Backup und Wiederherstellung von Kubernetes-Daten

Cloud Backup

NetApp
December 15, 2022

Inhaltsverzeichnis

Backup und Wiederherstellung von Kubernetes-Daten 1
Kubernetes-Cluster-Daten mit Cloud Backup schützen 1
Sichern Sie persistente Kubernetes-Volume-Daten in Amazon S3 5
Das Backup-Management für Kubernetes-Systeme 11
Wiederherstellung von Kubernetes-Daten aus Backup-Dateien 21

Backup und Wiederherstellung von Kubernetes-Daten

Kubernetes-Cluster-Daten mit Cloud Backup schützen

Cloud Backup bietet Backup- und Restore-Funktionen zur Sicherung und zum langfristigen Archiv Ihrer Kubernetes-Cluster-Daten. Backups werden automatisch erstellt und in einem Objektspeicher in Ihrem Public oder Private Cloud-Konto gespeichert.

Bei Bedarf können Sie ein ganzes *Volume* von einem Backup in dieselbe oder andere Arbeitsumgebung wiederherstellen.

Funktionen

Backup-Funktionen:

- Sichern Sie unabhängige Kopien Ihrer persistenten Volumes auf kostengünstigem Objekt-Storage.
- Anwendung einer einzelnen Backup-Richtlinie auf alle Volumes in einem Cluster oder Zuweisen verschiedener Backup-Richtlinien zu Volumes mit eindeutigen Recovery-Punkten
- Backup-Daten werden mit AES-256-Bit-Verschlüsselung im Ruhezustand und TLS 1.2 HTTPS-Verbindungen im Übertragungsprozess gesichert.
- Unterstützung für bis zu 4,000 Backups eines einzelnen Volumes.

Wiederherstellungsfunktionen:

- Wiederherstellung von Daten aus einem bestimmten Zeitpunkt
- Stellen Sie ein Volume auf dem Quellsystem oder einem anderen System wieder her.
- Stellt Daten auf Blockebene wieder her, indem die Daten direkt an dem von Ihnen angegebenen Speicherort platziert werden, während gleichzeitig die ursprünglichen ACLs beibehalten werden.

Unterstützte Kubernetes-Arbeitsumgebungen und Objekt-Storage-Provider

Cloud Backup ermöglicht die Erstellung von Kubernetes Volumes aus den folgenden Arbeitsumgebungen in Objekt-Storage bei folgenden Public- und Private-Cloud-Providern:

Quelle Arbeitsumgebung	Ziel der Backup-Datei ifdef::aws[]
Kubernetes-Cluster in AWS	Amazon S3 endif::aws[] ifdef::Azure[]
Kubernetes-Cluster in Azure	Azure Blob endif::Azure[] ifdef::gcp[]
Kubernetes-Cluster in Google	Google Cloud Storage endif::gcp[]

Sie können ein Volume aus einer Kubernetes-Backup-Datei in den folgenden Arbeitsumgebungen wiederherstellen:

Speicherort Der Sicherungsdatei	Zielarbeitsumgebung ifdef::aws[]
Amazon S3	Kubernetes Cluster in AWS endif::AWS[] ifdef::Azure[]

Speicherort Der Sicherungsdatei	Zielarbeitsumgebung ifdef::aws[]
Azure Blob	Kubernetes Cluster in Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Kubernetes Cluster in Google endif::gcp[]

Kosten

Mit Cloud Backup fallen zwei Kostenarten in Verbindung: Ressourcengebühren und Servicegebühren.

Ressourcengebühren

Ressourcengebühren werden beim Cloud-Provider für Objekt-Storage-Kapazität in der Cloud gezahlt. Da Cloud Backup die Storage-Effizienzfunktionen des Quell-Volume beibehalten, bezahlen Sie die Objekt-Storage-Kosten des Cloud-Providers für die Daten *nach* ONTAP-Effizienz (für die geringere Datenmenge, die nach der Deduplizierung und Komprimierung angewendet wurde).

Servicegebühren

Servicegebühren werden an NetApp gezahlt und decken sowohl die Kosten für die Erstellung *Backups* Backups und *Wiederherstellung* Volumes aus diesen Backups ab. Sie bezahlen nur die Daten, die Sie sichern, berechnet anhand der verwendeten logischen Quellkapazität (*before* ONTAP-Effizienzfunktionen) der Volumes, die im Objekt-Storage gesichert werden. Diese Kapazität wird auch als Front-End Terabyte (FETB) bezeichnet.

Es gibt zwei Möglichkeiten, für den Backup-Service zu bezahlen. Als erste Option können Sie Ihren Cloud-Provider abonnieren, sodass Sie monatlich bezahlen können. Die zweite Option besteht darin, Lizenzen direkt von NetApp zu erwerben. Lesen Sie die Lizenzierung Weitere Informationen finden Sie in diesem Abschnitt.

Lizenzierung

Cloud Backup ist in zwei Lizenzoptionen erhältlich: Pay-as-you-go (PAYGO) und Bring-Your-Own-License (BYOL). Eine kostenlose 30-Tage-Testversion ist verfügbar, wenn Sie keine Lizenz haben.

Kostenlose Testversion

Wenn Sie die kostenlose 30-Tage-Testversion verwenden, werden Sie über die Anzahl der kostenlosen Testtage informiert, die noch verbleiben. Am Ende Ihrer kostenlosen Testversion werden Backups nicht mehr erstellt. Sie müssen den Service abonnieren oder eine Lizenz erwerben, um den Service weiterhin nutzen zu können.

Sicherungsdateien werden nicht gelöscht, wenn der Dienst deaktiviert ist. Cloud-Provider stellen weiterhin die Kosten für Objekt-Storage für die von Ihren Backups verwendete Kapazität in Rechnung, es sei denn, die Backups werden gelöscht.

Pay-as-you-go-Abonnement

Cloud Backup bietet eine nutzungsbasierte Lizenzierung in einem Pay-as-you-go-Modell. Nachdem Sie sich über den Marktplatz Ihres Cloud-Providers registriert haben, zahlen Sie pro GB für gesicherte Daten – there keine Vorauszahlung. Die Abrechnung erfolgt von Ihrem Cloud-Provider über Ihre monatliche Abrechnung.

Sie sollten sich auch dann abonnieren, wenn Sie eine kostenlose Testversion haben oder Ihre eigene Lizenz mitbringen (BYOL):

- Das Abonnieren sorgt dafür, dass es keine Serviceunterbrechung gibt, nachdem Ihre kostenlose Testversion endet.

  Wenn die Studie endet, werden Sie stündlich nach der Menge der Daten, die Sie sichern berechnet.

- Wenn Sie mehr Daten als mit Ihrer BYOL-Lizenz zulässig sichern, wird das Daten-Backup über Ihr Pay-as-you-go-Abonnement fortgesetzt.

  Wenn Sie beispielsweise eine 10-TB-BYOL-Lizenz haben, wird die gesamte Kapazität über 10 TB hinaus über das PAYGO Abonnement abgerechnet.

Sie werden nicht von Ihrem Pay-as-you-go-Abonnement während der kostenlosen Testversion oder wenn Sie nicht überschritten haben Ihre Byol-Lizenz.

"Erfahren Sie, wie Sie ein Pay-as-you-go-Abonnement einrichten".

Mit Ihrer eigenen Lizenz

Byol ist nach Terminus basiert (12, 24 oder 36 Monate) *und* kapazitätsbasiert in Schritten von 1 TB. Sie bezahlen NetApp für einen Zeitraum, sagen wir, 1 Jahr und für eine maximale Kapazität, sagen wir 10 TB.

Sie erhalten eine Seriennummer, die Sie auf der Seite BlueXP Digital Wallet eingeben, um den Dienst zu aktivieren. Wenn eine der beiden Limits erreicht ist, müssen Sie die Lizenz erneuern. Die BYOL-Lizenz für Backup gilt für alle mit dem verbundenen Quellsysteme "BlueXP-Konto".

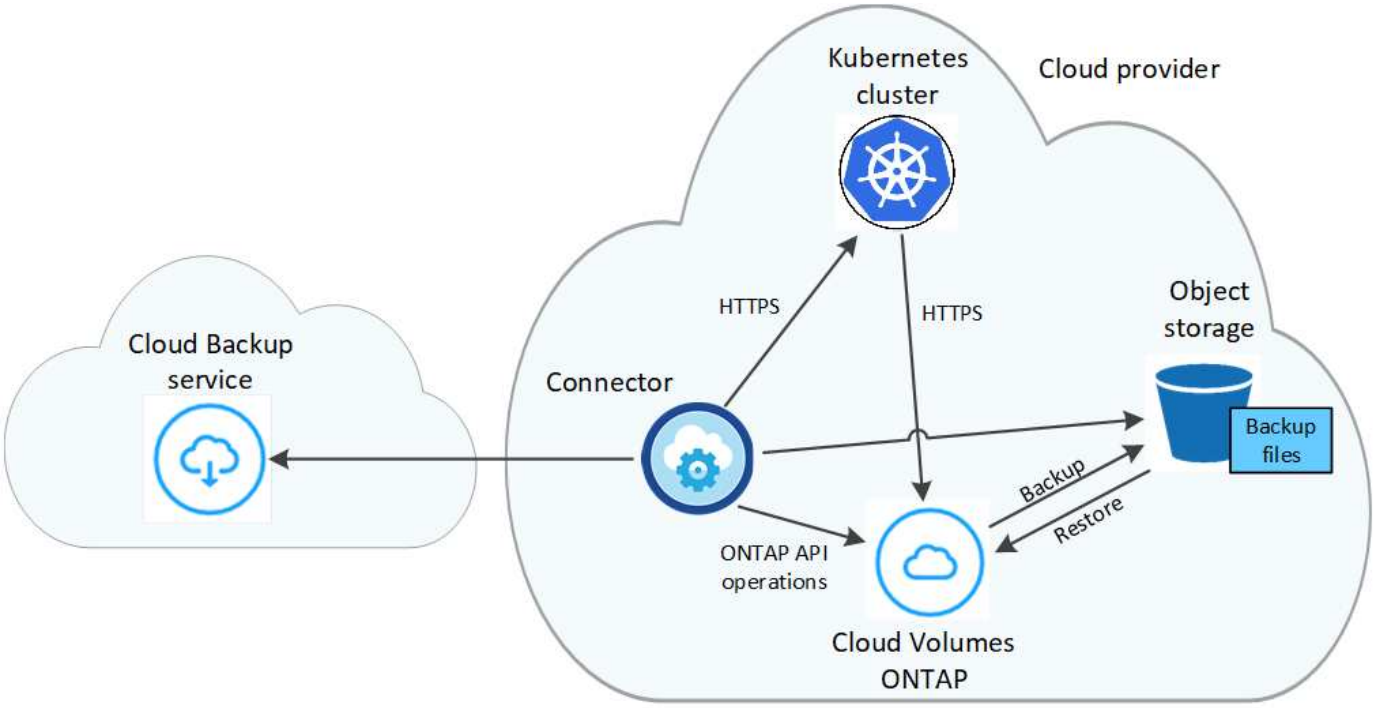
"Erfahren Sie, wie Sie Ihre BYOL-Lizenzen managen".

Funktionsweise von Cloud Backup

Wenn Sie Cloud-Backup auf einem Kubernetes-System aktivieren, führt der Service ein vollständiges Backup Ihrer Daten durch. Nach dem ersten Backup sind alle weiteren Backups inkrementell, das heißt, dass nur geänderte Blöcke und neue Blöcke gesichert werden. Dadurch wird der Netzwerkverkehr auf ein Minimum reduziert.

Alle Aktionen, die direkt aus Ihrer Cloud-Provider-Umgebung zum Verwalten oder Ändern von Backup-Dateien übernommen werden, können die Dateien beschädigen und führen zu einer nicht unterstützten Konfiguration.

Die folgende Abbildung zeigt die Beziehung zwischen den einzelnen Komponenten:



Unterstützte Storage-Klassen oder Zugriffsebenen

- In AWS beginnen Backups in der Klasse „ *Standard* Storage“ und wechseln nach 30 Tagen in die Storage-Klasse „ *Standard-infrequent Access*“.

Individuell anpassbare Backup-Zeitpläne und Aufbewahrungseinstellungen pro Cluster

Wenn Sie Cloud-Backup für eine Arbeitsumgebung aktivieren, werden alle Volumes, die Sie anfangs auswählen, mithilfe der definierten Standard-Backup-Richtlinie gesichert. Um bestimmten Volumes mit verschiedenen Recovery Point Objectives (RPOs) unterschiedliche Backup-Richtlinien zuzuweisen, können Sie zusätzliche Richtlinien für diesen Cluster erstellen und diese Richtlinien anderen Volumes zuweisen.

Es steht eine Kombination aus stündlichen, täglichen, wöchentlichen und monatlichen Backups aller Volumes zur Verfügung.

Sobald Sie die maximale Anzahl von Backups für eine Kategorie oder ein Intervall erreicht haben, werden ältere Backups entfernt, sodass Sie immer über die aktuellsten Backups verfügen.

Unterstützte Volumes

Cloud Backup unterstützt persistente Volumes (PVS).

Einschränkungen

- Wenn eine Backup-Richtlinie erstellt oder bearbeitet wird, wenn dieser Richtlinie keine Volumes zugewiesen werden, kann die Anzahl der zurückbehaltenen Backups maximal 1018 sein. Als Workaround können Sie die Anzahl der Backups zur Erstellung der Richtlinie verringern. Anschließend können Sie die Richtlinie bearbeiten, um bis zu 4000 Backups zu erstellen, nachdem Sie der Richtlinie Volumes zugewiesen haben.
- Ad-hoc-Volume-Backups mit dem Button **Backup Now** werden auf Kubernetes-Volumes nicht unterstützt.

Sichern Sie persistente Kubernetes-Volume-Daten in Amazon S3

Führen Sie einige Schritte aus, um die Datensicherung von Daten der persistenten Volumes auf EKS Kubernetes-Clustern in Amazon S3 Storage zu starten.

Schnellstart

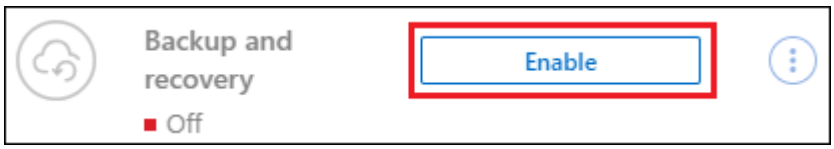
Führen Sie diese Schritte schnell durch, oder scrollen Sie nach unten zu den verbleibenden Abschnitten, um ausführliche Informationen zu erhalten.

1 Voraussetzungen prüfen

- Sie haben den Kubernetes Cluster als BlueXP-Arbeitsumgebung erkannt.
  - Trident muss auf dem Cluster installiert sein, und die Trident Version muss mindestens 21.1 sein.
  - Alle PVCs, die verwendet werden sollen, um persistente Volumes zu erstellen, die Sie sichern möchten, müssen „Snapshot Policy“ auf „Standard“ gesetzt sein.
  - Der Cluster muss für seinen Back-End Storage Cloud Volumes ONTAP on AWS verwenden.
  - Das Cloud Volumes ONTAP System muss ONTAP 9.7P5 oder höher ausführen.
- Sie verfügen über ein gültiges Cloud-Provider-Abonnement für den Speicherplatz, auf dem sich Ihre Backups befinden.
- Sie haben sich für das angemeldet "BlueXP Marketplace Backup-Angebot", An "AWS Jahresvertrag", Oder Sie haben gekauft "Und aktiviert" Eine Cloud Backup BYOL-Lizenz von NetApp
- Die IAM-Rolle, die den BlueXP Connector mit Berechtigungen bereitstellt, umfasst die neuesten S3-Berechtigungen "BlueXP-Richtlinie".

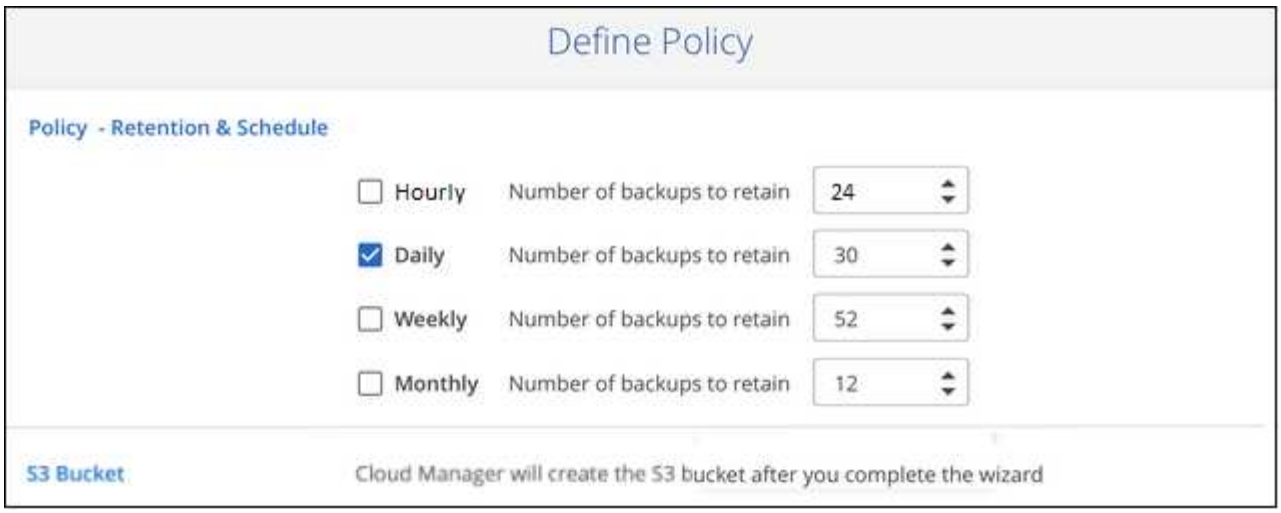
2 Cloud Backup für bestehenden Kubernetes Cluster aktivieren

Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren** neben dem Backup- und Recovery-Dienst im rechten Fenster, und folgen Sie dann dem Setup-Assistenten.



3 Definieren der Backup-Richtlinie

Die Standardrichtlinie sichert Volumes täglich und speichert die letzten 30 Backup-Kopien jedes Volumes. Wechseln Sie zu stündlichen, täglichen, wöchentlichen oder monatlichen Backups oder wählen Sie eine der systemdefinierten Richtlinien aus, die mehr Optionen bieten. Sie können auch die Anzahl der zu behaltenden Backup-Kopien ändern.



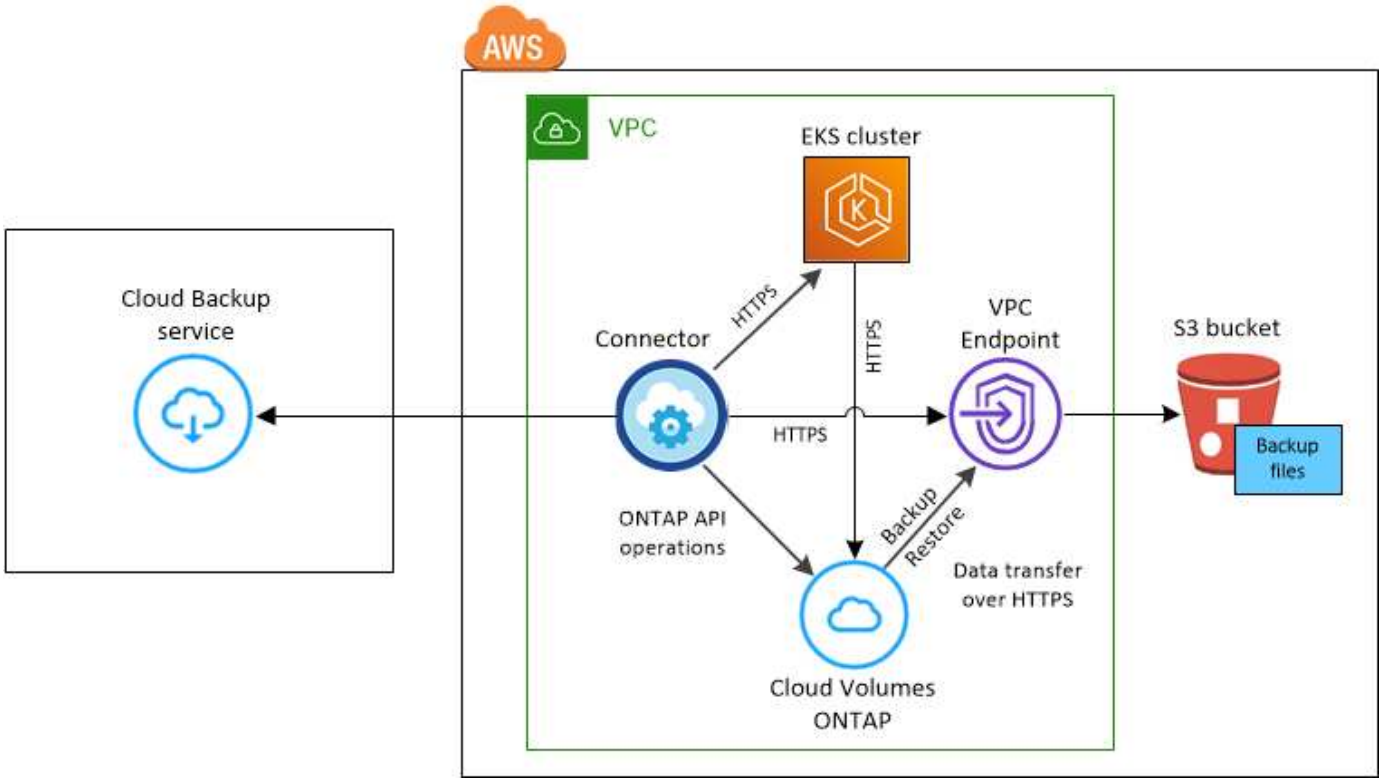
4 **Wählen Sie die Volumes aus, die Sie sichern möchten**

Legen Sie fest, welche Volumes Sie in der Seite Volumes auswählen sichern möchten. Ein S3-Bucket wird automatisch im selben AWS-Konto und in derselben Region wie das Cloud Volumes ONTAP System erstellt und die Backup-Dateien dort gespeichert.

Anforderungen

Lesen Sie die folgenden Anforderungen, um sicherzustellen, dass Sie über eine unterstützte Konfiguration verfügen, bevor Sie mit dem Backup persistenter Kubernetes-Volumes in S3 beginnen.

Die folgende Abbildung zeigt die einzelnen Komponenten und die Verbindungen, die zwischen den Komponenten vorbereitet werden müssen:



Der VPC Endpunkt ist optional.

Kubernetes-Cluster-Anforderungen

- Sie haben den Kubernetes Cluster als BlueXP-Arbeitsumgebung erkannt. "Erkennung des Kubernetes-Clusters".
- Trident muss auf dem Cluster installiert werden, und die Trident Version muss mindestens 21.1 sein. Siehe "Anleitung zur Installation von Trident" Oder "So aktualisieren Sie die Trident Version".
- Der Cluster muss für seinen Back-End Storage Cloud Volumes ONTAP on AWS verwenden.
- Das Cloud Volumes ONTAP System muss sich in derselben AWS Region wie der Kubernetes-Cluster befinden. Es muss ONTAP 9.7P5 oder höher ausgeführt werden (ONTAP 9.8P11 und höher wird empfohlen).

  Beachten Sie, dass Kubernetes-Cluster an On-Premises-Standorten nicht unterstützt werden. Es werden nur Kubernetes-Cluster in Cloud-Implementierungen unterstützt, die Cloud Volumes ONTAP Systeme nutzen.

- Für alle Persistent Volume Claim-Objekte, die zum Erstellen der persistenten Volumes verwendet werden sollen, die Sie sichern möchten, muss „Snapshot Policy“ auf „Standard“ gesetzt sein.

  Sie können dies für einzelne VES tun, indem Sie hinzufügen `snapshotPolicy` Unter Anmerkungen:

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

  Sie können dies für alle VES, die mit einem bestimmten Back-End-Speicher verknüpft sind, tun, indem Sie die hinzufügen `snapshotPolicy` Feld unter den Standardeinstellungen im `backend.json` Datei:

```
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
```

Lizenzanforderungen

Für Cloud Backup PAYGO-Lizenzen ist im AWS Marketplace ein Abonnement verfügbar, das die Implementierung von Cloud Volumes ONTAP und Cloud Backup ermöglicht. Sie müssen "Melden Sie sich für dieses BlueXP-Abonnement an" Vor Aktivierung von Cloud Backup: Die Abrechnung für Cloud Backup erfolgt über dieses Abonnement.

Bei einem Jahresvertrag, mit dem Sie sowohl Cloud Volumes ONTAP Daten als auch ONTAP Daten vor Ort sichern können, müssen Sie den Abonnement von abonnieren "AWS Marketplace Seite" Und dann "Verbinden Sie das Abonnement mit Ihren AWS Zugangsdaten".

Für einen Jahresvertrag, mit dem Sie Cloud Volumes ONTAP und Cloud Backup bündeln können, müssen Sie bei der Erstellung einer Cloud Volumes ONTAP Arbeitsumgebung den Jahresvertrag abschließen. Mit dieser Option können Sie Backups von Daten vor Ort nicht erstellen.

Für die BYOL-Lizenzierung von Cloud Backup benötigen Sie die Seriennummer von NetApp, mit der Sie den Service für die Dauer und die Kapazität der Lizenz nutzen können. "Erfahren Sie, wie Sie Ihre BYOL-Lizenzen managen".

Zudem benötigen Sie ein AWS-Konto für den Speicherplatz, auf dem sich Ihre Backups befinden.

Unterstützte AWS-Regionen

Cloud Backup wird in allen AWS Regionen unterstützt "Wobei Cloud Volumes ONTAP unterstützt wird".

AWS Backup Berechtigungen erforderlich

Die IAM-Rolle, die BlueXP Berechtigungen bereitstellt, muss die neuesten S3-Berechtigungen enthalten "BlueXP-Richtlinie".

Im Folgenden sind die spezifischen S3 Berechtigungen aus der Richtlinie aufgeführt:

```
{
            "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-*"
            ]
        },
```

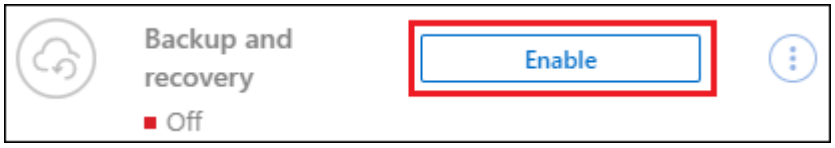
Unterstützung Von Cloud Backup

Cloud-Backup kann jederzeit direkt aus der Kubernetes-Arbeitsumgebung aktiviert werden.

Schritte

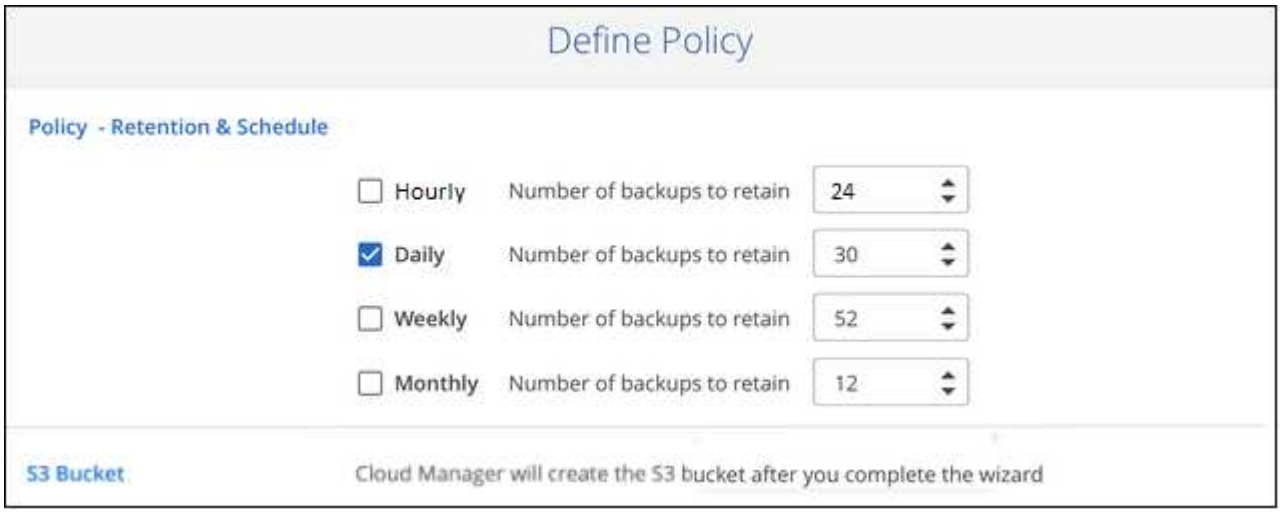
1. Wählen Sie die Arbeitsumgebung aus und klicken Sie auf **Aktivieren** neben dem Backup- und Recovery-Dienst im rechten Fenster.

   Wenn das Amazon S3 Ziel für Ihre Backups als Arbeitsumgebung auf dem Canvas existiert, können Sie das Kubernetes-Cluster in die Amazon S3-Arbeitsumgebung ziehen, um den Setup-Assistenten zu starten.

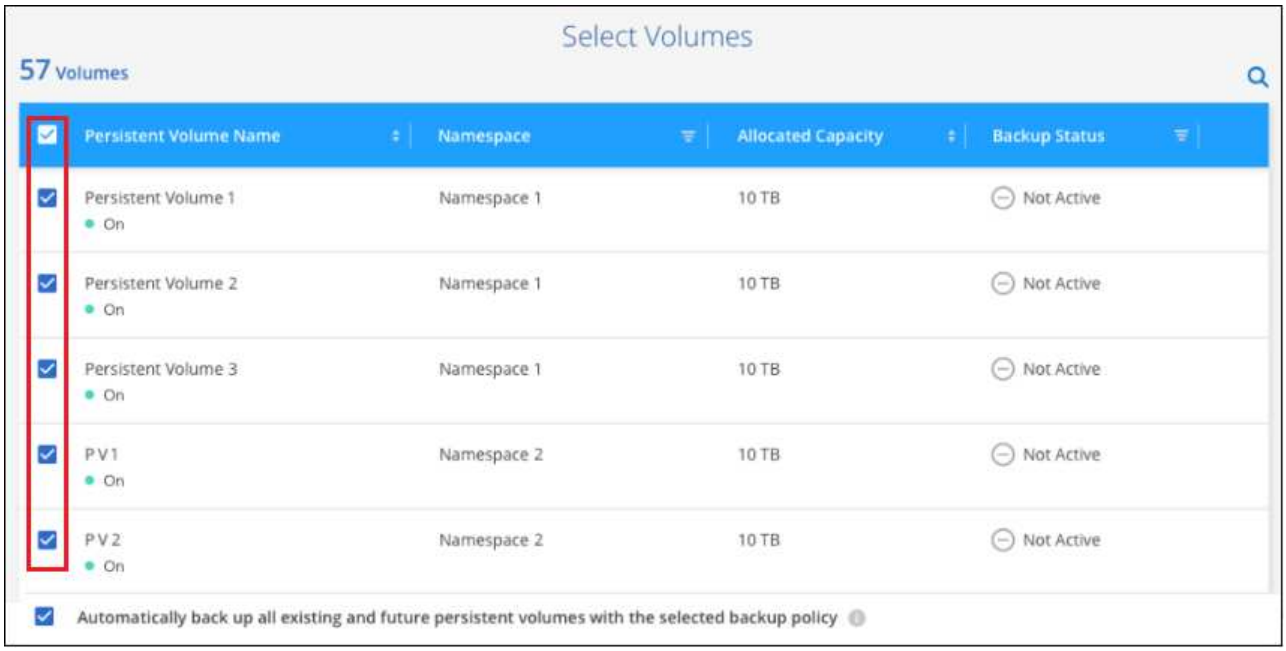


2. Geben Sie die Backup Policy Details ein und klicken Sie auf **Weiter**.

   Sie können den Backup-Zeitplan festlegen und die Anzahl der zu behaltenden Backups auswählen.



3. Wählen Sie die persistenten Volumes aus, die Sie sichern möchten.
   - Um alle Volumes zu sichern, aktivieren Sie das Kontrollkästchen in der Titelzeile (Volume Name).
   - Um einzelne Volumes zu sichern, aktivieren Sie das Kontrollkästchen für jedes Volume (Volume_1).



4. Wenn Sie möchten, dass alle aktuellen und zukünftigen Volumes Backups aktiviert sind, lassen Sie einfach das Kontrollkästchen „zukünftige Volumes automatisch sichern…“ aktiviert. Wenn Sie diese Einstellung deaktivieren, müssen Sie manuell Backups für zukünftige Volumes aktivieren.
5. Klicken Sie auf **Activate Backup** und Cloud Backup beginnt die Erstellung der ersten Backups jedes ausgewählten Volumes.

Ergebnis

Ein S3-Bucket wird automatisch im selben AWS-Konto und in derselben Region wie das Cloud Volumes ONTAP System erstellt und die Backup-Dateien dort gespeichert.

Das Kubernetes Dashboard wird angezeigt, damit Sie den Status der Backups überwachen können.

Was kommt als Nächstes?

Das können Sie "Starten und Stoppen von Backups für Volumes oder Ändern des Backup-Zeitplans". Das können Sie auch "Wiederherstellung vollständiger Volumes aus einer Backup-Datei" Für ein neues Volume auf demselben oder einem anderen Kubernetes-Cluster in AWS (in derselben Region)

Das Backup-Management für Kubernetes-Systeme

Backups für Kubernetes-Systeme lassen sich verwalten, indem der Backup-Zeitplan geändert, Volume-Backups aktiviert/deaktiviert, Backups gelöscht usw.

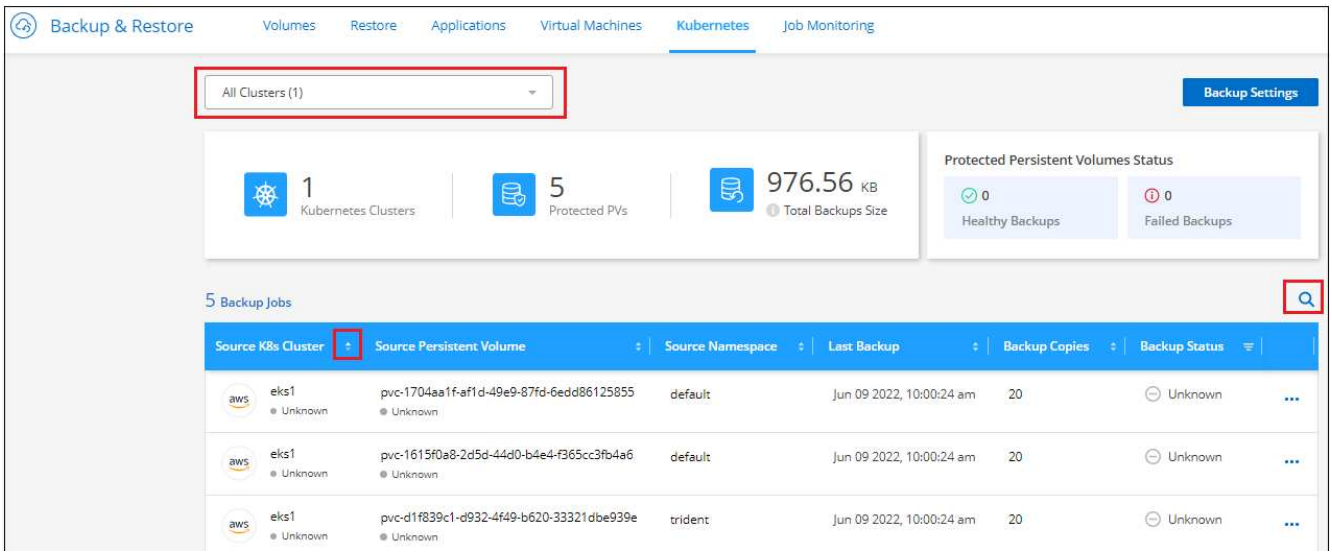
Backup-Dateien lassen sich nicht direkt in der Umgebung Ihrer Cloud-Provider managen oder ändern. Dies kann die Dateien beschädigen und zu einer nicht unterstützten Konfiguration führen.

Anzeigen der Volumes, die gesichert werden

Sie können eine Liste aller Volumes anzeigen, die derzeit durch Cloud Backup gesichert werden.

Schritte

1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Kubernetes**, um eine Liste der persistenten Volumes für Kubernetes-Systeme anzuzeigen.



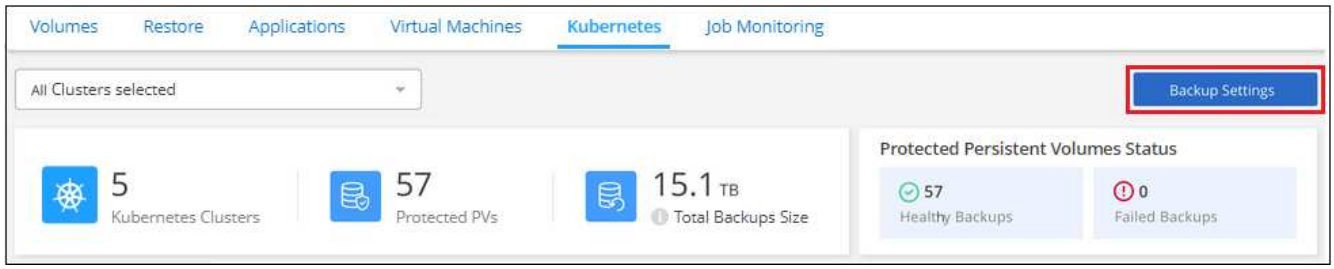
Wenn Sie in bestimmten Clustern nach bestimmten Volumes suchen, können Sie die Liste nach Cluster und Volume verfeinern oder Sie verwenden den Suchfilter.

Aktivieren und Deaktivieren von Backups von Volumes

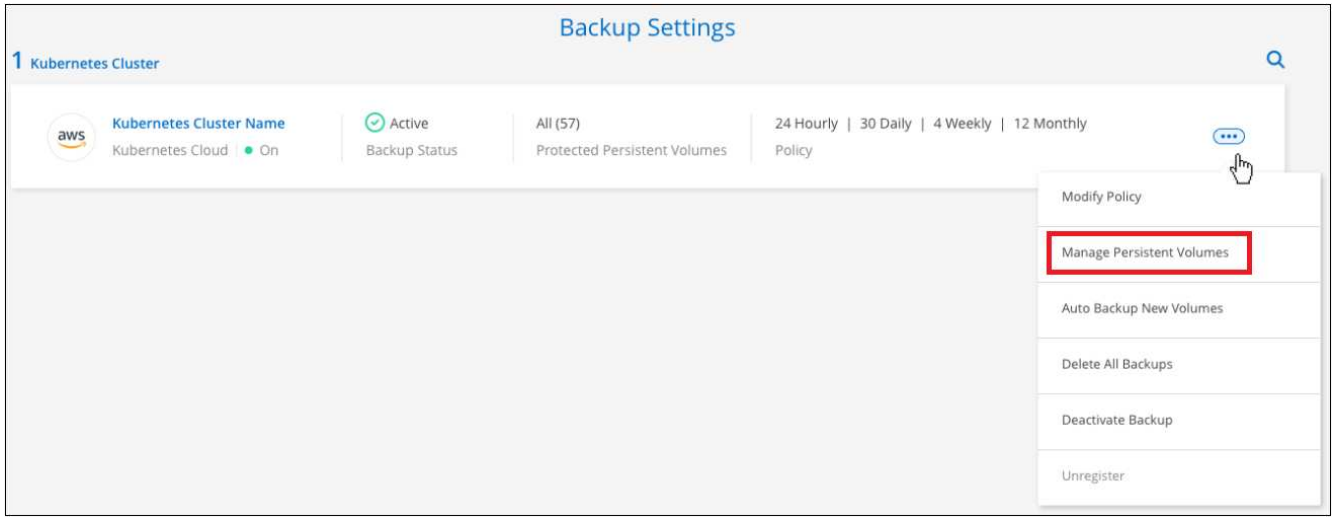
Sie können die Sicherung eines Volumes anhalten, wenn Sie keine Backup-Kopien dieses Volumes benötigen und nicht für die Kosten für die Speicherung der Backups bezahlen möchten. Sie können auch ein neues Volume zur Backup-Liste hinzufügen, wenn das Volume derzeit nicht gesichert wird.

Schritte

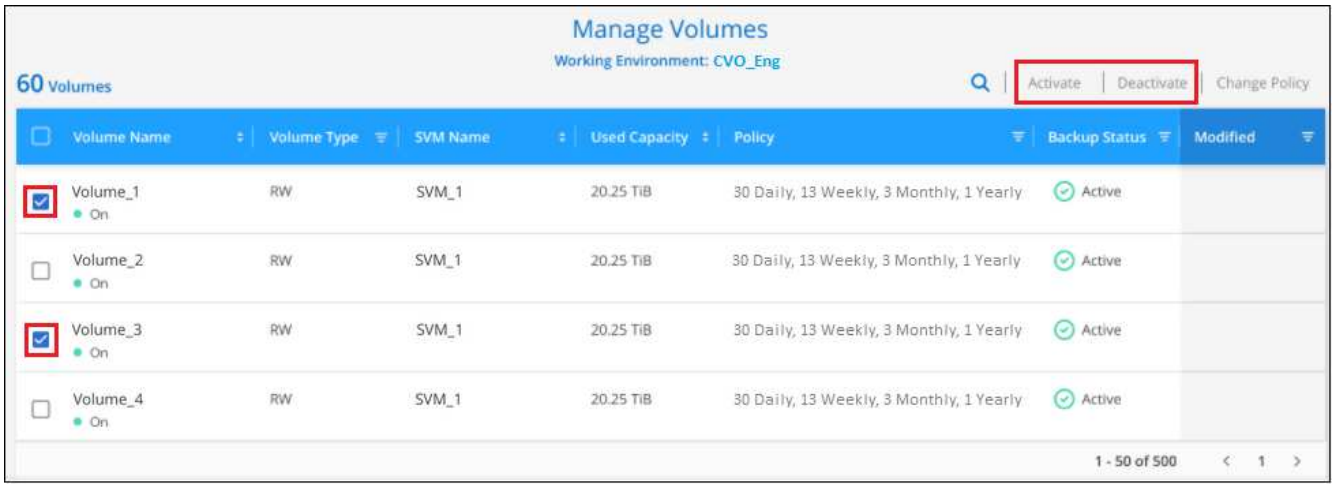
1. Wählen Sie auf der Registerkarte **Kubernetes** die Option **Backup-Einstellungen** aus.



2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für den Kubernetes-Cluster **Persistent Volumes** managen aus.



3. Aktivieren Sie das Kontrollkästchen für ein Volume oder ein Volume, das Sie ändern möchten, und klicken Sie dann auf **Aktivieren** oder **Deaktivieren**, je nachdem, ob Sie Backups für das Volume starten oder beenden möchten.



4. Klicken Sie auf **Speichern**, um Ihre Änderungen zu speichern.

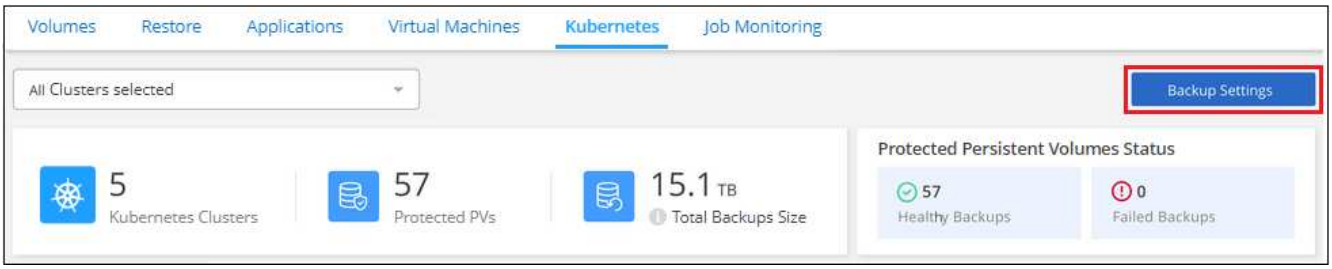
Hinweis: Wenn ein Volume nicht gesichert werden soll, werden Sie Ihrem Cloud Provider weiterhin die Kosten für die Objektspeicherung für die Kapazität in Rechnung gestellt, die die Backups nutzen, es sei denn, Sie Löschen Sie die Backups.

Bearbeiten einer vorhandenen Backup-Richtlinie

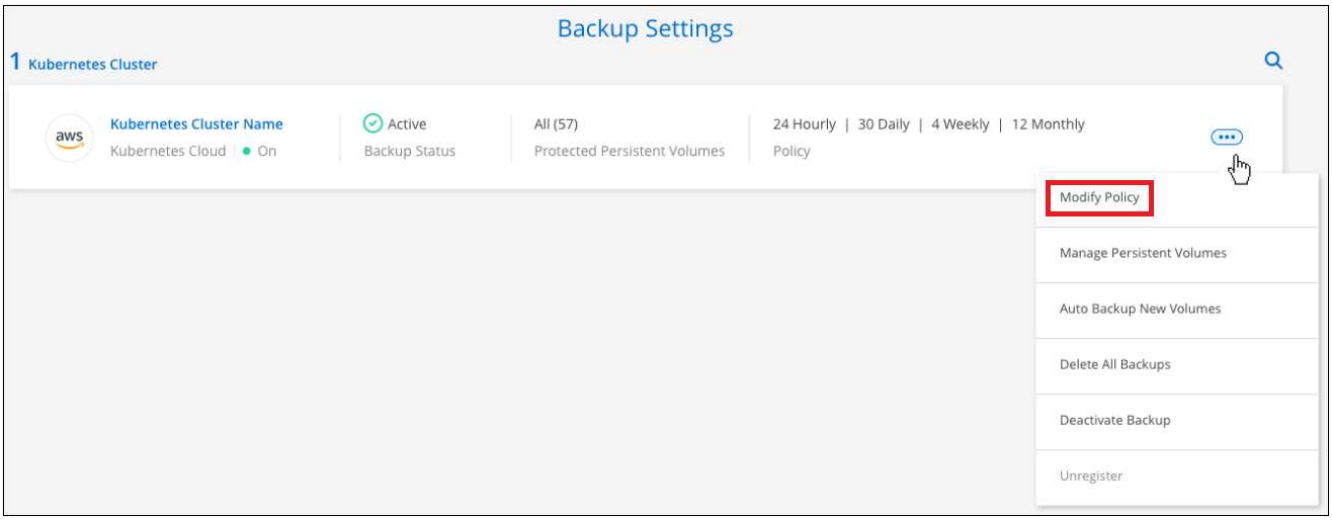
Sie können die Attribute für eine Backup-Richtlinie ändern, die derzeit auf Volumes in einer Arbeitsumgebung angewendet wird. Die Änderung der Backup-Richtlinie wirkt sich auf alle vorhandenen Volumes aus, die diese Richtlinie verwenden.

Schritte

1. Wählen Sie auf der Registerkarte **Kubernetes** die Option **Backup-Einstellungen** aus.

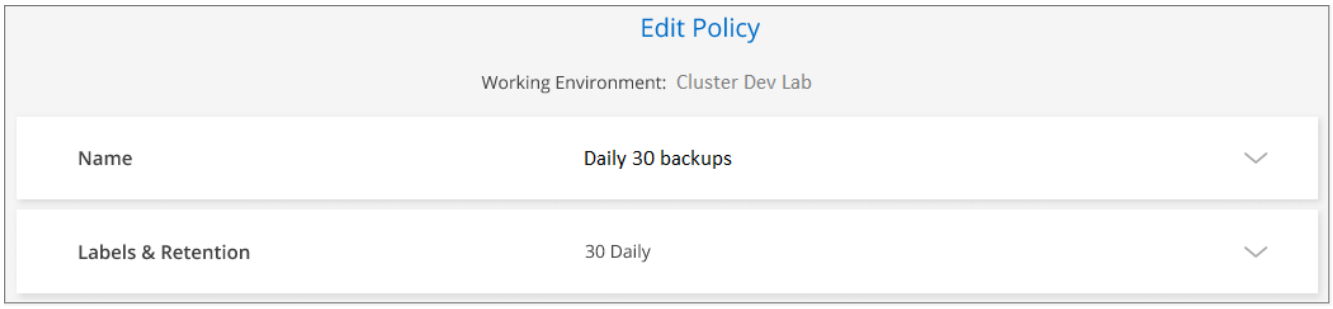


2. Klicken Sie auf der Seite „ Backup Settings_“ auf ••• Wählen Sie für die Arbeitsumgebung, in der Sie die Einstellungen ändern möchten, und wählen Sie **Richtlinien verwalten**.



3. Klicken Sie auf der Seite *Manage Policies* auf **Edit Policy** für die Backup Policy, die Sie in dieser Arbeitsumgebung ändern möchten.

4. Ändern Sie auf der Seite *Edit Policy* den Zeitplan und die Backup-Aufbewahrung und klicken Sie auf **Save**.



Legen Sie eine Backup-Richtlinie fest, die neuen Volumes zugewiesen werden soll

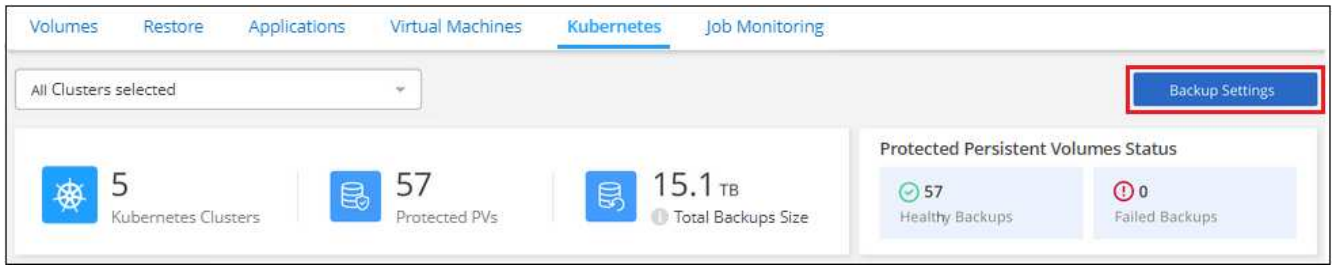
Falls Sie beim ersten Aktivieren von Cloud Backup auf Ihrem Kubernetes Cluster nicht die Option zum automatischen Zuweisen einer Backup-Richtlinie zu neu erstellten Volumes gewählt haben, können Sie diese Option später auf der Seite „*Backup Settings* “ auswählen. Eine Backup-Richtlinie, die neu erstellten Volumes zugewiesen wurde, stellt sicher, dass alle Ihre Daten geschützt sind.

Beachten Sie, dass die Richtlinie, die Sie auf die Volumes anwenden möchten, bereits vorhanden sein muss. Erfahren Sie, wie Sie eine neue Backup-Richtlinie für eine Arbeitsumgebung hinzufügen.

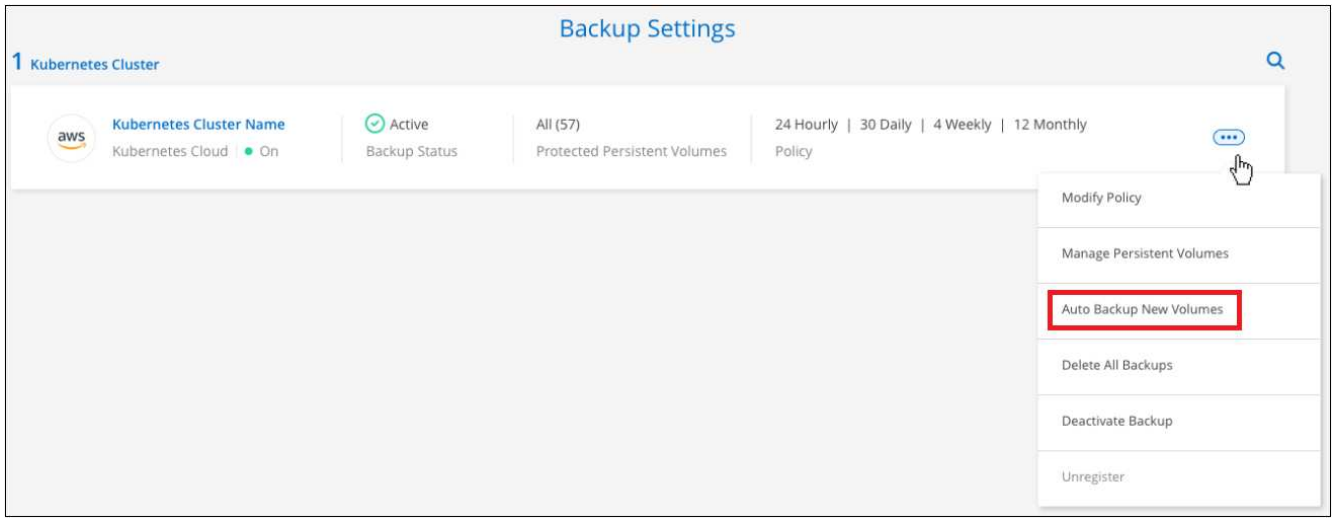
Sie können diese Einstellung auch deaktivieren, damit neu erstellte Volumes nicht automatisch gesichert werden. In diesem Fall müssen Sie Backups manuell für alle spezifischen Volumes aktivieren, die Sie in Zukunft sichern möchten.

Schritte

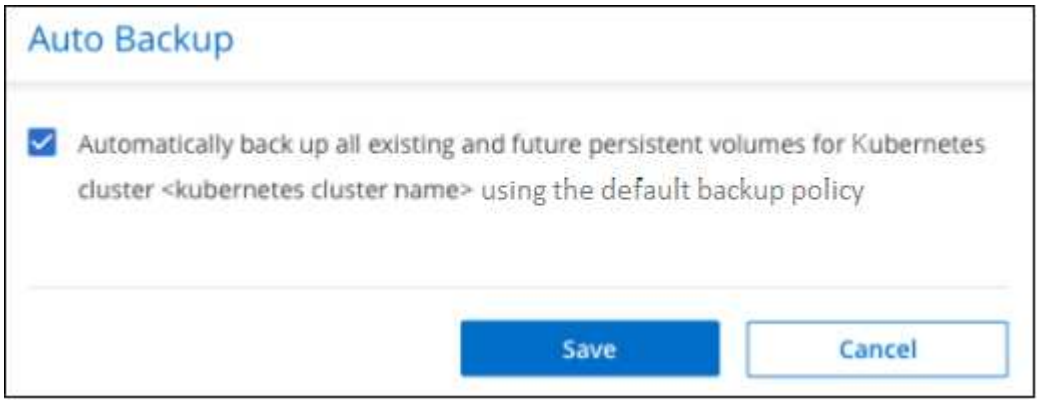
1. Wählen Sie auf der Registerkarte **Kubernetes** die Option **Backup-Einstellungen** aus.



2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Wählen Sie für den Kubernetes-Cluster, in dem die Volumes vorhanden sind, **Auto Backup New Volumes** aus.



3. Aktivieren Sie das Kontrollkästchen „künftige persistente Volumes automatisch sichern…“, wählen Sie die Backup-Richtlinie aus, die Sie auf neue Volumes anwenden möchten, und klicken Sie auf **Speichern**.



Ergebnis

Diese Backup-Richtlinie wird nun auf alle neuen Volumes angewendet, die in diesem Kubernetes Cluster erstellt wurden.

Anzeigen der Liste der Backups für jedes Volume

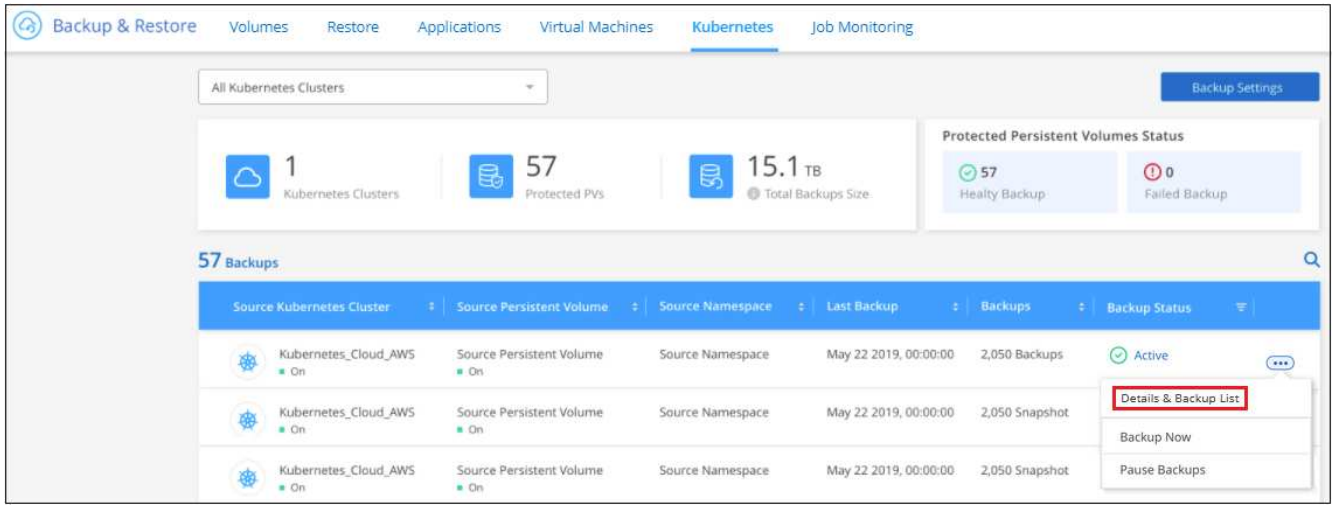
Sie können eine Liste aller Backup-Dateien anzeigen, die für jedes Volume vorhanden sind. Auf dieser Seite werden Details zum Quell-Volume, zum Zielort und zu Backup-Details wie zum Beispiel zum letzten Backup, zur aktuellen Backup-Richtlinie, zur Größe der Sicherungsdatei und mehr angezeigt.

Auf dieser Seite können Sie außerdem die folgenden Aufgaben ausführen:

- Löschen Sie alle Sicherungsdateien für das Volume
- Löschen einzelner Backup-Dateien für das Volume
- Backup-Bericht für das Volume herunterladen

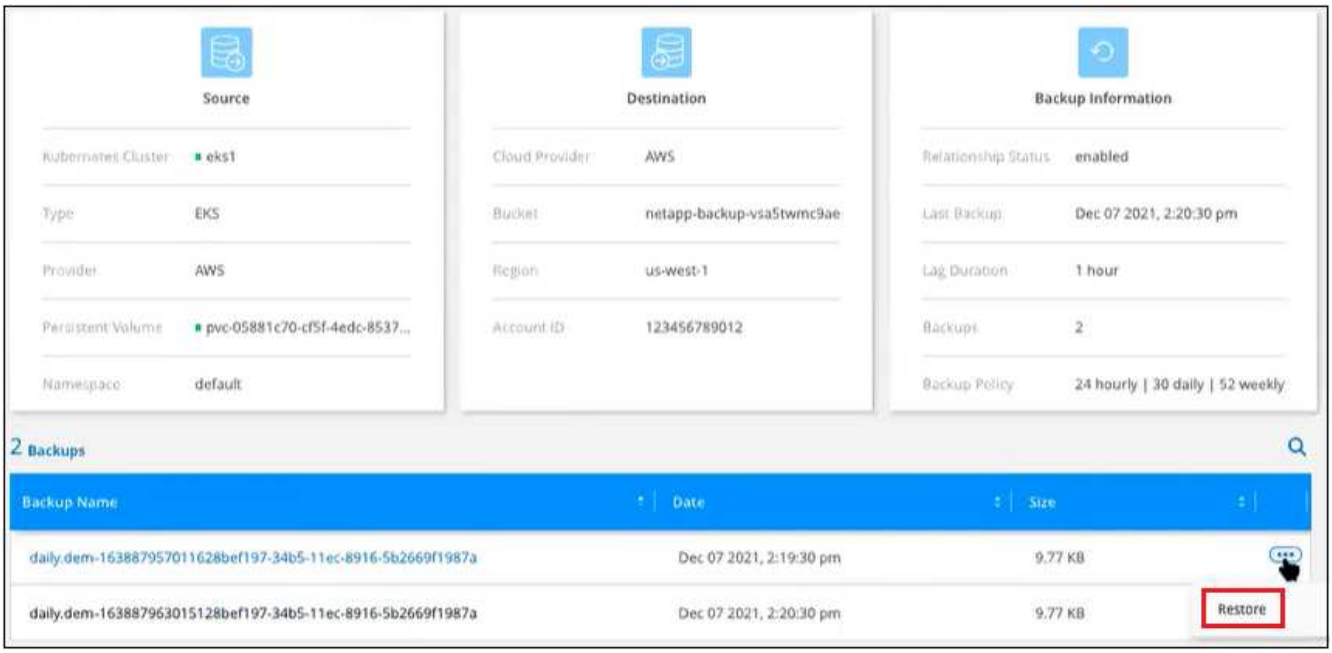
Schritte

1. Klicken Sie auf der Registerkarte **Kubernetes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.



Die Liste aller Sicherungsdateien wird zusammen mit Details zum Quell-Volume, dem Zielspeicherort und

Backup-Details angezeigt.



Backups werden gelöscht

Cloud Backup ermöglicht die Löschung einer einzelnen Backup-Datei, das Löschen aller Backups für ein Volume oder das Löschen aller Backups aller Volumes in einem Kubernetes Cluster. Sie können alle Backups löschen, wenn Sie die Backups nicht mehr benötigen oder wenn Sie das Quell-Volume gelöscht haben und alle Backups entfernen möchten.

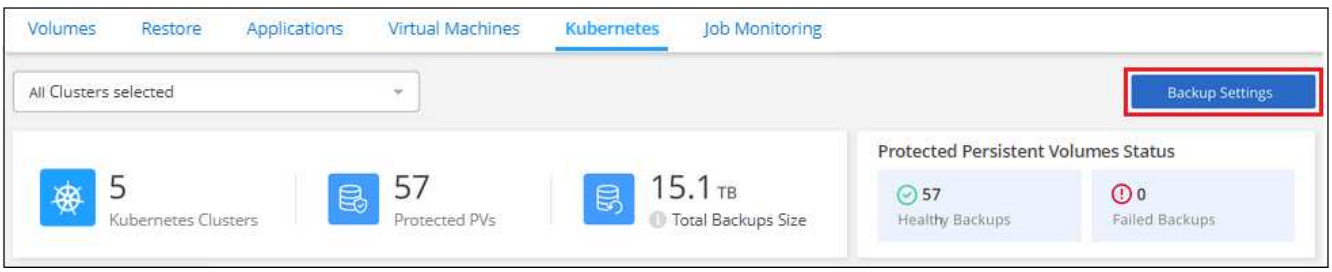
Wenn Sie planen, eine Arbeitsumgebung oder ein Cluster mit Backups zu löschen, müssen Sie die Backups *löschen, bevor Sie das System löschen. Cloud Backup nicht automatisch löschen Backups, wenn Sie ein System löschen, und es gibt keine aktuelle Unterstützung in der UI, die Backups zu löschen, nachdem das System gelöscht wurde. Für alle verbleibenden Backups werden weiterhin die Kosten für Objekt-Storage in Rechnung gestellt.

Löschen aller Sicherungsdateien für eine Arbeitsumgebung

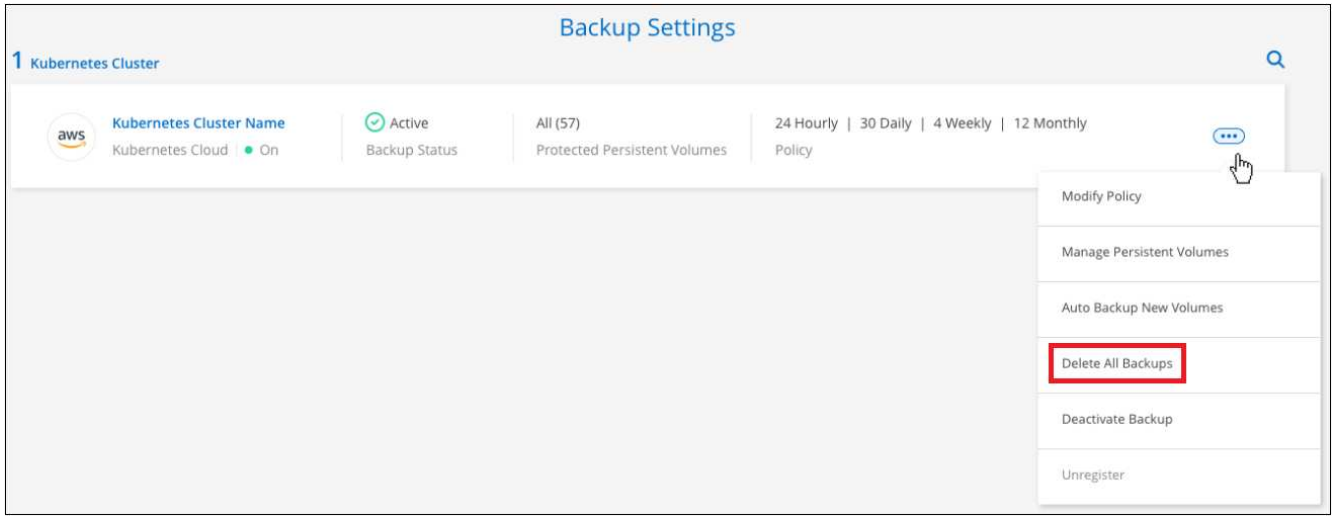
Durch das Löschen aller Backups für eine Arbeitsumgebung werden keine zukünftigen Backups von Volumes in dieser Arbeitsumgebung deaktiviert. Wenn Sie die Erstellung von Backups aller Volumes in einer Arbeitsumgebung beenden möchten, können Sie Backups deaktivieren Wie hier beschrieben.

Schritte

1. Wählen Sie auf der Registerkarte **Kubernetes** die Option **Backup-Einstellungen** aus.



2. Klicken Sie Auf ••• Für den Kubernetes-Cluster, wo Sie alle Backups löschen und wählen Sie **Alle Backups löschen**.



3. Geben Sie im Bestätigungsdialogfeld den Namen der Arbeitsumgebung ein und klicken Sie auf **Löschen**.

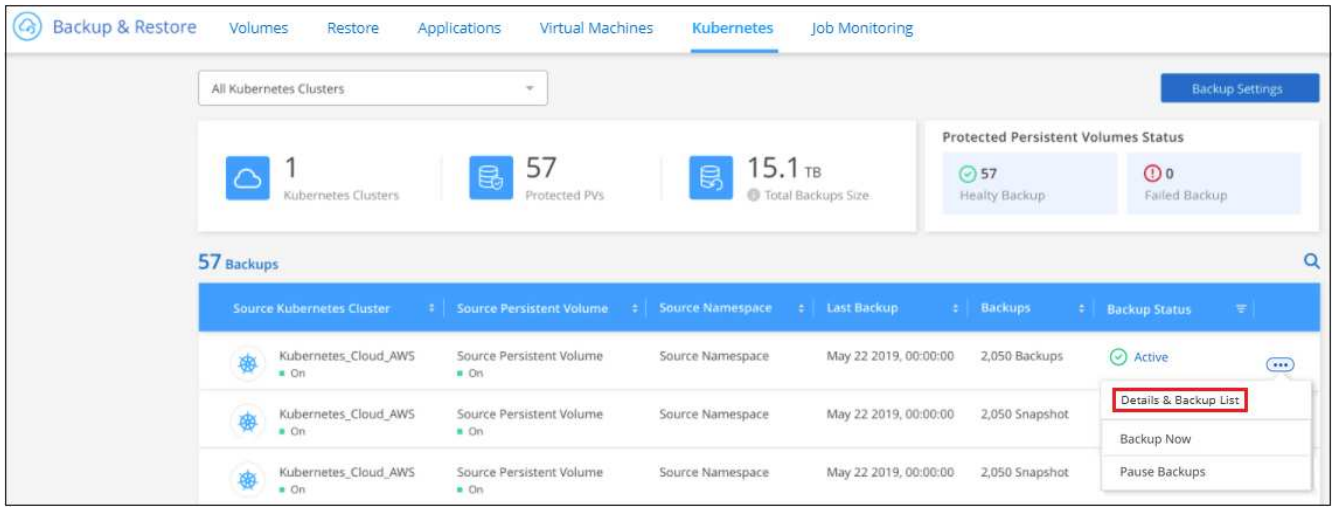
Löschen aller Sicherungsdateien für ein Volume

Durch das Löschen aller Backups für ein Volume werden auch künftige Backups für dieses Volume deaktiviert.

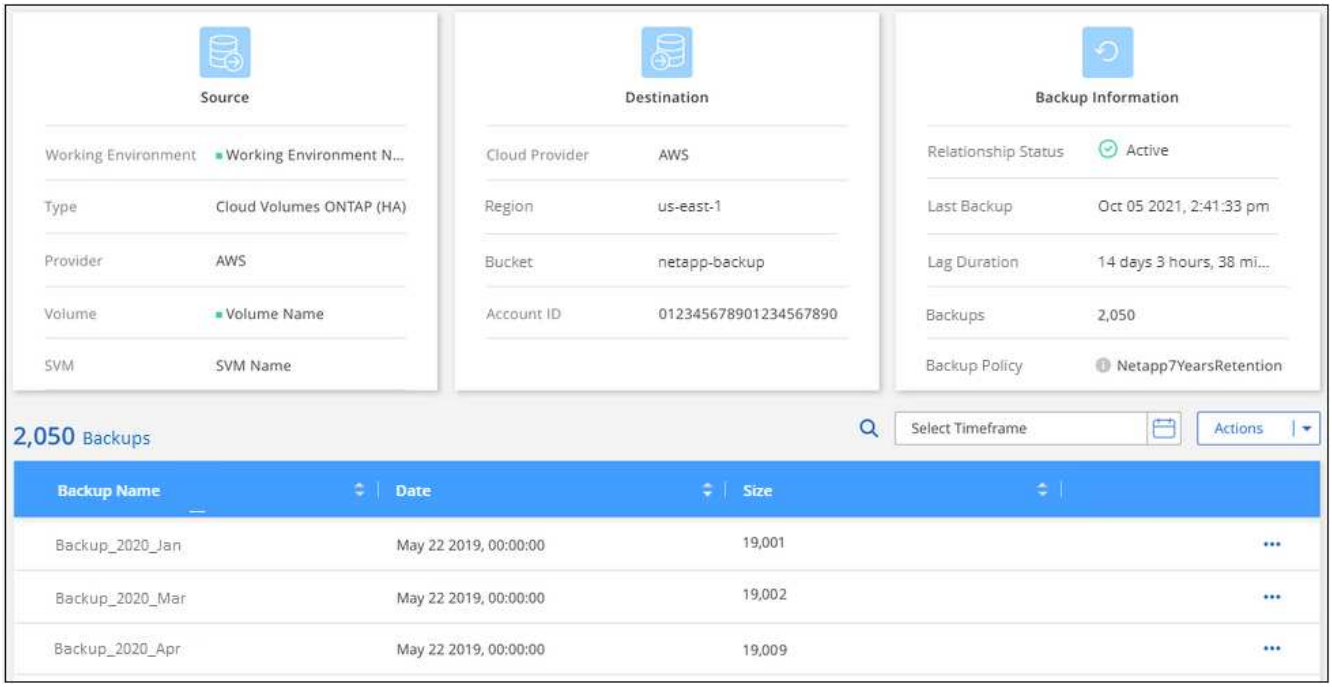
Das können Sie Starten Sie neu, um Backups für das Volume zu erstellen Auf der Seite „Backups verwalten“ können Sie jederzeit Backups managen.

Schritte

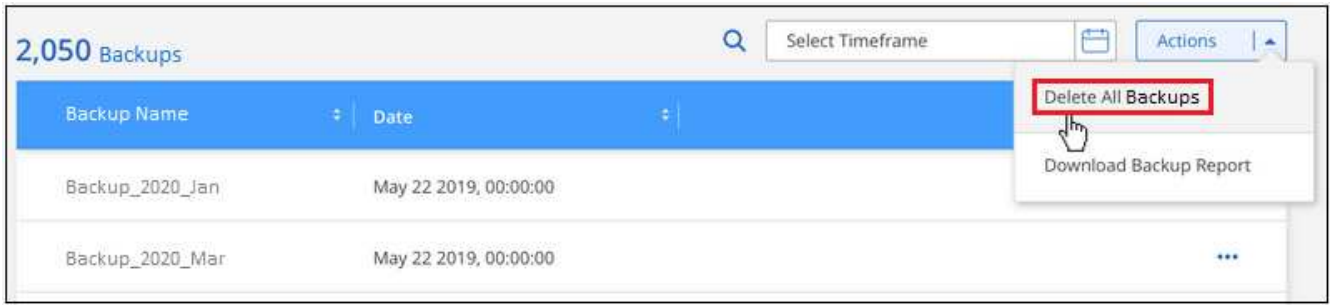
1. Klicken Sie auf der Registerkarte **Kubernetes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.



Die Liste aller Sicherungsdateien wird angezeigt.



2. Klicken Sie auf **Aktionen** > **Alle Backups löschen**.



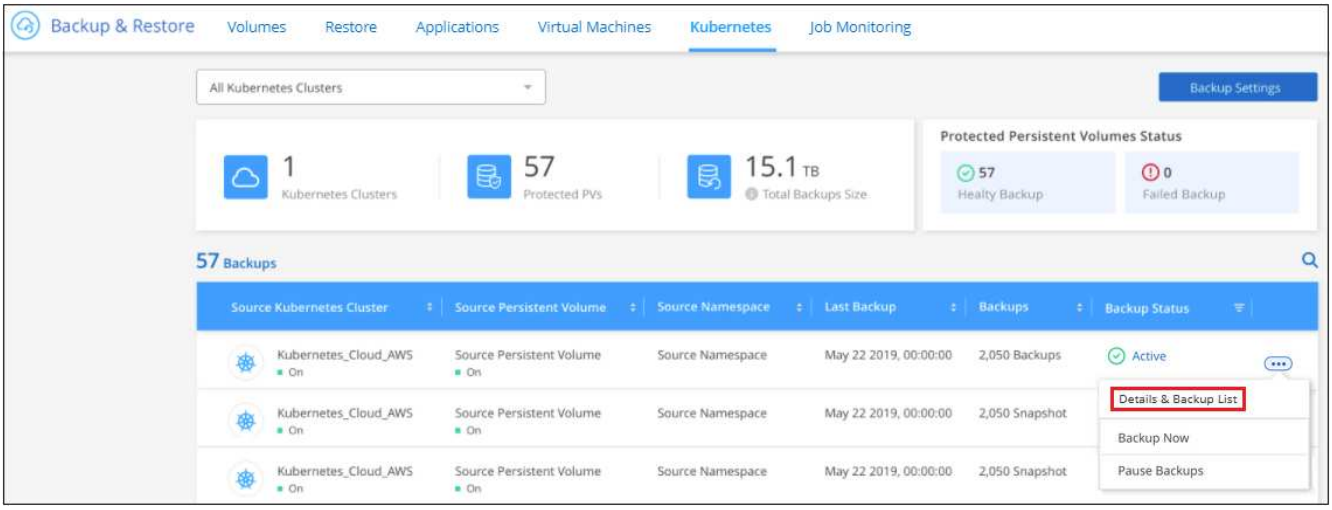
3. Geben Sie im Bestätigungsdialogfeld den Namen des Datenträgers ein und klicken Sie auf **Löschen**.

Löschen einer einzelnen Backup-Datei für ein Volume

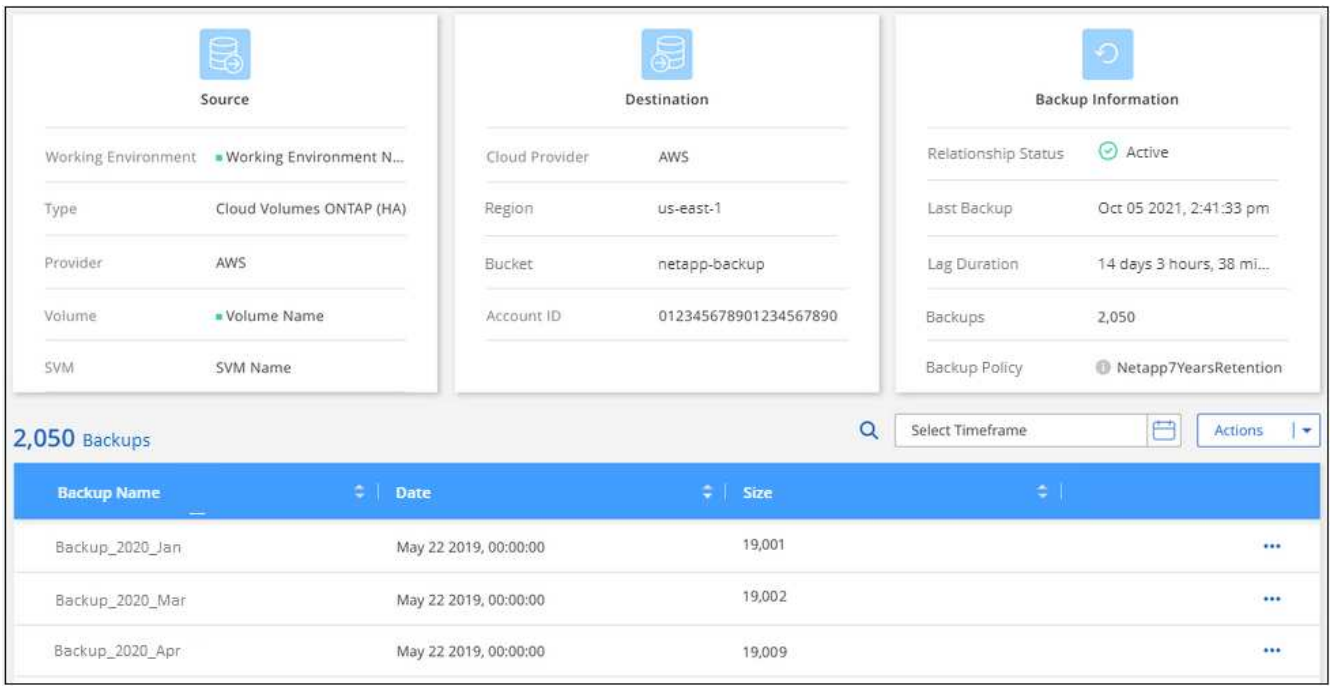
Sie können eine einzelne Sicherungsdatei löschen. Diese Funktion ist nur verfügbar, wenn das Volume Backup aus einem System mit ONTAP 9.8 oder neuer erstellt wurde.

Schritte

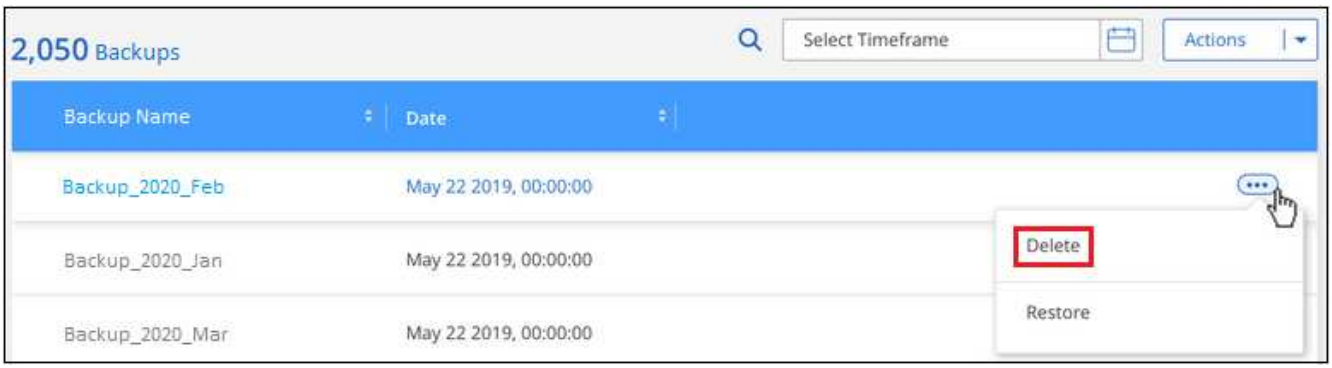
1. Klicken Sie auf der Registerkarte **Kubernetes** auf ••• Wählen Sie für das Quellvolume **Details & Sicherungsliste** aus.



Die Liste aller Sicherungsdateien wird angezeigt.



2. Klicken Sie Auf ••• Für die Sicherungsdatei des Datenträgers, die Sie löschen möchten, klicken Sie auf **Löschen**.



3. Klicken Sie im Bestätigungsdialogfeld auf **Löschen**.

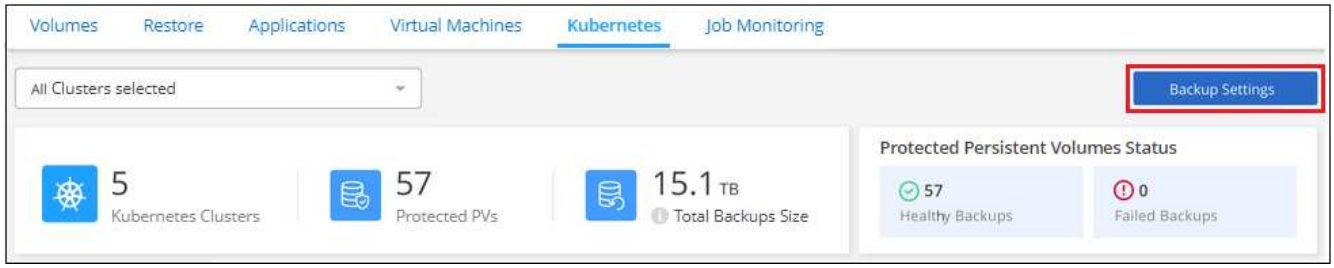
Deaktivieren von Cloud Backup für eine Arbeitsumgebung

Durch das Deaktivieren von Cloud Backup für eine Arbeitsumgebung werden Backups jedes Volumes auf dem System deaktiviert, zudem wird die Möglichkeit zur Wiederherstellung eines Volumes deaktiviert. Vorhandene Backups werden nicht gelöscht. Dadurch wird die Registrierung des Backup-Service in dieser Arbeitsumgebung nicht aufgehoben. Im Grunde können Sie alle Backup- und Wiederherstellungsaktivitäten für einen bestimmten Zeitraum anhalten.

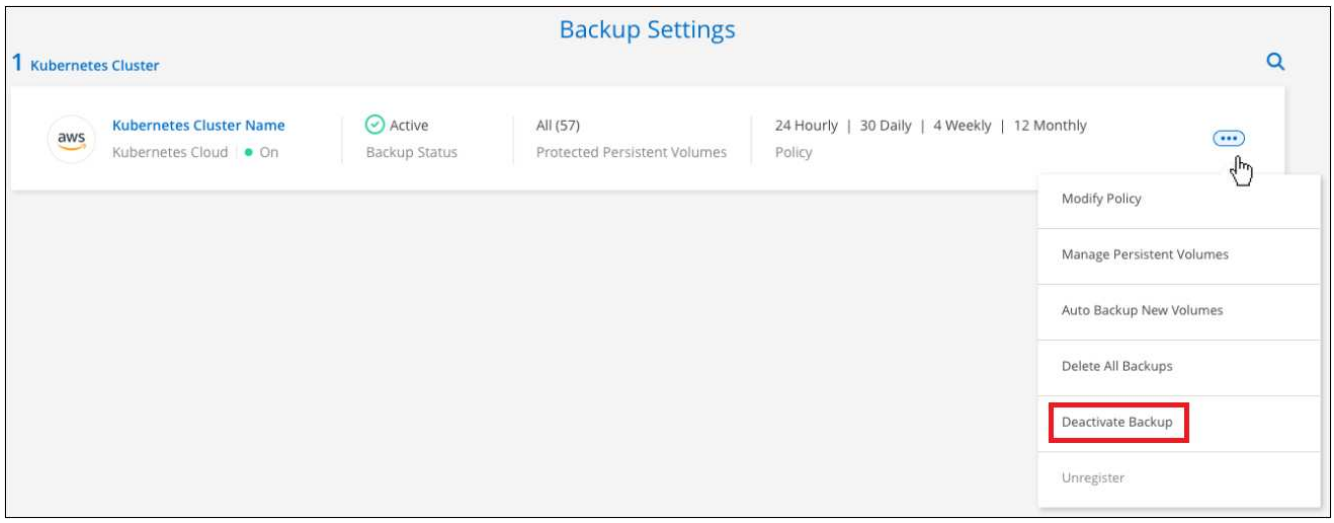
Beachten Sie, dass Cloud-Provider Ihnen weiterhin die Kosten für Objekt-Storage für die Kapazität in Ihrem Backup in Rechnung stellen, es sei denn, Sie sind erforderlich Löschen Sie die Backups.

Schritte

1. Wählen Sie auf der Registerkarte **Kubernetes** die Option **Backup-Einstellungen** aus.



2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Für die Arbeitsumgebung oder den Kubernetes-Cluster, wo Sie Backups deaktivieren und **deactivate Backup** wählen möchten.



3. Klicken Sie im Bestätigungsdialogfeld auf **Deaktivieren**.

Für diese Arbeitsumgebung wird während der Sicherung eine **Sicherung aktivieren** -Schaltfläche angezeigt. Sie können auf diese Schaltfläche klicken, wenn Sie die Backup-Funktion in dieser Arbeitsumgebung erneut aktivieren möchten.

Registrieren von Cloud Backup für eine Arbeitsumgebung wird aufgehoben

Sie können Cloud Backup für eine Arbeitsumgebung unregistrieren, wenn Sie die Backup-Funktion nicht mehr verwenden möchten, und Sie nicht mehr mit dem Aufladen von Backups in dieser Arbeitsumgebung belastet werden möchten. Diese Funktion wird in der Regel verwendet, wenn Sie planen, einen Kubernetes-Cluster zu löschen, und Sie den Backup-Service abbrechen möchten.

Sie können diese Funktion auch verwenden, wenn Sie den Zielobjektspeicher ändern möchten, in dem Ihre Cluster-Backups gespeichert werden. Nachdem Sie Cloud Backup für die Arbeitsumgebung registriert haben, können Sie Cloud Backup für diesen Cluster mithilfe der neuen Cloud-Provider-Informationen aktivieren.

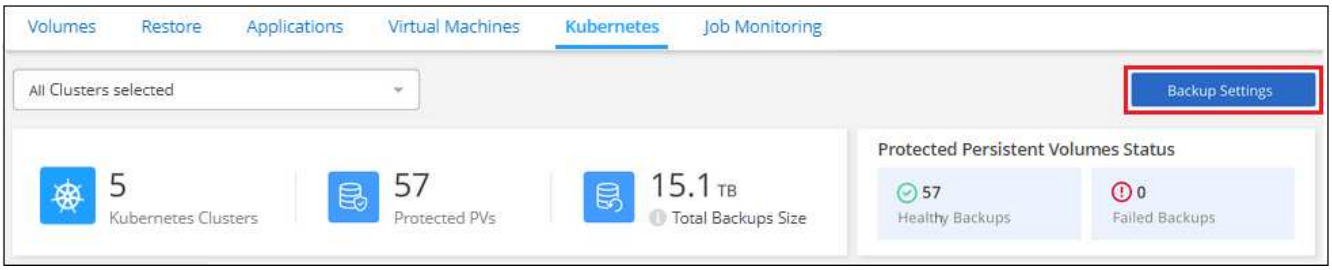
Bevor Sie die Registrierung von Cloud Backup aufheben können, müssen Sie die folgenden Schritte in der folgenden Reihenfolge durchführen:

- Deaktivieren Sie Cloud Backup für die Arbeitsumgebung
- Löschen Sie alle Backups für die Arbeitsumgebung

Die Option zum Aufheben der Registrierung ist erst verfügbar, wenn diese beiden Aktionen abgeschlossen sind.

Schritte

1. Wählen Sie auf der Registerkarte **Kubernetes** die Option **Backup-Einstellungen** aus.



2. Klicken Sie auf der Seite „ Backup Settings “ auf ••• Für den Kubernetes-Cluster, wo Sie den Backup-Service wieder registrieren und wählen Sie **Unregister**.

3. Klicken Sie im Bestätigungsdialogfeld auf **Registrierung aufheben**.

Wiederherstellung von Kubernetes-Daten aus Backup-Dateien

Backups werden in einem Objektspeicher in Ihrem Cloud-Konto gespeichert, sodass Sie Daten von einem bestimmten Zeitpunkt wiederherstellen können. Sie können ein gesamtes persistentes Kubernetes Volume aus einer gespeicherten Backup-Datei wiederherstellen.

Sie können ein persistentes Volume (als neues Volume) in derselben Arbeitsumgebung oder in einer anderen Arbeitsumgebung wiederherstellen, die dasselbe Cloud-Konto verwendet.

Unterstützte Arbeitsumgebungen und Objekt-Storage-Anbieter

Sie können ein Volume aus einer Kubernetes-Backup-Datei in den folgenden Arbeitsumgebungen wiederherstellen:

Speicherort Der Sicherungsdatei	Zielarbeitsumgebung ifdef::aws[]
Amazon S3	Kubernetes Cluster in AWS endif::AWS[] ifdef::Azure[]
Azure Blob	Kubernetes Cluster in Azure endif::Azure[] ifdef::gcp[]
Google Cloud Storage	Kubernetes Cluster in Google endif::gcp[]

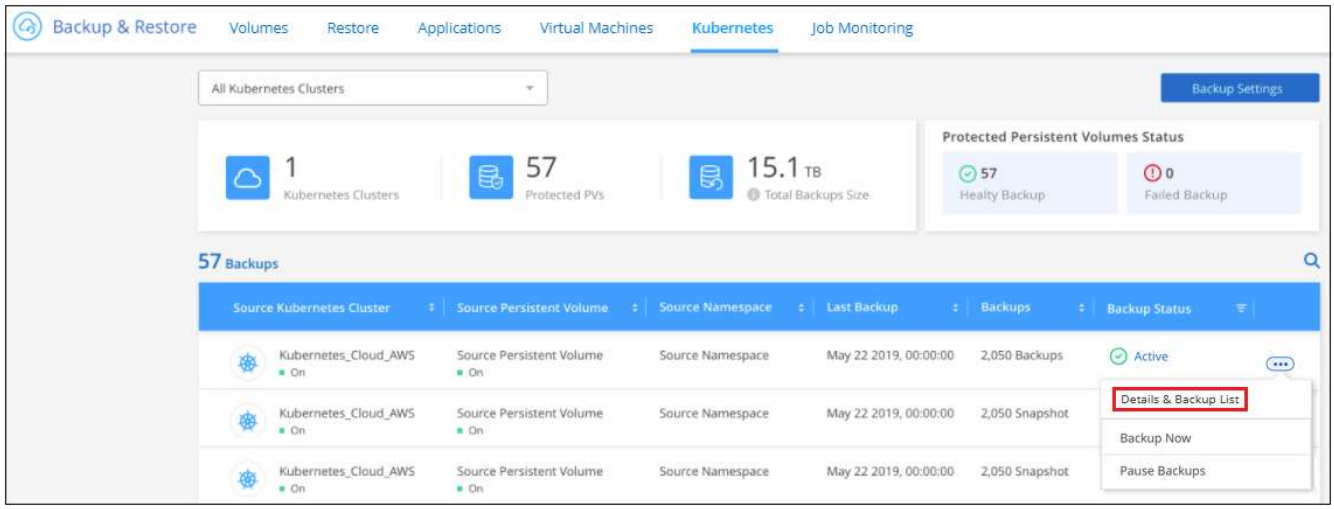
Wiederherstellung von Volumes aus einer Kubernetes-Backup-Datei

Wenn Sie ein persistentes Volume aus einer Sicherungsdatei wiederherstellen, erstellt BlueXP mithilfe der Daten aus dem Backup ein *neues* Volume. Die Daten können in einem Volume im selben Kubernetes-Cluster oder in einem anderen Kubernetes-Cluster wiederhergestellt werden, der sich im selben Cloud-Konto wie der Kubernetes-Quell-Cluster befindet.

Bevor Sie beginnen, sollten Sie den Namen des wiederherzustellenden Volumes und das Datum der Sicherungsdatei kennen, mit der Sie das neu wiederhergestellte Volume erstellen möchten.

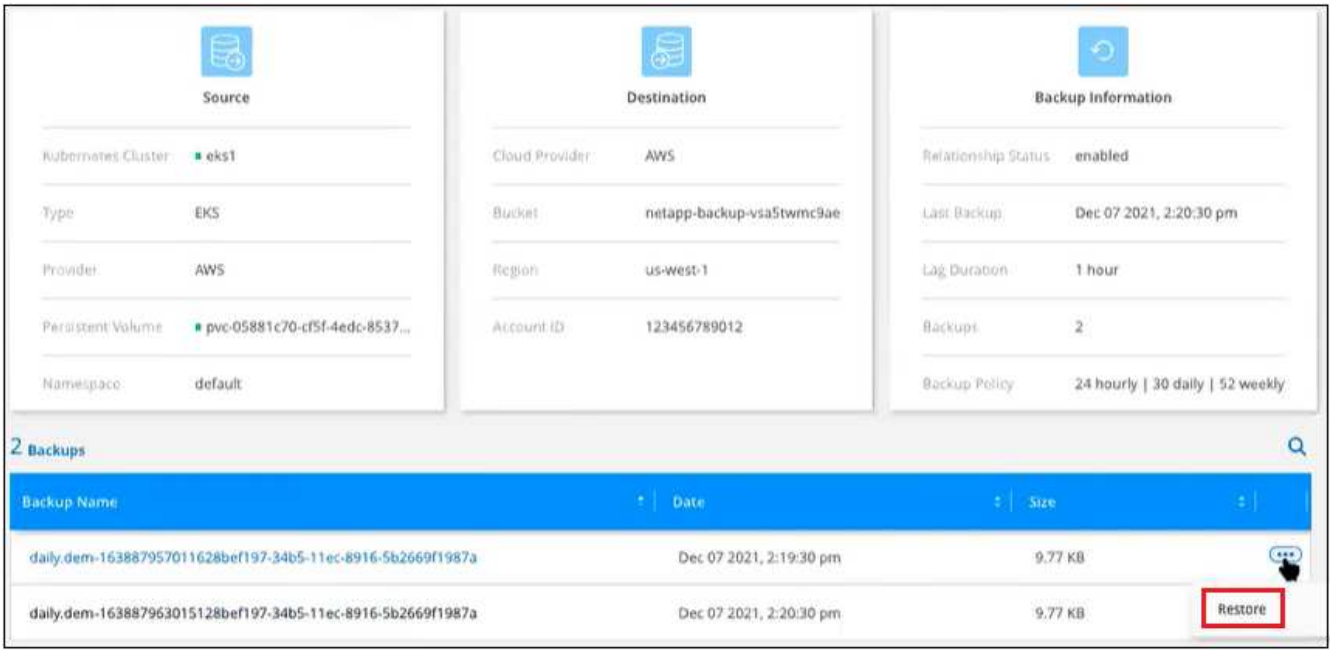
Schritte

1. Wählen Sie im Menü BlueXP die Option **Schutz > Sicherung und Wiederherstellung**.
2. Klicken Sie auf die Registerkarte **Kubernetes** und das Kubernetes Dashboard wird angezeigt.



3. Suchen Sie das wiederherzustellende Volume, klicken Sie auf ⋯, Und klicken Sie dann auf **Details & Sicherungsliste**.

   Die Liste aller Backup-Dateien für dieses Volume wird zusammen mit Details zum Quell-Volume, zum Zielspeicherort und Backup-Details angezeigt.



4. Suchen Sie anhand des Datums-/Zeitstempels die Backup-Datei, die Sie wiederherstellen möchten, und klicken Sie auf •••, Und dann **Restore**.
5. Wählen Sie auf der Seite *Select Destination* den *Kubernetes Cluster* aus, wo Sie das Volume, den *Namespace*, die *Storage Class* und den neuen Namen *Persistent Volume* wiederherstellen möchten.

6. Klicken Sie auf **Restore** und Sie werden wieder zum Kubernetes Dashboard, damit Sie den Fortschritt des Wiederherstellungsvorgangs überprüfen können.

Ergebnis

BlueXP erstellt im Kubernetes-Cluster ein neues Volume basierend auf dem ausgewählten Backup. Das können Sie "Verwalten Sie die Backup-Einstellungen für dieses neue Volume" Nach Bedarf.