Sichern Sie Unix-Dateisysteme

SnapCenter software

NetApp
November 06, 2025

Inhalt

Sichern Sie Unix-Dateisysteme

Entdecken Sie die für die Sicherung 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 durchzuführen.

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 einer Virtual Machine Disk (VMDK) oder Raw Device Mapping (RDM) befinden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren.

  Weitere Informationen finden Sie unter "Bereitstellen des SnapCenter Plug-in for 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, zugehörigen Ressourcengruppen und Richtlinien sowie Status angezeigt.

Erstellen Sie Sicherungsrichtlinien 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 Sicherungsrichtlinie ist ein Satz von Regeln, der regelt, wie Sie Sicherungen verwalten, planen und aufbewahren. Sie können auch die Replikations-, Skript- und Sicherungstypeinstellungen angeben. 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 den Datenschutz vorbereitet haben, indem Sie Aufgaben wie die Installation von SnapCenter, das Hinzufügen von Hosts, das Erkennen der Dateisysteme und das Erstellen von Speichersystemverbindungen abgeschlossen haben.
- Wenn Sie Snapshots auf einen Spiegel- oder Tresor-Sekundärspeicher replizieren, muss der SnapCenter Administrator Ihnen die SVMs sowohl für das Quell- als auch für das Zielvolume zugewiesen haben.
- Überprüfen Sie die spezifischen Voraussetzungen und Einschränkungen der SnapMirror Active Sync.

Weitere Informationen finden Sie unter "Objektlimits für SnapMirror Active Sync" .

Informationen zu diesem Vorgang

- SnapLock
  - Wenn die Option „Sicherungskopien für eine bestimmte Anzahl von Tagen aufbewahren“ ausgewählt ist, muss die SnapLock -Aufbewahrungsdauer kleiner oder gleich der angegebenen Aufbewahrungsdauer in Tagen sein.

    Durch die Angabe einer Snapshot-Sperrfrist wird das Löschen der Snapshots verhindert, bis die Aufbewahrungsfrist abgelaufen ist. Dies kann dazu führen, dass mehr Snapshots aufbewahrt werden als in der Richtlinie angegeben.

Bei ONTAP 9.12.1 und niedrigeren Versionen erben die im Rahmen der Wiederherstellung aus den SnapLock Vault-Snapshots erstellten Klone die Ablaufzeit von SnapLock Vault. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock manuell bereinigen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Einstellungen**.
2. Klicken Sie auf der Seite „Einstellungen“ auf **Richtlinien**.
3. Wählen Sie **Unix-Dateisysteme** aus der Dropdownliste.
4. Klicken Sie auf **Neu**.
5. Geben Sie auf der Seite „Name“ den Richtliniennamen und die Details ein.
6. Führen Sie auf der Seite „Sicherung und Replikation“ die folgenden Aktionen aus:
   a. Geben Sie die Sicherungseinstellungen an.
   b. Geben Sie die Zeitplanhäufigkeit an, indem Sie **Auf Anfrage**, **Stündlich**, **Täglich**, **Wöchentlich** oder **Monatlich** auswählen.
   c. Wählen Sie im Abschnitt „Sekundäre Replikationsoptionen auswählen“ eine oder beide der folgenden sekundären Replikationsoptionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Aktualisieren Sie SnapMirror , nachdem Sie eine lokale Snapshot-Kopie erstellt haben	Wählen Sie dieses Feld aus, um Spiegelkopien der Sicherungssätze auf einem anderen Volume zu erstellen (SnapMirror -Replikation). Diese Option sollte für die aktive Synchronisierung von SnapMirror aktiviert werden.
Aktualisieren Sie SnapVault , nachdem Sie eine lokale Snapshot-Kopie erstellt haben	Wählen Sie diese Option, um eine Backup-Replikation von Festplatte zu Festplatte durchzuführen (SnapVault -Backups).
Fehleranzahl der Wiederholungsversuche	Geben Sie die maximale Anzahl an Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

7. Geben Sie auf der Seite „Aufbewahrung“ die Aufbewahrungseinstellungen für den Sicherungstyp und den Zeitplantyp an, die auf der Seite „Sicherung und Replikation“ ausgewählt wurden:

Wenn Sie wollen…	Dann…
Behalten Sie eine bestimmte Anzahl von Snapshots	Wählen Sie **Zu behaltende Kopien** und geben Sie dann die Anzahl der Snapshots an, die Sie behalten möchten. Wenn die Anzahl der Snapshots die angegebene Anzahl überschreitet, werden die Snapshots gelöscht, wobei die ältesten Kopien zuerst gelöscht werden. Der maximale Aufbewahrungswert beträgt 1018. Sicherungen schlagen fehl, wenn die Aufbewahrung auf einen höheren Wert eingestellt ist, als von der zugrunde liegenden ONTAP Version unterstützt wird. Sie müssen die Aufbewahrungsanzahl auf 2 oder höher einstellen, wenn Sie die SnapVault -Replikation aktivieren möchten. Wenn Sie die Aufbewahrungsanzahl auf 1 setzen, schlägt der Aufbewahrungsvorgang möglicherweise fehl, da der erste Snapshot der Referenz-Snapshot 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 aufbewahren für** und geben Sie dann die Anzahl der Tage an, für die Sie die Snapshots aufbewahren möchten, bevor sie gelöscht werden.
Sperrzeitraum für Snapshot-Kopien	Wählen Sie **Sperrzeitraum für Snapshot-Kopien** und geben Sie die Dauer in Tagen, Monaten oder Jahren an. Die Aufbewahrungsdauer von Snaplock sollte weniger als 100 Jahre betragen.

8. Wählen Sie die Richtlinienbezeichnung 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 Präskripts oder Postskripts ein, das Sie

vor bzw. nach dem Sicherungsvorgang ausführen möchten.

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

Sie können auch den Timeout-Wert des Skripts angeben. Der Standardwert beträgt 60 Sekunden.

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

Erstellen Sie Ressourcengruppen und fügen Sie Richtlinien für Unix-Dateisysteme hinzu

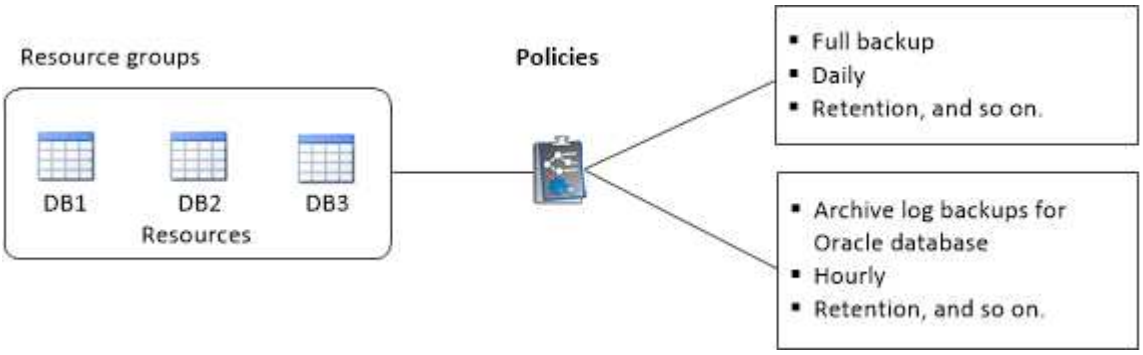
Eine Ressourcengruppe ist ein Container, dem Sie Ressourcen hinzufügen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle mit den Dateisystemen verknüpften Daten sichern.

Informationen zu diesem Vorgang

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

  Fügen Sie der Ressourcengruppe eine oder mehrere Richtlinien hinzu, um die Art des Datenschutzjobs zu definieren, den Sie ausführen möchten.

  Die folgende Abbildung veranschaulicht die Beziehung zwischen Ressourcen, Ressourcengruppen und Richtlinien für Datenbanken:



- Wenn Sie für SnapLock -fähige Richtlinien für ONTAP 9.12.1 und niedrigere Versionen eine Snapshot-Sperrdauer angeben, erben die im Rahmen der Wiederherstellung aus den manipulationssicheren Snapshots erstellten Klone die SnapLock Ablaufzeit. Der Speicheradministrator sollte die Klone nach Ablauf des SnapLock 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-Zustand 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 aus:
   a. Geben Sie im Feld „Name“ einen Namen für die Ressourcengruppe ein.

      Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.

   b. Geben Sie im Feld „Tag“ eine oder mehrere Bezeichnungen ein, um die spätere Suche nach der Ressourcengruppe zu erleichtern.

      Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

   c. Aktivieren Sie das Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

      Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

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

   Die Ressourcen werden nur dann im Abschnitt „Verfügbare Ressourcen“ aufgeführt, wenn die Ressource erfolgreich erkannt wurde. Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

5. Wählen Sie die Ressourcen aus dem Abschnitt „Verfügbare 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 „Skripts“ aus und geben Sie die Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge ein. Sie können auch die Vorbefehle eingeben, die im Falle eines Fehlers vor dem Beenden ausgeführt werden sollen.
   - Wählen Sie eine der Optionen zur Sicherungskonsistenz aus:
     - Wählen Sie **Dateisystemkonsistent**, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten des Dateisystems vor dem Erstellen der Sicherung gelöscht werden und während der Erstellung der Sicherung keine Eingabe- oder Ausgabevorgänge auf dem Dateisystem zulässig sind.

       Für die Dateisystemkonsistenz werden Konsistenzgruppen-Snapshots für die an der Volume-Gruppe beteiligten LUNs erstellt.

     - Wählen Sie **Absturzkonsistent**, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten des Dateisystems vor dem Erstellen der Sicherung gelöscht werden.

       Wenn Sie der Ressourcengruppe unterschiedliche Dateisysteme hinzugefügt haben, werden alle Volumes aus unterschiedlichen Dateisystemen in der Ressourcengruppe in eine Konsistenzgruppe eingefügt.

7. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:
   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

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

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

b. Klicken + in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan konfigurieren möchten.

c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

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

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden.

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

Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

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

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

Erstellen Sie Ressourcengruppen und aktivieren Sie den 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 den sekundären Schutz auch beim Erstellen der Ressourcengruppe bereitstellen.

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 Sie keine Datenbank mit ONTAP 9.x-Ressourcen und ASA r2-Ressourcen haben.

Informationen zu diesem Vorgang

- Der sekundäre Schutz ist nur verfügbar, wenn dem angemeldeten Benutzer die Rolle zugewiesen ist, für die die Funktion **SecondaryProtection** aktiviert ist.
- Wenn Sie den sekundären Schutz aktiviert haben, wird die Ressourcengruppe beim Erstellen der primären und sekundären Konsistenzgruppen in den Wartungsmodus versetzt. Nachdem die primäre und sekundäre

Konsistenzgruppe erstellt wurden, wird der Wartungsmodus der Ressourcengruppe beendet.

- 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 aus:
   a. Geben Sie im Feld „Name“ einen Namen für die Ressourcengruppe ein.

      Der Name der Ressourcengruppe sollte nicht länger als 250 Zeichen sein.

   b. Geben Sie im Feld „Tag“ eine oder mehrere Bezeichnungen ein, um die spätere Suche nach der Ressourcengruppe zu erleichtern.

      Wenn Sie beispielsweise „HR“ als Tag zu mehreren Ressourcengruppen hinzufügen, können Sie später alle mit dem HR-Tag verknüpften Ressourcengruppen finden.

   c. Aktivieren Sie dieses Kontrollkästchen und geben Sie ein benutzerdefiniertes Namensformat ein, das Sie für den Snapshot-Namen verwenden möchten.

      Beispiel: benutzerdefinierter Text_Ressourcengruppenrichtlinien-Hostname oder Ressourcengruppen-Hostname. Standardmäßig wird dem Snapshot-Namen ein Zeitstempel angehängt.

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

      Sie sollten genau dasselbe Ziel verwenden, das in der Anwendung festgelegt wurde, gegebenenfalls einschließlich Präfix.

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

   Die Ressourcen werden nur dann im Abschnitt „Verfügbare Ressourcen“ aufgeführt, wenn die Ressource erfolgreich erkannt wurde. Wenn Sie kürzlich Ressourcen hinzugefügt haben, werden diese erst in der Liste der verfügbaren Ressourcen angezeigt, nachdem Sie Ihre Ressourcenliste aktualisiert haben.

5. Wählen Sie die ASA r2-Ressourcen aus dem 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 Dropdownliste aus.

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

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

   b. Klicken + in der Spalte „Zeitpläne konfigurieren“ für die Richtlinie, für die Sie einen Zeitplan

konfigurieren möchten.

c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtlinienname* hinzufügen“ den Zeitplan und klicken Sie dann auf **OK**.

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

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

Sicherungspläne von Drittanbietern werden nicht unterstützt, wenn sie sich mit den Sicherungsplänen von SnapCenter überschneiden.

8. Wenn der sekundäre Schutz für die von Ihnen 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 synchrone Replikationsrichtlinie wird nicht unterstützt.

   b. Geben Sie das Konsistenzgruppensuffix an, das Sie verwenden möchten.
   c. Wählen Sie aus den Dropdown-Menüs „Zielcluster“ und „Ziel-SVM“ den Peering-Cluster und die SVM aus, die Sie verwenden möchten.

      Das Cluster- und SVM-Peering wird 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 „Sekundär geschützte Ressourcen“ angezeigt.

1. Führen Sie auf der Seite „Verifizierung“ die folgenden Schritte aus:
   a. Klicken Sie auf **Locators laden**, um die SnapMirror oder SnapVault -Volumes zu laden und die Überprüfung auf dem sekundären Speicher durchzuführen.
   b. Klicken + in der Spalte „Zeitpläne konfigurieren“, um den Überprüfungszeitplan für alle Zeitplantypen der Richtlinie zu konfigurieren.
   c. Führen Sie im Dialogfeld „Verifizierungszeitpläne hinzufügen“ (Richtlinienname) die folgenden Aktionen aus:

Wenn Sie wollen…	**Machen Sie Folgendes…**
Führen Sie nach der Sicherung eine Überprüfung durch	Wählen Sie **Überprüfung nach Sicherung ausführen**.
Planen Sie eine Überprüfung	Wählen Sie **Geplante Überprüfung ausführen** und wählen Sie dann den Zeitplantyp aus der Dropdownliste aus.

   d. Wählen Sie **Am sekundären Speicherort überprüfen**, um Ihre Sicherungen auf dem sekundären Speichersystem zu überprüfen.

e. Klicken Sie auf **OK**.

   Die konfigurierten Überprüfungszeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

2. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mails senden möchten.

   Sie müssen außerdem die E-Mail-Adressen des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den an der Ressourcengruppe durchgeführten Vorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

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

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

Sichern Sie Unix-Dateisysteme

Wenn eine Ressource nicht Teil einer Ressourcengruppe ist, können Sie die Ressource von der Seite „Ressourcen“ aus 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 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 Sie für den Snapshot-Namen verwenden möchten.

      Zum Beispiel, `customtext_policy_hostname` oder `resource_hostname` . Dem Snapshot-Namen wird standardmäßig ein Zeitstempel angehängt.

6. Führen Sie auf der Seite „Anwendungseinstellungen“ die folgenden Schritte aus:
   - Wählen Sie den Pfeil „Skripts“ aus und geben Sie die Pre- und Post-Befehle für Quiesce-, Snapshot- und Unquiesce-Vorgänge ein. Sie können auch die Vorbefehle eingeben, die im Falle eines Fehlers vor dem Beenden ausgeführt werden sollen.
   - Wählen Sie eine der Optionen zur Sicherungskonsistenz aus:
     - Wählen Sie **Dateisystemkonsistent**, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten des Dateisystems vor dem Erstellen der Sicherung geleert werden und während der Erstellung der Sicherung keine Vorgänge am Dateisystem ausgeführt werden.
     - Wählen Sie **Absturzkonsistent**, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten des Dateisystems vor dem Erstellen der Sicherung gelöscht werden.
7. Führen Sie auf der Seite „Richtlinien“ die folgenden Schritte aus:

   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdownliste aus.

Sie können eine Richtlinie erstellen, indem Sie auf + .

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

b. Klicken + in der Spalte „Zeitpläne konfigurieren“, um einen Zeitplan für die gewünschte Richtlinie zu konfigurieren.

c. Konfigurieren Sie im Fenster „Zeitpläne für Richtlinie *Richtliniennamе* hinzufügen“ den Zeitplan und wählen Sie dann `OK` .

policy_name ist der Name der von Ihnen ausgewählten Richtlinie.

Die konfigurierten Zeitpläne werden in der Spalte „Angewandte Zeitpläne“ aufgelistet.

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 des Absenders und des Empfängers sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den für die Ressource durchgeführten Sicherungsvorgang anhängen möchten, wählen Sie **Jobbericht anhängen**.

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

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

Die Topologieseite wird angezeigt.

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

a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdownliste „Richtlinie“ die Richtlinie aus, die Sie für die Sicherung verwenden möchten.

Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

b. Klicken Sie auf **Sichern**.

12. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

Sichern von Ressourcengruppen von Unix-Dateisystemen

Sie können die in der Ressourcengruppe definierten Unix-Dateisysteme sichern. Sie können eine Ressourcengruppe bei Bedarf von der Seite „Ressourcen“ aus sichern. Wenn einer Ressourcengruppe eine Richtlinie zugeordnet und ein Zeitplan konfiguriert ist, werden Sicherungen 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 „Anzeigen“ 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 , um den Filterbereich zu schließen.

4. Wählen Sie auf der Seite „Ressourcengruppe“ die zu sichernde Ressourcengruppe aus.
5. Führen Sie auf der Seite „Sichern“ die folgenden Schritte aus:
   a. Wenn der Ressourcengruppe mehrere Richtlinien zugeordnet sind, wählen Sie aus der Dropdownliste **Richtlinie** die gewünschte Sicherungsrichtlinie aus.

      Wenn die für die On-Demand-Sicherung ausgewählte Richtlinie mit einem Sicherungszeitplan verknüpft ist, werden die On-Demand-Sicherungen basierend auf den für den Zeitplantyp angegebenen Aufbewahrungseinstellungen aufbewahrt.

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

Überwachen Sie die Sicherung von Unix-Dateisystemen

Erfahren Sie, wie Sie den Fortschritt von Sicherungs- und Datenschutzvorgängen überwachen.

Überwachen Sie Sicherungsvorgänge für Unix-Dateisysteme

Sie können den Fortschritt verschiedener Sicherungsvorgänge mithilfe der SnapCenterJobs-Seite überwachen. Möglicherweise möchten Sie den Fortschritt überprüfen, um festzustellen, wann der Vorgang abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

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

- Im Gange
- Erfolgreich abgeschlossen
- Fehlgeschlagen
- Mit Warnungen abgeschlossen oder konnte aufgrund von Warnungen nicht gestartet werden
- In der Warteschlange
- Abgesagt

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 um die Liste so zu filtern, dass nur Sicherungsvorgänge aufgelistet werden.
b. Geben Sie das Start- und Enddatum an.
c. Wählen Sie aus der Dropdownliste **Typ** die Option **Backup** aus.
d. Wählen Sie aus der Dropdown-Liste **Status** den Sicherungsstatus aus.
e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.

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

> Obwohl der Status des Sicherungsauftrags angezeigt wird Wenn Sie auf die Auftragsdetails klicken, sehen Sie möglicherweise, dass einige der untergeordneten Aufgaben des Sicherungsvorgangs noch ausgeführt werden oder mit Warnzeichen markiert sind.

5. Klicken Sie auf der Seite „Auftragsdetails“ auf **Protokolle anzeigen**.

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

Überwachen von Datenschutzvorgängen im Aktivitätsbereich

Im Aktivitätsbereich werden die fünf zuletzt ausgeführten Vorgänge angezeigt. Im Aktivitätsbereich wird auch angezeigt, wann der Vorgang gestartet wurde und welchen Status er hat.

Im Aktivitätsbereich werden Informationen zu Sicherungs-, Wiederherstellungs-, Klon- und geplanten Sicherungsvorgängen angezeigt.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Ressourcen** und wählen Sie dann das entsprechende Plug-In aus der Liste aus.
2. Klicken im Aktivitätsbereich, um die fünf letzten Vorgänge anzuzeigen.

   Wenn Sie auf einen der Vorgänge klicken, werden die Vorgangsdetails auf der Seite **Auftragsdetails** aufgelistet.

Geschützte Unix-Dateisysteme auf der Seite „Topologie“ anzeigen

Wenn Sie das Sichern, Wiederherstellen oder Klonen einer Ressource vorbereiten, kann es hilfreich sein, eine grafische Darstellung aller Sicherungen, wiederhergestellten Dateisysteme und Klone auf dem primären und sekundären Speicher anzuzeigen.

Über diese Aufgabe

Auf der Seite „Topologie“ können Sie alle Sicherungen, wiederhergestellten Dateisysteme und Klone sehen, die für die ausgewählte Ressource oder Ressourcengruppe verfügbar sind. Sie können die Details dieser Sicherungen, wiederhergestellten Dateisysteme und Klone anzeigen und sie dann auswählen, um Datenschutzvorgänge durchzuführen.

Sie können die folgenden Symbole in der Ansicht „Kopien verwalten“ überprüfen, um festzustellen, ob die

Sicherungen und Klone auf dem primären oder sekundären Speicher verfügbar sind (Spiegelkopien oder Tresorkopien).

-  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 Speicher gespiegelt werden.
-  zeigt die Anzahl der Backups und Klone an, die mithilfe der SnapVault -Technologie auf dem sekundären Speicher repliziert werden.

  Die angezeigte Anzahl der Backups umfasst die aus dem sekundären Speicher gelöschten Backups. Wenn Sie beispielsweise 6 Sicherungen mit einer Richtlinie zum Aufbewahren von nur 4 Sicherungen erstellt haben, wird die Anzahl der angezeigten Sicherungen mit 6 angegeben.

Klone einer Sicherung eines versionsflexiblen Spiegels auf einem Volume vom Typ „Mirror-Vault“ werden in der Topologieansicht angezeigt, die Anzahl der Spiegelsicherungen in der Topologieansicht umfasst jedoch nicht die versionsflexible Sicherung.

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

-  Die Replikationssite ist aktiv.
-  Die Replikationssite ist ausgefallen.
-  Die sekundäre Spiegel- oder Tresorbeziehung 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 die Ressourcengruppe aus der Dropdownliste **Anzeigen** aus.
3. Wählen Sie die Ressource entweder aus der Ressourcendetailansicht oder aus der Ressourcengruppendetailansicht aus.

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

4. Überprüfen Sie die Karte „Zusammenfassung“, um eine Übersicht über die Anzahl der auf dem primären und sekundären Speicher verfügbaren Sicherungen und Klone anzuzeigen.

   Im Abschnitt „Zusammenfassungskarte“ wird die Gesamtzahl der Sicherungen und Klone angezeigt.

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

Wenn eine SnapLock -fähige Sicherung durchgeführt wird, wird durch Klicken auf die Schaltfläche **Aktualisieren** die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock aktualisiert. Ein wöchentlicher Zeitplan aktualisiert auch die von ONTAP abgerufene Ablaufzeit des primären und sekundären SnapLock .

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

Bei der aktiven Synchronisierung von SnapMirror wird durch Klicken auf die Schaltfläche **Aktualisieren** das SnapCenter -Sicherungsinventar aktualisiert, indem ONTAP sowohl nach primären als auch nach Replikationsstandorten abgefragt wird. Ein wöchentlicher Zeitplan führt diese Aktivität auch für alle Datenbanken aus, die eine aktive Synchronisierungsbeziehung mit SnapMirror enthalten.

- Für SnapMirror Active Sync und nur für ONTAP 9.14.1 sollten Async Mirror- oder Async MirrorVault-Beziehungen 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 für SnapCenter erstellt werden, um über das Failover informiert zu sein. Sie können erst auf **Aktualisieren** klicken, nachdem eine Sicherung erstellt wurde.

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

   Die Details der Backups und Klone werden in einem Tabellenformat angezeigt.

6. Wählen Sie die Sicherung aus der Tabelle aus und klicken Sie dann auf die Datenschutzsymbole, um Wiederherstellungs-, Klon- und Löschvorgänge durchzuführen.

   Sie können Sicherungen, die sich auf dem sekundären Speicher befinden, weder umbenennen noch 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