Sichern Sie Unix-Dateisysteme

SnapCenter software

NetApp
January 09, 2026

Inhalt

Sichern Sie Unix-Dateisysteme

Ermitteln Sie die für Backups verfügbaren UNIX-Dateisysteme

Nach der Installation des Plug-ins werden alle Dateisysteme auf diesem Host automatisch erkannt und auf der Seite „Ressourcen“ angezeigt. Sie können diese Dateisysteme zu Ressourcengruppen hinzufügen, um Datenschutzvorgänge auszuführen.

Bevor Sie beginnen

- Sie müssen Aufgaben wie die Installation des SnapCenter-Servers, das Hinzufügen von Hosts und das Erstellen von Speichersystemverbindungen abgeschlossen haben.
- Wenn sich die Dateisysteme auf einem virtuellen Maschinenlaufwerk (VMDK) oder Raw Device Mapping (RDM) befinden, müssen Sie das SnapCenter-Plug-in für VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren.

  Weitere Informationen finden Sie unter "Implementieren Sie das SnapCenter Plug-in für VMware vSphere".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste Ansicht die Option **Pfad** aus.
3. Klicken Sie Auf **Ressourcen Aktualisieren**.

   Die Dateisysteme werden zusammen mit Informationen wie Typ, Hostname, zugeordnete Ressourcengruppen und Richtlinien sowie Status angezeigt.

Erstellen Sie Backup-Richtlinien für Unix-Dateisysteme

Bevor Sie SnapCenter zum Sichern von Unix-Dateisystemen verwenden, müssen Sie eine Sicherungsrichtlinie für die Ressource oder die Ressourcengruppe erstellen, die Sie sichern möchten. Eine Backup-Richtlinie ist eine Reihe von Regeln, die das Managen, Planen und Aufbewahren von Backups regeln. Sie können auch die Einstellungen für Replikation, Skript und Backup-Typ festlegen. Das Erstellen einer Richtlinie spart Zeit, wenn Sie die Richtlinie für eine andere Ressource oder Ressourcengruppe wiederverwenden möchten.

Bevor Sie beginnen

- Sie müssen sich auf die Datensicherung vorbereitet haben, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Erkennen der Dateisysteme und das Erstellen von Storage-System-Verbindungen durchführen.
- Wenn Sie Snapshots auf einen sekundären gespiegelten oder Vault-Storage replizieren, muss Ihnen der SnapCenter Administrator die SVMs sowohl für die Quell- als auch für die Ziel-Volumes zugewiesen haben.

- Prüfen Sie die spezifischen Voraussetzungen und Einschränkungen von SnapMirror Active Sync. Weitere Informationen finden Sie unter "Objektgrenzen für die aktive SnapMirror Synchronisierung".

Über diese Aufgabe

- SnapLock
  - Wenn die Option „Backup-Kopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock Aufbewahrungsfrist kleiner oder gleich den genannten Aufbewahrungstagen sein.

    Wenn Sie eine Snapshot-Sperrfrist festlegen, wird das Löschen der Snapshots bis zum Ablauf der Aufbewahrungsfrist verhindert. Dies kann dazu führen, dass eine größere Anzahl von Snapshots beibehalten wird als in der Richtlinie angegeben.

  Bei ONTAP Version 9.12.1 und niedriger übernehmen die im Rahmen der Wiederherstellung aus den SnapLock Vault Snapshots erstellten Klone die Verfallszeit von SnapLock Vault. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite Einstellungen auf **Richtlinien**.
3. Wählen Sie **Unix File Systems** aus der Dropdown-Liste aus.
4. Klicken Sie Auf **Neu**.
5. Geben Sie auf der Seite Name den Richtliniennamen und Details ein.
6. Führen Sie auf der Seite Backup and Replication die folgenden Aktionen durch:

   a. Geben Sie die Backup-Einstellungen an.

   b. Geben Sie die Zeitplanhäufigkeit an, indem Sie **on Demand**, **hourly**, **Daily**, **Weekly** oder **Monthly** auswählen.

   c. Wählen Sie im Abschnitt sekundäre Replikationsoptionen auswählen eine oder beide der folgenden sekundären Replikationsoptionen aus:

Für dieses Feld…	**Tun Sie das…**
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation). Diese Option sollte für SnapMirror Active Sync aktiviert sein.
Aktualisieren Sie SnapVault nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen.
Fehler bei Wiederholungszählung	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

7. Geben Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für den Sicherungstyp und den

auf der Seite Sicherung und Replikation ausgewählten Zeitplantyp an:

Ihr Ziel ist	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots bei	Wählen Sie **Kopien, die behalten werden sollen**, und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Zahl überschreitet, werden die Snapshots mit den ältesten zuerst gelöschten Kopien gelöscht. Der maximale Aufbewahrungswert ist 1018. Backups schlagen fehl, wenn die Aufbewahrung auf einen Wert festgelegt ist, der höher ist, als die zugrunde liegende ONTAP Version unterstützt. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault-Replikation aktivieren möchten. Wenn Sie den Aufbewahrungszeitraum auf 1 festlegen, kann der Aufbewahrungsvorgang fehlschlagen, weil der erste Snapshot der ReferenzSnapshot für die SnapVault-Beziehung ist, bis ein neuerer Snapshot auf das Ziel repliziert wird.
Bewahren Sie die Snapshots für eine bestimmte Anzahl von Tagen auf	Wählen Sie **Kopien behalten für**, und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots vor dem Löschen aufbewahren möchten.
Sperrzeitraum für Snapshot-Kopien	Wählen Sie **Sperrzeitraum für Snapshot-Kopien** und geben Sie die Dauer in Tagen, Monaten oder Jahren an. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

8. Wählen Sie die Bezeichnung der Richtlinie aus.

Sie können primären Snapshots SnapMirror Labels für die Remote-Replikation zuweisen, sodass die primären Snapshots den Snapshot-Replikationsvorgang von SnapCenter auf sekundäre ONTAP -Systeme auslagern können. Dies kann erfolgen, ohne die Option SnapMirror oder SnapVault auf der Richtlinienseite zu aktivieren.

9. Geben Sie auf der Seite Skript den Pfad und die Argumente des Prescript oder Postscript ein, das Sie vor oder nach dem Backup ausführen möchten.

   Sie sollten überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host verfügbar ist, über den Pfad _ /opt/NetApp/SnapCenter/scc/etc/allowed_commands.config_.

   Sie können auch den Wert für das Skript-Timeout angeben. Der Standardwert ist 60 Sekunden.

10. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Unix-Dateisysteme

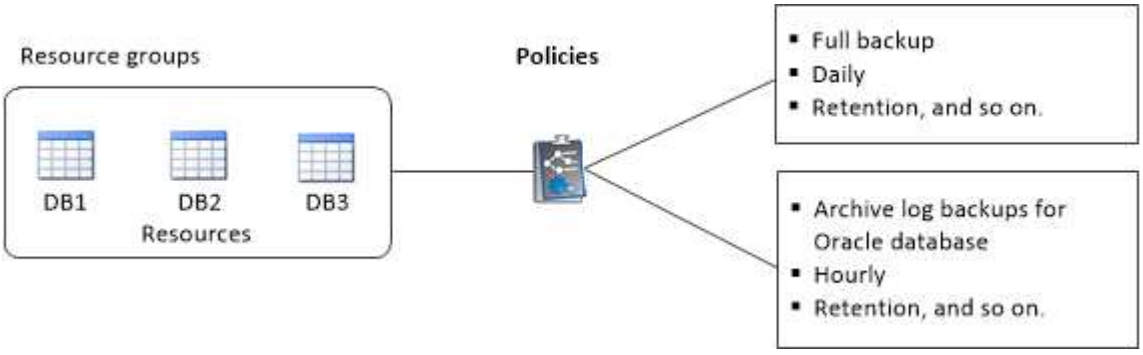
Eine Ressourcengruppe ist ein Container, in dem Sie Ressourcen hinzufügen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten sichern, die mit den Dateisystemen verknüpft sind.

Über diese Aufgabe

- Eine Datenbank mit Dateien in ASM-Datenträgergruppen muss sich im „MOUNT“- oder „OPEN“-Zustand befinden, um ihre Backups mit dem Dienstprogramm Oracle DBVERIFY zu überprüfen.

  Fügen Sie der Ressourcengruppe eine oder mehrere Richtlinien hinzu, um den Typ des Datenschutzauftrags zu definieren, den Sie ausführen möchten.

  Das folgende Bild veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



- Wenn Sie für Richtlinien mit aktiviertem SnapLock für ONTAP 9.12.1 und ältere Versionen einen Sperrzeitraum für Snapshots festlegen, übernehmen die Klone, die im Rahmen der Wiederherstellung aus den manipulationssicheren Snapshots erstellt wurden, die SnapLock-Auslaufzeit. Der Storage-Administrator sollte die Klone nach Ablauf der SnapLock-Gültigkeitsdauer manuell bereinigen.
- Das Hinzufügen neuer Dateisysteme ohne SnapMirror Active Sync zu einer vorhandenen Ressourcengruppe, die Ressourcen mit SnapMirror Active Sync enthält, wird nicht unterstützt.
- Das Hinzufügen neuer Dateisysteme zu einer vorhandenen Ressourcengruppe im Failover-Modus von SnapMirror Active Sync wird nicht unterstützt. Sie können der Ressourcengruppe nur im regulären oder Failback-Status Ressourcen hinzufügen.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-in aus der Liste aus.

2. Klicken Sie auf der Seite Ressourcen auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite Name die folgenden Aktionen durch:
   a. Geben Sie im Feld Name einen Namen für die Ressourcengruppe ein.

      Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

   b. Geben Sie eine oder mehrere Beschriftungen in das Feld Tag ein, um später nach der Ressourcengruppe zu suchen.

      Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.

   c. Aktivieren Sie das Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

      Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

4. Wählen Sie auf der Seite Ressourcen einen Host-Namen für Unix-Dateisysteme aus der Dropdown-Liste **Host** aus.

   Die Ressourcen werden im Abschnitt Verfügbare Ressourcen nur dann aufgelistet, wenn die Ressource erfolgreich ermittelt wurde. Wenn Sie vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

5. Wählen Sie im Abschnitt Verfügbare Ressourcen die Ressourcen aus, und verschieben Sie sie in den Abschnitt Ausgewählte Ressourcen.
6. Führen Sie auf der Seite Anwendungseinstellungen die folgenden Schritte aus:
   - Wählen Sie den Pfeil für Skripte aus und geben Sie die Befehle vor und nach für Stilllegung, Snapshots und Stilllegung ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.
   - Wählen Sie eine der Backup-Konsistenzoptionen aus:
     - Wählen Sie **File System consistent** aus, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden und keine ein- oder Ausgabevorgänge im Dateisystem während der Erstellung der Sicherung erlaubt sind.

       Für File-System-konsistente Snapshots werden für LUNs, die in der Volume-Gruppe beteiligt sind, Snapshots von Konsistenzgruppen erstellt.

     - Wählen Sie **Crash-konsistent**, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden.

       Wenn Sie verschiedene Dateisysteme in der Ressourcengruppe hinzugefügt haben, werden alle Volumes aus verschiedenen Dateisystemen in der Ressourcengruppe in eine Konsistenzgruppe aufgenommen.

7. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:

a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

   Sie können eine Richtlinie auch erstellen, indem Sie auf klicken .

   Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

b. Klicken Sie Auf In der Spalte Zeitplan konfigurieren für die Richtlinie konfigurieren, für die Sie einen Zeitplan konfigurieren möchten.

c. Konfigurieren Sie im Fenster Add Schedules for Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

   Dabei ist *Policy_Name* der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht des Vorgangs anhängen möchten, der in der Ressourcengruppe ausgeführt wird, wählen Sie **Job-Bericht anhängen**.

   Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Erstellen Sie Ressourcengruppen und aktivieren Sie sekundären Schutz für Unix-Dateisysteme auf ASA r2-Systemen

Sie sollten die Ressourcengruppe erstellen, um die Ressourcen hinzuzufügen, die sich auf ASA r2-Systemen befinden. Sie können auch den sekundären Schutz bereitstellen, während Sie die Ressourcengruppe erstellen.

Bevor Sie beginnen

- Sie sollten sicherstellen, dass Sie nicht sowohl ONTAP 9.x-Ressourcen als auch ASA r2-Ressourcen zur gleichen Ressourcengruppe hinzufügen.
- Sie sollten sicherstellen, dass keine Datenbank mit ONTAP 9.x-Ressourcen und ASA r2-Ressourcen vorhanden ist.

Über diese Aufgabe

- Der sekundäre Schutz ist nur verfügbar, wenn der angemeldete Benutzer der Rolle zugewiesen ist, die die Funktion **SecondaryProtection** aktiviert hat.

- Wenn Sie den sekundären Schutz aktiviert haben, wird die Ressourcengruppe beim Erstellen der primären und sekundären Konsistenzgruppen in den Wartungsmodus versetzt. Nach dem Erstellen der primären und sekundären Konsistenzgruppen wird die Ressourcengruppe aus dem Wartungsmodus versetzt.
- SnapCenter unterstützt keinen sekundären Schutz für eine Klonressource.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf der Seite Ressourcen auf **Neue Ressourcengruppe**.
3. Führen Sie auf der Seite Name die folgenden Aktionen durch:
   a. Geben Sie im Feld Name einen Namen für die Ressourcengruppe ein.

      Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

   b. Geben Sie eine oder mehrere Beschriftungen in das Feld Tag ein, um später nach der Ressourcengruppe zu suchen.

      Wenn Sie beispielsweise HR als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle Ressourcengruppen finden, die mit dem HR-Tag verknüpft sind.

   c. Aktivieren Sie dieses Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

      Beispiel: Custtext_Resource Group_Policy_hostname oder Resource Group_hostname. Standardmäßig wird an den Snapshot Namen ein Zeitstempel angehängt.

   d. Geben Sie die Ziele der Archivprotokolldateien an, die Sie nicht sichern möchten.

      Sie sollten bei Bedarf genau das gleiche Ziel verwenden, wie es in der Anwendung einschließlich Präfix festgelegt wurde.

4. Wählen Sie auf der Seite Ressourcen den Hostnamen der Datenbank aus der Dropdown-Liste **Host** aus.

   Die Ressourcen werden im Abschnitt Verfügbare Ressourcen nur dann aufgelistet, wenn die Ressource erfolgreich ermittelt wurde. Wenn Sie vor Kurzem Ressourcen hinzugefügt haben, werden diese erst nach einer Aktualisierung der Ressourcenliste in der Liste der verfügbaren Ressourcen angezeigt.

5. Wählen Sie die ASA r2-Ressourcen im Abschnitt „Verfügbare Ressourcen“ aus, und verschieben Sie sie in den Abschnitt „Ausgewählte Ressourcen“.
6. Wählen Sie auf der Seite Anwendungseinstellungen die Sicherungsoption aus.
7. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:
   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

      Sie können eine Richtlinie auch erstellen, indem Sie auf klicken + .

      Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

b. Klicken Sie Auf  In der Spalte Zeitplan konfigurieren für die Richtlinie konfigurieren, für die Sie einen Zeitplan konfigurieren möchten.

c. Konfigurieren Sie im Fenster Add Schedules for Policy_Name_ den Zeitplan, und klicken Sie dann auf **OK**.

Dabei ist *Policy_Name* der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

Backup-Zeitpläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit SnapCenter Backup-Zeitplänen überschneiden.

8. Wenn der sekundäre Schutz für die ausgewählte Richtlinie aktiviert ist, wird die Seite sekundärer Schutz angezeigt, und Sie müssen die folgenden Schritte ausführen:

a. Wählen Sie den Typ der Replikationsrichtlinie aus.

Die Richtlinie für die synchrone Replizierung wird nicht unterstützt.

b. Geben Sie das Suffix für die Konsistenzgruppe an, das Sie verwenden möchten.

c. Wählen Sie in den Drop-Downs Ziel-Cluster und Ziel-SVM den zu verwendenden Peering-Cluster und die SVM aus.

Cluster und SVM-Peering werden von SnapCenter nicht unterstützt. Sie sollten System Manager oder ONTAP CLIs verwenden, um Cluster- und SVM-Peering durchzuführen.

Wenn die Ressourcen bereits außerhalb von SnapCenter geschützt sind, werden diese Ressourcen im Abschnitt sekundäre geschützte Ressourcen angezeigt.

1. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:

a. Klicken Sie auf **Lokatoren laden**, um die SnapMirror oder SnapVault Volumes zu laden, um eine Überprüfung auf dem sekundären Speicher durchzuführen.

b. Klicken Sie Auf  In der Spalte Configure Schedules (Zeitpläne konfigurieren), um den Überprüfungsplan für alle Zeitplantypen der Richtlinie zu konfigurieren.

c. Führen Sie im Dialogfeld Add Verification Schedules Policy_Name die folgenden Aktionen durch:

Ihr Ziel ist	**Tun Sie das…**
Führen Sie die Verifizierung nach dem Backup durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planung einer Verifizierung	Wählen Sie **geplante Überprüfung ausführen** und wählen Sie dann den Terminplantyp aus der Dropdown-Liste aus.

d. Wählen Sie **am sekundären Standort überprüfen**, um Ihre Backups auf dem sekundären Speichersystem zu überprüfen.

e. Klicken Sie auf **OK**.

   Die konfigurierten Überprüfungszeitpläne sind in der Spalte „angewendete Zeitpläne“ aufgeführt.

2. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails versenden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht des Vorgangs anhängen möchten, der in der Ressourcengruppe ausgeführt wird, wählen Sie **Job-Bericht anhängen**.

   Für eine E-Mail-Benachrichtigung müssen Sie die SMTP-Serverdetails entweder mit der GUI oder mit dem PowerShell-Befehlssatz Set-SmtpServer angegeben haben.

3. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Sichern Sie Unix-Dateisysteme

Wenn eine Ressource nicht zu einer Ressourcengruppe gehört, können Sie die Ressource auf der Seite Ressourcen sichern.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste Ansicht die Option **Pfad** aus.
3. Klicken Sie auf , und wählen Sie dann den Hostnamen und die Unix-Dateisysteme aus, um die Ressourcen zu filtern.
4. Wählen Sie das Dateisystem aus, das Sie sichern möchten.
5. Auf der Seite „Ressourcen“ können Sie die folgenden Schritte ausführen:
   a. Aktivieren Sie das Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

      Beispiel: `customtext_policy_hostname` Oder `resource_hostname`. Standardmäßig wird ein Zeitstempel an den Snapshot Namen angehängt.

6. Führen Sie auf der Seite Anwendungseinstellungen die folgenden Schritte aus:
   - Wählen Sie den Pfeil für Skripte aus und geben Sie die Befehle vor und nach für Stilllegung, Snapshots und Stilllegung ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.
   - Wählen Sie eine der Backup-Konsistenzoptionen aus:
     - Wählen Sie **File System consistent** aus, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden und keine Vorgänge auf dem Dateisystem während der Erstellung der Sicherung ausgeführt werden.
     - Wählen Sie **Crash-konsistent**, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden.
7. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

Sie können eine Richtlinie erstellen, indem Sie auf klicken .

Im Abschnitt „Zeitpläne für ausgewählte Richtlinien konfigurieren“ werden die ausgewählten Richtlinien aufgelistet.

b. Klicken Sie Auf In der Spalte Configure Schedules (Zeitpläne konfigurieren) können Sie einen Zeitplan für die gewünschte Richtlinie konfigurieren.

c. Konfigurieren Sie im Fenster Add Schedules for Policy *Policy_Name* den Zeitplan, und wählen Sie dann aus `OK`.

Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails senden möchten.

Sie müssen die E-Mail-Adressen von Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht des auf der Ressource durchgeführten Sicherungsvorgangs anhängen möchten, wählen Sie **Job-Bericht anhängen**.

Für E-Mail-Benachrichtigungen müssen Sie die SMTP-Serverdetails entweder über die GUI oder über den PowerShell-Befehl angegeben haben `Set-SmSmtpServer`.

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Die Topologieseite wird angezeigt.

10. Klicken Sie auf **Jetzt sichern**.
11. Führen Sie auf der Seite Backup die folgenden Schritte aus:

a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste Richtlinie die Richtlinie aus, die Sie für das Backup verwenden möchten.

Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

b. Klicken Sie Auf **Backup**.

12. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Erstellen Sie ein Backup von Ressourcengruppen für Unix-Dateisysteme

Sie können die in der Ressourcengruppe definierten Unix-Dateisysteme sichern. Auf der Seite „Ressourcen“ können Sie ein Backup einer Ressourcengruppe nach Bedarf erstellen. Wenn einer Ressourcengruppe eine Richtlinie angehängt und ein Zeitplan konfiguriert ist, werden Backups gemäß dem Zeitplan erstellt.

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste **Ansicht** die Option **Ressourcengruppe** aus.
3. Geben Sie den Namen der Ressourcengruppe in das Suchfeld ein, oder klicken Sie auf , und wählen Sie das Tag aus.

   Klicken Sie auf , um das Filterfenster zu schließen.
4. Wählen Sie auf der Seite Ressourcengruppe die Ressourcengruppe aus, die gesichert werden soll.
5. Führen Sie auf der Seite Backup die folgenden Schritte aus:
   a. Wenn Sie mehrere Richtlinien mit der Ressourcengruppe verknüpft haben, wählen Sie die zu verwendende Sicherungsrichtlinie aus der Dropdown-Liste **Policy** aus.

      Wenn die für das On-Demand-Backup ausgewählte Richtlinie einem Backup-Zeitplan zugeordnet ist, werden die On-Demand-Backups auf Basis der für den Zeitplantyp festgelegten Aufbewahrungseinstellungen beibehalten.

   b. Wählen Sie **Backup**.
6. Überwachen Sie den Fortschritt, indem Sie **Monitor > Jobs** auswählen.

Überwachen Sie das Backup von Unix-Dateisystemen

Erfahren Sie, wie Sie den Fortschritt von Backup-Vorgängen und Datensicherungsvorgängen überwachen.

Überwachen Sie die Backup-Vorgänge für Unix-Dateisysteme

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Jobs angezeigt und zeigen den entsprechenden Status der Vorgänge an:

- In Bearbeitung
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Abgeschlossen mit Warnungen oder konnte aufgrund von Warnungen nicht gestartet werden
- Warteschlange
- Storniert

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.
3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:

a. Klicken Sie hier , um die Liste so zu filtern, dass nur Backup-Vorgänge aufgeführt werden.
b. Geben Sie das Start- und Enddatum an.
c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.

4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

> Obwohl der Status des Sicherungsauftrags angezeigt wird , wird beim Klicken auf Jobdetails möglicherweise angezeigt, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.

   Die Schaltfläche **Protokolle anzeigen** zeigt die detaillierten Protokolle für den ausgewählten Vorgang an.

Überwachen Sie Datensicherungsvorgänge im Teilfenster „Vorgang“

Im Aktivitätsbereich werden die fünf zuletzt durchgeführten Operationen angezeigt. Der Bereich „Aktivität“ wird auch angezeigt, wenn der Vorgang initiiert wurde und der Status des Vorgangs.

Im Fensterbereich Aktivität werden Informationen zu Backup-, Wiederherstellungs-, Klon- und geplanten Backup-Vorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Klicken Sie auf den Bereich „Aktivität“, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Job-Details** aufgeführt.

Zeigen Sie geschützte Unix-Dateisysteme auf der Seite Topologie an

Wenn Sie die Erstellung von Backups, Wiederherstellungen oder Klonvorgängen für eine Ressource vorbereiten, ist es möglicherweise hilfreich, eine grafische Darstellung aller Backups, wiederhergestellten Dateisysteme und Klone im primären und sekundären Storage anzuzeigen.

Über diese Aufgabe

Auf der Seite Topologie werden alle Backups, wiederhergestellten Dateisysteme und Klone angezeigt, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details zu diesen Backups, wiederhergestellten Dateisystemen und Klonen anzeigen und sie dann auswählen, um Datensicherungsvorgänge durchzuführen.

In der Ansicht Kopien managen können Sie die folgenden Symbole überprüfen, um festzustellen, ob die Backups und Klone auf dem primären oder sekundären Storage (Mirror-Kopien oder Vault-Kopien) verfügbar

sind.

-  Zeigt die Anzahl der Backups und Klone an, die auf dem primären Speicher verfügbar sind.
-  Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapMirror Technologie auf dem sekundären Storage gespiegelt werden.
-  Zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault Technologie auf dem sekundären Storage repliziert werden.

  Die Anzahl der angezeigten Backups umfasst die Backups, die aus dem sekundären Speicher gelöscht wurden. Wenn Sie beispielsweise 6 Backups mit einer Richtlinie für die Aufbewahrung von nur 4 Backups erstellt haben, wird die Anzahl der angezeigten Backups 6 angezeigt.

Klone eines Backups einer versionsflexiblen Spiegelung auf einem Volume vom Typ Mirror werden in der Topologieansicht angezeigt, aber die Anzahl der gespiegelten Backups in der Topologieansicht umfasst nicht das versionsflexible Backup.

Wenn Sie eine sekundäre Beziehung als SnapMirror Active Sync haben (ursprünglich als SnapMirror Business Continuity [SM-BC] veröffentlicht), werden die folgenden zusätzlichen Symbole angezeigt:

-  Der Replikatstandort ist hochgefahren.
-  Der Replikatstandort ist ausgefallen.
-  Die sekundäre Spiegel- oder Vault-Beziehung wurde nicht wiederhergestellt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen entweder die Ressource oder Ressourcengruppe aus der Dropdown-Liste **Ansicht** aus.
3. Wählen Sie die Ressource entweder in der Ansicht „Ressourcendetails“ oder in der Ansicht „Ressourcengruppendetails“ aus.

   Wenn die Ressource geschützt ist, wird die Topologieseite der ausgewählten Ressource angezeigt.

4. Prüfen Sie die Übersichtskarte, um eine Zusammenfassung der Anzahl der Backups und Klone anzuzeigen, die auf dem primären und sekundären Storage verfügbar sind.

   Im Abschnitt „Übersichtskarte“ wird die Gesamtanzahl der Backups und Klone angezeigt.

   Durch Klicken auf die Schaltfläche **Aktualisieren** wird eine Abfrage des Speichers gestartet, um eine genaue Anzahl anzuzeigen.

Wenn ein SnapLock-fähiges Backup durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die primäre und sekundäre SnapLock-Ablaufzeit aktualisiert, die von ONTAP abgerufen wird. Ein wöchentlicher Zeitplan aktualisiert auch die primäre und sekundäre SnapLock-Ablaufzeit, die von ONTAP abgerufen wird.

Wenn das Dateisystem über mehrere Volumes verteilt ist, ist die SnapLock-Ablaufzeit für das Backup die längste SnapLock-Ablaufzeit, die für einen Snapshot in einem Volume festgelegt ist. Die längste SnapLock-Ablaufzeit wird von ONTAP abgerufen.

Bei aktiver SnapMirror-Synchronisierung wird durch Klicken auf die Schaltfläche * Aktualisieren* das SnapCenter-Backup-Inventar aktualisiert, indem ONTAP sowohl für primäre als auch für Replikatstandorte abgefragt wird. Ein wöchentlicher Zeitplan führt diese Aktivität auch für alle Datenbanken durch, die die aktive SnapMirror Synchronisierung enthalten.

- Bei aktiver SnapMirror Synchronisierung und nur für ONTAP 9.14.1 sollten die Beziehungen zwischen Async Mirror und Async MirrorVault zum neuen primären Ziel nach dem Failover manuell konfiguriert werden. Ab ONTAP 9.15.1 wird Async Mirror oder Async MirrorVault automatisch auf das neue primäre Ziel konfiguriert.
- Nach dem Failover sollte ein Backup erstellt werden, damit SnapCenter den Failover erkennt. Sie können erst dann auf **Refresh** klicken, wenn ein Backup erstellt wurde.

5. Klicken Sie in der Ansicht Kopien verwalten auf **Backups** oder **Klone** auf dem primären oder sekundären Speicher, um Details zu einem Backup oder Klon anzuzeigen.

   Die Details zu Backups und Klonen werden in einem Tabellenformat angezeigt.

6. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf die Datensicherungssymbole, um Restore-, Klon- und Löschvorgänge durchzuführen.

   Sie können Backups, die sich im sekundären Speicher befinden, nicht umbenennen oder löschen.

7. Wenn Sie einen Klon löschen möchten, wählen Sie den Klon aus der Tabelle aus, und klicken Sie dann auf .

Beispiel für Backups und Klone auf dem Primärspeicher


Manage Copies
2 Backups
1 Clone
Local copies
Summary Card
2 Backups
1 Clone
0 Snapshots Locked