custom namespace]
   ```

5. Attendere che le condizioni di stato di Astra indichino che l'aggiornamento è completo e pronto:

   ```
   kubectl get -o yaml -n [netapp-acc or custom namespace]
   astracontrolcenters.astra.netapp.io astra
   ```

   Risposta:

```
conditions:
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Astra is deployed
    reason: Complete
    status: "True"
    type: Ready
  - lastTransitionTime: "2021-10-25T18:49:26Z"
    message: Upgrading succeeded.
    reason: Complete
    status: "False"
    type: Upgrading
```

6. Effettua nuovamente l'accesso e verifica che tutti i cluster e le applicazioni gestiti siano ancora presenti e protetti.
7. Se l'operatore non ha aggiornato il Cert-manager, aggiornare i servizi di terze parti, quindi.

Upgrade dei servizi di terze parti (opzionale)

I servizi di terze parti Traefik e Cert-manager non vengono aggiornati durante le fasi di aggiornamento precedenti. Se necessario, è possibile aggiornarli utilizzando la procedura descritta qui o conservare le versioni dei servizi esistenti.

- **Traefik**: Per impostazione predefinita, Astra Control Center gestisce il ciclo di vita dell'implementazione di Traefik. Impostazione `externalTraefik` a. `false` (Impostazione predefinita) indica che non esiste alcun Traefik esterno nel sistema e che Traefik viene installato e gestito da Astra Control Center. In questo caso, `externalTraefik` è impostato su `false`.

  D'altra parte, se si dispone di una propria implementazione Traefik, impostare `externalTraefik` a. `true`. In questo caso, si mantiene l'implementazione e Astra Control Center non aggiornerà i CRD, a meno che non sia `shouldUpgrade` è impostato su `true`.

- **Cert-manager**: Per impostazione predefinita, Astra Control Center installa il cert-manager (e i CRD), a meno che non sia stato impostato `externalCertManager` a. `true`. Impostare `shouldUpgrade` a. `true` Per fare in modo che Astra Control Center aggiorni i CRD.

Traefik viene aggiornato se viene soddisfatta una delle seguenti condizioni:

- ExternalTraefik: Falso
- ExternalTraefik: True E shouldUpgrade: True.

Fasi

1. Modificare il `acc` CR:

```
kubectl edit acc -n [netapp-acc or custom namespace]
```

2. Modificare il `externalTraefik` e il `shouldUpgrade` su entrambi i campi `true` oppure `false` in base alle necessità.

```
crds:
    externalTraefik: false
    externalCertManager: false
    shouldUpgrade: false
```

Verificare lo stato del sistema

1. Accedere ad Astra Control Center.
2. Verificare che tutti i cluster e le applicazioni gestiti siano ancora presenti e protetti.

Impostare l'ingresso per il bilanciamento del carico

È possibile impostare un oggetto Kubernetes Ingress che gestisca l'accesso esterno ai servizi, ad esempio il bilanciamento del carico in un cluster.

- L'aggiornamento predefinito utilizza l'implementazione di ingresso generica. In questo caso, sarà necessario anche configurare un controller di ingresso o una risorsa di ingresso.
- Se non si desidera un controller di ingresso e si desidera conservare ciò che si dispone già, impostare `ingressType` a. `AccTraefik`.

> Per ulteriori informazioni sul tipo di servizio "LoadBalancer" e sull'ingresso, vedere "Requisiti".

I passaggi variano a seconda del tipo di controller di ingresso utilizzato:

- Controller di ingresso nginx
- Controller di ingresso OpenShift

Di cosa hai bisogno

- Nella specifica CR,
  - Se `crd.externalTraefik` è presente, deve essere impostato su `false` OPPURE
  - Se `crd.externalTraefik` è `true`, `crd.shouldUpgrade` dovrebbe anche essere `true`.
- Il necessario "controller di ingresso" dovrebbe essere già implementato.
- Il "classe di ingresso" corrispondente al controller di ingresso dovrebbe già essere creato.
- Si stanno utilizzando versioni di Kubernetes comprese tra v1.19 e v1.21.

Procedura per il controller di ingresso Nginx

1. Utilizzare il segreto esistente `secure-testing-cert` oppure creare un segreto di tipo[`kubernetes.io/tls`] Per una chiave privata TLS e un certificato in `netapp-acc` (o con nome personalizzato) come descritto in "Segreti TLS".
2. Implementare una risorsa income in `netapp-acc` namespace (o personalizzato) per uno schema obsoleto o nuovo:
   a. Per uno schema obsoleto, seguire questo esempio:

```
apiVersion: extensions/v1beta1
kind: IngressClass
metadata:
  name: ingress-acc
  namespace: [netapp-acc or custom namespace]
  annotations:
    kubernetes.io/ingress.class: nginx
spec:
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: [ACC address]
    http:
      paths:
      - backend:
        serviceName: traefik
        servicePort: 80
        pathType: ImplementationSpecific
```

b. Per un nuovo schema, seguire questo esempio:

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: netapp-acc-ingress
  namespace: [netapp-acc or custom namespace]
spec:
  ingressClassName: [class name for nginx controller]
  tls:
  - hosts:
    - <ACC address>
    secretName: [tls secret name]
  rules:
  - host: <ACC address>
    http:
      paths:
        - path:
          backend:
            service:
              name: traefik
              port:
                number: 80
          pathType: ImplementationSpecific
```

Procedura per il controller di ingresso OpenShift

1. Procurarsi il certificato e ottenere la chiave, il certificato e i file CA pronti per l'uso con il percorso OpenShift.
2. Creare il percorso OpenShift:

```
oc create route edge --service=traefik
--port=web -n [netapp-acc or custom namespace]
--insecure-policy=Redirect --hostname=<ACC address>
--cert=cert.pem --key=key.pem
```

Verificare la configurazione dell'ingresso

È possibile verificare la configurazione dell'ingresso prima di continuare.

1. Assicurarsi che Traefik sia cambiato in `clusterIP` Da LoadBalancer:

```
kubectl get service traefik -n [netapp-acc or custom namespace]
```

2. Verificare i percorsi in Traefik:

```
Kubectl get ingressroute ingressroutetls -n [netapp-acc or custom
namespace]
-o yaml | grep "Host("
```

Il risultato deve essere vuoto.

Disinstallare Astra Control Center

Potrebbe essere necessario rimuovere i componenti di Astra Control Center se si esegue l'aggiornamento da una versione di prova a una versione completa del prodotto. Per rimuovere Astra Control Center e Astra Control Center Operator, eseguire i comandi descritti in questa procedura in sequenza.

In caso di problemi con la disinstallazione, vedere Risoluzione dei problemi di disinstallazione.

Di cosa hai bisogno

- Utilizzare l'interfaccia utente di Astra Control Center per annullare la gestione di tutto "cluster".

Fasi

1. Eliminare Astra Control Center. Il seguente comando di esempio si basa su un'installazione predefinita. Modificare il comando se sono state create configurazioni personalizzate.

   ```
   kubectl delete -f astra_control_center_min.yaml -n netapp-acc
   ```

   Risultato:

   ```
   astracontrolcenter.astra.netapp.io "astra" deleted
   ```

2. Utilizzare il seguente comando per eliminare `netapp-acc` spazio dei nomi:

   ```
   kubectl delete ns netapp-acc
   ```

   Risultato:

   ```
   namespace "netapp-acc" deleted
   ```

3. Utilizzare il seguente comando per eliminare i componenti del sistema dell'operatore di Astra Control Center:

   ```
   kubectl delete -f astra_control_center_operator_deploy.yaml
   ```

   Risultato:

```
namespace/netapp-acc-operator deleted
customresourcedefinition.apiextensions.k8s.io/astracontrolcenters.astra.
netapp.io deleted
role.rbac.authorization.k8s.io/acc-operator-leader-election-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-manager-role deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-metrics-reader
deleted
clusterrole.rbac.authorization.k8s.io/acc-operator-proxy-role deleted
rolebinding.rbac.authorization.k8s.io/acc-operator-leader-election-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-manager-
rolebinding deleted
clusterrolebinding.rbac.authorization.k8s.io/acc-operator-proxy-
rolebinding deleted
configmap/acc-operator-manager-config deleted
service/acc-operator-controller-manager-metrics-service deleted
deployment.apps/acc-operator-controller-manager deleted
```

Risoluzione dei problemi di disinstallazione

Utilizzare le seguenti soluzioni alternative per risolvere eventuali problemi riscontrati durante la disinstallazione di Astra Control Center.

La disinstallazione di Astra Control Center non riesce a pulire il pod operatore di monitoraggio sul cluster gestito

Se i cluster non sono stati disgestiti prima della disinstallazione di Astra Control Center, è possibile eliminare manualmente i pod nello spazio dei nomi di monitoraggio netapp e nello spazio dei nomi con i seguenti comandi:

Fasi

1. Eliminare `acc-monitoring` agente:

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

   Risultato:

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

2. Eliminare lo spazio dei nomi:

   ```
   kubectl delete ns netapp-monitoring
   ```

Risultato:

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

3. Conferma la rimozione delle risorse:

```
kubectl get pods -n netapp-monitoring
```

Risultato:

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

4. Conferma rimozione dell'agente di monitoraggio:

```
kubectl get crd|grep agent
```

Risultato del campione:

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

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

```
kubectl delete crds agents.monitoring.netapp.com
```

Risultato:

```
customresourcedefinition.apiextensions.k8s.io
"agents.monitoring.netapp.com" deleted
```

La disinstallazione di Astra Control Center non consente di eliminare i CRD Traefik

È possibile eliminare manualmente i CRD Traefik. Le CRDS sono risorse globali e l'eliminazione di queste risorse potrebbe avere un impatto sulle altre applicazioni del cluster.

Fasi

1. Elencare i CRD Traefik installati sul cluster:

```
kubectl get crds |grep -E 'traefik'
```

Risposta

```
ingressroutes.traefik.containo.us             2021-06-23T23:29:11Z
ingressroutetcps.traefik.containo.us          2021-06-23T23:29:11Z
ingressrouteudps.traefik.containo.us          2021-06-23T23:29:12Z
middlewares.traefik.containo.us               2021-06-23T23:29:12Z
middlewaretcps.traefik.containo.us            2021-06-23T23:29:12Z
serverstransports.traefik.containo.us         2021-06-23T23:29:13Z
tlsoptions.traefik.containo.us                2021-06-23T23:29:13Z
tlsstores.traefik.containo.us                 2021-06-23T23:29:14Z
traefikservices.traefik.containo.us           2021-06-23T23:29:15Z
```

2. Eliminare i CRD:

```
kubectl delete crd ingressroutes.traefik.containo.us
ingressroutetcps.traefik.containo.us
ingressrouteudps.traefik.containo.us middlewares.traefik.containo.us
serverstransports.traefik.containo.us tlsoptions.traefik.containo.us
tlsstores.traefik.containo.us traefikservices.traefik.containo.us
middlewaretcps.traefik.containo.us
```

Trova ulteriori informazioni

- "Problemi noti per la disinstallazione"