



# Utilizzare Astra Control Service

## Astra Control Service

NetApp  
June 04, 2024

# Sommario

- Utilizzare Astra Control Service ..... 1
  - Accedere a Astra Control Service ..... 1
  - Gestire e proteggere le applicazioni..... 1
  - Visualizza lo stato di salute delle applicazioni e del calcolo..... 41
  - Gestire i bucket ..... 43
  - Monitorare le attività in esecuzione ..... 48
  - Gestisci il tuo account ..... 48
  - Gestire le istanze cloud ..... 58
  - Abilita Astra Control Provisioner..... 58
  - Annulla la gestione di app e cluster ..... 67
  - Implementa un'istanza autogestita di Astra Control..... 69

# Utilizzare Astra Control Service

## Accedere a Astra Control Service

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



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

### Prima di iniziare

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

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

### Fasi

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

## Gestire e proteggere le applicazioni

### Inizia a gestire le app

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

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

### Requisiti di gestione delle applicazioni

Astra Control ha i seguenti requisiti di gestione delle applicazioni:

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

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

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

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

## Metodi di installazione delle applicazioni supportati

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

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

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

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

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

- ["Apache K8ssandra"](#)



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

- ["Ci Jenkins"](#)
- ["Cluster XtraDB Percona"](#)

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

## Installa le app sul tuo cluster

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

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

- ["Scopri le classi di storage per i cluster GKE"](#)
- ["Scopri le classi di storage per i cluster AKS"](#)
- ["Scopri le classi di storage per i cluster AWS"](#)

## Definire le applicazioni

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

Sebbene Astra Control ti consenta di gestire separatamente entrambi i livelli della gerarchia (lo spazio dei nomi e le applicazioni nello spazio dei nomi o negli spazi dei nomi), la Best practice è scegliere uno o l'altro. Le azioni eseguite in Astra Control possono non riuscire se vengono eseguite contemporaneamente sia a livello di spazio dei nomi che di applicazione.



Ad esempio, è possibile impostare una policy di backup per "maria" con cadenza settimanale, ma potrebbe essere necessario eseguire il backup di "mariadb" (che si trova nello stesso namespace) con maggiore frequenza. In base a tali esigenze, sarebbe necessario gestire le applicazioni separatamente e non come un'applicazione con un singolo spazio dei nomi.

## Prima di iniziare

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



Un'etichetta è una coppia chiave/valore che è possibile assegnare agli oggetti Kubernetes per l'identificazione. Le etichette semplificano l'ordinamento, l'organizzazione e la ricerca degli oggetti Kubernetes. Per ulteriori informazioni sulle etichette Kubernetes, ["Consultare la documentazione ufficiale di Kubernetes"](#).

## A proposito di questa attività

- Prima di iniziare, dovresti anche capire ["gestione degli spazi dei nomi standard e di sistema"](#).

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

### Opzioni di gestione delle applicazioni

- [Definire le risorse da gestire come applicazione](#)
- [Definire uno spazio dei nomi da gestire come applicazione](#)

### Definire le risorse da gestire come applicazione

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

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



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

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

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

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

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

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

### Fasi

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

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



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

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



Per ulteriori informazioni sulle etichette Kubernetes, "[Consultare la documentazione ufficiale di Kubernetes](#)".

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



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

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

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



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



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

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

### Definire uno spazio dei nomi da gestire come applicazione

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

#### Fasi

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



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



Selezionare la casella di controllo **Show system namespace** (Mostra spazi dei nomi di sistema) per visualizzare gli spazi dei nomi di sistema solitamente non utilizzati nella

gestione delle applicazioni per impostazione predefinita.

Show system namespaces

["Scopri di più"](#).

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

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

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

#### Fasi

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



## spec.includedClusterScopedResources

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

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

## spec.includedNamespaces

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

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

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

Esempio YAML:

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

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

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

## E gli spazi dei nomi di sistema?

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

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



Astra Control non è un'applicazione standard, ma un'applicazione di sistema. Non si dovrebbe tentare di gestire Astra Control da solo. Per impostazione predefinita, Astra Control non viene visualizzato per la gestione.

## Proteggi le app con snapshot e backup

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

Scopri di più "[Protezione dei dati in Astra Control](#)".

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

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

### Configurare un criterio di protezione

Una policy di protezione protegge un'applicazione creando snapshot, backup o entrambi in base a una pianificazione definita. È possibile scegliere di creare snapshot e backup ogni ora, ogni giorno, ogni settimana e ogni mese, nonché specificare il numero di copie da conservare. È possibile definire un criterio di protezione utilizzando l'interfaccia utente Web Astra Control o un file di risorse personalizzato (CR).

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



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



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

## Configurare un criterio di protezione utilizzando l'interfaccia utente Web

### Fasi

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

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

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

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

[Schermata di una policy di configurazione di esempio in cui è possibile scegliere di eseguire snapshot e backup su base oraria, giornaliera, settimanale o mensile.]

5. **[Tech preview]** Scegliete un bucket di destinazione per i backup o le istantanee dall'elenco dei bucket di storage.
6. Selezionare **Revisione**.
7. Selezionare **Imposta policy di protezione**.

## [Anteprima tecnica] configurare un criterio di protezione utilizzando una CR

### Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-schedule-cr.yaml`. Aggiorna i valori tra parentesi `<>` per soddisfare le tue esigenze di ambiente Astra Control, configurazione del cluster e protezione dei dati:
  - `<CR_NAME>`: Il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per l'ambiente.
  - `<APPLICATION_NAME>`: Il nome Kubernetes dell'applicazione di cui eseguire il backup.
  - `<APPVAULT_NAME>`: Il nome dell'AppVault in cui devono essere memorizzati i contenuti di backup.
  - `<BACKUPS_RETAINED>`: Il numero di backup da conservare. Zero indica che non è necessario creare backup.
  - `<SNAPSHOTS_RETAINED>`: Il numero di snapshot da conservare. Zero indica che non è necessario creare snapshot.
  - `<GRANULARITY>` (frequenza): La frequenza di esecuzione della pianificazione. Valori possibili, insieme ai campi associati obbligatori:
    - `hourly` (richiede di specificare `spec.minute`)
    - `daily` (richiede di specificare `spec.minute` e `spec.hour`)
    - `weekly` (richiede di specificare `spec.minute`, `spec.hour`, e `spec.dayOfWeek`)
    - `monthly` (richiede di specificare `spec.minute`, `spec.hour`, e `spec.dayOfMonth`)

- <DAY\_OF\_MONTH>: (*facoltativo*) il giorno del mese (1 - 31) in cui deve essere eseguito il programma. Questo campo è obbligatorio se la granularità è impostata su `monthly`.
- <DAY\_OF\_WEEK>: (*opzionale*) il giorno della settimana (0 - 7) in cui dovrebbe essere eseguito il programma. I valori di 0 o 7 indicano la domenica. Questo campo è obbligatorio se la granularità è impostata su `weekly`.
- <HOUR\_OF\_DAY>: (*opzionale*) l'ora del giorno (0 - 23) in cui deve essere eseguito il programma. Questo campo è obbligatorio se la granularità è impostata su `daily`, `weekly`, o `monthly`.
- <MINUTE\_OF\_HOUR>: (*opzionale*) il minuto dell'ora (0 - 59) che la programmazione dovrebbe essere eseguita. Questo campo è obbligatorio se la granularità è impostata su `hourly`, `daily`, `weekly`, o `monthly`.

```

apiVersion: astra.netapp.io/v1
kind: Schedule
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  backupRetention: "<BACKUPS_RETAINED>"
  snapshotRetention: "<SNAPSHOTS_RETAINED>"
  granularity: <GRANULARITY>
  dayOfMonth: "<DAY_OF_MONTH>"
  dayOfWeek: "<DAY_OF_WEEK>"
  hour: "<HOUR_OF_DAY>"
  minute: "<MINUTE_OF_HOUR>"

```

2. Dopo aver popolato il `astra-control-schedule-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-schedule-cr.yaml
```

## Risultato

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

## Creare un'istantanea

Puoi creare uno snapshot on-demand in qualsiasi momento.

## A proposito di questa attività

Astra Control supporta la creazione di snapshot utilizzando classi di storage supportate dai seguenti driver:

- `ontap-nas`

- `ontap-san`
- `ontap-san-economy`



Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, impossibile creare snapshot. Utilizzare una classe di storage alternativa per gli snapshot.

## Creare un'istantanea utilizzando l'interfaccia utente Web

### Fasi

1. Selezionare **applicazioni**.
2. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) dell'applicazione desiderata, selezionare **Snapshot**.
3. Personalizzare il nome dell'istantanea, quindi selezionare **Avanti**.
4. **[Tech preview]** Scegli un bucket di destinazione per l'istantanea dall'elenco dei bucket di storage.
5. Esaminare il riepilogo dell'istantanea e selezionare **Snapshot**.

### [Anteprima tecnica] Crea un'istantanea utilizzando una CR

#### Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-snapshot-cr.yaml`. Aggiorna i valori tra parentesi `<>` per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
  - `<CR_NAME>`: Il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per l'ambiente.
  - `<APPLICATION_NAME>`: Il nome Kubernetes dell'applicazione da snapshot.
  - `<APPVAULT_NAME>`: Il nome dell'AppVault in cui devono essere memorizzati i contenuti dello snapshot.
  - `<RECLAIM_POLICY>`: (*opzionale*) definisce cosa accade a uno snapshot quando lo snapshot CR viene eliminato. Opzioni valide:
    - Retain
    - Delete (impostazione predefinita)

```
apiVersion: astra.netapp.io/v1
kind: Snapshot
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
  reclaimPolicy: <RECLAIM_POLICY>
```

2. Dopo aver popolato il `astra-control-snapshot-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-snapshot-cr.yaml
```

### Risultato

Viene avviato il processo di snapshot. Un'istantanea ha successo quando lo stato è **integro** nella colonna

## Creare un backup

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



Tenere presente come viene gestito lo spazio di storage quando si esegue il backup di un'applicazione ospitata sullo storage Azure NetApp Files. Fare riferimento a ["Backup delle applicazioni"](#) per ulteriori informazioni.

Astra Control supporta la creazione di backup utilizzando classi di storage supportate dai seguenti driver:



- `ontap-nas`
- `ontap-nas-economy`
- `ontap-san`
- `ontap-san-economy`

### A proposito di questa attività

I bucket in Astra Control non riportano la capacità disponibile. Prima di eseguire il backup o il cloning delle applicazioni gestite da Astra Control, controllare le informazioni del bucket nel sistema di gestione dello storage appropriato.

Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, è necessario [attivare il backup e il ripristino](#) funzionalità. Accertarsi di aver definito un `backendType` nel ["Oggetto storage Kubernetes"](#) con un valore di `ontap-nas-economy` prima di eseguire qualsiasi operazione di protezione.



## Creare un backup utilizzando l'interfaccia utente Web

### Fasi

1. Selezionare **applicazioni**.
2. Dal menu Opzioni nella colonna **azioni** dell'applicazione desiderata, selezionare **Backup**.
3. Personalizzare il nome del backup.
4. Scegliere se eseguire il backup dell'applicazione da uno snapshot esistente. Se si seleziona questa opzione, è possibile scegliere da un elenco di snapshot esistenti.
5. **[Tech preview]** Scegli un bucket di destinazione per il backup dall'elenco dei bucket di storage.
6. Selezionare **Avanti**.
7. Esaminare il riepilogo del backup e selezionare **Backup**.

### [Anteprima tecnica] creare un backup utilizzando una CR

#### Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-backup-cr.yaml`. Aggiorna i valori tra parentesi `<>` per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:
  - `<CR_NAME>`: Il nome di questa risorsa personalizzata; scegliere un nome univoco e sensibile per l'ambiente.
  - `<APPLICATION_NAME>`: Il nome Kubernetes dell'applicazione di cui eseguire il backup.
  - `<APPVAULT_NAME>`: Il nome dell'AppVault in cui devono essere memorizzati i contenuti di backup.

```
apiVersion: astra.netapp.io/v1
kind: Backup
metadata:
  namespace: astra-connector
  name: <CR_NAME>
spec:
  applicationRef: <APPLICATION_NAME>
  appVaultRef: <APPVAULT_NAME>
```

2. Dopo aver popolato il `astra-control-backup-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-backup-cr.yaml
```

### Risultato

Astra Control crea un backup dell'applicazione.



- Se la rete presenta un'interruzione o è eccessivamente lenta, potrebbe verificarsi un timeout dell'operazione di backup. In questo modo, il backup non viene eseguito correttamente.
- Per annullare un backup in esecuzione, seguire le istruzioni riportate in [Annullare i backup](#). Per eliminare il backup, attendere il completamento, quindi seguire le istruzioni riportate in [Eliminare i backup](#).
- Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

### **Abilita backup e ripristino per le operazioni economiche a ontap-nas**

Astra Control Provisioner fornisce funzionalità di backup e ripristino che possono essere abilitate per i backend di storage che stanno utilizzando `ontap-nas-economy` classe di storage.

#### **Prima di iniziare**

- Hai abilitato Astra Control provisioner o Astra Trident.
- Hai definito un'applicazione in Astra Control. Questa applicazione dispone di funzionalità di protezione limitate fino al completamento di questa procedura.
- Lo hai fatto `ontap-nas-economy` selezionata come classe di archiviazione predefinita per il backend di archiviazione.

## Espandere per la procedura di configurazione

### 1. Sul back-end dello storage ONTAP:

- Trova la SVM che ospita `ontap-nas-economy` volumi basati su -dell'applicazione.
- Accedere a un terminale connesso a ONTAP in cui vengono creati i volumi.
- Nascondi la directory snapshot per la SVM:



Questo cambiamento influisce sull'intera SVM. La directory nascosta continuerà ad essere accessibile.

```
nfs modify -vserver <svm name> -v3-hide-snapshot enabled
```

+



Verificare che la directory snapshot sul backend di archiviazione ONTAP sia nascosta. La mancata visualizzazione di questa directory potrebbe causare la perdita di accesso all'applicazione, in particolare se si utilizza NFSv3.

### 2. Esegui le seguenti operazioni in Astra Control Provisioner o Astra Trident:

- Abilitare la directory Snapshot per ogni PV in base a ontap-nas-Economy e associata all'applicazione:

```
tridentctl update volume <pv name> --snapshot-dir=true --pool  
-level=true -n trident
```

- Confermare che la directory snapshot è stata abilitata per ogni PV associato:

```
tridentctl get volume <pv name> -n trident -o yaml | grep  
snapshotDir
```

Risposta:

```
snapshotDirectory: "true"
```

- In Astra Control, aggiorna l'applicazione dopo aver abilitato tutte le directory di snapshot associate, in modo che Astra Control riconosca il valore modificato.

### Risultato

L'applicazione è pronta per il backup e il ripristino utilizzando Astra Control. Ciascun PVC è inoltre disponibile per essere utilizzato da altre applicazioni per backup e ripristini.

## Creare un backup immutabile

Un backup immutabile non può essere modificato, eliminato o sovrascritto se la politica di conservazione nel bucket che archivia il backup lo vieta. Puoi creare backup immutabili eseguendo il backup delle applicazioni in bucket che hanno configurato un criterio di conservazione. Fare riferimento a ["Protezione dei dati"](#) per informazioni importanti sull'utilizzo dei backup immutabili.

### Prima di iniziare

È necessario configurare il bucket di destinazione con un criterio di conservazione. La scelta varia in base al provider di storage utilizzato. Per ulteriori informazioni, consultare la documentazione del provider di storage:

- **Amazon Web Services:** ["Abilitare il blocco degli oggetti S3 durante la creazione del bucket e impostare una modalità di conservazione predefinita di "governance" con un periodo di conservazione predefinito"](#).
- **Google Cloud:** ["Configurare un bucket con un criterio di conservazione e specificare un periodo di conservazione"](#).
- **Microsoft Azure:** ["Configurare un bucket storage BLOB con una politica di conservazione basata sul tempo sull'ambito a livello di container"](#).
- **NetApp StorageGRID:** ["Abilitare blocco oggetto S3 durante la creazione del bucket e impostare una modalità di conservazione predefinita di "conformità" con un periodo di conservazione predefinito"](#).



I bucket in Astra Control non riportano la capacità disponibile. Prima di eseguire il backup o il cloning delle applicazioni gestite da Astra Control, controllare le informazioni del bucket nel sistema di gestione dello storage appropriato.



Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, assicurarsi di aver definito un `backendType` nel ["Oggetto storage Kubernetes"](#) con un valore di `ontap-nas-economy` prima di eseguire qualsiasi operazione di protezione.

### Fasi

1. Selezionare **applicazioni**.
2. Dal menu Opzioni nella colonna **azioni** dell'applicazione desiderata, selezionare **Backup**.
3. Personalizzare il nome del backup.
4. Scegliere se eseguire il backup dell'applicazione da uno snapshot esistente. Se si seleziona questa opzione, è possibile scegliere da un elenco di snapshot esistenti.
5. Scegliere un bucket di destinazione per il backup dall'elenco dei bucket di storage. Un bucket WORM (Write Once Read Many) viene indicato con lo stato "bloccato" accanto al nome del bucket.



Se la benna è di tipo non supportato, ciò viene indicato quando si passa il mouse o si seleziona la benna.

6. Selezionare **Avanti**.
7. Esaminare il riepilogo del backup e selezionare **Backup**.

### Risultato

Astra Control crea un backup immutabile dell'app.



- Se la rete presenta un'interruzione o è eccessivamente lenta, potrebbe verificarsi un timeout dell'operazione di backup. In questo modo, il backup non viene eseguito correttamente.
- Se provi a creare due backup immutabili della stessa app nello stesso bucket contemporaneamente, Astra Control impedisce l'avvio del secondo backup. Attendere il completamento del primo backup prima di avviarne un altro.
- Non è possibile annullare un backup immutabile in esecuzione.
- Dopo un'operazione di protezione dei dati (clone, backup, ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo di venti minuti prima che le nuove dimensioni del volume vengano visualizzate nell'interfaccia utente. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.

## Visualizzare snapshot e backup

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



Un backup immutabile viene indicato con lo stato "bloccato" accanto al bucket in uso.

### Fasi

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

Le istantanee vengono visualizzate per impostazione predefinita.

3. Selezionare **Backup** per fare riferimento all'elenco dei backup.

## Eliminare le istantanee

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

### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare **Data Protection** (protezione dati).
3. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per lo snapshot desiderato, selezionare **Delete snapshot** (Elimina snapshot).
4. Digitare la parola "DELETE" per confermare l'eliminazione, quindi selezionare **Yes, Delete snapshot**.

### Risultato

Astra Control elimina lo snapshot.

## Annullare i backup

È possibile annullare un backup in corso.



Per annullare un backup, il backup deve essere in `Running` stato. Non è possibile annullare un backup in `Pending` stato.



Non è possibile annullare un backup immutabile in esecuzione.

### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Backup**.
4. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per il backup desiderato, selezionare **Cancel** (Annulla).
5. Digitare la parola "CANCEL" per confermare l'operazione, quindi selezionare **Yes, CANCEL backup** (Sì, Annulla backup\*).

### Eliminare i backup

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



Per annullare un backup in esecuzione, seguire le istruzioni riportate in [Annullare i backup](#). Per eliminare il backup, attendere che sia stato completato, quindi seguire queste istruzioni.



Non è possibile eliminare un backup immutabile prima della scadenza del periodo di conservazione.

### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Backup**.
4. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per il backup desiderato, selezionare **Delete backup** (Elimina backup).
5. Digitare la parola "DELETE" per confermare l'eliminazione, quindi selezionare **Yes, Delete backup**.

### Risultato

Astra Control elimina il backup.

## [Anteprima tecnica] proteggi un intero cluster

È possibile creare un backup pianificato e automatico di uno o di tutti gli spazi dei nomi non gestiti su un cluster. Questi workflow sono forniti da NetApp as a Kubernetes Service account, binding di ruolo e un job cron, orchestrato con uno script Python.

### Come funziona

Quando si configura e installa il flusso di lavoro del backup completo del cluster, un processo cron viene eseguito periodicamente e protegge qualsiasi namespace non ancora gestito, creando automaticamente criteri di protezione in base alle pianificazioni scelte durante l'installazione.

Se non si desidera proteggere ogni spazio dei nomi non gestito sul cluster con l'intero flusso di lavoro di backup del cluster, è possibile utilizzare invece il flusso di lavoro di backup basato su etichette. Il flusso di lavoro di backup basato su etichetta utilizza anche un task cron, ma invece di proteggere tutti i namespace non

gestiti, identifica i namespace in base alle etichette fornite per proteggere facoltativamente i namespace in base a policy di backup Bronze, Silver o Gold.

Quando viene creato un nuovo namespace che rientra nell'ambito del flusso di lavoro scelto, viene automaticamente protetto, senza alcun intervento dell'amministratore. Questi flussi di lavoro vengono implementati per ogni cluster in modo che cluster diversi possano utilizzare entrambi i flussi di lavoro con livelli di protezione unici, a seconda dell'importanza del cluster.

### **Esempio: Protezione completa del cluster**

Ad esempio, quando configuri e installi l'intero workflow di backup del cluster, tutte le applicazioni in qualsiasi namespace vengono periodicamente gestite e protette senza ulteriori interventi da parte dell'amministratore. Lo spazio dei nomi non deve esistere al momento dell'installazione del flusso di lavoro; se in futuro viene aggiunto uno spazio dei nomi, verrà protetto.

### **Esempio: Protezione basata sull'etichetta**

Per una maggiore granularità, è possibile utilizzare il flusso di lavoro basato su etichette. Ad esempio, è possibile installare questo flusso di lavoro e dire agli utenti di applicare una delle diverse etichette a qualsiasi namespace che desiderano proteggere, a seconda del livello di protezione necessario. In questo modo, gli utenti possono creare lo spazio dei nomi con una di queste etichette e non devono inviare notifiche a un amministratore. Il nuovo namespace e tutte le applicazioni all'interno dell'IT sono protetti automaticamente.

## **Creare un backup pianificato di tutti gli spazi dei nomi**

È possibile creare un backup pianificato di tutti i namespace in un cluster utilizzando il flusso di lavoro di backup completo del cluster.

### **Fasi**

1. Scaricare i seguenti file su un computer con accesso di rete al cluster:
  - ["File CRD Components.yaml"](#)
  - ["protectCluster.py script Python"](#)
2. Per configurare e installare il toolkit, ["seguire le istruzioni incluse"](#).

## **Creare un backup pianificato di spazi dei nomi specifici**

È possibile creare un backup pianificato di spazi dei nomi specifici mediante le relative etichette utilizzando il flusso di lavoro di backup basato su etichette.

### **Fasi**

1. Scaricare i seguenti file su un computer con accesso di rete al cluster:
  - ["File CRD Components.yaml"](#)
  - ["protectCluster.py script Python"](#)
2. Per configurare e installare il toolkit, ["seguire le istruzioni incluse"](#).

## **Ripristinare le applicazioni**

Astra Control può ripristinare l'applicazione da uno snapshot o da un backup. Il ripristino da uno snapshot esistente sarà più rapido quando si ripristina l'applicazione nello stesso cluster. È possibile utilizzare l'interfaccia utente di Astra Control o ["L'API Astra Control"](#) per ripristinare le applicazioni.



Se si aggiunge un filtro dello spazio dei nomi a un gancio di esecuzione che viene eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o del clone si trovano in spazi dei nomi diversi, il filtro dello spazio dei nomi viene applicato solo allo spazio dei nomi di destinazione.

## Prima di iniziare

- **Proteggi prima le tue applicazioni:** Ti consigliamo vivamente di creare un'istantanea o un backup dell'applicazione prima di ripristinarla. Ciò consente di clonare dallo snapshot o dal backup se il ripristino non ha avuto esito positivo.
- **Check destination Volumes** (Controlla volumi di destinazione): Se si esegue il ripristino in una classe di storage diversa, assicurarsi che la classe di storage utilizzi la stessa modalità di accesso al volume persistente (ad esempio ReadWriteMany). L'operazione di ripristino non riesce se la modalità di accesso al volume persistente di destinazione è diversa. Ad esempio, se il volume persistente di origine utilizza la modalità di accesso RWX, selezionare una classe di storage di destinazione che non è in grado di fornire RWX, come Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, causa l'errore dell'operazione di ripristino. Per ulteriori informazioni sulle modalità di accesso al volume persistente, fare riferimento a ["Kubernetes"](#) documentazione.
- **Pianificare le esigenze di spazio:** Quando si esegue un ripristino in-place di un'applicazione che utilizza lo storage NetApp ONTAP, lo spazio utilizzato dall'applicazione ripristinata può raddoppiare. Dopo aver eseguito un ripristino in-place, rimuovere eventuali snapshot indesiderati dall'applicazione ripristinata per liberare spazio di storage.
- **Driver di classe di archiviazione supportati:** Astra Control supporta il ripristino dei backup utilizzando classi di archiviazione supportate dai seguenti driver:
  - `ontap-nas`
  - `ontap-nas-economy`
  - `ontap-san`
  - `ontap-san-economy`
- \* (Solo driver `ontap-nas-Economy`) esegue backup e ripristini\*: Prima di eseguire il backup o il ripristino di un'app che utilizza una classe di storage supportata da `ontap-nas-economy` driver, verificare che ["La directory snapshot sul backend dello storage ONTAP è nascosta"](#). La mancata visualizzazione di questa directory potrebbe causare la perdita di accesso all'applicazione, in particolare se si utilizza NFSv3.



L'esecuzione di un'operazione di ripristino in-place su un'applicazione che condivida le risorse con un'altra applicazione può avere risultati non intenzionali. Tutte le risorse condivise tra le applicazioni vengono sostituite quando viene eseguito un ripristino in-place su una delle applicazioni.

## Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Dal menu Opzioni nella colonna azioni, selezionare **Ripristina**.
3. Scegliere il tipo di ripristino:
  - **Ripristina gli spazi dei nomi originali:** Utilizzare questa procedura per ripristinare l'applicazione sul posto nel cluster originale.
    - i. Seleziona lo snapshot o il backup da utilizzare per ripristinare l'applicazione in-place, che ripristina l'applicazione a una versione precedente di se stessa.
    - ii. Selezionare **Avanti**.





Se si ripristina uno spazio dei nomi precedentemente cancellato, viene creato un nuovo spazio dei nomi con lo stesso nome come parte del processo di ripristino. Tutti gli utenti che disponevano dei diritti per gestire le applicazioni nello spazio dei nomi precedentemente cancellato devono ripristinare manualmente i diritti nello spazio dei nomi appena ricreato.

- **Ripristina nuovi spazi dei nomi:** Utilizzare questa procedura per ripristinare l'applicazione in un altro cluster o con spazi dei nomi diversi dall'origine. È inoltre possibile utilizzare questa procedura per migrare un'applicazione a una classe di storage diversa.
  - i. Specificare il nome dell'applicazione ripristinata.
  - ii. Scegliere il cluster di destinazione per l'applicazione che si desidera ripristinare.
  - iii. Immettere uno spazio dei nomi di destinazione per ogni spazio dei nomi di origine associato all'applicazione.



Astra Control crea nuovi spazi dei nomi di destinazione come parte di questa opzione di ripristino. Gli spazi dei nomi di destinazione specificati non devono essere già presenti nel cluster di destinazione.

- iv. Selezionare **Avanti**.
- v. Selezionare lo snapshot o il backup da utilizzare per ripristinare l'applicazione.
- vi. Selezionare **Avanti**.
- vii. Scegliere una delle seguenti opzioni:
  - **Ripristina utilizzando le classi di storage originali:** L'applicazione utilizza la classe di storage originariamente associata, a meno che non esista nel cluster di destinazione. In questo caso, viene utilizzata la classe di storage predefinita per il cluster.
  - **Ripristinare utilizzando una classe di storage diversa:** Selezionare una classe di storage esistente nel cluster di destinazione. Tutti i volumi delle applicazioni, indipendentemente dalle classi di storage originariamente associate, verranno migrati in questa diversa classe di storage come parte del ripristino.
- viii. Selezionare **Avanti**.

#### 4. Scegli le risorse da filtrare:

- **Restore all resources** (Ripristina tutte le risorse): Ripristina tutte le risorse associate all'applicazione originale.
- **Filter resources:** Specificare le regole per ripristinare un sottoinsieme delle risorse applicative originali:
  - i. Scegliere di includere o escludere risorse dall'applicazione ripristinata.
  - ii. Selezionare **Aggiungi regola di inclusione** o **Aggiungi regola di esclusione** e configurare la regola per filtrare le risorse corrette durante il ripristino dell'applicazione. È possibile modificare una regola o rimuoverla e crearne di nuovo fino a quando la configurazione non è corretta.



Per ulteriori informazioni sulla configurazione delle regole di inclusione ed esclusione, vedere [Filtrare le risorse durante il ripristino di un'applicazione](#).

5. Selezionare **Avanti**.
6. Esaminare attentamente i dettagli relativi all'azione di ripristino, digitare "restore" (se richiesto) e selezionare **Restore**.

## **[Tech preview] Ripristino da backup utilizzando una risorsa personalizzata (CR)**

È possibile ripristinare i dati da un backup utilizzando un file di risorse personalizzato (CR) in uno spazio dei nomi diverso o nello spazio dei nomi di origine originale.

## Ripristino da backup utilizzando una CR

### Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-backup-restore-cr.yaml`. Aggiorna i valori tra parentesi `<>` per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:

- `<CR_NAME>`: Il nome di questa operazione CR; scegliere un nome sensibile per il proprio ambiente.
- `<APPVAULT_NAME>`: Il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
- `<BACKUP_PATH>`: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Ad esempio:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-20231213023800_94347756-9d9b-401d-a0c3
```

- `<SOURCE_NAMESPACE>`: Lo spazio dei nomi di origine dell'operazione di ripristino.
- `<DESTINATION_NAMESPACE>`: Lo spazio dei nomi di destinazione dell'operazione di ripristino.

```
apiVersion: astra.netapp.io/v1
kind: BackupRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
  namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
"destination": "<DESTINATION_NAMESPACE>"}]
```

Direttiva non risolta in `<stdin>` - `include:./_include/selective-restore-cr.adoc[]`

1. Dopo aver popolato il `astra-control-backup-restore-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-backup-restore-cr.yaml
```

## Eeguire il ripristino dal backup allo spazio dei nomi originale utilizzando una CR

### Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-backup-ipr-cr.yaml`. Aggiorna i valori tra parentesi `<>` per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:

- `<CR_NAME>`: Il nome di questa operazione CR; scegliere un nome sensibile per il proprio ambiente.

- <APPVAULT\_NAME>: Il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
- <BACKUP\_PATH>: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Ad esempio:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appVaultRef: <APPVAULT_NAME>
  appArchivePath: <BACKUP_PATH>
```

Direttiva non risolta in <stdin> - include:./\_include/selective-restore-cr.adoc[]

1. Dopo aver popolato il astra-control-backup-ipr-cr.yaml File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-backup-ipr-cr.yaml
```

### [Anteprima tecnica] Ripristino da snapshot utilizzando una risorsa personalizzata (CR)

È possibile ripristinare i dati da uno snapshot utilizzando un file di risorse personalizzato (CR) in uno spazio dei nomi diverso o nello spazio dei nomi di origine originale.

## Eeguire il ripristino da uno snapshot utilizzando una CR

### Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-snapshot-restore-cr.yaml`. Aggiorna i valori tra parentesi `<>` per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:

- `<CR_NAME>`: Il nome di questa operazione CR; scegliere un nome sensibile per il proprio ambiente.
- `<APPVAULT_NAME>`: Il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
- `<BACKUP_PATH>`: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Ad esempio:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-20231213023800_94347756-9d9b-401d-a0c3
```

- `<SOURCE_NAMESPACE>`: Lo spazio dei nomi di origine dell'operazione di ripristino.
- `<DESTINATION_NAMESPACE>`: Lo spazio dei nomi di destinazione dell'operazione di ripristino.

```
apiVersion: astra.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
  namespaceMapping: [{"source": "<SOURCE_NAMESPACE>",
"destination": "<DESTINATION_NAMESPACE>"}]
```

Direttiva non risolta in `<stdin>` - `include:./_include/selective-restore-cr.adoc[]`

1. Dopo aver popolato il `astra-control-snapshot-restore-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-snapshot-restore-cr.yaml
```

## Eeguire il ripristino dallo snapshot allo spazio dei nomi originale utilizzando una CR

### Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome `astra-control-snapshot-igr-cr.yaml`. Aggiorna i valori tra parentesi `<>` per farli corrispondere all'ambiente Astra Control e alla configurazione del cluster:

- `<CR_NAME>`: Il nome di questa operazione CR; scegliere un nome sensibile per il proprio ambiente.

- <APPVAULT\_NAME>: Il nome dell'AppVault in cui sono memorizzati i contenuti di backup.
- <BACKUP\_PATH>: Il percorso all'interno di AppVault in cui sono memorizzati i contenuti di backup. Ad esempio:

```
ONTAP-S3_1343ff5e-4c41-46b5-af00/backups/schedule-
20231213023800_94347756-9d9b-401d-a0c3
```

```
apiVersion: astra.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: <CR_NAME>
  namespace: astra-connector
spec:
  appArchivePath: <BACKUP_PATH>
  appVaultRef: <APPVAULT_NAME>
```

Direttiva non risolta in <stdin> - include:./\_include/selective-restore-cr.adoc[]

1. Dopo aver popolato il `astra-control-snapshot-ipr-cr.yaml` File con i valori corretti, applicare il CR:

```
kubectl apply -f astra-control-snapshot-ipr-cr.yaml
```

## Risultato

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



Dopo un'operazione di protezione dei dati (cloning, backup o ripristino) e il successivo ridimensionamento persistente del volume, si verifica un ritardo fino a venti minuti prima che la nuova dimensione del volume venga visualizzata nell'interfaccia utente Web. L'operazione di protezione dei dati viene eseguita correttamente in pochi minuti ed è possibile utilizzare il software di gestione per il back-end dello storage per confermare la modifica delle dimensioni del volume.



Qualsiasi utente membro con vincoli di spazio dei nomi in base al nome/ID dello spazio dei nomi o alle etichette dello spazio dei nomi può clonare o ripristinare un'applicazione in un nuovo spazio dei nomi nello stesso cluster o in qualsiasi altro cluster dell'account dell'organizzazione. Tuttavia, lo stesso utente non può accedere all'applicazione clonata o ripristinata nel nuovo namespace. Dopo che un'operazione di clonazione o ripristino crea un nuovo spazio dei nomi, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo affinché l'utente interessato conceda l'accesso al nuovo spazio dei nomi.

## Filtrare le risorse durante il ripristino di un'applicazione

È possibile aggiungere una regola di filtro a un "ripristinare" operazione che specifica le risorse applicative esistenti da includere o escludere dall'applicazione ripristinata. È possibile includere o escludere risorse in base a uno spazio dei nomi, un'etichetta o un GVK (GroupVersionKind) specificati.

### Scopri di più sugli scenari di inclusione ed esclusione

- **Si seleziona una regola di inclusione con spazi dei nomi originali (ripristino in-place):** Le risorse applicative esistenti definite nella regola verranno eliminate e sostituite da quelle dello snapshot o del backup selezionato che si sta utilizzando per il ripristino. Tutte le risorse non specificate nella regola di inclusione resteranno invariate.
- **Selezionare una regola di inclusione con nuovi spazi dei nomi:** Utilizzare la regola per selezionare le risorse specifiche che si desidera utilizzare nell'applicazione ripristinata. Le risorse non specificate nella regola di inclusione non verranno incluse nell'applicazione ripristinata.
- **Si seleziona una regola di esclusione con spazi dei nomi originali (ripristino in-place):** Le risorse specificate per l'esclusione non verranno ripristinate e rimarranno invariate. Le risorse non specificate da escludere verranno ripristinate dallo snapshot o dal backup. Tutti i dati sui volumi persistenti verranno cancellati e ricreati se il corrispondente StatefulSet fa parte delle risorse filtrate.
- **Selezionare una regola di esclusione con nuovi spazi dei nomi:** Utilizzare la regola per selezionare le risorse specifiche che si desidera rimuovere dall'applicazione ripristinata. Le risorse non specificate da escludere verranno ripristinate dallo snapshot o dal backup.

Le regole possono includere o escludere tipi. Non sono disponibili regole che combinano inclusione ed esclusione delle risorse.

### Fasi

1. Dopo aver scelto di filtrare le risorse e aver selezionato un'opzione di inclusione o esclusione nella procedura guidata Restore App, selezionare **Aggiungi regola di inclusione** o **Aggiungi regola di esclusione**.



Non è possibile escludere risorse con ambito cluster che vengono automaticamente incluse da Astra Control.

2. Configurare la regola di filtro:



È necessario specificare almeno uno spazio dei nomi, un'etichetta o un GVK. Assicurarsi che tutte le risorse conservate dopo l'applicazione delle regole di filtro siano sufficienti per mantenere l'applicazione ripristinata in uno stato di integrità.

- a. Selezionare uno spazio dei nomi specifico per la regola. Se non si effettua una selezione, nel filtro verranno utilizzati tutti gli spazi dei nomi.



Se l'applicazione conteneva originariamente più spazi dei nomi e la ripristinerai in nuovi spazi dei nomi, tutti gli spazi dei nomi verranno creati anche se non contengono risorse.

- b. (Facoltativo) inserire un nome di risorsa.
- c. (Facoltativo) **selettore di etichette:** Includere un "selettore di etichette" da aggiungere alla regola. Il selettore di etichette viene utilizzato per filtrare solo le risorse corrispondenti all'etichetta selezionata.

d. (Facoltativo) selezionare **Use GVK (GroupVersionKind) set to filter resources** for additional filtering options.



Se si utilizza un filtro GVK, è necessario specificare versione e tipo.

- i. (Facoltativo) **Group**: Dall'elenco a discesa, selezionare il gruppo Kubernetes API.
- ii. **Kind**: Dall'elenco a discesa, selezionare lo schema dell'oggetto per il tipo di risorsa Kubernetes da utilizzare nel filtro.
- iii. **Version** (versione): Selezionare la versione dell'API Kubernetes.

3. Esaminare la regola creata in base alle voci immesse.

4. Selezionare **Aggiungi**.



È possibile creare tutte le regole di inclusione ed esclusione delle risorse desiderate. Le regole vengono visualizzate nel riepilogo dell'applicazione di ripristino prima di avviare l'operazione.

## Clonare e migrare le applicazioni

È possibile clonare un'applicazione esistente per creare un'applicazione duplicata sullo stesso cluster Kubernetes o su un altro cluster. Quando Astra Control clona un'applicazione, crea un clone della configurazione dell'applicazione e dello storage persistente.

La clonazione può essere di aiuto nel caso in cui sia necessario spostare applicazioni e storage da un cluster Kubernetes a un altro. Ad esempio, è possibile spostare i carichi di lavoro attraverso una pipeline ci/CD e attraverso gli spazi dei nomi Kubernetes.



Se si aggiunge un filtro dello spazio dei nomi a un gancio di esecuzione che viene eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o del clone si trovano in spazi dei nomi diversi, il filtro dello spazio dei nomi viene applicato solo allo spazio dei nomi di destinazione.

### Prima di iniziare

- **Check destination Volumes** (Controlla volumi di destinazione): Se si esegue la clonazione in una classe di storage diversa, assicurarsi che la classe di storage utilizzi la stessa modalità di accesso al volume persistente (ad esempio ReadWriteMany). L'operazione di clonazione non riesce se la modalità di accesso al volume persistente di destinazione è diversa. Ad esempio, se il volume persistente di origine utilizza la modalità di accesso RWX, selezionare una classe di storage di destinazione che non è in grado di fornire RWX, come Azure Managed Disks, AWS EBS, Google Persistent Disk o. `ontap-san`, causerà l'errore dell'operazione di clonazione. Per ulteriori informazioni sulle modalità di accesso al volume persistente, fare riferimento a. "[Kubernetes](#)" documentazione.
- Per clonare le applicazioni in un cluster diverso, è necessario assicurarsi di aver assegnato un bucket predefinito per l'istanza cloud contenente il cluster di origine. Se l'istanza del cloud di origine non ha un bucket predefinito impostato, l'operazione di cloni tra cluster avrà esito negativo.
- Durante le operazioni di cloni, le applicazioni che necessitano di una risorsa IngressClass o di webhook per funzionare correttamente non devono disporre di tali risorse già definite nel cluster di destinazione.

### Limitazioni dei cloni



- **Classi di storage esplicite:** Se si implementa un'applicazione con una classe di storage esplicitamente impostata e si deve clonare l'applicazione, il cluster di destinazione deve avere la classe di storage specificata in origine. La clonazione di un'applicazione con una classe di storage esplicitamente impostata su un cluster che non ha la stessa classe di storage non avrà esito positivo.
- **Applicazioni supportate da ontap-nas a economia:** Non è possibile utilizzare le operazioni di clonazione se la classe di storage dell'applicazione è supportata da `ontap-nas-economy` driver. Tuttavia, è possibile ["abilita backup e ripristino per le operazioni economiche a ontap-nas"](#).
- **Cloni e vincoli dell'utente:** Qualsiasi utente membro con vincoli dello spazio dei nomi in base al nome/ID dello spazio dei nomi o alle etichette dello spazio dei nomi può clonare o ripristinare un'applicazione in un nuovo spazio dei nomi sullo stesso cluster o in qualsiasi altro cluster dell'account dell'organizzazione. Tuttavia, lo stesso utente non può accedere all'applicazione clonata o ripristinata nel nuovo namespace. Dopo che un'operazione di clonazione o ripristino crea un nuovo spazio dei nomi, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo affinché l'utente interessato conceda l'accesso al nuovo spazio dei nomi.
- **I cloni utilizzano bucket predefiniti:**
  - Durante il backup o il ripristino di un'applicazione, è possibile specificare un bucket da utilizzare. È necessario specificare un bucket predefinito quando si clonano tra cluster, ma specificare un bucket è facoltativo quando si esegue la clonazione all'interno dello stesso cluster.
  - Quando si clonano tra cluster, l'istanza cloud contenente il cluster di origine dell'operazione di clone deve avere un bucket predefinito.
  - Non esiste alcuna opzione per modificare i bucket per un clone. Se si desidera controllare quale bucket viene utilizzato, è possibile farlo ["modificare l'impostazione predefinita del bucket"](#) oppure fare una ["backup"](#) seguito da un ["ripristinare"](#) separatamente.
- **Con Jenkins ci:** Se si clonano istanze distribuite dall'operatore di Jenkins ci, è necessario ripristinare manualmente i dati persistenti. Si tratta di un limite del modello di implementazione dell'applicazione.

## Fasi

1. Selezionare **applicazioni**.
2. Effettuare una delle seguenti operazioni:
  - Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per l'applicazione desiderata.
  - Selezionare il nome dell'applicazione desiderata e l'elenco a discesa Status (Stato) in alto a destra nella pagina.
3. Selezionare **Clone**.
4. Specificare i dettagli per il clone:
  - Immettere un nome.
  - Scegliere un cluster di destinazione per il clone.
  - Immettere gli spazi dei nomi di destinazione per il clone. Ogni namespace di origine associato all'applicazione viene mappato a uno spazio dei nomi di destinazione.



Astra Control crea nuovi spazi dei nomi di destinazione come parte dell'operazione di clone. Gli spazi dei nomi di destinazione specificati non devono essere già presenti nel cluster di destinazione.

- Selezionare **Avanti**.
- Scegliere di mantenere la classe di storage originale associata all'applicazione o di selezionare una classe di storage diversa.



Puoi migrare la classe di storage di un'app a una classe di storage di un cloud provider nativo o a un'altra classe di storage supportata, migrare un'app da una classe di storage supportata da `ontap-nas-economy` a una classe di storage supportata da `ontap-nas` sullo stesso cluster oppure copiare l'applicazione in un altro cluster con una classe di storage supportata da `ontap-nas-economy` driver.



Se si seleziona una classe di storage diversa e questa classe di storage non esiste al momento del ripristino, viene restituito un errore.

5. Selezionare **Avanti**.

6. Esaminare le informazioni relative al clone e selezionare **Clone**.

### Risultato

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

Dopo che un'operazione di clonazione o ripristino crea un nuovo spazio dei nomi, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo affinché l'utente interessato conceda l'accesso al nuovo spazio dei nomi.

## Gestire gli hook di esecuzione delle applicazioni

Un gancio di esecuzione è un'azione personalizzata che è possibile configurare per l'esecuzione in combinazione con un'operazione di protezione dei dati di un'applicazione gestita. Ad esempio, se si dispone di un'applicazione di database, è possibile utilizzare un gancio di esecuzione per mettere in pausa tutte le transazioni del database prima di uno snapshot e riprendere le transazioni al termine dello snapshot. Ciò garantisce snapshot coerenti con l'applicazione.

### Tipi di hook di esecuzione

Astra Control Service supporta i seguenti tipi di hook di esecuzione, in base a quando possono essere eseguiti:

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

### Esecuzione dei filtri hook

Quando si aggiunge o si modifica un gancio di esecuzione a un'applicazione, è possibile aggiungere filtri a un gancio di esecuzione per gestire i contenitori corrispondenti. I filtri sono utili per le applicazioni che utilizzano la stessa immagine container su tutti i container, ma possono utilizzare ogni immagine per uno scopo diverso (ad esempio Elasticsearch). I filtri consentono di creare scenari in cui gli hook di esecuzione vengono eseguiti su alcuni container identici, ma non necessariamente su tutti. Se si creano più filtri per un singolo gancio di esecuzione, questi vengono combinati con un operatore AND logico. È possibile avere fino a 10 filtri attivi per gancio di esecuzione.

Ogni filtro aggiunto a un gancio di esecuzione utilizza un'espressione regolare per far corrispondere i contenitori nel cluster. Quando un gancio corrisponde a un container, il gancio esegue lo script associato su quel container. Le espressioni regolari per i filtri utilizzano la sintassi RE2 (espressione regolare), che non supporta la creazione di un filtro che esclude i contenitori dall'elenco di corrispondenze. Per informazioni sulla sintassi supportata da Astra Control per le espressioni regolari nei filtri hook di esecuzione, vedere "[Supporto della sintassi RE2 \(Regular Expression 2\)](#)".



Se si aggiunge un filtro dello spazio dei nomi a un gancio di esecuzione che viene eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o del clone si trovano in spazi dei nomi diversi, il filtro dello spazio dei nomi viene applicato solo allo spazio dei nomi di destinazione.

## Note importanti sugli hook di esecuzione personalizzati

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



Poiché gli hook di esecuzione spesso riducono o disattivano completamente le funzionalità dell'applicazione con cui vengono eseguiti, si consiglia di ridurre al minimo il tempo necessario per l'esecuzione degli hook di esecuzione personalizzati.

Se si avvia un'operazione di backup o snapshot con gli hook di esecuzione associati, ma poi si annulla, gli hook possono ancora essere eseguiti se l'operazione di backup o snapshot è già iniziata. Ciò significa che la logica utilizzata in un gancio di esecuzione post-backup non può presumere che il backup sia stato completato.

- La funzionalità hook di esecuzione è disabilitata per impostazione predefinita per le nuove implementazioni di Astra Control.
  - È necessario attivare la funzione di hook di esecuzione prima di poter utilizzare i hook di esecuzione.
  - Gli utenti proprietari o amministratori possono attivare o disattivare la funzionalità di hook di esecuzione per tutti gli utenti definiti nell'account Astra Control corrente. Fare riferimento a [Attivare la funzione ganci di esecuzione](#) e [Disattivare la funzione ganci di esecuzione](#) per istruzioni.
  - Lo stato di abilitazione delle funzioni viene mantenuto durante gli aggiornamenti di Astra Control.
- Un gancio di esecuzione deve utilizzare uno script per eseguire le azioni. Molti hook di esecuzione possono fare riferimento allo stesso script.
- Astra Control richiede che gli script utilizzati dagli hook di esecuzione siano scritti nel formato degli script shell eseguibili.
- La dimensione dello script è limitata a 96 KB.
- Astra Control utilizza le impostazioni degli uncino di esecuzione e qualsiasi criterio corrispondente per determinare quali hook sono applicabili a un'operazione di snapshot, backup o ripristino.
- Tutti i guasti degli uncini di esecuzione sono guasti di tipo soft; altri hook e l'operazione di protezione dei dati vengono ancora tentati anche in caso di interruzione di un hook. Tuttavia, quando un gancio non funziona, viene registrato un evento di avviso nel registro eventi della pagina **attività**.
- Per creare, modificare o eliminare gli hook di esecuzione, è necessario essere un utente con autorizzazioni Owner, Admin o Member.
- Se l'esecuzione di un gancio di esecuzione richiede più di 25 minuti, l'hook non riesce, creando una voce del registro eventi con un codice di ritorno "N/A". Qualsiasi snapshot interessata verrà contrassegnata come non riuscita e una voce del registro eventi risultante annoterà il timeout.
- Per le operazioni di protezione dei dati ad hoc, tutti gli eventi hook vengono generati e salvati nel registro eventi della pagina **Activity**. Tuttavia, per le operazioni di protezione dei dati pianificate, nel registro eventi

vengono registrati solo gli eventi di errore hook (gli eventi generati dalle operazioni di protezione dei dati pianificate vengono ancora registrati).

### Ordine di esecuzione

Quando viene eseguita un'operazione di protezione dei dati, gli eventi hook di esecuzione hanno luogo nel seguente ordine:

1. Gli eventuali hook di esecuzione pre-operation personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook pre-operation personalizzati necessari, ma l'ordine di esecuzione di questi hook prima dell'operazione non è garantito né configurabile.
2. Viene eseguita l'operazione di protezione dei dati.
3. Gli eventuali hook di esecuzione post-operation personalizzati applicabili vengono eseguiti sui container appropriati. È possibile creare ed eseguire tutti gli hook post-operation personalizzati necessari, ma l'ordine di esecuzione di questi hook dopo l'operazione non è garantito né configurabile.

Se si creano più hook di esecuzione dello stesso tipo (ad esempio, pre-snapshot), l'ordine di esecuzione di tali hook non è garantito. Tuttavia, è garantito l'ordine di esecuzione di ganci di tipi diversi. Ad esempio, l'ordine di esecuzione di una configurazione con tutti i diversi tipi di hook è simile al seguente:

1. Hook pre-backup eseguiti
2. Hook pre-snapshot eseguiti
3. Esecuzione di hook post-snapshot
4. Hook post-backup eseguiti
5. Esecuzione degli hook di post-ripristino

È possibile vedere un esempio di questa configurazione nello scenario numero 2 dalla tabella nella [Determinare se verrà eseguito un gancio](#).



Prima di abilitarli in un ambiente di produzione, è necessario verificare sempre gli script hook di esecuzione. È possibile utilizzare il comando 'kubectl exec' per testare comodamente gli script. Dopo aver attivato gli hook di esecuzione in un ambiente di produzione, testare le snapshot e i backup risultanti per assicurarsi che siano coerenti. Per eseguire questa operazione, clonare l'applicazione in uno spazio dei nomi temporaneo, ripristinare lo snapshot o il backup e quindi testare l'applicazione.

### Determinare se verrà eseguito un gancio

Utilizza la seguente tabella per determinare se verrà eseguito un gancio di esecuzione personalizzato per l'applicazione.

Si noti che tutte le operazioni di alto livello delle applicazioni consistono nell'eseguire una delle operazioni di base di snapshot, backup o ripristino. A seconda dello scenario, un'operazione di cloni può consistere in varie combinazioni di queste operazioni, quindi gli hook di esecuzione eseguiti da un'operazione di cloni variano.

Le operazioni di ripristino in-place richiedono un'istantanea o un backup esistente, in modo che queste operazioni non eseguano snapshot o hook di backup.

Se si avvia e poi si annulla un backup che include uno snapshot e sono associati degli hook di esecuzione, alcuni hook potrebbero essere eseguiti e altri no. Ciò significa che un gancio di esecuzione post-backup non può presumere che il backup sia stato completato. Tenere presente i seguenti punti per i backup annullati con gli hook di esecuzione associati:



- Gli hook pre-backup e post-backup sono sempre in esecuzione.
- Se il backup include un nuovo snapshot e lo snapshot è stato avviato, vengono eseguiti gli hook pre-snapshot e post-snapshot.
- Se il backup viene annullato prima dell'avvio dello snapshot, gli hook pre-snapshot e post-snapshot non vengono eseguiti.

| Scenario | Operazioni             | Snapshot esistente | Backup esistente | Namespace | Cluster | Esecuzione di Snapshot Hooks | Esecuzione dei ganci di backup | Esecuzione degli hook di ripristino |
|----------|------------------------|--------------------|------------------|-----------|---------|------------------------------|--------------------------------|-------------------------------------|
| 1        | Clonare                | N                  | N                | Novità    | Stesso  | Y                            | N                              | Y                                   |
| 2        | Clonare                | N                  | N                | Novità    | Diverso | Y                            | Y                              | Y                                   |
| 3        | Clonare o ripristinare | Y                  | N                | Novità    | Stesso  | N                            | N                              | Y                                   |
| 4        | Clonare o ripristinare | N                  | Y                | Novità    | Stesso  | N                            | N                              | Y                                   |
| 5        | Clonare o ripristinare | Y                  | N                | Novità    | Diverso | N                            | N                              | Y                                   |
| 6        | Clonare o ripristinare | N                  | Y                | Novità    | Diverso | N                            | N                              | Y                                   |
| 7        | Ripristinare           | Y                  | N                | Esistente | Stesso  | N                            | N                              | Y                                   |
| 8        | Ripristinare           | N                  | Y                | Esistente | Stesso  | N                            | N                              | Y                                   |
| 9        | Snapshot               | N/A.               | N/A.             | N/A.      | N/A.    | Y                            | N/A.                           | N/A.                                |
| 10       | Backup                 | N                  | N/A.             | N/A.      | N/A.    | Y                            | Y                              | N/A.                                |
| 11       | Backup                 | Y                  | N/A.             | N/A.      | N/A.    | N                            | N                              | N/A.                                |

### Esempi di gancio di esecuzione

Visitare il "[Progetto NetApp Verda GitHub](#)" Per scaricare gli hook di esecuzione per le applicazioni più diffuse come Apache Cassandra ed Elasticsearch. Puoi anche vedere esempi e trovare idee per strutturare i tuoi hook di esecuzione personalizzati.

### Attivare la funzione ganci di esecuzione

Se si è un utente Proprietario o Amministratore, è possibile attivare la funzione ganci di esecuzione. Quando si attiva la funzionalità, tutti gli utenti definiti in questo account Astra Control possono utilizzare i ganci di esecuzione e visualizzare i ganci di esecuzione e gli script hook esistenti.

### Fasi

1. Accedere a **applicazioni** e selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare **Abilita ganci di esecuzione**.

Viene visualizzata la scheda **account > Impostazioni funzioni**.

4. Nel riquadro **ganci di esecuzione**, selezionare il menu delle impostazioni.
5. Selezionare **Abilita**.
6. Prendere nota dell'avviso di protezione visualizzato.
7. Selezionare **Sì, abilita i ganci di esecuzione**.

### Disattivare la funzione ganci di esecuzione

Se si è un utente Proprietario o Amministratore, è possibile disattivare la funzionalità Hook di esecuzione per tutti gli utenti definiti in questo account Astra Control. È necessario eliminare tutti i ganci di esecuzione esistenti prima di disattivare la funzione ganci di esecuzione. Fare riferimento a [Eliminare un gancio di esecuzione](#) per istruzioni sull'eliminazione di un gancio di esecuzione esistente.

#### Fasi

1. Andare su **account**, quindi selezionare la scheda **Impostazioni funzione**.
2. Selezionare la scheda **Execution Hooks**.
3. Nel riquadro **ganci di esecuzione**, selezionare il menu delle impostazioni.
4. Selezionare **Disable** (Disattiva).
5. Prendere nota dell'avviso visualizzato.
6. Tipo `disable` per confermare che si desidera disattivare la funzione per tutti gli utenti.
7. Selezionare **Sì, disabilita**.

### Visualizzare gli hook di esecuzione esistenti

È possibile visualizzare gli hook di esecuzione personalizzati esistenti per un'applicazione.

#### Fasi

1. Accedere a **applicazioni** e selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.

È possibile visualizzare tutti gli hook di esecuzione attivati o disattivati nell'elenco risultante. È possibile visualizzare lo stato di un gancio, il numero di contenitori corrispondenti, il tempo di creazione e il momento in cui viene eseguito (pre- o post-operazione). È possibile selezionare + accanto al nome dell'hook per espandere l'elenco dei container su cui verrà eseguito. Per visualizzare i registri degli eventi relativi agli hook di esecuzione per questa applicazione, accedere alla scheda **attività**.

### Visualizzare gli script esistenti

È possibile visualizzare gli script caricati. In questa pagina puoi anche vedere quali script sono in uso e quali hook li stanno utilizzando.

#### Fasi

1. Vai a **account**.
2. Selezionare la scheda **script**.

In questa pagina è possibile visualizzare un elenco degli script caricati. La colonna **Used by** mostra gli hook di esecuzione che utilizzano ogni script.

### Aggiungere uno script

Ogni gancio di esecuzione deve utilizzare uno script per eseguire le azioni. È possibile aggiungere uno o più script a cui possono fare riferimento gli hook di esecuzione. Molti hook di esecuzione possono fare riferimento allo stesso script; ciò consente di aggiornare molti hook di esecuzione modificando solo uno script.

#### Fasi

1. Verificare che la funzione ganci di esecuzione sia **attivato**.
2. Vai a **account**.
3. Selezionare la scheda **script**.
4. Selezionare **Aggiungi**.
5. Effettuare una delle seguenti operazioni:
  - Caricare uno script personalizzato.
    - i. Selezionare l'opzione **carica file**.
    - ii. Selezionare un file e caricarlo.
    - iii. Assegnare allo script un nome univoco.
    - iv. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
    - v. Selezionare **Salva script**.
  - Incollare uno script personalizzato dagli Appunti.
    - i. Selezionare l'opzione **Incolla o tipo**.
    - ii. Selezionare il campo di testo e incollare il testo dello script nel campo.
    - iii. Assegnare allo script un nome univoco.
    - iv. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
6. Selezionare **Salva script**.

#### Risultato

Il nuovo script viene visualizzato nell'elenco della scheda **script**.

### Eliminare uno script

È possibile rimuovere uno script dal sistema se non è più necessario e non viene utilizzato da alcun hook di esecuzione.

#### Fasi

1. Vai a **account**.
2. Selezionare la scheda **script**.
3. Scegliere uno script da rimuovere e selezionare il menu nella colonna **azioni**.
4. Selezionare **Delete** (Elimina).



Se lo script è associato a uno o più hook di esecuzione, l'azione **Delete** non è disponibile. Per eliminare lo script, modificare prima gli hook di esecuzione associati e associarli a uno script diverso.

## Creare un gancio di esecuzione personalizzato

È possibile creare un gancio di esecuzione personalizzato per un'applicazione e aggiungerlo ad Astra Control. Fare riferimento a [Esempi di gancio di esecuzione](#) per esempi di gancio. Per creare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner (Proprietario), Admin (Amministratore) o Member (membro).



Quando si crea uno script shell personalizzato da utilizzare come uncino di esecuzione, ricordarsi di specificare la shell appropriata all'inizio del file, a meno che non si stiano eseguendo comandi specifici o fornendo il percorso completo di un eseguibile.

### Fasi

1. Verificare che la funzione ganci di esecuzione sia [attivato](#).
2. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
3. Selezionare la scheda **Execution Hooks**.
4. Selezionare **Aggiungi**.
5. Nell'area **Dettagli gancio**:
  - a. Determinare quando il gancio deve funzionare selezionando un tipo di operazione dal menu a discesa **operazione**.
  - b. Immettere un nome univoco per l'hook.
  - c. (Facoltativo) inserire gli argomenti da passare al gancio durante l'esecuzione, premendo il tasto Invio dopo ogni argomento inserito per registrarne ciascuno.
6. (Facoltativo) nell'area **Dettagli filtro gancio**, è possibile aggiungere filtri per controllare i contenitori su cui viene eseguito l'gancio di esecuzione:
  - a. Selezionare **Aggiungi filtro**.
  - b. Nella colonna **tipo filtro gancio**, scegliere un attributo sul quale filtrare dal menu a discesa.
  - c. Nella colonna **Regex**, immettere un'espressione regolare da utilizzare come filtro. Astra Control utilizza ["Sintassi regex espressione regolare 2 \(RE2\)"](#).



Se si filtra sul nome esatto di un attributo (ad esempio il nome di un pod) senza altro testo nel campo di espressione regolare, viene eseguita una corrispondenza di sottostringa. Per associare un nome esatto e solo il nome, utilizzare la sintassi di corrispondenza stringa esatta (ad esempio, `^exact_podname$`).

- d. Per aggiungere altri filtri, selezionare **Aggiungi filtro**.



I filtri multipli per un gancio di esecuzione sono combinati con un operatore and logico. È possibile avere fino a 10 filtri attivi per gancio di esecuzione.

7. Al termine, selezionare **Avanti**.
8. Nell'area **script**, eseguire una delle seguenti operazioni:
  - Aggiungere un nuovo script.



i. Selezionare **Aggiungi**.

ii. Effettuare una delle seguenti operazioni:

- Caricare uno script personalizzato.
  - I. Selezionare l'opzione **carica file**.
  - II. Selezionare un file e caricarlo.
  - III. Assegnare allo script un nome univoco.
  - IV. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
  - V. Selezionare **Salva script**.
- Incollare uno script personalizzato dagli Appunti.
  - I. Selezionare l'opzione **Incolla o tipo**.
  - II. Selezionare il campo di testo e incollare il testo dello script nel campo.
  - III. Assegnare allo script un nome univoco.
  - IV. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.

◦ Selezionare uno script esistente dall'elenco.

In questo modo, il gancio di esecuzione deve utilizzare questo script.

9. Selezionare **Avanti**.

10. Esaminare la configurazione degli uncino di esecuzione.

11. Selezionare **Aggiungi**.

## Controllare lo stato di un gancio di esecuzione

Al termine dell'esecuzione di un'operazione di snapshot, backup o ripristino, è possibile controllare lo stato degli hook di esecuzione eseguiti come parte dell'operazione. È possibile utilizzare queste informazioni di stato per determinare se si desidera mantenere l'esecuzione agganciata, modificarla o eliminarla.

### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Data Protection**.
3. Selezionare **Snapshot** per visualizzare le snapshot in esecuzione o **Backup** per visualizzare i backup in esecuzione.

Lo stato **Hook** mostra lo stato dell'esecuzione dell'hook al termine dell'operazione. Per ulteriori informazioni, passare il mouse sullo stato. Ad esempio, se si verificano errori di uncino di esecuzione durante uno snapshot, passando il mouse sullo stato di uncino per tale snapshot si ottiene un elenco di uncini di esecuzione non riusciti. Per visualizzare i motivi di ciascun guasto, consultare la pagina **Activity** (attività) nell'area di navigazione a sinistra.

## Visualizzare l'utilizzo dello script

È possibile vedere quali hook di esecuzione utilizzano uno script specifico nell'interfaccia utente Web di Astra Control.

## Fasi

1. Selezionare **account**.
2. Selezionare la scheda **script**.

La colonna **Used by** nell'elenco degli script contiene i dettagli su quali hook utilizzano ciascuno script dell'elenco.

3. Selezionare le informazioni nella colonna **utilizzato da** per lo script desiderato.

Viene visualizzato un elenco più dettagliato con i nomi degli hook che utilizzano lo script e il tipo di operazione con cui sono configurati per l'esecuzione.

## Modificare un gancio di esecuzione

È possibile modificare un gancio di esecuzione se si desidera modificarne gli attributi, i filtri o lo script utilizzato. Per modificare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner, Admin o Member.

### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per un gancio che si desidera modificare.
4. Selezionare **Modifica**.
5. Apportare le modifiche necessarie, selezionando **Avanti** dopo aver completato ciascuna sezione.
6. Selezionare **Salva**.

## Disattiva un gancio di esecuzione

È possibile disattivare un gancio di esecuzione se si desidera impedirne temporaneamente l'esecuzione prima o dopo un'istantanea di un'applicazione. Per disattivare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner, Admin o Member.

### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per un gancio che si desidera disattivare.
4. Selezionare **Disable** (Disattiva).

## Eliminare un gancio di esecuzione

È possibile rimuovere completamente un gancio di esecuzione se non è più necessario. Per eliminare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner, Admin o Member.

### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per il gancio che si desidera

eliminare.

4. Selezionare **Delete** (Elimina).
5. Nella finestra di dialogo visualizzata, digitare "DELETE" per confermare.
6. Selezionare **Sì, elimina gancio di esecuzione**.

#### Per ulteriori informazioni

- ["Progetto NetApp Verda GitHub"](#)

## Visualizza lo stato di salute delle applicazioni e del calcolo

### Visualizza un riepilogo dello stato delle applicazioni e dei cluster

Fai clic su **Dashboard** per visualizzare una vista di alto livello delle tue applicazioni, dei cluster e della loro salute.

Il riquadro Apps (applicazioni) consente di identificare i seguenti elementi:

- Quante applicazioni stai attualmente gestendo.
- Se queste applicazioni gestite sono in buona salute.
- Se le applicazioni sono completamente protette (sono protette se sono disponibili backup recenti).

Si noti che questi non sono solo numeri o stati, ma è possibile eseguire il drill-down da ciascuno di questi. Ad esempio, se le applicazioni non sono completamente protette, puoi passare il mouse sull'icona per identificare le applicazioni non completamente protette, il che include un motivo.

Il riquadro Clusters fornisce dettagli simili sullo stato del cluster ed è possibile eseguire il drill-down per ottenere ulteriori dettagli come si può fare con un'applicazione.

### Visualizza lo stato di salute e i dettagli dei cluster

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

#### Fasi

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



Se un cluster si trova in `removed` state Yet la connettività di rete e del cluster sembra sana (i tentativi esterni di accesso al cluster utilizzando le API di Kubernetes sono riusciti), il kubeconfig che hai fornito ad Astra Control potrebbe non essere più valido. Ciò può essere dovuto alla rotazione o alla scadenza del certificato sul cluster. Per risolvere questo problema, aggiornare le credenziali associate al cluster in Astra Control utilizzando ["API di controllo Astra"](#).

3. Visualizzare le informazioni nelle schede **Overview**, **Storage** e **Activity** per trovare le informazioni desiderate.

- **Panoramica:** Dettagli sui nodi di lavoro, incluso il loro stato.
- **Storage:** I volumi persistenti associati al calcolo, inclusi la classe e lo stato dello storage.
- **Attività:** Le attività correlate al cluster.



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

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

Dopo aver iniziato a gestire un'app, Astra Control fornisce dettagli sull'app che ti permette di identificarne lo stato di comunicazione (se Astra Control è in grado di comunicare con l'app), il suo stato di protezione (se è completamente protetto in caso di guasto), i pod, lo storage persistente e altro ancora.

### Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Trova le informazioni che cerchi:

#### Stato dell'app

Fornisce uno stato che riflette se Astra Control può comunicare con l'applicazione.

#### Stato di protezione dell'app

Fornisce uno stato di protezione dell'applicazione:

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

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

#### Panoramica

Informazioni sullo stato dei pod associati all'applicazione.

#### Protezione dei dati

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

#### Storage

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

## Risorse

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

## Attività

Le attività di Astra Control correlate all'applicazione.

# Gestire i bucket

È possibile gestire i bucket utilizzati da Astra per backup e cloni. È possibile aggiungere bucket aggiuntivi, rimuovere bucket esistenti e modificare il bucket predefinito per i cluster Kubernetes in un'istanza cloud.

Solo i proprietari e gli amministratori possono gestire i bucket.

## Come Astra Control utilizza i bucket

Quando inizi a gestire il tuo primo cluster Kubernetes per un'istanza cloud, Astra Control Service crea il bucket iniziale per questo "istanza di cloud".

È possibile designare manualmente un bucket come bucket predefinito per un'istanza di cloud. In tal caso, Astra Control Service utilizza questo bucket per impostazione predefinita per i backup e i cloni creati su qualsiasi cluster gestito in tale istanza del cloud (è possibile selezionare un bucket diverso per i backup). Se si esegue un clone live di un'applicazione da uno qualsiasi dei cluster gestiti in un'istanza cloud a un altro cluster, Astra Control Service utilizza il bucket predefinito per l'istanza del cloud di origine per eseguire l'operazione di clone.

È possibile impostare lo stesso bucket del bucket predefinito per più istanze cloud.

È possibile selezionare da qualsiasi bucket quando si crea una policy di protezione o si avvia un backup ad-hoc.



Astra Control Service verifica se un bucket di destinazione è accessibile prima di avviare un backup o un clone.

## Visualizzare i bucket esistenti

Visualizza l'elenco dei bucket disponibili per Astra Control Service per determinarne lo stato e identificare il bucket predefinito (se definito) per la tua istanza di cloud.

Un bucket può avere uno dei seguenti stati:

### In sospeso

Dopo aver aggiunto un bucket, questo inizia nello stato in sospeso mentre Astra Control lo rileva.

### Disponibile

Il bucket è disponibile per l'utilizzo da parte di Astra Control.

### Rimosso

Al momento il bucket non è operativo. Passare il mouse sull'icona di stato per identificare il problema.

Se un bucket si trova nello stato rimosso, è comunque possibile impostarlo come bucket predefinito e

assegnarlo a un programma di protezione. Tuttavia, se il bucket non si trova nello stato disponibile entro il momento in cui viene avviata un'operazione di protezione dei dati, l'operazione non riuscirà.

## Fase

### 1. Accedere a **Bucket**.

Viene visualizzato l'elenco dei bucket disponibili per Astra Control Service.

## Aggiungere un bucket aggiuntivo

È possibile aggiungere altri bucket in qualsiasi momento. Ciò consente di scegliere tra bucket durante la creazione di una policy di protezione o l'avvio di un backup ad-hoc e consente di modificare il bucket predefinito utilizzato da un'istanza del cloud.

È possibile aggiungere i seguenti tipi di bucket:

- Amazon Web Services
- Generico S3
- Piattaforma Google Cloud
- Microsoft Azure
- NetApp ONTAP S3
- NetApp StorageGRID S3

## Prima di iniziare

- Assicurarsi di conoscere il nome di un bucket esistente.
- Assicurarsi di disporre di credenziali per il bucket che forniscono ad Astra Control le autorizzazioni necessarie per gestire il bucket.
- Se il bucket è in Microsoft Azure:
  - Il bucket deve appartenere al gruppo di risorse denominato *astra-backup-rg*.
  - Se l'impostazione delle prestazioni dell'istanza dell'account di storage Azure è impostata su "Premium", l'impostazione "Premium account type" deve essere impostata su "Block blob".

## Fasi

### 1. Accedere a **Bucket**.

### 2. Selezionare **Add** (Aggiungi) e seguire le istruzioni per aggiungere il bucket.

- **Type**: Scegli il tuo cloud provider.
- **Nome bucket esistente**: Immettere il nome del bucket.
- **Description**: Se si desidera, inserire una descrizione del bucket.
  - **Storage account** (solo Azure): Immettere il nome dell'account di storage Azure. Questo bucket deve appartenere al gruppo di risorse denominato *astra-backup-rg*.
  - **Nome server S3 o indirizzo IP** (solo per i tipi di bucket AWS e S3): Immettere il nome di dominio completo dell'endpoint S3 che corrisponde alla propria regione, senza `https://`. Fare riferimento a ["La documentazione Amazon"](#) per ulteriori informazioni.
  - **Select credentials** (Seleziona credenziali): Immettere le credenziali che forniscono ad Astra Control Service le autorizzazioni necessarie per gestire il bucket. Le informazioni da fornire variano a seconda del tipo di bucket.

- a. Selezionare **Aggiungi** per aggiungere il bucket.

## Risultato

Astra Control Service aggiunge il bucket. È ora possibile scegliere questo bucket quando si crea una policy di protezione o si esegue un backup ad-hoc. È anche possibile impostare questo bucket come bucket predefinito per un'istanza di cloud.

## Modificare il bucket predefinito

È possibile modificare il bucket predefinito per un'istanza cloud. Astra Control Service utilizzerà questo bucket per impostazione predefinita per backup e cloni. Ogni istanza di cloud ha un proprio bucket predefinito.



Astra Control non assegna automaticamente un bucket predefinito per nessuna istanza di cloud. È necessario impostare manualmente un bucket predefinito per un'istanza cloud prima di eseguire operazioni di cloni delle applicazioni tra due cluster.

## Fasi

1. Accedere a **istanze cloud**.
2. Selezionare il menu di configurazione nella colonna **azioni** dell'istanza di cloud che si desidera modificare.
3. Selezionare **Modifica**.
4. Nell'elenco dei bucket, selezionare il bucket che si desidera impostare come predefinito per questa istanza di cloud.
5. Selezionare **Aggiorna**.

## Rimuovere una benna

È possibile rimuovere un bucket che non è più in uso o che non è integro. Questa operazione può essere utile per mantenere la configurazione dell'archivio di oggetti semplice e aggiornata.



- Non è possibile rimuovere un bucket predefinito. Se si desidera rimuovere tale bucket, selezionare prima un altro bucket come predefinito.
- Non è possibile rimuovere un bucket WORM (Write Once Read Many) prima che il periodo di conservazione del cloud provider del bucket sia scaduto. Le benne A VITE SENZA FINE sono contrassegnate con "bloccate" accanto al nome della benna.

## Prima di iniziare

- Prima di iniziare, verificare che non vi siano backup in esecuzione o completati per questo bucket.
- È necessario verificare che il bucket non venga utilizzato per i backup pianificati.

In tal caso, non sarà possibile continuare.

## Fasi

1. Accedere a **Bucket**.
2. Dal menu **azioni**, selezionare **Rimuovi**.



Astra Control garantisce innanzitutto che non vi siano policy di pianificazione che utilizzano il bucket per i backup e che non vi siano backup attivi nel bucket che si sta per rimuovere.

3. Digitare "remove" per confermare l'azione.
4. Selezionare **Sì, Rimuovi bucket**.

## [Anteprima tecnica] Gestione di un bucket utilizzando una risorsa personalizzata

È possibile aggiungere un bucket utilizzando una risorsa personalizzata (CR) Astra Control sul cluster di applicazioni. L'aggiunta di provider di bucket di archivi di oggetti è essenziale se si desidera eseguire il backup delle applicazioni e dello storage persistente o se si desidera clonare le applicazioni tra cluster. Astra Control memorizza i backup o i cloni nei bucket dell'archivio di oggetti definiti dall'utente. Se si utilizza il metodo di risorsa personalizzato, la funzionalità snapshot applicazione richiede un bucket.

Non è necessario un bucket in Astra Control se si esegue il clonaggio della configurazione dell'applicazione e dello storage persistente sullo stesso cluster.

La risorsa personalizzata bucket per Astra Control è nota come AppVault. Questo CR contiene le configurazioni necessarie per l'uso di una benna nelle operazioni di protezione.

### Prima di iniziare

- Assicurati di avere un bucket raggiungibile dai cluster gestiti da Astra Control Center.
- Assicurarsi di disporre delle credenziali per il bucket.
- Assicurarsi che la benna sia di uno dei seguenti tipi:
  - NetApp ONTAP S3
  - NetApp StorageGRID S3
  - Microsoft Azure
  - Generico S3



Amazon Web Services (AWS) e Google Cloud Platform (GCP) utilizzano il tipo di bucket S3 generico.



Sebbene Astra Control Center supporti Amazon S3 come provider di bucket S3 generico, Astra Control Center potrebbe non supportare tutti i vendor di archivi di oggetti che rivendicano il supporto S3 di Amazon.

### Fasi

1. Creare il file di risorse personalizzate (CR) e assegnargli un nome (ad esempio, `astra-appvault.yaml`).
2. Configurare i seguenti attributi:
  - **metadata.name:** (*obbligatorio*) il nome della risorsa personalizzata AppVault.
  - **Spec.prefix:** (*Optional*) percorso preceduto dai nomi di tutte le entità memorizzate in AppVault.
  - **spec.providerConfig:** (*obbligatorio*) Memorizza la configurazione necessaria per accedere ad AppVault utilizzando il provider specificato.
  - **spec.providerCredentials:** (*obbligatorio*) archivia i riferimenti a qualsiasi credenziale richiesta per accedere ad AppVault utilizzando il provider specificato.
    - **spec.providerCredentials.valueFromSecret:** (*opzionale*) indica che il valore della credenziale deve provenire da un segreto.



- **Key:** (obbligatorio se viene utilizzato il valore *FromSecret*) la chiave valida del segreto da selezionare.
- **Nome:** (obbligatorio se viene utilizzato il valore *FromSecret*) Nome del segreto che contiene il valore per questo campo. Deve trovarsi nello stesso spazio dei nomi.
- **spec.providerType:** (obbligatorio) determina cosa fornisce il backup; ad esempio, NetApp ONTAP S3 o Microsoft Azure.

Esempio YAML:

```
apiVersion: astra.netapp.io/v1
kind: AppVault
metadata:
  name: astra-appvault
spec:
  providerType: generic-s3
  providerConfig:
    path: testpath
    endpoint: 192.168.1.100:80
    bucketName: bucket1
    secure: "false"
  providerCredentials:
    accessKeyID:
      valueFromSecret:
        name: s3-creds
        key: accessKeyID
    secretAccessKey:
      valueFromSecret:
        name: s3-creds
        key: secretAccessKey
```

3. Dopo aver popolato il `astra-appvault.yaml` File con i valori corretti, applicare il CR:

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



Quando si aggiunge un bucket, Astra Control contrassegna un bucket con l'indicatore bucket predefinito. Il primo bucket creato diventa quello predefinito. Con l'aggiunta di bucket, è possibile decidere in un secondo momento ["impostare un altro bucket predefinito"](#).

## Trova ulteriori informazioni

- ["Utilizzare l'API di controllo Astra"](#)

## Monitorare le attività in esecuzione

In Astra Control è possibile visualizzare i dettagli relativi alle attività in esecuzione e alle attività che sono state completate, non riuscite o annullate nelle ultime 24 ore. Ad esempio, è possibile visualizzare lo stato di un'operazione di backup, ripristino o clonazione in esecuzione e visualizzare dettagli come percentuale completata e tempo rimanente stimato. È possibile visualizzare lo stato di un'operazione pianificata eseguita o avviata manualmente.

Durante la visualizzazione di un'attività in esecuzione o completata, è possibile espandere i dettagli dell'attività per visualizzare lo stato di ciascuna delle attività secondarie. La barra di avanzamento dell'attività è verde per le attività in corso o completate, blu per le attività annullate e rossa per le attività non riuscite a causa di un errore.



Per le operazioni di cloni, le sottoattività dell'attività consistono in un'operazione di snapshot e un'operazione di ripristino dello snapshot.

Per ulteriori informazioni sulle attività non riuscite, fare riferimento a ["Monitorare l'attività dell'account"](#).

### Fasi

1. Mentre un'attività è in esecuzione, passare a **applicazioni**.
2. Selezionare il nome di un'applicazione dall'elenco.
3. Nei dettagli dell'applicazione, selezionare la scheda **Tasks**.

È possibile visualizzare i dettagli delle attività correnti o passate e filtrare in base allo stato dell'attività.



Le attività vengono conservate nell'elenco **Tasks** per un massimo di 24 ore. È possibile configurare questo limite e altre impostazioni di monitoraggio attività utilizzando ["API di controllo Astra"](#).

## Gestisci il tuo account

### Impostare la fatturazione

Puoi utilizzare più metodi per gestire la fatturazione del tuo account Astra Control Service. Se utilizzi Azure o Amazon AWS, puoi sottoscrivere un piano Astra Control Service tramite Microsoft Azure Marketplace o AWS Marketplace. In questo modo, è possibile gestire i dettagli di fatturazione tramite Marketplace. In alternativa, puoi iscriverti direttamente a NetApp. Se ti iscrivi direttamente a NetApp, puoi gestire i tuoi dati di fatturazione tramite Astra Control Service. Se utilizzi Astra Control Service senza un abbonamento, sei automaticamente iscritto al Free Plan.

Il piano gratuito di Astra Control Service ti consente di gestire fino a 10 spazi dei nomi nel tuo account. Se si desidera gestire più di 10 spazi dei nomi, è necessario impostare la fatturazione eseguendo l'aggiornamento dal piano gratuito al piano Premium o iscrivendosi a Azure Marketplace o AWS Marketplace.

## Panoramica sulla fatturazione

Ci sono due tipi di costi associati all'utilizzo di Astra Control Service: Costi da parte di NetApp per l'Astra Control Service e costi da parte del cloud provider per volumi persistenti e storage a oggetti.

### Fatturazione Astra Control Service

Astra Control Service offre tre piani:

#### Piano gratuito

Gestisci fino a 10 spazi dei nomi gratuitamente.

#### Premium PayGo

Gestisci una quantità illimitata di spazi dei nomi a una velocità specifica, per spazio dei nomi.

#### Abbonamento Premium

Paga in anticipo a una tariffa scontata con un abbonamento annuale che ti consente di gestire fino a 20 spazi dei nomi per *namespace pack*. Contatta il reparto vendite NetApp per acquistare tutti i pacchetti necessari per la tua organizzazione. Ad esempio, acquistare 3 pacchetti per gestire 60 namespace da Astra Control Service. Se gestisci più spazi dei nomi di quelli consentiti dal tuo abbonamento annuale, ti verrà addebitato il costo del tasso di overage dipendente dall'abbonamento per spazio dei nomi aggiuntivo. Se non disponi ancora di un account Astra Control, l'acquisto dell'abbonamento Premium crea automaticamente un account Astra Control. Se disponi di un piano gratuito, sarai automaticamente convertito in un abbonamento Premium.

Quando crei un account Astra Control, sei automaticamente iscritto al Free Plan. La dashboard di Astra Control mostra quanti spazi dei nomi stai attualmente gestendo dai 10 spazi dei nomi liberi consentiti. La fatturazione inizia per uno spazio dei nomi quando viene gestita la prima applicazione contenente lo spazio dei nomi e si interrompe per tale spazio dei nomi quando l'ultima applicazione contenente lo spazio dei nomi non viene gestita.

Se cerchi di gestire un 11esimo spazio dei nomi, Astra Control ti avvisa che hai raggiunto il limite del Free Plan. Viene quindi richiesto di eseguire l'aggiornamento dal piano gratuito a un piano Premium. Ti verrà addebitata la tariffa di overage dipendente dall'abbonamento per spazio dei nomi extra.

Puoi passare a un Premium Plan in qualsiasi momento. Dopo l'aggiornamento, Astra Control inizia a addebitare i nomi dell'account. I primi 10 spazi dei nomi non rimangono nel piano libero.

### Fatturazione Google Cloud

I volumi persistenti sono supportati da NetApp Cloud Volumes Service e i backup delle applicazioni vengono memorizzati in un bucket di storage cloud di Google.

- ["Visualizza i dettagli dei prezzi per Cloud Volumes Service"](#).

Si noti che Astra Control Service supporta tutti i tipi di servizio e i livelli di servizio. Il tipo di servizio utilizzato dipende dal ["Regione di Google Cloud"](#).

- ["Visualizza i dettagli dei prezzi per i bucket di storage Google Cloud"](#).

### Fatturazione a Microsoft Azure

I volumi persistenti sono supportati da Azure NetApp Files e i backup delle applicazioni vengono memorizzati in un container Azure Blob.

- ["Visualizza i dettagli dei prezzi per Azure NetApp Files"](#).
- ["Visualizza i dettagli sui prezzi per lo storage Microsoft Azure Blob"](#).
- ["Visualizza i piani e i prezzi dei servizi Astra Control in Azure Marketplace"](#)



La tariffa di fatturazione di Azure per Astra Control Service è all'ora e una nuova ora di fatturazione inizia dopo 29 minuti dell'ora di utilizzo.

### Fatturazione Amazon Web Services

I volumi persistenti sono supportati da EBS o FSX per NetApp ONTAP e i backup delle tue applicazioni sono memorizzati in un bucket AWS.

- ["Visualizza i dettagli dei prezzi per Amazon Web Services"](#).

### Iscriviti a Astra Control Service in Azure Marketplace

Puoi iscriverti ad Astra Control Service utilizzando Azure Marketplace. Il tuo account e i dati di fatturazione vengono gestiti tramite Marketplace.



Per visualizzare una panoramica video della procedura di abbonamento a Azure Marketplace, visitare il sito Web all'indirizzo ["TV NetApp"](#).

### Fasi

1. Accedere alla ["Azure Marketplace"](#).
2. Selezionare **Get IT Now** (Ottieni ora).
3. Seguire le istruzioni per iscriversi a un piano.

### Iscriviti a Astra Control Service in AWS Marketplace

Puoi iscriverti ad Astra Control Service utilizzando AWS Marketplace. Il tuo account e i dati di fatturazione vengono gestiti tramite Marketplace.

### Fasi

1. Accedere alla ["Mercato AWS"](#).
2. Selezionare **Visualizza opzioni di acquisto**.
3. Se richiesto, accedere all'account AWS o creare un nuovo account.
4. Seguire le istruzioni per iscriversi a un piano.

### Iscriviti ad Astra Control Service direttamente con NetApp

Puoi iscriverti ad Astra Control Service dall'interfaccia utente di Astra Control Service o contattando NetApp Sales.

### Passa dal piano gratuito al piano Premium PayGo

Aggiorna il tuo piano di fatturazione in qualsiasi momento per iniziare a gestire più di 10 spazi dei nomi da Astra Control pagando a consumo. Tutto ciò di cui hai bisogno è una carta di credito valida.

### Fasi

1. Selezionare **account**, quindi **Billing**.
2. In **piani**, accedere a **Premium PayGo** e selezionare **Aggiorna ora**.
3. Fornisci i dettagli di pagamento per una carta di credito valida e seleziona **Upgrade to Premium Plan**.



Astra Control ti invia un'e-mail se la carta di credito sta per scadere.

### Risultato

Ora puoi gestire più di 10 spazi dei nomi. Astra Control inizia a addebitare *tutti* gli spazi dei nomi che stai attualmente gestendo.

### Passa dal piano gratuito all'abbonamento Premium

Contatta il reparto vendite NetApp per effettuare il prepagamento a un prezzo scontato con un abbonamento annuale.

### Fasi

1. Selezionare **account**, quindi **Billing**.
2. In **piani**, accedere a **abbonamento Premium** e selezionare **contatto vendite**.
3. Fornire i dettagli al team di vendita per avviare il processo.

### Risultato

Un rappresentante commerciale NetApp ti contatterà per elaborare l'ordine di acquisto. Una volta completato l'ordine, Astra Control rifletterà il piano corrente nella scheda **Billing**.

### Visualizza i costi correnti e la cronologia di fatturazione

Astra Control mostra i costi mensili correnti, oltre a una cronologia di fatturazione dettagliata per spazio dei nomi. Se si è sottoscritto un piano tramite un Marketplace, la cronologia di fatturazione non è visibile (ma è possibile visualizzarla accedendo al Marketplace).

### Fasi

1. Selezionare **account**, quindi **Billing**.

I costi correnti vengono visualizzati sotto la panoramica di fatturazione.

2. Per visualizzare la cronologia di fatturazione in base allo spazio dei nomi, selezionare **Cronologia fatturazione**.

Astra Control mostra i minuti di utilizzo e i costi per ogni namespace. Un minuto di utilizzo è il numero di minuti in cui Astra Control ha gestito lo spazio dei nomi durante un periodo di fatturazione.

3. Selezionare l'elenco a discesa per selezionare un mese precedente.

### Cambiare la carta di credito per Premium PayGo

Se necessario, puoi cambiare la carta di credito che Astra Control ha in archivio per la fatturazione.

### Fasi

1. Seleziona **account > fatturazione > metodo di pagamento**.
2. Selezionare l'icona di configurazione.

3. Modificare la carta di credito.

## Note importanti

- Il tuo piano di fatturazione è per account Astra Control.

Se si dispone di più account, ciascuno dispone di un proprio piano di fatturazione.

- La fattura di Astra Control include i costi per la gestione degli spazi dei nomi. Il tuo cloud provider addebita separatamente il back-end dello storage per i volumi persistenti.

["Scopri di più sui prezzi di Astra Control"](#).

- Ogni periodo di fatturazione termina l'ultimo giorno del mese.
- Non è possibile eseguire il downgrade da un piano Premium a un piano gratuito.

## Invitare e rimuovere utenti

Invita gli utenti a unirsi al tuo account Astra Control e rimuovi gli utenti che non dovrebbero più avere accesso all'account.

### Invitare utenti

I proprietari e gli amministratori dell'account possono invitare altri utenti a iscriversi all'account Astra Control.

### Fasi

1. Assicurarsi che l'utente disponga di un ["Accedi BlueXP"](#).
2. Selezionare **account**.
3. Nella scheda **utenti**, selezionare **invita**.
4. Inserire il nome, l'indirizzo e-mail e il ruolo dell'utente.

Tenere presente quanto segue:

- L'indirizzo e-mail deve corrispondere all'indirizzo e-mail utilizzato dall'utente per l'iscrizione a BlueXP.
  - Ciascun ruolo fornisce le seguenti autorizzazioni:
    - Un **Owner** dispone delle autorizzazioni di amministratore e può eliminare gli account.
    - Un **Admin** dispone delle autorizzazioni Member e può invitare altri utenti.
    - Un **Member** può gestire completamente app e cluster.
    - Un **Viewer** può visualizzare le risorse.
5. Per aggiungere vincoli a un utente con ruolo membro o visualizzatore, attivare la casella di controllo **limita ruolo ai vincoli**.

Per ulteriori informazioni sull'aggiunta di vincoli, fare riferimento a ["Gestire i ruoli"](#).

6. Per invitare un altro utente, selezionare **Aggiungi un altro utente** e immettere le informazioni relative al nuovo utente.

È possibile invitare fino a 10 utenti alla volta. È possibile spostarsi tra gli utenti che si stanno invitando nella parte sinistra della finestra di dialogo **invita utenti**.

7. Selezionare **invita utenti**.

### Risultato

L'utente o gli utenti riceveranno un'e-mail che li invita a unirsi al tuo account.

### Modificare il ruolo di un utente

Un account Owner può modificare il ruolo di tutti gli utenti, mentre un account Admin può modificare il ruolo degli utenti che hanno il ruolo di Amministratore, membro o visualizzatore.

### Fasi

1. Selezionare **account**.
2. Nella scheda **utenti**, selezionare il menu nella colonna **azioni** dell'utente.
3. Selezionare **Modifica ruolo**.
4. Selezionare un nuovo ruolo.
5. Per aggiungere vincoli a un utente con ruolo membro o visualizzatore, attivare la casella di controllo **limita ruolo ai vincoli**.

Per ulteriori informazioni sull'aggiunta di vincoli, fare riferimento a ["Gestire i ruoli"](#).

6. Selezionare **Conferma**.

### Risultato

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

### Rimuovere gli utenti

Un utente con il ruolo Owner può rimuovere altri utenti dall'account in qualsiasi momento.

### Fasi

1. Selezionare **account**.
2. Nella scheda **utenti**, selezionare gli utenti che si desidera rimuovere.
3. Selezionare il menu nella colonna **azioni** e selezionare **Rimuovi utente**.
4. Quando richiesto, confermare l'eliminazione digitando "Remove" (Rimuovi), quindi selezionare **Yes (Sì)**, **Remove User (Rimuovi utente)**.

### Risultato

Astra Control rimuove l'utente dall'account.

## Gestire i ruoli

È possibile gestire i ruoli aggiungendo vincoli dello spazio dei nomi e limitando i ruoli utente a tali vincoli. In questo modo è possibile controllare l'accesso alle risorse all'interno dell'organizzazione. È possibile utilizzare l'interfaccia utente di Astra Control o ["L'API Astra Control"](#) per gestire i ruoli.

### Aggiungere un vincolo dello spazio dei nomi a un ruolo

Un utente Admin o Owner può aggiungere vincoli dello spazio dei nomi.

## Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore.
4. Selezionare **Modifica ruolo**.
5. Attivare la casella di controllo **limita ruolo ai vincoli**.

La casella di controllo è disponibile solo per i ruoli Member o Viewer. È possibile selezionare un ruolo diverso dall'elenco a discesa **ruolo**.

6. Selezionare **Aggiungi vincolo**.

È possibile visualizzare l'elenco dei vincoli disponibili in base allo spazio dei nomi o all'etichetta dello spazio dei nomi.

7. Nell'elenco a discesa **tipo di vincolo**, selezionare **spazio dei nomi Kubernetes** o **etichetta dello spazio dei nomi Kubernetes** a seconda della configurazione degli spazi dei nomi.
8. Selezionare uno o più spazi dei nomi o etichette dall'elenco per comporre un vincolo che limiti i ruoli a tali spazi dei nomi.
9. Selezionare **Conferma**.

La pagina **Modifica ruolo** visualizza l'elenco dei vincoli scelti per questo ruolo.

10. Selezionare **Conferma**.

Nella pagina **account**, è possibile visualizzare i vincoli per qualsiasi ruolo membro o visualizzatore nella colonna **ruolo**.



Se si abilitano i vincoli per un ruolo e si seleziona **Conferma** senza aggiungere alcun vincolo, il ruolo viene considerato con restrizioni complete (al ruolo viene negato l'accesso a tutte le risorse assegnate agli spazi dei nomi).

## Rimuovere un vincolo dello spazio dei nomi da un ruolo

Un utente Admin o Owner può rimuovere un vincolo dello spazio dei nomi da un ruolo.

## Fasi

1. Nell'area di navigazione **Gestisci account**, selezionare **account**.
2. Selezionare la scheda **utenti**.
3. Nella colonna **azioni**, selezionare il pulsante di menu per un utente con ruolo membro o visualizzatore con vincoli attivi.
4. Selezionare **Modifica ruolo**.

La finestra di dialogo **Modifica ruolo** visualizza i vincoli attivi per il ruolo.

5. Selezionare la **X** a destra del vincolo da rimuovere.
6. Selezionare **Conferma**.



## Per ulteriori informazioni

- ["Ruoli e spazi dei nomi degli utenti"](#)

## Aggiungere e rimuovere le credenziali

Aggiungi e rimuovi le credenziali del cloud provider dal tuo account in qualsiasi momento. Astra Control utilizza queste credenziali per rilevare un cluster Kubernetes, le applicazioni sul cluster e per eseguire il provisioning delle risorse per conto dell'utente.

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

### Aggiungere credenziali

Il metodo più comune per aggiungere credenziali ad Astra Control consiste nella gestione dei cluster, ma è anche possibile aggiungere credenziali dalla pagina account. Le credenziali saranno quindi disponibili per la gestione di cluster Kubernetes aggiuntivi.

### Prima di iniziare

- Per Amazon Web Services, è necessario disporre dell'output JSON delle credenziali dell'account IAM utilizzato per creare il cluster. ["Scopri come configurare un utente IAM"](#).
- Per GKE, è necessario disporre del file della chiave dell'account di servizio per un account di servizio che dispone delle autorizzazioni necessarie. ["Scopri come configurare un account di servizio"](#).
- Per AKS, è necessario disporre del file JSON che contiene l'output dell'interfaccia CLI di Azure al momento della creazione dell'entità del servizio. ["Scopri come configurare un service principal"](#).

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

### Fasi

1. Selezionare **account > credenziali**.
2. Selezionare **Aggiungi credenziali**.
3. Selezionare **Microsoft Azure**.
4. Selezionare **Google Cloud Platform**.
5. Selezionare **Amazon Web Services**.
6. Immettere un nome per le credenziali che le distinguano dalle altre in Astra Control.
7. Fornire le credenziali richieste.
8. **Microsoft Azure**: Fornisci ad Astra Control i dettagli sull'entità del servizio Azure caricando un file JSON o incollando il contenuto del file JSON dagli Appunti.

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

9. **Google Cloud Platform**: Fornire il file delle chiavi dell'account del servizio Google Cloud caricando il file o incollando il contenuto dagli Appunti.
10. **Amazon Web Services**: Fornisci le credenziali utente IAM di Amazon Web Services caricando il file o incollando il contenuto dagli Appunti.
11. Selezionare **Aggiungi credenziali**.

## Risultato

Le credenziali sono ora disponibili per la selezione quando si aggiunge un cluster ad Astra Control.

## Rimuovere le credenziali

Rimuovere le credenziali da un account in qualsiasi momento. Rimuovere le credenziali solo dopo "[annullamento della gestione di tutti i cluster](#)", a meno che non si stiano ruotando le credenziali (fare riferimento a [Ruotare le credenziali](#)).



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

## Fasi

1. Selezionare **account > credenziali**.
2. Selezionare l'elenco a discesa nella colonna **Stato** per le credenziali che si desidera rimuovere.
3. Selezionare **Rimuovi**.
4. Digitare il nome delle credenziali per confermare l'eliminazione, quindi selezionare **Sì, Rimuovi credenziali**.

## Risultato

Astra Control rimuove le credenziali dall'account.

## Ruotare le credenziali

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

## Fasi

1. Rimuovere le credenziali esistenti seguendo la procedura descritta in [Rimuovere le credenziali](#).
2. Aggiungere le nuove credenziali seguendo la procedura descritta in [Aggiungere credenziali](#).
3. Aggiorna tutti i bucket per utilizzare le nuove credenziali:
  - a. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
  - b. Selezionare l'elenco a discesa nella colonna **azioni** per il bucket che si desidera modificare.
  - c. Selezionare **Modifica**.
  - d. Nella sezione **Select credentials** (Seleziona credenziali), scegliere le nuove credenziali aggiunte ad Astra Control.
  - e. Selezionare **Aggiorna**.
  - f. Ripetere i passaggi da **b** a **e** per tutti i bucket rimanenti sul sistema.

## Risultato

Astra Control inizia a utilizzare le nuove credenziali del cloud provider.

## Monitorare l'attività dell'account

Puoi visualizzare i dettagli delle attività nel tuo account Astra Control. Ad esempio, quando sono stati invitati nuovi utenti, quando è stato aggiunto un cluster o quando è

stata acquisita una snapshot. È inoltre possibile esportare l'attività dell'account in un file CSV.

### Visualizza tutte le attività dell'account in Astra Control

1. Selezionare **Activity** (attività).
2. Utilizza i filtri per restringere l'elenco delle attività o utilizza la casella di ricerca per trovare esattamente ciò che stai cercando.
3. Selezionare **Export to CSV** (Esporta in CSV) per scaricare l'attività dell'account in un file CSV.

### Visualizzare l'attività dell'account per un'applicazione specifica

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Activity** (attività).

### Visualizzare l'attività dell'account per i cluster

1. Selezionare **Clusters**, quindi il nome del cluster.
2. Selezionare **Activity** (attività).

## Visualizzare e gestire le notifiche

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

Il numero di notifiche non lette è disponibile nella parte superiore destra dell'interfaccia.

Puoi visualizzare queste notifiche e contrassegnarle come lette (questa operazione può risultare utile se desideri cancellare le notifiche non lette come noi).

### Fasi

1. Selezionare il numero di notifiche non lette in alto a destra.
2. Esaminare le notifiche, quindi selezionare **Contrassegna come letto** o **Mostra tutte le notifiche**.

Se si seleziona **Mostra tutte le notifiche**, viene caricata la pagina Notifiche.

3. Nella pagina **Notifiche**, visualizzare le notifiche, selezionare quelle che si desidera contrassegnare come lette, selezionare **azione** e selezionare **Contrassegna come letta**.

## Chiudere l'account

Se non hai più bisogno del tuo account Astra Control, puoi chiuderlo in qualsiasi momento.



I bucket creati automaticamente da Astra Control verranno eliminati automaticamente alla chiusura dell'account.

### Fasi

1. ["Annulla la gestione di tutte le applicazioni e i cluster"](#).
2. ["Rimuovere le credenziali da Astra Control"](#).

3. Seleziona **account > fatturazione > metodo di pagamento**.
4. Selezionare **Chiudi account**.
5. Inserire il nome dell'account e confermare per chiudere l'account.

## Gestire le istanze cloud

Un'istanza di cloud è un dominio unico all'interno di un cloud provider. È possibile creare più istanze cloud per ciascun provider cloud e ogni istanza cloud ha il proprio nome, le proprie credenziali e i cluster associati.

Si crea un'istanza cloud quando si aggiunge un nuovo cluster ad Astra Control. È possibile modificare un'istanza cloud per modificarne il nome o il bucket predefinito utilizzando l'interfaccia utente di Astra Control ed eseguire altre azioni con l'istanza cloud utilizzando l'API di Astra Control.

### Aggiungere un'istanza cloud

È possibile aggiungere una nuova istanza di cloud quando si aggiunge un nuovo cluster ad Astra Control. Fare riferimento a ["Inizia a gestire i cluster Kubernetes da Astra Control Service"](#) per ulteriori informazioni.

### Modificare un'istanza di cloud

È possibile modificare un'istanza di cloud esistente per un provider di cloud.

#### Fasi

1. Accedere a **istanze cloud**.
2. Nell'elenco delle istanze cloud, selezionare il menu **azioni** dell'istanza cloud che si desidera modificare.
3. Selezionare **Modifica**.

In questa pagina, è possibile aggiornare il nome e il bucket predefinito per l'istanza del cloud.



Ogni istanza di cloud in Astra Control deve avere un nome univoco.

### Ruotare le credenziali per un'istanza cloud

È possibile utilizzare l'API di controllo Astra per ruotare le credenziali per un'istanza cloud. Per saperne di più, ["Consultare i documenti di automazione Astra"](#).

### Rimuovere un'istanza cloud

È possibile utilizzare l'API Astra Control per rimuovere un'istanza cloud da un provider cloud. Per saperne di più, ["Consultare i documenti di automazione Astra"](#).

## Abilita Astra Control Provisioner

Astra Trident le versioni 23,10 e successive includono la possibilità di utilizzare Astra Control Provisioner, che consente agli utenti dotati di licenza Astra Control di accedere a funzionalità avanzate di provisioning dello storage. Astra Control Provisioner fornisce questa funzionalità estesa oltre alle funzionalità standard basate su CSI Astra Trident. È

possibile utilizzare questa procedura per abilitare e installare Astra Control Provisioner.

L'abbonamento a Astra Control Service include automaticamente la licenza per l'utilizzo di Astra Control Provisioner.

In arrivo gli update di Astra Control, Astra Control Provisioner sostituirà Astra Trident come provisioner di storage e orchestrator e sarà obbligatorio per l'utilizzo di Astra Control. Per questo motivo, si consiglia vivamente agli utenti di Astra Control di attivare Astra Control Provisioner. Astra Trident continuerà a rimanere open source e ad essere rilasciato, mantenuto, supportato e aggiornato con le nuove CSI e altre funzionalità di NetApp.

### Come faccio a sapere se devo abilitare Astra Control Provisioner?

Se Aggiungi un cluster a Astra Control Service che non ha Astra Trident precedentemente installato, il cluster verrà contrassegnato come `Eligible`. Dopo di lei "[Aggiungi il cluster a Astra Control](#)", Astra Control provisioner verrà abilitato automaticamente.

Se il cluster non è contrassegnato `Eligible`, verrà contrassegnato `Partially eligible` per uno dei seguenti motivi:

- Sta utilizzando una versione meno recente di Astra Trident
- Sta utilizzando un Astra Trident 23,10 che non ha ancora attivato l'opzione di provisioning
- Si tratta di un tipo di cluster che non consente l'abilitazione automatica

Per `Partially eligible` Casi, usa queste istruzioni per abilitare manualmente Astra Control Provisioner per il tuo cluster.

**Add cluster** STEP 2/4: CLUSTER

CLUSTER

Choose an Azure Kubernetes Service cluster to enable application data management and the Astra Control storage operator.

Some Kubernetes cluster(s) below have private networking. [Learn more](#)

| Cluster  | Location      | Eligibility        |
|--|---------------|--------------------|
| <input checked="" type="radio"/> sandbox-ragnarok-aks-02 | centraluseuap | Eligible           |
| <input type="radio"/> sandbox-ragnarok-aks-03            | centraluseuap | Partially eligible |
| <input type="radio"/> sandbox-rstephe2-aks-01            | centraluseuap | Eligible           |

Configuration required  
Failed to detect Astra Control Provisioner on cluster

← Back   Next →

### Prima di attivare Astra Control Provisioner

Se hai già un Astra Trident senza Astra Control Provisioner e vuoi abilitare Astra Control Provisioner, esegui prima quanto segue:

- **Se Astra Trident è installato, conferma che la sua versione si trovi all'interno di una finestra a quattro release:** Puoi eseguire un aggiornamento diretto a Astra Trident 24,02 con Astra Control Provisioner se il tuo Astra Trident si trova all'interno di una finestra a quattro release della versione 24,02. Ad esempio, puoi eseguire l'upgrade direttamente da Astra Trident 23,04 a 24,02.
- **Confermi che il tuo cluster ha un'architettura di sistema AMD64:** L'immagine Astra Control Provisioner è fornita in entrambe le architetture CPU AMD64 e ARM64, ma solo AMD64 è supportato da Astra Control.

## Fasi

1. Accedere al Registro di sistema dell'immagine di controllo Astra di NetApp:
  - a. Effettua l'accesso all'interfaccia utente di Astra Control Service e registra l'ID account Astra Control.
    - i. Selezionare l'icona della figura in alto a destra nella pagina.
    - ii. Selezionare **API access**.
    - iii. Annotare l'ID account.
  - b. Nella stessa pagina, selezionare **generate API token**, copiare la stringa del token API negli Appunti e salvarla nell'editor.
  - c. Accedere al registro Astra Control utilizzando il metodo preferito:

```
docker login cr.astra.netapp.io -u <account-id> -p <api-token>
```

```
crane auth login cr.astra.netapp.io -u <account-id> -p <api-token>
```

2. (Solo registri personalizzati) attenersi alla seguente procedura per spostare l'immagine nel registro personalizzato. Se non si utilizza un registro, seguire i passaggi dell'operatore Trident nel [sezione successiva](#).



Per i seguenti comandi, puoi utilizzare Podman al posto di Docker. Se si utilizza un ambiente Windows, si consiglia di utilizzare PowerShell.

## Docker

- a. Estrarre l'immagine di Astra Control provisioner dal Registro di sistema:



L'immagine estratta non supporta più piattaforme e supporta solo la stessa piattaforma dell'host che ha estratto l'immagine, ad esempio Linux AMD64.

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform <cluster platform>
```

### Esempio:

```
docker pull cr.astra.netapp.io/astra/trident-acp:24.02.0
--platform linux/amd64
```

- b. Contrassegnare l'immagine:

```
docker tag cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

- c. Inviare l'immagine al registro personalizzato:

```
docker push <my_custom_registry>/trident-acp:24.02.0
```

## Gru

- a. Copiare il manifesto di Astra Control Provisioner nel registro personalizzato:

```
crane copy cr.astra.netapp.io/astra/trident-acp:24.02.0
<my_custom_registry>/trident-acp:24.02.0
```

3. Determinare se il metodo di installazione originale di Astra Trident ha utilizzato un.
4. Abilita Astra Control Provisioner in Astra Trident utilizzando il metodo di installazione utilizzato originariamente:

## Operatore Astra Trident

- a. ["Scaricare il programma di installazione di Astra Trident ed estrarlo"](#).
- b. Completa questi passaggi se non hai ancora installato Astra Trident o se hai rimosso l'operatore dall'implementazione originale di Astra Trident:
  - i. Creare il CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.1
6.yaml
```

- ii. Creare lo spazio dei nomi tridente (`kubectl create namespace trident`) o confermare che lo spazio dei nomi tridente esiste ancora (`kubectl get all -n trident`). Se lo spazio dei nomi è stato rimosso, crearlo di nuovo.
- c. Aggiorna Astra Trident alla versione 24.02.0:



Per i cluster che eseguono Kubernetes 1.24 o versioni precedenti, utilizzare `bundle_pre_1_25.yaml`. Per i cluster che eseguono Kubernetes 1.25 o versioni successive, utilizzare `bundle_post_1_25.yaml`.

```
kubectl -n trident apply -f trident-installer/deploy/<bundle-
name.yaml>
```

- d. Verificare che Astra Trident sia in esecuzione:

```
kubectl get torc -n trident
```

Risposta:

```
NAME          AGE
trident       21m
```

- e. se si dispone di un registro che utilizza segreti, creare un segreto da utilizzare per estrarre l'immagine di Astra Control Provisioner:

```
kubectl create secret docker-registry <secret_name> -n trident
--docker-server=<my_custom_registry> --docker-username=<username>
--docker-password=<token>
```

- f. Modificare il TridentOrchestrator CR e apportare le seguenti modifiche:



```
kubectl edit torc trident -n trident
```

- i. Impostare una posizione del Registro di sistema personalizzata per l'immagine Astra Trident o estrarla dal Registro di sistema Astra Control (`tridentImage: <my_custom_registry>/trident:24.02.0` oppure `tridentImage: netapp/trident:24.02.0`).
- ii. Abilita Astra Control Provisioner (`enableACP: true`).
- iii. Impostare la posizione del Registro di sistema personalizzata per l'immagine Astra Control Provisioner o estrarla dal Registro di sistema Astra Control (`acpImage: <my_custom_registry>/trident-acp:24.02.0` oppure `acpImage: cr.astra.netapp.io/astra/trident-acp:24.02.0`).
- iv. Se stabilito [segreti di estrazione delle immagini](#) in precedenza, è possibile impostarle qui (`imagePullSecrets: - <secret_name>`). Usare lo stesso nome segreto che hai stabilito nei passaggi precedenti.

```
apiVersion: trident.netapp.io/v1
kind: TridentOrchestrator
metadata:
  name: trident
spec:
  debug: true
  namespace: trident
  tridentImage: <registry>/trident:24.02.0
  enableACP: true
  acpImage: <registry>/trident-acp:24.02.0
  imagePullSecrets:
  - <secret_name>
```

- g. Salvare e uscire dal file. Il processo di distribuzione si avvia automaticamente.
- h. Verificare che l'operatore, la distribuzione e i replicaset siano stati creati.

```
kubectl get all -n trident
```



In un cluster Kubernetes dovrebbe esserci solo **un'istanza** dell'operatore. Non creare implementazioni multiple dell'operatore Astra Trident.

- i. Verificare `trident-acp` il container è in esecuzione e così `acpVersion` è `24.02.0` con stato di `Installed`:

```
kubectl get torc -o yaml
```

Risposta:

```
status:
  acpVersion: 24.02.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:24.02.0
    enableACP: "true"
    ...
  ...
status: Installed
```

### tridentctl

- "Scaricare il programma di installazione di Astra Trident ed estrarlo".
- "Se disponi già di un Astra Trident, disinstallarlo dal cluster che lo ospita".
- Installa Astra Trident con Astra Control Provisioner abilitato (`--enable-acp=true`):

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:24.02
```

- Confermare che Astra Control Provisioner è stato abilitato:

```
./tridentctl -n trident version
```

Risposta:

```
+-----+-----+-----+ | SERVER
VERSION | CLIENT VERSION | ACP VERSION | +-----+
+-----+-----+-----+ | 24.02.0 | 24.02.0 | 24.02.0. |
+-----+-----+-----+
```

### Timone

- Se hai installato Astra Trident 23.07.1 o una versione precedente, "disinstallazione" l'operatore e gli altri componenti.
- Se il cluster Kubernetes esegue la versione 1,24 o precedente, elimina psp:

```
kubectl delete psp tridentoperatorpod
```

- Aggiungere il repository Astra Trident Helm:

```
helm repo add netapp-trident https://netapp.github.io/trident-helm-chart
```

d. Aggiornare il grafico Helm:

```
helm repo update netapp-trident
```

Risposta:

```
Hang tight while we grab the latest from your chart
repositories...
...Successfully got an update from the "netapp-trident" chart
repository
Update Complete. ☐Happy Helming!☐
```

e. Elencare le immagini:

```
./tridentctl images -n trident
```

Risposta:

```
| v1.28.0 | netapp/trident:24.02.0|
| | docker.io/netapp/trident-
autosupport:24.02 |
| | registry.k8s.io/sig-storage/csi-
provisioner:v4.0.0|
| | registry.k8s.io/sig-storage/csi-
attacher:v4.5.0|
| | registry.k8s.io/sig-storage/csi-
resizer:v1.9.3|
| | registry.k8s.io/sig-storage/csi-
snapshotter:v6.3.3|
| | registry.k8s.io/sig-storage/csi-node-
driver-registrar:v2.10.0 |
| | netapp/trident-operator:24.02.0 (optional)
```

f. Assicurarsi che l'operatore di tridente 24.02.0 sia disponibile:

```
helm search repo netapp-trident/trident-operator --versions
```

Risposta:

| NAME                            | CHART VERSION | APP VERSION |   |
|---------------------------------|---------------|-------------|---|
| DESCRIPTION                     |               |             |   |
| netapp-trident/trident-operator | 100.2402.0    | 24.02.0     | A |

g. Utilizzare `helm install` ed eseguire una delle seguenti opzioni che includono queste impostazioni:

- Un nome per la posizione di distribuzione
- La versione di Astra Trident
- Il nome dell'immagine di Astra Control provisioner
- Il flag per abilitare il provisioner
- (Facoltativo) percorso del Registro di sistema locale. Se si utilizza un registro locale, il "Immagini Trident" Può trovarsi in un registro o in registri diversi, ma tutte le immagini CSI devono trovarsi nello stesso registro.
- Il namespace Trident

### Opzioni

- Immagini senza registro

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=cr.astra.netapp.io/astra/trident-
acp:24.02.0 --set enableACP=true --set operatorImage=netapp/trident-
operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

- Immagini in uno o più registri

```
helm install trident netapp-trident/trident-operator --version
100.2402.0 --set acpImage=<your-registry>:<acp image> --set
enableACP=true --set imageRegistry=<your-registry>/sig-storage --set
operatorImage=netapp/trident-operator:24.02.0 --set
tridentAutosupportImage=docker.io/netapp/trident-autosupport:24.02
--set tridentImage=netapp/trident:24.02.0 --namespace trident
```

È possibile utilizzare `helm list` per rivedere i dettagli dell'installazione, ad esempio nome, spazio dei nomi, grafico, stato, versione dell'applicazione, e numero di revisione.

Se hai problemi nell'implementazione di Trident utilizzando Helm, esegui questo comando per disinstallare completamente Astra Trident:

```
./tridentctl uninstall -n trident
```

**Non fare "Rimuovere completamente i CRD Astra Trident"** Come parte della disinstallazione prima di tentare di attivare nuovamente Astra Control Provisioner.

## Risultato

La funzionalità Astra Control Provisioner è abilitata ed è possibile utilizzare qualsiasi funzionalità disponibile per la versione in esecuzione.

Dopo l'installazione di Astra Control provisioner, il cluster che ospita il provisioner nell'interfaccia utente Astra Control mostrerà un `ACP version` piuttosto che `Trident version` campo e numero della versione installata corrente.

**CLUSTER STATUS**

Available

|  |                                 |   |                           |
|--|---------------------------------|---|---------------------------|
| Version<br>v1.24.9+rke2r2              | Managed<br>2024/03/15 17:32 UTC | Kube-system namespace UID<br>[redacted]     | ACP Version<br>[redacted] |
| Private route identifier<br>[redacted] | Cloud instance<br>private       | Default bucket<br>astra-bucket1 (inherited) |                           |

Overview | Namespaces | Storage | Activity

## Per ulteriori informazioni

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

# Annulla la gestione di app e cluster

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

## Interrompere la gestione di un'applicazione

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

Quando si annulla la gestione di un'applicazione:

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

## Fasi

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

## Risultato

Astra Control interrompe la gestione dell'applicazione.

## Interrompere la gestione di un cluster

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



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

Come Best practice, si consiglia di rimuovere il cluster da Astra Control prima di eliminarlo tramite GCP.

Quando si annulla la gestione di un cluster:

- Questa azione impedisce la gestione del cluster da parte di Astra Control. Non apporta modifiche alla configurazione del cluster e non elimina il cluster.
- Astra Control Provisioner o Astra Trident non verranno disinstallati dal cluster. ["Scopri come disinstallare Astra Trident"](#).

## Fasi

1. Selezionare **Clusters**.
2. Selezionare la casella di controllo del cluster che non si desidera più gestire.
3. Dal menu delle opzioni nella colonna **azioni**, selezionare **Annulla gestione**.
4. Confermare che si desidera annullare la gestione del cluster, quindi selezionare **Sì, Annulla gestione**.

## Risultato

Lo stato del cluster cambia in **Removing** (Rimozione). In seguito, il cluster verrà rimosso dalla pagina **Clusters** e non sarà più gestito da Astra Control.

## Eliminazione di cluster dal provider cloud

Prima di eliminare un cluster Kubernetes con volumi persistenti (PV) che risiedono nelle classi di storage NetApp, è necessario prima eliminare le dichiarazioni di volumi persistenti (PVC) seguendo uno dei metodi riportati di seguito. Eliminando PVC e PV prima di eliminare il cluster, non riceverai fatture inattese dal tuo cloud provider.

- Metodo n. 1\*: Eliminare gli spazi dei nomi dei carichi di lavoro dell'applicazione dal cluster. Non eliminare lo spazio dei nomi Trident.
- Metodo 2\*: Eliminare i PVC e i pod o l'implementazione in cui sono montati i PVS.

Quando gestisci un cluster Kubernetes da Astra Control, le applicazioni su quel cluster utilizzano il tuo cloud provider come back-end dello storage per i volumi persistenti. Se elimini il cluster dal tuo cloud provider senza prima rimuovere il PVS, i volumi di back-end vengono *non* cancellati insieme al cluster.

Utilizzando uno dei metodi descritti in precedenza, il PVS corrispondente viene eliminato dal cluster. Assicurarsi che non vi siano PVS che risiedono nelle classi di storage NetApp sul cluster prima di eliminarlo.

Se i volumi persistenti non sono stati eliminati prima dell'eliminazione del cluster, sarà necessario eliminare manualmente i volumi di back-end dal provider cloud.

# Implementa un'istanza autogestita di Astra Control

Se desideri un'istanza autogestita di Astra Control all'interno della rete, puoi implementare Astra Control Center direttamente da Astra Control Service.

## Fasi

1. Nell'area Getting Started del Dashboard, selezionare **distribuire un'istanza autogestita di Astra Control**.
2. Effettuare una delle seguenti operazioni:
  - Generare un nuovo token API selezionando **generate**.
  - Incolla in un token dell'API REST Astra Control esistente. Fare riferimento a. "[Documentazione di Astra Automation](#)" Per istruzioni sulla generazione di un token API.
3. Seguire le istruzioni nella finestra **Deploy Astra Control Center**.

## Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

## Informazioni sul marchio commerciale

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