Schutz von VMware-Workloads

NetApp Backup and Recovery

NetApp
June 24, 2026

Inhalt

Schutz von VMware-Workloads

Überblick zum Schutz von VMware-Workloads mit NetApp Backup and Recovery

VMware-VMs und Datenspeicher lassen sich mit NetApp Backup and Recovery schützen. NetApp Backup and Recovery bietet schnelle, platzsparende, absturzkonsistente und VM-konsistente Backup- und Wiederherstellungsvorgänge. VMware-Workloads können auf unterstützte Backup-Ziele gesichert und auf einen lokalen VMware-Host wiederhergestellt werden.

Diese Version von NetApp Backup and Recovery unterstützt nur VMware vCenter und erkennt keine vVols oder VMs auf vVols.

Verwenden Sie NetApp Backup and Recovery , um eine 3-2-1-Strategie 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 VMware-Workloads ausführen:

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

Entdecken Sie VMware-Workloads mit NetApp Backup and Recovery

Damit Sie den Dienst nutzen können, muss der NetApp Backup and Recovery -Dienst zunächst VMware-Datenspeicher und VMs erkennen, die auf ONTAP -Systemen ausgeführt werden. Sie können optional Sicherungsdaten und Richtlinien aus dem SnapCenter Plug-in for VMware vSphere importieren, wenn Sie es bereits installiert haben.

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" .

Entdecken Sie VMware-Workloads und importieren Sie optional SnapCenter -Ressourcen

Während der Erkennungsphase analysiert NetApp Backup and Recovery die VMware-Workloads innerhalb Ihrer Organisation und bewertet und importiert vorhandene Schutzrichtlinien, Snapshots sowie Backup- und Wiederherstellungsoptionen.

Sie können VMware NFS- und VMFS-Datenspeicher und VMs von ihrem lokalen SnapCenter Plug-in for VMware vSphere in das NetApp Backup and Recovery Inventar importieren.

Diese Version von NetApp Backup and Recovery unterstützt nur VMware vCenter und erkennt keine vVols oder VMs auf vVols.

Während des Importvorgangs führt NetApp Backup and Recovery die folgenden Aufgaben aus:

- Ermöglicht sicheren SSH-Zugriff auf den vCenter-Server.
- Aktiviert den Wartungsmodus für alle Ressourcengruppen im vCenter-Server.
- Bereitet die Metadaten des vCenters vor und markiert es in der NetApp Console als nicht verwaltet.
- Konfiguriert den Datenbankzugriff.
- Erkennt VMware vCenter, Datenspeicher und VMs.
- Importiert bestehende Schutzrichtlinien, Snapshots sowie Sicherungs- und Wiederherstellungsoptionen aus dem SnapCenter Plug-in for VMware vSphere.
- Zeigt die erkannten Ressourcen auf der Inventarseite von NetApp Backup and Recovery an.

Die Ermittlung erfolgt auf folgende Weise:

- Wenn Sie bereits über das SnapCenter Plug-in for VMware vSphere verfügen, importieren Sie SnapCenter Ressourcen mithilfe der NetApp Backup and Recovery -Benutzeroberfläche in NetApp Backup and Recovery and Recovery.

  Wenn Sie bereits über das SnapCenter -Plug-in verfügen, stellen Sie sicher, dass Sie die Voraussetzungen erfüllt haben, bevor Sie aus SnapCenter importieren. Beispielsweise sollten Sie zunächst in der NetApp Console Systeme für den gesamten lokalen SnapCenter -Clusterspeicher erstellen, bevor Sie aus SnapCenter importieren. Sehen"Voraussetzungen für den Import von Ressourcen aus SnapCenter" .

- Wenn Sie das SnapCenter -Plug-in noch nicht haben, können Sie Workloads in Ihren Systemen trotzdem ermitteln, indem Sie manuell ein vCenter hinzufügen und die Erkennung durchführen.

Wenn das SnapCenter Plug-in noch nicht installiert ist, fügen Sie ein vCenter hinzu und ermitteln Sie Ressourcen

Wenn Sie das SnapCenter Plug-in für VMware noch nicht installiert haben, fügen Sie vCenter-Informationen hinzu und lassen Sie NetApp Backup and Recovery die Workloads erkennen. Wählen Sie in jedem Konsolenagenten die Systeme aus, auf denen Sie Workloads ermitteln möchten.

Schritte

1. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Sicherung und Wiederherstellung**.

   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.

2. Wählen Sie **Ressourcen entdecken**.
3. Geben Sie die folgenden Informationen ein:
   a. **Workload-Typ**: Wählen Sie **VMware**.
   b. **vCenter-Einstellungen**: Fügen Sie ein neues vCenter hinzu. Um ein neues vCenter hinzuzufügen, geben Sie den FQDN oder die IP-Adresse, den Benutzernamen, das Kennwort, den Port und das Protokoll des vCenters ein.

      Wenn Sie vCenter-Informationen eingeben, geben Sie Informationen sowohl für die vCenter-Einstellungen als auch für die Host-Registrierung ein. Wenn Sie hier vCenter-Informationen hinzugefügt oder eingegeben haben, müssen Sie als Nächstes auch Plugin-Informationen in den erweiterten Einstellungen hinzufügen.

   c. **Host-Registrierung**: Für VMware nicht erforderlich.
4. Wählen Sie **Entdecken**.

   Dieser Vorgang kann einige Minuten dauern.

5. Fahren Sie mit den erweiterten Einstellungen fort.

Wenn das SnapCenter -Plugin bereits installiert ist, importieren Sie das SnapCenter -Plugin für VMware-Ressourcen in NetApp Backup and Recovery

Wenn Sie das SnapCenter Plug-in für VMware bereits installiert haben, importieren Sie die SnapCenter Plug-in-Ressourcen mit diesen Schritten in NetApp Backup and Recovery . Die Konsole erkennt ESXi-Hosts, Datenspeicher und VMs in vCentern und plant sie vom Plug-in aus. Sie müssen diese Informationen nicht alle neu erstellen.

Sie können dies auf folgende Weise tun:

- Wählen Sie während der Erkennung eine Option zum Importieren von Ressourcen aus dem SnapCenter -Plug-in aus.
- Wählen Sie nach der Erkennung auf der Inventarseite eine Option zum Importieren von SnapCenter -Plug -in-Ressourcen aus.
- Wählen Sie nach der Erkennung im Menü „Einstellungen“ eine Option zum Importieren von SnapCenter -Plug-in-Ressourcen aus. Weitere Einzelheiten finden Sie unter"Konfigurieren von NetApp Backup and Recovery" . Dies wird für VMware nicht unterstützt.

Dies ist ein zweiteiliger Prozess, der in diesem Abschnitt beschrieben wird:

1. Importieren Sie die vCenter-Metadaten aus dem SnapCenter -Plug-in. Die importierten vCenter-Ressourcen werden noch nicht von NetApp Backup and Recovery verwaltet.
2. Starten Sie die Verwaltung ausgewählter vCenter, VMs und Datenspeicher in NetApp Backup and Recovery. Nachdem Sie die Verwaltung initiiert haben, kennzeichnet NetApp Backup and Recovery das vCenter auf der Inventarseite als „Verwaltet“ und kann die von Ihnen importierten Ressourcen sichern und wiederherstellen. Nachdem Sie die Verwaltung in NetApp Backup and Recovery initiiert haben, verwalten Sie diese Ressourcen nicht mehr im SnapCenter Plug-in.

Importieren Sie vCenter-Metadaten aus dem SnapCenter -Plug-in

In diesem ersten Schritt werden vCenter-Metadaten aus dem SnapCenter -Plug-in importiert. Zu diesem Zeitpunkt werden die Ressourcen noch nicht von NetApp Backup and Recovery verwaltet.

Nachdem Sie vCenter-Metadaten aus dem SnapCenter -Plug-in importiert haben, übernimmt NetApp Backup and Recovery die Schutzverwaltung nicht automatisch. Dazu müssen Sie explizit auswählen, dass die importierten Ressourcen in NetApp Backup and Recovery verwaltet werden sollen. Dadurch wird sichergestellt, dass Sie bereit sind, diese Ressourcen durch NetApp Backup and Recovery sichern zu lassen.

Schritte

1. Wählen Sie in der linken Navigation der Konsole **Schutz** > **Sicherung und Wiederherstellung**.
2. Wählen Sie **Inventar**.
3. Wählen Sie auf der Seite „Workload-Ressourcen von NetApp Backup and Recovery ermitteln“ die Option „Aus SnapCenter importieren“ aus.
4. Wählen Sie im Feld „Importieren von“ die Option „SnapCenter Plug-in für VMware“ aus.
5. Geben Sie **VMware vCenter-Anmeldeinformationen** ein:
   a. **vCenter-IP/Hostname**: Geben Sie den FQDN oder die IP-Adresse des vCenters ein, das Sie in NetApp Backup and Recovery importieren möchten.
   b. **vCenter-Portnummer**: Geben Sie die Portnummer für das vCenter ein.
   c. **vCenter-Benutzername** und **Passwort**: Geben Sie den Benutzernamen und das Passwort für das vCenter ein.
   d. **Connector**: Wählen Sie den Konsolenagenten für das vCenter aus.
6. Geben Sie * Host-Anmeldeinformationen für das SnapCenter -Plug-in* ein:
   a. **Vorhandene Anmeldeinformationen**: Wenn Sie diese Option auswählen, können Sie die vorhandenen Anmeldeinformationen verwenden, die Sie bereits hinzugefügt haben. Wählen Sie den Namen der Anmeldeinformationen.
   b. **Neue Anmeldeinformationen hinzufügen**: Wenn Sie keine vorhandenen Anmeldeinformationen für den SnapCenter Plug-in-Host haben, können Sie neue Anmeldeinformationen hinzufügen. Geben Sie den Anmeldenamen, den Authentifizierungsmodus, den Benutzernamen und das Kennwort ein.
7. Wählen Sie **Importieren**, um Ihre Eingaben zu bestätigen und das SnapCenter -Plug-in zu registrieren.

Wenn das SnapCenter Plug-in bereits registriert ist, können Sie die vorhandenen Registrierungsdetails aktualisieren.

Ergebnis

Auf der Inventarseite wird das vCenter in NetApp Backup and Recovery als nicht verwaltet angezeigt, bis Sie es explizit für die Verwaltung auswählen.

Verwalten von aus dem SnapCenter -Plug-in importierten Ressourcen

Nachdem Sie die vCenter-Metadaten aus dem SnapCenter -Plug-in für VMware importiert haben, verwalten Sie die Ressourcen in NetApp Backup and Recovery. Nachdem Sie die Verwaltung dieser Ressourcen ausgewählt haben, kann NetApp Backup and Recovery die importierten Ressourcen sichern und wiederherstellen. Nachdem Sie die Verwaltung in NetApp Backup and Recovery initiiert haben, verwalten Sie diese Ressourcen nicht mehr im SnapCenter Plug-in.

Nachdem Sie die Verwaltung der Ressourcen ausgewählt haben, werden die Ressourcen, VMs und Richtlinien aus dem SnapCenter -Plug-in für VMware importiert. Die Ressourcengruppen, Richtlinien und Snapshots werden vom Plug-in migriert und in NetApp Backup and Recovery verwaltet.

Schritte

1. Nachdem Sie die VMware-Ressourcen aus dem SnapCenter -Plug-in importiert haben, wählen Sie im Menü „Sichern und Wiederherstellen“ die Option „Inventar“ aus.
2. Wählen Sie auf der Inventarseite das importierte vCenter aus, das von nun an von NetApp Backup and Recovery verwaltet werden soll.
3. Wählen Sie das Symbol Aktionen ••• > **Details anzeigen**, um die Arbeitslastdetails anzuzeigen.
4. Wählen Sie auf der Seite Inventar > Arbeitslast das Symbol Aktionen ••• > **Verwalten**, um die Seite „vCenter verwalten“ anzuzeigen.
5. Aktivieren Sie das Kontrollkästchen „Möchten Sie mit der Migration fortfahren?“ und wählen Sie **Migrieren**.

Ergebnis

Auf der Inventarseite werden die neu verwalteten vCenter-Ressourcen angezeigt.

Weiter zum NetApp Backup and Recovery Dashboard

1. Um das Dashboard anzuzeigen, wählen Sie im Menü „Sicherung und Wiederherstellung“ die Option **Dashboard**.
2. Überprüfen Sie den Zustand des Datenschutzes. Die Anzahl der gefährdeten oder geschützten Workloads steigt basierend auf den neu entdeckten, geschützten und gesicherten Workloads.

   "Erfahren Sie, was Ihnen das Dashboard anzeigt".

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

Erstellen Sie Schutzgruppen, um die Sicherungs- und Wiederherstellungsvorgänge für eine Reihe von Workloads zu verwalten. Eine Schutzgruppe ist eine logische Gruppierung von Ressourcen wie VMs und Datenspeichern, die Sie gemeinsam schützen möchten.

Sie können die folgenden Aufgaben im Zusammenhang mit Schutzgruppen ausführen:

- Erstellen Sie eine Schutzgruppe, indem Sie VMs manuell zur Gruppe hinzufügen oder VMware vSphere-Tags verwenden.
- Schutzdetails anzeigen.
- Sichern Sie jetzt eine Schutzgruppe. Siehe "Sichern Sie jetzt VMware-Workloads".
- Unterbrechen und Fortsetzen des Sicherungszeitplans einer Schutzgruppe.
- Löschen Sie eine Schutzgruppe.

Tag-basierte Schutzgruppen

Bei der Auswahl von Ressourcen, die einer Schutzgruppe hinzugefügt werden sollen, können Sie diese nach Datenspeichern, virtuellen Maschinen oder nach vSphere Tags organisieren.

Der tagbasierte Schutz (mittels vSphere Tags) vereinfacht die Verwaltung von Schutzgruppen in Backup und Recovery.

Die Verwendung von tagbasiertem Schutz bietet einige Vorteile:

- Wenn Sie einem VM oder Datastore in vCenter ein vSphere-Tag hinzufügen, wird dieses Objekt automatisch in das nächste Backup für jede NetApp Backup and Recovery-Schutzgruppe aufgenommen, die auf dieses Tag verweist.
- Wenn Sie einen vSphere-Tag von einer VM oder einem Datenspeicher entfernen, wird dieses Objekt automatisch von nachfolgenden Backups für diese tagbasierte Schutzgruppe ausgeschlossen.
- Wenn ein vSphere-Tag in vCenter gelöscht wird, überspringen zukünftige Backups diesen Tag und melden eine Warnung.
- Wird eine VM in einen anderen Datenspeicher migriert, bleibt sie so lange geschützt, wie sie noch das Tag besitzt, das Teil einer tagbasierten Schutzgruppe ist.

Die Tag-Zugehörigkeit wird zum Zeitpunkt der Sicherung von vCenter aufgelöst. Alle Änderungen, die Sie an Tags in vCenter vornehmen (Hinzufügen/Entfernen von Tags, Löschen von Tags, Hinzufügen/Entfernen von VMs), werden automatisch in der nächsten Sicherung berücksichtigt.

Erstellen einer Schutzgruppe

Erstellen Sie eine Schutzgruppe, um die Ressourcen zu organisieren, die Sie gemeinsam sichern und wiederherstellen möchten.

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

- Stellen Sie sicher, dass in Ihrer Umgebung unterstützte Versionen von VMware vSphere verwendet werden.
- Beim Erstellen einer tagbasierten Schutzgruppe stellen Sie sicher, dass die virtuellen Maschinen und Datenspeicher, die Sie schützen möchten, bereits einem oder mehreren vSphere-Tags in vCenter zugeordnet sind.
- Beachten Sie, dass bei VMware Workloads die geplante Sicherungszeit in der Zeitzone des Verwaltungshosts interpretiert wird. Weitere Informationen finden Sie unter "Erstellen und Verwalten von VMware-Sicherungsrichtlinien 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 die Registerkarte **Schutzgruppen**.
5. Wählen Sie **Schutzgruppe erstellen**.
6. Geben Sie einen Namen für die Schutzgruppe an und wählen Sie aus, wie Sie Ressourcen zur Schutzgruppe hinzufügen möchten. Sie können Ressourcen nach **Datenspeichern**, **Virtuellen Maschinen** oder **Tags** hinzufügen.

Das Mischen von Ressourcentypen (z. B. das Kombinieren von Tags mit einzelnen VMs oder Datenspeichern in derselben Schutzgruppe) wird nicht unterstützt.

7. Wählen Sie aus der angezeigten Liste die Ressourcen aus, die Sie in die Schutzgruppe aufnehmen möchten.

   Sie können die verfügbaren Ressourcen in der Liste filtern, indem Sie ein bestimmtes vCenter oder Rechenzentrum auswählen. Die ausgewählten Ressourcen werden rechts in der Liste angezeigt.

8. Wenn Sie fertig sind, wählen Sie **Weiter**.
9. Wählen Sie aus, wie die Schutzgruppe mit VMs umgeht, deren virtuelle Festplatten sich über mehrere Datenspeicher erstrecken:
   - **Alle übergeordneten Datenspeicher immer ausschließen**: Die Schutzgruppe umfasst nur Datenspeicher, die ihr direkt hinzugefügt werden, sowie den primären Datenspeicher aller VMs, die direkt der Schutzgruppe hinzugefügt wurden.
   - **Alle übergreifenden Datenspeicher immer einbeziehen**: Die Schutzgruppe umfasst alle Datenspeicher, die von den einbezogenen VMs übergreifend genutzt werden.
   - **Manuelle Auswahl der einzuschließenden übergreifenden Datenspeicher**: Wenn Sie diese Option wählen, müssen Sie die übergreifenden Datenspeicher, die in die Schutzgruppe aufgenommen werden sollen, manuell aus der angezeigten Liste auswählen. Diese Auswahl ist statisch; Sie müssen die Liste der übergreifenden Datenspeicher jedes Mal aktualisieren, wenn neue VMs zur Gruppe hinzugefügt werden.
10. Wählen Sie **Weiter**.
11. Wählen Sie die Datensicherungsstrategie, die Sie auf die Schutzgruppe anwenden möchten.

    Um eine neue Richtlinie zu erstellen, wählen Sie **Neue Richtlinie erstellen** und folgen Sie den Anweisungen. Weitere Informationen finden Sie unter "Erstellen von Richtlinien".

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

Aussetzen des Sicherungszeitplans einer Schutzgruppe

Setzen Sie eine Schutzgruppe aus, um ihre geplanten Sicherungen anzuhalten.

Wenn Sie eine Schutzgruppe aussetzen, ändert sich der Schutzstatus in „In Wartung“. Sie können den Sicherungszeitplan jederzeit fortsetzen.

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 das Symbol Aktionen ••• > **Schutzgruppe aussetzen**.
6. Überprüfen Sie die Bestätigungsnachricht und wählen Sie **Aussetzen**.

Fortsetzen des Sicherungszeitplans einer Schutzgruppe

Durch die Wiederaufnahme einer angehaltenen Schutzgruppe werden die geplanten Sicherungen für die Schutzgruppe neu gestartet.

Der Schutzstatus ändert sich von „In Wartung“, wenn Sie eine Schutzgruppe aussetzen, zu „Geschützt“, wenn Sie sie wieder aufnehmen. Sie können den Sicherungszeitplan jederzeit fortsetzen.

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 das Symbol Aktionen ••• > **Schutzgruppe fortsetzen**.
6. Überprüfen Sie die Bestätigungsnachricht und wählen Sie **Fortsetzen**.

Ergebnis

Das System validiert die Zeitpläne und ändert den Schutzstatus auf „Geschützt“, wenn die Zeitpläne gültig sind. Wenn die Zeitpläne ungültig sind, zeigt das System eine Fehlermeldung an und nimmt die Schutzgruppe nicht wieder auf.

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 vCenter-Zeitzone auf eine bestehende Schutzgruppe anwenden

Geplante Backups verwenden die vCenter Server-Zeitzone, die beim Erstellen des Zeitplans der Schutzgruppe festgelegt wird. Wenn die vCenter Server-Zeitzone geändert wird, laufen bestehende Schutzgruppen weiterhin in ihrer ursprünglichen Zeitzone (typischerweise 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. Aktualisieren Sie den vCenter Server, damit 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

Wenn Sie eine Schutzgruppe löschen, entfernen Sie diese und alle Sicherungszeitpläne für die Gruppe. Löschen Sie eine Schutzgruppe, wenn Sie sie nicht mehr benötigen.

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 VMware-Sicherungsrichtlinien in NetApp Backup und Recovery

In NetApp Backup and Recovery können Sie Ihre eigenen VMware-Backup-Richtlinien erstellen, die die Backup-Häufigkeit, den Zeitpunkt der Backup-Erstellung und die Anzahl der aufzubewahrenden 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 löschen

Für VMware-Workloads verwenden Sicherungspläne die Zeitzone des VMware vCenter Servers, nicht UTC oder die lokale Zeit Ihres Browsers. Diese Zeitzone wird beim Erstellen des Zeitplans festgelegt. Wenn sich die Zeitzone des Hosts ändert, ist eine Aktualisierung des Hosts und eine Neuerstellung des Zeitplans erforderlich, damit die neue Zeitzone wirksam wird. Weitere Informationen sind unter "Erstellen und Verwalten von Schutzgruppen für VMware-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 **VMware**.
- 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.

     Für VMware-Workloads wird dadurch der lokale Snapshot auf den Datenspeichern oder VMs auf dem primären Speicher und eine Kaskade vom primären Festplattenspeicher zum sekundären Festplattenspeicher und dann zum Cloud-Objektspeicher konfiguriert.

   - **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.

     Bei VMware-Workloads wird dadurch der lokale Snapshot auf den Datenspeichern oder VMwares auf dem primären Speichersystem konfiguriert und anschließend werden die Daten vom primären Festplattenspeichersystem auf das sekundäre Festplattenspeichersystem repliziert.

   - **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.

     Für VMWare-Workloads wird hierdurch der lokale Snapshot auf den Datenspeichern oder VMs auf dem primären Server und die Replikation vom primären Festplattenspeicher zum Cloud-Objektspeicher konfiguriert.

   - **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.

     Bei VMware-Workloads wird dadurch der primäre Festplattenspeicher auf den sekundären Festplattenspeicher konfiguriert und der primäre Festplattenspeicher auf den sekundären Festplattenspeicher repliziert.

- **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.

  Für VMware-Workloads wird hierdurch der lokale Snapshot auf den Datenspeichern oder VMs auf dem primären Speichersystem konfiguriert.

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.
   - * Sekundäre Beziehung zwischen SnapMirror und SnapVault SMAS*: Verwenden Sie sekundäre Beziehungen zwischen SnapMirror und SnapVault SMAS für SQL Server-Workloads.
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 müssen VMware Tools auf der VM ausgeführt werden. Wenn VMware Tools nicht ausgeführt werden, werden stattdessen absturzkonsistente Snapshots erstellt. Beachten Sie, dass die Aktivierung dieser Option die Sicherungszeit verlängern und mehr Speicherplatz beanspruchen kann. Zusätzlich wird der aktive Arbeitsspeicher der VM in konsistenten Snapshots nicht berücksichtigt.
   - **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.

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 VMware-Workloads mit NetApp Backup and Recovery

Sichern Sie VMware-VMs und Datenspeicher 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 regelmäßig zu sichern, erstellen Sie Richtlinien, die die Sicherungs- und Wiederherstellungsvorgänge steuern. Siehe "Schutzrichtlinien erstellen" für Anweisungen.
- Erstellen Sie Schutzgruppen, um die Backup- und Recovery-Vorgänge für eine Gruppe von Ressourcen zu verwalten. Siehe "Schutzgruppen erstellen und verwalten" für weitere Informationen.
- Sichern Sie jetzt Workloads (erstellen Sie jetzt ein On-Demand-Backup).

Sichern Sie Workloads jetzt mit einem On-Demand-Backup

Erstellen Sie sofort ein On-Demand-Backup. Möglicherweise möchten Sie eine On-Demand-Sicherung ausführen, wenn Sie Änderungen an Ihrem System vornehmen und sicherstellen möchten, dass Sie vor dem Start über eine Sicherung verfügen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung oder Backup-Administratorrolle für Backup und Wiederherstellung. "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste" .

Schritte

1. Wählen Sie im Menü „Sicherung und Wiederherstellung“ die Option „Inventar“ aus.
2. Wählen Sie eine Arbeitslast aus, um die Schutzdetails anzuzeigen.
3. Wählen Sie das Symbol Aktionen > **Details anzeigen**.
4. Wählen Sie die Menüüberschrift **Protection Groups**, **Datastores**, **Virtual machines** oder **Tags** aus.

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

> Die für die Datensicherung angewendete Richtlinie ist dieselbe Richtlinie, die der Schutzgruppe, dem Datenspeicher, der virtuellen Maschine oder den getaggten Ressourcen zugewiesen ist.

7. Wählen Sie die Zeitplanstufe aus.
8. Wählen Sie **Jetzt sichern**.

VMware-Workloads mithilfe von NetApp Backup and Recovery klonen

Verwenden Sie NetApp Backup and Recovery, um beschreibbare Klone von VMware-VMs aus primären oder sekundären Snapshots zu erstellen. Mit VM-Klonen können Sie virtuelle Maschinen für Tests, Integration und Schulungen erstellen und verwalten, ohne die Produktionsdaten zu beeinträchtigen.

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

Stellen Sie sicher, dass alle VMs, deren Snapshots Sie klonen möchten, einer Schutzgruppe hinzugefügt und gesichert wurden.

Erstellen Sie einen Klon einer VMware-VM

Erstellen Sie sofort einen Klon aus einem vorhandenen Snapshot.

> Nach dem Erstellen eines VM-Klons müssen Sie die IP-Adresse der geklonten virtuellen Maschine aktualisieren, um IP-Adresskonflikte mit der ursprünglichen VM zu vermeiden.

Schritte

1. Wählen Sie im NetApp Console **Schutz > Sicherung und Wiederherstellung**.
2. Wählen Sie unter **Workloads** die Kachel **VMware** aus.
3. Wählen Sie **Clone** aus.
4. Wählen Sie **Neuen Klon erstellen**.
5. Im Abschnitt **Virtuelle Maschinen auswählen** wählen Sie eine Schutzgruppe aus. Die VMs in der Schutzgruppe werden in der Auswahlliste angezeigt.
6. Wählen Sie eine oder mehrere VMs aus der Liste zum Klonen aus. Die ausgewählten VMs werden rechts in der Liste der ausgewählten VMs angezeigt.
7. Wenn Sie fertig sind, wählen Sie **Weiter**.
8. Im Abschnitt **Snapshots** auf der Seite **Snapshot auswählen** wählen Sie einen Zeitraum aus, um die Snapshots nach Erstellungsdatum zu filtern.

9. Wählen Sie aus der Liste einen vorhandenen Snapshot als Basis für den Klon aus und klicken Sie auf **Weiter**.

   Die Option **Speicherort für Snapshots auswählen** erscheint, wenn der Snapshot an mehr als einem Speicherort gespeichert ist.

10. Wählen Sie den Snapshot-Speicherort aus und wählen Sie **Weiter**.
11. Gehen Sie auf der Seite **Zieleinstellungen** wie folgt vor:
    a. Wählen Sie den FQDN oder die IP-Adresse des Ziel-vCenter-Servers, auf dem der VM-Klon erstellt werden soll.
    b. Wählen Sie den ESXi-Host aus, der den Klon hosten soll.
    c. Wählen Sie die Netzwerkumgebung für den Klon aus.
    d. Geben Sie im Feld **Name der virtuellen Maschine** ein Suffix für die neu geklonte virtuelle Maschine ein.
12. Wählen Sie **Clone** aus.

Einen Klon teilen

Sie können einen Klon einer VMware-VM aufteilen, um ihn vom übergeordneten Volume zu trennen. Nach der Aufteilung wird der Klon zu einem unabhängigen Volume, das nicht mehr vom übergeordneten Volume abhängig ist.

Nach der Aufteilung werden die mit der geklonten VM verbundenen Datenspeicher zu einem neuen, unabhängigen Datenspeicher. Die geklonte VM selbst bleibt erhalten.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.
2. Wählen Sie einen Klon aus.
3. Wählen Sie das Symbol Aktionen ••• > **Geteilter Klon**.
4. Überprüfen Sie die Details im Dialogfeld und wählen Sie **Split**.
5. Sobald die neue, unabhängige VM erstellt ist, können Sie sie auf der Seite **Inventory** anzeigen.

Einen Klon entfernen

Sie können einen VMware-VM-Klon entfernen. Wenn Sie einen VM-Klon entfernen, wird der Klon aus vCenter entfernt, und die mit der VM verbundenen Datastores werden ausgehängt und vom Speichersystem gelöscht.

Wenn eine Richtlinie den Klon schützt, werden sowohl der Klon als auch sein Job entfernt.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Klonen** aus.
2. Wählen Sie einen Klon aus.
3. Wählen Sie das Symbol „Aktionen“ ••• > **Entfernen**.
4. Überprüfen Sie im Bestätigungsdialogfeld „Entfernen“ die Details der Löschung.
5. Wählen Sie **Remove**.
6. Wenn der Klon gelöscht wird, wird er von der Seite **Inventar** entfernt.

Wiederherstellen von VMware-Workloads

Wiederherstellen von VMware-Workloads mit NetApp Backup and Recovery

VMware-Workloads können mithilfe von NetApp Backup and Recovery aus Snapshots, aus einer auf einen Sekundärspeicher replizierten Workload-Sicherung oder aus in Objektspeichern gespeicherten Sicherungen wiederhergestellt werden.

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 einer Objektspeichersicherung

Stellen Sie diese Punkte wieder her

Sie können Daten bis zu diesen Punkten wiederherstellen:

- **Wiederherstellung am ursprünglichen Speicherort**: Die VM wird am ursprünglichen Speicherort wiederhergestellt, und zwar in derselben vCenter-Bereitstellung, auf demselben ESXi-Host und im selben Datenspeicher. Die VM und alle darauf befindlichen Daten werden überschrieben.
- **Wiederherstellung an einem alternativen Speicherort**: Sie können einen anderen vCenter-Server, ESXi-Host oder Datenspeicher als Wiederherstellungsziel für die VM auswählen. Dies ist nützlich, um verschiedene Kopien derselben VM an unterschiedlichen Standorten und in verschiedenen Zuständen zu verwalten.

Überlegungen zur Wiederherstellung aus dem Objektspeicher

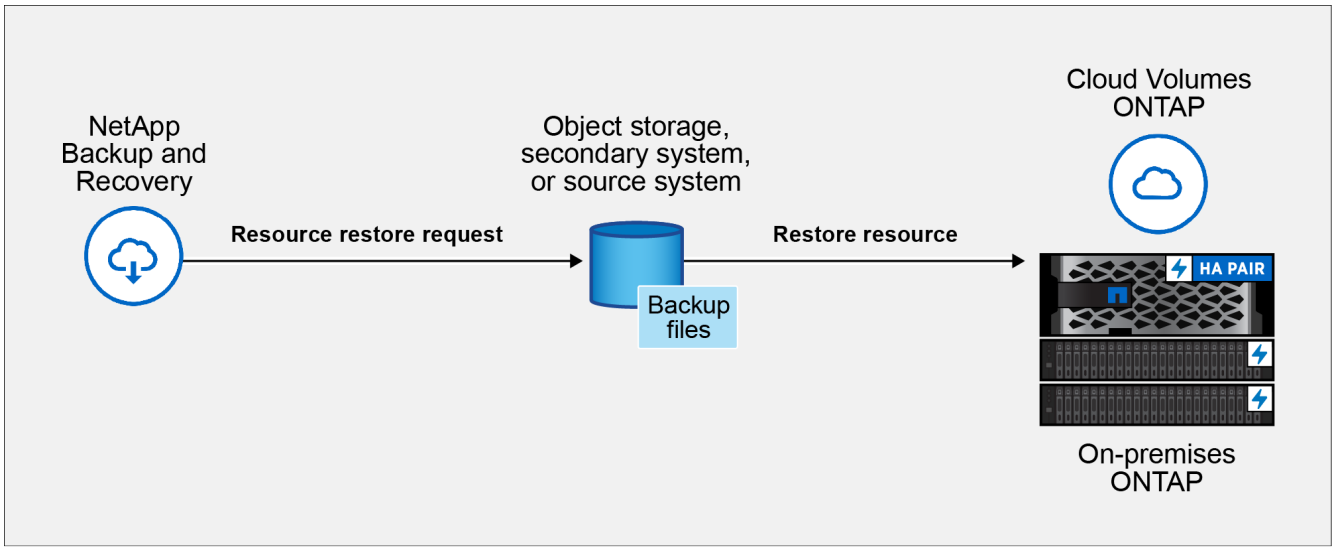
Wenn für eine Sicherungsdatei im Objektspeicher ein Ransomware-Schutz aktiviert ist, werden Sie aufgefordert, vor der Wiederherstellung eine zusätzliche Prüfung durchzuführen. Wir empfehlen, die Prüfung durchzuführen.

Möglicherweise zahlen Sie Ihrem Cloud-Anbieter zusätzliche Gebühren für den Zugriff auf die Sicherungsdatei.

So funktioniert die Wiederherstellung von Workloads

Beim Wiederherstellen von Workloads geschieht Folgendes:

- Wenn Sie eine Arbeitslast aus einem lokalen Snapshot oder einem Remote-Backup wiederherstellen, überschreibt NetApp Backup and Recovery die ursprüngliche VM, wenn Sie die Wiederherstellung am ursprünglichen Speicherort vornehmen, und erstellt eine *neue* Ressource, wenn Sie die Wiederherstellung an einem alternativen Speicherort vornehmen.
- Bei der Wiederherstellung einer replizierten Arbeitslast können Sie die Arbeitslast auf dem ursprünglichen lokalen ONTAP System oder auf einem anderen 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“ (Suchen und Wiederherstellen) können Sie eine Ressource wiederherstellen, indem Sie mithilfe von Filtern nach dem Snapshot suchen, auch wenn Sie sich nicht an den genauen Namen, den Speicherort oder das letzte bekannte Datum erinnern.

Wiederherstellen von Workload-Daten über die Option „Wiederherstellen“ (Suchen und Wiederherstellen)

Stellen Sie VMware-Workloads mithilfe der Option „Wiederherstellen“ wieder her. Sie können nach dem Snapshot anhand seines Namens oder mithilfe von Filtern suchen.

*Erforderliche NetApp Console * Speicherbetrachter, Superadministrator für Backup und Wiederherstellung, Administratorrolle für Backup- und Wiederherstellungswiederherstellung. "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 in der Dropdown-Liste rechts neben dem Namenssuchfeld **VMware** aus.
3. Geben Sie den Namen der Ressource ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem vCenter, Rechenzentrum oder Datenspeicher, in dem sich die wiederherzustellende Ressource befindet.

   Es erscheint eine Liste virtueller Maschinen, die Ihren Suchkriterien entsprechen.

4. Suchen Sie in der Liste die VM, von der Sie die VM wiederherstellen möchten, und wählen Sie die entsprechende Menüschaltfläche für diese VM aus.
5. Wählen Sie im daraufhin angezeigten Menü die Option **Virtuelle Maschine wiederherstellen**.

   Es wird eine Liste der auf dieser virtuellen Maschine erstellten Snapshots (Wiederherstellungspunkte) angezeigt. Standardmäßig werden die neuesten Snapshots für den im Dropdown-Menü **Zeitraum** ausgewählten Zeitraum angezeigt.

   Für jeden Snapshot zeigen alle leuchtenden Symbole in der Spalte **Speicherort** die Speicherorte an, an denen der Snapshot verfügbar ist (primärer Speicher, sekundärer Speicher oder Objektspeicher).

6. Aktivieren Sie das Optionsfeld für den Snapshot, den Sie wiederherstellen möchten.
7. Wählen Sie **Weiter**.

   Optionen zum Speichern des Schnappschusses werden angezeigt.

8. Wählen Sie das Wiederherstellungsziel für den Snapshot aus:
   - **Lokal**: Stellt den Snapshot vom lokalen Speicherort wieder her.
   - **Sekundär**: Stellt den Snapshot von einem entfernten Speicherort wieder her.
   - **Objektspeicher**: Stellt den Snapshot aus dem Objektspeicher wieder her.

     Wenn Sie sich für einen sekundären Speicher entscheiden, wählen Sie den Zielspeicherort aus der Dropdown-Liste aus.

9. Wählen Sie **Weiter**, um fortzufahren.
10. Wählen Sie das Wiederherstellungsziel und die Einstellungen aus:

Zielauswahl

Am ursprünglichen Speicherort wiederherstellen

Bei der Wiederherstellung am ursprünglichen Speicherort können Sie weder das Ziel-vCenter, den ESXi-Host, den Datenspeicher noch den Namen der VM ändern. Die ursprüngliche VM wird bei der Wiederherstellungsoperation überschrieben.

1. Wählen Sie den Bereich **Ursprünglicher Speicherort** aus.
2. Wählen Sie aus den folgenden Optionen:
   - Abschnitt **Optionen vor der Wiederherstellung**:
     - **Vorgabe**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie vor Beginn des Wiederherstellungsvorgangs ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
   - Abschnitt **Optionen nach der Wiederherstellung**:
     - **Virtuelle Maschine neu starten**: Aktivieren Sie diese Option, um die virtuelle Maschine nach Abschluss des Wiederherstellungsvorgangs und nach Anwendung des Nachwiederherstellungsskripts neu zu starten.
     - **Nachtrag**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie nach Abschluss der Wiederherstellung ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
3. Wählen Sie **Wiederherstellen**.

An einem anderen Speicherort wiederherstellen

Bei der Wiederherstellung an einem alternativen Speicherort können Sie das Ziel-vCenter, den ESXi-Host, den Datenspeicher und den Namen der VM ändern, um eine neue Kopie der VM an einem anderen Speicherort oder mit einem anderen Namen zu erstellen.

1. Wählen Sie den Bereich **Alternativer Standort** aus.
2. Geben Sie die folgenden Informationen ein:
   - Abschnitt **Zieleinstellungen**:
     - **vCenter FQDN oder IP-Adresse**: Wählen Sie den vCenter-Server aus, auf dem Sie den Snapshot wiederherstellen möchten.
     - **ESXi-Host**: Wählen Sie den Host aus, auf dem Sie den Snapshot wiederherstellen möchten.
     - **Netzwerk**: Wählen Sie das Netzwerk aus, in dem Sie den Snapshot wiederherstellen möchten.
     - **Datenspeicher**: Wählen Sie in der Dropdown-Liste den Namen des Datenspeichers aus, in dem Sie den Snapshot wiederherstellen möchten.
     - **Name der virtuellen Maschine**: Geben Sie den Namen der VM ein, auf der Sie den Snapshot wiederherstellen möchten. Wenn der Name mit einer bereits im Datenspeicher vorhandenen VM übereinstimmt, sorgt Backup and Recovery für einen eindeutigen Namen, indem ein aktueller Zeitstempel angehängt wird.
   - **Zielspeicher**-Abschnitt (nur sichtbar beim Wiederherstellen aus Objektspeicher):
     - **Standardspeicherort ändern**: Aktivieren Sie diese Option, um eine Objektspeichersicherung auf einer anderen Speicher-VM wiederherzustellen, falls der Quellspeicherort nicht erreichbar oder voll ist. Wählen Sie einen anderen Cluster, eine andere Speicher-VM oder ein anderes Aggregat aus.

- Abschnitt **Optionen vor der Wiederherstellung**:
  - **Schnellwiederherstellung**: Aktivieren Sie diese Option, um NetApp Backup and Recovery anzuweisen, nur VM-Metadaten (Dateien, LUNs und Namespaces) aus dem Objektspeicher wiederherzustellen. Dadurch stehen Volumes schneller zur Verfügung als bei einer vollständigen Wiederherstellung.
  - **Vorgabe**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie vor Beginn des Wiederherstellungsvorgangs ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
- Abschnitt **Optionen nach der Wiederherstellung**:
  - **Virtuelle Maschine neu starten**: Aktivieren Sie diese Option, um die virtuelle Maschine nach Abschluss des Wiederherstellungsvorgangs und nach Anwendung des Nachwiederherstellungsskripts neu zu starten.
  - **Nachtrag**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie nach Abschluss der Wiederherstellung ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.

3. Wählen Sie **Wiederherstellen**.

Bestimmte virtuelle Festplatten aus Backups wiederherstellen

Sie können vorhandene virtuelle Festplatten (VMDKs) oder gelöschte bzw. getrennte virtuelle Festplatten aus primären oder sekundären Backups herkömmlicher VMs wiederherstellen. Dadurch können Sie nur bestimmte VM-Daten oder Anwendungen wiederherstellen, sodass Sie nicht die gesamte VM und alle zugehörigen virtuellen Festplatten wiederherstellen müssen, wenn nur bestimmte Daten betroffen sind. Nach der Wiederherstellung der virtuellen Festplatte wird diese wieder an die ursprüngliche VM angebunden und ist sofort einsatzbereit.

Sie können eine oder mehrere virtuelle Maschinenfestplatten (VMDKs) einer VM auf demselben Datenspeicher oder auf verschiedenen Datenspeichern wiederherstellen.

Aktivieren Sie die VMware-Anwendung vStorage API for Array Integration (VAAI), um die Leistung von Wiederherstellungsvorgängen in NFS-Umgebungen zu verbessern.

Bevor Sie beginnen

- Es muss ein Backup vorhanden sein.
- Die VM darf sich nicht im Transit befinden.

  Die VM, die Sie wiederherstellen möchten, darf sich nicht im Zustand vMotion oder Storage vMotion befinden.

Informationen zu diesem Vorgang

- Wenn das VMDK gelöscht oder von der VM getrennt wird, wird das VMDK beim Wiederherstellungsvorgang an die VM angehängt.
- Ein Wiederherstellungsvorgang kann fehlschlagen, wenn die Speicherebene des FabricPool , in dem sich die VM befindet, nicht verfügbar ist.

- Anfügen- und Wiederherstellungsvorgänge verbinden VMDKs mithilfe des Standard-SCSi-Controllers. Wenn jedoch VMDKs gesichert werden, die an eine VM mit einer NVMe-Festplatte angeschlossen sind, verwenden die Anfüge- und Wiederherstellungsvorgänge den NVMe-Controller, sofern verfügbar.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
2. Wählen Sie in der Dropdown-Liste rechts neben dem Namenssuchfeld **VMware** aus.
3. Geben Sie den Namen der Ressource ein, die Sie wiederherstellen möchten, oder filtern Sie nach dem vCenter, Rechenzentrum oder Datenspeicher, in dem sich die wiederherzustellende Ressource befindet.

   Es erscheint eine Liste virtueller Maschinen, die Ihren Suchkriterien entsprechen.

4. Suchen Sie in der Liste die VM, von der Sie die VM wiederherstellen möchten, und wählen Sie die entsprechende Menüschaltfläche für diese VM aus.
5. Wählen Sie im daraufhin angezeigten Menü die Option **Virtuelle Festplatten wiederherstellen**.

   Es wird eine Liste der auf dieser virtuellen Maschine erstellten Snapshots (Wiederherstellungspunkte) angezeigt. Standardmäßig werden die neuesten Snapshots für den im Dropdown-Menü **Zeitraum** ausgewählten Zeitraum angezeigt.

   Für jeden Snapshot zeigen alle leuchtenden Symbole in der Spalte **Speicherort** die Speicherorte an, an denen der Snapshot verfügbar ist (primärer Speicher, sekundärer Speicher oder Objektspeicher).

6. Aktivieren Sie das Optionsfeld für den Snapshot, den Sie wiederherstellen möchten.
7. Wählen Sie **Weiter**.

   Optionen zum Speichern des Schnappschusses werden angezeigt.

8. Wählen Sie das Wiederherstellungsziel für den Snapshot aus:
   - **Lokal**: Stellt den Snapshot vom lokalen Speicherort wieder her.
   - **Sekundär**: Stellt den Snapshot von einem entfernten Speicherort wieder her.
   - **Objektspeicher**: Stellt den Snapshot aus dem Objektspeicher wieder her.

     Wenn Sie sich für einen sekundären Speicher entscheiden, wählen Sie den Zielspeicherort aus der Dropdown-Liste aus.

9. Wählen Sie **Weiter**, um fortzufahren.
10. Wählen Sie das Wiederherstellungsziel und die Einstellungen aus:

Zielauswahl

Am ursprünglichen Speicherort wiederherstellen

Bei der Wiederherstellung am ursprünglichen Speicherort können Sie weder das Ziel-vCenter, den ESXi-Host, den Datenspeicher noch den Namen der virtuellen Festplatte ändern. Die ursprüngliche virtuelle Festplatte wird überschrieben.

1. Wählen Sie den Bereich **Ursprünglicher Speicherort** aus.
2. Aktivieren Sie im Abschnitt **Zieleinstellungen** das Kontrollkästchen für alle virtuellen Festplatten, die Sie wiederherstellen möchten.
3. Wählen Sie aus den folgenden Optionen:
   - Abschnitt **Optionen vor der Wiederherstellung**:
     - **Vorgabe**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie vor Beginn des Wiederherstellungsvorgangs ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
   - Abschnitt **Optionen nach der Wiederherstellung**:
     - **Nachtrag**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie nach Abschluss der Wiederherstellung ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
4. Wählen Sie **Wiederherstellen**.

An einem anderen Speicherort wiederherstellen

Bei der Wiederherstellung an einem alternativen Speicherort kann der Zieldatenspeicher geändert werden. Die virtuelle Festplatte wird nach dem Wiederherstellungsvorgang unabhängig vom gewählten Datenspeicher an die ursprüngliche VM angehängt.

1. Wählen Sie den Bereich **Alternativer Standort** aus.
2. Aktivieren Sie im Abschnitt **Zieleinstellungen** das Kontrollkästchen für alle virtuellen Festplatten, die Sie wiederherstellen möchten.
3. Für alle von Ihnen ausgewählten virtuellen Festplatten:
   a. Wählen Sie **Datenspeicher auswählen**, um ein anderes Datenspeicherziel für die Wiederherstellung der virtuellen Festplatte auszuwählen.
   b. Wählen Sie **Auswählen**, um Ihre Auswahl zu bestätigen und das Auswahlfenster zu schließen.
4. Wählen Sie aus den folgenden Optionen:
   - Abschnitt **Optionen vor der Wiederherstellung**:
     - **Vorgabe**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie vor Beginn des Wiederherstellungsvorgangs ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
   - Abschnitt **Optionen nach der Wiederherstellung**:
     - **Nachtrag**: Aktivieren Sie diese Option, um zusätzliche Aufgaben zu automatisieren, indem Sie nach Abschluss der Wiederherstellung ein benutzerdefiniertes Skript ausführen. Geben Sie den vollständigen Pfad zu dem auszuführenden Skript sowie alle Argumente an, die das Skript benötigt.
5. Wählen Sie **Wiederherstellen**.

VMware-Dateien und -Ordner wiederherstellen

Anforderungen und Einschränkungen beim Wiederherstellen von Gastdateien und -ordnern

Sie können Dateien oder Ordner von einer virtuellen Maschinenfestplatte (VMDK) auf einem Windows- oder Linux-Gast-OS wiederherstellen.

Workflow zur Gastwiederherstellung

Die Wiederherstellungsvorgänge des Gastbetriebssystems umfassen die folgenden Schritte:

1. Befestigen

   Binden Sie eine virtuelle Festplatte an eine Gast-VM oder eine Proxy-VM an und starten Sie eine Gast-VM-Dateiwiederherstellungssitzung.

2. Warten

   Warten Sie, bis der Anfügevorgang abgeschlossen ist, bevor Sie durchsuchen und wiederherstellen können. Nach Abschluss des Anfügevorgangs wird automatisch eine Gastdatei-Wiederherstellungssitzung erstellt.

3. Dateien oder Ordner auswählen

   Durchsuchen Sie die virtuellen Festplattendateien und wählen Sie eine oder mehrere Dateien oder Ordner zur Wiederherstellung aus.

4. Wiederherstellen

   Stellen Sie die ausgewählten Dateien oder Ordner an einem angegebenen Speicherort wieder her.

Voraussetzungen für die Wiederherstellung von Gastdateien und -ordnern

Prüfen Sie alle Voraussetzungen, bevor Sie Dateien oder Ordner aus einer VMDK wiederherstellen.

- VMware-Tools müssen installiert und ausgeführt werden.

  NetApp Backup and Recovery nutzt Informationen von VMware Tools, um eine Verbindung zum VMware-Gastbetriebssystem herzustellen.

- Sie müssen den Sicherungs-Snapshot und das VMDK kennen, von dem die Wiederherstellung durchgeführt werden soll.
- Die anzuhängende virtuelle Festplatte muss sich in einem NetApp Backup and Recovery -Backup befinden.

  Die virtuelle Festplatte, die die wiederherzustellende Datei oder den Ordner enthält, muss sich in einer VM-Sicherung befinden, die mit NetApp Backup and Recovery erstellt wurde.

- Um eine Proxy-VM zu verwenden, muss die Proxy-VM konfiguriert werden.

  Wenn Sie eine virtuelle Festplatte an eine Proxy-VM anhängen möchten, muss die Proxy-VM konfiguriert werden, bevor der Anhänge- und Wiederherstellungsvorgang beginnt.

- Dateien mit Namen, die nicht aus dem englischen Alphabet stammen, müssen Sie in einem Verzeichnis

und nicht als einzelne Datei wiederherstellen.

Sie können Dateien mit nicht-alphabetischen Namen, wie etwa japanische Kanji, wiederherstellen, indem Sie das Verzeichnis wiederherstellen, in dem sich die Dateien befinden.

Für die aktuellsten Informationen zur Unterstützung von Gastbetriebssystemen konsultieren Sie bitte die "NetApp Interoperability Matrix Tool (IMT)".

Windows-Gäste

- Als Gastbetriebssystem muss Windows Server 2008 R2 oder höher ausgeführt werden.

  Aktuelle Informationen zu unterstützten Versionen finden Sie unter "NetApp Interoperability Matrix Tool (IMT)" .

- Die Anmeldeinformationen für die Ziel-VM verwenden das integrierte Domänen- oder lokale Administratorkonto mit dem Benutzernamen „Administrator“. Bevor Sie mit dem Wiederherstellungsvorgang beginnen, konfigurieren Sie die Anmeldeinformationen für die VM, an die Sie die virtuelle Festplatte anhängen möchten. Für den Anfüge- und Wiederherstellungsvorgang werden Anmeldeinformationen benötigt. Benutzer von Arbeitsgruppen können das integrierte lokale Administratorkonto verwenden.

  Wenn Sie ein Konto verwenden müssen, das nicht das integrierte Administratorkonto ist, aber über Administratorrechte innerhalb der VM verfügt, müssen Sie die Benutzerkontensteuerung auf der Gast-VM deaktivieren.

Linux-Gastsysteme

- Folgende Gastbetriebssystemdistributionen werden unterstützt:
  - Red Hat Enterprise Linux
  - Ubuntu
  - Debian
- Das Benutzerkonto „Ausführen als“ benötigt Root- oder Sudo-Berechtigungen.
- Für eine VM-übergreifende Wiederherstellung (Wiederherstellung auf einer anderen Linux-VM) muss SSH auf der Ziel-VM ausgeführt werden.

Einschränkungen bei der Wiederherstellung von Gastdateien

Bevor Sie eine Datei oder einen Ordner aus einem Gastbetriebssystem wiederherstellen, sollten Sie sich über die Funktionsbeschränkungen im Klaren sein.

- Sie können dynamische Datenträgertypen nicht innerhalb eines Gastbetriebssystems wiederherstellen.
- Wenn Sie eine verschlüsselte Datei oder einen verschlüsselten Ordner wiederherstellen, bleibt das Verschlüsselungsattribut nicht erhalten.
- Sie können keine Dateien oder Ordner in einem verschlüsselten Ordner wiederherstellen.
- Versteckte Dateien und Ordner werden auf der Dateiauswahlseite angezeigt und können nicht gefiltert werden.
- Dateien oder Ordner können nicht zwischen Gastsystemen mit unterschiedlichen Betriebssystemen wiederhergestellt werden (bei der Wiederherstellung auf eine andere Gast-VM muss der

Zielbetriebssystemtyp mit dem Quellbetriebssystemtyp übereinstimmen).

- Sie können keine Wiederherstellung von einem NTFS-Dateisystem auf ein FAT-Dateisystem durchführen.

  Wenn Sie versuchen, vom NTFS-Format ins FAT-Format wiederherzustellen, wird der NTFS-Sicherheitsdeskriptor nicht kopiert, da das FAT-Dateisystem keine Windows-Sicherheitsattribute unterstützt.

- Sie können keine Gastdateien aus einem geklonten VMDK oder einem nicht initialisierten VMDK wiederherstellen.
- Sie können die Verzeichnisstruktur einer Datei nicht wiederherstellen.

  Wenn Sie eine Datei aus einem verschachtelten Verzeichnis wiederherstellen, stellt das System nur die Datei selbst wieder her, nicht aber die Verzeichnisstruktur. Um die gesamte Verzeichnisstruktur wiederherzustellen, kopieren Sie das oberste Verzeichnis.

- Sie können keine Gastdateien von einer vVol-VM auf einem alternativen Host wiederherstellen.
- Sie können verschlüsselte Gastdateien nicht wiederherstellen.

Dateien und Ordner von virtuellen Festplatten wiederherstellen

Einzelne Dateien oder Ordner einer virtuellen Festplatte lassen sich auf der ursprünglichen VM oder einer anderen VM wiederherstellen. Dies ist nützlich, wenn Sie nicht die gesamte VM wiederherstellen müssen, sondern nur bestimmte Dateien oder Ordner benötigen.

Dateien und Ordner von virtuellen Festplatten wiederherstellen

Stellen Sie Dateien oder Ordner von einer virtuellen Festplatte auf der ursprünglichen VM oder auf einer anderen VM wieder her. Wenn Sie die virtuelle Festplatte nicht an die ursprüngliche VM anbinden möchten, können Sie sie stattdessen an eine Proxy-VM anbinden.

Bevor Sie beginnen

- Überprüfen Sie die Voraussetzungen und Einschränkungen in "Anforderungen und Einschränkungen beim Wiederherstellen von Gastdateien und -ordnern".
- Um Dateien und Ordner mithilfe einer Proxy-VM wiederherzustellen, stellen Sie sicher, dass die Proxy-VM bereits konfiguriert ist, bevor Sie mit dem Wiederherstellungsprozess für Dateien und Ordner beginnen.
- Sie müssen Anmeldeinformationen für die virtuelle Quellfestplatte und die Ziel-VM in NetApp Backup and Recovery erstellen, bevor Sie Dateien und Ordner wiederherstellen können. NetApp Backup and Recovery verwendet diese Anmeldeinformationen, um sich bei der virtuellen Festplatte und der Ziel-VM zu authentifizieren, wenn Dateien und Ordner wiederhergestellt werden.

Informationen zu diesem Vorgang

Die Leistungsfähigkeit beim Wiederherstellen von Dateien oder Ordnern hängt von zwei Faktoren ab: der Größe der wiederherzustellenden Dateien oder Ordner und der Anzahl der wiederherzustellenden Dateien oder Ordner. Die Wiederherstellung einer großen Anzahl kleiner Dateien kann länger dauern als erwartet, verglichen mit der Wiederherstellung einer kleinen Anzahl großer Dateien, wenn die wiederherzustellenden Datenmengen die gleiche Größe haben.

Sie können eine Wiederherstellung auf einer entfernten VM durchführen (bekannt als Cross-VM-Wiederherstellung), aber Quell- und Zielbetriebssystem müssen identisch sein.

Auf einer VM kann gleichzeitig nur ein Anfüge- oder Wiederherstellungsvorgang ausgeführt werden. Sie können auf derselben VM keine parallelen Anfüge- oder Wiederherstellungsvorgänge ausführen.

Mit der Funktion zum Wiederherstellen von Dateien und Ordnern können Sie System- 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. Während des Wiederherstellungsvorgangs werden die Attribute „Versteckt“, „System“ und „Verschlüsselt“ von Gastdateien in der wiederhergestellten Datei nicht beibehalten. Das Anzeigen oder Durchsuchen reservierter Partitionen kann zu einem Fehler führen.

Hängen Sie die VMDK an die ursprüngliche VM an, um Dateien und Ordner wiederherzustellen

Gastdateien und -ordner von einer virtuellen Festplatte auf die ursprüngliche (Quell-)VM wiederherstellen.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
2. Wählen Sie **VMware** aus der Workload-Liste oben rechts auf der Seite aus.
3. Wählen Sie in der Liste der virtuellen Maschinen das Aktionssymbol ••• für eine VM aus, die Dateien enthält, die Sie wiederherstellen möchten.
4. Wählen Sie **Dateien und Ordner wiederherstellen**.
5. Wählen Sie einen Snapshot aus, aus dem die Wiederherstellung erfolgen soll, und klicken Sie dann auf **Weiter**.
6. Wählen Sie den Speicherort des Snapshots aus, von dem die Wiederherstellung erfolgen soll. Wenn Sie einen sekundären Speicherort auswählen, wählen Sie den sekundären Snapshot aus der Liste aus.
7. Wählen Sie **Weiter**.
8. 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.
9. 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. Im Abschnitt **Anmeldeinformationen für die Gast-VM** wählen Sie **Anmeldeinformationen hinzufügen**, wenn Sie noch keine Anmeldeinformationen für die Quellfestplatte und die Ziel-Gast-VM gespeichert haben, geben Sie die Windows- oder Linux-Anmeldeinformationen ein und wählen Sie **Hinzufügen**.

    ⓘ Die Quell- und Ziel-VMs müssen zur selben Betriebssystemfamilie gehören; die Betriebssystemversionen können unterschiedlich sein.

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

    d. Wählen Sie **Weiter**.

    NetApp Backup and Recovery verbindet die virtuelle Festplatte mit der ursprünglichen VM und zeigt alle Dateien und Ordner an, einschließlich der versteckten. Für Windows-Gäste wird jeder Partition, einschließlich systemreservierter Partitionen, 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.

10. Wählen Sie die wiederherzustellenden Dateien oder Ordner aus.

    Die Dateien und Ordner, die Sie zur Wiederherstellung ausgewählt haben, werden im rechten Bereich des Bildschirms aufgelistet.

11. Wählen Sie **Weiter**.
12. Geben Sie im Abschnitt „Wiederherstellen unter Pfad“ den Pfad zur Ziel-VM und zum Dateisystemspeicherort ein, an dem die ausgewählten Dateien wiederhergestellt werden sollen:

- Für Windows-Gastsysteme geben Sie den UNC-Freigabepfad ein:
  - IPv4-Pfadbeispiel: `\\10.60.136.65\c$`
  - IPv6-Pfadbeispiel: `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`
- Für Linux-Gastsysteme geben Sie den lokalen Dateisystempfad oder die Adresse und den Pfad des Remote-Gastsystems ein:
  - Beispiel für einen lokalen Pfad: `/home/user/documents/file.txt`
  - IPv4-Pfadbeispiel: `10.60.136.65:/home/user/restore/`
  - IPv6-Pfadbeispiel: `fd20-8b1e-b255-832e—61.ipv6-literal.net:/home/user/restore/`

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

13. 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.
14. Wählen Sie **Wiederherstellen**.

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

Hängen Sie die VMDK an eine Proxy-VM an, um Dateien und Ordner wiederherzustellen.

Verwenden Sie eine Proxy-VM (eine andere VM auf demselben vCenter wie die Original-VM), um Gastdateien und -ordner wiederherzustellen, wenn Sie die virtuelle Festplatte nicht an die Original-VM anhängen möchten.

Schritte

1. Wählen Sie im NetApp Backup and Recovery -Menü **Wiederherstellen** aus.
2. Wählen Sie **VMware** aus der Workload-Liste oben rechts auf der Seite aus.
3. Wählen Sie in der Liste der virtuellen Maschinen das Aktionssymbol ••• für eine VM aus, die Dateien enthält, die Sie wiederherstellen möchten.
4. Wählen Sie **Dateien und Ordner wiederherstellen**.
5. Wählen Sie einen Snapshot aus, aus dem die Wiederherstellung erfolgen soll, und klicken Sie dann auf **Weiter**.
6. Wählen Sie den Speicherort des Snapshots aus, von dem die Wiederherstellung erfolgen soll. Wenn Sie einen sekundären Speicherort auswählen, wählen Sie den sekundären Snapshot aus der Liste aus.
7. Wählen Sie **Weiter**.
8. 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.
9. Führen Sie auf der Seite *Details zur Gast-VM* die folgenden Schritte aus:

   a. Im Abschnitt **Details zur Gast-VM**:

      i. Verbinden Sie die virtuelle Festplatte mit einer Proxy-VM, indem Sie **Proxy virtual machine** auswählen.

ii. Wählen Sie ein vCenter, ein Rechenzentrum und einen Datenspeicher aus den Listen aus, in dem sich die Proxy-VM befindet.

iii. Wählen Sie aus der Liste eine VM aus, die als Proxy-VM verwendet werden soll. Die virtuelle Festplatte wird an diese VM angehängt. Die ausgewählte Proxy-VM wird im rechten Bereich angezeigt.

b. Im Abschnitt **Anmeldeinformationen für die Gast-VM** wählen Sie **Anmeldeinformationen hinzufügen**, wenn Sie noch keine Anmeldeinformationen für die Quellfestplatte und die Ziel-Gast-VM gespeichert haben, geben Sie die Windows- oder Linux-Anmeldeinformationen ein und wählen Sie **Hinzufügen**.

Die Quell- und Ziel-VMs müssen zur selben Betriebssystemfamilie gehören; die Betriebssystemversionen können unterschiedlich sein.

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

d. Wählen Sie **Weiter**.

NetApp Backup and Recovery verbindet die virtuelle Festplatte mit der Proxy-VM und zeigt alle Dateien und Ordner an, einschließlich der versteckten. Für Windows-Gäste wird jeder Partition, einschließlich der systemreservierten Partitionen, 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.

10. Wählen Sie die wiederherzustellenden Dateien oder Ordner aus.

Die Dateien und Ordner, die Sie zur Wiederherstellung ausgewählt haben, werden im rechten Bereich des Bildschirms aufgelistet.

11. Wählen Sie **Weiter**.

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

- Für Windows-Gastsysteme geben Sie den UNC-Freigabepfad ein:
  - IPv4-Pfadbeispiel: `\\10.60.136.65\c$`
  - IPv6-Pfadbeispiel: `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`
- Für Linux-Gastsysteme geben Sie den lokalen Dateisystempfad oder die Adresse und den Pfad des Remote-Gastsystems ein:
  - Beispiel für einen lokalen Pfad: `/home/user/documents/file.txt`
  - IPv4-Pfadbeispiel: `10.60.136.65:/home/user/restore/`
  - IPv6-Pfadbeispiel: `fd20-8b1e-b255-832e—61.ipv6-literal.net:/home/user/restore/`

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

13. 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.

14. Wählen Sie **Wiederherstellen**.

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

Aktive VMDK-Mountsitzungen anzeigen

Aktive Gast-VM-Sitzungen werden beim Wiederherstellen von Dateien oder Ordnern angezeigt. Hier sehen Sie die VMDKs, die aktuell mit offenen Sitzungen verbunden sind.

Schritte

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

   Es wird eine Liste der offenen VMDK-Mount-Sitzungen angezeigt. Sie können die zugehörige Sicherung, die Quell-VM, den Mount-Pfad und weitere Informationen einsehen.

Fehlerbehebung bei der Wiederherstellung von Gastdateien

Beim Versuch, eine Gastdatei wiederherzustellen, können die folgenden Szenarien auftreten.

Die Gastdateiwiederherstellungssitzung ist leer

Dieses Problem tritt auf, wenn Sie eine Gastdatei-Wiederherstellungssitzung erstellen und das Gastbetriebssystem während der Sitzung neu startet. VMDKs im Gastbetriebssystem könnten offline bleiben, sodass die Liste der Wiederherstellungssitzungen für Gastdateien leer ist.

Um das Problem zu beheben, schalten Sie die VMDKs im Gastbetriebssystem manuell wieder online. Wenn die VMDKs online sind, zeigt die Dateiwiederherstellungssitzung des Gastes den richtigen Inhalt an.

Der Vorgang zum Anhängen der Festplatte beim Wiederherstellen der Gastdatei schlägt fehl

Dieses Problem tritt auf, wenn Sie einen Gastdateiwiederherstellungsvorgang starten, der Vorgang zum Anschließen der Festplatte jedoch fehlschlägt, obwohl VMware Tools ausgeführt wird und die Anmeldeinformationen des Gastbetriebssystems korrekt sind. In diesem Fall wird der folgende Fehler zurückgegeben:

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMware Tools is running properly on the system and that the account used is an Administrator account. Error is SystemError vix error codes = (3016, 0).
```

Um das Problem zu beheben, starten Sie den VMware Tools-Windows-Dienst auf dem Gastbetriebssystem neu und versuchen Sie dann erneut, die Gastdatei wiederherzustellen.

Sicherungen werden nicht getrennt, nachdem die Gastdateiwiederherstellungssitzung abgebrochen wurde

Dieses Problem tritt auf, wenn Sie einen Gastdateiwiederherstellungsvorgang aus einer VM-konsistenten

Sicherung durchführen. Während die Gastdateiwiederherstellungssitzung aktiv ist, wird eine weitere VM-konsistente Sicherung für dieselbe VM durchgeführt. Wenn die Gastdateiwiederherstellungssitzung entweder manuell oder automatisch nach 24 Stunden getrennt wird, werden die Sicherungen für die Sitzung nicht getrennt.

Um das Problem zu beheben, trennen Sie die VMDKs, die an die aktive Gastdateiwiederherstellungssitzung angehängt waren, manuell.