Proteggi i carichi di lavoro di Kubernetes (anteprima)

NetApp Backup and Recovery

NetApp
October 21, 2025

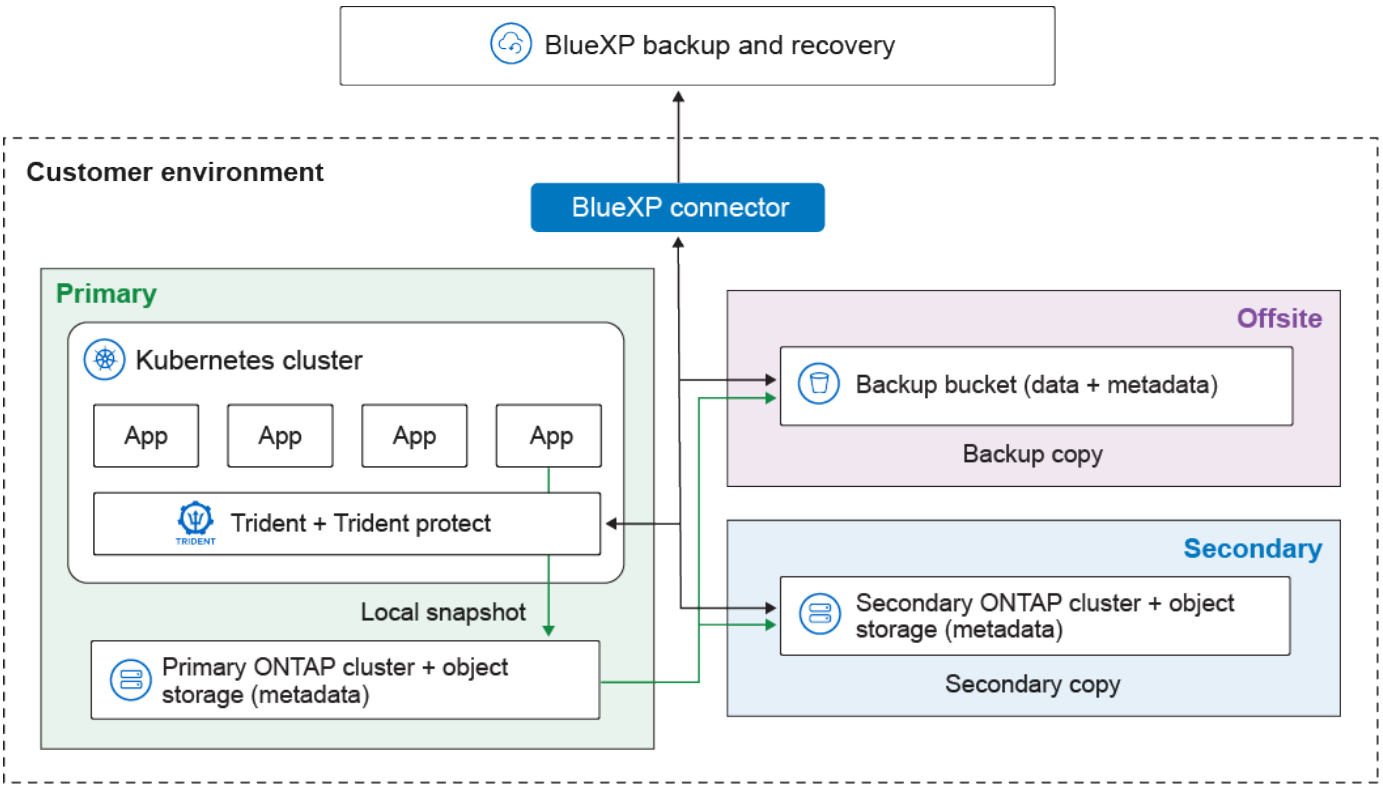
Sommario

Proteggi i carichi di lavoro di Kubernetes (anteprima)

Panoramica sulla gestione dei carichi di lavoro Kubernetes

La gestione dei carichi di lavoro Kubernetes in NetApp Backup and Recovery consente di individuare, gestire e proteggere i cluster e le applicazioni Kubernetes, il tutto in un unico posto. Puoi gestire risorse e applicazioni ospitate sui tuoi cluster Kubernetes. Puoi anche creare e associare policy di protezione ai tuoi carichi di lavoro Kubernetes, il tutto utilizzando un'unica interfaccia.

Il diagramma seguente mostra i componenti e l'architettura di base del backup e del ripristino per i carichi di lavoro Kubernetes e come diverse copie dei dati possono essere archiviate in posizioni diverse:



NetApp Backup and Recovery offre i seguenti vantaggi per la gestione dei carichi di lavoro Kubernetes:

- Un unico piano di controllo per proteggere le applicazioni in esecuzione su più cluster Kubernetes. Queste applicazioni possono includere container o macchine virtuali in esecuzione sui cluster Kubernetes.
- Integrazione nativa con NetApp SnapMirror, che consente funzionalità di offload dello storage per tutti i flussi di lavoro di backup e ripristino.
- Backup incrementali permanenti per le applicazioni Kubernetes, che si traducono in Recovery Point Objectives (RPO) e Recovery Time Objectives (RTO) inferiori.

La presente documentazione viene fornita come anteprima tecnologica. Durante l'anteprima, la funzionalità Kubernetes non è consigliata per i carichi di lavoro di produzione. Con questa offerta di anteprima, NetApp si riserva il diritto di modificare i dettagli, i contenuti e la tempistica dell'offerta prima della disponibilità generale.

È possibile svolgere le seguenti attività relative alla gestione dei carichi di lavoro Kubernetes:

- "Scopri i carichi di lavoro di Kubernetes".
- "Gestire i cluster Kubernetes".
- "Aggiungi e proteggi le applicazioni Kubernetes".
- "Gestire le applicazioni Kubernetes".
- "Ripristina le applicazioni Kubernetes".

Scopri i carichi di lavoro Kubernetes in NetApp Backup and Recovery

NetApp Backup and Recovery deve rilevare i carichi di lavoro Kubernetes prima di proteggerli.

*Ruolo richiesto NetApp Console * Super amministratore di backup e ripristino. Scopri di più"Ruoli e privilegi di backup e ripristino" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Scopri i carichi di lavoro di Kubernetes

Nell'inventario di backup e ripristino, scopri i carichi di lavoro Kubernetes nel tuo ambiente. L'aggiunta di un carico di lavoro aggiunge un cluster Kubernetes a NetApp Backup and Recovery. È quindi possibile aggiungere applicazioni e proteggere le risorse del cluster.

Passi

1. Eseguire una delle seguenti operazioni:
   - Se stai rilevando carichi di lavoro Kubernetes per la prima volta, in NetApp Backup and Recovery, seleziona **Discover and Manage** nel tipo di carico di lavoro Kubernetes.
   - Se hai già individuato i carichi di lavoro Kubernetes, in NetApp Backup and Recovery seleziona **Inventario** > **Carichi di lavoro** e quindi seleziona **Individuazione risorse**.
2. Selezionare il tipo di carico di lavoro **Kubernetes**.
3. Inserisci un nome per il cluster e scegli un connettore da utilizzare con il cluster.
4. Seguire le istruzioni della riga di comando che appaiono:
   - Crea uno spazio dei nomi Trident Protect
   - Crea un segreto Kubernetes
   - Aggiungi un repository Helm
   - Installare Trident Protect e il connettore Trident Protect

   Questi passaggi garantiscono che NetApp Backup and Recovery possa interagire con il cluster.
5. Dopo aver completato i passaggi, seleziona **Scopri**.

Il cluster viene aggiunto all'inventario.

6. Selezionare **Visualizza** nel carico di lavoro Kubernetes associato per visualizzare l'elenco di applicazioni, cluster e namespace per quel carico di lavoro.

Continua alla dashboard NetApp Backup and Recovery

Per visualizzare la dashboard NetApp Backup and Recovery , seguire questi passaggi.

1. Dal menu NetApp Console , selezionare **Protezione** > **Backup e ripristino**.
2. Selezionare un riquadro del carico di lavoro (ad esempio, Microsoft SQL Server).
3. Dal menu Backup e ripristino, seleziona **Dashboard**.
4. Esaminare lo stato di salute della protezione dei dati. Il numero di carichi di lavoro a rischio o protetti aumenta in base ai carichi di lavoro appena scoperti, protetti e sottoposti a backup.

   "Scopri cosa ti mostra la Dashboard".

Aggiungi e proteggi le applicazioni Kubernetes

NetApp Backup and Recovery ti consente di individuare facilmente i tuoi cluster Kubernetes, senza dover generare e caricare file kubeconfig. È possibile connettere i cluster Kubernetes e installare il software necessario utilizzando semplici comandi copiati dall'interfaccia utente NetApp Console .

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Aggiungi e proteggi una nuova applicazione Kubernetes

Il primo passo per proteggere le applicazioni Kubernetes è creare un'applicazione all'interno NetApp Backup and Recovery. Quando si crea un'applicazione, si fa in modo che la Console sia a conoscenza dell'applicazione in esecuzione sul cluster Kubernetes.

Prima di iniziare

Prima di poter aggiungere e proteggere un'applicazione Kubernetes, è necessario"scopri i carichi di lavoro di Kubernetes" .

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Seleziona **Crea applicazione**.
5. Inserisci un nome per l'applicazione.
6. Facoltativamente, seleziona uno dei seguenti campi per cercare le risorse che desideri proteggere:
   - Cluster associato
   - Spazi dei nomi associati

- Tipi di risorse
- Selettori di etichette

7. Facoltativamente, seleziona **Risorse con ambito cluster** per scegliere tutte le risorse con ambito a livello di cluster. Se le includi, verranno aggiunte all'applicazione al momento della creazione.
8. Facoltativamente, seleziona **Cerca** per trovare le risorse in base ai tuoi criteri di ricerca.

> La console non memorizza i parametri o i risultati della ricerca; i parametri vengono utilizzati per cercare nel cluster Kubernetes selezionato le risorse che possono essere incluse nell'applicazione.

9. La Console visualizza un elenco di risorse che corrispondono ai criteri di ricerca.
10. Se l'elenco contiene le risorse che si desidera proteggere, selezionare **Avanti**.
11. Facoltativamente, nell'area **Criterio**, seleziona un criterio di protezione esistente per proteggere l'applicazione o creane uno nuovo. Se non selezioni un criterio, l'applicazione verrà creata senza criterio di protezione. Puoi"aggiungere una politica di protezione" Dopo.
12. Nell'area **Prescript e postscript**, abilitare e configurare tutti gli hook di esecuzione prescript o postscript che si desidera eseguire prima o dopo le operazioni di backup. Per abilitare prescript o postscript, devi averne già creato almeno uno"modello di gancio di esecuzione" .
13. Seleziona **Crea**.

Risultato

L'applicazione viene creata e appare nell'elenco delle applicazioni nella scheda **Applicazioni** dell'inventario Kubernetes. La NetApp Console consente la protezione dell'applicazione in base alle impostazioni e puoi monitorare l'avanzamento nell'area **Monitoraggio** del backup e del ripristino.

Proteggere un'applicazione Kubernetes esistente

Abilita un criterio di protezione su un'applicazione Kubernetes che hai già aggiunto.

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione che desideri proteggere e seleziona il menu Azioni associato.
5. Seleziona **Proteggi**.
6. Nell'area **Criterio**, seleziona un criterio di protezione esistente per proteggere l'applicazione oppure creane uno nuovo. Fare riferimento a"Crea una politica" per maggiori informazioni sulla creazione di policy di protezione.
7. Nell'area **Prescript e postscript**, abilitare e configurare tutti gli hook di esecuzione prescript o postscript che si desidera eseguire prima o dopo le operazioni di backup. È possibile configurare il tipo di hook di esecuzione, il modello utilizzato, gli argomenti e i selettori di etichetta.
8. Selezionare **Fatto**.

Risultato

La Console abilita la protezione dell'applicazione in base alle impostazioni e puoi monitorare l'avanzamento nell'area **Monitoraggio** del backup e del ripristino. Non appena si attiva la protezione per un'applicazione, la

Console crea un backup completo dell'applicazione. Eventuali backup incrementali futuri vengono creati in base alla pianificazione definita nella policy di protezione associata all'applicazione.

Esegui subito il backup di un'applicazione Kubernetes

Crea manualmente un backup di un'applicazione Kubernetes per stabilire una base di riferimento per backup e snapshot futuri o per garantire la protezione dei dati più recenti.

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione di cui vuoi eseguire il backup e seleziona il menu Azioni associato.
5. Seleziona **Esegui backup ora**.
6. Assicurarsi che sia selezionato il nome corretto dell'applicazione.
7. Selezionare **Backup**.

Risultato

La Console crea un backup dell'applicazione e visualizza l'avanzamento nell'area **Monitoraggio** di Backup e Ripristino. Il backup viene creato in base ai criteri di protezione associati all'applicazione.

Ripristina le applicazioni Kubernetes

NetApp Backup and Recovery consente di ripristinare le applicazioni protette tramite una policy di protezione. Per ripristinare un'applicazione, è necessario che quest'ultima disponga di almeno un punto di ripristino. Un punto di ripristino può essere costituito dallo snapshot locale o dal backup nell'archivio oggetti (o da entrambi). È possibile ripristinare un'applicazione utilizzando l'archivio locale, secondario o dell'archivio oggetti.

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione che desideri ripristinare e seleziona il menu Azioni associato.
5. Seleziona **Visualizza e ripristina**.

   Viene visualizzato l'elenco dei punti di ripristino.

6. Aprire il menu Azioni per il punto di ripristino che si desidera utilizzare e selezionare **Ripristina**.

Impostazioni generali

1. Selezionare l'origine da cui effettuare il ripristino (archivio locale o archivio oggetti).
2. Selezionare il cluster di destinazione dall'elenco **Cluster**.
3. Selezionare lo spazio dei nomi di destinazione del ripristino.

   È possibile ripristinare lo spazio dei nomi originale o uno nuovo.

4. Selezionare **Avanti**.

Selezione delle risorse

1. Scegli se desideri ripristinare tutte le risorse associate all'applicazione oppure utilizzare un filtro per selezionare risorse specifiche da ripristinare:

Ripristina tutte le risorse

1. Seleziona **Ripristina tutte le risorse**.
2. Selezionare **Avanti**.

Ripristina risorse specifiche

1. Seleziona **Risorse selettive**.
2. Scegli il comportamento del filtro delle risorse. Se scegli **Includi**, le risorse selezionate verranno ripristinate. Se si sceglie **Escludi**, le risorse selezionate non verranno ripristinate.
3. Selezionare **Aggiungi regole** per aggiungere regole che definiscono i filtri per la selezione delle risorse. Per filtrare le risorse è necessaria almeno una regola.

   Ogni regola può filtrare in base a criteri quali lo spazio dei nomi della risorsa, le etichette, il gruppo, la versione e il tipo.

4. Selezionare **Salva** per salvare ciascuna regola.
5. Dopo aver aggiunto tutte le regole necessarie, seleziona **Cerca** per visualizzare le risorse disponibili nell'archivio di backup che corrispondono ai criteri di filtro.

   Le risorse mostrate sono le risorse attualmente presenti nel cluster.

6. Una volta soddisfatti dei risultati, selezionare **Avanti**.

Impostazioni di destinazione

1. Scegliere se ripristinare la classe di archiviazione predefinita o una classe di archiviazione diversa.
2. Facoltativamente, se si sceglie di ripristinare in una classe di archiviazione diversa, selezionare una classe di archiviazione di destinazione che corrisponda a ciascuna classe di archiviazione di origine.
3. Selezionare **Ripristina**.

Gestire i cluster Kubernetes

NetApp Backup and Recovery ti consente di scoprire e gestire i tuoi cluster Kubernetes in modo da poter proteggere le risorse ospitate dai cluster.

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Per scoprire i cluster Kubernetes, fare riferimento a"Scopri i carichi di lavoro di Kubernetes" .

Modifica le informazioni del cluster Kubernetes

È possibile modificare un cluster se è necessario cambiarne il nome.

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario** > **Cluster**.
2. Nell'elenco dei cluster, seleziona il cluster che desideri modificare e seleziona il menu Azioni associato.
3. Seleziona **Modifica cluster**.
4. Apportare le modifiche necessarie al nome del cluster. Il nome del cluster deve corrispondere al nome utilizzato con il comando Helm durante il processo di individuazione.
5. Selezionare **Fatto**.

Rimuovere un cluster Kubernetes

Per interrompere la protezione di un cluster Kubernetes, disabilitare la protezione ed eliminare le applicazioni associate, quindi rimuovere il cluster da NetApp Backup and Recovery. NetApp Backup and Recovery non elimina il cluster o le sue risorse; rimuove solo il cluster dall'inventario della NetApp Console .

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario** > **Cluster**.
2. Nell'elenco dei cluster, seleziona il cluster che desideri modificare e seleziona il menu Azioni associato.
3. Selezionare **Rimuovi cluster**.
4. Rivedi le informazioni nella finestra di dialogo di conferma e seleziona **Rimuovi**.

Gestire le applicazioni Kubernetes

NetApp Backup and Recovery consente di rimuovere la protezione ed eliminare le applicazioni Kubernetes e le risorse associate.

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Rimuovere la protezione di un'applicazione Kubernetes

È possibile rimuovere la protezione da un'applicazione se non si desidera più proteggerla. Quando si rimuove la protezione di un'applicazione, NetApp Backup and Recovery interrompe la protezione dell'applicazione ma conserva tutti i backup e gli snapshot associati.

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.

2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione di cui desideri rimuovere la protezione e seleziona il menu Azioni associato.
5. Selezionare **Rimuovi protezione**.
6. Leggi l'avviso e, quando sei pronto, seleziona **Rimuovi protezione**.

Eliminare un'applicazione Kubernetes

Elimina un'applicazione di cui non hai più bisogno. NetApp Backup and Recovery interrompe la protezione e rimuove tutti i backup e gli snapshot delle applicazioni eliminate.

Passi

1. In NetApp Backup and Recovery, seleziona **Inventario**.
2. Scegli un'istanza di Kubernetes e seleziona **Visualizza** per visualizzare le risorse associate a tale istanza.
3. Selezionare la scheda **Applicazioni**.
4. Nell'elenco delle applicazioni, seleziona l'applicazione che desideri eliminare e seleziona il menu Azioni associato.
5. Seleziona **Elimina**.
6. Abilita **Elimina snapshot e backup** per rimuovere tutti gli snapshot e i backup dell'applicazione.

   Non sarà più possibile ripristinare l'applicazione utilizzando questi snapshot e backup.

7. Confermare l'azione e selezionare **Elimina**.

Gestisci i modelli di hook di esecuzione di NetApp Backup and Recovery per i carichi di lavoro Kubernetes

Un hook di esecuzione è un'azione personalizzata che viene eseguita con un'operazione di protezione dei dati in un'applicazione Kubernetes gestita. Ad esempio, è possibile creare snapshot coerenti con l'applicazione utilizzando un hook di esecuzione per mettere in pausa le transazioni del database prima di uno snapshot e riprenderle dopo. Quando si crea un modello di hook di esecuzione, specificare il tipo di hook, lo script da eseguire e i filtri per i contenitori di destinazione. Utilizza il modello per collegare gli hook di esecuzione alle tue applicazioni.

NetApp Backup and Recovery blocca e sblocca i file system per applicazioni come KubeVirt durante la protezione dei dati. È possibile disattivare questo comportamento a livello globale o per applicazioni specifiche utilizzando la documentazione di Trident Protect:

- Per disattivare questo comportamento per tutte le applicazioni, fare riferimento a "Protezione dei dati con le VM KubeVirt" .
- Per disattivare questo comportamento per un'applicazione specifica, fare riferimento a "Definire un'applicazione" .

Ruolo richiesto NetApp Console

Amministratore dell'organizzazione o amministratore SnapCenter . "Scopri di più sui ruoli di accesso a NetApp Backup and Recovery" . "Scopri di più sui ruoli di accesso NetApp Console per tutti i servizi" .

Tipi di ganci di esecuzione

NetApp Backup and Recovery supporta i seguenti tipi di hook di esecuzione, in base al momento in cui possono essere eseguiti:

- Pre-istantanea
- Post-istantanea
- Pre-backup
- Post-backup
- Post-ripristino

Ordine di esecuzione

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

1. Tutti gli hook di esecuzione pre-operazione personalizzati applicabili vengono eseguiti sui contenitori appropriati. È possibile creare più hook pre-operativi personalizzati, ma il loro ordine di esecuzione non è garantito né configurabile.
2. Se applicabile, si verificano blocchi del file system.
3. L'operazione di protezione dei dati è eseguita.
4. I file system congelati vengono sbloccati, se applicabile.
5. NetApp Backup and Recovery esegue tutti gli hook di esecuzione pre-operazione personalizzati applicabili sui contenitori appropriati. È possibile creare più hook post-operazione personalizzati, ma il loro ordine di esecuzione non è garantito né configurabile.

Se si creano più hook dello stesso tipo, il loro ordine di esecuzione non è garantito. I ganci di tipo diverso vengono sempre eseguiti nell'ordine specificato. Ad esempio, ecco l'ordine di esecuzione di una configurazione che presenta tutti i diversi tipi di hook:

1. Eseguiti i pre-snapshot hook
2. Eseguiti i ganci post-snapshot
3. Hook pre-backup eseguiti
4. Hook post-backup eseguiti

Testare gli script di hook di esecuzione prima di abilitarli in produzione. Utilizzare 'kubectl exec' per testare gli script, quindi verificare gli snapshot e i backup clonando l'app in uno spazio dei nomi temporaneo e ripristinandola.

Se un hook di esecuzione pre-snapshot aggiunge, modifica o rimuove risorse Kubernetes, tali modifiche vengono incluse nello snapshot o nel backup e in qualsiasi successiva operazione di ripristino.

Note importanti sui ganci di esecuzione personalizzati

Quando pianifichi gli hook di esecuzione per le tue app, tieni presente quanto segue.

- Un hook di esecuzione deve utilizzare uno script per eseguire azioni. Molti hook di esecuzione possono fare riferimento allo stesso script.
- Gli hook di esecuzione devono essere scritti nel formato degli script shell eseguibili.
- La dimensione dello script è limitata a 96 KB.
- Le impostazioni dell'hook di esecuzione e tutti i criteri corrispondenti vengono utilizzati per determinare quali hook sono applicabili a un'operazione di snapshot, backup o ripristino.

> Gli hook di esecuzione possono ridurre o disabilitare la funzionalità dell'applicazione. Fai in modo che i tuoi hook personalizzati vengano eseguiti il più velocemente possibile. Se si avvia un'operazione di backup o snapshot con hook di esecuzione associati ma poi la si annulla, gli hook possono comunque essere eseguiti se l'operazione di backup o snapshot è già iniziata. Ciò significa che la logica utilizzata in un hook di esecuzione post-backup non può presumere che il backup sia stato completato.

Filtri di hook di esecuzione

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

Ogni filtro aggiunto a un hook di esecuzione utilizza un'espressione regolare per abbinare i contenitori nel cluster. Quando un hook corrisponde a un contenitore, eseguirà lo script associato su quel contenitore. Le espressioni regolari per i filtri utilizzano la sintassi Regular Expression 2 (RE2), che non supporta la creazione di un filtro che escluda i contenitori dall'elenco delle corrispondenze. Per informazioni sulla sintassi supportata da NetApp Backup and Recovery per le espressioni regolari nei filtri di hook di esecuzione, vedere "Supporto della sintassi Regular Expression 2 (RE2)" .

> Se si aggiunge un filtro namespace a un hook di esecuzione eseguito dopo un'operazione di ripristino o clonazione e l'origine e la destinazione del ripristino o della clonazione si trovano in namespace diversi, il filtro namespace viene applicato solo al namespace di destinazione.

Esempi di hook di esecuzione

Visita il "Progetto GitHub NetApp Verda" per scaricare veri e propri hook di esecuzione per app popolari come Apache Cassandra ed Elasticsearch. Puoi anche vedere esempi e trarre spunti per strutturare i tuoi hook di esecuzione personalizzati.

Creare un modello di hook di esecuzione

È possibile creare un modello di hook di esecuzione personalizzato da utilizzare per eseguire azioni prima o dopo un'operazione di protezione dei dati su un'applicazione.

Passi

1. Nella Console, vai a **Protezione** > **Backup e ripristino**.
2. Selezionare la scheda **Impostazioni**.
3. Espandi la sezione **Modello di hook di esecuzione**.
4. Selezionare **Crea modello di hook di esecuzione**.
5. Immettere un nome per l'hook di esecuzione.
6. Facoltativamente, scegli un tipo di hook. Ad esempio, un hook post-restore viene eseguito al termine dell'operazione di ripristino.
7. Nella casella di testo **Script**, immettere lo script shell eseguibile che si desidera eseguire come parte del modello di hook di esecuzione. Facoltativamente, puoi selezionare **Carica script** per caricare un file di script.
8. Seleziona **Crea**.

   Dopo aver creato il modello, questo viene visualizzato nell'elenco dei modelli nella sezione **Modello di hook di esecuzione**.