Schützen Sie Unix-Dateisysteme

SnapCenter software

NetApp
November 06, 2025

Inhalt

Schützen Sie Unix-Dateisysteme

Was Sie mit dem SnapCenter Plug-in für Unix-Dateisysteme tun können

Wenn das Plug-in für Unix-Dateisysteme in Ihrer Umgebung installiert ist, können Sie SnapCenter zum Sichern, Wiederherstellen und Klonen von Unix-Dateisystemen verwenden. Sie können auch Aufgaben ausführen, die diese Vorgänge unterstützen.

- Ressourcen entdecken
- Sichern Sie Unix-Dateisysteme
- Planen von Sicherungsvorgängen
- Wiederherstellen von Dateisystemsicherungen
- Klonen von Dateisystemsicherungen
- Überwachen von Sicherungs-, Wiederherstellungs- und Klonvorgängen

Unterstützte Konfigurationen

Artikel	Unterstützte Konfiguration
Umgebungen	• Physischer Server • Virtueller Server vVol-Datenspeicher auf NFS und SAN. vVol-Datenspeicher können nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
Dateisysteme	• SAN: ◦ Sowohl LVM- als auch nicht LVM-basierte Dateisysteme ◦ LVM über VMDK ext3, ext4 und xfs • NFS: NFS v3, NFS v4.x
Protokolle	• FC • FCoE • iSCSI • NFS

Artikel	Unterstützte Konfiguration
Mehrwege	Ja

Einschränkungen

- Eine Mischung aus RDMs und virtuellen Datenträgern in einer Datenträgergruppe wird nicht unterstützt.
- Die Wiederherstellung auf Dateiebene wird nicht unterstützt.

  Sie können jedoch eine manuelle Wiederherstellung auf Dateiebene durchführen, indem Sie die Sicherung klonen und die Dateien dann manuell kopieren.

- Eine Mischung aus Dateisystemen, die über VMDKs verteilt sind und sowohl aus NFS- als auch aus VMFS-Datenspeichern stammen, wird nicht unterstützt.
- NVMe wird nicht unterstützt.
- Bereitstellung wird nicht unterstützt.

Features

- Ermöglicht dem Plug-in für Oracle Database, Datenschutzvorgänge auf Oracle-Datenbanken durchzuführen, indem der zugrunde liegende Host-Speicherstapel auf Linux- oder AIX-Systemen verwaltet wird
- Unterstützt Network File System (NFS)- und Storage Area Network (SAN)-Protokolle auf einem Speichersystem, auf dem ONTAP ausgeführt wird.
- Für Linux-Systeme werden Oracle-Datenbanken auf VMDK und RDM-LUNs unterstützt, wenn Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren.
- Unterstützt Mount Guard für AIX auf SAN-Dateisystemen und LVM-Layout.
- Unterstützt Enhanced Journaled File System (JFS2) mit Inline-Protokollierung auf SAN-Dateisystemen und LVM-Layout nur für AIX-Systeme.

  Es werden native SAN-Geräte, Dateisysteme und auf SAN-Geräten erstellte LVM-Layouts unterstützt.

- Automatisiert anwendungsorientierte Sicherungs-, Wiederherstellungs- und Klonvorgänge für UNIX-Dateisysteme in Ihrer SnapCenter -Umgebung

Installieren Sie das SnapCenter Plug-in für Unix-Dateisysteme

Voraussetzungen für das Hinzufügen von Hosts und die Installation des Plug-In-Pakets für Linux

Bevor Sie einen Host hinzufügen und das Plug-In-Paket für Linux installieren, müssen Sie alle Anforderungen erfüllen.

- Wenn Sie iSCSI verwenden, muss der iSCSI-Dienst ausgeführt werden.
- Sie können entweder die passwortbasierte Authentifizierung für den Root- oder Nicht-Root-Benutzer oder die SSH-Schlüssel-basierte Authentifizierung verwenden.

Das SnapCenter Plug-in für Unix-Dateisysteme kann von einem Nicht-Root-Benutzer installiert werden. Sie sollten jedoch die Sudo-Berechtigungen für den Nicht-Root-Benutzer konfigurieren, um den Plug-In-Prozess zu installieren und zu starten. Nach der Installation des Plug-Ins werden die Prozesse effektiv als Nicht-Root-Benutzer ausgeführt.

- Erstellen Sie Anmeldeinformationen mit dem Authentifizierungsmodus „Linux“ für den Installationsbenutzer.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

  Stellen Sie sicher, dass Sie nur die zertifizierte Edition von JAVA 11 auf dem Linux-Host installiert haben.

  Informationen zum Herunterladen von JAVA finden Sie unter: "Java-Downloads für alle Betriebssysteme"

- Sie sollten **bash** als Standard-Shell für die Plug-In-Installation haben.

Linux-Hostanforderungen

Sie sollten sicherstellen, dass der Host die Anforderungen erfüllt, bevor Sie das SnapCenter Plug-Ins-Paket für Linux installieren.

Artikel	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
Mindest-RAM für das SnapCenter -Plug-In auf dem Host	2 GB
Minimaler Installations- und Protokollspeicherplatz für das SnapCenter -Plug-In auf dem Host	2 GB Sie sollten ausreichend Speicherplatz zuweisen und den Speicherverbrauch des Protokollordners überwachen. Der erforderliche Protokollspeicherplatz variiert je nach Anzahl der zu schützenden Entitäten und der Häufigkeit der Datenschutzvorgänge. Wenn nicht genügend Speicherplatz vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Artikel	Anforderungen
Erforderliche Softwarepakete	Java 11 Oracle Java und OpenJDK Stellen Sie sicher, dass Sie nur die zertifizierte Edition von JAVA 11 auf dem Linux-Host installiert haben. Wenn Sie JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die Option JAVA_HOME unter /var/opt/snapcenter/spl/etc/spl.properties auf die richtige JAVA-Version und den richtigen Pfad eingestellt ist.

Die neuesten Informationen zu unterstützten Versionen finden Sie im "NetApp Interoperabilitätsmatrix-Tool" .

Fügen Sie Hosts hinzu und installieren Sie das Plug-In-Paket für Linux über die GUI

Sie können auf der Seite „Host hinzufügen“ Hosts hinzufügen und dann das SnapCenter Plug-In-Paket für Linux installieren. Die Plug-Ins werden automatisch auf den Remote-Hosts installiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Stellen Sie sicher, dass oben die Registerkarte **Verwaltete Hosts** ausgewählt ist.
3. Klicken Sie auf **Hinzufügen**.
4. Führen Sie auf der Seite „Hosts“ die folgenden Aktionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Hosttyp	Wählen Sie **Linux** als Hosttyp.
Hostname	Geben Sie den vollqualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter ist auf die richtige Konfiguration des DNS angewiesen. Daher empfiehlt es sich, den FQDN einzugeben. Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Subdomäne ist, müssen Sie den FQDN angeben.

Für dieses Feld…	Machen Sie Folgendes…
Anmeldeinformationen	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldeinformationen. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Einzelheiten finden Sie in den Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen bewegen. Der Authentifizierungsmodus für Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten „Host hinzufügen“ angeben.

5. Wählen Sie im Abschnitt „Zu installierende Plug-ins auswählen“ die Option **Unix-Dateisysteme** aus.
6. (Optional) Klicken Sie auf **Weitere Optionen**.

Für dieses Feld…	Machen Sie Folgendes…
Hafen	Behalten Sie entweder die Standard-Portnummer bei oder geben Sie die Portnummer an. Die Standard-Portnummer ist 8145. Wenn der SnapCenter -Server auf einem benutzerdefinierten Port installiert wurde, wird diese Portnummer als Standardport angezeigt. Wenn Sie die Plug-Ins manuell installiert und einen benutzerdefinierten Port angegeben haben, müssen Sie denselben Port angeben. Andernfalls schlägt der Vorgang fehl.
Installationspfad	Der Standardpfad ist */opt/ NetApp/snapcenter*. Optional können Sie den Pfad anpassen. Wenn Sie den benutzerdefinierten Pfad verwenden, stellen Sie sicher, dass der Standardinhalt der Sudoers mit dem benutzerdefinierten Pfad aktualisiert wird.

Für dieses Feld…	Machen Sie Folgendes…
Überspringen optionaler Vorinstallationsprüfungen	Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Plug-ins bereits manuell installiert haben und nicht überprüfen möchten, ob der Host die Anforderungen für die Installation des Plug-ins erfüllt.

7. Klicken Sie auf **Senden**.

   Wenn Sie das Kontrollkästchen „Vorabprüfungen überspringen“ nicht aktiviert haben, wird der Host validiert, um zu überprüfen, ob er die Anforderungen für die Installation des Plug-Ins erfüllt.

   Das Vorabprüfungsskript validiert den Firewall-Status des Plug-In-Ports nicht, wenn dieser in den Ablehnungsregeln der Firewall angegeben ist.

   Sollten die Mindestanforderungen nicht erfüllt sein, werden entsprechende Fehler- bzw. Warnmeldungen angezeigt. Wenn der Fehler mit dem Speicherplatz oder RAM zusammenhängt, können Sie die Datei web.config unter *C:\Programme\ NetApp\ SnapCenter WebApp* aktualisieren, um die Standardwerte zu ändern. Wenn der Fehler mit anderen Parametern zusammenhängt, sollten Sie das Problem beheben.

   Wenn Sie in einem HA-Setup die Datei web.config aktualisieren, müssen Sie die Datei auf beiden Knoten aktualisieren.

8. Überprüfen Sie den Fingerabdruck und klicken Sie dann auf **Bestätigen und senden**.

   SnapCenter unterstützt den ECDSA-Algorithmus nicht.

   Die Überprüfung des Fingerabdrucks ist obligatorisch, auch wenn derselbe Host zuvor zu SnapCenter hinzugefügt und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.

   Die installationsspezifischen Protokolldateien befinden sich unter */custom_location/snapcenter/logs*.

Ergebnis

Alle auf dem Host gemounteten Dateisysteme werden automatisch erkannt und auf der Ressourcenseite angezeigt. Wenn nichts angezeigt wird, klicken Sie auf **Ressourcen aktualisieren**.

Überwachen des Installationsstatus

Sie können den Fortschritt der Installation des SnapCenter -Plug-In-Pakets auf der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Installationsfortschritt überprüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs an:

- Im Gange

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Überwachen** auf **Jobs**.
3. Um auf der Seite **Jobs** die Liste so zu filtern, dass nur Plug-In-Installationsvorgänge aufgeführt werden, gehen Sie wie folgt vor:
   a. Klicken Sie auf **Filter**.
   b. Optional: Geben Sie das Start- und Enddatum an.
   c. Wählen Sie im Dropdown-Menü „Typ“ die Option „Plug-in-Installation“ aus.
   d. Wählen Sie im Dropdown-Menü „Status“ den Installationsstatus aus.
   e. Klicken Sie auf **Übernehmen**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite **Auftragsdetails** auf **Protokolle anzeigen**.

Konfigurieren des SnapCenter Plug-in Loader -Dienstes

Der SnapCenter Plug-in Loader -Dienst lädt das Plug-in-Paket für Linux, um mit dem SnapCenter -Server zu interagieren. Der SnapCenter Plug-in Loader -Dienst wird installiert, wenn Sie das SnapCenter Plug-ins-Paket für Linux installieren.

Über diese Aufgabe

Nach der Installation des SnapCenter Plug-ins-Pakets für Linux wird der SnapCenter Plug-in Loader -Dienst automatisch gestartet. Wenn der SnapCenter Plug-in Loader -Dienst nicht automatisch gestartet wird, sollten Sie:

- Stellen Sie sicher, dass das Verzeichnis, in dem das Plug-In ausgeführt wird, nicht gelöscht wird
- Erhöhen Sie den der Java Virtual Machine zugewiesenen Speicherplatz

Die Datei spl.properties, die sich unter */custom_location/ NetApp/snapcenter/spl/etc/* befindet, enthält die folgenden Parameter. Diesen Parametern sind Standardwerte zugewiesen.

Parametername	Beschreibung
LOG_LEVEL	Zeigt die unterstützten Protokollebenen an. Die möglichen Werte sind TRACE, DEBUG, INFO, WARN, ERROR und FATAL.

Parametername	Beschreibung
SPL_PROTOCOL	Zeigt das vom SnapCenter Plug-in Loader unterstützte Protokoll an. Es wird nur das HTTPS-Protokoll unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SNAPCENTER_SERVER_PROTOKOLL	Zeigt das vom SnapCenter Server unterstützte Protokoll an. Es wird nur das HTTPS-Protokoll unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SKIP_JAVAHOME_UPDATE	Standardmäßig erkennt der SPL-Dienst den Java-Pfad und aktualisiert den JAVA_HOME-Parameter. Daher ist der Standardwert auf FALSE gesetzt. Sie können es auf TRUE setzen, wenn Sie das Standardverhalten deaktivieren und den Java-Pfad manuell korrigieren möchten.
SPL_KEYSTORE_PASS	Zeigt das Passwort der Keystore-Datei an. Sie können diesen Wert nur ändern, wenn Sie das Kennwort ändern oder eine neue Keystore-Datei erstellen.
SPL_PORT	Zeigt die Portnummer an, auf der der SnapCenter Plug-in Loader -Dienst ausgeführt wird. Sie können den Wert hinzufügen, wenn der Standardwert fehlt. Sie sollten den Wert nach der Installation der Plug-Ins nicht mehr ändern.
SNAPCENTER_SERVER_HOST	Zeigt die IP-Adresse oder den Hostnamen des SnapCenter -Servers an.
SPL_KEYSTORE_PATH	Zeigt den absoluten Pfad der Keystore-Datei an.
SNAPCENTER_SERVER_PORT	Zeigt die Portnummer an, auf der der SnapCenter -Server ausgeführt wird.

Parametername	Beschreibung
LOGS_MAX_COUNT	Zeigt die Anzahl der Protokolldateien des SnapCenter Plug-in Loader an, die im Ordner */custom_location/snapcenter/spl/logs* gespeichert sind. Der Standardwert ist auf 5000 eingestellt. Wenn die Anzahl größer als der angegebene Wert ist, werden die letzten 5000 geänderten Dateien beibehalten. Die Überprüfung der Anzahl der Dateien erfolgt automatisch alle 24 Stunden ab dem Start des SnapCenter Plug-in Loader -Dienstes. Wenn Sie die Datei „spl.properties“ manuell löschen, wird die Anzahl der beizubehaltenden Dateien auf 9999 festgelegt.
JAVA_HOME	Zeigt den absoluten Verzeichnispfad des JAVA_HOME an, der zum Starten des SPL-Dienstes verwendet wird. Dieser Pfad wird während der Installation und beim Starten von SPL festgelegt.
LOG_MAX_SIZE	Zeigt die maximale Größe der Job-Protokolldatei an. Sobald die maximale Größe erreicht ist, wird die Protokolldatei komprimiert und die Protokolle in die neue Datei dieses Auftrags geschrieben.
Protokolle der letzten Tage aufbewahren	Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.
Zertifikatsvalidierung aktivieren	Zeigt „true“ an, wenn die CA-Zertifikatvalidierung für den Host aktiviert ist. Sie können diesen Parameter entweder durch Bearbeiten der spl.properties oder mithilfe der SnapCenter -GUI oder des Cmdlets aktivieren oder deaktivieren.

Wenn einem dieser Parameter nicht der Standardwert zugewiesen ist oder Sie den Wert zuweisen oder ändern möchten, können Sie die Datei spl.properties ändern. Sie können auch die Datei „spl.properties“ überprüfen und bearbeiten, um alle Probleme im Zusammenhang mit den den Parametern zugewiesenen Werten zu beheben. Nachdem Sie die Datei spl.properties geändert haben, sollten Sie den SnapCenter Plug-in Loader -Dienst neu starten.

Schritte

1. Führen Sie je nach Bedarf eine der folgenden Aktionen aus:
   - Starten Sie den SnapCenter Plug-in Loader -Dienst:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Stoppen Sie den SnapCenter Plug-in Loader -Dienst:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     Sie können die Option -force mit dem Stoppbefehl verwenden, um den SnapCenter Plug-in Loader -Dienst zwangsweise zu stoppen. Allerdings sollten Sie dabei vorsichtig sein, da dadurch auch die bestehenden Vorgänge beendet werden.
   - Starten Sie den SnapCenter Plug-in Loader -Dienst neu:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - Ermitteln Sie den Status des SnapCenter Plug-in Loader Dienstes:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
     - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
   - Suchen Sie die Änderung im SnapCenter Plug-in Loader -Dienst:
     - Führen Sie als Root-Benutzer Folgendes aus: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
     - Führen Sie als Nicht-Root-Benutzer Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

Konfigurieren Sie das CA-Zertifikat mit dem SnapCenter Plug-in Loader (SPL)-Dienst auf dem Linux-Host

Sie sollten das Kennwort des SPL-Schlüsselspeichers und seines Zertifikats verwalten, das CA-Zertifikat konfigurieren, Stamm- oder Zwischenzertifikate für den SPL-Truststore konfigurieren und das von der CA signierte Schlüsselpaar für den SPL-Truststore mit dem SnapCenter Plug-in Loader -Dienst konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

SPL verwendet die Datei „keystore.jks“, die sich unter „/var/opt/snapcenter/spl/etc“ befindet, sowohl als Truststore als auch als Keystore.

Verwalten Sie das Kennwort für den SPL-Schlüsselspeicher und den Alias des verwendeten CA-signierten Schlüsselpaars

Schritte

1. Sie können das Standardkennwort für den SPL-Schlüsselspeicher aus der SPL-Eigenschaftendatei abrufen.

   Dies ist der Wert, der dem Schlüssel „SPL_KEYSTORE_PASS“ entspricht.

2. Ändern Sie das Keystore-Passwort:

```
 keytool -storepasswd -keystore keystore.jks
. Ändern Sie das Kennwort für alle Aliase der privaten Schlüsseleinträge im Schlüsselspeicher in dasselbe Kennwort, das für den Schlüsselspeicher verwendet wird:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

   Aktualisieren Sie dasselbe für den Schlüssel SPL_KEYSTORE_PASS in der Datei spl.properties.

3. Starten Sie den Dienst nach der Änderung des Kennworts neu.

> Das Kennwort für den SPL-Schlüsselspeicher und für alle zugehörigen Aliaskennwörter des privaten Schlüssels müssen identisch sein.

Konfigurieren Sie Stamm- oder Zwischenzertifikate für den SPL-Truststore

Sie sollten die Stamm- oder Zwischenzertifikate ohne den privaten Schlüssel für den SPL-Truststore konfigurieren.

Schritte

1. Navigieren Sie zum Ordner, der den SPL-Schlüsselspeicher enthält: */var/opt/snapcenter/spl/etc*.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
 keytool -list -v -keystore keystore.jks
. Fügen Sie ein Stamm- oder Zwischenzertifikat hinzu:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Starten Sie den Dienst neu, nachdem Sie die Stamm- oder
Zwischenzertifikate für den SPL-Truststore konfiguriert haben.
```

Sie sollten das Stamm-CA-Zertifikat und dann die Zwischen-CA-Zertifikate hinzufügen.

Konfigurieren Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den SPL-Vertrauensspeicher

Sie sollten das von der CA signierte Schlüsselpaar für den SPL-Truststore konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher /var/opt/snapcenter/spl/etc.
2. Suchen Sie die Datei „keystore.jks“.
3. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf:

```
 keytool -list -v -keystore keystore.jks
. Fügen Sie das CA-Zertifikat mit privatem und öffentlichem Schlüssel
hinzu.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Listen Sie die hinzugefügten Zertifikate im Schlüsselspeicher auf.
```

```
 keytool -list -v -keystore keystore.jks
. Überprüfen Sie, ob der Schlüsselspeicher den Alias enthält, der dem
neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher hinzugefügt
wurde.
. Ändern Sie das hinzugefügte private Schlüsselkennwort für das CA-
Zertifikat in das Schlüsselspeicherkennwort.
```

Das Standardkennwort für den SPL-Schlüsselspeicher ist der Wert des Schlüssels SPL_KEYSTORE_PASS in der Datei spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Wenn der Aliasname im CA-Zertifikat lang ist und Leerzeichen oder
Sonderzeichen („*“, „,“) enthält, ändern Sie den Aliasnamen in einen
einfachen Namen:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Konfigurieren Sie den Aliasnamen aus dem Schlüsselspeicher in der
Datei spl.properties.
```

Aktualisieren Sie diesen Wert anhand des Schlüssels SPL_CERTIFICATE_ALIAS.

4. Starten Sie den Dienst neu, nachdem Sie das von der Zertifizierungsstelle signierte Schlüsselpaar für den SPL-Truststore konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für SPL

Sie sollten die CRL für SPL konfigurieren

Über diese Aufgabe

- SPL sucht in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien.
- Das Standardverzeichnis für die CRL-Dateien für SPL ist */var/opt/snapcenter/spl/etc/crl*.

Schritte

1. Sie können das Standardverzeichnis in der Datei spl.properties anhand des Schlüssels SPL_CRL_PATH ändern und aktualisieren.
2. Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen.

   Die eingehenden Zertifikate werden anhand der einzelnen CRLs überprüft.

CA-Zertifikate für Plug-Ins aktivieren

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter -Server und den entsprechenden Plug-In-Hosts bereitstellen. Sie sollten die CA-Zertifikatvalidierung für die Plug-Ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet „*Set-SmCertificateSettings*“ aktivieren oder deaktivieren.
- Den Zertifikatsstatus der Plug-ins können Sie sich mit *Get-SmCertificateSettings* anzeigen lassen.

Informationen zu den mit dem Cmdlet verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von *Get-Help command_name*. Alternativ können Sie auch auf die "Referenzhandbuch für SnapCenter -Software-Cmdlets" .

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Seite „Hosts“ auf **Verwaltete Hosts**.
3. Wählen Sie einzelne oder mehrere Plug-In-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung aktivieren**.

Nach Abschluss

Auf der Registerkarte „Managed Hosts“ wird ein Vorhängeschloss angezeigt und die Farbe des Vorhängeschlosses zeigt den Status der Verbindung zwischen SnapCenter Server und dem Plug-in-Host an.

- * 🔒 * zeigt an, dass das CA-Zertifikat weder aktiviert noch dem Plug-In-Host zugewiesen ist.
- * 🔒 * zeigt an, dass das CA-Zertifikat erfolgreich validiert wurde.

- * * zeigt an, dass das CA-Zertifikat nicht validiert werden konnte.
- * * zeigt an, dass die Verbindungsinformationen nicht abgerufen werden konnten.

Wenn der Status gelb oder grün ist, wurden die Datenschutzvorgänge erfolgreich abgeschlossen.

Installieren Sie das SnapCenter Plug-in for VMware vSphere

Wenn Ihre Datenbank oder Ihr Dateisystem auf virtuellen Maschinen (VMs) gespeichert ist oder Sie VMs und Datenspeicher schützen möchten, müssen Sie das SnapCenter Plug-in for VMware vSphere Appliance bereitstellen.

Informationen zur Bereitstellung finden Sie unter "Bereitstellungsübersicht" .

CA-Zertifikat bereitstellen

Informationen zum Konfigurieren des CA-Zertifikats mit dem SnapCenter Plug-in for VMware vSphere finden Sie unter "SSL-Zertifikat erstellen oder importieren" .

Konfigurieren der CRL-Datei

Das SnapCenter Plug-in for VMware vSphere sucht in einem vorkonfigurierten Verzeichnis nach den CRL-Dateien. Das Standardverzeichnis der CRL-Dateien für das SnapCenter Plug-in for VMware vSphere ist */opt/netapp/config/crl*.

Sie können mehr als eine CRL-Datei in diesem Verzeichnis ablegen. Die eingehenden Zertifikate werden anhand der einzelnen CRLs überprüft.

Bereiten Sie sich auf den Schutz von Unix-Dateisystemen vor

Bevor Sie Datenschutzvorgänge wie Sicherungs-, Klon- oder Wiederherstellungsvorgänge durchführen, sollten Sie Ihre Umgebung einrichten. Sie können den SnapCenter -Server auch für die Verwendung der SnapMirror und SnapVault -Technologie einrichten.

Um die Vorteile der SnapVault und SnapMirror -Technologie nutzen zu können, müssen Sie eine Datenschutzbeziehung zwischen den Quell- und Zielvolumes auf dem Speichergerät konfigurieren und initialisieren. Sie können diese Aufgaben mit NetAppSystem Manager oder über die Befehlszeile der Speicherkonsole ausführen.

Bevor Sie das Plug-in für Unix-Dateisysteme verwenden, sollte der SnapCenter Administrator den SnapCenter -Server installieren und konfigurieren und die erforderlichen Aufgaben ausführen.

- Installieren und konfigurieren Sie SnapCenter Server."Mehr erfahren"
- Konfigurieren Sie die SnapCenter -Umgebung, indem Sie Speichersystemverbindungen hinzufügen."Mehr erfahren"

SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jedes SVM, das bei SnapCenter entweder per SVM-Registrierung oder Cluster-Registrierung registriert wird, muss eindeutig sein.

- Fügen Sie Hosts hinzu, installieren Sie die Plug-Ins und entdecken Sie die Ressourcen.
- Wenn Sie SnapCenter Server zum Schutz von Unix-Dateisystemen verwenden, die sich auf VMware RDM LUNs oder VMDKs befinden, müssen Sie das SnapCenter Plug-in for VMware vSphere bereitstellen und das Plug-in bei SnapCenter registrieren.
- Installieren Sie Java auf Ihrem Linux-Host.
- Konfigurieren Sie SnapMirror und SnapVault auf ONTAP, wenn Sie eine Backup-Replikation wünschen.

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.

Für dieses Feld…	Machen Sie Folgendes…
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

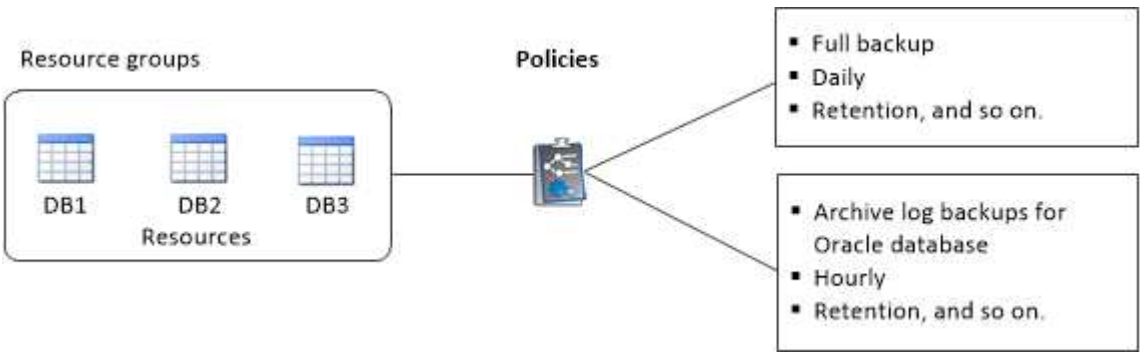
Eine Ressourcengruppe ist ein Container, dem Sie Ressourcen hinzufügen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle mit den Dateisystemen verknüpften Daten sichern.

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 *Richtlinienname* 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

Wiederherstellen und Wiederherstellen von Unix-Dateisystemen

Stellen Sie Unix-Dateisysteme wieder her

Im Falle eines Datenverlusts können Sie SnapCenter verwenden, um Unix-Dateisysteme wiederherzustellen.

Über diese Aufgabe

- Sie sollten die folgenden Befehle ausführen, um die Verbindung mit dem SnapCenter -Server herzustellen, die Sicherungen aufzulisten, ihre Informationen abzurufen und die Sicherung wiederherzustellen.

  Informationen zu den mit dem Befehl verwendbaren Parametern und deren Beschreibungen erhalten Sie durch Ausführen von Get-Help *command_name*. Alternativ können Sie auch auf die "SnapCenter Software-Befehlsreferenzhandbuch" .

- Für den Wiederherstellungsvorgang mit SnapMirror Active Sync müssen Sie die Sicherung vom primären Speicherort auswählen.

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 „Pfad“ oder „Ressourcengruppe“ aus der Liste „Ansicht“ aus.
3. Wählen Sie das Dateisystem entweder aus der Detailansicht oder der Detailansicht der Ressourcengruppe aus.

   Die Topologieseite wird angezeigt.

4. Wählen Sie in der Ansicht „Kopien verwalten“ **Backups** entweder vom primären oder vom sekundären (gespiegelten oder replizierten) Speichersystem aus.
5. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf *  *.
6. Gehen Sie auf der Seite „Wiederherstellungsbereich“ wie folgt vor:
   - Für NFS-Dateisysteme ist standardmäßig die Wiederherstellung mit **Verbinden und Kopieren** ausgewählt. Sie können auch **Volume Revert** oder **Fast Restore** auswählen.
   - Bei Nicht-NFS-Dateisystemen wird der Wiederherstellungsumfang je nach Layout ausgewählt.

     Die nach der Sicherung neu erstellten Dateien sind je nach Dateisystemtyp und -layout nach der Wiederherstellung möglicherweise nicht verfügbar.
7. Geben Sie auf der Seite „PreOps“ Befehle zur Vorwiederherstellung ein, die vor der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.
8. Geben Sie auf der Seite „PostOps“ Post-Restore-Befehle ein, die nach der Durchführung eines Wiederherstellungsauftrags ausgeführt werden sollen.

   Sie sollten überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-In-Host am Speicherort */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config* path verfügbar ist.

9. Wählen Sie auf der Benachrichtigungsseite aus der Dropdownliste **E-Mail-Einstellungen** die Szenarien aus, in denen Sie die E-Mail-Benachrichtigungen 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 durchgeführten Wiederherstellungsvorgang anhängen möchten, müssen Sie **Jobbericht anhängen** auswählen.

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

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

    Wenn der Wiederherstellungsvorgang fehlschlägt, wird ein Rollback nicht unterstützt.

    Bei der Wiederherstellung eines Dateisystems, das sich auf einer Datenträgergruppe befindet, werden die alten Inhalte des Dateisystems nicht gelöscht. Nur der Inhalt des geklonten Dateisystems wird in das Quelldateisystem kopiert. Dies ist anwendbar, wenn sich in der Datenträgergruppe mehrere Dateisysteme befinden und das Standard-NFS-Dateisystem wiederhergestellt wird.

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

Überwachen Sie Wiederherstellungsvorgänge für Unix-Dateisysteme

Sie können den Fortschritt verschiedener SnapCenter -Wiederherstellungsvorgänge mithilfe der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Fortschritt eines Vorgangs überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Zustände nach der Wiederherstellung beschreiben den Zustand der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsaktionen, die Sie durchführen können.

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs 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 Wiederherstellungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdownliste **Typ** die Option **Wiederherstellen** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie den Wiederherstellungsauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite **Auftragsdetails** auf **Protokolle anzeigen**.

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

Klonen Sie Unix-Dateisysteme

Klonen Sie die Sicherung des Unix-Dateisystems

Sie können SnapCenter verwenden, um das Unix-Dateisystem mithilfe der Sicherung des Dateisystems zu klonen.

Bevor Sie beginnen

- Sie können die Aktualisierung der fstab-Datei überspringen, indem Sie den Wert von *SKIP_FSTAB_UPDATE* in der Datei *agent.properties* unter */opt/ NetApp/snapcenter/scc/etc* auf **true** setzen.
- Sie können einen statischen Klon-Volume-Namen und Junction-Pfad haben, indem Sie den Wert von *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* in der Datei *agent.properties* unter */opt/ NetApp/snapcenter/scc/etc* auf **true** setzen. Nach der Aktualisierung der Datei sollten Sie den SnapCenter Plug-in Creator-Dienst neu starten, indem Sie den folgenden Befehl ausführen: `/opt/NetApp/snapcenter/scc/bin/scc restart .`

  Beispiel: Ohne diese Eigenschaft lauten der Name des Klon-Volumes und der Verbindungspfad wie <Source_volume_name>_Clone_<Timestamp>, jetzt jedoch <Source_volume_name>_Clone_<Clone_Name>

  Dadurch bleibt der Name konstant, sodass Sie die fstab-Datei manuell auf dem neuesten Stand halten können, wenn Sie die fstab-Datei nicht lieber durch SnapCenter aktualisieren möchten.

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 „Pfad“ oder „Ressourcengruppe“ aus der Liste „Ansicht“ aus.
3. Wählen Sie das Dateisystem entweder aus der Detailansicht oder der Detailansicht der Ressourcengruppe aus.

   Die Topologieseite wird angezeigt.
4. Wählen Sie in der Ansicht „Kopien verwalten“ die Sicherungen entweder aus „Lokale Kopien“ (primär), „Spiegelkopien“ (sekundär) oder „Tresorkopien“ (sekundär) aus.
5. Wählen Sie das Backup aus der Tabelle aus und klicken Sie dann auf *  *.
6. Führen Sie auf der Seite „Standort“ die folgenden Aktionen aus:

Für dieses Feld…	Machen Sie Folgendes…
Server klonen	Standardmäßig ist der Quellhost ausgefüllt.
Einhängepunkt klonen	Geben Sie den Pfad an, in dem das Dateisystem gemountet wird.

7. Führen Sie auf der Seite „Skripts“ die folgenden Schritte aus:
   a. Geben Sie die Befehle für „Pre-Clone“ oder „Post-Clone“ ein, die vor bzw. nach dem Klonvorgang ausgeführt werden sollen.

   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.
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 durchgeführten Klonvorgang 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**.
10. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

Einen Klon teilen

Sie können SnapCenter verwenden, um eine geklonte Ressource von der übergeordneten Ressource zu trennen. Der geteilte Klon wird unabhängig von der übergeordneten Ressource.

Informationen zu diesem Vorgang

- Sie können den Klon-Split-Vorgang nicht auf einem Zwischenklon durchführen.

  Nachdem Sie beispielsweise Klon1 aus einer Datenbanksicherung erstellt haben, können Sie eine Sicherung von Klon1 erstellen und diese Sicherung dann klonen (Klon2). Nachdem Sie Klon2 erstellt haben, ist Klon1 ein Zwischenklon und Sie können den Klonaufteilungsvorgang nicht auf Klon1 durchführen. Sie können den Klon-Split-Vorgang jedoch auf Klon2 durchführen.

  Nachdem Sie Klon2 geteilt haben, können Sie den Klon-Teilungsvorgang für Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Sicherungskopien und Klonaufträge des Klons gelöscht.
- Informationen zu FlexClone -Volume-Split-Vorgängen finden Sie unter "Teilen Sie ein FlexClone -Volume von seinem übergeordneten Volume" .
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Speichersystem online ist.

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** die entsprechende Option aus der Liste „Anzeigen“ aus:

Option	Beschreibung
Für Datenbankanwendungen	Wählen Sie **Datenbank** aus der Ansichtsliste.
Für Dateisysteme	Wählen Sie **Pfad** aus der Ansichtsliste.

3. Wählen Sie die entsprechende Ressource aus der Liste aus.

   Die Seite „Ressourcentopologie“ wird angezeigt.

4. Wählen Sie in der Ansicht **Kopien verwalten** die geklonte Ressource (z. B. die Datenbank oder LUN) aus und klicken Sie dann auf *  *.

5. Überprüfen Sie die geschätzte Größe des aufzuteilenden Klons und den erforderlichen verfügbaren Speicherplatz auf dem Aggregat und klicken Sie dann auf **Start**.
6. Überwachen Sie den Vorgangsfortschritt, indem Sie auf **Überwachen** > **Jobs** klicken.

   Der Klon-Split-Vorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird. Sie sollten das Cmdlet „Stop-SmJob“ ausführen, um den Klon-Split-Vorgang zu stoppen, und ihn dann erneut versuchen.

   Wenn Sie eine längere oder kürzere Abfragezeit wünschen, um zu überprüfen, ob der Klon aufgeteilt ist oder nicht, können Sie den Wert des Parameters *CloneSplitStatusCheckPollTime* in der Datei *SMCoreServiceHost.exe.config* ändern, um das Zeitintervall festzulegen, in dem SMCore den Status des Klonaufteilungsvorgangs abfragt. Der Wert wird in Millisekunden angegeben und der Standardwert beträgt 5 Minuten.

   Beispiel:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   Der Startvorgang für die Klonaufteilung schlägt fehl, wenn eine Sicherung, Wiederherstellung oder eine andere Klonaufteilung ausgeführt wird. Sie sollten den Klon-Split-Vorgang erst neu starten, nachdem die laufenden Vorgänge abgeschlossen sind.

Ähnliche Informationen

"SnapCenter -Klon oder -Verifizierung schlägt fehl, da Aggregat nicht vorhanden ist"

Überwachen Sie Klonvorgänge für Unix-Dateisysteme

Sie können den Fortschritt der SnapCenter -Klonvorgänge auf der Seite „Jobs“ überwachen. Möglicherweise möchten Sie den Fortschritt eines Vorgangs überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Informationen zu diesem Vorgang

Die folgenden Symbole werden auf der Seite „Jobs“ angezeigt und geben den Status des Vorgangs 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 Klonvorgänge aufgelistet werden.
b. Geben Sie das Start- und Enddatum an.
c. Wählen Sie aus der Dropdownliste **Typ** die Option **Klon** aus.
d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
e. Klicken Sie auf **Übernehmen**, um die erfolgreich abgeschlossenen Vorgänge anzuzeigen.

4. Wählen Sie den Klonauftrag aus und klicken Sie dann auf **Details**, um die Auftragsdetails anzuzeigen.
5. Klicken Sie auf der Seite „Auftragsdetails“ auf **Protokolle anzeigen**.