Utilizzare Astra Control Center

Astra Control Center

NetApp
August 11, 2025

This PDF was generated from https://docs.netapp.com/it-it/astra-control-center-2310/use/manage-apps.html on August 11, 2025. Always check docs.netapp.com for the latest.

Sommario

Utilizzare Astra Control Center . . . 1
- Inizia a gestire le app . . . 1
  - Requisiti di gestione delle applicazioni . . . 1
  - Metodi di installazione delle applicazioni supportati . . . 1
  - Installa le app sul tuo cluster . . . 2
  - Definire le applicazioni . . . 2
  - E gli spazi dei nomi di sistema? . . . 6
  - Esempio: Policy di protezione separata per release diverse . . . 6
  - Trova ulteriori informazioni . . . 6
- Proteggi le app . . . 6
  - Panoramica della protezione . . . 7
  - Proteggi le app con snapshot e backup . . . 7
  - Ripristinare le applicazioni . . . 15
  - Replica delle applicazioni tra back-end di storage utilizzando la tecnologia SnapMirror . . . 20
  - Clonare e migrare le applicazioni . . . 27
  - Gestire gli hook di esecuzione delle applicazioni . . . 30
  - Proteggi Astra Control Center con Astra Control Center . . . 39
- Monitorare lo stato delle applicazioni e del cluster . . . 49
  - Visualizza un riepilogo dello stato delle applicazioni e dei cluster . . . 49
  - Visualizzare lo stato dei cluster e gestire le classi di storage . . . 50
  - Visualizza lo stato di salute e i dettagli di un'applicazione . . . 51
- Gestisci il tuo account . . . 52
  - Gestire utenti e ruoli locali . . . 52
  - Gestire l'autenticazione remota . . . 55
  - Gestire utenti e gruppi remoti . . . 57
  - Visualizzare e gestire le notifiche . . . 59
  - Aggiungere e rimuovere le credenziali . . . 60
  - Monitorare l'attività dell'account . . . 60
  - Aggiornare una licenza esistente . . . 61
- Gestire i bucket . . . 62
  - Modificare un bucket . . . 63
  - Impostare il bucket predefinito . . . 63
  - Ruotare o rimuovere le credenziali bucket . . . 63
  - Rimuovere una benna . . . 64
  - Trova ulteriori informazioni . . . 65
- Gestire il back-end dello storage . . . 65
  - Visualizza i dettagli del back-end dello storage . . . 65
  - Modificare i dettagli dell'autenticazione back-end dello storage . . . 66
  - Gestire un backend di storage rilevato . . . 67
  - Annullare la gestione di un backend di storage . . . 67
  - Rimuovere un backend di storage . . . 68
  - Trova ulteriori informazioni . . . 68
- Monitorare le attività in esecuzione . . . 68

Monitorare l’infrastruttura con connessioni Cloud Insights, Prometheus o Fluentd . . . 69
Aggiungere un server proxy per le connessioni a Cloud Insights o al sito di supporto NetApp . . . 69
Connettersi a Cloud Insights . . . 71
Connettiti a Prometheus . . . 74
Connettersi a Fluentd . . . 76
Annulla la gestione di app e cluster . . . 78
Annullare la gestione di un’applicazione . . . 78
Annullare la gestione di un cluster . . . 78
Aggiornare Astra Control Center . . . 79
Scarica ed estrai Astra Control Center . . . 81
Rimuovere il plug-in NetApp Astra kubectl e installarlo di nuovo . . . 82
Aggiungere le immagini al registro locale . . . 83
Installare l’operatore Astra Control Center aggiornato . . . 85
Aggiornare Astra Control Center . . . 89
Verificare lo stato del sistema . . . 91
Abilita Astra Control Provisioner . . . 91
(Fase 1) scaricare ed estrarre Astra Control Provisioner . . . 92
(Fase 2) attiva Astra Control Provisioner in Astra Trident . . . 95
Risultato . . . 98
Disinstallare Astra Control Center . . . 99
Risoluzione dei problemi di disinstallazione . . . 100
Trova ulteriori informazioni . . . 102

Utilizzare Astra Control Center

Inizia a gestire le app

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

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 le applicazioni utilizzando Astra Control Center, è necessaria la licenza di valutazione di Astra Control Center o una licenza completa.
- **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 risorse Kubernetes 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 garantire che ciò avvenga.

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

  - "Apache K8ssandra"

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

  - "Ci Jenkins"
  - "Cluster XtraDB Percona"

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

Installa le app sul tuo cluster

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

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, "Consulta 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 intendi utilizzare più spazi dei nomi con le tue applicazioni in Astra Control, "modificare i ruoli utente con vincoli dello spazio dei nomi" Dopo l'aggiornamento a una versione di Astra Control Center con supporto di più namespace.
- Per istruzioni su come gestire le applicazioni utilizzando l'API Astra Control, vedere "Astra Automation e informazioni API".

Opzioni di gestione delle applicazioni

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

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 delle policy di protezione sulle risorse Kubernetes può causare conflitti di dati. Scopri di più in un esempio.

Espandi per ulteriori informazioni 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, "Consulta 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 nella Search (Cerca) per visualizzare le risorse aggiuntive incluse nell'ambito del cluster.

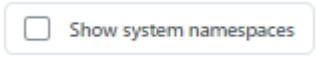
Definire uno spazio dei nomi da gestire come applicazione

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 si intende gestire e proteggere tutte le risorse in un determinato namespace in modo simile e a intervalli comuni.

Fasi

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

Se si desidera 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 con più spazi dei nomi, vedere Definire le risorse da gestire come applicazione.

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

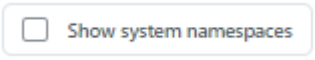
"Scopri di più".

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

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**.



Per impostazione predefinita, Astra Control Center non viene visualizzato come applicazione gestibile, ma è possibile eseguire il backup e il ripristino di un'istanza di Astra Control Center utilizzando un'altra istanza di Astra Control Center.

Esempio: Policy di protezione separata per release diverse

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

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

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

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

Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"
- "Annullare la gestione di un'applicazione"

Proteggi le app

Panoramica della protezione

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

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

Workflow di protezione delle app

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

[Uno] Proteggi tutte le app

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

[Due] Configurare una policy di protezione per ogni applicazione

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

[Tre] Modificare i criteri di protezione

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

[Quattro] Replica delle applicazioni su un cluster remoto

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

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

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

Proteggi le app con snapshot e backup

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

A proposito di questa attività

- **Helm ha implementato le app**: Se utilizzi Helm per implementare le app, Astra Control Center richiede Helm versione 3. La gestione e la clonazione delle applicazioni implementate con Helm 3 (o aggiornate da

Helm 2 a Helm 3) sono completamente supportate. Le app implementate con Helm 2 non sono supportate.

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

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

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

- Configurare un criterio di protezione
- Creare un'istantanea
- Creare un backup
- 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.

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.

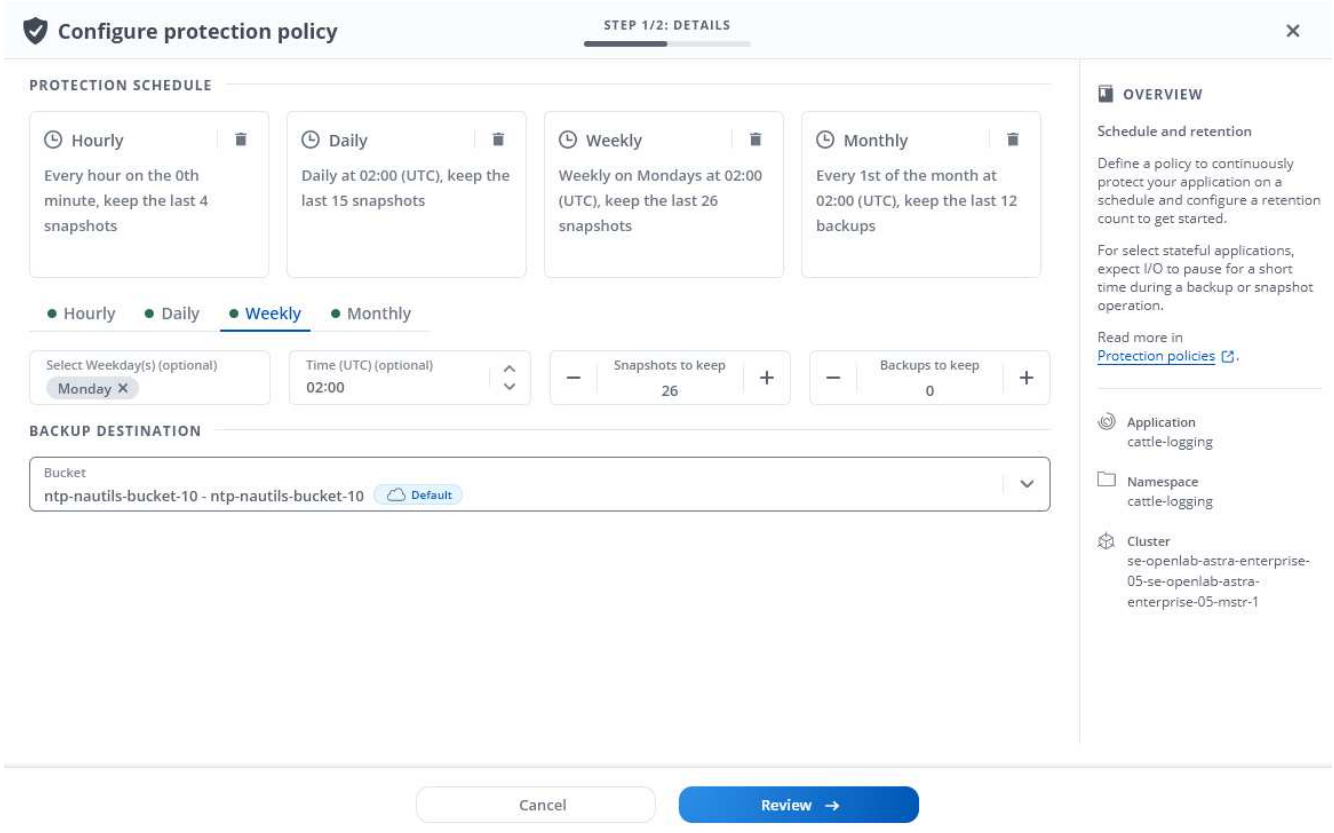
Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Configura policy di protezione**.
4. Definire un programma di protezione scegliendo il numero di snapshot e backup da conservare ogni ora, ogni giorno, ogni settimana e ogni mese.

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

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.



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

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.

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. Esaminare il riepilogo dell'istantanea e selezionare **Snapshot**.

Risultato

Viene avviato il processo di snapshot. Un'istantanea ha successo quando lo stato è **integro** nella colonna **Stato** della pagina **Data Protection** > **Snapshot**.

Creare un backup

Puoi eseguire il backup di un'app in qualsiasi momento.

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.

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`

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

Risultato

Astra Control crea un backup dell'applicazione.

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

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

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

Prima di iniziare

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

Espandere per la procedura di configurazione

1. Sul back-end dello storage ONTAP:

   a. Trova la SVM che ospita `ontap-nas-economy`volumi basati su -dell'applicazione.

   b. Accedere a un terminale connesso a ONTAP in cui vengono creati i volumi.

   c. Nascondi la directory snapshot per la SVM:

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

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

   +

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

2. In Astra Trident:

   a. Abilitare la directory snapshot per ogni PV `ontap-nas-economy` basato e associato all'applicazione:

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

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

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

   Risposta:

   ```
   snapshotDirectory: "true"
   ```

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

Risultato

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

Creare un backup immutabile

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

Prima di iniziare

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

- **Amazon Web Services**: "Abilitare il blocco degli oggetti S3 durante la creazione del bucket e impostare una modalità di conservazione predefinita di "governance" con un periodo di conservazione predefinito".
- **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.
2. Selezionare **Data Protection** (protezione dati).

   Le istantanee vengono visualizzate per impostazione predefinita.
3. Selezionare **Backup** per visualizzare l'elenco dei backup.

Eliminare le istantanee

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

Non è possibile eliminare uno snapshot attualmente in fase di replica.

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. Non è possibile eliminare un backup eseguito in un bucket immutabile finché il criterio di conservazione del bucket non lo consente.

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

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.

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.

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. "API di controllo Astra" per ripristinare le applicazioni.

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.
- **(solo cluster Red Hat OpenShift) Aggiungi criteri**: Quando si crea un progetto per ospitare un'app su un cluster OpenShift, al progetto (o spazio dei nomi Kubernetes) viene assegnato un UID SecurityContext. Per consentire ad Astra Control Center di proteggere la tua applicazione e spostarla in un altro cluster o progetto in OpenShift, devi aggiungere policy che consentano all'applicazione di essere eseguita come qualsiasi UID. Ad esempio, i seguenti comandi CLI di OpenShift concedono le policy appropriate a un'applicazione WordPress.

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

- **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.
- **Helm ha implementato le applicazioni**: Le applicazioni implementate con Helm 3 (o aggiornate da Helm 2 a Helm 3) sono completamente supportate. Le app implementate con Helm 2 non sono supportate.

> L'esecuzione di un'operazione di ripristino in-place su un'applicazione che condivida le risorse con un'altra applicazione può avere risultati non intenzionale. Tutte le risorse condivise tra le applicazioni vengono sostituite quando viene eseguito un ripristino in-place su una delle applicazioni. Per ulteriori informazioni, vedere questo esempio.

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.

> Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, è necessario ripristinare l'applicazione utilizzando le classi di storage originali. Non è possibile specificare un'altra classe di storage se si ripristina l'applicazione nello stesso namespace.

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.

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**.

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.

Espandere per ulteriori informazioni 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.

Problemi di ripristino in-place per un'applicazione che condivide le risorse con un'altra applicazione

È possibile eseguire un'operazione di ripristino in-place su un'applicazione che condivide le risorse con un'altra applicazione e produce risultati non desiderati. Tutte le risorse condivise tra le applicazioni vengono sostituite quando viene eseguito un ripristino in-place su una delle applicazioni.

Di seguito viene riportato uno scenario di esempio che crea una situazione indesiderabile quando si utilizza la replica di NetApp SnapMirror per un ripristino:

1. L'applicazione viene definita `app1` utilizzo dello spazio dei nomi `ns1`.
2. Viene configurata una relazione di replica per `app1`.
3. L'applicazione viene definita `app2` (sullo stesso cluster) utilizzando gli spazi dei nomi `ns1` e. `ns2`.
4. Viene configurata una relazione di replica per `app2`.
5. La replica inversa per `app2`. Questo causa il `app1` app sul cluster di origine da disattivare.

Replica delle applicazioni tra back-end di storage utilizzando la tecnologia SnapMirror

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

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

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

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

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

> È possibile replicare contemporaneamente un'altra applicazione nella direzione opposta. Ad esempio, è possibile replicare le applicazioni A, B, C dal Datacenter 1 al Datacenter 2 e le applicazioni X, Y, Z dal Datacenter 2 al Datacenter 1.

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

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

Prerequisiti per la replica

La replica dell'applicazione Astra Control richiede che i seguenti prerequisiti siano soddisfatti prima di iniziare:

Cluster ONTAP

- * Astra Trident*: Astra Trident versione 22.10 o successiva deve esistere sia sui cluster Kubernetes di origine che di destinazione che utilizzano ONTAP come backend. Astra Control supporta la replica con la tecnologia NetApp SnapMirror utilizzando classi di storage supportate dai seguenti driver:
  - `ontap-nas`
  - `ontap-san`
- **Licenze**: Le licenze asincrone di ONTAP SnapMirror che utilizzano il bundle di protezione dati devono essere attivate sia sul cluster ONTAP di origine che su quello di destinazione. Fare riferimento a. "Panoramica sulle licenze SnapMirror in ONTAP" per ulteriori informazioni.

Peering

- **Cluster e SVM**: I backend dello storage ONTAP devono essere peering. Fare riferimento a. "Panoramica del peering di cluster e SVM" per ulteriori informazioni.

  > Assicurati che i nomi delle SVM utilizzati nella relazione di replica tra due cluster ONTAP siano univoci.

- * Astra Trident e SVM*: Le SVM remote con peering devono essere disponibili per Astra Trident sul cluster di destinazione.

Centro di controllo Astra

- **Backend gestiti**: È necessario aggiungere e gestire i backend di storage ONTAP in Astra Control Center per creare una relazione di replica.

  solo per Astra Control Provisioner: L'aggiunta e la gestione di backend di storage ONTAP in Astra Control Center è opzionale se hai abilitato Astra Control Provisioner per Astra Control Center 23,10 o versioni successive.

- **Cluster gestiti**: Aggiungere e gestire i seguenti cluster con Astra Control, idealmente in diversi domini o

siti di errore:

  - Cluster Kubernetes di origine
  - Cluster Kubernetes di destinazione
  - Cluster ONTAP associati

- **Account utente**: Quando si aggiunge un backend di storage ONTAP al centro di controllo Astra, applicare le credenziali utente con il ruolo "admin". Questo ruolo dispone di metodi di accesso `http` e. `ontapi` Abilitato sia sui cluster di origine che di destinazione ONTAP. Fare riferimento a. "Gestire gli account utente nella documentazione di ONTAP" per ulteriori informazioni.

  Astra Control Provisioner only: Se hai abilitato la funzionalità Astra Control Provisioner, non hai più bisogno di definire specificamente un ruolo "admin" per gestire i cluster in Astra Control Center, poiché queste credenziali non sono più necessarie all'interno di Astra Control Center.

"Implementare Astra Control Center" in un terzo dominio di errore o sito secondario per un disaster recovery perfetto.

Astra Control Center non supporta la replica SnapMirror di NetApp per backend di storage che utilizzano il protocollo NVMe over TCP.

Configurazione di Astra Trident/ONTAP

Astra Control Center richiede la configurazione di almeno un backend di storage che supporti la replica per i cluster di origine e di destinazione. Se i cluster di origine e di destinazione sono gli stessi, l'applicazione di destinazione deve utilizzare un backend di storage diverso da quello dell'applicazione di origine per ottenere la migliore resilienza.

La replica di Astra Control supporta le applicazioni che utilizzano una singola classe di storage. Quando Aggiungi un'applicazione a uno spazio dei nomi, assicurati che l'applicazione abbia la stessa classe di storage delle altre applicazioni nello spazio dei nomi. Quando si aggiunge un PVC a un'applicazione replicata, assicurarsi che il nuovo PVC abbia la stessa classe di storage degli altri PVC nello spazio dei nomi.

Impostare una relazione di replica

L'impostazione di una relazione di replica comporta quanto segue:

- Scelta della frequenza con cui Astra Control deve acquisire uno snapshot dell'applicazione (che include le risorse Kubernetes dell'applicazione e le snapshot dei volumi per ciascun volume dell'applicazione)
- Scelta della pianificazione della replica (incluse le risorse Kubernetes e i dati dei volumi persistenti)
- Impostazione dell'ora in cui eseguire l'istantanea

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Selezionare la scheda **Data Protection** > **Replication**.
3. Selezionare **Configura policy di replica**. In alternativa, dalla casella protezione applicazione, selezionare l'opzione azioni e selezionare **Configura policy di replica**.
4. Inserire o selezionare le seguenti informazioni:
   - **Destination cluster** (cluster di destinazione): Inserire un cluster di destinazione (che può essere lo

stesso del cluster di origine).

- **Destination storage class** (Classe di storage di destinazione): Selezionare o immettere la classe di storage che utilizza la SVM in peering sul cluster ONTAP di destinazione. Come Best practice, la classe di storage di destinazione deve puntare a un backend di storage diverso da quello della classe di storage di origine.
- **Tipo di replica**: `Asynchronous` è attualmente l'unico tipo di replica disponibile.
- **Destination namespace** (spazio dei nomi di destinazione): Immettere spazi dei nomi di destinazione nuovi o esistenti per il cluster di destinazione.
- (Facoltativo) aggiungere spazi dei nomi aggiuntivi selezionando **Aggiungi spazio dei nomi** e scegliendo lo spazio dei nomi dall'elenco a discesa.
- **Replication frequency** (frequenza di replica): Consente di impostare la frequenza con cui Astra Control deve acquisire uno snapshot e replicarlo nella destinazione.
- **Offset**: Consente di impostare il numero di minuti dall'inizio dell'ora in cui si desidera che Astra Control prenda un'istantanea. È possibile utilizzare un offset in modo che non coincidano con altre operazioni pianificate.

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.

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

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

Astra Control crea uno snapshot dell'applicazione utilizzato per la replica.

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

Il nome dello snapshot utilizza il formato di `replication-schedule-<string>`. Astra Control conserva l'ultimo snapshot utilizzato per la replica. Eventuali snapshot di replica meno recenti vengono eliminati dopo il completamento della replica.

Risultato

In questo modo si crea la relazione di replica.

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

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

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

Ad esempio:
Normale | stabilito

Scopri di più sugli stati e sullo stato della replica alla fine di questo argomento.

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

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

Fasi

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

Risultato

Le seguenti azioni si verificano in seguito alla procedura di failover:

- L'applicazione di destinazione viene avviata in base all'ultimo snapshot replicato.
- Il cluster e l'applicazione di origine (se operativi) non vengono arrestati e continueranno a funzionare.
- Lo stato di replica cambia in "failover", quindi in "failover" una volta completato.
- La policy di protezione dell'applicazione di origine viene copiata nell'applicazione di destinazione in base alle pianificazioni presenti nell'applicazione di origine al momento del failover.
- Se nell'applicazione di origine sono attivati uno o più hook di esecuzione post-ripristino, tali hook di esecuzione vengono eseguiti per l'applicazione di destinazione.
- Astra Control mostra l'applicazione sia sul cluster di origine che di destinazione, nonché il relativo stato di salute.

Risincronizzare una replica con esito negativo

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

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

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

Fasi

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

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

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

Risultato

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

Replica inversa delle applicazioni

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

In questa situazione, si sta sostituendo l'origine e la destinazione.

Fasi

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

Risultato

Le seguenti azioni si verificano in seguito alla replica inversa:

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

Eseguire il failback delle applicazioni nel cluster di origine originale

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

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

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

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Selezionare la scheda **Data Protection** > **Replication**.
3. Dal menu Actions (azioni), selezionare **Resync**.
4. Per un'operazione di fail back, scegliere l'applicazione failed over come origine dell'operazione di risync (mantenendo i dati scritti dopo il failover).
5. Digitare "resync" per confermare.
6. Selezionare **Sì, risincronizzare** per terminare.
7. Al termine della risincronizzazione, nel menu azioni della scheda protezione dati > Replica, selezionare **Replica inversa**.
8. Nella pagina Replica inversa, esaminare le informazioni e selezionare **Replica inversa**.

Risultato

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

Eliminare una relazione di replica dell'applicazione

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

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.
2. Selezionare la scheda **Data Protection** > **Replication**.
3. Nella casella protezione applicazione o nel diagramma delle relazioni, selezionare **Elimina relazione di replica**.

Risultato

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

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

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

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

Stati di integrità delle relazioni di replica

I seguenti stati indicano lo stato della relazione di replica:

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

stati del ciclo di vita della replica

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

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

Clonare e migrare le applicazioni

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. È possibile utilizzare l'interfaccia utente di Astra Control Center o. "API di controllo Astra" per clonare e migrare le applicazioni.

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 che le istanze cloud che contengono i cluster di origine e di destinazione (se non sono uguali) abbiano un bucket predefinito. Sarà necessario assegnare un bucket predefinito per ogni istanza del cloud.
- 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.

> Durante la clonazione delle applicazioni in ambienti OpenShift, Astra Control Center deve consentire a OpenShift di montare volumi e modificare la proprietà dei file. Per questo motivo, è necessario configurare un criterio di esportazione dei volumi ONTAP per consentire queste operazioni. Puoi farlo con i seguenti comandi:
>
> 1. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -superuser sys`
> 2. `export-policy rule modify -vserver <storage virtual machine name> -policyname <policy name> -ruleindex 1 -anon 65534`

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 ID bucket. Un'operazione di cloni dell'applicazione, tuttavia, utilizza sempre il bucket predefinito definito. Non esiste alcuna opzione per modificare i bucket per un clone. Se si desidera

controllare quale bucket viene utilizzato, è possibile farlo "modificare l'impostazione predefinita del bucket" oppure fare una "backup" seguito da un "ripristinare" separatamente.

- **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.
- **Con i bucket S3**: I bucket S3 in Astra Control Center non riportano la capacità disponibile. Prima di eseguire il backup o la clonazione delle applicazioni gestite da Astra Control Center, controllare le informazioni del bucket nel sistema di gestione ONTAP o StorageGRID.
- **Con una versione specifica di PostgreSQL**: I cloni delle applicazioni all'interno dello stesso cluster si guastano costantemente con il grafico BitNami PostgreSQL 11.5.0. Per clonare correttamente, utilizzare una versione precedente o successiva del grafico.

Considerazioni su OpenShift

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

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

Fasi

1. Selezionare **applicazioni**.
2. Effettuare una delle seguenti operazioni:
   - Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per l'applicazione desiderata.
   - Selezionare il nome dell'applicazione desiderata e l'elenco a discesa Status (Stato) in alto a destra nella pagina.
3. Selezionare **Clone**.
4. 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 allo spazio dei nomi di destinazione definito dall'utente.

     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.

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

Gestire gli hook di esecuzione delle applicazioni

Un gancio di esecuzione è un'azione personalizzata che è possibile configurare per l'esecuzione in combinazione con un'operazione di protezione dei dati di un'applicazione gestita. Ad esempio, se si dispone di un'applicazione di database, è possibile utilizzare 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 Center supporta i seguenti tipi di hook di esecuzione, in base al momento in cui possono essere eseguiti:

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

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).
- Se Astra Control Center esegue il failover di un'applicazione di origine replicata nell'applicazione di destinazione, tutti gli hook di esecuzione post-failover abilitati per l'applicazione di origine vengono eseguiti per l'applicazione di destinazione al termine del failover.

> Se sono stati eseguiti hook dopo il ripristino con Astra Control Center 23,04 e l'Astra Control Center è stato aggiornato alla versione 23,07 o successiva, i hook di esecuzione post-ripristino non verranno più eseguiti dopo una replica di failover. Devi creare nuovi hook di esecuzione post-failover per le tue applicazioni. In alternativa, è possibile modificare il tipo di operazione degli hook post-ripristino esistenti destinati ai failover da "post-ripristino" a "post-failover".

Ordine di esecuzione

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

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

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

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

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

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

Determinare se verrà eseguito un gancio

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

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

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

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

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

Scenario	Operazione	Snapshot esistente	Backup esistente	Namespace	Cluster	Esecuzione di Snapshot Hooks	Esecuzione dei ganci di backup	Esecuzione degli hook di ripristino	Esecuzione degli hook di failover
1	Clonare	N	N	Novità	Stesso	Y	N	Y	N
2	Clonare	N	N	Novità	Diverso	Y	Y	Y	N
3	Clonare o ripristinare	Y	N	Novità	Stesso	N	N	Y	N
4	Clonare o ripristinare	N	Y	Novità	Stesso	N	N	Y	N
5	Clonare o ripristinare	Y	N	Novità	Diverso	N	N	Y	N
6	Clonare o ripristinare	N	Y	Novità	Diverso	N	N	Y	N

Scenario	Operazione	Snapshot esistente	Backup esistente	Namespace	Cluster	Esecuzione di Snapshot Hooks	Esecuzione dei ganci di backup	Esecuzione degli hook di ripristino	Esecuzione degli hook di failover
7	Ripristinare	Y	N	Esistente	Stesso	N	N	Y	N
8	Ripristinare	N	Y	Esistente	Stesso	N	N	Y	N
9	Snapshot	N/A.	N/A.	N/A.	N/A.	Y	N/A.	N/A.	N
10	Backup	N	N/A.	N/A.	N/A.	Y	Y	N/A.	N
11	Backup	Y	N/A.	N/A.	N/A.	N	N	N/A.	N
12	Failover	Y	N/A.	Creato dalla replica	Diverso	N	N	N	Y
13	Failover	Y	N/A.	Creato dalla replica	Stesso	N	N	N	Y

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"

Proteggi Astra Control Center con Astra Control Center

Per garantire una maggiore resilienza contro errori fatali nel cluster Kubernetes in cui è in esecuzione Astra Control Center, proteggere l'applicazione Astra Control Center stessa. Puoi eseguire il backup e il ripristino di Astra Control Center utilizzando un'istanza secondaria di Astra Control Center o utilizzare la replica Astra se lo storage sottostante utilizza ONTAP.

In questi scenari, una seconda istanza di Astra Control Center viene implementata e configurata in un dominio di errore diverso e viene eseguita in un secondo cluster Kubernetes diverso rispetto all'istanza primaria Astra Control Center. La seconda istanza di Astra Control viene utilizzata per eseguire il backup e ripristinare potenzialmente l'istanza primaria di Astra Control Center. Un'istanza di Astra Control Center, ripristinata o replicata, continuerà a fornire la gestione dei dati delle applicazioni per le applicazioni cluster e a ripristinare l'accessibilità ai backup e alle snapshot di tali applicazioni.

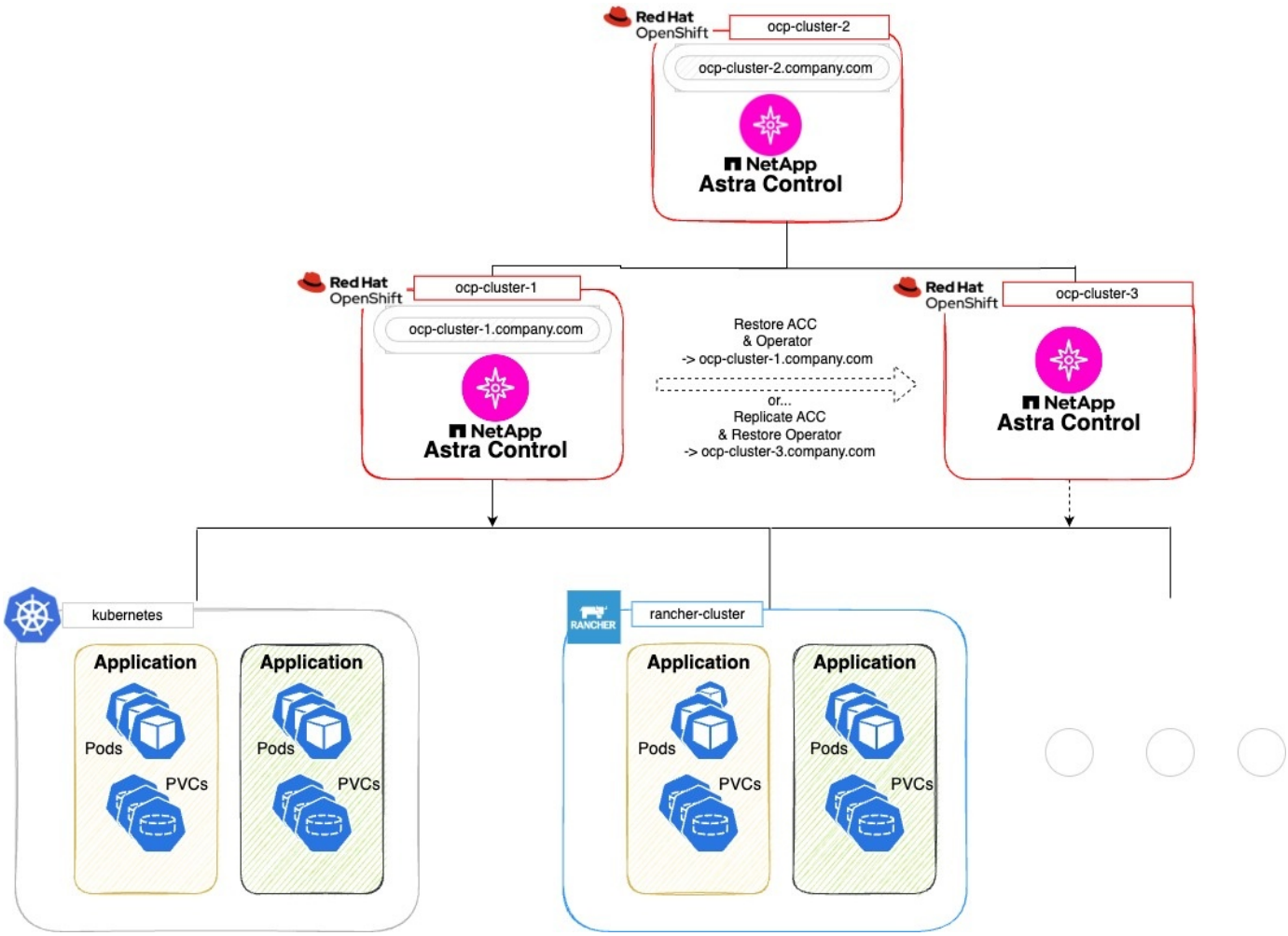
Prima di iniziare

Prima di impostare scenari di protezione per Astra Control Center, assicurarsi di disporre dei seguenti requisiti:

- **Un cluster Kubernetes che esegue l'istanza primaria Astra Control Center**: Questo cluster ospita l'istanza primaria Astra Control Center che gestisce i cluster di applicazioni.
- **Un secondo cluster Kubernetes dello stesso tipo di distribuzione Kubernetes del primario che esegue l'istanza secondaria di Astra Control Center**: Questo cluster ospita l'istanza di Astra Control Center che gestisce l'istanza primaria di Astra Control Center.
- **Un terzo cluster Kubernetes dello stesso tipo di distribuzione Kubernetes del primario**: Questo cluster ospiterà l'istanza ripristinata o replicata di Astra Control Center. Deve avere lo stesso namespace Astra Control Center disponibile che è attualmente distribuito nel primario. Ad esempio, se Astra Control Center viene implementato nello spazio dei nomi `netapp-acc` nel cluster di origine, lo spazio dei nomi `netapp-acc` Deve essere disponibile e non deve essere utilizzato da alcuna applicazione sul cluster Kubernetes di destinazione.
- **Bucket compatibili con S3**: Ogni istanza di Astra Control Center dispone di un bucket di storage a oggetti accessibile compatibile con S3.
- **Un bilanciatore di carico configurato**: Il bilanciatore di carico fornisce un indirizzo IP per Astra e deve avere connettività di rete ai cluster di applicazioni ed entrambi i bucket S3.
- **I cluster soddisfano i requisiti di Astra Control Center**: Ogni cluster utilizzato nella protezione Astra Control Center è conforme "Requisiti generali di Astra Control Center".

A proposito di questa attività

Queste procedure descrivono i passaggi necessari per ripristinare Astra Control Center in un nuovo cluster mediante uno dei due backup e ripristino oppure replica. I passaggi si basano sulla configurazione di esempio qui illustrata:



In questa configurazione di esempio, viene visualizzato quanto segue:

- **Un cluster Kubernetes che esegue l'istanza primaria Astra Control Center**:
  - Cluster OpenShift: `ocp-cluster-1`
  - Istanza primaria Astra Control Center: `ocp-cluster-1.company.com`
  - Questo cluster gestisce i cluster di applicazioni.
- **Il secondo cluster Kubernetes dello stesso tipo di distribuzione Kubernetes del primario che esegue l'istanza secondaria Astra Control Center**:
  - Cluster OpenShift: `ocp-cluster-2`
  - Istanza secondaria Astra Control Center: `ocp-cluster-2.company.com`
  - Questo cluster verrà utilizzato per eseguire il backup dell'istanza primaria di Astra Control Center o per configurare la replica su un cluster diverso (in questo esempio, il `ocp-cluster-3` cluster).
- **Un terzo cluster Kubernetes dello stesso tipo di distribuzione Kubernetes del primario che verrà utilizzato per le operazioni di ripristino**:
  - Cluster OpenShift: `ocp-cluster-3`
  - Terza istanza di Astra Control Center: `ocp-cluster-3.company.com`
  - Questo cluster verrà utilizzato per il ripristino di Astra Control Center o il failover della replica.

Idealmente, il cluster di applicazioni dovrebbe essere situato al di fuori dei tre cluster Astra Control Center, come illustrato dai cluster kuBoost e rancher nell'immagine precedente.

Non raffigurato nello schema:

- Tutti i cluster dispongono di backend ONTAP con Trident installato.
- In questa configurazione, i cluster OpenShift utilizzano MetalLB come bilanciatore del carico.
- Il controller dello snapshot e VolumeSnapshotClass vengono installati anche in tutti i cluster, come descritto nella "prerequisiti".

Opzione passaggio 1: Eseguire il backup e il ripristino di Astra Control Center

Questa procedura descrive i passaggi necessari per ripristinare Astra Control Center in un nuovo cluster utilizzando il backup e il ripristino.

In questo esempio, Astra Control Center è sempre installato in `netapp-acc` spazio dei nomi e l'operatore viene installato sotto `netapp-acc-operator` namespace.

Anche se non descritto, l'operatore di Astra Control Center può essere distribuito nello stesso namespace di Astra CR.

Prima di iniziare

- È stato installato Astra Control Center primario in un cluster.
- È stato installato Astra Control Center secondario su un cluster diverso.

Fasi

1. Gestire le applicazioni Astra Control Center primarie e il cluster di destinazione dall'istanza Astra Control Center secondaria (in esecuzione su `ocp-cluster-2` cluster):
   a. Accedere all'istanza secondaria di Astra Control Center.
   b. "Aggiungere il cluster Astra Control Center primario" (`ocp-cluster-1`).
   c. "Aggiungere il terzo cluster di destinazione" (`ocp-cluster-3`) che verrà utilizzato per il ripristino.
2. Gestire Astra Control Center e l'operatore Astra Control Center sul secondario Astra Control Center:
   a. Dalla pagina applicazioni, selezionare **Definisci**.
   b. Nella finestra **Definisci applicazione**, immettere il nome della nuova applicazione (`netapp-acc`).
   c. Scegli il cluster che esegue l'Astra Control Center primario (`ocp-cluster-1`) Dall'elenco a discesa **Cluster**.
   d. Scegliere `netapp-acc` Spazio dei nomi per Astra Control Center dall'elenco a discesa **namespace**.
   e. Nella pagina risorse cluster, selezionare **Includi risorse aggiuntive con ambito cluster**.
   f. Selezionare **Aggiungi regola di inclusione**.
   g. Selezionare queste voci, quindi selezionare **Aggiungi**:
      - Selettore etichette: <label name>
      - Gruppo: ApiExtensions.k8s.io
      - Versione: V1

- Tipo: CustomResourceDefinition

h. Confermare le informazioni sull'applicazione.

i. Selezionare **Definisci**.

Dopo aver selezionato **define**, ripetere il processo di definizione dell'applicazione per l'operatore `netapp-acc-operator`) e selezionare `netapp-acc-operator` Spazio dei nomi nella procedura guidata Definisci applicazione.

3. Eseguire il backup di Astra Control Center e dell'operatore:

a. Nell'Astra Control Center secondario, accedere alla pagina applicazioni selezionando la scheda applicazioni.

b. "Backup" L'applicazione Astra Control Center (`netapp-acc`).

c. "Backup" l'operatore (`netapp-acc-operator`).

4. Dopo aver eseguito il backup di Astra Control Center e dell'operatore, simulare uno scenario di disaster recovery (DR) di "Disinstallazione di Astra Control Center" dal cluster primario.

> Astra Control Center verrà ripristinato in un nuovo cluster (il terzo cluster Kubernetes descritto in questa procedura) e utilizzerai lo stesso DNS del cluster primario per Astra Control Center appena installato.

5. Utilizzando l'Astra Control Center secondario, "ripristinare" L'istanza principale dell'applicazione Astra Control Center dal proprio backup:

a. Selezionare **applicazioni**, quindi selezionare il nome dell'applicazione Astra Control Center.

b. Dal menu Opzioni nella colonna azioni, selezionare **Ripristina**.

c. Scegliere **Restore to new namespaces** come tipo di ripristino.

d. Immettere il nome del ripristino (`netapp-acc`).

e. Scegliere il terzo cluster di destinazione (`ocp-cluster-3`).

f. Aggiornare lo spazio dei nomi di destinazione in modo che sia lo stesso spazio dei nomi dell'originale.

g. Nella pagina origine ripristino, selezionare il backup dell'applicazione che verrà utilizzato come origine di ripristino.

h. Selezionare **Ripristina utilizzando le classi di archiviazione originali**.

i. Selezionare **Ripristina tutte le risorse**.

j. Esaminare le informazioni di ripristino, quindi selezionare **Restore** (Ripristina) per avviare il processo di ripristino che ripristina Astra Control Center nel cluster di destinazione (`ocp-cluster-3`). Il ripristino è completo all'accesso dell'applicazione `available` stato.

6. Configurare Astra Control Center sul cluster di destinazione:

a. Aprire un terminale e collegarsi utilizzando kubeconfig al cluster di destinazione (`ocp-cluster-3`) Che contiene Astra Control Center ripristinato.

b. Verificare che il `ADDRESS` Nella configurazione Astra Control Center fa riferimento al nome DNS del sistema primario:

```
kubectl get acc -n netapp-acc
```

Risposta:

```
NAME  UUID                                   VERSION    ADDRESS
READY
astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
1.company.com           True
```

a. Se il `ADDRESS` Nel campo della risposta sopra riportata non è presente l'FQDN dell'istanza primaria di Astra Control Center, aggiornare la configurazione per fare riferimento al DNS di Astra Control Center:

```
kubectl edit acc -n netapp-acc
```

i. Modificare il `astraAddress` sotto `spec:` All'FQDN (`ocp-cluster-1.company.com` In questo esempio) dell'istanza primaria Astra Control Center.

ii. Salvare la configurazione.

iii. Verificare che l'indirizzo sia stato aggiornato:

```
kubectl get acc -n netapp-acc
```

b. Accedere alla Ripristinare l'operatore Astra Control Center di questo documento per completare il processo di ripristino.

Opzione fase 1: Protezione di Astra Control Center con la replica

Questa procedura descrive i passaggi necessari per la configurazione "Replica di Astra Control Center" Per proteggere l'istanza primaria Astra Control Center.

In questo esempio, Astra Control Center è sempre installato in `netapp-acc` spazio dei nomi e l'operatore viene installato sotto `netapp-acc-operator` namespace.

Prima di iniziare

- È stato installato Astra Control Center primario in un cluster.
- È stato installato Astra Control Center secondario su un cluster diverso.

Fasi

1. Gestire l'applicazione Astra Control Center primaria e il cluster di destinazione dall'istanza Astra Control Center secondaria:
   a. Accedere all'istanza secondaria di Astra Control Center.
   b. "Aggiungere il cluster Astra Control Center primario" (`ocp-cluster-1`).
   c. "Aggiungere il terzo cluster di destinazione" (`ocp-cluster-3`) che verrà utilizzato per la replica.
2. Gestire Astra Control Center e l'operatore Astra Control Center sul secondario Astra Control Center:
   a. Selezionare **Cluster** e selezionare il cluster che contiene Astra Control Center primario (`ocp-cluster-1`).

b. Selezionare la scheda **spazi dei nomi**.

c. Selezionare `netapp-acc` e. `netapp-acc-operator` namespace.

d. Selezionare il menu azioni e selezionare **Definisci come applicazioni**.

e. Selezionare **Visualizza in applicazioni** per visualizzare le applicazioni definite.

3. Configurare i backend per la replica:

> La replica richiede che il cluster Astra Control Center primario e il cluster di destinazione (`ocp-cluster-3`) Utilizzare differenti backend di archiviazione ONTAP con peered. Dopo che ogni backend è stato sottoposto a peering e aggiunto ad Astra Control, il backend viene visualizzato nella scheda **scoperto** della pagina Backend.

a. "Aggiungere un backend con peered" Ad Astra Control Center sul cluster primario.

b. "Aggiungere un backend con peered" Ad Astra Control Center nel cluster di destinazione.

4. Configurare la replica:

a. Nella schermata applicazioni, selezionare `netapp-acc` applicazione.

b. Selezionare **Configura policy di replica**.

c. Selezionare `ocp-cluster-3` come cluster di destinazione.

d. Selezionare la classe di archiviazione.

e. Invio `netapp-acc` come namespace di destinazione.

f. Se necessario, modificare la frequenza di replica.

g. Selezionare **Avanti**.

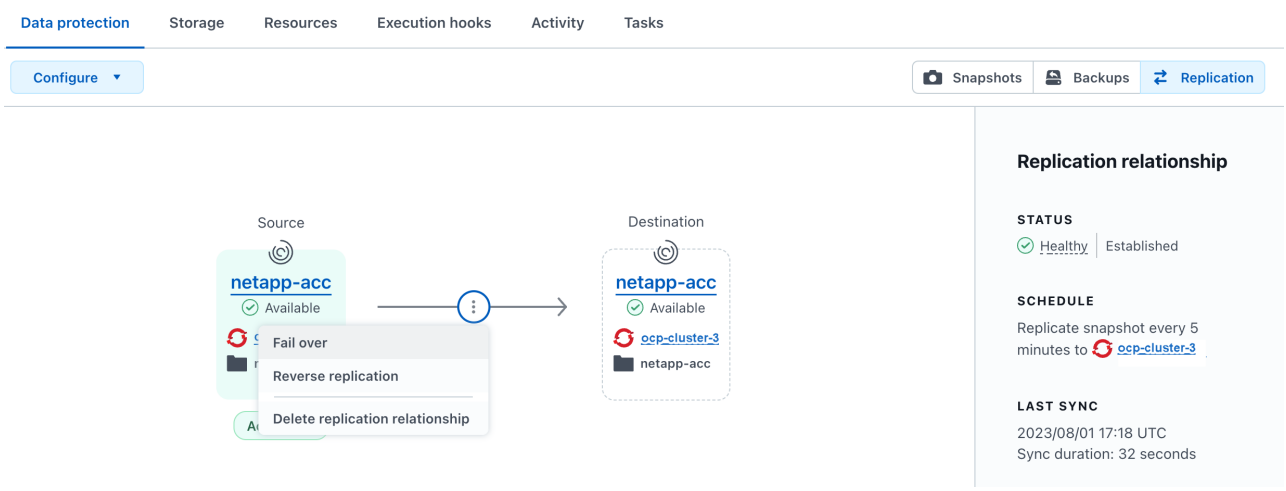
h. Verificare che la configurazione sia corretta e selezionare **Salva**.

Il rapporto di replica passa da `Establishing` a. `Established`. Quando è attiva, la replica viene eseguita ogni cinque minuti fino all'eliminazione della configurazione della replica.

5. Esegui il failover della replica nell'altro cluster se il sistema primario è danneggiato o non più accessibile:

> Assicurarsi che nel cluster di destinazione non sia installato Astra Control Center per garantire un failover corretto.

a. Selezionare l'icona ellissi verticali e selezionare **failover**.



b. Confermare i dettagli e selezionare **failover** per avviare il processo di failover.

   Lo stato della relazione di replica cambia in `Failing over` e poi `Failed over` al termine dell'operazione.

6. Completare la configurazione di failover:

   a. Aprire un terminale e connettersi utilizzando il kubeconfig del terzo quadro strumenti (`ocp-cluster-3`). In questo cluster è ora installato Astra Control Center.

   b. Determinare l'FQDN Astra Control Center sul terzo cluster (`ocp-cluster-3`).

   c. Aggiornare la configurazione per fare riferimento al DNS di Astra Control Center:

```
kubectl edit acc -n netapp-acc
```

      i. Modificare il `astraAddress` sotto `spec:` Con l'FQDN (`ocp-cluster-3.company.com`) del terzo cluster di destinazione.

      ii. Salvare la configurazione.

      iii. Verificare che l'indirizzo sia stato aggiornato:

```
kubectl get acc -n netapp-acc
```

   d. confermare la presenza di tutti i CRD traefik richiesti:

```
kubectl get crds | grep traefik
```

   CRDS traefik richiesti:

```
ingressroutes.traefik.containo.us
ingressroutes.traefik.io
ingressroutetcps.traefik.containo.us
ingressroutetcps.traefik.io
ingressrouteudps.traefik.containo.us
ingressrouteudps.traefik.io
middlewares.traefik.containo.us
middlewares.traefik.io
middlewaretcps.traefik.containo.us
middlewaretcps.traefik.io
serverstransports.traefik.containo.us
serverstransports.traefik.io
tlsoptions.traefik.containo.us
tlsoptions.traefik.io
tIsstores.traefik.containo.us
tIsstores.traefik.io
traefikservices.traefik.containo.us
traefikservices.traefik.io
```

a. Se alcuni dei CRD sopra elencati non sono presenti:
   i. Passare a. "documentazione di traefik".
   ii. Copiare l'area "Definitions" (definizioni) in un file.
   iii. Applica modifiche:

```
kubectl apply -f <file name>
```

   iv. Riavvia traefik:

```
kubectl get pods -n netapp-acc | grep -e "traefik" | awk '{print
$1}' | xargs kubectl delete pod -n netapp-acc
```

b. Accedere alla Ripristinare l'operatore Astra Control Center di questo documento per completare il processo di ripristino.

Fase 2: Ripristinare l'operatore Astra Control Center

Utilizzando Astra Control Center secondario, ripristinare l'operatore Astra Control Center primario dal backup. Lo spazio dei nomi di destinazione deve essere lo stesso dello spazio dei nomi di origine. Nel caso in cui Astra Control Center sia stato eliminato dal cluster di origine primario, i backup esisteranno ancora per eseguire la stessa procedura di ripristino.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome dell'applicazione operatore (`netapp-acc-operator`).

2. Dal menu Opzioni nella colonna azioni, selezionare **Ripristina**
3. Scegliere **Restore to new namespaces** come tipo di ripristino.
4. Scegliere il terzo cluster di destinazione (`ocp-cluster-3`).
5. Modificare lo spazio dei nomi in modo che sia lo stesso dello spazio dei nomi associato al cluster di origine primario (`netapp-acc-operator`).
6. Selezionare il backup eseguito in precedenza come origine di ripristino.
7. Selezionare **Ripristina utilizzando le classi di archiviazione originali**.
8. Selezionare **Ripristina tutte le risorse**.
9. Esaminare i dettagli, quindi fare clic su **Ripristina** per avviare il processo di ripristino.

   La pagina Applications (applicazioni) mostra l'operatore Astra Control Center ripristinato nel terzo cluster di destinazione (`ocp-cluster-3`). Al termine del processo, lo stato indica come `Available`. Entro dieci minuti, l'indirizzo DNS dovrebbe risolversi nella pagina.

Risultato

Astra Control Center, i suoi cluster registrati e le applicazioni gestite con snapshot e backup sono ora disponibili nel terzo cluster di destinazione (`ocp-cluster-3`). Tutti i criteri di protezione dell'originale sono presenti anche nella nuova istanza. Puoi continuare a eseguire backup e snapshot pianificati o on-demand.

Risoluzione dei problemi

Determinare lo stato del sistema e se i processi di protezione hanno avuto esito positivo.

- **I pod non sono in esecuzione**: Verificare che tutti i pod siano attivi e in esecuzione:

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

  Se alcuni pod sono in `CrashLookBackOff` specificare, riavviarli e dovrebbero passare a. `Running` stato.

- **Confermare lo stato del sistema**: Verificare che il sistema Astra Control Center sia attivo `ready` stato:

  ```
  kubectl get acc -n netapp-acc
  ```

  Risposta:

  ```
  NAME  UUID                                   VERSION    ADDRESS
  READY
  astra 89f4fd47-0cf0-4c7a-a44e-43353dc96ba8 23.10.0-68 ocp-cluster-
  1.company.com           True
  ```

- **Conferma lo stato di distribuzione**: Mostra le informazioni di distribuzione di Astra Control Center per confermare `Deployment State` è `Deployed`.

```
kubectl describe acc astra -n netapp-acc
```

- **L'interfaccia utente di Astra Control Center ripristinata restituisce un errore 404**: Se questo accade quando si seleziona `AccTraefik` come opzione di ingresso, controllare CRD traefik per assicurarsi che siano tutti installati.

Monitorare lo stato delle applicazioni e del cluster

Visualizza un riepilogo dello stato delle applicazioni e dei cluster

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

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

Sezione applicazioni

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

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

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

Riquadro dei cluster

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

Riquadro backend storage

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

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

Visualizzare lo stato dei cluster e gestire le classi di storage

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

Visualizzare lo stato e i dettagli del cluster

È possibile visualizzare i dettagli del cluster, ad esempio la posizione, i nodi di lavoro, i volumi persistenti e le classi di storage.

Fasi

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

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

3. Visualizzare le informazioni nelle schede **Overview**, **Storage** e **Activity** per trovare le informazioni desiderate.
   - **Panoramica**: Dettagli sui nodi di lavoro, incluso il loro stato.
   - **Storage**: I volumi persistenti associati al calcolo, inclusi la classe e lo stato dello storage.
   - **Attività**: Mostra le attività correlate al cluster.

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

Modificare la classe di storage predefinita

È possibile modificare la classe di storage predefinita per un cluster. Quando Astra Control gestisce un cluster, tiene traccia della classe di storage predefinita del cluster.

> Non modificare la classe di storage utilizzando i comandi kubectl. Utilizzare questa procedura. Astra Control ripristinerà le modifiche se effettuate utilizzando kubectl.

Fasi

1. Nell'interfaccia utente Web di Astra Control Center, selezionare **Clusters**.
2. Nella pagina **Clusters**, selezionare il cluster che si desidera modificare.
3. Selezionare la scheda **Storage**.
4. Selezionare la categoria **classi di storage**.

5. Selezionare il menu **azioni** per la classe di storage che si desidera impostare come predefinita.
6. Selezionare **Imposta come predefinito**.

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. Nell'interfaccia utente di Astra Control Center, selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Esaminare le informazioni.

   Stato dell'app

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

   - **App Protection Status**: 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.
   - **Data Protection**: Consente di configurare una policy di protezione dei dati e di visualizzare le snapshot e i backup esistenti.
   - **Storage**: Mostra i volumi persistenti a livello di applicazione. Lo stato di un volume persistente è dal punto di vista del cluster Kubernetes.
   - **Risorse**: Consente di verificare quali risorse vengono sottoposte a backup e gestite.
   - **Attività**: Mostra le attività correlate all'applicazione.

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

Gestisci il tuo account

Gestire utenti e ruoli locali

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

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

Utilizzare LDAP

LDAP è un protocollo standard di settore per l'accesso alle informazioni di directory distribuite e una scelta popolare per l'autenticazione aziendale. È possibile collegare Astra Control Center a un server LDAP per eseguire l'autenticazione per gli utenti Astra Control selezionati. Ad alto livello, la configurazione prevede l'integrazione di Astra con LDAP e la definizione degli utenti e dei gruppi Astra Control corrispondenti alle definizioni LDAP. È possibile utilizzare l'API Astra Control o l'interfaccia utente Web per configurare l'autenticazione LDAP e gli utenti e i gruppi LDAP. Per ulteriori informazioni, consultare la seguente documentazione:

- "Utilizzare l'API Astra Control per gestire l'autenticazione remota e gli utenti"
- "Utilizzare l'interfaccia utente di Astra Control per gestire utenti e gruppi remoti"
- "Utilizzare l'interfaccia utente di Astra Control per gestire l'autenticazione remota"

Aggiungere utenti

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

Fasi

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

   L'utente dovrà modificare la password al primo accesso.

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

   Ciascun ruolo fornisce le seguenti autorizzazioni:

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

6. Per aggiungere vincoli a un utente con ruolo membro o visualizzatore, attivare la casella di controllo **limita ruolo ai vincoli**.

Per ulteriori informazioni sull'aggiunta di vincoli, fare riferimento a. "Gestire utenti e ruoli locali".

7. Selezionare **Aggiungi**.

Gestire le password

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

Modificare la password

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

Fasi

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

Reimpostare la password di un altro utente

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

Fasi

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

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

6. Selezionare **Ripristina password**.

Rimuovere gli utenti

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

Fasi

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

User (Sì, Rimuovi utente).

Risultato

Astra Control Center rimuove l'utente dall'account.

Gestire i ruoli

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

Aggiungere un vincolo dello spazio dei nomi a un ruolo

Un utente Admin o Owner può aggiungere vincoli di spazio dei nomi ai ruoli Member o Viewer.

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"

Gestire l'autenticazione remota

LDAP è un protocollo standard di settore per l'accesso alle informazioni di directory distribuite e una scelta popolare per l'autenticazione aziendale. È possibile collegare Astra Control Center a un server LDAP per eseguire l'autenticazione per gli utenti Astra Control selezionati.

Ad alto livello, la configurazione prevede l'integrazione di Astra con LDAP e la definizione degli utenti e dei gruppi Astra Control corrispondenti alle definizioni LDAP. È possibile utilizzare l'API Astra Control o l'interfaccia utente Web per configurare l'autenticazione LDAP e gli utenti e i gruppi LDAP.

> Astra Control Center utilizza l'attributo user login, configurato quando l'autenticazione remota è abilitata, per cercare e tenere traccia degli utenti remoti. In questo campo deve esistere un attributo di un indirizzo e-mail ("mail") o di un nome principale utente ("userPrincipalName") per qualsiasi utente remoto che si desidera visualizzare in Astra Control Center. Questo attributo viene utilizzato come nome utente in Astra Control Center per l'autenticazione e la ricerca di utenti remoti.

Aggiungere un certificato per l'autenticazione LDAPS

Aggiungere il certificato TLS privato per il server LDAP in modo che Astra Control Center possa autenticarsi con il server LDAP quando si utilizza una connessione LDAPS. Questa operazione deve essere eseguita una sola volta o alla scadenza del certificato installato.

Fasi

1. Vai a **account**.
2. Selezionare la scheda **certificati**.
3. Selezionare **Aggiungi**.
4. Caricare il `.pem` archiviare o incollare il contenuto del file dagli appunti.
5. Selezionare la casella di controllo **attendibile**.
6. Selezionare **Aggiungi certificato**.

Abilitare l'autenticazione remota

È possibile attivare l'autenticazione LDAP e configurare la connessione tra Astra Control e il server LDAP remoto.

Prima di iniziare

Se si intende utilizzare LDAPS, assicurarsi che il certificato TLS privato per il server LDAP sia installato in Astra Control Center in modo che Astra Control Center possa autenticarsi con il server LDAP. Vedere Aggiungere un certificato per l'autenticazione LDAPS per istruzioni.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Connect**.
4. Inserire l'indirizzo IP del server, la porta e il protocollo di connessione preferito (LDAP o LDAPS).

> Come Best practice, utilizzare LDAPS per la connessione con il server LDAP. È necessario installare il certificato TLS privato del server LDAP in Astra Control Center prima di connettersi a LDAPS.

5. Inserire le credenziali dell'account di servizio nel formato e-mail (administrator@example.com). Astra Control utilizza queste credenziali per la connessione con il server LDAP.
6. Nella sezione **corrispondenza utente**, procedere come segue:
   a. Inserire il DN di base e un filtro di ricerca utente appropriato da utilizzare per recuperare le informazioni utente dal server LDAP.
   b. (Facoltativo) se la directory utilizza l'attributo di accesso utente `userPrincipalName` invece di `mail`, invio `userPrincipalName` Nell'attributo corretto nel campo **attributo di accesso utente**.
7. Nella sezione **corrispondenza gruppo**, immettere il DN della base di ricerca gruppo e un filtro di ricerca gruppo personalizzato appropriato.

> Assicurarsi di utilizzare il nome distinto (DN) di base corretto e un filtro di ricerca appropriato per **corrispondenza utente** e **corrispondenza gruppo**. Il DN di base indica ad Astra Control a quale livello della struttura di directory avviare la ricerca e il filtro di ricerca limita le parti della struttura di directory da cui Astra Control esegue la ricerca.

8. Selezionare **Invia**.

Risultato

Lo stato del riquadro **Remote Authentication** (autenticazione remota) passa a **Pending** (in sospeso), quindi a **Connected** (connesso) quando viene stabilita la connessione al server LDAP.

Disattiva autenticazione remota

È possibile disattivare temporaneamente una connessione attiva al server LDAP.

> Quando si disattiva una connessione a un server LDAP, vengono salvate tutte le impostazioni e vengono conservati tutti gli utenti e i gruppi remoti aggiunti ad Astra Control da tale server LDAP. È possibile riconnettersi a questo server LDAP in qualsiasi momento.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Disable** (Disattiva).

Risultato

Lo stato del riquadro **Remote Authentication** passa a **Disabled**. Tutte le impostazioni di autenticazione remota, gli utenti remoti e i gruppi remoti vengono preservati e la connessione può essere riattivata in qualsiasi momento.

Modificare le impostazioni di autenticazione remota

Se la connessione al server LDAP è stata disattivata o il pannello **Remote Authentication** è in stato "Connection error" (errore di connessione), è possibile modificare le impostazioni di configurazione.

> Non è possibile modificare l'URL o l'indirizzo IP del server LDAP quando il pannello **Remote Authentication** (autenticazione remota) è in stato "Disabled" (Disattivato). È necessario Disconnettere l'autenticazione remota prima di tutto.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Modifica**.
4. Apportare le modifiche necessarie e selezionare **Modifica**.

Disconnettere l'autenticazione remota

È possibile disconnettersi da un server LDAP e rimuovere le impostazioni di configurazione da Astra Control.

> Se si è un utente LDAP e si disconnette, la sessione si concluderà immediatamente Quando ci si disconnette dal server LDAP, tutte le impostazioni di configurazione per quel server LDAP vengono rimosse da Astra Control, così come tutti gli utenti e i gruppi remoti che sono stati aggiunti da quel server LDAP.

Fasi

1. Accedere a **account > connessioni**.
2. Nel riquadro **Remote Authentication**, selezionare il menu di configurazione.
3. Selezionare **Disconnect**.

Risultato

Lo stato del riquadro **Remote Authentication** (autenticazione remota) passa a **Disconnected** (disconnesso). Le impostazioni di autenticazione remota, gli utenti remoti e i gruppi remoti vengono rimossi da Astra Control.

Gestire utenti e gruppi remoti

Se è stata attivata l'autenticazione LDAP sul sistema Astra Control, è possibile cercare utenti e gruppi LDAP e includerli negli utenti approvati del sistema.

Aggiungere un utente remoto

Gli account Owner e gli amministratori possono aggiungere utenti remoti ad Astra Control. Astra Control Center supporta fino a 10,000 utenti remoti LDAP.

> Astra Control Center utilizza l'attributo user login, configurato quando l'autenticazione remota è abilitata, per cercare e tenere traccia degli utenti remoti. In questo campo deve esistere un attributo di un indirizzo e-mail ("mail") o di un nome principale utente ("userPrincipalName") per qualsiasi utente remoto che si desidera visualizzare in Astra Control Center. Questo attributo viene utilizzato come nome utente in Astra Control Center per l'autenticazione e la ricerca di utenti remoti.

> Non è possibile aggiungere un utente remoto se nel sistema esiste già un utente locale con lo stesso indirizzo e-mail (basato sull'attributo "mail" o "nome principale utente"). Per aggiungere l'utente come utente remoto, eliminare prima l'utente locale dal sistema.

Fasi

1. Accedere all'area **account**.
2. Selezionare la scheda **utenti e gruppi**.
3. All'estrema destra della pagina, selezionare **utenti remoti**.
4. Selezionare **Aggiungi**.
5. In alternativa, cercare un utente LDAP inserendo l'indirizzo e-mail dell'utente nel campo **Filtra per email**.
6. Selezionare uno o più utenti dall'elenco.
7. Assegnare un ruolo all'utente.

> Se si assegnano ruoli diversi a un utente e al gruppo dell'utente, il ruolo più permissivo ha la precedenza.

8. Facoltativamente, assegnare uno o più vincoli dello spazio dei nomi a questo utente e selezionare **limita ruolo ai vincoli** per applicarli. È possibile aggiungere un nuovo vincolo dello spazio dei nomi selezionando **Aggiungi vincolo**.

> Quando a un utente vengono assegnati ruoli multipli tramite l'appartenenza al gruppo LDAP, i limiti nel ruolo più permissivo sono gli unici che hanno effetto. Ad esempio, se un utente con un ruolo Viewer locale unisce tre gruppi associati al ruolo Member, la somma dei vincoli dei ruoli Member ha effetto e tutti i vincoli del ruolo Viewer vengono ignorati.

9. Selezionare **Aggiungi**.

Risultato

Il nuovo utente viene visualizzato nell'elenco degli utenti remoti. In questo elenco, è possibile visualizzare i vincoli attivi sull'utente e gestire l'utente dal menu **azioni**.

Aggiungere un gruppo remoto

Per aggiungere più utenti remoti contemporaneamente, gli account Owners e gli amministratori possono aggiungere gruppi remoti ad Astra Control. Quando si aggiunge un gruppo remoto, tutti gli utenti remoti di tale gruppo sono disponibili per accedere ad Astra Control e ereditano lo stesso ruolo del gruppo.

Astra Control Center supporta fino a 5,000 gruppi remoti LDAP.

Fasi

1. Accedere all'area **account**.
2. Selezionare la scheda **utenti e gruppi**.
3. All'estrema destra della pagina, selezionare **gruppi remoti**.
4. Selezionare **Aggiungi**.

   In questa finestra, è possibile visualizzare un elenco dei nomi comuni e dei nomi distinti dei gruppi LDAP recuperati da Astra Control.

5. In alternativa, cercare un gruppo LDAP inserendo il nome comune del gruppo nel campo **Filtra per nome comune**.
6. Selezionare uno o più gruppi dall'elenco.
7. Assegnare un ruolo ai gruppi.

   Il ruolo selezionato viene assegnato a tutti gli utenti di questo gruppo. Se si assegnano ruoli diversi a un utente e al gruppo dell'utente, il ruolo più permissivo ha la precedenza.

8. Facoltativamente, assegnare uno o più vincoli dello spazio dei nomi a questo gruppo e selezionare **limita ruolo ai vincoli** per applicarli. È possibile aggiungere un nuovo vincolo dello spazio dei nomi selezionando **Aggiungi vincolo**.

   Quando a un utente vengono assegnati ruoli multipli tramite l'appartenenza al gruppo LDAP, i limiti nel ruolo più permissivo sono gli unici che hanno effetto. Ad esempio, se un utente con un ruolo Viewer locale unisce tre gruppi associati al ruolo Member, la somma dei vincoli dei ruoli Member ha effetto e tutti i vincoli del ruolo Viewer vengono ignorati.

9. Selezionare **Aggiungi**.

Risultato

Il nuovo gruppo viene visualizzato nell'elenco dei gruppi remoti. Gli utenti remoti di questo gruppo non vengono visualizzati nell'elenco degli utenti remoti fino a quando ciascun utente remoto non effettua l'accesso. In questo elenco, è possibile visualizzare i dettagli sul gruppo e gestire il gruppo dal menu **azioni**.

Visualizzare e gestire le notifiche

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

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

Fasi

1. Selezionare il numero di notifiche non lette in alto a destra.

2. Esaminare le notifiche, quindi selezionare **Contrassegna come letto** o **Mostra tutte le notifiche**.

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

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

Aggiungere e rimuovere le credenziali

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

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

Aggiungere credenziali

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

> Se si crea il proprio file kubeconfig, si dovrebbe definire solo **un** elemento di contesto al suo interno. Fare riferimento a. "Documentazione Kubernetes" per informazioni sulla creazione di file kubeconfig.

Rimuovere le credenziali

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

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

Fasi

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

Risultato

Astra Control Center rimuove le credenziali dall'account.

Monitorare l'attività dell'account

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

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

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

Visualizza tutte le attività dell'account in Astra Control

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

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

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

Visualizzare l'attività dell'account per i cluster

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

Intraprendere azioni per risolvere gli eventi che richiedono attenzione

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

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

Aggiornare una licenza esistente

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

Fasi

1. Accedere a. "Sito di supporto NetApp".
2. Accedere alla pagina di download di Astra Control Center, inserire il numero di serie e scaricare il file di licenza NetApp completo (NLF).
3. Accedere all'interfaccia utente di Astra Control Center.
4. Dalla barra di navigazione a sinistra, selezionare **account** > **licenza**.

5. Nella pagina **account** > **licenza**, selezionare il menu a discesa dello stato della licenza esistente e selezionare **Sostituisci**.
6. Individuare il file di licenza scaricato.
7. Selezionare **Aggiungi**.

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

Per ulteriori informazioni

- "Licenza Astra Control Center"

Gestire i bucket

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

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

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

- NetApp ONTAP S3
- NetApp StorageGRID S3
- Microsoft Azure
- Generico S3

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

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

Un bucket può trovarsi in uno dei seguenti stati:

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

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

È possibile eseguire queste attività relative alla gestione dei bucket:

- "Aggiungi un bucket"

- Modificare un bucket
- Impostare il bucket predefinito
- Ruotare o rimuovere le credenziali bucket
- Rimuovere una benna

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

Modificare un bucket

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

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

Fasi

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

   Impossibile modificare il tipo di bucket.

4. Selezionare **Aggiorna**.

Impostare il bucket predefinito

Quando si esegue un clone tra i cluster, Astra Control richiede un bucket predefinito. Seguire questi passaggi per impostare un bucket predefinito per tutti i cluster.

Fasi

1. Accedere a **istanze cloud**.
2. Selezionare il menu nella colonna **azioni** per l'istanza di cloud nell'elenco.
3. Selezionare **Modifica**.
4. Nell'elenco **bucket**, selezionare il bucket che si desidera impostare come predefinito.
5. Selezionare **Salva**.

Ruotare o rimuovere le credenziali bucket

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

Ruotare le credenziali del bucket

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

Procedura per modificare e ruotare le credenziali

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

Rimuovere le credenziali bucket

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

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

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

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

Rimuovere una benna

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

- Non è possibile rimuovere un bucket predefinito. Se si desidera rimuovere tale bucket, selezionare prima un altro bucket come predefinito.
- 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.

- Non è possibile rimuovere un bucket predefinito. Se si desidera rimuovere tale bucket, selezionare prima un altro bucket come predefinito.

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 in alcuna policy di protezione attiva.

In tal caso, non sarà possibile continuare.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Bucket**.
2. Dal menu **azioni**, selezionare **Rimuovi**.

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

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

Trova ulteriori informazioni

- "Utilizzare l'API di controllo Astra"

Gestire il back-end dello storage

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

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

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

- "Aggiungere un backend di storage"
- Visualizza i dettagli del back-end dello storage
- Modificare i dettagli dell'autenticazione back-end dello storage
- Gestire un backend di storage rilevato
- Annullare la gestione di un backend di storage
- Rimuovere un backend di storage

Visualizza i dettagli del back-end dello storage

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

Visualizza i dettagli del back-end dello storage dalla dashboard

Fasi

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

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

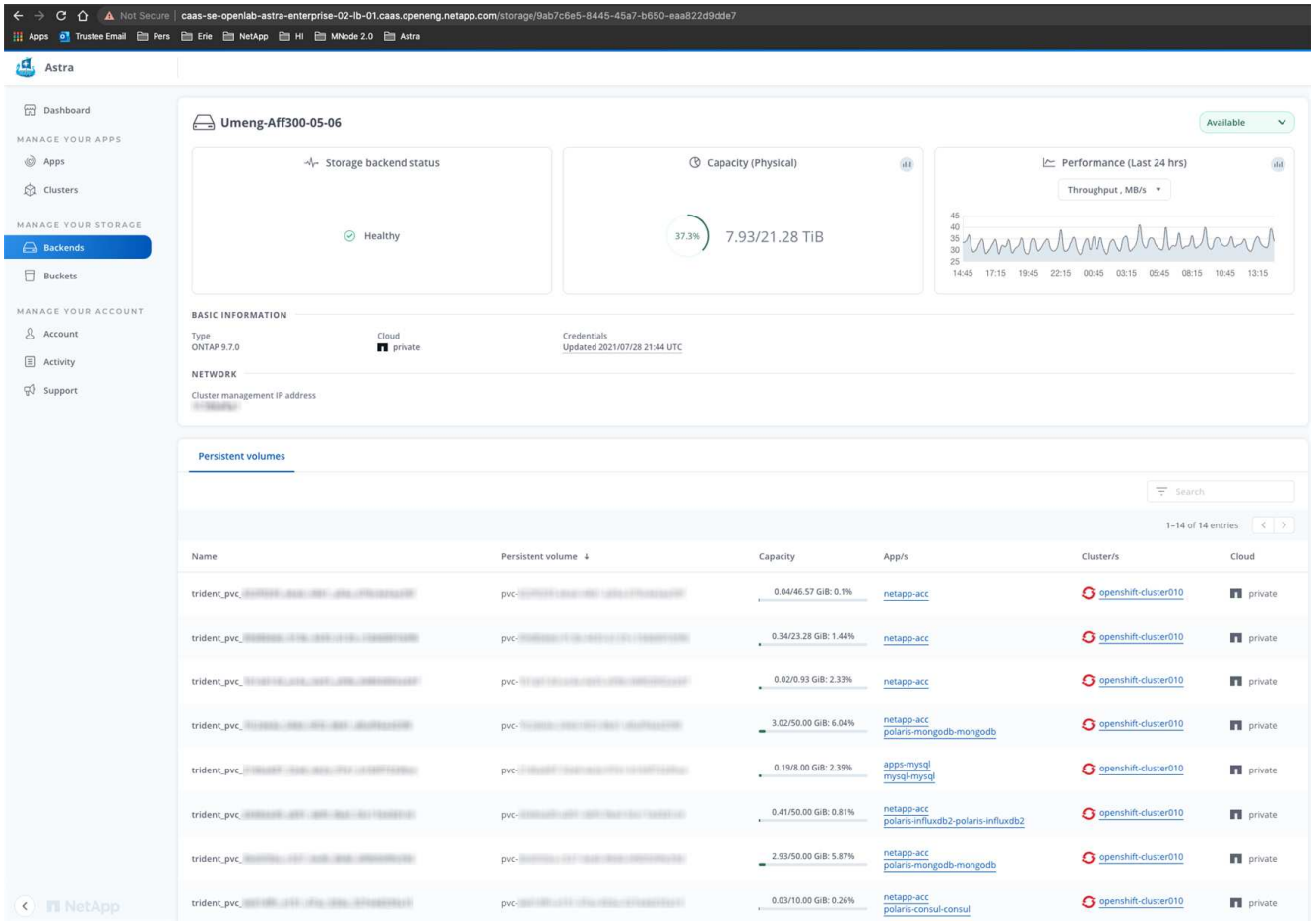
Visualizza informazioni sullo stato, la capacità e le performance del back-end (throughput IOPS e/o latenza).

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

Fasi

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

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



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

Modificare i dettagli dell'autenticazione back-end dello storage

Centro di controllo Astra offre due modalità di autenticazione di un backend ONTAP.

- **Autenticazione basata su credenziali**: Nome utente e password di un utente ONTAP con le autorizzazioni richieste. È necessario utilizzare un ruolo di accesso di sicurezza predefinito, ad esempio admin, per garantire la massima compatibilità con le versioni di ONTAP.

- **Autenticazione basata su certificato**: Il centro di controllo Astra può anche comunicare con un cluster ONTAP utilizzando un certificato installato sul back-end. Utilizzare il certificato client, la chiave e il certificato CA attendibile, se utilizzato (consigliato).

È possibile aggiornare i backend esistenti per passare da un tipo di autenticazione a un altro metodo. È supportato un solo metodo di autenticazione alla volta.

Per ulteriori informazioni sull'attivazione dell'autenticazione basata su certificati, fare riferimento a. "Abilitare l'autenticazione sul backend dello storage ONTAP".

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare il backend dello storage.
3. Nel campo credenziali, selezionare l'icona **Modifica**.
4. Nella pagina Edit (Modifica), selezionare una delle seguenti opzioni.
   - **Usa credenziali amministratore**: Inserire l'indirizzo IP di gestione del cluster ONTAP e le credenziali di amministratore. Le credenziali devono essere credenziali a livello di cluster.

     L'utente di cui si inseriscono le credenziali deve disporre di `ontapi` Metodo di accesso all'accesso dell'utente abilitato in Gestione di sistema di ONTAP sul cluster ONTAP. Se si intende utilizzare la replica SnapMirror, applicare le credenziali utente con il ruolo "admin", che dispone dei metodi di accesso `ontapi` e. `http`, Sui cluster ONTAP di origine e di destinazione. Fare riferimento a. "Gestire gli account utente nella documentazione di ONTAP" per ulteriori informazioni.

   - **Usa un certificato**: Carica il certificato `.pem` file, la chiave del certificato `.key` e, facoltativamente, il file dell'autorità di certificazione.
5. Selezionare **Salva**.

Gestire un backend di storage rilevato

È possibile scegliere di gestire un backend di storage non gestito ma rilevato. Quando si gestisce un backend di storage, Astra Control indica se un certificato per l'autenticazione è scaduto.

Fasi

1. Dalla barra di navigazione a sinistra, selezionare **Backend**.
2. Selezionare l'opzione **rilevato**.
3. Selezionare il backend dello storage.
4. Dal menu Opzioni nella colonna **azioni**, selezionare **Gestisci**.
5. Apportare le modifiche.
6. Selezionare **Salva**.

Annullare la gestione di un backend di storage

È possibile annullare la gestione del backend.

Fasi

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

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

Rimuovere un backend di storage

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

Prima di iniziare

- Assicurarsi che il backend dello storage non sia gestito.
- Assicurarsi che il backend dello storage non abbia volumi associati al cluster.

Fasi

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

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".

Monitorare l'infrastruttura con connessioni Cloud Insights, Prometheus o Fluentd

È possibile configurare diverse impostazioni opzionali per migliorare l'esperienza di Astra Control Center. Per monitorare e ottenere informazioni sulla tua infrastruttura completa, crea una connessione a NetApp Cloud Insights, configura Prometheus o Aggiungi una connessione Fluentd.

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

- Connettersi a Cloud Insights
- Connettiti a Prometheus
- Connettersi a Fluentd

Aggiungere un server proxy per le connessioni a Cloud Insights o al sito di supporto NetApp

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

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

Fasi

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

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

Risultato

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

Modificare le impostazioni del server proxy

È possibile modificare le impostazioni del server proxy.

Fasi

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

Disattiva la connessione al server proxy

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

Fasi

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

Connettersi a Cloud Insights

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

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

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

Quando Astra Control Center è associato a Cloud Insights, non utilizzare l'opzione **Modifica distribuzione** in Cloud Insights.

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

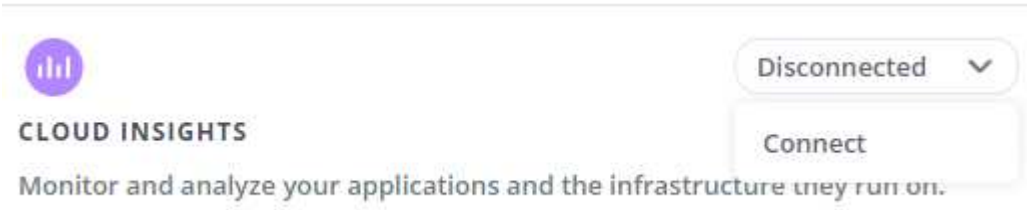
Prima di iniziare

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

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

Fasi

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



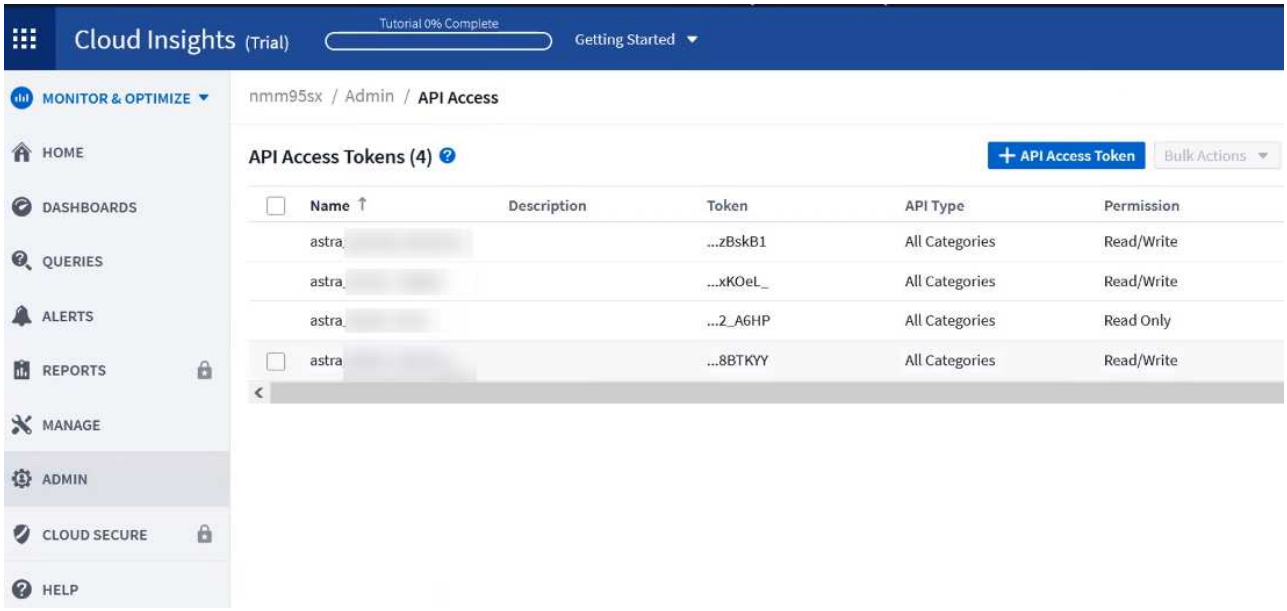
4. Inserire i token API Cloud Insights e l'URL del tenant. L'URL del tenant ha il seguente formato, ad esempio:

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

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

a. Per ottenere il "Token API", Accedere all'URL del tenant Cloud Insights.

b. In Cloud Insights, generare un token di accesso API **lettura/scrittura** e **sola lettura** facendo clic su **Amministratore** > **accesso API**.



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

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

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

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

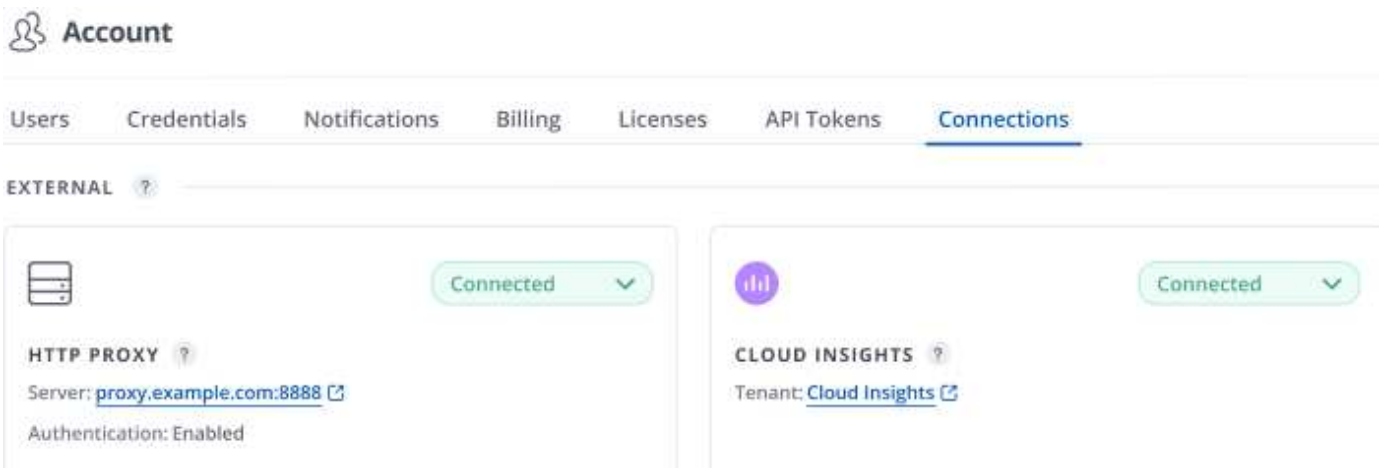
5. Selezionare **Connect**.

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

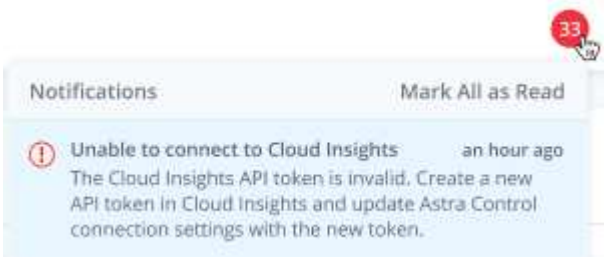
> Per passare facilmente da un'unità di controllo Astra a un'interfaccia utente Cloud Insights e viceversa, assicurarsi di aver effettuato l'accesso a entrambe.

Visualizzare i dati in Cloud Insights

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

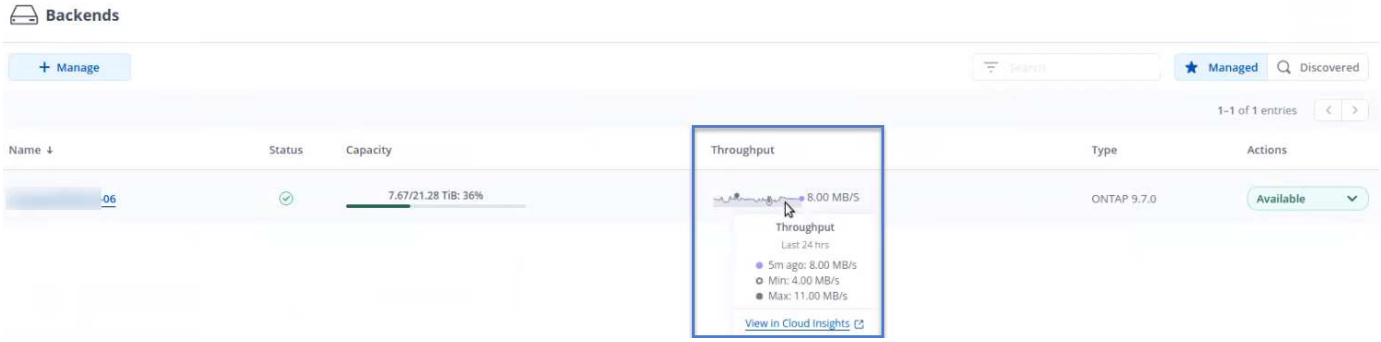


Se la connessione non è riuscita per qualche motivo, lo stato visualizza **Failed** (non riuscito). Il motivo del guasto è disponibile in **Notifiche** nella parte superiore destra dell'interfaccia utente.



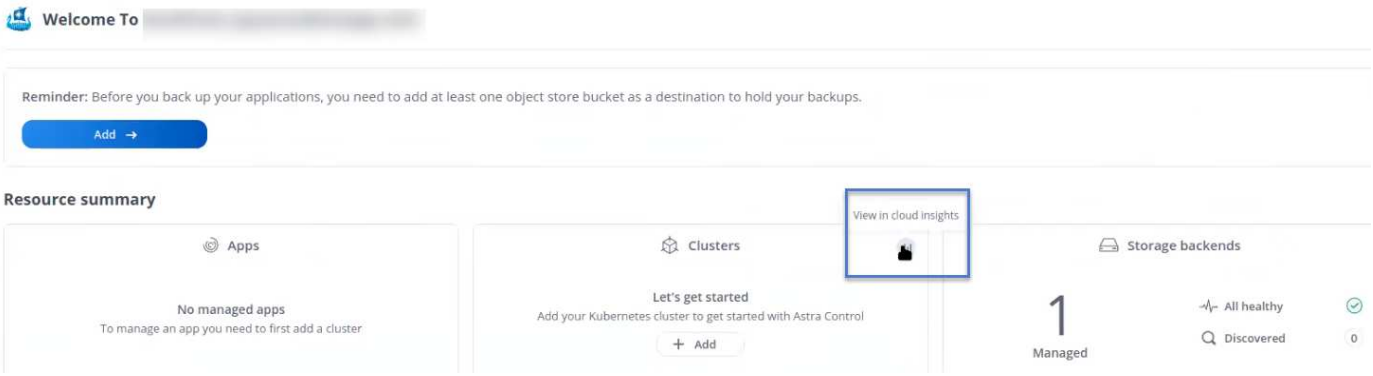
Le stesse informazioni sono disponibili anche in **account** > **Notifiche**.

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



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

Le informazioni sono disponibili anche nella * Dashboard*.



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

Modificare la connessione Cloud Insights

È possibile modificare la connessione Cloud Insights.

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

Fasi

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

Disattiva la connessione Cloud Insights

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

Fasi

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

Connettiti a Prometheus

Con Prometheus è possibile monitorare i dati di Astra Control Center. Puoi configurare Prometheus per raccogliere le metriche dall'endpoint di metriche del cluster Kubernetes e utilizzare Prometheus anche per visualizzare i dati delle metriche.

Per ulteriori informazioni sull'utilizzo di Prometheus, consultare la relativa documentazione all'indirizzo "Introduzione a Prometheus".

Di cosa hai bisogno

Assicurarsi di aver scaricato e installato il pacchetto Prometheus sul cluster Astra Control Center o su un cluster diverso in grado di comunicare con il cluster Astra Control Center.

Seguire le istruzioni nella documentazione ufficiale per "Installare Prometheus".

Prometheus deve essere in grado di comunicare con il cluster Astra Control Center Kubernetes. Se Prometheus non è installato sul cluster Astra Control Center, è necessario assicurarsi che sia in grado di comunicare con il servizio di metriche in esecuzione sul cluster Astra Control Center.

Configurare Prometheus

Astra Control Center espone un servizio di metriche sulla porta TCP 9090 nel cluster Kubernetes. Devi configurare Prometheus per raccogliere le metriche da questo servizio.

Fasi

1. Accedere al server Prometheus.
2. Aggiungere la voce del cluster in `prometheus.yml` file. In `yml` aggiungere una voce simile alla seguente per il cluster in `scrape_configs section`:

```
job_name: '<Add your cluster name here. You can abbreviate. It just
needs to be a unique name>'
  metrics_path: /accounts/<replace with your account ID>/metrics
  authorization:
     credentials: <replace with your API token>
  tls_config:
     insecure_skip_verify: true
  static_configs:
    - targets: ['<replace with your astraAddress. If using FQDN, the
prometheus server has to be able to resolve it>']
```

> Se si imposta `tls_config insecure_skip_verify` a. `true`, Il protocollo di crittografia TLS non è richiesto.

3. Riavviare il servizio Prometheus:

```
sudo systemctl restart prometheus
```

Accedi a Prometheus

Accedere all'URL Prometheus.

Fasi

1. In un browser, inserire l'URL Prometheus con la porta 9090.

2. Verificare la connessione selezionando **Status** > **Targets**.

Visualizza i dati in Prometheus

Puoi utilizzare Prometheus per visualizzare i dati di Astra Control Center.

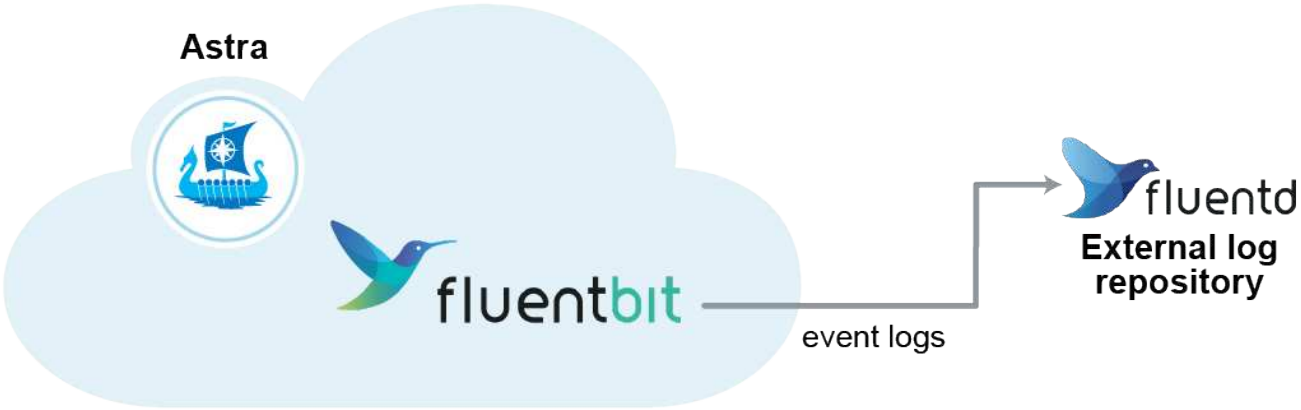
Fasi

1. In un browser, inserire l'URL Prometheus.
2. Dal menu Prometheus, selezionare **grafico**.
3. Per utilizzare Metrics Explorer (Esplora metriche), selezionare l'icona accanto a **Execute** (Esegui).
4. Selezionare `scrape_samples_scraped` E selezionare **Esegui**.
5. Per visualizzare lo scraping dei campioni nel tempo, selezionare **Graph** (grafico).

Se sono stati raccolti più dati del cluster, le metriche di ciascun cluster appaiono in un colore diverso.

Connettersi a Fluentd

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



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

Prima di iniziare

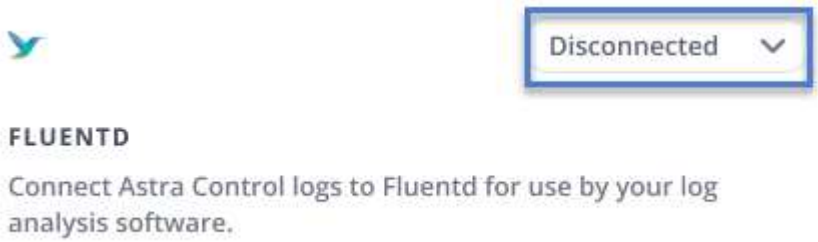
- Un account Astra Control Center con privilegi **admin**/**owner**.
- Astra Control Center installato e in esecuzione su un cluster Kubernetes.

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

Fasi

1. Accedere ad Astra Control Center utilizzando un account con privilegio **admin**/**owner**.
2. Selezionare **account** > **connessioni**.

3. Selezionare **Connect** dall'elenco a discesa in cui viene visualizzato **disconnected** per aggiungere la connessione.



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

Risultato

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

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

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

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

Modificare la connessione Fluentd

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

Fasi

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

Disattiva la connessione Fluentd

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

Fasi

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

Annulla la gestione di app e cluster

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

Annullare la gestione di un'applicazione

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

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 Center interrompe la gestione dell'applicazione.

Annullare la gestione di un cluster

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

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

Quando si annulla la gestione di un cluster:

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

Fasi

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

Risultato

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

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

Aggiornare Astra Control Center

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

Queste istruzioni descrivono il processo di upgrade per Astra Control Center dalla seconda release più recente a questa release corrente. Non è possibile eseguire l'aggiornamento direttamente da una versione che è costituita da due o più versioni precedenti alla release corrente. Se la versione installata di Astra Control Center è più recente, potrebbe essere necessario eseguire gli aggiornamenti della catena alle versioni più recenti fino a quando Astra Control Center installato non è solo una versione precedente alla versione più recente. Per un elenco completo delle versioni rilasciate, vedere "note di rilascio".

Prima di iniziare

Prima di eseguire l'aggiornamento, assicurarsi che l'ambiente soddisfi ancora "Requisiti minimi per l'implementazione di Astra Control Center". L'ambiente deve avere i seguenti requisiti:

- **A "supportato" Versione Astra Trident**

  Espandere per i passaggi

  Determinare la versione di Trident in esecuzione:

  ```
  kubectl get tridentversion -n trident
  ```

  Aggiornare Astra Trident, se necessario, utilizzando questi elementi "istruzioni".

La release 23,10 è l'ultima release di Astra Control Center che supporterà Astra Trident. Si consiglia vivamente di farlo "Abilita Astra Control Provisioner" Per accedere a funzionalità avanzate di gestione e provisioning dello storage oltre a quelle offerte da Astra Trident. È necessario eseguire l'aggiornamento ad Astra Control Center 23,10 e abilitare Astra Control Provivisioner per utilizzare questa funzionalità estesa. Astra Control Provisioner non funzionerà con le versioni precedenti di Astra Control Center.

- **Una distribuzione Kubernetes supportata**

Espandere per i passaggi

Determinare la versione di Kubernetes in esecuzione:

```
kubectl get nodes -o wide
```

- **Risorse cluster sufficienti**

  Espandere per i passaggi

  Determinare le risorse del cluster disponibili:

  ```
  kubectl describe node <node name>
  ```

- **Un registro che è possibile utilizzare per inviare e caricare le immagini di Astra Control Center**
- **Una classe di archiviazione predefinita**

  Espandere per i passaggi

  Determinare la classe di storage predefinita:

  ```
  kubectl get storageclass
  ```

- **Servizi API sani e disponibili**

  Espandere per i passaggi

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

  ```
  kubectl get apiservices
  ```

- **(solo OpenShift) operatori cluster sani e disponibili**

  Espandere per i passaggi

  Assicurarsi che tutti gli operatori del cluster siano in buono stato e disponibili.

  ```
  kubectl get clusteroperators
  ```

- **Accedere al Registro di sistema dell'immagine di controllo Astra di NetApp**:

È possibile ottenere le immagini di installazione e i miglioramenti delle funzionalità per Astra Control, come Astra Control provisioner, dal registro delle immagini di NetApp.

Espandere per i passaggi

a. Registrare l'ID dell'account Astra Control necessario per accedere al Registro di sistema.

   Puoi visualizzare l'ID dell'account nell'interfaccia utente Web di Astra Control Service. Selezionare l'icona a forma di figura in alto a destra nella pagina, selezionare **accesso API** e 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:

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

A proposito di questa attività

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

Disconnettersi dall'interfaccia utente di Astra Control Center prima di iniziare l'aggiornamento.

- Scarica ed estrai Astra Control Center
- Rimuovere il plug-in NetApp Astra kubectl e installarlo di nuovo
- Aggiungere le immagini al registro locale
- Installare l'operatore Astra Control Center aggiornato
- Aggiornare Astra Control Center
- Verificare lo stato del sistema

Non eliminare l'operatore di Astra Control Center (ad esempio, `kubectl delete -f astra_control_center_operator_deploy.yaml`) In qualsiasi momento durante l'aggiornamento o l'operazione di Astra Control Center per evitare di eliminare i pod.

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

Scarica ed estrai Astra Control Center

Puoi scegliere di scaricare il bundle Astra Control Center dal sito di supporto di NetApp o utilizzare Docker per estrarre il bundle dal registro delle immagini di Astra Control Service.

Sito di supporto NetApp

1. Scarica il bundle contenente Astra Control Center (`astra-control-center-[version].tar.gz`) da "Pagina di download di Astra Control Center".
2. (Consigliato ma opzionale) Scarica il bundle di certificati e firme per Astra Control Center (`astra-control-center-certs-[version].tar.gz`) per verificare la firma del bundle.

   Espandere per i dettagli

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

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

   Viene visualizzato l'output `Verified OK` una volta completata la verifica.

3. Estrarre le immagini dal bundle Astra Control Center:

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

Registro delle immagini di Astra Control

1. Effettua l'accesso ad Astra Control Service.
2. Nella Dashboard, selezionare **distribuire un'istanza autogestita di Astra Control**.
3. Seguire le istruzioni per accedere al registro delle immagini di Astra Control, estrarre l'immagine di installazione di Astra Control Center ed estrarre l'immagine.

Rimuovere il plug-in NetApp Astra kubectl e installarlo di nuovo

È possibile utilizzare il plug-in della riga di comando di NetApp Astra kubectl per inviare immagini a un repository Docker locale.

1. Determinare se il plug-in è installato:

   ```
   kubectl astra
   ```

2. Eseguire una delle seguenti operazioni:
   - Se il plugin è installato, il comando dovrebbe restituire il plugin kubectl help ed è possibile rimuovere la versione esistente di kubectl-astra: `delete /usr/local/bin/kubectl-astra`.
   - Se il comando restituisce un errore, il plug-in non è installato ed è possibile procedere con la fase successiva per installarlo.

3. Installare il plug-in:

   a. Elencare i binari del plugin NetApp Astra kubectl disponibili e annotare il nome del file necessario per il sistema operativo e l'architettura della CPU:

      La libreria di plugin kubectl fa parte del bundle tar e viene estratta nella cartella `kubectl-astra`.

```
ls kubectl-astra/
```

   a. Spostare il binario corretto nel percorso corrente e rinominarlo `kubectl-astra`:

```
cp kubectl-astra/<binary-name> /usr/local/bin/kubectl-astra
```

Aggiungere le immagini al registro locale

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

Docker

1. Passare alla directory root del tarball. Viene visualizzata la `acc.manifest.bundle.yaml` file e queste directory:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Trasferire le immagini del pacchetto nella directory delle immagini di Astra Control Center nel registro locale. Eseguire le seguenti sostituzioni prima di eseguire `push-images` comando:

   - Sostituire <BUNDLE_FILE> con il nome del file bundle di controllo Astra (`acc.manifest.bundle.yaml`).
   - Sostituire <MY_FULL_REGISTRY_PATH> con l’URL del repository Docker; ad esempio, "<a href="https://<docker-registry>"" class="bare">https://<docker-registry>".
   - Sostituire <MY_REGISTRY_USER> con il nome utente.
   - Sostituire <MY_REGISTRY_TOKEN> con un token autorizzato per il registro.

   ```
   kubectl astra packages push-images -m <BUNDLE_FILE> -r
   <MY_FULL_REGISTRY_PATH> -u <MY_REGISTRY_USER> -p
   <MY_REGISTRY_TOKEN>
   ```

Podman

1. Passare alla directory root del tarball. Vengono visualizzati il file e la directory seguenti:

   ```
   acc/
   kubectl-astra/
   acc.manifest.bundle.yaml
   ```

2. Accedere al Registro di sistema:

   ```
   podman login <YOUR_REGISTRY>
   ```

3. Preparare ed eseguire uno dei seguenti script personalizzato per la versione di Podman utilizzata. Sostituire <MY_FULL_REGISTRY_PATH> con l'URL del repository che include le sottodirectory.

   ```
   <strong>Podman 4</strong>
   ```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

```
<strong>Podman 3</strong>
```

```
export REGISTRY=<MY_FULL_REGISTRY_PATH>
export PACKAGENAME=acc
export PACKAGEVERSION=23.10.0-68
export DIRECTORYNAME=acc
for astraImageFile in $(ls ${DIRECTORYNAME}/images/*.tar) ; do
astraImage=$(podman load --input ${astraImageFile} | sed 's/Loaded
image: //')
astraImageNoPath=$(echo ${astraImage} | sed 's:.*/::')
podman tag ${astraImageNoPath} ${REGISTRY}/netapp/astra/
${PACKAGENAME}/${PACKAGEVERSION}/${astraImageNoPath}
podman push ${REGISTRY}/netapp/astra/${PACKAGENAME}/${
PACKAGEVERSION}/${astraImageNoPath}
done
```

Il percorso dell'immagine creato dallo script deve essere simile al seguente, a seconda della configurazione del Registro di sistema:

```
https://downloads.example.io/docker-astra-control-
prod/netapp/astra/acc/23.10.0-68/image:version
```

Installare l'operatore Astra Control Center aggiornato

1. Modificare la directory:

```
cd manifests
```

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

```
vim astra_control_center_operator_deploy.yaml
```

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

```
imagePullSecrets: [{name: astra-registry-cred}]
```

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

   c. Cambiare `ASTRA_IMAGE_REGISTRY` per `acc-operator` al percorso del registro in cui sono state inviate le immagini in a. passaggio precedente.

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

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

Esempio astra_control_center_operator_deploy.yaml:

```
apiVersion: apps/v1
kind: Deployment
metadata:
  labels:
    control-plane: controller-manager
  name: acc-operator-controller-manager
  namespace: netapp-acc-operator
spec:
  replicas: 1
  selector:
    matchLabels:
      control-plane: controller-manager
  strategy:
    type: Recreate
  template:
    metadata:
      labels:
        control-plane: controller-manager
    spec:
      containers:
      - args:
        - --secure-listen-address=0.0.0.0:8443
        - --upstream=http://127.0.0.1:8080/
        - --logtostderr=true
        - --v=10
        image: ASTRA_IMAGE_REGISTRY/kube-rbac-proxy:v4.8.0
        name: kube-rbac-proxy
        ports:
        - containerPort: 8443
          name: https
      - args:
        - --health-probe-bind-address=:8081
        - --metrics-bind-address=127.0.0.1:8080
        - --leader-elect
        env:
        - name: ACCOP_LOG_LEVEL
          value: "2"
        - name: ACCOP_HELM_UPGRADETIMEOUT
          value: 300m
        image: ASTRA_IMAGE_REGISTRY/acc-operator:23.10.72
        imagePullPolicy: IfNotPresent
        livenessProbe:
          httpGet:
            path: /healthz
```

```
            port: 8081
          initialDelaySeconds: 15
          periodSeconds: 20
        name: manager
        readinessProbe:
          httpGet:
            path: /readyz
            port: 8081
          initialDelaySeconds: 5
          periodSeconds: 10
        resources:
          limits:
            cpu: 300m
            memory: 750Mi
          requests:
            cpu: 100m
            memory: 75Mi
        securityContext:
          allowPrivilegeEscalation: false
      imagePullSecrets: []
      securityContext:
        runAsUser: 65532
      terminationGracePeriodSeconds: 10
```

3. Installare l'operatore Astra Control Center aggiornato:

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

Esempio di risposta:

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

4. Verificare che i pod siano in esecuzione:

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

Aggiornare Astra Control Center

1. Modificare la risorsa personalizzata Astra Control Center (CR):

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

2. Modificare il numero di versione di Astra (`astraVersion` all'interno di `spec`) da `23.07.0` a. `23.10.0`:

> Non è possibile eseguire l'aggiornamento direttamente da una versione che è costituita da due o più versioni precedenti alla release corrente. Per un elenco completo delle versioni rilasciate, vedere "note di rilascio".

```
spec:
  accountName: "Example"
  astraVersion: "[Version number]"
```

3. Verificare che il percorso del Registro di sistema dell'immagine corrisponda al percorso del Registro di sistema in cui sono state inviate le immagini in passaggio precedente. Aggiornare `imageRegistry` all'interno di `spec` se il registro di sistema è stato modificato dall'ultima installazione.

```
  imageRegistry:
    name: "[your_registry_path]"
```

4. Aggiungere quanto segue al `crds` configurazione all'interno di `spec`:

```
crds:
  shouldUpgrade: true
```

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

```
additionalValues:
    nautilus:
      startupProbe:
        periodSeconds: 30
        failureThreshold: 600
    keycloak-operator:
      livenessProbe:
        initialDelaySeconds: 180
      readinessProbe:
        initialDelaySeconds: 180
```

6. Salvare e uscire dall'editor di file. Le modifiche verranno applicate e l'aggiornamento avrà inizio.
7. (Facoltativo) verificare che i pod terminino e diventino nuovamente disponibili:

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

8. Attendere che le condizioni di stato di Astra Control indichino che l'aggiornamento è completo e pronto (`True`):

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

Risposta:

```
NAME    UUID                                   VERSION     ADDRESS
READY
astra   9aa5fdae-4214-4cb7-9976-5d8b4c0ce27f   23.10.0-68
10.111.111.111  True
```

Per monitorare lo stato dell'aggiornamento durante l'operazione, eseguire il seguente comando: `kubectl get AstraControlCenter -o yaml -n [netapp-acc or custom namespace]`

Per esaminare i registri dell'operatore di Astra Control Center, eseguire il seguente comando:
`kubectl logs deploy/acc-operator-controller-manager -n netapp-acc-operator -c manager -f`

Verificare lo stato del sistema

1. Accedere ad Astra Control Center.
2. Verificare che la versione sia stata aggiornata. Consultare la pagina **supporto** nell'interfaccia utente.
3. Verificare che tutti i cluster e le applicazioni gestiti siano ancora presenti e protetti.

Abilita Astra Control Provisioner

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

In arrivo gli update di Astra Control, Astra Control Provivisioner sostituirà Astra Trident come provisioner di storage e orchestrator nell'architettura 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.

A proposito di questa attività

È necessario seguire questa procedura se si è un utente di Astra Control Center con licenza e si sta cercando di utilizzare la funzionalità di Astra Control Provisioner. Devi seguire questa procedura anche se sei un utente di Astra Trident e desideri utilizzare le funzionalità aggiuntive fornite da Astra Control Provisioner senza utilizzare Astra Control.

Per ogni caso, la funzionalità di provisioning non è abilitata per impostazione predefinita in Astra Trident 23,10, ma può essere abilitata utilizzando questo processo.

Prima di iniziare

Se stai abilitando Astra Control provisioner, esegui prima quanto segue:

Utenti di Astra Control Provisioners con Astra Control Center

- **Ottenere una licenza Astra Control Center**: È necessario un "Licenza Astra Control Center" Per abilitare Astra Control Provisioner e accedere alle funzionalità fornite.
- **Installa o esegui l'aggiornamento ad Astra Control Center 23,10**: Avrai bisogno di questa versione se hai intenzione di utilizzare Astra Control Provisioner con Astra Control.
- **Confirmi che il tuo cluster ha un'architettura di sistema AMD64**: L'immagine Astra Control Provivisioner è fornita in entrambe le architetture CPU AMD64 e ARM64, ma solo AMD64 è supportato da Astra Control Center.
- **Ottenere un account del Servizio di controllo Astra per l'accesso al Registro di sistema**: Se si intende utilizzare il Registro di sistema di controllo Astra piuttosto che il Sito di supporto NetApp per scaricare l'immagine del revisioner di controllo Astra, completare la registrazione per un "Account Astra Control Service". Dopo aver completato e inviato il modulo e creato un account BlueXP, riceverai un'email di benvenuto con Astra Control Service.
- **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 23,10 con Astra Control Provisioner se il tuo Astra Trident si trova all'interno di una finestra a quattro release della versione 23,10. Ad esempio, puoi eseguire l'upgrade direttamente da Astra Trident 22,10 a 23,10.

Solo utenti di Astra Control provisioner

- **Ottenere una licenza Astra Control Center**: È necessario un "Licenza Astra Control Center" Per abilitare Astra Control Provisioner e accedere alle funzionalità fornite.
- **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 23,10 con Astra Control Provisioner se il tuo Astra Trident si trova all'interno di una finestra a quattro release della versione 23,10. Ad esempio, puoi eseguire l'upgrade direttamente da Astra Trident 22,10 a 23,10.
- **Prendi un account Astra Control Service per l'accesso al Registro di sistema**: Per scaricare le immagini di Astra Control provisioner, è necessario accedere al Registro di sistema. Per iniziare, completa la registrazione per un "Account Astra Control Service". Dopo aver completato e inviato il modulo e creato un account BlueXP, riceverai un'email di benvenuto con Astra Control Service.

(Fase 1) scaricare ed estrarre Astra Control Provisioner

Gli utenti di Astra Control Center possono scaricare l'immagine usando il metodo del registro di sistema o il sito di supporto di NetApp. Gli utenti di Astra Trident che desiderano utilizzare Astra Control Protivisioner senza Astra Control devono utilizzare il metodo del Registro di sistema.

(Opzionale) Sito di supporto NetApp

1. Scarica il bundle Astra Control Provisioner (`trident-acp-[version].tar`) da "Pagina di download di Astra Control Center".
2. (Consigliato ma facoltativo) scaricate il pacchetto di certificati e firme per Astra Control Center (astra-control-center-certs-[version].tar.gz) per verificare la firma del pacchetto trident-acp-[version] tar.

Espandere per i dettagli

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

```
openssl dgst -sha256 -verify certs/AstraControlCenterDockerImages-public.pub -signature certs/trident-acp-[version].tar.sig trident-acp-[version].tar
```

3. Caricare l'immagine di Astra Control provisioner:

```
docker load < trident-acp-23.10.0.tar
```

Risposta:

```
Loaded image: trident-acp:23.10.0-linux-amd64
```

4. Contrassegnare l'immagine:

```
docker tag trident-acp:23.10.0-linux-amd64 <my_custom_registry>/trident-acp:23.10.0
```

5. Inviare l'immagine al registro personalizzato:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

(Opzione) Registro di sistema delle immagini Astra Control

È possibile utilizzare Podman invece di Docker per i comandi di questa procedura. Se si utilizza un ambiente Windows, si consiglia di utilizzare PowerShell.

1. Accedere al Registro di sistema dell'immagine di controllo Astra di NetApp:
   a. Accedere all'interfaccia utente Web di Astra Control Service e selezionare l'icona raffigurata in alto a destra nella pagina.
   b. Selezionare **API access**.
   c. Annotare l'ID account.
   d. Nella stessa pagina, selezionare **generate API token**, copiare la stringa del token API negli Appunti e salvarla nell'editor.
   e. 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. Se si dispone di un Registro di sistema personalizzato, attenersi alla procedura descritta di seguito per spostare l'immagine nel Registro di sistema 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:23.10.0
--platform <cluster platform>
```

Esempio:

```
docker pull cr.astra.netapp.io/astra/trident-acp:23.10.0
--platform linux/amd64
```

b. Contrassegnare l'immagine:

```
docker tag cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

c. Inviare l'immagine al registro personalizzato:

```
docker push <my_custom_registry>/trident-acp:23.10.0
```

Gru

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

```
crane copy cr.astra.netapp.io/astra/trident-acp:23.10.0
<my_custom_registry>/trident-acp:23.10.0
```

(Fase 2) attiva Astra Control Provisioner in Astra Trident

Determinare se il metodo di installazione originale ha utilizzato un e completare i passaggi appropriati in base al metodo originale.

> Non utilizzare Helm per abilitare Astra Control Provisioner. Se hai utilizzato Helm per l'installazione originale e stai effettuando l'aggiornamento a 23,10, dovrai utilizzare l'operatore Trident o tridentctl per eseguire l'abilitazione di Astra Control Provisioner.

Operatore Astra Trident

1. "Scaricare il programma di installazione di Astra Trident ed estrarlo".
2. Completa questi passaggi se non hai ancora installato Astra Trident o se hai rimosso l'operatore dall'implementazione originale di Astra Trident:
   a. Creare il CRD:

```
kubectl create -f
deploy/crds/trident.netapp.io_tridentorchestrators_crd_post1.16.y
aml
```

   b. 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.
3. Aggiorna Astra Trident alla versione 23.10.0:

> 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-
23.10.0/deploy/<bundle-name.yaml>
```

4. Verificare che Astra Trident sia in esecuzione:

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

   Risposta:

```
NAME      AGE
trident   21m
```

5. 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>
```

6. Modificare il TridentOrchestrator CR e apportare le seguenti modifiche:

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

a. 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:23.10.0` oppure `tridentImage: netapp/trident:23.10.0`).

b. Abilita Astra Control Provisioner (`enableACP: true`).

c. Impostare la posizione del Registro di sistema personalizzata per l'immagine Astra Control Provivioner o estrarla dal Registro di sistema Astra Control (`acpImage: <my_custom_registry>/trident-acp:23.10.0` oppure `acpImage: cr.astra.netapp.io/astra/trident-acp:23.10.0`).

d. 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:23.10.0
  enableACP: true
  acpImage: <registry>/trident-acp:23.10.0
  imagePullSecrets:
  - <secret_name>
```

7. Salvare e uscire dal file. Il processo di distribuzione si avvia automaticamente.
8. 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.

9. Verificare `trident-acp` il container è in esecuzione e così `acpVersion` è `23.10.0` con stato di `Installed`:

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

Risposta:

```
status:
  acpVersion: 23.10.0
  currentInstallationParams:
    ...
    acpImage: <registry>/trident-acp:23.10.0
    enableACP: "true"
    ...
  ...
  status: Installed
```

tridentctl

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

```
./tridentctl -n trident install --enable-acp=true --acp
-image=mycustomregistry/trident-acp:23.10
```

4. Confermare che Astra Control Provisioner è stato abilitato:

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

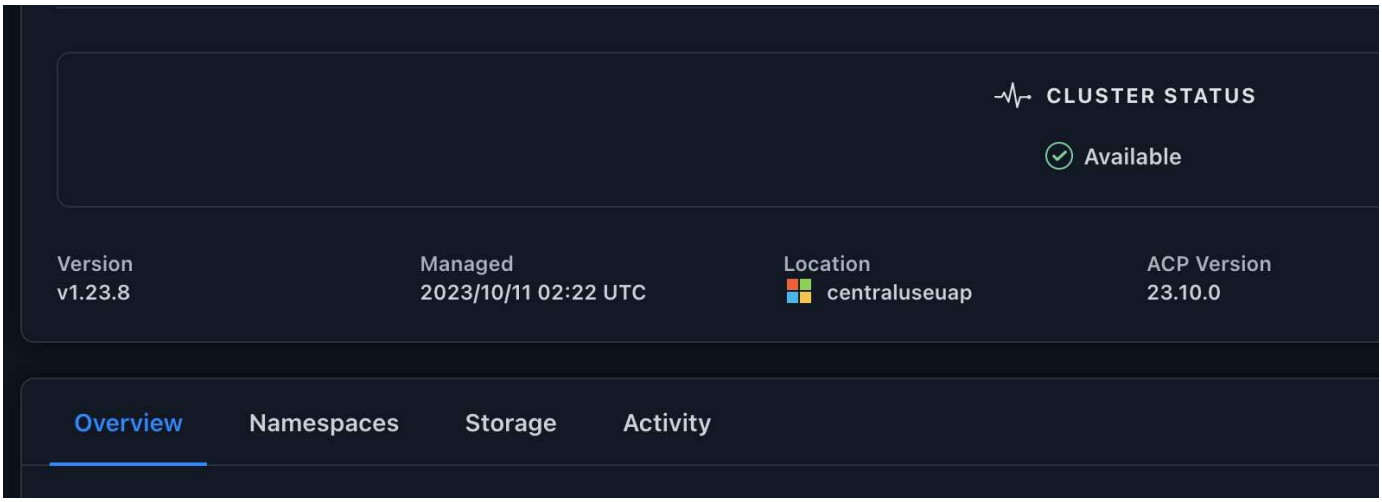
Risposta:

```
+----------------+----------------+-------------+ | SERVER VERSION |
CLIENT VERSION | ACP VERSION | +----------------+----------------
+-------------+ | 23.10.0 | 23.10.0 | 23.10.0. | +----------------
+----------------+-------------+
```

Risultato

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

(Solo per gli utenti di Astra Control Center) dopo l'installazione di Astra Control provisioner, il cluster che ospita il provisioner nell'interfaccia utente di Astra Control Center mostrerà un `ACP version` piuttosto che `Trident version` campo e numero della versione installata corrente.



Per ulteriori informazioni

- "Documentazione sugli aggiornamenti di Astra Trident"

Disinstallare Astra Control Center

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

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

Prima di iniziare

1. "Annulla gestione di tutte le applicazioni" sui cluster.
2. "Annulla gestione di tutti i cluster".

Fasi

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

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

   Risultato:

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

2. Utilizzare il seguente comando per eliminare `netapp-acc` namespace (o personalizzato):

   ```
   kubectl delete ns [netapp-acc or custom namespace]
   ```

   Risultato di esempio:

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

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

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

Risultato:

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

Risoluzione dei problemi di disinstallazione

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

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

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

Fasi

1. Eliminare `acc-monitoring` agente:

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

Risultato:

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

2. Eliminare lo spazio dei nomi:

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

Risultato:

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

3. Conferma la rimozione delle risorse:

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

Risultato:

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

4. Conferma rimozione dell'agente di monitoraggio:

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

Risultato del campione:

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

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

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

Risultato:

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

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

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

Fasi

1. Elencare i CRD Traefik installati sul cluster:

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

   Risposta

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

2. Eliminare i CRD:

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

Trova ulteriori informazioni

- "Problemi noti per la disinstallazione"

Informazioni sul copyright

Copyright © 2025 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 COMMERCIABILITÀ 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 CONSEQUENZIALE (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.