Schützen Sie KVM -Workloads

NetApp Backup and Recovery

NetApp
June 25, 2026

Inhalt

Schützen Sie KVM -Workloads . . . 1
- Übersicht über den Schutz von KVM-Workloads . . . 1
- Entdecken Sie KVM-Workloads in NetApp Backup and Recovery . . . 1
  - Fügen Sie eine Managementplattform und einen KVM-Host hinzu und ermitteln Sie die Ressourcen. . . . 1
  - Weiter zum NetApp Backup and Recovery Dashboard . . . 3
- Erstellen und verwalten Sie Schutzgruppen für KVM-Workloads mit NetApp Backup and Recovery . . . 3
  - Erstellen einer Schutzgruppe . . . 3
  - Bearbeiten Sie eine Schutzgruppe . . . 4
  - Löschen einer Schutzgruppe . . . 4
- Erstellen und Verwalten von KVM-Backup-Richtlinien in NetApp Backup und Recovery . . . 5
  - Richtlinien anzeigen . . . 5
  - Erstellen einer Richtlinie . . . 5
  - Bearbeiten einer Richtlinie . . . 10
  - Löschen einer Richtlinie . . . 10
- Sichern Sie KVM-Workloads mit NetApp Backup and Recovery . . . 11
  - Sichern Sie Schutzgruppen jetzt mit einem On-Demand-Backup . . . 11
- Wiederherstellen virtueller KVM-Maschinen mit NetApp Backup and Recovery . . . 12
  - So funktioniert die Wiederherstellung virtueller Maschinen . . . 12
  - Wiederherstellen von KVM-VMs . . . 12

Schützen Sie KVM -Workloads

Übersicht über den Schutz von KVM-Workloads

Schützen Sie Ihre verwalteten KVM-VMs und Speicherpools mit NetApp Backup and Recovery. NetApp Backup and Recovery bietet schnelle, speichereffiziente, absturzsichere und VM-konsistente Backup- und Wiederherstellungsvorgänge. Bevor Sie Ihre KVM-Hosts und VMs mithilfe von Backup und Recovery schützen können, müssen diese über eine Managementplattform wie Apache CloudStack verwaltet werden.

Sie können KVM-Workloads auf Amazon Web Services S3, Azure NetApp Files oder StorageGRID sichern und KVM-Workloads auf einem lokalen KVM-Host wiederherstellen.

Verwenden Sie NetApp Backup and Recovery , um eine 3-2-1-Schutzstrategie zu implementieren, bei der Sie 3 Kopien Ihrer Quelldaten auf 2 verschiedenen Speichersystemen sowie 1 Kopie in der Cloud haben. Zu den Vorteilen des 3-2-1-Ansatzes gehören:

- Mehrere Datenkopien schützen vor internen und externen Cybersicherheitsbedrohungen.
- Die Verwendung unterschiedlicher Medientypen erleichtert Ihnen die Wiederherstellung, wenn ein Typ ausfällt.
- Sie können die Wiederherstellung schnell von der Vor-Ort-Kopie durchführen und die Offsite-Kopien verwenden, wenn die Vor-Ort-Kopie kompromittiert ist.

Mit NetApp Backup and Recovery können Sie die folgenden Aufgaben im Zusammenhang mit KVM-Workloads ausführen:

- "Entdecken Sie KVM-Workloads"
- "Erstellen und Verwalten von Schutzgruppen für KVM-Workloads"
- "KVM-Workloads sichern"
- "KVM-Workloads wiederherstellen"

Entdecken Sie KVM-Workloads in NetApp Backup and Recovery

NetApp Backup and Recovery muss KVM-Hosts und virtuelle Maschinen erkennen, bevor diese geschützt werden können. Bevor Sie Ihre KVM-Hosts und VMs zu Backup und Recovery hinzufügen können, müssen diese über eine Managementplattform wie Apache CloudStack verwaltet werden.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung. Erfahren Sie mehr über"Rollen und Berechtigungen für Backup und Wiederherstellung" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Fügen Sie eine Managementplattform und einen KVM-Host hinzu und ermitteln Sie die Ressourcen.

Fügen Sie Informationen zur Managementplattform und zum KVM-Host hinzu, damit NetApp Backup and

Recovery die Workloads automatisch erkennt.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **KVM** aus.

   Wenn Sie sich zum ersten Mal bei Backup and Recovery anmelden und zwar ein System in der Konsole haben, aber keine Ressourcen erkannt wurden, wird die Seite *Willkommen bei der neuen NetApp Backup and Recovery* mit einer Option zum **Erkennen von Ressourcen** angezeigt.

3. Wählen Sie **Ressourcen entdecken**.
4. Geben Sie die folgenden Informationen ein:
   a. **Workload-Typ**: Wählen Sie **KVM**.
   b. Falls Sie Ihre Managementplattform noch nicht in Backup and Recovery integriert haben, wählen Sie **Managementplattform hinzufügen**.
      i. Geben Sie die folgenden Informationen ein:
         - **IP-Adresse oder FQDN der Managementplattform**: Geben Sie die IP-Adresse oder den vollqualifizierten Domänennamen der Managementplattform ein.
         - **API-Schlüssel**: Geben Sie den API-Schlüssel ein, der zur Authentifizierung von API-Anfragen verwendet werden soll.
         - **Geheimer Schlüssel**: Geben Sie den geheimen Schlüssel ein, der zur Authentifizierung von API-Anfragen verwendet werden soll.
         - **Port**: Geben Sie den Port ein, der für die Kommunikation zwischen Backup und Recovery und der Managementplattform verwendet werden soll.
         - **Agenten**: Wählen Sie einen Konsolenagenten aus, der die Kommunikation zwischen Backup und Recovery und der Managementplattform erleichtern soll.
      ii. Wenn Sie fertig sind, wählen Sie **Hinzufügen**.
   c. **KVM-Einstellungen**: Fügen Sie einen neuen KVM-Host hinzu, indem Sie die folgenden Informationen eingeben:
      - **KVM FQDN oder IP-Adresse**: Geben Sie den FQDN oder die IP-Adresse des Hosts ein.
      - **Anmeldedaten**: Geben Sie den Benutzernamen und das Passwort für den KVM-Host ein.
      - **Konsolenagent**: Wählen Sie den Konsolenagenten aus, der für die Kommunikation zwischen Backup und Recovery und dem KVM-Host verwendet werden soll.
      - **Portnummer**: Geben Sie den Port ein, der für die Kommunikation zwischen Backup und Recovery und dem KVM-Host verwendet werden soll.
      - **Verwaltungsplattform**: Wenn der KVM-Host verwaltet wird und Sie die Verwaltungsplattform zu Backup und Wiederherstellung hinzugefügt haben, wählen Sie die Verwaltungsplattform aus der Liste aus.
5. Wählen Sie **Entdecken**.

   Dieser Vorgang kann einige Minuten dauern.

Ergebnis

Die KVM-Arbeitslast wird in der Liste der Arbeitslasten auf der Inventarseite angezeigt.

Weiter zum NetApp Backup and Recovery Dashboard

Schritte

1. Wählen Sie im NetApp Console **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie eine Workload-Kachel aus (z. B. Microsoft SQL Server).
3. Wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Dashboard“ aus.
4. Überprüfen Sie den Zustand des Datenschutzes. Die Anzahl der gefährdeten oder geschützten Workloads steigt basierend auf den neu entdeckten, geschützten und gesicherten Workloads.

Erstellen und verwalten Sie Schutzgruppen für KVM-Workloads mit NetApp Backup and Recovery

Erstellen Sie Schutzgruppen, um die Sicherungsvorgänge für eine Reihe von KVM-Ressourcen zu verwalten. Eine Schutzgruppe ist eine logische Gruppierung von Ressourcen wie VMs und Speicherpools, die Sie gemeinsam schützen möchten. Sie müssen eine Schutzgruppe erstellen, um virtuelle KVM-Maschinen oder Speicherpools zu sichern.

Sie können die folgenden Aufgaben im Zusammenhang mit Schutzgruppen ausführen:

- Erstellen Sie eine Schutzgruppe.
- Schutzdetails anzeigen.
- Sichern Sie jetzt eine Schutzgruppe. Sehen"Sichern Sie jetzt KVM-Workloads" .
- Bearbeiten Sie eine Datensicherungsgruppe.
- Löschen Sie eine Schutzgruppe.

Erstellen einer Schutzgruppe

Gruppieren Sie VMs und Speicherpools, die Sie gemeinsam schützen möchten, in einer Schutzgruppe.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Backupadministratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie **Schutzgruppe erstellen**.
6. Geben Sie einen Namen für die Schutzgruppe ein.
7. Wählen Sie einen Host aus, um die auf diesem Host verfügbaren VMs aufzulisten. Um VMs von allen gefundenen Hosts einzubeziehen, wählen Sie in der Hostliste **All** aus.
8. Wählen Sie einzelne VMs aus, die Sie in die Datensicherungsgruppe aufnehmen möchten, oder wählen Sie **All**, um alle VMs in die Liste aufzunehmen.

Die von Ihnen ausgewählten VMs werden im Bereich **Added virtual machines** angezeigt. Sie können einzelne VMs aus der Liste entfernen oder die Liste vollständig leeren. Sie können VMs von mehreren KVM-Hosts zur Liste hinzufügen.

9. Wählen Sie **Weiter**.
10. Wählen Sie die Datensicherungsstrategie, die Sie auf die Schutzgruppe anwenden möchten, oder erstellen Sie eine neue Strategie, indem Sie **Create new policy** auswählen.

    Weitere Informationen zum Erstellen einer Sicherungsrichtlinie finden Sie unter"Erstellen und Verwalten von Richtlinien" .

11. Wählen Sie **Weiter**.
12. Überprüfen Sie die Konfiguration.
13. Wählen Sie **Erstellen** aus, um die Schutzgruppe zu erstellen.

Bearbeiten Sie eine Schutzgruppe

Bearbeiten Sie eine Datensicherungsgruppe, wenn Sie Details der Datensicherungsgruppe ändern müssen, ohne sie zu löschen und neu zu erstellen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie die Schutzgruppe aus, die Sie bearbeiten möchten.
6. Wählen Sie das Symbol „Aktionen“ aus. ••• > **Bearbeiten**.
7. Nehmen Sie alle erforderlichen Änderungen an den allgemeinen Details und den VMs in der protection group vor.
8. Wählen Sie **Weiter**.
9. Ändern Sie bei Bedarf die mit der Schutzgruppe verknüpfte Datensicherungsstrategie.
10. Wählen Sie **Weiter**.
11. Überprüfen Sie die Konfiguration und wählen Sie **Absenden**.

Löschen einer Schutzgruppe

Durch das Löschen einer Schutzgruppe werden diese und alle zugehörigen Sicherungszeitpläne entfernt. Möglicherweise möchten Sie eine Schutzgruppe löschen, wenn sie nicht mehr benötigt wird.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Inventar** aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
4. Wählen Sie die Registerkarte **Schutzgruppen**.
5. Wählen Sie die Schutzgruppe aus, die Sie löschen möchten.

6. Wählen Sie das Symbol Aktionen ••• > **Löschen**.
7. Überprüfen Sie die Bestätigungsmeldung zum Löschen der zugehörigen Sicherungen und bestätigen Sie den Löschvorgang.

Erstellen und Verwalten von KVM-Backup-Richtlinien in NetApp Backup und Recovery

In NetApp Backup und Recovery können Sie eigene KVM-Backup-Richtlinien erstellen, die die Backup-Häufigkeit, den Zeitpunkt des Backups und die Anzahl der aufbewahrten Backup-Dateien regeln.

Einige dieser Optionen und Konfigurationsabschnitte sind nicht für alle Workloads verfügbar.

Wenn Sie Ressourcen aus SnapCenter importieren, können Sie auf Unterschiede zwischen den in SnapCenter und den in NetApp Backup and Recovery verwendeten Richtlinien stoßen. Sehen"Richtlinienunterschiede zwischen SnapCenter und NetApp Backup and Recovery" .

Sie können die folgenden Ziele im Zusammenhang mit Richtlinien erreichen:

- Erstellen einer lokalen Snapshot-Richtlinie
- Erstellen einer Richtlinie für die Replikation auf sekundären Speicher
- Erstellen einer Richtlinie für Objektspeichereinstellungen
- Konfigurieren erweiterter Richtlinieneinstellungen
- Richtlinien bearbeiten (nicht verfügbar für VMware workloads)
- Richtlinien löschen

Richtlinien anzeigen

1. Wählen Sie im NetApp Backup and Recovery -Menü **Richtlinien** aus.
2. Überprüfen Sie die Richtliniendetails. Zum Beispiel:
    - **Workload**: Beispiele sind Microsoft SQL Server, ONTAP Volumes, VMware, KVM, Hyper-V, Oracle Database oder Kubernetes.
    - **Sicherungstyp**: Beispiele sind vollständige Sicherung und Protokollsicherung.
    - **Architektur**: Beispiele hierfür sind lokaler Snapshot, Fan-Out, Kaskadierung, Disk-to-Disk und Disk-to-Object-Store.
    - **Geschützte Ressourcen**: Zeigt an, wie viele Ressourcen der Gesamtressourcen dieser Arbeitslast geschützt sind.
    - **Ransomware-Schutz**: Zeigt an, ob die Richtlinie eine Snapshot-Sperre für den lokalen Snapshot, eine Snapshot-Sperre für den sekundären Speicher oder eine DataLock-Sperre für den Objektspeicher umfasst.

Erstellen einer Richtlinie

Sie können Richtlinien erstellen, die Ihre lokalen Snapshots, Replikationen auf sekundären Speicher und Backups auf Objektspeicher regeln. Ein Teil Ihrer 3-2-1-Strategie besteht darin, einen Snapshot der Instanzen, Datenbanken, Anwendungen oder VMs auf dem **primären** Speichersystem zu erstellen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung, Backupadministrator für Backup und Wiederherstellung. Erfahren Sie mehr über"Rollen und Berechtigungen für Backup und Wiederherstellung" . "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Bevor Sie beginnen

Wenn Sie eine Replikation auf einen sekundären Speicher planen und die Snapshot-Sperre auf lokalen Snapshots oder auf einem Remote ONTAP Sekundärspeicher verwenden möchten, müssen Sie zunächst die ONTAP Compliance-Uhr auf Clusterebene initialisieren. Dies ist eine Voraussetzung zum Aktivieren der Snapshot-Sperre in der Richtlinie.

Anweisungen hierzu finden Sie unter "Initialisieren Sie die Compliance-Uhr in ONTAP" .

Allgemeine Informationen zum Sperren von Snapshots finden Sie unter "Snapshot-Sperre in ONTAP" .

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Richtlinien** aus.
2. Wählen Sie auf der Seite „Richtlinien“ die Option „Neue Richtlinie erstellen“ aus.

   Die Seite „Richtlinien“ wird angezeigt.

3. Geben Sie im Abschnitt **Details** Informationen ein:
   - Arbeitslasttyp: Wählen Sie **KVM**.
   - Geben Sie einen Richtliniennamen ein.
   - Wählen Sie einen Konsolenagenten aus der Liste **Agent** aus.
4. Geben Sie im Abschnitt **Backup-Architektur** Informationen ein. Wählen Sie den Datenfluss für das Backup aus der Liste aus:
   - **3-2-1-Fanout**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte) zu Cloud (Objektspeicher). Erstellt mehrere Kopien von Daten auf verschiedenen Speichersystemen, wie ONTAP zu ONTAP und ONTAP zu Objektspeicher-Konfigurationen. Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher sein. Am besten geeignet für optimale Datensicherung und Disaster Recovery. Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.
   - **3-2-1-Kaskade**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte) und Primärspeicher (Festplatte) zu Cloud-Speicher (Objektspeicher). Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher wie StorageGRID sein. Dadurch entsteht eine Kette der Datenreplizierung über mehrere Systeme hinweg, um Redundanz und Zuverlässigkeit zu gewährleisten. Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.
   - **Festplatte zu Festplatte**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte). Die ONTAP zu ONTAP Datensicherungsstrategie repliziert Daten zwischen zwei ONTAP Systemen, um hohe Verfügbarkeit und Disaster Recovery zu gewährleisten. Dies wird typischerweise mithilfe von SnapMirror erreicht, das sowohl synchron als auch asynchrone Replizierung unterstützt. Diese Methode hält Ihre Daten standortübergreifend aktuell und verfügbar für eine starke Datensicherung.
   - **Disk-to-object storage**: Primärspeicher (Festplatte) zu Cloud (Objektspeicher). Dabei werden Daten von einem ONTAP System zu einem Objektspeichersystem repliziert. Dies kann ein Cloud-Hyperscaler-Objektspeicher oder ein privater Objektspeicher wie StorageGRID sein. Diese Methode ist ideal für die langfristige Datenaufbewahrung und Archivierung. Diese Option ist für Amazon FSx for NetApp ONTAP nicht verfügbar.
   - **Disk-to-Disk-Fanout**: Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte) und Primärspeicher (Festplatte) zu Sekundärspeicher (Festplatte). Sie können mehrere sekundäre Einstellungen für die Disk-to-Disk-Fanout-Option konfigurieren.

- **Lokale Snapshots**: Lokaler Snapshot des ausgewählten Volumes. Dadurch werden schreibgeschützte, zeitpunktgenaue Kopien der Produktionsvolumes erstellt, auf denen Ihre Workloads ausgeführt werden. Sie können lokale Snapshots verwenden, um Datenverlust oder -beschädigung zu beheben sowie um Backups für die Notfallwiederherstellung zu erstellen.

5. Geben Sie Informationen für den Abschnitt **Lokale Snapshot-Einstellungen** an:
   - Wählen Sie die Option **Zeitplan hinzufügen**, um den oder die Snapshot-Zeitpläne auszuwählen. Sie können maximal 5 Zeitpläne haben.
   - **Schnappschusshäufigkeit**: Wählen Sie die Häufigkeit stündlich, täglich, wöchentlich, monatlich oder jährlich. Die jährliche Häufigkeit ist für Kubernetes-Workloads nicht verfügbar.
   - **Aufbewahrung von Snapshots**: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.
6. Geben Sie Informationen für den Abschnitt **Sekundäre Einstellungen** (Replikation auf Sekundärspeicher) an:
   - **Sicherung**: Wählen Sie die Häufigkeit stündlich, täglich, wöchentlich, monatlich oder jährlich.
   - **Sicherungsziel**: Wählen Sie das Zielsystem auf dem Sekundärspeicher für die Sicherung aus.
   - **Aufbewahrung**: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.
   - **Snapshot-Sperre aktivieren**: Wählen Sie aus, ob Sie manipulationssichere Snapshots aktivieren möchten.
   - **Sperrzeitraum für Snapshots**: Geben Sie die Anzahl der Tage, Monate oder Jahre ein, für die Sie den Snapshot sperren möchten.
   - **Wechsel zur weiterführenden Schule**:
     - Die Option * ONTAP Übertragungsplan – Inline* ist standardmäßig ausgewählt und gibt an, dass Snapshots sofort auf das sekundäre Speichersystem übertragen werden. Sie müssen die Sicherung nicht planen.
     - Weitere Optionen: Wenn Sie eine aufgeschobene Überweisung wählen, erfolgen die Überweisungen nicht sofort und Sie können einen Zeitplan festlegen.
   - **Vorhandene SnapMirror und SyncMirror sekundäre Beziehung verwenden**: Mit dieser Option wird die vorhandene SnapMirror oder SyncMirror Beziehung genutzt, um Snapshots an den festgelegten Ziel-Cluster zu übertragen.
7. Geben Sie Informationen für den Abschnitt **Objektspeichereinstellungen** (Sicherung im Objektspeicher) an:

   Die angezeigten Felder unterscheiden sich je nach ausgewähltem Anbieter und Architektur.

   - **Anbieter**: Wählen Sie den Anbieter für Ihren Objektspeicher und geben Sie die Anmeldeinformationen in die entsprechenden Felder ein (die Felder für die Anmeldeinformationen unterscheiden sich je nach Anbieter).
   - **Sicherungsziel**: Wählen Sie ein registriertes Objektspeicherziel aus. Stellen Sie sicher, dass das Ziel in Ihrer Sicherungsumgebung zugänglich ist.
   - **IPspace**: Wählen Sie den IPspace aus, der für die Sicherungsvorgänge verwendet werden soll. Dies ist nützlich, wenn Sie über mehrere IP-Bereiche verfügen und steuern möchten, welcher für Sicherungen verwendet wird.
   - **Zeitplaneinstellungen**: Wählen Sie den Zeitplan aus, der für die lokalen Snapshots festgelegt wurde. Sie können einen Zeitplan entfernen, aber keinen hinzufügen, da die Zeitpläne entsprechend den lokalen Snapshot-Zeitplänen festgelegt werden.
   - **Aufbewahrungskopien**: Geben Sie die Anzahl der aufzubewahrenden Snapshots ein.

- **Ausführen um**: Wählen Sie den ONTAP Übertragungszeitplan zum Sichern von Daten im Objektspeicher.
- **Stufen Sie Ihre Backups vom Objektspeicher in den Archivspeicher auf**: Wenn Sie Backups in den Archivspeicher (z. B. AWS Glacier) aufstufen möchten, wählen Sie die Stufenoption und die Anzahl der Tage für die Archivierung aus.
- **Integritätsprüfung aktivieren**: Wählen Sie aus, ob Sie Integritätsprüfungen (Snapshot-Sperrung) für den Objektspeicher aktivieren möchten. Dadurch wird sichergestellt, dass Ihre Backups gültig und wiederherstellbar sind. Die Integritätsprüfung erfolgt standardmäßig alle 7 Tage. Um Ihre Backups vor Änderungen oder Löschung zu schützen, wählen Sie die Option **Integritätsprüfung**. Die Prüfung wird nur für den neuesten Snapshot durchgeführt. Sie können Integritätsprüfungen für den neuesten Snapshot aktivieren oder deaktivieren.

Konfigurieren Sie erweiterte Einstellungen in der Richtlinie

Sie können optional erweiterte Einstellungen in der Richtlinie konfigurieren. Diese Optionen stehen Ihnen für alle Backup-Architekturen und Speicherziele zur Verfügung. Die verfügbaren erweiterten Optionen hängen von der oben auf der Seite ausgewählten Arbeitslast ab, daher treffen einige der hier beschriebenen Optionen möglicherweise nicht auf alle Arbeitslasten zu.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Richtlinien** aus.
2. Wählen Sie auf der Seite „Richtlinien“ die Option „Neue Richtlinie erstellen“ aus.
3. Wählen Sie im Abschnitt „Richtlinie > Erweitert*-Einstellungen“ das Menü „Erweiterte Aktion auswählen*, um aus einer Liste erweiterter Einstellungen auszuwählen.
4. Aktivieren Sie alle Einstellungen, die Sie anzeigen oder ändern möchten, und wählen Sie dann **Akzeptieren**.
5. Geben Sie die folgenden Informationen an:
   - **VM-Einstellungen**:
     - **VM- und applikationskonsistente Snapshots aktivieren**: Aktivieren Sie diese Option, um VM- und applikationskonsistente Snapshots zu erstellen. Hierfür muss der KVM QEMU Guest Agent auf der VM ausgeführt werden. Wenn der Guest Agent nicht läuft, werden stattdessen absturzkonsistente Snapshots erstellt. Beachten Sie, dass die Aktivierung dieser Option die Backup-Zeit verlängern und mehr Speicherplatz beanspruchen kann. Zudem wird der aktive RAM der VM nicht in konsistente Snapshots einbezogen.
   - **SnapMirror Volume- und Snapshot-Format**: Wählen Sie aus den folgenden Optionen:
     - **Benutzerdefiniertes Namensformat für Snapshot-Kopien verwenden**: Wählen Sie ein Namensschema für Snapshots. Wenn Sie dieses Feld leer lassen, wird jedem Snapshot-Namen ein Zeitstempel hinzugefügt.
     - **SnapMirror-Volume-Format angeben**: Geben Sie ein Präfix, ein Suffix oder beides an, um den Standard-SnapMirror-Volume-Namen zu ändern. Standardmäßig übernimmt ein SnapMirror-Volume den Namen des Quell-Volumes.
   - **Maximale Transferrate**: Um kein Limit für die Bandbreitennutzung festzulegen, wählen Sie **Unbegrenzt**. Wenn Sie die Transferrate begrenzen möchten, wählen Sie **Begrenzt** und wählen Sie die Netzwerkbandbreite zwischen 1 und 1.000 Mbps, die für das Hochladen von Backups in den Objektspeicher zugewiesen wird. Standardmäßig kann ONTAP eine unbegrenzte Menge an Bandbreite verwenden, um die Backup-Daten von Volumes im System in den Objektspeicher zu übertragen. Wenn der Backup-Datenverkehr die Workloads beeinträchtigt, reduzieren Sie die Netzwerkbandbreite für Übertragungen.
   - **Wiederholungsversuche für Backups**: Um den Auftrag im Fehlerfall oder bei einer Unterbrechung zu wiederholen, wählen Sie **Wiederholungsversuche bei Fehlern aktivieren**. Geben Sie die maximale Anzahl an Wiederholungsversuchen für Snapshot- und Backup-Aufträge sowie das Wiederholungsintervall ein. Die Anzahl der Wiederholungsversuche muss weniger als 10 sein.

     Wenn die Snapshot-Frequenz auf 1 Stunde eingestellt ist, sollte die maximale Verzögerung zusammen mit der Anzahl der Wiederholungsversuche 45 Minuten nicht überschreiten.

   - **Ransomware-Scan**: Wählen Sie aus, ob Sie den Ransomware-Scan für jeden Bucket aktivieren möchten. Dies erfordert eine DataLock-Sperre auf dem Objektspeicher. Geben Sie die Häufigkeit des Scans in Tagen ein. Diese Option gilt für AWS- und Microsoft Azure-Objektspeicher. Beachten Sie, dass für diese Option je nach Cloud-Anbieter zusätzliche Kosten anfallen können.

- **Benachrichtigung**: Wählen Sie aus, ob E-Mail-Benachrichtigungen für Backup-Vorgänge aktiviert werden sollen. Sie können auswählen, welche Ereignisse eine Benachrichtigung auslösen – zum Beispiel, wenn ein Backup erfolgreich ist, fehlschlägt oder mit Warnungen abgeschlossen wird.

Bearbeiten einer Richtlinie

Sie können die Backup-Architektur, die Backup-Frequenz, die Aufbewahrungsrichtlinie und weitere Einstellungen einer Richtlinie bearbeiten. Für Kubernetes-Workload-Richtlinien können Sie nur die Zeitplan- und Aufbewahrungseinstellungen bearbeiten.

Sie können beim Bearbeiten einer Richtlinie eine weitere Schutzebene hinzufügen, aber keine Schutzebene entfernen. Wenn die Richtlinie beispielsweise nur lokale Snapshots schützt, können Sie die Replikation zum sekundären Speicher oder die Backups zum Objektspeicher hinzufügen. Wenn Sie über lokale Snapshots und Replikation verfügen, können Sie Objektspeicher hinzufügen. Wenn Sie jedoch über lokale Snapshots, Replikation und Objektspeicher verfügen, können Sie keine dieser Ebenen entfernen.

Wenn Sie eine Richtlinie bearbeiten, die eine Sicherung im Objektspeicher vornimmt, können Sie die Archivierung aktivieren.

Wenn Sie Ressourcen aus SnapCenter importiert haben, stoßen Sie möglicherweise auf einige Unterschiede zwischen den in SnapCenter und NetApp Backup and Recovery verwendeten Richtlinien. Sehen"Richtlinienunterschiede zwischen SnapCenter und NetApp Backup and Recovery" .

Erforderliche NetApp Console

Superadministrator für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Gehen Sie in der NetApp Console zu **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie die Option **Richtlinien**.
3. Wählen Sie die Richtlinie aus, die Sie bearbeiten möchten.
4. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Bearbeiten**.

Löschen einer Richtlinie

Sie können eine Richtlinie löschen, wenn Sie sie nicht mehr benötigen.

Sie können keine Richtlinie löschen, die einer Arbeitslast zugeordnet ist.

Schritte

1. Gehen Sie in der Konsole zu **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie die Option **Richtlinien**.
3. Wählen Sie die Richtlinie aus, die Sie löschen möchten.
4. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Löschen**.
5. Bestätigen Sie die Aktion und wählen Sie **Löschen**.

Sichern Sie KVM-Workloads mit NetApp Backup and Recovery

Sichern Sie KVM-Schutzgruppen von lokalen ONTAP -Systemen auf Amazon Web Services, Azure NetApp Files oder StorageGRID , um sicherzustellen, dass Ihre Daten geschützt sind. Wenn Sie eine Schutzgruppe sichern, sichert die NetApp Console die in der Schutzgruppe enthaltenen VMs und Speicherpools. Backups werden automatisch erstellt und in einem Objektspeicher in Ihrem öffentlichen oder privaten Cloud-Konto gespeichert.

Um Schutzgruppen nach einem Zeitplan zu sichern, erstellen Sie Richtlinien, die die Sicherungs- und Wiederherstellungsvorgänge steuern. Sehen"Erstellen von Richtlinien" Anweisungen hierzu finden Sie unter.

- Erstellen Sie Schutzgruppen, um die Sicherungs- und Wiederherstellungsvorgänge für eine Reihe von Ressourcen zu verwalten. Sehen"Erstellen und verwalten Sie Schutzgruppen für KVM-Workloads mit NetApp Backup and Recovery" für weitere Informationen.

Sichern Sie Schutzgruppen jetzt mit einem On-Demand-Backup

Sie können sofort eine On-Demand-Sicherung ausführen. Dies ist hilfreich, wenn Sie Änderungen an Ihrem System vornehmen und sicherstellen möchten, dass Sie vor dem Start über eine Sicherungskopie verfügen.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Backupadministratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie in der KVM-Kachel **Erkennen und verwalten** aus.
3. Wählen Sie **Inventar**.
4. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
5. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**.
6. Wählen Sie die Registerkarte **Schutzgruppen**, **Datenspeicher** oder **Virtuelle Maschinen**.
7. Wählen Sie die Schutzgruppe aus, die Sie sichern möchten.
8. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.

   Die auf die Sicherung angewendete Richtlinie ist dieselbe Richtlinie, die der Schutzgruppe zugewiesen ist.

9. Wählen Sie die Zeitplanstufe aus.
10. Wählen Sie **Sichern**.

Wiederherstellen virtueller KVM-Maschinen mit NetApp Backup and Recovery

Stellen Sie virtuelle KVM-Maschinen aus Snapshots, aus einer auf einen Sekundärspeicher replizierten Schutzgruppensicherung oder aus in Objektspeichern gespeicherten Sicherungen mithilfe von NetApp Backup and Recovery wieder her.

Von diesen Speicherorten wiederherstellen

Sie können virtuelle Maschinen von verschiedenen Startorten aus wiederherstellen:

- Wiederherstellung von einem primären Standort (lokaler Snapshot)
- Wiederherstellen von einer replizierten Ressource auf einem sekundären Speicher
- Wiederherstellung aus einer Objektspeichersicherung

Stellen Sie diese Punkte wieder her

Sie können Daten bis zu diesen Punkten wiederherstellen:

- Am ursprünglichen Speicherort wiederherstellen
- An einem alternativen Speicherort wiederherstellen

Überlegungen zur Wiederherstellung aus dem Objektspeicher

Wenn Sie eine Sicherungsdatei im Objektspeicher auswählen und für diese Sicherung der Ransomware-Schutz aktiviert ist (wenn Sie Datalock und Ransomware-Schutz in der Sicherungsrichtlinie aktiviert haben), werden Sie aufgefordert, vor der Wiederherstellung der Daten eine zusätzliche Integritätsprüfung der Sicherungsdatei durchzuführen. Wir empfehlen, die Überprüfung durchzuführen.

Für den Zugriff auf den Inhalt der Sicherungsdatei fallen bei Ihrem Cloud-Anbieter zusätzliche Kosten für den Datenverkehr an.

So funktioniert die Wiederherstellung virtueller Maschinen

Wenn Sie virtuelle Maschinen wiederherstellen, geschieht Folgendes:

- Wenn Sie eine Workload aus einer lokalen Sicherungsdatei wiederherstellen, erstellt NetApp Backup and Recovery mithilfe der Daten aus der Sicherung eine *neue* Ressource.
- Wenn Sie eine Wiederherstellung von einer replizierten VM durchführen, können Sie diese auf dem Originalsystem oder auf einem lokalen ONTAP -System wiederherstellen.
- Wenn Sie eine Sicherung aus dem Objektspeicher wiederherstellen, können Sie die Daten auf dem ursprünglichen System oder auf einem lokalen ONTAP -System wiederherstellen.

Auf der Seite „Wiederherstellen“ können Sie eine VM wiederherstellen, selbst wenn Sie sich nicht mehr an den genauen Namen, den Speicherort oder das Datum des letzten fehlerfreien Zustands erinnern. Sie können mithilfe von Filtern nach dem Snapshot suchen.

Wiederherstellen von KVM-VMs

Stellen Sie KVM-VMs über das Menü „Wiederherstellen“ wieder her. Sie können den Snapshot anhand seines Namens oder mithilfe von Filtern suchen.

Erforderliche Konsolenrolle Superadministrator für Backup und Wiederherstellung oder Administratorrolle für Backup und Wiederherstellung zur Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
3. Wählen Sie aus der Dropdown-Liste rechts neben dem Namenssuchfeld **KVM** aus.
4. Geben Sie den Namen der VM ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem VM-Host oder Speicherpool, in dem sich die wiederherzustellende Ressource befindet.

   Es wird eine Liste mit Snapshots angezeigt, die Ihren Suchkriterien entsprechen.

5. Wählen Sie die Schaltfläche **Wiederherstellen** für den Snapshot, den Sie wiederherstellen möchten.

   Es wird eine Liste möglicher Wiederherstellungspunkte angezeigt.

6. Wählen Sie den Wiederherstellungspunkt aus, den Sie verwenden möchten.
7. Wählen Sie einen Quellspeicherort für den Snapshot aus.
8. Wählen Sie **Weiter**, um fortzufahren.
9. Wählen Sie das Wiederherstellungsziel und die Einstellungen aus:

   Zielauswahl

Am ursprünglichen Speicherort wiederherstellen

a. Wählen Sie den Bereich **Ursprünglicher Speicherort** aus.

b. Aktivieren Sie im Abschnitt **Optionen nach der Wiederherstellung** die Option **Virtuelle Maschine neu starten**, um die VM nach Abschluss des Wiederherstellungsvorgangs neu zu starten.

An einem anderen Speicherort wiederherstellen

a. Wählen Sie den Bereich **Alternativer Standort** aus.

b. Geben Sie im Abschnitt **Cloudstack settings**: die folgenden Informationen an:

- **Zone**: Wählen Sie eine Zielzone CloudStack aus der Liste.
- **Pod**: Wählen Sie aus der Liste einen Ziel-Pod innerhalb der ausgewählten Zone aus.
- **Cluster**: Wählen Sie einen Ziel-Cluster innerhalb des ausgewählten Pods aus der Liste aus.
- **Host**: Wählen Sie aus der Liste einen Zielhost im Cluster aus.
- **Speicherpool**: Wählen Sie einen Zielspeicherpool aus der Liste (das Zielvolume sollte sich hier befinden).
- **Netzwerk**: Wählen Sie das Netzwerk aus, mit dem die wiederhergestellte VM verbunden wird.
- **VM-Name**: Geben Sie einen Namen für die wiederherzustellende VM ein.
- **Anzeigename**: Geben Sie den Namen ein, der für diese VM in Backup and Recovery angezeigt werden soll.
- **Speicherpoolpfad**: Geben Sie den Speicherpoolpfad ein, in dem die VM-Volumes gespeichert werden sollen.

c. Wählen Sie aus der Liste **Serviceangebot auswählen** das Serviceangebot aus, das Ihrem bevorzugten Ressourceneinsatz entspricht.

d. Aktivieren Sie die Option **Erzwungen**, um die wiederhergestellte VM auch dann zu importieren, wenn eine oder mehrere MAC-Adressen der Netzwerkkarte der VM bereits vorhanden sind. Existiert eine MAC-Adresse bereits, wird für diese Netzwerkkarte eine neue MAC-Adresse generiert.

e. Im Abschnitt **Optionen nach der Wiederherstellung** sollten Sie folgende Optionen in Betracht ziehen:

- **Virtuelle Maschine neu starten**: Aktivieren Sie diese Option, um die neue virtuelle Maschine nach der Wiederherstellung zu starten.

10. Wählen Sie **Wiederherstellen**.