Schützen Sie Hyper-V-Workloads

NetApp Backup and Recovery

NetApp
June 25, 2026

Inhalt

Schützen Sie Hyper-V-Workloads

Übersicht zum Schützen von Hyper-V-Workloads

Schützen Sie Ihre Hyper-V-VMs mit NetApp Backup and Recovery. NetApp Backup and Recovery bietet schnelle, speichereffiziente, absturzsichere und VM-konsistente Backup- und Wiederherstellungsvorgänge sowohl für eigenständige Instanzen als auch für FCI-Cluster-Instanzen. Sie können auch Hyper-V-VMs schützen, die mit System Center Virtual Machine Manager (SCVMM) bereitgestellt und auf einer CIFS-Freigabe gehostet werden.

Sie können Hyper-V-Workloads auf Amazon Web Services S3 oder StorageGRID sichern und Hyper-V-Workloads auf einem lokalen Hyper-V-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.
- Mehrere Medientypen gewährleisten die Failover-Funktionalität im Falle eines physischen oder logischen Ausfalls eines Medientyps.
- Mithilfe der Vor-Ort-Kopie können Sie Daten schnell wiederherstellen und Sie können die Offsite-Kopien verwenden, wenn die Vor-Ort-Kopie kompromittiert ist.

Wenn Sie Hyper-V-Hosts hinzufügen und Ressourcen ermitteln, installiert NetApp Backup and Recovery das NetApp Hyper-V-Plug-in und das NetApp SnapCenter Windows FileSystem-Plug-in auf dem Hyper-V-Host, um die Verwaltung und den Schutz virtueller Maschinen zu unterstützen.

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

- "Entdecken Sie Hyper-V-Workloads"
- "Erstellen und Verwalten von Schutzgruppen für Hyper-V-Workloads"
- "Sichern Sie Hyper-V-Workloads"
- "Wiederherstellen von Hyper-V-Workloads"

Entdecken Sie Hyper-V-Workloads in NetApp Backup and Recovery

NetApp Backup and Recovery muss virtuelle Hyper-V-Maschinen erkennen, bevor Sie sie schützen können.

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" .

Hinzufügen eines Hyper-V-Hosts und Ermitteln von Ressourcen

Fügen Sie Hyper-V-Hostinformationen hinzu und lassen Sie NetApp Backup and Recovery virtuelle Maschinen erkennen. Wählen Sie in jedem Konsolenagenten die Systeme aus, auf denen Sie die Ressourcen ermitteln möchten.

Wenn Sie Hyper-V-Hosts hinzufügen und Ressourcen ermitteln, installiert NetApp Backup and Recovery das NetApp Hyper-V-Plug-in und das NetApp SnapCenter Windows FileSystem-Plug-in auf dem Hyper-V-Host, um die Verwaltung und den Schutz virtueller Maschinen zu unterstützen.

Schritte

1. Wählen Sie im NetApp Console **Schutz** > **Sicherung und Wiederherstellung**.

   Wenn Sie sich zum ersten Mal bei NetApp Backup and Recovery anmelden und bereits ein System in der Konsole haben, aber noch keine Ressourcen entdeckt haben, wird die Zielseite „Willkommen beim neuen NetApp Backup and Recovery“ angezeigt und bietet die Option „Ressourcen entdecken“.

2. Wählen Sie **Ressourcen entdecken**.
3. Geben Sie die folgenden Informationen ein:
   a. **Workload-Typ**: Wählen Sie **Hyper-V**.
   b. Wenn Sie für diesen Hyper-V-Host noch keine Anmeldeinformationen gespeichert haben, wählen Sie **Anmeldeinformationen hinzufügen**.
      i. Wählen Sie den Konsolenagenten aus, der mit diesem Host verwendet werden soll.
      ii. Geben Sie einen Namen für diese Anmeldeinformationen ein.
      iii. Geben Sie den Benutzernamen und das Kennwort für das Konto ein.
      iv. Wählen Sie **Fertig**.
   c. **Hostregistrierung**: Fügen Sie einen neuen Hyper-V-Host hinzu, indem Sie den FQDN oder die IP-Adresse des Hosts, die Anmeldeinformationen, den Konsolenagenten und die Portnummer eingeben. Falls der FQDN vom Konsolenagenten nicht aufgelöst werden kann, verwenden Sie stattdessen die IP-Adresse. Geben Sie für FCI-Cluster die Management-IP-Adresse des FCI-Clusters ein.
4. Wählen Sie **Entdecken**.

   Dieser Vorgang kann einige Minuten dauern.

Ergebnis

Nachdem NetApp Backup and Recovery Ressourcen erkannt hat, wird auf der Seite „Inventar“ die Hyper-V-Arbeitslast in der Liste der Arbeitslasten 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 Hyper-V-Workloads mit NetApp Backup and Recovery

Erstellen Sie Schutzgruppen, um die Sicherungsvorgänge für eine Reihe virtueller Maschinen zu verwalten. Eine Schutzgruppe ist eine logische Gruppierung von Ressourcen wie VMs, die Sie gemeinsam schützen möchten.

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 Hyper-V-Workloads" .
- Löschen Sie eine Schutzgruppe.

Erstellen einer Schutzgruppe

Gruppieren Sie Workloads, die Sie gemeinsam schützen möchten, in einer Schutzgruppe. Erstellen Sie eine Schutzgruppe, um Workloads gemeinsam zu sichern und wiederherzustellen.

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" .

Bevor Sie beginnen

- Beachten Sie, dass bei Hyper-V-Workloads die geplante Sicherungszeit in der Zeitzone des Verwaltungshosts interpretiert wird. Weitere Informationen finden Sie unter "Erstellen und Verwalten von Hyper-V-Backup-Richtlinien in NetApp Backup und Recovery".

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 das Menü **Schutzgruppen**.
5. Wählen Sie **Schutzgruppe erstellen**.
6. Geben Sie einen Namen für die Schutzgruppe ein.
7. Wählen Sie die VMs aus, die Sie in die Schutzgruppe aufnehmen möchten.
8. Wählen Sie **Weiter**.
9. Wählen Sie die **Sicherungsrichtlinie** aus, die Sie auf die Schutzgruppe anwenden möchten.
10. Wählen Sie **Weiter**.
11. Überprüfen Sie die Konfiguration.
12. Wählen Sie **Erstellen** aus, um die Schutzgruppe zu erstellen.

Bearbeiten Sie eine Schutzgruppe

Bearbeiten Sie eine Schutzgruppe, um deren Namen oder Einstellungen zu ändern. Möglicherweise möchten Sie eine Schutzgruppe bearbeiten, wenn sich die Ressourcen in der Gruppe geändert haben.

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**.

   Der Assistent zum Bearbeiten der Schutzgruppe führt Sie durch die Einstellungen in der Schutzgruppe.

7. Auf jedem Bildschirm des Assistenten sind die erforderlichen Änderungen vorzunehmen.
8. Nach Abschluss **Absenden** auswählen.

Eine aktualisierte Host-Zeitzone auf eine bestehende Schutzgruppe anwenden

Geplante Backups verwenden die Zeitzone des Hyper-V-Hosts, die beim Erstellen des Zeitplans der Schutzgruppe festgelegt wurde. Wenn die Zeitzone des Hosts geändert wird, laufen bestehende Schutzgruppen weiterhin in ihrer ursprünglichen Zeitzone (in der Regel UTC), bis deren Zeitpläne aktualisiert werden.

> ⓘ Zeitpläne werden nur neu erstellt, wenn der Name der Schutzgruppe geändert, eine VM hinzugefügt oder entfernt, die zugewiesene Richtlinie geändert oder Vor-/Nachbearbeitungsskripte aktualisiert werden. Das Speichern ohne Änderungen aktualisiert die Zeitpläne nicht. Diese Aktualisierung des Zeitplans ist eine einmalige Aktion pro Schutzgruppe und startet keine sofortige Sicherung.

Schritte

1. Der Hyper-V-Host wird aktualisiert, sodass seine aktuelle Zeitzone abgerufen wird.
2. Die Schutzgruppe kann bearbeitet und ihr Name auf einen anderen Wert geändert werden, anschließend wird gespeichert.

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 Hyper-V-Backup-Richtlinien in NetApp Backup und Recovery

In NetApp Backup and Recovery können Sie Ihre eigenen Hyper-V-Backup-Richtlinien erstellen, die die Backup-Häufigkeit, den Zeitpunkt der Backup-Erstellung und die Anzahl der aufzubewahrenden Backup-Dateien festlegen.

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
- Richtlinien löschen

> Bei Hyper-V-Workloads verwenden Sicherungszeitpläne die Zeitzone des Hyper-V-Hosts, nicht UTC oder die lokale Zeit Ihres Browsers. Diese Zeitzone wird beim Erstellen des Zeitplans festgelegt. Wenn sich die Zeitzone des Hosts ändert, ist es erforderlich, den Host zu aktualisieren und den Zeitplan neu zu erstellen, damit die neue Zeitzone wirksam wird. Weitere Informationen sind unter "Erstellen und Verwalten von Schutzgruppen für Hyper-V-Workloads" verfügbar.

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 **Hyper-V**.
   - 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.

     Bei VMware-Workloads wird dadurch der lokale Snapshot auf den Datenspeichern oder VMs auf dem primären Speicher konfiguriert und vom primären Festplattenspeicher auf den sekundären Festplattenspeicher sowie vom primären auf den Cloud-Objektspeicher repliziert.

   - **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.
     - **Archivprotokolle nach der Sicherung löschen**: Wenn die Sicherung von Protokollen aktiviert ist, können Sie diese Funktion optional aktivieren, um die Aufbewahrungsdauer der Oracle-Archivprotokolle durch Backup and Recovery zu begrenzen. Sie können die Aufbewahrungsdauer sowie den Ort festlegen, an dem Backup and Recovery die Archivprotokolle löschen soll.
   - **Anbieter**: Wählen Sie den Speicheranbieter aus, der die Kubernetes-Anwendungsressourcen hostet, und geben Sie die Anmeldeinformationen zur Authentifizierung beim Anbieter 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**:
     - **Applikationskonsistenten Snapshot aktivieren**: Aktivieren Sie diese Option, um applikationskonsistente Snapshots zu erstellen. Hierfür müssen sowohl Hyper-V Integration Services als auch VSS auf der VM ausgeführt werden. Falls einer der beiden Dienste nicht ausgeführt wird, wird stattdessen ein absturzkonsistenter Backup erstellt. Beachten Sie, dass die Aktivierung der Applikationskonsistenz sowohl die Backup-Zeit als auch den Speicherplatzbedarf erhöhen kann. Zusätzlich wird der Gast-Arbeitsspeicher (RAM) der VM nicht in applikationskonsistente 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 DataLock-Sperrung auf dem Objektspeicher. Geben Sie die Scanfrequenz in Tagen ein. Diese Option gilt für Objektspeicher. Beachten Sie, dass diese Option

je nach Cloud-Anbieter zusätzliche Kosten verursachen kann.

- **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.

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 Hyper-V-Workloads mit NetApp Backup and Recovery

Sichern Sie Hyper-V-VMs von lokalen ONTAP Systemen auf Amazon Web Services, Azure NetApp Files oder StorageGRID, um sicherzustellen, dass Ihre Daten geschützt sind. Backups werden automatisch erstellt und in einem Objektspeicher in Ihrem öffentlichen oder privaten Cloud-Konto gespeichert.

- Um Workloads 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 Hyper-V-Workloads mit NetApp Backup and Recovery" für weitere Informationen.
- Sichern Sie jetzt Workloads (erstellen Sie jetzt ein On-Demand-Backup).

Sichern Sie Workloads jetzt mit einem On-Demand-Backup

Verwenden Sie On-Demand-Backups, damit Ihre Daten geschützt sind, bevor Sie Systemänderungen vornehmen.

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 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**, **Datenspeicher** oder **Virtuelle Maschinen**.
5. Wählen Sie die Schutzgruppe oder virtuellen Maschinen aus, die Sie sichern möchten.
6. Wählen Sie das Symbol Aktionen ••• > **Jetzt sichern**.

   Für die Sicherung wird dieselbe Richtlinie verwendet, die Sie der Schutzgruppe oder virtuellen Maschine zugewiesen haben.

7. Wählen Sie die Zeitplanstufe aus.
8. Wählen Sie **Sichern**.

Wiederherstellen von Hyper-V-Workloads

Wiederherstellen von Hyper-V-Workloads mit NetApp Backup and Recovery

Stellen Sie Hyper-V-Workloads aus Snapshots, aus einer auf Sekundärspeicher replizierten Workload-Sicherung oder aus in Objektspeichern gespeicherten Sicherungen mithilfe von NetApp Backup and Recovery wieder her.

Von diesen Speicherorten wiederherstellen

Sie können Workloads von verschiedenen Startorten wiederherstellen:

- Wiederherstellung von einem primären Standort (lokaler Snapshot)
- Wiederherstellen von einer replizierten Ressource auf einem sekundären Speicher
- Wiederherstellung aus einem Objektspeicher-Backup (nur am ursprünglichen Speicherort)

Stellen Sie diese Punkte wieder her

Sie können Daten bis zu diesen Punkten wiederherstellen:

- Wiederherstellung am ursprünglichen Speicherort (vom primären, sekundären und Objektspeicher)
- Wiederherstellung an einem alternativen Speicherort (vom primären und sekundären Speicher)

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 von Workloads

Beim Wiederherstellen von Workloads 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 aus einem replizierten Workload durchführen, können Sie den Workload auf dem ursprünglichen System oder auf einem lokalen ONTAP System wiederherstellen.

Auf der Seite „Wiederherstellen“ können Sie eine Ressource wiederherstellen, selbst wenn Sie sich nicht mehr an den genauen Namen, den Speicherort oder das Datum erinnern, an dem sie zuletzt in einwandfreiem Zustand war. Sie können mithilfe von Filtern nach dem Snapshot suchen.

Wiederherstellen von Hyper-V-Workloads

Stellen Sie Hyper-V-Workloads 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 Backup and Recovery -Menü **Wiederherstellen** aus.
2. Wählen Sie aus der Dropdown-Liste rechts neben dem Namenssuchfeld **Hyper-V** aus.
3. Geben Sie den Namen der Ressource ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem VM-Namen, VM-Host oder Speicherpool, in dem sich die wiederherzustellende Ressource befindet.

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

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

   Es wird eine Liste möglicher Wiederherstellungspunkte angezeigt.

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

   Zielauswahl

   Am ursprünglichen Speicherort wiederherstellen

   a. Wählen Sie den Bereich **Ursprünglicher Speicherort** aus. Wenn Sie zum ursprünglichen Speicherort wiederherstellen, können Sie die Zieleinstellungen anzeigen, indem Sie den Abschnitt **Zieleinstellungen** erweitern, aber Sie können sie nicht ändern.

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

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

   An einem anderen Speicherort wiederherstellen

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

   b. Geben Sie im Abschnitt **Zieleinstellungen** die folgenden Informationen ein:

      - **Hyper-V FQDN oder IP-Adresse**: Geben Sie den vollqualifizierten Domänennamen oder die IP-Adresse des Ziel-Hyper-V-Hosts ein.
      - **Netzwerk**: Wählen Sie das Zielnetzwerk aus, in dem Sie den Snapshot wiederherstellen möchten.
      - **Name der virtuellen Maschine**: Geben Sie den Namen der VM ein, die Sie wiederherstellen möchten.
      - **Zielort**: Geben Sie den Zielordner oder die CIFS-Freigabe ein, die die wiederhergestellten Daten enthalten soll.

   c. Im Abschnitt **Vorbereitende Wiederherstellungsoptionen** sollten Sie folgende Optionen in Betracht ziehen:

      - **Schnellwiederherstellung**: Aktivieren Sie diese Option, um die wiederhergestellte VM sofort verfügbar zu machen. Aus dem Objektspeicher werden nur die zum Ausführen der VM benötigten Dateien wiederhergestellt, nicht das gesamte Volume.

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

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

9. Wählen Sie **Wiederherstellen**.

Dateien und Ordner aus Hyper-V-VM-Backups wiederherstellen

Stellen Sie Dateien und Ordner aus Hyper-V-VM-Backups auf primärem oder sekundärem Speicher in einer Windows-Gast-VM wieder her.

Dateien und Ordner wiederherstellen

Eine virtuelle Festplatte aus einem Snapshot einbinden und Dateien und Ordner von dort in die ursprüngliche (Quell-)Windows-VM wiederherstellen.

Bevor Sie beginnen

Bevor Sie Dateien und Ordner wiederherstellen können, müssen Sie eine Anmeldeinformation für die Quell-VM in NetApp Backup and Recovery erstellen. Diese Anmeldeinformation wird zur Authentifizierung bei der VM während des Wiederherstellungsprozesses verwendet.

Informationen zu diesem Vorgang

Wenn Sie eine Datei- und Ordnerwiederherstellungssitzung durch Einbinden eines virtuellen Laufwerks öffnen, bleibt die Sitzung 48 Stunden lang aktiv.

Die Wiederherstellungsleistung hängt sowohl von der Größe als auch von der Anzahl der wiederherzustellenden Dateien oder Ordner ab. Bei gleicher Datensatzgröße dauert die Wiederherstellung einer großen Anzahl kleiner Dateien in der Regel länger als die Wiederherstellung einer kleinen Anzahl großer Dateien.

Beachten Sie beim Wiederherstellen von Dateien und Ordnern Folgendes:

- Derzeit ist es nicht möglich, Dateien und Ordner auf Linux-Gast-VMs wiederherzustellen.
- Das Wiederherstellen von Dateien und Ordnern aus auf Objektspeicher abgelegten Backups wird nicht unterstützt.
- Auf einer VM kann gleichzeitig nur ein Anfüge- oder Wiederherstellungsvorgang ausgeführt werden. Sie können auf derselben VM keine parallelen Anfüge- oder Wiederherstellungsvorgänge ausführen.
- Das Anzeigen oder Durchsuchen reservierter Partitionen kann zu einem Fehler führen.
- Während des Wiederherstellungsvorgangs werden die Attribute „Versteckt“, „System“ und „Verschlüsselt“ von Gastdateien in der wiederhergestellten Datei nicht beibehalten.
- Sie können Systemdateien und versteckte Dateien anzeigen und wiederherstellen sowie verschlüsselte Dateien anzeigen.
- Überschreiben Sie keine vorhandene Systemdatei und stellen Sie verschlüsselte Dateien nicht in einem verschlüsselten Ordner wieder her.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
2. Wählen Sie **Hyper-V** aus der Liste der Workloads oben rechts auf der Seite aus.
3. Wählen Sie in der Liste der virtuellen Maschinen die Aktion **Wiederherstellen** für eine VM aus, die Dateien oder Ordner enthält, die Sie wiederherstellen möchten.
4. Wählen Sie **Dateien und Ordner** aus.
5. Gehen Sie auf der Seite **Aus Snapshots wiederherstellen** wie folgt vor:
   a. Optional können Sie einen Zeitraum auswählen, um die Liste der Snapshots nach Erstellungszeit zu

filtern.

b. Wählen Sie einen Snapshot auf dem primären oder sekundären Speicher aus, von dem die Wiederherstellung erfolgen soll, und klicken Sie dann auf **Weiter**.

6. Wählen Sie in der Liste eine virtuelle Festplatte aus, die die Dateien und Ordner enthält, die Sie wiederherstellen müssen, und wählen Sie dann **Weiter** aus.
7. Führen Sie auf der Seite *Details zur Gast-VM* die folgenden Schritte aus:

   a. Im Abschnitt **Details zur Gast-VM** hängen Sie die virtuelle Festplatte an die ursprüngliche VM an, indem Sie **Original virtual machine** auswählen.

   b. Optional können Sie im Abschnitt **Anmeldeinformationen der Gast-VM**, falls Sie noch keine Anmeldeinformationen für die Quell-VM-Festplatte und die Ziel-VM gespeichert haben, **Anmeldeinformationen hinzufügen** auswählen, die Windows-Anmeldeinformationen eingeben und **Hinzufügen** auswählen.

   c. Wählen Sie aus der Liste die Anmeldeinformationen für die virtuelle Maschine aus.

   d. Wählen Sie **Weiter**.

      NetApp Backup und Recovery verbindet die virtuelle Festplatte mit der ursprünglichen VM und zeigt alle Dateien und Ordner an, einschließlich der versteckten. Jedem Partition, einschließlich der systemreservierten Partitionen, wird ein Laufwerksbuchstabe zugewiesen.

   Sie können das Lupensymbol (Suchsymbol) neben dem Dateibrowser verwenden, um nach Dateien und Ordnern zu suchen. Die Mustererkennung wird nicht unterstützt, aber Sie können nach Dateien oder Ordnern anhand eines Teils des Namens oder der Erweiterung suchen.

8. Gehen Sie auf der Seite „Dateien oder Ordner zum Wiederherstellen auswählen“ wie folgt vor:

   a. Wählen Sie die wiederherzustellenden Dateien oder Ordner aus.

      Die zur Wiederherstellung ausgewählten Dateien und Ordner werden im Bereich **Ausgewählte Dateien und Ordner** aufgelistet.

   b. Wählen Sie **Weiter**.

9. Führen Sie auf der Seite „Gastdatei wiederherstellen – Ziel“ folgende Schritte aus:

   a. Geben Sie im Abschnitt „Wiederherstellen unter Pfad“ den UNC-Pfad zum Ziel-VM- und Dateisystemspeicherort ein, an dem die ausgewählten Dateien wiederhergestellt werden sollen:

      - IPv4-Pfadbeispiel: `\\10.60.136.65\c$`
      - IPv6-Pfadbeispiel: `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`

   Falls bereits Dateien mit demselben Namen existieren, können Sie diese überschreiben oder überspringen.

10. Im Abschnitt „Optionen nach der Wiederherstellung“ können Sie die Gastsitzung nach Abschluss der Wiederherstellung optional trennen, indem Sie die Einstellung **Gastsitzung nach Abschluss der Wiederherstellung trennen** aktivieren. Dadurch wird die virtuelle Festplatte getrennt und der Datenspeicher ausgehängt. Das bedeutet, dass Sie die Gastsitzung erneut verbinden müssen, bevor Sie weitere Datei- und Ordnerwiederherstellungsvorgänge durchführen können.
11. Wählen Sie **Wiederherstellen**.

    Den Fortschritt der Wiederherstellung können Sie auf der Seite „Auftragsüberwachung“ einsehen.

Aktive Live-Disk-Mount-Sitzungen verwalten

Zeigen Sie die aktiven Hyper-V-Datei- und Ordnerwiederherstellungssitzungen in Backup und Recovery an, verwenden Sie sie und löschen Sie sie.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.
2. Wählen Sie **Hyper-V** aus der Liste der Workloads oben rechts auf der Seite aus.
3. Wählen Sie das Menü **Live-Disk-Mount-Sitzungen**.

   Es wird die Liste der offenen virtuellen Festplatten-Mount-Sitzungen angezeigt.

4. Optional können Sie eine Sitzung nutzen, um Dateien und Ordner auf einer Gast-VM wiederherzustellen. Öffnen Sie dazu das Menü ••• „Aktionen“ der Sitzung und wählen Sie **Dateien und Ordner wiederherstellen**.
5. Optional können Sie eine Sitzung löschen, indem Sie das Menü ••• „Aktionen“ für die jeweilige Sitzung öffnen und **Löschen** auswählen.