



Backup e ripristino dei dati Kubernetes

BlueXP backup and recovery

NetApp
April 30, 2024

Sommario

- Backup e ripristino dei dati Kubernetes 1
 - Proteggi i dati del cluster Kubernetes utilizzando il backup e ripristino BlueXP 1
 - Backup dei dati persistenti del volume di Kubernetes su Amazon S3 5
 - Backup di Kubernetes dati di volumi persistenti nello storage Azure Blob 11
 - Backup di Kubernetes dati di volume persistenti su storage Google Cloud 16
 - Gestione dei backup per i sistemi Kubernetes 21
 - Ripristino dei dati Kubernetes dai file di backup 32

Backup e ripristino dei dati Kubernetes

Proteggi i dati del cluster Kubernetes utilizzando il backup e ripristino BlueXP

Il backup e ripristino BlueXP offre funzionalità di backup e ripristino per la protezione e l'archiviazione a lungo termine dei dati del cluster Kubernetes. I backup vengono generati e memorizzati automaticamente in un archivio di oggetti nel tuo account di cloud pubblico o privato.

Se necessario, è possibile ripristinare un intero *volume* da un backup nello stesso ambiente di lavoro o in un ambiente di lavoro diverso.

Caratteristiche

Funzionalità di backup:

- Eseguire il backup di copie indipendenti dei volumi persistenti in uno storage a oggetti a basso costo.
- Applicare una singola policy di backup a tutti i volumi di un cluster oppure assegnare policy di backup diverse a volumi che hanno obiettivi di punto di ripristino univoci.
- I dati di backup sono protetti con crittografia AES-256 bit a riposo e connessioni HTTPS TLS 1.2 in volo.
- Supporto di un massimo di 4,000 backup di un singolo volume.

Funzionalità di ripristino:

- Ripristinare i dati da un momento specifico.
- Ripristinare un volume nel sistema di origine o in un sistema diverso.
- Ripristina i dati a livello di blocco, posizionando i dati direttamente nella posizione specificata, mantenendo gli ACL originali.

Ambienti di lavoro Kubernetes supportati e provider di storage a oggetti

Il backup e ripristino BlueXP consente di eseguire il backup dei volumi Kubernetes dai seguenti ambienti di lavoro allo storage a oggetti nei seguenti provider di cloud pubblici e privati:

Ambiente di lavoro di origine	Destinazione del file di backup <code>ifdef::aws[]</code>
Cluster Kubernetes in AWS	Amazon S3 <code>endif::aws[] ifdef::Azure[]</code>
Kubernetes in Azure	Azure Blob <code>endif::Azure[] ifdef::gcp[]</code>
Kubernetes in Google	Google Cloud Storage <code>endif::gcp[]</code>

È possibile ripristinare un volume da un file di backup di Kubernetes nei seguenti ambienti di lavoro:

Percorso del file di backup	Ambiente di lavoro di destinazione <code>ifdef::aws[]</code>
Amazon S3	Cluster Kubernetes in AWS <code>endif::aws[] ifdef::Azure[]</code>
Azure Blob	Cluster Kubernetes in Azure <code>endif::Azure[] ifdef::gcp[]</code>

Percorso del file di backup	Ambiente di lavoro di destinazione <code>ifdef::aws[]</code>
Storage Google Cloud	Cluster Kubernetes in Google <code>endif::gcp[]</code>

Costo

L'utilizzo del backup e ripristino di BlueXP comporta due tipi di costi: Costi delle risorse e costi del servizio.

Costi delle risorse

I costi delle risorse vengono pagati al cloud provider per la capacità dello storage a oggetti nel cloud. Poiché il backup e ripristino BlueXP preserva l'efficienza dello storage del volume di origine, il cloud provider paga i costi dello storage a oggetti per l'efficienza dei dati *dopo* ONTAP (per la minore quantità di dati dopo l'applicazione della deduplica e della compressione).

Costi di servizio

I costi di servizio vengono pagati a NetApp e coprono sia il costo per *creare* backup che per *ripristinare* volumi, da tali backup. Si paga solo per i dati protetti, calcolati in base alla capacità logica utilizzata di origine (*before* efficienze ONTAP) dei volumi di cui viene eseguito il backup nello storage a oggetti. Questa capacità è nota anche come terabyte front-end (FETB).

Esistono due modi per pagare il servizio di backup. La prima opzione è iscriversi al tuo cloud provider, che ti consente di pagare al mese. La seconda opzione consiste nell'acquistare le licenze direttamente da NetApp. Leggere il [Licensing](#) per ulteriori informazioni.

Licensing

Il backup e ripristino BlueXP è disponibile in due opzioni di licenza: Pay as You Go (PAYGO) e Bring Your Own License (BYOL). Se non si dispone di una licenza, è disponibile una versione di prova gratuita di 30 giorni.

Versione di prova gratuita

Quando utilizzi la versione di prova gratuita di 30 giorni, ti viene notificato il numero di giorni di prova gratuiti rimasti. Al termine della prova gratuita, i backup non vengono più creati. Per continuare a utilizzare il servizio, è necessario sottoscrivere il servizio o acquistare una licenza.

I file di backup non vengono cancellati quando il servizio viene disattivato. Il tuo cloud provider continuerà a addebitare i costi di storage a oggetti per la capacità utilizzata dai backup, a meno che non elimini i backup.

Abbonamento pay-as-you-go

Il backup e ripristino BlueXP offre licenze basate sui consumi in un modello pay-as-you-go. Dopo aver effettuato l'iscrizione attraverso il marketplace del tuo cloud provider, pagherai per GB i dati di cui hai eseguito il backup, senza alcun pagamento anticipato da parte di there. Il tuo cloud provider ti addebita la fattura mensile.

È necessario iscriversi anche se si dispone di una versione di prova gratuita o se si porta la propria licenza (BYOL):

- L'iscrizione garantisce che non vi siano interruzioni del servizio al termine della prova gratuita.

Al termine del periodo di prova, ti verrà addebitato ogni ora in base alla quantità di dati di cui hai effettuato il backup.

- Se si esegue il backup di un numero di dati superiore a quello consentito dalla licenza BYOL, il backup dei dati prosegue con l'abbonamento pay-as-you-go.

Ad esempio, se si dispone di una licenza BYOL da 10 TB, tutta la capacità oltre i 10 TB viene addebitata tramite l'abbonamento PAYGO.

Non ti verrà addebitato alcun costo dal tuo abbonamento pay-as-you-go durante la prova gratuita o se non hai superato la licenza BYOL.

["Scopri come impostare un abbonamento pay-as-you-go"](#).

Porta la tua licenza

BYOL è basato sui termini (12, 24 o 36 mesi) e sulla capacità in incrementi di 1 TB. Pagherai NetApp per utilizzare il servizio per un periodo di tempo, ad esempio 1 anno, e per una capacità massima, ad esempio 10 TB.

Riceverai un numero di serie che inserisci nella pagina del portafoglio digitale BlueXP per attivare il servizio. Una volta raggiunto il limite, è necessario rinnovare la licenza. La licenza BYOL di backup si applica a tutti i sistemi di origine associati al ["Account BlueXP"](#).

["Scopri come gestire le tue licenze BYOL"](#).

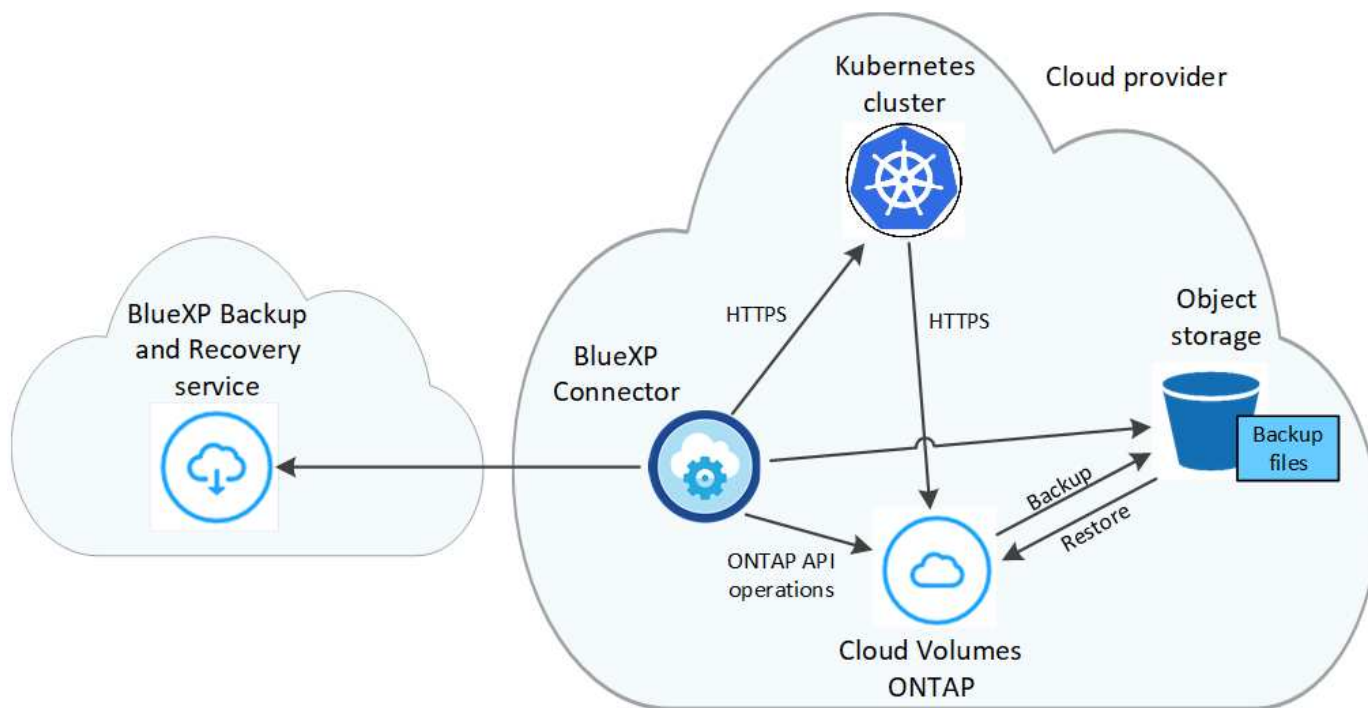
Come funziona il backup e ripristino di BlueXP

Quando si abilita il backup e il ripristino BlueXP su un sistema Kubernetes, il servizio esegue un backup completo dei dati. Dopo il backup iniziale, tutti i backup aggiuntivi sono incrementali, il che significa che viene eseguito il backup solo dei blocchi modificati e dei nuovi blocchi. In questo modo il traffico di rete viene ridotto al minimo.



Qualsiasi azione intrapresa direttamente dall'ambiente del provider cloud per gestire o modificare i file di backup potrebbe corrompere i file e causare una configurazione non supportata.

La seguente immagine mostra la relazione tra ciascun componente:



Classi di storage o livelli di accesso supportati

- In AWS, i backup iniziano nella classe di storage *Standard* e passano alla classe di storage *Standard-infrequent Access* dopo 30 giorni.
- In Azure, i backup sono associati al Tier di accesso *Cool*.
- In GCP, i backup sono associati alla classe di storage *Standard* per impostazione predefinita.

Pianificazione di backup personalizzabile e impostazioni di conservazione per cluster

Quando si attiva il backup e il ripristino BlueXP per un ambiente di lavoro, tutti i volumi selezionati inizialmente vengono sottoposti a backup utilizzando il criterio di backup predefinito definito dall'utente. Se si desidera assegnare criteri di backup diversi a determinati volumi con obiettivi RPO (Recovery Point Objective) diversi, è possibile creare criteri aggiuntivi per tale cluster e assegnarli ad altri volumi.

È possibile scegliere una combinazione di backup orari, giornalieri, settimanali e mensili di tutti i volumi.

Una volta raggiunto il numero massimo di backup per una categoria o intervallo, i backup meno recenti vengono rimossi in modo da avere sempre i backup più aggiornati.

Volumi supportati

Il backup e ripristino BlueXP supporta i volumi persistenti (PVS).

Limitazioni

- Quando si crea o modifica un criterio di backup quando non sono assegnati volumi al criterio, il numero di backup conservati può essere massimo di 1018. Come soluzione alternativa, è possibile ridurre il numero di backup per creare il criterio. Quindi, è possibile modificare il criterio per creare fino a 4000 backup dopo aver assegnato i volumi al criterio.
- I backup dei volumi ad-hoc che utilizzano il pulsante **Backup Now** non sono supportati sui volumi Kubernetes.

Backup dei dati persistenti del volume di Kubernetes su Amazon S3

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dai volumi persistenti sui cluster EKS Kubernetes sullo storage Amazon S3.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1

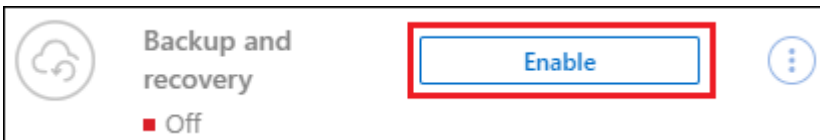
Esaminare i prerequisiti

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP.
 - Trident deve essere installato sul cluster e la versione di Trident deve essere 21.1 o superiore.
 - Tutti i PVC che verranno utilizzati per creare volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".
 - Il cluster deve utilizzare Cloud Volumes ONTAP su AWS per lo storage back-end.
 - Il sistema Cloud Volumes ONTAP deve eseguire ONTAP 9.7P5 o versione successiva.
- Hai un abbonamento valido al cloud provider per lo spazio di storage in cui verranno collocati i backup.
- Si è abbonati a ["Offerta di backup di BlueXP Marketplace"](#), an ["Contratto annuale AWS"](#), oppure è stato acquistato ["e attivato"](#) Una licenza BYOL di backup e ripristino BlueXP di NetApp.
- Il ruolo IAM che fornisce a BlueXP Connector le autorizzazioni include le autorizzazioni S3 dell'ultima versione ["Policy BlueXP"](#).

2

Abilitare il backup e il ripristino BlueXP sul cluster Kubernetes esistente

Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra, quindi seguire la procedura di installazione guidata.



3

Definire il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di ciascun volume. Passare a backup orari, giornalieri, settimanali o mensili oppure selezionare una delle policy definite dal sistema che fornisca più opzioni. È inoltre possibile modificare il numero di copie di backup che si desidera conservare.

Define Policy

Policy - Retention & Schedule

<input type="checkbox"/> Hourly	Number of backups to retain	24
<input checked="" type="checkbox"/> Daily	Number of backups to retain	30
<input type="checkbox"/> Weekly	Number of backups to retain	52
<input type="checkbox"/> Monthly	Number of backups to retain	12

S3 Bucket
Cloud Manager will create the S3 bucket after you complete the wizard

4

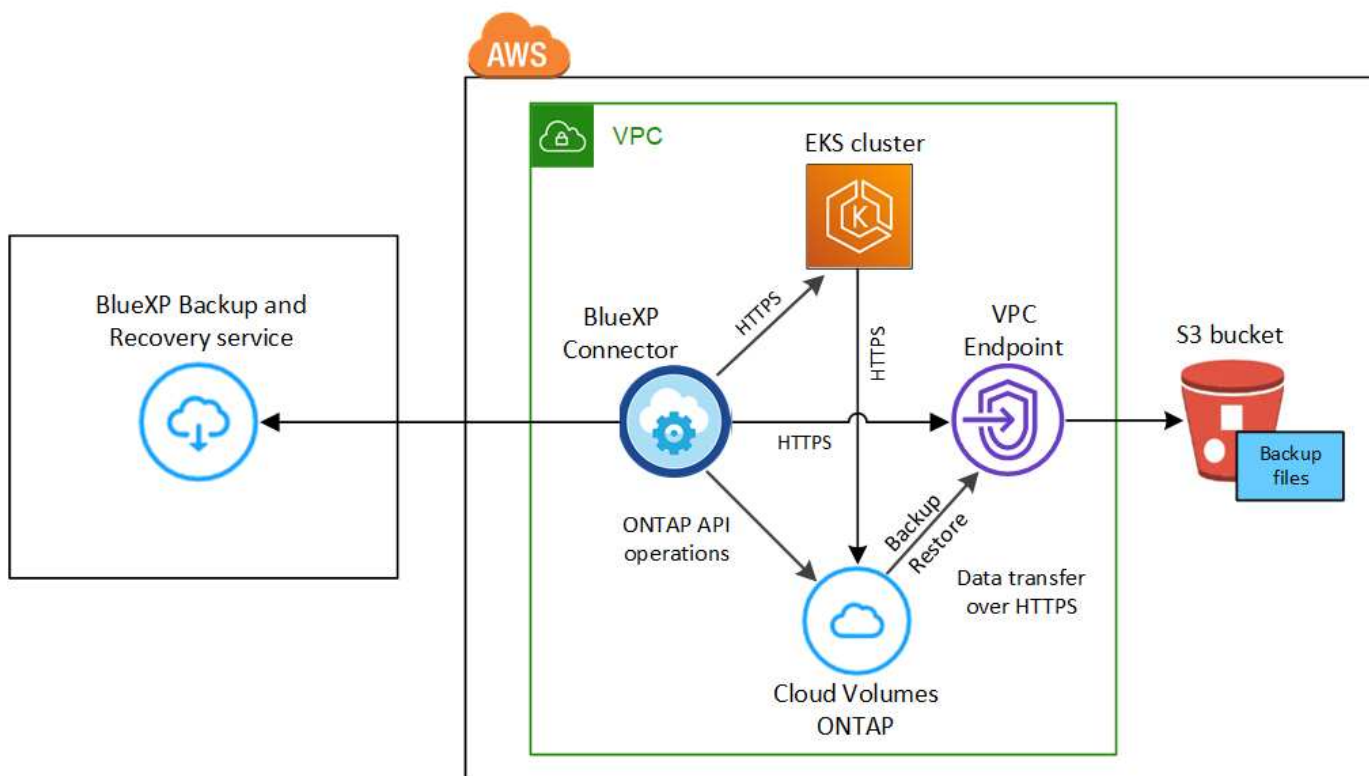
Selezionare i volumi di cui si desidera eseguire il backup

Identificare i volumi di cui si desidera eseguire il backup nella pagina Select Volumes (Seleziona volumi). Un bucket S3 viene creato automaticamente nello stesso account AWS e nella stessa regione del sistema Cloud Volumes ONTAP e i file di backup vengono memorizzati in tale area.

Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi persistenti di Kubernetes su S3.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi:



Tenere presente che l'endpoint VPC è opzionale.

Requisiti del cluster Kubernetes

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP. ["Scopri come scoprire il cluster Kubernetes"](#).
- Trident deve essere installato sul cluster e la versione di Trident deve essere almeno 21.1. Vedere ["Come installare Trident"](#) oppure ["Come aggiornare la versione di Trident"](#).
- Il cluster deve utilizzare Cloud Volumes ONTAP su AWS per lo storage back-end.
- Il sistema Cloud Volumes ONTAP deve trovarsi nella stessa regione AWS del cluster Kubernetes e deve eseguire ONTAP 9.7P5 o versioni successive (si consiglia ONTAP 9.8P11 e versioni successive).

Si noti che i cluster Kubernetes in ubicazioni on-premise non sono supportati. Sono supportati solo i cluster Kubernetes nelle implementazioni cloud che utilizzano sistemi Cloud Volumes ONTAP.

- Tutti gli oggetti persistenti di richiesta di rimborso del volume che verranno utilizzati per creare i volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".

È possibile eseguire questa operazione per singoli PVC aggiungendo `snapshotPolicy` in annotazioni:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

È possibile eseguire questa operazione per tutti i PVC associati a uno storage back-end specifico aggiungendo `snapshotPolicy` sotto i valori predefiniti in `backend.json` file:

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
    deletionPolicy: retain

```

Requisiti di licenza

Per le licenze PAYGO di backup e ripristino BlueXP, è disponibile un abbonamento nel marketplace AWS che consente le implementazioni di backup e ripristino di Cloud Volumes ONTAP e BlueXP. È necessario ["Iscriviti a questo abbonamento BlueXP"](#) Prima di attivare il backup e ripristino BlueXP. La fatturazione per il backup e il ripristino BlueXP viene effettuata tramite questo abbonamento.

Per un contratto annuale che consente di eseguire il backup dei dati Cloud Volumes ONTAP e dei dati ONTAP on-premise, è necessario iscriversi al ["Pagina AWS Marketplace"](#) e poi ["Associare l'abbonamento alle credenziali AWS"](#).

Per un contratto annuale che consente di raggruppare backup e ripristino di Cloud Volumes ONTAP e BlueXP, è necessario impostare il contratto annuale quando si crea un ambiente di lavoro Cloud Volumes ONTAP. Questa opzione non consente di eseguire il backup dei dati on-premise.

Per le licenze BYOL di backup e ripristino BlueXP, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. ["Scopri come gestire le tue licenze BYOL"](#).

Inoltre, è necessario disporre di un account AWS per lo spazio di storage in cui verranno collocati i backup.

Regioni AWS supportate

Il backup e ripristino BlueXP è supportato in tutte le regioni AWS ["Dove è supportato Cloud Volumes ONTAP"](#).

Autorizzazioni di backup AWS richieste

Il ruolo IAM che fornisce a BlueXP le autorizzazioni deve includere le autorizzazioni S3 della versione più recente "Policy BlueXP".

Di seguito sono riportate le autorizzazioni S3 specifiche del criterio:

```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource": [
    "arn:aws:s3:::netapp-backup-*"
  ]
},
```

Attivazione del backup e ripristino BlueXP

Abilita backup e ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro Kubernetes.

Fasi

1. Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra.

Se la destinazione Amazon S3 per i backup esiste come ambiente di lavoro su Canvas, puoi trascinare il cluster Kubernetes sull'ambiente di lavoro Amazon S3 per avviare l'installazione guidata.



2. Inserire i dettagli del criterio di backup e fare clic su **Avanti**.

È possibile definire la pianificazione del backup e scegliere il numero di backup da conservare.

Define Policy

Policy - Retention & Schedule

☐ Hourly Number of backups to retain 24

☒ Daily Number of backups to retain 30

☐ Weekly Number of backups to retain 52

☐ Monthly Number of backups to retain 12

S3 Bucket Cloud Manager will create the S3 bucket after you complete the wizard

3. Selezionare i volumi persistenti di cui si desidera eseguire il backup.

- Per eseguire il backup di tutti i volumi, selezionare la casella nella riga del titolo (☒ Volume Name).
- Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☒ Volume_1).

Select Volumes

57 Volumes

<input checked="" type="checkbox"/>	Persistent Volume Name	Namespace	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Persistent Volume 1 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	Persistent Volume 2 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	Persistent Volume 3 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	PV 1 On	Namespace 2	10 TB	Not Active
<input checked="" type="checkbox"/>	PV 2 On	Namespace 2	10 TB	Not Active

☒ Automatically back up all existing and future persistent volumes with the selected backup policy

4. Se si desidera che il backup di tutti i volumi correnti e futuri sia attivato, lasciare selezionata la casella di controllo "Backup automatico dei volumi futuri...". Se si disattiva questa impostazione, sarà necessario attivare manualmente i backup per i volumi futuri.

5. Fare clic su **Activate Backup** (attiva backup) per avviare il backup e il ripristino di BlueXP con i backup iniziali di ciascun volume selezionato.

Risultato

Un bucket S3 viene creato automaticamente nello stesso account AWS e nella stessa regione del sistema Cloud Volumes ONTAP e i file di backup vengono memorizzati in tale area.

Viene visualizzata la dashboard di Kubernetes, che consente di monitorare lo stato dei backup.

Quali sono le prossime novità?

È possibile ["avviare e arrestare i backup dei volumi o modificare la pianificazione del backup"](#). Puoi anche farlo ["ripristinare interi volumi da un file di backup"](#) Come nuovo volume nello stesso cluster Kubernetes o in un altro cluster in AWS (nella stessa regione).

Backup di Kubernetes dati di volumi persistenti nello storage Azure Blob

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dai volumi persistenti sui cluster AKS Kubernetes nello storage Azure Blob.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1

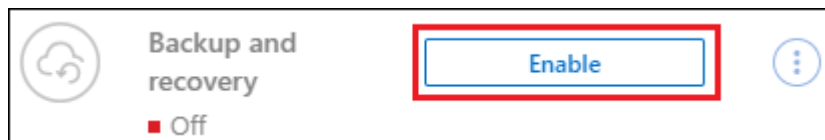
Esaminare i prerequisiti

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP.
 - Trident deve essere installato sul cluster e la versione di Trident deve essere 21.1 o superiore.
 - Tutti i PVC che verranno utilizzati per creare volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".
 - Il cluster deve utilizzare Cloud Volumes ONTAP su Azure per lo storage back-end.
 - Il sistema Cloud Volumes ONTAP deve eseguire ONTAP 9.7P5 o versione successiva.
- Hai un abbonamento valido al cloud provider per lo spazio di storage in cui verranno collocati i backup.
- Si è abbonati a. ["Offerta di backup di BlueXP Marketplace"](#), oppure è stato acquistato ["e attivato"](#) Una licenza BYOL di backup e ripristino BlueXP di NetApp.

2

Abilitare il backup e il ripristino BlueXP sul cluster Kubernetes esistente

Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra, quindi seguire la procedura di installazione guidata.



3

Definire il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di ciascun volume. Passare a backup orari, giornalieri, settimanali o mensili oppure selezionare una delle policy definite dal sistema che fornisca più opzioni. È inoltre possibile modificare il numero di copie di backup che si desidera conservare.

Define Policy

Policy - Retention & Schedule

<input type="checkbox"/> Hourly	Number of backups to retain	24
<input checked="" type="checkbox"/> Daily	Number of backups to retain	30
<input type="checkbox"/> Weekly	Number of backups to retain	52
<input type="checkbox"/> Monthly	Number of backups to retain	12

Storage Account Cloud Manager will create the storage account after you complete the wizard

4

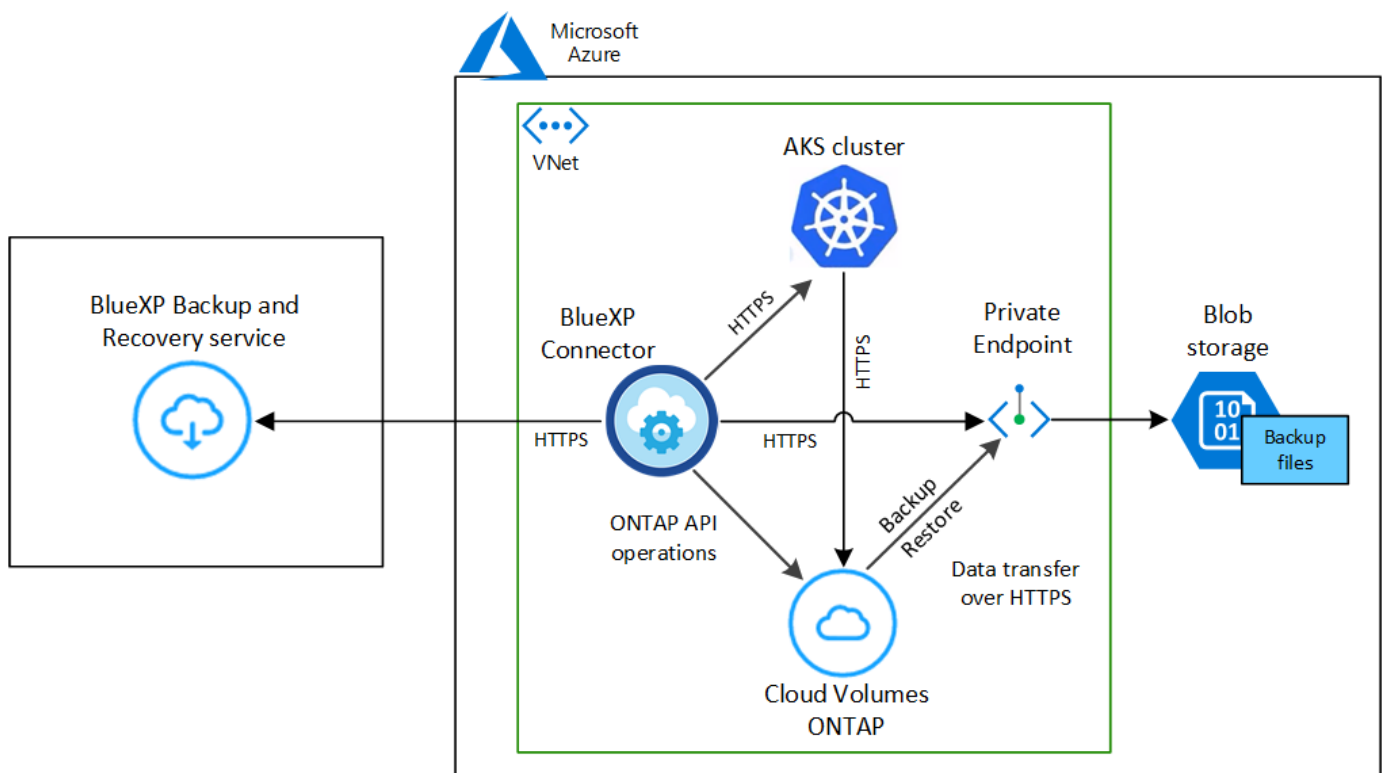
Selezionare i volumi di cui si desidera eseguire il backup

Identificare i volumi di cui si desidera eseguire il backup nella pagina Select Volumes (Seleziona volumi). I file di backup vengono memorizzati in un container Blob utilizzando la stessa sottoscrizione Azure e la stessa regione del sistema Cloud Volumes ONTAP.

Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi persistenti di Kubernetes sullo storage Blob.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi:



Tenere presente che l'endpoint privato è facoltativo.

Requisiti del cluster Kubernetes

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP. ["Scopri come scoprire il cluster Kubernetes"](#).
- Trident deve essere installato sul cluster e la versione di Trident deve essere almeno 21.1. Vedere ["Come installare Trident"](#) oppure ["Come aggiornare la versione di Trident"](#).
- Il cluster deve utilizzare Cloud Volumes ONTAP su Azure per lo storage back-end.
- Il sistema Cloud Volumes ONTAP deve trovarsi nella stessa regione Azure del cluster Kubernetes e deve eseguire ONTAP 9.7P5 o versioni successive (si consiglia ONTAP 9.8P11 e versioni successive).

Si noti che i cluster Kubernetes in ubicazioni on-premise non sono supportati. Sono supportati solo i cluster Kubernetes nelle implementazioni cloud che utilizzano sistemi Cloud Volumes ONTAP.

- Tutti gli oggetti persistenti di richiesta di rimborso del volume che verranno utilizzati per creare i volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".

È possibile eseguire questa operazione per singoli PVC aggiungendo `snapshotPolicy` in annotazioni:

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

È possibile eseguire questa operazione per tutti i PVC associati a uno storage back-end specifico aggiungendo `snapshotPolicy` sotto i valori predefiniti in `backend.json` file:

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
    deletionPolicy: retain

```

Requisiti di licenza

Per le licenze PAYGO di backup e ripristino BlueXP, è necessario un abbonamento tramite Azure Marketplace prima di attivare il backup e ripristino BlueXP. La fatturazione per il backup e il ripristino BlueXP viene effettuata tramite questo abbonamento. ["È possibile iscriversi dalla pagina Dettagli credenziali della procedura guidata dell'ambiente di lavoro"](#).

Per le licenze BYOL di backup e ripristino BlueXP, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. ["Scopri come gestire le tue licenze BYOL"](#).

Inoltre, è necessario disporre di un abbonamento a Microsoft Azure per lo spazio di storage in cui verranno collocati i backup.

Aree Azure supportate

Il backup e ripristino BlueXP è supportato in tutte le regioni Azure ["Dove è supportato Cloud Volumes ONTAP"](#).

Attivazione del backup e ripristino BlueXP

Abilita backup e ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro Kubernetes.

Fasi

1. Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra.



2. Inserire i dettagli del criterio di backup e fare clic su **Avanti**.

È possibile definire la pianificazione del backup e scegliere il numero di backup da conservare.

3. Selezionare i volumi persistenti di cui si desidera eseguire il backup.

- Per eseguire il backup di tutti i volumi, selezionare la casella nella riga del titolo (☒ Volume Name).
- Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☒ Volume_1).

<input checked="" type="checkbox"/>	Persistent Volume Name	Namespace	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Persistent Volume 1 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	Persistent Volume 2 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	Persistent Volume 3 On	Namespace 1	10 TB	Not Active
<input checked="" type="checkbox"/>	PV 1 On	Namespace 2	10 TB	Not Active
<input checked="" type="checkbox"/>	PV 2 On	Namespace 2	10 TB	Not Active
<input checked="" type="checkbox"/>	Automatically back up all existing and future persistent volumes with the selected backup policy			

4. Se si desidera che il backup di tutti i volumi correnti e futuri sia attivato, lasciare selezionata la casella di controllo "Backup automatico dei volumi futuri...". Se si disattiva questa impostazione, sarà necessario attivare manualmente i backup per i volumi futuri.
5. Fare clic su **Activate Backup** (attiva backup) per avviare il backup e il ripristino di BlueXP con i backup iniziali di ciascun volume selezionato.

Risultato

I file di backup vengono memorizzati in un container Blob utilizzando la stessa sottoscrizione Azure e la stessa regione del sistema Cloud Volumes ONTAP.

Viene visualizzata la dashboard di Kubernetes, che consente di monitorare lo stato dei backup.

Quali sono le prossime novità?

È possibile ["avviare e arrestare i backup dei volumi o modificare la pianificazione del backup"](#). Puoi anche farlo ["ripristinare interi volumi da un file di backup"](#) Come nuovo volume nello stesso cluster Kubernetes o in un altro cluster in Azure (nella stessa regione).

Backup di Kubernetes dati di volume persistenti su storage Google Cloud

Completa alcuni passaggi per iniziare a eseguire il backup dei dati dai volumi persistenti sui cluster GKE Kubernetes sullo storage Google Cloud.

Avvio rapido

Inizia subito seguendo questi passaggi o scorri verso il basso fino alle restanti sezioni per ottenere informazioni dettagliate.

1

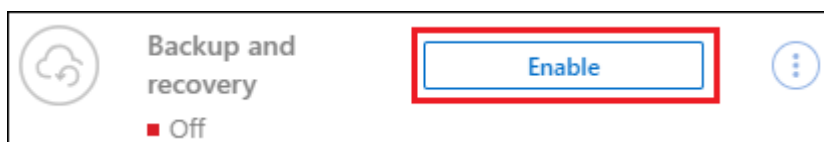
Esaminare i prerequisiti

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP.
 - Trident deve essere installato sul cluster e la versione di Trident deve essere 21.1 o superiore.
 - Tutti i PVC che verranno utilizzati per creare volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".
 - Il cluster deve utilizzare Cloud Volumes ONTAP su GCP per lo storage back-end.
 - Il sistema Cloud Volumes ONTAP deve eseguire ONTAP 9.7P5 o versione successiva.
- Si dispone di un abbonamento GCP valido per lo spazio di storage in cui verranno collocati i backup.
- Nel progetto Google Cloud hai un account di servizio con il ruolo predefinito Storage Admin.
- Si è abbonati a ["Offerta di backup di BlueXP Marketplace"](#), oppure è stato acquistato ["e attivato"](#) Una licenza BYOL di backup e ripristino BlueXP di NetApp.

2

Abilitare il backup e il ripristino BlueXP sul cluster Kubernetes esistente

Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra, quindi seguire la procedura di installazione guidata.



3

Definire il criterio di backup

Il criterio predefinito esegue il backup dei volumi ogni giorno e conserva le 30 copie di backup più recenti di ciascun volume. Passare a backup orari, giornalieri, settimanali o mensili oppure selezionare una delle policy definite dal sistema che fornisca più opzioni. È inoltre possibile modificare il numero di copie di backup che si desidera conservare.

The screenshot shows a 'Define Policy' window with a 'Policy - Retention & Schedule' section. It contains four radio button options for backup frequency: 'Hourly' (unchecked, 24 backups), 'Daily' (checked, 30 backups), 'Weekly' (unchecked, 52 backups), and 'Monthly' (unchecked, 12 backups). Each option has a corresponding 'Number of backups to retain' with a numeric input field and up/down arrows. Below this section is a 'Storage Account' section with a note: 'Cloud Manager will create the storage account after you complete the wizard'.

Frequency	Number of backups to retain
<input type="checkbox"/> Hourly	24
<input checked="" type="checkbox"/> Daily	30
<input type="checkbox"/> Weekly	52
<input type="checkbox"/> Monthly	12

Storage Account Cloud Manager will create the storage account after you complete the wizard

4

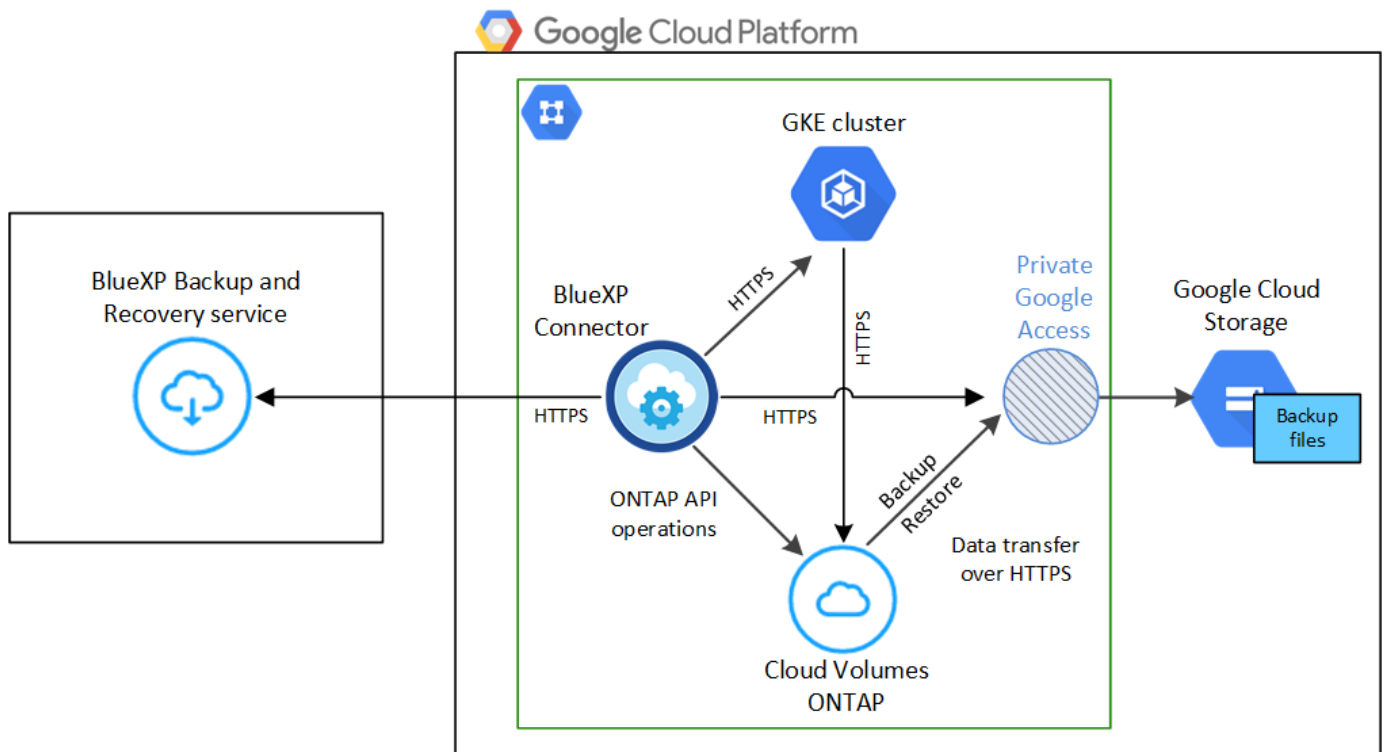
Selezionare i volumi di cui si desidera eseguire il backup

Identificare i volumi di cui si desidera eseguire il backup nella pagina Select Volumes (Seleziona volumi). I file di backup vengono memorizzati in un bucket di storage cloud Google utilizzando la stessa sottoscrizione GCP e la stessa regione del sistema Cloud Volumes ONTAP.

Requisiti

Leggere i seguenti requisiti per assicurarsi di disporre di una configurazione supportata prima di avviare il backup dei volumi persistenti Kubernetes sullo storage Google Cloud.

L'immagine seguente mostra ciascun componente e le connessioni che è necessario preparare tra di essi:



Tenere presente che l'endpoint privato è facoltativo.

Requisiti del cluster Kubernetes

- Hai scoperto il cluster Kubernetes come ambiente di lavoro BlueXP. ["Scopri come scoprire il cluster Kubernetes"](#).
- Trident deve essere installato sul cluster e la versione di Trident deve essere almeno 21.1. Vedere ["Come installare Trident"](#) oppure ["Come aggiornare la versione di Trident"](#).
- Il cluster deve utilizzare Cloud Volumes ONTAP su GCP per lo storage back-end.
- Il sistema Cloud Volumes ONTAP deve trovarsi nella stessa regione GCP del cluster Kubernetes e deve eseguire ONTAP 9.7P5 o versioni successive (si consiglia ONTAP 9.8P11 e versioni successive).

Si noti che i cluster Kubernetes in ubicazioni on-premise non sono supportati. Sono supportati solo i cluster Kubernetes nelle implementazioni cloud che utilizzano sistemi Cloud Volumes ONTAP.

- Tutti gli oggetti persistenti di richiesta di rimborso del volume che verranno utilizzati per creare i volumi persistenti di cui si desidera eseguire il backup devono avere "snapshotPolicy" impostato su "default".

È possibile eseguire questa operazione per singoli PVC aggiungendo snapshotPolicy in annotazioni:

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver

```

È possibile eseguire questa operazione per tutti i PVC associati a uno storage back-end specifico aggiungendo `snapshotPolicy` sotto i valori predefiniti in `backend.json` file:

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
    deletionPolicy: retain

```

Regioni GCP supportate

Il backup e ripristino BlueXP è supportato in tutte le regioni GCP ["Dove è supportato Cloud Volumes ONTAP"](#).

Requisiti di licenza

Per le licenze PAYGO di backup e ripristino BlueXP, è necessario un abbonamento tramite ["Mercato GCP"](#). È necessario prima di attivare il backup e il ripristino BlueXP. La fatturazione per il backup e il ripristino BlueXP viene effettuata tramite questo abbonamento. ["È possibile iscriversi dalla pagina Dettagli credenziali della procedura guidata dell'ambiente di lavoro"](#).

Per le licenze BYOL di backup e ripristino BlueXP, è necessario il numero di serie di NetApp che consente di utilizzare il servizio per la durata e la capacità della licenza. ["Scopri come gestire le tue licenze BYOL"](#).

Inoltre, è necessario disporre di un abbonamento Google per lo spazio di storage in cui verranno collocati i backup.

Account di servizio GCP

Devi disporre di un account di servizio nel tuo progetto Google Cloud con il ruolo predefinito Storage Admin. ["Scopri come creare un account di servizio"](#).

Attivazione del backup e ripristino BlueXP

Abilita backup e ripristino BlueXP in qualsiasi momento direttamente dall'ambiente di lavoro Kubernetes.

Fasi

1. Selezionare l'ambiente di lavoro e fare clic su **Enable** (attiva) accanto al servizio di backup e ripristino nel pannello di destra.



2. Inserire i dettagli del criterio di backup e fare clic su **Avanti**.

È possibile definire la pianificazione del backup e scegliere il numero di backup da conservare.

3. Selezionare i volumi persistenti di cui si desidera eseguire il backup.
 - Per eseguire il backup di tutti i volumi, selezionare la casella nella riga del titolo (☒ Volume Name).
 - Per eseguire il backup di singoli volumi, selezionare la casella relativa a ciascun volume (☒ Volume_1).

Select Volumes				
57 volumes				
<input checked="" type="checkbox"/>	Persistent Volume Name	Namespace	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Persistent Volume 1 ● On	Namespace 1	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Persistent Volume 2 ● On	Namespace 1	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Persistent Volume 3 ● On	Namespace 1	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	P.V.1 ● On	Namespace 2	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	P.V.2 ● On	Namespace 2	10 TB	⊖ Not Active
<input checked="" type="checkbox"/> Automatically back up all existing and future persistent volumes with the selected backup policy ⓘ				

- Se si desidera che il backup di tutti i volumi correnti e futuri sia attivato, lasciare selezionata la casella di controllo "Backup automatico dei volumi futuri...". Se si disattiva questa impostazione, sarà necessario attivare manualmente i backup per i volumi futuri.
- Fare clic su **Activate Backup** (attiva backup) per avviare il backup e il ripristino di BlueXP con i backup iniziali di ciascun volume selezionato.

Risultato

I file di backup vengono memorizzati in un bucket di storage cloud Google utilizzando la stessa sottoscrizione GCP e la stessa regione del sistema Cloud Volumes ONTAP.

Viene visualizzata la dashboard di Kubernetes, che consente di monitorare lo stato dei backup.

Quali sono le prossime novità?

È possibile ["avviare e arrestare i backup dei volumi o modificare la pianificazione del backup"](#). Puoi anche farlo ["ripristinare interi volumi da un file di backup"](#) Come nuovo volume nello stesso cluster Kubernetes o in un altro cluster in GCP (nella stessa regione).

Gestione dei backup per i sistemi Kubernetes

Puoi gestire i backup per i tuoi sistemi Kubernetes modificando la pianificazione del backup, attivando/disattivando i backup dei volumi, eliminando i backup e molto altro ancora.



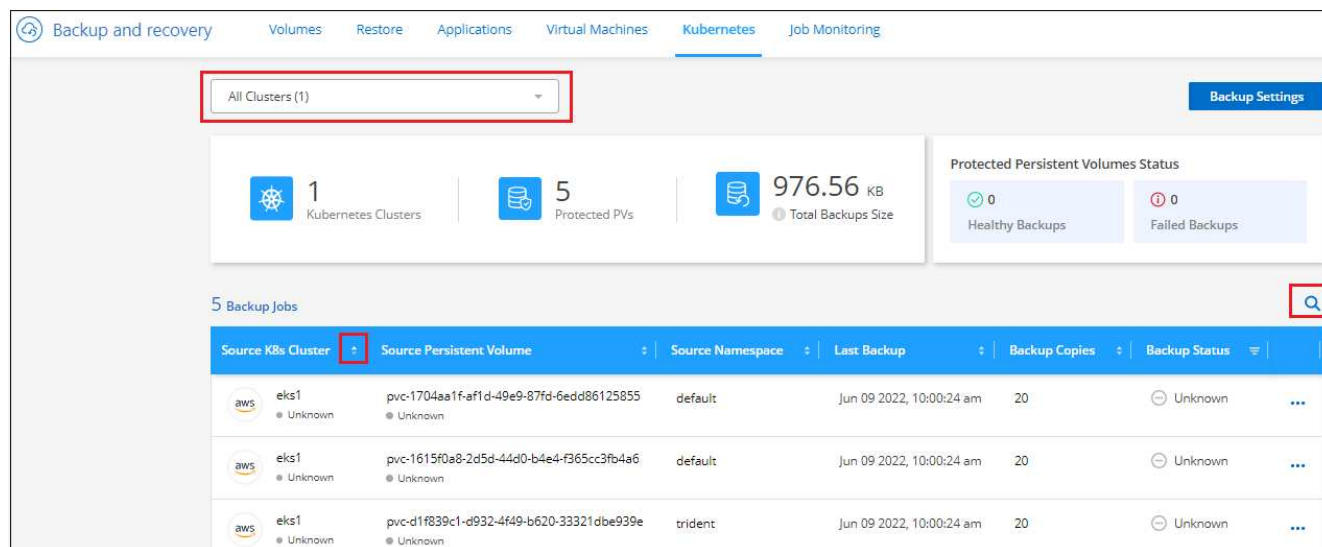
Non gestire o modificare i file di backup direttamente dall'ambiente del cloud provider. Questo potrebbe danneggiare i file e causare una configurazione non supportata.

Visualizzazione dei volumi di cui viene eseguito il backup

È possibile visualizzare un elenco di tutti i volumi attualmente sottoposti a backup con il backup e ripristino di BlueXP.

Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Fare clic sulla scheda **Kubernetes** per visualizzare l'elenco dei volumi persistenti per i sistemi Kubernetes.



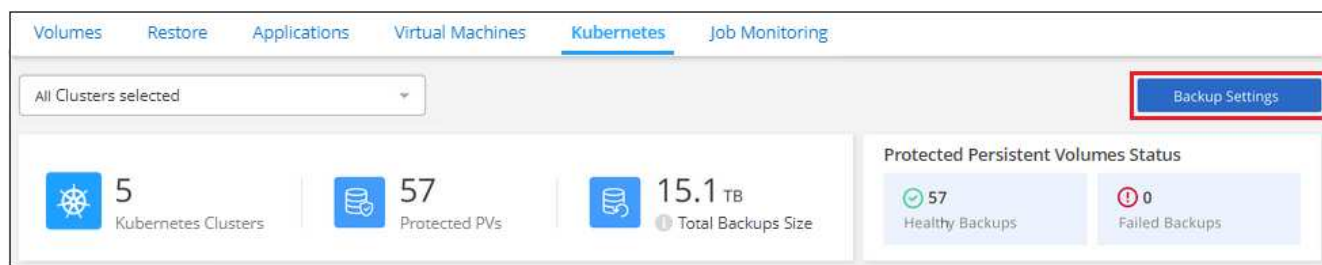
Se si cercano volumi specifici in determinati cluster, è possibile perfezionare l'elenco in base al cluster e al volume oppure utilizzare il filtro di ricerca.

Attivazione e disattivazione dei backup dei volumi

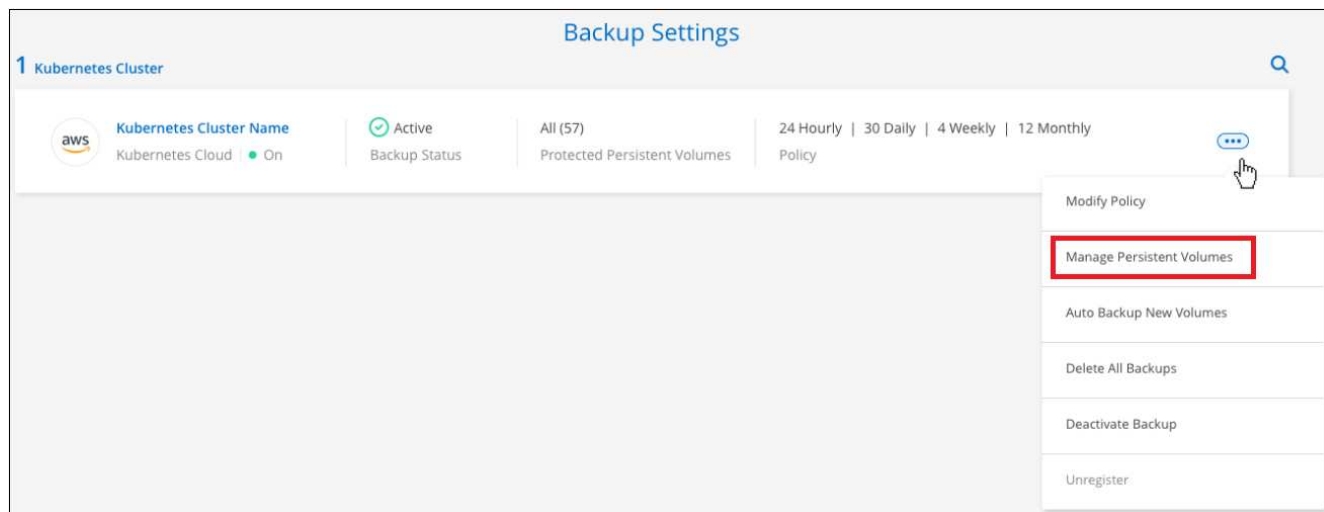
È possibile interrompere il backup di un volume se non sono necessarie copie di backup di quel volume e non si desidera pagare il costo di archiviazione dei backup. È inoltre possibile aggiungere un nuovo volume all'elenco di backup, se non viene eseguito il backup.

Fasi

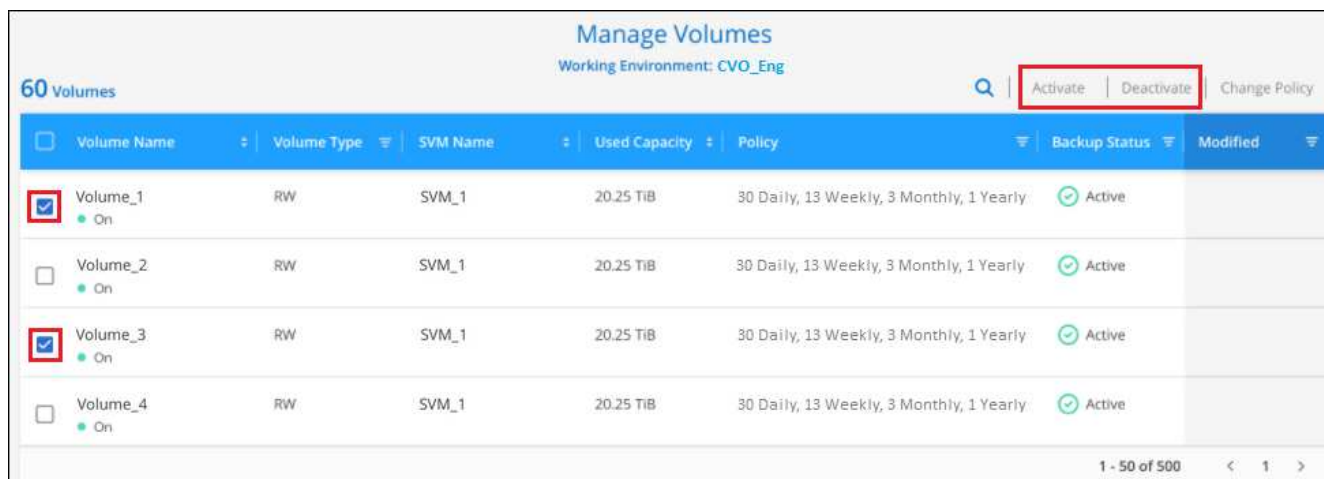
1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Dalla *pagina Backup Settings*, fare clic su **...** Per il cluster Kubernetes e selezionare **Manage Persistent Volumes** (Gestisci volumi persistenti).



3. Selezionare la casella di controllo di uno o più volumi da modificare, quindi fare clic su **Attivate** o **Deactivate** (Disattiva) a seconda che si desideri avviare o interrompere i backup del volume.



4. Fare clic su **Save** (Salva) per confermare le modifiche.

Nota: quando si interrompe il backup di un volume, il provider di cloud continuerà a addebitare i costi di storage a oggetti per la capacità utilizzata dai backup a meno che non si utilizzi [eliminare i backup](#).

Modifica di un criterio di backup esistente

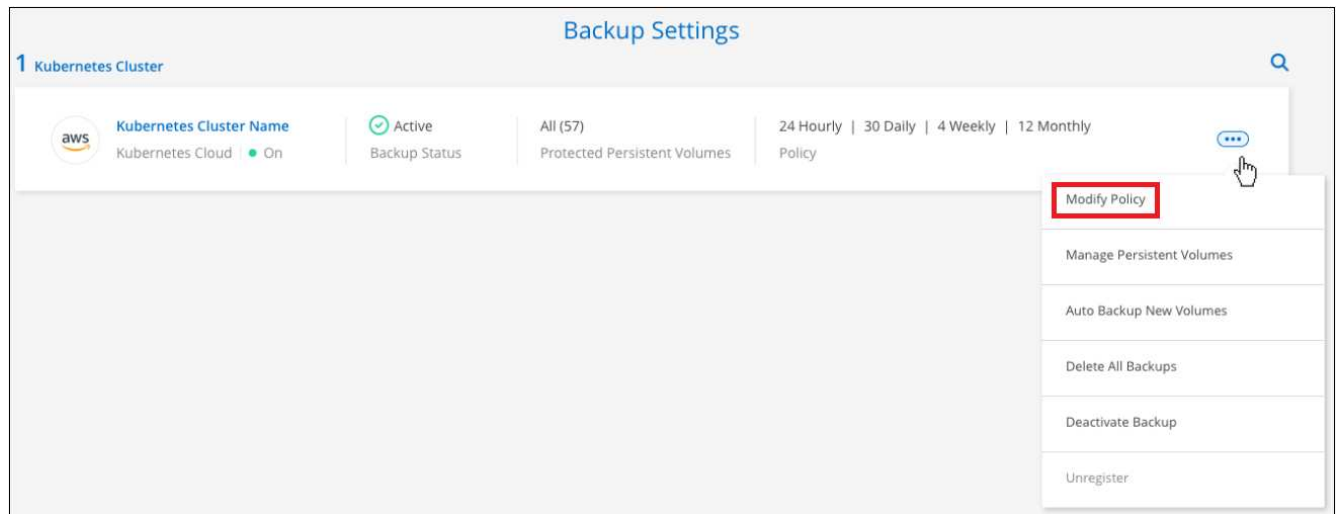
È possibile modificare gli attributi di un criterio di backup attualmente applicato ai volumi in un ambiente di lavoro. La modifica del criterio di backup influisce su tutti i volumi esistenti che utilizzano il criterio.

Fasi

1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Nella pagina *Backup Settings*, fare clic su **...** Per l'ambiente di lavoro in cui si desidera modificare le impostazioni e selezionare **Gestisci policy**.



3. Dalla pagina *Manage Policies*, fare clic su **Edit Policy** (Modifica policy) per il criterio di backup che si desidera modificare in quell'ambiente di lavoro.



4. Dalla pagina *Edit Policy*, modificare la pianificazione e la conservazione del backup e fare clic su **Save** (Salva).

Edit Policy	
Working Environment: Cluster Dev Lab	
Name	Daily 30 backups ▼
Labels & Retention	30 Daily ▼

Impostazione di un criterio di backup da assegnare ai nuovi volumi

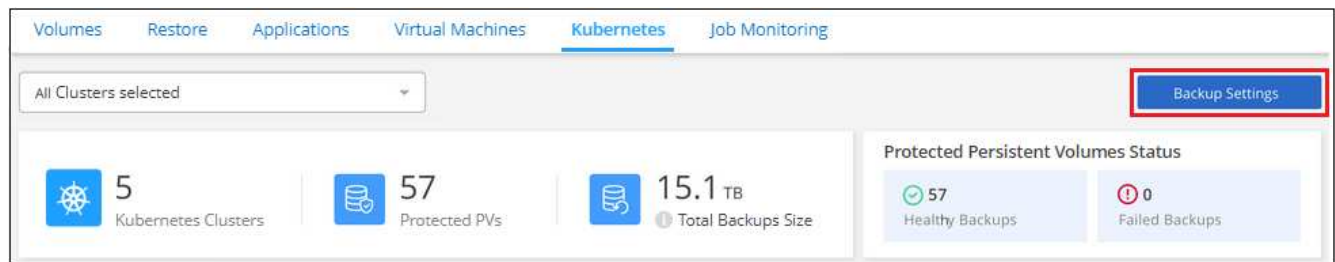
Se non è stata selezionata l'opzione che consente di assegnare automaticamente un criterio di backup ai volumi appena creati al momento dell'attivazione del backup e ripristino BlueXP sul cluster Kubernetes, è possibile scegliere questa opzione nella pagina *Backup Settings* più avanti. L'assegnazione di una policy di backup ai volumi appena creati garantisce la protezione di tutti i dati.

Tenere presente che il criterio che si desidera applicare ai volumi deve già esistere.

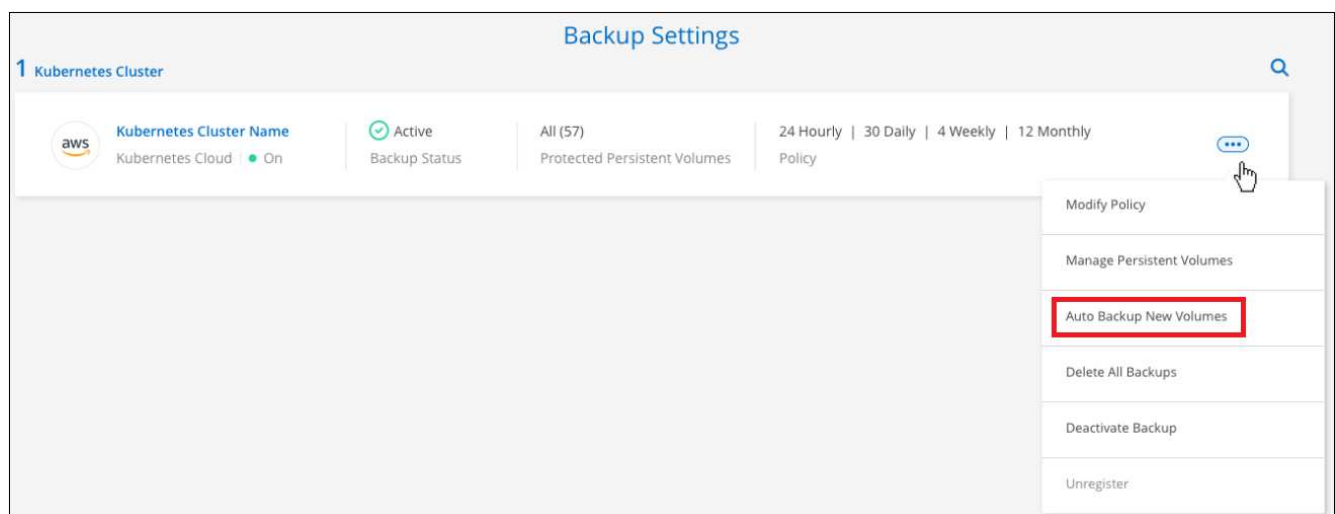
È inoltre possibile disattivare questa impostazione in modo che il backup dei volumi appena creati non venga eseguito automaticamente. In tal caso, sarà necessario attivare manualmente i backup per tutti i volumi specifici di cui si desidera eseguire il backup in futuro.

Fasi

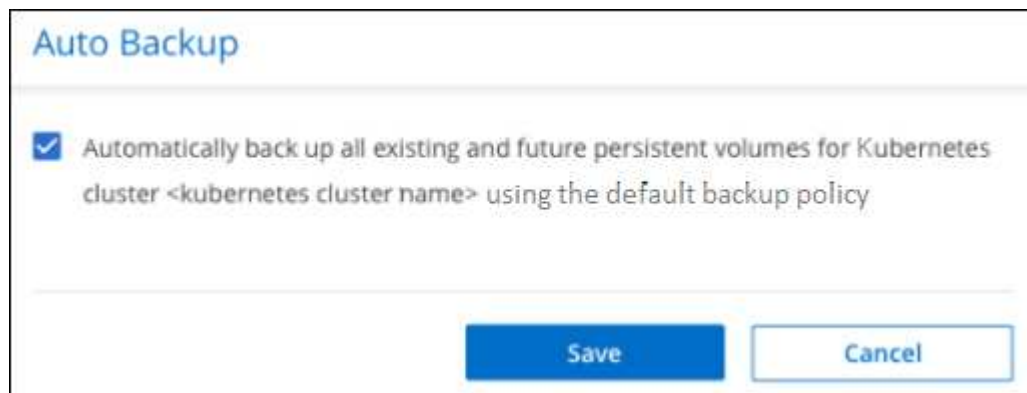
1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Dalla *pagina Backup Settings*, fare clic su **...** Per il cluster Kubernetes in cui sono presenti i volumi e selezionare **Backup automatico nuovi volumi**.



3. Selezionare la casella di controllo "Backup automatico dei volumi persistenti futuri...", scegliere il criterio di backup che si desidera applicare ai nuovi volumi e fare clic su **Salva**.



Auto Backup

☒ Automatically back up all existing and future persistent volumes for Kubernetes cluster <kubernetes cluster name> using the default backup policy

Save **Cancel**

Risultato

A questo punto, questa policy di backup verrà applicata a tutti i nuovi volumi creati in questo cluster Kubernetes.

Visualizzazione dell'elenco dei backup per ciascun volume

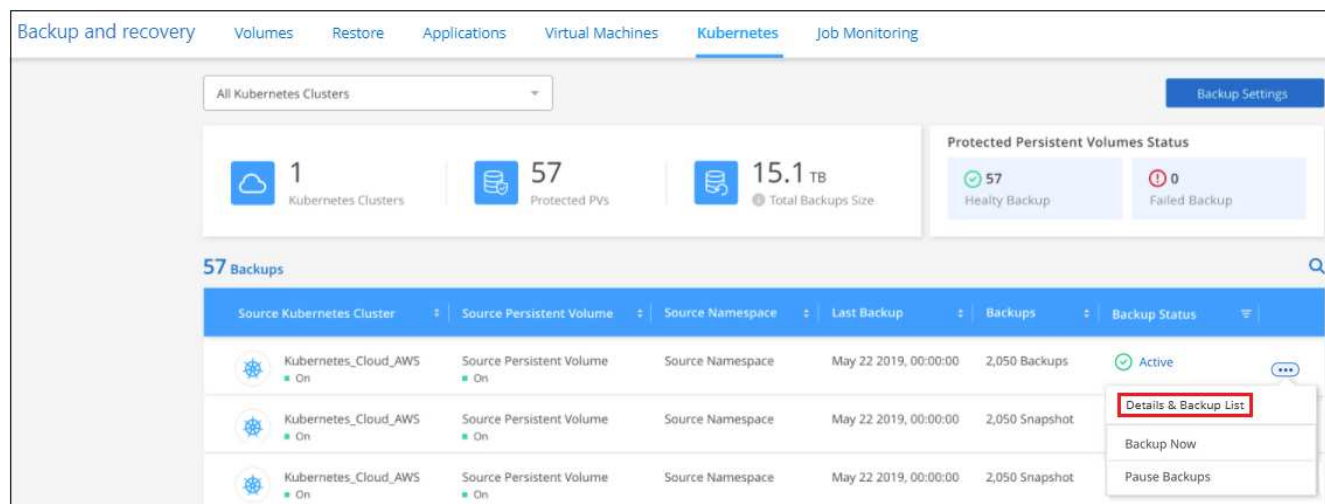
È possibile visualizzare l'elenco di tutti i file di backup esistenti per ciascun volume. In questa pagina vengono visualizzati i dettagli relativi al volume di origine, alla posizione di destinazione e ai dettagli del backup, ad esempio l'ultimo backup eseguito, la policy di backup corrente, le dimensioni del file di backup e altro ancora.

Questa pagina consente inoltre di eseguire le seguenti operazioni:

- Eliminare tutti i file di backup per il volume
- Eliminare singoli file di backup per il volume
- Scarica un report di backup per il volume

Fasi

1. Dalla scheda **Kubernetes**, fare clic su **...** Per il volume di origine e selezionare **Details & Backup List**.



Backup and recovery | Volumes | Restore | Applications | Virtual Machines | **Kubernetes** | Job Monitoring

All Kubernetes Clusters

1 Kubernetes Clusters | **57** Protected PVs | **15.1 TB** Total Backups Size

Protected Persistent Volumes Status

57 Healthy Backup | **0** Failed Backup

57 Backups

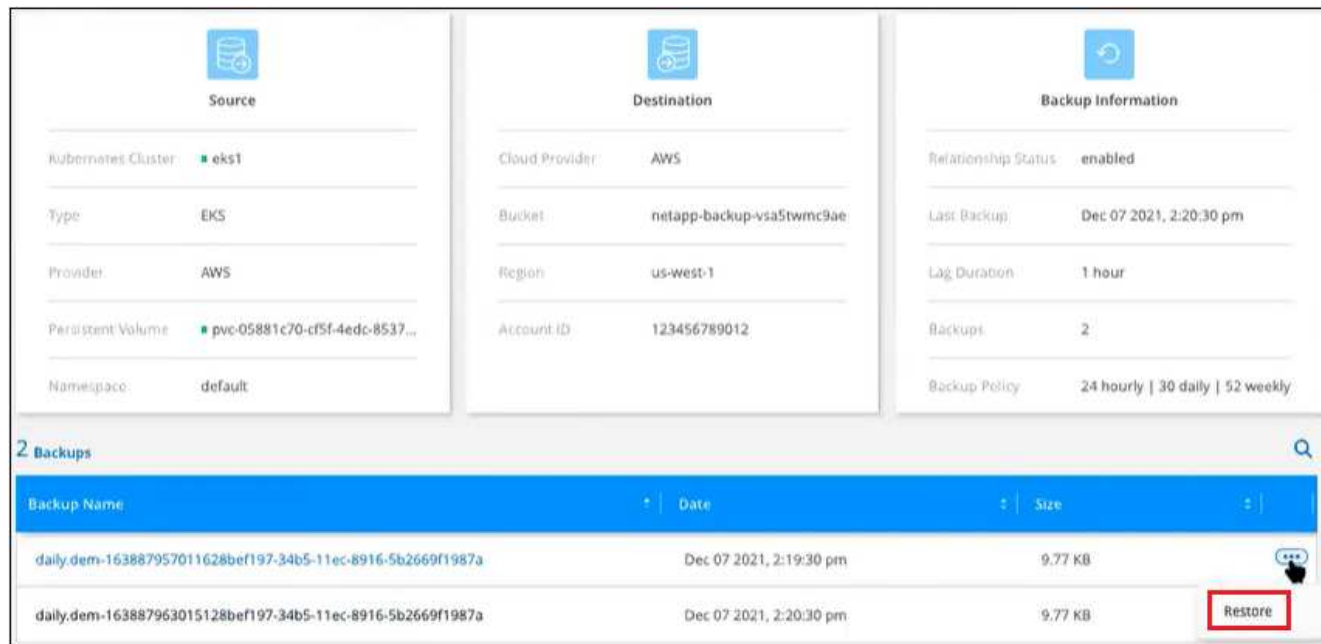
Source Kubernetes Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backups	Backup Status
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Backups	Active
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	

Details & Backup List

Backup Now

Pause Backups

Viene visualizzato l'elenco di tutti i file di backup con i dettagli relativi al volume di origine, alla posizione di destinazione e ai dettagli del backup.



Eliminazione dei backup

Il backup e ripristino BlueXP consente di eliminare un singolo file di backup, eliminare tutti i backup di un volume o eliminare tutti i backup di tutti i volumi in un cluster Kubernetes. È possibile eliminare tutti i backup se non sono più necessari o se è stato eliminato il volume di origine e si desidera rimuovere tutti i backup.



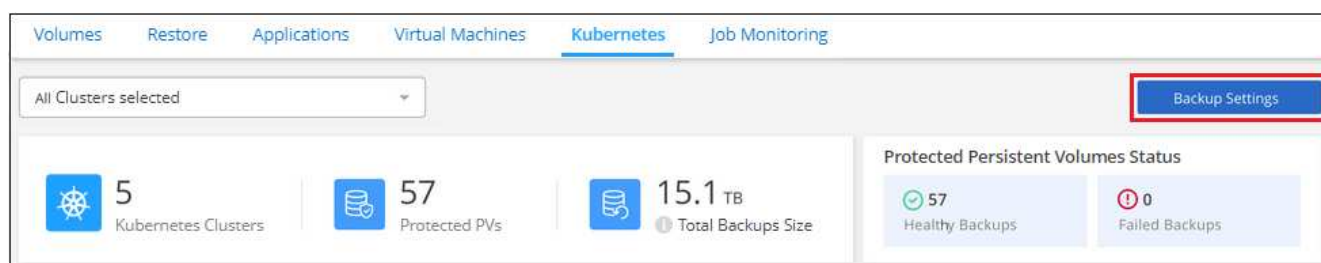
Se si prevede di eliminare un ambiente di lavoro o un cluster con backup, è necessario eliminare i backup **prima** di eliminare il sistema. Il backup e il ripristino di BlueXP non eliminano automaticamente i backup quando si elimina un sistema e non esiste attualmente alcun supporto nell'interfaccia utente per eliminare i backup dopo che il sistema è stato eliminato. I costi di storage a oggetti per i backup rimanenti continueranno a essere addebitati.

Eliminazione di tutti i file di backup per un ambiente di lavoro

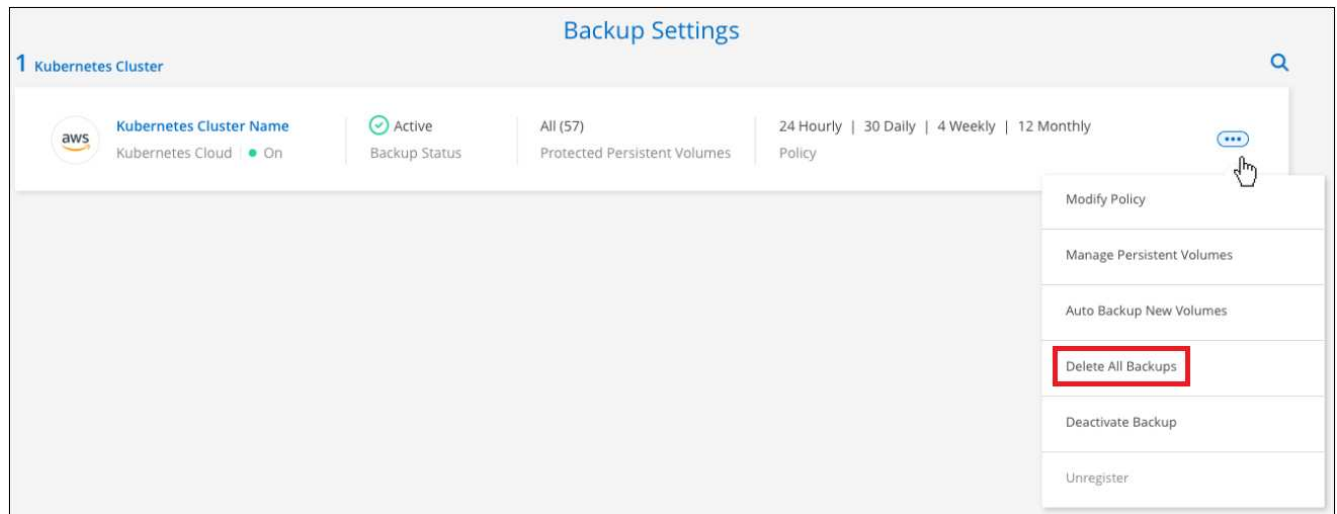
L'eliminazione di tutti i backup per un ambiente di lavoro non disattiva i backup futuri dei volumi in questo ambiente di lavoro. Se si desidera interrompere la creazione di backup di tutti i volumi in un ambiente di lavoro, è possibile disattivare i backup [come descritto qui](#).

Fasi

1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Fare clic su **...** Per il cluster Kubernetes in cui si desidera eliminare tutti i backup e selezionare **Delete All backups** (Elimina tutti i backup).



3. Nella finestra di dialogo di conferma, immettere il nome dell'ambiente di lavoro e fare clic su **Delete** (Elimina).

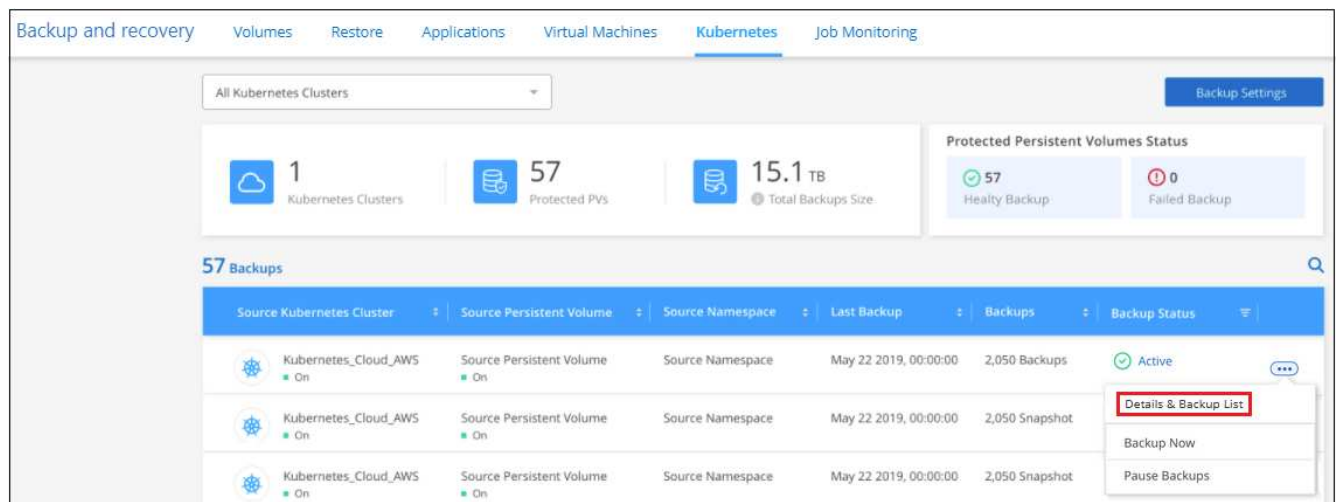
Eliminazione di tutti i file di backup di un volume

L'eliminazione di tutti i backup per un volume disattiva anche i backup futuri per quel volume.

È possibile [riavviare l'esecuzione dei backup per il volume](#) In qualsiasi momento dalla pagina Gestisci backup.

Fasi

1. Dalla scheda **Kubernetes**, fare clic su **...** Per il volume di origine e selezionare **Details & Backup List**.



Viene visualizzato l'elenco di tutti i file di backup.

The screenshot displays the NetApp backup management interface. It is divided into three main sections: Source, Destination, and Backup Information.

- Source:**
 - Working Environment: Working Environment N...
 - Type: Cloud Volumes ONTAP (HA)
 - Provider: AWS
 - Volume: Volume Name
 - SVM: SVM Name
- Destination:**
 - Cloud Provider: AWS
 - Region: us-east-1
 - Bucket: netapp-backup
 - Account ID: 012345678901234567890
- Backup Information:**
 - Relationship Status: Active
 - Last Backup: Oct 05 2021, 2:41:33 pm
 - Lag Duration: 14 days 3 hours, 38 mi...
 - Backups: 2,050
 - Backup Policy: Netapp7YearsRetention

Below these sections, there is a table titled "2,050 Backups". The table has columns for Backup Name, Date, and Size. The first three rows are:

Backup Name	Date	Size
Backup_2020_Jan	May 22 2019, 00:00:00	19,001
Backup_2020_Mar	May 22 2019, 00:00:00	19,002
Backup_2020_Apr	May 22 2019, 00:00:00	19,009

2. Fare clic su **azioni** > **Elimina tutti i backup**.

The screenshot shows the "2,050 Backups" table with the "Actions" menu open. The "Delete All Backups" option is highlighted with a red box. The "Download Backup Report" option is also visible below it.

3. Nella finestra di dialogo di conferma, inserire il nome del volume e fare clic su **Delete** (Elimina).

Eliminazione di un singolo file di backup per un volume

È possibile eliminare un singolo file di backup. Questa funzione è disponibile solo se il backup del volume è stato creato da un sistema con ONTAP 9.8 o superiore.

Fasi

1. Dalla scheda **Kubernetes**, fare clic su **...** Per il volume di origine e selezionare **Details & Backup List**.

Backup and recovery Volumes Restore Applications Virtual Machines **Kubernetes** Job Monitoring

All Kubernetes Clusters Backup Settings

1
Kubernetes Clusters

57
Protected PVs

15.1 TB
Total Backups Size

Protected Persistent Volumes Status

57
Healthy Backup

0
Failed Backup

57 Backups

Source Kubernetes Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backups	Backup Status	
Kubernetes_Cloud_AWS On	Source Persistent Volume On	Source Namespace	May 22 2019, 00:00:00	2,050 Backups	Active	⋮
Kubernetes_Cloud_AWS On	Source Persistent Volume On	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot		<div> Details & Backup List </div>
Kubernetes_Cloud_AWS On	Source Persistent Volume On	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot		<div> Backup Now </div> <div> Pause Backups </div>

Viene visualizzato l'elenco di tutti i file di backup.

Source

Working Environment Working Environment N...

Type Cloud Volumes ONTAP (HA)

Provider AWS

Volume Volume Name

SVM SVM Name

Destination

Cloud Provider AWS

Region us-east-1

Bucket netapp-backup

Account ID 012345678901234567890

Backup Information

Relationship Status Active

Last Backup Oct 05 2021, 2:41:33 pm

Lag Duration 14 days 3 hours, 38 mi...

Backups 2,050

Backup Policy Netapp7YearsRetention

2,050 Backups

Select Timeframe Actions

Backup Name	Date	Size	
Backup_2020_Jan	May 22 2019, 00:00:00	19,001	⋮
Backup_2020_Mar	May 22 2019, 00:00:00	19,002	⋮
Backup_2020_Apr	May 22 2019, 00:00:00	19,009	⋮

- Fare clic su **⋮** Per il file di backup del volume che si desidera eliminare e fare clic su **Delete** (Elimina).

2,050 Backups

Select Timeframe Actions

Backup Name	Date	
Backup_2020_Feb	May 22 2019, 00:00:00	⋮
Backup_2020_Jan	May 22 2019, 00:00:00	⋮
Backup_2020_Mar	May 22 2019, 00:00:00	⋮

Delete

Restore

- Nella finestra di dialogo di conferma, fare clic su **Delete** (Elimina).

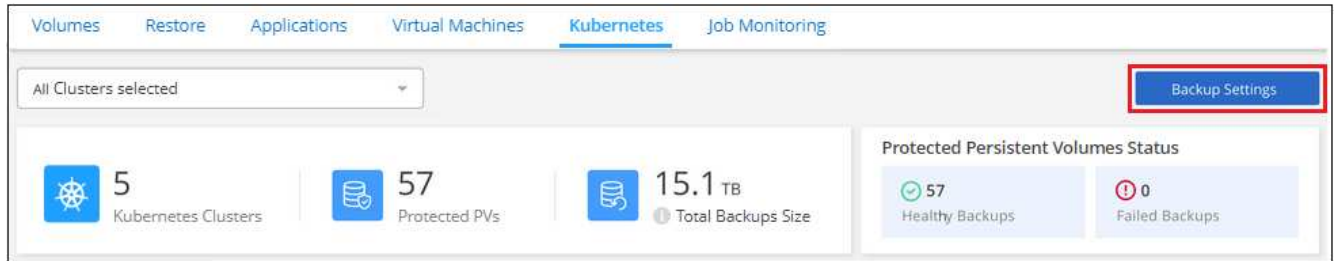
Disattivazione del backup e ripristino BlueXP per un ambiente di lavoro

La disattivazione del backup e ripristino di BlueXP per un ambiente di lavoro disattiva i backup di ciascun volume sul sistema e disattiva anche la possibilità di ripristinare un volume. I backup esistenti non verranno eliminati. In questo modo non si annulla la registrazione del servizio di backup da questo ambiente di lavoro, ma è possibile sospendere tutte le attività di backup e ripristino per un determinato periodo di tempo.

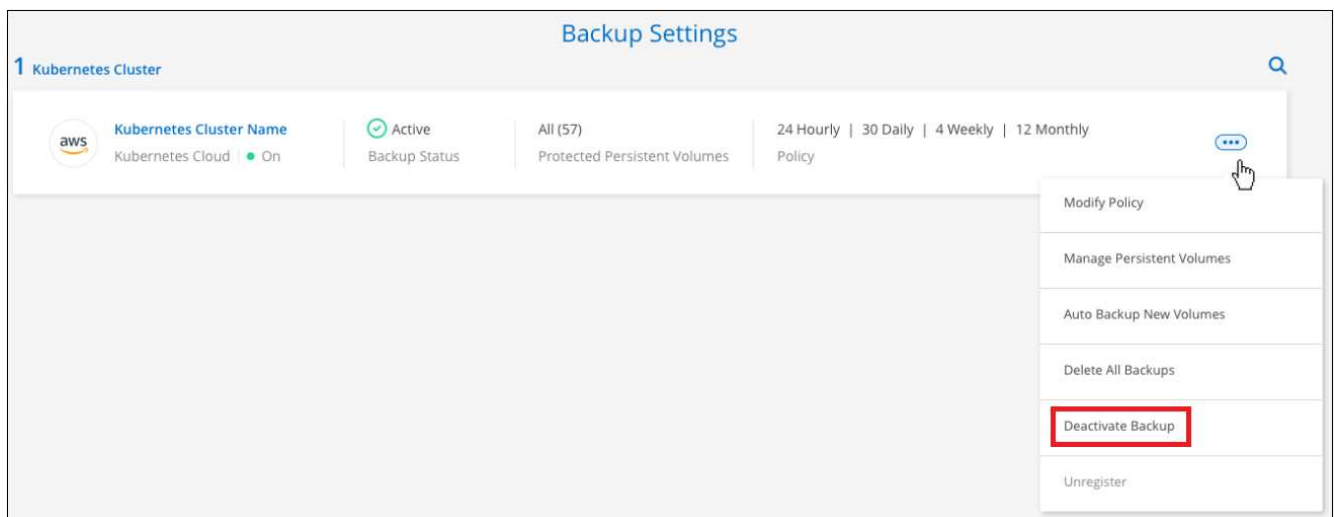
Tieni presente che il tuo cloud provider continuerà a addebitare i costi dello storage a oggetti per la capacità utilizzata dai backup, a meno che tu non lo utilizzi [eliminare i backup](#).

Fasi

1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Dalla *pagina Backup Settings*, fare clic su **...** Per l'ambiente di lavoro o il cluster Kubernetes, in cui si desidera disattivare i backup e selezionare **Disattiva backup**.



3. Nella finestra di dialogo di conferma, fare clic su **Disattiva**.



Quando il backup è disattivato, viene visualizzato il pulsante **Activate Backup** (attiva backup) per quell'ambiente di lavoro. Fare clic su questo pulsante per riattivare la funzionalità di backup per l'ambiente di lavoro.

Annullamento della registrazione di backup e ripristino BlueXP per un ambiente di lavoro

È possibile annullare la registrazione di backup e ripristino BlueXP per un ambiente di lavoro se non si desidera più utilizzare la funzionalità di backup e si desidera smettere di pagare per i backup in tale ambiente di lavoro. In genere, questa funzionalità viene utilizzata quando si intende eliminare un cluster Kubernetes e si desidera annullare il servizio di backup.

È inoltre possibile utilizzare questa funzione se si desidera modificare l'archivio di oggetti di destinazione in cui vengono memorizzati i backup del cluster. Dopo aver disregistrato il backup e il ripristino BlueXP per l'ambiente di lavoro, è possibile attivare il backup e il ripristino BlueXP per quel cluster utilizzando le informazioni del nuovo provider di cloud.

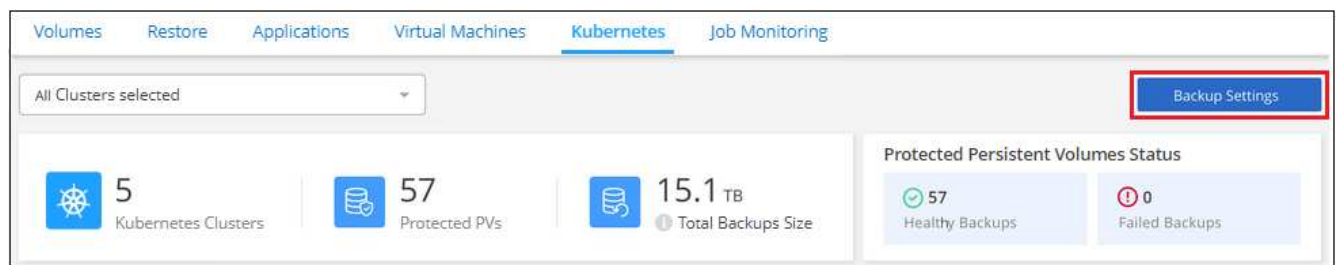
Prima di annullare la registrazione di backup e ripristino BlueXP, è necessario eseguire le seguenti operazioni, nell'ordine indicato:

- Disattivare il backup e ripristino BlueXP per l'ambiente di lavoro
- Eliminare tutti i backup per l'ambiente di lavoro

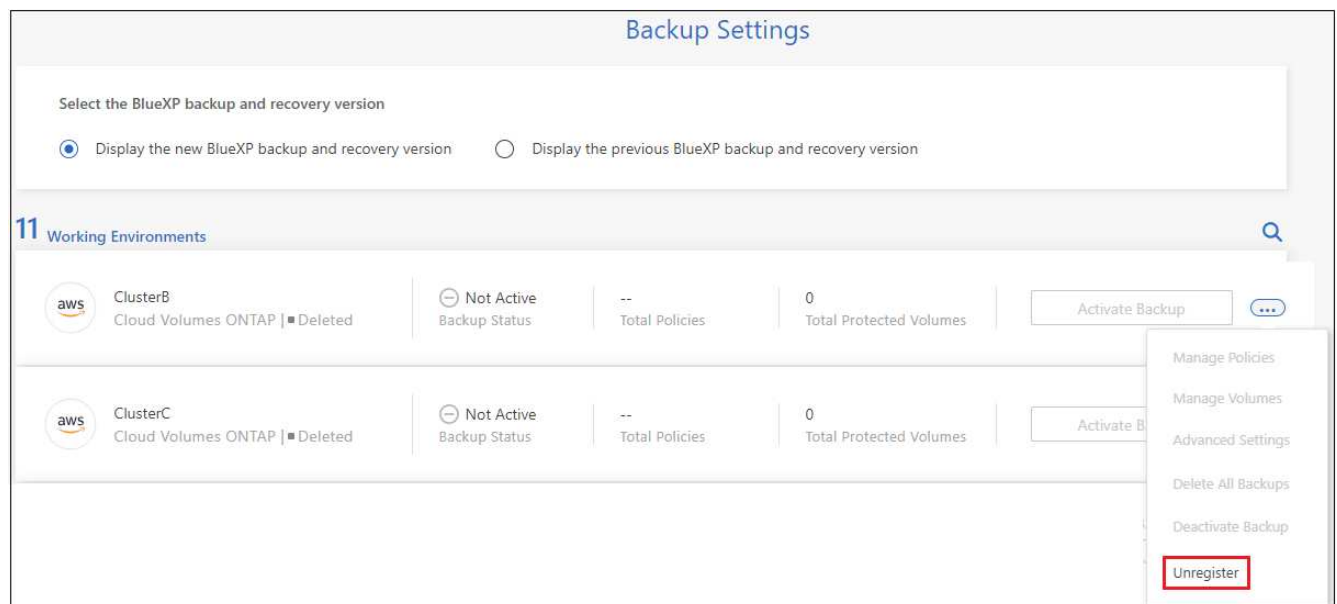
L'opzione di annullamento della registrazione non è disponibile fino al completamento di queste due azioni.

Fasi

1. Dalla scheda **Kubernetes**, selezionare **Backup Settings**.



2. Dalla *pagina Backup Settings*, fare clic su **...** Per il cluster Kubernetes in cui si desidera annullare la registrazione del servizio di backup e selezionare **Annulla registrazione**.



3. Nella finestra di dialogo di conferma, fare clic su **Annulla registrazione**.

Ripristino dei dati Kubernetes dai file di backup

I backup vengono memorizzati in un archivio di oggetti nel tuo account cloud in modo da poter ripristinare i dati da un punto specifico. È possibile ripristinare un intero volume

persistente Kubernetes da un file di backup salvato.

Puoi ripristinare un volume persistente (come nuovo volume) nello stesso ambiente di lavoro o in un ambiente di lavoro diverso che utilizza lo stesso account cloud.

Ambienti di lavoro supportati e provider di storage a oggetti

È possibile ripristinare un volume da un file di backup di Kubernetes nei seguenti ambienti di lavoro:

Percorso del file di backup	Ambiente di lavoro di destinazione <code>ifdef::aws[]</code>
Amazon S3	Cluster Kubernetes in AWS <code>endif::aws[]</code> <code>ifdef::Azure[]</code>
Azure Blob	Cluster Kubernetes in Azure <code>endif::Azure[]</code> <code>ifdef::gcp[]</code>
Storage Google Cloud	Cluster Kubernetes in Google <code>endif::gcp[]</code>

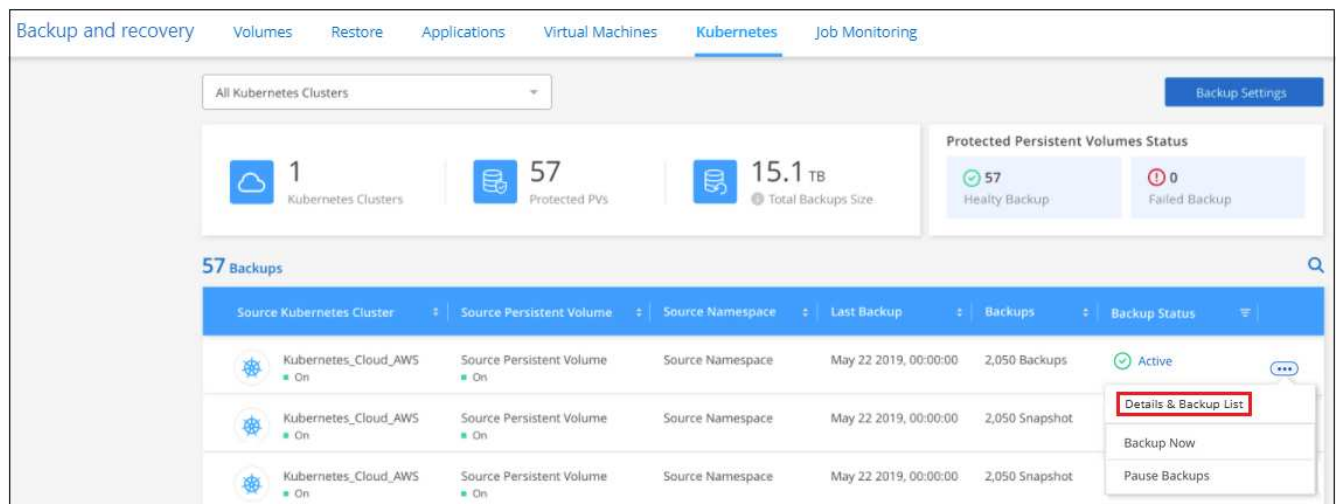
Ripristino dei volumi da un file di backup di Kubernetes

Quando si ripristina un volume persistente da un file di backup, BlueXP crea un *nuovo* volume utilizzando i dati del backup. È possibile ripristinare i dati in un volume nello stesso cluster Kubernetes o in un cluster Kubernetes diverso che si trova nello stesso account cloud del cluster Kubernetes di origine.

Prima di iniziare, è necessario conoscere il nome del volume che si desidera ripristinare e la data del file di backup che si desidera utilizzare per creare il volume appena ripristinato.

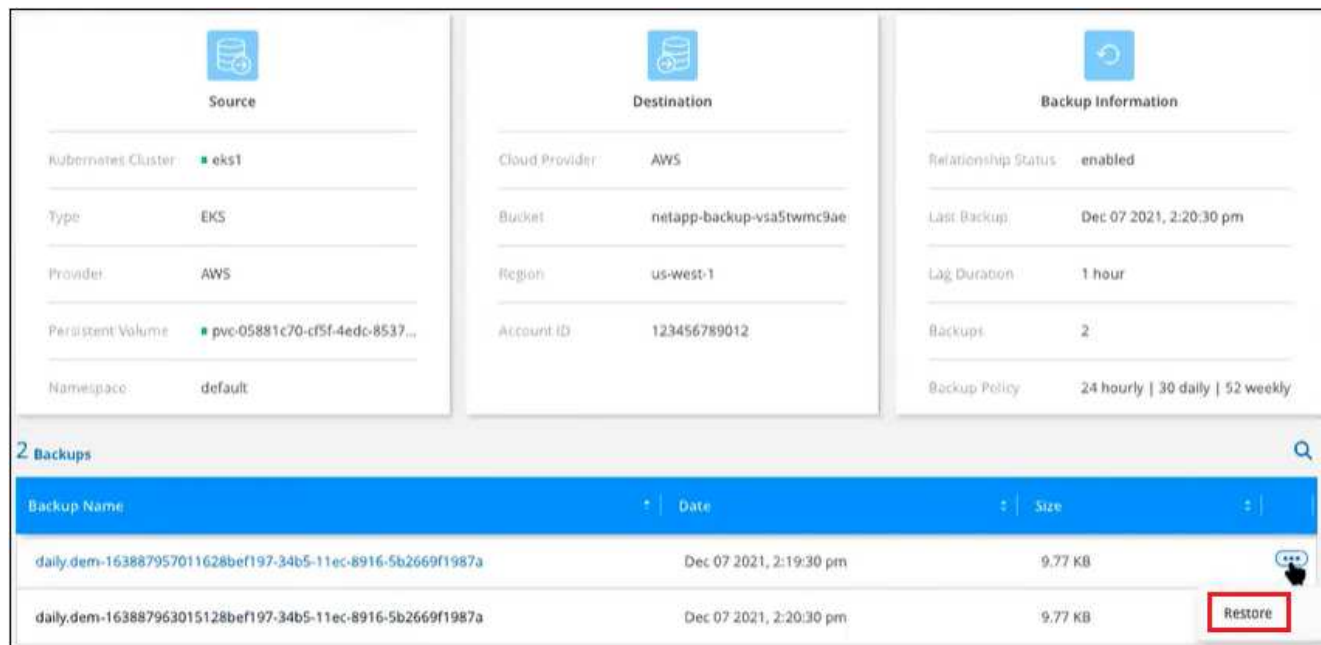
Fasi

1. Dal menu BlueXP, selezionare **protezione > Backup e ripristino**.
2. Fare clic sulla scheda **Kubernetes** per visualizzare la dashboard Kubernetes.



3. Individuare il volume che si desidera ripristinare, quindi fare clic su **...**, Quindi fare clic su **Details & Backup List**.

Viene visualizzato l'elenco di tutti i file di backup per quel volume, insieme ai dettagli relativi al volume di origine, alla posizione di destinazione e ai dettagli del backup.



4. Individuare il file di backup specifico che si desidera ripristinare in base alla data/ora, quindi fare clic su **...** e quindi **Restore**.
5. Nella pagina *Select Destination*, selezionare il cluster *Kubernetes* in cui si desidera ripristinare il volume, il *namespace*, la *Storage Class* e il nuovo *nome del volume persistente*.

Select Destination

Select Kubernetes Cluster

eks1

Namespace

default

Storage Class

basic

PVC Name

pvc-05881c70-cf5f-4edc-8537-a0a5ce36f9a1-restore

Cancel

Restore

6. Fare clic su **Restore** (Ripristina) per tornare alla dashboard di Kubernetes, in modo da esaminare l'avanzamento dell'operazione di ripristino.

Risultato

BlueXP crea un nuovo volume nel cluster Kubernetes in base al backup selezionato. È possibile ["gestire le impostazioni di backup per questo nuovo volume"](#) secondo necessità.

Informazioni sul copyright

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

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

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

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

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

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

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

Informazioni sul marchio commerciale

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