Proteggi le app

Astra Control Center

NetApp
November 27, 2023

Sommario

Proteggi le app . . . 1
Panoramica della protezione . . . 1
Proteggi le app con snapshot e backup . . . 1
Ripristinare le applicazioni . . . 6
Replica delle applicazioni tra back-end di storage utilizzando la tecnologia SnapMirror . . . 11
Clonare e migrare le applicazioni . . . 18
Gestire gli hook di esecuzione delle applicazioni . . . 20
Proteggi Astra Control Center con Astra Control Center . . . 29

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

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

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

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

Configurare un criterio di protezione

Una policy di protezione protegge un'applicazione creando snapshot, backup o entrambi in base a una pianificazione definita. È possibile scegliere di creare snapshot e backup ogni ora, ogni giorno, ogni settimana e ogni mese, nonché specificare il numero di copie da conservare.

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".

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.

Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, non è possibile utilizzare policy di protezione. Migrare a una classe di storage supportata da Astra Control se si desidera pianificare backup e snapshot.

Fasi

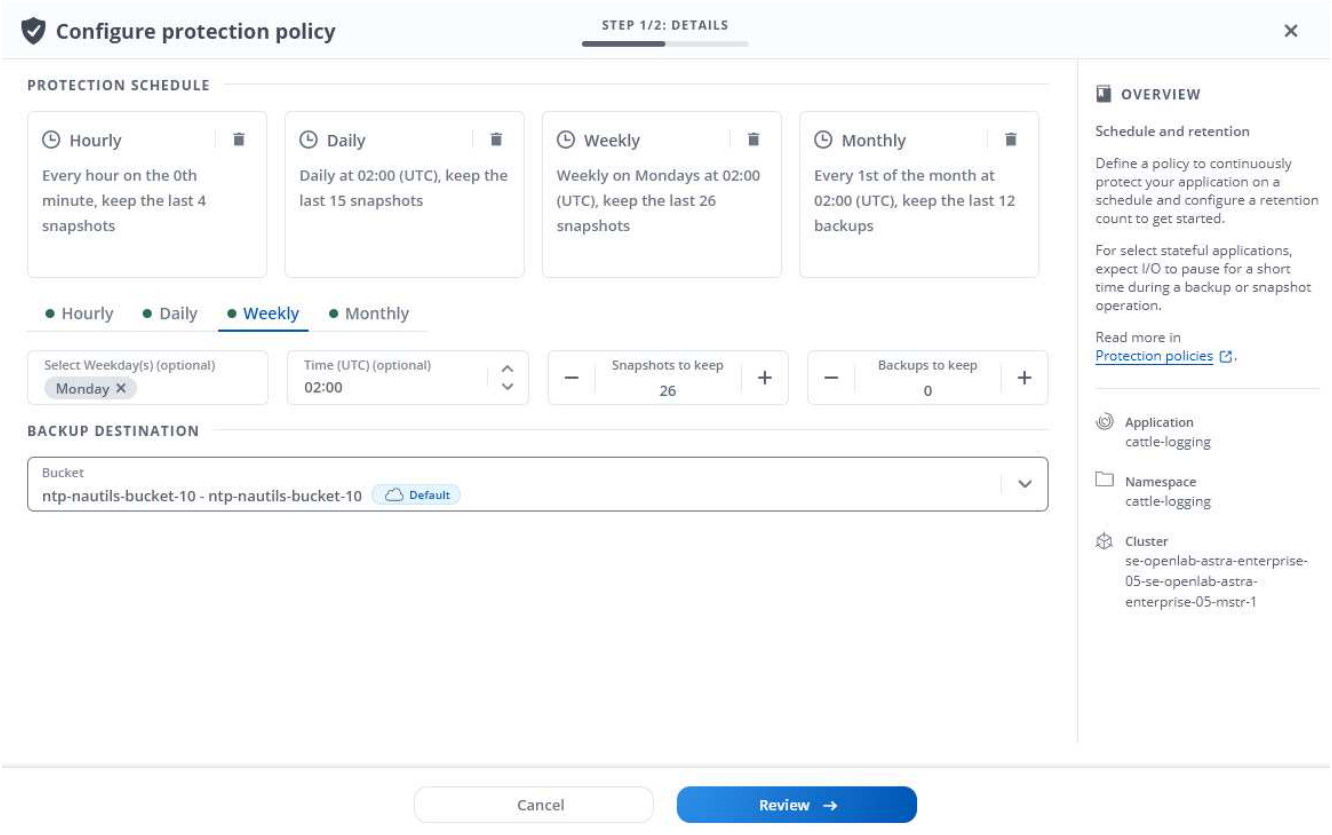
1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Configura policy di protezione**.

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.

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

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

> 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. Backup delle applicazioni supportate da `ontap-nas-economy` sono disruptive e l'applicazione non sarà disponibile fino al completamento dell'operazione di backup.

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.

Visualizzare snapshot e backup

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

Fasi

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

   Le istantanee vengono visualizzate per impostazione predefinita.

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

Eliminare le istantanee

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

Non è possibile eliminare 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.

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione.
2. Selezionare **Data Protection** (protezione dati).
3. Selezionare **Backup**.
4. Dal menu Options (Opzioni) nella colonna **Actions** (azioni) per il backup desiderato, selezionare **Cancel**

(Annulla).

5. Digitare la parola "CANCEL" per confermare l'operazione, quindi selezionare **Yes, CANCEL backup** (Sì, Annulla backup*).

Eliminare i backup

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

> Per annullare un backup in esecuzione, seguire le istruzioni riportate in Annullare i backup. Per eliminare il backup, attendere che sia stato completato, quindi seguire queste istruzioni.

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.

A proposito di questa attività

- **Proteggi prima le tue applicazioni**: Ti consigliamo vivamente di creare un'istantanea o un backup dell'applicazione prima di ripristinarla. In questo modo, è possibile clonare lo snapshot o il backup nel caso in cui il ripristino non abbia esito positivo.
- **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 OpenShift) Aggiungi policy*: 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
```

- **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.

     > È possibile utilizzare questa procedura per eseguire una delle due operazioni a una classe di storage supportata da `ontap-nas` Sullo stesso cluster **O** copiare l'applicazione in un altro cluster con una classe di storage supportata da `ontap-nas-economy` driver.

     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 la creazione di un nuovo spazio dei nomi mediante un'operazione di clone o ripristino, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo per consentire all'utente interessato di accedere al nuovo spazio dei nomi.

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.

Migrazione dallo storage ontap-nas-Economy allo storage ontap-nas

È possibile utilizzare Astra Control "ripristino dell'applicazione" oppure "clone dell'applicazione" operazione per migrare i volumi delle applicazioni da una classe di storage supportata da `ontap-nas-economy`, che consente opzioni di protezione applicativa limitate, a una classe di storage supportata da `ontap-nas` Con la sua gamma completa di opzioni di protezione Astra Control. L'operazione di cloning o restore esegue la migrazione dei volumi basati su Qtree che utilizzano un `ontap-nas-economy` back-end per volumi standard supportati da `ontap-nas`. A prescindere dal fatto che lo siano `ontap-nas-economy` supportato solo o misto, verrà migrato alla classe di storage di destinazione. Una volta completata la migrazione, le opzioni di protezione non sono più limitate.

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.

  - **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.
- **Astra Control Center**:

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

  - **Cluster gestiti**: I seguenti cluster devono essere aggiunti e gestiti da 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.
- **Configurazione di Astra Trident/ONTAP**: Il Centro di controllo Astra 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.
- **ontap-nas-economy-backed storage class**: Se l'applicazione utilizza una classe di storage supportata da `ontap-nas-economy` driver, la parte di backup di un'operazione clone è disgregante. L'applicazione di origine non è disponibile fino al completamento del backup. La parte di ripristino dell'operazione clone non ha interruzioni.
- **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 la creazione di un nuovo spazio dei nomi mediante un'operazione di clone o ripristino, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo per consentire all'utente interessato di accedere al nuovo spazio dei nomi.

- **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.

È possibile migrare la classe di storage di un'applicazione a un cloud provider nativo di classe di storage o ad un'altra classe di storage supportata, 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 la creazione di un nuovo spazio dei nomi mediante un'operazione di clone o ripristino, l'amministratore/proprietario dell'account può modificare l'account utente membro e aggiornare i vincoli di ruolo per consentire all'utente interessato di accedere al nuovo spazio dei nomi.

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 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.

- 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 hai eseguito gli hook post-restore con Astra Control Center 23.04 e hai aggiornato Astra Control Center alla versione 23.07, gli hook di esecuzione post-restore non saranno 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.

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

Risultato

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

Eliminare uno script

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

Fasi

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

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

Creare un gancio di esecuzione personalizzato

È possibile creare un gancio di esecuzione personalizzato per un'applicazione 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. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare **Aggiungi**.
4. 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.
5. (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.

6. Al termine, selezionare **Avanti**.
7. 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.

8. Selezionare **Avanti**.
9. Esaminare la configurazione degli uncino di esecuzione.
10. 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.

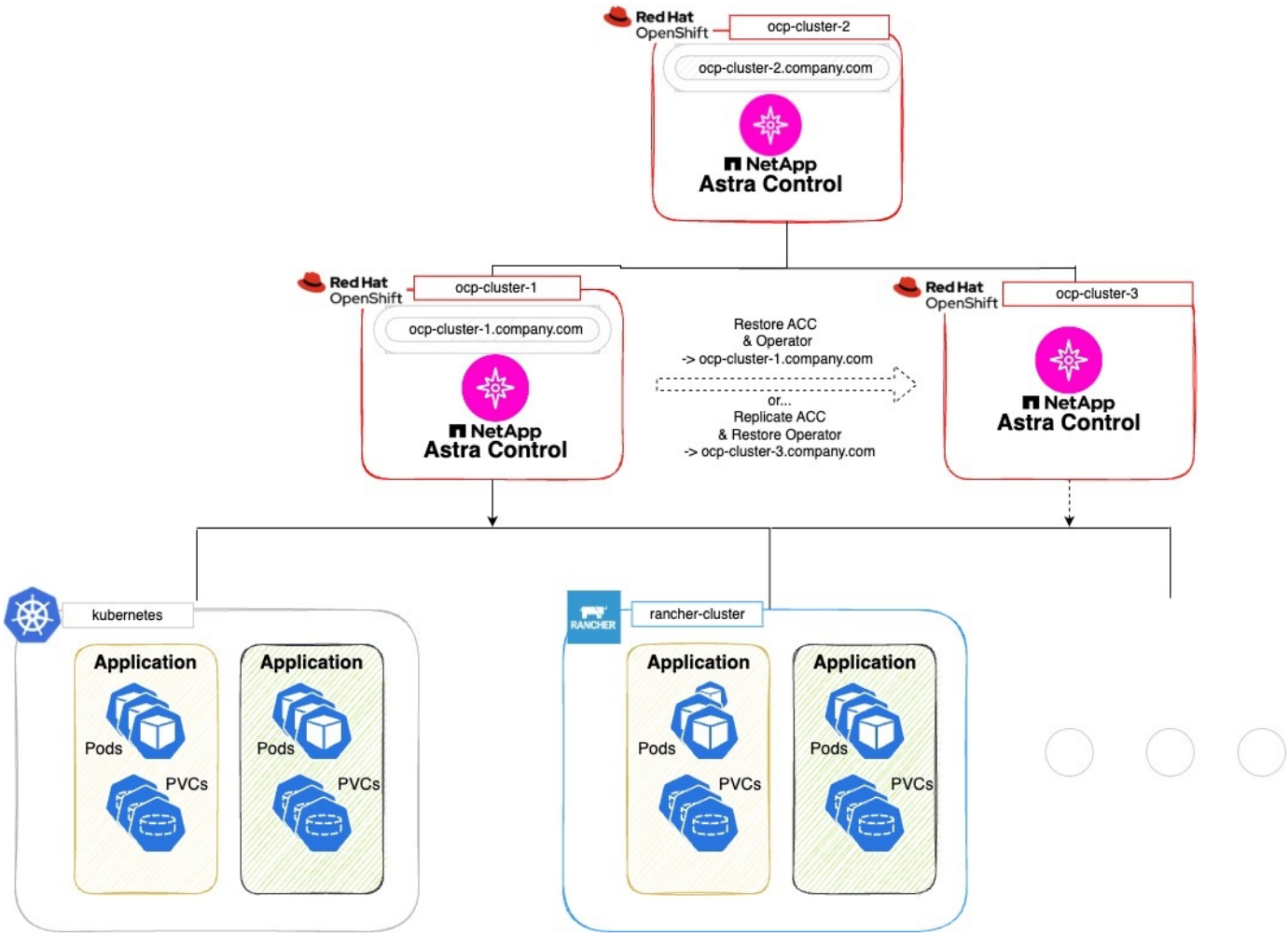
Prima di iniziare

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 etichetta: acc-crds
      - 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 23.07.0-24 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**.

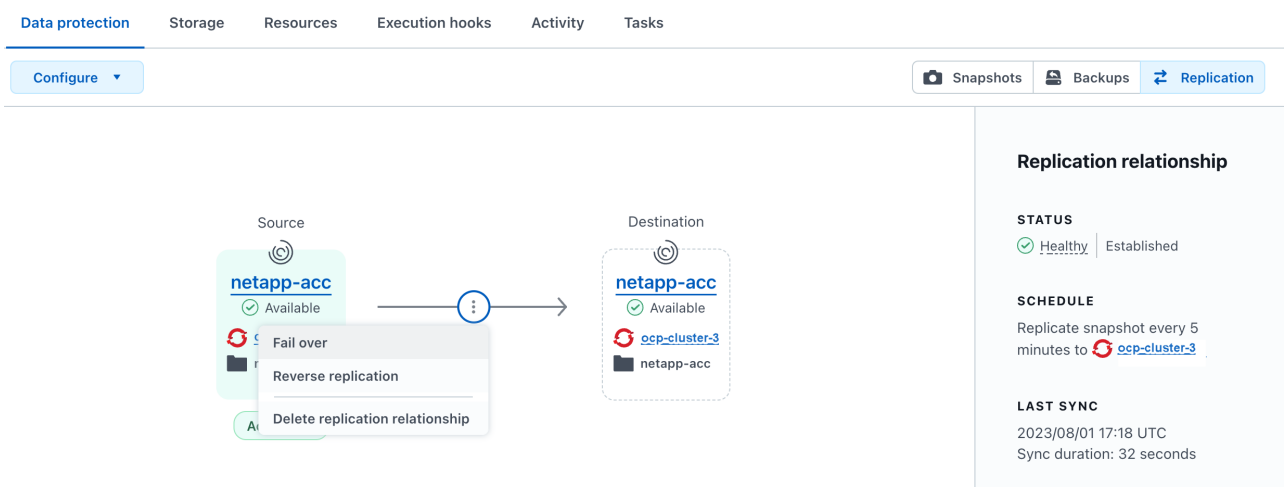
h. Verificare che la configurazione sia corretta e selezionare **Salva**.

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 23.07.0-24 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.

Informazioni sul copyright

Informazioni sul marchio commerciale