Proteggi le app

Astra Control Center

NetApp
June 06, 2024

Sommario

Proteggi le app

Panoramica della protezione

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

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

Workflow di protezione delle app

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

[Uno] Proteggi tutte le app

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

[Due] Configurare una policy di protezione per ogni applicazione

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

[Tre] Modificare i criteri di protezione

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

[Quattro] Replica delle applicazioni su un cluster remoto

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

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

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

Proteggi le app con snapshot e backup

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

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

completamente supportate. Le app implementate con Helm 2 non sono supportate.

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

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

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

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

Configurare un criterio di protezione

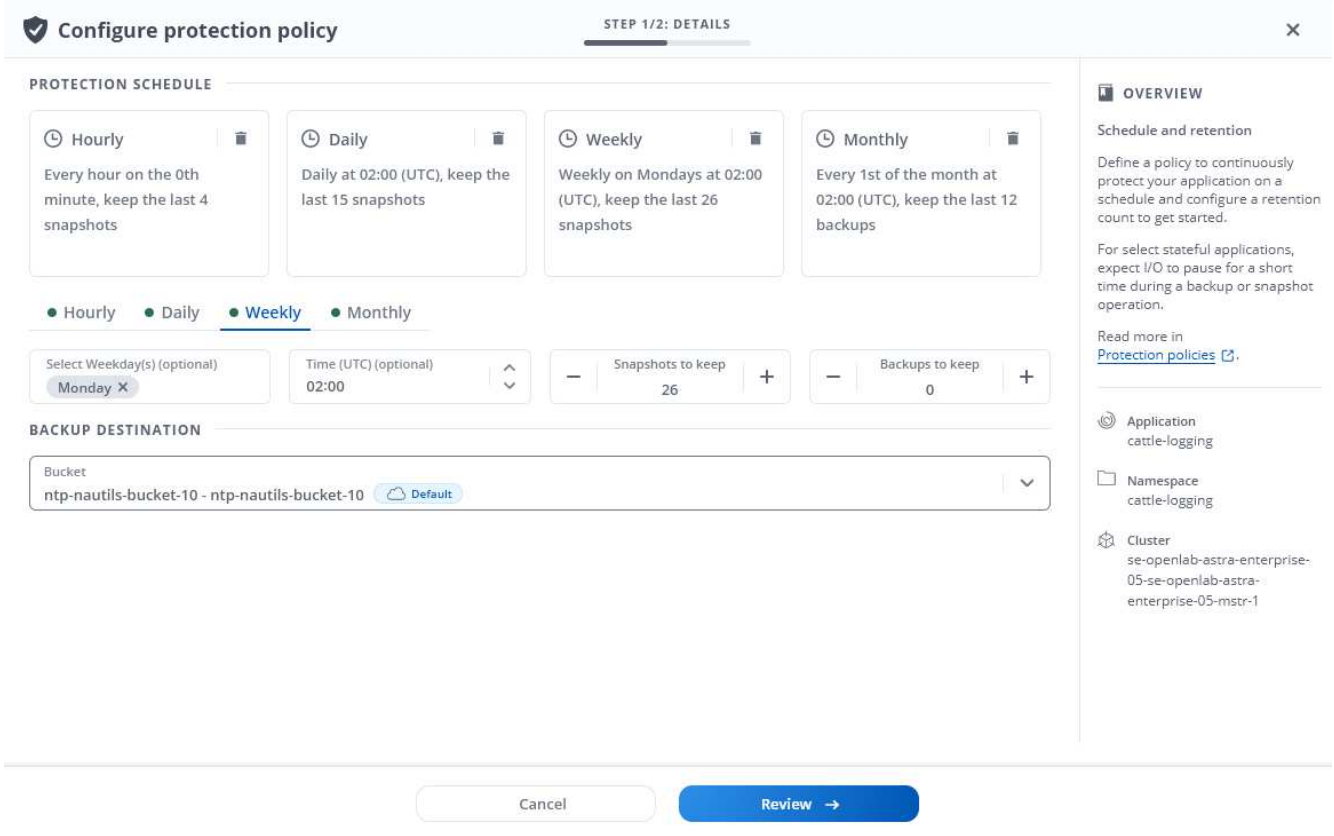
Una policy di protezione protegge un'applicazione creando snapshot, backup o entrambi in base a una pianificazione definita. È possibile scegliere di creare snapshot e backup ogni ora, ogni giorno, ogni settimana e ogni mese, nonché specificare il numero di copie da conservare. Ad esempio, una policy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

Fasi

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

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

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



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

Risultato

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

Creare un'istantanea

Puoi creare uno snapshot on-demand in qualsiasi momento.

Fasi

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

Risultato

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

Creare un backup

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

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

Fasi

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

Risultato

Astra Control Center crea un backup dell'applicazione.

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

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

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

Visualizzare snapshot e backup

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

Fasi

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

   Le istantanee vengono visualizzate per impostazione predefinita.

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

Eliminare le istantanee

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

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

Fasi

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

Risultato

Astra Control Center elimina lo snapshot.

Annullare i backup

È possibile annullare un backup in corso.

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

Fasi

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

Eliminare i backup

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

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

Fasi

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

Risultato

Astra Control Center elimina il backup.

Ripristinare le applicazioni

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

A proposito di questa attività

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

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

Fasi

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

◦ Selezionare **Revisione**.

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

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

Risultato

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

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

Replica delle applicazioni su un sistema remoto utilizzando la tecnologia SnapMirror

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

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

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

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

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

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

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

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

Prerequisiti per la replica

Vedere "prerequisiti per la replica" prima di iniziare.

Impostare una relazione di replica

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

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

Fasi

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

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

   - **Replication frequency** (frequenza di replica): Consente di impostare la frequenza con cui Astra Control deve acquisire un'istantanea e replicarla nella destinazione.
   - **Offset**: Consente di impostare il numero di minuti dall'inizio dell'ora in cui si desidera che Astra Control prenda un'istantanea. È possibile utilizzare un offset in modo che non coincidano con altre operazioni pianificate. Ad esempio, se si desidera acquisire l'istantanea ogni 5 minuti a partire dalle 10:02, immettere "02" come minuti di offset. Il risultato sarebbe 10:02, 10:07, 10:12, ecc.
5. Selezionare **Avanti**, rivedere il riepilogo e selezionare **Salva**.

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

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

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

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

Risultato

In questo modo si crea la relazione di replica.

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

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

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

Ad esempio: Normale | stabilito

Scopri di seguito gli stati e lo stato della replica.

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

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

Fasi

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

Risultato

La procedura di failover consente di eseguire le seguenti operazioni:

- Sul cluster di destinazione, l'applicazione viene avviata in base all'ultima snapshot replicata.
- Il cluster e l'applicazione di origine (se operativi) non vengono arrestati e continueranno a funzionare.
- Lo stato di replica cambia in "failover", quindi in "failover" una volta completato.
- La policy di protezione dell'applicazione di origine viene copiata nell'applicazione di destinazione in base alle pianificazioni presenti nell'applicazione di origine al momento del failover.

- Astra Control mostra l'applicazione sia sul cluster di origine che di destinazione, nonché il relativo stato di salute.

Risincronizzare una replica con esito negativo

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

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

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

Fasi

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

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

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

Risultato

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

Replica inversa delle applicazioni

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

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

Fasi

1. Dalla barra di navigazione a sinistra di Astra Control, selezionare **applicazioni**.

2. Nella pagina Application (applicazione), selezionare la scheda **Data Protection** > **Replication** (protezione dati).
3. Nella scheda Data Protection > Replication (protezione dati > Replica), dal menu Actions (azioni), selezionare **Reverse Replication** (replica inversa).
4. Nella pagina Replica inversa, esaminare le informazioni e selezionare **Replica inversa** per continuare.

Risultato

Le seguenti azioni si verificano in seguito alla replica inversa:

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

Eseguire il failback delle applicazioni nel cluster di origine originale

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

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

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

Fasi

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

Risultato

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

Eliminare una relazione di replica dell'applicazione

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

Fasi

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

Risultato

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

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

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

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

Stati di integrità delle relazioni di replica

I seguenti stati indicano lo stato della relazione di replica:

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

stati del ciclo di vita della replica

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

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

Clonare e migrare le applicazioni

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

La clonazione può essere di aiuto nel caso in cui sia necessario spostare applicazioni e storage da un cluster Kubernetes a un altro. Ad esempio, è possibile spostare i carichi di lavoro attraverso una pipeline ci/CD e attraverso gli spazi dei nomi Kubernetes. È possibile utilizzare l'interfaccia utente Astra o. "L'API Astra Control" per clonare e migrare le applicazioni.

Di cosa hai bisogno

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

A proposito di questa attività

- Se si implementa un'applicazione con un StorageClass esplicitamente impostato e si deve clonare l'applicazione, il cluster di destinazione deve avere la StorageClass specificata in origine. Il cloning di un'applicazione con un StorageClass esplicitamente impostato su un cluster che non ha lo stesso StorageClass avrà esito negativo.
- Se si clonano istanze distribuite dall'operatore di Jenkins ci, è necessario ripristinare manualmente i dati persistenti. Si tratta di un limite del modello di implementazione dell'applicazione.

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

Considerazioni su OpenShift

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

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

Fasi

1. Selezionare **applicazioni**.
2. Effettuare una delle seguenti operazioni:
   - Selezionare il menu Options (Opzioni) nella colonna **Actions** (azioni) per l'applicazione desiderata.
   - Selezionare il nome dell'applicazione desiderata e l'elenco a discesa Status (Stato) in alto a destra nella pagina.
3. Selezionare **Clone**.
4. **Clone Details**: Specificare i dettagli per il clone:
   - Immettere un nome.
   - Immettere uno spazio dei nomi per il clone.
   - Scegliere un cluster di destinazione per il clone.
   - Scegliere se si desidera creare il clone da uno snapshot o da un backup esistente. Se non si seleziona questa opzione, Astra Control Center crea il clone dallo stato corrente dell'applicazione.
5. **Origine**: Se si sceglie di clonare da uno snapshot o da un backup esistente, scegliere lo snapshot o il backup che si desidera utilizzare.
6. Selezionare **Revisione**.

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

Risultato

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

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

Gestire gli hook di esecuzione delle applicazioni

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

Tipi di hook di esecuzione

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

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

Note importanti sugli hook di esecuzione personalizzati

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

- Un gancio di esecuzione deve utilizzare uno script per eseguire le azioni. Molti hook di esecuzione possono fare riferimento allo stesso script.
- Astra Control richiede che gli script utilizzati dagli hook di esecuzione siano scritti nel formato degli script shell eseguibili.
- La dimensione dello script è limitata a 96 KB.
- Astra Control utilizza le impostazioni degli uncino di esecuzione e qualsiasi criterio corrispondente per determinare quali hook sono applicabili a un'operazione di snapshot, backup o ripristino.
- Tutti i guasti degli uncini di esecuzione sono guasti di tipo soft; altri hook e l'operazione di protezione dei dati vengono ancora tentati anche in caso di interruzione di un hook. Tuttavia, quando un gancio non

funziona, viene registrato un evento di avviso nel registro eventi della pagina **attività**.

- Per creare, modificare o eliminare gli hook di esecuzione, è necessario essere un utente con autorizzazioni Owner, Admin o Member.
- Se l'esecuzione di un gancio di esecuzione richiede più di 25 minuti, l'hook non riesce, creando una voce del registro eventi con un codice di ritorno "N/A". Qualsiasi snapshot interessata verrà contrassegnata come non riuscita e una voce del registro eventi risultante annoterà il timeout.
- Per le operazioni di protezione dei dati ad hoc, tutti gli eventi hook vengono generati e salvati nel registro eventi della pagina **Activity**. Tuttavia, per le operazioni di protezione dei dati pianificate, nel registro eventi vengono registrati solo gli eventi di errore hook (gli eventi generati dalle operazioni di protezione dei dati pianificate vengono ancora registrati).

> Poiché gli hook di esecuzione spesso riducono o disattivano completamente le funzionalità dell'applicazione con cui vengono eseguiti, è consigliabile ridurre al minimo il tempo necessario per l'esecuzione degli hook di esecuzione personalizzati. Se si avvia un'operazione di backup o snapshot con gli hook di esecuzione associati, ma poi si annulla, gli hook possono ancora essere eseguiti se l'operazione di backup o snapshot è già iniziata. Ciò significa che un gancio di esecuzione post-backup non può presumere che il backup sia stato completato.

Ordine di esecuzione

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

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

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

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

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

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

Determinare se verrà eseguito un gancio

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

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

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

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

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

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

Scenario	Operazione	Snapshot esistente	Backup esistente	Namespace	Cluster	Esecuzione di Snapshot Hooks	Esecuzione dei ganci di backup	Esecuzione degli hook di ripristino
8	Ripristinare	N	Y	Esistente	Stesso	N	N	Y
9	Snapshot	N/A.	N/A.	N/A.	N/A.	Y	N/A.	N/A.
10	Backup	N	N/A.	N/A.	N/A.	Y	Y	N/A.
11	Backup	Y	N/A.	N/A.	N/A.	N	Y	N/A.

Visualizzare gli hook di esecuzione esistenti

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

Fasi

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

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

Visualizzare gli script esistenti

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

Fasi

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

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

Aggiungere uno script

È possibile aggiungere uno o più script a cui possono fare riferimento gli hook di esecuzione. Molti hook di esecuzione possono fare riferimento allo stesso script; ciò consente di aggiornare molti hook di esecuzione modificando solo uno script.

Fasi

1. Vai a **account**.
2. Selezionare la scheda **script**.
3. Selezionare **Aggiungi**.
4. Effettuare una delle seguenti operazioni:

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

5. Selezionare **Salva script**.

Risultato

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

Eliminare uno script

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

Fasi

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

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

Creare un gancio di esecuzione personalizzato

È possibile creare un gancio di esecuzione personalizzato per un'applicazione. Vedere "Esempi di gancio di esecuzione" per esempi di gancio. Per creare gli hook di esecuzione, è necessario disporre delle autorizzazioni Owner (Proprietario), Admin (Amministratore) o Member (membro).

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

Fasi

1. Selezionare **applicazioni**, quindi selezionare il nome di un'applicazione gestita.
2. Selezionare la scheda **Execution Hooks**.
3. Selezionare **Aggiungi**.

4. Nell'area **Dettagli gancio**, determinare quando eseguire il gancio selezionando un tipo di operazione dal menu a discesa **operazione**.
5. Immettere un nome univoco per l'hook.
6. (Facoltativo) inserire gli argomenti da passare al gancio durante l'esecuzione, premendo il tasto Invio dopo ogni argomento inserito per registrarne ciascuno.
7. Nell'area **Container Images** (immagini container), se il gancio deve essere eseguito su tutte le immagini container contenute nell'applicazione, attivare la casella di controllo **Apply to all container images** (Applica a tutte le immagini container). Se invece il gancio dovrebbe agire solo su una o più immagini container specificate, inserire i nomi delle immagini container nel campo **nomi delle immagini container da abbinare**.
8. Nell'area **script**, eseguire una delle seguenti operazioni:
   - Aggiungere un nuovo script.
     i. Selezionare **Aggiungi**.
     ii. Effettuare una delle seguenti operazioni:
       - Caricare uno script personalizzato.
         I. Selezionare l'opzione **carica file**.
         II. Selezionare un file e caricarlo.
         III. Assegnare allo script un nome univoco.
         IV. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
         V. Selezionare **Salva script**.
       - Incollare uno script personalizzato dagli Appunti.
         I. Selezionare l'opzione **Incolla o tipo**.
         II. Selezionare il campo di testo e incollare il testo dello script nel campo.
         III. Assegnare allo script un nome univoco.
         IV. (Facoltativo) inserire eventuali note che altri amministratori dovrebbero conoscere sullo script.
   - Selezionare uno script esistente dall'elenco.

     In questo modo, il gancio di esecuzione deve utilizzare questo script.
9. Selezionare **Aggiungi gancio**.

Controllare lo stato di un gancio di esecuzione

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

Fasi

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

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

Visualizzare l'utilizzo dello script

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

Fasi

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

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

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

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

Disattiva un gancio di esecuzione

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

Fasi

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

Eliminare un gancio di esecuzione

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

Fasi

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

Esempi di gancio di esecuzione

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

Semplice esempio di successo

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

```
#!/bin/sh

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


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


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

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

```
#
# main
#

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

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

Semplice esempio di successo (versione bash)

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

```
#!/bin/bash

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


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


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

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


#
# main
#

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

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

Semplice esempio di successo (versione zsh)

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

```
#!/bin/zsh

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


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

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

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

#
# main
#

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

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

Esempio di successo con argomenti

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

```
#!/bin/sh

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

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

```
msg() {
    echo "$*"
}


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

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


#
# main
#

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


# collect args
arg1=$1
arg2=$2

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

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

Esempio di gancio pre-snapshot/post-snapshot

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

```
#!/bin/sh

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

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


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


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

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

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


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

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


#
# main
#

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

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

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

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

```
    fi
fi

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

exit ${rc}
```

Esempio di guasto

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

```
#!/bin/sh

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


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


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

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


#
# main
#

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

argexitcode=$1

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

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

Esempio di errore dettagliato

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

```
#!/bin/sh

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


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

```
}


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

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


#
# main
#

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


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

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

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

Errore con un esempio di codice di uscita

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

```
#!/bin/sh

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


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


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

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


#
# main
#
```

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

argexitcode=$1

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

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

Esempio di successo dopo il guasto

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

```
#!/bin/sh

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

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


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

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


#
# main
#

# log something to stdout
info "running failure_success sample.sh"


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

Informazioni sul copyright

Informazioni sul marchio commerciale