Schützen Sie Unix-Dateisysteme

SnapCenter software

NetApp
January 09, 2026

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 mit SnapCenter Unix-Dateisysteme sichern, wiederherstellen und klonen. Sie können auch Aufgaben zur Unterstützung dieser Operationen ausführen.

- Und entdecken Sie Ressourcen
- Sichern Sie Unix-Dateisysteme
- Planen von Backup-Vorgängen
- Wiederherstellung von Dateisystemsicherungen
- Backups von Dateisystemen klonen
- Monitoring von Backup-, Restore- und Klonvorgängen

Unterstützte Konfigurationen

Element	Unterstützte Konfiguration
Umgebungen Beschrieben Sind	• Physischer Server • Virtueller Server VVol Datastores auf NFS und SAN. VVol Datastore kann nur mit ONTAP Tools für VMware vSphere bereitgestellt werden.
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
File-Systeme	• 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

Element	Unterstützte Konfiguration
Multipath	ja

Einschränkungen

- Die Kombination aus RDMs und virtuellen Laufwerken in einer Volume-Gruppe wird nicht unterstützt.
- Wiederherstellung auf Dateiebene wird nicht unterstützt.

  Sie können jedoch manuell Wiederherstellungen auf Dateiebene durchführen, indem Sie das Backup klonen und die Dateien dann manuell kopieren.

- Kombination aus auf VMDKs verteilten Filesystemen, die sowohl von NFS- als auch von VMFS-Datastore stammen, wird nicht unterstützt.
- NVMe wird nicht unterstützt.
- Bereitstellung wird nicht unterstützt.

Funktionen

- Ermöglicht das Plug-in für Oracle Database die Durchführung von Datensicherungsvorgängen auf Oracle Datenbanken, indem es den zugrunde liegenden Host Storage Stack auf Linux oder AIX Systemen unterstützt
- Unterstützt NFS-Protokolle (Network File System) und SAN (Storage Area Network) auf einem Storage-System, auf dem ONTAP ausgeführt wird
- Bei Linux Systemen werden Oracle-Datenbanken auf VMDK und RDM-LUNs unterstützt, wenn Sie das SnapCenter Plug-in für VMware vSphere implementieren und das Plug-in mit 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 LVM-Layouts unterstützt, die auf SAN-Geräten basieren.

- Automatisierung von applikationsorientierten Backup-, Restore- und Klonvorgängen für UNIX File-Systeme in der SnapCenter-Umgebung

Installieren Sie das SnapCenter-Plug-in für Unix-Dateisysteme

Voraussetzungen für das Hinzufügen von Hosts und das Installieren von Plug-ins Package 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-Schlüsselauthentifizierung verwenden.

Das SnapCenter-Plug-in für Unix-Dateisysteme kann von einem Benutzer installiert werden, der kein Root-Benutzer ist. 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 als effektiver nicht-Root-Benutzer ausgeführt.

- Anmeldedaten mit Authentifizierungsmodus als Linux für den Installationsbenutzer erstellen.
- Sie müssen Java 11 auf Ihrem Linux-Host installiert haben.

  Stellen Sie sicher, dass Sie nur die zertifizierte Version 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 Host-Anforderungen

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

Element	Anforderungen
Betriebssysteme	• Red Hat Enterprise Linux • Oracle Linux • SUSE Linux Enterprise Server (SLES)
MindestRAM für das SnapCenter Plug-in auf dem Host	2 GB
Minimale Installation und Protokollierung von Speicherplatz für das SnapCenter Plug-in auf dem Host	2 GB Sie sollten genügend Festplattenspeicher zuweisen und den Speicherverbrauch durch den Protokollordner überwachen. Der erforderliche Protokollspeicherplatz ist abhängig von der Anzahl der zu sichernden Einheiten und der Häufigkeit von Datensicherungsvorgängen. Wenn kein ausreichender Festplattenspeicher vorhanden ist, werden die Protokolle für die kürzlich ausgeführten Vorgänge nicht erstellt.

Element	Anforderungen
Erforderliche Softwarepakete	Java 11 Oracle Java und OpenJDK Stellen Sie sicher, dass Sie nur die zertifizierte Version VON JAVA 11 auf dem Linux-Host installiert haben. Wenn SIE JAVA auf die neueste Version aktualisiert haben, müssen Sie sicherstellen, dass die JAVA_HOME-Option 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 Interoperabilitäts-Matrix-Tool" .

Fügen Sie Hosts hinzu und installieren Sie Plug-ins Package for Linux mithilfe der GUI

Sie können die Seite Host hinzufügen verwenden, um Hosts hinzuzufügen und anschließend das SnapCenter-Plug-ins-Paket für Linux zu installieren. Die Plug-ins werden automatisch auf den Remote-Hosts installiert.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Überprüfen Sie, ob die Registerkarte **verwaltete Hosts** oben ausgewählt ist.
3. Klicken Sie Auf **Hinzufügen**.
4. Führen Sie auf der Seite Hosts die folgenden Aktionen durch:

Für dieses Feld…	Tun Sie das…
Host-Typ	Wählen Sie **Linux** als Hosttyp aus.
Host-Name	Geben Sie den vollständig qualifizierten Domänennamen (FQDN) oder die IP-Adresse des Hosts ein. SnapCenter hängt von der richtigen Konfiguration des DNS ab. Daher empfiehlt es sich, den FQDN einzugeben. Wenn Sie einen Host mithilfe von SnapCenter hinzufügen und der Host Teil einer Unterdomäne ist, müssen Sie den FQDN angeben.

Für dieses Feld…	Tun Sie das…
Anmeldedaten	Wählen Sie entweder den von Ihnen erstellten Anmeldeinformationsnamen aus oder erstellen Sie neue Anmeldedaten. Die Anmeldeinformationen müssen über Administratorrechte auf dem Remote-Host verfügen. Weitere Informationen finden Sie unter Informationen zum Erstellen von Anmeldeinformationen. Sie können Details zu den Anmeldeinformationen anzeigen, indem Sie den Cursor über den von Ihnen angegebenen Anmeldeinformationsnamen positionieren. Der Authentifizierungsmodus für die Anmeldeinformationen wird durch den Hosttyp bestimmt, den Sie im Assistenten zum Hinzufügen von Hosts angeben.

5. Wählen Sie im Abschnitt zu installierende Plug-ins auswählen **Unix-Dateisysteme** aus.
6. (Optional) Klicken Sie Auf **Weitere Optionen**.

Für dieses Feld…	Tun Sie das…
Port	Behalten Sie die Standard-Port-Nummer bei oder geben Sie die Port-Nummer an. Die Standardanschlussnummer 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…	Tun Sie das…
Überspringen Sie optionale Prüfungen vor der Installation	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 **Absenden**.

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

   Das Precheck-Skript überprüft den Firewall-Status des Plug-in-Ports nicht, wenn er in den Regeln für die Ablehnung der Firewall angegeben ist.

   Wenn die Mindestanforderungen nicht erfüllt werden, werden entsprechende Fehler- oder Warnmeldungen angezeigt. Wenn der Fehler mit dem Festplattenspeicher oder RAM zusammenhängt, können Sie die Datei Web.config unter *C:\Program Files\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 keinen ECDSA-Algorithmus.

   Eine Fingerabdruck-Verifizierung ist erforderlich, auch wenn zuvor derselbe Host zu SnapCenter hinzugefügt wurde und der Fingerabdruck bestätigt wurde.

9. Überwachen Sie den Installationsfortschritt.

   Die installationsspezifischen Log-Dateien befinden sich unter */Custom_Location/snapcenter/logs*.

Ergebnis

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

Überwachung des Installationsstatus

Sie können den Fortschritt der Installation des SnapCenter-Plug-in-Pakets über die Seite Jobs überwachen. Möglicherweise möchten Sie den Installationsfortschritt prüfen, um festzustellen, wann die Installation abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

- In Bearbeitung

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Um die Liste auf der Seite **Jobs** so zu filtern, dass nur Plug-in-Installationsvorgänge aufgelistet 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**.
   d. Wählen Sie im Dropdown-Menü Status den Installationsstatus aus.
   e. Klicken Sie Auf **Anwenden**.
4. Wählen Sie den Installationsauftrag aus und klicken Sie auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

Konfigurieren Sie den SnapCenter-Plug-in-Loader-Dienst

Der SnapCenter-Plug-in-Loader-Dienst lädt das Plug-in-Paket, damit Linux mit dem SnapCenter-Server interagieren kann. 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 Folgendes tun:

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

Die Datei spl.properties befindet sich unter */Custom_Location/NetApp/snapcenter/spl/etc/* und enthält die folgenden Parameter: Diesen Parametern werden Standardwerte zugewiesen.

Parametername	Beschreibung
PROTOKOLL_LEVEL	Zeigt die unterstützten Protokollebenen an. Mögliche Werte sind TRACE, DEBUG, INFO, WARN, FEHLER, Und TÖDLICH.

Parametername	Beschreibung
SPL_PROTOKOLL	Zeigt das von SnapCenter Plug-in Loader unterstützte Protokoll an. Nur das HTTPS-Protokoll wird unterstützt. Sie können den Wert hinzufügen, wenn der Standardwert fehlt.
SNAPCENTER_SERVER_PROTOCOL	Zeigt das von SnapCenter-Server unterstützte Protokoll an. Nur das HTTPS-Protokoll wird 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 auf „TRUE“ setzen, wenn Sie das Standardverhalten deaktivieren und den java-Pfad manuell korrigieren möchten.
SPL_KEYSTORE_PASS	Zeigt das Kennwort der Schlüsselspeicherdatei an. Sie können diesen Wert nur ändern, wenn Sie das Passwort ändern oder eine neue Schlüsselspeicherdatei erstellen.
SPL_PORT	Zeigt die Portnummer an, auf der der SnapCenter-Plug-in-Loader ausgeführt wird. Sie können den Wert hinzufügen, wenn der Standardwert fehlt. Nach der Installation der Plug-ins sollten Sie den Wert nicht ändern.
SNAPCENTER_SERVER_HOST	Zeigt die IP-Adresse oder den Hostnamen des SnapCenter-Servers an.
SPL_KEYSTORE_PATH	Zeigt den absoluten Pfad der Schlüsselspeicherdatei an.
SNAPCENTER_SERVER_PORT	Zeigt die Portnummer an, auf der der SnapCenter-Server ausgeführt wird.

Parametername	Beschreibung
„LOGS_MAX_COUNT“	Zeigt die Anzahl der SnapCenter-Plug-in-Loader-Protokolldateien an, die im Ordner */Custom_location/snapcenter/spl/logs* aufbewahrt werden. Der Standardwert ist 5000. Wenn der Zähler größer als der angegebene Wert ist, werden die letzten 5000 geänderten Dateien beibehalten. Die Prüfung auf die 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 zu behaltenden 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 im Rahmen des Startens von SPL festgelegt.
LOG_MAX_SIZE	Zeigt die maximale Größe der Job-Log-Datei an. Sobald die maximale Größe erreicht ist, wird die Protokolldatei gezippt und die Protokolle werden in die neue Datei dieses Jobs geschrieben.
BEIBEHALTEN_LOGS_OF_LAST_DAYS	Zeigt die Anzahl der Tage an, bis zu denen die Protokolle aufbewahrt werden.
ENABLE_CERTIFICATE_VALIDATION	Zeigt true an, wenn die Zertifikatvalidierung für den Host aktiviert ist. Sie können diesen Parameter entweder aktivieren oder deaktivieren, indem Sie den spl.properties bearbeiten oder den SnapCenter GUI oder Cmdlet verwenden.

Wenn einer dieser Parameter dem Standardwert nicht 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 die Datei bearbeiten, um Probleme zu beheben, die mit den Werten, die den Parametern zugeordnet sind, zusammenhängen. Nachdem Sie die Datei spl.properties geändert haben, sollten Sie den SnapCenter-Plug-in-Loader-Dienst neu starten.

Schritte

1. Führen Sie bei 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 Benutzer ohne Root 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 Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     Sie können die Option -Force mit dem Befehl STOP verwenden, um den SnapCenter Plug-in Loader Dienst nachdrücklich zu stoppen. Vor diesem Verfahren sollten Sie jedoch Vorsicht walten lassen, da 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 Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - Suchen 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 Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
   - Finden 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 Benutzer ohne Root Folgendes aus: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

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

Sie sollten das Passwort von SPL Keystore und dessen Zertifikat verwalten, das CA-Zertifikat konfigurieren, Root- oder Zwischenzertifikate für SPL Trust-Store konfigurieren und das CA-signierte Schlüsselpaar für SPL Trust-Store mit dem SnapCenter Plug-in Loader Service konfigurieren, um das installierte digitale Zertifikat zu aktivieren.

SPL verwendet die Datei 'keystore.jks', die sich bei ‘/var/opt/snapcenter/spl/etc’ sowohl als Vertrauensspeicher als auch als Schlüsselspeicher befindet.

Passwort für SPL-Schlüsselspeicher und Alias des verwendeten CA-signierten Schlüsselpaares verwalten

Schritte

1. Sie können SPL Schlüsselspeicher Standardpasswort aus SPL Eigenschaftsdatei abrufen.

   Dieser Wert entspricht dem Schlüssel 'SPL_KEYSTORE_PASS'.

2. Ändern Sie das Schlüsselspeicher-Passwort:

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

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

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

3. Starten Sie den Dienst neu, nachdem Sie das Passwort geändert haben.

> Passwort für SPL-Schlüsselspeicher und für alle zugeordneten Alias-Passwort des privaten Schlüssels sollte gleich sein.

Konfigurieren Sie Root- oder Zwischenzertifikate in SPL Trust-Store

Sie sollten die Stammzertifikate oder Zwischenzertifikate ohne privaten Schlüssel in den SPL Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zum Ordner mit dem SPL-Schlüsselspeicher: */var/opt/snapcenter/spl/etc*.
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

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

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

Sie sollten das Root-CA-Zertifikat und anschließend die Zwischenzertifizierungszertifikate hinzufügen.

Konfigurieren Sie das CA-signierte Schlüsselpaar für SPL Trust-Store

Sie sollten das CA-signierte Schlüsselpaar für den SPL Trust-Store konfigurieren.

Schritte

1. Navigieren Sie zu dem Ordner, der den SPL-Schlüsselspeicher /var/opt/snapcenter/spl/etc. Enthält
2. Suchen Sie die Datei 'keystore.jks'.
3. Liste der hinzugefügten Zertifikate im Schlüsselspeicher:

```
 keytool -list -v -keystore keystore.jks
. Fügen Sie das CA-Zertifikat mit einem privaten und einem öffentlichen
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
. Vergewissern Sie sich, dass der Schlüsselspeicher den Alias enthält,
der dem neuen CA-Zertifikat entspricht, das dem Schlüsselspeicher
hinzugefügt wurde.
. Ändern Sie das hinzugefügte Passwort für den privaten Schlüssel für
das CA-Zertifikat in das Schlüsselspeicher-Passwort.
```

Das Standard-SPL-Schlüsselspeicherkennwort ist der Wert des Schlüssels SPL_KEYSTORE_PASS in der Datei spl.properties.

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

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

Diesen Wert mit dem Schlüssel SPL_CERTIFICATE_ALIAS aktualisieren.

4. Starten Sie den Dienst neu, nachdem Sie das CA-signierte Schlüsselpaar auf SPL Trust-Store konfiguriert haben.

Konfigurieren der Zertifikatsperrliste (CRL) für SPL

Sie sollten die CRL für SPL konfigurieren

Über diese Aufgabe

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

Schritte

1. Sie können das Standardverzeichnis in der Datei spl.properties mit dem Schlüssel SPL_CRL_PATH ändern und aktualisieren.
2. Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren.

   Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Aktivieren Sie CA-Zertifikate für Plug-ins

Sie sollten die CA-Zertifikate konfigurieren und die CA-Zertifikate im SnapCenter-Server und den entsprechenden Plug-in-Hosts bereitstellen. Sie sollten die CA-Zertifikatsvalidierung für die Plug-ins aktivieren.

Bevor Sie beginnen

- Sie können die CA-Zertifikate mit dem Cmdlet "Run_set-SmCertificateSettings_" aktivieren oder deaktivieren.
- Sie können den Zertifikatsstatus für die Plug-ins mithilfe der *get-SmCertificateSettings* anzeigen.

Die Informationen zu den Parametern, die mit dem Cmdlet und deren Beschreibungen verwendet werden können, können durch Ausführen von *get-Help Command_Name* abgerufen werden. Alternativ können Sie auch auf die "SnapCenter Software Cmdlet Referenzhandbuch".

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Hosts**.
2. Klicken Sie auf der Host-Seite auf **verwaltete Hosts**.
3. Wählen Sie ein- oder mehrere Plug-in-Hosts aus.
4. Klicken Sie auf **Weitere Optionen**.
5. Wählen Sie **Zertifikatvalidierung Aktivieren**.

Nachdem Sie fertig sind

Auf dem Reiter Managed Hosts wird ein Schloss 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 lautet, werden die Datensicherungsvorgänge erfolgreich abgeschlossen.

Installieren Sie das SnapCenter Plug-in für VMware vSphere

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

Informationen zur Bereitstellung finden Sie unter "Implementierungsübersicht".

Bereitstellen eines CA-Zertifikats

Informationen zur Konfiguration des CA-Zertifikats mit dem SnapCenter-Plug-in für VMware vSphere finden Sie unter "Erstellen oder importieren Sie ein SSL-Zertifikat".

Konfigurieren Sie die CRL-Datei

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

Sie können mehrere CRL-Dateien in diesem Verzeichnis platzieren. Die eingehenden Zertifikate werden gegen jede CRL überprüft.

Bereiten Sie sich auf den Schutz von Unix-Dateisystemen vor

Bevor Sie Datensicherungsvorgänge wie z. B. Backup-, Klon- oder Restore-Vorgänge durchführen, sollten Sie Ihre Umgebung einrichten. Sie können den SnapCenter Server auch zur Verwendung von SnapMirror und SnapVault Technologie einrichten.

Um von der SnapVault und SnapMirror Technologie zu profitieren, müssen Sie eine Datensicherungsbeziehung zwischen den Quell- und Ziel-Volumes auf dem Storage-Gerät konfigurieren und initialisieren. Sie können entweder NetApp System Manager verwenden oder die Storage-Konsole verwenden, um diese Aufgaben auszuführen.

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

- Installation und Konfiguration von SnapCenter Server "Weitere Informationen ."
- Konfigurieren Sie die SnapCenter Umgebung durch Hinzufügen von Storage-Systemverbindungen. "Weitere Informationen ."

SnapCenter unterstützt nicht mehrere SVMs mit demselben Namen auf verschiedenen Clustern. Jede für SnapCenter registrierte SVM, die eine SVM-Registrierung oder eine Cluster-Registrierung verwendet, muss eindeutig sein.

- Fügen Sie Hosts hinzu, installieren Sie die Plug-ins und ermitteln 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 für VMware vSphere implementieren und das Plug-in bei SnapCenter registrieren.
- Installieren Sie Java auf Ihrem Linux-Host.
- Konfigurieren Sie SnapMirror und SnapVault auf ONTAP, wenn Sie Backup-Replizierung möchten.

Sichern Sie Unix-Dateisysteme

Ermitteln Sie die für Backups verfügbaren UNIX-Dateisysteme

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

Bevor Sie beginnen

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

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

Schritte

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

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

Erstellen Sie Backup-Richtlinien für Unix-Dateisysteme

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

wiederverwenden möchten.

Bevor Sie beginnen

- Sie müssen sich auf die Datensicherung vorbereitet haben, indem Sie Aufgaben wie das Installieren von SnapCenter, das Hinzufügen von Hosts, das Erkennen der Dateisysteme und das Erstellen von Storage-System-Verbindungen durchführen.
- Wenn Sie Snapshots auf einen sekundären gespiegelten oder Vault-Storage replizieren, muss Ihnen der SnapCenter Administrator die SVMs sowohl für die Quell- als auch für die Ziel-Volumes zugewiesen haben.
- Prüfen Sie die spezifischen Voraussetzungen und Einschränkungen von SnapMirror Active Sync. Weitere Informationen finden Sie unter "Objektgrenzen für die aktive SnapMirror Synchronisierung".

Über diese Aufgabe

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

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

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

Schritte

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

   a. Geben Sie die Backup-Einstellungen an.

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

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

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapMirror nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie dieses Feld aus, um Spiegelkopien der Backup-Sätze auf einem anderen Volume zu erstellen (SnapMirror Replikation). Diese Option sollte für SnapMirror Active Sync aktiviert sein.

Für dieses Feld…	Tun Sie das…
Aktualisieren Sie SnapVault nach dem Erstellen einer lokalen Snapshot Kopie	Wählen Sie diese Option aus, um Disk-to-Disk-Backup-Replikation (SnapVault-Backups) durchzuführen.
Fehler bei Wiederholungszählung	Geben Sie die maximale Anzahl von Replikationsversuchen ein, die zulässig sind, bevor der Vorgang beendet wird.

7. Geben Sie auf der Seite Aufbewahrung die Aufbewahrungseinstellungen für den Sicherungstyp und den auf der Seite Sicherung und Replikation ausgewählten Zeitplantyp an:

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

Sperrzeitraum für Snapshot-Kopien	Wählen Sie **Sperrzeitraum für Snapshot-Kopien** und geben Sie die Dauer in Tagen, Monaten oder Jahren an. Die SnapLock-Aufbewahrungsfrist sollte weniger als 100 Jahre betragen.

8. Wählen Sie die Bezeichnung der Richtlinie aus.

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

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

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

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

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

Erstellen von Ressourcengruppen und Anhängen von Richtlinien für Unix-Dateisysteme

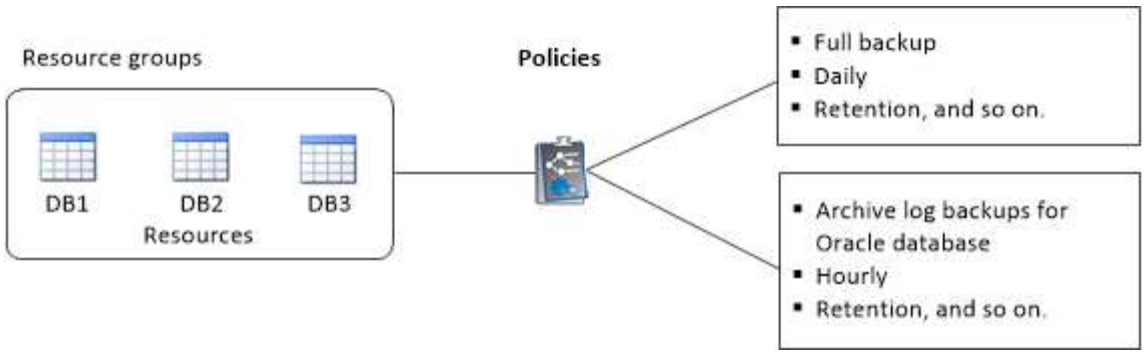
Eine Ressourcengruppe ist ein Container, in dem Sie Ressourcen hinzufügen, die Sie sichern und schützen möchten. Mit einer Ressourcengruppe können Sie alle Daten sichern, die mit den Dateisystemen verknüpft sind.

Über diese Aufgabe

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

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

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



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

Schritte

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

      Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

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

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

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

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

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

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

5. Wählen Sie im Abschnitt Verfügbare Ressourcen die Ressourcen aus, und verschieben Sie sie in den Abschnitt Ausgewählte Ressourcen.

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

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

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

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

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

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

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

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

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

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

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

      Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

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

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

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

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

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

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

Bevor Sie beginnen

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

Über diese Aufgabe

- Der sekundäre Schutz ist nur verfügbar, wenn der angemeldete Benutzer der Rolle zugewiesen ist, die die Funktion **SecondaryProtection** aktiviert hat.
- Wenn Sie den sekundären Schutz aktiviert haben, wird die Ressourcengruppe beim Erstellen der primären und sekundären Konsistenzgruppen in den Wartungsmodus versetzt. Nach dem Erstellen der primären und sekundären Konsistenzgruppen wird die Ressourcengruppe aus dem Wartungsmodus versetzt.
- SnapCenter unterstützt keinen sekundären Schutz für eine Klonressource.

Schritte

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

      Der Name der Ressourcengruppe darf 250 Zeichen nicht überschreiten.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.

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

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

   a. Wählen Sie den Typ der Replikationsrichtlinie aus.

   Die Richtlinie für die synchrone Replizierung wird nicht unterstützt.

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

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

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

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

1. Führen Sie auf der Seite Überprüfung die folgenden Schritte aus:
   a. Klicken Sie auf **Lokatoren laden**, um die SnapMirror oder SnapVault Volumes zu laden, um eine Überprüfung auf dem sekundären Speicher durchzuführen.
   b. Klicken Sie Auf  In der Spalte Configure Schedules (Zeitpläne konfigurieren), um den Überprüfungsplan für alle Zeitplantypen der Richtlinie zu konfigurieren.
   c. Führen Sie im Dialogfeld Add Verification Schedules Policy_Name die folgenden Aktionen durch:

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

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

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

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

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

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

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

Sichern Sie Unix-Dateisysteme

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

Schritte

1. Wählen Sie im linken Navigationsbereich **Ressourcen** und das entsprechende Plug-in aus der Liste aus.
2. Wählen Sie auf der Seite Ressourcen in der Liste Ansicht die Option **Pfad** aus.
3. Klicken Sie auf  , und wählen Sie dann den Hostnamen und die Unix-Dateisysteme aus, um die Ressourcen zu filtern.

4. Wählen Sie das Dateisystem aus, das Sie sichern möchten.
5. Auf der Seite „Ressourcen“ können Sie die folgenden Schritte ausführen:
   a. Aktivieren Sie das Kontrollkästchen, und geben Sie ein benutzerdefiniertes Namensformat ein, das für den Snapshot-Namen verwendet werden soll.

      Beispiel: `customtext_policy_hostname` Oder `resource_hostname`. Standardmäßig wird ein Zeitstempel an den Snapshot Namen angehängt.
6. Führen Sie auf der Seite Anwendungseinstellungen die folgenden Schritte aus:
   - Wählen Sie den Pfeil für Skripte aus und geben Sie die Befehle vor und nach für Stilllegung, Snapshots und Stilllegung ein. Sie können auch die vor dem Beenden auszuführenden Vorbefehle im Falle eines Fehlers eingeben.
   - Wählen Sie eine der Backup-Konsistenzoptionen aus:
     - Wählen Sie **File System consistent** aus, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden und keine Vorgänge auf dem Dateisystem während der Erstellung der Sicherung ausgeführt werden.
     - Wählen Sie **Crash-konsistent**, wenn Sie sicherstellen möchten, dass die zwischengespeicherten Daten der Dateisysteme vor der Erstellung der Sicherung gelöscht werden.
7. Führen Sie auf der Seite Richtlinien die folgenden Schritte aus:
   a. Wählen Sie eine oder mehrere Richtlinien aus der Dropdown-Liste aus.

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

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

   b. Klicken Sie Auf + In der Spalte Configure Schedules (Zeitpläne konfigurieren) können Sie einen Zeitplan für die gewünschte Richtlinie konfigurieren.
   c. Konfigurieren Sie im Fenster Add Schedules for Policy *Policy_Name* den Zeitplan, und wählen Sie dann aus `OK`.

      Policy_Name ist der Name der von Ihnen ausgewählten Richtlinie.

   Die konfigurierten Zeitpläne sind in der Spalte angewendete Zeitpläne aufgeführt.
8. Wählen Sie auf der Benachrichtigungsseite aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mails senden möchten.

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

   Für E-Mail-Benachrichtigungen müssen Sie die SMTP-Serverdetails entweder über die GUI oder über den PowerShell-Befehl angegeben haben `Set-SmSmtpServer`.
9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.

Die Topologieseite wird angezeigt.

10. Klicken Sie auf **Jetzt sichern**.
11. Führen Sie auf der Seite Backup die folgenden Schritte aus:
    a. Wenn Sie mehrere Richtlinien auf die Ressource angewendet haben, wählen Sie aus der Dropdown-Liste Richtlinie die Richtlinie aus, die Sie für das Backup verwenden möchten.

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

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

Erstellen Sie ein Backup von Ressourcengruppen für Unix-Dateisysteme

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

Schritte

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

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

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

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

Überwachen Sie das Backup von Unix-Dateisystemen

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

Überwachen Sie die Backup-Vorgänge für Unix-Dateisysteme

Sie können den Fortschritt verschiedener Backup-Vorgänge über die Seite SnapCenterJobs überwachen. Sie

können den Fortschritt überprüfen, um festzustellen, wann er abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

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

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite Überwachen auf **Jobs**.
3. Führen Sie auf der Seite Jobs die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Backup-Vorgänge aufgeführt werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Backup** aus.
   d. Wählen Sie im Dropdown-Menü **Status** den Sicherungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die abgeschlossenen Vorgänge anzuzeigen.
4. Wählen Sie einen Sicherungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.

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

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

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

Überwachen Sie Datensicherungsvorgänge im Teilfenster „Vorgang“

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

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

Schritte

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

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

Zeigen Sie geschützte Unix-Dateisysteme auf der Seite Topologie an

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

Über diese Aufgabe

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

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

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

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

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

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

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

Schritte

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Beispiel für Backups und Klone auf dem Primärspeicher

Stellen Sie Unix-Dateisysteme wieder her

Stellen Sie Unix-Dateisysteme wieder her

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

Über diese Aufgabe

- Sie sollten die folgenden Befehle ausführen, um die Verbindung zum SnapCenter-Server herzustellen, die Backups aufzulisten, seine 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 Command Reference Guide" .

- Für die Wiederherstellung der aktiven Synchronisierung von SnapMirror müssen Sie das Backup 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 in der Detailansicht oder in der Detailansicht der Ressourcengruppe aus.

   Die Topologieseite wird angezeigt.

4. Wählen Sie in der Ansicht Kopien verwalten die Option **Backups** aus den primären oder sekundären (gespiegelten oder replizierten) Speichersystemen aus.
5. Wählen Sie das Backup aus der Tabelle aus, und klicken Sie dann auf  .
6. Gehen Sie auf der Seite Wiederherstellungsumfang wie folgt vor:
   - Bei NFS-Dateisystemen ist standardmäßig **Connect and Copy** Restore ausgewählt. Sie können auch **Volume Revert** oder **Fast Restore** auswählen.
   - Für Dateisysteme, die kein NFS sind, wird der Wiederherstellungsumfang abhängig vom Layout ausgewählt.

     Die neuen Dateien, die nach der Sicherung erstellt wurden, sind nach der Wiederherstellung möglicherweise nicht verfügbar, je nach Typ und Layout des Dateisystems.
7. Geben Sie auf der Seite PreOps die vor der Wiederherstellung ausgeführten Befehle ein, bevor Sie einen Wiederherstellungsjob ausführen.
8. Geben Sie auf der PostOps-Seite Post-Restore-Befehle ein, die nach der Durchführung eines Wiederherstellungsjobs ausgeführt werden sollen.

   Sie sollten überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host unter der Adresse */opt/NetApp/SnapCenter/scc/etc/allowed_commands.config* Pfad verfügbar ist.

9. Wählen Sie auf der Seite Benachrichtigung aus der Dropdown-Liste **E-Mail-Präferenz** die Szenarien aus, in denen Sie die E-Mail-Benachrichtigungen senden möchten.

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail angeben. Wenn Sie den Bericht über den ausgeführten Wiederherstellungsvorgang anhängen möchten, müssen Sie **Job-Bericht anhängen** auswählen.

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

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

    Wenn der Wiederherstellungsvorgang fehlschlägt, wird ein Rollback nicht unterstützt.

    Bei der Wiederherstellung eines Dateisystems, das sich auf der Volume-Gruppe befindet, werden die alten Inhalte im Dateisystem nicht gelöscht. Nur der Inhalt des geklonten Dateisystems wird in das Quelldateisystem kopiert. Dies gilt, wenn mehrere Dateisysteme auf der Volume-Gruppe und standardmäßige NFS-Dateisystemwiederherstellungen vorhanden sind.

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

Überwachen Sie die Wiederherstellungsvorgänge von Unix-Dateisystemen

Sie können den Fortschritt der verschiedenen SnapCenter-Wiederherstellungen über die Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Status nach der Wiederherstellung beschreiben die Bedingungen der Ressource nach einem Wiederherstellungsvorgang und alle weiteren Wiederherstellungsmaßnahmen, die Sie ergreifen können.

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

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

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Monitor**.
2. Klicken Sie auf der Seite **Monitor** auf **Jobs**.
3. Führen Sie auf der Seite **Jobs** die folgenden Schritte aus:
   a. Klicken Sie hier , um die Liste so zu filtern, dass nur Wiederherstellungsvorgänge aufgelistet werden.
   b. Geben Sie das Start- und Enddatum an.
   c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Restore** aus.
   d. Wählen Sie aus der Dropdown-Liste **Status** den Wiederherstellungsstatus aus.
   e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.
4. Wählen Sie den Wiederherstellungsauftrag aus, und klicken Sie dann auf **Details**, um die Jobdetails anzuzeigen.
5. Klicken Sie auf der Seite **Job Details** auf **Protokolle anzeigen**.

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

Klonen von Unix-Dateisystemen

Klonen des Unix Filesystem-Backups

Sie können SnapCenter verwenden, um Unix-Dateisystem mit dem Backup des Dateisystems zu klonen.

Bevor Sie beginnen

- Sie können die Aktualisierung der fstab-Datei überspringen, indem Sie den Wert von *SKIP_FSTAB_UPDATE* auf **true** in der Datei *agent.properties* unter */opt/NetApp/snapcenter/scc/etc* setzen.
- Sie können einen statischen Klon-Volume-Namen und einen Verbindungspfad erhalten, 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 werden der Name des geklonten Volumes und der Verbindungspfad wie <Source_volume_name>_Clone_<Timestamp> sein, aber jetzt wird es <Source_volume_name>_Clone_<Clone_Name> sein

  Dadurch bleibt der Name konstant, so dass Sie die fstab-Datei manuell aktualisieren können, wenn Sie es nicht vorziehen, den fstab von SnapCenter zu aktualisieren.

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 in der Detailansicht oder in der Detailansicht der Ressourcengruppe aus.

   Die Topologieseite wird angezeigt.
4. Wählen Sie in der Ansicht Kopien managen die Backups entweder aus lokalen Kopien (primär), Spiegelkopien (sekundär) oder Vault Kopien (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 durch:

Für dieses Feld…	Tun Sie das…
Klonserver	Standardmäßig wird der Quell-Host befüllt.
Mount-Punkt klonen	Geben Sie den Pfad an, auf den das Dateisystem gemountet werden soll.

7. Führen Sie auf der Seite Skripts die folgenden Schritte aus:
   a. Geben Sie die Befehle für den vor- oder Nachklon ein, die vor oder nach dem Klonvorgang ausgeführt werden sollen.

   > Sie sollten überprüfen, ob die Befehle in der Befehlsliste vorhanden sind, die auf dem Plug-in-Host verfügbar ist, und zwar über den Pfad */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*.

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

   Außerdem müssen Sie die E-Mail-Adressen für Absender und Empfänger sowie den Betreff der E-Mail

angeben. Wenn Sie den Bericht über den ausgeführten Klonvorgang anhängen möchten, wählen Sie **Job-Bericht anhängen** aus.

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

9. Überprüfen Sie die Zusammenfassung und klicken Sie dann auf **Fertig stellen**.
10. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

Teilen Sie einen Klon auf

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

Über diese Aufgabe

- Sie können den Clone-Split-Vorgang nicht für einen Zwischenkon ausführen.

  Wenn Sie beispielsweise Klon1 aus einem Datenbank-Backup erstellen, können Sie eine Sicherung von Klon1 erstellen und dann dieses Backup klonen (Klon2). Nach dem Erstellen von Klon2 ist Klon1 ein Zwischenkon, und Sie können den Klonteilvorgang auf Klon1 nicht ausführen. Sie können jedoch den Vorgang zum Aufteilen von Klonen auf Klon2 durchführen.

  Nach dem Aufteilen von Klon2 können Sie den Clone Split-Vorgang auf Klon1 durchführen, da Klon1 nicht mehr der Zwischenklon ist.

- Wenn Sie einen Klon aufteilen, werden die Backup-Kopien und Klonjobs des Klons gelöscht.
- Informationen zu den Vorgängen für FlexClone-Volume-Split finden Sie unter, "Teilten Sie ein FlexClone Volume vom übergeordneten Volume auf".
- Stellen Sie sicher, dass das Volume oder Aggregat auf dem Storage-System 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 Ansicht aus:

Option	Beschreibung
Für Datenbankapplikationen	Wählen Sie in der Liste Ansicht die Option **Datenbank** aus.
Für File-Systeme	Wählen Sie in der Liste Ansicht **Pfad** aus.

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

   Die Seite „Ressourcentopologie“ wird angezeigt.

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

5. Überprüfen Sie die geschätzte Größe des zu teilenden Klons und den benötigten Speicherplatz auf dem Aggregat, und klicken Sie dann auf **Start**.
6. Überwachen Sie den Fortschritt des Vorgangs, indem Sie auf **Monitor** > **Jobs** klicken.

   Der Clone-Splitvorgang reagiert nicht mehr, wenn der SMCore-Dienst neu gestartet wird. Sie sollten das Cmdlet "Stop-SmJob" ausführen, um den Clone-Split-Vorgang zu beenden, und dann den Clone-Split-Vorgang wiederholen.

   Wenn Sie eine längere Abfragzeit oder kürzere Abfragzeit benötigen, um zu prüfen, ob der Klon geteilt ist oder nicht, können Sie den Wert von *CloneSplitStatusCheckPollTime* Parameter in der Datei *SMCoreServiceHost.exe.config* ändern, um das Zeitintervall für SMCore so einzustellen, dass der Status des Clone Split-Vorgangs angezeigt wird. Der Wert liegt in Millisekunden, und der Standardwert ist 5 Minuten.

   Beispiel:

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

   Der Startvorgang für die Klontrennung schlägt fehl, wenn gerade Backup-, Wiederherstellungs- oder andere Klonsplitonen durchgeführt werden. Sie sollten den Clone Split-Vorgang erst nach Abschluss der laufenden Vorgänge neu starten.

Verwandte Informationen

"Der SnapCenter Klon oder die Überprüfung schlägt fehl, wenn das Aggregat nicht vorhanden ist"

Überwachen Sie die Klonvorgänge von Unix-Dateisystemen

Sie können den Status von SnapCenter-Klonvorgängen mithilfe der Seite Jobs überwachen. Sie können den Fortschritt eines Vorgangs überprüfen, um zu bestimmen, wann dieser abgeschlossen ist oder ob ein Problem vorliegt.

Über diese Aufgabe

Die folgenden Symbole werden auf der Seite Aufträge angezeigt und geben den Status der Operation an:

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

Schritte

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

a. Klicken Sie hier  , um die Liste so zu filtern, dass nur Klonvorgänge aufgelistet werden.
b. Geben Sie das Start- und Enddatum an.
c. Wählen Sie aus der Dropdown-Liste **Typ** die Option **Clone** aus.
d. Wählen Sie aus der Dropdown-Liste **Status** den Klonstatus aus.
e. Klicken Sie auf **Anwenden**, um die Vorgänge anzuzeigen, die erfolgreich abgeschlossen wurden.

4. Wählen Sie den Klon-Job aus, und klicken Sie dann auf **Details**, um die Job-Details anzuzeigen.
5. Klicken Sie auf der Seite Jobdetails auf **Protokolle anzeigen**.